

GESELLSCHAFT
FÜR INFORMATIK



Melanie Volkamer, David Duenas-Cid, Peter B. Rønne,
Peter Y A Ryan, Jurlind Budurushi, Oksana Kulyk,
Adrià Rodriguez Pérez, Iuliia Spycher-Krivososova,
Michael Kirsten, Alexandre Debant and Nicole Goodman
(eds.)

**E-Vote-ID 2023:
Eight International Joint Conference on
Electronic Voting**

**October 3-6, 2023
Luxembourg**

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings

Series of the Gesellschaft für Informatik (GI)

Volume P-347

ISBN 978-3-88579-741-8

ISSN 1617-5468

Volume Editors

Melanie Volkamer, Karlsruhe Institute of Technology, Karlsruhe, Germany

David Duenas-Cid, Kozminski University, Warsaw, Poland

Peter B. Rønne, CNRS, LORIA, Université de Lorraine, Nancy, France

Peter Y A Ryan, University of Luxembourg, Esch-sur-Alzette, Luxembourg

Jurlind Budurushi, Qatar University, Doha, Qatar, and Baden-Wuerttemberg Cooperative
State University Karlsruhe

Oksana Kulyk, IT University of Copenhagen, Copenhagen, Denmark

Adrià Rodriguez Pérez, Pompeu Fabra University, Barcelona, Spain

Iuliia Spycher-Krivososova, University of Bern, Bern, Switzerland

Michael Kirsten, Karlsruhe Institute of Technology, Karlsruhe, Germany

Alexandre Debant, INRIA, Nancy, France

Nicole Goodman, Brock University, St. Catharines, Canada

Series Editorial Board

Andreas Oberweis, KIT Karlsruhe,

(Chairman, andreas.oberweis@kit.edu)

Torsten Brinda, Universität Duisburg-Essen, Germany

Dieter Fellner, Technische Universität Darmstadt, Germany

Ulrich Frank, Universität Duisburg-Essen, Germany

Barbara Hammer, Universität Bielefeld, Germany

Falk Schreiber, Universität Konstanz, Germany

Wolfgang Karl, KIT Karlsruhe, Germany

Michael Koch, Universität der Bundeswehr München, Germany

Heiko Roßnagel, Fraunhofer IAO Stuttgart, Germany

Kurt Schneider, Universität Hannover, Germany

Andreas Thor, HFT Leipzig, Germany

Ingo Timm, Universität Trier, Germany

Karin Vosseberg, Hochschule Bremerhaven, Germany

Maria Wimmer, Universität Koblenz-Landau, Germany

Dissertations

Rüdiger Reischuk, Universität Lübeck, Germany

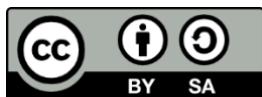
Thematics

Agnes Koschmider, Universität Kiel, Germany

Seminars

Judith Michael, RWTH Aachen, Germany

printed by Köllen Druck+Verlag GmbH, Bonn



This book is licensed under a Creative Commons BY-SA 4.0 licence.

Preface

The Eighth International Joint Conference on Electronic Voting, E-Vote-ID 2023, was held during October 3–6, 2023.

This was the first time the conference was held in Abbey Neumunster, Luxemburg, starting a new era in the conference in which the venue will change annually, and we will engage new audiences and organizers.

The E-Vote-ID Conference resulted from merging EVOTE and Vote-ID and counting up to 19 years since the first E-Vote conference, in Austria. Since the first conference in 2004, over 1600 experts have attended the venue, including scholars, practitioners, representatives of various authorities, electoral managers, vendors, and PhD Students. The conference collected the most relevant debates on the development of Electronic Voting, from aspects relating to security and usability through to practical experiences and applications of voting systems, also including legal, social, or political aspects, amongst others; it has turned out to be an important global referent concerning this issue.

This year, as in previous editions, the conference consisted of:

- Security, Usability, and Technical Issues Track;
- Governance of E-Voting Track;
- Election and Practical Experiences Track;
- PhD Colloquium;
- Poster and Demo Session.

E-VOTE-ID 2023 received 49 submissions for consideration in the first three tracks (Technical, Governance and Practical Tracks). Each submission was reviewed by 3 to 5 program committee members using a double-blind review process. As a result 15 papers were selected from the three tracks to be presented in this volume of Lecture Notes in Informatics (i.e. 31% of the submissions). The selected papers cover a wide range of topics connected with electronic voting, including experiences and revisions of the actual uses of E-voting systems and corresponding processes in elections.

We would like to thank the local chair, Peter Y A Ryan, and the local event organizer Magali Martin from the University of Luxembourg and the Interdisciplinary Centre for Security, Reliability, and Trust (SnT). Especially, we thank SnT for sponsoring in kind. Thanks also goes to the Ministry of Economy for financial support and a very special thanks go to the Luxembourg National Research Fund (FNR), which supported this conference generously via the FNR RESCOM scientific event grant. Also, we would like to thank and appreciate the international program members for their hard work in reviewing, discussing, and shepherding papers. They ensured, once again, the high quality of this proceedings with their knowledge, expertise and experience.

PhD Colloquium

The PhD Colloquium was chaired by

- Debant, Alexandre (INRIA, France)
- Goodman, Nicole (Brock University)

The goal of the colloquium is to foster the understanding and academic quality of PhD students' contributions in collaboration with senior researchers in the field. Further, the collaboration between PhD students from various disciplines working on e-voting is supported. The programme allowed for plenty of space for discussions.

The PhD colloquium took place on October 3, 2023, and featured six presentations

- “An encryption mechanism for receipt-free and perfectly private verifiable elections” by Thi Van Thao Doan.
- “Secure Post-Quantum E-Voting from the Hardness of Codes” by Rafieh Mosaheb.
- “Publicly Auditable Yet Private Electoral Rolls” by Prashant Agrawal.
- “Verification and Modelling of Polish Postal Voting” by Yan Kim.
- “Digitizing election issues. The history of voting technologies in Kenya (2002-2017)” by Cecilia Passanti.
- “Is electronic voting posing a "wicked problem"?” by Märt Pöder

The best presentation award went to by Rafieh Mosaheb for “Secure Post-Quantum E-Voting from the Hardness of Codes”.

The Demo and Poster Session

The Demo and Poster Session was chaired by

- Kirsten, Michael (Karlsruhe Institute of Technology, Germany)

This session allows for both posters depicting new ideas or approaches that should be discussed with the community or summarizing papers published at other venues but which are important for the E-Vote-ID community to know and to discuss, but also allows for demonstrations of electronic voting systems or parts thereof.

At E-Vote-ID 2023 the following posters were accepted

- “Proof of Work and Secure Element in Electronic Voting” by Vitaly Zuevsky
- “Ordinos: Remote Verifiable Tally-Hiding E-Voting - A Fully-Fledged Web-Based Implementation” by Julian Liedtke, Jan Adomat, Alexander Aßenmacher, Patrick Baisch, Linus Fischer, Jonas Geiselhart, Alex Heller, Julian Kieslinger, Mike Lauer, Paul Mayer, Xuan Viet Pham, André Sperrle, Carmen Wabartha, Pia Wippermann and Ralf Kuesters
- “PeaceFounder: e-voting by pseudonym braiding” by Janis Erdmanis
- “Solving the Electronic Voting Dilemma: The BallotBox™ Method and System” by Cesar Correa Parker and Josefina Correa Gutierrez
- “Soteria Online Voting Use Case” by Aleix Amill, Jordi Cucurull and Polina Toropova
- “No Cryptography Skills Required - Building a zk Voting App using Typescript” by Philip Kelly and Florian Kluge
- “Time-lock cryptographic protocols” by Najmeh Soroush and the azkr.org working group
- “Cast-as-intended verifiability with a second device” by Tobias Hilt, Tomasz Truderung, Margarita Udovychenko and Melanie Volkamer
- “Selene Web Application” by Aditya Damodaran, Peter B. Rønne, Peter Y. A. Ryan and Marie-Laure Zollinger

Luxembourg, July 2024

Melanie Volkamer, David Duenas-Cid, Peter B. Rønne, Peter Y A Ryan, Jurlind Budurushi, Oksana Kulyk, Adrià Rodríguez Pérez, Iuliia Spycher-Krivososova, Thomas Hofer, Beata Martin-Rozumilowicz, Michael Kirsten, Alexandre Debant and Nicole Goodman (chairs)

Sponsors

We would like to express our gratitude to the following for financial support of the conference

Ministry of Economy of Luxembourg

Luxembourg National Research Fund



Committees

General Chairs:	Melanie Volkamer, Karlsruhe Institute of Technology David Duenas-Cid, Kozminski University Peter B. Rønne, Université de Lorraine, CNRS
Track Chairs:	Security, Usability, and Technical Issues Melanie Volkamer, Karlsruhe Institute of Technology Jurlind Budurushi, Qatar University Oksana Kulyk, ITU Governance Issues Iuliia Spycher, University of Bern Adrià Rodriguez, Universitat Pompeu Fabra Election and Practical Experiences Thomas Hofer, Objectif Sécurité Beata Martin-Rozumilowicz, Independent Expert
Poster and Demo Session:	Michael Kirsten, Karlsruhe Institute of Technology
PhD Colloquium:	Alexandre Debant, INRIA Nicole Goodman, Brock University

Programme Committee

Security, Usability, and Technical Issues

Roberto Araujo	Universidade Federal do Pará (UFPA)
Bernhard Beckert	Karlsruhe Institute of Technology
Josh Benaloh	Microsoft
Matthew Bernhard	Voting Works
Michelle Blom	The University of Melbourne
Jeremy Clark	Concordia Institute
César Collazos	Universidad del Cauca
Veronique Cortier	Centre National de la Recherche Scientifique, Loria
Catalin Dragan	University of Surrey
Aleksander Essex	University of Western Ontario
Bryan Ford	École polytechnique fédérale de Lausanne
David Galindo	Crypto in Motion
J Paul Gibson	Mines Telecom
Rosario Giustolisi	IT University of Copenhagen
Kristian Gjøsteen	Norwegian University of Science and Technology
Rajeev Gore	The Australian National University
Ruediger Grimm	University of Koblenz

Rolf Haenni	Bern University of Applied Sciences
Thomas Haines	Queensland University of Technology
Feng Hao	The University of Warwick
Bart Jacobs	Radboud University
Wojciech Jamroga	Polish Academy of Sciences
Michael Kirsten	Karlsruhe Institute of Technology (KIT)
Reto Koenig Bern	University of Applied Sciences
Oksana Kulyk	IT University of Copenhagen
Ralf Küsters	University of Stuttgart
Andreas Mayer	Hochschule Heilbronn
Johannes Mueller	University of Luxembourg
Stephan Neumann	Landesbank Saar
Olivier Pereira	Université catholique de Louvain
Pascal Reisert	University of Stuttgart
Karen Renaud	University of Strathclyde
Stefan Roseman	Federal Office for Information Security
David Ruescas	Sequent
Peter Y. A. Ryan	University of Luxembourg
Mark Ryan	University of Birmingham
Steve Schneider	University of Surrey
Berry Schoenmakers	Eindhoven University of Technology
Carsten Schuermann	IT University of Copenhagen
Tjrerand Silde	Norwegian University of Science and Technology
Philip Stark	University of California at Berkeley
Ewa Syta	Yale University
Vanessa Teague	Thinking Cybersecurity
Tomasz Truderung	Polyas
Damjan Vukcevic	The University of Melbourne
Roland Wen	The University of New South Wales
Jan Willemsen	Cybernetica
Filip Zagorski	University of Wroclaw

Governance Issues

Marta Aranyossy Corvinus	University of Budapest
Jordi Barrat i Esteve	eVoting Legal Lab
Régis Dandoy Universidad	San Francisco de Quito
Rosa María Fernández Riveira	Universidad Complutense de Madrid
Micha Germann	University of Bath
Norbert Kersting	University of Munster
Leontine Loeber	University of East Anglia
Jon Pammett	Carleton University
Ismael Peña-López	Universitat Oberta de Catalunya
Carolina Plescia	University of Vienna
Rodney Smith	The University of Sydney
Mikhel Solvak	University of Tartu
Siim Trumm	University of Nottingham
Felix-Christopher von Nostitz	Université Catholique de Lille

Election and Practical Experiences

David Bismark	Votato
Christian Bull	Ministry of Local Gov. and Regio. Development, NOR
Susanne Caarls	Election Consultant
Gianpiero Catozzi	UNDP
Thomas Chanussot	IFES
Tarun Chaudhary	IFES
Philipp Egger	Staatskanzlei Kanton St.Gallen
Joshua Franklin	National Institute of Standards and Technology
Olivier Leclère	State of Geneva
Leontine Loeber	University of East Anglia
Ryan Macias	rsm election solutions
Ardita Maurer	Zentrum für Demokratie Aarau/Zurich University
Ronan McDermott	mcdis
Vladimir Misev	OSCE/ODIHR
Liisa Past	Ministry of Economic Affairs and Comm., Estonia
Goran Petrov	OSCE/ODIHR
Stéphanie Plante	University of Ottawa
Oliver Spycher	Swiss Federal Chancellery
Kåre Vollan	Quality AS
Gregor Wenda	BMI
Peter Wolf	IDEA
Michael Yard	IFES

Organisation team

Magali Martin	University of Luxembourg
---------------	--------------------------

Inhaltsverzeichnis

Tracks

Track 1: Security, Usability and Technical Issues

David Pointcheval <i>Linearly-Homomorphic Signatures for Short Randomizable Proofs of Subset Membership</i>	19
Rolf Haenni, Ilona Starý Kořánová <i>An Alternative Group for Applications of ElGamal in Cryptographic Protocols</i>	39
Diego F. Aranha, Michele Battagliola, Lawrence Roy <i>Faster coercion-resistant e-voting by encrypted sorting</i>	53
M. Bitussi, R. Longo, F. Antonio Marino, U. Morelli, A. Sharif, C. Spadafora, A. Tomasi <i>Coercion-resistant i-voting with short PIN and OAuth 2.0</i>	71

Track 2: Governance Issues

Yannick Erb, David Duenas-Cid, Melanie Volkamer <i>Identifying Factors Studied for Voter Trust in E-Voting - Review of Literature</i>	93
Radu Antonio Serrano Iova <i>Pitfalls at the Starting Line: Moldova's IVS Pilot</i>	119
David Duenas-Cid, Leontine Loeber, Beata Martin-Rozumilowicz, Ryan Macias <i>Trust Frameworks in Application to Technology in Elections</i>	125
Adrià Rodríguez-Pérez, Núria Costa, Tamara Finogina <i>Regulating for the “known unknowns” in i-voting: quantum computing and long-term privacy</i>	143

Track 3: Election and Practical Experiences

Olivier Esseiva, Audhild Høgåsen, Xavier Monnat
Improving the Swiss Post Voting System 169

Véronique Cortier, Pierrick Gaudry, Stéphane Glondou, Sylvain Ruhault
French 2022 legislatives elections: a verifiability experiment 189

Tobias Hilt, Kati Sein, Tanel Mällo, Jan Willemson, Melanie Volkamer
Voter Perception of Cast-as-Intended Verifiability 203

Tobias Hilt, Oksana Kulyk, Melanie Volkamer
German Social Elections in 2023: An Overview and first Analysis 221

Amanda K. Glazer, Jacob V. Spertus, Philip B. Stark
Stylish Risk-Limiting Audits in Practice 239

Oliver Spycher
Swiss Online Voting Redesigned 255

Adrià Rodríguez-Pérez, Jordi Barrat Esteve
Setting international standards on digital election technologies: mapping trends and stakeholders 263

Index of Authors

Tracks

Track 1: Security, Usability and Technical Issues

Linearly-Homomorphic Signatures for Short Randomizable Proofs of Subset Membership

David Pointcheval¹

Abstract: Electronic voting is one of the most interesting application of modern cryptography, as it involves many innovative tools (such as homomorphic public-key encryption, non-interactive zero-knowledge proofs, and distributed cryptography) to guarantee several *a priori* contradictory security properties: the integrity of the tally and the privacy of the individual votes. While many efficient solutions exist for *honest-but-curious* voters, that follow the official procedure but try to learn more than just the public result, preventing attacks from *malicious* voters is much more complex: when voters may have incentive to send biased ballots, the privacy of the ballots is much harder to satisfy, whereas this is the crucial security property for electronic voting.

We present a new technique to prove that an ElGamal ciphertext contains a message from a specific subset (quasi-adaptive NIZK of subset membership), using linearly-homomorphic signatures. The proofs are both quite efficient to generate, allowing the use of low-power devices to vote, and randomizable, which is important for the strong receipt-freeness property. They are well-suited to prevent vote-selling and replay attacks, which are the main threats against the privacy in electronic voting, with security proofs in the generic group model and the random oracle model.

Keywords: E-voting, non-interactive zero-knowledge proofs

1 Introduction

With the all-digital society, and more recently with the pandemic and multiple lock-down periods, democracy is moving towards remote electronic voting, *a.k.a.* internet voting. Several solutions have been developed that all encrypt the ballot on the voter-side to guarantee the voter's privacy. Thereafter, two major approaches exist for counting the tally, according to the complexity of the election: either one applies a mixing-network (mixnet), which permutes and randomizes the encrypted ballots, before decryption of all the individual ballots to perform the counting in the clear, as one does with paper-based voting systems when one opens the envelopes after having mixed them to remove any link with the voters; or one uses homomorphic encryption that allows to aggregate the encrypted ballots to get the encrypted tally, that is the unique value eventually decrypted. The latter approach is definitely the most appropriate for electronic voting, when the tally just consists in ranking the candidates w.r.t. their number of votes, as it allows a fast publication of the results, while mixing the ballots in a verifiable way is time-consuming for large scale elections. We will thus target this approach in the following, with the ElGamal encryption scheme.

¹ DIENS, École normale supérieure, CNRS, Inria, PSL University, Paris, France david.pointcheval@ens.fr

Replay Attacks and Vote-Selling. However, privacy is more complex than it appears: simple encryption is indeed fine when all the voters are honest, and really cast their intended votes following the official procedure. But voters might deviate from the honest behavior, for multiple reasons. Some might even be ready to change their votes for money or to break privacy. Then, more advanced protections have to be considered, to really achieve a high privacy level. For example, as explained by Cortier and Smyth [CS11], if a coalition of voters really wants to know Alice's vote, they can duplicate her encrypted ballot and cast it in their names. Indeed, contrarily to paper-based vote, cloning Alice's vote is usually trivial in electronic voting, as encrypted ballots are stored in the ballot-box, and should be public for verifiability. Therefore, if they are enough people, the bias in the final tally will reveal Alice's vote. The impact of such an attack has been analyzed in [MMR22], and it can be devastating. To avoid such an attack (called the CS-attack), the ballot-box can simply exclude multiple identical votes, but this is under the assumption that one cannot modify Alice's encrypted ballot without altering the content. This requires some non-malleability.

Vote-selling is another major threat, when some voters may have strong incentive (with a reward or external pressures) to vote for someone when being able to prove it later on. Actually, any technique that encrypts the ballot on the client-side, without any modification before storing it in the public ballot-box, is subject to vote-selling attacks, and even at high scale: the client-side code can always be patched in order to reveal the randomness used during encryption, as a receipt to convince anybody of the content of the vote. Similarly to the Benaloh challenge, where the randomness used during encryption is given to the voter to let him verify the *cast-as-intended*, this randomness is indeed enough to prove the content of the ballot sent and stored in the ballot-box to any other party. To avoid vote-selling (called VS-attack), encrypted ballots must be randomized before storage, which needs them to be malleable. This shows how electronic voting makes *a priori* contradictory requirements. In the literature, receipt-freeness prevents VS-attacks, while strong receipt-freeness prevents both VS-attacks and CS-attacks [Ch16, CFL19].

Randomizable Encryption. The usual approach to get receipt-freeness, without additional interactions, is thus to let the voter encrypt his choice with a randomizable encryption scheme, so that the ballot-box can randomize it before storage/publication. This is possible with the ElGamal encryption scheme. But the voter needs the guarantee that the ballot-box cannot alter his vote.

Signatures on randomizable ciphertexts [B111] was the first attempt to provide non-interactive receipt-freeness: the voter signs (using the Waters signature [Wa05]) his encrypted vote (under ElGamal encryption), and just sends it; then the ballot-box can randomize the ciphertext and adapt the signature, without being able to alter the plaintext. But because of the randomizability of the ballot, it does not preclude CS-attacks. This approach has been improved in [Ch16, CFL19], with an RCCA-secure encryption scheme, providing the strong receipt-freeness: the voter does not have any receipt to sell his vote and the ballot cannot be replayed without being detectable, with an additional proof of knowledge generated by the voter.

Instead of combining ElGamal encryption with Waters signature, [DPP22] uses the one-time Linearly-Homomorphic Signature (OT-LH-Sign) from [Li13] to get a more efficient instantiation, with Traceable-CCA security. This notion of signature has also been analyzed in [BF20]. We will use a more compact OT-LH-Sign, consisting of a unique group element [HPP20], in the slightly stronger generic bilinear group model (GGM) and algebraic group model (AGM).

Non-Interactive Zero-Knowledge Proofs. But this approach, with randomization of the ballots, is more complex in the homomorphic case, where only the aggregated tally is decrypted. In such a situation, ballots are never decrypted and cannot be individually checked in the clear, whereas a unique fake ballot can make the entire election meaningless. To make them verifiable, in their encrypted form, non-interactive zero-knowledge proofs (NIZKs) are required, to prove some specific properties are satisfied by the text in the clear, without revealing any additional information.

Let us first consider a classical setting: a 1-out-of- N choice (either the choice of one candidate, or one list, among N possibilities). To allow homomorphic tally, one usually encodes the vote into N concatenated bits b_i : $\vec{M} = (b_i)_i \in \mathbb{Z}_p^N$. The vote \vec{M} is then encrypted in a component-wise manner, and one proves $b_i \in \{0, 1\}$, for $i = 1, \dots, N$, and $\sum b_i = 1$. Such a validity proof is linear in N , for both the size and the generation time. An alternative proof can be $\vec{M} \in \mathcal{S} = \{\vec{V}_1, \dots, \vec{V}_N\} \subseteq \mathbb{Z}_p^N$, where \vec{V}_i is the vote for candidate i ($b_i = 1$, and all other values are 0, to allow homomorphic encrypted tally): this is a unique proof of N -subset membership. More proofs of subset membership, on $\mathbf{A}_k \cdot \vec{M} \in \mathcal{S}_k$ for multiple matrices \mathbf{A}_k , can be combined to encompass more complex elections, thanks to the linear property of the encryption scheme. NIZKs of subset membership are the core of homomorphic voting systems, and the main goal of this work.

Such NIZKs exist on ElGamal ciphertexts in groups \mathbb{G} , where the Diffie-Hellman assumption holds, or \mathbb{Z}_p , when working in the exponents. The most famous use the Fiat-Shamir paradigm on Schnorr-like proofs, to prove disjunctions (OR-proofs). It makes the ballot non-malleable, which helps to exclude CS-attacks but, on the other hand, this is in favor of VS-attacks. The Groth-Sahai methodology [GS08] provides another approach for non-interactive zero-knowledge proofs, that are randomizable, but this is at a very high computational cost (see [Ch16] for simple 0-1 proofs), which is not reasonable on low-power devices. Most importantly, both previous techniques lead to proofs that have a size and a generation-time linear in the size of the subset \mathcal{S} . On the other hand, recent SNARGs (or SNARKs), for *Succinct Non-Interactive Arguments (of Knowledge)* [Pa13, Ge13, Bo16, Gr16], and their zero-knowledge variants, lead to quite efficient proofs for algebraic circuits. However, they suffer two main drawbacks in the setting of electronic voting: (i) while the resulting proofs are quite short and fast to verify, their generation by the prover depends on the complexity of the algebraic circuit. And statements to be proven (as listed above, and in particular disjunctions such as range proofs or proofs of subset membership) lead to quite large algebraic circuits: proof generation-time might get quite high (at least linear in the size of the set \mathcal{S}); (ii) the SNARGs methodology requires a complex Common Reference String

(CRS). This is a structured tuple that must be generated in a trusted way. Because of the complex structure, it is quite hard to distribute the generation among the electoral board members, and it is not verifiable. Such an approach has been proposed in [Le19], using the Groth16 proofs [Gr16], which require a CRS with successive powers and inverses (that are inefficient to distribute) applied on group elements. Without distributed generation, this excludes the fundamental assumption in electronic voting: one only trusts the electoral board as a whole, not any individual party.

Contributions. We exploit linearly-homomorphic signatures [Li13, HPP20, HP22, DPP22] to design short and efficient homomorphic quasi-adaptive NIZKs of subset membership on ElGamal ciphertexts, where quasi-adaptive means that the CRS (or the setup) depends on the subset [JR13, KW15]. But contrarily to all the previous methods presented above, that were using signatures on randomizable ciphertexts just for allowing randomization on the server-side, and thus for achieving (strong) receipt-freeness for a mixnet-based system, we additionally use them on the client-side, from multiple signatures generated at the setup phase, by the electoral board, to derive efficient proofs of valid ballots. This can be seen in the same vein as [CFL19], with initial signatures on randomized ballots, but that paper only focused on the cast-as-intended property, and not the validity proof of the ballots, with a costly signature on randomizable ciphertexts, that cannot scale for elections with complex ballots. Our NIZK of subset membership (which is also a signature) has a constant size and takes a constant-time for generation on the voter device, whatever the size of the subset. We stress that when the signing keys and the initial signatures can be efficiently generated in a distributed way, this avoids the need of a trusted third party.

In order to get signatures on randomizable ciphertexts with unlinkability, from linearly-homomorphic signatures (LH-Sign) on ElGamal ciphertexts, we need *full-fledge* LH-Sign with tags [Li13, KW15], to have multiple vector sub-spaces, that cannot be combined. We also need randomizable tags to make signatures unlinkable, whichever is the vector sub-space: Hence, we use Linearly-Homomorphic Signatures with Randomizable Tags (LH-Sign-RTag), where the tags target the vector sub-spaces, but still being randomizable and unlinkable, as in [FHS19, HPP20, HP22], in order to keep privacy of the ciphertexts. Signatures for proofs can only be generated for valid ballots, without revealing any information about the votes.

Our contribution is thus the use of LH-Sign-RTag [FHS19, HPP20, HP22] in order to build efficient quasi-adaptive NIZKs of subset membership that are randomizable: they have constant generation-time and constant proof-size. This approach excludes VS-attacks and is compatible with the other improvements [Ch16, CFL19, DPP22]. In particular, the voter can use a one-time linearly-homomorphic signature (OT-LH-Sign) to trace and check his vote after randomization, and append a single Groth-Sahai Diffie-Hellman proof to avoid CS-attacks. This provides strong receipt-freeness. We furthermore finely-tune the SDH-based LH-Sign-RTag [HPP20, HP22] to avoid any unique trusted party, which is hard to obtain with any other similar approach.

Technical Overview. Let us first briefly explain the global idea for proving an ElGamal ciphertext $(C_0 = r \cdot P, \vec{C} = \vec{M} + r \cdot \vec{Z}) \in \mathbb{G}^{n+1}$ actually encrypts a plaintext $\vec{M} \in \mathcal{S} \subset \mathbb{G}^n$, under the encryption key $\vec{Z} \in \mathbb{G}^n$, where $\mathbb{G} = \langle P \rangle$ is a group spanned by a generator P , where the Diffie-Hellman assumption holds.

Thereafter, by applying a matrix \mathbf{A}_k on the second part of the ciphertext (C_0, \vec{C}) : $\vec{C}' = \mathbf{A}_k \cdot \vec{C} = \mathbf{A}_k \cdot \vec{M} + r \cdot \mathbf{A}_k \cdot \vec{Z}$, one can see (C_0, \vec{C}') as a ciphertext of $\vec{M}' = \mathbf{A}_k \cdot \vec{M}$ under the encryption key $\vec{Z}' = \mathbf{A}_k \cdot \vec{Z}$. The matrix \mathbf{A}_k can be a projection (to focus on some part of the vector) or an aggregation (to sum some components of the vector). Hence, the subset \mathcal{S} can be $\{0 \cdot P, 1 \cdot P\} \subset \mathbb{G}^1$, a larger range $\{0 \cdot P, \dots, k \cdot P\} \subset \mathbb{G}^1$, or any list of vectors $\{\vec{M}_1, \dots, \vec{M}_N\} \subset \mathbb{G}^n$ that specifies the admissible aggregations/sums. Multiple proofs can be combined, thanks to their high efficiency.

Let us target on one proof of subset membership, and thus on the set $\mathcal{S} = \{\vec{M}_1, \dots, \vec{M}_N\}$. The authority first generates LH-Sign-RTag signatures under a verification key VK: $\Sigma_{i,0}$ on $(P_S, 0, \vec{M}_i)$ and $\Sigma_{i,1}$ on $(0, P, \vec{Z})$, under the common tag τ_i , for $i = 1, \dots, N$. The first component P_S is a fixed group element that depends on the set \mathcal{S} . It can be set as $P_S = \mathcal{H}(\mathcal{S})$ where the function \mathcal{H} is assumed to be a full-domain hash function that outputs independent group elements for any new query (modelled as a random oracle onto \mathbb{G}). For a choice j , a random combination of the two signatures leads to a valid signature under VK on a ciphertext of $\vec{M} = \vec{M}_j$: $\Sigma_0 = \Sigma_{j,0} + r \cdot \Sigma_{j,1}$ is a valid signature on $(P_S, C_0 = r \cdot P, \vec{C} = r \cdot \vec{Z} + \vec{M}_j) = (P_S, 0, \vec{M}_j) + r \cdot (0, P, \vec{Z})$ under $\tau = \tau_j$. Note that the first components P_S and 0, later checked with respect to P_S for Σ_0 , imply the coefficient 1 on $(P_S, 0, \vec{M}_j)$ in the combination. We stress that without tags, one could not prevent someone to encrypt $(K+1) \cdot \vec{M}_1 - K \cdot \vec{M}_2$, for any K of its choice, which is not considered a legitimate ciphertext. One also keeps $\Sigma_1 = \Sigma_{j,1}$ as a valid signature on the *randomizer* $(0, D_0 = P, \vec{D} = \vec{Z})$ under the tag $\tau = \tau_j$, for further randomization.

We have dropped the index j in the signatures (Σ_0, Σ_1) and the tag τ , as there is a unique pair of ciphertexts that remains: $\mathcal{C} = (C_0, \vec{C})$ of \vec{M}_j and $\mathcal{D} = (D_0, \vec{D})$ of $\vec{0}$. They do not reveal information about j , under the DDH assumption (ElGamal encryption), but the signatures (Σ_0, Σ_1) are valid under τ_j only, which reveals j . Hence the need of randomizable tags to make the final tag τ and the signatures (Σ_0, Σ_1) unlinkable to τ_j , and thus independent from the choice j .

Linearly-Homomorphic Signature with Randomizable Tags. The rest of the paper will explain how to modify the above $(\mathcal{C}, \mathcal{D})$ and $(\Sigma_0, \Sigma_1, \tau)$ before sending them in order to keep vote-privacy, using the randomizable tags. There are two LH-Sign-RTag candidates in the literature.

First, the FHS signature [FHS19], in a type III pairing-friendly setting $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p, P, \hat{P}, e)$, also presented as a signature on randomizable ciphertexts [BF20]: a tag is $\tau = (\tau_1 = 1/t \cdot P, \tau_2 = 1/t \cdot \hat{P})$, for a scalar $t \xleftarrow{\$} \mathbb{Z}_p$, the signature of $\vec{M} = (M_k) \in \mathbb{G}^n$ is $\Sigma =$

$t \cdot (\sum s_k \cdot M_k) \in \mathbb{G}$, under $\text{VK} = (\hat{P}_k = s_k \cdot \hat{P})_k$, that can both be verified by $e(P, \tau_2) = e(\tau_1, \hat{P})$ and $e(\Sigma, \tau_2) = \prod e(M_k, \hat{P}_k)$. One can easily randomize τ and adapt the signature Σ , in a perfectly unlinkable way. Hence, the privacy relies on the ElGamal encryption scheme only. From a CRS of linear length in the size of the subset S (with the $(\Sigma_{i,0}, \Sigma_{i,1}, \tau_i)_i$ for all the $\vec{M}_i \in S$), proofs of subset membership are thereafter both size and time efficient (independent of the size of S) as the voter only has to generate $C = (C_0, \vec{C})$ for appropriate choice \vec{M}_j , and to randomize $(\Sigma_0, \Sigma_1, \tau) \in \mathbb{G}^3 \times \hat{\mathbb{G}}$, keeping $\mathcal{D} = (P, \vec{Z})$ unchanged. As the tags are self-verifiable (without any additional proof) signatures are very compact.

While the CRS has a similar size to the one for SNARGs (linear in the size of the algebraic circuit), SNARGs also have a linear generation-time of the proof, whereas ours is constant-time. Unfortunately, the setup that generates the CRS suffers the same drawback of being hard to distribute, because of the modular inverses to be computed. Hence, in the following, we consider the second LH-Sign-RTag candidate, with Square Diffie-Hellman tags $\tau = (P, t \cdot P, t^2 \cdot P)$, for $t \xleftarrow{\$} \mathbb{Z}_p$ [HPP20, HP22]. The tags will need additional proofs to be verifiable, but the CRS can be efficiently generated in a distributed way.

2 Preliminaries

Computational Assumptions. Our security analysis will be performed in the Generic Group Model (GGM) and the Algebraic Group Model (AGM) [FKL18], where the adversary can only make generic operations on the group (and pairing evaluations). Hence, any new generated group element comes as a linear combination of the input group elements. The former GGM is a slightly stronger model than the latter AGM, as encodings of group elements can even be chosen at random. But in both cases, any group element provided by the adversary comes with the explicit coefficients of the linear combination of the input elements. This will provide the simulation extractability of our proofs. We will use the following classical assumptions in a group \mathbb{G} of prime order p , for any $P \in \mathbb{G}$:

Discrete Logarithm (DL) Assumption. Given $(P, U = x \cdot P)$, for $x \xleftarrow{\$} \mathbb{Z}_p$, it is computationally hard to recover x ;

Decisional Diffie-Hellman (DDH) Assumption. For $U \xleftarrow{\$} \mathbb{G}$ and $x, y \xleftarrow{\$} \mathbb{Z}_p$, distributions $\mathcal{D}_{\text{dh}} = \{(P, x \cdot P, U, x \cdot U)\}$ and $\mathbb{G}_{\mathbb{S}}^4 = \{(P, x \cdot P, U, y \cdot U)\}$ are computationally hard to distinguish;

Square Discrete Logarithm (SDL) Assumption. Given $(P, U = x \cdot P, V = x^2 \cdot P)$, for $x \xleftarrow{\$} \mathbb{Z}_p$, it is computationally hard to recover x ;

Decisional Square Diffie-Hellman (DSDH) Assumption. For $x, y \xleftarrow{\$} \mathbb{Z}_p$, distributions $\mathcal{D}_{\text{sdh}} = \{(P, x \cdot P, x^2 \cdot P)\}$ and $\mathbb{G}_{\mathbb{S}}^3 = \{(P, x \cdot P, y \cdot P)\}$ are computationally hard to distinguish.

The SXDH assumption claims that the DDH assumption holds in both groups \mathbb{G} and $\hat{\mathbb{G}}$, when we are in a type III pairing-friendly setting $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p, P, \hat{P}, e)$, with e a bilinear map from $\mathbb{G} \times \hat{\mathbb{G}}$ into the target group \mathbb{G}_T .

Groth-Sahai Proofs. The Groth-Sahai methodology [GS08] is well-known for zero-knowledge and randomizable proofs of pairing-product relations. It is not appropriate for complex relations, but efficient enough for short statements, such as Diffie-Hellman tuples $(H, U = t \cdot H, R, V = t \cdot R) \in \mathbb{G}^4$, or SDH tuples: one defines the CRS as a random tuple $(\hat{V}_{1,1}, \hat{V}_{1,2}, \hat{V}_{2,1}, \hat{V}_{2,2}) \in \hat{\mathbb{G}}^4$, likely a non-Diffie-Hellman tuple.

From the witness $t \in \mathbb{Z}_p$, one commits it, for $\mu \xleftarrow{\$} \mathbb{Z}_p$:

$$\text{com} = (\hat{C} = t \cdot \hat{V}_{2,1} + \mu \cdot \hat{V}_{1,1}, \hat{D} = t \cdot \hat{V}_{2,2} + \mu \cdot \hat{V}_{1,2}),$$

and sets $\Theta = \mu \cdot H$ and $\Psi = \mu \cdot R$, which satisfy

$$\begin{aligned} e(H, \hat{C}) &= e(U, \hat{V}_{2,1}) \cdot e(\Theta, \hat{V}_{1,1}), & e(H, \hat{D}) &= e(U, \hat{V}_{2,2}) \cdot e(\Theta, \hat{V}_{1,2}), \\ e(R, \hat{C}) &= e(V, \hat{V}_{2,1}) \cdot e(\Psi, \hat{V}_{1,1}), & e(R, \hat{D}) &= e(V, \hat{V}_{2,2}) \cdot e(\Psi, \hat{V}_{1,2}). \end{aligned}$$

The proof is thus $\text{proof} = (\Theta, \Psi) \in \mathbb{G}^2$, on the tuple (H, U, R, V) and the commitment $\text{com} = (\hat{C}, \hat{D})$. To verify it, instead of checking the four equations independently, which require 12 pairing evaluations, one can apply a batch verification [B110] which just consists of 3 pairing evaluations. The soundness is perfect, while the zero-knowledge property relies on the SXDH assumption.

SDH Tags and Properties. We first recall some properties for the SDH tuples: the unlinkability and the non-miscibility studied in [HPP20, Full version]. As shown in [HPP20, HP22], the DSDH and the DDH assumptions imply the unlinkability of two SDH tuples. Furthermore, under the SDL assumption, SDH tuples with different scalars cannot be mixed under known linear combinations:

Proposition 1 (Unlinkability) *For any $P \in \mathbb{G}$, the DDH and DSDH assumptions imply the indistinguishability of \mathcal{D}_0 and \mathcal{D}_1 , whith $U \xleftarrow{\$} \mathbb{G}$, $x, y \xleftarrow{\$} \mathbb{Z}_p$:*

$$\mathcal{D}_0 = \{(P, x \cdot P, x^2 \cdot P, U, x \cdot U, x^2 \cdot U)\} \quad \mathcal{D}_1 = \{(P, x \cdot P, x^2 \cdot P, U, y \cdot U, y^2 \cdot U)\}$$

Proposition 2 (Non-Miscibility) *Given n SDH tuples $(P, U_i = x_i \cdot P, V_i = x_i \cdot U_i)$, for any generator P , but random $x_i \xleftarrow{\$} \mathbb{Z}_p$, outputting $(\alpha_i)_{i=1, \dots, n}$ such that $(H = \sum \alpha_i \cdot P, U = \sum \alpha_i \cdot U_i, V = \sum \alpha_i \cdot V_i)$ is an SDH tuple, with at least two non-zero coefficients α_i , is computationally hard under the SDL assumption.*

However, verifying an SDH tuple requires an additional proof, which can be done with the above Groth-Sahai methodology, with the CRS $(\hat{V}_{1,1}, \hat{V}_{1,2}, \hat{V}_{2,1}, \hat{V}_{2,2})$. Given an SDH

tuple $(H, U = x \cdot H, V = x \cdot U)$ in \mathbb{G} , knowing the witness $x \in \mathbb{Z}_p$, one first commits it, for a random $v \xleftarrow{\$} \mathbb{Z}_p$: $\text{com} = (\hat{C} = x \cdot \hat{V}_{2,1} + v \cdot \hat{V}_{1,1}, \hat{D} = x \cdot \hat{V}_{2,2} + v \cdot \hat{V}_{1,2})$, and one sets $\text{proof} = (\Theta = v \cdot H, \Psi = v \cdot U)$, which satisfies the four above equalities, where $R = U$. This proven tuple $(\vec{\tau} = (H, U, V), \text{com} = (\hat{C}, \hat{D}), \text{proof} = (\Theta, \Psi))$, which consists of 5 elements in \mathbb{G} and 2 elements in $\hat{\mathbb{G}}$, is randomizable: one can publicly update H in both $\vec{\tau}$ and proof (with a chosen multiplicative factor), and v in both com and proof (without knowing it, but just the additional value v'), making the new proven tuple unlinkable to the initial one, from the unlinkability of the tuples and the zero-knowledge property of the proof.

But for correct combinations, we need a stricter notion of equivalent (valid) tags.

Definition 1 (Equivalent SDH Tags) *An SDH tag will be a tuple $\text{Tag} = (\vec{\tau}, \text{proof}, \text{com})$, with valid proof, and two tags will be said equivalent if they not only are for the same scalar x , but also for the same commitment com .*

Proposition 3 (Linearity) *Given n equivalent SDH tags, with $\vec{\tau}_i = (H_i, U_i = x \cdot H_i, V_i = x^2 \cdot H_i)$, for the same $x \in \mathbb{Z}_p$, their proofs $\text{proof}_i = (\Theta_i = v \cdot H_i, \Psi_i = v \cdot U_i)$, for the same v , and thus the common commitment $\text{com} = (\hat{C} = x \cdot \hat{V}_{2,1} + v \cdot \hat{V}_{1,1}, \hat{D} = x \cdot \hat{V}_{2,2} + v \cdot \hat{V}_{1,2})$, for any linear combination $\vec{\tau} = \sum \alpha_i \cdot \vec{\tau}_i$, $\text{proof} = (\Theta = \sum \alpha_i \cdot \Theta_i, \Psi = \sum \alpha_i \cdot \Psi_i)$ is a valid proof for com .*

Actually, $\vec{\tau} = (H, U, V)$ with $H = \sum \alpha_i \cdot H_i$, hence the validity of proof. The proof and the commitment can thereafter be randomized, with a new $v \xleftarrow{\$} \mathbb{Z}_p$.

3 Linearly-Homomorphic Signatures

Linearly-homomorphic signatures (LH-Sign) were introduced in [Bo09], to sign vector sub-spaces. They allow to combine any signatures on vectors, so that one can derive the signature of a linear combination of the already signed vectors, but nothing else. Then, Libert *et al.* [Li13] proposed a linearly-homomorphic signature scheme, that is furthermore structure-preserving. More recently, H ebant *et al.* [HPP20] adapted their scheme for a simpler One-Time Linearly-Homomorphic signature (OT-LH-Sign), proven in the GGM, together with the family of Square Diffie-Hellman tags, to provide anonymity properties [HP22]. It can be seen as a Linearly-Homomorphic signature with Randomizable Tags (LH-Sign-RTag), where multiple sub-spaces can be signed independently (from now, referred as the SDH signature). Alternatively, the above Fuchsbauer *et al.* scheme [FHS19, BF20] can also be used (later referred as the FHS signature). The latter provides better efficiency and compactness, but the former allows efficient distributed generation of the CRS, which is more important for our voting application.

3.1 One-Time Linearly-Homomorphic Signature (OT-LH-Sign)

We first recall the simplified OT-LH-Sign, derived from Libert *et al.* [Li13], proven secure in the GGM [FHS19, HPP20, BF20], with messages in $\mathcal{M} = \mathbb{G}^n$:

Setup(1^κ): Given a security parameter κ , it outputs the global parameter param , that contains a pairing-friendly setting $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p, P, \hat{P}, e)$;

Keygen(param, n): Given param and an integer n , it generates $\text{sk} = \vec{s} \xleftarrow{\$} \mathbb{Z}_p^n$, sets $\text{vk} = \vec{s} \cdot \hat{P} = (\hat{P}_i = s_i \cdot \hat{P})_i \in \hat{\mathbb{G}}^n$, and outputs the key pair (sk, vk) ;

Sign(sk, \vec{M}): Given a signing key $\text{sk} = \vec{s}$ and a vector-message $\vec{M} = (M_i)_i \in \mathbb{G}^n$, it outputs the signature $\sigma = \langle \vec{s}, \vec{M} \rangle = \sum s_i \cdot M_i \in \mathbb{G}$;

DerivSign($\text{vk}, (w_i, \vec{M}_i, \sigma_i)_{i=1}^\ell$): Given a public key vk and ℓ tuples of weights $w_i \in \mathbb{Z}_p$ and signed messages \vec{M}_i in σ_i , it outputs the signature $\sigma = \sum_{i=1}^\ell w_i \cdot \sigma_i$ of the vector $\vec{M} = \sum_{i=1}^\ell w_i \cdot \vec{M}_i$;

Verif($\text{vk}, \vec{M}, \sigma$): Given a verification key vk , a vector-message \vec{M} and a signature σ , it outputs 1 if $e(\sigma, \hat{P}) = \prod e(M_i, \hat{P}_i)$, and 0 otherwise.

The correctness can be easily checked, thanks to the bilinearity of pairing e . Unforgeability holds in the GGM [FHS19, HPP20]: one can only derive signatures on messages in the span of the already signed messages. The GGM provides the simulator with the coefficients of the linear combination, while the programmable encodings allow to answer signing queries, in the chosen-message scenario. To allow multiple subspaces, one uses tags. Combinations should then only be possible between messages signed under the same tag.

3.2 SDH-Based Linearly-Homomorphic Signature

Thanks to the non-miscibility of the SDH tags (see Proposition 2), one can transform any One-Time Linearly-Homomorphic signature (OT-LH-Sign) into a (full-fledged) Linearly-Homomorphic Signature. The unlinkability of the SDH tags (see Proposition 1) make them randomizable tags (LH-Sign-RTag). But let us directly describe our signature scheme with messages in $\mathcal{M} = \mathbb{G}^n$:

Setup(1^κ): Given κ , it outputs param , that contains a pairing-friendly setting $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p, P, \hat{P}, e)$ and a random tuple $(\hat{V}_{1,1}, \hat{V}_{1,2}, \hat{V}_{2,1}, \hat{V}_{2,2}) \xleftarrow{\$} \hat{\mathbb{G}}^4$;

Keygen(param, n): Given param and an integer n , it generates $\text{sk} = \vec{s} \xleftarrow{\$} \mathbb{Z}_p^{n+3}$, sets $\text{vk} = \vec{s} \cdot \hat{P} = (\hat{P}_i = s_i \cdot \hat{P})_{i=1}^{n+3} \in \hat{\mathbb{G}}^{n+3}$, and outputs the key pair (sk, vk) ;

NewTag(param): Generates a verifiable tag $\text{Tag} = (\vec{\tau} = (P, t \cdot P, t^2 \cdot P), \text{proof}, \text{com})$, for random scalars $t, v \xleftarrow{\$} \mathbb{Z}_p$, used in proof and com;

Sign(sk, Tag, \vec{M}): Given a signing key sk, a verifiable tag $\text{Tag} = (\vec{\tau}, \text{proof}, \text{com})$, and a vector-message $\vec{M} = (M_i)_i \in \mathbb{G}^n$, it outputs the signature $\sigma = \langle \vec{s}, \vec{M} \parallel \vec{\tau} \rangle \in \mathbb{G}$, where $\vec{M} \parallel \vec{\tau} = (M_1, \dots, M_n, \tau_1, \tau_2, \tau_3) \in \mathbb{G}^{n+3}$;

DerivSign(vk, $(w_i, \text{Tag}_i, \vec{M}_i, \sigma_i)_{i=1}^\ell$): Given a public key vk and ℓ tuples of weights $w_i \in \mathbb{Z}_p$ and signed messages \vec{M}_i in σ_i , under equivalent tags Tag_i , it outputs the signature $\sigma = \sum w_i \cdot \sigma_i$, on the vector $\vec{M} = \sum_{i=1}^\ell w_i \cdot \vec{M}_i$, valid under the equivalent tag Tag' with $\vec{\tau}' = \sum w_i \cdot \vec{\tau}_i$, and adapted proof proof' , but the same commitment com;

Verif(vk, Tag, \vec{M} , σ): Given a verification key vk, a verifiable tag Tag, a vector-message \vec{M} and a signature σ , it outputs 1 if $e(\sigma, \hat{P}) = \prod_{i=1}^n e(M_i, \hat{P}_i) \times \prod_{i=1}^3 e(\tau_i, \hat{P}_{n+i})$ and the tag Tag is valid, and 0 otherwise.

3.3 Distributed Generation

The main advantage of our proofs using SDH signatures, compared to the FHS signatures or SNARGs, is the possible distributed setup, key generation, tag generation, and signatures, among multiple users $(\mathcal{U}_k)_k$:

Setup($1^k, k$): They all agree on the bilinear setting $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p, P, \hat{P}, e)$. User \mathcal{U}_k chooses and sends random points $\hat{V}_{1,1,k}, \hat{V}_{1,2,k}, \hat{V}_{2,1,k}, \hat{V}_{2,2,k} \xleftarrow{\$} \hat{\mathbb{G}}$. This leads to the global verification points $\hat{V}_{1,1} = \sum_k \hat{V}_{1,1,k}$, $\hat{V}_{1,2} = \sum_k \hat{V}_{1,2,k}$, $\hat{V}_{2,1} = \sum_k \hat{V}_{2,1,k}$, $\hat{V}_{2,2} = \sum_k \hat{V}_{2,2,k}$, to complete param.

Keygen(param, n, k): Given the public parameters param, \mathcal{U}_k randomly chooses $s_{i,k} \xleftarrow{\$} \mathbb{Z}_p$, for $i = 1, \dots, n+3$. \mathcal{U}_k computes and sends $\text{vk}_k = (\hat{P}_{i,k} = s_{i,k} \cdot \hat{P})_{i=1}^{n+3}$. This leads to the global verification key $\text{vk} = \sum_k \text{vk}_k$, while \mathcal{U}_k keeps its signing key share $\text{sk}_k = (\text{sk}_{i,k} = s_{i,k})_{i=1}^{n+3}$.

NewTag(param): each user \mathcal{U}_k chooses random $t_k, v_k \xleftarrow{\$} \mathbb{Z}_p$:

1. \mathcal{U}_k computes and sends $\text{com}_k = (\hat{C}_k = t_k \cdot \hat{V}_{2,1} + v_k \cdot \hat{V}_{1,1}, \hat{D}_k = t_k \cdot \hat{V}_{2,2} + v_k \cdot \hat{V}_{1,2})$, and $U_k = t_k \cdot P$, $\Theta_k = v_k \cdot P$;
2. \mathcal{U}_k computes $U = \sum_k U_k$, $\Theta = \sum_k \Theta_k$, and sends $V_k = t_k \cdot U$, $\Psi_k = v_k \cdot U$.

This allows to compute $V = \sum_k V_k$, $\Psi = \sum_k \Psi_k$, and $\hat{C} = \sum_k \hat{C}_k$, $\hat{D} = \sum_k \hat{D}_k$. This leads to $\text{Tag} = (\vec{\tau} = (P, U, V), \text{proof} = (\Theta, \Psi), \text{com} = (\hat{C}, \hat{D}))$, on $t = \sum t_k$ and $v = \sum v_k$.

$\text{Sign}(\text{sk}_k, \text{Tag}, \vec{M} = (M_i)_i)$: Given a signing key share $\text{sk}_k = (s_{i,k})_i$, a tag $\text{Tag} = (\vec{\tau}, \text{proof}, \text{com})$ and a vector-message $\vec{M} = (M_i)_i \in \mathbb{G}^n$, one outputs the signature share $\sigma_k = \sum_{i=1}^n s_{i,k} \cdot M_i + \sum_{i=1}^3 s_{n+i,k} \cdot \tau_i \in \mathbb{G}$. From those shares, one can compute $\sigma = \sum_k \sigma_k$.

The correctness can easily be verified, and parallelizing some steps, to generate the global parameters param , several tags, and signatures on pre-determined messages, a three-round protocol is enough, with public communications, in the honest-but-curious setting. No additional proofs are required in the malicious setting, as each step is already verifiable: (Θ_k, Ψ_k) is a DH proof on (P, U_k, U, V_k) for the commitment com_k , and σ_k is a valid signature of (Tag, \vec{M}) under vk_k . Additional extractable commitments on every sent value allows perfect simulation even against adaptive adversaries: from the committed values, the simulator can generate all the contributions of the honest players so that the final outcome corresponds to any pre-defined values. Such an extractable commitment on a value x can be done with $H(x, r)$, for a large enough random r , in the random oracle model. Because of the linearity of the operations, they essentially all run a full setup on their own. This is a quite simple interactive process.

4 New Efficient NIZK of Subset Membership

We now detail how one can generate efficient randomizable NIZK of subset membership on ElGamal ciphertexts, using SDH signatures, following the general approach presented in the technical overview, with some optimizations due to the SDH tags. We thereafter detail how to adapt [Ch16, DPP22] to get strong receipt-freeness.

4.1 Proof of Subset Membership for ElGamal Ciphertexts

We first focus on the setup and then on the ciphertext generation with the proof that the plaintext \vec{M} is in the subset $\mathcal{S} = \{\vec{M}_1, \dots, \vec{M}_N\} \subset \mathbb{G}^n$: we use a type III pairing-friendly setting $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, p, P, \hat{P}, e)$, with an ElGamal encryption key $\vec{Z} = \vec{z} \cdot P$ (note that $\vec{z} \xleftarrow{\$} \mathbb{Z}_p^n$ can also be generated in a distributed way).

Setup: CRS Generation. Using the above distributed algorithms, one generates signature keys, $\text{SK} = \vec{s} \xleftarrow{\$} \mathbb{Z}_p^{n+4}$ and $\text{VK} = \vec{\hat{S}} \leftarrow \vec{s} \cdot \hat{P} \in \hat{\mathbb{G}}^{n+4}$, as well as N tags $\text{Tag}_i = (\vec{\tau}_i, \text{proof}_i, \text{com}_i)$, for $\vec{\tau}_i = (\tau_{i,1} = P, \tau_{i,2} = t_i \cdot P, \tau_{i,3} = t_i^2 \cdot P)$, with $t_i \xleftarrow{\$} \mathbb{Z}_p^*$, for $i = 1, \dots, N$, with the validity proofs $\text{proof}_i \in \mathbb{G}^2$ and commitments $\text{com}_i \in \hat{\mathbb{G}}^2$ (on t_i , for random v_i), and N pairs of signatures, for $\vec{M}_i \in \mathcal{S}$:

$$\Sigma_{i,0} = \text{Sign}(\text{SK}, \text{Tag}_i, (P_S, 0, \vec{M}_i)) = \langle (P_S, 0, \vec{M}_i, \tau_{i,2}, \tau_{i,3}), \text{SK} \rangle \in \mathbb{G}$$

$$\Sigma_{i,1} = \text{Sign}(\text{SK}, \text{Tag}_i, (0, P, \vec{Z})) = \langle (0, P, \vec{Z}, \tau_{i,2}, \tau_{i,3}), \text{SK} \rangle \in \mathbb{G}$$

We note the optimization, where $\tau_{i,1} = P$ is a known constant, so there is no need to provide it: the length of the vectors is $n + 4$ only. The verification key VK , the tags $(\text{Tag}_i)_i$ and the pairs of signatures $(\Sigma_{i,0}, \Sigma_{i,1})_i$ constitute the CRS.

Proven Ciphertext Generation. The encryptor can generate a random ciphertext of \vec{M}_j as $C = (C_0, \vec{C}) = (r \cdot P, \vec{M}_j + r \cdot \vec{Z}) = (0, \vec{M}_j) + r \cdot (P, \vec{Z})$, and the random randomizer $\mathcal{D} = (D_0, \vec{D}) = (s \cdot P, s \cdot \vec{Z}) = s \cdot (P, \vec{Z})$, for random $r, s \xleftarrow{\$} \mathbb{Z}_p$, together with the associated signatures $\Sigma_0 = \Sigma_{j,0} + r \times \Sigma_{j,1}$ of (P_S, C_0, \vec{C}) and $\Sigma_1 = s \cdot \Sigma_{j,1}$ of $(0, D_0, \vec{D})$ under the equivalent tags $\vec{\tau}'_0 = (r + 1) \cdot \vec{\tau}_j$ and $\vec{\tau}'_1 = s \cdot \vec{\tau}_j$ for the key VK . The tags have already been randomized, and one can randomize com' and adapt $\text{proof}'_0, \text{proof}'_1$, with an additional random $v \xleftarrow{\$} \mathbb{Z}_p$. It then sends the twin-ciphertexts $(C, \mathcal{D}) \in \mathbb{G}^{2n+2}$, the twin-signatures $(\Sigma_0, \Sigma_1) \in \mathbb{G}^2$ and the twin-tags $(\vec{\tau}'_0, \text{proof}'_0, \vec{\tau}'_1, \text{proof}'_1, \text{com}') \in \mathbb{G}^8 \times \hat{\mathbb{G}}^2$. The first components of the tags are $C_0 + P$ and D_0 respectively, there is no need to duplicate them.

Randomization. The receiver can randomize the ciphertext into $C' = (C'_0, \vec{C}') = C + r' \cdot \mathcal{D}$, with $r' \xleftarrow{\$} \mathbb{Z}_p$, adapt the tag $\vec{\tau}' = \vec{\tau}'_0 + r' \cdot \vec{\tau}'_1$, and randomize it with $v' \xleftarrow{\$} \mathbb{Z}_p$ in proof' , com' , and adapt the signature $\Sigma' = \Sigma_0 + r' \cdot \Sigma_1$. In the end, one only stores $C' = (C'_0, \vec{C}') \in \mathbb{G}^{n+1}$ and the proof $(\Sigma', \text{Tag}' = (\vec{\tau}', \text{proof}', \text{com}')) \in \mathbb{G}^5 \times \hat{\mathbb{G}}^2$, which is independent of N .

Verifiable Tally. The valid ballots can be aggregated by summing component-wise all the ciphertexts $\{(C'_0, \vec{C}')\}$ from the public ballot-box into a global ciphertext $\mathcal{T} = (T_0, \vec{T})$, which decrypts to the tally using the decryption key \vec{z} , with zero-knowledge proofs of valid decryption (*à la Schnorr* with the Fiat-Shamir paradigm).

More Constraints. Our approach is thus quite efficient for a subset constraint, whatever the size of the subset. And multiple constraints on ciphertexts $(C_0, \mathbf{A}_k \cdot \vec{C})$ under the keys $\vec{Z}_k = \mathbf{A}_k \cdot \vec{Z}$ in sets S_k can be combined: each one needs twin-tags and twin-signatures, sent by the voter (10 elements of \mathbb{G} and 2 elements of $\hat{\mathbb{G}}$), but only one tag and one signature stored in the ballot-box (5 elements of \mathbb{G} and 2 elements of $\hat{\mathbb{G}}$). More complex formats of the ballots can be modelled as subset constraints. One just has to take care of the first component P_{S_k} that must be specific to S_k , to avoid combinations between elements in the CRS that are for different proofs. Any successful illegal combination would break the DL assumption in the algebraic group model and the random oracle model

Examples. The 0-1 choices (each i -th box must be a 0-1 choice) is a subset constraint, with $S_i = \{0 \cdot P, 1 \cdot P\} \subset \mathbb{G}^1$, for each i . This allows to prove the validity of the 0-1 encryption in (C_0, C_i) under the ElGamal key Z_i . However, this requires n subset membership proofs, for sets of size 2. And the less constraints there are, the more interesting is our approach, even if the sets get larger. Hence, one can consider $S = \{0, 1\}^n$, and thus only one subset membership proof, with a set of size 2^n , if n is not too large. But then the setup becomes exponential in n . One can also split n to have k parallel subset membership proofs of

length $2^{n/k}$. We however stress that even for any quite large (possibly exponential) CRS, the generation of the proof by the encryptor is constant-time.

For a more complex election, where one can check at most K boxes among N , when all boxes being 0-1, as above, one can consider the additional proof of subset membership with $S = \{0 \cdot P, \dots, K \cdot P\} \subset \mathbb{G}^1$ for the ciphertext $(C_0, \sum C_i)$ under the key $Z = \sum Z_i$.

4.2 Proofs on Randomizable Ciphertexts

Interestingly, this approach is compatible with [Ch16, DPP22] to get strong receipt-freeness: an encryptor can restrict transformations on his ElGamal ciphertext thanks to an OT-LH-Sign in \mathbb{G}^{n+2} , for a personal verification key vk , by signing both the ciphertext (P, C_0, \vec{C}) and the randomizer $(0, D_0, \vec{D})$ in (σ_0, σ_1) , without any need of tags, as this is the only vector sub-space with this signing key sk : any new signature σ on some (P, C'_0, \vec{C}') , valid under vk , is necessarily a randomization of (C_0, \vec{C}) . This provides receipt-freeness. We stress that (sk, vk) is an individual pair of keys that is owned by the signer, contrarily to (SK, VK) that was generated during the setup for the CRS.

According to [Ch16], one can add a Groth-Sahai proof of Diffie-Hellman tuple for $(P, T = \mathcal{H}(\text{vk}), C_0 = r \cdot P, W_0 = r \cdot T)$, as suggested in [Ch16]. But in our case, the RCCA-security requires the AGM to extract r from such a valid Diffie-Hellman tuple with a truly random T . The randomness r then allows the decryption. We also have to do it for $(P, T = \mathcal{H}(\text{vk}), D_0 = s \cdot P, W_1 = s \cdot T)$, for future randomization: for random ν_0, ν_1 , one generates $\text{com}_0 = (\hat{C}_0 = r \cdot \hat{V}'_{2,1} + \nu_0 \cdot \hat{V}'_{1,1}, \hat{D}_0 = r \cdot \hat{V}'_{2,2} + \nu_0 \cdot \hat{V}'_{1,2})$, $\text{com}_1 = (\hat{C}_1 = s \cdot \hat{V}'_{2,1} + \nu_1 \cdot \hat{V}'_{1,1}, \hat{D}_1 = s \cdot \hat{V}'_{2,2} + \nu_1 \cdot \hat{V}'_{1,2})$, and the proofs $\text{proof}_0 = (\Theta_0 = \nu_0 \cdot P, \Psi_0 = \nu_0 \cdot T)$, $\text{proof}_1 = (\Theta_1 = \nu_1 \cdot P, \Psi_1 = \nu_1 \cdot T)$, that can later be combined by into $\text{com} = \text{com}_0 + r' \cdot \text{com}_1$ and $\text{proof} = \text{proof}_0 + r' \cdot \text{proof}_1$ by the receiver(s) to verify $W = W_0 + r' \cdot W_1 = r'' \cdot T$, with unknown scalars $r'' = r + r' \cdot s$ and $\nu'' = \nu_0 + r' \cdot \nu_1$, after having also randomized the ciphertext $C'_0 = C_0 + r' \cdot D_0$ and $\vec{C}' = \vec{C} + r' \cdot \vec{D}$. We stress that an independent CRS $(\hat{V}'_{1,1}, \hat{V}'_{1,2}, \hat{V}'_{2,1}, \hat{V}'_{2,2})$ is used here. The same as for the SDH proofs could be used, but the separation will clarify the security analysis.

5 Homomorphic Voting System: Efficiency and Security

We first recap the communications and computations, in the N -subset case, for ballots where n boxes could be checked: $\vec{M} \in \mathcal{S} \subset \mathbb{G}^n$. Thereafter, we explain the security properties. We stress that we target a homomorphic voting system.

Communication. The full public information generated at the setup time, in a possibly distributed way, consists of $\text{VK} \in \hat{\mathbb{G}}^{n+4}$, $(\Sigma_{i,0}, \Sigma_{i,1})_i \in \mathbb{G}^{2N}$, with the tags, but without the constant P , $(\tau_{i,2}, \tau_{i,3})_i \in \mathbb{G}^{2N}$, together with their proofs and commitments in $(\mathbb{G}^2 \times \hat{\mathbb{G}}^2)^N$,

and the two Groth-Sahai CRS in $\hat{\mathbb{G}}^4$. The CRS thus consists of $6N$ elements from \mathbb{G} and $n + 2N + 12$ elements from $\hat{\mathbb{G}}$.

From the CRS, the voter sends the twin-ciphertexts $(C, \mathcal{D}) \in \mathbb{G}^{2n+2}$, the twin-validity-proofs $(\Sigma_0, \Sigma_1, \tilde{\tau}'_0, \text{proof}'_0, \tilde{\tau}'_1, \text{proof}'_1, \text{com}') \in \mathbb{G}^{10} \times \hat{\mathbb{G}}^2$, the twin-signatures $(\text{vk}, \sigma_0, \sigma_1) \in \hat{\mathbb{G}}^{n+2} \times \mathbb{G}^2$, and the twin-user-proofs $(W_0, W_1, \text{proof}_0, \text{proof}_1, \text{com}_0, \text{com}_1) \in \mathbb{G}^6 \times \hat{\mathbb{G}}^4$, using above notations. We thus globally have $2n + 20$ elements from \mathbb{G} and $n + 8$ elements from $\hat{\mathbb{G}}$ in the twin-ballot.

The ballot-box stores the randomized ciphertext $C' \in \mathbb{G}^{n+1}$, the validity proof $(\Sigma'', \tilde{\tau}'', \text{proof}'', \text{com}'') \in \mathbb{G}^5 \times \hat{\mathbb{G}}^2$, the user-signature $(\text{vk}, \sigma) \in \hat{\mathbb{G}}^{n+2} \times \mathbb{G}$, and the user-proof $(W'', \text{proof}, \text{com}) \in \mathbb{G}^3 \times \hat{\mathbb{G}}^2$. We thus globally have $n + 10$ elements from \mathbb{G} and $n + 6$ elements from $\hat{\mathbb{G}}$ for each randomized ballot.

We can use the type III pairing-friendly curve BLS12-381 [BLS03], as in all the zk-SNARKs applications: \mathbb{G} group elements are encoded on 48 bytes, while $\hat{\mathbb{G}}$ group elements are encoded on 96 bytes. For $N = n = 25$ (in the 1-out-of- n case), the public information is a bit more than 15KB, the twin-ballot is 6.5KB, while the ballot is 4.6KB. Which is quite reasonable in size.

Computations. We have implemented the voting process with both FHS and SDH signatures (centralized setup, twin-ballot generation, randomization and ballot-extraction, together with verification) in Rust, using https://github.com/zkcrypto/bls12_381 library, with the two additional enhancements for Strong Receipt-Freeness, but without any implementation optimizations. On Figure 1, we deal with the 1-out-of-25 ballot case. The most important

	param		Twin-ballot		Ballot	
	Generate	Verify	Generate	Verify	Rand-Extract	Verify
SDH	1225ms	4062ms	179ms	390ms	66ms	211ms
FHS	1019ms	3710ms	142ms	339ms	49ms	241ms

Fig. 1: Implementation of 1-out-of-25 Ballots (Rust on Macbook Pro 2021 – M1 Pro)

for practical use is the quite efficient generation of the full twin-ballots, with cross-compiled applications on mobile phones (see Figure 2, for the 1-out-of- n case). Encryption, signing key generation, and signature are all linear in n . The proof of validity (for one constraint) is almost constant. If we approximate the time as an affine function in $a \times n + b$, the time for each proof of subset membership is thus b : not much more than 100ms on a 6-year-old smartphone.

	$n = 5$	$n = 10$	$n = 25$	a	b
Using Linearly-Homomorphic Proofs, cross-compiled from Rust					
2017 – Snapdragon 835 (Android)	243ms	375ms	710ms	23.1ms	134.5ms
2019 – Intel i9-9880H (MacOS)	91ms	134ms	261ms	8.5ms	48.8ms
2021 – iPhone 13 A15 Bionic (iOS)	43ms	63ms	125ms	4.1ms	22.2ms

Fig. 2: Voting time (encrypt, prove, generate keys, and sign) for 1-out-of- n Choices

Privacy of the Votes. The first important property in electronic voting is the privacy of the vote. The voter derives the twin-ciphertexts $(C_0, \vec{C}) = (r \cdot P, \vec{M}_j + r \cdot \vec{Z})$ and $(D_0, \vec{D}) = (s \cdot P, s \cdot \vec{Z})$, the twin-tags $\vec{\tau}'_0 = (r + 1) \cdot \vec{\tau}_j$, $\vec{\tau}'_1 = s \cdot \vec{\tau}_j$, and randomized proofs $\text{proof}'_0, \text{proof}'_1, \text{com}'$, for random $r, s, v' \xleftarrow{\$} \mathbb{Z}_p$, which are unlinkable to \vec{M}_j .

In order to show it, let us denote $(\vec{\tau} = (P, U = x \cdot P, V = x^2 \cdot P), \text{proof} = (\Theta = v \cdot P, \Psi = v \cdot U), \text{com} = (\hat{C} = x \cdot \hat{V}_{2,1} + v \cdot \hat{V}_{1,1}, \hat{D} = x \cdot \hat{V}_{2,2} + v \cdot \hat{V}_{1,2}))$ the proven SDH tag for \vec{M}_j . Using random $r, s, v' \xleftarrow{\$} \mathbb{Z}_p$, the voter generates

$$\begin{aligned} (C_0, \vec{C}) &= r \cdot (P, \vec{Z}) + (0, \vec{M}_j) & (D_0, \vec{D}) &= s \cdot (P, \vec{Z}) \\ \vec{\tau}'_0 &= (r + 1) \cdot (P, U, V) & \vec{\tau}'_1 &= s \cdot (P, U, V) \\ \text{proof}'_0 &= (r + 1) \cdot [(\Theta, \Psi) + v' \cdot (P, U)] & \text{proof}'_1 &= s \cdot [(\Theta, \Psi) + v' \cdot (P, U)] \\ \text{com}' &= (\hat{C}, \hat{D}) + v' \cdot (\hat{V}_{1,1}, \hat{V}_{1,2}) = x \cdot (\hat{V}_{2,1}, \hat{V}_{2,2}) + (v + v') \cdot (\hat{V}_{1,1}, \hat{V}_{1,2}) \end{aligned}$$

One can indeed note that

$$\begin{aligned} \text{proof}'_0 &= (r + 1) \cdot [(\Theta, \Psi) + v' \cdot (P, U)] & \text{proof}'_1 &= s \cdot [(\Theta, \Psi) + v' \cdot (P, U)] \\ &= (v + v') \cdot [(r + 1) \cdot (P, U)] & &= (v + v') \cdot [s \cdot (P, U)] \end{aligned}$$

are valid proofs for $\vec{\tau}'_0$ and $\vec{\tau}'_1$ with com' .

Let us replace the CRS $(\hat{V}_{1,1}, \hat{V}_{1,2}, \hat{V}_{2,1}, \hat{V}_{2,2})$ with a Diffie-Hellman tuple $(\hat{V}_{1,1}, \hat{V}_{1,2}, \hat{V}_{2,1} = \alpha \cdot \hat{V}_{1,1}, \hat{V}_{2,2} = \alpha \cdot \hat{V}_{1,2})$. This is indistinguishable under the DDH assumption in \mathbb{G} . Then $\text{com}' = (\alpha x + (v + v')) \cdot (\hat{V}_{1,1}, \hat{V}_{1,2})$.

If we define $\text{com}' = \beta \cdot (\hat{V}_{1,1}, \hat{V}_{1,2})$, for a random $\beta \xleftarrow{\$} \mathbb{Z}_p$, which implicitly and randomly defines v' , and if we denote, for random $r, s \xleftarrow{\$} \mathbb{Z}_p$,

$$\begin{aligned} (P_0, U_0, V_0, \vec{Z}_0) &= (r + 1) \cdot (P, U, V, \vec{Z}) & (P_1, U_1, V_1, \vec{Z}_1) &= s \cdot (P, U, V, \vec{Z}) \\ (C_0, \vec{C}) &= (P_0 - P, \vec{Z}_0 - \vec{Z}) + (0, \vec{M}_j) & (D_0, \vec{D}) &= (P_1, \vec{Z}_1) \\ \vec{\tau}'_0 &= (P_0, U_0, V_0) & \vec{\tau}'_1 &= (P_1, U_1, V_1) \\ \text{proof}'_0 &= (v + v') \cdot (P_0, U_0) & \text{proof}'_1 &= (v + v') \cdot (P_1, U_1) \\ &= \beta \cdot (P_0, U_0) - \alpha \cdot (U_0, V_0) & &= \beta \cdot (P_1, U_1) - \alpha \cdot (U_1, V_1) \end{aligned}$$

Let us replace $(P_0, U_0, V_0, \vec{Z}_0)$ and $(P_1, U_1, V_1, \vec{Z}_1)$ by random tuples, which is indistinguishable under the DDH assumption in \mathbb{G} . This is also under the organizational assumption that the scalars in the tags generated during the setup are really private. As \vec{Z}_0 is random, we can note $(C_0, \vec{C}) = (P_0 - P, \vec{Z}_0)$.

For a new random $y \xleftarrow{\$} \mathbb{Z}_p$, we can go back to $(P_0, U_0, V_0) = (r + 1) \cdot (P, y \cdot P, y^2 \cdot P)$ and $(P_1, U_1, V_1, \vec{Z}_1) = s \cdot (P, y \cdot P, y^2 \cdot P, \vec{Z})$, which is indistinguishable under the DDH and

the SDH assumptions in \mathbb{G} . This then allows to honestly generate the proofs using y , even for a valid CRS $(\hat{V}_{1,1}, \hat{V}_{1,2}, \hat{V}_{2,1}, \hat{V}_{2,2})$ that is no longer a Diffie-Hellman tuple. The proven twin-tags are thus unlinkable to $\tilde{\tau}_j$, and the ciphertext (C_0, \vec{C}) encrypts a random plaintext. This is perfectly private.

We can stress that the ballot privacy (in the above honest-but-curious setting) is achieved in the standard model, under the SXDH assumption and the SDH assumption in \mathbb{G} .

Strong Receipt-Freeness. But we need stronger privacy properties, by preventing malicious voter behaviors, with replay and vote-selling attacks. When the voter has sent the ciphertext (C_0, \vec{C}) , he can open it with his randomness r . But the ciphertext in the public ballot-box is (C'_0, \vec{C}') that has been randomized with an unknown r' : this excludes VS-attacks. We stress that the receiver must first check $D_0 \neq 0$ for randomization to be effective. The additional Diffie-Hellman proof for $(P, T = \mathcal{H}(\text{vk}), C'_0, W)$ avoids replay attacks under a different signing key vk' . Excluding multiple ballots with the same vk then avoids replay attacks, and thus CS-attacks. But here, both GGM and ROM are needed.

To assess strong receipt-freeness, we can follow a similar path as in [Ch16, Theorem 3 – Figure 1], with their security game for the strong receipt-freeness (a stronger privacy notion, against malicious voters). The proof is performed in two main steps, with first the RCCA-security for our encryption scheme, thanks to the additional Diffie-Hellman proof, and then the privacy of the ciphertexts. But we cannot use the same approach as they do, for simulating the decryption oracle, as we take advantage of the compact randomness-reuse version of ElGamal. However, we can exploit the GGM/AGM extractor: any adversarially-generated Diffie-Hellman tuple $(P, \mathcal{H}(\text{vk}), C_0, W_0)$, for a *truly random* $T = \mathcal{H}(\text{vk})$, as we are in the ROM, allows to extract r such that $C_0 = r \cdot P$. This thus allows to simulate the decryption of any ballot with a valid signature under a *fresh* vk . Let us now simulate the public view of an adversary against the strong receipt-freeness:

1. in the initial security game, honest published ballots are generated as fresh ciphertexts, and all the adversarial ballots are honestly randomized before publication. Final tally decryption uses the decryption key and the Schnorr proof is performed honestly;
2. the Schnorr proof of correct tally decryption is simulated (by programming the random oracle used to derive the challenge);
3. the adversarial Groth-Sahai proofs of Diffie-Hellman tuples are additionally checked knowing the discrete logarithm of \mathcal{H} values (by programming the random oracle);
4. the adversarial twin-ballots, with *fresh* vk , are decrypted using the above RCCA-security: valid fresh Diffie-Hellman tuples $(P, T = \mathcal{H}(\text{vk}), C_0, W_0)$ and $(P, T = \mathcal{H}(\text{vk}), D_0, W_1)$ come with r and s , such that $C_0 = r \cdot P$ and $D_0 = s \cdot P$, respectively, which allows to decrypt, using the GGM/AGM extractor. A ballot with a replayed vk or invalid W_0, W_1 is rejected. The tally is computed on clear data, which does not impact the proof of correct decryption, that was already simulated;

5. from r and s , in the adversarial twin-ballots with *fresh* vk , one can recompute the tags $\vec{\tau}'_0$ and $\vec{\tau}'_1$. If these tags are not the expected ones, the ballots are rejected;
6. the simulator learns the users' signing keys sk associated to each sent vk , using the GGM/AGM extractor for adversarially generated vk , and keeps the signing keys SK generated during the setup;
7. for published ballots, the Groth-Sahai proofs of SDH tuples are simulated using a Diffie-Hellman CRS $(\hat{V}_{1,1}, \hat{V}_{1,2}, \hat{V}_{2,1}, \hat{V}_{2,2})$ and signatures are generated using the signing keys;
8. for published ballots, fresh random ciphertexts and random tags are generated (proofs are simulated and signatures use the signing keys).

We have built a simulator that generates views indistinguishable from real executions, without leaking any information about the votes. We stress that this stronger privacy in the malicious setting relies on the GGM and the random oracle model. They are widely admitted, in particular for efficient constructions.

Strong Verifiability. From the unforgeability under chosen-message attacks of the OT-LH-Sign in the GGM, and the non-miscibility of the SDH-tags (Proposition 2), the validity of signatures on (P_S, C_0, \vec{C}) , $(0, D_0, \vec{D})$ or (P_S, C'_0, \vec{C}') under the key VK (and a valid tag) implies that they are linear combinations of some $(P_S, 0, \vec{M}_j)$ and $(0, P, \vec{Z})$, again under the assumption that the scalars in the tags generated during the setup are really private, and even destroyed after use. Hence, no new signature can be generated by anybody, excepted under linear combinations on equivalent tags. Because of the first component P_S (specific to S) in (P_S, C'_0, \vec{C}') , this is necessarily for a valid ballot, but not necessarily for the same j as in (P_S, C_0, \vec{C}) : $C_0 = r \cdot P$ and $\vec{C} = r \cdot \vec{Z} + \vec{M}_j$, and $C'_0 = r' \cdot P$ and $\vec{C}' = r' \cdot \vec{Z} + \vec{M}_k$. Anyway, they are both valid ballots. Furthermore, the decryption of the tally is given with a proof of correct decryption, which provides the **universal verifiability** of ballots and tally.

