Robert Krimmer, Melanie Volkamer, David Duenas-Cid,
Micha Germann, Stéphane Glondu, Thomas Hofer, Iuliia Krivonosova,
Beata Martin-Rozumilowicz, Peter Rønne, Marie-Laure Zollinger (Eds.)

Seventh International Joint Conference on Electronic Voting

E-Vote-ID 2022

4-7 October 2022

Co-organized by:

University of Tartu
Johan Skytte Institute of Political Studies
Karlsruhe Institute of Technology
Institute of Applied Informatics and Formal Description Methods
Gdańsk University of Technology
Informatics in Management
E-Voting.CC GmbH
Competence Center for Electronic Voting and Participation
Gesellschaft für Informatik
German Informatics Society, SIG SEC/ECOM
Kastel
Competence Center for Applied Security Technology

PROCEEDINGS

Robert Krimmer, Melanie Volkamer, David Duenas-Cid
Micha Germann, Stéphane Glondu, Thomas Hofer, Iuliia Krivonosova,
Beata Martin-Rozumilowicz, Peter Rønne, Marie-Laure Zollinger (Eds.)

Seventh ***Joint International Conference on Electronic Voting***

E-Vote-ID 2022

4-7 October 2022

Co-organized by the University of Tartu, Karlsruhe Institute of Technology, Gdańsk University of Technology, E-Voting.CC, Gesellschaft für Informatik and Kastel

UNIVERSITY OF TARTU
Press
1632

Proceedings E-Vote-ID 2022
University of Tartu Press
ISBN 978-9916-27-035-6

Volume Editors

Prof. Dr. Dr. Robert Krimmer
University of Tartu
Johan Skytte Institute of Political Studies
Lossi 36
51003 Tartu, Estonia
robert.krimmer@ut.ee

Prof. Dr. Melanie Volkamer
Karlsruhe Institute of Technology
Institute of Applied Informatics and Formal Description Methods
Kaiserstr. 89
76131 Karlsruhe, Germany
melanie.volkamer@secuso.org

Dr. David Duenas-Cid
Gdansk University of Technology
Informatics in Management
Gabriela Narutowicza 11/12,
80-233 Gdańsk, Poland
david.duenas.cid@pg.edu.pl

Micha Germann
University of Bath
E-mail: mg2107@bath.ac.uk

Stéphane Glondu
Institut National de Recherche en Sciences et Technologies du Numérique
E-mail: stephane.glondu@inria.fr

Thomas Hofer
Objectif Securité
E-mail: thomas.hofer@objectif-securite.ch

Iuliia Krivonosova
Independent Researcher
E-mail: krivonosova.iuliia@gmail.com

Beata Martin-Rozumlowicz
European Commission
E-mail: rozumil@hotmail.com

Peter Rønne
LORIA - Lorraine Research Laboratory in Computer Science and its Applications
E-mail: peter.roenne@gmail.com

Marie-Laure Zollinger
University of Luxembourg
E-mail: marie-laure.zollinger@uni.lu

This conference is co-organized by:

University of Tartu - Johan Skytte Institute of Political Studies

Karlsruhe Institute of Technology - Institute of Applied Informatics and Formal Description Methods

Gdańsk University of Technology – Informatics in Management Department

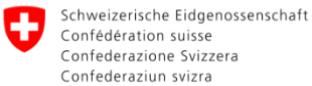
E-Voting.CC GmbH - Competence Center for Electronic Voting and Participation

Gesellschaft für Informatik, German Informatics Society, SIG SEC/ECOM

Kastel, Competence Center for Applied Security Technology

Supported by:

Regional Government of Vorarlberg



Swiss Federal Chancellery

General Chairs

Krimmer, Robert (University of Tartu - Johan Skytte Institute of Political Studies, Estonia)
Volkamer, Melanie (Karlsruhe Institute of Technology - Institute of Applied Informatics and Formal Description Methods, Germany)
Duenas-Cid, David (Gdańsk University of Technology – Informatics in Management, Poland)

Track on Security, Usability and Technical Issues

Peter Rønne
Lorraine Research Laboratory in Computer Science and its Applications, France
Melanie Volkamer
Karlsruhe Institute of Technology, Germany

Track on Administrative, Legal, Political and Social Issues

Micha Germann
University of Bath, UK
Robert Krimmer
University of Tartu, Estonia

Track on Election and Practical Experiences

Beata Martin-Rozumilowicz
European Commission, Brussels
Thomas Hofer
Objectif Securité, Switzerland

PhD Colloquium

Marie-Laure Zollinger
University of Luxembourg, Luxembourg
David Duenas-Cid
Gdańsk University of Technology, Poland

Poster and Demo Session

Stéphane Glondu
Institut National de Recherche en Sciences et Technologies du Numérique, France
Jurlind Budurushi
IT University Copenhagen, Denmark

Outreach Chairs

Rønne, Peter
University of Luxembourg, Luxembourg
Krivonosova, Iuliia
Independent Researcher, Switzerland

Organizational Committee

Tim Wurmbach
E-Voting.CC, Austria

Preface

This volume contains papers presented at E-Vote-ID 2022, the Seventh International Joint Conference on Electronic Voting, held during October 4–7, 2022. This was the first in-person conference following the COVID-19 pandemic, and, as such, it was a very special event for the community since we returned to the traditional venue in Bregenz, Austria. The E-Vote-ID conference resulted from merging EVOTE and Vote-ID, and 18 years have now elapsed since the first EVOTE conference in Austria.

Since that conference in 2004, over 1500 experts have attended the venue, including scholars, practitioners, authorities, electoral managers, vendors, and PhD students. E-Vote-ID collects the most relevant debates on the development of electronic voting, from aspects relating to security and usability through to practical experiences and applications of voting systems, also including legal, social, or political aspects, amongst others, turning out to be an important global referent on these issues.

Also, this year, the conference consisted of

– Security, Usability, and Technical Issues Track;

– Governance Track;

– Election and Practical Experiences Track;

– PhD Colloquium;

– Poster and Demo Session.

E-Vote-ID 2022 received 55 submissions for consideration in the conference. After the submission deadline, the Programme Committee members of the respective tracks bid for the papers to review: the respective track chairs assigned the papers, with the aim to have each reviewed by three to five Program Committee members using a double-blind review process. After completing the reviews, the track chairs led a discussion with the reviewing Programme Committee members regarding (conditional) acceptance or rejection. For a conditional acceptance, a shepherd was assigned to ensure that the reviewers' proposed changes were included and the revised paper could be accepted. Finally, after a joint discussion, the general chairs made the final decisions with the track chairs. As a result, 10 papers were accepted for the LNCS volume, representing 18% of the submitted proposals, and 27 for the University of Tartu Press Proceedings, representing 49%. The selected papers cover a wide range of topics connected with electronic voting, including technical, societal, and practical analyses of its use.

We would like to thank the German Informatics Society (Gesellschaft für Informatik), with its ECOM working group, and KASTEL for their partnership over many years. Further, we would like to thank the Swiss Federal Chancellery and the Regional Government of Vorarlberg for their kind support. E-Vote-ID 2022 was kindly supported through the European Union's Horizon 2020 projects ECEPS (grant agreement 857622) and mGov4EU (grant agreement 959072). Special thanks go to the international Programme Committee members for their hard work in reviewing, discussing, and shepherding papers. They ensured the high quality of these proceedings with their knowledge and experience.

October, 2022

Robert Krimmer
Melanie Volkamer
David Duenas-Cid
Peter Roenne
Micha Germann
Beata Martin-Rozumiłowicz
Thomas Hofer
Glondu, Stéphane
Jurlind Budurushi
Marie-Laure Zollinger

Table of Contents

General Conference

PhD Colloquium

Demo/Poster Session

Program Committee

Marta Aranyossy	Corvinus University of Budapest
Roberto Araujo	Universidade Federal do Pará
Jordi Barrat	eVoting Legal Lab
Bernhard Beckert	Karlsruhe Institute of Technology, Germany
Josh Benaloh	Microsoft
Matthew Bernhard	University of Michigan
David Bismark	Votato
Enka Blanchard	Université de Lorraine
Jurlind Budurushi	Qatar University
Christian Bull	The Norwegian Ministry of Local Government and Regional Development
Susanne Caarls	Election Consultant
Gianpiero Catozzi	UNDP
Thomas Chanussot	IFES
Jeremy Clark	Concordia University
Cesar A. Collazos	Universidad del Cauca
Veronique Cortier	Centre National de la Recherche Scientifique, Loria
Régis Dandoy	Universidad San Francisco de Quito
Staffan Darnolf	International Foundation for Electoral Systems
Constantin Catalin Dragan	University of Surrey
David Duenas-Cid	Gdańsk University of Technology
Helen Eenmaa	University of Tartu
Philipp Egger	Staatskanzlei Kanton St.Gallen
Aleksander Essex	University of Western Ontario
Joshua Franklin	National Institute of Standards and Technology
Chelsea Gabel	McMaster University
Micha Germann	University of Bath
J Paul Gibson	Mines Telecom
Rosario Giustolisi	IT University of Copenhagen
Kristian Gjøsteen	Norwegian University of Science and Technology
Stéphane Glondu	Inria, Loria
Nicole Goodman	Brock University
Rajeev Gore	The Australian National University
Ruediger Grimm	University of Koblenz
Rolf Haenni	Bern University of Applied Sciences
Thomas Haines	Queensland University of Technology
Thomas Hofer	Objectif Securité
Bart Jacobs	Radboud University
Wojtek Jamroga	Polish Academy of Sciences
Budurushi Jurlind	Qatar University
Norbert Kersting	University of Münster
Michael Kirsten	Karlsruhe Institute of Technology
Reto Koenig	Berne University of Applied Sciences
Steve Kremer	Institut National de Recherche en Sciences et Technologies du Numérique
Robert Krimmer	University of Tartu

Iuliia Krivonosova	Tallin University of Technology
Oksana Kulyk	IT University of Copenhagen
Ralf Küsters	University of Stuttgart
Olivier Leclère	State of Geneva
Leontine Loeber	University of East Anglia
Ryan Macias	RSM Election Solutions LLC
Beata Martin-Rozumilowicz	European Commission
Ardita Maurer	Zentrum für Demokratie Aarau/Zurich University
Andreas Mayer	Hochschule Heilbronn
Ronan McDermott	mcdis
Jevgeni Meo	MEO OÜ
Vladimir Misev	OSCE/ODIHR
Johannes Mueller	University of Luxembourg
Magdalena Musial-Karg	Adam Mickiewicz University
Andras Nemeslaki	Budapest University of Technology and Economics
Stephan Neumann	Landesbank Saar
Hannu Nurmi	University of Turku
Jon Pammett	Carleton University
Liisa Past	Information System Authority, Republic of Estonia
Olivier Pereira	UCLouvain
Goran Petrov	OSCE/ODIHR
Stéphanie Plante	University of Ottawa
Pascal Reisert	University of Stuttgart
Karen Renaud	University of Strathclyde
Adria Rodriguez	Scytl Election Technologies
Peter Roenne	Université de Lorraine
Stefan Roseman	Federal Office for Information Security
David Ruescas	nVotes
Mark Ryan	University of Birmingham
Peter Y A Ryan	University of Luxembourg
Giulia Sandri	European School of Political and Social Sciences
Peter Sasvari	National University of Public Service
Steve Schneider	University of Surrey
Berry Schoenmakers	Eindhoven University of Technology
Carsten Schuermann	IT University of Copenhagen
Ted Selker	University of California at Berkeley
Uwe Serdült	Ritsumeikan University
Rodney Smith	University of Sydney
Mihkel Solvak	University of Tartu
Oliver Spycher	Swiss Federal Chancellery
Philip Stark	University of California at Berkeley
Ewa Syta	Yale University
Vanessa Teague	Thinking Cybersecurity
Tomasz Truderung	University of Trier
Siim Trumm	University of Nottingham
Priit Vinkel	E-governance Academy
Melanie Volkamer	Karlsruhe Institute of Technology
Kåre Vollan	Quality AS

Felix von Nostitz	Université Catholique de Lille
Roland Wen	The University of New South Wales
Gregor Wenda	BMI
Jan Willemson	Cybernetica
Peter Wolf	IDEA
Michael Yard	IFES
Filip Zagorski	Wroclaw University of Technology
Marie-Laure Zollinger	Université du Luxembourg

Author Index

General Conference

"What Will Make Me Trust or Not Trust Will Depend Upon How Secure the Technology Is": Factors Influencing Trust Perceptions of the Use of Election Technologies

Samuel Agbesi[1], Asmita Dalela[2], Jurlind Budurushi[13], and Oksana Kulyk[1]

[1] IT Univserity of Copenhagen, Denmark, {sagb,jurb,okku}@itu.dk
[2] asmita.dalela@gmail.com
[3] Qatar University, jurlind@qu.edu.qa

Abstract. Trust in an election system has been commonly recognized as a crucial factor in the adoption of the system and in ensuring that voters as well as participating parties accept the election outcome as legitimate. Ensuring and maintaining such trust, however, can be challenging, particularly in systems that involve advanced technologies – thus, technologies that both present a larger potential attack surface and are less understandable to lay voters. In this paper, we aim to investigate factors that influence voters' trust in election technologies. For this, we have conducted semi-structured interviews with 14 eligible voters in Denmark. In our analysis, we identified a number of perceived risks that voters have towards the use of election technologies, as well as identified 11 themes, representing factors, that we grouped into *technological trust*, *institutional trust* and *others*. From our analysis, we conclude that there is a need in increasing transparency to ensure voters' understanding of the security level provided by election technologies, as well as in involving other stakeholders such as vendors and election authorities in measures to improve trust. We furthermore conclude that technical measures, while necessary, are not sufficient in ensuring trust in election technologies in absence of general trust towards institutions and society as a whole.

1 Introduction

Ensuring public trust in the election process is crucial regarding the legitimacy of the election and the acceptance of its result by the population, in particular by the supporters of losing parties. However, in the growing presence of threats to the election integrity, such as cyber attacks on election infrastructure or disinformation campaigns, it is particularly challenging to establish and maintain trust. These challenges are even exacerbate by the use of election technologies, such as electronic voting, which enable a larger attack surface (e.g. by allowing an attacker to conduct large-scale manipulations, when electronic voting systems are not protected sufficiently) and are difficult to understand for lay voters (e.g. due to lack of transparency).

This paper aims to understand the factors that influence trust in election technologies, which we define as all electronic systems that are used by the election authorities, such as electronic poll books that contain a list of eligible voters within a voting district, electronic voting system, and electronic tallying system. Thereby, we investigate trust towards election technologies in the context of Danish voters. While Denmark is considered a highly digitized country, its use of election technologies has been limited so far. As such, the voters use traditional, paper-based voting, both for authenticating themselves to election officials at the polling station via authorization letter they receive via mail, and for casting their vote via filling out a paper ballot. While technology is used for e.g. aggregating voting results from polling stations, such processes are usually outside of view for voters. The only aspect of Denmark's election system that uses some form of technology that directly involves the voters is the independent parliamentary candidate declaration process, where the candidates can collect voter declarations from eligible voters electronically, to be eligible to participate in the election [25]. This system, however, faced criticism from security researchers who were able to find security vulnerabilities [30]. In 2012 there was an attempt to introduce Internet voting in the national elections upon a request from mayors of 12 municipalities and the Local Government [10]. A team of experts was commissioned to investigate the feasibility of introducing Internet voting in the Danish electoral process. The investigation identified several advantages that could be achieved through the deployment of Internet voting; however, despite these advantages, trust issues were identified as the biggest disadvantage of introducing Internet voting. Therefore, our goal is to investigate such issues in depth, and to use the results of our investigation as a first step in understanding how to build systems that are not only secure but are also trusted by the voters. To achieve this goal we conducted a qualitative study aiming to answer the following research question:

RQ: What influences the trust of Danish citizens regarding the use of election technologies?

We have conducted interviews with 14 individuals in Denmark who are eligible to vote. We have found that even though the election technologies have the variegated nature, our participants perceived the term election technologies as Internet voting in a broader context, suggesting limited awareness about other kinds of election technologies, including the ones currently in use. The themes that emerged from our analysis show that voters are indeed concerned about security risks in election technologies, and that various measures – such as providing verifiability options, assurances from trusted entities, and transparency measures – can mitigate such concerns. At the same time, we find that trust in society and institutions plays a crucial role. Thus, we conclude and recommend that a holistic approach is necessary to establish voters' trust in elections supported by election technologies.

2 Related work

In this section we describe relevant work in terms of general theories on trust in technology, including election technologies, as well as on trust in the context of Danish society.

2.1 Trust in technology

Trust has been commonly defined as the willingness to rely on other parties while being vulnerable to risks [21]. Trust has been studied across various disciplines, focusing on different aspects of trust. For instance, in the field of computer science, research on trust has been focusing on technologies enabling various security measures such as authentication and access control [14]. On the other hand, studies on trust in social and behavioral sciences tend to focus on users' perceptions and attitudes that influence their trust in a particular entity (e.g. person, organisation or technology) [14]. Thus, it is possible that a mismatch exists between technologies used to ensure the trustworthiness of a system and the extent to which these technologies actually create trust among users [24].

In the context of technology, a number of studies have investigated users' perceptions of trust regarding different technologies, such as consumer-generated content [9], AI-based recommendation systems [32], mobile payment platforms [31], e-commerce services [35], online reviews [11], cloud-based systems [18], and IoT systems [15]. These studies have concluded that trust is crucial for the adoption of corresponding technologies, as well as identified factors as transparency of the system, security, privacy, perceived risk, social influence, information quality, and performance efficacy to influence users' trust in the context of technology.

Particularly relevant to our work is the investigation of trust in e-government services. As such, a recent study by Li and Xue [19] analyzed the factors influencing Chinese citizens' trust in the continuous use of e-government systems. The findings of the study showed that factors such as trust in government, trust in the Internet, information quality, and service quality are key factors influencing citizens' trust. The study by Gulati et al. [13] also identified motivation, willingness, competence, benevolence, predictability, honesty, and reciprocity as key factors influencing citizens' trust. Trust in the Internet was also identified by Aranyossy [3] to influence citizens' trust in e-government services. These findings were also supported by [2] and [27]. In the work by Alharbi et al. [2], trust in government, trust in the Internet, and social trust were found to influence citizens' intention to use e-government services. Apart from trust in the government and the Internet, the study conducted by Ranaweera [27] also identified perceived security, perceived privacy, and perceived risk to influence citizens' use of e-government service.

Other studies have focused on researching the role of trust in election technologies. As such, Dalela et al. investigated voters' trust in risk-limited audits, showing that voters had less confidence when informed about the details of the auditing process, namely, the number of ballots chosen to be audited [6]. Zhu et al. [38] identified privacy, security, usability, and validity of election technologies as key factors influencing citizens' intention to use e-voting. Other

factors such as convenience [17,20], ease of use and trust in the Internet [22], level of digitalisation in the society, perceived security of the Internet and voter socio-demographic status [20,8] have also been identified to influence citizens' intention to use election technologies. While these studies have emphasized the importance of trust in the adoption of election technologies, they did not explore what influences voters' individual willingness to trust in election technologies or lack of it. An investigation of some of these factors has been conducted by Ehin and Solvak [7] in the context of Estonian elections via a quantitative study, confirming the effect of voters' political preferences on trust towards Internet voting. We complement their work by conducting an explorative qualitative study, looking into further factors that influence voters' individual trust regarding the use of election technologies in an electoral process.

2.2 Trust in Denmark

Prior studies [33,23] have postulated that there is a high level of trust among Danish citizens, and one of the key factors that have influenced this level of trust within the Danish society has been attributed to the universal welfare state. According to the work by Svendsen et al. [33], the Scandinavian countries, which include Denmark enjoy a high level of social trust because of "institutional quality" and "equal access to public goods" [33], i.e. citizens having equal access to goods and services. Furthermore, the level of social trust in Denmark has also been attributed to the political stability in the country [33]. Political instability can destroy a country's social trust, and Denmark has accumulated this social trust over a period of time due to its stable political system [33].

Apart from the trust among the Danish citizens, there is also trust between the citizens and the authorities. A study conducted by Nilsen and Lindvall [23] during the COVID-19 pandemic showed that citizens had high trust in the authorities and the health officials in providing COVID guidelines. This trust in authorities has also been argued to play a role in citizens' trust in public digital services introduced by the government. Citizens have trust and confidence in the authorities to implement a secure public digital service [36], and this trust has played an important role in the increased use of digital services in Denmark. Nonetheless, despite the trust citizens have in the various digital services, their trust towards election technology and its use in an electoral process has not been systematically studied, yet.

3 Methodology

The main goal of this work is to gain an in-depth understanding of factors that influence citizens' trust in the use of election technologies, and to develop a theory out of themes emerging from the collected data. We followed an inductive approach [29] and conducted interviews with participants (eligible voters in Denmark). To achieve this goal, we developed an interview guide based on previous research, namely [2,37,39]. The guide consists of three sections. In the

first section, we investigated participants' perception regarding online services and their level of trust in these services. We questioned them about their experiences and concerns when using these services. In the second section, we explored participants' perceptions of election technologies by asking questions related to their confidence in the election result in the case of internet voting. Finally, in the third section, we examined participants' trust in election authorities by asking them about the integrity and accountability of the authorities.

Recruitment and Data Collection For our study we recruited participants that are eligible to vote in Denmark, which includes Danish citizens as well as expats who have the right to vote (e.g. in local elections). The participants were selected using purposive sampling, and whether they have voted on any of the elections conducted in Denmark and/or reported having knowledge about the electoral process in Denmark. None of the participants have used e-voting to vote in a political or non-political elections. The participants were contacted and invited to participate in the study via emails and personal phone calls. In total 14 participants took part in our study, consisting of four female and ten male participants. The age of the participants ranged from 18 to 70 years old, and their level of education ranged from High School diploma to Doctorate degree.

In order to collect data we conducted semi-structured interviews. The interviews were conducted either face-to-face or online. Note that the interview guide used to collect the data went through three iterations. In each iteration, we conducted a pilot interview and after the interview the project team meet to discuss and improve the questions based on the responses of the participant. Ambiguous questions were re-worded, and questions that did not add further value to our research were deleted.[4].

Data Analysis In order to analyse the collected data thematic analysis was used. "Thematic analysis is a method for identifying, analysing, and reporting patterns (themes) within data" [5]. Thematic analysis has been argued to be the appropriate technique for data analysis with respect to qualitative studies, which are not dependent on an initial theoretical framework. This method fits to our research goal of identifying themes from the collected data and using these to design a model with respect to factors that influence voters' trust in election technology. Our thematic analysis follows the steps described by Braun and Clark [5]. The first step was to familiarize with the content and to get a general overview of the collected data by reading through the interview transcripts. This step allowed us to take note of some initial ideas for the second step, namely coding. After the first step, we read through the interview transcripts again, but this time line-by-line. In this second step, extracts from the collected data that appeared interesting regarding our research question were assigned labels, so called codes. The list of codes generated in the second step were then classified. Codes were

[4] The resulting interview guide is available at `https://github.com/cometitu/interviews`

classified into different sub-themes/themes based on their relationship. Finally, the sub-themes/themes were reviewed, and final themes were identified. For our data analysis the NVIVO software package was used.

Reliability and Validity The reliability and validity of qualitative research assesses the rigor and the dependability of the procedures and methods followed during the data collection and analysis [28]. In the context of this study to ensure validity and reliability, we carefully selected interview participants. Furthermore, two other researchers randomly selected five interview transcripts for coding. Most of the codes generated by the two other researches were in line with the codes generated by the principal coder. The variations in the codes were discussed between the three researchers. Afterwards, the aligned codes were classified in sub-themes/themes. Finally, the sub-themes/themes were reviewed by four researchers and final themes were identified.

Ethics Before the beginning of each interview participants were provided with a consent form. In the face-to-face interviews we asked participants to read and fill out the consent form. In the online interviews, we read out the consent form and made sure participant's agreed to it before proceeding with the interview. Participants were assured that all information is used anonymously and only for research purposes. To ensure participants' anonymity, we removed all identifiable information that appeared in the interview transcript.

Study Limitations The study has some limitations. Most of the individuals that we interviewed were located in the capital city and had at least a Masters degree. Hence, it is not clear to which extent the findings can be generalized, e.g. to Danish voters in rural areas or to voters with lower levels of education. Even though our sample is considered sufficient for an exploratory, qualitative study [4,26], further large-scale studies need to be conducted in order to better understand to which extent our findings are common in a representative population.

4 Results

This section reports our findings from the data analysis[5]. First, we present the findings with respect to the perceived risks regarding election technologies. Since risk and trust are inextricably intertwined, that is, if no risk is perceived, then there is no need for trust. Therefore, it is important to look at factors that constitute perceived risk in our analysis. Afterwards, we introduce the factors that influence voters' trust regarding election technologies.

[5] The codebook containing the summary of derived codes and their frequences are available at `https://github.com/cometitu/interviews`

4.1 Perceived Risks

Our analysis shows that participants are aware and concerned about a variety of risks that election technologies can introduce in the election process. Since risk plays a significant role in establishing trust, it is important to discuss what constitutes the perceived risk.

Some participants (5 out of 14) mentioned that the introduction of election technologies in elections will lead to *hackers attack* as it is much easier to hack a thousand computers than to hack a thousand people. The participants also emphasized that the security of Big tech companies has been compromised in the past, therefore it will be easy for hackers to compromise the security of election technologies, if used in Danish elections: *"Even the biggest companies you know Sony, Microsoft, Google, Facebook, they all got hacked. Why would the state of Denmark be any better than those companies in maintaining you know their IT security."* Participants expressed that the risk of hacker attacks could make people insecure regarding the voting process. This would lead to voters' lack of trust in the election system.

Some participants (4 out of 14) mentioned that *manipulation of election results* could happen if election technologies are used. They argued that since a small group of people will be involved in the process, it could be easy to manipulate the election results. For instance, vote secrecy can be violated publishing online voters' preferences: *"In a digital voting system the amount of people involved would be much smaller and closer group where actually the risk for conspiracy or carteling would be... I think it would be easier to make conspiracy with the digital voting system."* Participants highlighted that this will create doubt in citizens' mind around the election results and make them distrust the election system. Further concerns were raised by some participants (5 out of 14) regarding possible *cyber attacks by nation states* and *cyberwarfare*. Thereby, participants expressed that the use of election technologies in Danish elections could make the elections vulnerable to cyber attacks. Malicious actors could try to influence the political scene in Denmark by manipulating the election results: *"We're talking Ukraine cyber war or pressure from Russia and if there's one thing we can do to expose ourselves towards like a Russian influence, that's by having an electronic voting system."*

A few participants (2 out of 14) expressed that *election technologies introduce points of failure* in the system. This can disrupt elections and make voters skeptical of casting their vote: *"If my vote is just a number in a database essentially, then the database is like a single point of failure, which could be influenced and that would make me suspicious."* In addition to the aforementioned factors of perceived risks regarding election technologies, participants raised concerns regarding the *reliability* of such technologies and the possibilities of flaws which could affect the election due to its complexity: *"There will be some, you know there will be places of failure where it could fail more catastrophically. Also, reliability, let's say you have a power cut in the middle of an election."*. Some participants (4 out of 14) expressed that the paper-based systems would be more robust and effective in eliminating such flaws: *"I think there are flaws in every technology*

and I think it would take quite a while before I personally would trust that this [election] technology would be working as it should."

4.2 Factors of Trust

When considering factors that could potentially mitigate or exacerbate the aforementioned risks, influencing the voters' trust in the election technologies – we distinguish between factors related to *Technological*, *Institutional*, and *Other* aspects of trust. All the factors are summarised in Figure 1

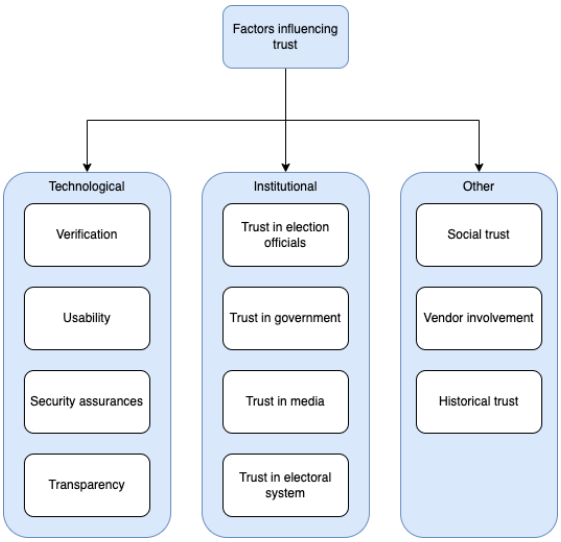


Fig. 1. Factors influencing voters' trust towards election technologies.

Technological Trust Technological trust describes the technical aspects that influence the voter's trust in the use of election technologies, related to the implementation and management of the used IT systems, as well as the communication with the voters regarding the status of these systems. Since election technologies have a significant reliance on IT systems, it is important to understand what technical dimensions contribute to this trust. The main sub-themes we identified hereby include *Verification*, *Usability*, Security Assurances and *Transparency*. We outline each of these sub-themes in the subsections below.

Verification When it comes to the use of election technologies, many participants (8 out of 14) expressed the need of verifying the election results, mentioning concepts such as system audit, verification or traceability. *"I would have confidence in the results, because I would trust that there would be so many verification*

processes of the result." Furthermore, participants expressed the importance of enabling voters to trace their votes. They argued that it is easier to ensure this with the current paper-based voting system because once you mark or cross your intention on the ballot paper it can no longer be altered, but the same cannot be guaranteed when using electronic voting system: *"it is very difficult for you to go back and establish what is called to establish intent of the voter... but for, in the paper I mean, once it is marked, it is marked, you know, that this person, this is whom he or she intended to vote for."*

Usability When it comes to usability of the election technologies, many participants (7 out of 14) emphasized the *ease of use* and the *rules and steps* to be followed while voting electronically, and that these *should be clearly stated*: *"But I will advise that in case the steps, you know, or the rules in voting electronically must be clearly stated so that one can easily go through and follow the steps and vote electronically."*

Security Assurances Half of the participants (7 out of 14) mentioned the necessity of *proper approaches*, i.e. procedures and techniques, when implementing the security assurances in election technologies: *"If implemented correctly and with certain security techniques, it should be more trustable than the current one."* Participants also emphasized that the *enhanced security design* of such technologies will help to restrain tampering of the election outcome: *"What will make me trust or not trust will depend upon how secure the technology is, you know, so if the security features are very well enhanced or are very strong such that the, our voting can not be in any way tampered electronically."* Some participants (4 out of 14) mentioned *authentication* as an important security assurance to influence the voters' trust in election technologies. Participants proposed the use of different authentication techniques such as secure login code, NemID or social security number to prevent unauthorized login into the voting platform: *"There should be a security or some sort of private code that pertains to everybody individually, such that it is known to you alone, that you can be able to use to enter into the system and vote."*

In addition to the need of following proper security approaches, many participants (7 out of 14) mentioned different kinds of assurances made on behalf of election authorities and other experts regarding the security of election technologies. Participants highlighted that elections authorities such as government official or representatives of opposing parties can convince voters regarding the safety and security of an election technologies which can lead to trust: *"Yes, I will feel confident if and only if, you know, before the vote is being cast... they are able to explain all the authorities concern are able to explain how secure the system is or how secure the e-voting is going to be."*

Apart from assurances by government officials, assurances from academic researchers and other professionals about the security of election technologies were also mentioned to influence voters' trust. Some participants (3 out of 14) stated that they trust these experts to investigate and determine the security of these technologies and also provide a solution that can make it more secure: *"I*

think for me personally, it would have to be a matter of like scholarly investigation of how to secure such a process. "

Transparency Transparency, also emerged as one of the main influencing factors of voters' trust in election technologies, as it is the need for the voters to be able to follow the workings of the election technologies. Participants (6 out of 14) revealed how the lack of transparency can have a negative effect on citizens' trust. In particular, one participant felt that an inherent disadvantage of election technologies is that it is designed as a black-box, so that lay voters are unable to understand how the system works – an issue that can be misused by a party that may want to create mistrust in the election outcome: *"It would be easier for the loser of the election to blame the loss on something that's been happening inside of this black box."* The raised issue with transparency in election technologies was contrasted with the paper-based voting process that was assumed to be easier to follow for every voter: *"I think from the general population have very little understanding of how a system like this would work, and it's easier to kind of visualize and understand how it works when you vote on paper."*

Institutional Trust Institutional trust describes the inherent trust of voters in the election officials, the government, media, and the electoral system. During the interviews it was evident that the collective trust in these entities creates a positive impression in the participant's mindset and convinces them to adopt the use of election technologies in the future elections. The main sub-themes include *Trust in Election Officials*, *Trust in Government*, *Trust in Media*, and *Trust in Electoral System*. We outline each of these sub-themes in the subsections below.

Trust in Election Officials Many participants (7 out of 14) mentioned that they believe in the integrity of the election officials and expect them behave according to the electoral law: *"I will just give them the benefit of the doubt that they will do something good."* Participants highlighted that the inclusion of diverse group of people from different demographics provides enough validation to maintain their collective integrity. The fact that the officials are the chosen representatives from all the parties participating in the election, ensures a positive mindset in the voters that a *self regulated system is maintained inside the system*: *"I would trust them because they are the people that are sitting there and taking the roles, they are elected by the local government within all parties. As far as I know, these are people from all parties. "* Participants mentioned also that there have never been any complaints or fraud that have surfaced which can make them question their trust in the officials: *"I have not heard any complaint. The last election that I participated in, I didn't heard any complaints or fraud."* When it comes to the implementation of election technologies, the technical competence of the election officials is also a driving factor for the acceptance and trustworthiness of the technologies by the voters. Many participants (7 out of 14) mentioned election authorities' lack of technical expertise for implementing such technologies and therefore they don't trust them to be able to run and

maintain such systems effectively. The participants conveyed their trust in the integrity of the election officials, however, they were sceptical of their technical competences: *"I can trust them to be honest. Right. I don't think I can trust them to be competent."* Participants also emphasized that it will be beneficial if some experts who have competence regarding election technologies can help the election officials in developing and maintaining such systems: *"Our authorities, I'm not sure that anyone there actually understands what it would take to make such a system, so we would have to have experts somewhere from where they have some good understanding of how such systems could run and and be created, I think."*

Trust in Government Some participants (4 out of 14) mentioned that they will trust the government decision to implement election technologies as they believe that the government will undertake proper testing and verification measures into consideration before implementing any new technology for future elections. Participants feel that government will assure the voters that the technology is reliable and secure to be used in elections, see also Section 4.2, for a discussion of a related theme of security assurances): *"I will say I trust it because this is recommended from government or from the politicians or whatever because and then we trust that this is OK because I would assume that there would be made so many testing and verification."* Participants also emphasized that the government is bound to take the right measures as any mishandling will be projected by the opposition party, which will create a negative image for the governing party in the voters: *"I may not have any mistrust issues when it [mishandling] happens that the opposing parties, I mean the losing parties start to complain and point out valid [arguments]."*

Trust in Media A few participants (3 out of 14) articulated that they have trust in media for creating news and exposing the mishandling of the data if that happened during the implementation of the technologies. Thus, avoiding potential corruption or cheating. Participants have a firm belief that the media will make sure that any discrepancy is reported to the voters: *"In Denmark, everything would be exposed if somebody tried to cheat the system, they would be exposed and they would rather they will be expelled of the system."*

Trust in Electoral System Participants (4 out of 14) mentioned that they have confidence in the Danish electoral system and believe that it works efficiently due to an involvement of diverse group of people from different parties making it difficult to forge a conspiracy. Participants also mentioned that new election technologies will not create any added value for them to trust more the election system: *"There's already trust in the electoral system itself, so I'm not sure that there is the need to introduce technology in order to create more trust."*

Others A number of further factors were identified that could not be clearly grouped into technological or institutional trust, although being related to the fac-

tors from these categories. These factors include *Social Trust*, *Vendor Involvement*, *Historical Trust*.

