Towards Long-Term Free and Secret Electronic Elections Providing Voter-Verifiability in the Bulletin Board Model

Lucie Langer
TU Darmstadt
Theoretical Computer Science
Hochschulstraße 10
64289 Darmstadt, Germany
langer@cdc.informatik.tu-darmstadt.de

Melanie Volkamer
CASED
Mornewegstraße 32
64293 Darmstadt, Germany
volkamer@cased.de

Stefan G. Weber
TU Darmstadt
Telecooperation
Hochschulstraße 10
64289 Darmstadt, Germany
sweber@tk.informatik.tu-darmstadt.de

Axel Schmidt
TU Darmstadt
Theoretical Computer Science
Hochschulstraße 10
64289 Darmstadt, Germany
axel@cdc.informatik.tu-darmstadt.de

Johannes Buchmann
TU Darmstadt
Theoretical Computer Science
Hochschulstraße 10
64289 Darmstadt, Germany
buchmann@cdc.informatik.tu-darmstadt.de

ABSTRACT

From a legal point of view, freedom and secrecy of the vote are as important as transparency and verifiability of the election. However, it is a challenge to reconcile the corresponding requirements for electronic voting schemes. This paper analyzes the link between individual verifiability on the one hand and anonymity, receipt-freeness and coercion-resistance on the other hand. We approach the issue by analyzing remote as well as paper-based cryptographic voting schemes which make use of public bulletin boards. We investigate to which extent the considered protocols meet the above requirements, especially in the long term when computational assumptions may no longer hold. We also give ideas on how to improve the protocols in this respect. The paper aims at providing an overview in order to support election hosts such as companies, associations and government agencies in selecting appropriate e-voting schemes with respect to the priority of either freedom and secrecy of the vote or voter-verifiability.

Categories and Subject Descriptors

D.2.1 [**Software Engineering**]: Requirements/Specifications; E.3 [**Data Encryption**]: [Public key cryptosystems]; H.4.3 [**Information Systems Applications**]: Communications Applications—*Bulletin boards*

ICEGOV2009, November 10-13, 2009, Bogota, Colombia

General Terms

Security, Standardization, Theory

Keywords

Electronic Voting, Security Requirements, Verifiability, Long-Term Anonymity

1. INTRODUCTION

Regarding democratic elections, a fundamental objective laid down in constitutional law is secrecy of the vote. It requires that only the voter knows his voting decision and nobody else is able to gain information about it. Moreover, secrecy of the vote is a precondition of casting one's vote freely and without coercion [19]. If the voter fears that his decision becomes public in the future, the freedom of vote is clearly limited. Thus, secrecy of the vote should hold not only during the election, but also in the future [25]. Still, it is arguable whether a voter's decision will be a matter of interest 20 years after the election. Long-term anonymity may, however, be a crucial point on the way to electronic voting in parliamentary elections. For example, German Basic Law requires the secrecy of the vote to hold forever [28].

The legal terms of secrecy and freedom of vote have to be translated to a more technical language if one wants to analyze voting protocols with respect to these requirements. In [25] it is stated that "the legal objectives of free and secret elections are related to anonymity, receipt-freeness and coercion-resistance of electronic voting". Thus, voting schemes should ensure long-term anonymity, receipt-freeness and coercion-resistance. However, current electronic voting protocols often rely on the security of underlying cryptosystems, which is temporally limited: Cryptosystems that provide computational security may be broken at some point in the future, e.g. by brute force attacks based on increased computational power or by solving an underlying mathematical problem that is widely believed, though unproved, to be

hard.

Another fundamental objective for democratic elections is transparency and verifiability. This was also stressed by a recent judgement of the German Federal Constitutional Court: The use of specific electronic voting machines in the last federal election of the German Bundestag was ruled unconstitutional[1] because the machines did not provide a sufficient level of voter-verifiability. This shows the importance of individual verifiability for legally binding electronic elections. Moreover, it emphasizes the need for a continuous dialog between jurists and computer scientists.

The use of bulletin boards has become a fundamental means to ensure individual and universal verifiability in an electronic election. However, public bulletin boards come along with the following challenge: Anyone able to read the bulletin board can copy the published information and store it. Then, however, temporally limited security becomes an issue: If, for example, encrypted votes are published next to the voters names, an adversary can simply wait until the encryption system is broken in the future. This compromises anonymity as well as receipt-freeness and coercion-resistance in the long term. Besides public bulletin boards, two more areas can be identified which are potentially affected by this threat: The network used for data transmission and the archiving system used for retention of electronic election data. This work focuses on bulletin boards and does not consider these two areas. However, we take them up in the following section.

Our paper aims at identifying relations and dependencies between different levels of individual verifiability on the one hand and anonymity, receipt-freeness and coercion-resistance on the other hand. We introduce a classification of these requirements which is comprehensible to both computer scientists and jurists. Then we analyze selected remote as well as paper-based cryptographic voting protocols regarding the question to which extent they meet the considered requirements. We also give ideas on how to improve the protocols in order to achieve a higher level of anonymity. The result can support election hosts such as companies, associations and government agencies in selecting appropriate voting schemes with respect to the legal priority of either voter-verifiability or (long-term) freedom and secrecy of the vote.

