Individual Verifiability with Return Codes: Manipulation Detection Efficacy

Paul Tim Thürwächter[1], Melanie Volkamer[1](✉), and Oksana Kulyk[2]

[1] Karlsruhe Institute of Technology, Karlsruhe, Germany
paul.thuerwaechter@student.kit.edu, melanie.volkamer@kit.edu
[2] IT University of Copenhagen, Copenhagen, Denmark
okku@itu.dk

Abstract. Researchers advocate for end-to-end verifiable voting schemes to maximise election integrity. At E-Vote-ID 2021, Kulyk et al. proposed to extend the verifiable scheme used in Switzerland (called original scheme) by voting codes to improve it with respect to vote secrecy. While the authors evaluated the general usability of their proposal, they did not evaluate its efficacy with respect to manipulation detection by voters. To close this gap, we conducted a corresponding user study. Furthermore, we study the effect of a video intervention (describing the vote casting process including individual verifiabilty steps) on the manipulation detection rate. We found that 65% of those receiving the video detected the manipulation and informed the support. If we only consider those who stated they (partially) watched the video the rate is 75%. The detection rate for those not having provided the video is 63%. While these rates are significantly higher than the 10% detection rate reported in related work for the original system, we discuss how to further increase the detection rate.

Keywords: End-to-end verifiability · Usability · Individual verifiability · Deceptive study · Manipulation detection rate

1 Introduction

Cryptographic end-to-end (E2E) verifiability facilitates detection of violations of the election integrity. From a usability perspective, individual verifiability (i.e. the ability to verify that the vote is cast as intended and stored as cast) is particularly challenging, as voters need to verify themselves. This is essential to preserve the secrecy of the vote. Thus, with E2E verifiability, in theory, it is possible to detect if voters are modified at any point in time, but only when voters know how to perform the individual verifiability and actually do so.

A range of manipulation-detection efficacy studies have been carried out to evaluate whether voters would detect if their vote is manipulated, e.g. in [11,22]. The corresponding user studies are conducted with different electronic voting systems in mind as well as with different types of attacks. In the user

R. Krimmer et al. (Eds.): E-Vote-ID 2022, LNCS 13553, pp. 139–156, 2022.
https://doi.org/10.1007/978-3-031-15911-4_9

study, participants are told that the usability of an electronic voting system is evaluated. However, they interact with one (or a corresponding mockup) that an attacker could have set up to make voters believe their vote is not manipulated while it is actually either altered before being sent to the ballot box or not being sent to the ballot box at all. Note, the concrete strategy an attacker could take to do so, depends on the voting system under consideration. Furthermore, not all strategies are the same, but some are more difficult for voters to detect than others. Correspondingly there is a broad range of detection rates being reported in the literature, e.g. in [18], authors report for one system a detection rate of 100% for a more easy to detect manipulation and 10% for a difficult to detect one for another system.

Our focus is on those attacks that are difficult to detect as an attacker is more likely to take those. Furthermore, our focus is on the voting system used in Switzerland (which is based on polling sheets with return and confirmation codes to enable voters to verify their vote) – more precisely, the improvement proposed at E-Vote-ID 2021 by Kulyk et al. [16]. The authors proposed to use QR Codes to enter codes and to use so-called voting codes in order to improve the guarantees with respect to the secrecy of the vote. They also conducted a user study in which they observed that their proposal has no negative impact on the general usability compared to the original scheme. Our research has the following goals:

- Improving the proposal of [16] (i.e. voting material and mockups of the voting interfaces) based on the feedback reported in their paper.
- Evaluating the manipulation detection efficacy of this improved proposal and comparing the detection rate with the one from the original scheme (note, to do so, we use the data from a similar study reported on in [18]).
- Studying the impact of providing voters additional information material about the vote casting process. We decided to use a video describing how to proceed to cast and verify votes as additional information material.

We conducted a user study with 50 participants. Our improved version of the Kulyk et al. proposal from [16] performed significantly better with respect to manipulation detection (63% detection rate) compared to the original system (10% detection rate, reported in [18]). While the detection rate for those participants who actually (at least partially) watched the video increased to 75%, it did not increase significantly. We discuss our findings in light of related work and deduce research directions for future work.

As a side contribution, our results confirm the conclusions from Kulyk et al. in [16] that, QR-code based code voting should be employed in certain types of election, as it avoids reliance on trustworthy voting clients. While they only argued based on the general usability, we showed that it has a positive effect on the manipulation detection rate too.

2 Related Work

Human aspects of verifiable voting systems have been a subject of several investigation, focusing on different aspects of verifiability, such as voters' attitudes, mental models and misconceptions of verifiability [1,2,4,9,21,22] or the usability of the actual verification process [1–5,9–11,15,17,19,20,22,26,28,30,31].

In particular, several studies focused on the effectiveness of verification procedure in different e-voting systems [2,7,18,24]. These studies show mixed results, showing that in several of the investigated systems, a significant amount of voters is not able to perform the verification correctly, thus being unable to tell whether their votes are being manipulated – e.g. less than half of participants were able to verify their votes using the Helios and the Scantegrity II voting system in the study by Acemyan et al. [2]. Other systems have demonstrated more promising results. In particular, the evaluations of voting systems implementing verification procedures based on the so-called check codes have shown a high level of verification efficiency in the studies that evaluated verification effectiveness by introducing vote manipulations in the experimental procedure and testing whether the participants of the experiment are able to detect these manipulations via the corresponding verification [18,24]. The studies in both of these works have shown a 100% verification efficiency rate with different variants of such code-based systems, meaning that all participants in their experiments were able to successfully verify their vote and detect manipulations. However, when different kinds of attacks were considered – in particular, with the adversary being able to modify the user interfaces with the goal of confusing the voter and preventing them from performing or correctly interpreting the verification results – the success rates for the verification decreased again, with only up to 56% of participants being able to detect such an attack according to the study in [18]. These studies conclude that evaluating verification efficacy via empirical experiments is crucial in understanding the security of proposed e-voting systems.