Social Trust Social trust examines how trust within Danish society influences voter's trust in election technologies. A few participants (3 out of 14) mentioned that the general trust in the society can play an important part in influencing the use of election technologies. Participants emphasized that without this general trust it will be difficult to adopt election technologies: *" So if there is general trust in society, then there is likelihood that I will trust, but if there is mistrust in the society, then there's the likelihood that I will also mistrust whatever outcome."* This general trust in the society also gives the confidence to the voters that in case of any mishandling on the part of election authorities – it will be reported: *"I have confidence in that if there is anything Wrong, someone will lift the finger and say hey, we have to look at this So that gives me a high degree of trust."*

Vendor Involvement The vendor involvement in implementing election technologies emerged as a significant theme during the interviews as some participants (5 out of 14) mentioned the need of secure technology as the key for executing fair elections. It became evident from the interviews that the voters distrust the vendors of election technologies. Participants believe that the security of the election technologies may get compromised if there is an involvement of vendors in developing, executing and managing these technologies. They emphasized on the need of developing technology internally to avoid potential security issues and data-breaches since election is a high-stake event: *" if you're designing own systems from scratch, you are not in trouble. If you are like allowing a private entity to, to control the information. Okay. That's problematic."* Participants also expressed that the vendors are just eager to sell the technology and don't do enough due-diligence when it comes to developing secure technologies. They also have a skepticism that the vendors could potentially sell the confidential information to the third-parties: *"You know the vendors and the kind of details they have about me. What they are going to use it for. It will be a kind of a worry to me."* A few participants (2 out of 14) also emphasized that vendors pedigree impacts their trust in election technologies. They articulated that it is important for them to know the vendor's affiliation with and reputation in Denmark: *"if I know that it is a Danish company, then I will assume that the kind of trustworthy that we have in this society would be translated into the voting and for that I'm secured."* A few participants (2 out of 14) mentioned that the affiliation of vendors with the Nation State could lead to privacy risk and manipulated election results. Therefore, it is important for them to know the vendor's intent so that the trust in their proposed technology can be established: *"you can't tell me that, OK, the company behind these technologies, coming from, let me see Russia or China right that has some kind of issues with privacy and also trustworthy instantly. I will not feel secured because I know my data will be used for other purpose or maybe they might even manipulate results."*

Historical Trust Our analysis revealed that participants have made a deep connection with the paper-based voting system and have complete trust in it. Some participants (4 out of 14) mentioned that since the paper-based system works well, there is no need to use election technologies. They prefer using the paper-based voting system as they find it less risky and more reliable: *"'cause I'm like what is wrong with the [paper based] system as... I don't see the current election process as broken. So I'm like what is it that needs fixing?"*

5 Discussion and Conclusion

Our findings confirm the importance of trust regarding voters' acceptance of election technologies, in particular when related to perceived security. The study's participants were aware of threats related to the use of technology in elections, and perceived these to be higher when compared to the paper-based systems. Predominantly participants mentioned general concerns, but only few specific to election technologies, namely election manipulation and denial of service attacks. Other threats, such as violation of vote secrecy, voter coercion, and vote buying were not mentioned. This shows either participants' lack of awareness or lack of concerns towards these threats.

Factors identified in our study, especially those relating to trust in technology, point to potential measures that can be taken to increase voters' trust in a specific election or a specific voting system. For instance, our participants point to the need of verifying the election result, confirming the need to use end-to-end verifiability (as opposed to black box systems) commonly pointed to also by experts [34]. Verifiability, in addition to providing a layer of security assurance regarding election integrity, can also serve as means for engaging the voter. It enables voters to experience security-related aspects of the system, and makes the system potentially more transparent. These and other measures of involving the voter can be used to enhance *transparency* of election technologies, which was another issue commonly mentioned by our participants. Indeed, ensuring transparency when using technology in elections is a known challenge, which has also been at the core of the German Constitutional Court decision regarding the use of electronic voting machines [12]. Effective ways to ensure transparency as a way to establish trust remain an open question, especially in light of studies showing that providing too much information about the technology without properly contextualising it might even lead to decreased confidence in the election integrity [6]. A significant role in ensuring some degree of transparency – assuming that lay voters do not have the expertise necessary to understand the details of how election technologies work – lies within security assurances presented by trusted entities, such as election authorities, representatives from opposing parties or independent experts.

With respect to various stakeholders involved in the election, our participants expressed high trust regarding the integrity of election officials. However, some doubted their expertise in implementing and administrating election technologies. Such, seemingly conflicting views point to the manifold nature of trust, in

particular, to both perceived integrity/benevolence and perceived competence being crucial to trusting intention [21]. While perceived integrity depends strongly on the general level of trust in society, competences of election authorities can be improved with corresponding training and/or by involving experts as consultants. The introduction and use of such measures should be communicated to the voters in a transparent manner. Our participants were less convinced of the trustworthiness of vendors who implement election technologies, doubting their commitment to the security of their products. Similar scepticism towards the intentions of private companies to ensure sufficient security and privacy protection has also been shown in other domains [15,16], thereby emphasising the importance of independent institutes (e.g. media reporting), appropriate legislation, and independent audits for security-critical systems. Transparent processes when procuring election technologies, including proper vetting and oversight over vendors, is therefore crucial.

When talking about election technologies, our participants mainly talked about Internet voting, which might be due to lower awareness about other technologies that are or can be used in the electoral process. Therefore, it remains an open question to which extent identified factors that influence trust in Internet voting are relevant to other kinds of election technologies, such as party endorsement system, electronic voter register or software used for tallying cast votes. While some of these factors are likely to be transferred directly, such as trust in government, other might require a more nuanced approach. In particular, applications of verifiability techniques to processes such as endorsing a party to be eligible for being elected can be relevant, especially in light of identified attacks on such processes in Denmark [30]. Studying such techniques as well as voters' attitudes towards them can be a worthwhile direction of future work.

A number of factors identified in our study were not connected to a specific technology or voting system. These factors pointed at the attitudes towards institutions and society as a whole, confirming findings by previous works [1,19]. This means that improving technology can only solve the problem of citizens' trust to a limited extent. Essentially, unless there is already a high level of social trust and trust in the governmental institutes, it is likely that the use of technology will fail.

Future Work We consider following directions to be particularly interesting for future research. As our study focused on the voters in Denmark, similar studies in other countries – especially countries characterised either by lower levels of social trust or more extensive use of election technologies compared to Denmark – would help to better understand how voters' trust is established and maintained. While our study was qualitative and served an exploratory purpose, further quantitative, large-scale evaluations can be used to validate and to elaborate our findings. Finally, ways to engage voters and other stakeholders in trust-building measures – including but not limited to the development and evaluation of usable verifiability measures, awareness materials and explanations of the security guarantees that election technologies provide – should be investigated.

Acknowledgements This work was supported by a research grant (40948) from VILLUM FONDEN.

References

1. Alharbi, A., Kang, K., Hawryszkiewycz, I.: The influence of trust and subjective norms on citizens' intentions to engage in E-participation on E-government websites. ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems (2015)
2. Alharbi, N., Papadaki, M., Dowland, P.: The impact of security and its antecedents in behaviour intention of using e-government services. Behaviour and Information Technology **36**(6), 620–636 (2017). https://doi.org/10.1080/0144929X.2016.1269198
3. Aranyossy, M.: Citizen adoption of e-government services-evidence from hungary. In: Bled eConference. p. 39 (2018)
4. Boddy, C.R.: Sample size for qualitative research. Qualitative Market Research: An International Journal (2016)
5. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology (2006). https://doi.org/10.1191/1478088706qp063oa
6. Dalela, A., Kulyk, O., Schürmann, C.: Voter perceptions of trust in risk-limiting audits. E-Vote-ID 2021 p. 335 (2021)
7. Ehin, P., Solvak, M.: Party cues and trust in remote internet voting: Data from estonia 2005–2019. In: International Joint Conference on Electronic Voting. pp. 75–90. Springer (2021)
8. Faraon, M., Stenberg, G., Budurushi, J., Kaipainen, M.: Positive but skeptical: A study of attitudes towards internet voting in sweden. In: CeDEM Asia 2014: International Conference for E-Democracy and Open Government, Hong Kong, December 4-6, 2014. pp. 191–205 (2015)
9. Filieri, R., Alguezaui, S., McLeay, F.: Why do travelers trust TripAdvisor? Antecedents of trust towards consumer-generated media and its influence on recommendation adoption and word of mouth. Tourism Management **51**, 174–185 (2015). https://doi.org/10.1016/j.tourman.2015.05.007
10. Folketinget: Technical dialogue on system for e-voting in denmark-summary report (1 2013), https://www.ft.dk/samling/20121/lovforslag/l132/bilag/1/1209863.pdf
11. Furner, C.P., Drake, J.R., Zinko, R., Kisling, E.: Online Review Antecedents of Trust, Purchase, and Recommendation Intention: A Simulation-Based Experiment for Hotels and AirBnBs. Journal of Internet Commerce **21**(1), 79–103 (2022). https://doi.org/10.1080/15332861.2020.1870342
12. German Federal Constitutional Court: Decisions: Order of 03 march 2009 - 2 bvc 3/07 (2009)
13. Gulati, S., Sousa, S., Lamas, D.: Modelling trust: An empirical assessment. In: IFIP Conference on Human-Computer Interaction. pp. 40–61. Springer (2017)
14. Hoffman, H., Söllner, M.: Incorporating behavioral trust theory into system development for ubiquitous applications. Personal and ubiquitous computing **18**(1), 117–128 (2014)
15. Kulyk, O., Milanovic, K., Pitt, J.: Does my smart device provider care about my privacy? investigating trust factors and user attitudes in iot systems. In: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. pp. 1–12 (2020)

16. Kulyk, O., Renaud, K.: "i need to know i'm safe and protected and will check": Users want cues to signal data custodians' trustworthiness. In: 2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW). pp. 171–178. IEEE (2021)
17. Kulyk, O., Volkamer, M., Fuhrberg, N., Berens, B., Krimmer, R.: German voters' attitudes towards voting online with a verifiable system. In: Workshop on Advances in Secure Electronic Voting (VOTING), Grenada, February 18, 2022 (2022), 46.23.01; LK 01
18. Lansing, J., Sunyaev, A.: Trust in cloud computing: Conceptual typology and trust-building antecedents. Data Base for Advances in Information Systems **47**(2), 58–96 (2016). https://doi.org/10.1145/2963175.2963179
19. Li, W., Xue, L.: Analyzing the Critical Factors Influencing Post-Use Trust and Its Impact on Citizens' Continuous-Use Intention of E-Government: Evidence from Chinese Municipalities. Sustainability (Basel, Switzerland) **13**(14), 7698 (2021). https://doi.org/10.3390/su13147698
20. Licht, N., Duenas-Cid, D., Krivonosova, I., Krimmer, R.: To i-vote or not to i-vote: Drivers and barriers to the implementation of internet voting. In: International Joint Conference on Electronic Voting. pp. 91–105. Springer (2021)
21. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. The Academy of Management Review (1995). https://doi.org/10.2307/258792
22. Nemeslaki, A., Aranyossy, M., Sasvári, P.: Could on-line voting boost desire to vote?–technology acceptance perceptions of young hungarian citizens. Government Information Quarterly **33**(4), 705–714 (2016)
23. Nielsen, J.H., Lindvall, J.: Trust in government in sweden and denmark during the covid-19 epidemic. West European Politics **44**(5-6), 1180–1204 (2021)
24. Nissenbaum, H.: Will security enhance trust online, or supplant it? Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions, Eds. R. Kramer and K. Cook, Russell Sage Publications (2004) pp. 155–188 (2004)
25. OSCE: Denmark, general elections, 5 june 2019: Needs assessment mission report (6 2019), $https://www.osce.org/files/f/documents/4/d/419231_0.pdf$
26. Plano Clark, V.L., Creswell, J.W.: Understanding research: A consumer's guide (2015)
27. Ranaweera, H.M.B.P.: Perspective of trust towards e-government initiatives in Sri Lanka. SpringerPlus **5**(1), 22 (2016). https://doi.org/10.1186/s40064-015-1650-y
28. Roberts, P., Priest, H.: Reliability and validity in research. (2006). https://doi.org/10.7748/ns2006.07.20.44.41.c6560
29. Saunders, M., Lewis, P., Thornhill, A.: Research methods for business students. Pearson education (2009)
30. Schürmann, C., Bruni, A.: Technical and socio-technical attacks on the danish party endorsement system. In: International Joint Conference on Electronic Voting. pp. 200–215. Springer (2019)
31. Shao, Z., Zhang, L., Li, X., Guo, Y.: Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. Electronic Commerce Research and Applications **33**(August 2018), 100823 (2019). https://doi.org/10.1016/j.elerap.2018.100823, https://doi.org/10.1016/j.elerap.2018.100823
32. Shi, S., Gong, Y., Gursoy, D.: Antecedents of Trust and Adoption Intention toward Artificially Intelligent Recommendation Systems in Travel Plan-

ning: A Heuristic–Systematic Model. Journal of Travel Research **60**(8), 1714–1734 (2021). https://doi.org/10.1177/0047287520966395, https://doi.org/10.1177/0047287520966395
33. Svendsen, G.L.H., Svendsen, G.T., Graeff, P.: Explaining the emergence of social trust: Denmark and germany. Historical Social Research/Historische Sozialforschung pp. 351–367 (2012)
34. Volkamer, M., Spycher, O., Dubuis, E.: Measures to establish trust in internet voting. In: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance. pp. 1–10 (2011)
35. Wang, S.W., Ngamsiriudom, W., Hsieh, C.H.: Trust disposition, trust antecedents, trust, and behavioral intention. Service Industries Journal **35**(10), 555–572 (2015). https://doi.org/10.1080/02642069.2015.1047827
36. Yasuoka, M., Meyerhoff Nielsen, M., Iversen, K.E.: The exercise of mandate–how mandatory service implementation promoted the use of e-government services in denmark. In: Proceedings of the 55th Hawaii International Conference on System Sciences (2022)
37. Zada, P., Falzon, G., Kwan, P.: Perceptions of the australian public towards mobile internet e-voting: risks, choice and trust. Electronic Journal of e-Government **14**(1), pp117–134 (2016)
38. Zhu, Y.Q., Azizah, A.H., Hsiao, B.: Examining multi-dimensional trust of technology in citizens' adoption of e-voting in developing countries. Information Development **37**(2), 193–208 (2021). https://doi.org/10.1177/0266666920902819
39. Zhu, Y.Q., Azizah, A.H., Hsiao, B.: Examining multi-dimensional trust of technology in citizens' adoption of e-voting in developing countries. Information Development **37**(2), 193–208 (2021)

End-to-end verifiable voting for developing countries - what's hard in Lausanne is harder still in Lahore

Hina Binte Haq[1,2], Syed Taha Ali[2], and Ronan McDermott[3]

[1] National University of Computer and Emerging Sciences, Islamabad, Pakistan.
hina.haq@nu.edu.pk
[2] School of Electrical Engineering and Computer Sciences (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan.
taha.ali@seecs.edu.pk
[3] MCDIS ronan@mcdis

Abstract. In recent years end-to-end verifiable voting (E2EVV) has emerged as a promising new paradigm to conduct evidence-based elections. However, E2EVV systems thus far have primarily been designed for the developed world and the fundamental assumptions underlying the design of these systems do not readily translate to the developing world, and may even act as potential barriers to adoption of these systems. This is unfortunate because developing countries account for 80% of the global population, and given their economic and socio-political dilemmas and their track record of contentious elections, these countries arguably stand to benefit most from this exciting new paradigm. In this paper, we highlight various limitations and challenges in adapting E2EVV systems to these environments, broadly classed across social, political, technical, operational, and human dimensions. We articulate corresponding research questions and identify significant literature gaps in these categories. We also suggest relevant strategies to aid researchers, practitioners, and policymakers in visualizing and exploring solutions that align with the context and unique ground realities in these environments. Our goal is to outline a broader research agenda for the community to successfully adapt E2EVV voting systems to developing countries.

Keywords: end-to-end verifiable voting · developing countries

1 Introduction

In recent years end-to-end verifiable voting (E2EVV) has emerged as a revolutionary new paradigm to enable secure and transparent elections [8]. E2EVV voting systems preclude implicit trust in administrators, polling staff, and voting machines, and instead make voters themselves active participants in auditing the election and certifying its results - "the Holy Grail for electronic voting" [82]. These systems are backed by expert bodies [55] and have been piloted in numerous small-scale mock elections and pilots [37] [89] [76], some large-scale politically

binding elections - Australia in 2016 [18] and, most notably, nationwide deployment in the Estonian parliamentary elections in 2019 [30]. This technology is also on the cusp of commercialization[17].

As these systems transition to the mainstream, we consider it an opportune moment to revisit gaps in the research literature, particularly with regards to deploying these systems in developing countries - environments which would arguably benefit most from the superior integrity and trust guarantees offered by these systems. E2EVV systems thus far have primarily been designed for the developed world, where it is largely assumed that there is a sufficient infrastructure for elections, voters are largely literate and relatively technically sophisticated, and dispute resolution mechanisms are reliable and effective. These assumptions do not necessarily translate to the developing world and may even act as potential barriers to adoption of E2EVV systems in these countries.

To motivate this study, we consider the fact that the overwhelming majority of the global population - approximately 80% - hails from the developing world [87]. Distrust in democracy and electoral processes runs high in many of these countries [56], and election fraud has resulted in mass protests [48], political deadlock [75], and violence [35]. Some of these countries have introduced electronic voting systems, and, in several, results have proved controversial [22].

We believe that E2EVV systems, with their potential to restore trust and confidence in electoral processes, have a vital role to play in the developing world. In recent years there have even been public calls to explore application of this technology in countries including Brazil [10], Pakistan [40] and India [19].
In this paper, we make the following contributions:

- We contend that certain fundamental assumptions implicit in the design of E2EVV systems developed thus far conflict with ground realities in developing countries. To make these assumptions explicit, we highlight the manifold challenges in adapting E2EVV systems to these environments.
- This reorientation opens up significant new ground. We identify various social, political, technical, operational, and human concerns specific to E2EVV systems in developing countries and frame specific research questions.
- We suggest potential strategies for the way forward based on relevant trends and success stories in developing countries as well as re-purposing solutions from research literature. Our goal is to aid the community to devise solutions that are appropriate to the unique ground realities of the developing world.

There is a considerable body of research on the challenges of deploying election technology in the developing world [38] [5]. To the best of our knowledge, we are the first to focus specifically on adapting *E2EVV systems* to the sociopolitical realities and infrastructure in these countries. One of our primary contributions is a detailed review of the literature, election experiences, and news reports from the developing world.

We believe this is a critical research gap, addressing which requires close collaboration between researchers, technologists, practitioners, and policymakers. We hope our paper stimulates exciting and impactful new thinking and research and extends the benefits of E2EVV voting systems to the developing world.

2 Background and Prior Work

In this section, we briefly describe E2EVV voting systems, we motivate the case for their application in the developing world, and we discuss prior work.

2.1 End-to-End Verifiable Voting Systems

E2EVV systems are a promising new class of voting systems which offer voters the benefits of automation, ease of vote-casting and quick reporting of results, along with stringent cryptographic guarantees of voter privacy and correct computation of the tally. Numerous such systems have been proposed over the years for precinct-based and Internet voting [8]. We summarize next the high-level workings of a representative system to convey to the reader a non-technical and intuitive understanding of end-to-end verifiable voting.

On the day of elections, our citizen, say Alice, arrives at a polling station and identifies herself as an eligible voter. She makes her candidate choice on a voting terminal. The machine records and encrypts her vote and issues her a **printed receipt**, bearing a unique serial number and a cryptographic commitment to her vote. This receipt allows her to later verify that her vote has been correctly processed and counted. However, the receipt does not reveal Alice's choice of candidate and she cannot use it to sell her vote.

However, Alice may suspect the machine is malfunctioning or has been tampered with. In this case, she avails an option to force the machine to reveal the cryptographic parameters it used to encrypt her vote. This step effectively 'spoils' her ballot but allows her to double-check that the machine is operating correctly. She can repeat this step several times until she is ready to cast her vote. In the parlance of E2EVV systems, Alice is now confident that **her vote has been cast as intended**.

When polls close, election staff post copies of all receipts online. Alice uses the serial number to navigate to her receipt. If anyone has tampered with her vote, she can detect it by comparing the receipt to the physical copy she holds in her hand, and can file a complaint using her physical receipt as hard evidence. This gives her confidence that **her vote has been recorded as cast**.

E2EVV systems usually employ two key techniques to tally results in a privacy-preserving manner: systems such as Prêt á Voter [71] and Scantegrity [21] rely on mixnets to anonymize and decrypt cast votes which are then added. The other approach, exemplified by STAR-Vote [13], employs homomorphic encryption to aggregate encrypted votes and decrypt only the tally. Both processes offer voters and observers cryptographic proofs of correct operation. Alice can use these proofs to verify that **her vote has been tallied as recorded**.

These three guarantees span all critical steps of the election life-cycle, and empower users to verify the integrity of the process for themselves. By empowering voters to verify the integrity of the process themselves, E2EVV represents a dramatic improvement over traditional 'black box' voting machines.

Because of space constraints, we have eschewed technical details and refer the reader to [8] for the same.

2.2 Prior Work

There is little work specifically on E2EVV systems and the developing world. Exceptions include E2EVV systems Threeballot, Twin [73] and Aperio [29], which are geared to provide verifiability in "minimally equipped election environments". These systems are of considerable interest due to their novel paper-based design which precludes any use of technology or cryptography. Unfortunately there has been no effort to adapt or pilot these systems in a developing country. Moreover, they lack the highly desirable benefits of automation such as less spoiled votes, prompt reporting of results, and enfranchisement of marginal communities [79].

There is, however, a considerable body of research on the application and challenges of electronic voting in the developing world which is relevant to our purposes. This includes feasibility studies [51], holistic frameworks [63], cost benefit analyses [58], and adoption studies [9] [5]. Some studies focus on specific topics, such as economic determinants of voter behaviour [57] or technical concerns [7]. There are case studies on e-voting in individual countries [10] [42], and efforts to adapt insightful metrics, such as the E-Voting Readiness Index [50].

This literature contains several findings, which generalize to E2EVV systems and which, as we noted earlier, clash directly with the ground realities in technologically advanced countries. For instance, in the developing world resources and infrastructure for elections is commonly inadequate [51] [63] and countries often face severe financial constraints [10] [51] [58]. Governments may also lack technical, administrative, and operational capacity to conduct elections [51] [10]. Election management bodies often face issues of autonomy [72] [6]. The political environment may be volatile which affects conduct of elections [58]. Corruption and election fraud are systemic and transparency and accountability are lacking [57] [58] [10]. Voters may be suspicious of election technology and acceptance and adoption can be problematic [9] [5] [20].

Any effort to introduce E2EVV systems has to engage with these fundamental ground realities. We explore these themes in more detail in the following sections.

3 Motivation

The vast majority of the world's population, a staggering 80%, live in the developing world [87], covering the landmass of Africa, Latin America, and much of the Middle East and Asia. These include six of the world's ten most populous countries, namely India, Indonesia, Pakistan, Brazil, Nigeria and Bangladesh [87]. Despite significant variance in size, demography, history, and culture, many of these countries face similar economic and socio-political problems: widespread poverty and inequality, low literacy, poor governance, systemic corruption, and dependence on foreign institutions [86]. Elections are routinely contentious and frequently result in political deadlock, street protests, and violence [56].

For instance, in Pakistan, major rigging allegations in the general elections of 2013 resulted in mass protests and a public sit-in by a major opposition party [68]. Likewise, in 2014, the Bangladesh saw a national strike lasting 85 days

and a violent crackdown on opposition workers. Opposition parties boycotted the election and over half the seats went uncontested [75]. Opposition boycotts, street protests, and civil unrest, also featured recently in Venezuela [44].

Perceptions of rigging can also trigger major political disruptions and take on life-threatening consequences. Allegations of "terrible fraud" were a key justification for the recent military coup in Myanmar, where army officials claim to have identified some 10.5 million irregularities in the voter list used in the last general elections [35]. The violence following the coup resulted in over 700 deaths and more than 3,300 people detained.

Technology has often been introduced, with mixed results, to resolve this issue of trust. Reported improvements in India include a significant decline in electoral fraud, a more competitive electoral process, and increased participation of marginalized groups in society [79]. Automated counting in Philippines corresponded with dramatic reduction in result compilation time. [78].

However, there are frequent discrepancies and irregularities which undermine trust in technology. In 2017, the Supreme Court of Kenya nullified election results citing irregularities in the results transmission system [16]. In Pakistan, in 2018 the results transmission system broke down inexplicably on the night of elections, raising extreme suspicion [84]. In Azerbaijan, introduction of a smartphone app in 2013 to report election results backfired when it released the election results the day before the actual election [14]. In India, numerous incidents were reported in different polls where electronic voting machines 'malfunctioned' by recording all votes in favour of the ruling party, no matter which choice the voter made [26]. In 2018, the introduction of untested voting machines in Democratic Republic of Congo was strongly opposed by opposition parties, and thousands of machines were subsequently destroyed in an act of arson [64].

Researchers have sought to explain these "unintended consequences" of election technology in terms of a "fetishization of technology" [22], or a silver bullet [27], which distracts stakeholders from rigorous assessments and stringent checks and balances in the overall ecosystem. This lack of attention can render election processes even more vulnerable than before.

To situate the potential contribution of E2EVV systems, it is helpful to differentiate between electoral efficiency and transparency as two desirable yet distinct outcomes of using election technology [88]. Unfortunately, there is a marked tendency to prioritize efficiency over transparency, and favor a "black box" approach which concentrates trust "away from the many" and into the "hands of the few". We anticipate that E2EVV systems - by incorporating security and integrity as core design features of the system - can help redress this balance between electoral efficiency and public transparency.

Similar sentiments have recently been voiced in the developing world, namely Brazil [10], Pakistan [43] [39], and India [19], where security professionals, researchers, and civil society organizations have urged election authorities to explore the adoption of E2EVV systems to restore credibility of electoral processes. Indeed, very recently in India, some 11 opposition parties unanimously passed

resolutions affirming that the existing EVMs do not comply with "democracy" principles in that his or her vote is not verifiable [1].

4 East is East and West is West: Misplaced Assumptions, Knowledge Gaps, and Other Challenges

As we noted earlier, the design of most E2EVV systems is based on implicit assumptions which hold true for technologically advanced countries and do not necessarily translate easily to developing regions. A key goal in this section is to make these assumptions explicit by describing the challenges and knowledge gaps relevant to these environments. We divide these into four categories: structural constraints, social and political factors, human factors, and technical and operational concerns. We also include issues which are generic to adapting election technology and are well studied, but which may become more pronounced or take on added dimensions for the case of E2EVV systems.

4.1 Structural Constraints

Shoestring Budgets: Developing countries routinely suffer from severe financial constraints, and, due to large populations, election funding can take on disproportionate dimensions compared to other government priorities, such as poverty alleviation, and healthcare. For instance in 2018 general elections in Pakistan cost 21 billion PKR (175 million USD) [45], comparable to the annual allocation for healthcare at 25 billion PKR (208 million USD) and almost quarter the education spending at 97 billion PKR (808 million USD) [33].

Expensive technology interventions further strain these shoestring budgets. For instance, upgrading voting machines with paper trails in the Indian context cost 32 billion INR (492 million USD) [41]. Nationwide deployment of electronic voting machines in Pakistan are estimated to cost 350 billion PKR (2 billion USD), almost three quarters the national GDP [2]. These realities can foster undesirable trends: to quote the UN Secretary General, "techniques and systems that might cause a State, in the conduct of its own elections, to be financially dependent on donors" [22].

There is therefore a pronounced need to develop compact and minimalist E2EVV systems in a low-cost, sustainable manner, along the lines of India's famous voting machines. Perhaps, existing minimal FPGA-based E2EVV solutions like VoteBox Nano could be adapted for these settings [59]. A modular design approach would further maximize options to recycle components.

The research community can contribute with open-source tools, software packages, libraries, kits, or hardware platforms to facilitate the development of such projects, similar to the ElectionGuard [17] effort or the wide availability of blockchain platforms like Hyperledger or Ethereum.

Another promising direction is to develop E2EVV solutions which integrate with existing voting systems in developing countries. This is the design approach behind Scantegrity [76]. Recently, Mohanti et al. adapted risk limiting audits for

Indian voting machines [52]. **Is it possible to upgrade Indian or Brazilian machines in a similar cost-effective manner for verifiability?**

Resource and Infrastructure Woes: Developing countries frequently suffer from resource shortages, including lack of essential equipment, IT systems, labs and storage facilities. Infrastructure problems include lack of utilities especially electricity, telecommunications, and Internet service. Expertise issues include poor access to IT expertise, quality technical support, and shortage of qualified polling staff. There is a dire need for indigenous capacity building and reforms for restructuring of broader management structures.

However there is encouraging evidence that technology can be creatively deployed within these constraints. India and Brazil's homegrown electronic voting machines are largely considered a success story. The under-banked in sub-Saharan Africa bypassed traditional banking and leap-frogged onto mobile money, accounting for 70% of the global 1 trillion USD mobile money market [62]. Alternatives need to be researched in response to specific challenges encountered in each country.

To consider how infrastructure issues relate to E2EVV systems, we consider the specific example of the online bulletin board requirement. Whereas Internet access is ubiquitous in the developed world, in developing countries basic cell phone coverage and Internet access can be limited and unreliable due to network faults or traffic congestion. Our question becomes: **what kind of public bulletin board for vote verification could we offer in Asia and Africa where cell phone coverage is unreliable and an estimated 1.3 billion people still use dumb phones [23]?**

The popularity of text-messaging services (like SMS) may offer a way forward. These services have been successfully used in phone-based financial services, voter registration drives, social security programs, and mass vaccination efforts. Researchers have proposed SMS-based primitives including one time pads, return codes and transaction authentication numbers to harden remote voting systems [12] which may potentially be leveraged for a bulletin board service over SMS.

Infrastructure constraints may also be leveraged by malicious actors (e.g. a spoofing attack which misdirects voters to a fake bulletin board [81]).

4.2 Social and Political Factors

Electoral Fraud is Systemic: It is well documented that developing countries often suffer from poor governance and endemic corruption [61], trends which also manifest in electoral practices. Vote buying, coercion, and suppression are commonplace: the 2013 Afrobarometer survey noted that 48 percent of voters in 33 African countries reported fearing violence during elections, whereas 16 percent reported being offered cash or goods for their vote. In Pakistan, in 2013, a watchdog body reported electoral irregularities at over 21,000 polling stations [31]. In 2017, the Supreme Court of Kenya nullified election results citing irregularities in the results received over the results transmission system [16]. In 2017, in Venezuela, vendor Smartmatic disclosed that general results were "manipulated" and off by a count of at least 1 million [32].

Persistent and systemic security threats in these environments necessitate additional security measures. **But what about attack scenarios caused by deploying E2EVV technology?** Poll workers can collect discarded receipts, voters may sell their receipts or surrender them on intimidation. Malicious parties could then manipulate the corresponding votes without fear of detection.

A potential countermeasure is a verifiable encrypted paper audit trail (VEPAT) which incorporates additional checks performed by independent auditing authorities [69]. These bodies could routinely verify the correspondence between the audit trail and receipts posted on the bulletin board. Solutions allowing voters to delegate the verification process to a trusted party [77] also merit investigation.

Another relevant concern: **how would E2EVV systems fare in environments where polling day security is lax and family voting, impersonation, and collusion are common?** These trends are well-documented in developing countries: a patriarch or another party obtains credentials of multiple legitimate voters and then casts votes on their behalf. Poll workers can cast votes on behalf of absentee voters. It is not surprising that the earliest election technology systems implemented in countries like Ghana, Nigeria, Kenya, DRC, Somaliland, Afghanistan are biometric voter verification systems. Following up on this, **can we integrate biometric checks with E2EVV systems in a binding way to provide enhanced security guarantees of voter identification, presence, and eligibility verifiability? Could these be done in a way that is universally verifiable?**

The Politics of Perfection: There is often lack of debate and rigorous analysis of election technology in developing countries. The Venezuelan government has described its electronic voting system as "the most perfect voting system in the world"[49]. The Indian Election Commission reacted angrily to reasonable security analysis of its voting machines [67]. **Can developing countries who see their particular EVM systems as already "perfect" even begin to accept the need to evolve towards evidence-based elections and E2EVV systems? What kind of outreach effort would this entail?**

4.3 Human Factors

Linguistic and Cultural Diversity Developing countries, marked by their linguistic diversity (dialects may change every few miles) ethnic diversity and varying cultural constructs [85], require localization of both the voting system and accompanying receipts and verification mechanisms, which adds complexity to processes. People are often hesitant to carry out important transactions, especially ones involving finances in an unfamiliar language. Language can potentially act as a barrier to election participation and disenfranchise certain voters [66]. **Can E2EVV systems cope with the sheer scope and scale of linguistic localization needed for many developing countries?**

What about Mental Models? Mental models are essential to help foster public understanding of novel technology and customize interventions. Most voters think about a voting system first and foremost in terms of how to vote [4]. Mental models for technology as well as attitudes and perceptions have been known

to vary considerably in developing countries for certain applications [36]. **What would mental models for E2EVV systems look like for voters in developing countries? How would these models vary, given the wide-ranging social and cultural diversity in these regions?**

Usability - the highest hurdle? Research points to correlation between low literacy (including digital literacy) and rejected ballots [34]. Extending usability recommendations (for low-literacy voters in traditional electronic voting) to the E2EVV scenario is not trivial. A preliminary study involving Helios, Pret-a-Voter, and Scantegrity II found that it took almost twice as long to cast a vote, a significant number of voters failed to cast votes, and many did not realize their errors [3]. Voting success rates in developing countries will likely be lower. **How will this play out in developing countries with massive populations and already long queues, where voter or poll workers have been known to die of exhaustion [80]. Can E2EVV systems be designed to emphasize usability in low-literacy contexts?**?