However, the voter needs the additional guarantee of no modification of his initial choice \vec{M}_j in (C_0, \vec{C}) after randomization in (C'_0, \vec{C}') , by the receiver: the voter, who has kept $T = \mathcal{H}(\text{vk})$, can ask for his vote, and check the validity of σ' with respect to (P, C'_0, \vec{C}') under vk . This implies (C'_0, \vec{C}') can only be a randomization of the initial ciphertext (C_0, \vec{C}) : $\vec{M}_k = \vec{M}_j$, under the unforgeability of the OT-LH-Sign, as vk is specific to a voter and used only once. This **individual verifiability** convinces every voter of the integrity of the ballot-box, with the presence of his vote.

Acknowledgments

This work was supported in part by the France 2030 ANR Project ANR-22-PECY-003 SecureCompute.

Bibliography

- [BF20] Bauer, Balthazar; Fuchsbauer, Georg: Efficient Signatures on Randomizable Ciphertexts. In (Galdi, Clemente; Kolesnikov, Vladimir, eds): SCN 20. volume 12238 of LNCS. Springer, Heidelberg, pp. 359–381, September 2020.
- [B110] Blazy, Olivier; Fuchsbauer, Georg; Izabachène, Malika; Jambert, Amandine; Sibert, Hervé; Vergnaud, Damien: Batch Groth-Sahai. In (Zhou, Jianying; Yung, Moti, eds): ACNS 10. volume 6123 of LNCS. Springer, Heidelberg, pp. 218–235, June 2010.
- [B111] Blazy, Olivier; Fuchsbauer, Georg; Pointcheval, David; Vergnaud, Damien: Signatures on Randomizable Ciphertexts. In (Catalano, Dario; Fazio, Nelly; Gennaro, Rosario; Nicolosi, Antonio, eds): PKC 2011. volume 6571 of LNCS. Springer, Heidelberg, pp. 403–422, March 2011.
- [BLS03] Barreto, Paulo S. L. M.; Lynn, Ben; Scott, Michael: Constructing Elliptic Curves with Prescribed Embedding Degrees. In (Cimato, Stelvio; Galdi, Clemente; Persiano, Giuseppe, eds): SCN 02. volume 2576 of LNCS. Springer, Heidelberg, pp. 257–267, September 2003.
- [Bo09] Boneh, Dan; Freeman, David; Katz, Jonathan; Waters, Brent: Signing a Linear Subspace: Signature Schemes for Network Coding. In (Jarecki, Stanislaw; Tsudik, Gene, eds): PKC 2009. volume 5443 of LNCS. Springer, Heidelberg, pp. 68–87, March 2009.
- [Bo16] Bootle, Jonathan; Cerulli, Andrea; Chaidos, Pyrros; Groth, Jens; Petit, Christophe: Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. In (Fischlin, Marc; Coron, Jean-Sébastien, eds): EUROCRYPT 2016, Part II. volume 9666 of LNCS. Springer, Heidelberg, pp. 327–357, May 2016.
- [CFL19] Cortier, Véronique; Filipiak, Alicia; Lallemand, Joseph: BeleniosVS: Secrecy and Verifiability Against a Corrupted Voting Device. In (Delaune, Stephanie; Jia, Limin, eds): CSF 2019 Computer Security Foundations Symposium. IEEE Computer Society Press, pp. 367–381, 2019.
- [Ch16] Chaidos, Pyrros; Cortier, Véronique; Fuchsbauer, Georg; Galindo, David: BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme. In (Weippl, Edgar R.; Katzenbeisser, Stefan; Kruegel, Christopher; Myers, Andrew C.; Halevi, Shai, eds): ACM CCS 2016. ACM Press, pp. 1614–1625, October 2016.
- [CS11] Cortier, Véronique; Smyth, Ben: Attacking and Fixing Helios: An Analysis of Ballot Secrecy. In (Backes, Michael; Zdancewic, Steve, eds): CSF 2011 Computer Security Foundations Symposium. IEEE Computer Society Press, pp. 297–311, 2011.
- [DPP22] Devillez, Henri; Pereira, Olivier; Peters, Thomas: Traceable Receipt-Free Encryption. In (Agrawal, Shweta; Lin, Dongdai, eds): ASIACRYPT 2022, Part III. volume 13793 of LNCS. Springer, Heidelberg, pp. 273–303, December 2022.
- [FHS19] Fuchsbauer, Georg; Hanser, Christian; Slamanig, Daniel: Structure-Preserving Signatures on Equivalence Classes and Constant-Size Anonymous Credentials. *Journal of Cryptology*, 32(2):498–546, April 2019.
- [FKL18] Fuchsbauer, Georg; Kiltz, Eike; Loss, Julian: The Algebraic Group Model and its Applications. In (Shacham, Hovav; Boldyreva, Alexandra, eds): CRYPTO 2018, Part II. volume 10992 of LNCS. Springer, Heidelberg, pp. 33–62, August 2018.

- [Ge13] Gennaro, Rosario; Gentry, Craig; Parno, Bryan; Raykova, Mariana: Quadratic Span Programs and Succinct NIZKs without PCPs. In (Johansson, Thomas; Nguyen, Phong Q., eds): EUROCRYPT 2013. volume 7881 of LNCS. Springer, Heidelberg, pp. 626–645, May 2013.
- [Gr16] Groth, Jens: On the Size of Pairing-Based Non-interactive Arguments. In (Fischlin, Marc; Coron, Jean-Sébastien, eds): EUROCRYPT 2016, Part II. volume 9666 of LNCS. Springer, Heidelberg, pp. 305–326, May 2016.
- [GS08] Groth, Jens; Sahai, Amit: Efficient Non-interactive Proof Systems for Bilinear Groups. In (Smart, Nigel P., ed.): EUROCRYPT 2008. volume 4965 of LNCS. Springer, Heidelberg, pp. 415–432, April 2008.
- [HP22] Héban, Chloé; Pointcheval, David: Traceable Constant-Size Multi-authority Credentials. In (Galdi, Clemente; Jarecki, Stanislaw, eds): SCN 2022 Security and Cryptography for Networks. volume 13409 of LNCS. Springer, pp. 411–434, 2022.
- [HPP20] Héban, Chloé; Phan, Duong Hieu; Pointcheval, David: Linearly-Homomorphic Signatures and Scalable Mix-Nets. In (Kiayias, Aggelos; Kohlweiss, Markulf; Wallden, Petros; Zikas, Vassilis, eds): PKC 2020, Part II. volume 12111 of LNCS. Springer, Heidelberg, pp. 597–627, May 2020.
- [JR13] Jutla, Charanjit S.; Roy, Arnab: Shorter Quasi-Adaptive NIZK Proofs for Linear Subspaces. In (Sako, Kazuo; Sarkar, Palash, eds): ASIACRYPT 2013, Part I. volume 8269 of LNCS. Springer, Heidelberg, pp. 1–20, December 2013.
- [KW15] Kiltz, Eike; Wee, Hoeteck: Quasi-Adaptive NIZK for Linear Subspaces Revisited. In (Oswald, Elisabeth; Fischlin, Marc, eds): EUROCRYPT 2015, Part II. volume 9057 of LNCS. Springer, Heidelberg, pp. 101–128, April 2015.
- [Le19] Lee, Jiwon; Choi, Jaekyoung; Kim, Jihye; Oh, Hyunok: , SAVER: Snark-friendly, Additively-homomorphic, and Verifiable Encryption and decryption with Rerandomization. Cryptology ePrint Archive, Report 2019/1270, 2019. <https://eprint.iacr.org/2019/1270>.
- [Li13] Libert, Benoît; Peters, Thomas; Joye, Marc; Yung, Moti: Linearly Homomorphic Structure-Preserving Signatures and Their Applications. In (Canetti, Ran; Garay, Juan A., eds): CRYPTO 2013, Part II. volume 8043 of LNCS. Springer, Heidelberg, pp. 289–307, August 2013.
- [MMR22] Mestel, D.; Muller, J.; Reisert, P.: How Efficient are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis. In (Calzavara, Stefano; Naumann, David, eds): CSF 2022 Computer Security Foundations Symposium. IEEE Computer Society, pp. 179–194, 2022.
- [Pa13] Parno, Bryan; Howell, Jon; Gentry, Craig; Raykova, Mariana; Pinocchio: Nearly Practical Verifiable Computation. In: 2013 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, pp. 238–252, May 2013.
- [Wa05] Waters, Brent R.: Efficient Identity-Based Encryption Without Random Oracles. In (Cramer, Ronald, ed.): EUROCRYPT 2005. volume 3494 of LNCS. Springer, Heidelberg, pp. 114–127, May 2005.

An Alternative Group for Applications of ElGamal in Cryptographic Protocols

Rolf Haenni,¹ Ilona Starý Kořánová²

Abstract: The subgroup of quadratic residues modulo a large safe prime is the most common choice in practice for the ElGamal cryptosystem. Computations in this group are simple and sufficiently efficient for at least 128 bits of security, and the DDH problem seems to be hard. In its practical application, however, this particular group has also several disadvantages, for example the relatively high cost for testing group membership or the uneven message space. In this paper, we discuss an alternative group for ElGamal, called multiplicative group of absolute values modulo a safe prime, which is isomorphic to the subgroup of quadratic residues, but with a slightly different group operation and much better properties for practical applications such as e-voting.

Keywords: ElGamal Encryption Scheme, DDH Assumption, Group Theory, Factoring Group, E-Voting Protocols, Practical Implementations

1 Introduction

In cryptographic protocol design, the ElGamal cryptosystem is a common choice for achieving confidentiality in different contexts, for example for protecting the secrecy of the submitted votes in an e-voting application. ElGamal is simple, efficient, and well understood, and its homomorphic property offers a flexible toolbox of cryptographic operations such as re-encryption or threshold decryption. In e-voting applications, homomorphic tallying and mixnets are the two most prominent approaches for achieving vote secrecy and E2E-verifiability simultaneously. Both techniques rely on the homomorphic property.

ElGamal is IND-CPA secure in groups in which the decisional Diffie-Hellman (DDH) problem cannot be solved efficiently. Since the DDH problem is simpler than the related CDH (computational Diffie-Hellman) or DL (discrete logarithm) problems, selecting an appropriate group is more delicate. In the multiplicative group \mathbb{Z}_p^* of integers modulo a prime p (also denoted as the *quotient group* $(\mathbb{Z}/p\mathbb{Z})^\times$ of units), for example, the DDH problem can be solved efficiently using the Legendre symbol, even if solving CDH or DL is generally believed to be a hard problem. Therefore, \mathbb{Z}_p^* is not a suitable group for ElGamal [Bo98].

¹ Bern University of Applied Sciences, 2501 Biel, Switzerland, rolf.haenni@bfh.ch

² Univerzita Karlova, 116 36 Prague 1, Czech Republic, ilona.koranova@ff.cuni.cz

1.1 The Subgroup of Quadratic Residues

A better choice is the subgroup $\mathbb{G}_q \subset \mathbb{Z}_p^*$ of quadratic residues modulo a large *safe* prime $p = 2q + 1$, which contains only half of the elements of \mathbb{Z}_p^* (the quadratic residues $x^2 \bmod p$). To this day, no efficient non-quantum algorithm is known for solving DDH in \mathbb{G}_q efficiently, and this is why \mathbb{G}_q is often selected for ElGamal. Other options such as elliptic curves are slightly more complicated to use and less flexible in concrete applications (their main advantage comes from the shorter keys). In practical applications, however, \mathbb{G}_q also has several disadvantages:

- In applications of ElGamal, where elements of \mathbb{G}_q are exchanged between the participants of a cryptographic protocol, it is important to confirm the membership of each received group element, because otherwise the IND-CPA property of ElGamal is no longer guaranteed.³ In a worst-case scenario, not checking group memberships in a single case may undermine the security of the whole application. In $\mathbb{Z}_p^* = \{1, \dots, p - 1\}$, all integers between 1 and $p - 1$ are group members, but in \mathbb{G}_q , the group members depend strongly on p . While 5 for example is a member of $\mathbb{G}_5 = \{1, 3, 4, 5, 9\}$, it is not a member of $\mathbb{G}_{11} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. Testing membership in \mathbb{G}_q requires the computation of either a modular exponentiation or a Legendre symbol. In both cases, compared to testing membership in \mathbb{Z}_p^* , this is relatively expensive and may have an impact on the overall performance of the application (see Sect. 4 for a discussion on the cost of membership testing in different programming languages).
- A related problem of using \mathbb{G}_q for ElGamal is the fact that \mathbb{G}_q itself is the message space of the encryption scheme. If a general-purpose message $m \in \{0, 1\}^n$ is given as a sequence of bits of length $n < \|\mathbb{G}_q\|$, then m needs to be encoded into \mathbb{G}_q as a preliminary step before the encryption and decoded from \mathbb{G}_q as a additional step after the decryption. Several options for such an encoding exist, but since they all have their advantages and disadvantages, expert knowledge is needed for selecting the most appropriate encoding depending on the application.⁴
- One particular approach for encoding messages into \mathbb{G}_q is to define an explicit mapping from the message space into corresponding elements of \mathbb{G}_q . Obviously, this approach only works if the size of the message space is reasonably small to allow the enumeration of all elements. In e-voting applications, for example, where the number of voting options is usually very limited, single voting options are often encoded as prime numbers in \mathbb{G}_q and multiple voting options as corresponding

³ Implementing systematic group membership tests is a general best practice in cryptographic protocol design. Here is a current blog about this topic: <https://blog.trailofbits.com/2022/11/29/specialized-zero-knowledge-proof-failures>. We also refer to [CE16, DCE17] for a related discussions on Helios and TLS backdoors.

⁴ Examples of common message encodings $\Gamma : \mathbb{Z}_q \rightarrow \mathbb{G}_q$ are the following: (1) $\Gamma(m) = \left(\frac{m+1}{p}\right)(m+1) \bmod p$, (2) $\Gamma(x) = g^m \bmod p$, and (3) $\Gamma(m) = (m+1)^2 \bmod p$. In [EGR20], these encodings are called T2, T3, and T4, respectively.

products of prime numbers (examples of systems using this representation can be found in [Pe09, Gj11, REH23, Ha22]). After decryption, individual votes are obtained from factorizing this product (under the condition that the product is smaller than p). The problem in such a system, in which p is not a fixed system parameter (for example to support different security levels), this mapping needs to be refined depending on the selected safe prime p . This is not a difficult problem, because for n voting options one could simply select the n smallest primes in \mathbb{G}_q , and they can be computed and stored efficiently, but it is still a bothersome complication.

- Typically, applications relying on the hardness of the discrete logarithm require the selection of one or multiple group generators. Since every element of \mathbb{G}_q (except the identity element 1) generates the whole group, generators can be found easily. However, if again p is not a fixed system parameter, then the generator selection must be repeated whenever a new safe prime p is selected. In a mixnet-based e-voting application, in which N denotes the number of submitted votes (for example $N = 100'000$), the same amount N of verifiably random (independent) generators needs to be chosen as a preparatory step for proving the correctness of the shuffle. This is again not a very difficult problem [Nis13, Appendix A.2.3], but it also complicates the implementation of ElGamal for such purposes.

To illustrate the practical difficulties of using \mathbb{G}_q for ElGamal, consider the current system specification of the Swiss Post e-voting system [REH23, Section 3.4.2]. To cope with the fact that the system selects a different safe prime in every election, the encoding of the voting options into prime numbers of \mathbb{G}_q is implemented by an object called `pTable`. This object needs to be known by every protocol participant, and they all need to have exactly the same object for executing the protocol. The latest protocol version properly takes care of this problem using digital signatures, but it clearly adds to the overall protocol complexity. Similar complications exist in other implementations [EGR20].

1.2 Contribution and Paper Overview

In this paper, we propose an alternative group for ElGamal, denoted by $\mathbb{Z}_p^+ = \{1, \dots, q\}$, which eliminates all the practical disadvantages of \mathbb{G}_q listed in the previous subsection. We call it *multiplicative group of absolute values modulo p* , where $p = 2q + 1$ is a safe prime as for \mathbb{G}_q . Its group operation is only slightly more expensive than modular multiplication, and in modular exponentiations, the small overhead is required only once. Nevertheless, we can show that \mathbb{Z}_p^+ and \mathbb{G}_q are isomorphic, and that the isomorphism can be computed efficiently in both directions. This implies that the hardness of the DDH problem in \mathbb{Z}_p^+ must be the same as in \mathbb{G}_q .

The rest of the paper is organized as follows: in Sect. 2, we introduce the alternative group \mathbb{Z}_p^+ for ElGamal and prove the existence of an efficient isomorphism between \mathbb{Z}_p^+ and \mathbb{G}_q , in Sect. 3, we review the practical problems mentioned in the previous subsection from the

perspective of \mathbb{Z}_p^+ , in Sect. 4, we discuss the cost of membership testing based on some experimental results, and in Sect. 5, we summarize our findings and formulate a general recommendation and final conclusion.

2 An Alternative DDH Secure Group for ElGamal

The motivation for finding an alternative group for ElGamal comes from a proposal in [Ha22, Subsection 12.1] to optimize the performance of group membership testing in \mathbb{G}_q . The idea of the proposed optimization is to represent quadratic residues $x \in \mathbb{G}_q$ by one of their square roots

$$\sqrt{x} = \pm x^{\frac{q+1}{2}} \bmod p,$$

and to use this square root as a witness to test group membership by checking the equality $x = (\sqrt{x})^2 \bmod p$ (using a single modular multiplication). Using this technique, it turns out that group operations can be performed directly on the square roots. This observation is the starting point for the alternative group discussed in this paper.

2.1 Background on Group Theory

A group is an algebraic structure $(G, \circ, \text{inv}, e)$, where G is a finite set of *group elements*, $\circ : G \times G \rightarrow G$ a binary operation called *group operation*, $\text{inv} : G \rightarrow G$ a unary operation called *inverse*, and $e \in G$ a specific group element called *identity*, such that the following properties are satisfied:

- Associativity: $x \circ (y \circ z) = (x \circ y) \circ z, \forall x, y, z \in G$,
- Inverse: $x \circ \text{inv}(x) = e, \forall x \in G$,
- Identity: $x \circ e = e \circ x = x, \forall x \in G$.

It is common to simply use G for referring to the whole group $(G, \circ, \text{inv}, e)$. If a group G is finite, then $q = |G|$ is called *group order*. If a subset $H \subseteq G$ is closed under the group operation, i. e., if $x \circ y \in H$ for all $x, y \in H$, then $(H, \circ, \text{inv}, e)$ is called a *subgroup* of G . Lagrange's theorem states that the subgroup order $|H|$ always divides the group order $|G|$.

Groups are sometimes written additively as $(G, +, -, 0)$ or multiplicatively as $(G, \cdot, ^{-1}, 1)$, depending on the nature of the group operation. In multiplicative groups, exponentiation $x = g^u$ is defined as the result of applying the group operator $u - 1$ times to a given element $g \in G$, and $g^0 = 1$ is defined to be the base case for $u = 0$. If g and x are given, then $u = \log_g x$ is the *discrete logarithm* to the base g of x . If $u = \log_g x$ exists for every $x \in G$ in a finite group of order q , then g is called a *generator*, because it generates the whole set $G = \{g^u : 0 \leq u < q\}$ of group elements. If at least one generator exists, the group is called *cyclic*. In a prime-order group, due to Lagrange's theorem, every element of $G \setminus \{1\}$ is a generator.

If a generator g of a finite cyclic group of order q is given, then computing u from a single given value $x = g^u$ is called *discrete logarithm problem* (DL), computing $z = g^{uv}$ from two given values $x = g^u$ and $y = g^v$ is called *computational Diffie-Hellman problem* (CDH), and deciding whether $w = uv \bmod q$ holds for three given values $x = g^u$, $y = g^v$, and $z = g^w$ is called *decisional Diffie-Hellman problem* (DDH). Clearly, solving DL also solves CDH and DDH, and solving CDH also solves DDH, but the converse is not true. DDH is therefore the simplest of the three problems.

In certain groups, these problems seem to be computationally hard, which means that no known algorithm solves the problem efficiently in polynomial time. In the multiplicative group $\mathbb{Z}_p^* = \{1, \dots, p-1\}$ of integers modulo a prime p , both DL and CDH are commonly believed to be hard, but DDH can be solved efficiently using the Legendre or Jacobi symbol. In large subgroups of \mathbb{Z}_p^* , however, DDH also seems to be hard. One particular case of such a subgroup is the prime-order group $\mathbb{G}_q = \{x^2 \bmod p : x \in \mathbb{Z}_p^*\}$ of quadratic residues for a safe prime $p = 2q + 1$. In this particular case, we have $|\mathbb{Z}_p^*| = 2q$ and $|\mathbb{G}_q| = q$, i. e., \mathbb{G}_q contains exactly half of the elements of \mathbb{Z}_p^* . Group membership $x \in \mathbb{G}_q$ can be tested either by modular exponentiation $x^q \bmod p = 1$ or by computing the Legendre symbol $(\frac{x}{p}) = 1$.

2.2 The Multiplicative Group of Absolute Values Modulo p

Consider the additive group $(\mathbb{Z}_p, +, -, 0)$, where $\mathbb{Z}_p = \{0, \dots, p-1\}$ denotes the set of non-negative integers smaller than the prime modulus p . Additions in \mathbb{Z}_p are computed modulo p , which implies that the additive inverse $-x \bmod p$ (called *negation*) is equal to $p - x$ for $x \neq 0$ (trivially, -0 is equal to 0). For an odd prime $p > 2$, which implies $\mathbb{Z}_p = \{0, \dots, 2q\}$ for some integer $q = (p-1)/2$ (not necessarily prime), we can decompose \mathbb{Z}_p naturally into two disjoint sets

$$\mathbb{Z}_p^+ = \{1, \dots, q\} \text{ and } \mathbb{Z}_p^- = \{q+1, \dots, 2q\}$$

of *positive* and *negative* elements modulo p , respectively, with the property that $x \in \mathbb{Z}_p^+$ implies $-x \in \mathbb{Z}_p^-$ and $x \in \mathbb{Z}_p^-$ implies $-x \in \mathbb{Z}_p^+$.⁵ Furthermore, we can define the *absolute value* $|x| \in \mathbb{Z}_p^+$ naturally as $|x| = x$ for $x \in \mathbb{Z}_p^+$ and $|x| = -x \bmod p$ for $x \in \mathbb{Z}_p^-$ (with the trivial case of $|0| = 0$), which is equivalent to computing $|x| = \min(x, p-x) \in \mathbb{Z}_p^+$ using one negation and one comparison.

Given these ingredients, we are now ready propose an alternative group for ElGamal. For this, consider the algebraic structure $(\mathbb{Z}_p^+, \otimes, \text{inv}, 1)$ with the group operation and inverse defined as follows:

⁵ Our intuition for calling the element of the larger half of \mathbb{Z}_p negative is the fact that they can be written equivalently as $\mathbb{Z}_p^- = \{p-q, \dots, p-1\} = \{-q, \dots, -1\}$. The full set of integers modulo p can then be written as $\mathbb{Z}_p = \{-q, \dots, -1, 0, 1, \dots, q\} = \{-q, \dots, q\}$ with a natural symmetry between \mathbb{Z}_p^+ and \mathbb{Z}_p^- around 0 (a similar idea has been used in the definition of the *absolute Rabin-function* [FS00, Section 6], but the context there is slightly different).

$$x \otimes y \stackrel{\text{def}}{=} |xy \bmod p|,$$

$$\text{inv}(x) \stackrel{\text{def}}{=} |x^{-1} \bmod p|.$$

Thus, compared to the operations in \mathbb{Z}_p^* , the overhead of the operations in \mathbb{Z}_p^+ is limited to the computation of the absolute value, which requires one comparison and at most one negation. Note that to minimize the overhead, for example in exponentiations, computing absolute values can always be postponed to a single ultimate step. This follows from the simple observation that

$$\begin{aligned} |(|x| \cdot |y| \bmod p)| &= \begin{cases} |xy \bmod p|, & \text{if } x, y \in \mathbb{Z}_p^+, \\ |-xy \bmod p|, & \text{if } x \in \mathbb{Z}_p^+, y \in \mathbb{Z}_p^-, \\ |-xy \bmod p|, & \text{if } x \in \mathbb{Z}_p^-, y \in \mathbb{Z}_p^+, \\ |xy \bmod p|, & \text{if } x, y \in \mathbb{Z}_p^-. \end{cases} \\ &= |xy \bmod p|, \\ |(|x|^{-1} \bmod p)| &= \begin{cases} |x^{-1} \bmod p|, & \text{if } x \in \mathbb{Z}_p^+, \\ |-x^{-1} \bmod p|, & \text{if } x \in \mathbb{Z}_p^-. \end{cases} \\ &= |x^{-1} \bmod p|, \end{aligned}$$

hold for all $x, y \in \mathbb{Z}_p^*$. This means that we can start with positive elements from \mathbb{Z}_p^+ , apply the group operations (multiplication, inverse, division, exponentiation) in \mathbb{Z}_p^* , and ultimately map the result from \mathbb{Z}_p^* back to \mathbb{Z}_p^+ by calculating a single absolute value. The overhead of working in \mathbb{Z}_p^+ is therefore always a single comparison and at most one negation, which is negligible in cryptographic applications that use considerably more expensive operations such as modular exponentiations.

Using the above property of the absolute value, it is simple to demonstrate that $(\mathbb{Z}_p^+, \otimes, \text{inv}, 1)$ satisfies the properties of a group:

- **Associativity:** $x \otimes (y \otimes z) = |x(|yz \bmod p|) \bmod p|$
 $= |x(yz \bmod p) \bmod p| = |xyz \bmod p|$
 $= |(xy \bmod p)z \bmod p| = |(|xy \bmod p|)z \bmod p|$
 $= (x \otimes y) \otimes z. \quad \blacksquare$
- **Inverse:** $x \otimes \text{inv}(x) = |x(|x^{-1} \bmod p|) \bmod p|$
 $= |x(x^{-1} \bmod p) \bmod p| = |xx^{-1} \bmod p| = |e| = e. \quad \blacksquare$
- **Identity:** $e \otimes x = |xe \bmod p| = |x| = x,$
 $e \otimes x = |xe \bmod p| = |x| = x. \quad \blacksquare$

We call \mathbb{Z}_p^+ *multiplicative group of absolute values modulo p* . In Appendix A, a numerical example is given to demonstrate computations in \mathbb{Z}_p^+ and its application to ElGamal. Note that so far we have not imposed any restrictions on p other than assuming that $p > 2$ is an odd prime, and we do not know whether DL, CDH, or DDH are hard problems in this group.

Another way of proving that \mathbb{Z}_p^+ with the operations as defined above forms a group comes from defining \mathbb{Z}_p^+ as the *quotient group* $\mathbb{Z}_p^*/\mathbb{G}_2$, where $\mathbb{G}_2 = \{1, p-1\}$ denotes the trivial subgroup of \mathbb{Z}_p^* of order 2. Since modular multiplication is commutative, it follows that \mathbb{G}_2 is a normal subgroup of \mathbb{Z}_p^* , which implies that $\mathbb{Z}_p^*/\mathbb{G}_2 = \{a \mathbb{G}_2 : a \in \mathbb{Z}_p^*\}$ with an operation defined as $(a \mathbb{G}_2)(b \mathbb{G}_2) = (ab) \mathbb{G}_2$ forms a group. Note that the $q = [\mathbb{Z}_p^* : \mathbb{G}_2] = \frac{p-1}{2}$ elements of $\mathbb{Z}_p^*/\mathbb{G}_2$ are the cosets $\{1, p-1\}, \{2, p-2\}, \dots, \{q, q+1\}$ of \mathbb{G}_2 , from which we obtain \mathbb{Z}_p^+ by simply selecting the smaller of the two values as coset representatives:

$$\mathbb{Z}_p^+ = \{\min(x, y) : \{x, y\} \in \mathbb{Z}_p^*/\mathbb{G}_2\} = \{1, \dots, q\}.$$

This alternative definition of \mathbb{Z}_p^+ , together with the above-mentioned group operation defined for the quotient group, leads directly to the group operation defined for \mathbb{Z}_p^+ at the beginning of this section.

2.3 Proving the Existence of an Isomorphism

To use \mathbb{Z}_p^+ for ElGamal, we must have good reasons to believe that DDH (and therewith CDH and DL) is a hard problem. In the special case of a safe prime $p = 2q + 1$, where q is also prime, we can demonstrate that DDH is equally hard in \mathbb{Z}_p^+ and \mathbb{G}_q by showing that these groups are isomorphic and that the isomorphism can be computed efficiently in both directions.⁶ Under this premise, an efficient DDH solver in \mathbb{Z}_p^+ would immediately imply an efficient DDH solver in \mathbb{G}_q by applying the isomorphism forth and back. Since this conjecture is in contradiction with current beliefs that DDH is hard in the subgroup of quadratic residues, we can assume that DDH is also hard in \mathbb{Z}_p^+ . In other words, \mathbb{Z}_p^+ and \mathbb{G}_q are equally applicable to cryptographic applications.

Two groups G and H are called *isomorphic*, denoted by $G \cong H$, if a structure-preserving (bijective and homomorphic) mapping $\phi : G \rightarrow H$ exists. For proving $\mathbb{Z}_p^+ \cong \mathbb{G}_q$, it is therefore sufficient to find a single candidate mapping $\phi : \mathbb{Z}_p^+ \rightarrow \mathbb{G}_q$ (and therefore $\phi^{-1} : \mathbb{G}_q \rightarrow \mathbb{Z}_p^+$) and to prove that the mapping is bijective and homomorphic. Our proposal is the following:

$$\begin{aligned} \phi(x) &= x^2 \bmod p, \text{ for } x \in \mathbb{Z}_p^+, \\ \phi^{-1}(y) &= |\sqrt{y}| \bmod p = |y^{\frac{q+1}{2}}| \bmod p, \text{ for } y \in \mathbb{G}_q. \end{aligned}$$

⁶ Note that p being a safe prime is not a necessary condition for finding an efficient isomorphism between the multiplicative group of absolute values and the group of quadratic residues modulo p . However, since q being prime ensures the absence of non-trivial subgroups, it is the most interesting case for cryptographic applications.

Note that, given this definition, the proposed mapping is efficiently computable in both directions, with essentially one modular multiplication for ϕ and one modular exponentiation for ϕ^{-1} .

A precondition for ϕ being a bijection is already met by the fact $q = |\mathbb{Z}_p^+| = |\mathbb{G}_q|$ is the order of both the domain and the codomain. What then remains to prove is that ϕ^{-1} inverts ϕ for all $x \in \mathbb{Z}_p^+$. From the fact that $x^q \equiv \pm 1 \pmod{p}$, depending on whether $x \in \mathbb{G}_q$ or $x \notin \mathbb{G}_q$, it follows that this is actually the case:

$$\begin{aligned}\phi^{-1}(\phi(x)) &= |(x^2 \bmod p)^{\frac{q+1}{2}} \bmod p| = |(x^2)^{\frac{q+1}{2}} \bmod p| \\ &= |x^{q+1} \bmod p| = |xx^q \bmod p| = |\pm x| = x.\end{aligned}$$

To prove that ϕ is homomorphic, we must show that $\phi(x \otimes y) = \phi(x)\phi(y) \bmod p$ holds for all $x, y \in \mathbb{Z}_p^+$:

$$\begin{aligned}\phi(x \otimes y) &= (|xy \bmod p|)^2 \bmod p \\ &= \begin{cases} (xy)^2 \bmod p, & \text{if } xy \bmod p \leq q, \\ (-xy)^2 \bmod p, & \text{if } xy \bmod p > q. \end{cases} \\ &= (xy)^2 \bmod p = (x^2 \bmod p)(y^2 \bmod p) \bmod p \\ &= \phi(x)\phi(y) \bmod p.\end{aligned}$$

Put together, this proves that $\mathbb{Z}_p^+ \cong \mathbb{G}_q$, and therefore we conclude that DDH is equally hard in \mathbb{Z}_p^+ and in \mathbb{G}_q . This means that we can recommend using \mathbb{Z}_p^+ for ElGamal without any restrictions or additional precautions. Note that due the symmetry between \mathbb{Z}_p^+ and \mathbb{Z}_p^- , a similar isomorphic group exists for \mathbb{Z}_p^- .

3 Discussion of Properties

If the group \mathbb{Z}_p^+ is used for ElGamal instead of \mathbb{G}_q , we benefit from the property that the new message space is compatible across different values of p in the sense that $\mathbb{Z}_p^+ \subset \mathbb{Z}_{p'}^+$ for $p < p'$. The absence of such a property for \mathbb{G}_q is the main reasons for the practical disadvantages listed in Sect. 1.1. We can now review the topics from this list in the light of \mathbb{Z}_p^+ :

- Testing membership $x \in \mathbb{Z}_p^+$ is very efficient, since only two comparisons $1 \leq x$ and $x \leq q$ are necessary (note that $1 \leq x$ is actually a signum test $\text{sgn}(x) = 1$). Compared to computing $x^q \bmod p = 1$ or equivalently $\left(\frac{x}{p}\right) = 1$ for testing membership in \mathbb{G}_q , the cost of two comparisons is negligible, as we can see in the performance results discussed in Sect. 4.
- Since $\mathbb{Z}_p^+ = \{1, \dots, q\}$ is a smooth message space in the sense that all consecutive elements between a lower and an upper limit are group members, the encoding of a

general-purpose message $m \in \{0, 1\}^n$ of length $n < \|q\|$ is much simpler than in \mathbb{G}_q . In the most straightforward encoding, where the bits of m are simply interpreted as a binary number, only the special case of $m = 0$ (all n bits set to 0) is excluded by \mathbb{Z}_p^+ . In applications where $m = 0$ is a possible message, one could either generally increase every m by 1 or substitute $m = 0$ by $m = q$. Both options can be regarded as a bijective mapping between \mathbb{Z}_q and \mathbb{Z}_p^+ . Therefore, different values for p only have an effect on the message length n , but not on the encoding of the messages itself.

- If a small message space is encoded into \mathbb{Z}_p^+ by defining an explicit mapping for each possible message, then this mapping can be defined independently of the choice of p . In the particular case, where the n voting options in an e-voting system are encoded as prime numbers, we can always use the exact same set of prime numbers, for example the n smallest prime numbers $p_1 = 2, p_2 = 3, p_3 = 5, \dots, p_n$. Redefining this mapping when p changes is therefore no longer necessary.
- Another advantage in the same context is the increased capacity of a single message for encoding combinations of voting options by corresponding products of prime numbers, even if this is rarely a problem in practice. The advantage comes from the compactness of the encoding in the sense that the n smallest prime numbers lie closer to each other in \mathbb{Z}_p^+ and therefore require less bits than in \mathbb{G}_q . If voters can select up to $k < n$ different voting options in a k -out-of- n election, then the bit length $\|p\|$ may impose an upper limit for k depending on n . Tab. 1 shows these upper bounds k_{\max} for $\|p\| \in \{2048, 3072\}$ and different values of n . The values are derived from the “worst case”, in which the voter selects the k largest from the n smallest prime group members. The values given under ℓ_{\max} are the sizes of corresponding combined vote encodings. As one can see, the limits for \mathbb{G}_q are approximately 10% smaller than the limits for \mathbb{Z}_p^+ .
- The problem of selecting suitable group generators is much simpler in \mathbb{Z}_p^+ , because any of the $q - 1$ values in the range $2 \leq g \leq q$ is a generator of \mathbb{Z}_p^+ , and also of any larger group $\mathbb{Z}_{p'}^+$, with $p' > p$. The selection can therefore be fixed independently of the actual choice of p . For example, if k (non-independent) generators are needed in an application, then one could simply take $g_1 = 2, g_2 = 3, \dots, g_k = k + 1$. If independent generators are needed, they must be chosen verifiably at random as for \mathbb{G}_q , but then they can be used universally across different groups (as long as p and p' are also picked verifiably at random).

This discussion shows that each of the practical disadvantages of using \mathbb{G}_q for ElGamal turns into an advantage for \mathbb{Z}_p^+ at almost no cost.

4 The Cost of Membership Testing

To underline our statements about the performance of different group membership tests, we conducted some experiments with different implementations of modular exponentiation

n	$\ p\ = 2048 \text{ bits}$						$\ p\ = 3072 \text{ bits}$					
	\mathbb{G}_q			\mathbb{Z}_p^+			\mathbb{G}_q			\mathbb{Z}_p^+		
	k_{\max}	$\ p_n\ $	ℓ_{\max}	k_{\max}	$\ p_n\ $	ℓ_{\max}	k_{\max}	$\ p_n\ $	ℓ_{\max}	k_{\max}	$\ p_n\ $	ℓ_{\max}
100	(99)	11	856	(99)	10	729	(99)	11	856	(99)	10	729
200	(199)	12	1958	(199)	11	1703	(199)	12	1958	(199)	11	1703
300	176	13	2038	201	11	2046	285	13	3066	(299)	11	2765
400	167	13	2046	186	12	2039	256	13	3062	290	12	3065
500	161	13	2042	178	12	2041	245	13	3064	273	12	3066
600	157	14	2046	172	13	2037	238	14	3069	263	13	3070
700	153	14	2038	168	13	2041	232	14	3064	255	13	3064
800	151	14	2046	165	13	2047	228	14	3070	249	13	3062
900	148	14	2037	162	13	2045	224	14	3066	245	13	3070
1000	146	15	2039	159	13	2038	221	15	3070	241	13	3069
1200	143	15	2047	155	14	2037	215	15	3066	234	14	3061
1400	140	15	2040	152	14	2039	211	15	3065	229	14	3060
1600	138	15	2044	150	14	2047	207	15	3058	225	14	3061
1800	136	16	2040	147	14	2036	205	16	3069	222	14	3066
2000	134	16	2035	145	15	2034	202	16	3061	219	15	3065

Tab. 1: Prime number encoding of combined voting options in k -out-of- n elections. In cases without an upper limit for k other than $k < n$, $k_{\max} = n - 1$ is shown in parentheses (for example $k_{\max} = 99$ for $n = 100$). The values shown for \mathbb{G}_q are approximate, because they depend slightly on the actual choice of p .

and the Jacobi symbol (which is equivalent to the Legendre symbol when p is prime). The results of these experiments are shown in Tab. 2. It is interesting to observe that modular exponentiation in C (using the GMP library) is approximately 35% faster than in Java, whereas computing the Jacobi symbol in C is more than 99 times faster than in Java (using the Bouncy Castle library). Therefore, it seems that the Jacobi symbol implementation in Bouncy Castle is far from being optimal (it is only between 3 to 5 times faster than modular exponentiation). The same holds for the modular exponentiation implementation in the Javascript library `verificatum-vjsc`, which is more than 30 times slower than in Java and about 5 times slower than in Python.

Our measurements also show that the GMP implementation of the Jacobi symbol is the only option with negligible costs for conducting 10'000 group membership tests in \mathbb{G}_q . Even for 1 million membership tests, which GMP could handle approximately in 10 seconds for 2048-bits integers and in 20 seconds for 3072-bits integers, performing these tests seems not to grow into a major factor compared to other computations in corresponding applications. Note that a batch of exactly one million group elements results from the output of a mixnet with 50'000 input ElGamal encryptions and 5 mixers (using Wikström's shuffle proof [TW10, LH14]). In all considered cases, the cost for testing group membership in \mathbb{Z}_p^+ remains negligible, and it will only grow to approximately 20 milliseconds for 1 million tests.

	$\ p\ = 2048 \text{ bits}$			$\ p\ = 3072 \text{ bits}$		
	$x \in \mathbb{Z}_p^+$	$x \in \mathbb{G}_q$		$x \in \mathbb{Z}_p^+$	$x \in \mathbb{G}_q$	
	$0 < x < q$	$(\frac{x}{p}) = 1$	$x^q \bmod p = 1$	$0 < x < q$	$(\frac{x}{p}) = 1$	$x^q \bmod p = 1$
C	< 1ms	98ms	23'224ms	< 1ms	186ms	72'992ms
Java	< 1ms	12'871ms	35'705ms	< 1ms	27'132ms	114'262ms
Python	< 1ms	15'447ms	243'561ms	< 1ms	34'762ms	691'568ms
Javascript	< 1ms	12'453ms	692'821ms	< 1ms	23'878ms	2'162'474ms

Tab. 2: Performance of membership testing in \mathbb{Z}_p^+ and \mathbb{G}_q using different methods and programming languages. The measurements were conducted on a MacBook Pro (2.3 GHz 8-Core Intel Core i9) using a single-core process over a batch of 10'000 test vectors, each of which consisting of an integer x and a safe prime $p = 2q + 1$ of the required length of either 2048 or 3072 bits. For C, we used the functions `mpz_jacobi` and `mpz_powm` from the GMP library (version 6.2.1). For Java, we used the build-in method `BigInteger::modPow` and the method `IntegerFunctions::jacobi` from the Bouncy Castle library (version 1.70). For Javascript, we used the functions `modPow` and `legendre` from Wikström's `verificatum-vjsc` library (version 1.1.1). And for Python, we used the `pow` and `jacobi_symbol` functions from the `SymPy` library (version 1.12).⁷

5 Conclusion

In this paper, we have shown that the commonly used group \mathbb{G}_q of quadratic residues modulo a safe prime should probably no longer be regarded as the best choice in practical applications of the ElGamal cryptosystem, which depends on the intractability of the DDH problem. We demonstrated that this group has several drawbacks, which make practical implementations more complicated, error-prone, and less efficient. Our proposal of using \mathbb{Z}_p^+ as an alternative group for ElGamal eliminates these drawbacks completely while preserving the intractability of the DDH problem. Therefore, to profit maximally from the advantages of \mathbb{Z}_p^+ , we generally recommend the replacement of \mathbb{G}_q by \mathbb{Z}_p^+ in applications of ElGamal. Existing implementations can be simplified accordingly.

A first implementation of \mathbb{Z}_p^+ can be found in the Java class `ZPlus.java` in the `utilities` submodule of the `OpenCHVote` project.⁸ In Version 1.3 of this library, this class replaces the implementation of \mathbb{G}_q from previous versions. This replacement implied a number of simplifications at different places of the CHVote protocol specification and the `OpenCHVote` code base. Examples are the implementations of the algorithms `GetPrimes` and `GetGenerators`,

⁷ Note that the Python library `SymPy` provides three similar functions `jacobi_symbol`, `legendre_symbol`, and `is_quad_residue`, each of which with a different implementation. While `jacobi_symbol` implements an iterative version of the efficient $O(\log x \log p)$ algorithm from [MOV96, Section 2.4.5], `legendre_symbol` and `is_quad_residue` both compute $x^{(p-1)/2} \bmod p$ if p is prime, i.e., their performance is equal to the `pow` function. Consequently, users of `SymPy` are likely to unintentionally pick the wrong function with sub-optimal performance. Problems like this can be avoided when working with \mathbb{Z}_p^+ .

⁸ See <https://gitlab.com/openchvote/cryptographic-protocol>.

which are now independent of any group parameters, and the removal of the algorithm `GetRandomElement`, which is now a special case of `GetRandomInteger`.

Acknowledgments

We thank Philipp Locher for his help in developing the initial idea of this approach and for providing the Javascript code to conduct the experiments with the `verificatum-vjsc` library. Our thanks also go to Pierrick Gaudry for pointing out the possibility of defining \mathbb{Z}_p^+ as a quotient group and to François Weissbaum and Florian Moser for proofreading an early draft of this paper. Finally, we would like to thank the reviewers for their valuable comments and exceptionally constructive suggestions for improvements.

Bibliography

- [Bo98] D. Boneh. The decision Diffie-Hellman problem. In J. Buhler, editor, *ANTS-III, 3rd International Symposium on Algorithmic Number Theory*, LNCS 1423, pages 48–63, Portland, Oregon, USA, 1998.
- [CE16] N. Chang-Fong and A. Essex. The cloudier side of cryptographic end-to-end verifiable voting: A security analysis of Helios. In W. Robertson and D. Balzarotti, editors, *ACSAC'16, 32nd Annual Conference on Computer Security Applications*, pages 324–335, Los Angeles, USA, 2016.
- [DCE17] K. Dorey, N. Chang-Fong, and A. Essex. Indiscreet logs: Diffie-Hellman backdoors in TLS. In A. Juels and P. Traynor, editors, *NDDS'17, 24th Annual Network and Distributed System Security Symposium*, San Diego, USA, 2017.
- [EGR20] M. El Laz, B. Grégoire, and T. Rezk. Security analysis of ElGamal implementations. In P. Samarati, S. De Capitani di Vimercati, M. S. Obaidat, and J. Ben-Othman, editors, *SECRYPT'20, 17th International on Security and Cryptography*, pages 310–321, Paris, France, 2020.
- [FS00] R. Fischlin, , and C. Schnorr. Stronger security proofs for RSA and Rabin bits. *Journal of Cryptology*, 13:221–244, 2000.
- [Gj11] K. Gjølsteen. The Norwegian Internet voting protocol. In A. Kiayias and H. Lipmaa, editors, *VoteID'11, 3rd International Conference on E-Voting and Identity*, LNCS 7187, pages 1–18, Tallinn, Estonia, 2011.
- [Ha22] R. Haenni, R. E. Koenig, P. Locher, and E. Dubuis. CHVote protocol specification – version 3.4. *IACR Cryptology ePrint Archive*, 2017/325, 2022.
- [LH14] P. Locher and R. Haenni. A lightweight implementation of a shuffle proof for electronic voting systems. In E. Plödereder, L. Grunske, E. Schneider, and D. Ull, editors, *INFORMATIK 2014, 44. Jahrestagung der Gesellschaft für Informatik*, number P-232 in Lecture Notes in Informatics, pages 1391–1400, Stuttgart, Germany, 2014.
- [MOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, USA, 1996.

- [Nis13] Digital signature standard (DSS). FIPS PUB 186-4, National Institute of Standards and Technology (NIST), 2013.
- [Pe09] K. Peng. A hybrid e-voting scheme. In F. Bao, H. Li, and G. Wang, editors, *ISPEC'09, 5th Information Security Practice and Experience Conference*, LNCS 5451, pages 195–206, Xi'an, China, 2009.
- [REH23] H. Renold, O. Esseiva, and T. Hofer. Swiss Post Voting System – System Specification – Version 1.3.1. Technical report, Swiss Post Ltd., Bern, Switzerland, June 2023.
- [TW10] B. Terelius and D. Wikström. Proofs of restricted shuffles. In D. J. Bernstein and T. Lange, editors, *AFRICACRYPT'10, 3rd International Conference on Cryptology in Africa*, LNCS 6055, pages 100–113, Stellenbosch, South Africa, 2010.

A Numerical Example

To illustrate the proposed approach with a numerical example, we consider the groups obtained for $p = 23$ (safe prime) and $q = 11$:

$$\mathbb{G}_{11} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\},$$

$$\mathbb{Z}_{23}^+ = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

In Tab. 3, we show the complete multiplication and exponentiation tables for both groups. The inverse elements can be observed in the multiplication tables, where each row and each column contains exactly one entry for the identity element 1, or in the last column ($y = 10$) of the exponentiation table (for example $2^{-1} = 12$ in \mathbb{G}_{11} and $2^{-1} = 11$ in \mathbb{Z}_{23}^+).

The isomorphism $\phi(x) = x^2 \bmod 23$ as defined in Sect. 2.3 leads to the following map between the elements of \mathbb{G}_{11} and \mathbb{Z}_{23}^+ :

$x \in \mathbb{Z}_{23}^+$	1	2	3	4	5	6	7	8	9	10	11
$\phi(x) \in \mathbb{G}_{11}$	1	4	9	16	2	13	3	18	12	8	6

If we select $g = 2$ (element of both groups) as a common generator, then $(sk, pk_1) = (7, 13)$ would be a valid ElGamal key pair for \mathbb{G}_{11} , and $(sk, pk_2) = (7, 10)$ would be the corresponding key pair for \mathbb{Z}_{23}^+ with the same private key $sk = 7$ from \mathbb{Z}_{11} . If we chose $m = 8$ (element of both groups) as message to encrypt with randomization $r = 4$, then

$$e_1 = (2^4 \bmod 23, 8 \cdot 13^4 \bmod 23) = (16, 6) \in \mathbb{G}_{11} \times \mathbb{G}_{11},$$

$$e_2 = (|2^4 \bmod 23|, |8 \cdot 10^4 \bmod 23|) = (7, 6) \in \mathbb{Z}_{23}^+ \times \mathbb{Z}_{23}^+,$$

are the resulting ElGamal ciphertexts. In both cases, we can perform the decryption using the private key $sk = 7$ to obtain the original plaintext message:

$$m = \begin{cases} 6/16^7 \bmod 23 = 6/18 \bmod 23 = 6 \cdot 9 \bmod 23 = 8, \\ |6/7^7 \bmod 23| = |6/5 \bmod 23| = |6 \cdot 9 \bmod 23| = 8. \end{cases}$$

		y															
x	\mathbb{G}_{11}	1	2	3	4	6	8	9	12	13	16	18					
	1	1	2	3	4	6	8	9	12	13	16	18					
	2	2	4	6	8	12	16	18	1	3	9	13					
	3	3	6	9	12	18	1	4	13	16	2	8					
	4	4	8	12	16	1	9	13	2	6	18	3					
	6	6	12	18	1	13	2	8	3	9	4	16					
	8	8	16	1	9	2	18	3	4	12	13	6					
	9	9	18	4	13	8	3	12	16	2	6	1					
	12	12	1	13	2	3	4	16	6	18	8	9					
	13	13	3	16	6	9	12	2	18	8	1	4					
	16	16	9	2	18	4	13	6	8	1	3	12					
	18	18	13	8	3	16	6	1	9	4	12	2					

$$z = xy \bmod 23$$

		y										
x	\mathbb{Z}_{23}^+	1	2	3	4	5	6	7	8	9	10	11
	1	1	2	3	4	5	6	7	8	9	10	11
	2	2	4	6	8	10	11	9	7	5	3	1
	3	3	6	9	11	8	5	2	1	4	7	10
	4	4	8	11	7	3	1	5	9	10	6	2
	5	5	10	8	3	2	7	11	6	1	4	9
	6	6	11	5	1	7	10	4	2	8	9	3
	7	7	9	2	5	11	4	3	10	6	1	8
	8	8	7	1	9	6	2	10	5	3	11	4
	9	9	5	4	10	1	8	6	3	11	2	7
	10	10	3	7	6	4	9	1	11	2	8	5
	11	11	1	10	2	9	3	8	4	7	5	6

$$z = |xy \bmod 23|$$

		y											
\mathbb{G}_{11}		0	1	2	3	4	5	6	7	8	9	10	
x	1	1	1	1	1	1	1	1	1	1	1	1	
	2	1	2	4	8	16	9	18	13	3	6	12	
	3	1	3	9	4	12	13	16	2	6	18	8	
	4	1	4	16	18	3	12	2	8	9	13	6	
	6	1	6	13	9	8	2	12	3	18	16	4	
	8	1	8	18	6	2	16	13	12	4	9	3	
	9	1	9	12	16	6	8	3	4	13	2	18	
	12	1	12	6	3	13	18	9	16	8	4	2	
	13	1	13	8	12	18	4	6	9	2	3	16	
	16	1	16	3	2	9	6	4	18	12	8	13	
	18	1	18	2	13	4	3	8	6	16	12	9	

$$z = x^y \bmod 23$$

		y											
\mathbb{Z}_{23}^+		0	1	2	3	4	5	6	7	8	9	10	
x	1	1	1	1	1	1	1	1	1	1	1	1	
	2	1	2	4	8	7	9	5	10	3	6	11	
	3	1	3	9	4	11	10	7	2	6	5	8	
	4	1	4	7	5	3	11	2	8	9	10	6	
	5	1	5	2	10	4	3	8	6	7	11	9	
	6	1	6	10	9	8	2	11	3	5	7	4	
	7	1	7	3	2	9	6	4	5	11	8	10	
	8	1	8	5	6	2	7	10	11	4	9	3	
	9	1	9	11	7	6	8	3	4	10	2	5	
	10	1	10	8	11	5	4	6	9	2	3	7	
	11	1	11	6	3	10	5	9	7	8	4	2	

$$z = |x^y \bmod 23|$$

Tab. 3: Multiplication and exponentiation tables for \mathbb{G}_{11} and \mathbb{Z}_{23}^+ .

Faster coercion-resistant e-voting by encrypted sorting

Diego F. Aranha¹ Michele Battagliola² Lawrence Roy³

Abstract: Coercion resistance is one of the most challenging security properties to achieve when designing an e-voting protocol. The JCJ voting scheme, proposed in 2005 by Juels, Catalano and Jakobsson, is one of the first voting systems where coercion-resistance was rigorously defined and achieved, making JCJ the benchmark for coercion-resistant protocols. Recently, the coercion-resistance definition proposed in JCJ has been disputed and improved by Cortier, Gaudry, and Yang. They identified a major problem, related to leakage of the number of discarded votes by revoting; and proposed CHide, a new protocol that solves the issue and satisfies a stronger security notion. In this work we present an improved version of CHide, with complexity $O(n \log n)$ instead of $O(n^2)$ in the number n of received ballots, that relies on sorting encrypted ballots to make the tallying phase faster. The asymptotic complexity of our protocol is competitive with other state-of-the-art coercion-resistant voting protocols satisfying the stronger notion for coercion resistance.

1 Introduction

Internet voting is a type of electronic voting that allows voters to cast their ballot remotely through the Internet, without the need of physically going to a polling station. Since the first attempts of introducing the Internet as a legally binding way of casting votes in Estonia and the United States in the early 2000's, Internet voting solutions increased in popularity and are currently used to varying degrees in several countries around the world [Idea; Ifes]. Prominent examples include Switzerland [HPT22], Canada [CAE19] and Australia [HT15].

As with other electronic voting initiatives, the promises of Internet voting are higher voter turnout, lower cost and accessibility [Li21]; potentially at the expense of simplicity, transparency and privacy. Cryptographic protocols are particularly suited to the task, and in recent years many protocols were designed to achieve secure Internet-based elections that ensure voter privacy, vote verifiability and the correctness of the outcome [Ad08; CCM08; RRI16].

There is one additional threat, however, that is equally crucial to address in a fair and democratic election process: *coercion resistance*. Informally, a coercion-resistant protocol must defend voters from attackers that pressure them to vote in a specific way, either through threats or rewards. Because of its remote nature, Internet voting substantially increases the attack surface with respect to coercion resistance, since it introduces new and convenient attacks compared to voting in person at the polling station. These include coercing voters to reveal all the voting material, or monitoring their behavior during the election day.

¹ Aarhus University, Aarhus, Denmark dfaranha@cs.au.dk

² Università degli Studi di Trento, Trento, Italy, michele.battagliola@unitn.it

³ Aarhus University, Aarhus, Denmark lance.roy@cs.au.dk

JCJ Protocol. Juels, Catalano and Jakobsson [JCJ10] achieved important progress in this field by proposing one of the first formal definitions of coercion resistance and designing a protocol to achieve it. To this date, JCJ still remains the reference point for research on the topic. Roughly speaking, a voting protocol is coercion resistant if and only if voters are able to generate some kind of *fake credential* that could be handed over to the coercer in case of attack, preserving the original legitimate ones and thus their ability to vote [JCJ10]. Votes with fake credentials are discarded later, in the *cleansing* phase of the election process.

One of the main drawbacks of JCJ and related protocols, such as Civitas [CCM08], is their quadratic complexity⁴, since they usually require to check each credential against the ones in the following votes. Consequently, this approach to voting has generally limited the scalability of the protocol.

JCJ Leakage. Recently, the security definition presented in JCJ was disputed, for example in [CGY22b] and [HS19], due to its limitation in handling revotes and ballots cast under invalid credentials. Ideally, the only types of leakage that should be allowed are those that inevitably arise from the election result. In particular, an unavoidable leakage is the difference between the total processed ballots and the number of valid votes. In [CGY22b] Cortier, Gaudry and Yang showed that the JCJ protocol leaks significantly more than this simple difference. Since the votes with duplicate credentials (i.e. the revotes) and votes with invalid credentials are handled and discarded separately, the JCJ protocol leaks the size of both sets individually, instead of leaking only the size of their union. Moreover, they presented CHide, an improved version of the original JCJ protocol that solves this particular security issue.

Contributions. However, CHide brings us back to the original scaling issue present in JCJ, as it also takes quadratic time in the number n of received ballots.⁵ The techniques used to run JCJ in linear time [Rø20] require leaking the duplicated and invalid credentials separately, and fail to generalize easily to CHide. In this work we overcome this issue and present an improved version of CHide, with complexity $O(n \log n)$ instead of $O(n^2)$, using sorting over encrypted data to make the tallying protocol faster. The resulting protocol achieves asymptotic complexity competitive with other state-of-the-art coercion-resistant voting protocols satisfying a stronger security notion. We also show an improved version of the protocol that removes the registrars altogether.

Organization. The rest of the paper is organized as follows. We start with the building blocks of our protocol in Sect. 2. In Sect. 3, we describe our protocol and prove its security for stronger coercion resistance in Sect. 4. We finish with estimates of efficiency gains in Sect. 5 and conclude in Sect. 6.

⁴ Civitas mitigates this quadratic complexity by splitting the voters into blocks and tally each block separately. However, this significantly increases leakage, revealing how many votes were eliminated for each block, rather than just once for the whole election.

⁵ The CHide preprint was independently updated by the authors to address this issue. We discuss further in Sect. 5.

2 Cryptographic Primitives

ElGamal Encryption Scheme. Due to its homomorphic properties, the ElGamal encryption scheme [Ga85] is a popular choice for designing voting schemes.

Let \mathbb{G} be a multiplicative group of order q , with generator g , for which solving the Decisional Diffie Hellman (DDH) problem is hard. The private key sk is sampled at random from \mathbb{Z}_q , while the public key pk is g^{sk} . The encryption of a message m is defined as $\text{Enc}(m, pk; r) = (g^r, g^m \cdot pk^r) \in \mathbb{G}^2$ where $r \in \mathbb{Z}_q$ is a random value. We omit to explicitly write the randomness when not strictly necessary.

Let $E_0 = (1, 1)$, $E_1 = (1, g)$, and $E_{-1} = (1, g^{-1})$ be the respective encryptions of 0, 1, -1 with randomness 0. Re-encryption can be done by multiplying a ciphertext by an encryption of 0. In particular, let $X \in \mathbb{G}^2$ be an ElGamal ciphertext, then we define $\text{ReEnc}(X, pk; r) = X \cdot \text{Enc}(0, pk; r)$, where the multiplication operation is component-wise.

For a number n_T of election trustees, we use a (t, n_T) -threshold version of ElGamal, so pk is produced via a distributed key generation, and a minimum of $t + 1$ parties are required to jointly decrypt.

Designated-Verifier Zero-Knowledge Proof. Similarly to JCJ and CHide, our protocol uses Designated-Verifier Zero Knowledge Proofs (DVZKPs) [JSI96]. Roughly speaking, a DVZKP is a zero-knowledge proof (ZKP) in which only the verifier designated by the prover is able to be convinced about the correctness of the proof. In particular the verifier V holds a key pair. Using the public key, the prover produces a proof for a statement, such that only V is convinced that the statement is true. This is achieved by allowing V to produce fake but valid DVZKPs for any statement, using their private key.

In particular, the usage of a DVZKP instead of a traditional ZKP is crucial for the evasion strategy, since it allows voters to be sure about the credentials received and, at the same time, they are able to produce fake credentials alongside fake proofs to hand over in case of attacks.

Circuits over encrypted bits. The basic building block for our tallying algorithm is the CGate protocol, originally presented in [ST04], in the re-randomized version [CGY22a]. Informally, on input of two encryptions X, Y of x and y , respectively, with $y \in \{0, 1\}$ it outputs a ciphertext Z which is the encryption of xy . If both x and y are bits, this allows to compute the conjunction And. Since the Not operator can be computed as $\text{Not}(X) = E_1 \cdot X^{-1}$, every other Boolean operator can be easily implemented by combining these two. Algorithm 1 formalizes the idea.

In particular, for our sorting algorithm, we need an operator for equality $\text{Eq}(X, Y) = \text{Not}(XY / \text{CGate}(X, Y)^2)$ and a less-than operator $\text{Less}(X, Y) = Y / \text{CGate}(X, Y)$. Indeed, let a, b be two values and A_1, \dots, A_k and B_1, \dots, B_k their bitwise encryptions. To check $a < b$ keeping the result encrypted we use this recursive formula: $L_0 = 0$, $L_i = \text{Less}(A_i, B_i) \cdot \text{CGate}(L_{i-1}, \text{Eq}(A_i, B_i))$ for $i = 1, \dots, n$. At the end L_k is the encryption of $a < b$.

Algorithm 1 CGate protocol

Require: X, Y encryptions of x, y , with $y \in \{0, 1\}$, number of participants a .
Ensure: Z an encryption of xy .

- 1: Compute $Y_0 = E_{-1} \cdot Y^2$ and set $X_0 = X, a = t + 1$
- 2: **for** $i = 1$ to a **do**
- 3: Participant P_i picks $r_1, r_2 \in \mathbb{Z}_q$ and $s \in \{-1, 1\}$ randomly
- 4: P_i computes $X_i = \text{ReEnc}(X_{i-1}^s, \text{pk}; r_1)$ and $Y_i = \text{ReEnc}(Y_{i-1}^s, \text{pk}; r_2)$
- 5: P_i produces a ZKP π_i that X_i and Y_i are well formed
- 6: P_i reveals X_i, Y_i and π_i
- 7: **end for**
- 8: P_1, \dots, P_a verify all the proofs. Let $\Pi = (X_1, Y_1, \pi_1) || \dots || (X_a, Y_a, \pi_a)$.
- 9: P_1, \dots, P_a jointly rerandomize X_a, Y_a to get X', Y' , producing transcript Π^{ReEnc}
- 10: P_1, \dots, P_a jointly compute $y_a = \text{Dec}(Y')$ and transcript Π^{Dec}
- 11: **return** $Z = (XX'^{y_a})^{\frac{1}{2}}$ and verification transcript $(y_a, \Pi^{\text{Dec}}) || (X', Y', \Pi^{\text{ReEnc}}) || \Pi$

In [ST04] the authors proved that the CGate algorithm is SUC-secure. We say that a protocol is SUC-secure if, for all adversary in the real process, there exists a simulator in the ideal process such that no PPT environment can tell whether they are interacting with the adversary in the real process or with the simulator in the ideal process.

Distributed Random Bit Generation. In the same way as CHide, credentials are generated by a particular set of authorities and are encrypted bit by bit. In order to do so, they need to use a distributed random bit generation protocol. In particular, they jointly produce an encrypted bit $\text{Enc}(b, pk)$, for which each participant knows only a share b_i of b . Furthermore, the transcript of the protocol communication is used as a DVZKP for the correctness of the protocol. We use the RandBit protocol proposed in [CGY22b].

Mixnet. Mixnets are widely used in secure e-voting systems. Informally, a mixnet allows a set of participants to shuffle and re-encrypt a set of ciphertexts, without needing to know the secret key (or a secret sharing of it). On a high level, participants privately shuffle all inputs and eventually publish them re-encrypted in random order. Informally, we say that a mixnet is secure if, given at least one honest participant, the permutation from the input to the output remains secret for all the participants involved. In the protocol we will need a verifiable mixnet, that ensures the correctness of the output (i.e. the output is indeed a permutation and re-encryption of the input). A suitable candidate for our protocol is the mixnet presented in [Wi09].

3 Protocol Description

At its core, our protocol is very similar to CHide. The participants, the Setup phase, the Registration phase and the Voting phase are essentially the same, while we changed both the Cleansing and Tallying phase to substantially reduce the computational complexity.

The main difference is that for each ballot, CHide requires to compare the encrypted credential to every successive one and to every credentials in the register (thus having quadratic complexity), while in our protocol we first perform a sorting algorithm on the encrypted votes. At the end of the protocol, votes with the same credentials and authorized credentials are consecutive, allowing the election authorities to recognize valid votes faster.

3.1 Participants

The participants in the protocol are:

- The *public board*, an append-only list of data, where all the other participants can write. The contents of the board can be read by anyone at any time, and the board is assumed to be honest.
- The election *trustees*, a set of n_T authorities that performs the cleansing and the tally. It is assumed that there are most t dishonest trustees, where $t < n_T$ is the threshold of the encryption protocol used.
- The *voters*. There are n_V voters and we assume that the adversary is able to control at most $n_V - 2$ of them.
- The *auditors*, a set of parties that check the consistency of the data published on the board. In particular auditors need to check the validity of all the ZKPs. We only need one auditor to be honest. Since every check involves only public data, any party could serve as auditor.
- The *registrars*, a second set of n_R authorities that provide credentials to voters. For coercion resistance it is assumed that all of them are honest. For privacy and verifiability, it is assumed that at least one registrar is honest.

Table 1 fixes the notation when referring to the various election participants.

Tab. 1: Parameters of an election conducted with CHide.

n_T	number of election trustees
n_R	number of registrars
n_C	number of candidates
n_V	number of voters
$n_{\mathcal{A}}$	number of voters controlled by \mathcal{A}
BB	the public board

3.2 Overview

Setup Phase. A security parameter k is chosen. The election trustees jointly run the distributed key generation (DKeyGen) protocol presented in [Ge07], obtaining a public key pk at the appropriate security level. Each trustee publishes a commitment h_i to its private share of pk on the public board, as well as pk . The private shares are denoted sk_i for $i = 1, \dots, n_T$.

Registration phase. As in CHide, credentials are created by a designated set of registrars, encrypted bitwise, sent to the voters and published on the public board. In particular, to generate a credential, the registrars run k times the RandBit protocol of [CGY22b] to generate a string $S = (S^1, \dots, S^k)$ and publish it on a public list R , comprising all the authorized credentials, alongside with a ZKP of correct computation. Let $s = (s^1, \dots, s^k)$ be the corresponding bits. Then, each registrar send privately the encrypted credential S (or its index in R), its shares of the bits in s and a designated zero-knowledge proof to guarantee voters that their credential is valid.⁶ Let R be the list of all the authorized credentials.

Voting Phase. To cast a vote for candidate v , voter v computes an encryption of their choice $C^1 = \text{Enc}(v, \text{pk})$ and a bitwise encryption of their credential $C^2 = (\text{Enc}(s_1, \text{pk}), \dots, \text{Enc}(s_k, \text{pk}))$, as well as two ZKPs: one to prove that C^2 contains encryptions of bits, and a second one proving knowledge of the randomness used in C^1 and that v is a valid voting option. These ZKPs are also used to link together C^1 and C^2 , making the tuple $C = (C^1, C^2)$ non-malleable. The tuple and the corresponding ZKPs are published on the public board using an anonymous channel.

During the Voting Phase, each voter can vote multiple times and only the last vote for each credential will be counted⁷. During this step the auditors verify the uniqueness of each ballot and that every ZKP is valid.

Cleansing and Tallying Phase. Once the Voting Phase is finished, the election trustees count the votes. Let $BB = \{C_i\}$ the list of all the votes, listed in chronological order, and $R = \{S_i\}$ the list of all authorized credentials.

First of all, the election trustees check the votes marked as invalid by the auditors and, if the votes is indeed invalid, they discard them. Then the election trustees parse each element e_i of $BB||R$ as $(\text{Data}_i, \sigma_i, f_i, c_i)$ where:

- $\text{Data}_i \leftarrow C_i^1$ if $e_i \in BB$; otherwise Data_i is set to be a random encryption.
- $\sigma_i \leftarrow C_i^2$ if $e_i \in BB$; $\sigma_i \leftarrow S_i$ otherwise.
- $f_i \leftarrow \text{Enc}(0, \text{pk})$ if $e_i \in BB$; $f_i \leftarrow \text{Enc}(1, \text{pk})$ otherwise.
- c_i is the bitwise encryption of an increasing counter and represents the chronological order of the votes.

Then the trustees apply a mixnet protocol (for example [Wi09] or [Ch81]) on $BB||R$ and produce a verification transcript. For simplicity we will refer to each element after the mixnet using the same notation as before, i.e. each element is in the form $(\text{Data}_i, \sigma_i, f_i, c_i)$.

⁶ Voter authentication is out of the scope of this paper but, for example, could be done via a digital signature by the user with a long-term key pair.

⁷ Note that different policies about revoting are possible and could be achieved with a different ordering in the tallying phase.

The election trustees perform a sorting algorithm on the set, with the following relation:

$$e_i <_{\text{Tally}} e_j \Leftrightarrow \text{Dec}(\sigma_i) || \text{Dec}(f_i) || \text{Dec}(c_i) <_{\text{Lex}} \text{Dec}(\sigma_j) || \text{Dec}(f_j) || \text{Dec}(c_j) \quad (3.1)$$

where, with an abuse of notation, $\text{Dec}(\sigma_i)$ denotes the concatenation of the decryptions of every ciphertext in σ_i and $<_{\text{Lex}}$ is the lexicographical order. It is important to note that:

- If two votes $e_i, e_j \in BB$ have the same credential, then they are sorted chronologically thanks to the counters c_i, c_j . Moreover if e_h is such that $e_i <_{\text{Tally}} e_h <_{\text{Tally}} e_j$ then e_h has the same credential of both e_i and e_j .
- If $e_i \in BB$ and $e_j \in R$ have the same credential (i.e. e_i is a ballot cast with an authorized credential) then $e_i <_{\text{Tally}} e_j$. Moreover if e_h is such that $e_i <_{\text{Tally}} e_h <_{\text{Tally}} e_j$ then e_h has the same credential of both e_i and e_j .
- No two distinct elements e_i, e_j will compare equally in this ordering, thanks to the counter c_i in each ballot.

Informally, the ordered list is composed of blocks of consecutive ballots cast with the same credential, ending with the corresponding element in R if they were made with an authorized one. During sorting, it is safe to leak the comparison result $e_i <_{\text{Tally}} e_j$, as the mixnet randomly permuted the votes and no two elements are equal. That is, the comparisons only reveal the order of the mixed values, which leaks nothing because they were initially in a random order.

After the sorting, for every pair of consecutive elements (e_i, e_{i+1}) in the ordered list, the election trustees check whether $\text{Dec}(\sigma_i) = \text{Dec}(\sigma_{i+1})$. This produces an encrypted bit I_i^1 . Let I_i be the conjunction between the bit encrypted in I_i^1 and f_{i+1} . In particular I_i is an encryption of 1 if and only if e_i is a vote with a valid credential and the last vote with that credential. At this point the trustees multiply I_i and Data_i in the exponent for every i , computing $\text{CGate}(\text{Data}_i, I_i)$, apply a second mixnet on the resulting list, and decrypt every vote.

The Sort algorithm can be any suitable comparison sort, such as Quicksort or Mergesort, thanks to the mixnet (the stability property is guaranteed by the flag f_i and the counter c_i , that also ensures the absence of equalities). The crucial part is the evaluation of the comparison as per Equation (3.1). Indeed, let a, b be two values and A_1, \dots, A_k and B_1, \dots, B_k their bitwise encryption. To obtain an encryption of $a < b$ we use this recursive formula: $L_0 = 0$, $L_i = \text{Less}(A_i, B_i) \cdot \text{CGate}(L_{i-1}, \text{Eq}(A_i, B_i))$ for $i = 1, \dots, n$, with $\text{Less}(X, Y) = Y / \text{CGate}(X, Y)$.

The result of every comparison can then be decrypted and used according to the chosen sorting algorithm, without leaking anything because of the mixing. Sorting $BB || R$ without mixing would leak the number of votes between two authorized credentials and could lead to potential attack (for example, if an attacker votes with a fake credential that is greater than any authorized one it would easily detect the lie). In fact, due to the mixnet, any adversary would have no information about the terms of each comparison, thus the result of the comparison is meaningless and can be simulated, as shown in the next section.

Algorithm 2 Tally

The participants must share of the secret key sk matching the public key pk

Require: The list of votes in BB and the list of keys R .

Ensure: The result of the election X and a proof Π for its correctness.

- 1: Parse each element in $BB||R$ as described
 - 2: Compute $L, \Pi_1^{\text{Mixnet}} = \text{Mixnet}(BB||R)$
 - 3: Compute $L_s, \Pi^{\text{Sort}} = \text{Sort}(L)$
 - 4: **for** $e_i \in L_s$ **do**
 - 5: $I_i = \text{CGate}(\text{Eq}(\sigma_i, \sigma_{i+1}), f_i)$
 - 6: $\text{Data}^i = \text{CGate}(\text{Data}_i, I_i)$
 - 7: **end for**
 - 8: Compute $L_f, \Pi_2^{\text{Mixnet}} = \text{Mixnet}(L_s)$
 - 9: **return** $X = \text{Dec}(\text{Data})$ for all $\text{Data} \in L_f$ and $\Pi = \Pi_1^{\text{Mixnet}} || \Pi_2^{\text{Mixnet}} || \Pi^{\text{Sort}} || \Pi^{\text{CGate}}$ where Π^{CGate} is the verification transcript of all CGate computations in the cycle.
-

In order to prove the correctness of the sorting algorithm, the trustees add the proofs of the correctness of every CGate computation as well the correctness of the decryption. For further details see Sect. 2.

Evasion Strategy. To evade coercion a voter can simply lie about their credential s , giving a fake credential \bar{s} to the coercer, and manipulating the DVZKP accordingly. In this way, voters are also able to vote with their correct credentials.

3.3 Security Model

We assume the Registration phase is coercion-free. It could take place physically, in which it must be protected from coercion using traditional physical security, and all registration material not needed for the voting process must be erased immediately afterwards as a final step. Otherwise, an adversary able to retrieve all the registration material, either by being present during the registration or receiving it afterwards, would easily be able to vote on behalf of the coerced voter. Alternatively, if the Registration is to take place remotely, it would itself need to be implemented using a coercion-resistant protocol, while also being authenticated by some preexisting credential. One can imagine a whole suite of coercion-resistant state functions a citizen could access remotely, including voter registration and voting, or perhaps census and welfare. Notice that an adversary receiving only the credential and the DVZKP would not be convinced by it, since the voter can produce a false DVZKP. We also suppose that each voter is able to store its credential securely and owns a device able to perform all the computation required for both voting and producing a DVZKP for the fake credential. A simple way to manage the credential within the device is using non-authenticated password-based encryption, such that the voter can give an incorrect password when coerced without risk of detection.

4 Security Proof

The proof is very similar to the one presented in [CGY22b]. We consider a distribution \mathcal{B} of sequence of pairs (j, ν) where j is a voter and ν is a voting option. Additionally, fake votes are modeled as pairs where $j \notin [1, n_V]$. In the following Algorithms 3 and 4, we employ the real-ideal paradigm.

In the real game (Algorithm 3), the adversary takes part of the setup process (line 2) and decides the set of voters $V_{\mathcal{A}}$ it controls and the coercion target (lines 3-5). Afterwards, votes are drawn according to a distribution \mathcal{B} and added to the list B , containing all the votes in order. Lines 13-22 model the coercion: if $b = 1$, the coerced voter obeys, hence any vote from j is removed from B and the real credential s^j is handled to the adversary. If $b = 0$ the voter follows the evasion strategy, i.e. they cast a vote for their intended preference β and give to the adversary a fake credential.

Votes are then added to BB , according to the sequence B (lines 23-29). After each vote the adversary is allowed to see the board and add votes. Lastly the tally is performed and the adversary guesses whether the evasion strategy was followed or not.

In the ideal world Algorithm 4, the adversary only selects the set of voters $V_{\mathcal{A}}$ it controls and the coercion target (lines 3 and 5). Then votes from $V_{\mathcal{A}}$ (line 27) and, possibly, the coerced votes (line 24-26) are directly added to B . Then B is handled to the tally functionality that publishes the result of the election X , without revealing anything else.

Definition 1. [CGY22b] A voting system is coercion resistant iff for all PPT adversary \mathcal{A} , for all parameters $n_T, t, n_V, n_{\mathcal{A}}, n_C$ and for all voting distribution \mathcal{B} , there exists a polynomial adversary \mathcal{F} and a negligible function μ such that:

$$|\mathbb{P}(\text{Ideal}(\mathcal{F}, k, n_{\mathcal{A}}, n_C, \mathcal{B}) = 1) - \mathbb{P}(\text{Real}(\mathcal{A}, k, n_T, t, n_V, n_{\mathcal{A}}, n_C, \mathcal{B}) = 1)| \leq \mu(k).$$

Theorem 1. Under the DDH assumption and in the Random Oracle Model, the voting system presented in Sect. 3 is coercion resistant.

Proof. Let \mathcal{A} be an adversary for the real game. We give to \mathcal{A} the power to impersonate t among n_T election trustees and up to $n_{\mathcal{A}}$ voters. Our goal is to build an adversary \mathcal{F} that wins the ideal game by interacting with \mathcal{A} and simulating the real game.

First of all, \mathcal{F} and \mathcal{A} run the Setup algorithm to generate a common public key pk , secret shares of the private key $\text{sk}_1, \dots, \text{sk}_{n_T}$ and the public commitments h_1, \dots, h_{n_T} . During this step \mathcal{F} is also able to reconstruct the secret key sk by extracting \mathcal{A} 's secrets.

Then \mathcal{F} follows the real game normally, until line 14, getting $V_{\mathcal{A}}, j$ and β . In the ideal game \mathcal{F} sends the same choices for $V_{\mathcal{A}}, j, \beta$.

In line 22, \mathcal{F} provides to \mathcal{A} the real credential s^j of the coerced voter. From the ideal game \mathcal{F} learns the size $|B|$ of the ideal board (line 23) and uses it to simulate the voting process (lines 23-29). For $|B|$ times:

- \mathcal{F} calls \mathcal{A} with input BB getting M .

- \mathcal{F} decrypts all the valid votes and credentials in M . For every authorized credential s^i , \mathcal{F} saves the tuple (s^i, ν) or updates a previously saved (s^i, ν') .
- \mathcal{F} adds all valid ballots in M to BB .
- \mathcal{F} chooses a random voter and a valid voting option and casts a valid vote, adding it to BB .

Then \mathcal{F} uses all the saved adversary ballots in lines 23-27, taking $\beta' = \nu_j$. \mathcal{F} learns X and its size in line 30 of the ideal game and use it to simulate the tallying process in the real game:

- \mathcal{F} runs the first mixnet for the honest authorities, while \mathcal{A} uses the dishonest ones.
- To perform the sorting, \mathcal{F} simulates all the CGate operations. This can be done since CGate is a SUC-secure protocol, as shown in [CGY22a]. \mathcal{F} also simulates the decryption step and thus randomly sorts the list.
- \mathcal{F} runs the second mixnet for the honest authorities, while \mathcal{A} uses the dishonest ones.
- \mathcal{F} chooses $|X|$ entries at random and simulates its partial decryption: every entry not chosen is decrypted to 0, while such $|X|$ entries are decrypted such that the result is exactly X .