Aside from evaluating verifiability from the human factors point of view, a number of studies focused on other techniques that are introduced to e-voting systems to enhance their security – namely, to the code-voting approach [6,8,13,14,27], aimed to decrease the need to trust the voting client with regards to vote secrecy. As such, the usability of such systems has been evaluated in [17,23], showing that code voting in general can be made usable and acceptable by the voters. However, only limited evaluations of the usability of verification in code-voting systems have been conducted; one such system has been the subject of the study by Kulyk et al. [16], showing high effectiveness in terms of voters being able to cast the vote using the system, however, the study only tested the system in absence of vote manipulations.

3 Background

3.1 Swiss Electronic Voting System

Our focus is on the Swiss voting system from the Swiss Post[1]. The process to cast a vote with this system[2] is as follows: Voters receive an individual code sheet (also called polling sheet) via postal service. This polling sheet contains one initialisation code, check codes for each voting option, one confirmation code, and one finalisation code. All cotes are different for each voter. As there is no electronic ID in Switzerland, the system generates an election specific election key pair for all voters – one pair for each voter. The voters' private key is indirectly provided to them in the polling sheet. The private key can be deduced from the initialisation code.

An overview is depicted in Fig. 1a. To start the vote casting process, voters open the election webpage (the URL is provided on the polling sheet). Next, they manually enter their initialisation code (i.e. by typing the corresponding characters in the corresponding field of the webpage). Afterwards, voters select their voting option using the election webpage, i.e. clicking the option they want to select. Next, the election webpages displays a check code. According to the description on the polling sheet), voters are supposed to compare this code with the one next to their voting option on their polling sheet. The result of this check can be a pass or a fail: If both codes are the same, the voter confirms his by manually entering the confirmation code.

In case, the check was passed and the confirmation code was correctly entered, voters are supposed to receive a finalisation code. According to the polling sheet, voters are supposed to check whether such a code is displayed and whether it matches the one on their polling sheet. Only if this second check is passed, voters can be assured that their vote has been stored as intended (i.e. cast as intended plus stored as cast). The voting scheme provides individual verifiability under the assumption that the printing server and the voting client do not collaborate. Note, we are aware that the implementation when it comes to the universal verifiability had severe shortcomings, see e.g. [12]. We believe that these are issues the company faced when implementing the underlying cryptographic primitives. Thus, it can be fixed and as such it is still worth to study the individual verifiabilty of schemes like the one used in Switzerland.

We refer to this system incl. the election material and user interfaces as **'original system'**.

3.2 E-Vote-ID-2021-Proposal

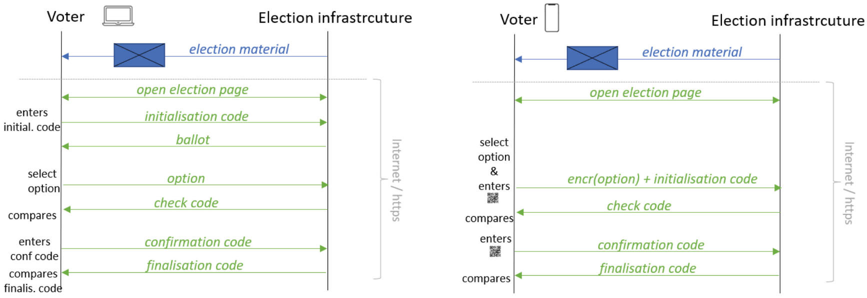
At E-Vote-ID-2021, Kulyk et al. proposed in [16] to extend the Swiss voting system by individual voting codes. With this extension, the individual polling

[1] https://evoting-community.post.ch/de?_ga=2.79449501.804715002.1658647288-420296842.1658647288.

[2] Note, the system is used for polls in which voters select *1 out of n* options. Usually 2–3 of such polls are conducted at the same time. For our research, we assume that there is only one poll.

sheet from the Swiss system also contains one voting code per option. The voting codes are different for each voter. Thus, voters are supposed to enter the voting code representing their chosen option (instead of clicking on the option they want to selection on the election webpage). As the voting client cannot map the voting code to any of the options, the assumption on the trustworthy voting client is no longer needed[3].

To address shortcoming of entering long voting codes, the authors proposed that voters use their camera-equipped smartphones, to cast a vote by scanning a corresponding QR code (containing the voting code). Their proposed (simplified) scheme is depicted in Fig. 1b. To integrate these ideas, the authors adopted the voting material and the election webpage from [18] accordingly. In particular, they introduce voting cards which contained on the front page the voting code as QR-code and on the back page the option and the corresponding return code.



(a) Swiss voting scheme

(b) E-Vote-ID-2021-proposal

Fig. 1. Vote casting

In this paper, we refer to the proposal incl. the election material and user interfaces from Kulyk et al. as **'E-Vote-ID-2021-proposal'**.

4 Improvements to E-Vote-ID-2021-Proposal and Descriptive Video

4.1 Improvements to the Voting Material and User Interfaces

Based on the feedback Kulyk et al. received from their participants, we deduced the following improvements:

- Providing the URL to the election webpage not only as text but also as a QR-code to make it easier for voters to open the correct election webpage.

[3] Note, however, that one needs to ensure that the mapping of the voting codes to options for each voter remains secret to the adversary. Therefore it is important that the printers are operated offline as they need to be fully trustworthy.