The paper is structured as follows. In Section 2 we review related work. Section 3 provides the definitions and classifications we use for our analysis of selected electronic voting protocols in Section 4. Section 5 concludes the paper.

2. RELATED WORK

Long-term security of e-voting and long-term anonymity in particular has been addressed in [10, 12, 20, 25]. In [12] it is stated that "secrecy requirements must be unconditionally ensured regardless of ongoing technological improvements". Similarly, in [25] it is pointed out that "we have to take into account that both, the computational resources as well as the knowledge on cryptography will steadily increase in the future." But a voting scheme which publishes encryptions of the votes usually relies on computational assumptions and therefore is only computationally private [20]. As observed in [10], electronic voting schemes often provide only computational election secrecy and do not even consider this to be questionable. However, if everlasting secrecy of the vote is to be achieved one cannot rely on computational assumptions.

The interrelations and trade-offs between different requirements for electronic voting have been studied in [7, 18]. Chevallier-Mames et al. define an election scheme to be unconditionally anonymous if nobody learns more about the votes than what is leaked by the tally [7]. The authors show that one generally cannot achieve universal verifiability of the tally and unconditional anonymity of the votes unless all the registered voters participate in the election. Similarly, it is not possible to have both universal verifiability and receipt-freeness unless one makes strong assumptions such as secure channels. Lambrinoudakis et al. have investigated to which extent current remote voting protocols comply with security requirements for electronic voting [18]. The authors also identify interrelated and contradicting properties, e.g. individual verifiability and coercion-resistance.

Long-term retention of electronic election data has been addressed in [9, 26]. The Council of Europe [9] recommends that "data retained after the election or referendum period shall be stored securely," which is specified by providing several copies on several mediums stored in different places. The Common Criteria Protection Profile [26] defines a basic set of security requirements for online voting systems. It requires that the election data which is retained cannot be used to link the voter and his vote in plaintext or in encrypted form. However, privacy-preserving retention of election data is useless if the data has previously been published on a bulletin board.

Long-term anonymity for electronic voting in open networks has been addressed for example in [16]. The authors show that an attacker tapping the communication channels is able to break anonymity in the long term, although he cannot prove the link between the voter and his vote to third parties in general. Juels et al. argue that anonymous channels can be implemented in a practical way, e.g. by using public terminals for vote casting [14]. An adversary may be able to view Internet communication but not to trace back IP addresses to voters. However, the issue of securing the physical communication channels in an online election is out of the scope of this work. We consider the protocol level rather than the physical layer and examine the election data published on the bulletin board in light of two questions:

- To which extent can the published data be used to compromise anonymity, receipt-freeness and coercion-resistance in the long term?
- To which extent does the scheme provide individual verifiability?

3. DEFINITIONS AND CLASSIFICATIONS

As we strive to be understood by readers without detailed technical knowledge such as election hosts in general, the following definitions are rather intuitive and informal. Formal definitions can be found for example in [13, 14].

3.1 Bulletin Board, Ballot and Vote

A *bulletin board* is a public channel where data can be published by authorized participants only and, once published, cannot be erased or overwritten by anyone. This communication model was first presented by Benaloh et al. [8, 5] and supports verifiability in electronic voting schemes.

[1] see `http://www.bverfg.de/en/press/bvg09-019en.html`

In the following, a *ballot* denotes the message which is issued by the voter in order to cast a *vote* for a specific candidate. Hence, the ballot masks the actual vote. The ballot could for example be an encryption of the vote.

3.2 Anonymity, Receipt-Freeness and Coercion-Resistance

We consider an outside adversary. Depending on the connection between the adversary and the voter as introduced in [17], we distinguish the following levels of secrecy and freedom of vote at protocol level:

Anonymity. The vote cannot be linked to the voter who cast it. There is no communication channel between the voter and the adversary. The adversary can only use the information published on the bulletin board.

Receipt-Freeness. The voter cannot prove to an adversary how he voted. There is a one-way communication channel from the voter to the adversary: The voter can send messages to the adversary, but the adversary cannot send messages to the voter.

Coercion-Resistance. The adversary cannot coerce the voter to vote in a particular way. There is a two-way communication channel between the voter and the adversary: Both voter and adversary can send messages to each other.

In the scenario of anonymity, the voter does not cooperate in order to prove his vote. In contrast, for receipt-freeness, the channel from the voter to the adversary conveys the voter's willingness to cooperate with the adversary. The messages sent can be considered as receipts. While the adversary is passive in this setting and restricted to receiving messages from the voter, the scenario of coercion-resistance considers an active adversary who can, for example, furnish the voter with voting material to be used. Additionally, the adversary can use the information published on the bulletin board in both settings. Note that, as the adversary capabilities are gradually amplified, coercion-resistance implies receipt-freeness, and receipt-freeness implies anonymity.