At this point \mathcal{A} makes its guess b and \mathcal{F} forward the same guess in the ideal game. The differences between a real execution and the simulation are:

- In the real game \mathcal{A} can get either the real credential s^j or a fake one. In the simulation \mathcal{A} always receives s^j . Since in both the real and ideal worlds fake credentials have uniformly random distribution and the DVZKP could be simulated, \mathcal{A} can only distinguish a real execution from a simulated one if and only if it is able to distinguish whether \tilde{s} is a plaintext of one of the encrypted credentials in R or not. Since the ElGamal encryption is IND-CPA secure under the DDH Assumption this is impossible.
- During the simulation of the voting loop (line 23-29 of the real game) \mathcal{F} adds random ballots, while in the real game ballots are drawn according to \mathcal{B} . As before, since the ballots are encrypted, the simulation is indistinguishable from the real game under the DDH Assumption.
- During the tally \mathcal{F} simulates the execution of the CGate protocol. By SUC-security, the simulation is indistinguishable from the real game [CGY22a].
- In the real game, the ballots are sorted as per relation 3.1, while in the ideal game each comparison is simulated and thus the order is random. Being able to distinguish between the correct order and a fake one would mean either being able to distinguish the ballots, that is unfeasible due to the IND-CPA security of the encryption scheme, or being able to recognize the ballots after the mixnet, that is unfeasible thanks to the security of the mixnet.

- In the simulation the result always include all the last valid ballots cast by honest voters. In a real execution the adversary may change it by casting ballots on behalf of an honest voter. However, to do so, the adversary must be able to create a valid ZKP about the credential used, and this is unfeasible.
- \mathcal{F} simulates the decryption protocol at the end. This simulation is indistinguishable from the real world under the DDH assumption in the Random Oracle Model.

□

Algorithm 3 Real**Require:** $\mathcal{A}, k, n_T, t, n_V, n_{\mathcal{A}}, n_C, \mathcal{B}$

```

1:  $BB \leftarrow \emptyset$ 
2:  $\text{pk}, \text{sk}_i, h_i \leftarrow \text{Setup}^{\mathcal{A}}(k, n_T, t)$ 
3:  $V_{\mathcal{A}} \leftarrow A()$ 
4:  $\{s^i\}_{i \in [1, n_V]}, R \leftarrow \text{Register}(k, \text{pk}, n_V)$ 
5:  $(j, \beta) \leftarrow \mathcal{A}(\{s^i\}_{i \in V}, R)$ 
6: if  $|V| \neq n_A$  or  $j \notin [1, n_V] \setminus V_{\mathcal{A}}$  or  $\beta \notin [1, n_C] \cup \{\emptyset\}$  then
7:   return 0
8: end if
9:  $B \leftarrow \mathcal{B}(n_V - n_{\mathcal{A}}, n_C)$ 
10: for  $(i, *) \in B, i \notin [1, n_V]$  do
11:    $s^i \leftarrow \text{FakeCred}(s^1)$ 
12: end for
13:  $b \xleftarrow{\$} \{0, 1\}$ 
14:  $\tilde{s} \leftarrow s^j$ 
15: if  $b == 1$  then
16:   Remove all  $(j, *)$  from  $B$ 
17: else
18:   Remove all  $(j, *)$  from  $B$  but the last
19:   Replace it with  $(j, \beta)$ 
20:    $\tilde{s} \leftarrow \text{FakeCred}(s^j)$ 
21: end if
22:  $\mathcal{A}(\tilde{s})$ 
23: for  $(i, \alpha) \in B$  do
24:    $M \leftarrow \mathcal{A}(BB)$ 
25:    $BB \leftarrow BB \cup \{m \in M \mid m \text{ valid}\}$ 
26:    $BB \leftarrow \{\text{Vote}(c_i, \alpha, \text{pk})\}$ 
27: end for
28:  $M \leftarrow \mathcal{A}(BB)$ 
29:  $BB \leftarrow BB \cup \{m \in M \mid m \text{ valid}\}$ 
30:  $X, \Pi \leftarrow \text{Tally}^{\mathcal{A}}(BB, R, \text{pk}, \{h_i, s_i\}, t)$ 
31:  $b' \leftarrow \mathcal{A}()$ 
32: return  $b == b'$ 

```

Algorithm 4 Ideal**Require:** $\mathcal{A}, k, n_V, n_{\mathcal{A}}, n_C, \mathcal{B}$

```

1:
2:
3:  $V_{\mathcal{A}} \leftarrow A()$ 
4:
5:  $(j, \beta) \leftarrow \mathcal{A}()$ 
6: if  $|V| \neq n_A$  or  $j \notin [1, n_V] \setminus V_{\mathcal{A}}$  or  $\beta \notin [1, n_C] \cup \{\emptyset\}$  then
7:   return 0
8: end if
9:  $B \leftarrow \mathcal{B}(n_V - n_{\mathcal{A}}, n_C)$ 
10:
11:
12:
13:  $b \xleftarrow{\$} \{0, 1\}$ 
14:
15: if  $b == 1$  then
16:   Remove all  $(j, *)$  from  $B$ 
17: else
18:   Remove all  $(j, *)$  from  $B$  but the last
19:   Replace it with  $(j, \beta)$ 
20:
21: end if
22:
23:  $(v_i)_{i \in V_{\mathcal{A}}}, \beta' \leftarrow \mathcal{A}(|B|)$ 
24: if  $b == 1$  and  $\beta \neq \emptyset$  then
25:    $B \leftarrow B \cup \{(j, \beta')\}$ 
26: end if
27:  $B \leftarrow B \cup \{(i, v_i) \mid i \in V_{\mathcal{A}}, v_i \in [1, n_C]\}$ 
28:
29:
30:  $X \leftarrow \text{result}(\text{cleanse}(B))$ 
31:  $b' \leftarrow \mathcal{A}(X)$ 
32: return  $b == b'$ 

```

4.1 Removing the registrars

Registrars are authorities whose only role is to provide authorized credentials to every user and to publish the list of encrypted authorized credentials R .

In the base protocol we assume that all the n_R registrars are honest to achieve coercion resistance. Indeed, if the adversary is able to control at least one registrar, it clearly has probability of at least $\frac{1}{n_R}$ to detect the evasion strategy, since trivially it knows one share that forms the credential.

Informally, their only purpose is to provide some credential to the user, with the property that the user could later deny to have received them. The same result could be achieved by letting every user generate their own credential, encrypt them, delete the used randomness and publish the credential. In this way we are able to remove a critical point of failure for coercion resistance.

In this setting, voters need to have a trusted device that is not corrupted before the election. The user use this device to authenticate itself⁸, then it publishes the encrypted credential on the register and store it in a secure way deleting the randomness used for the encryption. When coerced, the user can simply give a fake credential, without the need of producing DVZKP. To implement this, a possible solution is to use a panic password [CH12]: on input the correct password the device uses/shows the correct credential, while on input a wrong one it shows/uses a fake one.

To prove the security of the protocol without registrars we need to change the real world game (Algorithm 3) in line 4, replacing it with the following loop:

Algorithm 5 Proposed improvement to remove registrars

```

1:  $R \leftarrow \emptyset$ 
2: while  $|R_{\mathcal{A}}| < n_{\mathcal{A}}$  do
3:    $S \leftarrow \mathcal{A}(R)$ 
4:    $R \leftarrow R \cup \{s \in S | s \text{ valid}\}$ 
5:    $R_{\mathcal{A}} \leftarrow R_{\mathcal{A}} \cup \{s \in S | s \text{ valid}\}$ 
6:   if  $|R| < n_V - n_{\mathcal{A}}$  then
7:      $s \leftarrow \text{GenerateCred}()$ 
8:      $R \leftarrow R \cup \{s\}$ 
9:   end if
10: end while

```

The security proof remains the same, except for the initial part and the voting loop. Instead of receiving the credential from the registrars, \mathcal{F} performs the loop normally. At every iteration it checks whether the adversary created credential is already in R or not. If the credential is duplicate then \mathcal{F} increases an internal counter of duplicate credentials by one.

⁸ This setting requires additional checks to avoid voters with multiple credentials and to verify their identity. Moreover, attackers should not be able to link a credential in R to its owner. A possible solution could be linkable ring signature [LWW04], with the ring formed by long term authorized public keys. Lastly, k and the number of voters n_V should be such that the probability of collision is negligible.

The voting loop is simulated as before, but in the ideal world, \mathcal{F} casts one additional null vote for every duplicate credential, such that the number of voter and credentials is consistent and the election result remains the same.

5 Performance

The main goal of the paper is to improve the performance of the tallying protocol in CHide and JCJ. This is achieved by performing a preliminary sorting step, that reduces the complexity of the tallying from quadratic to quasi-linear.

5.1 Comparison with CHide

A performance comparison between our protocol and CHide can be performed by counting the number of CGate operations. We use as example the recent Estonian election, where for the first time more than half of the voters used a remote voting system, for a total of a little more than 3×10^5 valid votes. [Eest]. Since the Estonian voting system does not track the number of revotes and removed ballots, we suppose that a total of 6×10^5 votes were submitted (i.e. only half of the total votes are valid votes) and that every registered voter voted (i.e. the list of authorized credentials $|R|$ contains 3×10^5 registered credentials). In the following k is the bit-length of voters' credentials.

Each comparison during the sorting algorithm requires $3k$ CGate computations, as explained in 2. Thus for the sorting phase our algorithm requires $3k(9 \times 10^5 \times \log_2(9 \times 10^5)) \approx 54k \times 10^6$ CGate computations and 18×10^6 decryptions. Then, to compute the check bit I^i for every pair of votes the protocol requires $2k \times 9 \times 10^5$ CGate computations. In total, our protocols require around $56k \times 10^6$ CGate computations, 18×10^6 intermediate decryptions and two mixnet applications.

The CHide protocol instead requires to check that the credential of each vote cast is unique, comparing them with the ones included in each subsequent vote, and that it is an authorized one, comparing it with every registered credentials. Each equality operation requires only k CGate computations, thus for finding duplicates CHide requires $k(2 \times 6 \times 10^5 \times 3 \times 10^5) = 360k \times 10^9$ CGate computations and the same number of computations for checking authorized credentials. Then a mixnet is applied and the votes are decrypted. Thus, CHide requires a total of $720k \times 10^9$ CGate computations and one mixnet application.

Tab. 2: Performance comparison between CHide and our protocol with respect of the security parameter k .

	CGate	Mixnet	Preliminary Decryptions
CHide	$720k \times 10^9$	1	-
Our Protocol	$56k \times 10^6$	2	18×10^6

Recent Updates. The CHide preprint was independently updated by the authors to address the quadratic complexity of the protocol. Their solution is quite similar to our solution, leveraging the CGate protocol to sort all the votes and achieve a quasi-linear complexity.

While sharing the same philosophy and almost the same asymptotic complexity, the two protocols have a meaningful difference that could lead to different running times. Updated CHide avoids the preliminary mixnet by using a swap operation between ciphertexts, instead of simply decrypting the output of each comparison. This restricts their choice of sorting algorithms to be *data-oblivious*, with complexity $O(n \log^2 n)$. Moreover, instead of using a single bit, they use a fixed “special” counter for registered credentials, thus performing more comparisons in the last part of the tally (the computation of I_i , as per our notation).

5.2 Comparison with related works

During the last years many different coercion resistant protocols have been proposed, usually with the goal of reducing the quadratic complexity that is typical of protocols descending from JCJ. Notable examples of more efficient protocols are VoteAgain [LQT20], AFT [AFT10], Athena [Sm19] and protocols based on hash tables like [Rø20] and [WAB07]. The linear-time version of the JCJ protocol proposed in [Rø20] also uses fully homomorphic encryption. Table 3 summarizes the comparison between this and related work in terms of security and complexity.

Tab. 3: Comparison with other coercion resistant protocols.

Protocol	Complexity	Security
JCJ[JCJ10]	$O(n^2)$	JCJ
Civitas [CCM08]	$O(n^2)$	JCJ
AKLM [Ac15]	$O(n^2)$	AKLM
Revote [LHK16]	$O(n^2)$	AKLM
CHide[CGY22b]	$O(n^2)$ or $O(n \log^2 n)$	CHide
VoteAgain [LQT20]	$O(n \log n)$	VoteAgain
AFT [AFT10]	$O(n)$	JCJ
Athena [Sm19]	$O(n)$	JCJ + Dups
Hash-based [Rø20; WAB07]	$O(n)$	JCJ + Dups
This work	$O(n \log n)$	CHide

In the table, the security levels are defined as:

- JCJ is the security level achieved by the original JCJ protocol.
- JCJ+Dups is at lower security level than JCJ, where the number of votes for each credential also leak.
- AKLM is at lower security than JCJ, in which it is assumed that voters revote at the end of the voting period to escape from adversarial control.
- CHide is the security level achieved by CHide, higher than JCJ.
- VoteAgain follows its own coercion resistance definition introduced in [LQT20] and it is not comparable with the others.

From the state-of-the-art, achieving a better or equivalent complexity than our protocol requires to either change the security definition (as per [LQT20]) or to increase the leakage.

6 Conclusions

In this work we presented an enhanced version of CHide, that drastically reduces the computational complexity of the tallying from $O(n^2)$ to $O(n \log n)$, which is currently the best efficiency among voting protocols satisfying a stronger notion of coercion resistance.

A possible way to speed up the tally even further is amortizing the process through the whole voting phase, instead of waiting until the end of the election. A possible approach would consist of using a bucket sorting algorithm, like the one presented in [As20]. As votes come in, they are assigned to buckets. When the first two buckets are full, the first step of bucket sorting is performed. When the next two buckets are full, the authorities perform the first step of the sorting process on them and the second step on the whole for the bucket, and so on. While maintaining the same asymptotic complexity, this approach could lead to a vastly reduced delay between the end of the voting phase and the publication of the result. However, bucket sorting is usually susceptible to “overflow” attacks. Indeed, typical bucket sorting algorithms like [As20] allow for a fixed maximum number of elements in each bucket, thus an attacker could vote multiple time with the same credential, causing the corresponding bucket to overflow and making the sorting fail. In the end we not find any solution to this problem but it is a topic worthy of further examination.

Unfortunately, our protocol still has the same issue of CHide regarding the dimension of the credentials, that are encryptions of individual bit instead of a single encrypted string. The bitwise encryption is required to realize a secure tally, since we need to multiply ciphertexts in the exponents. A possible solution to this problem, while keeping the overall structure of the tally in place, would be to change the encryption protocol. This could be achieved using class group encryption, originally presented in [CL15] and later studied in a threshold version in [BDO22]. However this approach would need to design an ad-hoc mixnet suitable for this kind of encryption. Moreover, maintaining this level of efficiency could be challenging, since the sorting protocol would need some adaptations to work, in particular to avoid equal credentials.

Acknowledgements

Michele Battagliola acknowledges support from TIM S.p.A. through the PhD scholarship.

References

- [Ac15] Achenbach, D.; Kempka, C.; Löwe, B.; Müller-Quade, J.: Improved Coercion-Resistant Electronic Elections through Deniable Re-Voting. *USENIX Journal of Election Technology and Systems (JETS)* 3 (2), pp. 26–45, 2015, ISSN: 2328-2797, URL: <https://www.usenix.org/jets/issues/0302/achenbach>.

- [Ad08] Adida, B.: Helios: Web-based Open-Audit Voting. In: *USENIX Security Symposium*. USENIX Association, pp. 335–348, 2008.
- [AFT10] Araújo, R.; Foulle, S.; Traoré, J.: A Practical and Secure Coercion-Resistant Scheme for Internet Voting. In: *Towards Trustworthy Elections*. Vol. 6000. LNCS, Springer, pp. 330–342, 2010.
- [As20] Asharov, G.; Chan, T. H.; Nayak, K.; Pass, R.; Ren, L.; Shi, E.: Bucket Oblivious Sort: An Extremely Simple Oblivious Sort. In: *SOSA*. SIAM, pp. 8–14, 2020.
- [BDO22] Braun, L.; Damgård, I.; Orlandi, C.: Secure Multiparty Computation from Threshold Encryption based on Class Groups. *IACR ePrint Arch.* P. 1437, 2022, URL: <https://eprint.iacr.org/2022/1437>.
- [CAE19] Cardillo, A.; Akinyokun, N.; Essex, A.: Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology? In: *E-VOTE-ID*. Vol. 11759. LNCS, Springer, pp. 67–82, 2019.
- [CCM08] Clarkson, M. R.; Chong, S.; Myers, A. C.: Civitas: Toward a Secure Voting System. In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, pp. 354–368, 2008.
- [CGY22a] Cortier, V.; Gaudry, P.; Yang, Q.: A Toolbox for Verifiable Tally-Hiding E-Voting Systems. In: *ESORICS (2)*. Vol. 13555. LNCS, Springer, pp. 631–652, 2022.
- [CGY22b] Cortier, V.; Gaudry, P.; Yang, Q.: Is the JCJ voting system really coercion-resistant?, working paper or preprint, 2022, URL: <https://hal.inria.fr/hal-03629587>.
- [CH12] Clark, J.; Hengartner, U.: Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance. In (Danezis, G., ed.): *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 47–61, 2012, ISBN: 978-3-642-27576-0.
- [Ch81] Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Commun. ACM* 24 (2), pp. 84–88, 1981, URL: <https://doi.org/10.1145/358549.358563>.
- [CL15] Castagnos, G.; Laguillaumie, F.: Linearly Homomorphic Encryption from DDH. In: *CT-RSA*. Vol. 9048. LNCS, Springer, pp. 487–505, 2015.
- [Eest] How did Estonia carry out the world’s first mostly online national elections, <https://e-estonia.com/how-did-estonia-carry-out-the-worlds-first-mostly-online-national-elections/>, Accessed: 2023-05-06.
- [Ga85] Gamal, T. E.: A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* 31 (4), pp. 469–472, 1985, URL: <https://doi.org/10.1109/TIT.1985.1057074>.
- [Ge07] Gennaro, R.; Jarecki, S.; Krawczyk, H.; Rabin, T.: Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. *J. Cryptol.* 20 (1), pp. 51–83, 2007.
- [HPT22] Haines, T.; Pereira, O.; Teague, V.: Running the Race: A Swiss Voting Story. In: *E-Vote-ID*. Vol. 13553. LNCS, Springer, pp. 53–69, 2022.
- [HS19] Haines, T.; Smyth, B.: Surveying definitions of coercion resistance. *IACR ePrint Arch.* P. 822, 2019, URL: <https://eprint.iacr.org/2019/822>.
- [HT15] Halderman, J. A.; Teague, V.: The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In: *VoteID*. Vol. 9269. LNCS, Springer, pp. 35–53, 2015.

- [Idea] Use of E-Voting Around the World, <https://www.idea.int/news-media/media/use-e-voting-around-world@misc>, Accessed: 2023-05-06.
- [Ifes] Internet Voting: Past, Present and Future, <https://www.ifes.org/news/internet-voting-past-present-and-future>, Accessed: 2023-02-18.
- [JCJ10] Juels, A.; Catalano, D.; Jakobsson, M.: Coercion-Resistant Electronic Elections. In: Towards Trustworthy Elections. Vol. 6000. LNCS, Springer, pp. 37–63, 2010.
- [JSI96] Jakobsson, M.; Sako, K.; Impagliazzo, R.: Designated Verifier Proofs and Their Applications. In: EUROCRYPT. Vol. 1070. LNCS, Springer, pp. 143–154, 1996.
- [LHK16] Locher, P.; Haenni, R.; Koenig, R. E.: Coercion-Resistant Internet Voting with Everlasting Privacy. In: Financial Cryptography Workshops. Vol. 9604. LNCS, Springer, pp. 161–175, 2016.
- [Li21] Licht, N.; Duenas-Cid, D.; Krivosova, I.; Krimmer, R.: To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting. In: E-VOTE-ID. Vol. 12900. LNCS, Springer, pp. 91–105, 2021.
- [LQT20] Lueks, W.; Querejeta-Azurmendi, I.; Troncoso, C.: VoteAgain: A scalable coercion-resistant voting system. In: USENIX Security Symposium. USENIX Association, pp. 1553–1570, 2020.
- [LWW04] Liu, J. K.; Wei, V. K.; Wong, D. S.: Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract). In: ACISP. Vol. 3108. LNCS, Springer, pp. 325–335, 2004.
- [Rø20] Rønne, P. B.; Atashpendar, A.; Gjølsteen, K.; Ryan, P. Y. A.: Short Paper: Coercion-Resistant Voting in Linear Time via Fully Homomorphic Encryption. In (Bracciali, A.; Clark, J.; Pintore, F.; Rønne, P. B.; Sala, M., eds.): Financial Cryptography and Data Security. Springer International Publishing, Cham, pp. 289–298, 2020, ISBN: 978-3-030-43725-1.
- [RRI16] Ryan, P. Y. A.; Rønne, P. B.; Iovino, V.: Selene: Voting with Transparent Verifiability and Coercion-Mitigation. In: Financial Cryptography Workshops. Vol. 9604. LNCS, Springer, pp. 176–192, 2016.
- [Sm19] Smyth, B.: Athena: A verifiable, coercion-resistant voting system with linear complexity. IACR ePrint Arch. P. 761, 2019, URL: <https://eprint.iacr.org/2019/761>.
- [ST04] Schoenmakers, B.; Tuyls, P.: Practical Two-Party Computation Based on the Conditional Gate. In: ASIACRYPT. Vol. 3329. LNCS, Springer, pp. 119–136, 2004.
- [WAB07] Weber, S. G.; Araujo, R.; Buchmann, J.: On Coercion-Resistant Electronic Elections with Linear Work. In: The Second International Conference on Availability, Reliability and Security (ARES'07). Pp. 908–916, 2007, DOI: 10.1109/ARES.2007.108.
- [Wi09] Wikström, D.: A Commitment-Consistent Proof of a Shuffle. In: ACISP. Vol. 5594. LNCS, Springer, pp. 407–421, 2009.

Coercion-resistant i-voting with short PIN and OAuth 2.0

Matteo Bitussi¹, Riccardo Longo¹, Francesco Antonio Marino², Umberto Morelli¹, Amir Sharif¹, Chiara Spadafora³, Alessandro Tomasi¹

Abstract: This paper presents an architecture for an OAuth 2.0-based i-voting solution using a mobile native client in a variant of the Araújo-Traoré protocol. We follow a systematic approach by identifying relevant OAuth 2.0 specifications and best practices. Having defined our framework, we identify threats applicable to our proposed methodology and detail how our design mitigates them to provide a safer i-voting process.

Keywords: i-voting; Coercion Resistance; OAuth 2.0.

1 Introduction and Related Work

Electronic voting (e-voting) is becoming increasingly appealing to improve election efficiency and accuracy, and to make elections more accessible, inclusive, and transparent. As technology progresses, end-to-end verifiable voting protocols may also offer an enhanced level of trust. Several interesting proposals have been made in recent years, with particularly noteworthy examples including Helios [Ad08], Belenios [CGG19], and Civitas [CCM08]. These academic proposals are of great interest, but it is non-trivial to make the leap to concrete solutions.

In this paper, we make a proposal for how to use the OAuth 2.0 framework [Ha12] - the current standard for authorization at the application layer - for a concrete instance of a specific i-voting protocol, taking into account best current practice while attempting to ensure that the complex requirements of e-voting are still being met. The application of OAuth on its own to a concrete scenario requires knowledge of several specifications extending the core protocol, and requires effort and expertise [Sh22].

This paper extends the protocol proposed in [Lo22], derived from ABRTY [Ar10; AT13] with the following main contributions: (i) we give an architecture for an OAuth 2.0-based solution that supports i-voting through the identification of relevant OAuth 2.0 specifications and best current practices to provide a secure protocol and satisfy i-voting requirements; (ii) we introduce commitment access token to authorize the casting of a ballot, to prevent brute-forcing of the PIN, maintaining unlinkability between vote and voter; (iii) we integrate

¹ Center for Cybersecurity, Fondazione Bruno Kessler, Trento, Italy {mbitussi,rlongo,umorelli,asharif,altomasi}@fbk.eu

² Italian Government Printing Office and Mint, IPZS, Rome, Italy fa.marino@ipzs.it

³ Università degli Studi di Trento, Trento, Italy chiara.spadafora@unitn.it

short checks for Cast-As-Intended ballot verification, following [Co19]; and (iv) we identify threats applicable to our architecture, briefly explaining how our design can mitigate them.

The i-voting protocol satisfies coercion resistance through the *fake credential* mechanism as introduced in [JCJ10]; we call it Anti-Coercion Credentials (ACCs) as in [Lo22]. Each voter is provided with a different ACC, that will be used to validate their ballots, and can autonomously create a ruse ACC, indistinguishable from the valid one. Ballots cast with a ruse ACC do not count towards the final tally, but are indistinguishable from valid ballots, enabling anti-coercion strategies. Differently from Civitas and ABRTY [Ar10; AT13; CCM08], the assumptions of [Lo22] avoid an untappable channel and try to provide a safe ACC delivery and forging in an uncontrolled environment (for further discussion see [Lo22] and Sect. 4.2 on generation, issuance and forgery of ACCs; Sect. 5.1 on coercion and untappable channels). Moreover, the ACC is stored on the voting device masked by a PIN: to forge an ACC the voter can set up a ruse PIN. The use of a PIN to unlock voting credentials was proposed by Neumann and Volkamer [NV12] to improve usability, however, this mechanism is susceptible to various problems [Es20]. Enabling voters to set their choice of PIN remotely would enable a coercion strategy; a compromise proposed in [Lo22] to evade coercers is to deliver the PIN at a random time, but the authors “leave considerations on PIN length and brute force countermeasures as implementation choices”.

In Sect. 2 we provide background on OAuth; in Sect. 3 we describe our proposal for using commitment schemes in OAuth Access Tokens; in Sect. 4 we summarize the i-voting protocol with a focus on the voter’s interactions, and we describe our proposal for a framework to instantiate the protocol using OAuth; in Sect. 5 we follow a threat modeling process limited to client-server exchanges and coercers, summarizing how our proposed mitigations preserve the e-voting requirements and coercion resistance of the base protocol.

2 Background: OAuth 2.0

The OAuth 2.0 authorization framework [Ha12] enables a third-party application (Client) to obtain limited access to an online service hosted on a Resource Server (RS) on behalf of a Resource Owner (RO). The Client redirects the RO through the User Agent (UA) into the Authorization Server (AS), where the RO performs the authentication. After the successful authentication of the RO, the AS issues an Access Token which Clients use to access the RO’s resources in the RS.

A typical Access Token may be a JSON Web Token (JWT) [JCM15]. Unless otherwise specified, Access Tokens are bearer tokens, thus vulnerable to a range of attacks. OAuth Security best current practice recommendations [Lo23] include:

Replay prevention: AS should constrain tokens to their intended sender, typically by binding a token to a public key held by the sender and forcing the sender to prove its possession by digital signature. Two methods for sender-constrained Access Tokens are

mutual TLS (mTLS) [Ca20] and Demonstrating Proof-of-Possession (DPoP), which is currently an Internet-Draft [Fe23].

Client authentication: should be based on public key cryptography that enables stronger client authentication such as mTLS or signed JWT [JCM15].

Authorization code protection: to prevent authorization code theft or injection, Proof Key for Code Exchange [SBA15] (PKCE) is recommended.

Privilege restriction: Access Tokens should restrict privileges granted to the holder to the minimum required, in accordance with the principle of least privilege, e.g., making use of the audience, scope, and resource claims.

2.1 OAuth 2.0 Token Exchange

The OAuth 2.0 Token Exchange protocol, as defined in RFC8693 [Jo20], is an extension to the OAuth 2.0 protocol for implementing scenarios where one token needs to be swapped for another. There are scenarios where the Client needs to access resources hosted by other downstream Resource Servers on behalf of the User and in which the usage of the direct Access Token is not possible.

RFC8693 [Jo20] introduces a new grant type to define how a Client can request and obtain security tokens from AS that are playing the role of Security Token Service (STS) in the Token Exchange protocol. The STS validates security tokens (e.g., JWT) provided to it and issues a new security token in response, which the Client may use as access credentials for resources in heterogeneous environments or across security domains.

2.2 OAuth 2.0 Dynamic Client Registration

OAuth 2.0 Dynamic Client Registration [Ri15] (DCR) is an extension to OAuth 2.0 that enables a Client to obtain unique dynamic client identifiers (client id) for each instance of Client. Moreover, the Client is able to register a public key with the AS that can be used for the Client authentication based on signed JWT.

RFC7591 [Ri15] introduces a new endpoint called Dynamic Client Registration endpoint, which can be implemented by the AS as either Protected or Open - i.e., requiring an initial Access Token or not, respectively.

3 OAuth Commitment Access Token

Our proposal is based on cryptographic commitment schemes, which we provide brief background for in Sect. 3.1. Our proposal is described in Sect. 3.2.

Commitment schemes have also been used elsewhere in OAuth extensions, including one we use; we compare our proposal to significant others in Sect. 3.3.

3.1 Commitment schemes

A commitment scheme to a message m lets a Prover generate a commitment c and an opening o , such that c may be disclosed or published in advance, and any Verifier provided with the opening o at a later time can verify the correctness of the commitment. Commitments are *binding* if they can only be opened to a single message, and *hiding* if the commitment reveals no information about the message itself - see [BS23] for more details.

A simple commitment scheme to a message m based on a cryptographic hash function H may be instantiated as follows ($||$ denotes concatenation):

$\text{Commit}(m) : C(m) = (c, r)$ with the opening $o = r \xleftarrow{R} \{0, 1\}^\lambda, c \leftarrow H(m||r)$.

$\text{Open}(c, m, r) : c \stackrel{?}{=} H(m||r)$.

This scheme is computationally binding and hiding if H is collision resistant and the distribution of digests is computationally indistinguishable from uniformly random output, respectively [BS23]. The former depends on the hashing algorithm; for the latter to be the case, the input must have sufficiently high entropy [Tu18].

3.2 Commitment Access Token

We propose an authorization flow for a scenario in which an OAuth Client has a message b and needs an Access Token for an OAuth Client linked to b , but wants to preserve anonymity in the following sense: the AS should not learn b , and the Resource Server should not link b to the identity of the Client.

Our proposal is the following:

- to send the message b to an RS, the Client generates a random $r \xleftarrow{R} \{0, 1\}^\lambda$ and computes a commitment $c \leftarrow \text{Commit}(b, r) = H(b||r)$ to b (steps 1-2);
- the AS authenticates the Client and provides an Access Token - a JSON Web Signature (JWS) with c as payload - to the Client (steps 3-4);
- the Client requests the RS to process the message b by providing the JWS and the commitment opening r (step 5);

- the Resource Server accepts the message b if both the JWS and the commitment opening are valid (steps 6-7).

The flow is shown in Fig. 1, with the hash-based commitment scheme as in Sect. 3.1.

Commitment Access Token

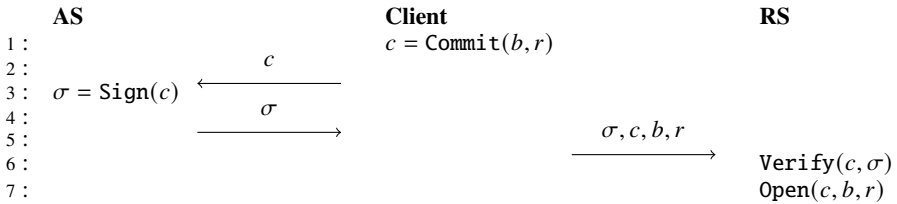


Fig. 1: Commitment Access Token (CAT). σ represents the JWS digital signature, with Sign and Verify determined by the chosen JOSE algorithm [IA23].

Trust model. In general, a Commitment Access Token (CAT) could be useful when (a) the Resource Owner wishes to perform a single, high-value operation; (b) the Authorization Server must not know the exact content of that operation, but must ensure the right audience and scope, and wishes to ensure that the rate of requests within that scope from an RO is limited without delegating this access control to the Client; (c) the Resource Server must ensure that the RO was authenticated when that specific access was authorized.

Replay protection. We allow the Client to generate the nonce r opening the commitment. This means that multiple uses of the service with the same token and message are possible. This is not an issue in our case as duplicate ballots are weeded out in a following step (see Sect. 4); other applications may mitigate against replay by adding further validation conditions on the token.

Holder binding. In some scenarios, there is no need to ensure holder binding to the Access Token because the commitment is binding to the payload. As long as the commitment can only be used with a specific message and the AS authorized the access, it may not matter which Client is actually accessing the RS. This decoupling helps to preserve the anonymity of the Client, and this property may be valuable for sensitive operations (e.g. ballot casting).

3.3 Comparison

A commitment scheme is used in the widely recommended OAuth extension Proof Key for Code Exchange (PKCE) [SBA15] to mitigate against code interception or injection.

A commitment scheme is also used in the proposed OpenID Connect (OIDC) extension OpenPubKey [He23] to bind an OIDC identity to a specific public key, without the AS knowing the key that will be used by the Client.

A commitment-like scheme is also used in the Google Play Integrity API [Go] (GPIA) to provide replay protection and integrity for a high-value message.

We summarize PKCE and GPIA below, and compare the proposed CAT with PKCE and GPIA in Tab. 1. We omit a comparison with OpenPubKey since it is, as far as we know, at an early proposal stage and we do not make use of it.

PKCE. Two separate OAuth requests are made by a public Client to an AS: (a) an Authorization Request, to which the AS replies with an Authorization Code (AC); and (b) an Authorization Grant, to which the AS replies with an Access Token. In exchange (a), messages are redirected via the User Agent so that the user (Resource Owner) may authenticate to the AS and grant consent; exchange (b) occurs directly between Client and AS, e.g., via TLS. Messages in exchange (a) are at higher risk of interception or disclosure.

To mitigate against AC interception using PKCE, the Client sends a commitment c to a random r to the AS in (a), and at a later time opens the commitment by revealing r in (b). Eavesdroppers intercepting the AC cannot craft a valid Authorization Grant request in (b), as they do not know the secret r .

GPIA. GPIA may be used to provide a mobile application’s back-end server (Verifier) with signed and encrypted attestations about the integrity of the app (Client) and the device it runs on. Additionally, it may be used to provide replay protection and integrity for a high-value message m generated by the app, by use of a Verifier-provided nonce and a hash function, respectively. The word *commitment* is not used in the documentation, but we would argue that the protection is commitment-based, and indeed it follows a very similar flow to Fig. 1, with notable differences. Firstly, the GPIA nonce r is set by the Verifier to provide replay protection, but is revealed to the GPIA attestation server. This enables GPIA to open the commitment if the message m is ever disclosed. Secondly, the GPIA commitment is computed as $c \leftarrow H(m)||r$. We observe that this commitment is binding, but not hiding, and indeed there are very clear warnings to that effect in the documentation. Which commitment to use is up to the developer: even m itself would be accepted in practice. This makes sense in the context of GPIA, which is not designed for hiding commitments, but is not sufficient in our case.

Notably, GPIA advise that requests are rate limited, and developers should be prepared to handle the absence of that service. In our application, rate limiting by the AS is a desirable feature to protect against brute force attacks.

4 Our framework: an i-Voting Protocol

Here we present the i-voting protocol, introducing the entities involved and specifying their OAuth roles. For background on OAuth, see Sect. 2. The protocol achieves end-to-end verifiability and ballot secrecy by encryption with a threshold modified ElGamal scheme [DF89], zero knowledge proofs of ballot correctness, and verifiable shuffling and

Tab. 1: Comparison of PKCE, GPIA, and CAT.

Scheme	PKCE	GPIA	CAT
Commitment	$H(r)$	$H(m) r$	$H(m r)$
Nonce generated by	Client	AS	Client
Nonce revealed to AS	Yes	Yes	No
AS role	Authorization	Attestation	Authorization
RP role	Authorization	Authorization	Resource
Main mitigation	Code interception	Replay, tampering	Brute force
Hiding commitment	Yes	No	Yes

re-encryption [Gr10]. We give a high-level overview of the steps from App installation to vote casting, and we also describe an adaptation of cast-as-intended verifiability following CDGT [Co19]. In Sect. 4.4 we describe the use of our proposed CAT during ballot casting, then in Sect. 4.5 we summarize the OAuth-based access control in the Client-server exchanges.

4.1 Protocol participants

Electoral Roll (ER). The ER matches authenticated voters with their right to vote. It acts as OAuth AS to i-voting RSs, regulating the distribution of both anti-coercion voting credentials (ACC, see [Lo22]) and casting tokens. It also acts as OpenID Relying Party (RP) to the OpenID [Sa14] Provider (OP).

eID Provider (OP). The OP is an OpenID [Sa14] Provider, on which the ER relies on the OP to authenticate voters to properly assess their eligibility.

Voting Application (App). The App is used by voters to receive voting credentials and cast ballots. It also enables anti-coercion strategies exploiting the ACC [Lo22]. The App is a native application, and each instance registers as a stand-alone confidential OAuth Client with the ER.

Notification Server (NS). The NS notifies Clients when resources are available to download. It acts as OAuth Resource Server.

Registration Teller (RT). The RTs issue ACCs to Apps and are involved in some anti-coercion strategies [Lo22]. They act as OAuth Resource Server.

Ballot Box (BB). The BBs receive and collect cast ballots, sent anonymously by Client applications. They act as OAuth Resource Server.

Outside our focus on the interactions between the App and the other entities, BBs are also responsible for checking the admissibility of ballots, publishing receipts of successful casting and providing all the collected ballots for tallying. Other participants include: Tabulation Tellers (TT), which tally cast ballots but are not directly accessed by the Client; and a Web Bulletin Board (WBB), which provides a public registry to all participants, but does not require authentication or authorization by the Client.

4.2 Voting Protocol Overview

The protocol can be summarized in the following high-level steps: (i) Client and Voter registration, (ii) PIN and proof of correctness retrieval, (iii) ruse PIN request, and (iv) ballot casting and individual verification.

4.2.1 Client and Voter registration

A voter \mathcal{V} starts with downloading the App from an official application store and installing it on their device. Once the App is installed, the voter can set it up and register to the election system:

1. \mathcal{V} opens the App which checks device integrity (app origin, device not rooted);
2. the App fetches from WBB the election parameters - including the blank ballot structure and public keys - and the identities of ER, RTs, BBs, NS;
3. the App registers as Client to the ER, including an *ER Authentication* public key for future authentications.
4. the App directs \mathcal{V} to authenticate to the ER via the OP; having verified the eligibility of \mathcal{V} , the ER issues a *Registration* token to the App;
5. the App generates its designated-verifier keys, and exchanges the Registration token via token exchange [Jo20] to obtain the following tokens:
 - an *PIN request* token for each RT (containing the designated public key), this type of token is used by the App to register, manage their ACC, set up a new device;
 - a *Notification Registration* token for the NS;
6. the App registers with the NS and the RTs with these tokens;
7. each RT_i checks the validity of the authorization token sent by the App and issues its masked ACC share (see [Lo22] for more details) to the App;
8. the App can interpolate the shares and compute the masked ACC, which is stored encrypted on the device.

4.2.2 PIN and proof of correctness retrieval

Before being able to vote, \mathcal{V} has to wait to receive the mask that will unlock the ACC and from which the PIN is derived. The procedure for the PIN delivery is as follows:

1. after a random time, each RT_i tells the NS that its mask share is ready.
2. once the NS has received confirmation that enough shares are ready, it notifies the App that the mask is ready to be retrieved.
3. the App alerts \mathcal{V} that the PIN is ready when the voter opens the App, they authenticate again to the ER via the OP;
4. after authentication, the ER issues three authorization tokens for the App:
 - a new *PIN request* token for each RT_i ;
 - a *PIN retrieval* token for each RT : this type of token will be used by the App to retrieve the mask shares from the RT s;
 - a *proof of correctness retrieval* token for each RT : this type of token will be used by the App to retrieve the Designated-Verifier Non-Interactive Zero-Knowledge Proof (DVNIZKP) shares from the RT s (see below);
5. the App requests the mask shares to the RT s with the *PIN retrieval* tokens, each RT_i sends its share if it is ready and the token is valid;
6. with enough shares, the App can compute the mask, whose least significant digits are the PIN.

The PIN is shown to the voter, while the other part of the mask is saved and encrypted on the device. In this way, the complete ACC cannot be retrieved without entering the correct PIN.

The correctness of the ACC can be checked with the DVNIZKP, which is issued by the RT s after a random time, just like the mask. This cryptographic proof has the interesting property that it can be forged in order to feign the validity of any ACC by the holder of the designated private key.

4.2.3 Ruse PIN request

Using the App, \mathcal{V} can set up a ruse PIN and forge a DVNIZKP to convince a coercer that this ruse PIN is a valid PIN.

The procedure to set up a *ruse PIN* is the following:

1. using the App, \mathcal{V} requests to set a ruse PIN and types in a PIN of their choice with the same length as the valid one;

2. the App computes a forged mask and its shares so that their interpolation gives a mask identical to the original one except for the least significant digits, which are the inserted ruse PIN instead;
3. furthermore, the App computes a forged DVNIZKP and its shares so that it validates the ACC completed with the inserted ruse PIN;
4. using the *PIN request* tokens provided by ER, the app sends to each RT_i a request for the re-sending of the PIN containing the forged shares;
5. each RT_i checks the validity of the authorization token sent by the App and after a random time sends (just like for the PIN delivery) the received forged shares back: first the forged mask share, then the forged DVNIZKP share.

Note that the setup of a ruse PIN does not undermine the ability of the valid PIN to cast a valid vote, since this setup is only intended to fool a coercer.

With the *PIN request* token, the App can also request a reminder of the PIN in case \mathcal{V} forgets it. To do so the procedure is similar to the ruse PIN request procedure, but the App sends empty shares instead of the forged ones and the RTs respond with the original shares instead of the received ones.

4.2.4 Ballot casting and individual verification

When the voting period starts, \mathcal{V} can cast a vote with the following procedure:

1. using the App, \mathcal{V} accesses the voting view where the ballot is shown, and they can select a list and a corresponding candidate or leave a blank choice;
2. \mathcal{V} inserts a PIN: the valid one will produce a valid vote, while any other PIN (including the ruse one) will produce a vote that will not be counted;
3. the App encrypts the choices and computes a set of NIZKP to prove the formal correctness of the encrypted ballot²;
4. once the ballot has been computed, the App authenticates \mathcal{V} to unlock the *ER Authentication* secret key from the keystore;
5. the App uses this key to authenticate a request to the ER for the issuing of a Commitment Access Token where the message is the encrypted ballot;
6. the ER verifies the validity of the request using the *ER Authentication* public key of \mathcal{V} , and if the policies on vote casting are satisfied (e.g. \mathcal{V} has not voted too recently or too frequently), the ER issues to the App for each BB a CAT (with limited time validity) tied to the ballot;

²Note that a vote that will not be counted due to the use of an invalid PIN will still pass all formal correctness checks, since these do not depend on the PIN used.

7. the app sends anonymously to each BB the ballot, authorized by the CAT;
8. each BB checks the authorization and the formal correctness of the received ballot; if these checks pass, the BB sends the ballot digest to the WBB, effectively time-stamping the casting;
9. once the App can confirm the digest publication on the WBB, it prompts \mathcal{V} to proceed with the vote confirmation by choosing two values to disclose for *Cast-As-Intended Verifiability* (see Sect. 4.3);
10. the values chosen by \mathcal{V} are sent by the App to the BBs to complete the disclosure, authenticating this message with a preimage of the ballot digest;
11. each BB uses the preimage to confirm that the sender knows the ballot, then partially decrypts it with the disclosure values, sending the result to WBB³;
12. once the App can confirm the publication of the correct data on the WBB, it displays to \mathcal{V} a confirmation message and encourages to manually verify the correctness of the sent vote, i.e., that the ballot was recorded as cast and that the ACC used to construct the ballot belonged to \mathcal{V} .

Once the voting period has ended, the BBs publish all the confirmed encrypted ballots on the WBB. The cryptographic protocol allows to filter out ballots cast using the same ACC (only the latest is kept) or invalid PINs, with a procedure that involves the TTs and the RTs and which does not undermine voters' privacy by using a verifiable mixnet [Gr10]. The remaining ballots are homomorphically aggregated and threshold-decrypted by the TTs to compute the final tally, which is published on the WBB alongside a set of NIZKPs that may be used by anyone to check the correctness of the tallying steps.

4.3 CDGT Cast-As-Intended Verifiability

Inspired by [Co19], the protocol includes checks for the Cast-As-Intended property, in which each vote is partially audited before submission, without breaking secrecy.

In [Co19] the checks are designed for a Helios/Belenios ballot where the preference expressed is the number of the chosen candidate. In the protocol proposed in [Lo22], the voter can select at most one list and at most one candidate from the ones associated to the chosen list. To enable efficient checks via NIZKPs on the correctness of the vote and homomorphic tallying, the vote in our encrypted ballot is encoded as a binary choice for each list ($l_i \in \{0, 1\}$) and candidate ($c_{i,j} \in \{0, 1\}$). To convert these choices in two numbers

³Note that only the App, that has computed the encrypted ballot, is able to produce with non-negligible probability a valid disclosure, so the disclosure message is properly authenticated. Note also that a replay would have no effect because the BB would just compute and publish the same result.

that represent, respectively, the index of the chosen list and candidate, with 0 representing a blank choice, we use a ranked sum:

$$\ell = \sum_{i=0}^{n_\ell} i \cdot l_i, \quad c = \sum_{i=0}^{n_\ell} \sum_{j=0}^{n_{c,i}} j \cdot c_{i,j},$$

where n_ℓ is the number of lists and $n_{c,i}$ is the number of candidates associated with the i -th list.

To ease the checks, enhancing user experience, we mask these values with two random shifts $s_\ell, s_c \in \{0, \dots, 99\}$. The ballot includes the encryptions of:

$$s_\ell, \quad (s_\ell + \ell) \bmod 100, \quad s_c, \quad (s_c + c) \bmod 100.$$

The App shows the voter \mathcal{V} these four values, unencrypted; to check their correctness, \mathcal{V} has to compute the sum of two two-digit numbers, and then consider only the last two digits. Since the number of lists and candidates is ~ 10 , this sum is likely a two-digit number, so the modulo operation is not noticeable.

To confirm the vote, \mathcal{V} has to choose whether to disclose the shift or the sum for both list and candidate. To disclose the two selected values after the ballot has been cast, the App sends \mathcal{V} 's choices to the BBs, together with the randomness that had been used to compute their encryption in the ballot.

Note that, as in [Co19], the disclosure of these values does not reveal anything about the vote cast; any voter auditing their ballot is guaranteed that the ballot encodes their intended vote, even if their voting device and the BBs collude.

4.4 CAT for casting authorization

During ballot casting steps 6 and 7 (Sect. 4.2) we use a CAT to authorize the casting of a ballot, to prevent brute-forcing of the PIN while maintaining unlinkability between the unsealed vote and the voter.

In this context the Client is the voting application, the Authorization Server is the Electoral Roll, and the Resource Server is the Ballot Box.

In the very specific scenario of i-voting, there is no need to ensure holder binding to the Access Token because the commitment is binding to the payload. In other words, as long as the commitment can only be used to cast one specific ballot and the AS authorized the casting of that ballot, it does not matter which Client is casting. The ballot itself is created using voting credentials, the validity of which is established when votes are tallied.

4.5 Client Resource Access Control

Here we summarize how the App interacts with the other protocol entities, and how these exchanges are protected.

Dynamic Client Registration (Client-ER)^I: The App registers as OAuth Client with the ER, following [Ri15], including a public key (JWK) for authentication to the ER and DPoP.

Notification Registration (Client-NS)^D: The App registers with the NS.

Masked ACC retrieval (Client-RT)^{DX}: The App obtains an Access Token from the ER and uses Token Exchange to obtain tokens with individual RTs as the audience, scoped to ACC retrieval.

PIN retrieval (Client-RT)^{DTX}: The mask shares are fetched from the RTs.

Proof of correctness retrieval (Client-RT)^{DTX}: The shares of DVNIZKP for the correctness of the ACCs are fetched from the RTs.

Ballot casting (Client-BB)^{CDX}: The App requests a Commitment Access Token (CAT) from the ER, and casts ballots to BBs. Honest BBs must reject ballots without valid CAT. The ER may limit the frequency of issued CAT to mitigate against brute force attacks.

Requests are protected as follows:

^C Commitment Access Token, described in Sect. 3.2, required to access BBs.

^D Demonstrating Proof-of-Possession (DPoP) [Fe23].

^IThe voter leverages their national electronic ID system to authenticate to the ER, establishing the right to vote. This is outside the scope of this paper.

^T At a random time, subsequent to the previous step, and following notification of availability by the NS.

^X Token Exchange [Jo20] used to reach multiple RS, i.e. RTs and BBs.

5 Threat model

We address the following parts of an OWASP threat modeling process [OW]: the main security and functionality properties and requirements (Sect. 5.2), assumptions on the use case scenario and on the infrastructure (Sect. 5.3), attackers and their capabilities (Sect. 5.4), and threat mitigation enabled by the proposed solution, and how it attempts to satisfy the stated requirements and properties (Sect. 5.5). However, in order to better explain and justify the assumptions and attackers considered in the analysis, we first introduce the context for which the protocol has been designed in Sect. 5.1.

5.1 Context and application scenario

Our threat model starts with the assumption that an untappable channel is not available to voters. The i-voting protocol in [Lo22] is developed specifically for the scenario of national elections in which citizens abroad have the right to vote, but the current paper-based postal voting system has known flaws.

In this context, voters are typically dispersed over a broad area spanning multiple countries, even considering only one constituency. This situation makes it impractical to provide enough secure voting booths so that every voter is reasonably close to one. Therefore, in order to increase voter turnout, the proposed protocol avoids to request physical presence of voters in a secure environment by making some assumptions (see Sect. 5.3).

This somewhat softens coercion resistance because some kinds of attacks (e.g. persistent surveillance malware on the voting device) cannot be thwarted without an untappable channel (in practice, a secure environment).

5.2 Requirements and Properties

Recommendations on standards for e-voting systems have been specified by the Council of Europe (CoE) [Co]. Requirements are enumerated under four suffrage principles - universality, equality, freedom, and secrecy - and other systemic requirements - regulatory, transparency, accountability, reliability, and security. In particular, we highlight the following requirements as relevant to our proposal:

Universality: CoE 1 The voter interface of an e-voting system shall be easy to understand and use by all voters.

Equality: CoE 7 Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.

CoE 8 The e-voting system shall only grant a user access after authenticating them as a person with the right to vote.

Freedom: CoE 10 The voter's intention shall not be affected by the voting system, or by any undue influence.

CoE 15 The voter shall be able to verify that their intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.

Secrecy: CoE 26 The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.

At a technical level, the protocol (Sect. 4) aims to guarantee correctness and coercion resistance [JCJ10], fairness [Co], accountability [KTV10], ballot secrecy and end-to-end verifiability [US21], and eligibility verifiability [CGG19; Sm10].

5.3 Assumptions

An untappable channel is typically required to issue the real ACC, so that a coercer cannot intercept it. The suggested implementation for this channel is typically the physical presence of the voter, which is difficult to reconcile with voters residing abroad. Given its application context (see Sect. 5.1), the ACC proposal in [Lo22] substitutes this requirement with the following assumptions:

A1: Surveillance gaps. The coercer cannot continuously oversee the voter, i.e., there are wide surveillance gaps in which the voter is free to act.

A2: A threshold of honest RS. At least one trusted RT does not collude with the coercer. More precisely, at least one trusted RT is required to construct an ACC, and at least one trusted RT is required to be available to respond to ruse PIN requests without informing a colluding coercer. Moreover a threshold of honest TTs assure that TTs do not collude to improperly decrypt ballots. The exact number of trusted RTs and TTs required depends on security vs availability trade-offs in the setup of the Secure MPC Protocols.

Note that malware could maintain continuous surveillance on a single device. See Sect. 5.5 for further details and mitigations.

Further assumptions, e.g., on trustworthiness of servers, the level of assurance of eID authentication, or the robustness of low-level cryptographic implementations, are inherited from the base protocol and beyond the scope of this paper.

5.4 Threats

The main attacker of concern to our proposal is the *Coercer* in the sense of [JCJ10]:

Coercer: an adversary attempting to unduly influence the result of the election.

Objectives: forcing voters to vote in a specific way and prove it (forced disclosure), or to not vote at all (forced abstention).

Capabilities: observing the voter, and requesting recordings of voter actions.

Threats: coercers mainly threaten vote freedom (CoE Principle III).

Vulnerabilities: exploit vulnerabilities to vote secrecy (CoE Principle IV).

Concretely, any i-voting solution in which votes are not cast in a secure environment is exposed to attacks such as direct oversight by the coercer in presence or by recording. The latter is enabled by the ability of the voter to record oneself while casting, or during any other stage of the voting process, such as when receiving a PIN or using the application. The unsupervised environment and the use of personal devices also increase risk of exposure to malware, which could be a more effective means of surveillance than a physically present coercer.

5.5 Mitigations

The protocol (Sect. 4) aims to satisfy voting requirements (Sect. 5.2) by ballot casting with ACC (possession factor) and PIN (knowledge factor). To mitigate against undue influence (freedom requirement CoE 10), the main anti-coercion mitigation is the ruse PIN, indistinguishable from the real PIN.

Coercion. Several coercion evasion strategies are enabled, including (i) claiming not to have received a PIN, (ii) verifying a ruse PIN with a forged DVNIZKP, (iii) casting an invalid vote by intentionally typing a ruse PIN, (iv) casting more than one ballot, and (v) using multiple devices.

Strategies (i) to (v) are effective against a physically present coercer; strategy (v) is effective against malware affecting a device after the registration phase, but surveillance malware active during registration enables a coercion strategy that reveals re-voting in tallying.

Brute force. Usability requirements (e.g., CoE 1) strongly suggest the PIN must be short, particularly if used seldom and delivered some time before usage. As pointed out in [Es20], a short PIN may be brute-forced: a coercer briefly in control of a voter's device could try multiple PINs, succeeding with non-negligible probability, then deprive the voter of the device. A rate-limiting measure on ballot casting is therefore advisable, but it must preserve all other requirements. In particular, anonymity (CoE 26) requires the ballot box does not authenticate the voter, and the BB cannot distinguish votes cast with the same ACC and/or PIN. Our proposed solution is the OAuth CAT (Sect. 3). Since the BB cannot do rate limiting, the AS must limit the number of cast attempts by a Client without revealing the identity of the voter to the BB: the CAT precisely allows anonymous authentication, thus considerably limits the impact of brute-force attacks. This countermeasure also mitigates against the "leaky duplicate removal" attack of [Es20], since it becomes more difficult to cast a valid (duplicate) vote.

Typos. Another problem with the PIN approach pointed out by [Es20] regards usability: humans are quite error-prone when entering a PIN, but the voting process cannot give feedback on its correctness to preserve coercion-resistance. In our proposal, the voter is aided in remembering the PIN by the possibility to check its correctness with the DVNIZKP

at any time, and re-requesting it⁴. Moreover we propose the usage of a visual representation - e.g., via a string of emojis - of the credential reconstructed with the inserted PIN that appears both when verifying the PIN and when voting. In this way the voter has some kind of feedback on the correctness of the inserted PIN.

The link between requirements (Sect. 5.2) and best practices (Sect. 2) with the proposed implementing measures is summarized in Tab. 2.

Tab. 2: Summary of requirements and implementing measures designed to meet them.

Requirement	Measure
CoE 1: Usability	Short PIN
CoE 7: Unique identification of voters	eID to authenticate at ER
CoE 8: Grant access after authenticating with the right to vote	ER as OAuth AS; OAuth best practices and CAT (Sect. 4.4)
CoE 10: No undue influence	CAT (Sect. 4.4), ruse PIN
CoE 15: Individual verifiability, undue influence detectability	Ruse PIN, CDGT (Sect. 4.3)
CoE 26: Vote anonymity - unlinkability of the unsealed vote and voter	CAT ⁵ (Sect. 4.4)
OAuth BCP 1: Replay prevention	DPoP
OAuth BCP 2: Client authentication	Signed JWT, DCR
OAuth BCP 3: Authorization code protection	PKCE
OAuth BCP 4: Privilege restriction	Token exchange

6 Final Remarks

In conclusion, this article offered an architecture for an OAuth 2.0-based solution that supports i-voting from a mobile native client using the protocol of [Lo22]. The proposed method makes use of two specific OAuth 2.0 extensions: Dynamic Client Registration and Token Exchange. Dynamic Client Registration provides two important functions inside the system. First, it allows for the acquisition of a unique client identity per app instance, essentially restricting the attack surface to particular instances of the app itself. Second, it makes it easier to register a public key, which is later used for authentication against the ER to acquire the CAT. Furthermore, the Access Tokens are bound to this public key using the DPoP mechanism, reducing the possibility of stolen tokens being reused. The token

⁴Note that the possibility to set a ruse PIN allows to employ anti-coercion strategies.

⁵in addition to measures specified by the protocol - verifiable mixing and re-encryption, additively homomorphic encryption, multi-party computation etc.

exchange is used to obtain a more restricted Access Token for downstream resource servers, which further improves security.

A threat model was established and discussed to guarantee the robustness of the proposed solution, and we suggested how the detected threats can be addressed within our design, ensuring a safe and trustworthy i-voting process. An interesting future work is a more comprehensive and rigorous threat analysis, and a formal proof of security of the protocol, which is also missing in [Lo22].

Acknowledgements

This work has been partially supported by “Futuro & Conoscenza Srl”, jointly created by the FBK and Poligrafico e Zecca dello Stato Italiano (IPZS, the Italian Government Printing Office and Mint), as well as by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU. The second and sixth authors are members of the INdAM Research Group GNSAGA.

References




- [Ad08] Adida, B.: Helios: Web-based Open-Audit Voting. In: USENIX Security Symposium. 2008, URL: <https://www.usenix.org/conference/17th-usenix-security-symposium/helios-web-based-open-audit-voting>.
- [Ar10] Araújo, R.; Ben Rajeb, N.; Robbana, R.; Traoré, J.; Youssfi, S.: Towards Practical and Secure Coercion-Resistant Electronic Elections. In: Cryptology and Network Security. Springer, 2010, DOI: [10.1007/978-3-642-17619-7_20](https://doi.org/10.1007/978-3-642-17619-7_20).
- [AT13] Araújo, R.; Traoré, J.: A practical coercion resistant voting scheme revisited. In: International Conference on E-Voting and Identity. Springer Berlin Heidelberg, 2013, DOI: [10.1007/978-3-642-39185-9_12](https://doi.org/10.1007/978-3-642-39185-9_12).
- [BS23] Boneh, D.; Shoup, V.: A graduate course in applied cryptography, <https://toc.cryptobook.us/>, 2023, visited on: 04/18/2023.
- [Ca20] Campbell, B.; Bradley, J.; Sakimura, N.; Lodderstedt, T.: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens, RFC 8705, 2020, DOI: [10.17487/RFC8705](https://doi.org/10.17487/RFC8705).
- [CCM08] Clarkson, M. R.; Chong, S.; Myers, A. C.: Civitas: Toward a secure voting system. In: 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, 2008, DOI: [10.1109/SP.2008.32](https://doi.org/10.1109/SP.2008.32).
- [CGG19] Cortier, V.; Gaudry, P.; Glondou, S.: Belenios: a simple private and verifiable electronic voting system. In: Foundations of Security, Protocols, and Equational Reasoning. Springer, 2019.
- [Co] Council of Europe: Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f, visited on: 10/22/2021.

- [Co19] Cortier, V.; Dreier, J.; Gaudry, P.; Turuani, M.: A simple alternative to Benaloh challenge for the cast-as-intended property in Helios/Belenios, working paper or preprint, 2019, URL: <https://hal.inria.fr/hal-02346420>.
- [DF89] Desmedt, Y.; Frankel, Y.: Threshold cryptosystems. In: Conference on the Theory and Application of Cryptology. Springer, 1989, DOI: [10.1007/0-387-34805-0_28](https://doi.org/10.1007/0-387-34805-0_28).
- [Es20] Estaji, E.; Haines, T.; Gjøsteen, K.; Rønne, P. B.; Ryan, P. Y.; Soroush, N.: Revisiting practical and usable coercion-resistant remote e-voting. In: Electronic Voting: 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6–9, 2020, Proceedings 5. Springer, pp. 50–66, 2020.
- [Fe23] Fett, D.; Campbell, B.; Bradley, J.; Lodderstedt, T.; Jones, M.; Waite, D.: OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP), RFC9449, Standards Track Draft, IETF WAP WG, 2023, URL: <https://www.rfc-editor.org/rfc/rfc9449>, visited on: 09/08/2023.
- [Go] Google Play Integrity API: Work with integrity verdicts, URL: <https://developer.android.com/google/play/integrity/verdict>, visited on: 04/14/2023.
- [Gr10] Groth, J.: A verifiable secret shuffle of homomorphic encryptions. Journal of Cryptology 23 (4), 2010, DOI: [10.1007/s00145-010-9067-9](https://doi.org/10.1007/s00145-010-9067-9).
- [Ha12] Hardt, D.: The OAuth 2.0 Authorization Framework, Best Current Practice, IETF RFC 6749, 2012, URL: <https://datatracker.ietf.org/doc/rfc6749/>, visited on: 04/07/2023.
- [He23] Heilman, E.; Mugnier, L.; Filippidis, A.; Goldberg, S.; Lipman, S.; Marcus, Y.; Milano, M.; Premkumar, S.; Unrein, C.: OpenPubkey: Augmenting OpenID Connect with User held Signing Keys, 2023, URL: <https://ia.cr/2023/296>.
- [IA23] IANA: JSON Object Signing and Encryption (JOSE), Assignment, IANA, 2023, URL: <https://www.iana.org/assignments/jose/jose.xhtml>, visited on: 04/18/2023.
- [JCJ10] Juels, A.; Catalano, D.; Jakobsson, M.: Coercion-resistant electronic elections. In: Towards Trustworthy Elections. Springer, 2010, DOI: [10.1007/978-3-642-12980-3_2](https://doi.org/10.1007/978-3-642-12980-3_2).
- [JCM15] Jones, M. B.; Campbell, B.; Mortimore, C.: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants, RFC 7523, RFC - Proposed Standard, 2015, URL: <https://datatracker.ietf.org/doc/rfc7523/>, visited on: 04/25/2023.
- [Jo20] Jones, M. B.; Nadalin, A.; Campbell, B.; Bradley, J.; Mortimore, C.: OAuth 2.0 Token Exchange, Proposed Standard, IETF RFC 8693, 2020, URL: <https://datatracker.ietf.org/doc/rfc8693/>, visited on: 04/14/2023.
- [KTV10] Küsters, R.; Truderung, T.; Vogt, A.: Accountability: definition and relationship to verifiability. In: Proceedings of the 17th ACM conference on Computer and communications security. 2010.
- [Lo22] Longo, R.; Morelli, U.; Spadafora, C.; Tomasi, A.: Adaptation of an i-voting scheme to Italian Elections for Citizens Abroad. In: E-Vote-ID 2022. 2022, DOI: <https://doi.org/10.15157/diss/027>.
- [Lo23] Lodderstedt, T.; Bradley, J.; Labunets, A.; Fett, D.: OAuth 2.0 Security Best Current Practice, Active Internet-Draft, OAuth WG, 2023, URL: <https://datatracker.ietf.org/doc/draft-ietf-oauth-security-topics/>, visited on: 04/25/2023.

- [NV12] Neumann, S.; Volkamer, M.: Civitas and the real world: problems and solutions from a practical point of view. In: Seventh International Conference on Availability, Reliability and Security. IEEE, 2012, DOI: [10.1109/ARES.2012.75](https://doi.org/10.1109/ARES.2012.75).
- [OW] OWASP: Threat Modeling Process, URL: https://owasp.org/www-community/Threat_Modeling_Process.
- [Ri15] Richer, J.; Jones, M. B.; Bradley, J.; Machulak, M.; Hunt, P.: OAuth 2.0 Dynamic Client Registration Protocol, Proposed Standard, IETF RFC 7591, 2015, URL: <https://datatracker.ietf.org/doc/rfc7591/>, visited on: 04/14/2023.
- [Sa14] Sakimura, N.; Bradley, J.; Jones, M. B.; de Medeiros, B.; Mortimore, C.: OpenID Connect Core 1.0, 2014, URL: https://openid.net/specs/openid-connect-core-1_0.html, visited on: 05/18/2023.
- [SBA15] Sakimura, N.; Bradley, J.; Agarwal, N.: Proof Key for Code Exchange by OAuth Public Clients, Best Current Practice, IETF RFC 7636, 2015, URL: <https://datatracker.ietf.org/doc/rfc7636/>, visited on: 04/04/2023.
- [Sh22] Sharif, A.; Carbone, R.; Sciarretta, G.; Ranise, S.: Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients. Journal of Information Security and Applications 65, 2022, DOI: <https://doi.org/10.1016/j.jisa.2021.103097>.
- [Sm10] Smyth, B.; Ryan, M.; Kremer, S.; Kourjieh, M.: Towards automatic analysis of election verifiability properties. In: Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security. Springer, 2010.
- [Tu18] Turan, M. S.; Barker, E.; Kelsey, J.; McKay, K. A.; Baish, M. L.; Boyle, M.: NIST SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, NIST, 2018, DOI: [10.6028/NIST.SP.800-90B](https://doi.org/10.6028/NIST.SP.800-90B).
- [US21] U.S. Election Assistance Commission: Voluntary Voting System Guidelines (VVSG) version 2.0, 2021, URL: <https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines>, visited on: 10/22/2021.

Track 2: Governance Issues

Identifying Factors Studied for Voter Trust in E-Voting – Review of Literature

Yannick Erb ¹, David Duenas-Cid ^{2,3}, Melanie Volkamer ⁴

Abstract: Trust is a precondition for the adoption of novel technologies (see, e.g., [ES21]). As more and more electoral commissions consider introducing e-voting solutions, research into voter trust in these systems grows in importance. As a basis for future research on trust in e-voting, we conducted a literature review. We identified 13 papers researching various factors influencing voters' trust in e-voting. In these papers, we determined a total of 64 potential factors, while the direction of their influence on voter trust may be either positive, negative, or both (positive/negative). These factors were subsequently systemized into five categories, ranging from socio-political to technology-related factors. These are then described and discussed. We also find shortcomings in the current empirical research on voter trust and propose directions for future research in order to address these.

Keywords: e-voting; i-voting; voter trust

1 Introduction

Digitization in society is now integrating digital technologies into all aspects of people's everyday lives, replacing analogue information with a digital form so it can be stored and processed digitally [FGR19] or creating new digital processes affecting our physical world [BMY20]. With a few exceptions, integration of digital technologies has not been as successful as expected in relation to democratic processes, such as elections and voting. In the early 2000s, the vision of voting remotely over the internet was voiced alongside growing interest in information and communication technologies (ICT), and experts were convinced that every democratic elections would be conducted using electronic voting in polling stations (e-voting) or remotely via the internet (i-voting) [Li21]. Even though ICT has been around for years, and there are success stories such as the Estonian i-voting system [En], we still cannot observe [In] widespread use of ICT for democratic processes. Use of ICT may deliver advantages for the field of voting, among others, offering improved

¹ Karlsruhe Institute of Technology, Institute of Applied Informatics and Formal Description Methods, Kaiserstraße 89, 76133 Karlsruhe, Germany. <https://orcid.org/0009-0006-7797-2061>. yannick.erb@kit.edu

² University of New South Wales, School of Information Systems and Technology Management, NSW 2052, Sydney, Australia

³ Gdansk University of Technology, Department of Informatics in Management, 11/12 Gabriela Narutowicza Street, 80-233 Gdańsk, Poland. <https://orcid.org/0000-0002-0451-4514>. david.duenas.cid@pg.edu.pl

⁴ Karlsruhe Institute of Technology, Institute of Applied Informatics and Formal Description Methods, Kaiserstraße 89, 76133 Karlsruhe, Germany. <https://orcid.org/0000-0003-2674-4043>. melanie.volkamer@kit.edu

accessibility to elections, higher efficiency in tallying [AS20] or greater convenience for younger or busy voters [LK17]; but also downsides that should likewise receive equal consideration such as security issues [LK17, FGR19], trust issues [Gi16], and social challenges such as computer literacy of the voting population [Tr16]. In the end, although offering advantages, e-voting is not only technically challenging but also impacts society and politics [Bu18].

Amongst the previous elements, “trust” appears to be one of the most relevant ones. Trust has been identified as a precondition for adoption and use of novel technologies [ES21]. The effects of missing trust in the e-voting system employed can be severe and may lead to a loss of voter confidence in elections and in overall comprehension of democracy, as was the case in the 2020 U.S. elections [SSP20, UL20]. Thus, establishing trust in e-voting solutions is crucial for democracies using such technologies. In order to tackle the topic, we aim to answer the following research question: *“Which factors influencing voters’ trust in e-voting have been researched in expert literature?”* in a generalistic manner, i.e., not focusing on specific countries, e-voting methods, or types of election.

To answer this question, we conducted a review of literature, studying empirical factors reported which potentially influence voter trust in e-voting. We consider research from different countries and regions, as well as different voting methods and types of elections. Following identification, factors are grouped thematically to enable a thematic discussion on these factors. While we identified 13 relevant papers with 64 such factors overall, and the direction of their influence on voter trust can be either positive, negative, or both (positive/negative), we also identified systematic issues with some of the research conducted and discuss directions for future research in order to encourage future research to focus on trust-related research questions in the context of e-voting.

2 Background

2.1 Electronic Voting and Internet Voting

E-voting is an umbrella term for “any process that benefits from use of [...] electronic technology by the election authorities [...] to run elections” [Bu18], including electronic voter registration, vote casting, tallying, and communication of results [Bu18].

Several countries have e-voting systems in use. The United States, for example, uses a mix of direct recording electronic voting machines and optical mark or character recognition [In]. Other countries, like Brazil, which employed an e-voting system in 1996, switched from paper voting because of election fraud [dFM17].

Envisioned by technology leaders like Bill Gates and Tim Cook, the idea of “cast(ing) [...] ballots from home or [...] wallet PCs” [GMR96] or “voting on phones” [SC21] has become a reality in what is referred to as ‘remote e-voting’ or, simply, i-voting (e.g., [ES21], [Li21]) or online voting (e.g., [BGG19], [GGB18]). For the purpose of simplicity, both terms for this special type of voting by e-voting will be subsumed under i-voting, as a clear distinction is not made in literature, and the terms are used interchangeably (see, e.g., [Li21]).

I-voting adoption has been prominently studied in the case of Estonian i-voting [FGR19, Li21], which has been used systematically since 2005, and provides much election data [ES21, SK19, So20]. Estonian i-voting, for example, is described as “cast[ing] [...] ballots from any internet-connected computer anywhere in the world” [En].

Licht et al. [Li21] offer an overview of literature concerned with i-voting and identify drivers and barriers to i-voting that can be observed in various contexts.

2.2 Trust in (New) Technology in General

Trust, representing a transversal concept that has been approached by different fields of research, can be broadly defined as “the belief that somebody [or something] is good, [...] and will not try to harm or deceive you” [Ox]. However, its inherent transversality crystalizes in the existence of various discipline-related definitions, and, in the end, the concept suffers from a lack of clarity [ES21]. Trust has been related to the need to reduce complexity and make social action affordable [Lu79], with the need for stability, transparency, and accountability [Sz03], or with the need to balance unequal knowledge distribution when facing complex systems [Gi91]. As suggested by Mayer et al.’s [23] definition (trust as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”), trust involves a number of participants that includes a trustor, a trustee and, in some occasions, an intermediary element such as an organization.

In this regard, technology appears as a mediating element [Bo21] that is generally understood by analyzing its capacity to provide expected outcomes due to the impossibility of inferring intentionality from it [DC22a] (although recent discussions connected with AI might question this [Hu17]). Trust in technology, hence, differs from trust in organizations or people, as the trustee is no longer a moral agent but a technological artifact created by humans that has limited capabilities [Mc11]. This point of departure allows us to approach trust in relation to electoral technology, such as e-voting [ES21]; but such an approach should not prevent understanding the role played by those stakeholders having the capacity to provide trust or distrust of the system even if not directly related to its functioning [DC22a].

3 Methodology – Conducting a Literature Review

To answer the research question, a literature review is undertaken of proceedings from E-Vote-ID conferences from the years 2016–2022. The E-Vote-ID conference serves as a meeting point for interdisciplinary experts related to e-voting (i.e., merging technical topics and governance-related topics), and their proceedings will be considered as a reference for research in this field. The conference produces two proceedings per year, one includes only academic papers published in the Springer LNCS series and a second publication including

all⁵ the peer-reviewed papers presented in the conference (published by different university press jackets⁶). The E-Vote-ID proceedings for the period 2016–2022 contain 247 unique records, of which 96 were published in Springer LNCS, and 151 were published under university jackets only.

This literature review is done *ad hoc* for the conference and serves as a measure of how the topic is approached in the conference community, tracing some general guidelines to understand the strengths and weaknesses of current approaches.

3.1 Description of the Steps of the Literature Review

The steps of the literature review and number of records included/excluded in the process are displayed in Fig. 1 and are explained in more detail in the following paragraphs.

In a first step (S1), we excluded the “PhD Papers” or “Demo” articles (n=68) from the 247 records, as they report the work briefly, and in the main with no detailed explanation. To identify relevant records, we searched for explicit use of the expression “*trust*” in full text recorded (S2) in the remaining 179 records, which led to removing 44 records not containing the expression. For the remaining 135 records, the full text PDF files were retrieved as papers (S3), and a two-step eligibility assessment (S4-S5) was carried out. Exclusion criteria for the eligibility assessment (S4-S5), screening step (S2), and initial removal of demo/PhD records (S1) are displayed in Tab. 1. In the first step of the eligibility assessment (S4), the remaining 135 papers were again searched for the expression “*trust*” and corresponding passages were read in detail, searching for factors that may influence voter trust in e-voting. That allowed us to exclude non-relevant records as “No Factors” (n=63). As this review sets out to identify empirically studied factors that influence voters’ trust in e-voting, a second assessment step (S5) reports that neither report a user nor expert study nor a literature review with matching focus were excluded as “No Study” (n=59). The final number of records fulfilling the research criteria (n=13) were included in the review (In1).

Fig. 2 provides an overview of papers per year according to whether they are related to trust or not and those actually conducting empirical studies on factors influencing voters’ trust. It reveals that research on topics related to voter trust makes up a substantial part of the conference proceedings, with at minimum 28% of articles (2022) published being related to voter trust. However, empirical research on voter trust does not reach the same numbers. Starting from 2017 (n=1), on average, only 7.27% of articles are concerned with empirical research on voter trust. Linear trend data shows increasing interest in empirical research into voter trust while the general interest in voter trust related topics seems to decrease. Interest in empirical research on voter trust peaked in 2019 and 2021.

⁵ Except for the proceedings of the E-Vote-ID 2022. Here, papers that are part of the Springer LNCS publication are not part of the university press cover publication.

⁶ 2016–2017: TUT Press, 2019–2020: TalTech Press, 2021–2022: University of Tartu Press

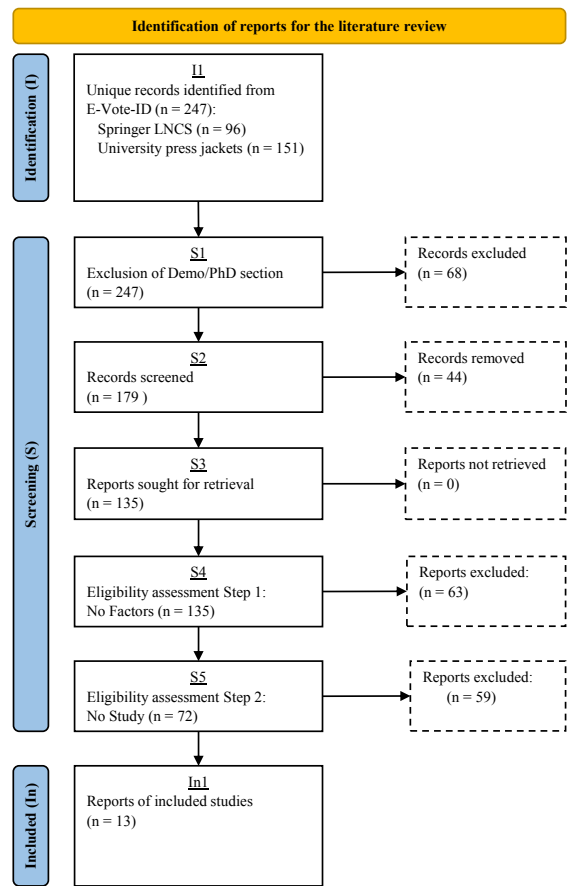


Fig. 1: Process of the literature review from the E-Vote-ID conference (adapted from [Pa21])

Step	Criterion	Description / Explanation	#Records excluded
S1: Exclusion of demo/PhD Section	Demo/PhD Paper	Papers of the E-Vote-ID PhD paper or demo section, being short and stating research is in progress.	68
S2: Screening	Not “*trust*”	All records that do not contain “*trust*” in the full text are excluded as they are outside the scope of this review.	44
S4. Eligibility assessment – Step 1	No factors	Papers for which no text passage that may hold a factor influencing voter trust could be identified (e.g., “trust” only in the name of institutions).	63
S5. Eligibility assessment – Step 2	No study	Papers that did not report user or expert studies; or were literature reviews with a matching focus.	59

Tab. 1: Overview of exclusion criteria for the different steps

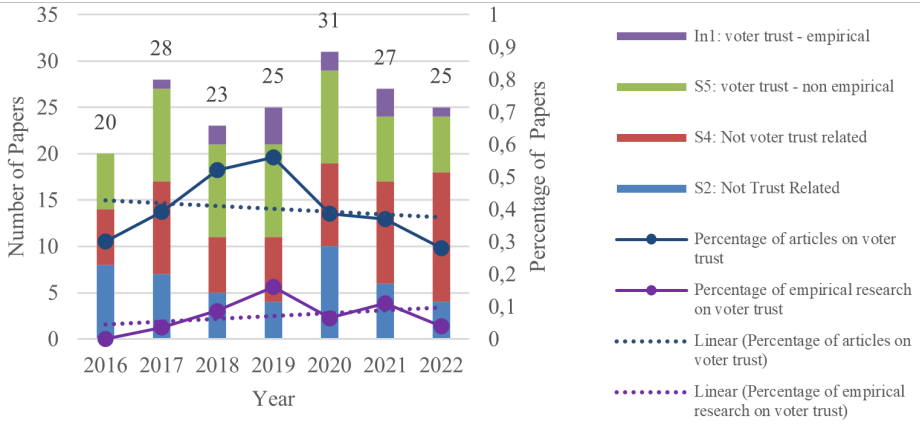


Fig. 2: Distribution of E-Vote-ID articles relating to trust (after excluding demo/PhD section records (S1))

The 13 papers included in the review are [Ag22], [AS20], [BGG19], [ES21], [FGR19], [GGB18], [Li21], [LK17], [SK18], [So20], [SK19], [Zo19], and [Zo21]. Appendix A1 (see [EDCV]) provides an overview of these, including the research approach chosen by the authors and the area, the type of elections, and the voting method studied.