- In order to scan the voting code, users had to scan two QR-codes at once: the one on the polling sheet and the one the voting card (which had to be placed above each other). Participants were confused as they were not aware that one can scan two QR-codes at the same time. Kulyk et al. proposed to have the QR-code on the polling sheet to make sure participants scan the voting code only when placed there[4]. We decided to trust voters to put it there. Furthermore, we added a tick-box on the start page of the vote casting interfaces where voters would need to confirm that they properly placed it. Thus, we could remove the second QR-code to make it less confusing for voters.
- Participants were missing that they have to confirm that they cast their vote on their own and were not observed (as this is the case with postal voting). We added such a confirmation statement.
- The user interfaces of Kulyk et al. did contain minimal information. Their motivation to do so was that voters should anyway follow the instructions on the polling sheet. However, participants were complaining that the interface looked not very trustworthy due to the minimal amount of text. Therefore, we added the instructions from the polling sheet also on the user interfaces of the election webpage. We are aware that this only increases perceived security but without this adoption we would ignore users' feedback. Furthermore perceived security is likely to influence voters' trust in the voting system in place. At the end, we need to achieve both: Having a trustworthy end-to-end verifiable voting system in place which voters trust.

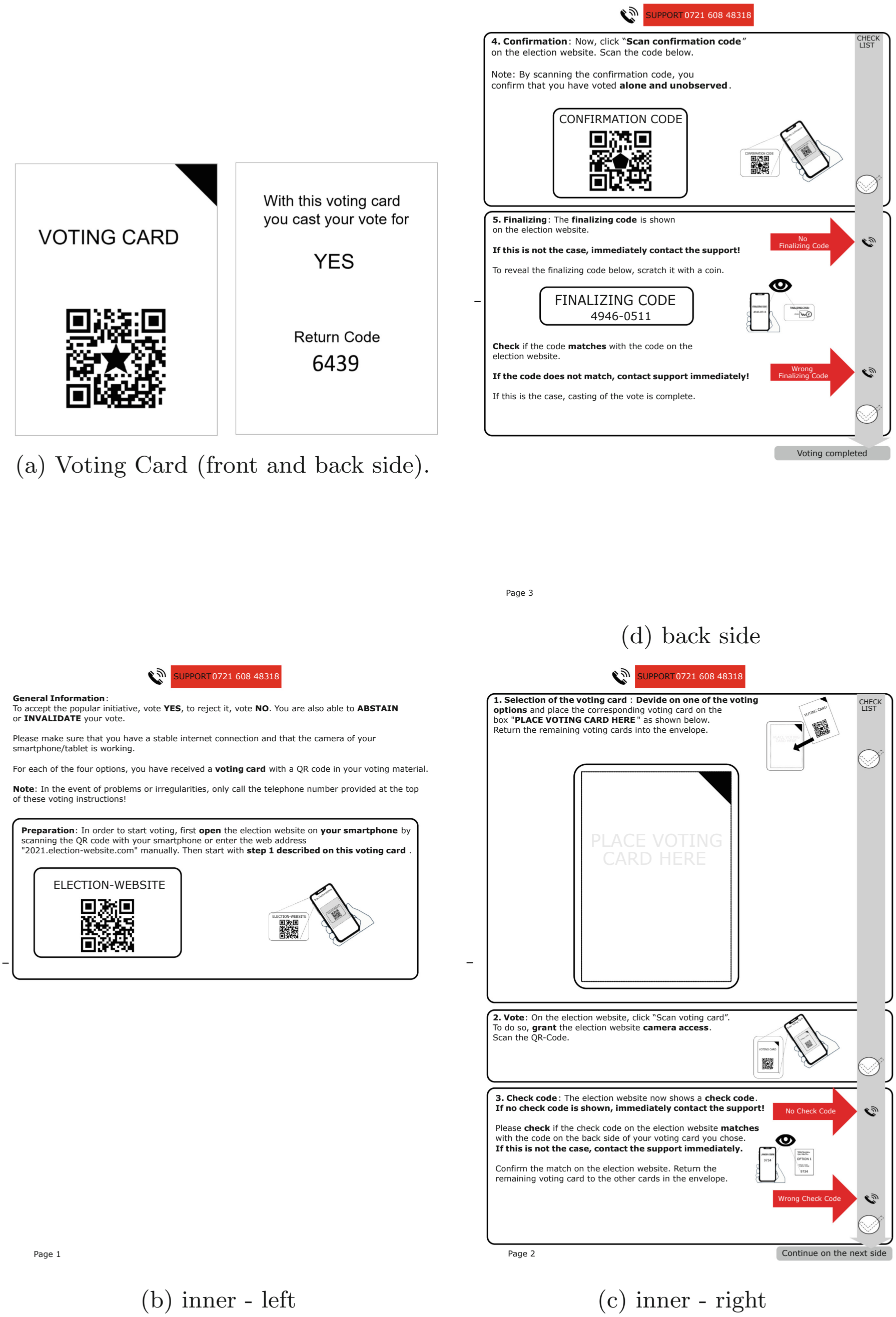
The modified voting material and user interfaces are depicted in Fig. 2 and 3. In this paper, we refer to this system as improved-proposal.

4.2 Descriptive Video

We were discussing what additional information voters may receive or have access to, regarding the online voting channel. There might be discussion forums, information about the company who provides the systems, the setup, maybe also about security evaluations in case there are some. In addition, we expect that their are videos describing the vote casting process to give voters an idea of the process and maybe what to particular care about. As we thought the first list might be very much related to the actual system in place, it is worth studying the impact of a video describing the process. Note, we decided to go with a video which provides the necessary information in a one-two lines text field rather than with audio, as we did not want that the audio is an issue when conducting the study (see Sect. 5).

The video therefore shows all the steps from receiving and opening the voting material to checking the finalisation code. The video takes 9 min. It also highlights twice the number of the support to be called. The reason it takes 9 min is that it gives the recipients time to read the text in the polling sheet at the

[4] Fore the exact reasons, we refer the reader to [16].



VOTING CARD

With this voting card you cast your vote for

YES

Return Code

6439

(a) Voting Card (front and back side).

☎ SUPPORT 0721 608 48318

4. Confirmation: Now, click "**Scan confirmation code**" on the election website. Scan the code below.

Note: By scanning the confirmation code, you confirm that you have voted **alone and unobserved**.