3.3 Long-Term vs. Short-Term

For the protocols analyzed in Section 4 we investigate whether each of the requirements defined in Section 3.2 is met in the long term or in the short term only. We define *in the short term* to be a period of up to ten years as it is reasonable to assume that cryptographic algorithms remain secure at least for this period of time if the underlying parameters (e.g. keylength) are chosen properly. This should also cover the legislative period of the elected body in most cases.

By contrast, *in the long term* refers to the time when 20 years or more have passed since the election was carried out. Cryptographic primitives used e.g. for encryption will possibly have been broken at that time.

3.4 Individual Verifiability

Individual verifiability or voter-verifiability expresses the chance for the voter to assure himself that his vote was correctly recorded and included in the tally. We distinguish basic and advanced individual verifiability as follows:

Basic Individual Verifiability. Each voter can verify that his vote has been cast. Verifiability extends only to the existence of the ballot, not to its content: The voter can verify that his ballot is published on the bulletin board, but there is no proof provided that the ballot contains the vote which the voter intended to cast.

Advanced Individual Verifiability. Each voter can verify that his vote has been cast as intended. Verifiability extends to the existence of the ballot and a proof regarding its content: The voter can verify that his ballot is published on the bulletin board, and is additionally provided with a proof that the ballot contains the vote which the voter intended to cast.

4. ANALYSIS OF SELECTED PROTOCOLS

In the following we analyze remote as well as polling booth based cryptographic voting protocols which make use of bulletin boards. We chose the protocol designed by Ohkubo et al. [23] as a representative protocol using blind signatures, the work of Juels et al. [14] for anonymous credentials, and the Helios 2.0 scheme [2] for homomorphic encryption. Furthermore, we selected Prêt à Voter [6] as a representative for paper-based e-voting and Neff's scheme [21] for electronic voting machines.

In the following we first give a brief description of the considered protocol. Only the main features of the protocols are provided to the extent to which they are important with respect to our analysis. Then we analyze the protocols with respect to anonymity, receipt-freeness, coercion-resistance on the one hand and individual verifiability on the other hand. We also give ideas for improvements.

4.1 Notation

In the following P denotes a participant, e.g. a voter or a tallier. Angle brackets indicate that the information enclosed is published on the bulletin board. Apart from the terms which are explained in the text or which are self-explanatory, we use the following notation:

V_i	voter i
ID_i	ID of voter i
BB	bulletin board
R	registration authority
T	tallying authority
C_j	candidate j
v_i	vote cast by voter i
b_i	ballot cast by voter i, containing the vote v_i
prf_P	zero-knowledge proof(s) provided by P
$encr_P(\cdot)$	encryption with P's public key
$decr_P(\cdot)$	decryption with P's secret key
$sig_P(\cdot)$	signature using P's secret signing key
$ver_P(\cdot)$	verification using P's public signing key

4.2 Blind Signatures: Ohkubo et al.

The protocol designed by Ohkubo et al. [23] is an improvement of the Fujioka et al. scheme [11] which was one of the first voting schemes based on blind signatures and anonymous channels.

Summary. The participants of the scheme are voters, a trustworthy registrar, and several talliers. Each voter encrypts his vote using the talliers' public key and then gets the encryption blindly signed by the registrar. The voter unblinds the signature and sends the encryption as well as

the signature to the bulletin board via an anonymous channel.[2] The talliers check the signature, cooperatively decrypt the votes and publish the voting results.

Setup. Let $bl_r(\cdot)$ denote a blinding procedure with random blinding factor r and $unbl_r(\cdot)$ the corresponding unblinding procedure. V_i encrypts the vote as $x_i = encr_T(v_i)$ sends the blinded encrypted vote and his signature to R:

$$V_i \longrightarrow R : ID_i, bl_r(encr_T(v_i)), sig_{V_i}(bl_r(encr_T(v_i)))$$

If the voter is eligible and has not applied for a signature before, R signs $bl_r(encr_T(v_i))$ and sends it back to V_i:

$$R \longrightarrow V_i : d_i = sig_R(bl_r(encr_T(v_i)))$$

At the end of the registration phase, R publishes the values he obtained from the voters:

$$R \longrightarrow BB : \langle ID_i, bl_r(encr_T(v_i)), sig_{V_i}(bl_r(encr_T(v_i)))\rangle \, \forall i$$

V_i unblinds d_i, i.e. computes $y_i = sig_R(encr_T(v_i))$ and verifies R's signature.

Voting. The voters use an anonymous channel to send their encrypted vote furnished with R's signature to the bulletin board:

$$V_i \longrightarrow BB : \langle x_i, y_i\rangle = \langle encr_T(v_i), sig_R(encr_T(v_i))\rangle$$

Tallying. The talliers T verify R's signature, cooperatively decrypt the votes by computing $v_i = dec_T(x_i) \forall i$ and publish the tally.

Analysis. Alongside the voter ID, the blinded encrypted vote signed by the voter is published on the bulletin board. The voter can check that the published values equal the ones he sent to the registrar. Hence, only **basic individual verifiability** is provided. Advanced individual verifiability can be achieved as follows: Supposed that a probabilistic encryption scheme is used, the encrypted vote is unique: As decryption must be unambiguous, it is not possible to have a different vote $v_i' \neq v_i$ such that $encr_T(v_i') = encr_T(v_i)$. Thus, the voter can recognize his vote next to his ID on the bulletin board by unblinding $bl_r(encr_T(v_i))$.