3.2 First Results on Type of E-Voting and Considered Context

Regarding the 13 papers which we identified, it is noteworthy that most papers included are user studies ($n=11$), except for Licht et al. [Li21], who conduct expert interviews to inform their research, and Lindemane & Kuzmina [LK17] conducting expert interviews. Nine out of the thirteen papers focus on European countries. Some countries are studied multiple times, for example, Estonia, which is examined three times ([ES21], [SK19], [So20]), and Canada ([BGG19], [GGB18]) and Switzerland ([FGR19], [SK18]), studied in two papers respectively. Almost every paper focuses on national or European parliament elections. However, Alsadi & Schneider [AS20] study the case of representative elections in the UK, and the two studies focusing on Canada research indigenous self-governance of First Nations in Canada. Looking at the voting type studied, except for two studies on general e-voting ([FGR19], [LK17]), all use i-voting systems as subject of their research. Regarding the notion of trust, we find that only three studies define the term trust. Ehin & Solvak [ES21] and Agbesi et al. [Ag22] refer to the trust definition of Mayer et al. [MDS95], as presented in section 2.2, whereas in Zollinger et al. [Zo19] trust is identified as a mental model of voters. Out of the eight qualitative studies ([Li21], [Zo21], [BGG19], [FGR19], [Zo19], [GGB18], [LK17], [Ag22]) included in this review, only four mention how trust was measured in their studies ([Zo21], [FGR19], [Zo19], [Ag22]) stating that the word and notion of trust was used by the participants of their studies. For the five quantitative studies

([ES21], [So20], [AS20], [SK19], [SK18]), trust was measured by three studies using a scale from 0-10 for “Do you trust the procedure of internet voting?” or similar questions, with 0 representing the lowest level of trust and 10 the highest ([ES21], [SK19], [SK18]), and one study reports their participants to use the term trust ([AS20]).

3.3 Process to Identify and Categorize Potential Factors in Influencing Trust

For further examination, the full text of the 13 papers was analyzed in detail to identify potential factors they study for voter trust in e-voting. The corresponding passages were recorded in an Excel spreadsheet, along with the source paper and pages, a factor name for the factor described in the passage, a unique factor ID for every factor-passage combination, and coding for the direction of influence on voter trust into positive, negative, or positive/negative. Factors described as enhancing voter trust in the corresponding text passage were coded as positive for this occurrence, those described as decreasing voter trust or increasing distrust were coded as negative, and occurrences for which the influence could swing either way or was unclear were coded as positive/negative. For example, the text passage ‘Five participants also mentioned it as a confidence or trust feature, like P11 mentioned that it “give(s) a little more confidence” [Zo21], was coded with the factor name “Verifiability (General)” and direction of influence positive (Ex1), whereas for the text passage ‘A verification impact was raised, mainly decreasing trust, e.g.,” I don’t trust the application after verification, even if the tracking number is private” (P33), even though an opposite positive effect on trust was also mentioned by some users: “the second phase makes me feel secure” (P4)’ [Zo19] was coded with the same factor name but positive/negative regarding direction of influence (Ex2).

Coding was carried out inductively. Text passages containing a factor already described before were coded with the existing factor name. Where a novel factor was described, a new factor name was created, taking the wording of the text passage into account. The coding of text passages and factors was performed by a single coder. The identified factors were then inductively grouped thematically into distinct categories, with consultation and discussion between the authors.

4 Results

4.1 Overview of Individual Factors Influencing Voter Trust in E-Voting

The procedure described above led to 133 text passages with factors described as influencing voter trust in e-voting, of which 56 were coded as positive, 55 as negative, and 22 as positive/negative. Of these, 64 unique potential factors could be identified. Twenty-eight of these were only associated with text passages coded as positive, 22 only with text passages coded as negative, and 14 associated with text passages coded as positive/negative at least

once or as positive for one text passage and as negative for another. Continuing the example from section 3.3, the factor “Verifiability (General),” as being associated with a text passage coded as “positive/negative” at least once, is coded as exerting “positive/negative” influence on voter trust. Appendix A2 (see [EDCV]) shows an overview of all factors and their trust codings. The categorization of factors, as we described above, leads to five distinct categories. The categories and number of factors grouped into the respective categories can be observed in Tab. 2.

Category	Number of Factors
Socio-Political Sphere	11
Individual Sphere	9
Trust in other Technology/Institutions/People	12
Process Related	4
Technology Related	28
	64

Tab. 2: Overview of categories and number of factors in each category

4.2 Categorization of Potential Factors Studied for Voter Trust in E-Voting

The categories identified and factors they embrace are presented subsequently below. For each category, the identified factors are presented in a table alongside a description of the factor, its influence on trust (P=positive, N=negative, P/N=positive/negative), the literature it is based on (its numbering in the references), and whether the factor is explicitly empirically validated or not for each of its literature sources (in the occurrence of paper in source column; E=empirically validated, T=theoretically only, E/T=theoretically and empirically validated). Furthermore, it can be seen whether a factor has been reported for general e-voting (E), for i-voting (I), or both (E/I). Even though this literature review focuses on literature that empirically researches voter trust, there are factors brought up by the empirical literature we researched that are not empirically validated in the studies reviewed. However, so as not to lose any factors brought up by the literature reviewed, these are still reported and discussed alongside empirically validated ones but are accordingly only marked as being theoretically validated.

4.2.1 Socio-Political Sphere

This category encompasses factors tied to the voters’ social sphere, such as trusted elites or a voter’s social media bubble and factors linked to voters’ political sphere, such as a country’s political system, the political discourse, and the position of political parties. Although divided into two subcategories for better visualization, both spheres are intertwined and, thus, are discussed alongside each other in the literature. In total, this category contains

11 factors, which are coded 21 times and based on four source papers. The factors in both subcategories are only discussed for i-voting in the literature. Tab. 3 provides an overview of the factors grouped into the subcategory *Social Sphere*.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Heuristics	Voters use heuristics as a shortcut for decision-making on complex technology.	P/N	[ES21]	[T]	[I]
Social Cue Taking	Voters rely on cues from their own social sphere when deciding on level of trust in e-voting.	P/N	[ES21]	[T]	[I]
Trusted Social Actors	Trusted social actors influence the approach towards and perception of e-voting of voters.	P/N	[ES21]	[T]	[I]
Social Media	Social media influences the approach towards and users' perception of e-voting.	P/N	[Li21]	[E/T]	[I]
Social Trust	General trust within society is important for adoption of voting technology. High levels of general trust increase the likelihood of trust in new voting technology and the authorities dealing with them.	P	[Ag22]	[E]	[I]

Tab. 3: Socio-political factors in the subcategory *Social Sphere*

Tab. 4 does the same for the subcategory *Political Sphere*. Please note that the factor "Heuristics" is shown in both tables for completeness, even though it is not part of any of the subcategories but resides on a higher level of abstraction.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Heuristics	Voters use heuristics as a shortcut for decision-making on complex technology.	P/N	[ES21]	[T]	[I]
Political Cue Taking	Voters consider political actors' opinions and perceptions when deciding on trust in e-voting.	P/N	[Ag22], [ES21]	[T], [E/T]	[I]
Trusted Political Actors	Trusted political actors influence the approach towards and perception of e-voting of voters.	P/N	[Ag22], [ES21]	[E], [T]	[I]

Continued on next page

Tab. 4: Socio-political factors in the subcategory *Political Sphere*

Tab. 4 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Political Discourse	Current political discourse on e-voting influences voters' positions and attitudes toward e-voting.	P/N	[Ag22], [Li21]	[E], [E/T]	[I]
Perception of Administration	Positive public perception of administration of the election (e.g., being local).	P	[SK18]	[T]	[I]
Account for Political Culture	The voting system and functionality fit the political culture and voting procedure voters are used to, in the country the voting system is employed in.	P	[SK18]	[E]	[I]
Foreign Interference on Political Scene	The threat of malicious actors influencing the political landscape of a country.	N	[Ag22]	[E]	[I]

Tab. 4: Socio-political factors in the subcategory *Political Sphere*

4.2.2 Individual Sphere

The second category of factors entails factors that originate in the voters themselves, such as their education, experiences, knowledge, and perceptions. “Individual Sphere” contains nine factors that are coded ten times in total, and are distributed across six sources. We can observe that even though six sources discuss the factors, all of them only refer to i-voting. Tab. 5 provides an overview of these factors.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Perception of Technology	The voter's negative perception of the technologies/e-voting system in use and their security.	N	[Li21]	[E]	[I]
Changed Voter Behavior	Change in voting behavior leads to insecurities and opposition to the novel technology.	N	[BGG19]	[E]	[I]
Voter Education	Voters' level of education and cognitive sophistication (measured by the type of highest educational degree).	P/N	[ES21]	[E]	[I]

Continued on next page

Tab. 5: Factors in the category “Individual Sphere”

Tab. 5 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Past Experience / Path Dependency	Voters' past experiences with e-voting or with related technologies.	P/N	[Li21]	[T]	[I]
Experiences with Electronical Services in the Public Sector	Positive and plenty of experience with other electronic services in the public sector.	P	[SK19]	[E]	[I]
Computer Literacy	Voters have sufficient computer literacy and skills.	P	[SK19]	[E]	[I]
Lack of knowledge in Internet Technologies	Voters lack knowledge of internet technologies that form the basis for e-voting solutions.	N	[Zo19]	[E]	[I]
Voting Electronically	Voters have actually voted electronically in elections.	P	[SK19]	[E]	[I]
Additional Information	Sufficient additional information is given to the voter to understand the system and base a judgment on.	P	[Zo21]	[E]	[I]

Tab. 5: Factors in the category “Individual Sphere”

4.2.3 Trust in other Technology/Institutions/People

The category “Trust in other Technology/Institutions/People” encompasses factors tied to voters' trust in related technologies, institutions, and people that may (not) be transferred to e-voting. The category holds 12 factors in three subcategories. These are coded 24 times and appear in 7 out of the 13 papers included in the literature review. We find that several factors, especially all factors of the *Trust in Technology* subcategory, are reported for general e-voting as well as i-voting in particular. Tab. 6 provides an overview of the factors in this category.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Trust in Novel Technology (T)	Trust-Transference of trust in novel technology to e-voting.	P/N	[LK17]	[E]	[E/I]
Trust in Related Technology (T)	Trust in technologies related to e-voting (e.g., internet banking) and technology in general.	P	[FGR19], [Zo19]	[E], [E]	[E/I]
Correlation to Trust in Other Institutions (I)	Correlation of voters' trust in other institutions and their trust in e-voting.	P/N	[ES21]	[E]	[I]
Trust in Institutions (I)	Trust-transference of voters' trust in (state) institutions.	P	[Ag22], [FGR19], [Zo19]	[E], [E], [E]	[E/I]
Trust in Electoral System (I)	Trust in the current electoral system (involving various parties).	P	[Ag22]	[E]	[I]
Mistrust in Institutions (I)	Trust-transference of voters' mistrust in other institutions (that are in charge of the election) to e-voting.	N	[Li21]	[E]	[I]
Institutional Incompetence (I)	The election officials lack technical expertise when it comes to implementing voting technologies.	N	[Ag22]	[E]	[I]
Trust in Professionals (I)	Trust-transference of voter trust in professionals dealing with the technologies in use.	P	[Ag22], [FGR19]	[E], [E]	[E/I]
Trust in Media (I)	Trust in the media to expose corruption or cheating.	P	[Ag22]	[E]	[I]
Trust in Vendor (I)	Trust in the vendor of the election technology in use and knowledge of their affiliation and reputation.	P	[Ag22]	[E]	[I]
Mistrust in Vendor (I)	Mistrust in the vendor of the election technology in use, as they are involved with nation-states perceived as untrustworthy.	N	[Ag22]	[E]	[I]
Trust in Paper Voting (PV)	Trust-transference from trust in paper voting to using e-voting.	P	[So20]	[T]	[I]
*Subcategory: (T) = Trust in Technology, (I) = Trust in Institutions/People, (PV) = Trust in Paper Voting					

Tab. 6: Factors in the category "Trust in other Technology/Institutions/People"

4.2.4 Process Related

For the “Process Related” category, we find factors tied to the election proceedings, organization, vote counting, and election results. This category covers four factors in two subcategories. The factors are based on three source papers and coded four times. Tab. 7 provides an overview of the category.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Transparency (P)	Transparency of the voting process (e.g., voters can observe every step of the voting process).	P	[FGR19]	[E]	[E]
Understandability of Election Proceedings (P)	Understandability of the voting process (e.g., voters understand every process step).	P	[Zo19]	[E]	[I]
Immediate Results (R)	Election results can be provided immediately.	P	[GGB18]	[T]	[I]
Simplifying Tabulation (R)	Election tabulation is simplified and can be performed automatically.	P	[GGB18]	[T]	[I]
*Subcategory: (P) = Election Proceeding, (R) = Election Result					

Tab. 7: Factors in the category “Process Related”

4.2.5 Technology Related

The largest category contains factors tied to the e-voting system, its technical implementation and understandability, security and data privacy propositions, and verifiability of votes. The category contains 28 factors in 5 subcategories. They are coded 74 times in total and based on 10 out of the 13 papers included in the review. Tab. 8 provides an overview of the first four subcategories, and Tab. 9 provides an overview of the subcategory *Security & Privacy*, which is presented separately due to its size.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Lack of Trust in one Component (S)	A lack of voter trust in one system component undermines trust in the whole system.	N	[ES21]	T	[I]
Continued on next page					

Tab. 8: Factors in the category “Technology Related” (with the subcategory *Security & Privacy* excluded)

Tab. 8 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
System Reliability in Verifiability (S)	Voters have a negative attitude towards reliability of the verifiability mechanism (e.g., because of missing additional information to base judgments on).	N	[Zo21]	[E]	[I]
Demonstration (S)	Demonstration of the system to the public and/or within institutions.	P	[Li21], [SK18]	[E], [E]	[I]
System Reliability (S)	Reliability of the system as a whole (e.g., in case of power cuts, failures or outages)	N	[Ag22]	[E]	[I]
Usability (S)	Ease of use and clearly stated rules/steps must be followed.	P	[Ag22]	[E]	[I]
Technical Failure (T)	Technical failures and problems accepting their occurrence by the voter.	N	[Ag22], [Li21], [FGR19]	[E], [E], [E]	[E/I]
Distributed Ledger Technology (T)	Immutability induced by usage of distributed ledger technology.	P	[AS20]	[T]	[I]
Complexity (T)	E-voting systems are complex to understand and use.	N	[Ag22], [Li21], [Zo21]	[E], [E], [T]	[I]
Complexity of Verifiability (T)	Verifiability methods are complex to understand, and voters question their necessity.	N	[Zo21]	[T]	[I]
Verifiability (General) (V)	Verifiability is a key feature of creating observability for voters and the general public.	P/N	[Ag22], [Zo21], [So20], [AS20], [Zo19], [SK18]	[E], [E], [E], [E/T], [E], [E]	[I]
Possibility to Verify (V)	Being able to verify one's vote without necessarily performing the verification.	P	[So20], [AS20], [SK19]	[E/T], [E], [E]	[I]
Traceability (V)	It is possible for voters to trace their vote and ensure it matches their intention.	P	[Ag22]	[E]	[I]
Implementation (V_A)	The specific implementation of verifiability methods.	N	[Zo21]	[E]	[I]
Novelty (V_A)	Verifiability methods are novel, new, and unknown to voters.	N	[Zo21]	[T]	[I]

Continued on next page

Tab. 8: Factors in the category “Technology Related” (with the subcategory *Security & Privacy* excluded)

Tab. 8 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Understandability Issues (U)	Voters do not or cannot fully understand the e-voting system.	N	[Ag22], [Li21]	[E/T], [E]	[I]
Lack of Understanding of Verification (U)	A lack of understanding of the verifiability method b use, its available features, and prerequisites.	N	[Zo21], [AS20], [Zo19]	[E], [T], [E]	[I]
*Subcategory: (S) = System Related, (T) = Technology Related, (V) = Verifiability, (V_A) = Verifiability Aspects, (U) = Understandability					

Tab. 8: Factors in the category “Technology Related” (with the subcategory *Security & Privacy* excluded)

For *Security & Privacy*, several factors are reported for e-voting and i-voting. For all other categories, however, only damage to the public was reported for both voting types.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Data Privacy (P)	Voter data may be disclosed to private vendors selling e-voting technology.	N	[Ag22], [FGR19]	[E], [E]	[E/I]
Privacy Concerns in Verifiability (P)	The use of verifiability methods is viewed as a privacy breach by voters.	N	[Zo21]	[T]	[I]
Source Code Publication (S)	Publication of the source code or part of it to the public to engage with public and external experts.	P	[SK18]	[E]	[I]
Expert Audit (S)	Expert auditing of the e-voting system.	P	[Ag22], [SK18]	[E], [E]	[I]
Enhanced Voting Security (S)	Enhanced security of e-voting systems.	P	[Ag22], [AS20]	[E], [T]	[I]
Security Concerns (S)	Concerns regarding the security of e-voting systems (may include not only actual security breaches/risks but also perceived security).	P/N	[Ag22], [Li21], [FGR19], [Zo19]	[E], [E], [E], [E]	[E/I]
Security Risks (S)	Risks related to the security of systems.	P/N	[Ag22], [Zo21]	[E/T], [T]	[I]
Continued on next page					

Tab. 9: Factors in the subcategory *Security & Privacy* of the category “Technology Related”

Tab. 9 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Security Breaches (S)	A breach in voting system security may allow attackers to tamper with or disclose data.	N	[Li21], [FGR19]	[E], [E]	[E/I]
Damage to Public (S)	Problems in an e-voting system's security may lead to harm to the public community in general.	N	[FGR19]	[E]	[E]
Vote Forging (S)	Forging of votes in any way.	N	[Ag22], [FGR19]	[E], [E]	[E/I]
Authentication (S)	Authentication to prevent unauthorized logins to the voting platform as a security assurance.	P	[Ag22]	[E]	[I]
Explainability of Security Propositions (S)	Election authorities provide a complete and understandable explanation of levels of security provided.	P	[Ag22]	[E]	[I]
*Subcategory: (P)=Privacy, (S)=Security					

Tab. 9: Factors in the subcategory *Security & Privacy* of the category “Technology Related”

5 Discussion

5.1 Potential Factors for “Socio-Political Sphere”

Forming judgments on novel technology is complex, and citizens use effort reduction strategies to help form an opinion, such as heuristic methods. Literature describes how citizens use cue-taking from trusted social or political actors as an heuristic that helps them decide on their opinion towards i-voting. “Because of the cognitive and temporal costs of rational reasoning, individuals look to other trusted social actors [. . .] for signals suggesting what to think or how to behave” [ES21].

Two sources providing social cues influencing voter opinions for trusting i-voting were determined: Trusted social actors [ES21] and social media [Li21]. However, there is no empirical data on either cue-taking from social actors or social media provided by the authors. Those cues voters rely on when forming judgments on i-voting may also come from political parties, as empirically studied in the case of Estonian i-voting by Ehin et al. [ES21]. They found a correlation between voters’ position and political leanings and parties they voted for: those voting for parties with a high trust position toward i-voting also have higher trust in i-voting and vice-versa. This relation is described as being vivid and mutable, so party supporters change their individual position if their chosen party’s position on trust in i-voting changes. This is especially interesting because it opens the door

to considering new elements for understanding trust-related issues since parties' position on electoral innovation might be based on their expectations of how it could affect their electoral prospects and hence, this potential fear of innovation might be transferred to a trust-related dimension.

Besides cue-taking, other elements influencing individual opinions regarding trust and distrust were uncovered: the political discourse [Li21], the fear of foreign interference in the political landscape [Ag22], and general social trust within society [Ag22]. Data on Swiss trust in e-voting suggests that an e-voting system's features must furthermore match the political culture of the country it is employed in to have the intended effect [SK18]. For example, the possibility to cast multiple votes as is used in Estonia and considered trust building there, did not increase Swiss trust in e-voting as it did not correspond to Swiss voting behavior.

5.2 Potential Factors for “Individual Sphere”

Voter trust is negatively impacted by voters' perception regarding the technology itself. The lack of comprehension of how complex voting systems work or fears and concerns regarding their security are listed among these factors [Li21]. However, a change in voter behavior may also induce distrust. This can be observed in the case of Canadian First Nations, which oppose any change for historical reasons, and accordingly are opposed to i-voting even though its use would allow them better self-administration [BGG19].

Similarly, voter education [ES21] and computer literacy [SK19] impact voter trust. Ehin et al. [ES21] discovered that during the earlier years of Estonian i-voting, lower levels of education were associated with higher trust, shifting in later elections to higher levels of education, generating added trust. However, a statistical interpretation and explanation of this reported effect is not possible based on the data used. Regarding computer literacy, on the other hand, a positive relationship was identified [SK19]. In accordance with the above, voter education levels appear not to be explicative variables for understanding trust-related positions, while computer literacy appears to be a good predictor for them.

Voter trust also appears to be influenced by past experiences voters had [Li21]. This so-called path dependency can be observed in all fields of the social sphere and, hence, for use in election systems. In the case of Estonia, for example, extensive experience voters have gained using electronic services in the public sector is also considered as increasing trust in i-voting [SK19].

5.3 Potential Factors for “Trust in other Technology/Institutions/People”

Previous levels of trust in elements relating to implementation of e-voting and i-voting appear to exhibit a positive correlation with further adoption of it. For example, voters with higher levels of trust in technology [Zo19] or who are used to related technologies, such as e-banking [FGR19], also tend to trust e-voting and i-voting solutions. Similarly, people

working in digitized environments or experiencing digitization processes are found to be more likely to adopt i-voting [Zo19].

Similar patterns for e-voting and i-voting are further described in relation to trusting other institutions. A positive correlation has been described between trust in i-voting and trust in political institutions, such as the parliament, government, or politicians [ES21, Zo19]. But this relation is limited to certain conditions, and for such a trust transference towards e-voting to succeed, the government must be sole guarantor of the system [FGR19]; and even then, there is no guarantee that trust established with political institutions is going to transfer to i-voting [Li21]. For i-voting, it is reported that the same relationship also works in the opposite direction; systems can only be as trustworthy as the people proposing and constructing them: e-voting technologies might not be accepted if voters do not trust election authorities [Li21].

Finally, trust transference is also observed from other voting channels. Besides the obvious differences between paper and e-voting and the various risks involved, trusting paper voting has been found to positively influence levels of trust concerning i-voting [So20]. In this case, we might infer that trusting institutions can transversally positively influence different voting channels, and therefore, the explanation for transferring trust from paper to e-voting might not be due to the system itself but due to previously existing levels of trust.

5.4 Potential Factors for “Process Related”

E-voting trust-related elements are described as extending beyond the technology itself, including elements relating to the process followed or employed for its implementation and management. For example, voters have increased trust in processes they understand [Zo19]. Simpler voting systems, such as traditional paper-based voting, are based on steps that are easy to understand and observe for every voter [FGR19, Zo19], although this is not reproduced in the same manner in e-voting or i-voting processes. Mistakes made by humans involved in this process are described as easier to accept than those made by software [FGR19]. Increasing transparency by sharing backstage processes of an e-voting election via, for example, live broadcasting may help mitigate these issues [FGR19]. While transparency was reported for general e-voting systems, understandability was highlighted for i-voting as a voting method, indicating that transparency of background processes alone may not be sufficient for voters to trust i-voting solutions, as they do not understand the steps necessary to take in order to vote or the processes behind these.

On the other hand, i-voting also delivers some simplification of processes that help build trust. The use of technology increases processual convenience, providing simplified ballot tabulation and immediate results and positively impacting trust in voting and election results, and between the government and citizens [GGB18].

5.5 Potential Factors for “Technology Related”

As this category covers many factors, it is divided into five subcategories, the first of which is *System-Related Aspects*, all of which factors are only described for i-voting. Serving as a general remark, it must be noted that lacking trust in a single system component can undermine the trust in the whole i-voting system [ES21]. On the other hand, demonstrating the system to the public before using it for elections is described as a method contributing to helping build trust in the new system [Li21, SK18], empirically observed in use of a demo website in Switzerland [SK18]. Demonstrations such as this may include not only demonstrations to voters but also rhetoric and competence demonstrations with a focus on institutions [Li21].

For the *Technical Aspects* subcategory, the literature suggests that technical failure is reported to be a factor negatively influencing trust in e-voting as well as i-voting solutions [Ag22, FGR19, Li21]. Aligned with this, system or software failures are difficult to accept by voters [FGR19]. Demonstrations of technology, once again, were proven effective to re-establish trust in systems that had previously experienced technical failures [Li21]. Regarding i-voting in particular, the complexity of voting systems contributes negatively to building trust [Ag22, Li21], especially when verification is in place [Zo21].

Privacy & Security aspects are important elements in relation to technical aspects of e-voting and i-voting. Looking at the privacy propositions e-voting and i-voting are associated with, there are concerns that private companies offering such voting solutions may obtain voters' personal data and voting preferences [Ag22, FGR19]. Moreover, for the case of i-voting, voters may view verifiability methods as privacy breaches [Zo21]. Regarding security, we find that enhancing an i-voting system's security is a factor positively influencing voter trust in the system [Ag22, AS20]. However, security is not an obvious element that average voters can understand immediately, and therefore, perceived security is more important than security actually provided. This perception and, consequently, trust are negatively influenced by security concerns voters may have [FGR19, Li21, Zo19], security risks they can perceive [Zo21], or security breaches occurring [FGR19, Li21]. Such negative effects on trust are reported for general e-voting as well as i-voting in particular. This is especially crucial, as e-voting systems may be available globally and can be attacked from anywhere in the world, affecting the entire nation and leading to fear of harm to the public setting [FGR19]. Publishing source codes and expert audits are considered as enhancement measures to increase levels of trust in i-voting solutions [SK18]. However, a survey conducted on i-voting usage in Switzerland revealed that expert audits were supported as trust-building measures, but not publication of source codes [SK18]. To increase levels of trust in and integrity of i-voting process, verifiability is one of the key trust features for i-voting systems [AS20]. It provides mechanisms for voters (individual verifiability) and the public (universal verifiability) to observe correct system behavior [AS20]. Its positive impact in increasing confidence in election results is supported by the findings of qualitative (e.g., [Zo21], [Zo19]) and quantitative studies (e.g., [So20], [AS20]). However, verification may also increase distrust, for example, because of privacy concerns or because voters cannot see its purpose [Zo19]. Interestingly, the possibility of verification has already increased trust in Estonian

studies, even if it was not actually used [So20, SK19]. For non-national representative elections, it was considered a bonus for a case study in England but deemed necessary for general elections [AS20].

A final subcategory is *Understandability*. We find that for i-voting, understandability issues lead to increasing security concerns and, thus, mistrust [Li21]. This is especially true for systems that also apply verifiability. A lack of understanding of verifiability, its purpose, and the way it works may lead to mistrust [AS20, Zo19], as verification is not natural for voters [Zo19] and may lead to their questioning the integrity of the election [AS20]. Additional information, evidence, and proofs [Zo21], as well as easy-to-perform mechanisms [Zo19], may help mitigate these problems. Understandability issues were not reported for general e-voting.

6 Conclusion

This work set out to answer the question of which factors are reported as potentially influencing voter trust in e-voting, performing a literature review of E-Vote-ID conference proceedings dating back to 2016. We identified 13 articles (see A1 in [EDCV] for an overview of these) with relevance for the matter of interest, from which we could identify 64 potential factors and their described direction of influence on voter trust in e-voting and i-voting. These factors were grouped into five distinct categories for further discussion, namely (1) “Socio-Political Sphere,” (2) “Individual Sphere,” (3) “Trust in Other Technology/Institutions/People,” (4) “Process Related,” and (5) “Technology Related.” Our findings and empirical literature identified can be used as a stepping stone for further research and assistance to understand how voter trust in e-voting can be established.

This work brings with it four major implications for research and practice. First, we present and discuss a large set of factors reported as influencing voter trust in e-voting and i-voting for different settings and countries. We believe these are potential factors worth considering, as their (direction of) impact may differ across different voting settings and/or countries. To the best of the authors’ knowledge, this is the first literature review of this kind, considering multiple countries and e-voting scenarios. The importance of our review’s findings has grown as research on e-voting in general has become more timely and important due to the COVID-19 pandemic (see, e.g., [KDCK21]) and as trust is a precondition for using novel technologies [ES21].

Second, a lack of empirical research on voter trust becomes apparent when regarding the distribution of papers covering the topic of voter trust in E-Vote-ID (see Fig. 2), which can be viewed as a reference for research in the field. Furthermore, this research is Europe-centric and focuses mainly on i-voting. Therefore, e-voting research lacks points of view, including non-European or developing countries, other e-voting methods, and voting scenarios not included in the review.

Third, the factors identified are categorized for further use in research and practice, building a stepping stone for future research in the field or a reference point for designing new e-voting solutions or the evaluation of existing systems. While we acknowledge that the

(direction of) impact of the potential factors identified may vary for different use cases, we argue that a large set of factors worth considering for e-voting solutions enables solutions perceived as being more trustworthy by voters. We also discuss the factors with regard to their respective voting type. Most factors have been studied prominently or only for i-voting. However, general e-voting and i-voting share factors regarding data privacy, security issues, and technical failure. Also, trust transference from trust in technology, institutions, and professionals can be observed for both voting types. On the other hand, differences seem to be present for the proceeding of the election, with trust in e-voting being influenced by the transparency of the proceedings but trust in i-voting by its understandability to the voter. The discrepancies in factors for e-voting and i-voting may be due to the relative majority of i-voting as studied voting method for the reviewed literature.

Fourth, current empirical research on voter trust seems to focus largely on the technical point of view, as we find that factors relating to the technology in use constitute almost half of factors determined, and 70% of articles in the review are associated with this category. Security topics and verifiability comprise the greatest number of factors within this category. Thus, we identify a need for more research in directions other than technology. For example, factors relating to the e-voting process or the voters themselves appear to have been insufficiently studied, and research on socio-political factors is mainly based on two studies ([ES21] and [Ag22]).

However, this work does not come without limitations, which open the door to further improvements and can be summarized as follows. For this work, only papers published in E-Vote-ID conference proceedings were used. Thus, interesting related work or studies from other journals and conferences are not included, along with factors that may be described there. Furthermore, the coding of articles was performed by only a single researcher. The absence of a second coder and co-coding discussion may lead to subjective bias concerning the text passages chosen and interpretation of these that leads to uncovering/naming the factors and direction of their influence. However, the categorization of factors found was performed in a discussion between the authors, decreasing subjective bias in this process step. Finally, there is only one axis used for capturing the direction of influence. However, there are more fine-grained views on trust in e-voting. For example, Duenas-Cid [DC22a, DC22b] consider trust and distrust on two different axes, each from “(Dis)Trust” to “Not to (Dis)Trust,” leading to a more fine-grained interpretation.

To leverage the work done in this article and overcome its limitations, we propose future research directions in the field of voter trust in e-voting. Building on this work, empirical studies of voter trust in e-voting could be conducted with or without focusing on specific factors or categories. Ideally, these studies would focus on categories considered underrepresented by this work (such as individual, socio-political, or process-related factors) and would be designed as cross-country studies to grasp effects shared by several countries and find differences between them. Such a call for cross-country considerations is also formulated for the European Union in [Tr16]. Studies like this would help to close the gap in empirical research on voter trust identified above. Furthermore, future work should investigate the differences in trust behaviour with regard to different voting methods (such as general e-voting, i-voting, etc.) in more detail or breadth. This could be, for example,

done by building on this study but including other outlets as well to increase the number of publications in the review.

7 Acknowledgments

The work of David Duenas-Cid has received funding from the Electrust (EU H2020 MSCA programme, grant agreement no. 101038055) and Dynamika (braku) zaufania w kreowaniu systemów głosowania internetowego (Narodowe Centrum Nauki, OPUS-20 competition, grant agreement no. 2020/39/B/HS5/01661) projects.

This work was supported by funding from the project “Engineering Secure Systems” of the Helmholtz Association (HGF) [topic 46.23.01 Methods for Engineering Secure Systems] and by KASTEL Security Research Lab.

References

- [Ag22] Agbesi, Samuel; Dalela, Asmita; Budurushi, Jurlind; Kulyk, Oksana: “What Will Make Me Trust or Not Trust Will Depend Upon How Secure the Technology Is”: Factors Influencing Trust Perceptions of the Use of Election Technologies. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Germann, Micha; Glondou, Stéphane; Hofer, Thomas; Krivososova, Iuliia; Martin-Rozumilowicz, Beata; Rønne, Peter; Zollinger, Marie-Laure, eds): Seventh International Joint Conference on Electronic Voting (E-Vote-ID) 2022. University of Tartu Press, Tartu, Estonia, pp. 1–17, 2022.
- [AS20] Alsadi, Mohammed; Schneider, Steve: Verify My Vote: Voter Experience. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Glondou, Stéphane; Krivososova, Iuliia; Kulyk, Oksana; Küsters, Ralf; Martin-Rozumilowicz; Rønne, Peter; Solvak, Mihkel; Spycher Oliver, eds): Fifth International Joint Conference on Electronic Voting (E-Vote-ID 2020). TalTech Press, Tallinn, Estonia, pp. 280–295, 2020.
- [BGG19] Budd, Brian; Gabel, Chelsea; Goodman, Nicole: Online Voting in a First Nation in Canada: Implications for Participation and Governance. In (Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique; Beckert, Bernhard; Küsters, Ralf; Serdült, Uwe; Duenas-Cid, David, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 50–66. Springer International Publishing, Cham, 2019.
- [BMV20] Baskerville, Richard L.; Myers, Michael D.; Yoo, Youngjin: Digital First: The Ontological Reversal and New Challenges for Information Systems Research. *MIS Quarterly*, 44(2):509–523, 2020.
- [Bo21] Bodó, Balázs: Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, 23(9):2668–2690, 2021.
- [Bu18] Budurushi, Jurlind; Neumann, Stephan; Renaud, Karen; Volkamer, Melanie: Introduction to special issue on e-voting. *Journal of Information Security and Applications*, 38:122–123, 2018.

- [DC22a] Duenas-Cid, David: A theoretical framework for understanding trust and distrust in internet voting. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Germann, Micha; Glondou, Stéphane; Hofer, Thomas; Krivonosova, Iuliia; Martin-Rozumilowicz, Beata; Rønne, Peter; Zollinger, Marie-Laure, eds): Seventh International Joint Conference on Electronic Voting (E-Vote-ID) 2022. University of Tartu Press, Tartu, Estonia, pp. 57–62, 2022.
- [DC22b] Duenas-Cid, David: The sociotechnical construction of trust and distrust in electronic voting: The case of the Netherlands [Presentation], 25.05.2022.
- [dFM17] de Freitas, Jorge Lheureux; Macadar, Marie Anne: The Brazilian Electronic Voting System: evolution and challenges. In (Krimmer, Robert; Volkamer, Melanie; Braun-Binder, Nadja; Loeber, Leontine; Maurer, Ardit Driza; Pereira Olivier; Duenas-Cid, David; Roenne, Peter; Kersting, Norbert; Schürmann, Carsten; Kulyk, Oksana; Vinkel, Priit, eds): Second Joint International Conference on Electronic Voting (E-Vote-ID 2017). TUT Press, Tallinn, Estonia, pp. 59–71, 2017.
- [EDCV] Erb, Yannick; Duenas-Cid, David; Volkamer, Melanie: Appendix A. https://secuso.aifb.kit.edu/downloads/documents/EVoting_Trust_Paper_Appendix_A.pdf. Accessed: 2023-09-14.
- [En] Enterprise Estonia: e-Governance - e-Democracy & open data. <https://e-estonia.com/solutions/e-governance/e-democracy/>. Accessed: 2022-08-17.
- [ES21] Ehin, Piret; Solvak, Mihkel: Party Cues and Trust in Remote Internet Voting: Data from Estonia 2005–2019. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel; Germann, Micha, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 75–90. Springer International Publishing, Cham, 2021.
- [FGR19] Fragnière, Emmanuel; Grèzes, Sandra; Ramseyer, Randolph: How do the Swiss Perceive Electronic Voting? Social Insights from an Exploratory Qualitative Research. In (Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique; Beckert, Bernhard; Küsters, Ralf; Serdült, Uwe; Duenas-Cid, David, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 100–115. Springer International Publishing, Cham, 2019.
- [GGB18] Goodman, Nicole; Gabel, Chelsea; Budd, Brian: Online Voting in Indigenous Communities: Lessons from Canada. In (Krimmer, Robert; Volkamer, Melanie; Cortier, Véronique; Goré, Rajeev; Hapsara, Manik; Serdült, Uwe; Duenas-Cid, David, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 67–83. Springer International Publishing, Cham, 2018.
- [Gi91] Giddens, Anthony: The consequences of modernity. Polity Press, Cambridge, 1991.
- [Gi16] Gibson, J. Paul; Krimmer, Robert; Teague, Vanessa; Pomares, Julia: A Review of E-voting: The Past, Present and Future. *Annals of Telecommunications*, 71(7-8):279–286, 2016.
- [GMR96] Gates, Bill; Myhrvold, Nathan; Rinearson, Peter: The Road Ahead. Penguin Books, Harmondsworth, Middlesex, UK, 2 edition, 1996.
- [Hu17] Hurlburt, George: How much to Trust Artificial Intelligence? *IT Professional*, 19(4):7–11, 2017.

- [In] International Institute for Democratic and Electoral Assistance: ICTS in Elections Database. <https://www.idea.int/data-tools/data/icts-elections>. Accessed: 2022-08-17.
- [KDCK21] Krimmer, Robert; Duenas-Cid, David; Krivososova, Iuliia: Debate: Safeguarding Democracy During Pandemics. Social Distancing, Postal, or Internet Voting— the Good, the Bad or the Ugly? *Public Money & Management*, 41(1):8–10, 2021.
- [Li21] Licht, Nathan; Duenas-Cid, David; Krivososova, Iuliia; Krimmer, Robert: To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel; Germann, Micha, eds): *Electronic Voting, Lecture Notes in Computer Science*, pp. 91–105. Springer International Publishing, Cham, 2021.
- [LK17] Lindemane, Marija; Kuzmina, Jekaterina: Outstripping of the eVoting Evolution. In (Krimmer, Robert; Volkamer, Melanie; Braun-Binder, Nadja; Loeber, Leontine; Maurer, Ardita Driza; Pereira Olivier; Duenas-Cid, David; Roenne, Peter; Kersting, Norbert; Schürmann, Carsten; Kulyk, Oksana; Vinkel, Priit, eds): *Second Joint International Conference on Electronic Voting (E-Vote-ID 2017)*. TUT Press, Tallinn, Estonia, 2017.
- [Lu79] Luhmann, Niklas: *Trust and Power*. Wiley-Blackwell, Chichester, 1979.
- [Mc11] Mcknight, D. Harrison; Carter, Michelle; Thatcher, Jason Bennett; Clay, Paul F.: Trust in a Specific Technology. *ACM Transactions on Management Information Systems*, 2(2):1–25, 2011.
- [MDS95] Mayer, Roger C.; Davis, James H.; Schoorman, F. David: An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3):709, 1995.
- [Ox] Oxford Academic Dictionary: trust - noun. <https://www.oxfordlearnersdictionaries.com/definition/academic/trust1?q=trust>. Accessed: 2023-09-11.
- [Pa21] Page, Matthew J.; McKenzie, Joanne E.; Bossuyt, Patrick M.; Boutron, Isabelle; Hoffmann, Tammy C.; Mulrow, Cynthia D.; Shamseer, Larissa; Tetzlaff, Jennifer M.; Akl, Elie A.; Brennan, Sue E.; Chou, Roger; Glanville, Julie; Grimshaw, Jeremy M.; Hróbjartsson, Asbjørn; Lalu, Manoj M.; Li, Tianjing; Loder, Elizabeth W.; Mayo-Wilson, Evan; McDonald, Steve; McGuinness, Luke A.; Stewart, Lesley A.; Thomas, James; Tricco, Andrea C.; Welch, Vivian A.; Whiting, Penny; Moher, David: The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ (Clinical research ed.)*, 372:n71, 2021.
- [SC21] Swisher, Kara; Cook, Tim: Apple's C.E.O. Is Making Very Different Choices From Mark Zuckerberg. <https://www.nytimes.com/2021/04/05/opinion/apples-ceo-is-making-very-different-choices-from-mark-zuckerberg.html>, 05.04.2021. Accessed: 2022-08-18.
- [SK18] Serdült, Uwe; Kryssanov, Victor: Internet Voting User Rates and Trust in Switzerland. In (Krimmer, Robert; Volkamer, Melanie; Cortier, Véronique; Duenas-Cid, David; Goré, Rajeev; Hapsara, Manik; Koenig, Reto; Martin Steven; McDermott, Ronan; Roenne Peter; Serdült, Uwe; Truderung, Tomasz, eds): *Third International Joint Conference on Electronic Voting (E-Vote-ID 2018)*. TalTech Press, 2018.

- [SK19] Solvak, Mihkel; Krimmer, Robert: The Curse of Knowledge? Does Having More Technology Skills Lead to Less Trust Towards iVoting? In (Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Cortier, Véronique; Maurer, Ardita Driza; Duenas-Cid, David; Helbach Jörg; Koenig, Reto; Krivososova, Iuliia; Küsters, Ralf; Rønne, Peter; Serdült, Uwe; Spycher Oliver, eds): Fourth Joint International Conference on Electronic Voting (E-Vote-ID 2019). TalTech Press, Tallinn, Estonia, pp. 204–207, 2019.
- [So20] Solvak, Mihkel: Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. In (Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Küsters, Ralf; Kulyk, Oksana; Duenas-Cid, David; Solvak, Mihkel, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 213–228. Springer International Publishing, Cham, 2020.
- [SSP20] Sanger, David E.; Stevens, Matt; Perlroth, Nicole: Election Officials Directly Contradict Trump on Voting System Fraud. <https://www.nytimes.com/2020/11/12/us/politics/election-officials-contradict-trump.html>, 2020. Accessed: 2022-08-17.
- [Sz03] Sztompka, Piotr: Trust: A sociological theory. Cambridge University Press, Cambridge, 2003.
- [Tr16] Trechsel, Alexander H.; Kucherenko, Vasyl; Silva, Frederico; Gasser, Urs: Potential and Challenges of E-Voting in the European Union. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf, 2016. Accessed: 2022-09-06.
- [UL20] Ulmer, Alexandra; Layne, Nathan: Trump Allies Breach U.S. Voting Systems in Search of 2020 Fraud 'Evidence': A Reuters Special Report. <https://www.reuters.com/investigates/special-report/usa-election-breaches/>, 2020. Accessed: 2022-08-18.
- [Zo19] Zollinger, Marie-Laure; Distler, Verena; Rønne, Peter; Ryan, Peter Y. A.; Lallemand, Carine; Koenig, Vincent: User Experience Design for E-Voting: How Mental Models Align with Security Mechanisms. In (Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Cortier, Véronique; Maurer, Ardita Driza; Duenas-Cid, David; Helbach Jörg; Koenig, Reto; Krivososova, Iuliia; Küsters, Ralf; Rønne, Peter; Serdült, Uwe; Spycher Oliver, eds): Fourth Joint International Conference on Electronic Voting (E-Vote-ID 2019). TalTech Press, Tallinn, Estonia, pp. 187–202, 2019.
- [Zo21] Zollinger, Marie-Laure; Estaji, Ehsan; Ryan, Peter Y. A.; Marky, Karola: “Just for the Sake of Transparency”: Exploring Voter Mental Models of Verifiability. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel; Germann, Micha, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 155–170. Springer International Publishing, Cham, 2021.

Pitfalls at the Starting Line: Moldova's IVS Pilot

Radu Antonio Serrano Iova¹

Abstract: The Republic of Moldova has been interested in internet voting since 2008. However, it is only now that preparations are currently ongoing to pilot an internet voting system (IVS) for its future use in elections. In this short paper, we explore the current endeavors to set it up, through the perspective of the Mirabilis of IVS failure, in order to identify current pitfalls that are affecting the process, and that could still be addressed in time.

Keywords: Moldova; Internet Voting; Convenience Voting

1 Introduction

The Republic of Moldova has been interested in automating elections since 2008, when a corresponding law was passed. However, the interest on this endeavor fluctuated throughout the years. It was only recently that the concrete actions have been actively undertaken to move forwards with the piloting of an internet voting system (IVS). This short paper presents Moldova's efforts and explores them through the Mirabilis of IVS failure. While Moldova's Internet Voting Project cannot yet be categorized as either success or failure, the Mirabilis is solely used as a tool to identify current pitfalls that are affecting the process and that could still be addressed in time.

2 The Republic of Moldova and i-Voting

The Republic of Moldova is a landlocked country bounded by Ukraine and Romania. It has a population of 2,6 million inhabitants [Mol23] and has a diaspora between 1,11 and 1,25 million people (according to 2021 data) [Mak21]. Primarily because of this last number, the applicability of distance voting was researched in 2007. Back then, the diaspora was smaller (comparatively to the 2021 data) but still accounted for 1/3 of the country's population. The study presented the possibility of voting by traditional mail, via the Internet, and via SMS or PDA. However, in addition to the lack of legal framework in all three cases, technological, organizational and societal constraints affected the two electronic methods [CG07]. In May 2008, the Parliament of Moldova passed Law 101

¹ Tallinn University of Technology, Ragnar Nurkse Department of Innovation and Governance, Akadeemia tee 3, 12618 Tallinn, Estonia raduantonio.serranoiova@taltech.ee

which adopted the concept of the Automated State Information System 'Elections' and mandated the Central Electoral Commission (CEC) to develop, regulate and implement it, and the Government to finance it, assist the CEC and develop and implement the corresponding legislative frameworks [Mol08]. The system was conceived for the purposes of automating the processes of preparing, conducting and totalizing the results of elections and referendums, with the first focus being the numbering of the votes until the corresponding legal, technical and organizational frameworks were developed and put into place for the rest of the responsibilities[Mol08; VG18]. Since then, many technical building blocks for internet voting were legislated, developed and implemented (due to so many of them being also relevant to the digitalization endeavors of the country, e.g. digital registries, digital identity, identification and signatures, data protection, e-ID cards, e-Government solutions, etc.) [VG18]. However, they still need to be interconnected for an election, and the IVS is also missing. That's where Moldova's Internet Voting Project comes in. In 2019, the CEC's strategic 4-year plan included concrete steps to develop an IVS. In December 2021 a first Interinstitutional Working Group (between govern-mental entities, like the CEC, the Ministry of Justice, the Public Services Agency, among others, and Civil Society Organizations) was created to develop the IVS Con-cept (I-1, I-2). This document includes the description and implementation method of the IVS in the electoral process, defines its basic notions and describes the basic principles that the IVS must follow. It also contains, as an Annex, proposed amendments to the electoral code [Com22]. With the approval of this concept, the CEC was allocated funds by the Parliament by October 2022. A second Interinstitutional Working Group (similar in composition to the first one, except for the Ministry of Justice) was created to oversee the implementation of the IVS, which includes drafting the specifications, contracting the corresponding company that will create the system, and piloting the IVS (I-1). The specifications were unveiled for public consultation in March of 2023. As of the writing of this short paper, the final specifications have not been published, and no progress appears to have been made in the search for the corresponding vendor to create and pilot the IVS.

3 Methodology

Data collection for this short paper took place between January and May 2023. During this period, multiple visits were conducted to Chisinau. Most of the interviews were conducted during these visits, with some in another country, to reach out to Moldova's voting diaspora. A total of 5 semi-structured interviews were carried out with the CEC, representatives of Civil Society Organizations (CSOs), a member of the Moldovan diplomatic corps and a citizen living outside of Moldova (see Table 1). The CSOs interviewed were the ones actively participating in the Interinstitutional Working Groups. The author also attended online two internet voting awareness events that the authorities of Moldova held for their citizens in February and March 2023.

The data was analyzed using an inductive approach consisting of identifying the core components of the Mirabilis of IVS failure (e.g. stakeholders, IVS, project organization,

Number	Occupation	Date
I-1	Deputy Head of the CEC	February 2023
I-2	Representative I of CSO	March 2023
I-3	Representative II of CSO	March 2023
I-4	Moldovan Ambassador	March 2023
I-5	Citizen outside the country	March 2023

Tab. 1: List of interviewees, anonymized.

context dimensions) and the relationships between them. The Mirabilis of IVS failure was introduced to analyze the failed implementation of Internet Voting Project of the Åland Islands [Da20]. Moldova's Internet Voting Project is still in development and cannot be categorized as a success or failure, yet. The Mirabilis is used as a tool to identify the current pitfalls that are affecting the process and that could still be addressed in time for the successful implementation of internet voting in Moldova.

4 Analysis

The CEC's vision is the adaptation of the Estonian model, i.e. IVS implementation for the whole country (I-1). However, the benefit will be felt primarily by the diaspora (I-1, I-2, I-3, I-4, I-5). The pilot IVS will not have any legal validity, will be conducted outside any electoral cycle and will only be available for those having a valid digital ID and/or signature (I-1). Applying the Mirabilis, the context seems contain multiple pitfalls for IVS implementation. The technological dimension is severely lacking in regard to the national adoption of a digital national ID card and signature. Seven percent of the population is able to identify themselves digitally (I-1), but the cost-benefit does not make it attractive to the population [VG18]. Regarding the law dimension, the electoral code does not contain articles on internet voting. A draft of the changes was attached to the IVS Concept, and it is planned to amend it by the time the pilot of the IVS (I-2), but due to the characteristics of the pilot, this step seems like a recommendation and not a necessity. The political dimension is lacking an official attitude toward internet voting. On one hand, the Parliament allocated the budget for the development of the IVS pilot, but on the other, members of the Parliament ignore invitations to workshops and discussions on the topic (I-1, I-2, I-3). On the societal dimension, the level of citizens' trust has not been effectively measured, and it is being put to the test by the war next door (I-4) and the Transnistria breakaway region. Regarding the elephant in the room/Mirabilis, the IVS has not yet been developed. After the completion of the final specifications, a public international bid will be launched to find and select the IVS supplier. The project organization is effectively being managed by the CEC and the Interinstitutional Working Group (I-1, I-2, I-3). The two member CSOs are actively participating in the implementation of the IVS. However, the rest of the stakeholders do not seem to be interested in the process. People only seem interested in elections when one is

approaching (I-3, I-4). Nevertheless, the CSOs and the CEC have been actively trying to inform the citizens, via media campaigns and their two public events (I-1, I-2, I-3).

5 Discussion and Conclusion

The context of this whole endeavor is incomplete. All the dimensions are lacking key items that are necessary for the successful implementation of an IVS. If these are ignored, possibly due to this being a pilot IVS and not the real deal, the failure of the pilot would set back or even annihilate any possibility of future IVS implementation in the country. The lacking context also deforms the demands of the stakeholders and might undermine their trust in the electoral process, the IVS and the government. The implementation environment of the IVS pilot seems to be indifferent, with the exception of the people working on it. Politicians, candidates, the media and observers are not willing to be troubled or to be engaged long enough on the topic. Additionally, the requirements for the IVS are primarily coming from the project organization, not from the stakeholders. This might lead to a mismatch between the expectations of the IVS among the stakeholders and the project organization, culminating in a system that does not satisfy the needs of the stakeholders. As it currently stands, there are failures appearing in-between the context and the stakeholders, and them and the project organization. The pitfalls identified should be resolved in a timely manner, since they might lead to the failure of the pilot, and in the long-term, to that of any IVS implementation. Further monitoring of the pilot and future efforts is warranted, to see if Moldova will be able to implement an IVS.

Acknowledgements

The data was collected as part of the MOLDOVA CYBERSECURITY RAPID ASSISTANCE project funded by the European Union and implemented by the e-Governance Academy.

References

- [CG07] Ion Cosuleanu and Constantin Gaiandric. “Distance voting (e-voting): the ways of its applicability in Moldova”. In: *Computer Science Journal of Moldova* 15.3(45) (2007), pp. 354–380.
- [Mol08] Parliament of Moldova. *Law 101/2008 Regarding the Concept of the Automated State Information System Elections*. 2008.
- [VG18] Ina Vîrtosu and Ion Guceac. “Democracy at the one-click distance: Is electronic voting the best option for Moldova?”. In: *CEE e|Dem and e|Gov Days 2018*. Facultas Verlags- und Buchhandels AG, 2018, pp. 359–372.

- [Da20] David Duenas-Cid and al. "Tripped at the Finishing Line: The Åland Islands Internet Voting Project". In: *Electronic Voting. Fifth International Joint Conference, EVote-ID 2020*. Springer International Publishing, Cham, 2020, pp. 33–49.
- [Mak21] Kanat Makhanov. *Emigrant Moldova and the Changing Concept of Migration*. In: Eurasian Research Institute website. Last accessed 2023/05/10. 2021.
- [Com22] Central Electoral Commission. *Decision 572/2022 Regarding the Concept of the Internet Voting System "e-Votare"*. 2022.
- [Mol23] Statistica Moldovei. *Populația*. In: Statistica Moldovei website. Last accessed 2023/05/10. 2023.

Trust Frameworks in Application to Technology in Elections: selected case studies

David Duenas-Cid,¹ Leontine Loeber,² Beata Martin-Rozumiłowicz,³ Ryan Macias⁴

Abstract: The prevalence of technology in elections has increased in recent decades, both in terms of voting systems as well as ancillary ones. At the same time, the issue of public confidence and trust has come to the fore as certain threat actors have sought to undermine electoral integrity through publicized attacks and disinformation campaigns against such technology. This paper examines the nexus between this public trust and the implementation of technology through an electoral cycle approach. It also presents a number of case studies at various points of democratic development and election management body type to examine how various trust variables impact implementation to either increase trust or distrust. This is done to better understand the directionality of these criteria through a methodologically driven approach, based on a uniquely developed trust model. It is hoped that this study will help experts to better understand how these variables impact the critical trust that underpins robust democratic institutions.

Keywords: Trust, Distrust, Election Technologies

1 Introduction

Trust in elections and the outcome of elections is being actively undermined in many countries in the world. Looking at the current trust deficit, the political aims this is being put to it is imperative that such issues need to be addressed explicitly if voter confidence is to be maintained. This is especially relevant in the field of technology in elections where undermining trust is becoming a global phenomenon and likely to spread to various election tech areas (voter reg., RMS, etc.). This makes it important to understand what factors lead to trust and which factors contribute to distrust. This paper approaches those factors combining academic literature and real case-based knowledge.

We also want to highlight the difference between trust in a system and the trustworthiness of the system. This distinction remains underexplored in the specific literature, and this paper aims to show its importance for the cases presented. In some instances, high-trust levels were posited in untrustworthy systems and, in others, the reverse can be seen. Trust and distrust can manifest in different forms during different stages of the electoral cycle. The erstwhile focus on the election day phase of casting, counting and tabulation of the

1 Kozminski University, Pub-Tech Research Center, 57/59 Jagiellońska, 03-301 Warszawa, Poland and University of New South Wales, School of Information Systems and Technology Management, NSW 2052, Sydney, Australia david.duenas.cid@pg.edu.pl

2 University of East Anglia, Research Park, Norwich NR4 7TJ, United Kingdom

3 Independent expert consultant

4 RSM Election Solutions, 1717 N Street NW STE 1, Washington, United States

votes is a too narrow approach; for example, the spread of misinformation during boundary delimitation, voter registration, or the campaign phase can also lead to trust or distrust. Another important phase is post-electoral disputes and the judicial processes with regard to election complaints. Although this is meant to create trust, long procedures with difficult rulings, lack of technical knowledge on the part of justices, and focused disinformation campaigns can also easily lead to mistrust. Again, the paper aims to contribute to the existing knowledge by applying the theory about these stages on real cases.

2 Theoretical Framework and Methodology

In order to develop a comprehensive theoretical framework for the comprehension of trust and distrust in electoral technology, it is of utmost importance to identify its potential sources including aspects related to the technology itself but, also, to the organizational and societal environment surrounding the elections and their organization. Election technologies are inserted in a complex socio-technical environment with a significant number of stakeholders that can, potentially, influence the perception that citizens have of the system. The list includes elements and stakeholders related to the technology but also the institutional framework, with the rest of the citizens and even with geopolitical relations [Du22].

But the adequate approach to those elements needs to be accompanied with a theoretical framework depicting how the process of creation of trust and distrust can be understood. For that, three main elements are to be considered.

First of all, trust and distrust should be understood as related but different theoretical constructs to be assessed and evaluated independently of one another. It has been stated that trust and distrust provoke different reactions [TH00]; the absence of trust affects the willingness to take risks and increases the demand for protection [TK96], while distrust creates anxiety and insecurity [Go92]. To embed this distinction between trust and distrust into the research on electoral technology, we can refer to the existing work in other social contexts [LMB98; Lu17; Lu79; MRW12; Ro98; TL06] approaching both constructs as independent variables. Assuming this distinction opens the door to their coexistence in parallel and towards the same target [OLS97; PP96]. That can contribute to enlarging the existing scope in the research on electoral innovations, where approaching what makes citizens trust has been notably predominant in front of what they lead them to distrust. Also, this approach allows understanding citizens' trusting / distrusting decisions as complex processes where several inputs are considered, and positions are mutable depending on the moment and the situation. Also allows understanding that similar inputs might have different impacts on citizens.

Secondly, trust and trustworthiness should also be understood as different constructs. The latter has been defined as an antecedent to trust [To20], as an aspect that affects a trusting relation by referring to a property of the trustee. Trustworthiness, then, plays an important role in the creation of trust, but the relation between them is not necessary causal since trust

is influenced by several other factor. In the case of electoral management, and given the relevance of the topic, the list of potential elements influencing trust creation is long and covers a wide range of actors [Wa06].

The different elements highlighted raise immediately a question of methodological nature: *how can we conduct a comprehensive analysis of the use of electoral technology and its impact on the different types of trust?* Prior electoral research has already described the different parts of the electoral cycle being more or less detailed (see Electoral Cycle section below) and even modelling parts of the electoral process [KDK21b]. In this research we opt for using the electoral cycle to detect and compare the touchpoints between technology and trust occurring in the different stages of the electoral process, and to compare them between different cases. Using this scope adds an interesting feature to the existing research: focusing on the moments that transcend what happens on the election day and vote casting process and widening the scope to other uses of technology used in the electoral process.

This paper uses an inductive approach to the question how the use of electoral technology impacts trust and distrust. To shed light on this research question, the paper uses the acquired in-depth knowledge from the cases to reflect on the relationship between election technology and trust. The dependent variable that the paper looks at is the perceived level of trust in the countries. The cases that are used are Poland, Kenya, the Netherlands and the United States. These cases were chosen based on their different structure of their Electoral Management Body (EMB) [Wa06]. Here, it has to be taken into account that the actual independence might change when ICT is introduced in elections, due to the technical knowledge, and thus often the reliance on vendors that is required when using ICT [Ja19]

Kenya has an independent EMB, the Netherlands and the U.S. have a governmental structure and Poland has an EMB that is comprised of the judiciary. Next to that, the trust level in the countries in question is quite different. Whereas trust in the Netherlands has always been high, the same can't be said for Poland and Kenya. In the US, trust in elections has declined since 2000. The cases also differ in the amount of experience that EMBs have had with the organization of elections. The Netherlands and the U.S. are usually considered to be old democracies, since they have held elections for over 100 years. Poland is a younger democracy, being part of the third wave of democratization. Kenya is a developing democracy, with less experience. Furthermore, the case of the U.S. adds another dimension to the study due to its singularity, complexity, and interest.

2.1 Electoral Cycle

The introduction of technology in elections has increased considerably in recent decades, both in terms of voting systems, but also ancillary ones. Many countries have looked at applying technology to improve efficiency and reduce the costs of aspects like voter registration and identification, and results management systems. Others have moved beyond voting machines

in controlled environments (e.g., polling station DREs), to piloting electronic voting in uncontrolled environments (e.g., internet voting) for certain categories of voter.

International support (either bilateral or organizational) for such initiatives, especially in developing democracies have supported this space financially and programmatically. Initial iterations focused primarily on provision of hardware and software for such systems. However, there is now a greater understanding within the international community that procedural, legal and feasibility elements should also be key elements of international assistance. There is also a growing awareness that technology introduction and increased trust do not necessarily go hand-in-hand.

That said, there is still a lack of a cohesive, coordinated methodology that starts with a needs-based approach. It is also apparent that any introduction of technology in elections needs to be buttressed through a more cohesive electoral cycle approach (see figure 1). This would place the introduction of electoral technologies as the locus of better electoral integrity, rather than as a potentially complicating problem in many recent cases of democratic backsliding. It also makes clear that electoral stakeholders need to be the drivers of ‘follow-up processes’ in between elections in order for reforms to have maximal impact. This should be the desired outcome, rather than the current *status quo* of approaching elections six months to one year out and not having the time, resources or knowledge to implement truly impactful change.

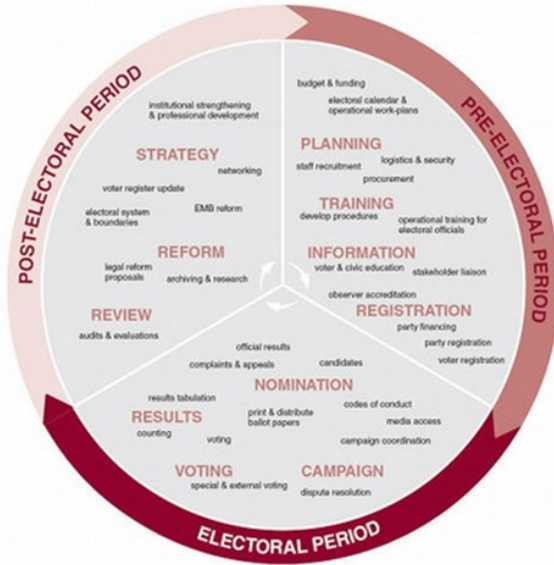


Abb. 1: The Electoral Cycle (developed by the European Commission, IDEA, and UNDP) [AC]

Various crises of public trust have also led to a better understanding that the introduction of technology in elections and increase in trust are not colinear processes. Rather, the

interaction between different trust variables at different stages of the electoral cycle needs to be better understood and documented. Without this fundamental understanding, it is possible that greater damage than good will result in building trust in democratic institutions. The cases studies are an addition to the existing literature by showing this interaction.

Very often, technology introduction is partially or wholly disconnected from this fundamental electoral cycle approach. Often, electoral stakeholders (be they government actors, political parties, or electoral commissions) have their own prioritization of programming that should be undertaken. Assistance providers are often driven by institutional impetuses, by aid agency priorities, and, to a certain level, by inertia in implementing activities done successfully in other countries, or at other time periods. Thus, very often, the disconnect happens by institutional ossification rather than by design. In contrast, the overarching approach should be of how technology can contribute to the democratic electoral process by increasing trust, rather than compromising it or reducing public trust. It is this question which forms the next part of our analysis.

3 Case Studies

For each of the cases, the paper will map out trust / distrust factors during the electoral cycle over a period of time that included decision-making, implementation, and post-electoral disputes. We will then look at causal variables that increase trust or distrust, specifically aspects related to voter trust or distrust in contrast to that of decision-makers. The relevant factors stem from the theoretical framework. The paper will rely on secondary data and research already published on the selected cases.

3.1 THE UNITED STATES OF AMERICA

In America, elections are conducted under the rules set forth by the respective legislature and certified by the Chief Election Official in each of the 50 States [BP21]. This means that the technology to conduct the elections also varies between states. The disperse structure can be both a security benefit, in that there is no single point of failure, but it can also lead to distrust in the process since voters are unfamiliar with the processes and technologies used in other jurisdictions across the country. Threat actors have exploited the disparate set of processes and technologies to call into question the election integrity amongst election jurisdictions.

It has been suggested that trust in American institutions, generally, is declining [St22b], amongst the reasons, the ongoing process since 2016 in which threat actors are attacking election technologies to try and decrease trust in democratic institutions. A Massachusetts Institute of Technology (MIT) report [MI21] states that the Bush v. Gore election of 2000 and the controversy around the recount introduced the term “voter confidence” into the

American elections. Following the 2000 election, the Help America Vote Act (HAVA) of 2002 [Se02] banned the use of pre-scored punch card voting technology and provided for the expansion of new voting technologies (NVT) across the country. The increased use of NVT in American elections has not gone without controversy. Many computer scientists and researchers exposed many of the security vulnerabilities that left opportunities for manipulation in election results via the NVT [Bo03; FHF06; Sc03]. This, along with many others, created opportunities for the American electorate, and potentially foreign adversaries, to spread theories that the NVT or the companies that developed the technologies had been manipulated or perpetuated fraud in the tabulation process.

While no manipulation of NVT software was or ever has been detected, over time the awareness of the vulnerabilities in the systems led to policy changes aiming to increase the security and resilience of both the NVT and the overall election process. As trust in NVT steadied, and at times increased, in 2016 the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) compromised the Illinois State Board of Elections (SBOE) computer network and was able to gain access and exfiltrate data of Illinois registered voters. Additionally, the GRU used spearphishing techniques to install malware on the network of an election technology company that develops software to manage voter lists [Mu16]. On January 6, 2017, the federal government designated elections as critical infrastructure. The designation allowed for election infrastructure to become more secure and resilient.

Trust in American election technology prior to 2016 had focused on NVT or more specifically the technology used to tabulate the votes. The GRU targeting electronic voter registration and verification systems (EVRVS) and companies developing software to maintain electronic voter lists, was used by threat actors to try to sow distrust in American elections by targeting all election technology, including ancillary ICT-election technology that is not used in determining the outcome of elections.

Leading into the 2020 election, a group of domestic threat actors used data obtained from election jurisdictions to purport that there had been manipulation, fraud, or other election integrity concerns through the exploitation of vulnerabilities in election technologies and the companies that develop those election technologies [Br21]. Additionally, according to the U.S. DOJ, Iranian nationals attempted to compromise, approximately 11 state voter websites, including state voter registration websites and state voter information websites, including gaining access to information on some voters in a state [De21] and that they gained access to a results management system (RMS).

As previously discussed ever since the designation of critical infrastructure American elections tried to become more resilient. There was an increase in the use of hand-marked paper ballots, and in the number of tabulation or outcome-based audits being conducted. As jurisdictions transitioned back to hand-marked paper ballots, especially postal voted ballots, there has been a need to adjudicate more ballots to determine the intent of the voter. Each of these situations has created complexities for the EMBs, so the NVT companies

have developed software aiming to make the process more efficient, secure, and transparent. But threat actors took the opportunity to exploit this new functionality stating that the NVT software allowed an EMB to change votes and manipulate the results. These changes are completely legal, appropriate, and required by law or policy. Further, EMBs have always been allowed, and required, to make such changes through a manual or ‘remake’ process. However, the automatization of the process and its integration into the NVT software as used as a means to decrease trust in the NVT. Specifically, the use of a Dominion Voting System application, Adjudication, was at the forefront of this attack and was exploited by threat actors. The claim that Dominion changed votes through the Adjudication software was amplified by many media outlets. That was one of the claims ultimately led to multiple defamation lawsuits by Dominion against media outlets and television personalities. One of those lawsuits was the Fox News defamation case where Fox News paid Dominion the unprecedented amount of \$787.5 million to settle the case [Ra20].

As a result, after the 2020 election some voters were convinced that the NVT had been manipulated and wanted answers. In a small number of jurisdictions, the courts, legislatures, government officials, or members of the public legally forced or threatened EMBs into having the NVT software copied or reviewed. Many, if not all, of those instances have resulted in unauthorized entities, including potentially threat actors, gaining access to the NVT software and data which has been and may still be used to sow discord and reduce trust in American elections [Bi21; Co23; Gr22b; St22a; WA21]. The repercussion of these reviews has been seen in two local EMBs where they have regressed from electronic tabulation to conducting a full hand count tally of all results [Pa22a; Pi23]; experts agree that a full hand count tally in American elections is a less secure and less accurate method of tabulating votes [Pa22a]. Other people have attempted to have a court force a local EMB to get rid of their NVT and conduct hand counts in future elections; each of these cases has been unsuccessful to date [Gr22a; Le22; Me22; PK22; US22].

Continuing on after the 2022 election and as recent as the past few months, threat actors continue to sow discord by building distrust in ancillary ICT-election technologies. The attacks on NVT, and other ICT-election technologies, such as EVRVS, electronic voter lists, RMS, etc., have not subsided. Recently, the attacks have expanded to systems adjacent to elections (i.e., not used in the conduct of the election process). Threat actors have publicly attacked systems as innocuous as intrusion detection systems [Pa22b], ballot printing technology [SE22], and systems that are used to clean voter registration databases in order to prevent voter fraud [CC23].

With attacks against election technology continuing and expanding into new technologies, it is assumed that the trust in election technologies would further decrease. The MIT Trust in Elections study [MI21], however, actually found the opposite. As it pertains to voter confidence in election technology specifically, the study states “Americans were more confident in the electoral machinery following the 2020 election than they were in 2016. The difference is they were more polarized. . .” Further, in two of the incidents mentioned, the voters have decided to recall the election officials who were trying to sow distrust in the

NVT; one has resulted in a successful recall of the election official the other is currently awaiting a recall election. In both these incidents voters said they trusted the NVT and elections processes in their jurisdiction and wanted to oust the elected officials who were trying to distrust the democratic institution. While the study and recalls show there is more confidence in the election machinery, the increased polarization is creating chaos and sowing discord in American and democratic institutions.

3.2 THE NETHERLANDS

The case of the Netherlands is an interesting one because this is a country which went from elections with a high amount of technology back to paper ballots, even though public trust in the technology was not an issue. However, the use of software to tabulate and determine the results has now become a topic of discussion, due to experts calling the security of that software into question. Overall, even though trust in the electoral process is still high, certain parties are using the rhetoric of possible election fraud, which could undermine this public trust.

The Netherlands introduced voting computers (DRE's) in the early 1960's and continued to use these until 2006. At that time, almost 95% of the voters cast their vote using technology. The Netherlands also experimented with internet voting for voters living abroad, using it in binding parliamentary elections in 2004 and 2006. In 2006 however, an NGO called we don't trust voting computers successfully challenged the certification of the voting computers, claiming that they were not meeting the standards of transparency, verifiability and voter secrecy. The main problem that the action group had with the machines in use was the fact that they were lacking a paper trail, making it impossible to check if the outcome of the election was indeed what the voters wanted. The issues this group raised eventually let to the withdrawal of the certification of the voting computers and a return to voting with paper ballots [Lo14; Lo16]. In 2008, internet voting was considered for nationwide elections for the waterboards, a form of decentralized governments. Because of the discussion on the voting computers, a more substantial technical analysis of the intended system was performed, showing several weaknesses. This led to the decision not to use the internet voting system anymore.

During the 2017 Dutch Parliamentary Election Study, voters were asked two questions with regard to the use of technology in the process of casting a vote in elections. First people were asked which voting method they would prefer. It turned out that a small majority at that time stated that they preferred to use paper ballots, in contrast with 2006 and 2010 [Lo11]. Next, people were asked which voting method they would consider the most reliable. Almost 2/3 of the respondents felt that voting by paper ballot is the most reliable voting method. Curiously, this means, compared to the results mentioned above about the preferred method, that even though people do not feel that voting by voting computer is the most reliable, some of them would still prefer this. This difference in appreciation between preferred and most reliable method is even greater when it comes to internet voting; 18.1% of the respondents

prefer this method, whereas only 6.2% feel this is the most trusted method. In these cases, convenience of the voting method seems to prevail over the question of trust [Lo18].

Another area in the electoral cycle where technology is used in the Netherlands is for the tabulation and calculation of the votes. Software for this purpose, called OSV, was developed in 2008 by the Electoral Council and first used during the elections for the European Parliament in 2009. During the election process, nearly all political parties and municipalities use the software, although this is not legally mandatory. The software is used in different phases of the electoral cycle, both in the nomination phase and in the tabulation phase. Political parties that want to run in the elections can use the software to register their candidates. Furthermore, the software is used for the vote tabulation and seat distribution. For this part of the process, it should be noted that OSV is not used in the polling stations themselves. Votes are cast on paper and are still counted manually. The results are then manually entered into the software to determine the results on the municipal level. This process is repeated at the district level by the principal electoral committees and eventually by the Electoral Council. At various moments during the process, results are printed on paper, are brought to the next level in person and manually re-entered into the system. Up until the 2017 election it was also standard procedure that a digital file of the results was transferred together with the paper print by using usb-sticks. Due to questions concerning the safety of that procedure, this was abandoned [CY18].

Just before the 2017 parliamentary elections, a news report stated that the software was not safe, that it could be hacked in a way that would make it possible to change the outcome of the results. In order to ensure the integrity of the final results, the Electoral Council has introduced two new checks, where random samples from the polling stations are compared to the results from the software, looking at the total number of votes, but also at the seat distribution for parties and candidates. This was first done during the municipal elections of 2022 and resulted in the finding that there had been no issues with the software [Ho22].

So, what has all this done with the trust in elections in the Netherlands? Compared to other countries, trust has always been high and this continued. During the 2021 elections, 79% of the voters that were involved in the Dutch Parliamentary Election Study stated that they felt that the elections were fair. Almost 10% found them not fair. Although this number is, as stated, low compared to other countries, it is almost twice as high as in 2017, when only 5% of Dutch voters stated that they lacked trust in the outcome of the elections. Voters that did not trust the outcome mentioned different reasons for their lack of trust. During these elections, mail voting was used on a bigger scale than in previous elections, due to Covid-19. Some people felt that this wasn't safe. Also, voters mentioned the counting process as a reason not to trust the outcome. Interestingly, some of these latter voters pointed towards the (perceived) problems in the United States with the counting as a reason not to trust this part of the process in the Dutch elections [SLM21].

The case of the Netherlands has some important aspects for questions on trust in technology used in elections. First, the fact that technology has been used on a large scale and for a

long time doesn't mean that the issue of the trustworthiness of the technology will not surface. Therefore, it is important to ensure that the EMBs using the technology are aware of (technological) developments that can lead to questions of trustworthiness. The second thing that should be considered is that voters can trust technology, even when it is not trustworthy. The final point is that trust will often depend on what is stated in the media about the technology. Even though the counting of the ballots is still done by hand in the Netherlands, based on some news reports, many voters thought that this was done by possible malfunctioning software. Also, media reports on similar events in other countries can play a role, as shown by the fact that some Dutch voters had less trust in Dutch elections, due to the events in the 2020 U.S. elections.

3.3 POLAND

Although Poland never used or considered any form of electronic or internet voting, it is possible to extract from events occurred in the recent years in the management of Polish elections that are relevant for the understanding of trust-related aspects and election reform and technology adoption in other parts of the electoral cycle beyond the election day, and in other moments besides the moment of casting the vote. In this description, we will pay attention to the failure of the IT systems in 2014 Elections and the failure in the introduction of all-postal elections in 2020.

Poland hosts four types of elections (Sejm/Parliament, Presidential (two-round), Local and European), featured by a low turnout (in average). This low average turnout [MK20] (Sejm - 49,50; Presidential - 58,15; Local - 45,14; European Parliament - 28,73 – average values) triggered the introduction of postal and proxy voting in Poland in 2011 [St20], raising questions about election fraud and vote buying. It was argued that postal voting may pose a risk of vote declassification that would lead to fraudulent elections [Mu20]. The election code proposed in 2011 allowed significant vote-value disparities, conflicting with the Polish constitution requirement of voters equality [PS17]. Some of these concerns came back to the public debate on the occasion of the failed implementation of all-postal elections in 2020 to overcome the problems derived from Covid [KDK21a]. A combination of legal, managerial and trust-related issues [MK21] forced to cancel and postpone the elections, adopting a different format combining paper and postal elections. Trust, in this context, was related to the managerial capacity of the electoral management bodies and the Polish postal service to provide the service requested within the correct time and cost frames [Ko22; Zb13].

The second example shedding light on the functioning of Polish elections relates to the problems occurred in the Local Elections of 2014, when the electoral results were communicated late, due to a problem in the IT systems. Once presented, the results diverged substantially from the exit polls, provoking an important controversy in the country regarding the acceptance of the results. Two factors also strengthened the discussion: the exit polls were very accurate in the previous years, and the number of invalid votes was significantly higher on this election [Ś15].

A report by Fundacja Batorego [F115] describes how the problem in the IT system for calculating the results escalated and end up with the resignation of the members of the National Electoral Commission, demonstrations, media exposition and political tension. The same report highlights the causes of the crisis including the IT system, but also a number of organizational (including the lack of a contingency plan, the lack of auditing or the poor time management of the tender) and systemic reasons (including the lack of reflection about the election process, the lack of renovation of the National Electoral Office or the lack of interaction between the Electoral Office and external experts). Technology, hence, appears as the trigger of distrust, but a number of other elements that could have served as firewalls to prevent distrust expansion were not in place or correctly managed, allowing the escalation of the problems, and risking the overall elections.

3.4 KENYA

The case of Kenya here is educative in terms of public trust and the introduction of technology in elections. This case study takes a deep dive into the introduction of technology in elections in Kenya and the key role of trust / distrust in this process. The case of Kenya is particularly telling since it has included technology in some parts of the electoral process since the recommendations of the Kriegler report following the 2007 post-election violence. The introduction of technology in elections, however, has also become a focus for polarization, within society and across the political class.

On the surface, one would expect that the introduction of technology in elections would improve public trust in the election process and to reduce polarization. Yet, in the Kenyan case, the opposite proved true. In the previous 2017 general elections, the losing Orange Democratic Movement (ODM), led by Raila Odinga challenged the electoral results and his opponent, Uhuru Kenyatta (Jubilee Party), before the Supreme Court, claiming that various levels of institutional infractions meant that the elections should be overturned and re-run. Technology played a key role in this call for annulment.