Moreover, recent testing and 'live' applications of E2E systems have resulted not just in consistently low rates of voter verification but even lower rates for those who actually report discrepancies [53]. Chipcase [24] observe that non-literate populations avoid complex functions and this reinforces the assumption that if a step is optional, it will be skipped [28].

Can we develop technical solutions to simplify or automate the vote verification process in the context of developing countries? Researchers have proposed solutions to make verifiability universal [54] [70], delegate it, or enable mass verification by bundling multiple receipts for batch verification [15]. Could these be made more usable and practical for low-literacy users? Perhaps we could leverage research on textual key-fingerprint representations [25] and hash visualization [11] for this purpose. Research also shows that motivating messages can persuade voters to verify [60]. **What sort of nudges or incentives could we devise to encourage voter verification in developing countries?**

4.4 Governance and Operational Factors

E-Governance and Digital Transformation:

Developing countries often lack overarching institutional frameworks for governance, suffer from fragmentation and poor coordination of processes, and low uptake of digital technology. In the context of E2EVV systems, this can manifest in multiple ways. We consider the simple example of effective management of cryptographic credentials, recognized as problematic in trials of E2EVV systems. Logically, this problem will be more pronounced in developing countries.

Moreover, end-to-end verifiability and voter privacy are sensitive to human behaviour in the protocol. Errors in use of cryptography could result in exposure of critical data and undermine the integrity of the whole process. It would be helpful to characterize the set of behaviours under which security can be preserved and also higlight explicit scenarios where it fails [46]. **How can we customize the key management and ceremonies to ensure separation of duties and principles of least privilege?**

Cybersecurity - Canaries in the Coalmine? Developing countries lag far behind in terms of capacities and resources for cybersecurity. For E2EVV, therefore, vulnerabilities such as DDoS attacks on bulletin boards become more likely. Attacks on electoral information systems are on the increase and are often conducted by external or state actors with significant resources. The design of E2EVV systems must take this into account. **Can E2EVV systems be designed to be more "tamper-proof" (to use the infosec term) as well as "tamper-evident" (the elections term)?**

Legal Framework In case of E2EVV systems, it should be legally binding on election management bodies (EMBs) to issue a receipt to every voter, upload all the receipts on a bulletin board within a stipulated time frame, verifying the results through the software provided to observers, making the software open source, sharing of public cryptographic parameters, conduct of Risk Limiting Audits. without which the security guarantees of E2EVV systems become moot.

As noted in the Brazil experience, "important judicial decisions are not based on scientific research; they are often based on the personal opinions of judges who have no understanding of (election) technology.[10]" Accordingly, for disputes involving technologies, defining the requirements for the admissibility of evidence, training the judiciary to handle the intricacies of E2EVV systems based digital evidence is of utmost importance. Moreover, comprehensive and high quality voter instruction is critical to uptake of a radically new system like E2EVV and typically falls under the auspices of the legal framework ensuring equal access. [8] Transparency and accountability are key to minimizing risk, and risk perception.

Although it is not possible to have a generic, one-size-fits-all set of requirements for E2EVV, we need to avoid the idea that all countries can do completely different things - fundamentally, technical requirements, and regulations, laws, and indeed constitutions, must deliver E2EVV systems that are fully compliant with universal principles.

Toothless or Compromised EMBs and Ineffective Dispute Resolution Many EMBs lack the regulatory teeth and political autonomy needed to ensure that incumbent government and political parties do not interfere in their duties, and they often operate under political influence and fear.[83]. The lack of technical skills means there is unreliable implementation of technical protocols.

In developing countries, disputes over elections results often act as triggers for mass protests, violence, political deadlock and animosity, often times bordering civil war. This situation can be exacerbated when judicial mechanisms cannot resolve these disputes in a timely, fair and transparent manner [56].

Another implicit assumption is that evidence of election malfeasance, if available from an E2EVV system, and provided to the authorities, would facilitate interventions by said authorities. There are various examples of EMBs in developing countries ignoring compelling evidence of electoral malfeasance. Moreover, in developing countries it is not uncommon for electoral processes to be politically controlled and for EMBs to be compromised. For instance, in Mozambique in 2014, the regime turned biometric registration into a technique of manipulation, suppressing registration in opposition areas by provisioning inadequate

equipment and under-trained teams. In Kenya, over a million dead citizens were maintained in the voter register in an attempt to rig the polls [47]. Venezuelan election results were internally 'manipulated' by at least 1 million votes [32].

In such situations, E2EVV systems, with their rigorous security guarantees, may well be perceived as an existential threat. **In this regard, to what degree could E2EVV systems be corrupted in a compromised ecosystem? Moreover, could E2EVV systems possibly be developed to offer guarantees against a compromised ecosystem? Could solutions be developed to render these ecosystem issues transparent as well?**

Electoral Integrity Theatre The security guarantees of E2EVV systems become moot if the verification step is not undertaken, and the system is not auditable. If legislatures in developing countries cannot pass and enforce laws that are sufficiently detailed to address both core and ancillary processes, E2EVV risks becoming nothing more than the electoral equivalent of "security theatre" [74]. To quote Park et al "*Auditability* alone isn't enough", and "must be accompanied by *auditing* to be effective. [65]". **There is therefore a need for public awareness on this issue and devising satisfactory mechanisms, policies, and legislation to enforce electoral integrity checks.**

Belt and Braces E2EVV systems need to be made resilient with backup 'belt and braces' mechanism. For instance, Star-Vote is a system which incorporates Risk Limiting Audits to an E2EVV system. Risk Limiting Audits have even been devised to cater to on-ground realities in India. It is essential to work in close engagement with existing systems on the ground.

5 Conclusion

Despite formidable recent efforts to portray elections management in the United States as dysfunctional and corrupt, the reality in developed countries is of well-resourced EMBs, reliable infrastructure, competent staff, reliable dispute resolution mechanisms, digitally literate voters and empowered civil society and media stakeholders. In contrast, we have outlined systemic problems in most developing countries in most of those aspects. Accordingly, the underlying assumptions of most E2EVV systems mean that implementation of E2EVV in developing countries is an uphill task. Some of the solutions we have discussed thus far even clash with one another. For example, if biometrics need to be introduced to deal with corruption and fraud, that would increase the cost, thereby counteracting efforts to reduce that cost. Significant research with an explicit focus on developing country contexts is needed in order to bridge this gap. Given the potential benefits of E2EVV, we believe this pivot is well justified. We hope our paper is a catalyst in this regard.

Acknowledgement

This research was supported by the 'Research for Social Transformation & Advancement' (RASTA), a Pakistan Institute of Development Economics (PIDE) initiative, through Competitive Grants Programme Award [Grant No. CGP-01-127/2021].

Bibliography

[1] Will Fight Against Voting Machine "Misuse", Say 11 Opposition Parties (Sept 2022), https://www.ndtv.com/india-news/will-fight-against-electronic-voting-machine-evm-misuse-say-11-opposition-parties-3252460

[2] Abbasi, A.: EVM-based general polls may cost up to Rs 350 bn. The News International (Dec 2021), https://www.thenews.com.pk/print/920735-evm-based-general-polls-may-cost-up-to-rs350-bn

[3] 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}. In: 2014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 14) (2014)

[4] Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: Users' mental models for three end-to-end voting systems: Helios, prêt à Voter, and Scantegrity ii. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. pp. 463–474. Springer (2015)

[5] Agbesi, S.: Adoption of e-voting system to enhance the electoral process in developing countries. In: Evaluating Media Richness in Organizational Learning, pp. 262–273. IGI global (2018)

[6] Ahmad, S., Abdullah, S., Arshad, R.B.: Issues and challenges of transition to e-voting technology in Nigeria. Public Policy and Administration Research **5**(4), 95–102 (2015)

[7] Akinyokun, O.N.: Secure voter authentication for poll-site elections in developing countries. Ph.D. thesis, University of Melbourne (2020)

[8] Ali, S.T., Murray, J.: An overview of end-to-end verifiable voting systems. Real-world electronic voting: Design, analysis and deployment **173** (2016)

[9] Alomari, M.K.: E-voting adoption in a developing country. Transforming Government: People, Process and Policy (2016)

[10] Aranha, D.F., van de Graaf, J.: The good, the bad, and the ugly: two decades of e-voting in Brazil. IEEE Security & Privacy **16**(6), 22–30 (2018)

[11] Azimpourkivi, M., Topkara, U., Carbunar, B.: Human distinguishable visual key fingerprints. In: 29th {USENIX} Security Symposium ({USENIX} Security 20). pp. 2237–2254 (2020)

[12] Backes, M., Gagné, M., Skoruppa, M.: Using mobile device communication to strengthen e-voting protocols. In: Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society. pp. 237–242 (2013)

[13] Bell, S., Benaloh, J., Byrne, M.D., DeBeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P.B., Wallach, D.S., et al.: Star-vote: A secure, transparent, auditable, and reliable voting system. In: 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13) (2013)

[14] Bigg, C., Dilaverli, K.: Official App Releases Azerbaijani Vote Results – A Day Early. Radio Free Europe (Oct 2013), https://www.rferl.org/a/azerbaijan-election-app-results/25131902.html

[15] Bohli, J.M., Henrich, C., Kempka, C., Muller-Quade, J., Rohrich, S.: Enhancing electronic voting machines on the example of bingo voting. IEEE Transactions on Information Forensics and Security **4**(4), 745–750 (2009)

[16] Burke, J.: Kenyan election annulled after result called before votes counted, says court. the Guardian (Sep 2017), https://www.theguardian.com/world/2017/sep/20/kenyan-election-rerun-not-transparent-supreme-court
[17] Burt, T.: New cyberthreats require new ways to protect democracy - Microsoft On The Issues (July 2019), https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy
[18] Burton, C., Culnane, C., Schneider, S.: vvote: Verifiable electronic voting in practice. IEEE Security & Privacy **14**(4), 64–73 (2016)
[19] CCE: CCE Report | Reclaim the Republic (May 2021), https://www.reclaimtherepublic.co/report
[20] Chauhan, S., Jaiswal, M., Kar, A.K.: The acceptance of electronic voting machines in India: a UTAUT approach. Electronic Government, an International Journal **14**(3), 255–275 (2018)
[21] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., Vora, P.: Scantegrity: End-to-end voter-verifiable optical-scan voting. IEEE Security & Privacy **6**(3), 40–46 (2008)
[22] Cheeseman, N., Lynch, G., Willis, J.: Digital dilemmas: The unintended consequences of election technology. Democratization **25**(8), 1397–1418 (2018)
[23] Cheney, C.: Want to reach the world's poorest? Design for dumb phones (Mar 2018), https://www.devex.com/news/want-to-reach-the-world-s-poorest-design-for-dumb-phones-90993
[24] Chipchase, J.: Understanding non-literacy as a barrier to mobile phone communication (2005)
[25] Dechand, S., Schürmann, D., Busse, K., Acar, Y., Fahl, S., Smith, M.: An empirical study of textual key-fingerprint representations. In: 25th {USENIX} Security Symposium ({USENIX} Security 16). pp. 193–208 (2016)
[26] Desk, N.H.W.: Why EVMs always 'malfunction' in favour of the BJP? National Herald (Oct 2019), https://www.nationalheraldindia.com/india/why-evms-always-malfunction-in-favour-of-the-bjp
[27] Electronic voting machines: The promise and perils of a new technology (2011)
[28] Ellison, C.: Upnp security ceremonies design document for upnp device architecture 1.0. In: UPnP Forum (2003)
[29] Essex, A., Clark, J., Adams, C.: Aperio: High integrity elections for developing countries. In: Towards Trustworthy Elections, pp. 388–401. Springer (2010)
[30] of Estonia, S.E.O.: General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia, https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf
[31] General Election 2013: FAFEN Observation - Key Findings and Recommendations (Oct 2015), https://fafen.org/general-election-2013-fafen-observation-key-findings-and-recommendations
[32] Faiola, A.: Venezuela election results 'manipulated' by at least 1 million votes, polling company says. Washington Post (Aug 2017)
[33] Finance Division, G.o.P.: Federal Budget 2018-2019, Pakistan (2018), https://www.finance.gov.pk/fb_2018_19.html
[34] Fujiwara, T.: Voting technology, political responsiveness, and infant health: Evidence from brazil. Econometrica **83**(2), 423–464 (2015)
[35] Goodman, B.J.: Myanmar coup: Does the army have evidence of voter fraud? BBC News (Feb 2021), https://www.bbc.com/news/55918746

[36] Hanel, P.H., Maio, G.R., Soares, A.K., Vione, K.C., de Holanda Coelho, G.L., Gouveia, V.V., Patil, A.C., Kamble, S.V., Manstead, A.S.: Cross-cultural differences and similarities in human value instantiation. Frontiers in Psychology **9**, 849 (2018)

[37] Hao, F., Wang, S., Bag, S., Procter, R., Shahandashti, S.F., Mehrnezhad, M., Toreini, E., Metere, R., Liu, L.Y.: End-to-end verifiable e-voting trial for polling station voting. IEEE Security & Privacy **18**(6), 6–13 (2020)

[38] Hapsara, M., Imran, A., Turner, T.: E-Voting in Developing Countries. In: Electronic Voting, pp. 36–55. Springer, Cham, Switzerland (Jan 2017). https://doi.org/10.1007/978-3-319-52240-1_3

[39] Haq, H.B., Ali, S.T.: Electronic voting machines for pakistan: Opportunities, challenges, and the way forward. 1st RASTA Conference (2022), https://www.pide.org.pk/rasta/wp-content/uploads/Hina-Bint-Haq-Conference-Paper.pdf

[40] Haq, H.B., McDermott, R., Ali, S.T.: Pakistan's Internet Voting Experiment. arXiv preprint arXiv:1907.07765 (2019)

[41] Rs 3,200 crore granted to EC for EVM paper trail units (2017), https://economictimes.indiatimes.com/news/politics-and-nation/rs-3200-crore-granted-to-ec-for-evm-paper-trail-units/articleshow/58269901.cms?from=mdr

[42] Inuwa, I., Oye, N.: The impact of e-voting in developing countries: focus on Nigeria. International Journal of Pure and Applied Sciences and Technology **30**(2), 43 (2015)

[43] Findings and Assessment Report of Internet Voting Task Force on voting rights of overseas Pakistanis (2018)

[44] Joe Sterling, F.C., Gillespie, P.: Deadly election day in Venezuela as protesters clash with troops. CNN (July 2017), https://edition.cnn.com/2017/07/30/americas/venezuela-on-edge-vote/index.html

[45] Kiani, K.: The most expensive elections. DAWN (Jul 2018), https://www.dawn.com/news/1421946

[46] Kiayias, A., Zacharias, T., Zhang, B.: Ceremonies for end-to-end verifiable elections. In: IACR International Workshop on Public Key Cryptography. pp. 305–334. Springer (2017)

[47] Kimani, N.: Kenyan poll haunted by the ghosts of voters passed - The Mail & Guardian (Jul 2017), https://mg.co.za/article/2017-07-14-00-kenyan-poll-haunted-by-the-ghosts-of-voters-passed

[48] López, V.: On the frontline of Venezuela's punishing protests. The Guardian (May 2017), https://www.theguardian.com/world/2017/may/25/venezuela-protests-riots-frontline-caracas-nicolas-maduro

[49] Machin-Mastromatteo, J.D.: The most "perfect" voting system in the world. Information Development **32**(3), 751–755 (2016)

[50] Maletić, M., Barać, D., Rakočević, V., Naumović, T., Bjelica, A.: Scaffolding e-voting in developing countries. Management: Journal of Sustainable Business and Management Solutions in Emerging Economies **24**(2), 47–62 (2019)

[51] Maphunye, K.J.: The feasibility of electronic voting technologies in Africa: Selected case examples (2019)

[52] Mohanty, V., Culnane, C., Stark, P.B., Teague, V.: Auditing Indian elections. In: International Joint Conference on Electronic Voting. pp. 150–165. Springer (2019)

[53] Moher, E., Clark, J., Essex, A.: Diffusion of voter responsibility: Potential failings in E2E voter receipt checking. {USENIX} Journal of Election Technology and Systems ({JETS}) **1**, 1–17 (2014)
[54] Nandi, M., Popoveniuc, S., Vora, P.L.: Stamp-it: a method for enhancing the universal verifiability of E2E voting systems. In: International Conference on Information Systems Security. pp. 81–95. Springer (2010)
[55] Securing the vote: Protecting american democracy (2018)
[56] Norris, P., Frank, R.W., i Coma, F.M.: Contentious elections: From ballots to barricades. Routledge (2015)
[57] Oganesyan, R.: Economic voting in the developing world (2014)
[58] Okoro, E.: A Cost-Benefit Analysis of Electronic Voting Operations and Capabilities in sub-Saharan Africa
[59] Oksuzoglu, E., Wallach, D.S.: Votebox nano: A smaller, stronger FPGA-based voting machine (short paper). In: Proceedings of the 2009 USENIX/Accurate Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (2009)
[60] Olembo, M.M., Renaud, K., Bartsch, S., Volkamer, M.: Voter, what message will motivate you to verify your vote. In: Workshop on Usable Security, USEC (2014)
[61] Olken, B.A., Pande, R.: Corruption in developing countries. Annu. Rev. Econ. **4**(1), 479–509 (2012)
[62] Onyango, S.: GSMA: 70% of the world's $1 trillion mobile money market is in Africa (May 2022), https://qz.com/africa/2161960/gsma-70-percent-of-the-worlds-1-trillion-mobile-money-market-is-in-africa
[63] Osho, L.O., Abdullahi, M.B., Osho, O.: Framework for an e-voting system applicable in developing economies. International Journal of Information Engineering & Electronic Business **8**(6) (2016)
[64] Paravicini, G.: Congo fire destroys thousands of voting machines for presidential election. U.S (Dec 2018), https://www.reuters.com/article/us-congo-election-fire-idUSKBN1OC0VP
[65] Park, S., Specter, M., Narula, N., Rivest, R.L.: Going from bad to worse: from Internet voting to blockchain voting. Journal of Cybersecurity **7**(1), tyaa025 (2021)
[66] Pool, J.: The multilingual election problem. Journal of Theoretical Politics **4**(1), 31–52 (1992)
[67] Rao, G.N.: Democracy at Risk! Citizens for Verifiability,Transparency & Accountability in Elections. Veta (2010), http://indianevm.com/book.php
[68] Reporter, T.N.S.: NA briefed on economic cost of sit-ins. DAWN (Jul 2020), https://www.dawn.com/news/1569471
[69] Ryan, P.Y.: Verified Encrypted Paper Audit Trails. Citeseer (2006)
[70] Ryan, P.Y.: Prêt à voter with confirmation codes. EVT/WOTE **11** (2011)
[71] Ryan, P.Y., Bismark, D., Heather, J., Schneider, S., Xia, Z.: Prêt à voter: a voter-verifiable voting system. IEEE transactions on information forensics and security **4**(4), 662–673 (2009)
[72] Salimonu, R.I., Osman, W., Shittu, A.J.K., Jimoh, R.: Adoption of e-voting system in Nigeria: A conceptual framework. International Journal of Applied Information Systems **5**(5), 8–14 (2013)
[73] Santin, A.O., Costa, R.G., Maziero, C.A.: A three-ballot-based secure electronic voting system. IEEE Security & Privacy **6**(3), 14–21 (2008)
[74] Schneier, B.: Essays: In Praise of Security Theater - Schneier on Security (May 2021), https://www.schneier.com/essays/archives/2007/01/in_praise_of_securit.html

[75] Shah, A.: Democracy deadlocked in Bangladesh. Current History **115**(780), 130 (2016)
[76] Sherman, A.T., Carback, R., Chaum, D., Clark, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., et al.: Scantegrity mock election at Takoma Park. In: 4th International Conference on Electronic Voting 2010. Gesellschaft für Informatik eV (2010)
[77] Simpson, R., Storer, T.: Third-party verifiable voting systems: Addressing motivation and incentives in e-voting. Journal of information security and applications **38**, 132–138 (2018)
[78] Philippine Votes Transmitted in Record Time in Largest Ever Electronic Vote Count (May 2016), https://www.smartmatic.com/media/article/philippine-votes-transmitted-in-record-time-in-largest-ever-electronic-vote-count/
[79] Somanathan, M.: India's electoral democracy: How EVMs curb electoral fraud. Brookings (May 2019), https://www.brookings.edu/blog/up-front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud
[80] The: Voting-made-easy has a cost: Over 400 deaths (May 2021), https://www.thejakartapost.com/academia/2019/05/07/voting-made-easy-has-a-cost-over-400-deaths.html
[81] Tjostheim, T., Peacock, T., Ryan, P.Y.: A case study in system-based analysis: the ThreeBallot voting system and Prêt à Voter. School of Computing Science Technical Report Series (2007)
[82] Ummelas, O.: World's Most High-Tech Voting System to Get New Hacking Defenses (2017), https://www.bloomberg.com/news/articles/2017-07-17/world-s-most-high-tech-voting-system-to-get-new-hacking-defenses
[83] Understanding Electoral Violence in Asia (2012)
[84] Wasim, A.: RTS controversy likely to haunt ECP, Nadra for a long time (Aug 2018), https://www.dawn.com/news/1424394
[85] Weber, S., Davydov, D., et al.: Societal and economic effects of linguistic diversity. Voprosy Economiki **11** (2017)
[86] West, J., Desai, P.: Diverse structures and common characteristics of developing nations. Inggris: Oxford University p. 39 (2002)
[87] Population by Country (2021) - Worldometer (May 2021), https://www.worldometers.info/world-population/population-by-country
[88] Yard, M.: Direct Democracy: Progress and Pitfalls of Election Technology. International Foundation for Electoral Systems Washington, DC (2010)
[89] Zagórski, F., Carback, R.T., Chaum, D., Clark, J., Essex, A., Vora, P.L.: Remotegrity: Design and use of an end-to-end verifiable remote voting system. In: International Conference on Applied Cryptography and Network Security. pp. 441–457. Springer (2013)

Visual Secrets : A recognition-based security primitive and its use for boardroom voting

Enka Blanchard
CNRS
LAMIH, Université Polytechnique Hauts-de-France, Valenciennes
Center for Internet and Society, Paris, France

Sébastien Bouchard
Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

Ted Selker,
Cyber Defense Lab
University of Maryland, Baltimore County (UMBC), USA

Abstract. This paper presents and evaluates a new security primitive in the form of non-transferable "visual secrets". We show how they can be used in the design of voting systems. More specifically, we introduce a receipt-free low-tech visually verifiable boardroom voting system which is built for simplicity and can serve as a teaching tool to introduce people to verifiable voting.

Keywords: Usable security, Boardroom voting, Verifiability, User studies, Cognitive psychology

1 Introduction : defining visual secrets

After 20 years of advances in verifiable voting, there is still limited understanding by the public of both how verification works, and why voting systems should be verifiable [3]. Besides, the usability costs remain high, both for end-users and administrators, limiting the number of users who verify their votes [12]. We initially sought to improve usability by simplifying verification based on long vote-codes, and instead found a new security primitive that could have multiple applications, including as the central component of a simple voting system meant to introduce users to the concept of verifiable voting.

Most secrets employed in usable security are shareable : one can give their home keys to a friend, be coerced into revealing passwords, or even have their biometrics such as fingerprints stolen [9]. One natural question is then to ask whether it is possible for humans to have (useful) secrets that cannot be shared ? In a formal way, the answer seems to be no, but if we set reasonable constraints, some tentative solutions can be found.

Our lead is to use specialised human cognitive functions and in particular image recognition. As has been demonstrated since the 1960s, humans have an

extensive memory for visual stimuli [6]. A significant aspect of this image recognition happens in a pre-semantic and pre-cognitive fashion, requiring no conscious effort, thanks to specialised neural pathways in multiple areas of the brain [10, 6]. This is related to the difference between recognition and recall [5]. The mind's pre-semantic treatment means that there might be a loss of information during image recognition. The ability to recognise an image is not directly related to our mental description of it, and any description might ignore some key elements of the picture. This pre-semantic treatment is used as a source of secrets that are recognisable but not shareable, and we call the resulting primitive a *visual secret*.

A user with unlimited time and good eyesight might be able to describe exhaustively each pixel of an image. However, practical protocols would have reasonable constraints on the time spent describing images. These constraints are especially appropriate in our case, as the first proposed application of visual secrets concerns verifiable voting in a boardroom setting. This corresponds to a small group of participants — e.g., jury members — having to quickly vote on an issue, generally between two possibilities.

2 Empirical study

The goal of the study was to test the viability of visual secrets as a security primitive. Subjects were shown three pictures and had to describe them, before having to find their initial pictures among two sets of 10 similar pictures in random order. For the three series, we settled on public domain images of animal faces (lions), natural scenes (mountains), and abstract images, as we conjectured that the latter would be harder to describe. We recruited 164 volunteers through John Krantz's Psychological Research on the Net index [7]. We eliminated subjects who had not provided intelligible answers when asked to describe pictures, leaving 151 subjects.

Subjects could recognise their pictures with high reliability (83%, 86% and 79% for the lions, mountains and abstracts pictures respectively). When compared to a null hypothesis of 5% (for optimised random choice), this is highly significant (z-scores >40 for all series, corresponding to p-values $< 10^{-350}$).

To estimate image describability, two of the authors independently categorised the full list of descriptions subjects wrote about their assigned images. For each description, the assessors selected all images that could potentially fit — without knowing what the correct answer was.

To assess the security of the images as potential visual secrets, one question is crucial : can they be accurately and unambiguously de-

	Assessor	Lion	Mountain	Abstract
Correctly unambiguous	Strict	36	40	35
	Lenient	32	23	7
Wrongly unambiguous	Strict	17	16	16
	Lenient	8	5	3
Unambiguous accuracy	Strict	68%	71%	69%
	Lenient	80%	82%	70%

scribed, or in other words, does a description fits a single image ? The adjoining table shows for each image series and assessor the number of descriptions thought to be unambiguous, how many of those were in fact attributed to the wrong image, and the accuracy. The proportion of unambiguous descriptions was at most 37%, and those descriptions were wrongly attributed in 18-32% of cases. A coercer trying to obtain the secret would then have succeeded in at most 26% of cases, with an additional 8% of cases where they would have been (wrongly) sure that they had found the correct secret. We've thus established that visual secrets are close to our objectives: highly recognisable (79-86%) but poorly describable.

3 Visually Verifiable Ballots (VVB)

We now describe a first application of visual secrets in the form of a low-tech — in our case, paper — voting system appropriate for boardroom elections. VVB are meant to be low-tech system that is not subject to the attacks mentioned in [2] and a cheap teaching tool that is easy to use and can introduce users to the concepts of verifiable voting (before moving on to more secure and complex systems such as Belenios [4]).

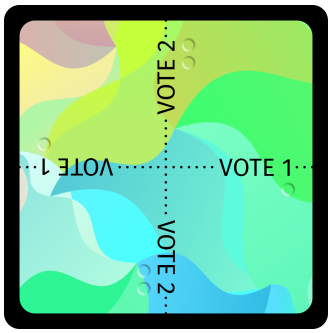


Fig. 1. Example of a Visually Verifiable Ballot.

Visually Verifiable Ballots look and feel like square cards (shown on Figure 1). One side is left blank — or with a regular symmetrical pattern — and the other has the relevant information : a picture from a common set of visual secrets, covering the whole card, and two orthogonal lines crossing the picture, labelled "Vote 1" and "Vote 2". This visual information is complemented by tactile information in the form of texture — bumps — present on both ends of each line, with one bump for the first and two for the second. The protocol goes as follows :

1. The vote organiser opens a new pack of ballots in front of all voters ;
2. One ballot is distributed face down to each voter ;
3. Each voter lifts up their ballot to look at the image and memorise it ;
4. Each voter rotates their ballot a few times, keeping track of its orientation ;
5. Each voter folds their ballot along the line of their choice to select "Vote 1" or "Vote 2" to be on the inside fold, without marking or modifying their ballot in any other way ;
6. The voters cast their ballots in a ballot box or a bag ;
7. The ballot box is upturned and all the ballots are unfolded on a table in front of all the voters' eyes ;
8. The vote organiser tallies the votes orally while the voters check that the ballot featuring their assigned picture are present with the correct fold ;
9. If a voter sees their ballot folded the wrong way or cannot find their ballot, they announce as much without giving any additional information ;
10. The vote organiser announces the result and the vote is over unless someone challenges the result.

4 Concluding remarks

This paper introduced a security primitive called visual secrets, a kind of non-shareable secret that is pure information and does not depend on possessing an item. Its strength comes from the following two properties of pictures. They are highly recognisable, with subjects having 80%+ chance of recognising their own secret. It is difficult to unambiguously describe them. No assessor managed to get better than 82% accuracy on the 15-25% of descriptions which they thought were unambiguous. This primitive shows that cognitive responses can be used to design or improve low-tech voting protocols, and we propose one such protocol for boardroom voting. Visual secrets could also be used as a replacement for the identifying marks used in other verifiable voting systems such as sElect [8] or protocols inspired by Ron Rivest's ThreeBallot [11, 1].

A longer version of this paper and the data files for the experiment are available at `https://hal.archives-ouvertes.fr/hal-03133412`.

References

1. Blanchard, E., Selker, T.: Origami voting: a non-cryptographic approach to transparent ballot verification. In: 5th Workshop on Advances in Secure Electronic Voting (2020)
2. Blanchard, E., Selker, T., Sherman, A.T.: Boardroom voting: Practical verifiable voting with ballot privacy using low-tech cryptography in a single room (2019), https://hal.archives-ouvertes.fr/hal-02908421/
3. Burton, C., Culnane, C., Schneider, S.: vvote: Verifiable electronic voting in practice. IEEE Security & Privacy **14**(4), 64–73 (2016)
4. Cortier, V., Gaudry, P., Glondu, S.: Belenios: a simple private and verifiable electronic voting system. In: Foundations of Security, Protocols, and Equational Reasoning, pp. 214–238. Springer (2019)
5. Haist, F., Shimamura, A.P., Squire, L.R.: On the relationship between recall and recognition memory. Journal of Experimental Psychology: Learning, Memory, and Cognition **18**(4), 691 (1992)
6. Kafkas, A., Montaldi, D.: Recognition memory strength is predicted by pupillary responses at encoding while fixation patterns distinguish recollection from familiarity. The Quarterly Journal of Experimental Psychology **64**(10), 1971–1989 (2011)
7. Krantz, J.H.: Psychological research on the net (2019), `https://psych.hanover.edu/research/exponnet.html`
8. Küsters, R., Müller, J., Scapin, E., Truderung, T.: select: A lightweight verifiable remote voting system. In: 2016 IEEE 29th Computer Security Foundations Symposium (CSF). pp. 341–354 (2016). https://doi.org/10.1109/CSF.2016.31
9. Li, S., Kot, A.C.: Attack using reconstructed fingerprint. In: IEEE International Workshop on Information Forensics and Security – WIFS. pp. 1–6. IEEE (2011)
10. Naber, M., Frässle, S., Rutishauser, U., Einhäuser, W.: Pupil size signals novelty and predicts later retrieval success for declarative memories of natural scenes. Journal of vision **13**(2), 11–11 (2013)
11. Rivest, R.L., Smith, W.D.: Three voting protocols: Threeballot, vav, and twin. In: Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology. pp. 16–16. EVT'07, USENIX Association, Berkeley, CA, USA (2007)
12. Solvak, M.: Does vote verification work: Usage and impact of confidence building technology in internet voting. In: International Joint Conference on Electronic Voting. pp. 213–228. Springer (2020)

VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections (extended abstract)

David Chaum[1], Richard T. Carback[1], Jeremy Clark[2], Chao Liu[3], Mahdi Nejadgholi[2], Bart Preneel[4], Alan T. Sherman[3], Mario Yaksetig[1], Zeyuan Yin[6], Filip Zagórski[5], and Bingsheng Zhang[6]

[1] xx.network, USA
[2] Concordia University, Canada
[3] Cyber Defense Lab, University of Maryland, Baltimore County (UMBC), USA
[4] COSIC, KU Leuven and imec, Belgium
[5] Wroclaw University of Technology, Department of Computer Science, Poland
[6] Zhejiang University, Hangzhou, China

Abstract. We solve a long-standing challenge to the integrity of votes cast without the supervision of a voting booth: "*improper influence*," which we define as any combination of vote buying and voter coercion. Our approach allows each voter, or their trusted agent(s), to cancel their vote in a way that is unstoppable, irrevocable, and forever unattributable to the voter. In particular, our approach enhances security of online, remote, public-sector elections, for which there is a growing need and the threat of improper influence is most acute. In this extended abstract, we introduce the new approach, compare it with previous methods, and concisely summarize the protocols. In our full paper, we give detailed cryptographic protocols, show how they can be applied to several voting settings, describe our implementation in a full voting system called *VoteXX*, and provide UC proofs. Our system protects against the strongest adversary considered in prior related work and is suitable for widespread use in public elections.

1 Introduction

For over 150 years, the voting booth helped prevent voters from being bribed and coerced. For example, a controlling spouse might coerce their partner by observing them vote, if the partner votes online from home or by mail. The booth, however, is becoming untenable as information technology provides the means for people to vote more frequently and conveniently without booths, including using combinations of mailed paper forms and online interactions. Moreover, growing use of technology facilitates vote buying and voter coercion with electronic payments, live video streaming from voter phones, and online threats.

We present a solution to the problem of *improper influence* in voting without booths that enables any voter to *"nullify"* (effectively cancel) their vote in a way that is unstoppable, irrevocable, and forever unattributable to that voter. Our approach allows each voter to recruit one or more trusted agents, which we call "*hedgehogs*." The voter, or their hedgehog(s), can nullify the vote by proving knowledge of the voter's secret key using a zero-knowledge proof. Hedgehogs can be recruited before or during the election, from the voter's acquaintances or

using a service selected on reputation. Our approach can be applied to a variety of voting settings, including unscheduled elections.

Contributions. Our primary contributions are: (1) We introduce the new notions of nullification and hedgehogs, and present a new solution to improper influence based on them. (2) We give cryptographic protocols realizing nullification, and show how it can be applied to several voting settings, including vote-by-mail and online. (3) We present a new fully-decentralized scalable voting system, VoteXX, including registration, voting, nullification, and tallying. (4) We describe our implementation of VoteXX, which uses an *anonymous communication system (ACS)* for registration, vote casting, and other communication. While other systems complicate registration and vote casting, our approach allows simple registration and vote casting by keeping nullification separate.