The relation between the encrypted ballot x_i and the voter's identity ID_i is hidden by the blind signature scheme. Anonymity is thus maintained even if the cryptographic primitive used for encryption is broken in the future. This is due to the blindness property, i.e. unlinkability of $e_i = bl_r(x_i)$ and the signature y_i of x_i. The random value r ensures that an adversary cannot learn anything about the signed message. This holds as long as the random blinding factor r remains secret. Thus, the scheme offers **long-term anonymity**.

The scheme is **not receipt-free** as the voter can reveal both r and the randomness used for encrypting the vote, thus providing the adversary with the means to verify that the correct vote is contained in $bl_r(encr_T(v_i))$ which is published next to the voter ID.

[2]Ohkubo et al. suggest that the anonymous channel is realized by employing a mixnet. This changes the voting scheme slightly as the voters use the mixnet's public key to encrypt the vote which was encrypted with the tallier's key beforehand. However, as this is not relevant to our approach, we refer to the basic scheme.

4.3 Anonymous Credentials: Juels et al.

The scheme proposed by Juels et al. was the first one to offer coercion-resistance in terms of protecting the voter against forced abstention, randomization and simulation attacks [14]. (This interpretation is compatible with our definition of coercion-resistance provided in Section 3.) After the scheme was published, several proposals for improvements followed [24, 27, 3], of which only the last one succeeds in maintaining coercion-resistance. However, as the improvements in [3] only pertain to efficiency, they are not relevant to our approach. Thus, we stick to the original scheme.

Summary. The participants are voters, trustworthy registrars, and several talliers. The scheme employs anonymous credentials for voter authentication. They are distributed in the registration phase via an untappable channel. The indirect authorization by means of anonymous credentials also allows for multiple voting: If a voter wants the vote to be accounted, he includes his valid credential; if not, an invalid credential is attached. The voter can hereafter vote again, this time casting a valid vote. The resistance to coercive attacks is based on the inability of the adversary to distinguish invalid credentials from valid ones. An anonymous channel is required in the voting phase, to allow for unsupervised voting in the moment the actual valid vote is cast. A modified version of the ElGamal scheme is used for probabilistic encryption. Hence, coercion-resistance holds under the Decisional Diffie-Hellman assumption.

Setup. R verifies V_i's eligibility, issues a credential σ_i over an untappable channel and publishes its encryption next to the voter ID:

$$\begin{aligned} R \longrightarrow V_i : &\quad \sigma_i \\ R \longrightarrow BB : &\quad \langle ID_i, encr_T(\sigma_i)\rangle \end{aligned}$$

Voting. The ballot cast by V_i contains ciphertexts of both the chosen candidate and the credential as well as a zero-knowledge proof of validity:

$$V_i \longrightarrow BB : \langle b_i\rangle = \langle encr_T(v_i), encr_T(\sigma_i), prf_{V_i}\rangle$$

Tallying. In the tallying phase, ballots with invalid zero-knowledge proofs are discarded first, yielding two lists A_1 (encrypted votes) and B_1 (encrypted credentials). Then, ballots with duplicate credentials are removed, keeping only the latest ones. Let A_2 and B_2 denote the corresponding lists. In the next step the lists A_2 and B_2 are mixed using the same, secret permutation, resulting in lists A_3 and B_3. Then the list of valid encrypted credentials which was created in the registration phase is mixed as well. Next, votes in list A_3 which correspond to invalid credentials in B_3 are eliminated by means of blind credential checks against the list of valid encrypted credentials which was created in the registration phase. Finally the votes are cooperatively decrypted by T and tallied.

Analysis. The scheme offers only **basic individual verifiability** as the voter does not obtain a proof on the correct content of his ballot. Advanced individual verifiability can be achieved in a similar way as for the Ohkubo et al. scheme [23]: As a probabilistic encryption scheme is used,

both the encrypted vote and the encrypted credential are unique. Thus, the voter can recognize his ballot on the bulletin board. However, this is not considered in the protocol.

The bulletin board contains the list of encrypted credentials alongside the voter IDs and the list of all submitted ballots consisting of encrypted vote, encrypted credential and zero-knowledge proofs. Hence, the voter ID is linked to the encrypted credential, and the encrypted credential is linked to the encrypted vote. It follows that, in the long term, voter ID and vote can be linked. It then suffices to trace the voter ID back to the voter and anonymity is compromised. Thus, the scheme offers only **short-term anonymity**. Therefore, we propose that encrypted credentials should not be published alongside the plaintext names of the voters. Still, both lists, i.e. the voters' register as well as the list of encrypted credentials should be published for the sake of verifiability. Hence, an improvement in terms of long-term anonymity would be to detach the lists and scramble them already in the registration phase in order to hide the relation between the voter and the encrypted credential. For the voter it would be sufficient to see the anonymized list of encrypted credentials published on the bulletin board and obtain a proof from the registrars that the encryption of his credential is valid and contained in this list. However, this approach cannot save receipt-freeness and coercion-resistance in the long term as the adversary learns the valid credentials if the encryption is broken. Hence, he can tell whether he has obtained a valid or a fake credential from the coerced voter. Only **short-term coercion-resistance and receipt-freeness** is thus achieved.