CONFIRMATION CODE

5. Finalizing: The **finalizing code** is shown on the election website.

If this is not the case, immediately contact the support!

To reveal the finalizing code below, scratch it with a coin.

FINALIZING CODE

4946-0511

Check if the code **matches** with the code on the election website.

If the code does not match, contact support immediately!

If this is the case, casting of the vote is complete.

Page 3

(d) back side

☎ SUPPORT 0721 608 48318

General Information:
To accept the popular initiative, vote **YES**, to reject it, vote **NO**. You are also able to **ABSTAIN** or **INVALIDATE** your vote.

Please make sure that you have a stable internet connection and that the camera of your smartphone/tablet is working.

For each of the four options, you have received a **voting card** with a QR code in your voting material.

Note: In the event of problems or irregularities, only call the telephone number provided at the top of these voting instructions!

Preparation: In order to start voting, first **open** the election website on **your smartphone** by scanning the QR code with your smartphone or enter the web address "2021.election-website.com" manually. Then start with **step 1 described on this voting card** .

ELECTION-WEBSITE

Page 1

☎ SUPPORT 0721 608 48318

1. Selection of the voting card : **Devide on one of the voting options** and place the corresponding voting card on the box "**PLACE VOTING CARD HERE**" as shown below.
Return the remaining voting cards into the envelope.

PLACE VOTING CARD HERE

2. Vote: On the election website, click "Scan voting card".
To do so, **grant** the election website **camera access**.
Scan the QR-Code.

3. Check code: The election website now shows a **check code**.
If no check code is shown, immediately contact the support!

Please **check** if the check code on the election website **matches** with the code on the back side of your voting card you chose.
If this is not the case, contact the support immediately.

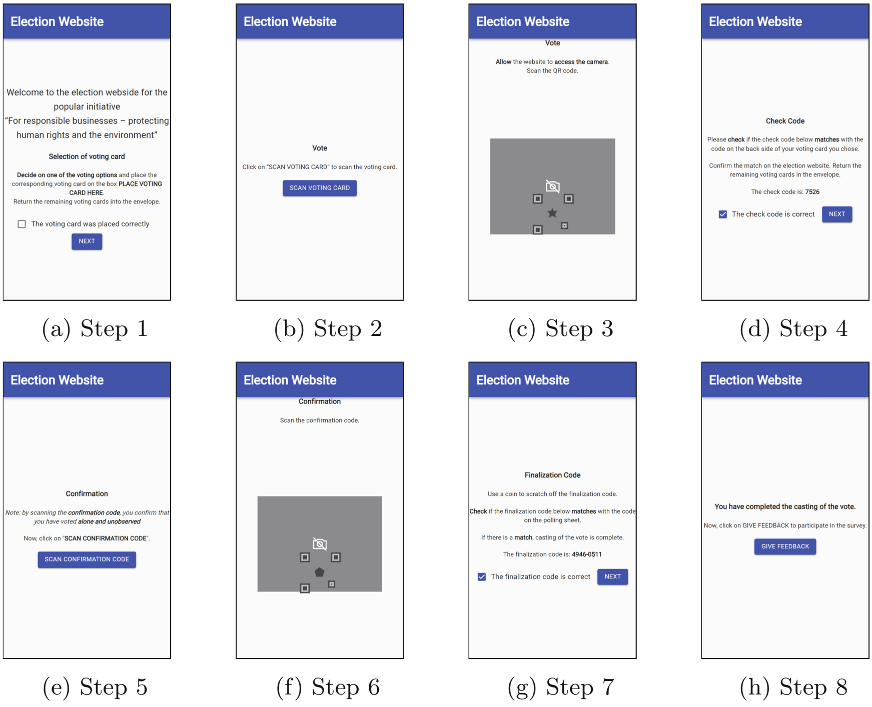
Confirm the match on the election website. Return the remaining voting card to the other cards in the envelope.

Page 2

(b) inner - left

(c) inner - right

Fig. 2. Polling sheet (b–d) with the scratch field being removed in (d); and voting cards (a)



Welcome to the election webside for the popular initiative
“For responsible businesses – protecting human rights and the environment”

Selection of voting card

Decide on one of the voting options and place the corresponding voting card on the box **PLACE VOTING CARD HERE**.
Return the remaining voting cards into the envelope.

□ The voting card was placed correctly

(a) Step 1

Vote

Click on “SCAN VOTING CARD” to scan the voting card.

(b) Step 2

Vote

Allow the website to **access the camera**.
Scan the QR code.

(c) Step 3

Check Code

Please **check** if the check code below **matches** with the code on the back side of your voting card you chose.

Confirm the match on the election website. Return the remaining voting cards in the envelope.

The check code is: **7526**

☑ The check code is correct

(d) Step 4

Confirmation

Note: by scanning the ***confirmation code****, you confirm that you have voted* ***alone and unobserved***

Now, click on "**SCAN CONFIRMATION CODE**".

(e) Step 5

Confirmation

Scan the confirmation code.

(f) Step 6

Finalization Code

Use a coin to scratch off the finalization code.

Check if the finalization code below **matches** with the code on the polling sheet.

If there is a **match**, casting of the vote is complete.

The finalization code is: **4946-0511**

☑ The finalization code is correct

(g) Step 7

You have completed the casting of the vote.

Now, click on GIVE FEEDBACK to participate in the survey.

(h) Step 8

Fig. 3. Voting webpage. Note, the steps, we refer to, correspond to those in the polling sheet.

same time, i.e. reading one paragraph or one step before continuing, i.e. actually conducting this step in the video. The video is available online[5].

5 Methodology

We first introduce our research questions and corresponding hypotheses, afterwards we describe the study procedure before discussing ethics, how we meet data protection regulations, and how we recruited our participants.