Previous Work. As shown in Table 1, our approach differs from previous approaches—e.g., revoting, fake credentials, panic passwords, secure hardware, and decoy ballots—by leveraging the realistic assumption of an unknowable and untappable channel between the voter and their hedgehog(s). Our system does not have to make any of the following strong assumptions, which can be readily violated by realistic adversaries: an untappable registration channel, a final time when the voter can vote securely, or that voters are willing to help discourage vote buying by selling decoy ballots. We protect against what we believe to be the strongest possible adversarial model (apart from coercers blocking registration or voting), in which adversaries can learn all voter secrets and observe all voter interactions with the system (excluding interactions with the hedgehogs).

Informally, a voting system is *coercion resistant* means voters cannot prove how they voted (beyond what is inferable from the tally). Formally defining coercion resistance remains an open research problem. For example, Smyth [8]

Table 1. Assumptions and properties of related work for resisting improper influence in online *end-to-end (E2E)* verifiable elections. Properties are fully present (●), partially present (◐), or not present (○). Decoy ballots act indirectly against influence (◉).

Assumptions: System resists coercion when the influencer: (0) acts before/during registration; (1) colludes with the EA; (2) colludes with hardware manufactures; (3) acts at any time; (4) learns all information stored by the voter, including all keys required by the protocol; (5) learns every action taken by the vote. **Properties:** (6) voter can undo coercion undetectably; (7) system is inexpensive; (8) system has low cognitive burden; (9) system has security proof (none/game-based/UC).

		0	1	2	3	4	5	6	7	8	9
Type	**Example**	**Assumption**						**Property**			
Baseline (coercible)	Helios (2008) [1]	○	○	○	○	○	○	○	●	●	◐
Fake credentials	JCJ (2005) [6]	○	◐	●	○	○	○	●	●	●	◐
Masked ballots	WeBu09 (2009) [9]	○	●	●	○	○	○	○	●	○	●
Panic passwords	Selections (2011) [5]	○	●	●	○	○	○	●	●	◐	◐
Decoy ballots	RS-Voting (2012) [3]	●	◐	●	◉	◉	○	○	●	◐	●
Secure hardware	AOZZ (2015) [2]	●	◐	○	○	●	○	●	○	●	●
Re-voting (E2E)	VoteAgain (2020) [7]	●	●	●	○	●	○	●	●	●	◐
Hedgehogs	VoteXX (2022)	●	●	●	●	●	○	○	●	●	●

argues that some proposed definitions are too strong, and others are too weak. Meaningful comparisons among prior coercion-resistance mechanisms require a careful consideration of the associated definitions, assumptions, and properties.

2 Protocol

The VoteXX protocol comprises seven phases:

(1) **Registration Protocol.** Registration is an in-person ceremony between the voter, using a *voting client* device, and an officer for the EA. The voter registers two public keys to be used to vote YES and NO, respectively (one key for each ballot question). The keys are for a digital signature. They are based on a passphrase that can be regenerated from any voting client. The *election authority (EA)* does not learn the passphrase but has high assurance through the protocol that the human voter knows the passphrase. At completion, the *bulletin board (BB)* contains a list of eligible voters, a list of YES public keys, and a list of NO public keys. Only the voter knows the association between their identity and the associated keys.

(2) **Recruiting Protocol.** Each voter concerned with possible coercion can, at any time before nullification ends, recruit one or more hedgehog(s). The voter sends the private key associated with the voter's intention (*i.e.,* to vote YES or NO) to the hedgehog over an untappable channel. In addition, the voter and hedgehog arrange the conditions under which the hedgehog will act.

(3) **Voting Protocol.** Voting is an online procedure in which each voter posts their ballot on the BB over an ACS. The ballot consists of a signature using either the YES or NO key to indicate the voter's selection. The signature is encrypted by the voter under the EA's threshold-shared public key to prevent observers from determining a running tally for the election. At completion, the BB contains a list of encrypted ballots.

(4) **Pre-Tallying Protocol.** After the voting period ends, the trustees of the EA decrypt all submitted ballots in the order they were received. At completion, the BB contains this pre-tally without any nullification actions.

(5) **Activating Protocol.** At any time after a voter recruits a hedgehog and before nullification ends, the voter can activate the hedgehog, consistently with their prior arrangement. For example, the voter might activate the hedgehog by sending an active signal (*e.g.,* moving a potted plant or posting a specific photo to social media), using a "dead person switch" that is the absence of a signal, or relying on the hedgehog to inspect the contents of the BB (*e.g.,* activate if and only if a YES vote has been cast by the voter after the pre-tally protocol).

(6) **Nullification Protocol.** The goal of nullification is to allow voters to flag their cast ballots, particularly in the case of coercion, for "nullification." Each election has a policy defining what nullification means—for example ballots are canceled, flipped, or some other option. The default policy is to flip. The hedgehog (or voter) submits a nullification request under the EA's encryption key that flags a specific ballot. Also, they prove, under zero-knowledge, that they know the appropriate key that authorizes them to nullify the voter's ballot. At completion, the BB contains a set of encrypted nullification requests.

(7) **Tallying Protocol.** After the nullification period ends, the trustees of the EA process the nullification requests under encryption. If a voted ballot is nullified more than once, the EA applies an XOR logical operation to the set of flags to determine if the nullification will be effected. The EA then sums the number of nullifications. Next, the EA decrypts two numbers: the number of nullified YES votes and the number of nullified NO votes. The pre-tally is adjusted using these numbers to produce the final tally. Throughout pre-tallying, nullification, and tallying, the protocols do not reveal any information about how any individual voter voted beyond what can be learned from the final tally itself.

3 Discussion

Leveraging hedgehogs, an ACS, BBs, and user-generated passphrases, VoteXX provides a versatile solution to improper influence in elections against strong adversaries who learn the voter's voting keys. Our full paper [4] includes more details and a formal statement and UC proof of VoteXX's ballot secrecy, coercion resistance, and tally integrity. Future work includes piloting VoteXX in real elections to assess its usability and voter acceptance.

Currently, election systems without voting booths are vulnerable to potential improper influence attacks. Having demonstrated that coercion resistance is possible, even in Internet voting, democratic societies should insist that, as a matter of due diligence, all voting systems should provide coercion resistance. Our work protects voting beyond the booth, and such voting is an essential enabler for the advance of democracy.

Acknowledgments. This project was supported in part by xx network. Clark was supported in part by NSERC and Raymond Chabot Grant Thornton; Sherman by the National Science Foundation and the U.S. Department of Defense.

References

1. Adida, B.: Helios: Web-Based open-audit voting. In: USENIX Security Symposium. pp. 335–348 (2008)
2. Alwen, J., Ostrovsky, R., Zhou, H.S., Zikas, V.: Incoercible multi-party computation and universally composable receipt-free voting. In: Annual Cryptology Conference. pp. 763–780. Springer (2015)
3. Chaum, D.: Random-Sample Voting (2012), online
4. Chaum, D., Carback, R.T., Clark, J., Liu, C., Nejadgholi, M., Preneel, B., Sherman, A.T., Yaksetig, M., Zagórski, F., Zhang, B.: VoteXX: A solution to improper influence in voter-verifiable elections. Cryptology ePrint Archive (2022)
5. Clark, J., Hengartner, U.: Selections: Internet voting with over-the-shoulder coercion-resistance. In: Financial Cryptography (2011)
6. Juels, A., Catalano, D., Jacobsson, M.: Coercion-Resistant electronic elections. In: ACM WPES (2005)
7. Lueks, W., Querejeta-Azurmendi, I., Troncoso, C.: Voteagain: A scalable coercion-resistant voting system. In: USENIX Security (2020)
8. Smyth, B.: Surveying definitions of coercion resistance. Cryptology ePrint Archive, Report 2019/822 (2019)
9. Wen, R., Buckland, R.: Masked ballot voting for receipt-free online elections. In: VOTE-ID (2009)

iVote Issues

Assessment of potential impacts on the 2021 NSW local government elections

Andrew Conway[1] and Vanessa Teague[2]

[1] Silicon Econometrics Pty Ltd.
[2] Thinking Cybersecurity Pty Ltd. and The Australian National University
vanessa.teague@anu.edu.au

1 Introduction

In early December 2021, the Australian state of New South Wales (NSW) conducted one of the largest-ever Internet voting runs in the world,[3] receiving more than 650,000 votes over the Internet via a system called iVote, representing approximately 10% of votes in NSW local government elections. Like prior runs of iVote, the system suffered significant downtime during the election period and an analysis of its source code raised serious questions about its security.

On December 23, the NSW Electoral Commission (NSWEC) released a report which attempts to quantify how these problems affected election outcomes. They focused on voter exclusion resulting from downtime. They also published extensive and detailed data about the election. They concluded that six local government elections were potentially affected by iVote's problems, but that the remainder of results should be trusted.

The NSWEC successfully applied to the NSW Supreme Court to have three outcomes voided on the basis that the system downtime had unfairly prevented people from voting. [4] These three elections were re-run in July 2022. As far as we know, this is the first time in the world that an Internet voting failure led to election results being annulled.

However, the court was not asked to consider whether any other results should also be voided. In this report we conduct an alternative analysis based on NSWEC data, examining which NSW local government election results could have been altered by either voter exclusion due to downtime, or small changes in votes. Our main findings are as follows.

- In 25 contests, the election outcome based only on paper ballots is different from the outcome that incorporates iVote ballots. This does not mean that the official results are wrong, but it does mean that iVotes affected outcomes.
- In most contests, including both mayoral and councillor contests, the number of vote-changes sufficient to alter the election outcome is less than the number of votes received from iVote.
- In 39 contests, the election outcome can be changed by adding fewer votes than the number that NSWEC acknowledges were excluded by iVote's known performance issue. This includes the 6 contests that the NSWEC acknowledges were affected, plus 33 others.

New South Wales local government elections are conducted by a combination of attendance paper voting, postal voting and Internet voting. Seats are allocated via the Single Transferable Vote algorithm, for which general margin computation is infeasible. Our analysis therefore gives lower bounds but may not find the exact smallest change or addition necessary to alter the election result.

All our code is available at https://github.com/AndrewConway/ConcreteSTV.

[3] Estonia runs a larger *fraction* of their votes over the Internet, but fewer by absolute number; Moscow runs a larger number of votes by Internet.
[4] https://www.caselaw.nsw.gov.au/decision/17f913a39e2ade551b821020

1.1 Brief overview of the Single Transferable Vote count and its use in NSW local government elections

The Single Transferable Vote (STV) is a complex social choice function incorporating both proportional and preferential aspects. Voters rank candidates in order, from their first preference downwards. The following is a high-level overview of the general algorithm—for NSW-specific details, see The NSW Local Government (General) Regulation (2005).[5]

Initially, a *quota* Q is computed as

$$Q = \lfloor \frac{v}{s+1} \rfloor + 1,$$

where v is the total number of valid votes and s is the number of seats to be filled.

Any candidate who has at least Q votes from first preferences is immediately elected.

The rest of the algorithm consists of repeating the following steps until all the seats are filled.

1. For any candidate who received a tally $T \geq Q$ (and hence won a seat) in the last step, redistribute their excess votes (that is, $T - Q$ votes) to the next preference specified on the ballot.[6]
2. If any candidate now has a tally $T \geq Q$, declare them elected and go to Step 1.
3. If no candidate has a tally $T \geq Q$, find the candidate with the lowest tally T and *exclude* them: remove them from consideration and distribute each of their ballots to the next-preferred candidate on that ballot.
4. If the number of remaining (i.e. neither seated nor excluded) candidates is equal to the number of unfilled seats, declare the remaining candidates to be winners and stop.

The state of NSW has more than 100 local councils, each with 5–15 councillors elected by STV. Some elect the mayor from within the council, others have a separate mayoral election using instant-runoff voting (IRV), which is the single-seat version of STV.

Because the STV counting algorithm is so complex, it is computationally intractable to answer simple questions that are obvious for many other social choice functions, such as, "What is the minimum number of vote changes sufficient to change the outcome?" and, "If x voters were excluded, is it possible that that was sufficient to alter the outcome?" For many social choice functions, these questions can be answered with (very) basic arithmetic; for STV, much more difficult analysis is necessary.

1.2 The NSWEC's analysis and why it is not convincing

The NSWEC analysis[7] attempts to assess which of the 2021 Local Government contests were affected by iVote's downtime. Their methodology consists of simulating missing iVotes by randomly resampling them from existing iVotes. This is repeated 1000 times, and if no alternative outcomes appear, the results are accepted. This makes three significant assumptions, which are not supported by evidence.

1. It assumes all iVote results are accurate, hence disregarding possible security issues or bugs. The report does not provide any statistics about voter-verification attempts, nor any account of whether any other attempt to verify the iVote votes was made. Since the iVote protocol does not provide end-to-end verifiability, it does not seem possible at this stage to derive evidence supporting the apparent iVotes.
2. Its count of the number of potential additional iVotes includes only those who successfully registered but were not sent a voting credential, thus omitting

[5] https://legislation.nsw.gov.au/view/whole/html/2020-10-27/sl-2005-0487#sch.5

[6] This step is complicated, but the main idea is to distribute the votes to their next preferences, but with a reduced weight so that the total value of transferred votes is equal to $T - Q$, because Q votes have been "used up" to elect a candidate. The exact details vary across jurisdictions.

[7] https://elections.nsw.gov.au/NSWEC/media/NSWEC/LGE21/iVote-Assessment-Methodology.pdf

- people who were unable to register,
- people who received a voting credential but were unable to vote, and
- people who heard about the technical problems and did not try to vote.

3. It assumes missing iVotes are distributed the same as existing iVotes, thus assuming no difference introduced by demographic differences between early and later voters, differences of opinion caused by recent news, or biases introduced by the downtime itself.[8]

In combination, these assumptions may cause a significant underestimate of the impact of iVote's performance and security issues.

iVote has a long history of issues affecting performance,[9] security [HT15], and cryptographic verification [HLPT20]. A report commissioned by NSWEC for the 2021 local government elections found that the codebase was so complex that the auditors could not tell whether the hardcoded passwords they found were in executable parts of the code [HS21]. They also noted that the NSWEC does not compile their own code, instead trusting the vendor to supply an executable version that matches the audited code. iVote does not provide any meaningful way for scrutineers or others to verify that its outputs accurately reflect voters' intentions, so complete trust in the accuracy of iVotes is not justified by evidence. This history is slowly influencing decisions: iVote will not be used for the NSW State General Election in 2023.[10]

There are also some evident calculation errors in the NSWEC analysis. For example, in Round 9 of the Albury council count,[11] C STAR was eliminated with 6 votes, but Esther HEATHER also had 6 votes and was not eliminated. Albury is listed in the NSWEC report as having a "Min vote difference during count" of 1 (p.18, Row 7, Col 5). It should be zero. We are not certain how much these calculation errors affected the analysis. If the source code for the NSWEC analysis is made openly available, we would be happy to help correct it.

We have, however, replicated the simulations described in the NSWEC report, adding the same number of votes that NSWEC acknowledges to be missing, and obtained broadly similar results. Hence the analysis is probably mostly correct *if* its assumptions are accepted. We ran one million simulations for each contest and discovered some low-frequency alternative outcomes that were not detected in NSWEC's thousand samples.

Example 1. In Blue Mountains Ward 3, an alternate outcome appeared 903 times out of one million samples, despite having occurred 0 times in the NSWEC's thousand samples: Kingsley LIU replaced Daniel MYLES (the official winner). The other elected councillors were unchanged.

The complete list of alternate outcomes with non-zero occurrences per million is listed in Appendix A of the full paper [CT22].

1.3 This report: Data-only analysis of election differences

In this report, we do not attempt to guess anything about the missing votes or the size of any iVote security or accuracy issues. We simply analyse the existing data and ask how many dropped or altered votes could have changed the election results.

[8] The authors are aware of at least one family that was intending to use iVote, but decided to go to a polling place when the performance issue made iVote inaccessible. This behaviour change might have been much easier for some voters than others. For example, those who were genuinely very distant from the nearest polling place, or genuinely living with a physical disability, might not have been as easily able to vote in person. Such a difference might have meant that the omitted iVotes were quite different from the iVotes that would have been received if it had not gone down.

[9] https://www.smh.com.au/nsw-election-2019/this-is-ridiculous-nsw-voters-struggle-to-lodge-early-vote-after
html

[10] https://www.elections.nsw.gov.au/About-us/Media-centre/News-media-releases/
Electoral-Commissioner-iVote-determination

[11] https://vtr.elections.nsw.gov.au/LG2101/albury/councillor/report/dop-cnt-009

We thank the NSWEC for the detailed election data and distribution-of-preferences transcripts that are freely available online. This gives us, and other interested members of the public, the opportunity to examine and check the results. Some other electoral commissions fail to make any useful election data available, and most do not share informal votes. We appreciate the opportunity to use real election data to make our own examination and share the results with others.

Section 2 examines the differences between the paper votes and the iVote votes, identifying those contests in which the paper-only outcomes differ from those that include iVotes. Section 3 computes the exact margins for each mayoral contest. Section 4 finds examples in which a small number of vote changes can change the overall election outcome—this quantifies the size of iVote security issues or software errors that could make a difference to the outcome. In almost all contests, this is fewer than the number of votes received over iVote. Section 5 does a similar analysis, but only for adding votes—this quantifies the number of excluded votes that could have altered the outcome. In 39 contests, the number of required additions is less than the number NSWEC acknowledges that they excluded. In many other contests, the number is only slightly more.

2 Comparing paper-only and paper-plus-iVote results

In prior runs of iVote, which all occured during state elections, it was argued that iVote's security was not important because "on the current scale of internet voting it is unlikely that people will want to intervene to try to alter the election result," and "it is highly likely that intervention that changed results would be detected. Psephologists, political parties, pollsters and other experts would most likely query and question outcomes that are inconsistent with expectations." [Wil18] Whether this was true previously,[12] it is certainly not true for the 2021 local government elections—the iVote results were sufficiently numerous, and in many cases sufficiently different from the paper-only returns, to alter election outcomes. We are not aware of any psephologists who have been able to compare these outcomes to any detailed predictions about the outcome of each mayoral race or precise composition of each multi-member council.

Example 2. In the City of Sydney, more than 33% of votes were received via iVote. If we count only the paper votes (including both postal and attendance), the elected councillors are Jess SCULLY, Shauna JARRETT, Linda SCOTT, Sylvie ELLSMORE, Robert KOK, Emelda DAVIS, William CHAN, Yvonne WELDON and Damien MINTON. Including the iVotes alters the outcome, substituting Lyndon GANNON for Damien MINTON. The Mayor of Sydney and the other councillors are unchanged.

Example 3. In the city of Maitland, the Mayor elected when we count only paper ballots is Loretta BAKER. Including the iVotes changes the outcome, electing Philip PENFOLD instead.

Table 1 lists all contests for which the paper-only results were different from the official results, which included both paper and iVote votes.

These differences do not prove that there were software bugs or security problems that affected the iVote results, because there are possible legitimate reasons for the differences. For example, iVote voters may have voted earlier, or may have come from different demographics, than those who voted on paper. It does, however, mean that any possible iVote security and verification issues do matter, because iVote votes changed election outcomes.

These differences are probably the main reason that the NSWEC's simulations produced a result different from the official result substantially more than half the time in Kempsey, out of only two possible results. It would otherwise be surprising to sample from

[12] This claim deserves skepticism even for prior iVote runs, because 5% of votes is enough to alter a close Legislative Assembly contest or a crossbench Legislative Council seat, which are hard to predict.

the same distribution and get the other result 61% of the time—it happens because the iVote returns are distributed differently from the paper ones.

The fraction of votes accepted through iVote varied by location, from less than 5% in some rural electorates to more than 33% in Sydney. On average, it was much higher than in the 2019 state election. Complete statistics, including iVote rates and overall turnout, are given in Appendix B of the full paper [CT22].

Contest	Official winner (iVotes included)	Paper-only winner
City of Blue Mountains - Ward 2	HOARE Brent	VAN DER KLEY Chris
Burwood	HULL David	YANG Alex
Byron	HUNTER Alan	CLARKE Bruce
Coonamble	DEANS Barbara	SMITH Steven (Jay Jay)
Dubbo Regional - Wellington Ward	GOUGH Jess	JONES Anne
Hilltops	FITZGERALD Patrick	HORTON John
Inner West - Marrickville	TSARDOULIAS Zoi	MACRI Victor
- Midjuburi (Lillypilly) Ward		
Kempsey	FREEMAN Joshua	SAUL Dean
Kiama	LARKINS Stuart	GEORGE Tanya
Lane Cove - East Ward	ROENFELDT David	VISSEL Frances
City of Maitland Mayoral	PENFOLD Philip	BAKER Loretta
Moree Plains	COCHRANE Mekayla	RITCHIE Stephen
Muswellbrook	BOWDITCH Mark	OGG Malcolm
Nambucca Valley	WILSON John	HALL David
Narrabri	BOEHM Rohan	STAINES Cameron
North Sydney - Cammeraygal Ward	LAMB Georgia	BAUER Hugo
Parkes	WEBER Daniel	SNYMAN Erik
City of Parramatta - Rosehill Ward	NOACK Paul	STRANO Franceska
City of Randwick - West Ward	VEITCH Philipa	STAVRINOS Harry
City of Shellharbour - Ward A	EDWARDS Maree	BITSCHKAT Shane
Singleton	McNAMARA Tony	JOHNSTONE Sarah
Snowy Valleys	IVILL Michael	DALE Kenneth
City of Sydney	GANNON Lyndon	MINTON Damien
Walgett	KEIR Jane	TAYLOR Michael
Yass Valley	REID Mike	GINN Bill

Table 1. Contests in which the paper-only outcome differs from the outcome when iVotes are included. In multi-winner contests, the other winners stay the same and are omitted from the table.

3 Calculating the exact margin for single-winner contests

In NSW, many Mayors are elected directly using a single-winner preferential (Instant Runoff) electoral system similar to that used in Australian lower-house parliamentary seats.

This section reports on the exact margins of all single-winner contests—this is the number of votes that would need to change in order to alter the outcome. To put it another way, this is the number of (iVote or other) votes that would need to have been altered by a software bug or security problem to divert the result from the correct one.

The calculations were conducted by Michelle Blom using her code at `https://github.com/michelleblom/margin-irv`, which implements the algorithms described in [BTST16].

In most cases, the true margin is the last-round margin, i.e. half the difference between the winner and the runner-up in the last stage of the count, when all but two candidates have been excluded. For example, if Alice and Bob are the only two candidates remaining after all others have been eliminated, and Alice wins with A votes while Bob loses with B votes, then we could make Bob win (or tie) by taking $\lceil (A-B)/2 \rceil$ of Alice's votes and changing them into votes for Bob.[13] To put it the other way, if a software bug or security

[13] $\lceil \cdot \rceil$ represents rounding up to the nearest whole number.

problem had inappropriately changed $\lceil (A-B)/2 \rceil$ of Bob's votes into votes for Alice, this election outcome would be wrong.

However, the true margin is not always the last-round margin, and the candidate who remains in the count second-longest is not always the alternative candidate closest to winning. Sometimes a small change earlier in the count can alter the elimination order and result in a different outcome.

Example 4. In Hunter's Hill, Richard QUINN was excluded at Count 3, with 2,153 votes.[14] If 109 votes are removed from Ross WILLIAMS and added to QUINN, WILLIAMS is excluded in Count 3 instead, then QUINN defeats Zac MILES (the official winner) in the last step.[15]

In NSW Local Government Elections 2021, the Mayoral contests in Broken Hill, Coffs Harbour and Lismore also had a true margin smaller than the last-round margin, because early elimination steps affected the final result. For all the rest, the true margin was the last-round margin. The smallest margins were:

Hunter's Hill	109
Kempsey	194
Orange	244
Port Stephens	284

For 2/3 of mayoral contests, the margin was smaller than the number of votes accepted from iVote. The full results are given in Appendix C of the full paper [CT22].

This is a much more useful value than the least-difference used in the NSWEC report, because it is both a *working example* and a *lower bound*: when we say that the margin for Kempsey Mayor 194 is votes, this means that altering 194 votes suffices for changing the outcome, and also that there is no change of less than 194 votes that changes the outcome.

4 Altering votes to change outcomes in multi-winner contests

Ideally we would also calculate exact margins for the multi-winner council elections. This would answer the question, "What is the smallest alteration or misrecording of votes that could have altered the outcome?" Unfortunately, however, there is no known efficient algorithm for answering this question—the problem is probably intractable in practice.

We have therefore implemented some simple heuristics that look for small alterations that change the outcome. These are exact working examples—if a solution is found, it definitely produces a different set of winners. However, unlike the IRV margins calculated in Section 3, the search is not exhaustive and does not produce a lower bound: there might be even smaller vote changes that alter the outcome, which our algorithm did not find. This paper has been updated slightly since the first version, as algorithmic improvements found better results in some contests.

Code for the heuristics in this section and the next are available at `https://github.com/AndrewConway/ConcreteSTV`. The main idea is to change which candidate is excluded or seated at each count, then check whether that change induces a different election outcome. The main steps are:

1. at each count where a candidate E is excluded, for each continuing candidate C,
   (a) calculate n, the number of votes that must be moved from C to E so that C's tally will be smaller than E's and hence E will not be excluded,
   (b) try to find n appropriate votes from among existing iVotes,
   (c) change them from votes that count for C to votes that count for E,
   (d) check whether this changes the election outcome,

[14] `https://vtr.elections.nsw.gov.au/LG2101/hunters-hill/mayoral/report/mayoral-dop`
[15] This assumes that the tie is broken in QUINN's favour—otherwise, one more vote would be required.

(e) if so, check whether changing a smaller number of them also changes the outcome;

2. do the same for each count at which some candidate C is seated, moving votes from the candidate who got a seat to the highest candidate who did not.

We found many contests in which small vote changes could alter the election outcome. In most contests, the number of votes received through iVote was much more than the number of changes sufficient to change the winners.

Example 5. In the council election for Walgett, altering two votes can change the election outcome. Changing two (below-the-line) votes that mention Jane KEIR to list Anna WITT instead causes Jo COLEMAN, rather than KEIR, to be elected. The rest of the elected council remains the same. The specific changes are:

	1st preference	2nd	3rd	
Vote Change 1: from	TRINDALL Garry	KEIR Jane	TURNBULL Robbie	...
to	TRINDALL Garry	WITT Anna	TURNBULL Robbie	...
Vote Change 2: from	TRINDALL Garry	KEIR Jane	COLEMAN Jo	...
to	TRINDALL Garry	WITT Anna	COLEMAN Jo	...

This can also be expressed in reverse: it means that if two iVotes were misrecorded or altered in the opposite way, the election outcome would be wrong. There are probably many other related ways to produce the same effect.

In addition to 6 contests acknowledged by NSWEC to have been problematic, many others were very close, including 17 for which the election outcome could be changed by altering 10 or fewer votes. These are listed in Table 2.

Contest	**Total votes**	**Added votes to change outcome**	**Vote changes to change outcome**
City of Blue Mountains - Ward 3	12567	19	10
Bogan	1467	17	7
Byron	17735	16	8
Carrathool - Ward A	694	7	4
Coolamon	2576	8	5
Coonamble	2096	5	3
Forbes	5628	27	6
Gilgandra	2492	20	10
Hay	1747	4	2
⋆ Kempsey	16204	1	1
Kiama	15016	10	5
Lockhart - B Ward	615	20	9
Muswellbrook	8756	16	9
Nambucca Valley	12043	12	6
Parkes	8027	12	6
⋆ City of Shellharbour - Ward A	13138	6	2
⋆ Singleton	12745	3	2
Snowy Valleys	8310	27	8
Walgett	2507	11	2
Warren - D Ward	335	6	3
Weddin	2380	15	7
City of Willoughby - Naremburn Ward	8633	19	9

Table 2. Contests with the closest margins found by our algorithm. The last column is the number of iVote changes that can alter the outcome. The second-last column is the number of added votes that can alter the outcome, which is usually (but not always) close to double. The three contests selected by NSWEC as having the highest simulated frequency of alternate outcomes are marked with ⋆.

The contests with very small margins tend to have small populations, but some larger cities require a very small number of changes as a fraction of the overall votes. The smallest margins as a fraction of the total number of votes are in Table 3—there were 13 contests

that could be altered by changing fewer than 0.2% (but more than 10) of the votes, of which only one (Paramatta - Rosehill Ward) was already acknowledged as problematic.

Contest	Total votes	Added votes to change outcome	Vote changes to change outcome	Vote changes as % of total
City of Albury	28378	34	17	0.06%
Armidale Regional	15223	46	25	0.16%
Bathurst Regional	24704	85	45	0.18%
City of Blue Mountains - Ward 2	12493	25	13	0.10%
City of Campbelltown	89337	240	120	0.13%
Goulburn Mulwaree	17394	89	28	0.15%
Hilltops	11021	21	11	0.10%
Inner West - Marrickville	20347	48	32	0.16%
- Midjuburi (Lillypilly) Ward				
City of Orange	23740	70	35	0.15%
City of Parramatta - Rosehill Ward	22283	20	13	0.06%
City of Shoalhaven - Ward 1	21724	99	39	0.18%
Snowy Monaro Regional	11746	40	20	0.17%
Tamworth Regional	35318	70	34	0.10%

Table 3. Councils with closest margins as a fraction of the total votes, excluding those with vote changes less than 11, which are in Table 2.

Another 9 council outcomes can be altered by 11–20 vote changes: Dubbo Regional - Wellington Ward, Junee, Oberon, Temora, Uralla - Ward B, Walcha - B & D Wards, Warren - A & B Wards.

Appendix D of the full paper [CT22] contains the complete list of the smallest vote changes we found that could alter the election outcome. In almost every case, there were sufficiently many iVotes that a carefully-chosen change could alter the outcome. Our companion website at https://andrewconway.github.io/ConcreteSTV/NSWLGE2021/ gives further details on each case, including the alternate winners. Note that we will continue to improve the heuristics after this paper is produced, so the numbers may improve.

5 Adding votes to change outcomes in multi-winner contests

It is extremely difficult to quantify the number of iVote votes that might have been misrecorded or altered—the system generally does not provide any evidence either way. However, it is broadly agreed that in the 2021 NSW LGE at least some voters were unable to vote due to iVote's performance issue. In this section we therefore consider only missing votes. We repeat the analysis of Section 4, but generate different election outcomes only by *adding* votes, without changing any. The heuristic is otherwise the same as that of Section 4 and is implemented as an option in the same code.

These results answer the question "Could the omission of a certain number of votes have altered the outcome?" This was the question most relevant in the 2013 West Australian Senate counting problem, in which a ballot box went missing—it sufficed to show that it had contained enough votes that its omission may have altered the outcome. This also seems to be the right question for analysing only the omissions caused by iVote's performance issue, assuming that the votes received from iVote were accurate.

Example 6. In the city of Albury council, NSWEC acknowledges missing at least **142** votes as a consequence of iVote's performance issue.

If **34** votes are added for Henk VAN DE VEN, the outcome changes: in Count 48 (where VAN DE VEN would be excluded[16]), David THURLEY is excluded instead.[17]

[16] https://vtr.elections.nsw.gov.au/LG2101/albury/councillor/report/dop-cnt-048

[17] This assumes the tie is resolved in favour of VAN DE VEN. If it were not, one more vote would be needed.

Then in the next count, Ross HAMILTON wins a seat instead of David THURLEY. The other elected councillors are unchanged.

This means that if the omitted votes contained 34 more votes for VAN DE VEN than THURLEY, and otherwise did not alter the distribution of preferences, the announced outcome would be wrong.

There are at least 39 contests in which the outcome can be changed by adding fewer votes than the NSWEC acknowledges missing. These are shown in Table 4. Appendix D of the full paper [CT22] contains the complete list of the smallest number of added votes that can change each election outcome. Our companion website at `https://andrewconway.github.io/ConcreteSTV/NSWLGE2021/` gives further details on each case, including the alternate winners.

As in Section 4, these results are working examples but not lower bounds: if we find a solution, it certainly suffices to change the outcome, but we may have missed smaller sets of added votes that also change the outcome. More sophisticated heuristics such as [BCST20] (`https://github.com/michelleblom/STV-manipulator`) would probably get better results.

These results are, therefore, probably an underestimate of the number of contests that could have been affected by iVote's performance issue. This is partly because our heuristic search may have missed some smaller solutions, and partly because NSWEC's estimate of the votes they missed may be conservative.

6 Discussion and Conclusion

The NSWEC has engaged with technology more extensively than any other electoral commission in Australia. Some of this is beneficial, such as their extensive publication of election data, allowing independent studies like this one. Some choices, however, put the foundations of democracy at risk. Use of iVote should be permanently discontinued because it does not securely convey votes, and leaves the state without a rigorous way of assessing how much its problems affected the integrity of the election. The same situation could easily recur if another election is run with the same unreliable, insecure and unverifiable technology.

Apart from the 6 contests identified as at risk by NSWEC, there are another 33 in which it is possible to change the outcome by adding fewer votes than the NSWEC acknowledges to be missing due to iVote's performance issue.

Many other outcomes are highly dependent on the integrity of the iVotes. In 25 contests (of which only 5 are acknowledged as problematic by NSWEC), the official outcome is different from the outcome when only paper ballots are tallied. This does not prove the iVotes are wrong, but it does prove that the integrity of the outcome is dependent on the accuracy of the iVote ballots, which cannot be verified. In most of the remaining contests, there are sufficient iVotes that a targeted manipulation or unlucky software error could have altered the outcome.

The tiny margins in Sections 4 and 5 indicate the importance of the assumptions behind the official NSWEC analysis of the impact of the iVote performance issue. The decision to retain the apparent outcome in all but three contests depends very strongly on their assumptions that the iVotes are accurate, and that the votes they are missing are distributed randomly according to the same distribution as the votes they already have. If those assumptions are not accepted, there is a possibility that many of the announced election outcomes do not accurately represent the choice of the people.

7 Acknowledgements

Thanks to Michelle Blom for computing exact margins for the mayoral contests.