4.4 Homomorphic Encryption: Helios 2.0

Helios 1.0 was one of the first web-based open-audit voting systems [1]. After a series of upgrades, Helios 2.0 was developed and used in the election of the University President of the Université catholique de Louvain (UCL) in Belgium [2]. The two main differences between version 1.0 and 2.0 are a distributed tallying authority and the use of homomorphic encryption instead of a mixnet.

Summary. The participants are voters, a registration authority, and several talliers. The ballot is composed of an encryption of a yes/no vote for each candidate and a zero-knowledge proof on the validity of the contained plaintexts. Ballot preparation is separated from ballot casting: Anyone can generate an encrypted ballot for a specific candidate. Next, the correct preparation of the ballot can either be audited, or the ballot can be cast after the voter has been authenticated (*Benaloh challenge* [4]). The voting system commits to the encrypted vote by displying a hash of the ciphertext. If the voter (or any interested party) chooses to audit the ballot, the ciphertext and the randomness used for encryption is displayed, which allows for checking that the encryption and the hash were computed correctly. If the voter chooses to seal the ballot, he is authenticated and a hash of the encrypted ballot is posted on the bulletin board next to the voter ID. The voter obtains a signed hash of his encrypted ballot. A sophisticated vote weighting according to the voter category is carried out before tallying. We do not consider this as it is not relevant to our analysis, for details refer to [2].

Setup. The private tallying key is generated and stored in a distributed way by the talliers (named "trustees" in [2].) In registration phase, each eligible voter obtains an anonymous ID and a password in a signed file from the registration authority (UCL central authority).

Voting. V_i computes an Exponential ElGamal encryption of the vote $v_i \in \{0,1\}$ (g and G are group generators, $h = g^s$ is the public key that corresponds to the private key s):

$$encr_T(v_i) = (x_i, y_i) = (g^{r_i}, h^{r_i} G^{v_i})$$

The ballot is composed of the encrypted vote[3] and a zero-knowledge proof on the validity of the contained plaintexts:

$$b_i = (encr(v_i), prf_{V_i})$$

If the voter decides to cast the vote and is successfully authenticated, a hash of the encrypted ballot is posted to the bulletin board next to the voter ID:

$$V_i \longrightarrow BB : \langle ID_i, hash(b_i) \rangle$$

Tallying. The talliers first check all proofs prf_{V_i}. Next, the product of all ballot parts x_i and y_i is formed:

$$(x, y) = (\prod_i x_i, \prod_i y_i) = (g^{\sum_i r_i}, h^{\sum_i r_i} G^{\sum_i v_i})$$

The talliers jointly decrypt the ballots and get $G^{\sum_i v_i}$. The sum of the votes is obtained by computing the discrete logarithm of this term, which is tractable as the exponent is relatively small. Finally the talliers publish the sum of the votes.

Analysis. The voting scheme provides only **short-term anonymity**: If the encryption scheme and the preimage resistance of the hash function used is broken, the vote can be linked to the ID of the voter who cast it. It then suffices to trace the voter ID back to the voter and anonymity is compromised. The Helios voting system is not designed to provide receipt-freeness or even coercion-resistance.

The voter can check that the receipt, i.e. the hash of his encrypted vote, is correctly posted next to his ID on the bulletin board. Individual ballots are never decrypted and no proof is provided on the correct content of the ballots that have been cast. Thus, in our model, only **basic individual verifiability** is established. Helios does, however, provide voter-verifiability (or "ballot casting assurance" as referred to in [2]) by means of the Benaloh challenge. We consider this in more detail in Section 5.

4.5 Paper Ballot: Prêt à Voter

Prêt à Voter [6] is an electronic voting system that uses paper-based ballot forms. These are scanned and turned into receipts to provide voter-verifiability while maintaining coercion-resistance.

Summary. The participants are voters, a *vote scanning device (VSD)*, an election authority, and several talliers. Prior to the election the authority generates a large number of ballot forms (significantly more than the amount of eligible

[3]In fact,v_i is not a vote for a single candidate but rather a series of yes/no votes for all eligible candidates. We omit this here for simplicity of notation.

voters because of the audit process). The voter registers at the polling station and randomly selects a ballot form which consists of two columns: While the left column lists the candidates in random order, the right column is for the voter to enter his choice and holds a random value at the bottom, called *onion*. The onion contains the information necessary for reconstructing the candidate ordering. The right column is later separated from the left one to generate a receipt.

Setup. Each of the k members of the tallying authority T creates two key pairs. The first key pair is used to encrypt and later to reconstruct the candidate ordering on each ballot form: The ordering is encrypted with the public keys of the k involved tellers, yielding the onion. The second key pair is only used for a specific audit process prior to vote casting (cf. Section 5) and not further considered here.