The landmark 2017 Supreme Court decision that overturned the results and called for new elections was very much part of this trust/distrust calculus. Technology and its inconsistencies were identified as one of the fields where there was so much lack of clarity that the court felt it was impossible for them to establish the results. Certain recommendations were made to improve the process prior to the 2022 general elections, yet many of these things did not take place and implementation was rushed.

Why was this? In the first place, the Kenyatta government that emanated from the 2017 re-held elections had declined international involvement and assistance for a variety of reasons; some historical, some personal, some ideological. Although this was essentially a government decision, it should have been made in a more open and transparent process. To the author's knowledge, this didn't take place and elite decision-making played a pre-eminent role. This also led to a lack of strategic focus on the part of Kenya's Independent Electoral

and Boundaries Commission (IEBC) in planning for the 2022 elections until a change of heart in 2021 allowed international assistance providers to design and implement programs that finally resulted in an IEBC strategic plan being adopted. That said, this was much delayed and many of the deadlines were compressed to what a proper electoral cycle approach would entail. Thus, the ‘management’ variable was also lacking at this crucial stage, contributing to distrust.

Within the technology sector and given the past debacle, a decision had been made to transition to a new technology provider to design and supply the Kenya Integrated Election Management System (KIEMS) system for these elections. This would normally entail extensive and inclusive consultations on specification, tender and procurement of the technology with proper societal oversight. What ended up taking place was perfunctory at best, with limited time for review and limited input from key electoral stakeholders. Again, the ‘technical trustworthiness’ variable was undermined as a result, again increasing distrust.

There was also the issue of limited capacity. Although electoral stakeholders had developed their technology capacity since the introduction of the Biometric Voter Registration System (BVR) in 2013, technical expertise was also quite limited in the time frames allocation. Thus, there was only a basic level discussion of what needs are expected from the systems and a dovetailing of the specifications that would lead to the tender on this inclusive basis. This contributed to the distrust in the ‘technical trustworthiness’ of the system prior to the 2022 elections.

Then, in the procurement, there were anomalies in the process and potentially more questions could have been asked by electoral stakeholders. As the 2022 EU EOM final report found, “the IEBC did not publish the evaluation either for this [KIEMS] or the additional election technology related public procurement processes, undermining transparency, and leaving room for speculation.” [Un22] Again, the ‘transparency’ variable was key here.

Throughout the implementation process, information to electoral stakeholders was rather limited. Some public testing was held with political party involvement, but independent mandatory audits of the system that had been put in place resulted in only limited information about its findings, recommendations, and subsequent changes made. Importantly:

“While party agents and stakeholders were given the opportunity to observe the assembling of the KIEMS kits and the IEBC published information on the security and contingency measures implemented in the KIEMS kits, no equivalent information was provided on the KIEMS backend applications used by the Constituency Returning Officers (CRO) and the National Returning Officers (NRO) nor on the hosting infrastructure, limiting stakeholders’ capacity to assess the election technology.”[Ke22]

So, in many ways, proper transparency and accountability of this important part of the electoral process fell short of what international standards would demand. At the same time, stakeholders did little to demand the level of transparency and accountability that should be required. The issue then became a central bone of contention in the formal and

information challenges to the electoral results at various levels and the lack of involvement also potentially sparked a greater level of disinformation of developments in this area, likely due to a sense of disconnection and impotence to do anything at the late stage.

Lastly was the roll of vendors in this process. While many EMBs choose to outsource the implementation of technology in their elections to outside vendors, many also try to abrogate ultimate responsibility to them for any gaps or system failure. Unfortunately, according to latest international standards, this is not a valid approach and EMBs should be considered ultimately responsible for any implementation of technology in elections.[Eu17]

One element that did serve to increase trust in the elections was the establishment of an online web portal where the polling station level results protocols (Forms 34A) could be uploaded for public scrutiny. Although the development of this portal was much delayed and untransparent, its appearance just prior to the election meant that on election day and after, stakeholders could check individual results remotely, which serve to raise public trust to some extent.

Throughout such technological application in elections, electoral stakeholders should have been better informed, better equipped to input and critique systems at a technical level, and better empowered to hold state institutions to account for their specification, procurement and implementation. In the case of Kenya, more targeted and incisive oversight could have led to greater transparency and accountability and, ultimately, to less polarization and disinformation in an already high-stakes environment.

From the analysis, we can conclude that the key variables of ‘technical trustworthiness’, ‘management of the electoral process’, but especially the lack of openness and ‘transparency’ meant that key moments in the electoral cycle in which public trust could be built were missed. Instead, the variables came together to decrease, rather than increase trust in the electoral process, although the element of the web portal operated in the opposite direction.

4 Findings and Conclusion

This paper seeks to analyse the concept of trust in technology in elections. It examines trust and distrust as two concurrent and collinear processes and develops a methodological framework of key variables that may impact on trust and distrust. It examines these variables through an election cycle approach and across four cases studies of countries that vary by election management body (EMB) model and by level of democratisation. Through a deep dive into the specific conditions surrounding technology in elections in Kenya, the Netherlands, Poland and the U.S., it aims to show which of the variables were salient and at what stages of the electoral cycle.

Key findings that can be induced from the cases include that trust issues are not only important when new technology is introduced, but can also become a topic of controversy at a later date. We see this most clearly in the Netherlands and U.S. case studies, but also in

that of Kenya. We also find that trust and trustworthiness are not the same thing. Very often, technology systems can be designed to be trustworthy, yet still not enjoy trust. Conversely, as the early stages of the Netherlands and Kenya implementation show, there can also be trust without trustworthiness. In addition to that, the use of NVT along the electoral cycle adds new layers of complexity at different levels (e.g. technical, managerial or procedural) that, in consequence, may serve as trigger for distrust related narrations (see USA case).

Overall, the cases found that throughout technology introduction and application in elections, electoral stakeholders should have been better informed, better equipped to input and critique systems at a technical level, and better empowered to hold state institutions to account for their specification, procurement and implementation. Ultimately, such a more holistic approach could have led to less polarization and disinformation in an already polarised environments. From the analysis, we can also conclude that the key variables of ‘technical trustworthiness’, ‘management of the electoral process’, but especially the lack of openness and ‘transparency’ meant that key moments in the electoral cycle in which public trust could be built were missed in all four cases. Instead, the variables came together to decrease, rather than increase trust in the electoral process. Also, it is worth to note that the number of stakeholders linked to the active provision of trust and those potentially providing distrust is clearly unbalanced towards distrust providers. In some occasions (see the Polish and USA cases) even actors that should be interested in providing trust in the democratic systems (political parties) can actively introduce distrust in the system searching for short term spurious benefits and not necessarily being aware of the potential long-lasting impacts in the overall trust in the electoral system.

Further research should look at the finding from the cases that trust and distrust are long-term issues that warrant much more incisive examination. They exist not just around election day, but at all stages of the electoral cycle, which proves to be a useful model of examination.

5 Acknowledgements

The work of David Duenas-Cid has received funding from the Electrust (EU H2020 MSCA programme, grant agreement no. 101038055) and Dynamika (braku) zaufania w kreowaniu systemów głosowania internetowego (Narodowe Centrum Nauki, OPUS-20 competition, grant agreement no. 2020/39/B/HS5/01661) projects.

Literaturverzeichnis

- [AC] ACE Project - The Electoral Knowledge Network: Electoral Cycle, URL: <https://aceproject.org/electoral-advice/electoral-assistance/electoral-cycle>, Stand: 16.05.2023.
- [Bi21] Birkeland, B.: Investigators: Mesa County Clerk Allowed Unauthorized Person To Compromise Voting Equipment. CPR News, 2021.




- [Bo03] Boyle, A.: E-voting flaws risk ballot fraud. NBC News, 2003.
- [BP21] Bush, S.; Prather, L.: Healthy democracy requires trust – these 3 things could start to restore voters’ declining faith in US elections. The Conversation, 2021.
- [Br21] Brown, E.; Davis, A.; Swaine, J.; Dawsey, J.: The making of a myth. Washington Post, 2021.
- [CC23] Cassidy, C.; Carr Smyth, J.: State voter fraud system fractures as Republicans opt out. AP News, 2023.
- [Co23] Cohen, Z.: Text messages reveal Trump operatives considered using breached voting data to decertify Georgia’s Senate runoff in 2021. CNN, 2023.
- [CY18] Castenmiller, P.; Young, P.: Elections and IT; the challenge of making it work in a changed world. In (Krimmer, R.; Volkamer, M.; Cortier, V., Hrsg.): Third International Joint Conference on Electronic Voting E-Vote-ID 2018. Taltech Press, Bregenz, S. 170–179, 2018.
- [De21] Department of Justice O of PA: Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election. Washington, 2021.
- [Du22] Duenas-Cid, D.: A theoretical framework for understanding trust and distrust in internet voting. In (Krimmer, R.; Volkamer, M.; Duenas-Cid, D. e. a., Hrsg.): E-Vote-ID 2022 Proceedings. University of Tartu Press, Tartu, S. 57–62, 2022.
- [Eu17] of Europe, C.: Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Council of Europe, 2017.
- [FHF06] Feldman, A.; Halderman, A.; Felten, E.: Security Analysis of the Diebold AccuVote-TS Voting Machine. Princeton, 2006.
- [Fl15] Flis, J.; Frydrych, A.; Gendźwiłł, A.; et al: Co się stało 16 listopada? Wybory samorządowe 2014. Batorego Foundation, Warszawa, 2015.
- [Go92] Govier, T.: Distrust as a practical problem. J Soc Philos 23, S. 52–63, 1992, doi: 10.1111/j.1467-9833.1992.tb00484.x.
- [Gr22a] Griswold, J.: Final agency order of dismissal. 2022.
- [Gr22b] Grossi, C.: Investigation into Third Party Access to Vote Tabulators. 2022.
- [Ho22] Hofmans, T.: Kiesraad vindt geen onregelmatigheden bij gebruik van OSV-verkiezingssoftware. Tweakers, 2022.
- [Ja19] James, T. S.; Garnett, H. A.; Loeber, L.; van Ham, C.: Electoral management and the organisational determinants of electoral integrity: Introduction. International Political Science Review 40, S. 295–312, 2019, doi: 10.1177/0192512119828206.
- [KDK21a] Krimmer, R.; Duenas-Cid, D.; Krivososova, I.: Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting — the good, the bad or the ugly. Public Money & Management, 2021.
- [KDK21b] Krimmer, R.; Duenas-Cid, D.; Krivososova, I.: New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper? Public Money and Management 41, S. 17–26, 2021, doi: 10.1080/09540962.2020.1732027.
- [Ke22] of Kenya, S. C.: Presidential Election Petition E005, E001, E002, E003, E004, E007 & E008 of 2022. Supreme Court of Kenya, 2022.
- [Ko22] Kobylski, P.: Powszechność w głosowaniu korespondencyjnym w dobie COVID-19. Wybrane zagadnienia. Studia z Polityki Publicznej, 2022.

- [Le22] Leavitt, J.: Cnty. of Fulton v. Sec'y of the Commonwealth. 2022.
- [LMB98] Lewicki, R.; McAllister, D.; Bies, R.: Trust and Distrust: New Relationships and Realities. *Academy of Management Review* 23, S. 438–458, 1998.
- [Lo11] Loeber, L.: Voter trust in the Netherlands between 2006 and 2010. In: *CeDEM11 Proceedings of the International Conference for E-Democracy and Open Government. International Conference for E-Democracy und Open Government*, S. 323–333, 2011.
- [Lo14] Loeber, L.: E-voting in the Netherlands; past, current, future? In (Krimmer, R.; Volkamer, M., Hrsg.): *Proceedings of the 6th international conference on electronic voting (EVOTE)*. TUT Press, Tallinn, S. 43–46, 2014.
- [Lo16] Loeber, L.: E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years. In: *3rd International Conference on Electronic Voting 2008. Gesellschaft für Informatik, Bregenz*, S. 21–30, 2016.
- [Lo18] Loeber, L.: The E-voting Readiness Index and the Netherlands. In (Krimmer, R.; Volkamer, M.; Cortier, V., Hrsg.): *Electronic Voting: Third International Joint Conference, E-Vote-ID 2018, Proceedings*. Springer, Bregenz, S. 146–159, 2018.
- [Lu17] Lumineau, F.: How Contracts Influence Trust and Distrust. *J Manage* 43, S. 1553–1577, 2017, doi: 10.1177/0149206314556656.
- [Lu79] Luhmann, N.: *Trust and Power*. Wiley-Blackwell, Chichester, 1979.
- [Me22] Merrill, B.: *Alabama Voting Machines Challenge*. 2022.
- [MI21] MIT Election Data and Science Lab: *Voter Confidence*, 2021, URL: <https://electionlab.mit.edu/>.
- [MK20] Musiał-Karg, M.; Kapsa, I.: *Alternatywne metody głosowania w opiniach Polaków. Postawy i poglądy względem wybranych form partycypacji w wyborach*. UAM-WNPiD, Poznań, 2020.
- [MK21] Musiał-Karg, M.; Kapsa, I.: *Debate: Voting challenges in a pandemic—Poland*. *Public Money & Management*, 2021.
- [MRW12] McEvily, B.; Radzevick, J.; Weber, R.: Whom do you distrust and how much does it cost? An experiment on the measurement of trust. *Games Econ Behav* 74, S. 285–298, 2012, doi: 10.1016/j.geb.2011.06.011.
- [Mu16] Mueller III, R.: *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Washington, 2016.
- [Mu20] Musiał-Karg, M.: *Głosowanie korespondencyjne podczas pandemii Covid-19. Doświadczenia z polskich wyborów prezydenckich w 2020 r. Przegląd Prawa Konstytucyjnego*, 2020.
- [OLS97] Otnes, C.; Lowrey, T. M.; Shrum, L. J.: Toward an Understanding of Consumer Ambivalence. *Journal of Consumer Research* 24, S. 80–93, 1997, doi: 10.1086/209495.
- [Pa22a] Parks, M.: *Hand-counting ballots may sound nice. It's actually less accurate and more expensive*. NPR, 2022.
- [Pa22b] Parks, M.: *Some Republicans in Washington state cast a wary eye on an election security device*. NPR, 2022.
- [Pi23] Pierce, A.: *Shasta County Supervisors Opt To Hand Count Vote. Details Remain Scarce*. ShastaScout, 2023.
- [PK22] Prentice, P.; Kirkwood, T.: *Verified Petition For Relief*. 2022.

- [PP96] Priester, J. R.; Petty, R. E.: The gradual threshold model of ambivalence: Relating the positive and negative bases of attitudes to subjective ambivalence. *J Pers Soc Psychol* 71, S. 431–449, 1996.
- [PS17] Pierzgalski, M.; Stępień, P.: A Peculiar Interpretation of the Constitutional Principle of “One Person, One Vote” in Poland: Voter (In)equality in the Elections to 1,200 Local Legislatures. *East European Politics and Societies*, 2017.
- [Ra20] Ramsland, R.: Antrip Michingan Forensic Report. 2020.
- [Ro98] Rousseau, D.; Sitkin, S.; Burt, R.; Camerer, C.: Not So Different After All: A Cross-Discipline View Of Trust. *Academy of Management Review* 23, S. 393–404, 1998.
- [Sc03] Schwartz, J.: Ohio study finds flaws in electronic voting. *NY Times*, 2003.
- [Se02] Senate and House of Representatives of the United States of America: Help America Vote Act of 2002. Senate und House of Representatives of the United States of America, Washington, 2002.
- [SE22] Snow, A.; Ellgren, N.: Voting snag in Arizona fuels election conspiracy theories. *AP News*, 2022.
- [Ś115] Śleszyński, P.: Hipotezy głosów nieważnych w wyborach powszechnych w Polsce po 1989 r. *Social Space Journal*, 2015.
- [SLM21] Sipma, T.; Lubbers, M.; van der Meer, T.: Versplinterde vertegenwoordiging: Nationaal kiezersonderzoek 2021. *SKON*, 2021.
- [St20] Stelmach, A.: Postal Voting. Poland and Solutions in Other Countries. *Przegląd Prawa Konstytucyjnego*, 2020.
- [St22a] Stern, G.: Nevada high court rejects plea to stop county’s hand-count. *AP News*, 2022.
- [St22b] Stewart, C.: Trust in Elections. *Daedalus* 151, S. 234–253, 2022, doi: 10.1162/daed_a_01953.
- [TH00] Tschannen-Moran, M.; Hoy, W.: A Multidisciplinary Analysis of the Nature, Meaning, and Measurement of Trust. *Rev Educ Res* 70, S. 547–593, 2000, doi: 10.3102/00346543070004547.
- [TK96] Tyler, T.; Kramer, R.: Whither Trust? In: *Trust in Organizations: Frontiers of Theory and Research*. SAGE Publications, Inc., Thousand Oaks California 91320 United States, S. 1–15, 1996.
- [TL06] Tomlinson, E.; Lewicki, R.: Managing Distrust in Intractable Conflict. *Conflict Resolution Quarterly* 24, S. 219–228, 2006, doi: 10.1002/crq.
- [To20] Tomlinson, E. C.; Schnackenberg, A. K.; Dawley, D.; Ash, S. R.: Re-visiting the trustworthiness–trust relationship: Exploring the differential predictors of cognition-and affect-based trust. *J Organ Behav* 41, S. 535–550, 2020, doi: 10.1002/job.2448.
- [Un22] Union, E.: European Union Election Observation Mission: Kenya 2022, Final Report, Techn. Ber., European Union, 2022.
- [US22] U.S. District Court in the District of Arizona: Lake v. Hobbs – Electronic Voting Machines (AZ). 2022.
- [Wa06] Wall, A.: Electoral Management Design: The International IDEA Handbook. International Institute for Democracy und Electoral Assistance (International IDEA), Stockholm, 2006.
- [WA21] WAKE Technology Services: Fulton County Pennsylvania - Election System Analysis. 2021.

- [Zb13] Zbieranek, J.: Alternatywne procedury głosowania w polskim prawie wyborczym. Gwarancja zasady powszechności wyborów czy mechanizm zwiększania frekwencji wyborczej? Difin, Warszawa, 2013.

Regulating for the “known unknowns” in Internet voting: quantum computing and long-term privacy

Adrià Rodríguez-Pérez¹ , Núria Costa¹ , Tamara Finogina¹ 

Abstract: Quantum computing is yet another example of the shift towards governance and policy-making amidst uncertain risks. We know it is coming and we anticipate that it will have a huge impact on today’s electronic communications: the underlying mathematical problems that allow us to securely send an email, shop online or transfer money are at stake. Voting online will no longer be secure either. In this paper we address a more fundamental concern: how the technological developments in quantum computing tomorrow may affect the fundamental rights of people voting online today. Internet voting is being progressively adopted in many electoral processes, including governmental ones. Countries like Canada, Estonia, France and Switzerland often use it. Their systems satisfy the legal requirements for democratic elections today, but they will no longer be secure once quantum computers are used to break the underlying mathematical problems behind public key cryptography. Our claim in this paper is that this is not only a problem for future regulations, but today’s secret ballots are already vulnerable to quantum cryptanalysis in the future (i.e., retrospective decryption). Despite governments and electoral administrations being aware of this risk, no specific measures are yet being adopted to mitigate it, as our analysis of the electoral regulations in the above-mentioned countries shows. Interestingly, there is already a set of alternatives that could be studied. In this paper we analyze several proposals that aim at providing long-term privacy in Internet voting, including secure data deletion, quantum-resistant cryptosystems, and anonymous voting. Whereas none of these alternatives is a silver bullet against quantum cryptanalysis, it is essential that their feasibility is studied so that technological developments do not harm citizen’s fundamental rights.

Keywords: Internet voting; quantum computing; long-term privacy.

1 Introduction

“Imagine a cat in a box. There are two possible states for the cat, namely dead or alive. [...] Traditionally we would say that the cat is either dead or alive, we just do not know which. However, quantum theory says that the cat is in a superposition of two states—it is both dead and alive, it satisfies all possibilities. Superposition occurs only when we lose sight of an object, and it is a way of describing an object during a period of ambiguity. When we eventually open the box, we can see whether the cat is alive or dead. The act of looking at the cat forces it to be in one particular state, and at that very moment the superposition disappears” [Si99]. The Schrödinger’s Cat experiment is frequently used to illustrate how quantum mechanics work and, more concretely, to give an intuition of the paradox of quantum superposition. Quantum computers are becoming more and more

¹ ScytI Election Technologies, S.L.U., Barcelona 08021, Spain

a reality and the potential impact they might have on society is clear: they could bring considerable benefits to many industries, such as finance or chemicals, but they also pose an inevitable threat to secure communications in which public-key cryptography plays a crucial role. The security of this type of cryptography is based on the hardness of solving certain computational problems, such as the discrete logarithm or the factorization. Unfortunately, none of these problems is hard to solve for a quantum computer, so any system using public-key algorithms is at risk. But is this a risk we must address now? Or, on the contrary, can we wait until large practical quantum computers are built? The answer is that it depends on what we are protecting. Internet voting systems provide voters with the chance to cast their votes from anywhere and require a high level of security to protect voters' secrecy and the integrity of final results. Asymmetric encryption, digital signatures and Zero-Knowledge proofs are some of the cryptographic primitives used by these systems in order to meet the security needs. Although all of these are considered robust nowadays, they won't survive the quantum age. Special attention should be given to encryption and the political and personal implications that revealing the contents of an encrypted vote could have in the future. Thus, when talking about privacy² in the long-term, it is clear that we should transition to quantum-safe alternatives; but do we know how? Is there any regulation which provides guidance on how to be protected against quantum computers? The goal of the paper is to address how to regulate future technological challenges to ensure that the principle of secret suffrage is respected in Internet voting both during an election and once it is over.

Risks and uncertainty are central problems in governance and regulation. Acknowledging that it is already considerably complex to provide solutions to existing problems, how should we respond to future risks and challenges? One option is to ban the exploitation of technologies whose consequences are unforeseeable. Nowadays, bans and moratoria are being claimed for facial-recognition technologies [Cr19], spyware [Un21] and, more recently, Artificial Intelligence [Vo23]. Nevertheless, it is also possible to think of restrictions in lieu of bans. Another approach is to protect the legal assets that these technologies could jeopardize. This is the approach that was adopted, for example, in 1979 with the Moon Agreement: although space technology was not widely available at the time, it was decided to preserve the moon as a common heritage of humankind [Ch80]. A similar and more general approach can be found in International Climate Change Law, the so-called precautionary principle. Based on this principle, regulation “does not require ‘full scientific certainty’ where there are ‘threats to serious or irreversible damage’, and its lower evidentiary threshold could strengthen the protective potential of international environmental law” [BBR17]. Nowadays, the neurorights movement [GHY22] is based on similar foundations. All in all, and rephrasing Ulrich Beck [Le95], we have moved from a risk society to a society of uncertain risks, where governance and policymaking need to be revisited to cope with

² Throughout the paper, we will adhere to the most common terminology of “long-term privacy” to refer to compliance with the principle of secret suffrage after the end of an election. However, “long-term secrecy”, which encompasses both privacy –or confidentiality– and anonymity as standards under this principle, would be more accurate. For a more detailed discussion about the principle of secret suffrage in remote electronic voting see section 2.2 below.

potential futures. The goal of this paper is, therefore, to provide guidance on how to regulate e-enabled elections in the face of uncertainty.

The case of quantum computing and long-term privacy in Internet voting is, in this regard, a good instance to illustrate the problems associated to the regulation of technologies that evolve quickly and to future threats, considering their impact on fundamental rights. As Keith Martin has put it, “[w]e know [quantum computing is] coming. We know it will impact contemporary cryptographic algorithms (to quite varying extents). We don’t know the time frames. We don’t know how realistically the theory can be converted into practice” [Ma20]. To analyse this precise scenario, section 2 starts by providing an overview of what is known so far about quantum computing and the state of the art of its developments, as well as by mapping the impacts that quantum computing could have on Internet voting in the medium and long-term. To do so, we resort to specific examples of systems being in use for governmental elections in Canada, Estonia, France, and Switzerland. These countries have been using Internet voting for several years now and there is a substantial body of evidence available about their electoral frameworks, technical requirements, and on how their systems work. Based on this overview, we identify three potential challenges of quantum computing to Internet voting: on secret suffrage, on election integrity, and on transparency and verifiability. Out of these three, we conclude, the challenges to secret suffrage (i.e., long-term privacy in Internet voting) require immediate action.

In section 3 we diagnose how ready these countries’ electoral regulations are to cope with the challenge of quantum computing for long-term privacy. We identify that even when authorities are aware of the threat posed by quantum computers, no specific measures are envisaged to mitigate or eliminate this risk. These findings are surprising because a great deal of theorizing already exists about the risks of quantum computing for Internet voting and there are also several technical alternatives to, at least, mitigate them. More specifically, we study data deletion, quantum-resistant cryptography, and anonymous voting (including blind signatures, anonymous channels, and oblivious transfers) as potential responses. While none of these is perfect, and we conduct a detailed evaluation of their advantages and limitations, the feasibility of pre-emptively legally requiring them today should be studied. Overall, in this paper we provide an interdisciplinary approach towards quantum computing and Internet voting, addressing the legal and cryptographic implications of emerging technologies for fundamental rights. For this reason, we conclude in section 4 by recommending that law- and policy-makers start discussing which alternative(s) should be adopted in their electoral frameworks for Internet voting today.

2 Quantum computing: what do we know so far, and what are the challenges for Internet voting?

2.1 Quantum computing: the state-of-the-art

Quantum computing is evolving quickly. The first significant contribution to the development of quantum computing came in 1982, when Richard Feynman [Fe82] postulated that to simulate the evolution of quantum systems in an efficient way, we would need to build quantum computers (computational machines that use quantum effects). Nevertheless, it was not until 1994 that the view on quantum computing changed. Peter Shor [Sh94] developed a polynomial time quantum algorithm allowing quantum computers to efficiently factorize large integers exponentially quicker than the best classical algorithm on traditional machines, turning a problem which is computationally intractable into one that can be solved in just a few hours by a large enough quantum computer. Then, two years later, Lov Grover [Gr96] presented the second major quantum computing algorithm, which demonstrated the capability of quantum computers to speed up database search. These two are probably the most famous quantum algorithms but there are other examples such as the Deutsch-Jozsa Algorithm [DJ92] and its extension, the Bernstein-Vazirani [BV97] algorithm, or the Simon's algorithm [Si97] which inspired the quantum algorithms based on the quantum Fourier transform. The Quantum Algorithm Zoo [Jo11] provides an up-to-date catalog of quantum algorithms. Although there has been a lot of work on quantum algorithms throughout the years, physical implementation has been slow: “[q]uantum computing is still at an early stage: researchers are building the first working prototypes, and others are arguing about whether these machines will ever be more than research curiosities” [HG22]. Large technology companies [Da22] such as Google, Microsoft, Amazon or IBM have been working for years with the objective of building a large-scale quantum device. In 2016, IBM was the first one putting a quantum processor on the cloud so anyone could run experiments (the IBM Quantum Experience [IBb]). Then, in the subsequent years the company developed Falcon, a 27-qubit quantum computer (2018) and the 65-qubit Hummingbird (2020). In 2021, IBM built the first quantum processor with more than 100 qubits, the 127 qubit Eagle. More recently, in 2022, the 433-qubit Osprey, which shows that the predictions Bob Sutor (vice president of IBM Quantum Strategy and Ecosystem) shared with TechRepublic in 2020 were accurate, “[. . .] the company [. . .] released its quantum hardware roadmap [IBa], calling for a 127-qubit system in 2021, a 433-qubit system in 2022, and a 1,121-qubit system in 2023 [Gr20].” Nevertheless, Mike Loukides (vice president of emerging tech content at IT learning firm O'Reilly Media) “[. . .] estimates that it would take 1,000 logical qubits [. . .] to accomplish any real work [Pu22]”.

On the other hand, Google presented in 2019 a 53-qubit quantum computer, Sycamore [Ae19], and claimed quantum supremacy³ for the first time, which generated a lot of debate in the community [IB19]. Microsoft, on its side, is offering Azure Quantum

³ Quantum supremacy describes the ability of a quantum computer for solving a problem that the most powerful conventional computer cannot process in a practical amount of time.

[Mi23], a cloud quantum computing service which provides an environment to develop quantum algorithms which can be run in simulators of quantum computers. Apart from well-established technology companies, there are also some emerging players which are working hard on quantum computing. An example is D-Wave Systems, which has quantum computers of thousands of qubits, although “[t]he numbers cannot be compared with other kinds of quantum computers because the D-Wave qubits are not universal: they can only be used to solve a limited range of quantum problems” [HG22]. The company was also the first to sell a quantum computer to the world.

Given these developments, some consider that “[c]hange may come as early as 2030, as several companies predict they will launch usable quantum systems by that time [Bi21]”. In 2016 the NIST estimated that quantum computers would be available in 20 years, that is: by 2036 [Ch16a]. According to the EU Agency for Cybersecurity (ENISA), however, some threat agents could already have quantum computers in the next five to 10 years [Be21]. Nevertheless, as ENISA states in their report: “not all development in the area is public and it is fairly likely that the first fully functional large quantum computer will not be publicly announced”.

Although the biggest problems that quantum computers can currently solve are still easily manageable for conventional computers, several potential applications are already being explored for quantum computing, such as machine learning, Artificial Intelligence, chemistry, finance or cryptography.

When it comes to cryptography, quantum computers will have a significant impact. Everyday tasks such as sending an e-mail, making an online purchase or authenticating your identity are protected by cryptography and, mostly, by public key algorithms⁴. The hardness of these algorithms is based either on the difficulty of finding prime factors (in the case of RSA or ElGamal) or working out the discrete logarithm (i.e., elliptic curves or finite fields). Both are computational problems already solved by Shor’s quantum algorithm.

2.2 Should Internet voting systems be ready?

But how could quantum computing have an impact on Internet voting systems? Being used in the context of public political elections, Internet voting must also comply with the standards for democratic elections as enshrined in the main international law instruments. These include universal, equal, secret, and free suffrage (see e.g., art. 21 of the Universal Declaration of Human Rights, art. 25 of the International Covenant on Civil and Political Rights or, at the regional level, art. 3 of the Convention for the Protection of Human Rights and Fundamental Freedoms).

⁴ In contrast to public-key cryptography, the impact of quantum algorithms on symmetric cryptography will not be as severe. A quantum computer could speed up computations required for symmetric encryption, but the speedup is not as significant enough to break the encryption in a feasible time. Doubling the secret key size of symmetric algorithms would be enough to preserve security.

Nowadays, Internet voting complies with these standards by means of cryptography: the votes are encrypted end-to-end to ensure the secrecy of the vote and the freedom of the voter; before counting, votes are mixed or tallied using homomorphic encryption to prevent the contents of a vote from being linked to the voter who has cast them, thus ensuring vote anonymity; and encrypted votes are also digitally signed with keys that are unique to each voter to ensure that all votes stored in the digital ballot box and tallied have been cast by eligible voters. The most advanced systems also offer end-to-end verifiability, so voters can check that their encrypted vote contains their choices (cast-as-intended verifiability), and that it has reached the digital ballot box unmodified (recorded-as-cast verifiability). Furthermore, third parties can also ascertain that the tally genuinely represents all votes cast and stored in the ballot box (counted-as-recorded verifiability) and that ballot boxes have not been stuffed with additional ballots (voter eligibility).

However, we have already explained that quantum computing could break some cryptographic algorithms, thus jeopardising Internet voting. In fact, during an expert dialogue about Internet voting that took place in Switzerland in 2020, some experts already pointed out that “[q]uantum computers or advances in cryptanalysis may at some point subvert the soundness of today’s standard building blocks” [Sw20]. In this section, we provide a detailed account of the specific risks that quantum computing poses to Internet voting. To do so, we look at the specific election standards by international organizations, like the Council of Europe, and assess specific systems as they are currently being implemented in governmental elections in Canada, Estonia, France, and Switzerland.

Secret suffrage and long-term privacy. When it comes to secret suffrage, most Internet voting systems use a combination of end-to-end asymmetric encryption with some form of anonymous tallying, such as mix-nets or homomorphic tallying. This helps ensure, on the one hand, the confidentiality aspect of secret suffrage and, on the other, the anonymity of the votes [Ro22a; Vi15]. Therefore, the risks of quantum computing, even if not feasible yet, are especially acute when it comes to secret suffrage. In this regard, any data that is published today is vulnerable against quantum attacks in the future. According to Ward Beullens et al., “[w]hat makes matters worse is that any encrypted communication intercepted today can be decrypted by the attacker as soon as he [sic] has access to a large quantum computer, whether in 5, 10 or 20 years from now” [Be21]. Such a threat – referred to as retrospective decryption – was also acknowledged by the e-voting experts at the Swiss dialogue [Sw20]. Therefore, in the Internet voting context, an adversary could learn how a person voted some years ago, which may have political as well as personal implications (e.g., in case of family coercion). Voting data can be intercepted either because it has been published in a bulletin board, accessed by auditors, or because it has somehow been eavesdropped or leaked by internal attackers. In what follows, we explain the specific risks of quantum computing for secret suffrage by looking at two of its standards: confidentiality and anonymity.

Risks to confidentiality based on the vulnerabilities of conventional asymmetric encryption algorithms. The majority of the systems used nowadays in governmental elections use some

form of asymmetric or public-key encryption to protect the voting choices. Estonia [Es23], Switzerland [Sw23b] or France [DH22] are examples of countries which are currently offering Internet voting to their population. Their systems use the ElGamal public-key cryptosystem for encrypting the votes, whose security is based on the hardness of solving the discrete logarithm problem. This cryptosystem, as well as RSA, will be vulnerable against quantum-computing attacks. Thus, it will be possible to decrypt votes in the long-term using quantum computers and without the need of having the private key. Nevertheless, this would not be necessarily a problem as long as these votes are not related to voters' identity.

Risks to anonymity. Managing to decrypt a vote cast 10 to 20 years ago may not seem so relevant, at the end of the day the results of that election would have already been published. The problem with decrypting votes cast using current Internet voting systems is that it will be possible for the attacker to know what each voter has voted. This is because, in order to ensure the eligibility of all votes cast and stored in the ballot box, or to prevent that more than one vote per voter is included in the election tally, Internet votes are usually encrypted and digitally signed before they are cast. In fact, this is how the systems used in Estonia [Es23], Switzerland [Sw23b], and most of the municipalities in Canada [EI20; GPD10] work: the voters make their choices, the vote is encrypted, and the encrypted vote is then signed and cast into the voting server. Nowadays, digitally signing an encrypted vote does not breach anonymity, because votes are usually anonymised before they are tallied, or they are counted without being decrypted (a method that is called homomorphic tallying). Furthermore, multi-party computations or key-sharing mechanisms prevent a malicious actor from decrypting the votes before they are anonymised, since decryption requires the cooperation of different parties who each guard a share of the private decryption key. However, having access to the votes encrypted with conventional cryptography and digitally signed in the future, when quantum computers are available, would allow an attacker to decrypt them at any time, even without meeting the threshold of shares of the private decryption key.

Equal and free suffrage (I): eligibility and election integrity (digital signatures). Based on what we said above, are digital signatures used to demonstrate voter eligibility and satisfy election integrity at stake as well? Whereas quantum computers will also be able to tamper digital signatures based on conventional cryptography, this is not such a considerable risk if compared to those posed to confidentiality and anonymity. At the end of the day, voter eligibility is information that must at least be accessed by the election administration and by auditors (meaning that it is not completely private); whereas election integrity, once satisfied, cannot be tampered with in the future. In short: voter eligibility and election integrity are checked while the election is taking place, and it is highly unlikely that modern quantum computing is at the point where it can break currently deployed cryptographic systems.

However, it cannot be ignored that actual quantum computers may already exist, or that they could exist anytime soon. It means that quantum computing is no longer a long-term

risk, but a medium-to-short one. For example, in the framework of the above-mentioned Swiss expert dialog, one expert noted that “[i]t is unclear whether quantum computers will exist in the near future or if they already exist. Therefore, it is not possible to determine when a post-quantum cryptographic redesign is necessary” [Sw20]. If we take into account that most developments in cryptography have been kept secret [Le01; Si99], this risk cannot be downplayed.

Free suffrage (II): end-to-end verifiability (zero-knowledge proofs). Internet voting systems are end-to-end verifiable if they can provide evidence that every step of the election was completed correctly and accurately. This stands for allowing voters to individually verify their votes, and any third-party to check that election results accurately reflect the voters’ intention. The latter is possible due to cryptographic mechanisms, such as homomorphic tally or verifiable mixing, which can be verified by either repetition or mathematical proofs. In this regard, the proofs demonstrate the correctness of a certain process without giving information that might compromise the process itself.

Notwithstanding, and just as for voter eligibility and election integrity, quantum computers are not yet a problem for end-to-end verifiability. As previously mentioned, cryptographic proofs are generated for auditing the tallying. These proofs are zero-knowledge, which is crucial for anonymity, but they also satisfy another property which directly affects verifiability: soundness. Soundness means that if a statement is false (e.g., votes that are going to be decrypted are not those sent by the voters), the proof cannot convince the verifiers of the contrary. Since proofs are usually verified during or right after the election, the situation is not as critical. Nevertheless, if for any reason they have to be verified when practical quantum computers are available, we will not be sure anymore that what they are proving is indeed true.

3 Long-term privacy in Internet voting: desirable or compulsory?

3.1 Long-term privacy in Internet voting: an overview of existing regulations

In order to dispel whether countries where Internet voting is available have mitigation measures in place against future breaches of the secrecy of the vote, in what follows we detail the existing regulations for elections and Internet voting, with special attention to secret suffrage and long-term privacy, in Canada, Estonia, France and Switzerland.

Canada. Internet voting in Canada is extensively used at the local level. A few municipalities in the province of Ontario started using this voting channel back in 2003, and others in Nova Scotia followed as soon as 2006 [GPD10]. The number of municipalities has increased steadily ever since [GPD10], and in the last October 2022 municipal elections in Ontario

217 municipalities offered online voting, in some cases as the only voting channel. More recently, higher level administrations have also started considering Internet voting. For example, Northwest Territories first offered Internet voting in the 2019 territorial general election [EI20]. In spite of this considerable uptake, the legal framework for Internet voting is not really detailed regarding the requirements that this technology should meet. For example, municipalities in Ontario base the lawfulness of Internet voting on section 42 of the Municipal Elections Act, which authorises them to “pass by-laws authorizing the use of an alternative voting method, such as voting by mail or by telephone, that does not require electors to attend at a voting place in order to vote” [CAE19]. Notwithstanding, this section does not detail any specific requirements that these remote voting methods should meet.

In an attempt to address this lack of legal standards, and following expert claims that additional regulations are needed [EG20; SD13], there is an on-going attempt by the Digital Governance Standards Institute (formerly known as CIO Strategy Council, CIOSC) to develop a “series of standards aim[ed] to specify minimum technical requirements for online electoral voting in Canada at the municipal, provincial and federal level” [CI20]. A technical committee on online electoral voting (Technical Committee 11) was set up in 2020⁵. At the time of writing, the technical committee is working on a third draft version of the standards. References to quantum-resistant cryptography were added to the second draft [CI22]. The current draft now mentions quantum-resistant cryptography twice: in section 4.1.1.4, “[a]ll data shall be encrypted with quantum-resistant encryption both in transit and at rest” [Di22]; and in section 8.1.1.2, “[t]he voting service shall ensure that the secrecy of the vote is guaranteed using quantum-resistant encryption during the casting, transfer, reception, collection, and tabulation of votes” [Di22]. However, the very same draft already comes with a warning that “[s]tandards have not yet been finalized for quantum-resistant encryption” [Di22]. Anyhow, these are voluntary standards that election administrators using Internet voting could decide whether to follow or not, which fall short of enshrining a requirement for long-term privacy and prescribing mitigation measures.

Estonia. Estonia remains to date the first and only European experience where online voting is offered to all the population, for all contests: national, local, and to the European parliament. Elections are regulated in three different acts: parliamentary elections are primarily regulated by the *Riigikogu* Election Act, while election for local government units are regulated by the Municipal Council Election Act and elections to the European Parliament by the European Parliament Election Act. Notwithstanding, the latter Acts refer to the *Riigikogu* Election Act on those aspects related to Internet voting. Likewise, the Referendum Act deals with referendums, which according to the provisions in Chapter 7 shall also provide the option to vote electronically. In addition to electoral regulations, “the Estonian e-government ecosystem is strongly regulated by legal instruments that provide a framework for security and protection of the personal data” [SV16]. This framework includes,

⁵ All the details about this process can be found at: <<https://dgc-cgn.org/standards/find-a-standard/standards-in-online-electoral-voting-2/can-ciosc-111-x202x-online-electoral-voting/>> [last accessed 30 August 2023]

among others, Estonia's Personal Data Protection Act (1996), the Public Information Act (2000), the Population Register Act (2000), the Digital Signatures Act (2000), and the Electronic Communications Act (2004) [SV16].

The technical aspects of Internet voting are detailed in lower-level regulations. In these regulations, the risk of retrospective decryption is identified. In this regard, the General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia acknowledges that “a theoretical risk remains that someone is able to copy personalized i-votes from the system and attempts to guess the private key over time, by using remarkable computer resources over a long period of time” [EN23]. To mitigate this risk, the Framework advises taking account of this risk when “choosing the crypto algorithm for encryption of votes and the length of the key” as well as “rely[ing] on up-to-date studies on the security of crypto algorithms” [EN23]. The Framework has been recently updated, ahead of the *Riigikogu* elections of March 2023. Notwithstanding, almost identical provisions can be found in the previous version [E116]. Furthermore, the National Electoral Committee's Decision on the technical requirements to ensure the general principles of electronic voting also prescribes that unanonymous logs, electronic votes, personal data of voters included in the electronic voting system and the key for opening electronic votes are destroyed by the state election service together within the legally established deadlines [Na21]. The private key used for decryption must also be destroyed shortly after the election, thus rendering the non-anonymous and encrypted votes unusable, as is also required by the General Framework [EN23].

France. France can also be considered an Internet voting pioneer, even if the option to vote online is limited to French voters abroad. The French legal framework for Internet voting has remained more or less the same since a Constitutional amendment in 2008 introduced 11 members of the National Assembly to be elected by French voters abroad. Subsequently, the law num. 2013-659 of 22 July 2013 on the representation of French citizens abroad, set up a new institution representing the interests for French citizens abroad (the Consular Councils, for whose election voters could vote online) and amended the Electoral Code. As in the case of Estonia, there is a considerable amount of secondary regulation which completes the legal framework for Internet voting. Amongst them, specific requirements are to be found in the recommendations of the national data protection agency, the Commission Nationale de l'Informatique et des Libertés (CNIL). The CNIL first adopted a Recommendation on the security of e-voting systems in 2003 and then updated it in 2010 [CN10a]. The Recommendation provides general guidelines regarding minimal privacy, secrecy, and security requirements for Internet voting, including physical (e.g., access controls to the servers or rules for the clearance of authorized employees) and software measures (such as firewalls).

The CNIL has further updated their Recommendation in 2019 to take stock of the new requirements introduced by the European Union's General Data Protection Regulation (GDPR) after it entered into force [CN10b]. The goal of the update was to apply to future

developments in Internet voting, with a view to better respect the principles of personal data protection, and to inform data controllers on their choice for an online voting system [CN19]. In its new Recommendation, no specific references are made to the threat posed by retrospective decryption. Notwithstanding, the CNIL does prescribe the secure destruction of the data as soon as the deadline for complaints and appeals have been exhausted: “[a]ll support files (copies of the source and executable codes of the programs and of the underlying system, voting materials, tally files, results files, backups) must be kept under seal until the exhaustion of the channels and deadlines for appeal” [CN19]. The erasure of the data must be conducted, according to the CNIL, under the supervision of the electoral commission. Notwithstanding, the same measures were already prescribed in equivalent terms in 2010 [CN10a], which makes it unlikely that it is the result of specific awareness about the threat posed by quantum computers.

Switzerland. Even if the first tests with Internet voting in Switzerland took place back in 2003 [Sw04], the Swiss legal framework for Internet voting has recently undergone a major overhaul. Following the decision by the two main Internet voting providers not to continue offering their systems back in 2019 [Sw19], the legal framework has been updated, including with the already mentioned dialogue with expert communities and the amendment of two federal ordinances: the Federal Council’s Ordinance on Political Rights and the Federal Chancellery’s Ordinance on Electronic Voting [Sw22b]. Surprisingly, and in spite of the expert voices raising the issue of quantum computing during the dialogue, the updated regulations have not included specific requirements for long-term privacy. The need to protect secret suffrage in the long-term is therefore not specifically required in the new ordinances. Notwithstanding, the federal authorities seem to be aware of the concern, which has been identified in a recent risk assessment by the Swiss Federal Chancellery [Sw23a]. Interestingly, the risk is considered with a high impact score (with 35 points in a scale from 0 to 49), but of low probability [Sw23a]. According to the national authorities, in the absence of standardized post-quantum algorithms, it is still possible to prevent and mitigate the impact resulting from the evolution of quantum computing by increasing the key size of current encryption mechanisms [Sw23a]. In this case, it is considered that a key size of 3072 bits is enough.

At the same time, it is important to stress existing references to data deletion in the federal documents. For example, in their guide for risk assessment of *La Poste Suisse*’s Internet voting system, the Swiss Federal Chancellery now identifies four key post-election processes: file deletion; the destruction or secure deletion/formatting of the data supports; the destruction of the passwords; and the destruction of the smartcards [Sw22a]. However, none of these measures has been expressly linked to the actual threat posed by quantum computing. In fact, similar requirements can be found in previous regulations [Sw14; Sw18]. Therefore, these requirements could instead arouse from data protection regulations. Notwithstanding, identified monitoring measures associated to quantum computing do indeed include closer cooperation with the scientific community and the development of the

system and its documentation [Sw23a]. All in all, this approach can be summarized, using the very same words of the Swiss Federal Chancellery, as the fact that “no one can predict the future” [Sw23a].

3.2 Technical alternatives (their advantages and limitations)

Having now identified the specific risks posed by quantum computing to Internet voting systems and the existing *lacunae* in national electoral frameworks, it is now necessary to address which specific mechanisms could at least mitigate these risks. Since the main challenge is on preserving long-term privacy, this section will focus on technical alternatives to current implementations, so this standard is ensured.

The first technical alternative which comes to our minds is to leverage quantum computing/cryptography to protect long-term privacy in Internet voting systems, instead of just jeopardising them. The best-known example of a quantum algorithm is the Quantum Key Distribution (QKD) that allows two parties to exchange a secret using a special quantum channel and guarantees that an eavesdropper of the communication would be detected, and the process aborted [Wo21]. This is because it is not possible to measure the quantum state of the system without disturbing it. Nevertheless, we cannot rely only on the QKD for building a long-term private voting system compliant with electoral regulations. Even if all voters can securely transmit their choice directly to the electoral authority without the risk of being eavesdropped on, we would still have an issue with secret suffrage. The receiving entity (electoral authority) would know the individual choices of all voters and the intermediate tally at all moments. Hence, we would need to trust that entity for secrecy and tally fairness. Otherwise, we will need a voting solution similar to the existing ones but based on quantum cryptography. However, quantum cryptography needs special requirements such as its own infrastructure (which is not there yet) and does not cover all the needs of secure-communications and secure Internet voting systems (e.g., digital signatures, public-key encryption, zero-knowledge proofs, etc.). For this reason, we need to find other technical alternatives which allow for quantum-resistant Internet voting systems but without relying on quantum physics. Data deletion, quantum-resistant cryptography, and anonymous voting are some of the possible alternatives.

Data deletion. As we have seen above, requirements for data deletion following the end of an election are common. We have already identified these requirements in Estonia [Na21], France [CN19], and Switzerland [Sw22a]. Additionally, similar provisions can be found in the technical standards currently being developed in Canada [Di22].

Even if these measures seem to be related to data protection regulations rather than to the aim of protecting long-term privacy, they could seem at first sight an adequate mitigation mechanism. After all, if all election data is deleted once the election is over and after all the complaints and appeals deadlines have been exhausted, it will be no longer possible

to decrypt it in the future. Despite secure processes for data deletion already existing and being standardized, the problem with this alternative is that there are no guarantees that indeed all election data has been securely deleted. This risk cannot be downplayed if we consider that votes in Internet voting are cast from unsupervised environments and devices that fall outside the scope of the election administration, and through an insecure channel such as Internet voting. That means that potential attackers have a considerable surface to eavesdrop (un)encrypted votes before they reach the voting server, which they could keep despite the secure data deletion procedures. Likewise, an internal attacker from an election administration could easily generate a copy of all encrypted election data and prevent this copy from being deleted at the end of the election by safeguarding it outside the official election’s voting infrastructure.

Therefore, this approach has important flaws. The main problems associated to this approach is that they are based on an analogy to paper-based voting channels, such as postal voting or voting in polling stations, that fails at apprehending the specific stakes in Internet voting (on the shortcomings of regulation by analogy see [Ro22a; Ro22b]). While deleting digital data is possible, it is virtually impossible to control the number of copies because copying digital data is far easier than doing so for hard, paper-based ballots, and does not require special tools. Quantum computing is a novel threat and, therefore, regulating by analogy does not work: no similar problems exist in paper-based voting channels, since physical voting supports (i.e., paper votes), cannot be as easily eavesdropped and/or copied as electronic ones.

Quantum-resistant cryptography. Another alternative, based on the draft standards currently being developed in Canada, is the use of quantum-resistant cryptography. Quantum-resistant or post-quantum cryptography are based on mathematical problems that quantum computers may not be able to solve easily. Some examples include lattice-based cryptography, supersingular elliptic curves, or codes [Ch16a]. Indeed, of all of these, lattice-based cryptography is the cryptosystem that has received more attention. Good evidence is the list of post-quantum candidates to be standardized by the NIST as a result of the process initiated in 2017. A clear majority (three cryptosystems out of the selected four) are based on hard problems over lattices.

When it comes to Internet voting, a first construction of a post-quantum Internet voting system was given in 2016 [Ch16b]. This system is inspired by Helios [Ad08] and is based on Learning With Errors (LWE) fully homomorphic encryption [DM15], unforgeable lattice-based signature and trapdoors for lattices. The authors do not propose any parameters neither an implementation of the system. One year later, the EVOLVE (Electronic Voting from Lattices with Verification) system was presented [Pi17], which is based on the voting protocol described in [Cr96]. Compared to the previous construction, EVOLVE makes use of zero-knowledge proofs and voters commit to their preferred voting options instead of encrypting them. Another proposal which uses fully homomorphic encryption is that presented in [AQA18]. The main contribution of these authors is the implementation of

an electronic voting system using the homomorphic encryption scheme (the BGV scheme [BGV12]) included in HELib, Homomorphic Encryption library). In [Rø20], the authors also make use of fully homomorphic encryption and propose to replace the classical proofs suggested in the coercion-resistant JCJ protocol [JCJ05] by quantum-resistant designated verifier proofs [STW14], thus making the protocol quantum-resistant. Another proposal from the same year [Gu20] designs an electronic voting scheme which supports ballots for multiple candidates. Each candidate is represented by a 0 or 1, the IBFHE scheme (Identity-Based Fully Homomorphic Encryption) is used for encryption and the ECDSA algorithm for signatures.

The last proposals we have found in the literature focus on verifiable mix-nets and build a post-quantum e-voting system using them as the main building block. The first proof of a shuffle based on lattices is presented in [CMM17] and is later significantly improved in [CMM20]. Also, based on this post-quantum proof of a shuffle, the authors construct a post-quantum Internet voting system which, in addition to providing long-term privacy, also meets the requirements of coercion-resistance and individual verifiability [Co21]. Similarly, in [Ar21] there are the following contributions: the first efficient verifiable shuffle of known values, the first post-quantum construction of a practical voting system that is suitable for more general ballots and that supports return codes and, finally, a concrete choice of parameters for the system and its implementation. The architecture of the voting protocol is very similar to previous voting systems such as the Norwegian internet voting protocol [Gj12]. Although the system does not provide universal verifiability, it provides privacy, cast-as-intended, and coercion-resistance by allowing re-voting and integrity if at least one auditor is honest. An extended version of the shuffle presented in the previous paper is given in [Ar22], as well as a compatible verifiable distributed decryption protocol. In addition, the authors give concrete parameters for their system, estimate the size of each component and provide an implementation of all sub-protocols, but not of the full system. They employ NFlib library for the polynomial arithmetic, the FLINT library for arithmetic routines not supported in NFlib, and for gaussian sampling they adapted COSAC.

Therefore, lattice-based cryptography seems to be a good alternative for the replacement of current asymmetric encryption algorithms such as RSA or discrete logarithm on prime fields or elliptic curves. It offers strong security guarantees and many cryptographic primitives which can be implemented using conventional computers. However, this is precisely one of the problems with these algorithms: they “need to be capable of running on conventional computers” [Ma20], and they may not be as efficient as the existing standards. For example, the proposal in [Co21] has been recently implemented in [FWK21]. The efficiency of their findings makes the actual implementation of this system not feasible for actual politically binding elections.

More important, the robustness of quantum-resistant crypto is theoretical, and “[a] new quantum algorithm may be discovered which breaks some of these schemes” [Ch16a]. A good example of this is the SIKE cryptographic algorithm, which was a NIST Post-Quantum Cryptography candidate that was cracked by experts using a conventional machine [CD23].

Moreover, when it comes to Internet voting, some of the key cryptographic building blocks (such as asymmetric encryption or key-sharing mechanisms) have not yet been standardized.

Anonymous voting. Most of the protocols presented above make use of traditional ways to build Internet voting protocols such as homomorphic primitives or mix-nets. Nevertheless, when trying to ensure voter’s anonymity there is another well-known technique which consists of using blind signatures. This technique anonymizes the encrypted votes when they are cast, so theoretically the link between the encrypted vote and the voter who cast it is broken from the very beginning. In [Ka21] the authors propose a construction, based on the framework of Fujioka et al. [FOO92], which uses a blind signature scheme and a commitment scheme as the main building blocks. The first one allows for the preservation of the anonymity of each voter, while it forbids voters from voting twice. The second one prevents any partial result from being leaked before the end of the election. As the authors explicitly mention in their publication, this is the first online voting scheme that simultaneously provides post-quantum public verifiability and everlasting privacy (information-theoretic ballot anonymity).

Nevertheless, blind signatures or anonymous credentials are not enough to provide long-term privacy. Even though votes are not related to signatures, they are connected via other voter-identifiable information such as their IP address, cookies, etc. Even if we could entirely remove or hide all metadata, the nature of the election usually implies that voter registration (obtaining anonymous credentials) and vote-casting (using anonymous credentials) happens within a short time window. Therefore, it would be easy to link voters with their votes if they cast them at odd hours. Increasing the time between registration and voting would only result in problems with intermediate credentials safe-keeping and would prolong the opportunity for credential theft and coercion.

The alternative of casting votes via anonymous channels, as Univote voting system does, is also hardly a long-term private solution [Re13]. For example, The Onion Router (Tor) network provides anonymity (or rather pseudonymity) to millions of users accessing the internet daily. Communication over Tor is usually done via several relay nodes, which forward the traffic from the client’s machine to the internet server and back. Yet, Tor is not perfectly anonymous. Many issues can result in personal data leakage ranging from misconfiguration and user mistakes to sophisticated attacks. It does not mean every user will be deanonymized every time, but a possibility remains. Unfortunately, even if we construct a perfectly anonymous Tor-like system, it would not be sufficient for long-term privacy. Imagine that the client entry point to the network - the guard relay in Tor’s terms - is malicious. Such a relay knows when the voter connects and observes which ballot is posted soon after that (traveling through the network does not take long), which allows the linking of voters and votes. Also, the first node can always keep a copy of all data and wait until encryption becomes vulnerable. Finally, legal issues surrounding anonymous channels in general, and in Tor specifically, remain relatively unexplored. For example, some electoral legislation allows voters to use an alternative voting channel in case of a problem,

or the voter credentials are reissued, and the previously cast vote is canceled. However, with anonymous voting, it would be impossible to ensure a one voter, one vote standard in case the voter has technical issues during voting.

The oblivious transfer could, in theory, allow the voter to get some information from a set of values that the election authority has without revealing requested elements. For example, in the BVOT voting system, voters can get encoding for the selected options from the list of all possible voting choices. However, if the protocol is not post-quantum secure, anyone observing the interaction can later break it and identify the requested values. Hence, the oblivious transfer would not work for long-term privacy protection.

4 Conclusions and recommendations

This paper has shown how developments in quantum computing are yet another example of the shift towards governance and policy-making amidst uncertain risks, and how this will impact Internet voting. We know it is coming and we anticipate that it will have a huge impact on today's electronic communications. More important, voting online will no longer be secure either. In this paper we have addressed a more fundamental concern: how the technological developments in quantum computing tomorrow may affect the fundamental rights of people voting online today. In spite of Internet voting systems used in governmental elections today satisfying the legal requirements for democratic elections, these will no longer be secure once quantum computers are used to break public key cryptography – and this may compromise voters' secrecy in the long term. Therefore, we have demonstrated that quantum computing is not only an issue that should be considered in future regulations for Internet voting, but that should be already addressed today. Whereas the impact of quantum computing on election integrity, voter eligibility and end-to-end verifiability is not an issue yet, today's secret ballots are already vulnerable. Our analysis of four governmental experiences (Canada, France, Estonia and Switzerland) shows that governments and electoral administrations are aware of this risk, but no sufficient measures are yet being adopted to mitigate it. Making this matter worse, the importance of long-term privacy in Internet voting has not sufficiently been considered and the principles for democratic elections have not been revisited in light of future challenges: it is important to rethink the principle of secret suffrage and enshrine a standard of long-term privacy in Internet voting.

Interestingly, there is also a set of alternatives that could already be studied to protect long-term privacy. In this paper, we have analysed several proposals, including secure data deletion, quantum-resistant cryptosystems, and anonymous voting. Amongst them, quantum-resistant or post-quantum cryptography seems the most suitable, even if its actual implementation still requires some effort. Therefore, and whereas none of these alternatives is a silver bullet against quantum computing, it is essential that their feasibility is studied so technological developments do not harm citizens' fundamental rights. Likewise, and even if none of the analysed experiences is satisfactory from the perspective of electoral standards and requirements, the Swiss example is the most promising. Authorities in

Switzerland conduct risk assessments ahead of each election, and they are already aware that technological developments in quantum computing may compromise long-term privacy. The conclusion they reach, however, is in our opinion unsatisfactory: increasing encryption keys’ size and deleting data is not enough to guarantee long-term privacy. Destroying paper ballots may be enough to ensure that nobody links a voter to the voter who has cast it in the future, but when votes are cast electronically, they can easily be eavesdropped or copied, and copies could remain even when the main electoral infrastructure is destroyed.

The possibility of quantum-based retrospective decryption means that in the future it will be possible to know for whom each person has voted. Following its previous experiences in engaging experts in a wider dialogue on Internet voting, Switzerland – and any country using Internet voting – should already start involving them in making Internet voting quantum-proof as well. Otherwise, our rights are at stake.

References

- [Ad08] Adida, B.: Helios: Web-Based Open-Audit Voting. In: Proceedings of the 17th Conference on Security Symposium. SS’08, USENIX Association, San Jose, CA, pp. 335–348, 2008.
- [Ae19] Arute, F.; et al.: Quantum supremacy using a programmable superconducting processor. *Nature* 574/, pp. 505–510, 2019.
- [AQA18] Aziz, A.; Qunoo, H.; Abusamra, A.: Using Homomorphic Cryptographic Solutions on E-voting Systems. *International Journal of Computer Network and Information Security* 10/, pp. 44–59, Jan. 2018.
- [Ar21] Aranha, D. F.; Baum, C.; Gjøsteen, K.; Silde, T.; Tunge, T.: Lattice-Based Proof of Shuffle and Applications to Electronic Voting. In: *Topics in Cryptology – CT-RSA 2021*. Vol. 12704, Springer International Publishing, Cham, pp. 227–251, 2021.
- [Ar22] Aranha, D. F.; Baum, C.; Gjøsteen, K.; Silde, T.: Verifiable Mix-Nets and Distributed Decryption for Voting from Lattice-Based Assumptions, *Cryptology ePrint Archive*, Paper 2022/422, 2022, URL: <https://eprint.iacr.org/2022/422>.
- [BBR17] Bodansky, D.; Brunnée, J.; Rajamani, L.: *International Climate Change Law*. Oxford University Press, 2017.
- [Be21] Beullens, W.; D’Anvers, J.; Hüsling, A.; Lange, T.; Panny, L.; de Saint Guilhem, C.; Smart, N.: Post-Quantum Cryptography: Current state and quantum mitigation, tech. rep., European Union Agency for Cybersecurity (ENISA), 2021, URL: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>.

- [BGV12] Brakerski, Z.; Gentry, C.; Vaikuntanathan, V.: (Leveled) Fully Homomorphic Encryption without Bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. ITCS '12, Association for Computing Machinery, Cambridge, Massachusetts, pp. 309–325, 2012.
- [Bi21] Biondi, M.; Heid, A.; Henke, N.; Mohr, N.; Pautasso, L.; Ostojic, I.; Wester, L.; Zammel, R.: Quantum computing use cases - what you need to know, tech. rep., McKinsey Digital, 2021, URL: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know#/>.
- [BV97] Bernstein, E.; Vazirani, U.: Quantum Complexity Theory. SIAM Journal on Computing 26/5, pp. 1411–1473, 1997.
- [CAE19] Cardillo, A.; Akinyokun, N.; Essex, A.: Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology? In (Krimmer, R.; et al., eds.): Electronic Voting, 4th International Joint Conference, E-Vote-ID. Vol. 11759, Springer International Publishing, Cham, pp. 67–82, 2019.
- [CD23] Castryck, W.; Decru, T.: An Efficient Key Recovery Attack on SIDH. In (Hazay, C.; Stam, M., eds.): Advances in Cryptology – EUROCRYPT 2023. Vol. 14008, Springer Nature Switzerland, Cham, pp. 423–447, 2023.
- [Ch16a] Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D.: Report on Post-Quantum Cryptography, tech. rep., National Institute of Standards and Technology (NIST), 2016, URL: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>.
- [Ch16b] Chillotti, I.; Gama, N.; Georgieva, M.; Izabachène, M.: A Homomorphic LWE Based E-voting Scheme. In (Takagi, T., ed.): Post-Quantum Cryptography. PQCrypto. Vol. 9606, Springer International Publishing, Cham, pp. 245–265, 2016.
- [Ch80] Christol, C. Q.: The Common Heritage of Mankind Provision in the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies. The International Lawyer 14/, pp. 429–483, 1980.
- [CI20] CIO Strategy Council: National Standard of Canada - Standards Proposal, 2020, URL: https://dgc-cgn.org/wp-content/uploads/2020/06/CIOSC_Standards-Proposal-Health-Data-Capability_2020-05-26-1.pdf, visited on: 09/13/2023.
- [CI22] CIO Strategy Council: Online Electoral Voting – Part X: Implementation of Online Voting in Canadian Municipal Elections (D2), 2022.
- [CMM17] Costa, N.; Martínez, R.; Morillo, P.: Proof of a Shuffle for Lattice-Based Cryptography. In: Secure IT Systems. NordSec 2017. Vol. 10674, pp. 280–296, Nov. 2017, ISBN: 978-3-319-70289-6.

- [CMM20] Costa, N.; Martínez, R.; Morillo, P.: Lattice-Based Proof of a Shuffle. In: Financial Cryptography and Data Security - FC 2019. Vol. 11599, Springer International Publishing, pp. 330–346, Mar. 2020.
- [CN10a] CNIL: Délibération n° 2010-371 du 21 octobre 2010 portant adoption d’une recommandation relative à la sécurité des systèmes de vote électronique, JORF number 0272 of 24 November 2010, text number 29, 2010, URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000023124205>, visited on: 08/23/2023.
- [CN10b] CNIL: Sécurité des systèmes de vote par internet : la CNIL actualise sa recommandation de 2010. Online press release, 2010, URL: <https://www.cnil.fr/fr/securite-des-systemes-de-vote-par-internet-la-cnil-actualise-sa-recommandation-de-2010>, visited on: 03/29/2023.
- [CN19] CNIL: Délibération n° 2019-053 du 25 avril 2019 portant adoption d’une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet, JORF number 0142, of 21 June 2019, text number 95, 2019.
- [Co21] Costa, N.: Long-term privacy in electronic voting systems, <https://upcommons.upc.edu/handle/2042/58888>, PhD thesis, Universitat Politècnica de Catalunya (UPC), 2021.
- [Cr19] Crawford, K.: Halt the use of facial-recognition technology until it is regulated. *Nature* 572/, pp. 565–565, Aug. 2019.
- [Cr96] Cramer, R.; Franklin, M.; Schoenmakers, B.; Yung, M.: Multi-Authority Secret-Ballot Elections with Linear Work. In (Maurer, U., ed.): *Advances in Cryptology - EUROCRYPT*. Vol. 1070, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 72–83, 1996.
- [Da22] Dargan, J., 2022, URL: <https://thequantuminsider.com/2022/09/05/quantum-computing-companies-ultimate-list-for-2022/>, visited on: 03/20/2023.
- [DH22] Debant, A.; Hirschi, L.: Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol, *Cryptology ePrint Archive*, Paper 2022/1653, <https://eprint.iacr.org/2022/1653>, 2022, URL: <https://eprint.iacr.org/2022/1653>.
- [Di22] Digital Governance Standards Institute: Online Electoral Voting – Part X: Implementation of Online Voting in Canadian Municipal Elections (D3), 2022.
- [DJ92] Deutsch, D.; Jozsa, R.: Rapid solutions of problems by quantum computation. In: *Proceedings of the Royal Society of London A*. Vol. 439, pp. 553–558, 1992.
- [DM15] Ducas, L.; Micciancio, D.: FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. In: *Advances in Cryptology - EUROCRYPT* 2015. Vol. 9056, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 617–640, 2015.

- [EG20] Essex, A.; Goodman, N.: Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada. *Election Law Journal: Rules, Politics, and Policy* 19/, pp. 1–18, May 2020.
- [EI16] Electronic Voting Committee: General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia, 2016, URL: https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf, visited on: 08/23/2023.
- [EI20] ElectionsNWT: CEO Report on the administration of the 2019 territorial general election, 2020, URL: https://www.electionsnwt.ca/sites/electionsnwt/files/report_of_the_chief_electoral_officer_on_the_administration_of_the_2019_general_election.pdf, visited on: 03/09/2023.
- [EN23] Estonian National Electoral Committee: General description of the framework of the i-voting system IVXV, 2023.
- [Es23] Requirements to IVXV framework, URL: <https://www.valimised.ee/sites/default/files/uploads/eh/IVXV%20raamistiku%20nC3%B5uded%20kr%C3%BCptos%C3%BCsteemile%20v02.pdf>, visited on: 03/29/2023.
- [Fe82] Feynman, R. P.: Simulating physics with computers. *International Journal of Theoretical Physics* 21/, pp. 467–488, 1982.
- [FOO92] Fujioka, A.; Okamoto, T.; Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: *Advances in Cryptology - AUSCRYPT*. 1992.
- [FWK21] Farzaliyev, V.; Willemson, J.; Kaasik, J. K.: Improved Lattice-Based Mix-Nets for Electronic Voting, *Cryptology ePrint Archive*, Paper 2021/1499, 2021, URL: <https://eprint.iacr.org/2021/1499>.
- [GHY22] Genser, J.; Herrmann, S.; Yuste, R.: International Human Rights Protection Gaps in the Age of Neurotechnology, *NeuroRights Foundation*, 2022.
- [Gj12] Gjøsteen, K.: The Norwegian Internet Voting Protocol. In (Kiayias, A.; Lipmaa, H., eds.): *E-Voting and Identity. Vote-ID 2011*. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–18, 2012.
- [GPD10] Goodmana, N.; Pammett, J. H.; DeBardeleben, J.: Internet Voting: The Canadian Municipal Experience, *Canadian Parliamentary Review* 33(3), 13-21, 2010.
- [Gr20] Greig, J., 2020, URL: <https://www.techrepublic.com/article/6-experts-share-quantum-computing-predictions-for-2021/>, visited on: 08/23/2023.
- [Gr96] Grover, L. K.: A Fast Quantum Mechanical Algorithm for Database Search. In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. STOC '96*, Association for Computing Machinery, Philadelphia, Pennsylvania, USA, pp. 212–219, 1996, ISBN: 0897917855.

- [Gu20] Guopeng, L.: Multi-Candidate Electronic Voting Scheme Based on Fully Homomorphic Encryption. *Journal of Physics: Conference Series* 1678/, p. 012064, Nov. 2020.
- [HG22] Hoofnagle, C.J.; Garfinkel, S.L.: *Law and Policy for the Quantum Age*. Cambridge University Press, 2022.
- [IBa] IBM, URL: <https://www.ibm.com/quantum/roadmap>, visited on: 03/20/2023.
- [IBb] IBM Quantum Platform, URL: <https://quantum-computing.ibm.com/>, visited on: 03/20/2023.
- [IB19] IBM Research Blog, 2019, URL: <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/>, visited on: 03/20/2023.
- [JCJ05] Juels, A.; Catalano, D.; Jakobsson, M.: Coercion-Resistant Electronic Elections. In: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. WPES '05, Association for Computing Machinery, Alexandria, VA, USA, pp. 61–70, 2005, ISBN: 1595932283.
- [Jo11] Jordan, S., 2011, URL: <https://quantumalgorithmzoo.org/>, visited on: 03/28/2023.
- [Ka21] Kaim, G.; Canard, S.; Roux-Langlois, A.; Traoré, J.: Post-quantum Online Voting Scheme. In: *FC 2021 - Financial Cryptography and Data Security*. International Workshops. Vol. *Lecture Notes in Computer Science*. 12676, Virtual event, France, pp. 290–305, 2021, URL: <https://hal.science/hal-03355875>.
- [Le01] Levy, S.: *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*. 2001.
- [Le95] Leiss, W.; Beck, U.; Ritter, M.; Lash, S.; Wynne, B.: Risk Society, Towards a New Modernity. *Canadian Journal of Sociology / Cahiers canadiens de sociologie* 19/, p. 544, Nov. 1995.
- [Ma20] Martin, K.: *Cryptography. The Key to Digital Security, How It Works, and Why It Matters*. W.W. Norton and Company, 2020.
- [Mi23] Microsoft, 2023, URL: <https://learn.microsoft.com/en-us/azure/quantum/overview-azure-quantum>, visited on: 03/20/2023.
- [Na21] National Electoral Committee: Tehnilised nõuded elektroonilise hääletamise üldpõhimõtete tagamiseks, 2021, URL: <https://www.riigiteataja.ee/akt/327012021006>, visited on: 08/23/2023.
- [Pi17] del Pino, R.; Lyubashevsky, V.; Neven, G.; Seiler, G.: Practical Quantum-Safe Voting from Lattices. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS '17, Association for Computing Machinery, Dallas, Texas, USA, pp. 1565–1581, 2017, ISBN: 9781450349468.
- [Pu22] Pure Storage, 2022, URL: <https://blog.purestorage.com/purely-informational/are-quantum-computers-real/>, visited on: 08/23/2023.

- [Re13] Research Institute for Security in the Information Society - E-Voting Group: UniVote, 2013, URL: <https://e-voting.bfh.ch/projects/univote/>.
- [Rø20] Rønne, P. B.; Atashpendar, A.; Gjøsteen, K.; Ryan, P. Y. A.: Short Paper: Coercion-Resistant Voting in Linear Time via Fully Homomorphic Encryption. In: *Financial Cryptography and Data Security*. Vol. 11599, Springer International Publishing, Cham, pp. 289–298, 2020.
- [Ro22a] Rodríguez-Pérez, A.: Secret texts and cipherballots: secret suffrage and remote electronic voting, PhD thesis, Universitat Rovira i Virgili, 2022, URL: <http://hdl.handle.net/10803/675606>.
- [Ro22b] Rodríguez-Pérez, A.: The Council of Europe’s CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update? In (Krimmer, R.; Volkamer, M.; Duenas-Cid, D.; Rønne, P.; Germann, M., eds.): *Electronic Voting. E-Vote-ID*. Vol. 13553, Springer International Publishing, Cham, pp. 90–105, 2022.
- [SD13] Schwartz, B.; Dan Grice, J.: Establishing a Legal Framework for E-Voting in Canada, 2013, URL: https://www.elections.ca/res/rec/tech/elfec/pdf/elfec_e.pdf, visited on: 09/13/2023.
- [Sh94] Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Pp. 124–134, 1994.
- [Si97] Simon, D. R.: On the Power of Quantum Computation. *SIAM Journal on Computing* 26/5, pp. 1474–1483, 1997.
- [Si99] Singh, S.: *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books, 1999.
- [STW14] Sun, X.; Tian, H.; Wang, Y.: Toward Quantum-Resistant Strong Designated Verifier Signature. 5/2, pp. 80–86, 2014.
- [SV16] Solvak, M.; Vassil, K.: E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015). In cooperation with Estonian National Electoral Committee, Johan Skytte Institute of Political Studies, University of Tartu, Ülikooli 18, 51003 Tartu, Estonia, 2016.
- [Sw04] Swiss Federal Chancellery: *Le vote électronique dans sa phase pilote - Rapport inter-médiaire*. 2004.
- [Sw14] Swiss Federal Chancellery: *Catalogue des exigences à remplir pour recourir au vote électronique lors de votations populaires fédérales*, 2014.
- [Sw18] Swiss Federal Chancellery: Annex to the FCh Ordinance of 13 December 2013 on Electronic Voting (OEV, SR 161.116). Technical and administrative requirements for electronic vote casting - version 2.0, 2018.
- [Sw19] Swiss Federal Chancellery: *Vote électronique – Public Intrusion Test 2019*. Final report of the steering committee, 2019.

- [Sw20] Swiss Federal Chancellery: Summary of the expert dialog - Redesign of Internet Voting Trials in Switzerland 2020, 2020, URL: <https://www.news.admin.ch/newsd/message/attachments/63915.pdf>, visited on: 09/12/2023.
- [Sw22a] Swiss Federal Chancellery: Guide pour l’appréciation des risques. Système du vote électronique de La Poste Suisse. 2022.
- [Sw22b] Swiss Federal Chancellery: Révision partielle de l’ordonnance sur les droits politiques et révision totale de l’ordonnance de la ChF sur le vote électronique (restructuration de la phase d’essai). Rapport explicatif en vue de l’entrée en vigueur au 1er juillet 2022, 2022.
- [Sw23a] Swiss Federal Chancellery: Appréciation des risques Vote électronique de la Chancellerie fédérale 2023, 2023.
- [Sw23b] Swiss Federal Chancellery: Swisspost e-voting documentation, 2023, URL: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/System/System_Specification.pdf, visited on: 03/09/2023.
- [Un21] United Nations, 2021, URL: <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening>, visited on: 09/08/2023.
- [Vi15] Vinkel, P.: Remote Electronic Voting in Estonia: Legality, Impact and Confidence, PhD thesis, Tallin University of Technology, Aug. 2015.
- [Vo23] Vox, 2023, URL: <https://www.vox.com/future-perfect/2023/3/29/23660833/ai-pause-musk-artificial-intelligence-moratorium-chatgpt-gpt4>, visited on: 09/08/2023.
- [Wo21] Wolf, R.: Quantum Key Distribution - An Introduction with Exercises. Part of the book series: Lecture Notes in Physics, Springer, 2021.

Track 3: Election and Practical Experiences

Improving the Swiss Post Voting System: Practical Experiences from the Independent Examination and First Productive Election Event

Olivier Esseiva¹ Audhild Høgåsen² Xavier Monnat³

Abstract:

The Swiss Post Voting System has undergone over the past few years a rigorous independent examination by experts mandated by the Swiss Federal Chancellery. Following the examination, Swiss Post has made improvements in several areas, including for voter authentication, synchronization, input validation, and universal verifiability. On 18 June 2023, the Swiss Post Voting System was put to trial in its first productive election event. 4,239 voters cast their vote online during the approximately one month that the e-voting channel was open. The adoption rate of the e-voting channel was high, especially among Swiss residents living abroad, with an adoption rate of more than 50%. Swiss Post extensively monitored the voting servers during the whole election period and did not detect any anomalies during the system's operation. The feedback collected regarding the voters' user experience was largely positive. A few voters experienced confusion with regard to the voting process or with browser compatibility issues. Swiss Post has learned important lessons from the independent examination and from the first productive election event, and will continue the work improving the Swiss Post Voting System.

Keywords: Swiss Post Voting System; Electronic Voting; Online Voting; Public Scrutiny; Independent Examination

¹ olivier.esseiva@post.ch All authors are employed by Swiss Post (Switzerland) and work in the E-voting team.

² audhild.hoegaasen@post.ch

³ xavier.monnat@post.ch

1 Introduction

1.1 Past Experiences

Switzerland has a longstanding tradition of direct democracy, allowing Swiss citizens to vote approximately four times a year in elections and referendums. While mail-in ballots have traditionally been the prevailing method of voting in Switzerland, some cantons have previously introduced e-voting to a portion of their electorate. A survey from gfs-zürich reveals that almost three quarters of the public would welcome online voting.⁴

Swiss Post provided an e-voting system between 2016 and 2019. However, due to substantial criticism from reputable security researchers [Ha19, Ha20, TP19, LHK19], the system was subsequently withdrawn from the market in 2019.

1.2 Relaunch of E-Voting Trials

In 2020, Swiss Post made the strategic decision to internalize the development process and establish a cryptography competence center in Neuchâtel, Switzerland. This center comprises a team of software engineers, cryptographic developers, and mathematicians who possess specialized expertise. Their responsibilities include designing the cryptographic protocol, implementing the specification, and ensuring the secure operation of the Swiss Post Voting System.

Since 2019, Swiss Post has made significant enhancements to the design, documentation, and implementation of the e-voting system. As a result, in March 2023 the Federal Council authorized the cantons of St. Gallen, Thurgau, and Basel-Stadt to employ the Swiss Post Voting System for a specific subset of their electorate.⁵ Subsequently, during the federal vote on 18 June 2023, a total of 4,239 voters opted to cast their ballots online using the Swiss Post Voting System.

1.3 Transparent Development and Public Scrutiny

Transparency and public scrutiny is crucial for enhancing trust and acceptance of online voting. Swiss Post strives to achieve this through an open, transparent development process, complemented by the active involvement of a community of security researchers, hackers, and students to perpetually scrutinize its system's documentation and implementation [MO21]. This section presents a concise overview of the initiatives undertaken by Swiss Post to foster this community.