Electorate	Votes	Added votes to change outcome	Votes NSWEC acknowledges excluding
City of Albury	28378	34	142
Armidale Regional	15223	46	71
Bathurst Regional	24704	85	137
Bayside - Ward 2	17168	109	245
City of Blue Mountains - Ward 2	12493	25	73
City of Blue Mountains - Ward 3	12567	19	94
City of Broken Hill	10395	26	38
Byron	17735	16	127
Cabonne	7836	42	57
City of Campbelltown	89337	240	764
Clarence Valley	30661	139	143
Coolamon	2576	8	19
Coonamble	2096	5	10
Forbes	5628	27	37
Goulburn Mulwaree	17394	89	93
City of Griffith	12556	60	73
Hay	1747	4	6
Hilltops	11021	21	45
Inner West - Marrickville - Midjuburi (Lillypilly) Ward	20347	48	242
⋆ Kempsey	16204	1	34
Kiama	15016	10	57
Muswellbrook	8756	16	69
Nambucca Valley	12043	12	35
North Sydney - Cammeraygal Ward	19088	182	251
Northern Beaches - Curl Curl Ward	29742	270	305
City of Orange	23740	70	172
Parkes	8027	12	41
City of Parramatta - Rosehill Ward	22283	20	119
City of Randwick - West Ward	13609	92	140
⋆ City of Shellharbour - Ward A	13138	6	54
City of Shellharbour - Ward B	10527	69	86
City of Shoalhaven - Ward 1	21724	99	145
⋆ Singleton	12745	3	55
Snowy Monaro Regional	11746	40	45
City of Sydney	117362	1044	2003
Tamworth Regional	35318	70	194
Walgett	2507	11	23
Weddin	2380	15	23
City of Willoughby - Naremburn Ward	8633	19	43

Table 4. Contests in which the added votes sufficient to change the outcome are fewer than the number NSWEC acknowledges missing due to iVote's performance issue. The last column is the number of missing votes acknowledged by NSWEC. The second-last is the number of votes that can alter the outcome if added. The three contests selected by NSWEC as in doubt are marked with ⋆.

References

BCST20. Michelle Blom, Andrew Conway, Peter J Stuckey, and Vanessa J Teague. Did that lost ballot box cost me a seat? Computing manipulations of STV elections. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, pages 13235–13240, 2020. https://researchmgt.monash.edu/ws/portalfiles/portal/337436562/337433276_oa.pdf.

BTST16. Michelle Blom, Vanessa Teague, Peter J Stuckey, and Ron Tidhar. Efficient computation of exact IRV margins. In *Proceedings of the Twenty-second European Conference on Artificial Intelligence*, pages 480–488, 2016. https://arxiv.org/abs/1508.04885.

CT22. Andrew Conway and Vanessa Teague. ivote issues: Assessment of potential impacts of the 2021 NSW local government elections (full version), January 2022. https://github.com/AndrewConway/ConcreteSTV/blob/main/reports/NSWLGE2021Report.pdf.

HLPT20. Thomas Haines, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. How not to prove your election outcome. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 644–660. IEEE, 2020. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2723423/main.pdf.

HS21. David Hook and Carsten Schürmann. Review of the revised iVote 2021 system, 2021. https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/demtech-source-code-review-report.pdf.

HT15. J Alex Halderman and Vanessa Teague. The new south wales iVote system: Security failures and verification flaws in a live online election. In *International conference on e-voting and identity*, pages 35–53. Springer, 2015. ArXiv: https://arxiv.org/abs/1504.05646.

Wil18. Roger Wilkins. Report on the security of the iVote system, May 2018. https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/Report-on-the-Security-of-the-iVote-System.PDF.

Features and usage of Belenios in 2022

Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu

Université de Lorraine, CNRS, Inria, France

Abstract. Belenios is an open-source Internet voting protocol associated to a free voting platform, launched in 2015. A detailed overview of the protocol has been presented in [6] in 2019 and its complete, up-to-date specification is public [7]. Since 2019, the use of Belenios has significantly increased with more than 1,400 elections organized each year in 2020 and 2021, and a total of more than 100,000 received ballots.
We report here on the new features added to Belenios since 2019 that include weighted votes, flexible counting methods (*e.g.* Condorcet or STV) thanks to mixnets, and crowdsourced translation with the support of more than 10 languages. Moreover, we have improved the auditability of Belenios in practice, both for voters and authorities.

1 Overview of Belenios

Belenios [5] has been originally inspired by Helios [1]. Compared to Helios, it involves an additional authority (credential authority) to prevent a dishonest server from ballot stuffing. Many cryptographic features have been added since then, such as threshold decryption, mixnets, and blank votes. We briefly survey here the general behaviour of Belenios.

Belenios includes four actors. The **voters** (and their voting devices), the **voting server**, the **decryption authorities**, the **credential authority (CA)**, the **administrator**, and **auditors**. The administrator has no cryptographic role but she is in charge of entering the voter list (a list of email addresses), managing the authorities, defining the start and end date of the election.

Setup. CA generates and sends a private credential to each voter, typically by email. It also sends the list of the associated public credentials to the voting server. The decryption authorities jointly compute the public key of the election.

Voting phase. A voter enters her credential and selects her candidates(s) on her voting device. Her voting choice is encrypted using an homomorphic encryption scheme (ElGamal) and signed with the credential. The signed and encrypted ballot is sent to the voting server once the voter has authenticated herself to the server, using a one-time password sent by email (other authentication mechanisms are supported). The need for both password and credential prevents from ballot stuffing unless the voting server and the credential authority collude. The voter can check on the (public) ballot box that her ballot is present.

Tally. Thanks to the homomorphic property, anyone can compute a ciphertext that contains the number of received votes, for each candidate. The decryption authorities jointly decrypt this ciphertext and produce a proof of correct decryption.

Security properties. The security of Belenios has been studied in several papers [5,4,2]. It preserves **vote secrecy** as long as a threshold of authorities are honest. More precisely, internally, Belenios supports any conjunction of thresholds k_i out of n_i of authorities; on our voting platform, we therefore require the need for the private key of the server and of a threshold of k out of n external decryption authorities, chosen by the electoral board. This protects against an administrator who would silently remove the server as trustee and impersonate all external decryption trustees, as it could be the case in Helios, if participants do not closely supervise who are the decryption authorities.

Belenios is **verifiable** in the following sense. Anyone can check that the result corresponds to the ballots on the bulletin board, thanks to the zero-knowledge proofs (*universal verifiability*). Anyone can check that ballots are encryption of valid candidates and have been produced by legitimate voters, assuming that either the server or the registrar is honest (*eligibility*). Voters can check that their ballot is on the bulletin board (*individual verifiability*).

Belenios however does not guarantee *cast-as-intended*: a malicious voting device could encrypt a candidate different from the choice of the voter. We could easily add the Benaloh challenge [3]. However, several studies [9] have shown that it is very hard to get right in practice and, when badly used, it may even leak the voter's vote. We hope to add a more practical cast-as-intended mechanism in the future.

2 New features

Belenios includes several recent features that, to our knowledge, are not available on other open (and secure) Internet voting platforms.

Weighted votes. A repeated request from our users was to offer weighted votes, where voters may have a different weight. For example, in some sport associations, a voter id may have a number of votes w_{id} that depends on the size of her club. Thanks to the homomorphic property of encryption, it is easy to combine the ballots b_{id} with their weights by computing $\prod_{id} b_{id}^{w_{id}}$ before decryption. The rest of the protocol remains unchanged. Of course, auditors should inspect the voting list even more carefully to check that voters have the expected weight.

Alternative voting. When homomorphic encryption is used, a voter selects between k_1 and k_2 candidates, among a list of n candidates, or vote

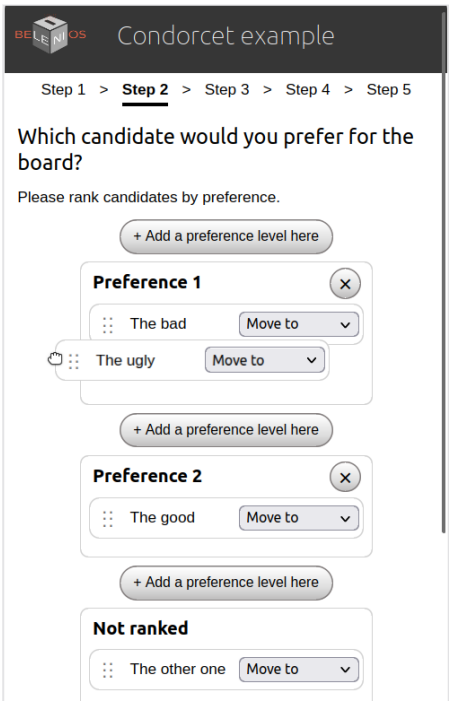


Fig. 1. Interface for preferential voting.

blank (if allowed). Mixnets have been implemented in Belenios so that alternative voting methods can be used, such as STV, Condorcet, or Majority Judgement. We have used the verifiable mixnets proposed in [8]. Despite the additional complexity of mixnets, decryption authorities can still play their role through their browser (our Javascript code takes about 5 minutes for shuffling 1000 ballots, and this grows linearly with the number of voters). We have also adapted the voting interface to support alternative voting as illustrated in Figure 1

Multiple languages. Belenios is used in several countries, well beyond the academic community, thanks to the fact that the voting platform is available in about 12 languages (Czech, English, French, German, Greek, Italian, Norwegian, Polish, Portuguese, Romanian, Spanish, Ukrainian). New languages can easily be added and translations may be amended by any volunteer, thanks to the Weblate platform, available at `https://hosted.weblate.org/projects/belenios/`.

3 Auditability

Many academic voting protocols are verifiable: the authorities as well as any external observer can monitor the ballot box and check that the ballots are well formed and that the result corresponds to the ballots. However, it is not that easy to have authorities who verify in practice since they do not have all the ability to run specific software. Therefore, in Belenios, the main page of an election includes a part, as illustrated in Figure 2, that displays several cryptographic elements (hashes). It allows decryption authorities to check easily (without any software) that their public keys are indeed used in the election and similarly for the credential authority.

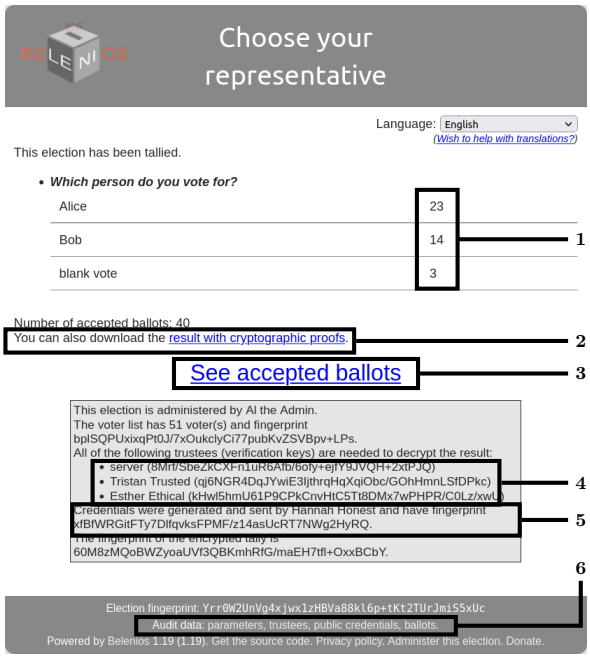


Fig. 2. Final page, including audit data. **1.** Results in human-readable form. **2.** Link to cryptographical proofs. **3.** Link to human-readable ballot box. **4.** Decryption authorities and fingerprints of their keys. **5.** Credential authority and fingerprints of their public parts. **6.** Links to complete machine-readable audit data.

Then a program automatically checks that the hashes displayed on the election page indeed correspond to the election data and that all the cryptographic checks are valid (e.g. validity of the signatures and zero-knowledge proofs). This program also makes sure that no ballot is removed. It can be run by any auditor.

Moreover, for usability reasons, voters vote using a Javascript downloaded from the server. The authorities similarly perform their operations through a Javascript. An auditor should check that these javascripts are indeed the genuine ones. To ease this audit, the pages served by the server have been made constant (this task of making all pages constant is not fully finished yet).

Importantly, the detailed audit procedure, for each actor of the protocol (including voters, authorities, and the administrator) is specified precisely on the Belenios website at `https://www.belenios.org/instructions.html`.

4 Usage of Belenios

Everyone is welcome to deploy their own Belenios server, fitting their technical or legal needs. We are aware of two dozens of such external deployments, because the persons in charge asked us for some help or advice. The only precise statistics we can do is for our own public platform, for which we report the monthly number of elections and number of voters on the Belenios public platform (see Figure 3). The effect of Covid-19 lockdowns is visible, but a good share of users who started using Belenios on this occasion continued thereafter. A seasonal effect is visible: less elections are run during Summer break. Typical users of our platform are academics and associations. Belenios is also used by a German political party and some EU institutions.

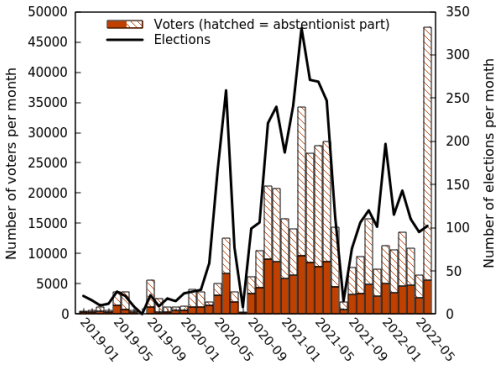


Fig. 3. Usage of the public platform.

References

1. B. Adida. Helios: Web-based open-audit voting. *USENIX'08*, pp 335–348, 2008.
2. S. Baloglu, S. Bursuc, S. Mauw, and J. Pang. Election verifiability revisited: Automated security proofs and attacks on Helios and Belenios. *CSF'21*, pp 1–15, 2021.
3. J. Benaloh. *Verifiable secret-ballot elections*. PhD thesis, Yale University, 1987.
4. V. Cortier, C. Dragan, P.-Y. Strub, F. Dupressoir, and B. Warinschi. Machine-checked proofs for electronic voting: privacy and verifiability for Belenios. *CSF'18*, pp 298–312, 2018.
5. V. Cortier, D. Galindo, S. Glondu, and M. Izabachene. Election verifiability for Helios under weaker trust assumptions. *ESORICS'14*, pp 327–344. Springer, 2014.
6. V. Cortier, P. Gaudry, and S. Glondu. *Belenios: A Simple Private and Verifiable Electronic Voting System*, pp 214–238. Springer, 2019.
7. S. Glondu. Belenios specification - version 1.19. `http://www.belenios.org/specification.pdf`, 2022.
8. R. Haenni, P. Locher, R. Koenig, and E. Dubuis. Pseudo-code algorithms for verifiable re-encryption mix-nets. *FC'17*, pp 370–384. Springer, 2017.
9. K. Marky, O. Kulyk, K. Renaud, and M. Volkamer. What did I really vote for? *ACM CHI'18*, 2018.

A theoretical framework for understanding trust and distrust in internet voting

David Duenas-Cid[0000-0002-0451-4514]

[1] Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland
david.duenas.cid@pg.edu.pl

Abstract. Each and every case of success and failure in the implementation of internet voting is permeated by a common element: the concept of trust. Several researchers highlighted the relevance of creating trust for the successful implementation of technology [15] and, in particular, of internet voting [13]. But the concept itself is complex and challenging to define, for one fundamental reason: it is a concept of everyday social use that has been transposed to academia. When used in academic environments, the laxity of its definition [21] is problematic, because it leaves several relevant questions unanswered. Some of them are discussed briefly in this short paper, which aims to contribute to better understanding of the concept and its implications. [1]

Keywords: Trust and Distrust, Internet Voting Adoption, Societal-related Elements.

1 The definition of trust: is there something missing?

Trust is a concept labeled as a central element for fostering interpersonal relations, cooperative endeavors, or understanding social interaction [12], and is currently experiencing a revival of academic interest due to the impact of digital technologies in social life [2].

Trust is regarded as an immaterial bond, including subjective evaluations and social projections; *without trust, only very simple forms of human cooperation that can be transacted on the spot are possible* [10]. This scenario can be enriched by identifying the originators and receptors of trust, differentiating between interpersonal and institutional trust, and including the trustee's experience. Regarding the first distinction, individuals cannot build interpersonal trust with all people who contribute to providing well-being; institutions take on that role by mediating between unknown individuals. In addition, trust in technology has some properties that differentiate it from trusting in individual people i.e. human beings (institutions included). According to McKnight et al. [11], while in the interaction with humans trust relates to the willingness to perform harmful acts; when related to technology, trust is connected more with the capacity to

[1] This present work received funding from the Electrust (EU H2020 MSCA programme, grant agreement no. 101038055), Dynamika (braku) zaufania w kreowaniu systemów głosowania internetowego (Narodowe Centrum Nauki, OPUS-20 competition, grant agreement no. 2020/39/B/HS5/01661) projects.

provide the expected results due to the lack of an ability to infer intentionally from technology. This lack of moral agency allows focusing on elements relating to belief in the features of the technology itself and, in any case, transferring the moral concerns to those (the human beings or institutions) using the technology [16].

Regarding the trustee's experience, trust appears as a living and evolving concept that changes over time, due to the inputs the trustor receives. The experiential dimension allows dividing the approach to trust into 1) Calculus-based trust - a strategic calculation of the costs and benefits of starting a trust relation; and 2) Knowledge-based trust: a process of creating trust based on information acquired through interactions[8].

2 Trust and distrust, a necessary distinction.

Maybe because this picture is already quite complex, research into trust often left distrust out of view [16], or when considered, it is described as the opposite end of a single continuum, thus considering trust and distrust to be mutually exclusive and opposite conditions [7]. This occurs when we analyze trust in technology [9] and specifically for research into internet voting [5]. Some of the approaches used most frequently to analyze the adoption of technology – the Technology Acceptance Model (TAM) and the Unified Theory of Acceptation and Use of Technology (UTAUT) – do not include trust amongst the set of elements and parameters for consideration [1], assuming that trust appears as a logical outcome of fulfilling the factors included in the model. If this approach were correct, it would be possible to create generalized trust by providing certain elements: a simple formula could serve as a roadmap to fulfill the final goal of building trust in a specific e-government tool. This also applies to studies on I-Voting, in which trust is largely regarded as a goal to be achieved during development of the I-Voting system, instead of also being a precondition for adopting the technology or a dynamic element relating to non-technological factors. The concept of trust, then, appears as a dependent variable, i.e., because of improvements to the system in various regards: transparency [18], usability [3], security [37], or verifiability [6]. Although some studies assess the role of trust in acceptance and adoption of I-Voting, these are based on an essentialist concept of trust [13, 20].

As suggested, trust and distrust should be understood as related, but different theoretical constructs and which must therefore be assessed and evaluated independently. The opposite of "trust" is "to not trust," which differs from distrust and vice-versa.

Acknowledging such a difference is crucial to 1) overcome a traditional limitation of research into I-Voting, notably a preponderance of attention to trusting citizens and what makes them trust, to the detriment of conditions leading citizens to be distrustful [19]; 2) to leverage on the hermeneutical potential of distrust to better explain the adoption of technology and functioning of democracy. Hence, the proposed approach understands trust and distrust as different concepts occurring in parallel and gives citizens inputs to negotiate their position concerning using a specific technology based on them. Moreover, certain elements can help build trust or distrust at different

moments of the interaction or can even contribute simultaneously to creating trust and distrust for other individuals who would react differently to a given input.

In order to develop a framework to comprehend trust and distrust, we must identify potential sources of trust and distrust, in the form of stakeholders or events that might occur during its implementation and use. The list includes elements relating to the technology but also to the institutional framework, with remaining citizens and even with geopolitical relationships (The order is random, it does not involve any gradation):

- Legal aspects relating to legislating for internet voting in electoral law
- Moral or Ethical problems relating to comprehension of democracy
- Expert discourses for or against its implementation and/or use
- Technical trustworthiness of the system
- Management of electoral processes
- Political Interest in irregularly influencing the results (internal and external to the government and even to the country or nation)
- Transparency and presence of external observations
- Relational interaction with others
- Political culture: Acquired knowledge concerning institutions

3 Conclusions: the need for a holistic approach to the analysis of trust and distrust in internet voting

Research into the creation of trust in internet voting has been dominated by approaches biased to its technical dimensions and excluding the logic of distrust. In this short paper, we draft a theoretical framework, proposing different understanding of these elements, and with increased focus on the significance of societal factors.

One of the main conclusions extracted is the need to circumscribe technological trustworthiness-related elements, limiting them to specific processes for creating trust and distrust (i.e., post-use creation of trust and distrust for decision-makers), including other aspects that are relevant for citizens and might not relate to the system per se, but to how it is understood by non-expert users. Simply as an example, while verifiability of the internet voting system has been linked to high levels of trust [17], recounting votes (risk-limiting audits) are not efficient measures for increasing trust since people do not understand the logic behind them [4]. Both elements are logically contradictory but socially possible, if we assume that the construction of trust does not necessarily involve direct comprehension and understanding but can be transferred by others.

A second element that we should extract is the unsuitability of simplified approaches to the logic of creating trust. Creating trust or distrust is complex and includes many variables that will not reveal whether we are using an agonistic question such as "do you trust in…?". It will provide a simple response that hinders the inclusion of complex elements and different weightings in the logical process when constructing an answer. Trusting in internet voting might be motivated by other aspects and might change depending on the moment and the context. Hence, it appears we must determine an

inclusive context to evaluate those elements and a methodology to turn the theory into valid and applicable knowledge.

4 Bibliography

1. Alharbi, S.T.: Trust and acceptance of cloud computing: A revised UTAUT model. Proceedings - 2014 International Conference on CSCI 2014. 2, Mm, 131–134 (2014). https://doi.org/10.1109/CSCI.2014.107.
2. Bodó, B.: Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. New Media Soc. 23, 9, 2668–2690 (2021). https://doi.org/10.1177/1461444820939922.
3. Carter, L., Campbell, R.L.: Internet voting usefulness: An empirical analysis of trust, convenience and accessibility. Journal of Organizational and End User Computing. 24, 3, 1–17 (2012). https://doi.org/10.4018/joeuc.2012070101.
4. Dalela, A. et al.: Voter Perceptions of Trust in Risk-Limiting Audits. In: Krimmer, R. et al. (eds.) Sixth International Joint Conference on Electronic Voting E-Vote-ID 2021. pp. 335–337 University of Tartu Press (2021).
5. Hopland, L., Hole, K.: Building and Maintaining Trust in Internet Voting. Computer. 74–80 (2012).
6. Kulyk, O., Volkamer, M.: Usability is not Enough: Lessons Learned from' Human Factors in Security' Research for Verifiability. In: Krimmer, R. and Volkamer, M. (eds.) Third International Joint Conference on Electronic Voting. pp. 66–81 TUT Press, Bregenz (2018).
7. Lewicki, R.J. et al.: Trust and Distrust : New Relationships and Realities. Academy of Management Review. 23, 3, 438–458 (1998).
8. Lewicki, R.J., Bunker, B.B.: Developing and Maintaining Trust in Work Relationships. In: Trust in Organizations: Frontiers of Theory and Research. pp. 114–139 SAGE, California (1996). doi.org/10.4135/9781452243610.n7.
9. Li, H., Singhal, M.: Trust Management in Distributed Systems. Computer. 40, 2, 45–53 (2007). https://doi.org/10.1109/MC.2007.76.
10. Luhmann, N.: Trust and Power. Wiley-Blackwell, Chichester (1979).
11. Mcknight, D.H. et al.: Trust in a specific technology. ACM Trans Manag Inf Syst. 2, 2, 1–25 (2011). https://doi.org/10.1145/1985347.1985353.
12. McKnight, D.H., Chervany, N.: The meanings of trust. , Minnesotta (1996).
13. Nemeslaki, A. et al.: Could on-line voting boost desire to vote? – Technology acceptance perceptions of young Hungarian citizens. Gov Inf Q. 33, 4, 705–714 (2016). https://doi.org/10.1016/j.giq.2016.11.003.
14. Oostveen, A.-M., van den Besselaar, P.: Security as belief User's perceptions on the security of electronic voting systems. Electronic Voting in Europe: Technology, Law, Politics and Society. 47, May 2014, 73–82 (2004).
15. Ou, C.X., Sia, C.L.: Consumer trust and distrust: An issue of website design. International Journal of Human Computer Studies. 68, 12, 913–934 (2010). https://doi.org/10.1016/j.ijhcs.2010.08.003.

16. Sharma, S.: Can' t change my political disaffection ! The role of political disaffection, trust, and resistance to change in internet voting. Digital Policy, Regulation and Governance. February, (2020). https://doi.org/10.1108/DPRG-07-2019-0049.
17. Solvak, M., Krimmer, R.: The curse of knowledge? Does having more technology skills lead to less trust towards ivoting? In: Fourth International Joint Conference on Electronic Voting E-Vote-ID 2019. pp. 204–208 Taltech Press, Bregenz (2019).
18. Spycher, O. et al.: Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting. In: Kiayias, A. and Lipmaa, H. (eds.) International Conference on E-Voting and Identity; Vote-ID 2011. pp. 19–35 Springer, Berlin, Heidelberg (2011).
19. van de Walle, S., Six, F.: Trust and Distrust as Distinct Concepts: Why Studying Distrust in Institutions is Important. Journal of Comparative Policy Analysis: Research and Practice. 16, 2, 158–174 (2014). doi.org/10.1080/13876988.2013.785146.
20. Warkentin, M. et al.: Social identity and trust in internet-based voting adoption. Gov Inf Q. 35, 2, 195–209 (2018). https://doi.org/10.1016/j.giq.2018.03.007.
21. Yamagishi, T., Yamagishi, M.: Trust and commitment in the United States and Japan. Motiv Emot. 18, 2, 129–166 (1994). doi.org/10.1007/BF02249397.

Internet Voting is Being Pushed by False Claims and Deceptive Marketing

Susan Greenhalgh[1] [0000-0002-2453-8572]

[1]Free Speech For People, Amherst MA 01002, USA

Abstract.

While the convenience of voting from a computer or smartphone over the Internet may seem to be desirable, there is overwhelming evidence that ballots cast electronically cannot be adequately secured to protect the legitimacy of the votes and integrity of our elections. Despite these conclusion, online voting has only increased in the U.S. This begs the question, why?

From public statements, news reports, press releases and marketing materials it becomes evident that the vendors of these online voting systems have been selling their systems to state and local officials with potentially false, misleading and/or deceptive marketing claims. These spurious claims have served to counter the scientific conclusion that online voting is dangerously insecure and unsuitable for public elections. Moreover, these specious assertions promising security have led state and local government officials to believe, incorrectly, that online voting can be secured, and for these officials to support or press for legislation to adopt and/or expand online voting.

This paper examines spurious or false claims made by the two most prominent Internet voting system vendors in the United States, and the impact these false claims have had on laws and policies to adopt online voting.

Keywords: Internet voting, online voting, cybersecurity.

1 Introduction

While the convenience of voting from a computer or smartphone over the Internet may seem to be desirable, there is overwhelming evidence that ballots cast electronically cannot be adequately secured to protect the legitimacy of the votes and integrity of our elections. There is undisputed, settled science that voted ballots transmitted over the Internet are highly vulnerable to manipulation and privacy risks through a variety of attack vectors, and should not be adopted for public elections. [1]

These cyber risks are intensified by the fact that state-sponsored hackers are actively targeting western democratic election systems to disrupt and/or tamper with elections. Following reports of Russian election interference in 2016, two European nations that had adopted online voting, France [2] and Norway [3], suspended the practice. In April 2020, the U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), National Institute of Standards and Technology (NIST) and U.S.

Election Assistance Commission (EAC) issued a risk assessment to U.S state election officials which concurred with previous research and academic consensus. The federal agencies risk assessment stated explicitly that online transmission of voted ballots is at high risk of manipulation, even with security controls in place, and that paper balloting is recommended. [4]

Despite these facts, online voting has only increased in the U.S. This begs the question, why?

From public statements, news reports, press releases and marketing materials it becomes evident that the vendors of these online voting systems have been pitching their systems to state and local officials with potentially false, misleading and/or deceptive marketing claims. These spurious claims have served to counter the scientific conclusion that online voting is dangerously insecure and unsuitable for public elections. Moreover, these specious assertions of security have led state and local government officials to believe, incorrectly, that online voting can be secured, and for these officials to press for the adoption and expansion of online voting.

This paper1 examines specious or false claims made by the two most prominent Internet voting system vendors in the United States, and the impact these false claims have had on laws and policies to adopt online voting.

2 Democracy Live

Democracy Live is a Seattle-based company that sells systems that provide electronic blank ballot delivery systems2, remote accessible ballot marking systems3, and full internet voting systems. Democracy Live is aggressively marketing its OmniBallot voting system configured to enable voters to cast and return a ballot online from their own computerized devices.

False Claims of Security

There is widespread consensus from computer scientists and national security experts that any online transmission of voted ballots cannot be secured. [6] In the risk assessment distributed by the DHS, FBI, EAC and NIST, the federal agencies warned, “Securing the return of voted ballots via the Internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time.” [3]

[1] This paper was updated in September 2022.

[2] Electronic blank ballot delivery allows a voter to access an electronic image of their ballot that can be printed by the voter, marked with a pen, and returned by mail or drop box.

[3] Remote accessible ballot marking systems allow a voter to access a ballot on her own computer, use accessible technology to make selections on the ballot and print the ballot to be returned by mail or drop box. Remote accessible ballot marking systems can be designed to retain all vote selection data on the voter’s computer, or to transmit the vote choices over the internet, back to a remote server even if the voter prints the ballot and physically returns the printed ballot. [5]

Yet, Democracy Live has maintained in marketing materials for its online ballot return system "OmniBallot," that ballots transmitted over the Internet through its portal are secure, claiming:

- "OmniBallot is an electronic method of delivering and **returning ballots via a secure online portal**."
- "OmniBallot offers **secure,** accessible remote balloting for all voters."
- "OmniBallot utilizes AWS Object Lock to **ensure immutable document (ballot) storage**."
- "The voter's ballot selections are encrypted and **securely stored**."
- "**Accurate** and efficient ballot delivery"
- "**Securely** delivering the correct ballot and ballot materials to eligible voters."
- "…voters with disabilities and remote voters, can **securely** access and return their ballots in a **more secure** and accessible method." [7]

Democracy Live has repeated brazen, baseless claims that its online ballot delivery and return system is secure in order to sell its product despite unanimous expert consensus to the contrary.

But more importantly, researchers at the University of Michigan and the Massachusetts Institute of Technology conducted an independent security review of Democracy Live's OmniBallot online ballot return system and found that it is "vulnerable to vote manipulation by malware on the voter's device and by insiders or other attackers." The security researchers went on to warn, "if at all possible, do not return your ballot through OmniBallot's website or by email or fax. These return modes cause your vote to be transmitted over the Internet, or via networks attached to the Internet, exposing the election to a critical risk that votes will be changed, at wide scale, without detection." [9]

Any notion that Democracy Live's claims of security may be founded in well-meaning naivete evaporates when considered alongside Democracy Live's cynically crafted legal policies and sales contracts which plainly acknowledge that they cannot warrant the accuracy or reliability of the Democracy Live system.

"7.2 democracy live does not represent or warrant that omniballot online will operate error-free or uninterrupted and that all program errors in omniballot online can be found in order to be corrected. Nor does democracy live make any warranties regarding the accuracy, reliability, or currency of any information content." [10]

This clause shows that Democracy Live is fully aware of this fact and leverages it to avoid legal liabilities, while simultaneously making untrue marketing claims that it can secure ballots sent over the Internet.

False Claim Regarding Federal Certification of OmniBallot Tablet[4]

Democracy Live's misleading and untrue statements are not limited to claims regarding the security of its online systems. In a press release issued November 2019, Democracy Live wrote:

"*Seattle-based Democracy Live has been awarded full certification of the first stand-alone accessible balloting device in the elections industry... The OmniBallot Tablet is the first vendor-neutral, off-the-shelf ballot marking device that has been reviewed and approved by an EAC-approved independent test lab.*" [11]

By claiming the device received "full certification," by an "EAC-approved test lab," the press release appears to boast that the OmniBallot Tablet was awarded federal certification by the EAC. However, no OmniBallot product has ever been granted EAC certification. [12] Democracy Live is not even a registered manufacturer of the EAC's testing and certification program, a pre-requisite for any voting system vendor that wishes to pursue EAC certification. [13]

Distorting Perception of Its Systems

Democracy Live has also tried to mute public opposition to its online voting system by falsely recasting the system to election officials and voters as something other than online or Internet voting. In an interview with NPR, Democracy Live CEO Brian Finney admitted "online voting" is "a loaded term" and claimed its system is instead a "document storage application." [14] This directly contradicts the EAC, the National Academies of Science, Engineering and Medicine, [1] and multiple other credible, relevant entities that define Internet or online voting as any process which transmits a voted ballot over the Internet. [15]

Democracy Live has taken this disinformation even further by falsely claiming that its system provides a "voter-verified paper ballot," which is widely viewed as the gold-standard for secure, auditable voting systems. It is true that ballots transmitted over the Internet by Democracy Live are routinely printed at the election office and counted by scanner. However, a paper ballot printed at the election office is not ever viewed or verified by the voter and is plainly not a "voter-verified paper ballot." Yet, in its marketing materials, Democracy Live has claimed, "[s]erving over 600 jurisdictions in the U.S., the OmniBallot portal has generated a voter-verified paper ballot in 100% of all elections." [16]

Democracy Live has repeated this distortion in public statements, press interviews and marketing materials in an attempt to rebrand its product as a paper-based voting system.

Democracy Live's CEO told a local Seattle news outlet:

[4] This section of the report was updated November 3, 2021 to more precisely reflect the fact that the referenced press release related to OmniBallot Tablet.

"*This is really a paper-based document transmission system…At the end of the day, there's going to be a paper ballot involved. It's simply storing a document — in this case that document happens to be a ballot — in a federally approved cloud environment.*" [17]

Accessible Voting that is Inaccessible

Democracy Live promotes its system as a solution to provide accessible, absentee voting to voters with disabilities that are unable to handle a paper absentee ballot, like those with visual impairments or manually dexterity issues. Democracy Live has claimed its system is fully accessible for voters with disabilities [18], and meets all accessibility requirements [19],

"*OmniBallot is a fully ADA Section 508, WCAG 2.0aa compliant remote ballot marking solution. The system has been tested to meet the accessibility requirements of over 90 combinations of browsers, operating systems, screen readers and devices. OmniBallot has been deployed as an accessible absentee tool since 2009 and has been tested and reviewed by members of most every leading disability organization in the nation*." [7]

In January 2020, Democracy Live was engaged to run the Conservation District elections for King County, Washington, boasting that the system would provide accessible ballots to voters with disabilities. [18]

But when it launched in 2020, the Democracy Live system was found to be incompatible with standard accessible screen readers, leaving voters with visual impairments, reliant on screen readers, few options to vote. In response to the undeniable failure, Democracy Live offered voters with disabilities free rides to a local polling place to cast a ballot on an accessible device.