Voting. V_i enters the polling booth and marks the ballot form in the usual way. Still in the polling booth, V_i removes the left hand strip of the ballot and shreds it. Note that the destruction of the left column of the ballot form must be enforced to ensure coercion-resistance. Next, the voter takes the right hand strip and feeds it into the vote scanning device (VSD). In case this ballot strip has not been used before, the position of the mark is stored together with the onion on the bottom of the strip. In addition, the VSD marks the strip as having been used for voting and returns it to V_i who keeps it as a receipt of the form $sig_{VSD}(encr_T(v_i))$. Note that the VSD does not learn V_i's voting decision.

Tallying. Once the election has closed the VSD transmits the stored receipts to the bulletin board:

$$VSD \longrightarrow BB : \langle sig_{VSD}(enc_T(v_i))\rangle$$

T performs an anonymizing mix and decryption on the batch of encrypted ballot receipts and published the final tally.

Analysis. The ballot receipts which enter the tallying process do not contain any personal information of the voter. Encryption by T is only used to hide the candidate ordering. Hence, the scheme provides **long-term anonymity**. By the anonymizing mix and decryption on the batch of encrypted ballots performed by T, the link between the encrypted ballot receipt and the resulting decrypted vote is hidden. This ensures receipt-freeness. However, if the primitive used for encryption is broken, the permutation performed by each of the talliers is revealed and the voter can use the receipt to prove his vote. Thus, the scheme offers only **short-term receipt-freeness and coercion-resistance**.

The voter can visit the bulletin board to check that his receipt is correctly posted and hence correctly entered into the tallying process. However, he is not provided a proof that the random onion belongs to the candidate order in the left column and thus will be decrypted to the vote which the voter intended to cast. Hence, in our model only **basic individual verifiability** is achieved. Prêt à Voter does, however, provide a different means to enhance voter-verifiability, namely using dummy votes for audit. We refer to this in Section 5.

4.6 DRE: Neff's Scheme

Neff's voting protocol [21] introduced a strong notion of voter-verifiability for e-voting based on direct-recording electronic (DRE) voting machines. The scheme was developed within the framework of the VoteHere voting system.[4] It allows a voter to verify that his ballot truly represents his choice (*cast-as-intended*) without having to trust the DRE. Moreover, anyone can verify that the tally was correctly computed from the ballots on the bulletin board (*counted-as-cast*).

Summary. The participants are voters, a DRE, and several talliers. The voter first enters his choice at the DRE. Then the DRE generates the according encrypted ballot and commits to it. Next, the voter provides a challenge and the DRE responds to it, thus convincing the voter that his vote is correctly represented by the ballot. This receipt cannot be used to prove the vote to a third party as it is based on the temporal sequence of the actions taken by voter and DRE. A threshold decryption system is used for tallying.

Setup. The talliers perform a distributed key generation protocol to compute the master public key. Decryption is only possible through the cooperation of all trustees in a threshold decryption operation. Furthermore, the security parameter l is determined (Neff suggests $10 \leq l \leq 15$ [15]).

Voting. The voter enters his choice for candidate C_j into the DRE:

$$V_i \longrightarrow DRE : j$$

Let l denote the security parameter. The DRE constructs the encrypted ballot, the *verifiable choice (VC)*, as a $n \times l$ matrix consisting of *ballot mark pairs (BMP)*. The BMPs in the row denoting the chosen candidate have the form $encr_T(bit), encr_T(bit)$ while all other BMPs are supposed to be of the form $encr_T(bit), encr_T(\neg bit)$ where $bit \in \{0,1\}$. A VC encoding a vote for candidate C_j could look as follows:

	1	2	3	...	l
C_1	0 1	0 1	1 0	...	0 1
C_2	0 1	0 1	1 0	...	0 1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
C_j	1 1	0 0	0 0	...	1 1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
C_n	0 1	0 1	1 0	...	0 1

The DRE then sends the unique *ballot sequence number (BSN)* as well as a hash of the VC to the voter. The DRE also commits to the VC by providing the pledge bits $p_1, \ldots, p_l$ where $p_k = bit_{j,2k-1} = bit_{j,2k}$:

$$DRE \longrightarrow V_i : BSN, hash(VC), p_1, \ldots, p_l$$

Next, the voter chooses a challenge of l random bits $c_1, \ldots, c_l$ where $c_k = 0$ means that he wants the left part of the k-th BMP in row j to be opened, while $c_k = 1$ refers to the right part.

$$V_i \longrightarrow DRE : c_1, \ldots, c_l$$

The DRE constructs fake challenges for all unchosen candidates. The voter may hereafter change them in order to

[4] For more information see `http://www.votehere.net/`

evade coercion. It then proves to the voter that the cipher text in position $2k-1+c_k$ ($k=1,\ldots,l$) indeed decrypts to p_k. The DRE does so by providing the randomness which was used for the probabilistic ElGamal encryption of the respective bits. The result is an *opened verifiable choice (OVC)*, which corresponds to a VC with one half of each BMP opened. The DRE sends the OVC to the bulletin board:

$$DRE \longrightarrow BB : \langle OVC \rangle$$

Tallying. The talliers remove the BSN from each ballot and process the ballots through a universally verifiable mixnet [22]. Then they cooperatively decrypt the votes and publish the voting results.