5.1 Research Questions, Hypotheses

The proposal from [16] improves the security level of the original scheme. The general usability was shown to be similar to the original system. An open question remains, however, how this idea perform with respect to the manipulation-detection efficacy - both with and without providing a descriptive video. Correspondingly, we define the following research questions:

[5] https://youtu.be/Yj7yz437OEc.

How does the improved-proposal performs in terms of manipulation-detection efficacy (measured as the rate of participants detecting the manipulation of their vote) with and without watching the video?

The authors of [16] based their voting material and election webpage on the improvements from [18]. We further improved both based on the feedback the authors reported on in [16]. The improvements of [18] resulted in a significantly higher manipulation detection rate than original system. Therefore, we expect that our improvements of the improved-proposal outperform the original system with respect to manipulation-detection efficacy. We therefore define the following hypotheses:

H_1: The improved-proposal without interventions has a significantly higher manipulation-detection efficacy than the original system.

H_2: The improved-proposal in combination with the watching the video has a significantly higher manipulation-detection efficacy than the original system.

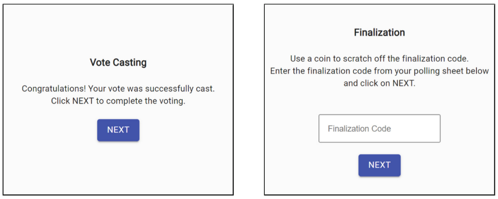
Note, the validation of this hypotheses come with some limitations as we collected only data for the improved-proposal (with and without the video) while we use for the original system the date from [18]. We discuss this further in the limitation section.

In particular for people using the improved-proposal the first time, the video helps to give them a better idea about the vote casting including scanning and verifying the various codes. The video in particular indicates that the support should be contacted in case the shown codes do not match the expected ones. We therefore define the following hypothesis:

H_3: The improved-proposal in combination with the watching the video has a significantly higher manipulation-detection efficacy than the improved-proposal without further descriptions or explanations.

5.2 Considered Manipulation-Types

Kulyk et al. studied two different types of manipulations in [18]. One of their attacks would not be possible in the proposal from Kulyk et al. [16]: Adversaries would need to know the voting code for the option they want to cast a vote for – which is not the case by design of any code voting scheme. In the other one, adversaries attempt to nullify cast votes by not sending the voting code to the election infrastructure and manipulating the voting client with the purpose to convince the voter that their vote has been cast successfully. For this attack after entering the voting-code, the election webpage would confirm the correctness of the check code. Furthermore, it would state that the check code is correct and that one can continue to finish the vote casting process. Note, it is not possible for the adversary to show the finalisation code as they cannot send a valid voting code to the election infrastructure. Therefore, the adversary would need to change these steps, too: Instead of asking voters to compare the displayed finalisation code with the one in the polling sheet, the manipulated voting client could ask voters to enter the finalisation code. Figure 4 shows the content of the manipulated interfaces.



Vote Casting

Congratulations! Your vote was successfully cast.
Click NEXT to complete the voting.

NEXT

(a) Step 4

Finalization

Use a coin to scratch off the finalization code.
Enter the finalization code from your polling sheet below and click on NEXT.

Finalization Code

NEXT

(b) Step 7

Fig. 4. Manipulated webpage, only displaying steps that are different, any only the actual text/UI elements.

5.3 Study Procedure

Figure 5 depicts an overview of the study procedure. The study was conducted in German. Voting material and election webpage were translated for this paper. Furthermore, it was a remote study. The ballot of the election we simulated for our study contained four options. Participants were randomly assigned to one of the two groups: The no-video-group and the video-group. Participants received the study material in an envelope either via postal service or from someone they know. The following content was included:

- A study letter describing the study, the time frame, which other material is included in the envelope, the conditions incl. the next steps to take, and information that they can cancel participation at any time. Note, in a footnote, the link to the post-survey was included.
- Role card explaining who they should suppose to be for the study and which option to vote for.
- Envelope with the actual voting material, i.e.,
  - the election letter from the election officials which recommended to first read the polling sheet before starting the vote casting process. Furthermore, it mentions that in case of problems or questions they should call the (study) support. For participants in the video-group this document also recommended to first watch a descriptive video. A corresponding link was provided.
  - the polling sheet; and
  - the voting cards with the voting-code.

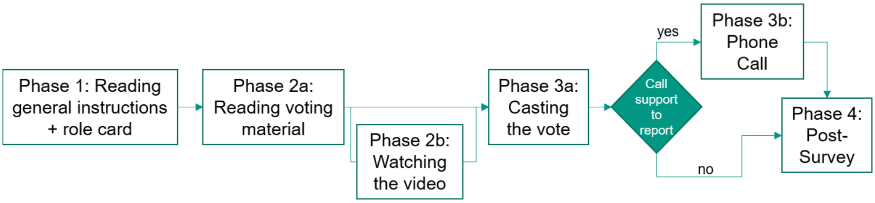

Phase 1: Reading general instructions + role card
Phase 2a: Reading voting material
Phase 2b: Watching the video
Phase 3a: Casting the vote
Call support to report
yes
no
Phase 3b: Phone Call
Phase 4: Post-Survey

Fig. 5. Study procedure for both groups (with and without the link to the video)

Participants were supposed to open the envelope, and read the study letter and the role card (phase 1). Afterwards, they were supposed to open the inner envelope with the voting material and to read the polling sheet (phase 2a). Participants in the video-group were asked to then watch the video (phase 2b). Afterwards, participants were supposed to start casting their vote (phase 3a). Both groups (the one with and without the link to the video) got the manipulated interfaces as described in Sect. 5.2.