⁴ Survey on e-voting from gfs.zürich: <https://gfs-zh.ch/schweizer-bevoelkerung-befuerwortet-e-voting/>

⁵ Federal Council approves resumption of online voting trials: <https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-93455.html>

1.3.1 Continuous Publication of Documentation

Swiss Post publishes a wide variety of documents on its GitLab platform.⁶ Table 1 summarizes the main documents that are particularly relevant for the e-voting community.

Document	Description
Computational proof	Mathematical proof of verifiability and privacy under a minimal set of computational assumptions
Symbolic model	Machine-checkable ProVerif model of the Swiss Post Voting System proving verifiability and privacy in a symbolic setting
System specification	Pseudo-code specification of the cryptographic protocol
Verifier specification	Pseudo-code specification of the auditor's technical aid for verifying the correctness of the election result
Crypto-primitives specification	Pseudo-code specification of the cryptographic primitives underpinning the cryptographic protocol
Infrastructure documentation	Documents describing the deployment, testing, and operations of the Swiss Post Voting System

Tab. 1: Overview of published documents on Swiss Post's GitLab platform.

1.3.2 Continuous Publication of Source Code

Swiss Post publishes the source code of the components of the e-voting ecosystem.

Table 2 summarizes the published source code. We publish the verifier and the libraries underpinning the Swiss Post Voting System under a permissive Apache-2 licence. The source code of the Swiss Post Voting System's components is published under a proprietary license granting non-commercial academic use.

Repository	Description	Lines of Code	License
E-voting	Source code of the e-voting system	55,000	Proprietary
Verifier	Source code of the verification software	11,000	Apache-2
Crypto-primitives	Java cryptographic library	9,000	Apache-2
Crypto-primitives-ts	TypeScript cryptographic library	2,000	Apache-2
E-voting-libraries	Shared functionality and domain objects	11,000	Apache-2
Data-integration-service	Tool to process configuration files	6,000	Proprietary

Tab. 2: Overview of the Swiss Post Voting System's source code repositories.

Furthermore, we provide security researchers with instructions and test data on how to run an end-2-end test locally on their machines using Docker containers.⁷

⁶ All documentation is found on GitLab: <https://gitlab.com/swisspost-evoting>

⁷ End-2-end instructions and test data: <https://gitlab.com/swisspost-evoting/e-voting/evoting-e2e-dev>

1.3.3 Reproducible Builds

To guarantee the integrity and intended functionality of the software, Swiss Post employs reproducible builds. There must be a reliable and verifiable software compilation and proof that the source code in the production environments is the same as the publicly available source code, thereby enabling anyone to verify that the binary of the system's component aligns with the inspectable source code published on GitLab. This ensures that the Swiss Post Voting System's components remain untampered with and perform as intended.

The cantons conduct trusted build ceremonies involving mandated experts. The protocols pertaining to these ceremonies are published openly on the GitLab platform.⁸

1.3.4 Permanent Bug Bounty Program

The Swiss Post Voting System is subject to a permanent bug bounty program. The bug bounty program covers the cryptographic protocol, specification, and source code, inviting researchers to identify vulnerabilities. Successful attacks targeting verifiability are eligible for bounties reaching up to EUR 230,000.⁹ Through this initiative, to date, 287 reports have been submitted, four significant issues have been discovered, and a total of EUR 170,000 in bounties has been paid out across all bounty reports.¹⁰ All accepted findings are also published on Swiss Post's GitLab. This includes the summary of the report and comments. The reporter of the findings will be credited if the reporter agrees to publication. The hunters can decide if they want to be credited with their name, stay anonymous, or use an alias.

1.3.5 Test Platform

Starting from April 2023, Swiss Post provided a test platform on which anyone could run through the electronic vote casting process.¹¹ In the span of two months, more than 2,000 votes were cast, and Swiss Post received more than 200 feedback messages through the corresponding feedback form.

⁸ Protocols for the trusted build ceremonies: <https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Trusted-Build>

⁹ Information about the bug bounty program: <https://yeswehack.com/programs/swiss-post-evoting>

¹⁰ Overview of received reports: <https://evoting-community.post.ch/en/contributions>

¹¹ Swiss Post test platform: <https://post-medien.ch/en/how-does-e-voting-work-anyone-can-now-try-out-casting-a-vote-on-swiss-posts-test-platform>

1.3.6 Regular Public Intrusion Tests

Swiss Post conducts periodic public intrusion tests, extending invitations to hackers worldwide, with the objective of assessing the security of its e-voting infrastructure. This initiative serves as a valuable complement to the permanent bug bounty program. The public intrusion test offers hackers a designated platform to target a production-like environment.

In 2022, the public intrusion test attracted the participation of 3,400 hackers. Despite their collective efforts, no hacker succeeded in breaching the e-voting system.¹² Nevertheless, the test proved beneficial as it enabled Swiss Post to identify areas for improvement, particularly with respect to voter authentication. In 2023, a public intrusion test took place from 8 to 31 July. As in the year before, no hacker succeeded in breaching the e-voting-system. The activity was similar to the year before. Four reports were submitted, and one was accepted as best practice.¹³

1.3.7 Further Contact with the Community

Regular information to our community is important. Since 2017, Swiss Post has been running a blog that is regularly updated with news about the Swiss Post Voting System.¹⁴ In addition, anyone interested can sign up to the regular infomail from the Swiss Post E-voting team.¹⁵ Since 2021, Swiss Post has held four webinars covering topics such as security by design, trust model, complete verifiability, open source, auditability, and end-to-end testing.¹⁶ In May 2023, Swiss Post organized an event at the cryptography competence center in Neuchâtel especially for IT and math students.¹⁷ Swiss Post engages with the academic community at the conference E-Vote-ID every year. Swiss Post has submitted several papers to this conference. In 2017, the paper *A secure e-voting infrastructure. Implementation by Swiss Post* [SMM17] by Raffaele Stefanelli, Denis Morel and Xavier Monnat was published. In 2021, the paper *The challenges of enabling public scrutiny* [MO21] by Xavier Monnat and Simon Oswald was published. Then in 2023, this paper was published.

¹² PIT 2022: <https://www.post.ch/en/about-us/media/press-releases/2022/hackers-put-e-voting-system-to-the-test> and <https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/issues/43>

¹³ PIT 2023: <https://post-medien.ch/en/swiss-posts-e-voting-system-to-be-used-for-the-first-time-in-elections-this-autumn-following-further-development-and-successful-hacker-test/>

¹⁴ E-voting blog: <https://www.evoting-blog.ch/en>

¹⁵ E-voting infomail: <https://evoting-community.post.ch/en/community-programme/infomail>

¹⁶ E-voting webinars: <https://digital-solutions.post.ch/en/e-government/blog/tag/event>

¹⁷ E-voting community event 2023: <https://digital-solutions.post.ch/en/e-government/blog/exclusive-insight-into-swiss-post-s-e-voting-system>

2 Independent Examination

Switzerland's federal law establishes various prerequisites for the approval of e-voting systems to be utilized in elections and referendums. Among these requirements is the mandate that the e-voting system and its operations undergo an independent examination commissioned by the Swiss Confederation.¹⁸ The independent examination is a continuous process, and every new release of the e-voting system triggers a new independent examination.

2.1 Reports by Independent Auditors

Between 2021 and 2023, the Federal Chancellery commissioned renowned experts from academia and industry to examine the Swiss Post Voting System. The examination covered four areas: the cryptographic protocol (Scope 1), the software (Scope 2), the infrastructure and operations at Swiss Post and the cantons (Scope 3), and an intrusion test (Scope 4). The experts produced a total of 28 audit reports. 13 of the reports examined the cryptographic protocol [Es22, Ba22, Ha22a, HPT22, Fo22, Es23c, Es23a, Es23b, RBS23, Ha23, HPT23c, HPT23a, HPT23b], 13 examined the software [HPT22, Fo22, Ha22b, FAD22, Oe23, OH23b, OH23a, OH23c, Fo23, HPT23c, HPT23a, HPT23b, Ha23], six examined infrastructure and operation [Fo22, AFD22, AO23a, AO23b, Ad23, AO23c] and three concerned intrusion testing [SC22, SC23, Kr22]. Several of the reports spanned multiple areas of examination.

In response to the examination reports, Swiss Post summarized the key recommendations, expressed its stance, and provided responses to the major findings and observations highlighted in the reports [Sw22, Sw23d].

Swiss Post is grateful for the extensive reports from the mandated experts and for the opportunity given to improve the Swiss Post Voting System. Numerous issues have already been addressed by Swiss Post, and numerous improvement suggestions have been implemented. However, certain enhancements necessitate a longer timeframe and substantial effort to implement. The Federal Chancellery has outlined a catalogue of measures for these pending improvements and enhancements, including a timeframe for when the measures must be addressed [FC23b].

2.2 Identified Issues and System Improvements

In this section, we highlight a few issues from the examination reports and describe how Swiss Post addressed them in the cryptographic protocol, specification, and code.

¹⁸ Information about the audit concept and all expert reports can be found here: https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html

2.2.1 Voter Authentication

The voting phase comprises two primary stages: firstly, the voter submits the encrypted vote, and secondly, the voter confirms the vote. However, before this, there is a preliminary voter authentication phase, wherein the voter receives an encrypted key store and public keys for vote encryption.¹⁹

The voter authentication protocol previously used by the Swiss Post Voting System up until April 2023 employed a challenge-response mechanism and did not expose any known security flaws. Nevertheless, various problems concerning the voter authentication were highlighted in the expert reports [Ha23, Section B.3.3] [Ba22, Section Assumptions and Limitations], [Es22, Section 7], [Fo22, Section 5.1]. The criticism highlighted the omission of voter authentication in the symbolic models, the absence of pseudo-code for these authentication algorithms, and an overly complex three-round communication process between the voting server and voting client.

To tackle this issue, Swiss Post rewrote the voter authentication protocol. The new voter authentication protocol is described in pseudo-code in the system specification and included in the symbolic analysis of the cryptographic protocol. The implementation of the new voter authentication protocol significantly simplifies the complexity of the source code. It enabled the retirement of two outdated cryptographic libraries and facilitated the removal of over 20,000 lines of code from the system, thereby streamlining and enhancing its overall efficiency.

Figure 1 shows the workflow of the voter authentication protocol. Importantly, the new voter authentication protocol retains its ability to safeguard against replay attacks from network adversaries, relying on the presence of a trustworthy voting server. The new voter authentication protocol draws inspiration from the TOTP protocol [M'11] and requires only a single round of communication, as opposed to the previous three rounds.

2.2.2 Synchronization

Haenni et al. [Ha22b, Section 2.6] observed that the Swiss Post Voting System lacked a robust mechanism to synchronize the execution of specific operations. This absence of synchronization posed significant concerns, particularly due to the system's deployment across multiple data centers for availability purposes. If an attacker could manage to deceive two instances of the same component into processing two distinct messages simultaneously, this could potentially undermine the system's verifiability.

¹⁹ It is worth noting that this preliminary voter authentication phase holds no relevance for the protocol's security analysis. An attacker with control over the voting client can access the contents of the voter's keystore, whereas an attacker lacking control over the voter or voting client cannot open the keystore.

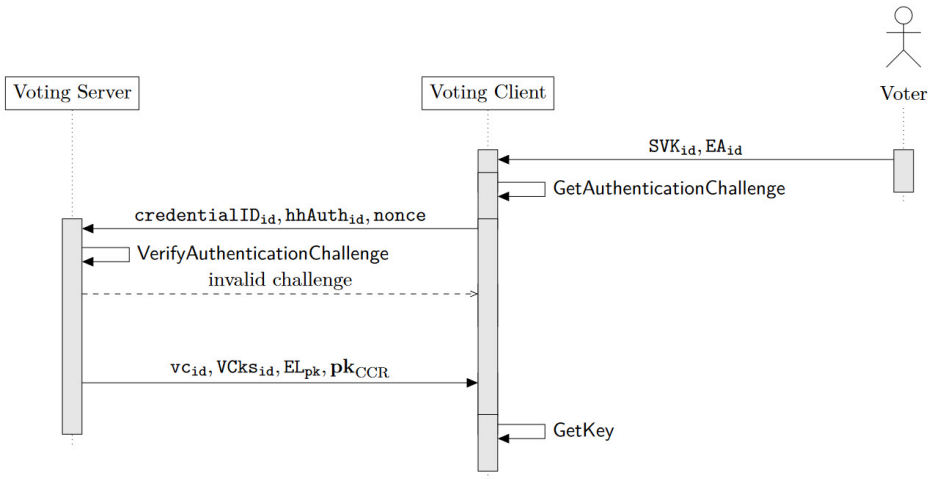


Fig. 1: Sequence diagram indicating the flow of messages in the new voter authentication protocol [Sw23b, page 58].

For instance, the attacker could transmit both a vote corresponding to the voter’s selection and a vote containing the attacker’s own selections concurrently to a control component. If both instances processed the messages, the attacker could send the expected return codes to the voter while simultaneously storing the manipulated vote in the ballot box—effectively compromising individual verifiability.

To solve this problem and ensure that each component processes every message exactly once, the Swiss Post Voting System now uses the mechanism of an exactly-once processor. The architecture document [Sw23a, Section 10.1.2] outlines this mechanism. The exactly-once processor leverages a widely adopted approach for achieving concurrency control in distributed systems, namely database transactions. The message broker’s at-least-once delivery ensures that messages are received by the control components, even in the presence of failures or network issues. Finally, the control component’s idempotent handling of messages guarantees that processing a message multiple times always yields the same result.

In the event that two instances of the same component receive different messages for the same voter simultaneously, the system employs a rollback mechanism within the database transactions. This ensures that only one message and response is ultimately saved, and a single response is transmitted to the requester. Consequently, the desired security properties are achieved.

Figure 2 illustrates the scenario in which the same message is delivered near simultaneously to both Control Component 1 instances. As there has been no previously computed response, both copies of the message will be processed. However, the database will detect the consistency violation and force a rollback of one transaction. Furthermore, only one message will be processed successfully, and only one response returned, since the second instance refrains from sending the processed message back to the requester.

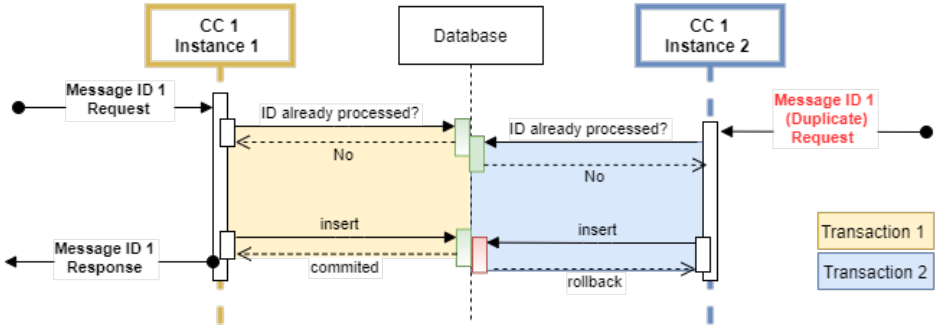


Fig. 2: Diagram showing the mechanism used in the Swiss Post Voting System to handle delayed duplicate messages to ensure exactly-once processing [Sw23a, page 61].

Importantly, the effectiveness of the exactly-once processor was validated during subsequent rounds of the experts' review:

[Ha23, Section 2.2.6]: They also implemented a property called exactly once processing, which guarantees that external messages are processed exactly once. This prevents not only identical messages from being processed more than once, but also similar messages (of the same type). For example, if a voter sends different ballots simultaneously, then these ballots are recognized as similar messages and only one of them will be processed.

2.2.3 Input Validation

The specification documents offers for each algorithm of the system a comprehensive pseudo-code description, including description of the context, input, operation, and output. The implementation must adhere to these pseudo-code instructions.

Nevertheless, the independent experts emphasized that the source code adhering faithfully to the pseudo-code specification is not sufficient. They stressed the significance of rigorous input validation and the necessity of taking the context from a trusted source:

[HPT22, Section A.2.1]: For example, the micro services allow the functions to be called many times on a wide range of data, but the security model in the proof assumes most functions can be called only once on a very rigid input. This is a significant discrepancy between the specification and the code, that makes it really hard to decide whether the code does what the specification says, while making it quite possible that the code will lead to many more possible system states than what the specification allows.

Other experts agreed on the importance of rigorous context and input validation [Es22, Section 1.2, Section 8, Section 9.2, Section 9.3] [Ha22b, Section 2.5].

A typical example of the principle of input validation is the group parameters of the ElGamal encryption scheme. These parameters are context for several pseudo-code algorithms in the cryptographic protocol. The algorithms must be instantiated with the group parameters from the component's internal view, where their validity was previously verified during an earlier stage of the protocol. The group parameters must not be taken from adversarially controlled messages.

In response to the criticism, we extensively reviewed the services invoking the protocol's algorithm and ensured that all components properly validate the input and take the context from a trusted source. Input validation involves verifying that the input adheres to the expected format, such as confirming that all elements belong to the designated group and that the vectors contain the appropriate number of elements. Additionally, we took measures to ensure that the context variables originate from the internal view of a component and/or undergo validation against previously encountered values. This approach safeguards effectively against potential attacks that aim to invoke the algorithm with invalid input or unmet preconditions.

The system specification has been enhanced with a subchapter addressing context, state, and input variables [Sw23b, Section 1.5]. This subchapter emphasizes to developers the importance of taking context variables from trusted sources. For certain algorithms in the specifications, we have included an overview which for each variable shows the source and the required input validation. Figure 3 illustrates this approach using the voter authentication algorithms.

2.2.4 Universal Verifiability and Importance of Consistency Checks

Haines et al. emphasized the significance of consistency checks and presented a possible attack on universal verifiability [HPT23c, Section 3.3.4]. The attack involved reordering shuffle payloads between different ballot boxes. To detect such an attack, the verifier needs to examine the consistency of file names associated with the payloads and compare them with

Information	Variable	Source	Use as	Preliminary Validation
Election Event ID	ee	Voting Client	Context	Check that ee exists in the internal view.
Authentication step	authStep	Voting Client	Context	Check that the authentication step is consistent with the state of the vc_{id} .
Derived voter identifier	credentialID_{id}	Voting Client	Input	Check in the internal view that credentialID_{id} corresponds to a vc_{id} for this ee , that the corresponding ballot box is currently open, and that the vc_{id} is consistent with other information received from the voting client.
Derived authentication challenge	hhAuth_{id}	Voting Client	Input	None. Checked within algorithm 5.2.
Base authentication challenge	hAuth_{id}	Internal view	Input	None, since retrieved from the trusted internal view.
Authentication nonce	nonce	Voting Client	Input	None, other than the implicit domain checks.

Fig. 3: Table from the System Specification [Sw23b, Page 60] showing the context and input validation for the voter authentication algorithms.

the actual payload content. However, the Swiss Post verifier specification only informally described such checks, and the checks were not implemented with sufficient rigor in the code.

To address this concern, the verifier specification has been augmented with more than 40 authenticity and consistency pseudo-code algorithms. These algorithms provide detailed instructions for the verifier to conduct checks aimed at preventing potential attacks and inconsistencies. Further refinements of the verifier specification are planned. An example of such pseudo-code algorithms for consistency verification is depicted in Figure 4.

Verification 3.03 VerifyCCRChoiceReturnCodesPublicKeyConsistency

Input:

- The CCR Choice Return Codes encryption public keys (**pk_{CCR_j}**) included in the following files from table 2:
- Online Control Component Public Keys ▷ 1 per component
 - Setup Component Public Keys
-

Operation:

- 1: **for** $j \in [1, 4]$ **do**
 - 2: $ok_j \leftarrow$ the CCR Choice Return Codes encryption public keys for control component j are identical from both sources
 - 3: **end for**
-

Output:

\top if all keys are identical, \perp otherwise.

Fig. 4: Pseudo-code algorithm from the verifier specification [Sw23c, Page 19] for one of the consistency verifications.

3 First Productive Election Event

The Swiss Post Voting System, incorporating individual and universal verifiability, was utilized for the first time during the election event on 18 June 2023. The e-voting system was used exclusively for a specific electorate in the cantons of Basel-Stadt, St. Gallen, and Thurgau.

The initial election event was considered a success by the involved cantons and by Swiss Post, with several positive indicators.²⁰ The open-source verification software successfully verified the correctness of the results, the level of support requests from voters remained low, and the adoption of e-voting demonstrated a high rate.

3.1 Involved Electorate and Participation

In Switzerland, the cantons possess the authority to determine the portion of the electorate eligible to utilize e-voting, provided they adhere to the Federal Chancellery's Ordinance [FC22], which stipulates a maximum limit of 30% of the cantonal electorate and 10% of the national electorate for e-voting participation.²¹ For the first productive election event, the cantons chose to offer e-voting to the following segment of the electorate:

- *Basel-Stadt*: Swiss citizens residing abroad and voters with disabilities.
- *Thurgau*: Swiss citizens residing abroad.
- *St. Gallen*: Swiss citizens residing abroad and voters from five pilot municipalities.

A total of 64,869 voters were eligible to vote online in the three cantons. However, voters with disabilities and those from the pilot municipalities are not automatically granted the option to vote online. Instead, they must explicitly register for this service, which adds an additional hurdle to the process. Out of the eligible voters, a total of 4,239 chose to cast their votes online.

²⁰ A successful premiere for Swiss Post's e-voting system: <https://post-medien.ch/en/a-successful-premiere-for-swiss-posts-e-voting-system/>

²¹ The info page of the cantons explains these requirements in detail (available in German): <https://www.evoting-info.ch/themen/politik-gesellschaft/e-voting-in-der-schweiz.html>

Table 3 shows the participation in the election event on 18 June 2023 in the cantons of Basel-Stadt and Thurgau.

Description	Basel-Stadt	Thurgau
Eligible Citizens	9,883	4,885
Mail-in/on-site ballots	1,208 (46.5%)	520 (43.8%)
Electronic votes	1,388 (53.5%)	667 (56.2%)
Votes cast in total	2,596 (100%)	1,187 (100%)

Tab. 3: E-voting participation for the cantons of Basel-Stadt and Thurgau in the voting event of 18 June 2023. The numbers originate from the statistics published by the Federal Chancellery [FC23a].

Notable is the high adoption rate of e-voting for the Swiss citizens residing abroad, clearly shown in the cantons of Basel-Stadt and Thurgau. Respectively, 53.5% and 56.2% of the citizens who were eligible for e-voting and chose to cast a vote in the election, chose to do so electronically.

The adoption rate for Swiss residents in the pilot municipalities of the Canton of St. Gallen is challenging to interpret due to the registration process required for online voting. Slightly more than 10% of the citizens who had the potential to register for e-voting and chose to cast a vote in the election, opted to both register and cast their votes electronically.

Worth mentioning is that the total mail-in and on-site ballots in Basel-Stadt, St. Gallen, and Thurgau all included invalid votes, whereas for the e-voting channel an invalid vote is not possible, since the voter portal only allows voters to submit valid votes.

3.2 System Deployment and Security Measures

From mid-May until 17 June, the electronic ballot boxes remained accessible to voters. To ensure seamless operation of the e-voting channel, Swiss Post employs a robust infrastructure, implements restrictions on system modifications, and proactively monitors the system for anomalies. The infrastructure documentation emphasizes key elements of the deployment, including redundancy, access controls, and a layered infrastructure that offers multiple lines of defense against diverse types of attacks.²²

Throughout the election event period, the system's load remained within normal levels. Additionally, we also monitored the system for any anomalies that might be observed during the election event's execution. Possible anomalies encompass various scenarios, such as:

²² Infrastructure documentation on GitLab: <https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Operations>

- Unforeseen errors or exceptions occurring in the server backend.
- Excessive utilization of system resources.
- Non-responsiveness exhibited by system components.
- A significant number of failed logins, either originating from the same IP address or in total.
- Lack of successful logins and submissions of votes.
- Substantial quantities of blocked suspicious requests by the web application firewall.
- Unusually elevated traffic levels, suggestive of a potential distributed denial-of-service (DDoS) attack.

The election event proceeded smoothly, with only a minor incident occurring during the voting period when the message broker component experienced a temporary outage. The monitoring system detected the issue and alerted Swiss Post operations, who resolved it within minutes. Although the problem was addressed effectively, there was some ambiguity regarding the communication channels, specifically regarding the responsibility of informing the cantons. As a result of the incident, a few voters encountered difficulties in submitting their votes and reported the issue to the cantonal support hotline, which was initially unaware of the outage.

In the subsequent after-action review of the incident, Swiss Post recognized the need for clearer and more proactive communication with all stakeholders, even in the event of minor incidents. Therefore, we made enhancements to the communication process, aiming to ensure that all relevant parties are informed promptly of potential similar incidents in the future.

During the final week of the election event, the Swiss federal government, along with certain cantonal and municipal governments and state-affiliated companies such as Swiss Post and the Swiss Federal Railways, fell victim to a distributed denial-of-service (DDoS) attack orchestrated by the Russian hacker group known as *No Name*.²³ The Swiss Post Voting System was not on the hacker group's target list and remained accessible throughout. Nevertheless, these attacks served as a reminder of the criticality of robust defense mechanisms against DDoS attacks. Additionally, it emphasized the significance of informing voters about the importance of casting their votes earlier in the election event period, rather than waiting until the final days.

²³ Information from the Federal Council about the DDoS attack: <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-95641.html>

3.3 User Experience and Feedback

Before the inaugural election event, rigorous testing was conducted on the user interface of the Swiss Post Voting System, resulting in its certification for accessibility level AA²⁴ according to the Web Content Accessibility Guidelines (WCAG) 2.1.

However, it was during the first productive election event that the system faced its true trial, enabling Swiss Post to observe the system's behavior and the frequency of support inquiries in the three participating cantons.

An essential metric that Swiss Post monitored was the ratio of submitted votes to confirmed votes within the Swiss Post Voting System. The Swiss Post Voting System uses a two-round return code scheme. First, the voter submits their vote and verifies the correctness of the received Choice Return Codes. Secondly, in order for their vote to be counted, the voter confirms their vote by entering the Ballot Casting Key and verifies the correctness of the received Vote Cast Return Code. It is, however, possible for the voter to abandon the process before confirming their vote and opt for an alternative voting channel. It could be expected that the occurrence of such instances is minimal. A higher percentage of unconfirmed votes would suggest voter confusion, forgetfulness in confirming their vote, or, worst-case scenario, potential manipulation by a deceptive voting client. For this first productive voting event, 99.5% of voters who submitted their vote also proceeded to confirm it. This number aligns with our past experiences with the Swiss Post e-voting system used from 2016 to 2019.

Furthermore, we conducted an analysis of the support requests that the cantons received from voters, examining both their quantity and nature. Encouragingly, the number of support requests remained relatively low, and no support request raised concerns of a potential attack, such as a voting client failing to display the expected return codes. Instead, most support requests pertained to confusion regarding the voting process or browser compatibility issues. For example, there were instances where voters mistakenly confused the start voting key, which needs to be entered into the voter portal, with the voting card identifier. In other instances, voters typed the voter portal's URL into the Google search engine instead of the browser's address bar. Additionally, some voters experienced confusion towards the end of the voting process. Specifically, the voter portal redirected them to the login screen after the voting process ended, leading to uncertainty regarding whether the process had been successfully completed. A very small fraction of voters experienced problems with older versions of iOS and the browser Safari. In response to some of the support requests, Swiss Post has acknowledged the need for targeted enhancements to the voter's user interface, to minimize confusion and enhance the clarity of the voting process.

²⁴ Access for all: <https://access-for-all.ch/leistungen/zertifizierung/zertifizierte-websites/>

4 Conclusions

Multiple rounds of independent examination have led to significant improvement in multiple aspects of the Swiss Post Voting System. The improvements encompass all parts of the system: the source code, specification documents, the computational and symbolic proofs. The independent examination rounds in 2021–2023 was an intensive period for Swiss Post, but the effort paid off with the increased quality of the system and the authorization obtained for the relaunch. Furthermore, the continuous activity of the bug bounty program is an indicator that the transparency measures put in place are working.

On 18 June 2023, the Swiss Post Voting System with individual and universal verifiability was used for the first time in a productive election event. Despite the system’s inherent complexity involving the user having to input and verify multiple code types, users were able to navigate the voting process with minimal difficulties. The operation of the system proceeded without encountering any significant issues.

Security is a process, and we will continue working on improving the quality of the Swiss Post Voting System. The Federal Chancellery’s catalogue of measures outlines the planned improvements and enhancements and specifies the deadlines by which they must be incorporated into the system [FC23b]. Now we are looking ahead to further productive voting events and examination rounds, while ensuring active engagement with the community of security researchers. Our focus remains on increasing security for online voting and continuously enhancing the Swiss Post Voting System.

References

- [Ad23] Adamiste, Stephane: Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider – Round 2. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [AFD22] Adamiste, Stephane; Fontes, Antonio; Domingues, Sergio Alves: Examination of the Swiss Internet Voting System Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [AO23a] Adamiste, Stephane; Oechslin, Philippe: Examination of the Swiss Internet Voting System, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the Abraxas print office. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [AO23b] Adamiste, Stephane; Oechslin, Philippe: Examination of the Swiss Internet Voting System, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the Baumer print office. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

- [AO23c] Adamiste, Stephane; Oechslin, Philippe: Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the canton. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Ba22] Basin, David: Review of Symbolic Proofs for Swiss Post’s Voting System. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Es22] Essex, Alexander: Analysis of the Swiss Post e-Voting System, Audit Scope 1: Cryptographic Protocol. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Es23a] Essex, Alexander: 2022 Re-evaluation of the Swiss Post e-Voting System (Addendum), Audit Scope 1: Cryptographic Protocol. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Es23b] Essex, Alexander: 2022 Re-evaluation of the Swiss Post e-Voting System (Addendum II), Audit Scope 1: Cryptographic Protocol. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Es23c] Essex, Alexander: 2022 Re-evaluation of the Swiss Post e-Voting System. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [FAD22] Fontes, Antonio; Adamiste, Stephane; Domingues, Sergio Alves: Examination of the Swiss Internet Voting System Audit scope 2a: Development process. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [FC22] FCh Swiss Federal Chancellery: Federal Chancellery Ordinance on Electronic Voting (OEV), 01 July 2022. 2022. Available at <https://www.fedlex.admin.ch/eli/cc/2022/336/en>.
- [FC23a] FCh Swiss Federal Chancellery: Eckdaten zum Einsatz der elektronischen Stimmabgabe am 18. Juni 2023. 2023. Retrieved on 2023-07-10 from <https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Eckdaten%20Versuch%2018.06.2023.pdf.download.pdf/Eckdaten%20Versuch%2018.06.2023.pdf>.
- [FC23b] FCh Swiss Federal Chancellery: Vote électronique - Catalogue of mesures by the Confederation and cantons, 4 August 2023. 2023. Available at <https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsuebersicht.html>.
- [Fo22] Ford, Bryan: Auditing the Swiss Post E-voting System: An Architectural Perspective. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Fo23] Fontes, Antonio: Examination of the Swiss Internet Voting System, Audit scope 2a (development process), Follow-up audit (round 2). 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Ha19] Haenni, Rolf: Swiss Post Public Intrusion Test: Undetectable attack against vote integrity and secrecy. 2019.
- [Ha20] Haines, Thomas; Lewis, Sarah Jamie; Pereira, Olivier; Teague, Vanessa: How not to prove your election outcome. In: 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020.

- [Ha22a] Haenni, Rolf; Koenig, Reto E; Locher, Philipp; Dubuis, Eric: Examination of the Swiss Post Internet Voting System, Scope 1: Cryptographic Protocol. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Ha22b] Haenni, Rolf; Koenig, Reto E; Locher, Philipp; Dubuis, Eric: Examination of the Swiss Post Internet Voting System, Scope 2: Software. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Ha23] Haenni, Rolf; Koenig, Reto E; Locher, Philipp; Dubuis, Eric: Re-Examination of the Swiss Post Internet Voting System, Scope 1 “Cryptographic Protocol” and Scope 2 “Software”, Version 1.0.2. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [HPT22] Haines, Thomas; Pereira, Olivier; Teague, Vanessa: Report on the Swiss Post e-Voting System. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [HPT23a] Haines, Thomas; Pereira, Olivier; Teague, Vanessa: Addendum on the Swiss Post e-Voting System. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [HPT23b] Haines, Thomas; Pereira, Olivier; Teague, Vanessa: Second Addendum on the Swiss Post e-Voting System*. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [HPT23c] Haines, Thomas; Pereira, Olivier; Teague, Vanessa: Examination Report on the Swiss Post e-Voting System. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [Kr22] Krähenbühl, Cyrill; Wyss, Marc; Burkhard, Robin; Wanner, Joel; Perrig, Adrian: Swiss Post E-Voting Scope 4: Network Security Analysis. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [LHK19] Locher, Philipp; Haenni, Rolf; Koenig, Reto E: Analysis of the cryptographic implementation of the swiss post voting protocol. 2019.
- [M’11] M’Raihi, David; Rydell, Johan; Pei, Mingliang; Machani, Salah: TOTP: Time-Based One-Time Password Algorithm. In: RFC 6238, <https://www.rfc-editor.org/info/rfc6238>. RFC Editor, 2011.
- [MO21] Monnat, Xavier; Oswald, Simon: The challenges of enabling public scrutiny. In: Electronic Voting (E-Vote-ID). Springer, 2021.
- [Oe23] Oechslin, Philippe: Security audit of the e-voting back-end. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [OH23a] Oechslin, Philippe; Hofer, Thomas: Code review of the Data Integration Service. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [OH23b] Oechslin, Philippe; Hofer, Thomas: Code Review of Voting Card Printing Service. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

-
- [OH23c] Oechslin, Philippe; Hofer, Thomas: Code Review of Voting Stimmunterlagen Offline. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [RBS23] Radomirović, Saša; Boureanu, Ioana; Schneider, Steve: Review of the Symbolic Proofs for the Swiss Post Voting System's Cryptographic Protocols. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [SC22] SCRT SA: E-VOTING WEB APPLICATION, SECURITY AUDIT REPORT. 2022. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [SC23] SCRT SA: E-VOTING WEB APPLICATION AUDIT, SECURITY AUDIT REPORT. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [SMM17] Stefanelli, Raffaele; Morel, Denis; Monnat, Xavier: A secure e-voting infrastructure. Implementation by Swiss Post. In: E-Vote-ID 2017. TUT Press, 2017.
- [Sw22] SwissPost: Swiss Post's reports in response to the expert reports. 2022. Available at <https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Reports/Examination2021>.
- [Sw23a] Swiss Post: E-Voting Architecture Document. 2023. Available at https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/System/SwissPost_Voting_System_architecture_document.pdf.
- [Sw23b] Swiss Post: Swiss Post Voting System. System Specification. Version 1.3.1. 2023. Available at <https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/System>.
- [Sw23c] Swiss Post: Swiss Post Voting System. Verifier Specification. Version 1.4.1. 2023. Available at https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/System/Verifier_Specification.pdf.
- [Sw23d] SwissPost: Response to examination reports launched by the federal government. 2023. Available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.
- [TP19] Teague, Vanessa; Pereira, Olivier: Report on the SwissPost-Scytl e-voting system, trusted-server version. 2019.

French 2022 legislatives elections: a verifiability experiment

Véronique Cortier¹, Pierrick Gaudry¹, Stéphane Glondou¹, Sylvain Ruhault²

Abstract: For the 2022 legislative elections, France made use of Internet voting for a fraction of its voters, namely French voters from abroad. For the first time, France introduced the notion of verifiability and third party. We report here the role of the third party, its interaction with the ANSSI, what it meant in terms of verifiability, as well as its limitations.

1 Context

Verifiability is a key property in electronic voting. It requires first a public and detailed specification of the system, as well as means for voters and observers to check that the result properly reflects the votes of the voters. Most academic protocols are verifiable by design, such as Helios [Ad08], Belenios [CGG19], Selene [RRI16], JCJ [JCJ05, CCM08], or Select [Kü16], just to cite a few ones. However, the deployment of verifiable electronic voting in politically binding elections is still an ongoing work in many countries. Switzerland is probably the country that has the most demanding regulation [Ord13], with public specification, open source code, cast-as-intended property, proxy-verifiability, and formally proved protocols. Estonia also relies on a system that offers proxy-verifiability and a cast-as-intended mechanism [HW14], with several associated publications that provide information about the system in use and its limitations [Mu22, SHR23]. Australia also tried to use a somewhat verifiable system, with some cast-as-intended property but at the price of a privacy loss since voters could hear confirmation of their vote by phone [HT15].

France makes use of Internet voting in its political elections only for the Legislative and Consulate elections, and only for the French voters from abroad. We focus here on legislative elections. Internet voting was offered in 2012 and was about to be used in 2017 but finally aborted a few months before the election. The last election for the French parliament happened in 2022, with a total of 577 deputies, out of which 11 deputies are elected by the French from abroad. These 11 deputies can be considered as a small proportion of the French parliament but this is still a high number, especially given the small margin between each party.

The Legislative election is run in two rounds: the first round selects the two (or three) candidates with the most votes and the second round determines the winner between the remaining candidates. Each deputy is elected by voters from a specific geographical area,

This work received funding from the France 2030 program managed by the French National Research Agency under grant agreement No. ANR-22-PECY-0006.

¹ Université de Lorraine, CNRS, Inria; Nancy, France

² Agence Nationale de la Sécurité des Systèmes d'Information; Paris, France

called *district* (*circonscription*, in French). Voters from abroad are offered three means for voting:

- in person voting: voters attend physical voting stations, typically in consulates. Of course, this may represent a long distance for voters, hence only 22.6% voters voted physically³.
- postal voting: voters receive their voting material by post, choose their preferred candidate and return their ballot by post. 0.4% voters used postal voting in 2022.
- Internet voting: voters can vote from any place, using their own voting device (smartphone, computer, tablet). This was the preferred mode of voting with 77% voters using Internet voting, with a total of more than 230 000 votes in the first round, and 270 000 in the second round [Res22].

The election is organized by the MEAE, the French ministry for Europe and foreign affairs. The ministry had a contract with the Docaposte Voxaly company for the Internet voting part, under the technical supervision of ANSSI, the French National Cybersecurity Agency. ANSSI was advising the MEAE for the definition of the desired level of security, as well as during the whole development process and during the deployment phase.

French Internet elections are mainly shaped by an independent entity, CNIL (Commission nationale de l'informatique et des libertés), in charge of protecting data privacy. Since 2019, CNIL has introduced the notion of verifiability in its regulation [CNI19]. For the highest level of security, it requires that the Internet voting system “makes the ballot box transparent to all voters using third-party tools”. This notion of transparency and of third party are not precisely defined in the CNIL recommendations but the CNIL clarified that a “third party” should be outside both the Ministry (MEAE) and the company (Docaposte Voxaly) and should develop its own tool.

In 2021, and on behalf of the MEAE, ANSSI approached academic researchers to act as third party to offer some form of verifiability. The present article has been written by the 3 academic researchers forming the third-party (the first 3 authors) and a member of ANSSI (the 4th author). The 4th author is therefore not part of the third-party. As a member of ANSSI, his role was to offer technical and scientific support to the MEAE, and to assist them in the discussions with the company and with the third-party. In this paper, we describe the role of the third party, what it meant in terms of verifiability and its limitations. The election was run in May and April 2022. However, among the 11 elections, 3 of them were finally canceled early 2023. One cancellation is due to a fraud that is independent from the voting system [Dec23a], the two other ones are due to major technical malfunctioning: for example in the 2nd district, only 11% voters had received their password at the opening of the voting phase, only 38% at the end of the voting phase [Dec23b]. Hence the three elections were re-run in March and April 2023 and with again a third party, and some new findings.

³ The figures are given for the first round of the election. They are similar for the second round.

2 Overview of the voting system

The voting system has a basis that is inspired by Helios [Ad08], with the notable difference that the bulletin board is not public.

During a setup phase, an encryption key is constructed, and the corresponding decryption key is split in 14 partial decryption keys. For each partial key, a member of the electoral board (we called them a trustee) is in charge. A threshold mechanism is in place, so that 4 trustees are enough to decrypt. The resulting encryption key is a classical ElGamal public key, based on the Ed25519 elliptic curve.

During the voting phase, the voters use a Javascript client to authenticate, form their encrypted ballot, and send it to the server. The authentication is based on personal data and a password sent over two distinct channels. It is interactive, in the sense that no data is added to the ballot that could prove that it comes from a legitimate voter (similar to Helios, but unlike Belenios [CGG19]).

A ballot is composed of several ElGamal encryptions of bits, together with zero-knowledge proofs of well-formedness, *à la* Chaum-Pedersen. The server collects the ballots and put them in a database, with metadata indicating for which of the 708 precincts this ballot is for. A precinct is a subdivision of a district, that corresponds to a physical polling station. Both electronic and paper ballots are counted in each precinct and then aggregated to provide the results at the level of the district.

At the end of the voter's journey, they are invited to (but not forced to) perform verifiability steps. They can download a PDF file as a receipt ("Récépissé") that contains the following data:

- A hash of the ballot, with a few characters indicating the precinct.
- A signature of this information, using a signing key from the server.
- Another hash of the ballot (that seemed to be unused in the process).
- Links to web services where the data can be verified.

An example of a Récépissé is shown in Appendix.

In total, 3 verification services are linked on the Récépissé. Two of them are hosted by the same entity (the MEAE) as the voting server, which defeats the purpose of verifiability, at least in some threat models. The other one was offered by the third-party auditors, whose role is described more thoroughly in the next section.

The voting phase ends a few days before the day where voters can physically go to a polling station. Voters who have voted by Internet have their names removed from the voter list, and therefore can no longer vote at polling station.

Finally, at the end of the voting day, the trustees meet at the MEAE. At least 4 of them come

to an isolated machine and type a password that unlocks their share of the decryption key and partially decrypt the result. Zero-knowledge proofs of correct decryption are produced as well. More precisely, the technique of homomorphic tally is used. Therefore, the trustees do not decrypt individual ballots but only the results for each of the 708 precincts.

We can remark here that the management of the decryption keys is not fully decentralized, and that a single machine is used for all the trustees during decryption (the same is true during the setup).

3 The role of the third-party auditors

The first role of the third-party auditors was to *define* with the MEAE what is the role of a third party. With the help of the ANSSI, they obtained an agreement on three transparency principles:

1. All the documents used for understanding the system and writing the third-party code will ultimately be made public, before the election. This is not as transparent as a fully public system specification but a partial specification of the voting system is now available [Spe22]. This was the first time in France.
2. As third party, no NDA was signed but instead a responsible disclosure clause, that let 90 days to the MEAE and Docaposte Voxaly to fix an issue before publication. The notion of responsible disclosure was new to the ministry and the company in this context.
3. The third party was given access to the ballot box, that is the set of the encrypted ballots. These ballots were treated as confidential material and destroyed a few weeks after the election, as requested by regulation. As a compromise towards a public bulletin board, the third party obtained however the right to publish the hash of each ballot of the ballot box, so that each voter could directly check that their ballot was counted.

Then their role was divided in two main steps:

- some sort of individual verifiability, during and after the election;
- some sort of universal verifiability, after the election.

A webpage⁴ (in French, of course) describes the role of the third party to voters, and also gave access to the verification tool and services.

⁴ <https://verifiabilite-legislatives2022.fr/>

3.1 Verifying the tally

The system has no public bulletin board. However the list of ballots, the decryption results, and the associated zero-knowledge proofs form a data set that allows to verify that the results that are claimed on the web site of the MEAE correspond to the list of ballots.

After the tally, the third-party auditors received the aforementioned data, together with the setup information (list of the precincts, list of candidates for each legislative district, the 14 partial public keys). Based on the public documentation that describes the format of the ballots, a command-line tool was written to perform the following operations:

- Check the consistency of the partial public keys;
- Check the validity of the zero-knowledge proofs in each ballot;
- Compute the homomorphic composition of the ballots, for each precinct;
- Check the validity of the zero-knowledge proofs for the decryption;
- Check (manually) that the result corresponds to what is announced on the official web site of the Ministry, at the district level;
- Compute the list of hashes of the ballot, exactly as they should appear on voter's Récépissé;
- Publish this list, and a report on all the checks.

This verification tool, called VVFE, is made publicly available as a git repository⁵, under a free software license. Even though the voters or external auditors can not run this code themselves, since the board is not public, this improves transparency and complements the specification.

The system is similar to Helios / Belenios, and the specification is actually close to that of Belenios, when it comes to the structure of the zero-knowledge proofs. Therefore, it was natural to start from the Belenios source code, and VVFE is a derivative of (part of) Belenios. At that time, Belenios did not have support for elliptic curves. It was using multiplicative groups of finite fields. Everything was in place to be able to switch from one group to another, and therefore adding elliptic curve support to VVFE was not too costly.

For efficiency reasons, on the server side, the Libsodium library was used for the critical function that does scalar multiplication on the Ed25519 curve. Bindings for this library in OCaml were added. The dedicated off-line machine that was used for the verification is a 10-core Intel i9-10900K. A single core of this machine can perform 12,000 elliptic scalar multiplications per second. The benchmark tool of VVFE allows to run a test with a fake election setup that includes 15 to 20 candidates per district, which is typical for the first round. With this setup, the whole election verification with 100,000 ballots takes 7 minutes and 56 seconds (using all available cores on the machine). It could be deduced that all the

⁵ <https://gitlab.inria.fr/vvfe/vvfe>

checks for the first round of the election could be done in about half an hour, which was indeed the case.

We remark that the elliptic curve code written for VVFE was integrated back into Belenios a few months after.

It was necessary to check manually that the results of each of the 11 districts correspond to what is announced on the official web site of the Ministry. For verifiability purposes, it would have been better to perform this check for each of the 708 precincts but of course, this is no longer possible manually. Unfortunately, automating these checks was not possible for these elections since even the format of the results varied from one precinct to another.

Lesson learned 1: *In order to obtain verifiability up to the detailed results provided to the public, it is necessary to develop an API or at least machine-readable results, while ensuring that voters and machines are reading the same data.*

3.2 Individual verifiability

During the election, the third party only had the server verification key. A service was offered to voters in order to check that the signature they received after voting (in their Récépissé) was indeed a valid signature from the Server. This forms a commitment from the system to the voters: if their signed ballot does not belong to the final ballot box, they hold a cryptographic proof that the Server misbehaved.

After the election, the third party were given the ballot box for each district. As mentioned earlier, the hash of each ballot was published so that voters can control that the ballot box contains their ballots. For usability reasons, a service was offered to allow voters to check that the hash appearing on their Récépissé was part of this set of hashes. The validity of the Server signature was also checked, although this was no longer necessary after the tally. Note that voters could also download the list of hashes from the third-party server and check directly that hashed ballot appeared inside.

This service was hosted on the webpage⁶. The underlying cryptographic code simply consists in a signature check and was also published as part of the VVFE tool. Figure 1 displays a screenshot of the online tool for verifying a ballot after the election.

4 Which verifiability properties are targeted?

In the MEAE terminology, the third-party auditors guaranteed individual and universal verifiability. With respect to the usual academic terminology, their role was more restricted. Note that the third-party auditors did not play any role w.r.t. vote secrecy.


⁶ The service was available from <https://verifiabilite-legislatives2022.fr/>, but is no longer active.

Vérifiabilité individuelle
Élections législatives partielles 2022 — Premier tour

En tant que tiers, nous avons eu accès à l'ensemble des bulletins dépouillés et nous avons vérifié qu'ils correspondent aux résultats de l'élection. Vous pouvez vérifier ici que votre bulletin a bien été compté dans votre circonscription.
 Le cachet apparaît sur le récépissé de votre bulletin.

[Plus d'information](#)

Veillez entrer le cachet de votre bulletin :



Copiez-collez votre cachet ici

[Mentions légales](#) [Assistance MEAE](#)

Fig. 1: Screenshot of the verification service for voters.

Individual verifiability. The system in use does not offer any cast-as-intended verification mechanism, hence the voting client has to be fully trusted. On the other hand, the system offers the usual recorded-as-cast property: a voter can check that their ballot belongs to the ballot box, thanks to the fact that the list of hashed ballots of the ballot box was published.

Universal verifiability. Since neither the ballot box nor the zero-knowledge proofs are public, the system cannot claim universal verifiability. Only the third-party auditors selected by the MEAE, could verify the zero-knowledge proofs. The process was not opened to other entities. Moreover, the system does not provide any form of eligibility verifiability: the Server has to be trusted regarding the fact that the ballots all came from legitimate voters. Third-party auditors can not check whether some ballots had been added.

In conclusion, we would say that the system offers recorded-as-cast verifiability and proxy tallied-as-recorded verifiability. This is true up to the attack found by Debant and Hirschi [DH23], as explained in Section 6.1.

5 Retrospective

5.1 During the development phase

The third-party auditors were hired at a late stage of the process (during Fall 2021, for an election running in June 2022). Furthermore, they first had to discuss with the MEAE and the ANSSI about their precise role.

A first difficulty came from the fact that the (partial) specification that was required to write an independent software was not stabilized. Details that would have been easy to figure out in an open-source setting were difficult to fill-in. An example of this situation is given by the byte-encoding of the various data that must be hashed in the zero-knowledge proofs (in the Fiat-Shamir setting). The encoding of large integers is not the same everywhere, and the field separator is not always the same character. The third party had access to a few test data, but when the check fails, the combinatorics of all possible plausible encoding choices was too large.

This sounds like a simple problem to solve: just ask the developers. This leads to a second difficulty: the third party did not have a direct communication channel with the developer team at Voxaly, and had to communicate via the project manager, who was very busy with other important issues, at this late stage of the project.

The general impression was that even at the last minute, the process was not yet fully settled and that there was room for mistakes on D-day. We give two examples of remaining imperfections that were mentioned to the MEAE but were not fixed, due to time constraints:

- The character encoding of the files that are sent to the third party varies. From one test to the other, or even, in the real election, from one round to the other, the same file is sometimes encoded in UTF-8, and sometimes in ISO-8859-1. This is visible in particular in the file that contains the general information about the election, with the names of the candidates that contain accents.
The VVFE software was made robust to this kind of change.
- For a given round of an election, the third party first receives the general information before the election starts, and then receives the ballots, after the election ends. These two transmissions both contain a file that describes the public key of the server that signs the ballots. During the 2023 elections, during the tests and at each round, the public key was wrong during the second transmission.
The third party decided to work around this, but failed to do so during the first round. This led us to observe the behaviour of the voters when verifiability failed. See Section 6.2.

Lesson learned 2: *Integration of verifiability should be done at the beginning of the process, in order to avoid a last-minute rush, that can lead to anomalies.*

5.2 Statistics

As explained in Section 3, a service was offered during the election in order for voters to check that their ballot has been counted. Before the tally, since the ballots were not yet known, it was only possible to check that their ballot was correctly signed by the server. After the tally, the service could check that their ballot was in the ballot box of their district. The MEAE offered a similar service, except that, since they were also hosting the voting

server, they also checked that the ballot was in the ballot box during the voting phase. Of course, in some threat models, having the same entity running the server and verifying the presence of ballots does not bring additional guarantee.

We report in Table 1 the number of verifications made by voters during the election (signature verif) and after the election (ballot verif), using the verification service. For comparison, we also give the figures provided by the MEAE service. No misbehavior from the server was detected during the verification, that is, no discovery of any correctly signed ballot that does not appear in the ballot box. We can note that there are much more visits of the verification page than the number of successful verifications. We see several explanations: voters (or even robots) may access the webpage and stop there. Moreover, the verification may fail due to bad copy-paste or simply voters playing with the interface.

	1st round	2nd round
# of votes	237379	273927
# of MEAE verifs	40148	37174
# of 3rd-party verif visits	3150	2064
# of 3rd-party successful signature verifs	603	324
# of 3rd-party successful ballot verifs	357	68

Tab. 1: Number of verifications made by voters during the 2022 French legislative elections. The last three lines report the usage on the third-party verification service. Signature verifications occur *during* the election, full ballot verifications occur once the election is tallied.

The main lesson learned is that very few voters successfully verified their ballot using the third-party service (less than 1%). Unsurprisingly, this is even lower if we count only the voters who returned after the election. In comparison, the MEAE service has a 17% verification rate⁷. Note that figures given by the MEAE may count the total number of accesses to their verification service (be it successful or not). The fact that the MEAE service was much more used than the third-party service could be explained by the fact that this service was the first proposed service on the Récépissé given to voters. It was probably hard for voters to understand why it would be meaningful to verify their ballot twice. This gives some hope that a third party could be much more used if better advertised. Note that anyway, the MEAE service provides less guarantee in the sense that if the service is trusted for verifiability then it should also be trusted to keep the received ballots.

Lesson learned 3: *Very few voters used the third-party service. But a better publicity could make a big change. Why not having the third-party service(s) be the only one(s) pointed to voters, or at least be the one(s) publicized in priority?*

One can also notice that voters verified less during the second round, while the participation

⁷ All the figures from the MEAE service have been provided by the MEAE to the third party.

was similar (even slightly higher). This may come from the fact that voters were reassured by their verification during the first round and did not see the point of verifying again during the second round.

6 Verifiability issues

6.1 The attack of Debant and Hirschi

The verification service assumes that the voting client is honest. This was made clear to voters on the third-party website. However, the third-party auditors implicitly assumed that the behaviour of the voting client was close to the behaviour of the Helios or Belenios voting clients. Debant and Hirschi [DH23] performed some reverse-engineering of the voting client and discovered that the hash of the ballot was sent back and forth between the voting client and the Server, leading to the following flaw: the voting client did not check that the hash of the ballot displayed to the voter was the one corresponding to the actual ballot of the voter. Moreover, the *Récépissé* (a pdf) offered to the voter was entirely generated by the Server, with no check from the voting client. Hence a dishonest Server could easily drop the voter's ballot and send a (valid) *Récépissé* for another ballot, encrypting a vote of its choice. Note that the paper from Debant and Hirschi [DH23] also reports flaws w.r.t. ballot secrecy, that we do not discuss here.

Lesson learned 4: *A partial specification is unsafe. At the very least, the specification of all trusted components should be provided.*

Lesson learned 5: *Publishing a specification a few weeks before the election is risky. In case flaws are discovered, there is no time to fix them.*

Of course, all the flaws reported in [DH23] need to be corrected.

6.2 Rerun in 2023

The results of legislative elections were canceled in three districts, hence the election was re-run in March and April 2023 for these three districts, with again a third-party auditor. The setting was very similar, with two main differences, from the verifiability point of view.

First, the attack from Debant and Hirschi [DH23] was fixed in the sense that the voting device now displays the hash of the ballot, *as computed by the voting device* as well as the hash received from the server. The voter is invited to check that the two hashes are equal (they are displayed on the same screen). However, the *Récépissé* is still generated by the Server. An informed voter can check that the same hash appears on the *Récépissé* but is not

instructed to do so. The voter is not instructed either to keep a copy of the hash displayed by its voting device.

Second, since very few voters return to the verification service after the election, it was decided to capture all valid signatures of ballots verified by voters during the election. It was then possible, after the election, to check that all verified ballots were present in the received ballot box. This way, voters do not need to come back after the election and their verification during the election is as powerful as the one after the tally.

We report in Table 2 the number of verifications made by voters. The number of verifications was again very low. No misbehavior from the server was detected.

	1st round	2nd round
# of votes	26667	28574
# verif visits	534	442
# of successful signature verifs	20	27
# of successful ballot verifs	3	2

Tab. 2: Number of third-party verifications made by voter during the 2023 French legislative elections. Signature verifications occur *during* the election, full ballot verifications occur once the election is tallied.

However, the verification service did not properly function w.r.t. the first round during 11 days after the election. Indeed, once the election is tallied, the third-party auditors received the ballots and checked that the results of the election correspond to the ballots, thanks to the zero-knowledge proofs. The set of hashes of ballots was then published on the third-party webpage. While uploading the set of hashes, the third-party auditors also wrongly updated the Server verification key with an invalid one, given by mistake by Docaposte Voxaly, as explained in Section 5.1. Hence, voters that verified their ballot of the first round after the election got an error message, saying that the signature was invalid, while this was not the case.

Interestingly, the analysis of the log showed that 18 voters (only) did encounter this error message. In principle, they should all have vigorously complain since their ballot was valid. Only 1 out 18 voters filled a form to complain. One week later, the complaint was correctly identified as a signature issue and the third-party auditors were notified. They fixed the incorrect verification key one hour later.

Lesson learned 6: *Voters do not complain! This unfortunate real-life experiment shows that verifiability is not enough. Even when voters are in position to detect a potentially severe issue, they do not complain.*

7 Conclusion

The French 2022 legislatives introduced the notion of verifiability for the first time in France, for politically binding elections. Verifiability was still limited: no cast-as-intended nor eligibility verifiability. However, third party auditors could check the tallied-as-recorded property and offered individual verifiability to the voters, up to the attack found by Debant and Hirschi [DH23], partially fixed in 2023. Moreover, and for the first time, the specification of the system was made partially public. We believe that this 2022 election forms an important step towards full verifiability in France. We hope that this effort will be pursued and amplified in the next years.

We note that France made the choice of proxy-verifiability rather than universal verifiability. This is also the case in Switzerland and Estonia for example. It seems that election authorities of national elections are reluctant to publish the encrypted ballots because of a possible loss of vote privacy, in case decryption keys are lost, or in case a weak random generator is used on the voter side [Gj16]. On the other hand, in order to achieve full verifiability, publishing some data related to the ballots seems unavoidable. This data does not necessarily leak information about the voters and may even hide the votes in an information-theoretical way [CPP13]. What can be disclosed on a public board, for national political elections, will certainly continue to be discussed in the next years.

Bibliography

- [Ad08] Adida, B.: Helios: Web-based Open-Audit Voting. In: USENIX'08. pp. 335–348, 2008.
- [CCM08] Clarkson, M. R.; Chong, S.; Myers, A. C.: Civitas: Toward a Secure Voting System. In: IEEE Symposium on Security and Privacy (S&P'08). IEEE Computer Society, pp. 354–368, 2008.
- [CGG19] Cortier, Véronique; Gaudry, Pierrick; Glondou, Stéphane: Belenios: A Simple Private and Verifiable Electronic Voting System. In: Foundations of Security, Protocols, and Equational Reasoning: Essays Dedicated to Catherine A. Meadows. Springer International Publishing, pp. 214–238, 2019.
- [CNI19] CNIL recommandations. Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet, <https://www.legifrance.gouv.fr/jorff/id/JORFTEXT000038661239>.
- [CPP13] Cuvelier, Edouard; Pereira, Olivier; Peters, Thomas: Election Verifiability or Ballot Privacy: Do We Need to Choose? In: 18th European Symposium on Research in Computer Security (Esorics 2013). LNCS. Springer, 2013.
- [Dec23a] Décision n° 2022-5773 AN du 3 février 2023, <https://www.conseil-constitutionnel.fr/decision/2023/20225773AN.htm>.
- [Dec23b] Décision n° 2022-5813/5814 AN du 20 janvier 2023, https://www.conseil-constitutionnel.fr/decision/2023/20225813_5814AN.htm.

- [DH23] Debant, Alexandre; Hirschi, Lucca: Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol. In: Usenix Security. 2023.
- [Gj16] Gjølsteen, Kristian: E-voting in Norway. CRC Press, 2016. Chap. 5 in Real-World Electronic Voting: Design, Analysis and Deployment.
- [HT15] Halderman, J. Alex; Teague, Vanessa: The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In: 5th International Conference on E-Voting and Identity, VoteID 2015. LNCS. Springer, 2015.
- [HW14] Heiberg, Sven; Willemson, Jan: Verifiable internet voting in Estonia. In: EVOTE'14. IEEE, 2014.
- [JCJ05] Juels, A.; Catalano, D.; Jakobsson, M.: Coercion-Resistant Electronic Elections. In: Workshop on Privacy in the Electronic Society (WPES'05). ACM, pp. 61–70, 2005.
- [Kü16] Küsters, Ralf; Müller, Johannes; Scapin, Enrico; Truderung, Tomasz: sElect: A Lightweight Verifiable Remote Voting System. In: 29th IEEE Computer Security Foundations Symposium (CSF'16). pp. 341–354, 2016.
- [Mu22] Mueller, Johannes: Breaking and Fixing Vote Privacy of the Estonian E-Voting Protocol IVXV. In: Workshop on Advances in Secure Electronic Voting 2022. 2022.
- [Ord13] Ordonnance de la ChF sur le vote électronique (OVotE) du 13 décembre 2013 (Etat le 15 janvier 2014). Chancellerie fédérale ChF.
- [Res22] Élections législatives - Résultats du 1er tour pour les Français de l'étranger. <https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/resultats-des-elections/article/elections-legislatives-resultats-du-1er-tour-pour-les-francais-de-l-etranger>, Last visited on July 3rd 2023.
- [RRI16] Ryan, Peter; Rønne, Peter; Iovino, Vincenzo: Selene: Voting with Transparent Verifiability and Coercion-Mitigation. In: Voting'16. pp. 176–192, 2016.
- [SHR23] Sutopo, Anggrio; Haines, Thomas; Roenne, Peter: On the Auditability of the Estonian IVXV System and an Attack on Individual Verifiability. In: Workshop on Advances in Secure Electronic Voting 2023. 2023.
- [Spe22] MEAE – Vérifiabilité – Spécifications v1.0. https://www.voxaly.com/wp-content/uploads/VOXALY_LEG2022_Verifiabilite_Specifications.pdf.

A Example of a voter's Récépissé



Elections législatives 2022 1er tour



Preuve de dépôt du bulletin de vote dans l'urne

Voici la preuve de dépôt de votre bulletin dans l'urne.

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.

80011&1&3318f83ea80861c9e6274f049c8df87c2da4fe03e43b7aa46b7192c0cfc3129c53

[Pour contrôler la référence de votre bulletin : cliquez ici](https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte)
<https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte>

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

[Vous pouvez accéder à l'outil en cliquant ici.](#)

Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.



eyJpbmZvU1U0iOiI4MDAxMxwxfDF1cmVfQ21yY29uc2NyaXB0aW9uX2R1c19GcmFuY2Fpc19kZV9aJ2V0cmFuZ2VyfDEwOXwzMzE4ZjgzZWE4MDg2MmM5ZTYyYzRmMDQ5YzhkZjg3YzJkYTRmZTAzZTQzYjdhYTQ2YjcxOTJjMGNmYzNmMjIjFDEUz1IwiczNoNm9yci16IjFfaW5kaTV2OHQzMGs3NXZhb2htMWhic292aTclbGE5TWQ2cXBabmNodXlaajU5c2tub3RlMTRaDlVAM9Zccz8yM0cqdWRUOWJxZm3MDpFAMRpWwObTQzaZv4am5qG0GmNmFynWg4dC1sInB1Ym9pOTclwN1JjoiLS0tLS1CRUdJTi19WRVJRklDQVRJT05fS0VLS0tLS1c1c1xNzdmVW02TQ0YQWxzG14ZDkxMDg1MmQ4Y2U0ODNkNzc0YTMyYTZmOTNhMmRlYzRhNjRmNzhhMmMfJ2mI2NDJjOCUzNjYzNmVlNTUxMzY2OWJmZDE2YTdlYTNI2mMzY2Q1Nm3MDUyMzh1YzksOTFhNDMOM2QwZTgzOWVjNjM3OTVhXHJcbi0tLS0tRU5EX1ZFUk1GSUNBVE1PT19LRVktLS0tLS1sImNsZUNhY2hldE5jdXQ1O1IyOSJ9

[Pour contrôler le cachet électronique, cliquez ici](https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur)
<https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur>

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.

b4e49757a5ae4cf256e5466a5d7e04476b31186a89ba02773549e68524f81e1e

Voter Perception of Cast-as-Intended Verifiability in the Estonian I-Vote Protocol

Tobias Hilt,¹ Kati Sein,² Tanel Mällo,³ Jan Willemson,⁴ Melanie Volkamer⁵

Abstract: The internet voting protocol deployed at Estonian political elections was enhanced by cast-as-intended vote verifiability mechanism in 2013 to reveal manipulations of the vote casting device by using a second device (most likely a mobile device as it needs to be equipped with a camera). This paper studies voters' perception and comprehension of this mobile-device-based cast-as-intended verifiability mechanism. We conducted semi-structured interviews with 13 eligible voters who have cast an electronic vote at least once since the availability of this mechanism. While most participants were in favor of having the option to verify available, , most were not aware of the main purpose to verify. Instead, they, for instance, thought it was designed to check that they had not made a mistake while selecting a candidate or to verify one's vote was tallied as intended. Thus, our findings highlight the need for improved communication on cast-as-intended verifiability in order to enable informed decisions whether to verify or not.

Keywords: Cast-as-intended verifiability; Online voting; Voter perception; comprehension; Interviews

1 Introduction

With the escalating global population, the costs and complexities associated with traditional elections have intensified [HS14]. While certain advancements in this domain have yielded positive outcomes, there exist adverse consequences resulting from the malevolent activities of individuals or groups aiming to disrupt elections conducted through online platforms [Gi19, HT15]. Adversaries may possess the capability to manipulate individual vote casting devices such as laptops or smartphones, as well as the online voting platform or parts of it, thereby enabling the replacement or elimination of votes – without voters or anyone noticing it.

One possibility to address this issue would be giving the voter an option to check that his/her vote was tallied the way he/she intended to (sometimes also called *end-to-end* (E2E) verifiability). Such a proof is difficult as a strong proof of vote integrity, might be used in coercive scenarios and for vote selling. While several research proposals for E2E secrecy ensuring verifiability exist, in practice, i.e. for real elections, weaker forms are offered to

¹ Karlsruhe Institut for Technology, AIfB, Kaiserstr. 89, 76131 Karlsruhe, Germany tobias.hilt@kit.edu

² Cybernetica AS, Narva mnt 20, Tartu, Estonia kati.sein@cyber.ee

³ Cybernetica AS, Narva mnt 20, Tartu, Estonia tanel.mallo@cyber.ee

⁴ Cybernetica AS, Narva mnt 20, Tartu, Estonia jan.willemson@cyber.ee

⁵ Karlsruhe Institut for Technology, AIfB, Kaiserstr. 89, 76131 Karlsruhe, Germany melanie.volkamer@kit.edu

voters, e.g. voters can verify that their vote reached the vote collection server in an unaltered way (called *cast-as-intended* verifiability).

A form of cast-as-intended verifiability has been implemented in the Estonian voting system since 2013 [HW14]. Its aim is to reveal manipulations of the vote casting device with a second (mobile) device while assuming that not both devices are manipulated.

For any cast-as-intended verifiability mechanism to deliver its promise, it relies on three key assumptions: (1) voters indeed perform the verifiability steps, (2) they notice if their vote has not been cast as intended, and (3) they report the observed disturbance. All three assumptions have been challenged by user studies while the focus was on cast-as-intended verifiability mechanisms different from the one used in Estonia [Ac14, Ka11b, Ma18, WH09]. These studies have revealed that the complexity and unfamiliarity of the corresponding steps can easily prevent voters from performing the necessary steps correctly, or at all. Even if the voters observe some issues, they are not likely to report them, as they may believe that verifying was not possible due to their own mistakes as they have a wrong comprehension of the purpose of verifying their vote [Vo22, TVK22].

Ten years after the introduction of cast-as-intended verifiability in Estonia, we wanted to study voters' perception and comprehension of it. To do so, we opted for a qualitative approach – in contrast to most of the recent related studies on other voting systems which predominantly use quantitative research methods. This choice was influenced by two considerations: First, Estonia stands out for having actually applied an electronic voting system providing cast-as-intended verifiability. Therefore it is possible to gain insights into the perceptions and comprehension of individuals who have used the e-voting system in real life. Second, since this study is a pioneering endeavor in exploring the perception and comprehension of Estonian voters, a qualitative approach is deemed more effective in providing in-depth insights compared to a quantitative one.

The paper is structured as follows. We discuss our work in light of related work in Sect. 2, followed by some background information about Estonian elections and a short description of the <https://www.overleaf.com/project/649d876efde0a1310a0f47f2Estonia> online voting system in Sect. 3. We present our research questions in Sect. 4 and describe our used methodology in the following Sect. 5. Our results are presented in Sect. 6. Sect. 7 provides several points of discussion, and finally, conclusions are drawn and directions for future work are presented in Sect. 8.

2 Related work

Three distinct methodologies for the realization of cast-as-intended verifiability in electronic voting systems have gained traction.

The first methodology utilizes return codes, is currently employed in Switzerland and is advocated by sources such as Galindo et al. [GGP15]. Here, the voters are provided with a

sheet of codes via postal mail prior to the election. Once the vote is cast, a confirmation code is generated which the voter must cross-verify with the codes listed on the sheet received earlier.

The second methodology encompasses the Benaloh challenge, also referred to as the verify-or-cast approach, which is to be employed before the vote is cast [Be06].

The third methodology, exemplified by its implementation in Estonia since 2013, entails the use of an ancillary device for vote verification [HW14]. This involves the use of an autonomous verification tool that accesses the random seed used in vote encryption, and is able to decrypt the vote in a separate mobile device.

The first two methodologies, namely the Benaloh challenge and the return code approach, have been the subject of usability studies and suggestions for enhancements in usability have been posited [WH09, Ka11b, Ka11a, Ne14, Ac14, Ac15b, Ac15a, Ma18, Ma19, Ku20, Ma20, Ku21, Ku21, TVK22]. Additionally, a study juxtaposing both methodologies was undertaken [Ku19].

Scholarly attention has also been paid to the third methodology. Notably, Marky et al. [MKV18] conducted an investigative study employing a cognitive walk-through technique across the three methodologies. Though this did not encompass a user study, it involved the identification of presumptions regarding voter behavior as posited by the different systems, and used these assumptions as a benchmark for comparison. The return code methodology emerged superior, requiring the least amount of assumptions in terms of the number of assumptions necessitated. However, the authors did not study users' perception of any of the systems but only concluded that a system with less assumptions on voters' behavior may have advantages in terms of motivating voters to verify and have them making less mistakes.

A user study that assessed all three methodologies concerning their efficacy was conducted [Ma21]. This study concluded that the return code methodology fared the best, while the Benaloh challenge came in second. Thus, the focus was only on being able to detect manipulations. Furthermore, it is important to note that the study had certain methodological limitations, including the fact that participants had to rely on the voting system they suspected to be manipulated to report any perceived manipulations.

3 Background Information

According to the Estonian constitution, parliamentary elections take place on the first Sunday of March once every four years. In practice, this is the day of polling site in-person paper voting.

Estonian legislation allows for more than ten alternative ways of submitting a vote. In recent years, Internet voting has become the most popular channel. Alternative vote casting methods (including Internet voting) are mostly utilized during the advance voting period

which spans over approximately one week before the election Sunday. In 2023, for example, Internet voting was possible from February 27th until March 4th (with March 5th being the election Sunday).

In order to cast an electronic vote, the voter first has to download the voting application (available for Windows, macOS and Linux) from the election organizer's website. Once this software is installed and started, voters authenticate themselves by using their state-issued electronic ID. Afterwards, the list of candidates corresponding to the electoral district of the voter is displayed. Once voters make their choice, the selected candidate is then encrypted. The voter signs the corresponding cyphertext with the voter's electronic ID.

As the voter's device is not necessarily trustworthy and can attempt to change the vote (e.g. as a result of a malware attack), the voter can ensure the integrity of the vote by verifying it, within 30 minutes after casting the vote. This cast-as-intended verifiability enables the voter to query the voting server for the vote associated with their signature. Note that verifying the vote later than 30 minutes after casting is disabled to limit coercion attacks.

It was decided that one cannot rely on the (potentially malicious!) voting device, in 2013 the Internet voting system was adopted to provide cast-as-intended verifiability. Since 2013 voters can verify the integrity of their vote using a second smart device install a corresponding app. During the cast-as-intended verifiability step, the randomness used to encrypt voters' candidate as well as a unique vote reference is transferred from the voting application on the vote casting device to the app on the second device via a QR-code (see Fig. 1)⁶.

The cast-as-intended verifiability application queries the voting server based on the vote reference, downloads the signed and encrypted vote, and verifies this information by mainly taking the following steps: First, it checks the signature. After this check passes successfully, the application checks which candidate encrypted with the randomness provided in the QR Code matches the cyphertext (encrypted vote) which was received from the server. This candidate is display on the screen of the mobile device. Voters then need to check whether the displayed candidate is the one they intended to cast (see Figure 2).

A more elaborate description of the Estonian Internet voting and protocol of the cast-as-intended verifiability mechanism is described by Ehin et al. [Eh22].

4 Research Questions

In this study, we aimed to examine how i-voters in Estonia perceive and comprehend the step of cast-as-intended verifiability.

There is a regular survey conducted in Estonia after every election event covering about 1000 respondents [ES21]. We were able to access the survey results of 2023, and it turns

⁶ <https://www.valimised.ee/en/internet-voting/guidelines/checking-i-vote>, last accessed 12 September 2023



Fig. 1: The last page of the Estonian voting application displaying the QR code for vote verification. The text reads: **“Your choice has been taken into account.** If you want, you can change your e-vote by voting electronically again (until March 4th, 20:00). If you have voted electronically several times, the last vote will be counted. If you want to make sure that your vote reached the election server in an unaltered form, use the app called “EH kontrollrakendus” on an Android or iPhone smartphone, and scan the QR-code from the screen. You can do this for the duration of 30 minutes up to three times. **Please close the application. E-voting has not started yet. Right now this is a TEST E-VOTE and will not be counted at the real elections.”**

out that, according to this survey, 50% of the electorate is aware of the cast-as-intended verifiability option⁷. Among the i-voters the respective percentage was 68.3, and among the paper voters it was 41.8. Still, only 5.5% of the i-votes were actually verified.⁸ A natural question arises, *why do i-voters not verify their vote?*

Our working hypothesis is that the electorate is not aware of the rationale behind cast-as-intended verifiability. Therefore, we try to answer the following research question:

RQ1: [Comprehension] What do Estonian i-voters think is the purpose of cast-as-intended verifiability?

In 2020, Solvak studied the usage patterns of Estonian i-vote verifiers based on the voting log data and how these affect voter confidence towards the integrity of the election [So20].

⁷ The question, we consider is: "Kas Te teate, et 2023. aasta valimistel sai valija oma interneti teel antud häält kontrollida?" which can be translated to: "Do you know that during 2023 elections it was possible for a voter to verify his/her Internet vote?"

⁸ <https://www.valimised.ee/et/valimiste-arhiiv/elektroonilise-haaletamise-statistika>, last accessed 07 July 2023

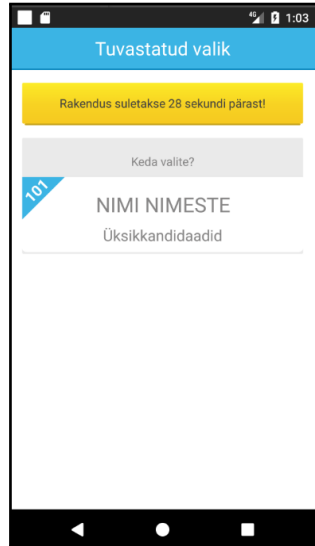


Fig. 2: Final screen of the cast-as-intended verifiability app. The text reads: “Identified choice. The application will be closed in 28 seconds. Whom did you choose? 101, Nimi Nimeste, Individual candidate”

However, the predefined multiple choice format of the questionnaire did not allow to dig deeper into the confidence building mechanisms. Thus, we extended the current study by setting the second research question.

RQ2: [Perception] How does the presence of cast-as-intended verifiability impact the perceived trustworthiness of the i-voting system?

5 Methodology

5.1 Recruitment

We required our study participants to meet one criterion: having cast an i-vote in Estonian elections at least once since 2013 (i.e. since the year cast-as-intended verifiability was introduced in Estonia). Participants were recruited through various channels: We made announcements to colleagues, friends, fellow Estonian researchers, and students of Tartu University. We also placed paper advertisements in public areas in Tartu city and its vicinity, and published advertisements on both LinkedIn and in the print version of *Maaleht*,⁹ an Estonian weekly newspaper with readership among rural and elder Estonians. We also

⁹ <https://maaleht.delfi.ee>, last accessed 07 July 2023

encouraged participants to disseminate the invitation among their acquaintances. It is important to note that no monetary or other forms of compensation were provided to participants.

Although in Estonia individuals aged 16 and above are eligible to vote in local municipal elections, no individuals under 18 volunteered for the study, so no parental consent was necessary.

5.2 Interview Procedure

We developed a semi-structured interview protocol to conduct the interviews. However, to facilitate clarity, participants were permitted to ask questions, which occasionally led to slight deviations in the interview process. Note, given the multilingual composition of the research team and the local execution of the study in Estonia, two language versions of materials were developed: First, study materials were developed and discussed in English. Later, the Estonian members of the research team translated it into Estonian.

We conducted one pilot interview in English to allow the entire research team to observe and identify areas for improvement. We identified some improvements in terms of wordings used in the interview protocol and altered it accordingly, e.g., changing the terminology from “check” to “verify” to accurately describe the process of verifying one’s vote. The final interview protocol is available online¹⁰. The main interviews were conducted in Estonian by the same interviewer. The interview procedure is illustrated in Fig. 3 and the individual parts are briefly explained below.

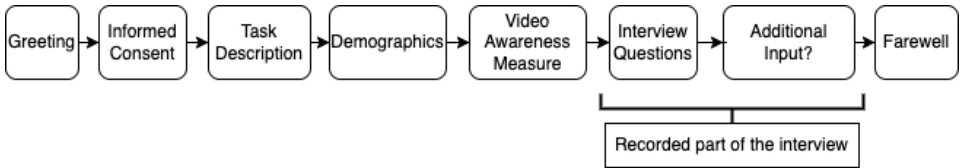


Fig. 3: Flowchart describing the various parts of the interview.

Informed consent & Task Description. If the participant had contacted the researchers via e-mail, the informed consent form was sent to them before the interview took place, detailing the scope of the research and the rights of the participants. The actual interview started with informing the participants of the nature of the research, their role in it and their rights. The participants were encouraged to ask questions if they had any.

In particular, participants were asked for permission to audio record the interview. The commencement and conclusion of the recording were explicitly confirmed with the participant.

¹⁰ https://secuso.aifb.kit.edu/downloads/documents/Interview_Guide.pdf, Last accessed 12 September 2023

Demographics. Participants were asked to specify their preferred gender and select the age ranges they fall into, with the options being 16-29, 30-39, 40-49, 50-59, 60-69, 70-79, and 80+.

Video Awareness Measure. Next, all participants watched a five-minutes video¹¹ to establish a common knowledge foundation. The video depicted a voter's perspective in a fictitious election, consisting of casting a vote and verifying this vote with a separate device and a corresponding app. The narrator of the video explained the process in real time in Estonian.