Analysis. If the Decisional Diffie-Hellman (DDH) assumption holds in the underlying group, then ElGamal encryption is semantically secure. The DDH assumption is related to the assumption that computing dicrete logarithms is hard. However, this assumption is merely computational, which means that ElGamal encryption does not provide long-term secrecy. If ElGamal is broken, the OVC published on the bulletin board shows the chosen candidate. As the BSN is removed from the ballot after vote-casting, the compromised OVC alone cannot be used to break anonymity. Hence, Neff's scheme provides **long-term anonymity**. However, if the voter shows the receipt to an adversary, the pledge bits and the challenge for the chosen candidate on the receipt can be compared with the opened BMPs. The probability that there is another voter whose receipt matches the compromised OVC is $1/2^l \cdot 1/2^l = 1/4^l$. Thus, only **short term receipt-freeness and coercion-resistance** is ensured.

The scheme provides **advanced individual verifiability** as the voter obtains a proof from the DRE that the ballot has been cast as intended. However, only basic individual verifiability is provided if the voter chooses a basic receipt containing only $(BSN, hash(VC))$ [15].

We conclude our analysis by providing an overview in Table 1. To enhance readability we use the abbreviations OMA+99 for Ohkubo et al. [23], JCJ05 for Juels et al. [14], AMPQ09 for Helios 2.0 [2], CRS05 for Prêt à Voter [6], and Neff04 for [21]. The improvement we suggested for the scheme by Juels et al. is depicted by a box. As noted in Section 3.2, coercion-resistance implies receipt-freeness, and receipt-freeness implies anonymity. Hence, a protocol which achieves short-/long-term coercion-resistance provides also short-/long-term receipt-freeness, and a protocol which achieves short-/long-term receipt-freeness provides short-/long-term anonymity as well.

		Individual verifiability	
		Basic	Advanced
A	ST	AMPQ09	ST
	LT	OMA+99, JCJ05, CRS05	LT Neff04
RF	ST		ST
	LT		LT
CR	ST	JCJ05, CRS05	ST Neff04
	LT		LT

Table 1: Rating of the voting protocols. A: anonymity, RF: receipt-freeness, CR: coercion-resistance; ST: short-term, LT: long-term.

5. CONCLUSION

It is a challenge for current voting schemes to reconcile secrecy and verifiability, particularly in the long term: How can individual verifibility be achieved without sacrificing anonymity and receipt-freeness or even coercion-resistance in the long term? While for parliamentary elections we should strive for the optimum, i.e. advanced individual verifiability and coercion-resistance in the long term, one could make concessions for elections of less importance.

We introduced an intuitive classification of anonymity, receipt-freeness and coercion-resistance as well as individual verifiability. As we believe that an effective dialog between computer scientists and jurists is a precondition for developing secure electronic voting schemes, our definitions were determined to be understandable to both sides. We analyzed representative remote as well as paper-based electronic voting protocols with respect to these requirements. We also provided improvements on the scheme by Juels et al. [14] with respect to long-term anonymity. Our protocol ratings can support election hosts in selecting appropriate voting schemes with respect to the priority of either freedom and secrecy of the vote or voter-verifiability.

A novel approach in order to reconcile anonymity and verifiability for the voter is the possibility of indirect auditing as proposed for Helios [1, 2] and Prêt à Voter [6]. With Prêt à Voter, each voter can cast dummy votes before the election opens in order to check on the correct construction of the ballot forms. The talliers return the decryption of the vote, thus proving that the candidate ordering on the ballot form is correctly captured by the onion. This leaves the voter confident that his actual vote will be cast as intended, too. With Helios, an even stronger form of indirect audit is provided: When the voting system commits to the encrypted ballot, it does not know whether the voter will choose to cast or to audit the ballot. Thus, fraud will be detected with high probability.

At present it seems to be impossible to achieve both advanced individual verifiability and coercion-resistance in the long term. This is also due to the fact that individual verifiability is still largely understood as the ability for the voter to check *his own* vote. It is to be considered whether the notion of individual verifiability should be extended to the indirect form provided for example by Helios or Prêt à Voter.

6. REFERENCES

[1] B. Adida. Helios: web-based open-audit voting. In *SS'08: Proceedings of the 17th conference on Security symposium*, pages 335–348, Berkeley, CA, USA, 2008. USENIX Association.

[2] B. Adida, O. de Marneffe, O. Pereira, and J.-J. Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios. In *EVT'09: Proceedings of Electronic Voting Technology Workshop / Workshop on Trustworthy Elections*. USENIX Association, 2009.

[3] R. Araujo, S. Foulle, and J. Traoré. A practical and secure coercion-resistant scheme for remote elections. In D. Chaum, M. Kutylowski, R. L. Rivest, and P. Y. A. Ryan, editors, *Frontiers of Electronic Voting*, volume 07311 of *Dagstuhl Seminar Proceedings*, 2007.