In the case that participants did not notice the manipulation or have noticed it but did not call the support, they could just finish vote casting. After having finished the vote casting process, the election webpage displayed the link to the post-survey (phase 4). This survey, first, provides information about the study and data collection. It contained the informed consent. Once consent was provided, participants were debriefed. If they decide to continue with the survey, they were asked whether they detected the manipulation they read about in the debriefing text. Note, the question on the manipulation detection had three options: (1) I noticed it and I called the (study) support, (2) I noticed it but I did not call the (study) support, and (3) I did not notice the manipulation. In case the first option was selected, this had to be confirmed by entering the number 22. Those who called the (study) support got this number on the phone once they have reported the manipulation they observed. In case the second option was selected, participants were asked an additional open text question on why they did not call the support. The survey also asked whether they first read the instructions on the polling sheet before starting the vote casting process and we asked demographic questions. Participants in the video-group got additional questions: Whether they watched the video (entirely) and whether it was helpful (to detect the manipulation).

In the case that study participants did notice the manipulation and called the (study) support[6] (phase 3b), the support first asked them to provide details about the issues they have. The goal was to first make sure they actually observed the manipulation and to find out to which group they were assigned. The study support took a note of this. Afterwards the participant who called was debriefed on the phone. If they decided to continue with the study, they were provided with the link to the post-survey[7] and with the number 22 needed for the post-survey. Finally, the study support thanked the caller.

5.4 Ethics, Data Protection, Recruitment

The study was announced with the goal to evaluate the usability of an online voting system. Thus, one may call it a deceptive study. Therefore, the study was approved by the ethic committee of our university. Their checks contain legal issues as well. As such the compliance with data protection laws was attested too. We still want to comment on some important aspects: The postal addresses were

[6] Note, in case the study support could not answer the call, this person was called back as soon as possible. All telephone numbers were deleted afterwards.

[7] The post-survey was the same for those not detecting all participants.

deleted once they were put on the envelopes. For the survey we used SocSciSurvey which is GDPR compliant[8]. Participants were debriefed either on the phone or through the post-survey. The study material contained a telephone number and an email address to get in touch with us in case of general questions regarding the study or any doubts.

Participants were recruited in various different ways: Public channels, social media, friends of friends (in case they were not aware of our research) as well as through a snow-ball principle, asking those who agreed to participate to announce it to friends and family, too. Due to the remote study setting, we decided to not offer a reimbursement.

6 Results

We sent out the voting instructions to 60 people (30 for each group). Eventually, a total of 50 people completed the post-survey (24 assigned to the no-video-group and 26 to the video-group). Table 1 shows their demographics, as well as of the participants in the study from [18] for the sake of comparison[9]. All statistical calculations for our hypotheses are performed using *R* packages "stats" and "rstatix". We report our results without corrections for multiple comparisons.

Table 1. Demographics of participants for age Mean/SD and gender

Experiment	Age	Gender
From [18]	34.34/15.54	66F, 62M
Our study	27.5/10.135	26F, 24M

6.1 Overall Manipulation Detection

Overall, 32 out of 50 participants reported detecting the manipulation. Of them, 17 were in the video-group and 15 were in the no-video-group, leading to detection rates of 65.4% and 62.5% correspondingly. We used Fischer's exact test [25] for the evaluation of our hypotheses, as commonly recommended for categorical data with 2 × 2 contingency tables with small sample sizes. Both of the groups had significantly higher detection rates compared to the original system (which according to [18] had a detection rate of 10%), as shown by Fisher's exact test[10] **confirming** H_1 ($OR = 13.98$, 95% CI $= [3.02, Inf]$, $p = .0004$) **and** H_2 ($OR = 15.83$, 95% CI $= [3.466, Inf]$, $p = .0002$). No significant differences were detected between the no-video-group and the video-group (Fisher's test, $OR = 1.13$, 95% CI $= [0.3679725, Inf]$, $p = .532$), thus **failing to confirm** H_3.

[8] Data protection policy: https://www.soscisurvey.de/en/data-protection .

[9] Note, the authors of [18] do not report the demographics separate for their groups.

[10] Note that for all our hypotheses one-tailed tests are used.

6.2 Manipulation Detection for Various Subgroups

The free-text answers were analysed by two of the authors independently and then discussed. As the provided free-text answers were rather short we took this approach rather than a formal open-coding approach. Eight participants (4 in the no-video-group and 4 in the video-group) answered in the post-survey that they noticed the manipulation, but did not report it to the study examiner. When asked to explain why they did not report it, the following reasons were stated[11]: Two mentioned that they did not want to call in the late hour, two answered that calling would be too much effort, two believed that the vote casting was successfully completed despite the fact that the steps on the interface did not match the ones on the polling sheet, two thought that they themselves were at fault and one believed that the missing code is displayed later in the process.

Overall 31 participants (17 in the video-group and 14 in the no-video-group) reported reading the voting material before starting with the voting procedure; 21 (ten in the video-group and 11 in the no-video-group) reported reading the materials while voting. Note that two participants reported both reading the materials completely beforehand and reading them again while voting. One participant (from the video-group) reported reading the study instructions and role card beforehand, but only reading the polling sheet while voting. Of the 31 participants who read the voting materials beforehand, 23 (74.1%) detected and reported the manipulation, as opposed to 9 out of 19 (47.4%) of those who did not read the materials beforehand.

6.3 Video Related Statements

Out of 26 participants assigned to the video-group, nine reported watching parts of the video, 11 reported watching all of it and six reported not watching the video at all. None of the participants reported watching the video more than once. The participants who reported not watching the video gave the following reasons for this: Two answered that the video was too long, one answered that watching the video would be too much effort and three answered that they believed watching the video was not necessary to complete the voting.

From those 20 participants who stated that they fully or partially watch the video, 15 participants reported the manipulation and called the support. In particular, nine out of 11 of participants that watched the video entirely reported the manipulation, compared to six out of nine of participants who watched parts of the video.