Interview Questions. At this point, the participants were informed that the recording was started. The interview questions encompassed both open-ended and multiple-choice formats. The interview consisted of 12 main questions, with several of them having detailed sub-questions to delve into specific nuances of the topic. For instance, a question concerning an imaginary scenario in which the voter detects that their vote was not cast-as-intended was used to examine the participants theoretical behavior in such a scenario. Therefore we asked them how they would react emotionally, what they would themselves do and what they would expect officials to do in such a situation. The complete interview guide is available online¹².

After an interviewee was asked how important they considered that the majority of voters verified their votes (Q7), they were explained the actual purpose and functionality of the cast-as-intended verifiability mechanism and why it was added to the Estonian i-voting system. Afterwards, some more questions were asked.

Once the participants answered all interview questions, they were offered the possibility to add information or opinions in case they felt something has remained without attention; or ask clarification questions from the interviewer. Then the recording was stopped and they were thanked for their help.

5.3 Data Analysis

The data from the interviews was processed and analyzed through a systematic approach. The recordings were transcribed using Kaldi Offline Transcriber for the Estonian language¹³. The outputs of the transcriber were edited by the interviewer to correct any speech recognition

¹¹ Version without voice but English subtitles of what was spoken on the video shown to the participants https://secuso.aifb.kit.edu/downloads/Videos/i-vote_Estonia2023_ENG_sub.mp4, last accessed 12 September 2023

¹² English version of the guide: https://secuso.aifb.kit.edu/downloads/documents/Interview_Guide.pdf, last accessed 12 September 2023

¹³ <https://koodivaramu.eesti.ee/taltechnlp/kaldi-offline-transcriber/-/tree/master>, last accessed 05 July 2023

mistakes and achieve intelligible verbatim transcription. An inductive coding approach was adopted for the analysis [Sa09, Th06]. Initially, each of the two coders individually reviewed four out of the thirteen interviews and devised codes to encapsulate the content. Following this, there was a group discussion within the research team. It was discerned that reviewing four interviews was insufficient to capture the entirety of the data, prompting the coders to analyze four additional interviews individually.

Separate codes were created for each question to maintain clarity and structure. The term “codebook” henceforth encompasses all these individual sets of codes. Following the analysis of the additional interviews, the coders convened to discuss their findings, culminating in the creation of an initial codebook encompassing all identified codes along with their definitions and criteria for application.

This initial codebook was then reviewed, discussed, and ratified by the entire research team. Subsequently, both coders independently re-applied this finalized codebook to all thirteen interviews. The coded data of both coders was then compared to determine discrepancies. The coders engaged in discussions to resolve these disagreements, primarily by clarifying any misunderstandings. The link to the final codebook is available online¹⁴

Once an agreement was reached on the final version of the applied codes, the data was analyzed using the software MaxQDA¹⁵, which facilitated the computation of the intercoder reliability coefficient Kappa, as outlined by Brennan and Prediger [BP81]. This process led to a substantial improvement in intercoder agreement, as measured by Brennan and Prediger’s Kappa, which increased from an initial value of $k=0.91$ to a final value of $k=0.99$ (as calculated across all interview questions), indicating near-perfect inter-rater agreement.

For the current analysis, the answers to the following questions were used. Q3, Q6, and Q7 were analyzed to answer RQ1, while Q9 and Q5 contributed to answering RQ2. The raw data collected as a result of the interviews actually allows to provide more insights. These insights will be covered in an upcoming extended version of the paper.

6 Results

In this section, we delve into the results obtained through the corresponding questions of the interview. For better readability, we summarize the process of performing cast-as-intended verifiability by using a dedicated app to verify one’s vote, as described in Sect. 3, in the following subsections by the term *verifiability step*. The section is structured along the research questions, while we start with some descriptive information about our participants.

¹⁴ <https://secuso.aifb.kit.edu/downloads/documents/Codebooks.pdf>, Last accessed 12 September 2023

¹⁵ <https://www.maxqda.com>, last accessed 07 July 2023

6.1 Interview Participants

The interviews engaged a total of 13 participants, from which three identified as male and ten as female. There was a considerable diversity in the age range of the participants, as detailed in Tab. 1.

Age range	16-29	30-39	40-49	50-59	60-69	70-79	80+
Number of participants	2	4	3	1	1	1	1

Tab. 1: Age range of participants

The interviews were thorough, with an average duration of 43 minutes per session, culminating in a total of 563 minutes of recorded content that was transcribed for analysis. Only two individuals had actually undertaken the step of verifying their vote in any of the elections since 2013. One of them succeeded and another one failed because of incomplete comprehension of the process (scanning the QR-code with an incorrect app).

6.2 Comprehension of the Cast-as-Intended Verifiability Mechanism

Various different interpretations were given in replies to the question about the purpose of the verifiability step (Q3): The interpretation from 12 out of 13 participants was related to various doubts and concerns associated with the voting process. These doubts included voter’s own performance during the voting process (e.g., a misclick while selecting the candidate), the voting-specific infrastructure (“system error”) as well as malfunctioning of infrastructure that is not specific to voting (e.g., incidental problems with the Internet connection).

Some answers were very abstract and, thus, leave room for interpretation: “[Verifying that] the vote has reached the server” was mentioned by seven participants. While this can be considered as partially correct comprehension of the mechanism, it leaves room for interpretation as it does not specify which potential problems are addressed and which server they had in mind (e.g. also the one tallying the votes which would then not be correct).

Two participants described the purpose of the verifiability step as detecting vote tampering but did not specify at which device (or maybe while send to the server) this could take place.

In addition, seven participants mentioned providing satisfaction for the voter’s need for proof and confidence, e.g. one of them sad that the verifiability step as such is specifically addressed to “people who like checking things”. Two participants expressed that the verifiability step cannot detect anything important and is only there to provide artificial confidence. Notably, we observed that nobody mentioned the possibility that the source of vote tampering could be the device used to cast the vote – the voter’s own computer which is the main purpose why the verifiability step was introduced in 2013.

In addition to the open-ended question (Q3), we use a multiple choice question to study participants comprehension of the verifiability step (Q6). Note, among the six choices presented¹⁶ only one was correct and the interviewees were informed that there is at least one correct answer.

We observed 12 out of 13 participants correctly identifying the correct answer (“My vote reached the vote collector server the way I intended to.”), however, four of them additionally picked a wrong one (“My vote is correctly tallied.”) and one declared that they cannot decide about the other two options about one’s individual vote.

Thus, seven out of thirteen participants demonstrated correct comprehension of the cast-as-intended verifiability mechanism when providing them a list of choices with one being the correct one.

The one participant, who did not select the proper choice, picked the option “My vote is correctly tallied.”, clearly indicating that more is expected from the verifiability step as it actually does provide.

In addition, we observed the participants perceiving the importance of verification differently, by asking them how important they deem the verifiability step to be taken by all i-voters (Q7).

Seven participants did not regard it crucial that voters verify their vote, two viewed it as somewhat important while four interviewees assessed it as very important. The reasons mentioned by those who considered it as very important justified it with statements like “fast detection of issues”, “demonstration of security of i-voting” or “increasing voter confidence”.

Those considering it as not important mentioned that it does not have an effect on the election results, and that the presence of verification option induces doubt. Two interviewees also expressed that the Estonian e-Government system is sufficiently secure even without the verifiability step.

One interviewee said that verifiability step is, in addition to failing to address the correctness of tallying, a waste of resources – electricity and time of voters and system developers – and as such should rather be avoided.

6.3 Perception - Impact of the Cast-as-Intended Verifiability Mechanism on Perceived Trustworthiness

Answering RQ2, one has to consider, that participants were explained the real purpose of the verifiability during the interview, as described in Sect. 5.2.

When questioned what a person with malicious intend could do if i-voters do not perform the verifiability step (Q3b), the interviewees expressed different comprehension. Six participants

¹⁶ Note, the choices were presented in a random order.

felt that the absence of the verifiability step would not necessarily make the system more vulnerable to malicious exploitation. The reasoning behind this belief was diverse, with three participants expressing faith in the inherent security of the system even without the verifiability step, and one surmising that an adversary with the capacity to compromise the voting system could equally circumvent the verifiability mechanism. It was also once stated, that ‘i-voting is logged and tempering would be detected using logs’. Additionally, one didn’t reason their decision, that an attacker could not do anything. While two interviewees expressed uncertainty, in total five interviewees stated potential malicious actions or exploits that could happen, if the verifiability step is not in place. Three interviewees believed that their vote could be tampered, without disclosing how exactly or at which point (e.g. on which device) this could take place. Vague expressions by two participants were captured using the codes “wider attack surface” and “voter coercion”. Important to mention is also, that four interviewees explicitly stated already earlier (Q3a), that the verifiability has no effect and especially does not increase trust for people who already mistrust the government or technology. E.g. one of the participants stated that “person who has doubt in the system would not have belief in scanning the/a QR code”. This again shows a wrong comprehension of the actual purpose of the verifiability step.

Presented with a hypothetical scenario in which the displayed vote (on the second device) would differ from the one they cast (on the vote casting device), they were asked what they would think and how they would feel in such a scenario (Q5a). Eight interviewees suspected technical error to be reason of the discrepancy between the vote they cast and the one they verified. The remaining five interviewees expressed suspicion and concerns, with two respondents suspecting system tampering and one suspecting bystanders. Eight participants also expressed doubt in their own performance and four that they would experience immediate negative feelings.

The participants were educated about the real purpose of the verifiability step before they were asked about the trustworthiness of the voting process (Q9b). Eight participants deemed the voting system more trustworthy with the verifiability step in place and four viewed the impact negligible¹⁷. Five interviewees expressed that the “additional control” enhances the credibility of the voting system. One interviewee addressed this enhanced credibility directly to the second device. Additionally, two interviewees reasoned, that the verifiability step is endorsed by security experts, which makes it trustworthy. When asked whether they would prefer a voting system with or without the verifiability step (Q9a), one participants expressed indifference and the rest of the participants expressing preference for a system with the verifiability step. Reasons for this preference that were mentioned at least once were the following: “increases trust”, “reduces scepticism”, “increases security”, “detection of technical errors”, “malware protection” and “preference for personal control”. The interviewee expressing indifference reasoned, that for them they would prefer the verifiability step to be available later in the election, such as shortly before tallying or a few days after the results have been announced¹⁸.

¹⁷ Note that in one of the interviews, we didn’t receive an answer to this question.

¹⁸ Note, this would be End-to-end verifiability.

7 Discussion

Our participants displayed a diverse comprehension by verbalizing what could be detected by performing the cast-as-intended verifiability step while all being very abstract, several misconceptions could be identified. In particular none of the participants noticed that the main purpose of the studied verifiability step is to enable voters to detect if their voting device is malicious (and changes their vote before encrypting it), given their second device is not malicious. When presented with multiple choices to describe the purpose of the verifiability step, nearly all participants were able to detect the correct choice. Important to highlight here is, that nearly half of them also picked an additional, wrong option or stated they were unsure about their decision. The fact, that nearly all were able to detect the correct option may be due to nature of the multiple choice question asked: six possible answers were given but only three distinct purposes were stated¹⁹, each having slight differences regarding the amount of votes under examination (my personal vote or all votes). By inspecting the choices one could deduct the obvious wrong answers and be left with fewer choices. This realization combined with the finding that nearly half of the participants also selected additional wrong options supports the conclusion, that the voters clearly lack comprehension of the real purpose of the verifiability step. Consequently, it is not surprising that only about a third of participants stated that the verifiability step is very important to be taken by all or most of the voters. Although nobody explicitly stated that they have changed their opinion after being exposed to education about the actual purpose of the verifiability step, nearly all expressed a preference of a voting system with the verifiability step in place and that such a system would be more trustworthy. This contrasts their prior assessment that somebody with malicious intent could do nothing in a voting system without the verifiability step. It shows that our participants themselves didn't had the right comprehension of the purpose of the verifiability step and therefore most likely regarded it as not essential. After being educated about the real purpose they seemed to attribute the verifiability step more importance and credibility, which could lead to a higher trustworthiness.

One important thing to mention is that several participants expressed high trust in the Estonian e-Government in general. It can be argued, that these people attribute less importance to the verifiability step itself because they trust the complete voting system with the verifiability step being part of it.

Preference for the availability to verify their vote shortly before tallying or after the election results has been announced was also mentioned. One of the reasons why some participants deemed the verifiability step unimportant was also that performing the step has no effect on the election result. This shows the insufficient comprehension of the purpose of the verifiability step once again, as these participants refer to end-to-end verifiability and not individual verifiability.

¹⁹ (1) Vote(s) reached vote collector server, (2) vote(s) are not altered on collector server until tallying and (3) vote(s) are correctly tallied.

7.1 Limitations

This research is subject to several limitations that should be considered while interpreting the findings. Firstly, the study's sample size, consisting of 13 participants, is small and therefore can not be considered as representative of the entire electorate in Estonia.

There is a possibility of self-selection bias, as participants voluntarily chose to be part of the study. The absence of monetary compensation could have deterred certain demographics from participating, further contributing to self-selection bias.

Another limitation is language and cultural factors, as the study was conducted in Estonian. Non-Estonian speaking residents who are eligible to vote were not represented in this study.

Thus, with a more representative sample even more misconceptions may occurred than those identified in our research.

Temporally, the study was conducted close to 2023 parliamentary elections, which could mean that the responses might have been influenced by the electoral atmosphere or recent political events, thus not reflecting long-term attitudes and comprehension.

Lastly, the qualitative nature of data collected through semi-structured interviews and its subsequent interpretation by the researchers could introduce subjectivity into the findings. The analysis of qualitative data is inherently interpretive, and the semi-structured format of interviews may have led to variations in the data collected.

8 Conclusion

The primary objective of this study was to examine voter perception and comprehension towards cast-as-intended verifiability in the Estonian online elections.

Our interviews revealed that several have noticed that there is something one can check, a number of misconception about the provided cast-as-intended mechanism as well as skepticism and diverse viewpoints concerning the criticality of the verification process (several did not view it as an essential component).

In conclusion, while being aware or at least not surprised about the option to check something, there is a need for explaining the purpose of the verifiability step. Currently, it is likely that voters cannot make an informed decision whether to verify or not due to their lack of comprehension of the purpose. The same holds for their perception whether or not the verifiability step increase the security or trustworthiness of the overall system. Currently, it is not surprising that some voters do not consider this step as necessary due to their lack of comprehension of its purpose.

Thus, we conclude that policymakers and election authorities should contemplate broader information campaigns to ensure that voters not only notice that there is something to check

but also understand its purpose; thus basically enable them to make an informed decision whether or not to verify.

Such campaigns should be carefully prepared to avoid causing distrust when starting explaining what the purpose is (but also what it is not for). We also recommend to accompany such information campaigns with research to study the impact on perception and comprehension, i.e. comparing it before and after the campaigns.

Acknowledgements

This paper has received funding from the Estonian Research Council under the grant number PRG920, from the project “Engineering Secure Systems” of the Helmholtz Association (HGF) [topic 46.23.01 Methods for Engineering Secure Systems], and by KASTEL Security Research Lab.

Bibliography

- [Ac14] Acemyan, Claudia Z; Kortum, Philip; Byrne, Michael D; Wallach, Dan S: Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. *The USENIX Journal of Election Technology and Systems*, 2(3):26–56, 2014.
- [Ac15a] Acemyan, Claudia Z; Kortum, Philip; Byrne, Michael D; Wallach, Dan S: From error to error: Why voters could not cast a ballot and verify their vote with Helios, Prêt à Voter, and Scantegrity II. *USENIX Journal of Election Technology and Systems*, 3(2):1–19, 2015. Publisher: USENIX.
- [Ac15b] Acemyan, Claudia Z.; Kortum, Philip; Byrne, Michael D.; Wallach, Dan S.: Users’ Mental Models for Three End-to-End Voting Systems: Helios, Prêt à Voter, and Scantegrity II. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, pp. 463–474, 2015.
- [Be06] Benaloh, Josh: Simple Verifiable Elections. *Electronic Voting Technology Workshop, EVT ’06*, 2006. Place: Berkeley, CA, USA Publisher: USENIX Association.
- [BP81] Brennan, Robert L.; Prediger, Dale J.: Coefficient Kappa: Some Uses, Misuses, and Alternatives. *Educational and Psychological Measurement*, 41(3):687–699, 1981.
- [Eh22] Ehlin, Piret; Solvak, Mihkel; Willemson, Jan; Vinkel, Priit: Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Gov. Inf. Q.*, 39(4):101718, 2022.
- [ES21] Ehlin, Piret; Solvak, Mihkel: Party Cues and Trust in Remote Internet Voting: Data from Estonia 2005–2019. In: *International Joint Conference on Electronic Voting*. Springer, pp. 75–90, 2021.
- [GGP15] Galindo, David; Guasch, Sandra; Puiggali, Jordi: Neuchâtel’s Cast-as-Intended Verification Mechanism. In: *International Conference on E-Voting and Identity (VOTE-ID)*. Springer, pp. 3–18, 2015.

- [Gi19] Giles, Martin: , US elections are still far too vulnerable to attack - at every level, 2019.
- [HS14] Harada, Masataka; Smith, Daniel M: You have to pay to play: Candidate and party responses to the high cost of elections in Japan. *Electoral Studies*, 36:51–64, 2014. Publisher: Elsevier.
- [HT15] Halderman, J Alex; Teague, Vanessa: The New South Wales iVote system: Security failures and verification flaws in a live online election. In: *International Conference on E-voting and Identity*, September 2–4. Springer, pp. 35–53, 2015.
- [HW14] Heiberg, Sven; Willemson, Jan: Verifiable internet voting in Estonia. In (Krimmer, Robert; Volkamer, Melanie, eds): *6th International Conference on Electronic Voting: Verifying the Vote, EVOTE 2014, Lochau / Bregenz, Austria, October 29–31, 2014*. IEEE, pp. 1–8, 2014.
- [Ka11a] Karayumak, Fatih; Kauer, Michaela; Olembo, M. Maina; Volk, Tobias; Volkamer, Melanie: User Study of the Improved Helios Voting System Interfaces. In: *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. IEEE, pp. 37–44, 2011.
- [Ka11b] Karayumak, Fatih; Olembo, Maina M.; Kauer, Michaela; Volkamer, Melanie: Usability Analysis of Helios-An Open Source Verifiable Remote Electronic Voting System. In: *EVT/WOTE. USENIX*, 2011.
- [Ku19] Kulyk, Oksana; Henzel, Jan; Renaud, Karen; Volkamer, Melanie: Comparing “Challenge-Based” and “Code-Based” Internet Voting Verification Implementations. In: *IFIP Conference on Human-Computer Interaction*. Springer, pp. 519–538, 2019.
- [Ku20] Kulyk, Oksana; Volkamer, Melanie; Müller, Monika; Renaud, Karen: Towards Improving the Efficacy of Code-Based Verification in Internet Voting. In: *VOTING*. Springer, 2020.
- [Ku21] Kulyk, Oksana; Ludwig, Jonas; Volkamer, Melanie; Koenig, Reto E.; Locher, Philipp: Usable Verifiable Secrecy-Preserving E-Voting. In: *6th International Joint Conference on Electronic Voting (E-Vote-ID)*. University of Tartu Press, 2021.
- [Ma18] Marky, Karola; Kulyk, Oksana; Renaud, Karen; Volkamer, Melanie: What Did I Really Vote For? In: *ACM CHI*. p. 176, 2018.
- [Ma19] Marky, Karola; Schmitz, Martin; Lange, Felix; Mühlhäuser, Max: Usability of Code Voting Modalities. In: *ACM CHI*. 2019.
- [Ma20] Marky, Karola; Zimmermann, Verena; Funk, Markus; Daubert, Jörg; Bleck, Kira; Mühlhäuser, Max: Improving the Usability and UX of the Swiss Internet Voting Interface. In: *ACM CHI*. 2020.
- [Ma21] Marky, Karola; Zollinger, Marie-Laure; Roenne, Peter; Ryan, Peter YA; Grube, Tim; Kunze, Kai: Investigating Usability and User Experience of Individually Verifiable Internet Voting Schemes. *ACM Trans. Comput.-Hum. Interact*, 28(5), 2021.
- [MKV18] Marky, Karola; Kulyk, Oksana; Volkamer, Melanie: Comparative Usability Evaluation of Cast-as-Intended Verification Approaches in Internet Voting. In: *SICHERHEIT. Gesellschaft für Informatik*, 2018.
- [Ne14] Neumann, Stephan; Olembo, Maina M.; Renaud, Karen; Volkamer, Melanie: Helios Verification: To Alleviate, or to Nominate: Is That the Question, or Shall we Have Both? In: *International Conference on Electronic Government and the Information Systems Perspective*. Springer, pp. 246–260, 2014.

- [Sa09] Saldaña, Johnny: The coding manual for qualitative researchers. Sage, 2009. OCLC: ocn233937452.
- [So20] Solvak, Mihkel: Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. In (Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Küsters, Ralf; Kulyk, Oksana; Duenas-Cid, David; Solvak, Mihkel, eds): Electronic Voting - 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6-9, 2020, Proceedings. volume 12455 of Lecture Notes in Computer Science. Springer, pp. 213–228, 2020.
- [Th06] Thomas, David R.: A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27(2):237–246, 2006.
- [TVK22] Thürwächter, Paul Tim; Volkamer, Melanie; Kulyk, Oksana: Individual Verifiability with Return Codes: Manipulation Detection Efficacy. In: 7th International Conference on Electronic Voting (E-Vote-ID). volume 13553. Springer LNCS, p. 139–156, 2022.
- [Vo22] Volkamer, Melanie; Kulyk, Oksana; Ludwig, Jonas; Fuhrberg, Niklas: Increasing security without decreasing usability: Comparison of various verifiable voting systems. In: Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). USENIX Association, Boston, MA, August 2022.
- [WH09] Weber, Janna-Lynn; Hengartner, Urs: , Usability Study of the Open Audit Voting System Helios, 2009.

German Social Elections in 2023: An Overview and first Analysis

Tobias Hilt,¹ Oksana Kulyk,² Melanie Volkamer³

Abstract: In 2023, the third largest election in German, the social elections (in German Sozialwahlen), offered an online channel for the first time. Of particular interest is the fact that the system provides a form of cast-as-intended verifiability, allowing the voter to verify that their vote was cast as intended and not manipulated by the device they used to cast their vote. This paper describes a first analysis of the overall voter experience with a special focus on this verifiability functionality. We utilize a cognitive walkthrough method, with three people having different levels of expertise regarding online voting, including a layman, a security expert, and a voting expert. Our findings reveal a number of issues with the system in terms of communication and presented information, and highlight areas in need of improvement to enhance user experience in particular with respect to the verifiability functionality.

Keywords: Sozialwahl; Online Voting; cast-as-intended verifiability; Cognitive Walkthrough

1 Introduction

This contribution explores the pioneering implementation of online voting in Germany's third largest election, the so called social elections (in German 'Sozialwahl'), in 2023. The possibility to cast the vote online for the first time in this election signifies a groundbreaking advancement, allowing voters to exercise their democratic rights through digital means – in particular as there is no online voting channel for any parliamentary election in Germany (not on federal, not on state and not on local level). Furthermore, a system is in place providing some form of cast-as-intended verifiability – namely voters can check that their vote is cast as intended, i.e. that their voting device did not manipulate their vote by changing it before sending it to the voting server (or not sending it at all). To do so voters are supposed to use a second device, e.g. their laptop for vote casting and their mobile phone to verify. Thus, as long as one of the devices is trustworthy, voters will detect misbehaving devices.

With limited information available in English about the election and the voting system in place, the first objective of this paper is to compile publicly accessible information, including requirement documents, voter-related information and the actual user interfaces, to provide an overview for the international electronic voting community.

¹ Karlsruhe Institut for Technology, AIfB, Kaiserstr. 89, 76131 Karlsruhe, Germany tobias.hilt@kit.edu

² IT University of Copenhagen, Computer Science, Rued Langgaardsvej 7, Copenhagen, Denmark okku@itu.dk

³ Karlsruhe Institut for Technology, AIfB, Kaiserstr. 89, 76131 Karlsruhe, Germany melanie.volkamer@kit.edu

The main purpose of this paper is then to conduct a first analyses of the usability of the online voting channel with a special focus on the effectiveness of the cast-as-intended verifiability. To do so a cognitive walkthrough methodology was employed. This approach involves systematically analyzing the provided information to use the system and the system's user interface design and interaction flow from the perspective of potential voters. Note, by simulating the thought process of users and identifying potential usability issues, the cognitive walkthrough aids in identifying areas for improvement and enhancing user experience.

The paper is structured as follows. We provide background information about the elections in Sect. 2. Sect. 3 describes the voting system used in online elections this year, as per official documentation and other publicly available information. Sect. 4 describes the voting process and all it's possible steps. The analysis of said voting process is discussed in Sect. 5, as well as the underlying limitations. Finally conclusions are drawn and directions for future work are presented in Sect. 7.

It is important to clarify that the authors of this contribution are not directly involved in the election administration or responsible for the operation of the voting system. However, they actively participated in discussions concerning the requirement documents, providing valuable insights for this research.

2 Background

In this section we shortly present some background information relevant for the reader's understanding. First we present some general information on the German social election, then we shortly present the requirements that needed to be met for the social election to be held in a partly digital format.

2.1 German Social Elections

The Sozialwahl in Germany is a democratic election where individuals (not necessary Germans) with a German public health insurance and pensioners at "Deutsche Rentenversicherung Bund" are eligible to elect representatives who advocate for their interests in the social parliaments of the pension and health insurance sectors⁴. The election takes place every six years since 1953, enabling voters to influence key aspects of the insurance systems such as their budget, policy decisions and overall management⁵⁶. As of 2023, a total of 52

⁴ <https://www.vdek.com/presse/pressemitteilungen/2023/sozialwahl-2023-ersatzkassen-online-wahl.html>, Last accessed on 23 Jun 2023

⁵ <https://www.sozialwahl.de/die-sozialwahl-2023/was-ist-die-sozialwahl>, Last accessed on 04 Jul 2023

⁶ <https://www.bundesregierung.de/breg-de/themen/arbeit-und-soziales/sozialwahl-2023-2188062>, Last accessed on 21 Jun 2023

million of people are eligible to vote in this election⁷. The voter turnout varied over time, ranging from 20% to 44% since the election's inception, with it being on a decline since 1986 [Dr08]. The latest available statistics show a turnout of 30% during the Sozialwahl in 2017 [Bu18].

Traditionally, the Sozialwahl was conducted exclusively through mail-in voting (i.e. postal voting). However, in the 2023 Sozialwahl, several insurance companies offered their voters the option to vote online in addition to the traditional mail-in voting method. Eligible voters were provided with their voting materials, which encompassed not only the required documents for mail-in voting but also the essential information for casting their votes online. According to the federal ministry of labor and social affairs (BMAS), online voting reflects efforts to modernize the election process and provide participants with alternative voting options⁸.

The possibility of voting online was implemented as part of a model project called "ARGE Modellprojekt Online-Wahlen 2023". The health insurance companies Techniker Krankenkasse (TK), BARMER, DAK-Gesundheit, Kaufmaennische Krankenkasse (KKH) and Handelskrankenkasse (hkk) joined forces for this purpose. A total of over 22 million members of these five insurers were entitled to cast their votes online in this year's Sozialwahl⁹.

While there are currently no comprehensive figures available from federal election organizers on the 2023 election, some of the health insurance companies have released data regarding voter turnout, showing a trend towards decreasing turnout. As such, TK (Techniker Krankenkasse) reported that this year's voter turnout declined, with only 23.45% of all eligible TK members participating, representing from a turnout of 32.09% in 2017¹⁰. Approximately one tenth of the eligible TK members voted online¹¹. Likewise, the DAK Gemeinschaft reported a decrease in voter turnout, with only 20.1% of DAK members participating in the election, compared to 28.4% in the previous Sozialwahl election held in 2017. Notably, less than 3% of eligible DAK members opted to exercise their voting rights online¹².

⁷ <https://www.sozialwahl.de/>, Last accessed on 21 Jun 2023.

⁸ <https://www.bmas.de/DE/Soziales/Sozialversicherung/Sozialversicherungswahlen/sozialversicherungswahlen-artikel.html>, Last accessed on 04 Jul 2023.

⁹ <https://www.vdek.com/presse/pressemitteilungen/2023/sozialwahl-2023-ersatzkassen-online-wahl.html>, Last accessed on 23 Jun 2023

¹⁰ <https://www.soziale-selbstverwaltung.de/wer-wir-sind/unsere-traeger/techniker-krankenkasse-wahlergebnis-2017>, Last accessed on 03 Jul 2023.

¹¹ <https://www.tk.de/techniker/unternehmensseiten/unternehmen/sozialwahl-2023/sozialwahl-2023-wahlergebnis-2012900>, Last accessed on 25 Jun 2023.

¹² <https://www.dak.de/dak/bundesthemen/sozialwahl-2023-ergebnis-steht-fest-2623564.html>, Last accessed on 22 Jun 2023

2.2 Requirements

There are mainly two documents which regulate which requirements must be met for the Sozialwahl, namely the Online Voting Regulation (“Verordnung zur Onlinewahl”) [Bu20] and the Technical Guideline TR-03162 issued by the German Federal Office for Information Security (“Bundesamt für Sicherheit in der Informationstechnik (BSI)”) [Bu23].

The Online Voting Regulation primarily addresses abstract content and defines important terminologies. With regard to the necessary security requirements, the regulation refers to the Technical Guideline TR-03162 issued by the BSI [Bu23]. Additionally, Paragraph 10 of the regulation briefly addresses rules on usability and accessibility. Specifically, Paragraph 10 mentions that the eligible voters must be informed about suitable security measures with the transmission of the election documents, with which the device used for the election action can be protected against third-party interference according to the state of the art [Bu20].

The Technical Guideline TR-03162 [Bu23] is a set of guidelines established by the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany. These guidelines are part of a model project pursuant to § 194a of the Fifth Book of the Social Code (SGB V) and are intended to complement the Online Voting Regulation. The technical guideline includes specifications for the operation and use of applications and IT systems used in the implementation of the online social election model project. This technical guideline largely aligns with and builds upon fundamental principles of IT protection and security. The key areas covered include: establishing basic requirements and determinations, implementing BSI IT basic protection guidelines, emphasizing the use of up-to-date encryption methods, and providing relevant information on election preparation and execution. A previous version of the TR is discussed and proposal how to improve the TR are included in [Be21].

For the electronic voting community and for the focus of our paper Section 5.2 of the Technical Guideline TR-03162 is of special interest as it addresses verifiability. The relevant points are translated below:

The individual voter SHOULD be given the opportunity to understand the election result. The following aspects of verifiability are considered:

- 1. The voter can verify that their online vote was sent as intended, received, and stored in the ballot box.*
- 2. The voter can verify that their vote was correctly included in the count.*
- 3. The voter can verify that all votes were correctly summed up to the election result.*

It is important to emphasize that these points are introduced with the verb “SHOULD”. As defined in the Technical Guideline, this expression means that a requirement should

normally be fulfilled, unless there is a good reason against doing so – as opposed to “MUST”, meaning that the requirement is mandatory in any case. In particular this paragraph of the TR has been criticized by researchers [Be21], arguing that there is a lack of specification on what constitutes as a good enough argument against implementing verifiability, potentially leading to this requirement being neglected by election organizers. While other critique by these researchers were addressed in the newest version, to our best knowledge, no explanation addressing this criticism has been publicly provided. Note, it is also not defined, who decides that the justification is deemed sufficient.

3 Voting system

In this section we summarize the available information about the voting system. The available information on the system and it’s security were very limited, although general information on the Sozialwahl was plentiful. Therefore the following sections are subdivided by the origin from which the information was retrieved, beginning by the voting material received by mail, the information found on TK’s website and finally, further information that was found online in an extensive google search. It’s important to note, that we exclusively focus on the information provided by Techniker Krankenkasse (TK), as the authors and all participants of the cognitive walkthrough have assurance in this specific health insurance company. Thus, it might be that it is different from company to company. In this case, the description and the late analysis strictly reflects the perspective of a TK-insured voter.

3.1 Information from the Voting Material

The material received by mail consisted of the following components:

- A personalized letter inviting the recipient to participate in the election. The letter contained two links and a QR code, which referred to the same URL as the second link.
- An envelope attached to the letter that could be used for postal voting. This voting envelope also included the personal election identification number.
- The ballot paper for postal voting and a pictorial instruction for postal voting enclosed with the letter.
- A detailed “Guide to Online Voting 2023”, which described the process of voting and verification through diagrams and text.

In particular, the included guide led participants through the process of online voting, beginning with the authentication. The two possibilities of authentication, via insurance

number and insurance card or via AusweisApp2, a mobile application designed for online identification using the electronic ID card (Online-Ausweis)¹³, were explained. Afterwards the process of casting a vote was briefly explained and it was mentioned that you have to confirm having read the security notes for protection against third party interference. Additionally, a website¹⁴ was given, where these instructions should be able to locate.

Regarding the security and encryption of the ballot, it was only stated, that there is a very strong encryption method in place and therefore it might take a moment to submit the vote. No further details were disclosed. The possibility to verify one's vote 30 minutes after vote casting using the "Sozialwahl Verifier" app was also briefly mentioned. The significance of this step was not explained but it was stressed, that this step is explicitly not obligatory. All information regarding cast-as-intended verifiability from the received voting material is translated into English below:

After the election, you have the option of photographing the displayed QR code within 30 minutes using the Social Election Verifier app. As a result, your vote stored in the electronic ballot box is displayed.

Lastly the election period was mentioned as well as, that in case somebody would cast their vote online and per mail, only the online vote would count.

3.2 Information presented on TK's Website

In analyzing the information available on TK's website pertaining to its online election system and security protocols, we prioritized the content that was most relevant. Among the plethora of articles and news available, particular emphasis was placed on the websites referenced in the printed voting material, which suggests their significance as deemed by TK. There were two websites of paramount importance linked in the voting material. The first linked website¹⁵ provided an overview that primarily consisted of news articles about the impending election and featured several related pages; of which, two were germane to the online election. The very first of these pages sketched an outline of how the online election was made possible, as already described in Sect. 2.1. Although it briefly mentioned that the voting application complied with high security standards set by BSI, it did not provide specific details on the system and security standards. The second website¹⁶ furnished general instructions about the voting procedure and mirrored the content in the voting material disseminated via mail. It contained a link leading to the election website, a flowchart illustrating the voting process, and a downloadable detailed instruction in PDF format

¹³ <https://www.ausweisapp.bund.de/home>, Last accessed on 03 Jul 2023.

¹⁴ <https://www.bsi.bund.de>, Last accessed on 07 Jul 2023

¹⁵ <https://www.tk.de/sozialwahl>, last accessed on 03 Jul 2023

¹⁶ <https://www.tk.de/techniker/unternehmensseiten/unternehmen/sozialwahl-2023/waehlen-sie-jetzt-online-2119940>, last accessed on 03 Jul 2023

which matched the guide sent with the voting documents. Additionally, there was a section titled *Security Notes for Protection against Third Party Interference* that cited a page from BSI¹⁷ for relevant instructions. Though it claimed encryption and security as the utmost priority, it did not offer any explications or supplementary information on these claims. The website did hint at security being pivotal, but fell short in providing concrete specifics, and critical inquiries regarding the secrecy of the vote, verifiability without traceability, and management of a substantial number of votes remained unaddressed. The mention of vote transmission potentially being time-consuming due to very strong encryption¹⁸ was present, but no additional insights into the encryption process were disclosed.

3.3 Further information

In an endeavor to glean additional information pertaining to the Sozialwahl 2023, several investigative measures were undertaken. Among the steps taken was reaching out to the press office via email with queries. Through this communication, it was ascertained that regio iT¹⁹ and Smartmatic²⁰ were engaged as IT service providers for the election. Additionally, a comprehensive Google search was conducted on 30.06.2023 to ascertain whether the necessary conditions were fulfilled for the election; however, this search did not yield pertinent information.

Moreover, during the search, an explanatory video was discovered which elucidated the general election process and discussed the voting rules²¹. It is important to note that the video primarily emphasized the usability of the voting system and the provision of a basic understanding of its operations. It did not delve into technical aspects such as encryption or security measures.

4 Voting process

In this section, a detailed analysis of the voting process employed during the Sozialwahl 2023 is provided, meticulously examining each step involved. Initially, upon receiving the voting materials, the voter was expected to familiarize themselves with the information described in Sect. 3.1. This phase of orientation was crucial to understanding the subsequent steps. It is important to note that one of the links available in the voting materials directed voters to an information page provided by the insurance company, where a flowchart illustrating the

¹⁷ https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html, Last accessed 07 Jul 2023

¹⁸ <https://www.tk.de/techniker/unternehmensseiten/unternehmen/sozialwahl-2023/waehlen-sie-jetzt-online-2119940>, Last accessed on 27 Jun 2023.

¹⁹ <https://www.regioit.de>, last accessed on 04 Jul 2023

²⁰ Smartmatic is also involved in the official elections in Estonia. <https://www.smartmatic.com>, last accessed on 04 Jul 2023

²¹ <https://www.youtube.com/watch?v=qn6mhcykCV0>, Last accessed on 29 Jun 2023

voting process was displayed. However, both the author of this paper and a participant of the cognitive walkthrough found the insurance company’s flowchart to be rather confusing. As such, this flowchart and the critiques against it will be elaborated upon and discussed in the subsequent Sect. 5.

To facilitate a more coherent understanding and to overcome the limitations of the insurance company’s flowchart, an alternative flowchart has been generated by the author that elucidates the progression from the acquisition of the voting materials, through the voting process, to the verification of the vote via a dedicated app (see Fig. 1). This author-created flowchart is particularly beneficial in visually comprehending the sequence and interactions involved in the process.

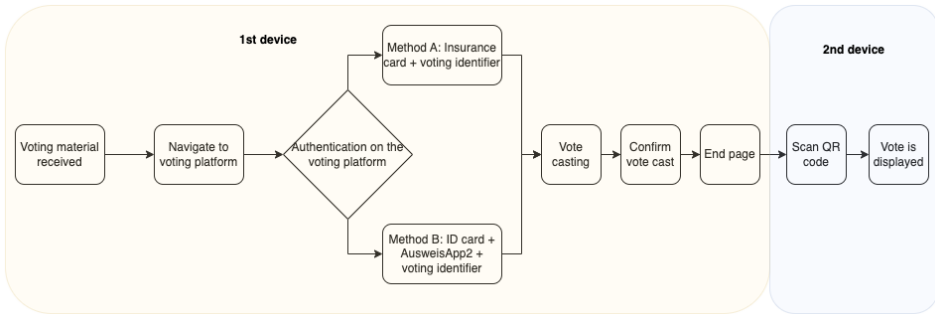


Fig. 1: Author-created Flowchart illustrating the complete voting process

Accompanying the author-created flowchart, screenshots from the voting application have been incorporated below. It is essential to mention that these screenshots are in German, mirroring the language used within the system, and no option was available for altering this setting. This serves to ensure authenticity and a representation of the user experience as encountered by the German-speaking electorate.

For the practical illustration of a voting procedure, a random selection was made from the available options. This decision to randomly select was executed to reflect how an elector might engage with the system. The choice fell on the first item in the list of options presented.

4.1 Authentication

The voter, having reviewed the materials, followed the embedded links. A circuitous path through these links led to the voting platform. Here, the participant was offered two methods for authentication. 'Method A' included the entering of the insurance number, the last six digits of the insurance card number, and the personal voting identifier received with the voting material. 'Method B' used the personal voting identifier, the ID card and a dedicated

App called 'AusweisApp2' which is commonly used in Germany to authenticate online. However, in this analysis, only the first method, termed 'Method A,' is employed, due to the author's lack of AusweisApp2.

4.2 Vote Casting

Following successful authentication, the system displayed the available lists, with a total of four choices. Once the voter selected an option, it was necessary to review this selection in order to proceed.

Fig. 2: The voter is asked to check their selection, submit having noticed the security notices before being able to cast their vote.

The system then presented the selected option and prompted the voter to acknowledge having read the before mentioned *Security Notes for Protecting the Device Used in the Voting Process Against Third-Party Interference According to Technological Standards*. Note, that this information was not linked, nor could it be found at the given destination²². Noteworthy on this account is, that the information on how to retrieve these security notes was conflicting, as the detailed guide referred to a different website as the TK website “How Online Voting works”. By selecting the “Stimme abgeben” button, the voter’s selection was transmitted to the digital ballot box (see Fig. 2). This transmission phase lasted a few seconds.

²² https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node, last accessed on 01 Jul 2023

4.3 Cast-as-Intended Verifiability

Subsequent to the vote submission, the participant was greeted with a confirmation message, signifying the completion of the voting process. This message informed the voter that it was now safe to exit the page. Additionally, a QR code was displayed on the same page, intended for verifying the submitted vote using the “SozialwahlVerifier” app (see Fig. 3).



Fig. 3: The successful transmission of the vote is signaled and the user is given permission to sign out. The optional possibility to verify one’ vote by scanning the QR code with the “SozialwahlVerifier” app is presented.

To utilize this verification feature, the voter needed to scan the QR code using a compatible secondary device such as a smartphone within the “SozialwahlVerifier” app. The app then displayed the vote that was submitted, providing an additional layer of confirmation. It is noteworthy that this verification procedure within the app did not require further authentication.

5 Methodology: Analysis from User Perspective

In this section an examination of the user experience in the Sozialwahl 2023 voting process is undertaken. The evaluation method employed for this analysis is informed by the *cognitive walkthrough* approach, which is a usability evaluation method that is fundamentally centered on comprehending and analyzing the cognitive processes involved as a new user encounters an interface or system for the first time [Wh94]. The primary questions that guide the cognitive walkthrough are: (1) Will the user endeavor to achieve the right outcome? (2) Will the user notice that the correct action is available? (3) Will the user associate the

correct action with the outcome they are trying to achieve? (4) If the correct action is performed, will the user perceive that progress is being made toward the solution of their task? [LW97]. In the context of this paper, the cognitive walkthrough approach was adapted to systematically analyze the Sozialwahl 2023 voting process from a first-time user's perspective. The walkthrough was conducted by three different people with varying levels of expertise and familiarity with online voting systems and security protocols. Two of these verified that their vote was cast-as-intended, with the other refraining from doing so, due to the process being too tedious.

6 Results

The general insights gathered from the cognitive walkthrough highlighted several concerns. Most of these concerns stem from information not being clearly communicated or even confusing: e.g., the flowchart (see Fig. 4 provided in the voting material) was perceived to be confusing by all participants. Furthermore, some information that was perceived as necessary, e.g. the before mentioned security notes, was either unavailable or difficult to find. Other information was perceived as too vague and lacking in precision, for example no details regarding the security of the voting system was disclosed, while it was just mentioned that the system is "very secure".

The most striking issues are listed below:

- No information why the possibility to verify one's vote or why this may be important was given, which led to one of the participants not verifying their vote.
- The requirement that the verification process required a second device (with a camera), was not communicated beforehand to the voters; a possible consequence of this might be, that some voters used their smartphone to cast their vote and were left unable to verify the vote, in case they did not have a second device with a camera to scan the QR code.
- The voting materials lacked clear instructions regarding the voting rules, such as the number of permissible votes. This is of particular relevance as voters were not warned if the selection they made would make their vote invalid (e.g. if they selected more than one voting options)
- In order to proceed with voting, voters had to confirm security notes, which none of the participants of the cognitive walkthrough managed to locate.
- The finalization of the voting process was not clearly communicated. In particular, the system did not provide any clear indication that closing the window or signing out would leave the voter unable to verify their vote.

We elaborate on specific insights from each participants of the cognitive walkthrough below.

Layperson: The layperson found the voting process to be complex, and chose not to engage in the verification process to avoid additional effort and because they lacked the understanding why it was even needed. The participant struggled to locate the necessary information in the voting material, such as the link to the actual voting platform. They found the voting identifier prone to errors, as it contained many special characters. The layperson was inclined to trust the system's security, mainly because it appeared too intricate for them to understand or assess. Due to being too tedious, needing to download of a dedicated app, the layperson refrained from verifying their vote.

Security Expert: The security expert lamented the absence of technical background information. They chose to ignore the QR code on the voting envelope due to security concerns, namely, that they could not figure out the destination of the QR code. The security expert noted that some form security notes were placed towards the bottom of the information page and could easily be overlooked. After inspecting these security notes, they negatively highlighted the absence of actual notes but rather only claims that encryption and security were the priority, without disclosing details, as already mentioned in Sub-Section Sect. 3.2. Although the expert did not have strong security concerns for this particular vote due to its perceived low relevance, they mentioned that in a more significant election, such as parliamentary elections, the concerns would be significant.

Voting Expert: The expert was particularly critical of the unavailability of the mentioned security notes, and the necessity to submit to those, in order to cast their vote. They highlighted, that all that was found in an extensive search phase, using Google, the general search functionality at BSI's website²³ and checking the links, provided in the voting material, was only vaguely related and pertained to conventional offline elections focusing on detecting and avoiding the receipt of fake news. On this account they noticed conflicting information provided by TK, how these security notes may be found. The detailed guide (see Fig. 4) referenced a different source than TK's website providing information about the election. Moreover, they also found the diagram to be confusing due to it being two-fold and illustrating a non-clear path through the voting process. This obscurity was mainly due to conflicting wording in the diagram. The expert was critical of the absence of an additional security step for the second device to protect the vote, such as time-based PIN, as proposed in similar applications²⁴, as this step serves two important purposes: (1) It assists in alleviating the confusion that non-experts might experience when they see their vote being directly displayed by the server, as this display could lead laypeople to mistakenly believe that the secrecy of their vote has been compromised. (2) It contributes to preventing vote-buying schemes, as individuals who might be inclined to sell their votes cannot easily furnish proof that they have voted in the manner they were compensated for. They noted an overwhelming number of similar links in the voting materials, which provided excessive

²³ <https://bsi.bund.de>, last accessed 07 Jul 2023

²⁴ <https://www.polyas.com/security/individual-verification>, last accessed 3 Jul 2023

information but lacked relevance, such as the first link provided²⁵ in the voting material, which served as a collection for all related links to the social election. The primary criticism was that, despite the abundance of information provided about the Sozialwahl, the majority of it lacked any pertinent connection to the aspect of online voting. They found that the extensive instructions (Fig. 4) were informative for the voting process but did not address voting rules or technical details about the underlying system or security. The voting expert was critical about the absence of information on several important aspects, including a layperson-friendly explanation about (1) the purpose of the cast-as-intended verifiability step, (2) why a voter should participate in this step and (3) against which kind of attack scenario this step protects.

Limitations: It is imperative to acknowledge the limitations of the analysis conducted. Firstly, the number of participants in the cognitive Walkthrough was limited, involving only three participants. A larger and more diverse group of participants could potentially provide a more comprehensive and varied set of insights. However, already the findings so far show a lot of room for improvements of both the voting material as well as the user interfaces. Secondly, the acquisition of information was constrained. The analysis was mainly based on information sourced from the insurance company's materials, which might not encompass all the relevant aspects of the voting process. It is possible that additional information and perspectives from external sources could contribute to a more in-depth understanding and critical evaluation of the system. This limitation in information acquisition could have affected the depth and breadth of the analysis. However, it is not very likely that the average voter would have spend time to search for additional information other than the information provided in the voting material or other sources send to him by the election officials. Thirdly it is important to highlight, that the main focus of this analysis was focused around the voting experience with regards to the cast-as-intended verifiability step and the accompanying material provided by TK. As every insurance that offered the possibility to vote online used their own voting platform and accordingly may have provided different material in preparation for their voters, it is likely that the gained impression may differ for voters from different insurances. However, our findings are relevant for the TK insurance company for sure. Considering these limitations, it is important to interpret the results of this analysis with caution, and to recognize that they represent a snapshot of experiences and insights within the constraints of the methodology employed. Further research involving a larger and more diverse set of participants, and a more exhaustive collection of information from various sources, could contribute to a more robust analysis of the Sozialwahl 2023 from a user's perspective.

7 Conclusion

While in general, it is good to see that the technical guideline [Bu23] considers verifiability and the system in place for the social election provides some form of cast-as-intended

²⁵ <https://www.tk.de/sozialwahl>, last accessed 03 Jul 2023

verifiability however, this research has identified several shortcomings regarding the communicated information and the user interfaces in general and in particular regarding the cast-as-intended verifiability process.

The analysis of the social election / Sozialwahl 2023 in Germany has exposed several pertinent concerns and areas for improvement in the realm of voting process, communication, and system security. The findings point to an overarching lack of information and clarity on critical elements of the voting system. It is striking that despite the scarcity of easily accessible information necessary for assessing the security of the voting system, there has been little media discussion or public criticism regarding these issues. One of the crucial aspects that require more attention is the verifiability of the votes. The information about this feature was not effectively communicated, and as a result, many voters may not have realized its importance or how to utilize it. Verifiability is a fundamental component of ensuring the integrity and reliability of an election system, and thus, it is vital that this aspect is transparent and easily understandable for all voters. Upon reviewing the technical guideline and considering the elements outlined regarding cast-as-intended verifiability, it is evident from the publicly accessible information that only the first criterion - namely, that the vote was transmitted as intended, received, and securely stored in the ballot box - is met only under specific assumptions. These assumptions are that at least one of the devices employed for voting and verification is not compromised, and that the election administrator is both ethical and free from manipulation. In further research conducted after the cognitive walkthrough, we also examined the information available from other health insurance companies, such as "DAK Gesundheit". Interestingly, DAK addressed some of the aspects we critiqued in TK's materials (e.g., existence of an explanatory video, stating the voting rules & the necessity of a second device), though it also had other areas that warranted criticism. For example DAK Gesundheit stated, that you can also be sure without checking that your vote is reliably recorded by the system, implying that verification is not necessary²⁶. As we look to the future, it is essential that election organizers invest in providing more comprehensive and accessible information. Future work should focus on enhancing the usability, perception, and understanding of the voting system among the electorate. This includes not only ensuring that the information is available but also that it is communicated in a way that is clear and understandable to the average voter. Additionally, feedback from diverse groups of stakeholders including security experts, voting experts, and laypeople should be sought to understand different perspectives and identify areas that need improvement. It is also important for the media and civil society to play a more active role in scrutinizing and discussing the election systems, especially in terms of security and verifiability. This will help in fostering an informed citizenry, which is crucial for the integrity and success of the democratic process.

In summary, while the Sozialwahl 2023 represents an important exercise in democratic participation, the findings of this paper suggest that there are significant areas for improvement in terms of communication, clarity, and voter education. A commitment to transparency,

²⁶ https://www.dak.de/dak/unternehmen/sozialwahl-bei-der-dak-gesundheit/sozialwahl-2023-erstmal-auch-als-online-wahl_33916, Last accessed on 30 Jun 2023.

accessibility, and continuous improvement is critical for ensuring the integrity and public trust in the election systems.

Bibliography

- [Be21] Beckert, Bernhard; Budurushi, Jurlind; Grunwald, Armin; Krimmer, Robert; Kulyk, Oksana; Küsters, Ralf; Mayer, Andreas; Müller-Quade, Jörn; Neumann, Stephan; Volkamer, Melanie: Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalen Abstimmungen. Technical report, 2021. 46.23.01; LK 01.
- [Bu18] Bundeswahlbeauftragte: Schlussbericht über die Sozialwahlen 2017. Technical report, October 2018. Last accessed on 04 Jul 2023.
- [Bu20] Bundesanzeiger: , Verordnung über die technischen und organisatorischen Vorgaben für die Durchführung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a des Fünften Buches Sozialgesetzbuch (Online-Wahl-Verordnung), September 2020. Last accessed on 27 Jun 2023.
- [Bu23] Bundesamt für Sicherheit in der Informationstechnik (BSI): , Technische Richtlinie TR-03162, March 2023. Last accessed on 27 Jun 2023.
- [Dr08] Dr. Braun, Bernhard; Dr. Klenk, Tanja; Prof. Dr. Kluth, Winfried; Prof. Dr. Nullmeier, Frank; Prof. Dr. Welti, Felix: Gutachten zur “Geschichte und Modernisierung der Sozialversicherungswahlen”. Technical report, April 2008. Last accessed on 4 Jul 2023.
- [LW97] Lewis, Clayton; Wharton, Cathleen: Cognitive walkthroughs. In: Handbook of human-computer interaction, pp. 717–732. Elsevier, 1997.
- [Wh94] Wharton, Cathleen: The cognitive walkthrough method: A practitioner’s guide. Usability Inspection Methods, New York, pp. 105–140, 1994.

Sozialwahl 2023
Für Gesundheit & Rente

Wie wähle ich online? Wenn Sie einen PC, ein Notebook, ein Smartphone oder ein Tablet mit Internetzugang besitzen, haben Sie alle technischen Voraussetzungen, um als wahlberechtigter Person Ihre Stimme online abzugeben. Wählen Sie einfach Ihr bevorzugtes Gerät mit Internetanschluss. Der Zugang zur Online-Wahlplattform erfolgt über unsere Internetseite [tk.de/sozialwahl](https://www.tk.de/sozialwahl).

Auf der Rückseite der Gesundheitskarte finden Sie die Kennnummer der Karte. Geben Sie bitte die letzten sechs Ziffern an. Bitte beachten Sie, dass bei jedem Austausch der Gesundheitskarte eine neue Kennnummer verwendet wird. Die Teilnahme an der Online-Wahl ist technisch leider nicht möglich, wenn Sie eine neue Gesundheitskarte Ende Februar / Anfang März erhalten haben. Sofern Sie Ihre alte Gesundheitskarte noch vorliegen haben, benutzen Sie bitte diese Karte.

Geben Sie bitte zusätzlich das Wahlkennzeichen ein, das Sie mit den Wahlunterlagen erhalten haben. Es ist auf dem roten Umschlag zu finden. Bitte achten Sie insbesondere auf Groß- und Kleinschreibung sowie Sonderzeichen.

Kommunen auf der Rückseite der Gesundheitskarte
(die letzten sechs Ziffern)

Wahlzeichen auf dem roten Wahlbriefumschlag

Hinweis: Bei Fragen zu den einzelnen Schritten oder erforderlichen Angaben können Sie die **Hilfefunktion** nutzen, um weitere Erläuterungen zu erhalten. Nach erfolgreicher Authentifizierung werden Sie direkt zum Stimmentwurf weitergeleitet.

2. Möglichkeit: Anmeldung mit der AusweisApp2 Hier können Sie sich mit Ihrem Personalausweis oder alternativ mit Ihrem elektronischen Aufenthaltstitel/Identitätsnachweis anmelden. Wichtig ist, dass die AusweisApp2 vor der Anmeldung auf Ihrem Gerät gestartet worden sein muss.

Geben Sie bitte zusätzlich das Wahlkennzeichen ein, welches Sie mit den Wahlunterlagen erhalten haben. Es ist auf dem roten Umschlag zu finden. Bitte achten Sie insbesondere auf Groß- und Kleinschreibung sowie Sonderzeichen.

Hinweis: Bei Fragen zu den einzelnen Schritten oder erforderlichen Angaben können Sie die **Hilfefunktion** nutzen, um weitere Erläuterungen zu erhalten. Nach erfolgreicher Authentifizierung werden Sie direkt zum Stimmzettel weitergeleitet.

Stimmabgabe Um Ihre Stimme abzugeben, wählen Sie eine der Listen des Stimmzettels, indem Sie auf das runde weiße Feld am rechten Rand im Namensfeld der Liste klicken. Wenn Sie eine der Listen ausgewählt haben, können Sie Ihre Auswahl im nächsten Schritt überprüfen und gegebenenfalls noch ändern.

Bevor Sie Ihre Stimme abgeben, bestätigen Sie bitte, dass Sie die „Sicherheitsanweisung zum Schutz des für die Durchführung der Wahlhandlung genutzten Endgerätes gegen Eingriffe Dritter nach dem Stand der Technik“ zu Kenntnis genommen haben. Diese finden Sie auf der Internetseite des BSI (<https://www.bsi.bund.de>). Hier gibt das BSI Empfehlungen für Bürgerinnen und Bürger zur Absicherung des lokalen Rechners heraus. Danach können Sie Ihre Stimme abgeben.

Während der Stimmabgabe wird Ihre Stimme sicher verschlüsselt und in der elektronischen Wahlurne gespeichert. Da es sich um ein sehr starkes Verschlüsselungsverfahren handelt, kann dieser Vorgang mehrere Sekunden dauern. Über eine Fortschrittsanzeige können Sie die Dauer der Verschlüsselung abschätzen. Die benötigte Zeit zur Verschlüsselung hängt sehr stark von der Rechenkraft Ihres Geräts ab. Bitte unternehmen Sie nichts, solange dieser Vorgang andauert.

Nach erfolgter Wahl haben Sie für 30 Minuten die Gelegenheit, Ihre Stimmabgabe auf eine korrekte Speicherung in der elektronischen Wahlurne zu überprüfen. Hierzu benötigen Sie ein zusätzliches Smartphone oder Tablet. Über die App „**sozialwahl Verifier**“ können Sie den nach der Stimmabgabe angezeigten QR-Code abfotografieren.

Als Ergebnis sind Ihre in der elektronischen Wahlurne gespeicherten Stimmen angezeigt. Die App „Sozialwahl Verifier“ finden Sie im **Apple App Store** und im **Google Play Store**. Wenn Sie Ihre abgegebenen Stimmen überprüfen wollen, muss die jeweilige App auf dem zusätzlichen Gerät (Smartphone oder Tablet) vor Beginn des Wahlvorganges installiert werden.

Sozialwati 2023



Optional besteht nach der Wahl die Möglichkeit, den angezeigten QR-Code innerhalb von 30 Minuten mit der App „Socialwahl“

Wichtige Hinweise:

- Sollten Sie bereits eine Stimme über die Wahlplattform abgegeben haben, können Sie nicht erneut wählen.
- Wenn Sie online gewählt haben, können Sie Ihre Wahlunterlagen entsorgen. Eine Stimmabgabe darf nur einmal erfolgen. Wenn Sie Ihre Stimme doppelt abgegeben haben, also sowohl per Briefwahl als auch per Online-Wahl, wird ausschließlich Ihre Stimme aus der Online-Wahl gezählt.

Fig. 4: Extensive guide to the different processes of the online election.

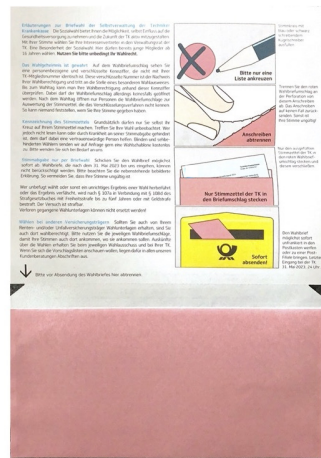


Fig. 5: Letter containing the invitation to the social election and instructions for mail-in voting.

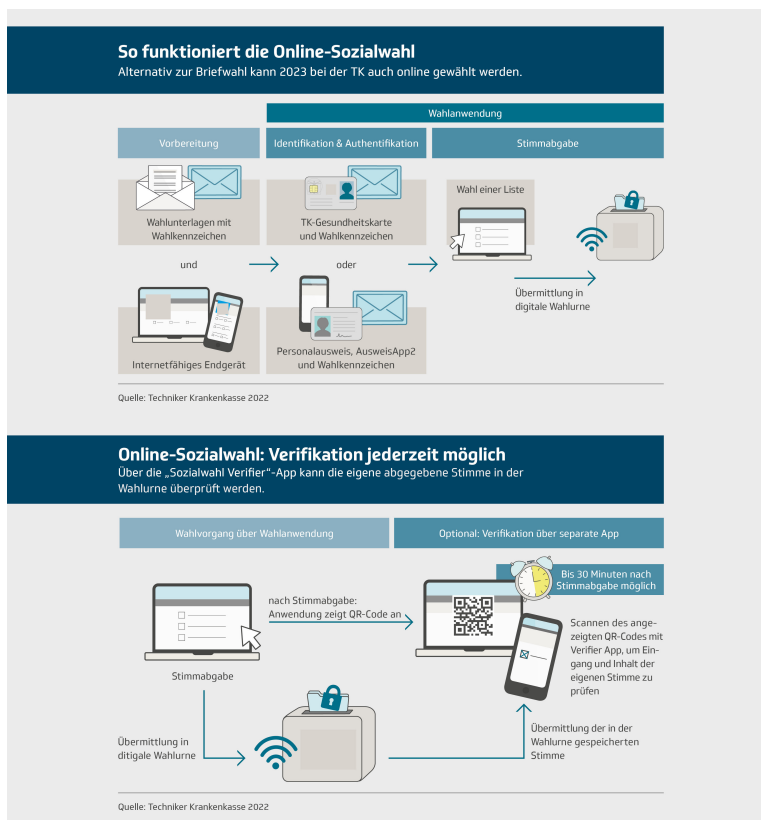


Fig. 6: Flowchart provided by TK describing the authentication possibilities at the voting application, vote casting process and the optional verifiability step (this flowchart was combined by the author into one figure for better visibility)

Stylish Risk-Limiting Audits in Practice

Amanda K. Glazer^{1,2}, Jacob V. Spertus³, Philip B. Stark⁴

Abstract: Risk-limiting audits (RLAs) can use information about which ballot cards contain which contests (*card-style data*, CSD) to ensure that each contest receives adequate scrutiny, without examining more cards than necessary. RLAs using CSD in this way can be substantially more efficient than RLAs that sample indiscriminately from all cast cards. We describe an open-source Python implementation of RLAs using CSD for the Hart InterCivic Verity voting system and the Dominion Democracy Suite[®] voting system. The software is demonstrated using all 181 contests in the 2020 general election and all 214 contests in the 2022 general election in Orange County, CA, USA, the fifth-largest election jurisdiction in the U.S., with over 1.8 million active voters. (Orange County uses the Hart Verity system.) To audit the 181 contests in 2020 to a risk limit of 5% without using CSD would have required a complete hand tally of all 3,094,308 cast ballot cards. With CSD, the estimated sample size is about 20,100 cards, 0.65% of the cards cast—including one tied contest that required a complete hand count. To audit the 214 contests in 2022 to a risk limit of 5% without using CSD would have required a complete hand tally of all 1,989,416 cast cards. With CSD, the estimated sample size is about 62,250 ballots, 3.1% of cards cast—including three contests with margins below 0.1% and 9 with margins below 0.5%.

Keywords: risk-limiting audit, election integrity, card-style data

1 Introduction

Risk-limiting audits (RLAs) manually inspect ballots from a trustworthy record of the votes⁵ to provide affirmative evidence that electoral outcomes (i.e., who won, not the exact vote counts) are correct if they are indeed correct, and (with a prespecified minimum probability) to correct any outcomes that are wrong. The maximum chance that an RLA does not correct a result that is wrong is the *risk limit*. For example, an RLA with a risk limit of 5% guarantees that if the reported outcome is wrong, the audit has at least a 95% chance of catching and correcting the reported outcome before it is certified. When the outcome is correct, RLAs may inspect only a small fraction of all ballot cards, saving considerable labor compared to a full manual recount.

According to the 2018 National Academies of Science, Engineering, and Medicine report *Securing the Vote: Protecting American Democracy* [Na18, Recommendation 5.8]:

¹ Authors listed alphabetically. Authors contributed equally to this work.

² Department of Statistics, University of California, Berkeley, CA, USA amandaglazer@berkeley.edu

³ Department of Statistics, University of California, Berkeley, CA, USA jakespertus@berkeley.edu

⁴ Department of Statistics, University of California, Berkeley, CA, USA pbstark@berkeley.edu

⁵ Not all paper vote records are trustworthy. See, e.g., [ADS20, AS20]. Absent a trustworthy record of the vote, no audit can provide affirmative evidence that the reported winners really won.

States should mandate risk-limiting audits prior to the certification of election results. With current technology, this requires the use of paper ballots. States and local jurisdictions should implement risk-limiting audits within a decade. They should begin with pilot programs and work toward full implementation. Risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible.

No jurisdiction currently mandates RLAs of every contest in every election, or even every federal and statewide contest. For example, Georgia law only requires auditing one contest every two years, and Colorado law requires auditing two contests in each election. While some officials claim that such sparse or infrequent auditing shows that their voting systems work flawlessly,⁶ auditing one reported outcome says nothing about whether any other reported outcome: every contest should get some scrutiny (or at least have a high probability of being audited).

Historically, auditing local contests together with jurisdiction-wide contests using a single audit sample has been infeasible. Indeed, when some contests are small and others are jurisdiction-wide, RLA methods that sample ballots uniformly at random would require a full hand count throughout the jurisdiction, even when every margin (as a percentage of votes in the contest) is large.

However, [GSS21] presented an approach to RLA sampling that allows many contests of different sizes to be audited efficiently using the same sample. Instead of sampling cards uniformly at random, the method uses *card-style data* (CSD) and *consistent sampling* to ensure that each contest gets the scrutiny it needs, without entailing unnecessary scrutiny of other contests. They illustrated their method with simplified examples involving only two contests, but in the U.S., there can be hundreds of contests in a single election.

We incorporated the [GSS21] method into the SHANGRLA Python RLA library,⁷ leveraging recent developments in formulating RLAs as hypothesis tests about the means of bounded, finite lists of numbers [St20] and efficiently measuring risk using test supermartingales [Sp23, St23b, WSSR21]. To illustrate the practical implications of CSD, we applied the method to historical data from the 2020 and 2022 general elections in Orange County, CA, which comprised 181 contests and 214 contests, respectively. In both elections, standard RLA methods would have required a full hand count to audit every contest to a risk limit of 5%. The new method reduces the estimated audit workload by more than 99% for the 2020 election and by 97% for the 2022 election.

⁶ See, e.g., Georgia Secretary of State Brad Raffensperger's claims that the audit of one contest in 2020 "reaffirmed that the state's new secure paper ballot voting system accurately counted and reported results." <https://sos.ga.gov/news/historic-first-statewide-audit-paper-ballots-upholds-result-presidential-race> (last visited 2 May 2023) and that the audit of one contest in 2022 "shows that our system works and that our county election officials conducted a secure, accurate election." <https://sos.ga.gov/news/georgias-2022-statewide-risk-limiting-audit-confirms-results> (last visited 2 May 2023)

⁷ <https://github.com/pbstark/SHANGRLA>

The next section reviews terminology, describes the problem, and summarizes the building blocks, including simultaneous card-level comparison audits of multi-style elections. Section 3 provides a high level description of our software. Section 4 describes the 2020 and 2022 Orange County elections, gives an overview of our implementation, and presents sample size estimates for RLAs with and without CSD. Code that produced our results is available at <https://github.com/pbstark/SHANGRLA>. Section 5, discusses ramifications for real-world RLAs and provides recommendations for practice.

2 Background

In the U.S., a *ballot* consists of one or more *cards*, individual pieces of paper. (U.S. elections often contain more contests than can be printed on a single piece of paper in a readable font.) Each card has a *style*, which for our purposes is the collection of contests on that card. Because ballot boxes are generally designed so that the cards do not land in the order in which they were cast, it is typically impossible to reassemble a ballot from its component cards once it has been cast. Thus cards, not ballots, are the atomic sampling unit in RLAs.

When ballots have multiple cards, no contest is on more than half the cards. Contests that are not jurisdiction-wide are on even fewer cards. Following the terminology of [St23b], the *sampling domain* of a contest is the population from which cards are sampled in an RLA. For the RLA to be valid, the sampling domain for a given contest generally must include every card that contains that contest. In practice, the sampling domain for RLAs has been either all cards cast in the election, or just the cards containing a particular contest. When the sampling domain for a contest includes cards that do not contain the contest, the audit generally needs to examine more ballots (when the outcome is correct) than it would if the sampling domain were limited to cards containing the contest.

In particular, audits that directly check the voting system’s interpretation and tabulation of votes are more efficient when the sampling domain is limited to cards that contain the contest because the error rate (per card) required to alter the outcome is smaller the larger the denominator (the sampling domain) is. Testing whether the error rate is below a small threshold requires more data than testing whether it is below a larger threshold.

The *diluted margin*, the margin in votes divided by the number of cards in the sampling domain for the contest, captures this phenomenon. Smaller diluted margins lead to larger audit sample sizes; expanding the sampling domain increases the “dilution,” reducing the diluted margin.

2.1 Card-level Comparison Audits and Card-Style Data

RLAs can use data from voting systems and from manually inspected cards in a number of ways. RLAs that check for error by comparing ballots to their machine interpretations are

called *comparison* audits; those that check outcomes without relying on the voting system's interpretations are *polling* audits. Furthermore, RLAs may sample and check vote totals for *batches* of ballot cards—typically machines or precincts—or individual cards. Adopting the terminology of [Stss], we refer to audits that sample individual cards and compare a human reading of the votes on each sampled card to the CVR for that card as *card-level* audits. The literature sometimes often calls these *ballot-level*, but card-level is more accurate nomenclature because CVRs are generally for individual cards, and ballots comprise more than one card in many jurisdictions.

All else equal, card-level audits are more efficient than batch-level audits; comparison audits are more efficient than polling audits; and *card-level comparison audits* are the most efficient approach. In a card-level comparison audit, the estimated sample size scales with the reciprocal of the diluted margin.

To conduct a card-level comparison audit, the voting system must produce *cast-vote records* (CVRs)—the system's record of the votes on each card. (However, see [Stss], which shows how to conduct a card-level comparison audit using “overstatement-net-equivalent” CVRs derived from batch-level results.) Moreover, there must be a known 1:1 mapping from the physical card to its particular CVR; some voting systems cannot provide such a link, or cannot provide a link without compromising voter privacy. That link might be provided by exporting CVRs in the order in which the cards were scanned and keeping the cards in that order, or by imprinting a number on each card before or as it is scanned, and including the imprinted number in the CVR for that ballot or as part of the filename of the CVR. [GSS21] showed that an audit can rely on CVRs to infer CSD: consider a card to contain a contest if the CVR for that card contains the contest. Even though the CVRs might be inaccurate or incomplete (otherwise, no audit would be needed), their method ensures that errors in CSD derived from CVRs do not compromise the risk limit. CSD makes it possible to minimize the sampling domain (maximizing the diluted margin) for each contest, considerably lowering audit workloads when contest outcomes are correct.

[GSS21] also showed how to combine CSD with *consistent sampling* [Ri18], which ensures that cards drawn for the purpose of auditing a given contest can also be used in the audit of other contests that appear on the sampled cards. Exploiting such overlap further reduces the estimated workload. If the voting system does not provide CVRs linked to cards, CSD can be derived by manually sorting the cards (a very labor intensive alternative), or by processing them in homogeneous batches in the first place. That is straightforward for precinct-based voting systems, but many jurisdictions do not sort cards by style before scanning them.

When CSD are derived from CVRs, the RLA can also use those CVRs for card-level comparison auditing, which is much more efficient than ballot-polling or batch-level comparison audits. For this reason, the audits we describe in the remainder of this paper are card-level comparison audits, but the software also supports ballot-polling audits with CSD. We now describe how the software is implemented to run a card-level comparison audit.

In broad brush, the procedure imports audit parameters (such as risk limits, risk-measuring functions, and the strategy for estimating the initial sample size), election data (including the reported winners, the CVRs, and upper bounds on the number of cards cast in each contest⁸), and contest-specific data (such as candidate names, and the social choice function).

CSD is inferred from the CVRs. The CVRs are checked for consistency with the other inputs. An initial sample size is determined for each contest, which implies a sampling probability for each card that contains the contest. The probability that a given card is sampled is the largest sampling probability for each audited contest on the card. Summing those maximum probabilities across cards is an estimate of the total initial sample size. A sample is drawn using *consistent sampling*; the corresponding cards are retrieved and interpreted manually; the resulting *manual vote records* (MVRs) are imported; the attained risk for each audited contest is calculated; and any contests for which the risk limit has been attained or for which there has been a full hand count are removed from future auditing rounds. If every audited contest has been removed, the audit stops; otherwise, a next-round sample size is determined for the remaining contests, and the process repeats.

In more detail, the algorithm is as follows (adapted from [GSS21]):

1. Set up the audit
 - a) Read contest descriptors, candidate names, social choice functions, upper bounds on the number of cards that contain each contest, and reported winners. Let N_c denote the upper bound on the number of cards that contain contest c , $c = 1, \dots, C$.
 - b) Read audit parameters (risk limit for each contest, risk-measuring function to use for each contest, assumptions about errors for computing initial sample sizes), and seed for pseudo-random sampling.
 - c) Read ballot manifest.
 - d) Read CVRs.
2. Pre-processing and consistency checks
 - a) Check that the winners according to the CVRs are the reported winners.
 - b) If there are more CVRs that contain any contest than the upper bound on the number of cards that contain the contest, stop: something is seriously wrong.
 - c) If the upper bound on the number of cards that contain any contest is greater than the number of CVRs that contain the contest, create a corresponding set of “phantom” CVRs as described in section 3.4 of [St20]. The phantom CVRs are generated separately for each contest: each phantom card contains only one contest.

⁸ All RLAs require information that a good canvass should generate routinely, including upper bounds on the number of validly cast cards that contain each contest, which can be derived from registration data, voter participation data, and physical inventories of ballot cards. Absent that information, even a “full” hand count is meaningless, since there is no way to know whether the count includes every validly cast ballot.

- d) If the upper bound N_c on the number of cards that contain contest c is greater than the number of physical cards whose locations are known, create enough “phantom” cards to make up the difference.
3. Prepare for sampling
 - a) Generate a set of SHANGRLA [St20] assertions \mathcal{A}_c for every contest c under audit.
 - b) Initialize $\mathcal{A} \leftarrow \cup_{c=1}^C \mathcal{A}_c$ and $C \leftarrow \{1, \dots, C\}$.
 - c) Assign independent uniform pseudo-random numbers to CVRs that contain one or more contests under audit (including “phantom” CVRs), using a high-quality PRNG [OS19]. (The code uses cryptographic quality pseudo-random integers uniformly distributed on $0, \dots, 2^{256} - 1$.) Let u_i denote the number assigned to CVR i .
4. Main audit loop. While \mathcal{A} is not empty:
 - a) Pick the (cumulative) sample sizes $\{S_c\}$ for $c \in C$ to attain by the end of this round of sampling. The software offers several options for picking $\{S_c\}$, including some based on simulation. The desired sampling fraction $f_c := S_c/N_c$ for contest c is the sampling probability for each card that contains contest k , treating cards already in the sample as having sampling probability 1. The probability p_i that previously unsampled card i is sampled in the next round is the largest of those probabilities: $p_i := \max_{c \in C \cap C_i} f_c$, where C_i denotes the contests on card i .
 - b) Estimate the total sample size to be $\sum_i p_i$, where the sum is across all cards except phantom cards.
 - c) Choose thresholds $\{t_c\}_{c \in C}$ so that S_c ballot cards containing contest c have a sample number u_i less than or equal to t_c .
 - d) Retrieve any of the corresponding ballot cards that have not yet been audited and inspect them manually to generate MVRs.
 - e) Import the MVRs.
 - f) For each MVR i :
For each $c \in C$:
If $u_i \leq t_c$, then for each $a \in \mathcal{A}_c \cap \mathcal{A}$:
 - If the i th CVR is a phantom, define $a(\text{CVR}_i) := 1/2$.
 - If card i cannot be found or if it is a phantom, define $a(\text{MVR}_i) := 0$.
 - Find the overstatement of assertion a for CVR i , $a(\text{CVR}_i) - a(\text{MVR}_i)$.
 - g) Use the overstatement data from the previous step to update the measured risk for every assertion $a \in \mathcal{A}$.
 - h) Optionally, conduct a full hand count of one or more contests, for instance,

- if the audit data suggest the outcome is wrong or if the auditors think a hand count will be less work than continuing to sample.
- i) Remove from \mathcal{A} all assertions a that have met their risk limits or that are for contests for which there has been a full hand count. (The audits of those assertions are complete.)
 - j) Remove from \mathcal{C} all contests c for which $\mathcal{A}_c \cap \mathcal{A} = \emptyset$ (the audits of those contests are complete).
5. Replace the reported outcomes of any contests that were fully hand counted by the outcomes according to those hand counts.

3 Software

The software can read Dominion Democracy Suite[®] and Hart InterCivic Verity CVRs and manifest files. Because file sizes in large jurisdictions can be unwieldy, the software can read compressed CVR files (.zip format containing XML records).

Figure 1 sketches the workflow to audit a collection of contests using CSD derived from CVRs. The user specifies parameters of the audit and the contests to be audited, including paths to data and output files, a trustworthy upper bound on the number of cards cast (e.g., a bound from participation records, ballot accounting, pollbook reconciliation, etc.—not the voting system’s own reported number of cards), contest information, risk limits, risk measuring functions and their tuning parameters (defaults are available), information used to estimate initial sample sizes (defaults are available), and whether to use CSD.

The software then constructs SHANGRLA assertions (or reads RAIRE assertions in json for IRV contests), reads CVRs and manifests, constructs “phantom” CVRs to account for missing cards if necessary, sets margins for overstatement assertions, estimates initial sample sizes, draws random ballots by consistent sampling, and returns their locations to the auditors.

The auditors retrieve the indicated cards, manually read the votes from those cards, and input the MVRs, which the audit software subsequently reads from a file. The software uses the specified risk-measuring function(s), the CVRs, and the MVRs to compute a P -value for every assertion. All assertions with P -values below the risk limit for their corresponding contests are considered “confirmed.” If any assertions remain unconfirmed, the software will estimate the number of additional cards to examine to confirm those assertions, draw a sample of that size, and export the identifiers of the ballot cards for the auditors to retrieve and interpret.

This process repeats until every assertion has been confirmed or there has been a full hand count of the contest. At any point, the auditors can choose to stop sampling at random and simply tabulate the rest of the votes in one or more contests (e.g., if they judge that that

would be more efficient, or if the audit sample indicates that the reported outcome is in fact wrong).