According to a bulletin posted on the King County website:

"*The current mobile voting solution being offered in the King Conservation District election allows voters with disabilities to access, mark, sign and return their ballot entirely independently. However, for vision impaired voters utilizing screen readers, voters must turn off screen readers to sign their name, before turning it back to submit their ballot.*

The issue, which was identified by Disability Rights WA, a local non-profit that protects the rights of people with disabilities statewide, is the result of screen reader incompatibility with Apple and Google operating systems. In order to provide an accessibility option for voters who are not able to turn off their screen reader to sign their ballot and screen, KCD will provide accessible voting locations at their office on Election Day, February 11th from 9:00am through 8:00pm. Free transportation to KCD's office will be provided for those effected [sic] by the screen reader issue through Democracy Live's ride-share service. Voters effected by the issue can call 855-655-

VOTE (8683) to arrange transportation to KCD's office, or for questions and assistance with voting from home." [20]

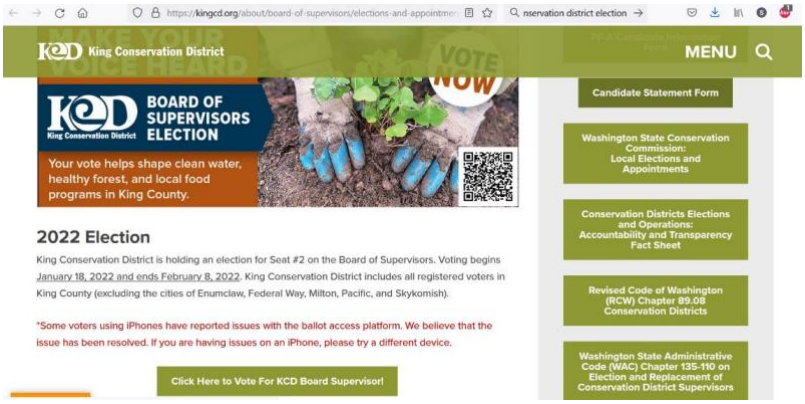


Fig. 1. Two years later, in the 2022 elections, voters were still experiencing issues with the Democracy Live ballot access platform on iPhones, according to a website announcement. In the 2022 election, disabled voters were given no additional options to vote.

The failure of Democracy Live's online voting system to provide ballot access for voters with disabilities was consequential. At a hearing this year of the Washington State legislature, an elected King County Conservation District member testified a constituent with a visual impairment told her she "simply gave up when she was trying to vote, and said, quote, "*It doesn't feel like they even want us to vote*." [21]

3 Voatz

Voatz is a Boston-based startup company that is developing and aggressively marketing an Internet-based voting system that employs a blockchain to enable voters to cast a ballot from an application loaded on to their mobile phones. Voatz' system has been used in municipal elections in Salt Lake City, Utah [22], West Virginia [23] and Denver, Colorado [24].

False Claims of Security

Voatz' campaign to promote its voting system has included bogus claims of "military grade security," [25] public statements asserting that votes cast on its platform could not be deleted or altered, [26] and published materials and presentations [27] promising that Voatz' system was robustly vetted and secure [28]. Though many computer security experts vociferously expressed skepticism or distrust at Voatz' claims as unsupported, spurious or misleading [29], [30] West Virginia elected to engage Voatz to offer its mobile voting system.

In a press release issued by the office of the Secretary of State, Secretary Mac Warner praised Voatz, saying he was pleased with the system. [23] Warner's support for Voatz and confidence in its security was repeated in multiple news stories and in presentations to other election officials. [31] Warner's general counsel Donald Kersey praised the system to a group of Secretaries of State and State election directors, and affirmed that his office was confident the system was trustworthy because of a purported security assessment. [32] In response to an op-ed criticizing Voatz' security and lack of transparency, Secretary Warner authored an op-ed that vigorously defended Voatz and attacked the criticisms as inaccurate. [33] Warner even tried to discredit the criticism by suggesting that opposition to Voatz' online voting system was motivated by a desire to hinder voting by members of the military. Warner's aggressive defense of Voatz' security indicates Voatz' campaign to persuade West Virginia election officials that its system is secure was fruitful.

West Virginia's support of Voatz served to validate the system to other election officials and helped Voatz sell its product in other states. [34] Warner's trust in Voatz' system also drove his efforts to have the legislature pass SB 94 which expands online voting to all West Virginia voters with disabilities. [35]

Similarly, Voatz' technology was actively promoted in Denver, Colorado, which adopted the system for municipal elections. Colorado election officials expressed confidence in Voatz and its security, echoing the false claims in Voatz' marketing materials. Denver County deputy director of elections Jocelyn Bucaro praised Voatz, saying "[w]e are very excited about the promise of this technology. Our goal was to offer a more convenient and secure method for military and overseas citizen voters to cast their ballots, and this pilot proved to be successful." [36]

These statements prove the campaign to persuade election officials that Voatz' system is secure was successful, resulting in an expansion of online voting.

Though Voatz had succeeded in hoodwinking several key election administrators, its failure to substantiate its security claims continued to breed distrust among others. In November 2019, U.S. Senator Ron Wyden (OR) sent a request to the Department of Defense and the National Security Agency asking both to conduct a security evaluation of Voatz, writing:

"*While Voatz claims to have hired independent security experts to audit the company, its servers and its app, it has yet to publish or release the results of those audits or any other cybersecurity assessments. In fact, Voatz won't even identify its auditors. This level of secrecy hardly inspires confidence*." [37]

In February of 2020, election officials and the public had their first look at Voatz' security from an independent third party when researchers at the Massachusetts Institute of Technology (MIT) published a report that contradicted many of Voatz' claims. The report was a stunning catalogue of security gaps, and documented multiple vulnerabilities "that allow different kinds of adversaries to alter, stop, or expose a user's vote."

By reverse engineering the publicly available Voatz mobile application, the MIT researchers were able to analyze and identify several opportunities to compromise,

corrupt or alter votes cast over the Voatz application before the ballot even enters the blockchain. The MIT researchers were able to circumvent Voatz' malware protections with "minimal effort," allowing an attacker to corrupt the Voatz application and undetectably alter or spy on vote choices. The researchers also found that votes cast on the application are not loaded directly onto the blockchain; instead, they first pass through a server which is also vulnerable to multiple attacks that could manipulate or delete votes before they even reach the blockchain, making any public audit of votes recorded on the blockchain meaningless.

In addition to documenting multiple, significant vulnerabilities with the Voatz mobile voting system, the MIT researchers included in the appendices a catalogue of eleven of Voatz' published security claims, annotated by the researchers with findings from their research demonstrating the falsity of Voatz' security representations. [38]

Concerned the vulnerabilities could have national security implications, the MIT researchers reached out to the Cybersecurity Infrastructure and Security Agency (CISA) at DHS to share their findings. CISA found the research credible and facilitated communication between the researchers and Voatz to responsibly disclose the security issues to Voatz before the report was made public. CISA also arranged calls between the MIT researchers and several affected election officials to alert them to the findings.

Voatz responded to the MIT researchers' findings forcefully; staunchly denying their conclusions and vigorously criticizing the research methods on its blog, and on a media call held on the same day the report was made public. Voatz called the research "flawed" [39] and "riddled with holes" as its officers claimed the attacks MIT identified were impossible. [40]

Even though the DHS had validated MIT's findings, Voatz' strenuous denials and attacks on the MIT report succeeded in convincing some of its customers that Voatz' security claims were valid and that the MIT findings were false. Utah County Clerk Amelia Powers Gardner repeated the same spurious explanations Voatz had provided to reporters when justifying the continued use of the application and told reporters there was no evidence the researchers' findings raised security concerns. [41]

A month after the MIT study was published, the independent security firm Trail of Bits (TOB) released a security review it conducted of the Voatz mobile voting platform on behalf of Tusk Philanthropies and Voatz. The Trail of Bits' study was a searing indictment of Voatz' security, affirming all of the assertions made by the MIT team and identifying additional security vulnerabilities in the system. Further, the Trail of Bits study exposes many of the public statements Voatz made in response to the MIT study as false, misleading or specious. According to the Trail of Bits report, TOB confirmed to Voatz all the security vulnerabilities identified by MIT on February 11 two days before Voatz published its denial of the MIT study and held a press call falsely excoriating the MIT report. [42]

Voatz Misleading and Potentially Illegal Use of the DHS Seal and CISA Logo

In September and October of 2019, at Voatz' request, the Hunt and Incident Response Team (HIRT) of DHS's CISA conducted an assessment of Voatz' systems to determine if they contained any evidence or artifacts indicating Voatz had suffered an intrusion.

[43] After its completion, the assessment was provided to Voatz only. As is CISA's practice, the assessment was not made public, nor was it classified.

As described above, in February of 2020, as the researchers at MIT were preparing to release their damning security review of Voatz' application, the MIT team alerted CISA to their findings and CISA in turn, facilitated a meeting between the researchers and Voatz. At the meeting, Voatz was made aware not only of the damaging findings, but that they would soon be reported in *The New York Times*.

In mid-February 2020, with a media storm looming, Voatz delivered a summary of HIRT's findings, written by Voatz, to the West Virginia Secretary of State's office. [44]

The Voatz' summary, provided February 11, 2020, prominently displays the DHS seal and CISA logo, as well as the Voatz logo. It contains no disclaimer or mark alerting the reader that the document was not written by DHS or CISA. [45]

Once the MIT report was published by *The New York Times*, a media frenzy ensued and Voatz held a press call to criticize and disavow the researchers' findings. On the press call Voatz' CEO Nimit Sawhney identified the Voatz summary as a DHS security audit, telling reporters:

"…there are some audits happening for which information is publicly available. One of them was conducted by the DHS. That's [sic] report is available on our website…" [40]

As one of the most vocal supporters of Voatz' system the West Virginia Secretary of State's office fielded multiple calls from reporters regarding the MIT report. The Secretary of State shared the falsely labeled summary with several reporters and cited it to counter the damaging revelations in the MIT study. [46] Several media reports then described the summary as a declassified DHS report. [5]

Voatz publicly released an updated version of this report sometime after February 14, 2020, which removed the DHS seal and CISA logo, and added a disclaimer clarifying that Voatz created the summary. **[43]** Voatz' falsely labeled summary may constitute a violation of 18 U.S.C. § 701 (prohibiting use of government insignias except as provided by regulations), [47] or 18 U.S.C. § 1017 (prohibiting false use of government insignias). [48]

Although the currently public version of the summary no longer uses the DHS seal, Voatz may have also used DHS branding on other materials it may have provided to its customers.

It appears the Voatz summary was written and distributed with the government logo to blunt the impact of the MIT report, and maintain the company's standing in the marketplace.

[5] The Mother Jones article continues to link to the original, falsely labeled, Voatz summary. *Id.* ("Warner's office also provided a copy of a declassified DHS assessment of the Voatz network.")

4 Conclusions and Recommendations

As reflected in testimony before the U.S. Congress, regulations on polling place voting machines are woefully insufficient. [49] Online voting systems and vendors are not regulated at all. There is absolutely no oversight, regulation or accountability for the vendors of online voting systems and they appear to have exploited this fact to sell their systems with spurious claims. Moreover, states are adopting policies and passing legislation to expand online voting, supported by the untrue expectation that vendors can supply secure systems.

We recommend the false claims made by these vendors be fully investigated by relevant authorities including: the Federal Trade Commission, the Department of Justice, State Attorneys General and relevant Congressional Committees. We must not permit the vendors' self-interested, untrue marketing strategies promote election policies and legislation that put our elections at risk.

Acknowledgements. Free Speech For People would like to thank Dr. Michael Spector and Professor J. Alex Halderman, whose research provided facts central to this report, and whose input was essential. We would also like to thank Ron Fein, Travis Arbor, Sarah Fender, and Zakary Kaddish for their contributions. Finally, we would like to thank Craig Newmark and Craig Newmark Philanthropies, and Marion Edy and the Threshold Foundation for making this report possible.

5 References

1. Securing the Vote, Protecting American Democracy, National Academies of Science, Engineering and Medicine. (2018). *https://www.nap.edu/read/25120/chapter/1*
2. France Drops Electronic Voting for Citizens Living Abroad Over Cyber Security Fears. Reuters. (2017). https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233.
3. Amundson, B.: No more online voting in Norway. Science Norway. (2019). https://sciencenorway.no/election-politics-technology/no-more-online-voting-in-norway/1562253
4. Risk Management For Electronic Ballot Delivery, Marking, and Return. U.S. Election Assistance Commission, National Institute of Standards and Technology, Federal Bureau of Investigation, Cybersecurity Infrastructure Security Agency. (2020). https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf?mod=article_
5. Greenhalgh, S., Newell S.: Leveraging Electronic Balloting Options Safely and Securely During the COVID-19 Pandemic. Free Speech For People and American Association for the Advancement of Science. (2020). https://freespeechforpeople.org/wp-content/uploads/2020/06/rabm.white_.paper_.6.23.20.pdf
6. Letter to Governors and Secretaries of State on the insecurity of online voting. AAAS Center for Scientific Evidence in Public Issues. (2020). https://www.aaas.org/programs/epi-center/internet-voting-letter

7. Omniballot Fact Sheet. https://democracylive.com/wp-content/uploads/2020/04/OmniBallot-Fact-Sheet-Democracy-Live-AWS_3.30.20.pdf (emphasis added).
8. Gutman, D.: Online voting is coming to Seattle, but only for an election you've likely never heard of. Seattle Times. (2020) https://www.seattletimes.com/seattle-news/politics/online-mobile-voting-is-coming-to-king-county-but-only-for-an-election-youve-likely-never-heard-of/
9. Spector, M, Halderman, J. Alex.: Security Analysis of the Democracy Live Online Voting System, University of Michigan. (2020). https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf
10. Contract between Democracy Live and Williamson County, TX. Page 3. https://agenda.wilco.org/docs/2020/COM/20200107_1503/23436_Williamson%20County%20UOCAVA%20Agreement%20revised%2012.17.19.pdf
11. Democracy Live Awarded Certification Approval for Dell/Windows 10 IoT Enterprise Balloting Solution. BusinessWire, (2019). https://www.businesswire.com/news/home/20191111005677/en/
12. https://www.eac.gov/voting-equipment/certified-voting-systems
13. https://www.eac.gov/voting-equipment/registered-manufacturers
14. Parks, M.: States Expand Internet Voting Experiments Amid Pandemic, Raising Security Fears, NPR (2020). https://www.npr.org/2020/04/28/844581667/states-expand-internet-voting-experiments-amid-pandemic-raising-security-fears
15. U.S. Election Assistance Commission: A survey of Internet voting (2011), https://www.eac.gov/sites/default/files/eac_assets/1/28/SIV-FINAL.pdf
16. https://democracylive.com/wp-content/uploads/2020/04/OmniBallot-Fact-Sheet-Democracy-Live-AWS_3.30.20.pdf
17. Bowman, N.: King County district to use one-of-a-kind smartphone voting platform for third straight year.MyNorthwest. (2022). https://mynorthwest.com/3301713/king-conservation-district-smartphone-voting-2022/
18. Democracy Live Press Release, Mobile Voting is Coming to Voters in King County, WA. (2020). https://www.prnewswire.com/news-releases/mobile-voting-is-coming-to-voters-in-king-county-wa-300990874.html
19. Democracy Live Omniballot Portal, Accessible Remote Balloting Portal flyer. https://democracylive.com/wp-content/uploads/2022/04/OmniBallot-Portal-Democracy-Live_1.17.22.jpg
20. King Conservation District and Democracy Live to Offer Additional Accessible Voting Options. (2020). Available at: King Conservation District and Democracy Live to Offer Additional Accessible Voting Options : King Conservation District (kingcd.org)
21. Testimony of Brittney Bush Bollay, elected member of the King County Conservation District, at the January 27, 2022 House State and Tribal Government Committee hearing of the Washington State legislature. https://tvw.org/video/house-state-government-tribal-relations-committee-2022011573/?eventID=2022011573 at 38:10.
22. Utah County to use voting app despite security concerns. Associated Press. (2020). https://apnews.com/article/0efd3ae8988bf3cf222329400119f1cf
23. Warner Pleased with Participation in Test Pilot for Mobile Voting.: Secretary of State Mac Warner. (2018). https://sos.wv.gov/news/Pages/11-16-2018-A.aspx

24. Kenney, A.: Denver will allow smartphone voting for thousands of people (but probably not you). Denver Post. (2019). https://www.denverpost.com/2019/03/07/voting-smartphone-blockchain-denver
25. Voatz.: Military-Grade Security, Easy To Use: Elections Technology & Civic Engagement. https://freespeechforpeople.org/wp-content/uploads/2020/04/Voatz_1Pager.military.grade_.pdf
26. Hackett, R.: Denver and West Virginia Deserve Praise for Voting on Blockchain. Fortune. (2019). https://fortune.com/2019/03/23/blockchain-vote-election-denver-west-virginia-voatz/
27. https://blog.voatz.com/wp-content/uploads/2019/02/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf
28. Voatz.: Frequently Asked Questions. https://www.voatz.com/faq.html
29. Kosoff, M.: A Horrifically Bad Idea: Smartphone Voting is Coming Just in Time for the Midterms. Vanity Fair. (2018). https://www.vanityfair.com/news/2018/08/smartphone-voting-is-coming-just-in-time-for-midterms-voatz
30. Jefferson, D.et al.: What We Don't Know About the Voatz "Blockchain" Internet Voting System. (2019). https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf
31. Mistich, D.: New Study Says West Virginia's Mobile Voting Pilot Increased Turnout, Notes Security Concerns. West Virginia Public Broadcasting. (2019). https://www.wvpublic.org/post/new-study-says-west-virginia-s-mobile-voting-pilot-increased-turnout-notes-security-concerns#stream/0
32. Freed, B.: West Virginia may offer blockchain-based ballots to all of its overseas voters this November. StateScoop (2018). https://statescoop.com/west-virginia-may-offer-blockchain-based-ballots-to-all-of-its-overseas-voters-this-november/
33. Warner, M.: Criticism of mobile voting project were misinformed, suspect. Charleston Gazette-Mail. (2018). https://www.wvgazettemail.com/opinion/op_ed_commentaries/mac-warner-criticism-of-military-mobile-voting-project-were-misinformed/article_7757947f-693d-5229-bce5-331e7ff35cb0.html
34. Sylte, A.: Need to cast a ballot from overseas? Denver now has an app for that 9News. (2019). https://www.9news.com/article/news/local/next/need-to-cast-a-ballot-from-overseas-denver-now-has-an-app-for-that/73-66118959-c135-4bdb-814d-a2233dc7c427
35. West Virginia pushes online voting for the disabled. GCN. (2020). https://gcn.com/articles/2020/02/03/west-virginia-mobile-voting-disabled-persons.aspx
36. National Cybersecurity Center Successfully Completes Third Party Audit for Denver's Mobile Voting Pilot. PRNewswire. (2019). https://www.prnewswire.com/news-releases/national-cybersecurity-center-successfully-completes-third-party-security-audit-for-denvers-mobile-voting-pilot-300896234.html
37. https://www.washingtonpost.com/context/sen-ron-wyden-d-ore-letter-regarding-voatz/e9e6dd4f-1752-4c46-8e37-08a0f21dd042/
38. Spector, M. et al: The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. Massachusetts Institute of Technology.(2020).
39. https://blog.voatz.com/?p=1209

40. Voatz Open Press Call Transcribed from February 13, 2020. https://blog.voatz.com/?p=1243
41. Utah County to use voting app despite security concerns. Utah Public Radio. (2020). https://www.upr.org/utah-news/2020-02-19/utah-county-to-use-voting-app-despite-security-concerns
42. Our Full Report on the Voatz Mobile Voting Platform. Trail of Bits. (2020). https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/
43. Voatz, Hunt Engagement Summary. https://voatz.com/Hunt-Engagement-Summary-Voatz.pdf (2020).
44. Donald Kersey, General Counsel to West Virginia Secretary of State, email to Susan Greenhalgh. Available at: https://bit.ly/3wEMDca
45. Initial Voatz Hunt Assessment Summary. https://bit.ly/3uqefAw
46. Vicens, AJ.: Security Researchers Find Flaws in Online Voting System Tested in Five States. Mother Jones (2020), https://bit.ly/3dcuQjq
47. 18 U.S.C. § 701 (official badges, identification cards, other insignia).
48. 18 U.S.C. § 1017 (government seals wrongfully used and instruments wrongfully sealed).
49. Testimony of Lawrence Norden. Election Security. Committee on House Administration, May 8, 2019. https://www.brennancenter.org/sites/default/files/analysis/Lawrence%20Norden%202019%20Congressional%20Testimony%20on%20Election%20Security.pdf

Auditing Ranked Voting Elections with Dirichlet-Tree Models: First Steps*

Floyd Everest[1 [0000−0002−2726−6736]], Michelle Blom[2 [0000−0002−0459−9917]], Philip B. Stark[3 [0000−0002−3771−9604]], Peter J. Stuckey[4 [0000−0003−2186−0459]], Vanessa Teague[5,6 [0000−0003−2648−2565]], and Damjan Vukcevic[1,7 [0000−0001−7780−9586]]

[1] School of Mathematics and Statistics, University of Melbourne, Parkville, Australia
[2] School of Computing and Information Systems, University of Melbourne, Parkville, Australia
[3] Department of Statistics, University of California, Berkeley, CA, USA
[4] Department of Data Science and AI, Monash University, Clayton, Australia
[5] Thinking Cybersecurity Pty. Ltd., Melbourne, Australia
[6] The Australian National University, Canberra, Australia
[7] Melbourne Integrative Genomics, University of Melbourne, Parkville, Australia
damjan.vukcevic@unimelb.edu.au

Abstract. Ranked voting systems, such as instant-runoff voting (IRV) and single transferable vote (STV), are used in many places around the world. They are more complex than plurality and scoring rules, presenting a challenge for auditing their outcomes: there is no known risk-limiting audit (RLA) method for STV other than a full hand count.
We present a new approach to auditing ranked systems that uses a statistical model, a Dirichlet-tree, that can cope with high-dimensional parameters in a computationally efficient manner. We demonstrate this approach with a ballot-polling Bayesian audit for IRV elections. Although the technique is not known to be risk-limiting, we suggest some strategies that might allow it to be calibrated to limit risk.

In *ranked voting*, voters rank candidates in order of preference; some elections require a complete ranking, others allow partial rankings. Counting the votes can be complex, e.g. involving potentially long sequences of eliminations of candidates (for IRV), and transfers of weighted votes between candidates (for STV).

Complexity arises in two ways: (i) a very large number of ways to fill out a ballot ($k!$ ways to rank k candidates); (ii) the social choice functions are sensitive, small changes can sometimes drastically alter the outcome. This poses a challenge for auditing: we require statistical inference in a very high-dimensional parameter space, for a function prone to erratic behaviour.

RLAs have been developed for some ranked voting systems: (i) IRV elections [1]; (ii) 2-seat STV elections [2]. Both RLAs project into lower dimensions, where

* We thank Ronald Rivest for many helpful suggestions for improving the paper. This work was supported by the University of Melbourne's Research Computing Services and the Petascale Campus Initiative; and by the Australian Research Council (Discovery Project DP220101012).

statistical testing is tractable. However, their projections typically capture only a subset of elimination sequences that lead to the winner. If the true sequence is not one of those, but leads to the same winner, then the audits will usually (and unnecessarily) escalate to a full count despite the reported winner being correct.

Thus, there is scope for further development for ranked systems. For IRV we seek a method that can work with a more complete set of elimination sequences, and for STV we want to be able to audit elections with more than 2 winners.[8]

We tackle the problem directly as a Bayesian audit [6]. This is challenging in high-dimensions; a previous attempt [3] gave up on fitting a full model and instead used a bootstrap approach (equivalent to a degenerate Bayesian model).

Our contribution is a new specification of the statistical model that works efficiently in high-dimensions, making Bayesian audits possible for ranked voting elections. We demonstrate this with examples of auditing IRV elections.

1 Dirichlet-tree model for ranked voting

An audit involves calculating the evidence in favour of the reported outcome using a sample of ballots and a statistical model. For ranked voting, the natural model is multinomial: each ballot type (ranking of the candidates) occurs with some (fixed but unknown) frequency across all ballots.

A Bayesian audit can work with this model directly, by specifying a prior distribution on the ballot probabilities. Given a sample of ballots, we obtain a posterior distribution for these probabilities, which induces a posterior distribution on the winner(s). If the reported outcome exceeds some desired posterior probability threshold, we stop the audit, otherwise we sample more ballots.

For a multinomial model, a typical choice of prior is a Dirichlet distribution. This is conjugate, allowing convenient and efficient implementation. It is defined by concentration parameters, $a_i > 0$, for each ballot type $i \in \{1, 2, \ldots, K\}$. The posterior is Dirichlet (by conjugacy) with concentration parameters $a_i + n_i$ after observing n_i ballots of type i. To make the prior candidate-agnostic: $\forall i, a_i = a_0$ for some a_0. Setting $a_0 = 1$ gives a uniform density on the space of probabilities.

This model behaves poorly as K grows very large. If we set $a_0 = 1$, the prior becomes very informative: it will swamp the data, making the posterior converge very slowly. If we set a_0 much smaller, for example $a_0 \approx 1/K$, then the posterior will strongly concentrate on the ballot types observed in the sample, approximating a 'bootstrap' method. This will likely understate the uncertainty. It will also be challenging to implement, with values of $1/K$ being smaller than typical machine precision once there are about 30 candidates.

To overcome these issues, we propose using a Dirichlet-tree prior distribution (e.g. [5]).[9] This is a set of nested Dirichlet distributions with the nesting described by a tree structure. It generalises the Dirichlet while retaining conjugacy with the multinomial. The nesting divides up the space, allowing efficient inference in high dimensions.

[8] E.g., Australian Senate elections use STV to elect up to 12 candidates for each state.
[9] Our implementation is available at: https://github.com/fleverest/elections.dtree

The tree structure we propose follows the preference ordering: the first split in the tree has a branch for each possible first preference (one branch per candidate), the next split has a branch for each possible second preference (amongst remaining candidates), etc. Partial ballots are modelled by 'termination' branches. To initialise the prior, we set the concentration parameter for each branch to be equal to a_0; see Figure 1 for an example with no partial ballots.

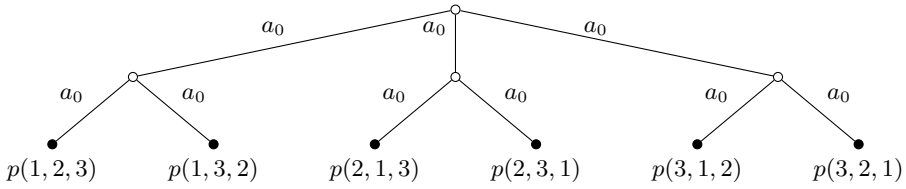


Fig. 1. Dirichlet-tree prior for ranked voting ballots with 3 candidates.

2 Ballot-polling Bayesian audits of IRV elections

We demonstrate our model using data from two elections of different sizes: (i) Seat of Albury, NSW 2015 lower house elections, Australia [5 candidates; 46,357 ballots]; (ii) San Francisco Mayoral election 2007 [18 candidates; 149,465 ballots].[10] The latter has more than $18! \approx 6.4 \times 10^{15}$ possible ballot types.

We used a Dirichlet-tree prior that allows partial ballots and had $a_0 = 0, 1, 10, 100$. We also used a Dirichlet prior with a_0 set such that its prior variance, for an arbitrary complete ballot, matched that of the corresponding Dirichlet-tree prior. Setting $a_0 = 0$ for either prior gives a 'bootstrap' audit [3].

For each election, we simulated 100 audits by randomly permuting the ballots (without introducing any errors). We took samples of up to 200 ballots for Albury and up to 50 for San Francisco, which was sufficient to illustrate the differing behaviour of the priors. At each point in the audit, we estimated posterior probabilities by taking the mean of 100 draws from the posterior.

Figure 2 shows how the posterior probability for the true winner evolved as the samples increased. The Dirichlet-tree model worked for both elections and responded to a_0 as expected: increasing it made the prior more informative and hence respond more slowly to data. The Dirichlet model behaved similarly when we had only a few candidates (Albury) but unstable when we had many (San Francisco), with all choices except the bootstrap ($a_0 = 0$) being too informative.

The bootstrap was erratic at the start (a wide range of posterior values) and stabilised once the sample was big enough. In practice, the poor regularisation at the start would lead to increased risk. Whether this can be curbed by simply specifying a minimum sample size is worth investigating in general.

[10] Data source: https://github.com/michelleblom/margin-irv

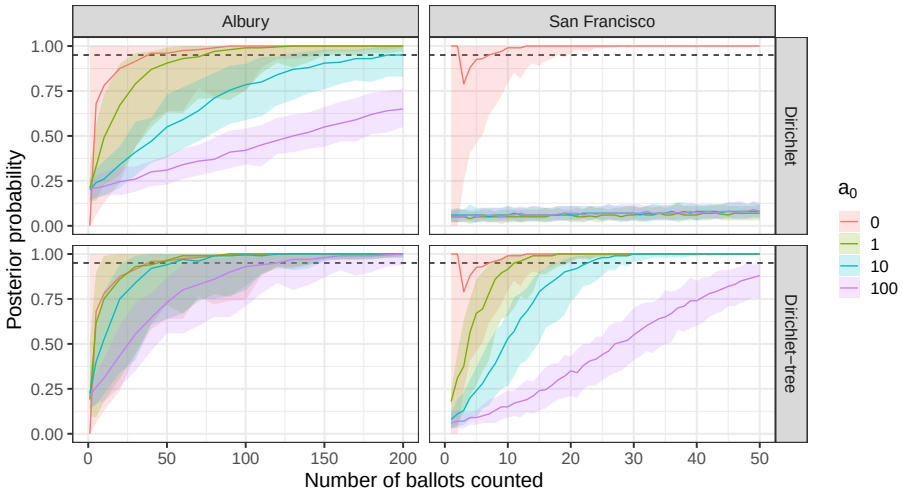


Fig. 2. Distribution of the posterior probability for the winner, vs sample size. The lines show the median across 100 simulated audits, the corresponding bands shade the values between the 5% and 95% quantiles. The dashed line shows a posterior probability of 0.95, for reference. The a_0 values refer to the Dirichlet-tree prior; for the Dirichlet a 'corresponding' value was chosen (see main text).

3 Discussion

We have demonstrated a statistical model that allows efficient ballot-polling Bayesian audits of ranked voting elections. While our example was specifically for IRV, the model can be applied to any ranked voting election by simply changing the social choice function in the calculation of the posterior distribution. Furthermore, the tree structure can be adapted to better suit specific features of particular elections, which should improve efficiency.

A current limitation of our approach is that it cannot be used to run an RLA. This requires an easy way to compute or impose a risk limit. We propose two ways to overcome this: (i) determine the maximum possible risk by deriving the worst-case configuration of true ballots, such as was done for 2-candidate elections [4]; (ii) use a prior-posterior ratio (PPR) martingale [7] to make an RLA using the Dirichlet-tree model. Another limitation is that our approach currently only supports ballot-polling audits. Adapting it to allow other types of audits, such as comparison audits, is another important avenue for future work.

References

1. Blom, M., Stuckey, P.J., Teague, V.: RAIRE: Risk-limiting audits for IRV elections. arXiv:1903.08804 (2019), Preliminary version appeared in Electronic Voting (E-Vote-ID 2018), Springer LNCS 11143.
2. Blom, M., Stuckey, P.J., Teague, V., Vukcevic, D.: A first approach to risk-limiting audits for single transferable vote elections. arXiv:2112.09921 (2021)

3. Chilingirian, B., Perumal, Z., Rivest, R.L., Bowland, G., Conway, A., Stark, P.B., Blom, M., Culnane, C., Teague, V.: Auditing Australian Senate ballots. arXiv:1610.00127 (2016)
4. Huang, Z., Rivest, R.L., Stark, P.B., Teague, V.J., Vukcevic, D.: A unified evaluation of two-candidate ballot-polling election auditing methods. In: Electronic Voting. Lecture Notes in Computer Science, vol. 12455, pp. 112–128. Springer, Cham (Sep 2020). https://doi.org/10.1007/978-3-030-60347-2_8, Preprint: arXiv:2008.08536
5. Minka, T.: The Dirichlet-tree distribution. Tech. rep., Justsystem Pittsburgh Research Center (July 1999), https://www.microsoft.com/en-us/research/publication/dirichlet-tree-distribution/
6. Rivest, R.L., Shen, E.: A Bayesian method for auditing elections. In: 2012 Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE '12) (2012)
7. Waudby-Smith, I., Ramdas, A.: Confidence sequences for sampling without replacement. In: Advances in Neural Information Processing Systems. vol. 33, pp. 20204–20214. Curran Associates, Inc. (2020), https://proceedings.neurips.cc/paper/2020/file/e96c7de8f6390b1e6c71556e4e0a4959-Paper.pdf, arXiv:2006.04347

Return Codes from Lattice Assumptions*

Audhild Høgåsen and Tjerand Silde

Department of Mathematical Sciences
Norwegian University of Science and Technology
audhildh@stud.ntnu.no, tjerand.silde@ntnu.no

Abstract. We present an approach for creating return codes for lattice-based electronic voting. For a voting system with four control components and two rounds of communication our scheme results in a total of 2.3 MB of communication per voter, taking less than 1 s of computation. Together with the shuffle and the decryption protocols by Aranha et al. [1,2], the return codes presented can be used to build a post-quantum secure cryptographic voting scheme.

Keywords: Lattice Cryptography · Return Codes · Electronic Voting

1 Introduction

In 2019, Switzerland put their electronic voting project on hold after having run electronic voting trials for 15 years. Now, electronic voting trials with a new and improved protocol [6] are in the planning. The new protocol offers individual and universal verifiability. Individual verifiability is achieved by using return codes, giving each voter a confirmation that the correct vote was registered by the system. The protocol does not assume a trustworthy voting server but does assume that at least one so-called control component is trustworthy.

The protocol [6] is based on discrete log-type assumptions, whose security could in a decade or two be broken by quantum computers. This is not only a future threat of integrity, but also a threat of privacy of votes cast today.

We present a lattice-based voting phase suitable for electronic voting with return codes, extending the framework by Aranha et al. [1,2]. While [1] includes return codes, but assumes a trustworthy voting server, [2] allows for an untrustworthy voting server, but does not include return codes. We fill this gap.

2 Lattice-Based Building Blocks

Let $R_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle$ where N a power of 2, and $p << q$ primes. We recall the setup in [2, Sec 3].

BGV Encryption [4] of message $m \in \mathbb{Z}_p^N$ with public key $\mathsf{pk} = (a, b) = (a, as+pe)$ with short uniform secret key $\mathsf{sk} = (s, e)$ is computed with short uniform r, e', e'':

$$c = \mathsf{Enc}(m, \mathsf{pk}) = (u, v) = (ar + pe', br + pe'' + m) \tag{1}$$

* This short paper is a compressed version of the master thesis of Audhild Høgåsen, which is available at ntnuopen.ntnu.no and tjerandsilde.no/academic.

Commitments [3] to messages $m \in R_q$ are computed with public matrices $A_1 = \left[I_n \; A_1' \right], A_2 = \left[0^{\ell \times n} \; I_\ell \; A_2' \right]$ where A_1' and A_2' are sampled uniformly random and a short uniform random vector d in the following way:

$$[\![m]\!] = \mathsf{Com}(m, d) = (c_1, c_2) = (A_1 d, A_2 d + m) \tag{2}$$

The described ciphertexts and commitments are additively homomorphic.