Furthermore, one could observe differences between manipulation detection rate depending on whether the participants familiarised themselves with the voting procedure before starting voting, either by watching the video fully (in the video-group) or by reading the voting materials beforehand (in both video-group and no-video-group). As such, 24 out of 34 participants who either watched the video fully or read the voting materials before voting were able to detect the

[11] Note that some of the participants mentioned several reasons for not calling.

manipulation (70.6%) as opposed to 8 out of 16 (50%) participants who did neither of these things.

Out of the participants who reported watching the video either fully or partially, who also have detected the manipulation and called the support (15 participants), the following answers were given regarding to whether the video was helpful to them for detecting the manipulation: nine agreed, four disagreed, and one were neutral.

7 Discussion

Our results clearly show that the E-Vote-ID-2021-proposal outperforms the original system with respect to the detection manipulation rate (62.5% to 10%). As the authors in [16] showed that the E-Vote-ID-2021-proposal outperforms the original system with respect to the provided guarantees for vote secrecy (because it uses voting codes) and that they have a similar general usability performance, it can clearly be recommended to consider the E-Vote-ID-2021-proposal for the elections and polls in Switzerland as well as for any other election contexts with simple ballots. Note, the proposal of Kulyk et al. [16] does also outperform the original one because (1) the assumption that the vote casting device is not violating vote secrecy is not needed and (2) it is only possible to conduct limited election integrity related attacks as one can only remove votes but not change them – thus large scale manipulations would result in a unexpected low turnout.

The findings from the free-text answers (e.g. they thought it is too much effort to call, they thought they made a mistake) indicate that increasing the manipulation rate would need additional measures such as awareness raising for verifiability and why the voting material received via postal service can be trusted but not necessary the election webpage. This is a clear and important direction for future work.

We also found that participants who reported that they read the voting material only as they voted were more likely to follow the instructions on their screen, thus missing the manipulation. Thus, those who familiarized themselves with the process beforehand are more likely to detect the manipulation (between 75% and 77% compared to 62.5% and 65%). Thus, in particular in contexts like in Switzerland in which elections and/or polls happen several times a year, it gets over time more likely that manipulations are detected: If we assume that voters have voted several times with a system that is not manipulated and thus get familiar with the correct process, they might be more likely to detect a manipulation with future elections than if already the first time the system is in place, it got manipulated. The evaluation of such hypotheses is part of our future work.

Our study furthermore detected higher rates of manipulation detection compared to related work evaluating same kind of attacks - as such, the study by Kulyk et al. [18] found 43% manipulation detection rates and the study by Volkamer et al. [29] reported 41% compared to 62.5% of participants in our study (those who did not watch the video). One explanation could be the difference in demographics, in particular, the fact that the participants in our study tended to be younger than in related work, see e.g. Table 1 for the comparison between our participants and those in [18]. A study on the effects of demographic factors, including but not limited to age, gender and education, on the voter's ability to detect manipulations is therefore an interesting direction of future work. An other one might be that less people in [18,29] have read the instructions before starting the vote casting process. Note, a comparison is not possible as the authors do not provide any related information.

Study Limitations: Our study has similar limitations to other user studies evaluating the manipulation-detection efficacy in verifiable electronic voting: It is about a mock election and no actual election. Participants cast a vote for the option they were asked to select. Thus, this vote is not very personal to them or important. Participating in a study and, thus, agreeing to take time for it may result in spending more time in reading the instructions compared to casting a vote in an actual election. However, introducing vote manipulations in an actual election to measure manipulation-detection efficacy would pose critical ethical and legal issues. Thus, there is not much one can do about it.

Another limitations of all these studies evaluating manipulation-detection efficacy (including ours) is that we need to trust that those few participants who know each other have not informed others about the manipulation. Furthermore, we evaluated the scheme in Germany with participants who have not cast a vote with the original system. The results may be different for participants who are familiar with the original system.

We studied one implementation of adversaries' attempt to make voters believe their vote was cast as intended while their vote is not considered in the tally. The details can vary, i.e., the text displayed to convince voters that everything is fine. As future work, one could study the attack with different text.

In order to test two of the three hypotheses, we used data from our previous paper, i.e. [18]. This comes with some limitations as the study in the previous paper was a lab study, i.e. the study instructor was in the same room while in this paper, the study instructor could only be reached via phone. However, on the one hand the difference with respect to the detection rates are large and several studies have already shown the issues with the original system. Therefore, we wanted to focus our own data collection on the new proposal and the effect of the video.

8 Conclusion

Verifiable voting schemes are the de-facto standard when considering online voting for political elections. At the same time, the verifiable voting systems in place only provide vote secrecy if the voting client is trustworthy. While this shortcoming can be addressed with code voting, such approaches are currently not considered, as the community and election officials are concerned about the usability implications. Kulyk et al. demonstrated in [16] that a code voting based extension of the original system can be as usable as the original one. We underline their conclusions as we show that such an extension can also significantly increase the manipulation-detection efficacy. Thus, it is worth considering code-voting verifiable voting schemes, as the cumbersome steps of entering voting codes manually can be replaced by easy-enough steps – i.e., scanning QR codes – without significantly reducing the usability while enabling systems with higher security guarantees. Thus, our research should encourage more research on combining code-voting with verifiable schemes.

While the manipulation-detection efficacy is significant higher for the studied scheme compared to the original system one, there is room for improvements. We evaluated whether a video intervention describing the vote casting steps including those to verify can further improve this rate. While we observed some increase, it was not significant. Based on the discussion of our results, we conclude that it is important to study various types of interventions with respect to their effect on manipulation-detection efficacy. In particular, approaches explaining the importance of verifiability should be developed and evaluated.