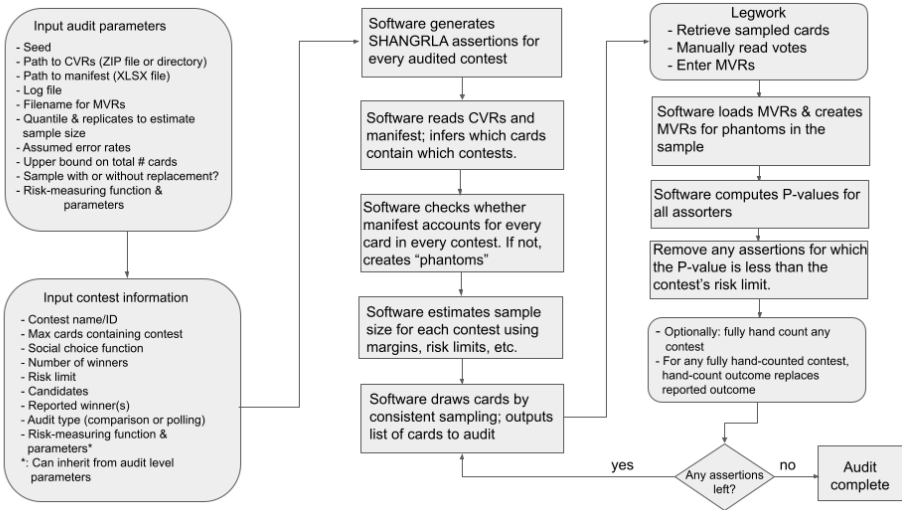


Fig. 1: Workflow for simultaneous card-level comparison audit using SHANGRLA software with CSD and consistent sampling. Boxes with rounded corners involve inputs from the auditors.

4 Orange County Election Audits

Orange County, CA, is the third most populous county in California (3.19 million as of the 2020 census, with over 1.81 million active voters⁹). It has more registered voters than 24 U.S. states, and is the country’s fifth-largest election jurisdiction, after Los Angeles, CA; Maricopa, AZ; Harris, TX; and San Diego, CA.¹⁰ As of this writing, Orange County has 2204 precincts and approximately 181 voting centers. Orange County uses the Hart Intercivic Verity system. The county first piloted an RLA in 2011,¹¹ conducted two additional pilots in 2018¹² and seven pilots between 2020 and 2022 mandated by California Elec. Code, §§ 15365–15367.

In this paper, we use data from the November 2020 and 2022 General Elections. We estimate the number of cards that would need to be inspected for an RLA with 5% risk limit, with and

⁹ <https://ocvote.gov/datacentral/>, last visited 8 June 2022

¹⁰ 2022 Election Administration and Voting Survey (EAVS), U.S. Election Assistance Commission, https://www.eac.gov/sites/default/files/2023-06/2022_EAVS_for_Public_Release_V1.xlsx, released 29 June 2023. Last visited 9 July 2023.

¹¹ See California Secretary of State Report to the US Election Assistance Commission, <https://admin.cdn.sos.ca.gov/reports/2011/post-election-audit-report-20111130.pdf>, last visited 15 May 2023.

¹² See <https://verifiedvoting.org/wp-content/uploads/2020/08/2018-RLA-Report-Orange-County-CA.pdf>, last visited 15 May 2023.

without style information. (While many states that require or authorize RLAs do not specify a risk limit in statute, 5% is a common value in practice. It was the statutory requirement in California’s pilot program, Cal. Elec. Code § 15367. Sample sizes for RLAs generally scale approximately like the log of the risk limit, so sample sizes for a risk limit of 1% would be about $\log(0.01)/\log(0.05) - 1 \approx 54\%$ larger.) Table 1 summarizes these elections and the results of our calculations for all contests, and for all contests with margins greater than 0.1%, 0.5%, or 1%. Section 4.1 that because of automatic manual recount laws in various states, it may make sense to omit contests with small margins from the workload estimates.

To audit cross-jurisdictional contests requires sampling from all cards cast in the contest, not just those cast in one jurisdiction. Since we did not have access to CVRs for other counties, the sample size estimates we report treat every contest in both elections as if it were entirely contained in Orange County. In particular, the estimates take the margins of statewide contests to be the margins within Orange County alone, and ignore the fact that the resulting audit burden would be shared across all jurisdictions with voters eligible to vote in those contests. The results still give a reasonable estimate of the workload required to audit a large number of (partially) overlapping contests simultaneously, and it is generally the *smaller* contests that drive audit workload for audits that do not use CSD, for reasons explained above. In particular, statewide contests appear on every ballot in each jurisdiction and on approximately the same fraction of cards in each jurisdiction (depending on the number of local contests in each jurisdiction). Moreover, because Orange County has more registered voters than 24 U.S. states, it is a reasonable proxy for many statewide audits.

The actual sample size depends on the luck of the draw—which particular cards end up in the sample—and on the errors in the CVRs for those cards. We estimate sample sizes using two assumed error rates: no error at all, and one 1-vote overstatement per 1,000 cards, i.e., a rate of 10^{-3} . (A one-vote overstatement occurs if the CVR has an error that increased the margin of a reported winner over a reported loser by one vote, e.g., if the card shows a valid vote for a loser but the CVR shows an undervote or overvote, or if the card shows an overvote, but the CVR shows a valid vote for a reported winner.) When CVRs are error-free, the sample size is deterministic. For the assumed rate of 10^{-3} , we generated artificial data that reflects a one-vote overstatement error every 1,000 ballots, starting with an error in the first CVR in the sample. The risk-measuring function is the ALPHA supermartingale [St23b], with the `optimal_comparison` estimator of [Sp23]. That estimator depends on an assumed rate of 2-vote overstatement errors in the CVRs, which we set to 10^{-4} .

4.1 Audits and Recounts

If a jurisdiction conducts a *manual* recount of the ballots after a robust canvass, there is no need for an RLA (some states allow machine recounts). Many U.S. states conduct automatic recounts for contests with small reported margins. Alabama, Arizona, Colorado, Connecticut, Delaware, Florida, New York, Ohio, Pennsylvania, and Washington recount

	Year	2020		2022	
1	Turnout	1,546,570		994,227	
2	Cards cast	3,094,308		1,989,416	
3	Total contests	181		214	
4	Exact ties	1		0	
5	Margins below 0.1%	1		3	
6	Margins below 0.5%	4		9	
7	Margins below 1.0%	5		14	
	Sample sizes	rate of 1-vote overstatements			
		0	10 ⁻³	0	10 ⁻³
8	all contests	20,112	37,996	62,251	119,814
9		(0.6%)	(1.2%)	(3.1%)	(6.0%)
10	omit margins ≤0.1%	15,964	33,852	22,110	33,215
11		(0.5%)	(1.1%)	(1.1%)	(1.7%)
12	omit margins ≤0.5%	9,228	11,347	11,053	14,125
13		(0.3%)	(0.4%)	(0.6%)	(0.7%)
14	omit margins ≤1%	7,827	9,634	8,123	9,980
15		(0.3%)	(0.3%)	(0.4%)	(0.5%)

Tab. 1: Summary of the 2020 and 2022 General Elections in Orange County, CA. Row 4 is the number of contests reported to be tied. Rows 5–7 are the number of contests with reported margins below 0.1%, 0.5%, and 1%, respectively. Rows 8–15 are the sample sizes to confirm all contests to a risk limit of 5%, expressed as the number of cards (rows 8, 10, 12, 14) or the percentage of all cards (in parentheses, rows 9, 11, 13, 15), when the audit finds no errors, or when the rate of one-vote overstatement errors is 1 in 1,000 CVRs. (A one-vote overstatement occurs if correcting the error reduces the margin between a reported winner and a reported loser by one vote, e.g., if the CVR erroneously counts a vote for the reported loser as an undervote.) When there is no error, the sample size is deterministic. When there are errors, the sample size depends not only on their rate, but on the order in which they occur. To simplify the calculations, we estimate the sample size by assuming that the first CVR shows an error, and thereafter errors are equispaced, one every 1,000 ballots. Rows 8 and 9 are for all contests, including tied contests. Rows 10 and 11 exclude contests with reported margins less than or equal to 0.1%, a threshold some states use for automatic recounts (see section 4.1). Rows 12 and 13 exclude contests with margins less than or equal to 0.5%, a common threshold for automatic recounts. Rows 14 and 15 exclude contests with margins less than or equal to 1%, another common automatic recount threshold. For the purpose of illustration, the calculations assume that every contest (including statewide contests) is entirely contained in Orange County.

contests with margins less than 0.5% (possibly with exceptions).¹³ Hawaii automatically recount if the margin is below 0.25%. Nebraska and Wyoming have automatic recounts if the margin is less than 1% of the winner’s tally. New Mexico and North Dakota automatically recount elections with margins less than 1%, 0.5%, or 0.25%, depending on the office. Ohio

¹³ https://ballotpedia.org/Election_recount_laws_and_procedures_in_the_50_states, last visited 2 July 2023. Washington’s automatic recounts are machine recounts, not hand recounts, so they do not obviate the need for an RLA.

has thresholds of 0.5% and 0.25%, depending on the office. Oregon has a threshold of 0.2%. South Carolina has a 1% threshold. Alaska, Montana, South Dakota, Texas, and Vermont automatically recount tied elections. Some states have a recount threshold based on the number of votes rather than the percentage margin; for instance, Michigan has automatic recounts for statewide contests with margins below 2,000 votes.

To understand how automatic recounts affect audit workloads, we estimate the number of ballots to inspect to audit all contests regardless of their margins, and all contests with reported margins greater than 0.1%, 0.5%, and 1%.

4.2 November 2020

In the November 2020 general election in Orange County, a total of 1,546,570 ballots (and 3,094,308 ballot cards) were cast in 181 contests. One contest was reported to be a tie, a margin of 0 votes: in the contest for Brea Olinda Unified School District Governing Board Member, Trustee Area 5, both Lauren Barnes and Gail Lyons were reported to receive 1,805 votes. Because the reported result was a tie, auditing this contest requires a full hand count. If there were no way to identify which cards contain this contest without manually inspecting the cards, a full hand count of that single contest would entail manually inspecting all 3,094,308 cards cast in the election. In all, 27 contests have diluted margins so small (with respect to all cards cast) that auditing each of them would require examining more than 99% of the cast cards, unless CSD are used.

But with CSD, auditing a contest never requires inspecting more cards than contain that contest. This reduces the workload substantially: the estimated workload to audit all 181 contests to a risk limit of 5% is only 20,112 cards in all, a reduction of more than 99%. Without the contest with margin less than 0.1%, the estimated sample size drops to 15,964 cards. Without the four contests with margins less than 0.5%, the estimated sample size drops to 9,228 cards. Without the five contests with margins less than 1%, the estimated sample size further drops to 7,827 cards. Table 2 lists the contests with margins under 1%, along with their margins and estimated sample size for that contest for a 5% risk limit RLA using CSD.

Figure 2 shows the proportion of ballot cards containing each contest that we would expect the RLA to inspect, versus the number of cards the contest appears on (both on log scale). In general, the sampling fraction decreases as the number of cards the contest appears on increases.

4.3 November 2022

In the November 2022 general election in Orange County, 994,227 ballots (comprising 1,989,416 cards) were cast in 214 contests. Several contests had small margins. For instance,

Contest	Cards Cast	Diluted Margin	Sample Size
Brea Olinda Unified School District Governing Board Member, Trustee Area 5	4,164	0	4,164
City of Irvine, City Council	129,948	0.2%	3,930
City of Lake Forest Member, City Council, District 1	10,042	0.2%	2,843
Proposition 17	1,546,210	0.4%	1,488
City of Laguna Beach Member, City Council	16,661	0.8%	746
South Coast Water District Director	22,046	0.9%	696
Member of the State Assembly 74th District	277,516	0.9%	652

Tab. 2: Contests with margins under 1% in the General Election in Orange County, CA, November 2020, number of cards cast, reported diluted margin, and estimated sample size to audit each of them to a risk limit of 5%, on the assumption that the CVRs have no errors.

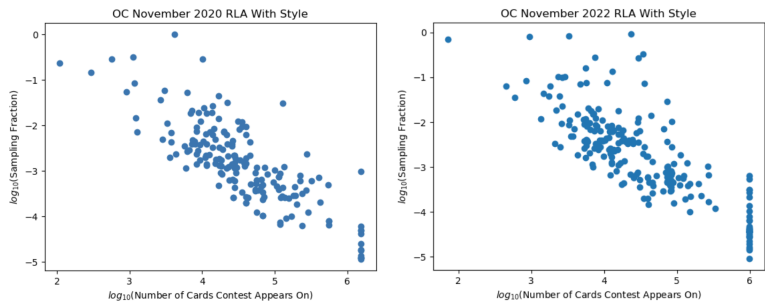


Fig. 2: Log of the sampling fraction (cards in the sample that contain the contest, divided by cards that contain the contest) versus the log number of cards the contest appears on, for a 5% risk limit RLA using CSD information, for General Elections in Orange County, CA, USA, in November 2020 (left panel, 181 contests) and 2022 (right panel, 214 contests). In general, for a given margin, larger contests with correct outcomes can be confirmed by examining a smaller fraction of the cards that contain the contest. The vertical set of points at the right edge of the plots are county-wide and statewide contests, which appear on the maximum possible number of cards. In 2020, all but one had a sampling fraction less than 1 in 10,000; the smallest was less than 1 in 100,000. In 2022, sampling fractions for the largest contests ranged from 1 in 100,000 to about 1 in 1,000.

in the vote-for-three Fountain Valley School District, Governing Board Member contest, the margin between the winner with the fewest votes, Phu Nguyen, and the loser with the most votes, Megan Irvine, was 0.02%. The City of Villa Park, City Council Member contest was also multiwinner plurality with three winners; the margin between the winner with the fewest votes (Jordan Wu) and the loser with the most votes (Donna Buxton) was 0.09%. The margin for Measure K in Costa Mesa, a simple majority contest, was 0.06%.

The estimated sample size to audit all 214 contests to a risk limit of 5% without using CSD is 1,989,415 ballot cards—essentially every card. Indeed, there are 33 contests which, if

each had been the *only* contest audited, would have required inspecting more than 99% of all cast ballot cards if CSD were not used to target the sample.

Using CSD reduces the estimated workload by 97%: the estimated sample size to audit all 214 contests to a risk limit of 5% is 62,251 ballot cards, about 3.1% of the cards cast. As mentioned above, state laws for automatic recounts typically have threshold margins of 1%, 0.5%, 0.25%, or 0.1%. Table 3 lists the contests with margins of 1% or less, their sizes, margins, and estimated sample size for a CSD RLA of each, at 5% risk limit, computed on the assumption that the CVRs are accurate. The right panel of Figure 2 plots sample sizes versus contest sizes for the 214 contests.

Contest	Cards Cast	Diluted Margin	Sample Size
Fountain Valley Sch Dist Governing Board Member	23,512	0.03%	21,772
K-City of Costa Mesa	34,626	0.06%	11,354
City of San Clemente Member, City Council	29,670	0.08%	7,999
City of Villa Park Member, City Council	3,260	0.1%	2,715
Ocean View Sch Dist Governing Board Member	35,990	0.2%	2,634
Orange Unif Sch Dist Governing Board Member, Trustee Area 4	73,665	0.3%	2,088
City of Westminster Member, City Council, District 1	7,467	0.3%	2,064
La Habra City Sch Dist Governing Board Member	12,915	0.3%	1,738
City of Los Alamitos Member, City Council, District 5	946	0.4%	750
Rossmoor Community Services District Director	5,540	0.6%	897
Member of the State Assembly 71st District	85,911	0.7%	873
City of Anaheim Member, City Council, District 2	10,997	0.7%	835
United States Senator Full Term	994,227	0.97%	626
City of Orange Mayor	43,813	0.99%	612

Tab. 3: Contests with margins under 1% in the General Election in Orange County, CA, November 2022, number of cards cast, reported diluted margin, and estimated sample size to audit each of them to a risk limit of 5%, on the assumption that the CVRs have no errors. Unif Sch Dist = Unified School District. The sample size does not decrease monotonically as the margin grows because the sample is drawn without replacement: the sampling fraction matters, too.

Without the three contests with margins below 0.1%, the estimated sample size would be 22,110 cards. Without the nine contests with margins below 0.5%, the estimated sample size would be 11,053 cards. Without the 14 contests with margins less than 1%, the estimated sample size would be 8,123 cards.

5 Discussion

It is prudent to give every contest outcome some audit scrutiny: auditing some contests has little bearing on whether the outcomes of other contests are correct. But conducting an RLA of a large number of partially overlapping contests with a wide range of sizes has

been thought to be logistically infeasible. By using CSD, the method of [GSS21] makes it practical to audit every contest in an election, which we illustrate using data from the 2020 and 2022 general elections in Orange County, California, the fifth largest election jurisdiction in the U.S., with more voters than 24 entire U.S. states. (With previous methods, auditing every contest in an election is generally more challenging in larger jurisdictions than in smaller ones, because larger jurisdictions have more contests and because the small contests are on a smaller fraction of the cards cast in the jurisdiction.)

CSD sampling would reduce the workload of a 5% risk limit RLA by more than 99% for the 2020 election and by 97% for the 2022 election compared to previous approaches. These estimates treat every contest in both elections as if they are entirely contained in Orange County. While this is not true for statewide contests, the estimates still give an idea of the workload to audit many overlapping contests simultaneously. These sample size estimates also assume that a card-level comparison audit could be conducted using all validly cast cards in Orange County. In reality, card-level comparison audits of cards cast in vote centers and polling places might require additional work, e.g., re-scanning cards centrally to create CVRs that are uniquely associated with individual cards. Non(c)esuch [St23a] could be used to avoid such re-scanning, but would require changes to the voting equipment to imprint nonces on cards as they are scanned. CSD-based sampling can also be used with ONEAudit [Stss] without re-scanning or changing the voting system, albeit with some increase in sample size. Future work will investigate the magnitude of that increase.

California law requires auditing the votes in approximately 1% of precincts. In 2020, Orange County’s statutory audit tabulated votes on 53,163 cards¹⁴ and in 2022, it tabulated votes on 51,346 cards.¹⁵ While it is easier to count the votes on all the cards in a precinct than to count the votes on the same number of cards selected at random, (i) the statutory 1% audit does not provide evidence that outcomes are correct, (ii) a CSD 5% risk-limit RLA would have involved examining fewer ballots in all in 2020, (iii) the CSD RLA generally involves transcribing data from fewer contests per audited card, and (iv) hand-counting teams generally comprise four people to tabulate votes on a single card, while comparison-audit teams generally comprise only two people.

CSD makes the recommendation of the 2018 National Academies report [Na18] practical: jurisdictions can efficiently audit every federal and state election contest as well as all local contests using samples that will generally comprise only a modest fraction of cards cast when reported outcomes are correct. An open-source Python implementation of the method is available at <https://github.com/pbstark/SHANGRLA/tree/main/shangr1a>.

¹⁴ <https://elections.cdn.sos.ca.gov/manual-tally/2020-general/orange.pdf> last visited 8 September 2023.

¹⁵ <https://elections.cdn.sos.ca.gov/manual-tally/2022-general/orange.pdf>, last visited 8 September 2023.

Acknowledgements.

We are grateful to the Orange County Registrar of Voters and its staff, including Justin Berardino, Roxana Castro, and Imelda Carrillo, for data, discussions, and comments on an earlier draft; and to Paul Burke for comments on an earlier draft. This work was supported by NSF Grant SaTC–2228884.

Bibliography

- [ADS20] Appel, A.W.; DeMillo, R.; Stark, P.B.: Ballot-marking devices cannot assure the will of the voters. *Election Law Journal, Rules, Politics, and Policy*, 19:432–450, 2020.
- [AS20] Appel, A.W.; Stark, P.B.: Evidence-Based Elections: Create a Meaningful Paper Trail, Then Audit. *Georgetown Law Technology Review*, 4.2:523–541, 2020.
- [GSS21] Glazer, Amanda K.; Spertus, Jacob V.; Stark, Philip B.: More style, less work: card-style data decrease risk-limiting audit sample sizes. *Digital Threats: Research and Practice (DTRAP)*, 2:1–15, 2021.
- [Na18] National Academies of Sciences, Engineering, and Medicine: Securing the Vote: Protecting American Democracy. The National Academies Press, Washington, DC, 2018.
- [OS19] Ottoboni, Kellie; Stark, Philip: Election Integrity and Electronic Voting Machines in 2018 Georgia, USA. In: *E-Vote-ID 2019 Proceedings*. 2019. Preprint: <https://ssrn.com/abstract=3426250>.
- [Ri18] Rivest, Ronald L.: Consistent sampling with replacement. <https://arxiv.org/pdf/1808.10016.pdf>, 2018.
- [Sp23] Spertus, J.V.: COBRA: Comparison-Optimal Betting for Risk-limiting Audits. The Workshop on Advances in Secure Electronic Voting, 2023. In Press.
- [St20] Stark, P.B.: Sets of Half-Average Nulls Generate Risk-Limiting Audits: SHANGRLA. *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, 12063, 2020.
- [St23a] Stark, P.B.: Non(c)esuch ballot-level risk-limiting audits for precinct-count voting systems. In (Katsikas, S. et al., ed.): *Computer Security. ESORICS 2022 International Workshops. Lecture Notes in Computer Science*, 13785. Springer, Cham, pp. 541–554, 2023.
- [St23b] Stark, Philip B.: ALPHA: Audit that Learns from Previously Hand-Audited Ballots. *Annals of Applied Statistics*, 17:641–679, 2023.
- [Stss] Stark, P.B.: ONEAudit: Overstatement-Net-Equivalent Risk-Limiting Audit. In: *Proceedings of the 8th Annual Workshop on Advances in Secure Electronic Voting (Voting’23)*. Springer, 2023 (in press).
- [WSSR21] Waudby-Smith, Ian; Stark, P.B.; Ramdas, Aaditya: RiLACS: Risk Limiting Audits via Confidence Sequences. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel; Germann, Micha, eds): *Electronic Voting*. Springer International Publishing, Cham, pp. 124–139, 2021.

Swiss Online Voting Redesigned

Oliver Spycher ¹

Abstract: Switzerland is one of the few countries with a strong record in online voting in national elections and votes. After 15 years during which parts of the electorate cast their vote online, the trials were brought to a halt in 2019. This short-paper summarizes the developments in Swiss online voting since 2019, when the trial framework was redesigned, allowing trials to take place again in 2023. This article is a non-scientific contribution aimed at providing the e-voting community with essential background information on Swiss online voting. Thereby it sets a focus on the new role of academia in the trial phase.

Keywords: Voting; Digitalization; Internet

1 Background

On the national level, Swiss citizens are called to the polls up to four times per year, be it to elect the members of the National Council or to give their “yes” or “no” on referenda or peoples’ initiatives. Typically, citizens also vote on cantonal and municipal issues on the same occasion. Over the past decades, voting from outside the polling station has become the norm, as up to 95% of the votes are cast by mail. The Swiss living abroad as well as people who have a disability that forces them to seek assistance to fill in their ballot call out for online voting. Studies suggest that the general population tends to be favorable towards online voting as well [gf23, gf20, Sw19].

Article 8a of the Federal Act on Political Rights (PRA; SR 161.1) offers the legal foundation for online voting trials. The first trials were conducted in 2004. In line with the Federal distribution of responsibilities in the political rights domain, the cantons are free to decide whether they participate in the trials, which partners they work with and thereby which system should be employed, whereas the Confederation imposes detailed requirements on the cantons. Notably, the Confederation’s requirements on online voting are far more stringent than for the paper-based voting channels and online voting even requires an authorization from the Confederation for each vote. All cantons that participated in the trials offered online voting to their citizens living abroad. Some cantons also offered online voting to their resident voters. As time passed, more and more cantons joined the trials. By

¹ Swiss Federal Chancellery, Political Rights Section, Federal Palace West, 3003 Bern, Switzerland. oliver.spycher@bk.admin.ch

the time of 2019, 15 out of 26 cantons had offered online voting on the Federal level at least on one occasion.

Throughout the years, the Confederation and the cantons acted along the lines of a “security first” approach. The Confederation imposed limits to the maximum number of citizens the cantons were allowed to offer online voting. In 2013, the Federal Chancellery, acting as the competent body on behalf of the executive government, enacted its Ordinance on Electronic Voting (OVE; SR 161.116) with new security-related requirements [Fe13]. The ordinance followed the logic of imposing strong security requirements in return for relaxing or even waiving the limits to the number of voters the cantons were allowed to provide with online voting. These requirements included “complete verifiability” – a feature which was detailed in the ordinance – and formal certification of the online voting system.

In 2019, online voting enjoyed broad public attention: Swiss Post – along with their software provider at the time – had their new system certified and some cantons announced to offer online voting with Swiss Post as their partner that same year. It was supposed to be the first trial with a certified system offering complete verifiability. During the same period of time, the Confederation had announced plans to end the trial phase and give online voting the status of an ordinary voting channel and passed a corresponding draft revision of the PRA to public consultation [Fe19b]. In response to a new requirement that the Federal Chancellery introduced to the OVE in 2018, the source code of Swiss Post’s new system was published. Based on an agreement between the Confederation and the cantons, a public intrusion test was carried out shortly thereafter. It was only at this stage of broad attention, when the actors involved in online voting had to learn that the new system and in particular the feature of complete verifiability was flawed. And they learned thanks to the voluntary work of independent academics from the e-voting community who looked into the system specification and the source code [Cu19, Ha20].

2 Redesigning the Trials

The flaws in the system stood witness for flaws in the overall trial framework: The requirements of the OVE dedicated to the software were meant to ensure that substantial mistakes are preempted. This did not work. The requirements on formal certification were meant to ensure that substantial mistakes are still caught in time. That did not work either. Publishing the source code and running a public intrusion test were meant to create incentives for independent experts from the public to examine the system and report on findings – that did not really work either, as the researchers who reported the substantial findings on complete verifiability clearly disapproved of the access policy to the published source code and chose not to participate in the program and follow the defined procedures. However, they agreed on a synchronized communication agenda with the involved actors supporting public discussion [Ha20]. In light of these insights, the trials were put to a halt and in June 2019 the Federal Council commissioned the Federal Chancellery to redesign the trials in collaboration with the cantons [Fe19a].

Subsequently, the Federal Chancellery appointed 23 experts from Switzerland and around the world, all holding a strong background relevant for contributing to Swiss online voting. Most of them were researchers from academia, some were from the IT security industry. In February 2020, the Federal Chancellery asked the experts for responses to a questionnaire that comprised 60 questions which included issues around cryptography, verifiability, security, scrutiny, trust and transparency, to name a few. Based on the responses to the questionnaire, the Federal Chancellery and the cantons held a moderated, written online dialog with the experts from 5 May to 17 July 2020. The insights of the dialog were compiled into a report [Fe20b] which offered a foundation for the changes to the framework then to be defined by the Federal Chancellery and the cantons. The Federal Chancellery and the cantons discussed and agreed on concrete measures that constitute the changes to the trial framework. They laid out these measures in a joint document called the “catalogue of measures”. The full catalogue as well as the reasoning that goes along with the measures are captured in their final report [Fe20a]. In consideration of the final report, the Federal Chancellery drafted revisions of the Ordinance on Political Rights (PoRo; SR 161.11) as well as the OEV and submitted both in a public consultation procedure lasting from 18 April until 28 August 2021 [Fe21a, Fe21b]. Finally, the Federal Government enacted the revised legal foundation on 25 May 2022 [Fe22b, Fe22c, Fe22a]. On 3 March and 16 August 2023 the Confederation approved requests of three cantons² to offer online voting at the Federal vote of 18 June 2023 and respectively at the elections to the National Council of 22 October 2023 for parts of their electorate [Fe23a, Fe23b].

3 The Redesigned Framework: Scrutiny

The revised legal foundation now sets the Federal Chancellery in charge of ensuring that online voting is examined, with the exception of the cantons remaining in charge of ensuring the certification of the information security management system of the system operator according to the ISO/IEC 27001 standard. The latter represents the only security-related formal certification required by the OVE. The remaining examinations are directly mandated by the Federal Chancellery to persons and organizations with the necessary skill set. In particular, academia now play an important part at scrutinizing online voting. The cryptographic protocol that stands in response to the requirements on complete verifiability as well as its implementation in the source code are mainly examined by institutions or individual researchers from academia. This decision is based on the insight that assessing online voting systems requires a skill set that grows through research activity in e-voting. The Federal Chancellery publishes the examination reports and uses them for assessing the cantons’ requests for authorizations.³ Both the Federal Chancellery and the cantons use them for assessing the need or the opportunity of establishing new measures and adding them to the catalogue. It is a deliberate decision to have multiple examinations performed for some of the scopes. It is thereby taken into account that – depending on their research

² The cantons of Basel-Stadt, St.Gallen and Thurgau

³ www.bk.admin.ch > Political Rights > E-Voting > Examination of systems

interests – experts assess the material from different angles. The Federal Chancellery does not impose any restrictions on what the experts are allowed to write in their reports or to state through any channel on the examined system or the examination itself.

In addition to the examinations mandated by Federal Chancellery, the OVE contains more stringent rules aiming at creating incentives for experts from around the globe to look into Swiss online voting systems and to take away concerns they might have regarding false allegations of misconduct. The system documentation and the source code must be published openly, i.e. without requiring interested persons to give their names, let alone to sign any agreements. The cantons must ensure that interested people may use the published material for any purpose, whereas the right to use the material commercially or to organize actual votes may be excluded. Also, they must ensure that people who report findings of value get paid for their work within a bug bounty program. System providers are obliged to guarantee and to explicitly state that they will not take any legal steps against people who do not follow the procedures for reporting findings. Only in cases where people use the published documentation for commercial purposes or to organize actual votes, may the system providers take legal action.

4 The Redesigned Framework: Constantly Getting Better

On the one hand, the measures reflecting the redesigned framework aim at ensuring a level of security and trustworthiness that is sufficient to mitigate the risks related to offering online voting at a given point in time. On the other hand – and this is a new key element – the measures are aimed at ensuring that over time online voting as a whole is constantly improved and the security features continuously strengthened and enhanced, that known flaws are corrected and that insights gained from actually conducting the trials are taken into consideration in the evolution of the upcoming trials. Accordingly, the catalogue of measures is revised on a running basis. It contains measures of various kinds: Improvements to the security and the quality of the employed system, corrections to the formal argumentation of compliance of the cryptographic protocol (*cryptographic* and *symbolic proofs*), but also substantial enhancements to cryptography-supported security features themselves, such as elaborating the possibility of introducing a public bulletin board and reducing trust assumptions, or introducing more independent components in order to avert single-points-of-failure [Fe23c]. There are measures dedicated to the voters' perspective, with regard to their voting experience, their trust and their behavior when it comes to making benefit of the security elements presented to them when voting. Moreover, measures are in place aiming at establishing and maintaining more partnerships between the actors in online voting and academia. Thereby the actors seek to contribute to research in the domain, with the natural goal of obtaining research results, but also with the goal of talents being educated to become e-voting researchers and at some point being available to online voting in Switzerland as scrutineers, advisors or experts involved at operations or as independent fact-checkers available to the media. We hereby emphasize the exceptional value of the

E-Vote-ID conference and we would wish to see more efforts directed at exchange and collaboration between EMBs and academia.

5 Concluding Remarks

The limits to the maximum number of online voters⁴ are now set back to *strict*, i.e. the Federal legislation does not allow to relax these limits in return for any particular efforts. This underlines the understanding obtained from the previous trial phase: there remains a lot to learn before going full scale – should this at all be the will of the legislator and the people in the future. We believe that despite all the known and unknown flaws the achievements so far are worth working with and worth building on and that the redesigned framework will contribute to trials that are purposive and sustainable.

References

- [Cu19] Culnane, Chris; Essex, Aleksander; Lewis, Sarah Jamie; Pereira, Olivier; Teague, Vanessa: Knights and Knaves Run Elections: Internet Voting and Undetectable Electoral Fraud. *IEEE Security Privacy*, 17(4):62–70, 2019.
- [Fe13] Federal Chancellery: Federal Chancellery Ordinance on Electronic Voting (VEleS) of 13 December 2013 (Status as of 15 January 2014). 2013.
<https://www.fedlex.admin.ch/eli/cc/2013/859/en>
Accessed 21 September 2023.
- [Fe19a] Federal Chancellery: e-Voting: Federal Council to reframe trial phase and delay introduction as a regular voting channel (media-release of 17 June 2019). 2019.
<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/bundesrat-beschliesst-naechste-schritte-zur-ausbreitung-der-elek.html>
Accessed 21 September 2023.
- [Fe19b] Federal Chancellery: Änderung des Bundesgesetzes über die politischen Rechte (Überführung der elektronischen Stimmabgabe in den ordentlichen Betrieb): Ergebnisbericht der Vernehmlassung vom 18. Juni 2019. 2019.
https://www.fedlex.admin.ch/de/consultation-procedures/ended/2018#https://fedlex.data.admin.ch/eli/dl/proj/6018/92/cons_1
Accessed 21 September 2023.
- [Fe20a] Federal Chancellery: Redesign and relaunch of trials - Final report of the Steering Committee Vote électronique (SC VE). 2020.
<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/berichte-und-studien.html>
Accessed 21 September 2023.
- [Fe20b] Federal Chancellery: Redesign of Internet Voting Trials in Switzerland 2020 - Summary of the expert dialog. 2020.

⁴ 10% nation-wide and 30% per canton

<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/berichte-und-studien.html>

Accessed 21 September 2023.

- [Fe21a] Federal Chancellery: Redesign of e-voting trials: consultation procedure opened (media-release of 28 April 2021). 2021.

<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/bundesrat-beschliesst-naechste-schritte-zur-ausbreitung-der-elek.html>

Accessed 21 September 2023.

- [Fe21b] Federal Chancellery: Teilrevision der Verordnung über die politischen Rechte und Totalrevision der Verordnung der BK über die elektronische Stimmabgabe (Neuausrichtung des Versuchsbetriebs): Ergebnisbericht der Vernehmlassung. 2021.

<https://www.fedlex.admin.ch/de/consultation-procedures/ended/2021>

Accessed 21 September 2023.

- [Fe22a] Federal Chancellery: E-voting: New legislation comes into force (media-release of 25 May 2022). 2022.

<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/bundesrat-beschliesst-naechste-schritte-zur-ausbreitung-der-elek.html>

Accessed 21 September 2023.

- [Fe22b] Federal Chancellery: Federal Chancellery Ordinance on Electronic Voting (VEleS) of 13 December 2013 (Status as of 1 July 2022). 2022.

<https://www.fedlex.admin.ch/eli/cc/2022/336/en>

Accessed 21 September 2023.

- [Fe22c] Federal Chancellery: Partial revision of the Ordinance on Political Rights and total revision of the Federal Chancellery Ordinance on Electronic Voting (Redesign of Trials): Explanatory report for its entry into force on 1 July 2022). 2022.

<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsbedingungen.html>

Accessed 21 September 2023.

- [Fe23a] Federal Chancellery: Federal Council approves resumption of online voting trials (media-release of 3 March 2023). 2023.

<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/bundesrat-beschliesst-naechste-schritte-zur-ausbreitung-der-elek.html>

Accessed 21 September 2023.

- [Fe23b] Federal Chancellery: Federal Council authorises use of online voting in 2023 National Council elections (media-release of 16 August 2023). 2023.

<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/bundesrat-beschliesst-naechste-schritte-zur-ausbreitung-der-elek.html>

Accessed 21 September 2023.

- [Fe23c] Federal Chancellery: Vote électronique: Catalogue of measures by the Confederation and cantons (version of 4 August 2023). 2023.

<https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsuübersicht.html>

Accessed 21 September 2023.

- [gf20] gfs-bern: Vorsichtige Offenheit im Bereich digitale Partizipation. 2020.
<https://www.digitale-mitbestimmung.bs.ch/bevoelkerungsumfrage.html>
Accessed 21 September 2023.
- [gf23] gfs-zürich: Einstellungen zu e-Voting. 2023.
<https://gfs-zh.ch/schweizer-bevoelkerung-befuerwortet-e-voting/>
Accessed 21 September 2023.
- [Ha20] Haines, Thomas; Lewis, Sarah Jamie; Pereira, Olivier; Teague, Vanessa: How not to prove your election outcome. In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 644–660, 2020.
- [Sw19] Swiss Confederation, State Secretariat for Economic Affairs: National eGovernment Study. 2019.
<https://www.digital-public-services-switzerland.ch/en/publications/studies>
Accessed 21 September 2023.

Setting international standards on digital election technologies: mapping trends and stakeholders

Adrià Rodríguez-Pérez¹ , Jordi Barrat Esteve² 

Abstract: In recent years, there has been a surge of international standards on digital election technologies: recommendations, guidelines, compendiums, etc. Whereas the legal character of some of these instruments may be put into question, there is no doubt that they prescribe certain good or ideal behaviour that electoral stakeholders should follow when digital technologies are introduced in electoral processes. This paper aims at taking stock of the development of these standards, assessing their degree of legalization, and mapping the stakeholders behind these standard-setting efforts. With this goal in mind, up to 37 international standards on digital election technologies are first identified. These standards deal with issues ranging from broader concerns about the introduction of digital technologies in elections and its compliance with international obligations to the observation and procurement of digital election technologies, as well as with cybersecurity and data protection issues. We are able to demonstrate that although these standards are (still) far from creating an international regime on digital election technologies, they do share many things in common: low levels of obligation and delegation, but high levels of precision that help complement actual hard-law instruments in the electoral field. Second, the paper discusses if the development of these standards can be framed in the context of the Governance Triangle and/or the institution of multi-stakeholderism. Far from what is seen in other areas of global and Internet governance, cooperation between different types of international actors is currently limited: most of the standards being either developed by States, intergovernmental organisations (IGOs), or non-governmental organisations (NGOs) independently.

Keywords: digital election technologies; international standards; soft law; international regime theory; legalization, Governance Triangle; multi-stakeholderism.

1 Introduction

In recent years, there has been a surge of international standards on digital election technologies³. Whereas the Council of Europe's Recommendation(s) on e-voting tends to be considered the only international standard(s) proposing a legal regulation in the field [Dr14; Dr17; EG20; SW14], it is actually coupled by guidelines, guides, compendiums, methodologies, frameworks, handbooks and manuals, as well as reports and technical

¹ ScytI Election Technologies, S.L.U., 08021, Barcelona, Spain adria.rodriguez@scytI

² Universitat Rovira i Virgili, 43002, Tarragona, Spain jordi.barrat@urv.cat

³ Throughout the paper, we will use the term “digital election technologies” to refer to the use of digital technologies with a view to replace and/or supplement different steps throughout the electoral cycle. This terminology is preferred to alternatives such as “digital technology/ies in elections”, since these could well include more basic tools used in elections, such as e-mail or office tools. However, we do not aim at implying that elections are digital, but the analysed technologies are.

documents, to mention just a few examples. All these instruments prescribe certain good or ideal behavior that electoral stakeholders (i.e., election management bodies, directly or indirectly; election observation groups; or even election technology providers) should follow when digital technologies are introduced in electoral processes by either translating, developing, and/or complementing higher international obligations for elections into the digital field. Therefore, and regardless of their legal character, they can be considered international standards.

This paper aims at taking stock of the development of these standards, mapping their degree of legalization, and identifying who is behind these standard-setting efforts. Therefore, this paper aims at answering several questions:

- What are the main international standards on digital election technologies?
- In which areas do these international standards provide guidance?
- What kind of international instruments are preferred when it comes to enshrining international standards and good practices on digital election technologies?
- What is their degree of legalization? Is it already possible to speak of an international regime for digital election technologies?
- Who is taking the lead and which actors are formally involved in these standard-setting efforts?
- Do different classes of actors collaborate in the development and review of these standards?

In our opinion, this effort is necessary at a time when multiple standards are being developed on the matter. Studying these standards is important because they impact election policy-making at the national level. More specifically, standards may be used by certain election observers missions to assess compliance and provide recommendations for improvement; by law-makers and policy-makers to make changes to the electoral framework; by election administrations when they make decisions on implementation; or even by donors before providing grants to beneficiary countries and/or organisations for electoral assistance projects.

All in all, with this exercise we aim at providing a first approach to the current constellation of standard-setting efforts in the field of digital election technologies. We argue that activity in this field has multiplied in recent years and that it is important to ensure the coherence, cohesion, and coordination between different initiatives. Therefore, we do not aim so much to analyse in detail all the existing standards, but rather to take stock of the bigger picture. Furthermore, we compare our findings to similar fields in the areas of global and Internet governance with a view to identify similarities and differences as well as to map current trends.

To do so, the first four questions are first addressed: section 2 provides a list of the main international standards on election technologies; we discuss their framing in the context of the legalization trend in global governance and as part of a growing body of soft law; and we discuss whether there is a nascent international regime on digital election technologies. Subsequently, section 3 addresses the two latter questions. We discuss the involvements of states and intergovernmental organisations (IGOs), non-governmental organisations (NGOs) as well as firms in the efforts to develop these standards (or their absence thereof) and compare it to other fields of global and Internet governance. Lastly, section 4 provides a summary of the main findings, identifies broader trends in these standard-setting efforts, and suggests future research lines.

2 Which international standards on digital election technologies?

2.1 From international law to soft-law and international standards

Sources of international law include, according to art. 38 of the Statue of the International Court of Justice: conventional law (treaties, conventions, etc. between States); customary law (derived from the practice of States); and general principles of international law. Additionally, case-law and doctrine are considered subsidiary means for the determination of these sources.

In the field of elections, however, provisions in these kinds of instruments tend to be scarce: article 25 (a) of the International Covenant on Civil and Political Rights (ICCPR), art. 3 of Protocol No. 1 to the to the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), art. 23(3) of the American Convention on Human Rights, art. 13(1) of the African Charter on Human and Peoples' Rights or art. 24(3) of the Arab Charter on Human Rights are the main examples. These instruments tend to only enshrine the right to vote and to list some basic and high-level principles for democratic elections (i.e., universal, equal, secret suffrage, etc.). When it comes to digital election technologies, no references can be found in any such legal instrument at all, at least for the time being.

By contrast, many (legal) provisions on digital election technologies are to be found in so-called soft law instruments: recommendations, codes of conduct, guidelines, etc. Soft law tends to be preferred by international actors to hard law in certain circumstances, such as when sovereignty issues are at the core of the standards [AS00]. Therefore, being central to the relationship between the state and its citizens, it should not come as a surprise that most standards on elections (whether they relate to digital technologies or not) are to be found in this kind of instrument.

The case of international standards on election technologies is, in this regard, not an exception. In this sense, Kenneth W. Abbot and Duncan Snidal already concluded that “most international law is “soft” in distinctive ways” [AS00]. Soft law is, in this regard, understood as “nonbinding rules or instruments that interpret or inform our understanding

of binding legal rules or represent promises that in turn create expectations about future conduct"[GM10]. According to Andrew T. Guzman and Timothy Meyer, soft law may be preferred to hard law for different reasons. For example, these instruments may be preferred by "lower ranking officials who are knowledgeable about a particular area without going through potentially cumbersome bureaucratic processes associated with making a binding agreement" [GM10]. It is not difficult to see the similarities between these examples and the development of some international standards on digital election technologies, such as those adopted by the Council of Europe.

Beyond soft law, and according to Benedict Kingsbury, Nico Krisch and Richard B. Stewart, the choice for alternative legal approaches could be framed within the emergence of global administrative law [KKS05]. In this regard, it is not difficult to imagine the development of international standards on digital election technologies as being "determined by transnational administrative bodies -including international organizations and informal groups of officials- that perform administrative functions" [KKS05], such as election management bodies, international observer groups, and/or international organisations providing technical assistance on elections.

More recently, Joost Pauwelyn, Ramses A. Wessel and Jan Wouters have framed this process as an active political preference and choice by international actors, or what they call "informal international law-making" [PWW14]. According to these authors, there is nothing administrative in many political initiatives at the international level, from the G20 or the adoption of "Guidelines for Implementation" of the Framework Convention on Tobacco Control by the World Health Organisation [PWW14].

Taking this literature into account, we have decided to broadly understand as an international standard any international source that prescribes certain good or ideal behaviour that electoral stakeholders should follow. Therefore, these may encompass anything from recommendations by international organisations to compendiums and guides on good practices in digital election technologies. At the same time, these standards must be international, meaning that they are aimed at different stakeholders in different countries, either global and/or regionally.

With this broad understanding of international standards, we have been able to map up to 37 different international standards in the field of digital election technologies. A chronological list with these standards can be found in the Appendix. From this point forward, we will be referring to these standards using the number in this list (e.g., the Venice Commission's *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe* will be referenced as [1]).

Some clarifications are necessary regarding our choice of standards. On one side, these are international standards. This means that they are developed to be implemented in more than one country, be it at a global or regional scale. Standards that are developed for one country only (e.g., a technical specification to develop and/or procure a country's election

technologies) are not taken into account. On the other side, it is important to stress that these are standards that specifically address issues of digital election technologies. We understand that standards for democratic elections also apply to the use of technology and that references to digital technology may be included in standards that do not deal specifically with this subject. However, our focus is on addressing international instruments that only touch upon digital election technologies and that do it directly.

With this scope in mind, we can see that the number of international standards has increased steadily in the last two decades. We observe that the first of these standards were adopted in the early 2000s, and some of them have undergone updates since they were first adopted (for example, the Council of Europe’s standards, first adopted in 2004 [2], were complemented in 2010 [8] and 2011 [9][10], updated in 2017 [19] and additional guidelines have been recently adopted to complement the core of the updated Recommendation [33]; the Carter Center’s *Developing a Methodology for Observing Electronic Voting* [4] became a *Handbook on Observing Electronic Voting* in January 2012 [13]; and most recently the IFES’ HEAT process for cybersecurity and elections [24] has been complemented with their reference document on understanding cybersecurity throughout the electoral process [31].

Still chronologically, it is possible to see some patterns. For example, in recent years there have been international standards adopted every year, whereas this was not always the case for the period between 2004 and 2010 (there were no new standards in 2005, 2006, 2008 and 2009). The only exception here would be 2021. It is also possible to see that the number of standards adopted in some years is considerably higher than in others, with four standards being adopted in 2010, 2011, and 2019, five in 2018, and up to seven in 2022.

Tab. 1: Chronological evolution of the international standards on digital election technologies

Year	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
New standards	2	0	0	2	0	0	4	4	1	1	2	1	1	2	5	4	1	0	7	1
Total standards	2	2	2	4	4	4	8	12	12 ⁴	13	15	16	17	16 ⁵	21	25	25	25	32	33

Another interesting classification of these international standards is by topic. We can find general standards dealing with the introduction of technology in elections and its compliance with international obligations for elections (12 standards, representing 32% of all identified standards); on election cybersecurity (11 standards, 29%); on how to observe election technology (6 standards, 16%), as well as issues of transparency and certification (4 standards, 11%); on specific technologies (2 standards, 5%); on data protection (2 standards, 5%); as well as on procurement (1 standard, 3%)⁶.

⁴ In 2012, standard [13] replaced standard [4].
⁵ In 2017, standard [19] replaced standards [2], [9], and [10].
⁶ The total number of standards in this count is 38 because standard [14] has been considered as dealing both with the introduction of technology in elections and its compliance with international obligations for elections as well as on how to observe election technology.

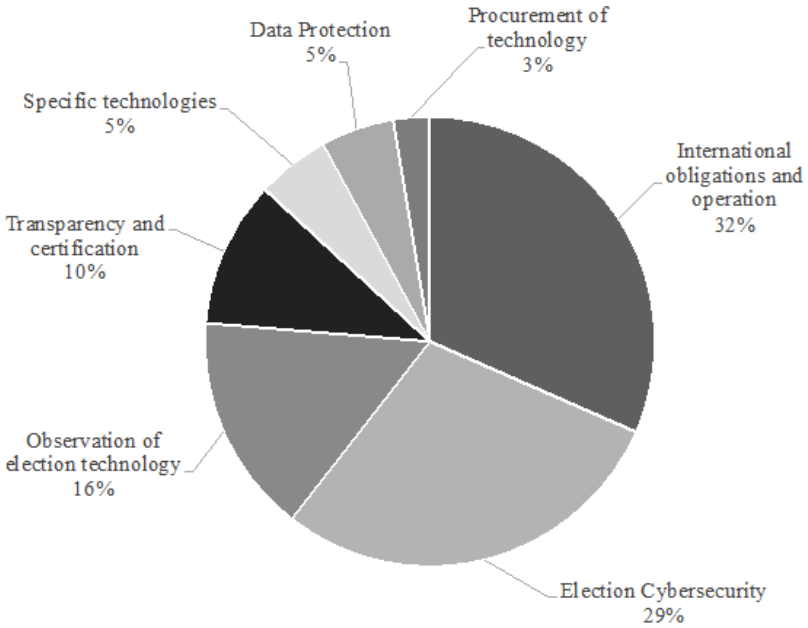


Fig. 1: Distribution by topic of the international standards on digital election technologies.

2.2 A nascent international regime on election technologies?

A question that arises upon identifying this growing body of international standards on digital election technologies is whether it is possible to locate such efforts as part of the development of an international regime on digital election technologies. International regimes are the set of “principles, norms, rules and decision-making procedures around which actor expectations converge in a given issue-area” [LYZ95]. With this basic definition, it could well seem that this set of standards could account for a set of principles, norms, rules and decision-making procedures around which actor expectations converge in the field of digital election technologies.

International regimes are, however, not homogeneous. For example, Marc Levy, Oran R. Young and Michael Zürn [LYZ95] identify up to three ideal types of international regimes, depending on their level of formality and the actual convergence of expectations by the international actors with the principles, norms, rules and decision-making procedures: classic regimes (high levels of both formality and convergence of expectations), tacit regimes (high levels of convergence of expectations but low levels of formality), and dead-letter regimes (high levels of formality but low levels of convergence of expectations). If we consider these standards as a high level of formalisation, then there could be reasons to

speak about a classic or a dead letter regime. In any case, and considering that these are mostly young standards for which it is hard to assess the convergence of expectations, it may be yet to soon to speak about an international regime on digital election technologies.

An alternative approach to assess the degree of legalization of these standards is provided by Kenneth W. Abbot et al. [Ab00]. These authors identify “a particular set of characteristics that institutions may (or may not) possess”. More specifically, these characteristics are [Ab00]:

- **Obligation:** States or other actors are bound by a rule or commitment or by a set of rules or commitments. Binding rules oblige actors to behave in a certain way.
- **Precision:** Rules unambiguously define the conduct they require, authorize or proscribe. Precise rules establish well-defined conditions for actors to behave in a certain way.
- **Delegation:** Third parties are granted authority to implement, interpret, and apply rules; to resolve disputes; and (possibly) to make further rules. Delegation processes establish the conditions for the participation of new authorities along the normative process.

According to the authors, any institution can be located somewhere between high and low levels of obligation, precision, and delegation. For our case, it seems obvious that these international standards have neither high levels of obligation (they are not binding) nor delegation (no third party can in principle implement, interpret, and apply them). On the other hand, however, they tend to be quite precise. This means that international standards on digital election technologies could be located in an ideal type of legalization (Type VII in the classification by the authors) at the same level as the Helsinki Final Act, the Nonbinding Forest Principles; or most of the technical standards [Ab00].

3 Who is behind the standard-setting efforts?

Hand in hand with the trend towards setting soft-law standards goes the proliferation of non-state actors responsible for their development and adoption. For example, Kenneth W. Abbot and Duncan Snidal identify different instances that involve non-state actors at the global level: “[i]nternational conferences and organizations have become more accessible to private groups, allowing them to act internationally as well as domestically. Transnational advocacy coalitions have emerged congruent with the scope of international issues and [...] individual governmental units have increasingly engaged in transnational rule making” [AS00]. Likewise, authors in the field of global administrative law also acknowledge that “increasingly important are regulation by private international standard-setting bodies and by hybrid public-private organizations that may include, variously, representatives of businesses, NGOs, national governments, and intergovernmental organizations.” [KKS05]. In this section of the paper, we explore whether any such trends can also be identified in the

field of international standards on digital election technologies. To do so, we resort to two different approaches or frameworks: the Governance Triangle [AS09] and the institution of multi-stakeholderism [RD15].

3.1 States and intergovernmental organisations, non-governmental organisations... and firms?

One useful way to map the involvement of different kind of actors in global governance is to resort to Kenneth W. Abbot and Duncan Snidal's Governance Triangle [AS09]. The Governance Triangle aims at tacking stock of "a plethora of non-state and public-private governance arrangements focused on setting and implementing standards" [AS09]. Whereas the Governance Triangle was conceived to map standards in the field of global production—including labour rights, human rights, and the environment—it has been used in other areas. For example, Robert Gorwa has recently used this framework to conceptualise the informal regulation of online content moderation [Go].

Three main types of actors are identified in the Triangle:

- States, by definition the only sovereign actor in international relations. In the Triangle, States and intergovernmental organizations (IGOs), as groups of States, are understood under a single category.
- Firms, namely those organisations focused by law and culture on profits [AS09].
- Non-governmental organisations (NGOs), a broad category that includes "advocacy groups, labour unions, consumer groups, socially responsible investors, social movements, and other non-commercial groups" [AS09]. NGOs are also private actors since they represent the private interests of their members, but they are not focused on profits.

To illustrate the involvement of one or more classes of actors in the development of the standards, the Triangle is divided into seven different zones [AS09]:

- In each vertex (zones 1-3), only one class of actor adopts and implements standards: States and intergovernmental organizations (IGOs), as groups of States (zone 1); firm and industry self-regulatory schemes (zone 2); and NGOs and NGO coalitions (zone 3).
- In the quadrilaterals along each side (zones 4–6), schemes are included in which actors from two groups are involved: States (including IGOs) and firms (zone 4); States (including IGOs) and NGOs (zone 5); and firms and NGOs (zone 6).
- The central triangle includes those standards in which actors of all three types play a role (zone 7).

Lastly, it is important to stress that the triangle depicts only the direct participation by States, Firms, and NGOs⁷ in these standard-setting efforts [AS09].

When mapping the standards identified above in the Governance Triangle, the following classification is obtained:

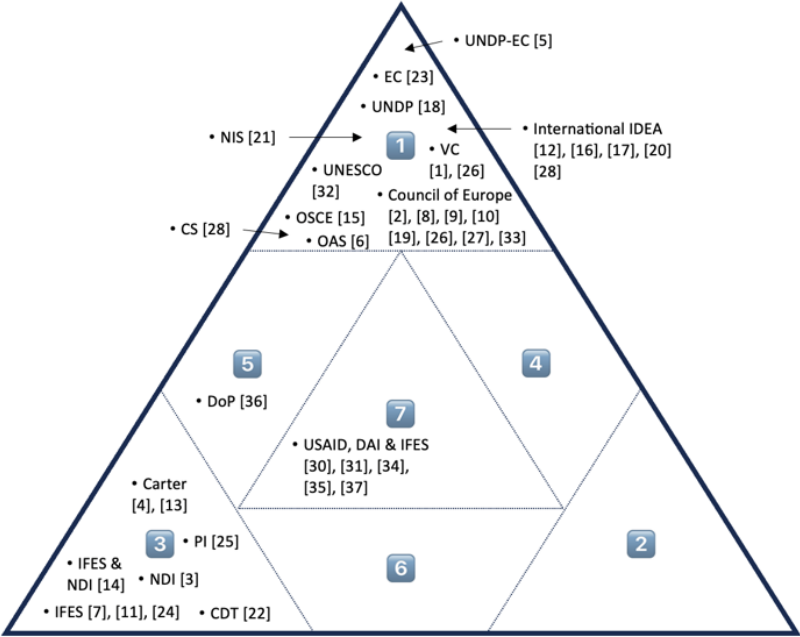


Fig. 2: The “Governance Triangle” of international standards on digital election technologies.

Therefore, this analysis allows us to draw three main conclusions:

- Most of the standards are developed by one class of actor independently: either by States (including IGOs), with 23 standards (zone 1), representing 59% of all identified standards; or by NGOs, with 9 standards (zone 3), representing 24% of all identified standards.
- Direct cooperation between different types of actors in the development of international standards on digital election technologies is limited. The exception is the cooperation between States (including IGOs), NGOs and firms in the context of the series on cybersecurity by USAID, DAI, and IFES ([30], [31], [34], [35], [37]), as well as between States (including IGOs) and NGOs as members of the Declaration of Principles for International Election Observation (DoP) in [36] (zone 5).

⁷ Whereas informal participation may be important as well, it is first necessary to identify which actors have a formal standing to take part in these initiatives and in which capacity.

- The involvement of Firms in the development of international standards on digital election technologies is residual, and the only instance of their participation we have found⁸ is hand in hand with other actors (namely, States and NGOs) in zone 7. In turn, zones 2, 4 and 6 include no standards at all.

Tab. 2: International standards on digital election technologies on the Governance Triangle

Zone		Standards
1: States (including IGOs)	[1] Venice Commission (VC)	[2] Council of Europe
	[5] Joint EC-UNDP Task Force	[6] The OAS
	[8] Council of Europe	[9] Council of Europe
	[10] Council of Europe	[12] International IDEA
	[15] OSCE/ODIHR	[16] International IDEA
	[17] International IDEA	[18] UNDP
	[19] Council of Europe	[20] International IDEA
	[21] NIS Cooperation Group	[23] European Commission
	[26] Council of Europe	[27] VC and Council of Europe
	[28] International IDEA	[29] The Commonwealth Sec.
	[32] UNESCO	[33] Council of Europe
2: Firms	-	
3: NGOs	[3] NDI	[4] The Carter Center
	[7] IFES	[11] IFES
	[13] The Carter Center	[14] IFES and NDI
	[22] CDT	[24] IFES
4: States (including IGOs) and firms	[25] Privacy International	
	-	
5: States (including IGOs) and NGOs	[36] DoP Organizations	
6: Firms and NGOs	-	
7: All	[30] USAID, DAI and IFES	[31] USAID, DAI and IFES
	[34] USAID, DAI and IFES	[35] USAID, DAI and IFES
	[37] USAID, DAI and IFES	

⁸ Furthermore, the consideration of DAI as an electoral stakeholder merits discussion. In this regard, DAI is indeed a private development company, but they do not seem to be working much in the field of elections. According to their website, they do work on Governance, but the areas identified in their website are limited to Local Governance and Decentralization; Public Financial Management and Domestic Revenue Mobilization; Anti-corruption, Transparency, and Accountability; Justice, Citizen Security, and Rule of Law; Institutions Building and Policy Reform; Public Administration and Civil Society Strengthening; and Legislative Strengthening (see: <https://www.dai.com/our-work/solutions/governance>). A quick search on their website does reveal their involvement in some electoral assistance projects (although not in the area of digital technologies), but it is more likely that their participation in the developments of the standards is due to their expertise in cybersecurity rather than to DAI being considered electoral stakeholders actively involved in digital election technologies.

3.1.1 Inchoated multi-stakeholderism?

Given the exceptionality of the standards located in zones 5 and 7, it is worth exploring the impact of multi-stakeholderism (or rather, its absence) in the development of international standards on digital election technologies. Compared to the Governance Triangle, an approach based on multi-stakeholderism has three main advantages:

- It focuses on how different classes of actors cooperate to achieve a common goal. In fact, the institution of multi-stakeholderism itself is understood as “two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature” [RD15].
- Captures the fact that cooperation between different classes of actors may take different forms, what Mark Raymond and Laura DeNardis describe as “polyarchic authority relations” [RD15]. In this regard, distinct classes of actors may possess different formal powers (heterogeneous polyarchy) or have similar formal powers (homogeneous polyarchy) [RD15].
- States and IGOs are considered separately [RD15], allowing for a more granular analysis of the different initiatives.

We have used Mark Raymond and Laura DeNardis’ matrix (2015) to classify the standards identified above in which more than one type of actor is involved in the standard-setting effort. It must be noticed that, in contrast to the Governance Triangle, States and IGO are considered as different categories of international actors under multi-stakeholderism, and therefore more standards than those in zones 4 to 7 in the Triangle (see section 3.1) fall under the current analysis. More specifically, the following standards initially located in zone 1 are now considered to be the result of a multi-stakeholder effort: [1], [2], [9], [10], [19], [21], [26], [27], [33]. All in all, the results are shown in Table 3.

When we use this framework to analyse the above-mentioned standards, it becomes evident that out of the 37 standards, only a handful are developed by different classes of international (and, more specifically, by States, IGOs, as well as NGOs, and to a lesser extent firms). The fact that numerous standards are developed together by States and IGOs should not come as a surprise, even if they are framed within forms of heterogeneous polyarchy (as we will discuss further in section 4 below).

4 Conclusions, trends, and discussion

Since 2004, a growing body of international standards prescribe how digital technologies should be introduced in electoral processes: there are currently 33 such standards in force, out of 37 standards that have been developed. These standards take different forms and names: recommendations, guidelines, guides, compendiums, methodologies, frameworks,

Tab. 3: Inchoated multi-stakeholderism in the setting of international standards on digital election technologies?

Stakeholder type	Nature of Authority Relations		
	Hierarchy	Polyarchy	
		Heterogeneous	Homogeneous
States, IGOs, Firms, NGOs		[30], [31], [34], [35], [37]	
States, IGOs, Firms			
IGOs, Firms, NGOs			
States, IGOs, NGOs			
States, Firms, NGOs			
States, IGOs		[1], [2], [9], [10], [19], [21], [26], [27], [33]	
States, Firms			
States, NGOs			
IGOs, Firms			
IGOs, NGOs			
Firms, NGOs			[36]

handbooks and manuals, as well as reports and technical documents, to mention just a few examples. They deal with many issues, from the introduction of technology in elections and its compliance with international obligations to cybersecurity and data protection, as well as methodologies for election observation. Whereas this body of standards is not sufficiently cohesive to be considered an international regime per se, the fact that most of these standards complement and refine higher-level obligations makes us think that more and more standards will be developed in the future. The current adoption trend also seems to support this prediction.

When it comes to the actors involved in this standard-setting effort, our analysis reveals three main trends:

Trend 1: Intergovernmentalism as the golden standard. Standard-setting in digital election technologies is still dominated by public actors, mainly States and IGOs: 23 standards, representing 59% of all identified standards, have been developed by these two classes of actors alone (and up to 28, representing 76% of all standards, in cooperation with other classes of actors). Amongst them, the recommendations by the Council of Europe could be considered the “golden” standard. According to Aleksander Essex and Nicole Goodman, the recommendations of the Council of Europe “are the only intergovernmental documents

that focus on regulation and standardization of voting technologies. All other international documents can be characterized as guidelines, efforts to formalize procedures, or provide advice regarding good practices” [EG20]. In their standard-setting efforts, the Council of Europe has opted for an intergovernmental approach, with the participation of its member States, in the framework of specific committees and (working) groups: a ‘multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting’ for the original Recommendation [Dr14; SW14]; an Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) for its updated version [Dr17; Ro22]; and more recently in the framework of a dedicated working group of national experts on democracy and technology (GT-DT) established by the European Committee on Democracy and Governance (CDDG) [DVK22]. The same approach has been followed for the adoption of [33] by the Cybercrime Convention Committee (T-CY) under the Budapest Convention. Beyond the Council of Europe, the work of International IDEA also should be mentioned. In this case, the organisation seems to have relied mostly on the work of its Secretariat to produce up to five different standards in the field. Lastly, the contribution of other regional IGOs active in the field of election observation, such as the OSCE/ODIHR the OAS and more, should also be stressed under this intergovernmental trend.

Trend 2: More stakeholders, not much more multi-stakeholderism. Beyond States and IGOs, there is a growing number of NGOs who are also involved in the standard-setting efforts, with 9 standards, representing 24% of all identified standards, being developed by this class of actors alone (and up to 14, representing 41% of all standards, in cooperation with other classes of actors). Likewise, the involvement of for-profit actor is also a recent phenomenon that can be identified in the multi-stakeholder efforts under the series of standards developed jointly by USAID, DAI and IFES (where DAI would be the only for-profit actor). In fact, and even if most of the standards have been developed independently and without cooperation among different classes of actors, some instances of multi-stakeholderism can already be observed: private actors are growingly involved hand-in-hand with public ones in such efforts. This is the clear case of the DoP and, to a lesser extent, the already mentioned work of USAID, DAI, and IFES. In this regard, it is worth analysing the standards in which NGOs, as private actors, are involved. The technical document by the DoP [36], and to a lesser extent the reports issued by USAID in cooperation with DAI and IFES (the series including [30], [31], [34], [35], [37]), indicate that elections may also benefit from mechanisms that are not that unusual in other areas. In this regard, the DoP is the only instance of homogeneous polyarchy in multi-stakeholder international standard-setting on digital election technologies and a clear example of a joint effort where a common goal, which in this case consists of establishing standards for election observation, may pave the path for a fruitful cooperation between States and non-profit civic organisations. The document on technologies is only the last output of a series of guidelines that have been endorsed by a plurality of organizations. When it comes to the DoP, it worth considering its governance (that is, who is deciding what and in particular who decides the membership): beyond the ones who launch the process, any other incorporation needs the approval of the current members thereby establishing a

filter that allows the network to maintain a consistent approach and an internal cohesion. Having said that, some form of inchoated multi-stakeholderism, even if under heterogeneous polyarchy, can be identified as well in the case of the standards mentioned under Trend 1 above. For example, the Council of Europe's committees and (working) groups were open to other Council of Europe's bodies, intergovernmental committees and even IGOs⁹. Likewise, their work has been supported by the contribution of independent experts [Dr17; DVK22], even if this class of actor is not necessarily framed with sufficient independence either in the Governance Triangle or within multi-stakeholderism. It is for this reason that we have considered standards [2],[9],[10],[19]¹⁰,[33]¹¹, as well as [26]¹², as instance of multi-stakeholderism under heterogeneous polyarchy (since only member States had the right to vote).

Trend 3: The absence of for-profit electoral stakeholders. Looking both at the Governance Triangle and the institution of multi-stakeholderism, it is quite apparent that an important gap or pending task exists: while States, IGOs and NGOs manage to establish different cooperation schemes, for-profit companies remain outside this circle. Such exclusion prompts different question marks because in fact companies could be one of the most knowledgeable stakeholders when dealing with election technologies: as election technology vendors, auditors, or certification and accreditation agencies, to name just a few examples. Therefore, it is worth wondering why most standards have been developed without some form of participation of specialized firms. Moreover, such absence is even more important when other sensitive areas, where standards are also needed, have large experience involving any actor, whether for-profit or not, in a constructive dialogue (e.g., the United Nation's Global Compact and the more recent Global Digital Compact, as well as the Council of Europe's digital partnership). Regarding this aspect, the absence of firms in the development of international standards in digital technologies could seem at first justified. In general terms, when addressing this issue, an alleged conflict of interests would prevent any cooperation between States or IGOs with private companies. While the latter would just pay attention to their revenues, the former would be concentrated in the public interest.

⁹ In contrast, and in spite of being one of the conclusions ahead of the update of Rec(2004)11, the review mechanisms fell short of being open "to the full range of stakeholders, e.g. civil society actors, e-voting systems providers and possibly non-member states"[SW14]. To the best of our knowledge, private stakeholders were only invited to the second meeting of CAHVE, with considerable short deadlines, and after the drafting process had concluded. As for the more recent adoption of the Guidelines on ICT and elections, private stakeholders do not seem to have been involved at all[DVK22]. Notwithstanding, representatives from an NGO and an election technology provider were invited to a recent Conference on "E-voting and use of Information and Communication Technologies (ICT) in elections: taking stock and moving forward", organised by the Council of Europe on 16 June 2023 in Strasbourg, France.

¹⁰ The terms of reference of the CAHVE can be found in the following link: https://search.coe.int/cm/Pages/result_details.aspx?objectId=09000016805c40c4 [accessed: 13 September 2023]

¹¹ The terms of reference of the CDDG for the current biennium can be found in the following link: https://search.coe.int/cm/Pages/result_details.aspx?objectId=0900001680a74d3c#globalcontainer [accessed: 13 September 2023]

¹² The list of observer organisations to the Cybercrime Convention Committee the T-CY can be found in the following link:<https://www.coe.int/en/web/cybercrime/parties-observers> [accessed: 13 September 2023]

However, such incompatibility has reached a higher-level, even apparently forbidding any public dialogue. It is not just in decision-making, but in the mere discussion which they are formally absent (e.g., because of the fear that proposals coming from for-profit entities will pollute what is supposed to become a neutral, orthodox and unbiased cooperation between impartial entities, that is: States, IGOs and NGOs).

Based on these three trends, we could draw yet another conclusion: the development of international standards in the field of digital election technologies and the involvement of different kinds of actors in such efforts deserves to be further studied. Whereas this paper does not intend to develop a comprehensive approach on how to build a confident relationship between such actors, the analyses mapped in the Governance Triangle and through the institution of multi-stakeholders provide enough evidence that something is missing when it comes to setting international standards in digital election technologies. Why can we not use what works elsewhere here? A future paper will dig into such a question, but it is time already to provide a couple of indicators that could facilitate the dialogue.

Firstly, it is important to remember that firms need clarity and stability. Moreover, firms can only undertake their tasks where public authorities enjoy citizen confidence. Finally, election management bodies, private vendors and civil society organisations all pursue the same outcome, that consists of a successful delivery of the elections. Having these premises in mind, it seems reasonable to bring all stakeholders on board and to keep them informed. This is especially relevant to elections as at least some steps of the electoral process very much rely on the capacity of service providers.

Secondly, a sort of confusion between discussions and decision-making seems to exist when a cooperation between public and private entities is proposed. Any dialogue should make a clear distinction between both phases, and, in terms of standards, it seems clear that States or IGOs will be the ones taking the final decision. However, it is nonetheless important to incorporate solid grounds, and normally firms –and to a lesser extent some NGOs– are the ones, and often the only ones, with enough knowledge and practical experience to nurture the debate accordingly. In this regard, it cannot be forgotten that for profit actors not only include technology vendors, but also auditors and certification agencies as well. At the same time, a better balance between the in-house capacities of election administrations on election technologies will likely pave the path for a more natural cooperation among all stakeholders that could result in standards decided by public authorities and endorsed by private firms and NGOs after a transnational and open participatory mechanism.

References

- [Ab00] Abbott, K. W.; Keohane, R. O.; Moravcsik, A.; Slaughter, A.-M.; Snidal, D.: The Concept of Legalization. *International Organization* 54/3, pp. 401–419, 2000.

- [AS00] Abbott, K. W.; Snidal, D.: Hard and Soft Law in International Governance. *International Organization* 54/3, pp. 421–456, 2000.
- [AS09] Abbott, K. W.; Snidal, D.: CHAPTER TWO. The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State. In (Mattli, W.; Woods, N., eds.): *The Politics of Global Regulation*. Princeton University Press, Princeton, pp. 44–88, 2009, ISBN: 9781400830732, URL: <https://doi.org/10.1515/9781400830732.44>.
- [Dr14] Driza Maurer, A.: Ten years Council of Europe Rec(2004)11: Lessons learned and outlook. In (Krimmer, R.; Volkamer, M., eds.): *6th International Conference on Electronic Voting*. Lochau/Bregenz, Austria, pp. 111–117, Oct. 2014.
- [Dr17] Driza Maurer, A.: Updated European Standards for E-voting. In (Krimmer, R.; Volkamer, M.; Braun Binder, N.; Kersting, N.; Pereira, O.; Schürmann, C., eds.): *Electronic Voting. E-Vote-ID 2017*. Vol. 10615, Springer International Publishing, Cham, pp. 146–162, 2017.
- [DVK22] Driza Maurer, A.; Volkamer, M.; Krimmer, R.: Council of Europe Guidelines on the Use of ICT in Electoral Processes. In: *Computer Security. ESORICS 2022 International Workshops*. Vol. 13785, Springer International Publishing, Copenhagen, Denmark, pp. 585–599, 2022.
- [EG20] Essex, A.; Goodman, N.: Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada. *Election Law Journal: Rules, Politics, and Policy* 19/2, pp. 162–179, May 2020.
- [GM10] Guzman, A. T.; Meyer, T. L.: International Soft Law. *Journal of Legal Analysis* 2/1, pp. 171–225, Mar. 2010, ISSN: 2161-7201.
- [Go] Gorwa, R.: The platform governance triangle: conceptualising the informal regulation of online content, tech. rep. 2, *Internet Policy Review*.
- [KKS05] Kingsbury, B.; Krisch, N.; Stewart, R. B.: The Emergence of Global Administrative Law. *Law and Contemporary Problems* 68/3/4, pp. 15–61, 2005, ISSN: 00239186, URL: <http://www.jstor.org/stable/27592106>, visited on: 09/15/2023.
- [LYZ95] Levy, M. A.; Young, O. R.; Zürn, M.: The Study of International Regimes. *European Journal of International Relations* 1/3, pp. 267–330, 1995.
- [PWW14] Pauwelyn, J.; Wessel, R.; Wouters, J.: When Structures Become Shackles: Stagnation and Dynamics in International Lawmaking. *European Journal of International Law* 25/, pp. 733–763, Oct. 2014.
- [RD15] Raymond, M.; DeNardis, L.: Multistakeholderism: anatomy of an inchoate global institution. *International Theory* 7/3, pp. 572–616, 2015.

- [Ro22] Rodríguez-Pérez, A.: The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update? In (Krimmer, R.; Volkamer, M.; Duenas-Cid, D.; Rønne, P.; Germann, M., eds.): *Electronic Voting. E-Vote-ID 2022*. Vol. 13553, Springer International Publishing, Cham, pp. 90–105, Sept. 2022, ISBN: 978-3-031-15910-7.
- [SW14] Stein, R.; Wenda, G.: The Council of Europe and e-voting: history and impact of Rec(2004)11. In (Krimmer, R.; Volkamer, M., eds.): *6th International Conference on Electronic Voting, EVOTE 2014*, Lochau / Bregenz, Austria. IEEE, pp. 1–6, 2014.

Appendix I: International standards on digital election technology

1. The Venice Commission's Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe (March 2004)
2. Council of Europe's Recommendation Rec(2004)11 of the Committee of Ministers to Member States on Legal, Operational and Technical Standards for E-voting (September 2004)
3. NDI's Monitoring Electronic Technologies in Electoral Processes: An NDI Guide for Political Parties and Civic Organizations (2007)
4. The Carter Center's Developing a Methodology for Observing Electronic Voting (October 2007)
5. Joint EC-UNDP Task Force on Electoral Assistance's Procurement Aspects of Introducing ICT Solutions in Electoral Processes: The Specific Case of Voter Registration (2010)
6. The Organization of American States' Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions (2010)
7. IFES' Direct Democracy: Progress and Pitfalls of Election Technology (2010)
8. Council of Europe's E-voting handbook (October 2010)
9. Council of Europe's Guidelines on transparency of e-enabled elections (February 2011)
10. Council of Europe's Certification of e-voting systems: Guidelines for developing processes that confirm compliance with prescribes requirements and standards (February 2011)
11. IFES' Electronic Voting & Counting Technologies: A guide to Conducting Feasibility Studies (May 2011)
12. International IDEA's Policy Paper on Introducing Electronic Voting: Essential Considerations (December 2011)

13. The Carter Center's Handbook on Observing Electronic Voting (January 2012)
14. IFES' and NDI's guide on Implementing and Overseeing Electronic Voting and Counting Technologies (2013)
15. OSCE/ODIHR's Handbook For the Observation of New Voting Technologies (2014)
16. International IDEA's guide on The Use of Open Source Technology in Elections (2014)
17. International IDEA's guide on Certification of ICTs in Elections (2015)
18. UNDP's guide on Electoral Results Management Systems (August 2016)
19. Council of Europe's Recommendation CM/Rec(2017)5 of the Committee of Ministers of the Council of Europe to member States on standards for e-voting, including its Explanatory Memorandum and the Guidelines on the implementation of the provisions of the recommendation (June 2017)
20. International's IDEA's guide on Introducing Biometric Technology in Elections (June 2017)
21. NIS Cooperation Group's Compendium on Cyber Security of Election Technology (July 2018)
22. Center for Democracy & Technology, Election Cybersecurity 101 Field Guide, several installments: Vol. 1 - Two Factor Authentication (August 2018); Vol 2 – Passwords (September 2018); Vol 3 – DDoS Attack Mitigation (November 2018); Vol. 4 – Cloud Services (July 2020); Vol. 5 – Physical Security (October 2020); glossary (September 2018).
23. European Commission, Commission guidance on the application of Union data protection law in the electoral context A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 (September 2018)
24. IFES' framework on Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Training (HEAT) Process for Election Management Bodies (October 2018)
25. Privacy International's briefing on Technology, data and elections: A "checklist" on the election cycle (June 2019)
26. Council of Europe's T-CY Guidance Note #9 Aspects of election interference by means of computer systems covered by the Budapest Convention (July 2019)
27. Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections (June 2019)

28. International IDEA's guide on Cybersecurity in Elections: Models of Interagency Collaboration (July 2019)
29. The Commonwealth Secretariat's Cybersecurity for Elections A Commonwealth Guide on Best Practice (2020)
30. USAID, DAI and IFES' Primer: Cybersecurity and Elections (2022)
31. USAID, DAI and IFES' Understanding cybersecurity throughout the electoral process a reference document (2022)
32. UNESCO's Elections in digital times: a guide for electoral practitioners (2022)
33. Council of Europe's Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States (February 2022)
34. USAID, DAI and IFES' Briefing paper on Cybersecurity and voter registration (July 2022)
35. USAID, DAI and IFES' Briefing paper on Cybersecurity of Election Results Management Systems (October 2022)
36. DoP organizations' technical document on General principles and guidelines related to ICT and elections (December 2022)
37. USAID, DAI and IFES' Electoral Cybersecurity: A Brief Guide for Donor Program Development (February 2023)

Index of Authors

A

Aranha, Diego F., 53

B

Battagliola, Michele, 53

Bitussi, M., 71

C

Cortier, Véronique, 189

Costa, Núria, 143

D

Duenas-Cid, David, 93, 125

E

Erb, Yannick, 93

Esseiva, Olivier, 169

Esteve, Jordi Barrat, 263

F

Finogina, Tamara, 143

G

Gaudry, Pierrick, 189

Glazer, Amanda K., 239

Glondou, Stéphane, 189

H

Haenni, Rolf, 39

Hilt, Tobias, 203, 221

Høgåsen, Audhild, 169

I

Iova, Radu Antonio Serrano, 119

K

Kořánová, Ilona Starý, 39

Kulyk, Oksana, 221

L

Loeber, Leontine, 125

Longo, R., 71

M

Macias, Ryan, 125

Mällo, Tanel, 203

Marino, F. Antonio, 71

Martin-Rozumiłowicz, Beata, 125

Monnat, Xavier, 169

Morelli, U., 71

P

Pointcheval, David, 19

R

Rodríguez-Pérez, Adrià, 143, 263

Roy, Lawrence, 53

Ruhault, Sylvain, 189

S

Sein, Kati, 203

Sharif, A., 71

Spadafora, C., 71

Spertus, Jacob V., 239

Spycher, Oliver, 255

Stark, Philip B., 239

T

Tomasi, A., 71

V

Volkamer, Melanie, 93, 203, 221

W

Willemson, Jan, 203