Zero-Knowledge Proofs are used to prove properties of commitments without revealing the openings. π_{LIN} [2, Sec 3.3] proves a linear relation $\alpha_1 m_1 + \cdots + \alpha_n m_n = \alpha_{n+1}$ with respect to commitments $[\![m_1]\!], \ldots [\![m_n]\!]$ and public scalars α_i. π_{AEx} [2, Sec 3.4] is an amortized exact proof of short openings. π_{NEx} [5, Section 5.2] is a proof of bounded opening. All these zero-knowledge proofs are proved secure in the random oracle model, but not in the quantum random oracle model.

3 The Swiss Post Voting Protocol

The Swiss Post Voting Protocol [6] is a return code-based electronic voting protocol. The voting phase consists of a SendVote protocol and a ConfirmVote protocol, with the following parties: voter (V), voting client (VC), voting server (VS) and several return code control components (CCR). The voter receives in advance of the election a voting card including return codes cc for each possible voting option of the election and a confirmation return code VCC. The setup and printing component making the voting cards are assumed to be trustworthy. It is assumed that at least one control component is trustworthy and that at least one honest auditor verifies the results using a trustworthy verifier. The voting client is trusted for privacy. $\mathsf{EL_{pk}}$ is the public election key. The SendVote Protocol shown in Figure 1 consists of the following steps:

1. V enters to VC the start voting key k from the voting card and selects voting options v corresponding to return codes cc.
2. VC computes the ballot b containing the encrypted vote ρ and encrypted partial return codes pCC. VC sends b to VS which forwards to CCR. Both verifies the ballot. CCR conducts a distributed decryption to retrieve pCC.
3. CCR generates return code shares $\mathsf{lCC_j}$ and sends them to VS.
4. VS combines the shares from CCR. With a mapping table it extracts return codes $\mathsf{cc}^\star$ that are sent to VC and shown to V.
5. V verifies $\mathsf{cc}^\star$ shown on the screen by checking that they are equal to cc.

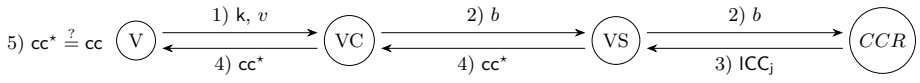


Fig. 1. The SendVote protocol of the Swiss Post Voting System [6, Figure 21].

In step 2, VC maps the selected voting options v of the voter to encodings $\{p_i\}$, then computes the vote $\rho = \prod p_i$ and the partial return codes $\{\mathsf{pCC}_i\} = \{p_i^k\}$. VC computes b consisting of two ciphertexts: an ElGamal encryption of

ρ using $\mathsf{EL}_{\mathsf{pk}}$ and a multi-recipient ElGamal encryption of $\{\mathsf{pCC}_i\}$ using the public key of CCR. b also includes one additional ciphertext and zero-knowledge proofs of correct exponentiation and of plaintext equality, proving that the initial ciphertexts were computed correctly, leaving no options for an untrustworthy VC to compute the two ciphertexts using different vote encodings $\{p_i\}$. Finally, b includes the identity of the voter and a signature [6, Sec 12.2.1.2].

In step 3, each component of CCR computes a return code share $\mathsf{ICC}_\mathsf{j} = \mathcal{H}(\mathsf{pCC})^{\mathsf{k}_\mathsf{j}}$ using a hash function and a secret user-specific key, and provides a zero-knowledge proof of correct exponentiation [6, Sec 12.2.1.6].

The ConfirmVote protocol [6, Sec 12.2.2] is only initiated by V if the verification from SendVote step 5 is successful. The steps of ConfirmVote are similar to the steps of SendVote. V types another key k' from the voting card. VC sends a confirmation key $\mathsf{CK}=(\mathsf{k}')^k$ to CCR. The CCR components compute shares $\mathsf{ICC}_\mathsf{j}{}' = \mathcal{H}(\mathsf{CK})^{\mathsf{k}'_\mathsf{j}}$ and a zero-knowledge proof of exponentiation. VS computes $\mathsf{VCC}^\star$ using the shares and a mapping table. Only after successfully verifying $\mathsf{VCC}^\star$ by comparing it with VCC from the voting card, V has completed the voting process.

We observe that in the ConfirmVote phase, VC gives no exponentiation proof for the computation of the confirmation key. An incorrect exponentiation would result in an unsuccessful confirmation attempt, but could not change the vote. The VC can always block the communication from the voter, thus an exponentiation proof would not change the security analysis.

4 Our Voting Protocol

Cryptographic primitives based on discrete log-type assumptions are used in the Swiss Post voting protocol [6] in steps 2 and 3 of the SendVote protocol of Figure 1, and similarly for the ConfirmVote protocol. The hash-functions used are considered post-quantum secure.

For privacy, the partial return codes are the weakest part of the protocol [6] as they are based on the ESGSP assumption. In the protocol we present, these partial return codes are uniformly random and therefore not an issue for long-term privacy. Still, these partial return codes must somehow be linked to the encrypted vote to avoid attacks from a cheating voting client. The ZK-proofs needed must be post-quantum secure to achieve long-time privacy. Therefore, when constructing a post-quantum secure voting system, we need to consider the voting phase as well, not only the tally phase as already described by [2].

Figure 2 presents a SendVote protocol using primitives based on lattice assumptions. In our protocol, VC does not encrypt the partial return codes pCC as the protocol security reductions for privacy [6, Sec 19.4] omit this encryption (but it could, if required). Commitments and shortness proofs to the polynomials k, k', k_j and k'_j are public information. The vote ρ is a bit-string which represents the voting options v chosen by V. There is a natural mapping from bit-strings to polynomials in R_q with coefficients modulo $p = 2$.

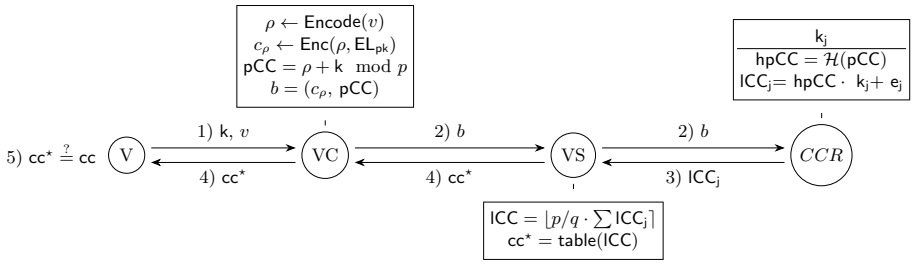


Fig. 2. Our SendVote protocol for lattice-based electronic voting.

In step 2, when VC computes $\mathsf{pCC} \mod p$, this might produce some computational overflow which is stored in a secret overflow binary vector z. VC computes commitments to z and to the randomness used in c_ρ. A proof π_{LIN} proves correct computation of pCC by proving that $\mathsf{pCC} + 2\ z = \rho + \mathsf{k} \mod q$. Proofs π_{LIN} prove correct computation of c_ρ as in Equation (1). A proof π_{AEx} proves that z and the randomness used in c_ρ are binary. Together, these proofs leave no options for an untrustworthy VC to compute c_ρ and pCC with different values of ρ or too much noise.

In step 3, each CCR component computes $\mathsf{ICC_j}$, a commitment to the added noise $\mathsf{e_j}$, a proof π_{LIN} proving that $\mathsf{ICC_j}$ was computed correctly with respect to hpCC, and a proof π_{NEx} proving that the noise value is bounded.

For the ConfirmVote protocol, VC computes $\mathsf{CK} = \mathsf{k}' + \mathsf{k} \mod p$. Each CCR component computes $\mathsf{ICC_j}' = \mathcal{H}(\mathsf{CK}) \cdot \mathsf{k_j'} + \mathsf{e_j'}$, a commitment to $\mathsf{e_j'}$, and proofs π_{LIN} and π_{NEx}.

5 Performance

We use equations, parameters and computed values from [2]. Sizes of ciphertexts, commitments, π_{LIN} are found in [Table 3]. The size of π_{AEx} for binary secrets and τ commitments is computed to $(443 + 6.3\tau)$ KB by [Equation 2] with parameters from [Sec 7.4]. The size of π_{NEx} for only one commitment proving that both the randomness and the message is computed correctly is estimated to 30 KB using [5, Section 5.2] with Gaussian standard deviation for one-time commitments like in [Table 1]. Timings of cryptographic operations to encrypt and commit are found in [Table 4]. Protocol timings from [Table 5] are given for an input of 1000 commitments. We use the given timings of π_{LIN} and assume the timings of π_{NEx} are at most the given timings of π_{ANEx}. By contacting the authors of [2] we received the following timings for an input of 10 commitments: 90τ ms for π_{AEx} and 60τ ms for π_{AExV}.

For the SendVote protocol, VC computes 1 ciphertext, 5 commitments, π_{LIN} for 8 commitments, and π_{AEx} for 5 commitments. Each CCR component computes 1 commitment, π_{LIN} for 2 commitments, and π_{NEx} for 1 commitment. For the ConfirmVote protocol, each CCR component computes 1 commitment, π_{LIN} for 2 commitments, and π_{NEx} for 1 commitment.

For the SendVote protocol we achieve 1095 KB of communication from VC, and 145 KB from each CCR component. For the ConfirmVote protocol we achieve

another 145 KB from each CCR component. As a concrete example having four CCR components the total communication size of the two round voting phase is 2.3 MB.

For the SendVote protocol we achieve timings of 498 ms for VC and 404 ms for each CCR component, computing in parallel, including verifying the proofs from VC. This results in total timings of 902 ms. For the ConfirmVote protocol we achieve timings of 65 ms for each CCR component.

The estimates of communication sizes and timings are meant to give an indication of the performance of the presented protocol, and not an exact performance of an actual implemented system. The waiting time for V until return codes are shown could be reduced if VC starts computing commitments and proofs while V is typing the voting options. We emphasize that the waiting time is not only dependent on the timing of the cryptographic operations, but would in practice be dominated by human operations and network-latency. Among the cryptographic operations, the proofs of exact shortness are the most expensive, both in terms of size and timings. Because exact proofs keep the overall parameters of the system low, they are to be preferred over relaxed proofs of boundedness. We expect that future work on more efficient lattice-based zero-knowledge proofs of exact shortness will improve the concrete efficiency of our protocol.

Acknowledgements

We thank Diego F. Aranha for providing timings of the underlying protocols.

References

1. Aranha, D.F., Baum, C., Gjøsteen, K., Silde, T., Tunge, T.: Lattice-based proof of shuffle and applications to electronic voting. In: CT-RSA (2021)
2. Aranha, D.F., Baum, C., Gjøsteen, K., Silde, T.: Verifiable mix-nets and distributed decryption for voting from lattice-based assumptions. Cryptology ePrint Archive, Report 2022/422 (2022), https://ia.cr/2022/422
3. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More efficient commitments from structured lattice assumptions. In: International Conference on Security and Cryptography for Networks. Springer (2018)
4. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (2014)
5. Lyubashevsky, V.: Basic lattice cryptography: Encryption and fiat-shamir signatures (2019), https://drive.google.com/file/d/1JTdW5ryznp-dUBBjN12QbvWz9R41NDGU/view
6. SwissPost: Protocol of the swiss post voting system – computational proof of complete verifiability and privacy – version 0.9.11 (2021), https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/97c83a77c9ebda4c3a47fca022c60cbcb006d452/Protocol/Swiss_Post_Voting_Protocol_Computational_proof.pdf

Dubious security practices in e-voting schemes
Between tech and legal standards

Tamara Finogina, Adrià Rodríguez-Pérez, and Jordi Puiggalí

Scytl Election Technologies, S.L.U., 08021, Barcelona, Spain
{tamara.finogina, adria.rodriguez, jordi.puiggali}@scytl.com

Abstract. Remote electronic voting has been around for a few decades now. However, some legal uncertainty regarding its uses remains. In this paper, we would like to highlight and discuss several techniques used in e-voting which may not be fully compliant with the law. We analyze several e-voting practices that rely on the addition of dummy ballots and show how they conflict with legal standards. Specifically, we focus on cases where dummy ballots are required for: better performance, testing, participation privacy, or preventing coercion. We argue that these practices may raise issues with the standards of authenticity and eligibility, as well as with the principle "one voter, one vote". Our research aims to offer a better understanding of how legal principles can be interpreted to ensure the legality of technological proposals in e-voting.

1 Introduction

Electronic voting is not a novel idea. It has been a topic of intense research for a few decades and has a history of successfully performing legally-binding elections [10,15,29]. Yet, the ambiguity in some legal aspects remains up to this day [9,18,30]. While it is true that the electoral procedure is, indeed, underspecified for electronic voting, some legal principles are channel-agnostic.

In this paper, we would like to highlight the problematic nature of including dummy ballots in the ballot box, commonly employed by e-voting schemes for fighting correction, optimizing tally, and testing. More specifically, we look into the casting of test votes in some Canadian municipalities, the optimization of some e-voting mix-nets, participatory privacy as suggested in the Helios-null scheme, and coercion-resistance mechanisms proposed in Selene II.

Through the paper, we focus only on basic requirements that are not likely to change in the future: equal suffrage, eligibility, and authentication. While it is true that the law might change, we look at legal principles that are likely to stay stable over time. It is important that electronic voting systems are designed with legal principles and requirements in mind

instead of designing systems first and then trying to fit them into pre-existing regulations.

With this work, we aim to encourage the consideration of electoral requirements in the early stages of e-voting solution development to facilitate its use in practice. We hope that it will help to re-evaluate the merit of some decisions and, perhaps, lead to better e-voting scheme designs.

Paper structure: In section 2, we briefly explain different scenarios leading to dummy votes addition to the ballot box. Then, in section 3, we recall general and national legal standards and discuss possible conflicts. After that, in section 4, we propose some recommendations and conclude our paper in section 5.

2 Addition of dummy ballot to the ballot box

In traditional elections, it is illegal to insert ballots of non-eligible voters (including empty or invalid ones) into a ballot box (i.e., ballot box stuffing) [6]. Yet many e-voting schemes add dummy votes to the ballot box for various reasons. By dummy votes, we mean any ballot that is stored in the ballot box during the election but not included in the election result: e.g., vote containing encryption of zero, vote used for testing the system, votes pre-added to the ballot box, etc.

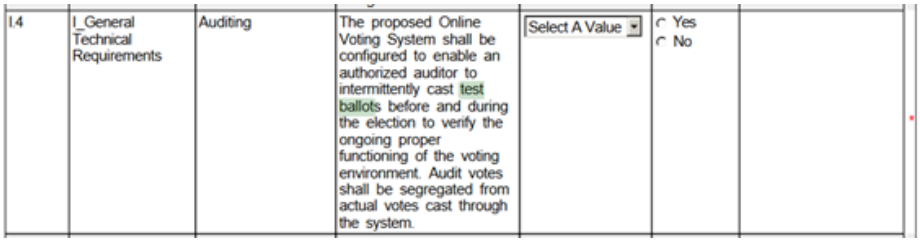
Usually, the goal of the dummy ballot addition is to hide that a voter voted or re-voted, facilitate the optimizations of cryptographic schemes (e.g., Mixing), enhance privacy, or perform an election audit. Typically, e-voting schemes claim that such votes are easily detectable and thus are in line with electoral principles and requirements. However, it is not as simple as it might appear.

In this section, we briefly explain how exactly different e-voting schemes utilize dummy ballots.

2.1 System audit during the election

Casting audit ballots during the election is a functionality required by some Election Management Bodies on their requirements when searching for an Internet voting solution (e.g. Figure 1). Examples are some of the Ontario Municipalities in Canada, such as the City of Markham [25] and the City of Vaughan [26]. In both cases, they request the possibility for auditors to cast test/audit ballots before and during the election to verify the proper behavior of the system. The audit ballots must be segregated

from valid ones to avoid their (audit ones) inclusion in the election results. Additionally, the system should provide reports for both audit and regular ballots to allow auditors to check if the audit vote's content corresponds to the intended one, thus ensuring the accuracy of the system.



I.4	I_General Technical Requirements	Auditing	The proposed Online Voting System shall be configured to enable an authorized auditor to intermittently cast test ballots before and during the election to verify the ongoing proper functioning of the voting environment. Audit votes shall be segregated from actual votes cast through the system.	Select A Value	○ Yes ○ No	

Fig. 1. Extract from audit ballot requirement on City of Markham RFP.

The main idea behind audit ballots is that the voting system provides special voting credentials for auditors that allow them to cast audit votes in the same voting system used by voters during the election period. That way, audit votes are not only cast in the same environment used by the voters but also stored in the same ballot box. Therefore, if there is something not properly implemented in the voting system or the voting system misbehaves, this could be detected by the auditors during the voting (e.g., there are missing or incorrect voting options) or counting (the contents of the audit votes are not the same as the ones cast by the auditors) phases. It is relevant in this requirement that the system is exactly the same one used in production used by the voters. Therefore, standard practices in IT systems such as: using pre-production environments to avoid testing in production are not valid in this case.

To allow audit ballots, auditors need at least one credential for casting an audit vote. However, it also is required that these audit votes must be distinguishable from the valid ones to avoid compromising election integrity (i.e., altering the election results). That means audit votes should include some information or mark that will allow to isolate them from the counting process. For this purpose, we can distinguish two different approaches: one is to permit identifying votes in the ballot box at any time of the election (i.e., during the voting process), and the other is to do the same but in the counting process only.

If votes are identifiable at any time (for instance, if they have a tag in the envelope [1] or correspond to the auditor credential), anybody can distinguish them at any step of the voting process. While this provides complete transparency on the type of vote, it limits the audit capabilities mainly to errors in the election configuration or on the behavior of the voting system. For example, an auditor who wishes to detect attacks focused on manipulating the election cannot do so since the attacker can identify the audit votes and hide attacks. For this reason, the alternative approach is to keep secret the mechanism that identifies audit votes from the valid ones during the voting process.

Mechanisms that hide the difference between audit and regular votes until the counting process is over require the audit votes to look like any other vote cast by any eligible voter. Therefore, attackers cannot identify an audit credential from a valid one nor detect a tag specific to auditors.

Using audit ballots implies the following requirements from an election management point of view:

- Provide audit credentials to auditors: to allow them to cast audit votes as if they were valid voters;
- Traceability of cast votes: to avoid that audit votes are not included with the valid ones on the final count.

In addition to distinguishing valid voters from the auditors, we also need to identify which ballot has been cast by these auditors. When auditors are not anonymous, we can easily group the votes with the same audit tag (e.g., with the same identifier in the envelope). When the auditor's identity must remain secret, we cannot use the audit tags; however, we still can rely on the link between cast votes and the credential used to cast them. Standard practice is to encrypt votes before sending them, so we should keep the link to this encrypted vote (envelope) instead of the contents (vote). This approach is similar to postal voting, where the envelope with a vote is inside a second envelope which contains the voter's identity.

However, this traceability requirement should be global, even for valid voters. Therefore, it becomes of paramount importance that Internet voting systems anonymize the encrypted votes (e.g., homomorphic tally or Mixing) before proceeding with decryption and counting.

[1] The envelope tag is an identifier concatenated to the encrypted vote that makes it different from the valid ones, like having an envelope with a specific color for audit votes.

2.2 Mix-net optimizations

The verifiable shuffle is one of the most used anonymization techniques in the tally phase. It allows breaking the correlation between voter identities and decrypted ballots; while simultaneously providing assurance that no vote was modified, omitted, or inserted. Among all verifiable shuffle proposals, the most efficient and famous are Bayer-Groth [3] and Terelius-Wikström [24] proofs.

However, generating and verifying the shuffling proof can be time-consuming, plus it requires a significant amount of memory. Consider the verification of the shuffle proofs for $N = 100000$ ElGamal ciphertexts done by four mix-nodes[2]. Verifying[3] a single Terelius-Wikström shuffle proof requires approximately $9N$ exponentiation, while a single Bayer-Groth proof needs $4N$ [11]. Assuming one modular exponentiation on 3072-bits integers takes about 9 milliseconds, we can estimate verification to roughly take 9 and 4 hours. In terms of poof size, the optimized Byer-Groth proof is by a factor of 50 more compact than Terelius-Wikström proof [3]. Therefore, in practice, implementations aim to optimize the shuffle part.

For example, a Bayer-Groth proof is more compact when the number of messages N is closer to a square [3]. Technically, the proof works for any matrix shape and, in general, has a sub-linear communication complexity. However, the minimal communication complexity $\mathcal{O}(\sqrt{N})$ can be achieved only if we can arrange messages into a square matrix $N = n \times m$ with $m = n$.

Another optimization, applicable to both Bayer-Groth and Terelius-Wikström proofs, was proposed in [24]. The idea is to significantly speed up the proof generation process by splitting it into online and offline phases [31]. In the offline phase, the prover computes a commitment to a permutation matrix and proves it is constructed correctly. It is a costly process, but it can be pre-computed. In the online phase, the prover demonstrates that the committed permutation matrix has been indeed used in the shuffle. The optimization makes the online part several times faster by shifting some of the heavy computations to the offline one. For example, optimized in that manner, Terelius-Wikström proof would have similar to Bayer-Groth proof performance.

The bottleneck, however, is the fact that the number of votes cast in an election is unknown in advance. Even the best statistic does not allow

[2] The example is taken from [11]

[3] To generate the proof, Terelius-Wikström requires $8N$ exponentiations and Bayer-Groth needs $2N \log m$, where $N = m \times n$ [11].

us to foresee how many votes will reach the tally phase. Therefore the practical use of mix-net optimizations is not that straightforward. Some propose to do the pre-computation for a fixed pre-selected number N and then, when finally only X ballots arrived to the mixnet, add $N - X$ trivial messages $(1, 1)$ [12] (e.g., encryption of 1 with randomness 0) to get N ciphertexts and enable the optimization. The justification for adding dummy votes is that they are easy to detect and remove from the final tally.

2.3 Participation privacy

In some cases, the dummy ballots are cast during the voting phase to hide whether a particular voter voted or re-voted. The expectation is that the coercer cannot attribute ballots to a particular voter; hence it cannot tell whether the voter changed the vote or even participated in the election at all.

For example, in the Helios-null scheme [16], the real votes are masked by the null votes cast by posting proxies and other voters. The idea is that anyone may add encryption of 1 to any voter's raw, and voters can update their votes. The addition of dummy null votes creates a constant flow that confuses the coercer. As a result, the scheme provides participation privacy.

To ensure that ballots arrive at unpredictable intervals, Helios-null requires another entity, a posting proxy, to submit multiple null votes on behalf of each voter at random times. Those null votes are indistinguishable from real ones and accepted as valid by the ballot box. For preventing vote modification, each ballot includes disjunctive proof showing that it is either an encryption of 1 or was cast by an eligible voter.

At the end of the election, the final ciphertext of each voter is a product of votes corresponding to the voter. Since the null votes are all encryptions of 1, only the non-null votes influence the tally. If some voters abstained, their resulting ciphertexts are encryption of 1.

2.4 Fighting coercion

Another idea for providing coercion-resistance was proposed in Selene II [23], which enhances the original Selene scheme. Selene relies on assigning tracking numbers to votes for enabling cast-as-intended verification. The voters cast their votes without knowing their tracking numbers just yet. Then all votes are shuffled, decrypted, and published along with corresponding tracking numbers. For performing verification, each voter should

return, and receive the tracking number shares from all Tellers. After that, the voter uses a private key to recover the corresponding tracking number and locate the decrypted vote. In case of coercion, the voter can fake the tracker and point it to any other line in the public ballot box. Because the shares are sent without any proof of origin, the coercer cannot distinguish between real and fake tracker.

The drawback of Selene is that a coerced voter might have the misfortune of choosing the coercer's tracking number. Alternatively, the coercer might falsely claim that it was his tracker. In both cases, the voter might not be confident enough to insist and hide disobedience.

Selene II addresses this issue by providing each voter with a set of personalized fake trackers and fake votes that the voter can use to trick the coercer. The bulletin board will now contain one extra vote per candidate per voter. On the one hand, it assures voters that their fake tracker will not be claimed by someone else. On the other hand, those dummy ballots should be removed before announcing the final tally.

In a nutshell, the idea of the Selene II tracking collision fix is to start an election with a ballot box already containing fake votes related to fake trackers (i.e., the ballot box is not empty). Before the election begins, each candidate already has one vote from each eligible voter. In a sense, each voter votes once for every candidate and twice for the intended selection. Though, the pre-added votes come from authorities rather than the eligible voters. After mixing and decryption, the ballot box contains a mix of real and pre-added ballots, and no one can tell them apart. However, since each candidate received the same number of additional votes, one can easily reconstruct the final tally.

3 Discussion

3.1 (International) standards for e-voting and how to observe them

It is important to evaluate these practices against international standards for democratic elections. In this regard, the techniques describe may need to comply with the principle of equal suffrage.

International standards for e-voting Equal suffrage is a fundamental principle of democratic elections. For example, art. 21 the Universal Declaration of Human Rights (UDHR) states that "[t]he will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and

equal suffrage and shall be held by secret vote or by equivalent free voting procedures" (emphasis added) [27]. Similarly, art. 25 of the International Convention on Civic and Political Rights (ICCPR) states that "Every citizen shall have the right and the opportunity, [...] (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors" (emphasis added) [28].

Comment no. 25 by the Human Rights Committee further develops the requirements in art. 25 ICCPR [13]. When it comes to equal suffrage, it states that "[t]he principle of one person, one vote, must apply, and within the framework of each State's electoral system, the vote of one elector should be equal to the vote of another" [13, §21]. In Europe, the European Commission for Democracy through Law (Venice Commission) has also developed standards from electoral principles. According to the Venice Commission, equal suffrage entails equal voting rights, meaning that "each voter has in principle one vote; where the electoral system provides voters with more than one vote, each voter has the same number of votes" [6]. In a similar fashion, paragraph 7.3 of the Copenhagen Document also says that participating States will provide "equal suffrage to adult citizens" [1].

When it comes to (remote) electronic voting, the only international reference is the Council of Europe's recommendation on e-voting: Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. The understanding of equal suffrage in the Recommendation is based on the Venice Commission's Code of Good Practice in electoral matters [4, §14]. It is summarized as "each voter has the same number of votes, each vote has the same weight and equality of opportunity has to be ensured" [4, §14]. The Recommendation identifies five standards regarding this principal [19, §5-9]:

5 All official voting information shall be presented in an equal way, within and across voting channels.

6 Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result.

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

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

9 The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.

The Explanatory Memorandum to the Recommendation further details these provisions. When it comes to authentication (standard 8), it reads that "[i]n cases where anonymous voting tokens prove that a voter is eligible to vote, identification of the voter may not be required at this point as it has already taken place at an earlier stage, namely when the specific token is assigned to a specific voter" (emphasis added) [4, §43]. Therefore, standard 9 can be linked to eligibility requirements. Eligibility is not defined in standard 9, but standard 18 in the Recommendation reads that "[t]he system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system" (emphasis added) [19, §18]. Here, the Explanatory Memorandum also provides some additional information. It states that "[v]oters and third parties should be able to check that only eligible voters' votes are included in the election result" (emphasis added) [4, §62]. In this regard, a vote is defined as "the expression of the choice of voting option" [19] (and by casting a vote it is understood "entering the vote in the ballot box" [19])

The Explanatory memorandum further develops the standard of "one person, one vote" (standard 9) as well. It sets that "[a]ll votes cast by either electronic or non-electronic voting channels are counted. It should be ensured that only eligible voters' votes are included in the election results" [4, §44]. Regarding the later standard, the Guidelines also provide some additional information. According to the Guidelines, "multiple votes are considered as an attempt to cast more votes than a particular voter is permitted. This risk might arise, for instance, if the voter tries to cast multiple votes him or herself or if another person tries to use the voter's identity in order to vote, in the voter's name, after he or she has voted" [5, §9.c].

Interestingly, the Recommendation does not preclude the possibility of multiple voting. Multiple voting has been introduced in several countries in order to mitigate coercion concerns in uncontrolled environments. The first country to introduce multiple voting was Estonia. In Estonia it is possible to cast several votes online and only the last one counts. Likewise, a voter can decide to cancel any online votes cast under duress by going to a polling station and voting in person. Since the last local elections, a voter can even cancel their e-vote by voting on election day (something

that was not possible before). Other cases where multiple voting has been introduced are Norway [2], and the Åland Islands in Finland [14].

In this regard, the Guidelines on the implementation of the provisions of the Recommendation [5] foresee two different scenarios with multiple voting. In the first scenario, "a voter is allowed to cast an electronic vote multiple times" [5, §9.a]. In the second, "a voter is allowed to cast a vote by more than one voting channel" [5, §9.b]. In both scenarios, is understood that multiple voting can be introduced "as a countermeasure to voter coercion, which remains possible when voting takes place outside a controlled environment" [5, §9.a-9.b].

Equal suffrage in national e-voting regulations

Switzerland: The Annex to the Federal Chancellery Ordinance explicitly states that votes stored in the ballot box must be properly cast:

"If the vote has been cast in conformity with the system, the system stores the vote in the electronic ballot box and informs the voter that the vote has been cast successfully. Votes not cast in conformity with the system are not stored in the electronic ballot box. [...]" [7, 2.6.3]. Later it is also clarified what "cast in conformity with the system means: "A vote is deemed to be cast in conformity with the system only if the client-sided authentication measure used corresponds to a server-sided authentication measure that was adopted and "assigned" to a voter in the preparatory phase of the ballot. The proof must therefore include confirmation that no unallocated authentication certificates for casting votes have been issued. In addition, during preparation for the ballot, the control components or the auditors must have been given corresponding data as the basis for making a comparison. The auditors must ascertain that the number of authentication certificates corresponds to the (official) number of authorised voters."[7, 4.4.6]

Estonia. Estonia is one of the countries where it is possible to cast multiple votes electronically, and even cancel any online vote by voting on paper during the advanced voting period or on election day.

Notwithstanding, there were discussions about the legality of multiple voting. On 12 July 2005, after the Riigikogu adopted the Local Government Election Act, the President of the Republic of Estonia turned to the Supreme Court to declare it unconstitutional. The President referred "in the reasons for his decision to contradictions with the principle of uniformity of local government councils elections stipulated in subsection

256 of the Constitution" [17, p. 19]. However, "[t]he Constitutional Review Chamber of the supreme Court refused to satisfy the application of the President of the Republic", who pursuant to the Constitution was obliged to proclaim the Act [17, p. 20]. The Supreme Court of Estonia justified the constitutionality of e-voting and of multiple voting ruling that "Despite the repeated electronic voting a voter has no possibility to affect the voting results to a greater degree than those voters who use other voting methods. A vote given by electronic means shall be counted as one vote and from the point of view of voting results this vote is in no manner more influential that the votes given by voters using other voting channel" [22].

However, this is not a breach of the principle "one voter, one vote". Legal provisions in Estonia are clear when it comes to ensure the principle of "one voter, one vote". In this regard, art. 48.7 of the Riigikogu elections act states which is the valid vote that should be taken into account when voters have cast more than one ballot: the last vote cast by electronic means [21, 48.7(1)], or any ballot cast on paper, since these take precedence over votes cast electronically [21, 48.7(4)]. Even more interesting, section (5) of this article clearly sets that "If a voter has voted several times outside the voting district of his or her residence, and using electronic means, all envelopes with ballot papers of the voter as well as the vote cast using electronic means shall not be taken into account."

How to observe new voting technologies? One of the limitations of the Recommendation is that it does not specify how compliance with the standards can be ascertained. In this regard, it is more useful to investigate the OSCE/ODIHR's methodologies for the observation of new voting technologies. The methodologies of the OSCE/ODIHR do not set standards as such, but rather "focus on identifying good practices or formalizing procedures. They do not aim at providing an evoting regulation and most of them are domain specific focusing on the needs of election officials, observers and so on."[8, p. 112] Although the OSCE/ODIHR's methodologies are based on the Copenhagen document, we have already seen that it does also include the principle of equal suffrage. More specifically, and according to the Handbook for the Observation of New Voting Technologies, "one of the aspects of the principle of equality is that no voter will be able to cast more votes than another, [...] This means that NVT systems must prevent any person from casting more votes than is established by law and must prevent any votes from being subtracted from the system" [20, §10]. For the OSCE/ODIHR, what can be assessed

to evaluate compliance with secret suffrage are: "What steps are taken to ensure that the electronic memory does not contain any votes prior to the start of voting? Is this verifiable?"[20, 58]

As it is the case for the Council of Europe's Recommendation, these provisions do not prevent the casting of multiple votes. In this regard, it is acknowledged that "[s]ome Internet voting systems allow voters to cast their vote more than once, with the condition that only the last cast vote counts. This helps to reduce the risk of voter coercion and vote buying. Consequently, it must be possible to verify that no violations of the principle of equality have taken place" [20, 10].

3.2 Dubious practices

Therefore, some of the techniques described may not either comply with the standards of authentication; with the standards of eligibility; or with none of them. In what follows we analyze the different practices against these two standards:

Issues with authentication and eligibility For example, mix-net optimizations as suggested by [12] require adding trivial messages to the ballot box. Regardless of the value of these messages, they can clearly be understood as votes cast into the ballot box based on the definitions in the Recommendation. However, the wording of standards 9 and 18 in the Recommendation establish that "only eligible voters' votes have been included in the respective final result" (emphasis added). Since the proposal only adds these votes during the mixing phase, the practice would be compliant as long as they are removed from the final results. The question is therefore how to ensure that those votes are dully deleted before the count.

In Selene II, several votes are cast for all candidates by a non-eligible entity as well. In fact, here the ballot box is not empty at the beginning of the election. The votes are stored in the ballot box until the actual decryption. It is only then that the election authority can subtract the extra votes for all candidates and reveal the actual election result. Therefore, the issue here is what is understood by "final result". Since the output of the decryption is not yet final, it is possible to argue that this system still complies with the international standards.

However, it is evident that this proposal does not satisfy the requirement by the Swiss and Estonian legislation on the validity of votes cast, and neither will they comply with the OSCE/ODIHR's criteria that no votes should be cast prior to the start of voting.

Issues with the principle "one voter, one vote" In the proposal for participation privacy, voters can cast dummy votes on behalf of other votes. This practice seems to breach the standard of "one voter, one vote". Furthermore, and in contrast to multiple voting, here it is not the voter themselves who cast the extra votes to cancel out any vote cast under duress.

Furthermore, the posting proxies also cast votes on behalf of the actual voters. This fact means that not only are more than one vote per voter cast, but that some of these votes are actually cast by proxies who are not eligible in the election. Therefore, their role breaches the two standards that we have identified.