[4] J. Benaloh. Ballot Casting Assurance via Voter-Initiated Poll Station Auditing. In *EVT'07: Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, pages 14–14, Berkeley, CA, USA, 2007. USENIX Association.

[5] J. D. C. Benaloh. *Verifiable secret-ballot elections*. PhD thesis, Yale University, New Haven, CT, USA, 1987.

[6] D. Chaum, P. Y. A. Ryan, and S. A. Schneider. A practical voter-verifiable election scheme. In S. D. C. di Vimercati, P. F. Syverson, and D. Gollmann, editors, *ESORICS*, volume 3679 of *Lecture Notes in Computer Science*, pages 118–139. Springer, 2005.

[7] B. Chevallier-Mames, P.-A. Fouque, D. Pointcheval, J. Stern, and J. Traoré. On some incompatible properties of voting schemes. In *Proceedings of the IAVoSS Workshop on Trustworthy Elections*, 2006.

[8] J. D. Cohen and M. J. Fischer. A robust and verifiable cryptographically secure election scheme. In *SFCS '85: Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, pages 372–382, Washington, DC, USA, 1985. IEEE Computer Society.

[9] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum. Council of Europe Publishing, 2004.

[10] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In W. Fumy, editor, *EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118. Springer, 1997.

[11] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In J. Seberry and Y. Zheng, editors, *AUSCRYPT*, volume 718 of *Lecture Notes in Computer Science*, pages 244–251. Springer, 1992.

[12] R. Grimm, R. Krimmer, N. Meißner, K. Reinhard, M. Volkamer, and M. Weinand. Security requirements for non-political internet voting. In R. Krimmer, editor, *Electronic Voting*, volume 86 of *LNI*, pages 203–212. GI, 2006.

[13] H. L. Jonker and E. P. de Vink. Formalising receipt-freeness. In S. K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, and B. Preneel, editors, *ISC*, volume 4176 of *Lecture Notes in Computer Science*, pages 476–488. Springer, 2006.

[14] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In V. Atluri, S. D. C. di Vimercati, and R. Dingledine, editors, *WPES*, pages 61–70. ACM, 2005.

[15] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: A systems perspective. In *Proceedings of the Fourteenth USENIX Security Symposium (USENIX Security 2005)*, pages 33–50, August 2005.

[16] R. Krimmer and M. Volkamer. Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting. In *Electronic Government – EGOV '06 – Conference Proceedings of the* 5^{th} *International EGOV Conference*, volume 18 of *Schriftenreihe Informatik*, pages 43–52, Linz, 2006.

[17] R. Küsters and T. Truderung. An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols. Technical Report arXiv:0903.0802, arXiv, 2009. An extended version of a paper from IEEE Symposium on Security and Privacy (S&P) 2009, available at `http://arxiv.org/abs/0903.0802`.

[18] C. Lambrinoudakis, D. Gritzalis, V. Tsoumas, M. Karyda, and S. Ikonomopoulos. *Secure electronic voting: The current landscape*, volume 7 of *Advances in Information Security*, chapter 7. Kluwer Academic Publishers, 2003.

[19] L. Mitrou, D. Gritzalis, S. Katsikas, and G. Quirchmayr. *E-voting: Constitutional and legal requirements and their technical implications*, volume 7 of *Advances in Information Security*, chapter 4. Kluwer Academic Publishers, 2003.

[20] T. Moran and M. Naor. Split-ballot voting: Everlasting privacy with distributed trust. In *CCS 2007*, pages 246–255. ACM, October 2007.

[21] C. A. Neff. Practical high certainty intent verification for encrypted votes. Draft, October 2004. `http://www.votehere.com/old/vhti/documentation/vsv-2.0.3638.pdf`.

[22] C. A. Neff. Verifiable mixing (shuffling) of elgamal pairs. VoteHere, April 2004. `http://people.csail.mit.edu/rivest/voting/papers/Neff-2004-04-21-ElGamalShuffles.pdf`.

[23] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto. An improvement on a practical secret voting scheme. In M. Mambo and Y. Zheng, editors, *ISW*, volume 1729 of *Lecture Notes in Computer Science*, pages 225–234. Springer, 1999.

[24] W. D. Smith. New cryptographic election protocol with best-known theoretical properties. In *Frontiers of Electronic Elections*, 2005.

[25] M. Volkamer and D. Hutter. From legal principles to an internet voting system. In A. Prosser and R. Krimmer, editors, *Electronic Voting in Europe*, volume 47 of *LNI*, pages 111–120. GI, 2004.

[26] M. Volkamer and R. Vogt. Basic set of security requirements for Online Voting Products. Common Criteria Protection Profile BSI-CC-PP-0037, Bundesamt für Sicherheit in der Informationstechnik, Bonn, April 2008.

[27] S. G. Weber, R. Araujo, and J. Buchmann. On coercion-resistant electronic elections with linear work. In *ARES*, pages 908–916. IEEE Computer Society, 2007.

[28] M. Will. *Internetwahlen - Verfassungsrechtliche Möglichkeiten und Grenzen*. Recht und neue Medien Band 2. Richard Boorberger Verlag GmbH & Co, 2002.