Acknowledgements. This research was further supported by funding from the topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

References

1. Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: Usability of voter verifiable, end-to-end voting systems: baseline data for Helios, Prêt à Voter, and Scantegrity II. USENIX J. Election Technol. Syst. **2**(3), 26–56 (2014)
2. Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.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 J. Election Technol. Syst. **3**(2), 1–19 (2015)
3. Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: Summative usability assessments of STAR-Vote: a cryptographically secure e2e voting system that has been empirically proven to be easy to use. Hum. Factors **64**, 1–24 (2018)
4. Bär, M., Henrich, C., Müller-Quade, J., Röhrich, S., Stüber, C.: Real world experiences with bingo voting and a comparison of usability. In: EVT/WOTE (2008)
5. Bernhard, M., et al.: Can voters detect malicious manipulation of ballot marking devices? In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 679–694. IEEE (2020)
6. Budurushi, J., Neumann, S., Olembo, M.M., Volkamer, M.: Pretty understandable democracy - a secure and understandable internet voting scheme. In: ARES, pp. 198–207 (2013)
7. Budurushi, J., Renaud, K., Volkamer, M., Woide, M.: An investigation into the usability of electronic voting systems for complex elections. Ann. Telecommun. **71**(7–8), 309–322 (2016)
8. Chaum, D.: SureVote: technical overview. In: Proceedings of the Workshop on Trustworthy Elections (WOTE 2001) (2001)
9. Distler, V., Zollinger, M.L., Lallemand, C., Roenne, P., Ryan, P., Koenig, V.: Security-visible, yet unseen? How displaying security mechanisms impacts user experience and perceived security. In: ACM CHI, pp. 605:1–605:13 (2019)

10. Fuglerud, K.S., Røssvoll, T.H.: An evaluation of web-based voting usability and accessibility. Univ. Access Inf. Soc. **11**(4), 359–373 (2012)
11. Gjøsteen, K., Lund, A.S.: An experiment on the security of the Norwegian electronic voting protocol. Ann. Telecommun. **71**(7–8), 299–307 (2016)
12. Haines, T., Lewis, S.J., Pereira, O., Teague, V.: How not to prove your election outcome. In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 644–660. IEEE (2020)
13. Helbach, J., Schwenk, J.: Secure internet voting with code sheets. In: Alkassar, A., Volkamer, M. (eds.) Vote-ID 2007. LNCS, vol. 4896, pp. 166–177. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77493-8_15
14. Joaquim, R., Ribeiro, C., Ferreira, P.: VeryVote: a voter verifiable code voting system. In: Ryan, P.Y.A., Schoenmakers, B. (eds.) Vote-ID 2009. LNCS, vol. 5767, pp. 106–121. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04135-8_7
15. Karayumak, F., Olembo, M.M., Kauer, M., Volkamer, M.: Usability analysis of Helios-an open source verifiable remote electronic voting system. In: EVT/WOTE. USENIX (2011)
16. Kulyk, O., Ludwig, J., Volkamer, M., Koenig, R.E., Locher, P.: Usable verifiable secrecy-preserving e-voting. In: Electronic Voting: 6th International Joint Conference, E-Vote-ID. University of Tartu Press (2021)
17. Kulyk, O., Neumann, S., Budurushi, J., Volkamer, M.: Nothing comes for free: how much usability can you sacrifice for security? IEEE Secur. Priv. **15**(3), 24–29 (2017)
18. Kulyk, O., Volkamer, M., Müller, M., Renaud, K.: Towards improving the efficacy of code-based verification in internet voting. In: Bernhard, M., et al. (eds.) FC 2020. LNCS, vol. 12063, pp. 291–309. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-54455-3_21
19. MacNamara, D., Gibson, P., Oakley, K.: A preliminary study on a DualVote and Prêt à voter hybrid system. In: CeDEM, p. 77 (2012)
20. MacNamara, D., Scully, T., Gibson, P.: DualVote addressing usability and verifiability issues in electronic voting systems (2011). http://www-public.it-sudparis.eu/~gibson/Research/Publications/E-Copies/MacNamaraSGCOQ11.pdf. Accessed 12 May 2022
21. Zollinger, M.-L., Estaji, E., Ryan, P.Y.A., Marky, K.: "Just for the Sake of Transparency": exploring voter mental models of verifiability. In: Krimmer, R., et al. (eds.) E-Vote-ID 2021. LNCS, vol. 12900, pp. 155–170. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-86942-7_11
22. Marky, K., Kulyk, O., Renaud, K., Volkamer, M.: What did I really vote for? In: ACM CHI, p. 176 (2018)
23. Marky, K., Schmitz, M., Lange, F., Mühlhäuser, M.: Usability of code voting modalities. In: ACM CHI (2019)
24. Marky, K., Zollinger, M.L., Roenne, P., Ryan, P.Y., Grube, T., Kunze, K.: Investigating usability and user experience of individually verifiable internet voting schemes. ACM Trans. Comput.-Hum. Interact **28**(5), 1–36 (2021)
25. McDonald, J.H.: Handbook of Biological Statistics, vol. 2. Sparky House Publishing, Baltimore (2009)
26. Oostveen, A.M., Van den Besselaar, P.: Users' experiences with e-voting: a comparative case study. J. Electron. Governance **2**(4), 357–377 (2009)

27. Ryan, P.Y.A., Teague, V.: Pretty good democracy. In: Christianson, B., Malcolm, J.A., Matyáš, V., Roe, M. (eds.) Security Protocols 2009. LNCS, vol. 7028, pp. 111–130. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36213-2_15
28. Sherman, A.T., et al.: An examination of vote verification technologies: findings and experiences from the Maryland study (2006)
29. Volkamer, M., Kulyk, O., Ludwig, J., Fuhrberg, N.: Increasing security without decreasing usability: comparison of various verifiable voting systems. In: Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). USENIX Association, Boston, August 2022. https://www.usenix.org/conference/soups2022/presentation/volkamer
30. Weber, J.L., Hengartner, U.: Usability study of the open audit voting system Helios (2009). https://www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf. 12 May 2022
31. Winckler, M., et al.: Assessing the usability of open verifiable E-voting systems: a trial with the system Prêt à voter. In: ICE-GOV, pp. 281–296 (2009)