Issues with both principles The proposal to cast audit impacts both standards. On the one hand, having audit credentials translates into additional voters being added to the electoral roll of the election since it is necessary to add auditor credentials. On the other hand, it is possible that an auditor is registered several times as different voters in case they want to make multiple tests or test different contents in the same election.

If it is not necessary to keep the audit credentials secret, the system and the parties involved can be aware of which votes are cast by auditors. However, this could limit the ability to detect attacks. Therefore, the main impact is when the auditors must be indistinguishable from regular voters since auditors should be registered as (fake) eligible ones. The list of the additional audit voters and their related auditors must be kept secret until the voting process ends. Afterward, the list must be made public to allow to distinguish between valid voters and audit ones to isolate audit votes in the counting process and provide real participation statistics.

An alternative to casting audit votes is to allow voters to participate in the validation of their votes cast. That implies adding Individual Verifiability capabilities (cast-as-intended and counted-as-cast) to the voting system. Therefore, it is not necessary to generate audit credentials for auditors or isolate audit votes from valid ones in the ballot box. So it is less intrusive from the vote casting and counting point of view. However, individual verifiability is not a traditional process and therefore, generates other conflicts from the election legislation point of view that must be also evaluated.

4 Recommendations

As a general recommendation, we advise storing in the ballot box only votes cast by eligible voters. This approach would be the most in line with all legal regulations. Moreover, it would prevent the spread of misconceptions regarding e-voting security, which commonly arise in cases of temporal addition of ballots to the ballot box. The general public often remarks that adding values to the ballot box (even if temporary) feels insecure.

Also, the addition of any values (no matter how temporary) unavoidably complicates the tally and audit processes as more ballots should be reviewed and/or anonymized. For example, Selene II would require shuffling significantly more ballots than any other system in similar settings, which would slow down the tallying.

In the case of audit ballots, the separation of audit and valid votes in a ballot box must happen before executing the anonymization and counting. We can do this through a reconciliation process (also known as cleansing) that uses the secret list of audit voters (revealed at the counting phase) to segregate the votes cast from these voters from the valid ones. The list of valid ones is sent through the anonymization and counting process to have the results. The audit votes should be decrypted directly to allow auditors to check if the cast votes indeed contain their selected voting options. In turn, it must be also audited that none of the ballots is included in the final tally

As for the mix-net optimizations, we recommend disabling precomputations and focusing on other optimization techniques.

5 Conclusion

In this paper, we analyzed several e-voting practices that rely on the addition of dummy ballots and showed how they conflict with legal standards, namely: authentication, eligibility, and the principle "one voter, one vote". In our analysis, we considered both international e-voting standards and national regulations. More specifically, we look into the casting of test votes in some Canadian municipalities, the optimization of some e-voting mix-nets, participatory privacy as suggested in the Helios-null scheme, and coercion-resistance mechanisms proposed in Selene II. We have concluded that such practices do not comply with the OSCE/ODIHR criteria or Swiss and Estonian legislations. We also provided some general recommendations that would be in line with regulations. We hope that our

observations and recommendations will facilitate the implementation of electoral requirements in the early stages of e-voting solution development to facilitate its use in practice.

References

1. *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE*, Copenhagen, June 1990. Organization for Security and Co-operation in Europe.
2. Jordi Barrat, Michel Chevalier, Ben Goldsmith, David Jandura, John Turner, and Rakesh Sharma. Internet voting and individual verifiability: the norwegian return codes. In Manuel J. Kripp, Melanie Volkamer, and Rüdiger Grimm, editors, *5th International Conference on Electronic Voting 2012 (EVOTE2012)*, pages 35–45, Bonn, 2012. Gesellschaft für Informatik e.V.
3. Stephanie Bayer and Jens Groth. Efficient zero-knowledge argument for correctness of a shuffle. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 263–280, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.
4. Council of Europe. 2.3 Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) a. Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Committee of Ministers.
5. Council of Europe. 2.3 Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) b. Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting. Committee of Ministers.
6. Council of Europe (Venice Commission). *Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report*. Council of Europe, Strasbourg, 2002.
7. Die Schweizerische Bundeskanzlei (BK). Annex to the FCh Ordinance of 13 December 2013 on Electronic Voting (OEV, SR 161.116). Technical and administrative requirements for electronic vote casting.
8. Ardita Driza Maurer. Ten years council of europe rec(2004)11: Lessons learned and outlook. In Robert Krimmer and Melanie Volkamer, editors, *Proceedings of Electronic Voting 2014 (EVOTE2014)*, pages 111–117, Tallinn, 2014. TUT Press.
9. Ardita Driza Maurer. Legality, separation of powers, stability of electoral law: The impact of new voting technologies. *Electoral Expert Review*, 01 2016.
10. J. Paul Gibson, Robert Krimmer, Vanessa Teague, and Julia Pomares. A review of e-voting: the past, present and future. *Annals of Telecommunications*, 71, 06 2016.
11. Rolf Haenni and Philipp Locher. Performance of shuffling: Taking it to the limits. In *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers*, page 369–385, Berlin, Heidelberg, 2020. Springer-Verlag.
12. Thomas Haines, Olivier Pereira, and Vanessa Teague. Report on the swiss post e-voting system. March 2022.
13. UN Human Rights Committee (HRC). Ccpr general comment no. 25: Article 25 (participation in public affairs and the right to vote), the right to par-

ticipate in public affairs, voting rights and the right of equal access to public service. UN General Assembly, 1996. https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2025.pdf.
14. Robert Krimmer, David Duenas-Cid, Iuliia Krivonosova, Radu Antonio Serrano, Marlon Freire, and Casper Wrede. Nordic pioneers: facing the first use of internet voting in the Åland islands (parliamentary elections 2019). SocArXiv 5zr2e, Center for Open Science, 2019.
15. Robert Krimmer, Stefan Triessnig, and Melanie Volkamer. The development of remote e-voting around the world: A review of roads and directions. In Ammar Alkassar and Melanie Volkamer, editors, *E-Voting and Identity*, pages 1–15, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.
16. Oksana Kulyk, Vanessa Teague, and Melanie Volkamer. Extending helios towards private eligibility verifiability. volume 9269, September 2015.
17. Ülle Madise, Priit Vinkel, and Epp Maaten. Internet voting at the elections of local government councils on october 2005 : Report, 01 2006.
18. Sutton Meagher. When personal computers are transformed into ballot boxes: How internet elections in estonia comply with the united nations international covenant on civil and political rights. *American University International Law Review*, 23, 2007.
19. Council of Europe. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Committee of Ministers.
20. OSCE Office for Democratic Institutions and Human Rights (ODIHR). *Handbook for the Observation of New Voting Technologies (NVT)*. November 2013.
21. Riigikogu. Riigikogu Election Act.
22. Riigikogu. SUPREME COURT OF ESTONIA. Constitutional judgment 3-4-1-13-05. JUDGMENT OF THE CONSTITUTIONAL REVIEW CHAMBER OF THE SUPREME COURT.
23. Peter Ryan, Peter Rønne, and Vincenzo Iovino. Selene: Voting with transparent verifiability and coercion-mitigation. volume 9604, pages 176–192, February 2016.
24. Björn Terelius and Douglas Wikström. Proofs of restricted shuffles. In Daniel J. Bernstein and Tanja Lange, editors, *Progress in Cryptology – AFRICACRYPT 2010*, pages 100–113, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.
25. THE CORPORATION OF THE CITY OF MARKHAM. RFP 079-R-21. Municipal Election (2022) – Supply and Implementation of an Online Voting System with Support and Services.
26. THE CORPORATION OF THE CITY OF VAUGHAN. RFP21-269. Provision of Internet voting services for the 2022 Municipal Election.
27. United Nations. *Universal Declaration of Human Rights*. December 1948.
28. United Nations (General Assembly). International covenant on civil and political rights. *Treaty Series*, 999:171, December 1966.
29. Carlos Vegas and Jordi Barrat. Overview of current state of e-voting worldwide. In Feng Hao and Peter Y. A. Ryan, editors, *Real-World Electronic Voting. Design, Analysis and Deployment.*, pages 51–75, New York, USA, 2016. Auerbach Publications.
30. Priit Vinkel. *Remote Electronic Voting in Estonia: Legality, Impact and Confidence*. PhD thesis, 08 2015.
31. Douglas Wikström. A commitment-consistent proof of a shuffle. In *Proceedings of the 14th Australasian Conference on Information Security and Privacy*, ACISP '09, page 407–421, Berlin, Heidelberg, 2009. Springer-Verlag.

Review of the Overseas E-voting (OSEV) system used in the Australian Capital Territory

Thomas Haines

The Australian National University, Canberra, Australia
thomas.haines@anu.edu.au

Abstract. The Australian Capital Territory (ACT) contains the Australian national capital Canberra; the territory has a 25-member legislative assembly combing both state and local government functions. The members of the assembly are elected using two electronic voting systems. The first, the EVACS system, uses Direct-Recording Electronic voting machines (DREs) to record the vast majority of ballots in physical polling-places. Overseas voters can use the Overseas E-voting system (OSEV) to vote online. In this paper we report on our review of the OSEV system and we also reflect on the transparency of the process by which the system was introduced.

1 Introduction

The Australian Capital Territory (ACT) continues to be one of the most prominent users of electronic voting in Australia. The territory has used the—Direct-Recording Electronic voting machine (DRE) based—Electronic Voting And Counting System (EVACS) since 2001; DRE based systems are not otherwise used in Australia. Building on earlier work on formally analysing voting systems [1,3,13], there has been a string of papers analysing the counting side of the EVACS system. Goré and Lebedeva [12] showed issues in real ACT elections because of errors in the EVACS counting software. This was followed by a paper from Moses et al. [17] called "No more Excuses: Automated Synthesis of Practical and Verifiable Vote-Counting Programs for Complex Voting Schemes" which showed that it was possible to produce verified and verifiable software which could be used to count the ballots in EVACS. In 2018, T Wilson-Brown highlighted important privacy issues in the EVACS system,[1] and in 2020 Conway and Teague demonstrated yet more errors in the counting software.[2] Alas, the ACT Electoral Commission, hereafter referred as the commission, has been reticent to address the issues raised by the academic community.

Despite the issues with the EVACS system, the publication of the source code at least allowed interested parties some ability to scrutinise the system; alas no longer, in the lead up to the 2020 election a new version of the EVACS

[1] https://www.abc.net.au/news/2018-08-14/voters-in-act-election-could-have-ballot-choices-identified/10115670

[2] https://github.com/AndrewConway/ConcreteSTV

system was proposed for use alongside a new online voting system called the Overseas E-voting (OSEV) system. The systems were not publicly available but the commission would, at its discretion, make them available upon the reviewer signing a Non-Disclosure Agreement (NDA). We will discuss the NDA in more detail section 3.3.

At this point, the commission was still insisting publicly (and on its website) that the source code was publicly available. Requests by academics to review the code were answered by saying the code wasn't ready for the review even though voting would be starting the following week. Freedom Of Information (FOI) requests to seek the code and audit specs were delayed because commission said that running an election was an "exceptional circumstance" for them. Finally on the 13th of November 2020, about a month after the election ended (17th October 2020), heavily redacted audit specs were released but access to code still required signing the extremely problematic NDA. In our review that follows we highlight that even the heavily redacted documents that were released were not accurate.

We formally requested access to the source code and offered to sign the NDA in early October 2020. We were notified in mid-February 2021 that the commission had declined our request "because it (was) not satisfied that the risk that the source code may be improperly accessed by others can be appropriately managed." After further discussions, we were finally able to access the source code of the OSEV system in June of 2021.

In the next subsection we will discuss what is publicly known about the OSEV system then the remainder of the paper follows in three sections. First, in Section 2 we detail the scope of the review and the findings. In Section 3, we reflect on the process surrounding e-voting in the ACT and the interplay between that process and the security of the e-voting systems and compare to the recommendations in the literature. Finally, we conclude in Section 4.

1.1 Overview of OSEV system

Public details of the OSEV system are sparse which makes it hard to provide much information without engaging in speculation or violating the NDA we signed. In the remainder of this subsection will summarise the publicly known information about the system and its security requirements.

Sources of information Publicly knowledge of the security goals and system design of OSEV is based upon the following (heavily redacted) documents as released in response to T Wilson-Brown's FOI request:[3]

OSEV Architecture Diagram v1.1
which provides a summary of the various components mentioned later in the report and their interaction [4].

[3] The FOI request can be found at `https://www.righttoknow.org.au/request/vote_secrecy_in_2020_election`

OSEV Authentication Sequence Diagram v0.6.2, OSEV Register Sequence Diagram v0.6.1, OSEV Check Sequence Diagram v0.6.0, OSEV Export Sequence Diagram v0.6.1
which provide summaries of the principal interactions between the various components [5,9,6,8].

OSEV System Design v3.0
which provides an overview of the components and the design goals [11].

OSEV Security Summary v1.4, OSEV Detailed Requirements v1.2
which detail the security requirements the system is designed to achieve [10,7].

In addition our review is based on the source code from version 4cba9731_v1_0_0_prod of the overseas e-voting system; this was made available to us upon signing a non-disclosure agreement. This source code did *not* include any documentation which provided additional insight into the system design or security goals.

Summary of security goals The (unredacted) security goals of OSEV are described vaguely and we summarise them below as they are found in the documents. We note the descriptions in the documents tends to focus on the security mechanism not the security goal.

OSEV System Design v3.0 [11] contains about seven pages of information which not been redacted. Only one page of this document covers design features such as:
- Separation of system components to distribute trust
- Not allowing voter preferences to be linked to a voter
- Vote integrity - the vote should not be tampered with
- Process integrity - the process flow of the election should be followed; for example, ballots should only be accepted if they come from registered voters and during the period that voting is open
- No direct link to existing systems such as the EVACS counting module or the system which stores the list of eligable voters

OSEV Security Summary v1.4 [10] contains about four page of information which has not been redacted. The security features emphasised, in addition to those, described above are:
- No database or storage for the Web and Verify applications to protect vote privacy
- Votes are encrypted in transit and rest
- Decryption keys are not used or stored in the online system to preserve vote privacy and prevent vote tampering

OSEV Detailed Requirements v1.2 [7] contains two pages of unredacted information about half of which pertains to security:
- Information on the use of encryption and signatures
- Only valid votes will be counted
- Requirements on the use of TLS

The main issue with description of the security goals is that no threat model is described. For example, the requirement that only valid votes be counted seems to have been "satisfied" by having the Vote storage application check that the ballots it received match the records kept by the Verify and Check applications. This only works if the vote storage application is trusted for this requirement. Similarly, saying that an application had no database works well for an honest but curious adversary but since the web application in particular is connected to the internet it seems unlikely this would prevent an active adversary from retrieving information from this component.

Summary of system components The system consists of four online components called Check, Verify, Vote storage, and Web application. The system also has a Desktop application and client side code which it serves to the voters' browsers, which we have denoted Web client in the Fig. 1.

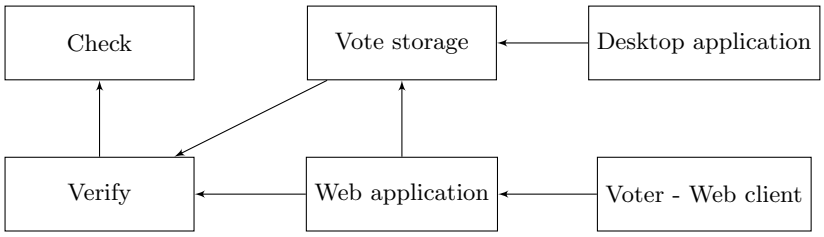


Fig. 1. Overview of components

We have provided in Fig. 1 an overview of the components with arrows denoting dependencies. For example, we denote that Web application as dependent on Verify and Vote Storage because uses the Verify API to check voter eligibility and the Vote Storage API to store votes. Fig.1 can be thought of as a simplified version of the OSEV Architecture diagram [4].

OSEV Web application: The OSEV Web application is the user-facing component of the system. This component mediates the users' interactions with the other components during registration, authentication, and voting as noted in the relevant diagrams [9,5].[4] It is also responsible for providing the web client code to the voter. To mitigate the risk to privacy and integrity of this component being compromised it does not have any storage, beyond its volatile memory; all voter identity and ballot information is stored only in the local variables of function handling the voter's request. It receives ballots from the voter over a TLS connection which it then encrypts using the public key of the OSEV system to ensure that ballots are encrypted in transit and at rest.

[4] The Authentication Sequence Diagram appears to reference a Voting Sequence Diagram which was not released in response to the FOI.

OSEV Web client: The voter uses a browser to register and vote through a website provided by the system. The web site does not directly encrypt the vote but relies upon the TLS protocol to secure the vote in transit to the OSEV Web application were it will be encrypted for storage. The web client is denoted as the voter in the relevant sequence diagrams [9,5].

OSEV Vote storage: The OSEV Vote storage is responsible for storing the ballots collected by the Web application and making them available to the OSEV Desktop application. It performs checks with OSEV Verify to ensure that the Web application does not add ballots from ineligible voters, as noted in the Export Sequence Diagram [8]. The Export Sequence Diagram shows the Vote storage system receiving the RSA private key (which can decrypt the ballots) during export process; this is a direct contradiction with the security requirement that online system not have access to the secret key. Fortunately, when looking at the code we found this was not the case and the private key is kept only on the (offline) Desktop application.

OSEV Verify and OSEV Check: OSEV Verify and OSEV Check are two components which work together to ensure that voters and ballots are authorised [5,9]; they also perform the other checks required to ensure the online part of the election runs in an orderly manner. In essence OSEV Verify serves as a stateless proxy to OSEV Check with the aim of increasing privacy. Together they: register voters for the OSEV system and check their eligibility, provide the ballot "paper" for a given voter, and key track of who has voted.

To provide this service OSEV Check interacts with other election management software outside the OSEV system, this other software is called Tiger in the OSEV Check Sequence Diagram [6]; we were not given details of this other software which hindered making conclusions about these two components.

OSEV Desktop application: The OSEV Desktop application downloads the votes at the end of the election period. These votes are then decrypted using the secret key of the OSEV system before the resulting decryptions are encrypted using the public key of the EVACS system. The encryptions under the EVACS key are added to the other votes which will then be tallied. The OSEV Desktop application, when exporting to EVACS, does not appear to include any information that would allow modifications of the ballots to be detected.

2 Review of the OSEV system

Our review was based on version 4cba9731_v1_0_0_prod of the Overseas E-voting system source code. It also draws upon the documents detailed previously released through a Freedom of Information (FOI) request by T Wilson-Brown. Overall, we find that the code in its current state offers no integrity advantage over a single web application, and little privacy advantage; in other words, the security goal of distributing trust by separating the system components was not

achieved. The security of the system relies upon procedural mechanisms which were not open to scrutiny in the course of this review.

In our review it very quickly became apparent that we were not going to be able to assess the deployed security of the system in detail due to lack of information; specifically, we lacked information about the interaction of the OSEV system with wider election management software and more crucially about the procedural mechanism around it's deployment. We therefore focused our review on assessing the distribution of trust among the system components and the use of cryptography. We did not, and could not, review the procedural mechanisms. Nor did we test exhaustively for the presence of buffer overflows, input sanitation errors, etc. All the findings detailed in this section and the next draw at least partially on the materials subject to the NDA.

2.1 Methodology and Scope

This review is based on 4cba9731_v1_0_0_prod of the Overseas E-voting system source code. The source code was delivered in a compressed file of around 80MB. We did not receive any documentation with the exception of some (outdated) README files.

We scoped our analysis to the code which handled ballots either by encrypting, decrypting, storing, or determining validity. Outside the scope were, in general, all other code. For example, we reviewed the parts of OSEV Verify and OSEV Check used by the Vote storage application when checking which ballots are valid but did not analysis the parts of OSEV Check and OSEV Verify which ensured ballots came from eligible voters. Also outside of scope was the external libraries used by the system.

Our review methodology relied upon manual code review using an IDE, which supported the relevant language. We were unable to build or execute the system as whole; however, we did isolate sections of the code for which we constructed test suites using a common unit testing framework. We assessed the code with respect to integrity and privacy goals of the system, which we summarised in 1.1.

We were unable to assess all procedural mechanisms not contained within the code. For example, the mechanism by which it was ensured that the Web application and OSEV Verify had no access to storage was not in scope.

2.2 Areas of Concern

1. The code and architecture documents show a clear intention to distribute trust over various components. Avoiding a single point of failure is a very desirable property for an e-voting system – some might say a necessary one – but the current system falls short of achieving this on a few points.
   (a) There are single points of failure for both privacy and integrity if a key component is compromised before or during the election, particularly the Web application as we will discuss in point 4.

(b) Several components accept the input of other components without adequate validation, as detailed in the following concerns.

Building a secure distributed system is a challenging task and the electoral commission will need to draw on additional expertise if they wish to achieve this.

2. The code was not in a polished state, which hinders analysis both by external parties and the internal development team. Specifically, the code contained unused legacy material which was hard to distinguish from what was actually relevant. We suggest that comments accompanying the code, including the README document, be kept clean and updated.
3. The version of the source code we were given access to did not meet the requirements listed in the documents released as a result of T Wilson-Brown's FOI request. In one specific instance, we were informed that the requirement had been removed. Assuming that the code we were given reflects the code used in the election on the 17th of October 2020, we are disturbed that documents released in response to the FOI request (on the 13th of November 2020) included requirements which had been removed.
4. The Web application learns the user's identity at registration and the vote when the user votes. It is, therefore, a single point of failure for privacy. The Web application can drop or modify ballots without detection; however, the checks performed by vote storage prevent the Web application from stuffing the ballot box. *The commission has assured us that these attacks are mitigated by procedural mechanisms which are outside the scope of this review and unassessable based on the material made available to us.*
5. The OSEV Web client depends on TLS to safeguard the privacy of the vote. We are concerned that the procedural mechanisms used by the commission, for example to protect against denial-of-service attacks, may allow a third party to read votes in transit. A similar issue occurred in iVote system [2]. *The commission has assured us that there is no attack here but we are unable to verify this without knowledge of the procedural mechanisms in place.*
6. The Vote storage application is a single point of failure for integrity since the Desktop application does not check the consistency of the Vote storage's output with other components.

   The commission initially claimed that no attack on integrity was possible because the Voter storage system did not know the (public) key used to encrypt the votes. We communicated to the commission that knowledge of the (public) key was not required to modify the votes for the encryption scheme they were using. They have now acknowledged the issue and "will work to address it in the future deployments of OSEV." *The commission has assured us that the attack was nevertheless mitigated by procedural mechanisms which are outside the scope of this review.*
7. The Verify and Check applications have been separated from each other, rather than existing as a single component, with the intention of improving privacy. In our judgement, the separation of OSEV Verify from OSEV Check does not appear to meaningfully improve the security of the system. This is certainly the case at present since the Web application is a single point

of failure for privacy already; we suspect this would remain the case even if the most obvious issues are fixed. However, due to the interaction of these components with other systems—which we were not given access to—we are not certain. Further investigation would be required to judge precisely what security is provided by the current separation; such an investigation would be complicated by the lack of a clear and detailed security goal.

2.3 Reflections and Recommendations:

Based on the areas of concern above we made several recommendations to the commission.

Due on our concern about the very under-defined security model, we strongly recommended the commission carefully review the security requirements to ensure that they are satisfied they are sufficient. Given that the commission may lack the capability to adequately do this in-house we encouraged them to seek external advice. Based on the issues currently present in the system, we strongly recommended the commission seek support from members of the public with relevant expertise to ensure they are aware of, and can address, issues with the system.

Following up on our first recommendation and desiring public transparency about the level of security, we encouraged the commission to release an unredacted document which clearly articulates the high level security properties they wish to achieve.

In our final recommendation we were again concerned about public transparency about security, we encouraged the commission to make sufficient information and parts of the system available to public scrutiny, to allow interested members of the public to check that the high level security properties are achieved.

2.4 Review results

The results of our review were released under section 5 of the non-disclosure agreement which allows publication of findings after a certain period. All findings in this report were disclosed to the commission no later than the 10 August 2021.

We have deliberately kept our results section short and avoided specifics as much as possible since our Non-Disclosure Agreement (NDA) says we may not include any part of the source code. We will discuss the NDA in Sec. 3.3 and specifically how we choose what information to try and make public.

Detailed recommendations arising from the review provided to the commission

The OSEV Desktop application should validate the received ballots to the greatest extent possible. Specifically, it should check that the data (encrypted votes) provided by OSEV Vote storage is consistent with OSEV Web application, Verify and Check.

This is will detect attempts by OSEV Vote storage component to tamper with the votes it receives.

Integrity The system should be constructed so that no ballot can be added, modified, or dropped without detection provided at least one component, of the five, is honest (ideally this should also protect against malware on the voter's computer).

Privacy The system should be constructed so that no information (beyond seeing a randomly ordered list of all ballots) is leaked provided the encrypting component and at least one other component is honest. Ideally, encryption should occur on the voter's device; barring this the encrypting component should not have any information about the identity of the voter (other than a token and what could be discerned from the user's connection).

Our second and third recommendations seems to capture the distribution of trust over the components which the high level descriptions of OSEV provided by the commission seem to envision but the system does not achieve. Realising this level of security would require a significant redesign; for example, at present the issues with the Web Application component seem to be unsolvable without introducing a cast-as-intended mechanism to the system.

Detailed comments on the documentation after reviewing the source code

- The documentation, and specifically requirement OSEV64 (from OSEV Detailed Requirements), requires that votes are signed by the Web application, but we could find no evidence of this occurring.

  In response to our report on this matter, the commission notified us that this requirement was actually removed. The given justification for removing the requirement was that the asymmetric encryption, of the votes, made this unnecessary. We are unsure when the requirement was removed but given that the asymmetric encryption does not prevent vote tampering we strongly recommend the commission reintroduce this requirement.
- Comment 3.a in the OSEV System Design document which appears under the section "Vote Integrity" says "Vote preferences cannot be read by an unauthorised party because they are encrypted using an RSA asymmetric algorithm so that they can only be decrypted by a key not stored by the system and instead held by Elections ACT." relates to privacy rather than integrity. The general confusion about basic security properties evidenced by the vendor and commission is a central reason why we conjecture the lack of transparency is likely to hide further vulnerabilities.

  In general it seems that several components could add, edit, or drop votes without detection; as we detailed in Sec. 2.2. We do not preclude that there are other mechanisms, which might catch the tampering, of which we are unaware. However, in the scope of the documents released, the integrity of the system is at best poor unless all components are behaving properly.

3 Reflections on the process

Two recent papers [14,16] by Haenni et al. and, Haines and Rønne comment on best practice for processes around e-voting systems. Below, we list selected best practices and contrast to the processes around the OSEV system. We have done this because we conjecture that specific vulnerabilities, like those we listed in the previous section, are symptoms of poor processes; we further conjecture that focusing on improving the processes is the best way to deliver secure systems. We cannot test this conjecture in this paper alone but our hope is that if papers like ours report not only vulnerabilities but also issues with processes then in several years we should have sufficient data to assess the claim.

3.1 Selected principles from CHVote: Sixteen Best Practices and Lessons Learned

Modelling the Electoral Systems The first principle is the importance of properly modelling the electoral system; this is required to provide a proper level of abstraction of the electoral process when designing the voting protocol.

The fact that ACT elections are for a single race, with the occasional exception of a referendum, makes creating a model of the election system relatively straightforward; our review indicates that the OSEV system complies with this principle.

Modelling the Electorate The second principle is strongly related to the first; the model of electoral system needs to properly and succinctly capture which voters are eligible to vote in which races.

Similar to the modelling the election system, modelling the electorate is straight forward in the ACT since all voters are eligible to vote on all issues, of which there is normally only one; our review indicates that the OSEV system complies with this principle.

Cryptographic Building Blocks A correct choice of cryptographic building blocks is essential to distribute the trust over multiple components. This principal highlights not only the need to select the appropriate building blocks from the literature but also the the importance of clearly documenting which have been chosen and why.

It does not seem that the vendor and the commission had a clear idea of the cryptographic building blocks available to them, or the functionality of those building blocks. This has resulted in a system where it is unclear what security is achieved; our review indicates that the OSEV system does not comply with this principle.

Cryptographic Parameters This principle highlights the importance of correctly and consistently chosen security parameters, as well documenting these well.

The OSEV system used existing libraries to implement the cryptographic building blocks. The choice of parameters was largely handled by these libraries. This seemed to work reasonable well, with the exception that the

cryptographic building blocks did not provide the functionality that the vendor and commission believed it did; our review indicates that the OSEV system does comply with this principle but highlights that compliance here without good choices of cryptographic building blocks does not provide the required security.

Parties and Communication This principle highlights the importance of clearly defining the responsibilities, abilities, goals, and trust assumptions for each participant in the protocol.

The OSEV system defines reasonably well the protocol participants and communication. However, the functionality required of each participant in the context of an overall security model, or lack thereof, was missing; our review indicates that the OSEV system does not comply with this principle.

Protocol Structure and Communication Diagrams This principle highlights the importance of precise and comprehensive description of the voting protocol.

The commission and the vendor produced a number of protocol and communication diagrams but the versions released to the public were heavily redacted; our review indicates that the OSEV system does not comply with this principle.

Pseudo-Code Algorithms This principle suggests presenting pseudo-code algorithms for every computational task in the protocol. This maximises the technical depth of the specification.

Pseudo-code algorithms were not available in the information made publicly available. This would have been very useful in analysing the protocol; our review indicates that the OSEV system does not comply with this principle.

Implementation of Pseudo-Code Algorithms This principle encourages implementing the system so that the alignment between the implementation and pseudo-code algorithms in specification are clear.

The lack of Pseudo-Code algorithms for OSEV put extra pressure on the code to be clear as to its purpose. In many cases, it was unclear what code was doing and how key requirements were met. This is was not helped by certain key requirements being achieved by intervention from outside the system; our review indicates that the OSEV system does not comply with this principle.

Cryptographically Relevant Code This principle encourages separating the cryptographically relevant and cryptographically irrelevant components, instead linking them over suitable interfaces.

The reliance on existing libraries to implement the cryptographic building blocks in OSEV turned out to be problematic. It seems clear from the documents that neither the vendor or the commission had a clear view of what cryptographic building blocks were being used except at a very high level. Crucially, the sufficiency of security properties of these building blocks in the context of the protocol were not considered; our review indicates that the OSEV system does not comply with this principle.

Transparency This principle highlights that transparency around the protocol is fundamental to the success of an e-voting project.

The lack of transparency around the OSEV system and the process is of great concern. The lack of publicly available high level security goals and sufficient information to verify that those goals are met means that stakeholders in the election have no means to assess the suitability of the system; our review indicates that the OSEV system does not comply with this principle.

Verifier The lack of any clear notation of a verifier, or verifiers, is a major problem in the OSEV system. As highlighted in our Areas of Concern (Sec. 2) the lack of validation the components perform on the input they receive from other components is one of the major reasons the system is not secure if one or more components are compromised; our review indicates that the OSEV system does not comply with this principle.

3.2 Principles from New Standards for E-voting Systems

Haines and Rønne [16] give nine high level principles about e-voting systems which focus heavily on the systems themselves and the process directly around them. *None* of their principles were met by the OSEV system and we give details below:

Clear claims The documentation accompanying the system should be clear about what security properties the system—and its sub-components—claim to achieve.

There are no clear security claims about the OSEV system due mainly to the lack of a threat model.

Thorough documentation The documentation—and source code comments—should be comprehensive, clear, correct, and consistent.

The OSEV documentation, while extensive, is heavily redacted and focuses on functionality not security.

Minimality The source code provided should be minimal; it should contain only code related to the system under review.

The code base includes out-of-date material which hindered analysis.

Buildable The released source code should be easy to build. Preferably it should come with a configuration using a standard tool, such as Maven. The system should not depend on proprietary libraries which have not been released.

The instructions on building the code included with the code did not work.

Executable The system, once built, should be executable. The intended execution flow of the code should be clear either from the documentation or tests.

Since the code was not buildable it was not executable.

Exportable It should be possible to export test vectors into a well defined format for testing with an independent verifier.

Since the system lacked a notation of a verifier it was not possible to export the data required for the, non-existent, verifier.

Consistent documentation and source The source code and the documentation should correspond to each other.

The alignment between the heavily redacted documentation and source was not clear; in several cases, there were clear gaps. For example, see the discussion in Sec. 2.4.

Regularly updated The open source variant of the system should be regularly updated so that experts can check that previous bugs are correctly fixed.

The lack of transparency around the code base makes it difficult to assess how regularly the code was updated. There were several cases were parts of the system were out-dated, which we discovered in discussion with the commission.

Minimal restriction on disclosure The restrictions on the disclosure of vulnerabilities should be minimal.

The NDA required to access the code is unclear as to what findings can be published and when, with seemingly punitive conditions for breaking the vaguely worded agreement.

3.3 Transparency and the NDA

The non-disclosure agreement required the reviewer to accept legal liability for all claims, costs and expenses made against the territory, its employees and agents as a result of the the reviewer breaching the NDA. The NDA did not make clear what information reviewers would eventually be allowed to make public or when they would be allowed to make it public; the waiting period was 60 days but it was unclear from when. The NDA did make clear that not even part of the source code could be made public. Therefore, we have withheld all information which would allow parts of the code to be reconstructed. We have furthermore avoided mentioning what language the system is implemented and what libraries it depends on.

During the course of our investigation it became clear that we were not going to be able to precisely analyse the claims around system based on the (lack of) information we had been given; it was also clear that the implementation of the system could not provide the distributed trust that the design document called for. Based on this we decide to limit our report primarily to high level issues and avoid publishing more specific, and speculative, points.

In making our initial public disclosure [15] we made not attempt to interpret what material we were allowed to disclose. Rather, we provided the commission with a draft report. We requested that either they explicitly give us permission us to publish that report or make public why our report should be withheld.

To our knowledge we are the only party to sign the NDA and get access to the source code. We were only willing to do this because of the academic freedom policy of our university which enshrines the right to discuss, and research and to disseminate and publish the results of our research. This allowed us to conduct the research as part of our employment and not as an individual. In discussion with our colleagues, at other academic institutions but particularly in industry,

we are aware of several highly qualified individuals who wished to provide feedback on the system but were unwilling to take the risk; their understandable decision means the NDA has cost the voters in the ACT invaluable feedback on the system used for their elections.

4 Conclusion

The Overseas E-voting (OSEV) system used in the Australian Capital Territory is an excellent case study in how not to do online voting. The system does not follow identified best practice (Sec. 3) and its security and security goals are not open to public scrutiny (Sec. 2). Furthermore, it seems clear that neither the vendor nor the commission have a clear understanding of the security level the system achieves.

References

1. Beckert, B., Goré, R., Schürmann, C.: On the specification and verification of voting schemes. In: VoteID. Lecture Notes in Computer Science, vol. 7985, pp. 25–40. Springer (2013)
2. Culnane, C., Eldridge, M., Essex, A., Teague, V.: Trust implications of ddos protection in online elections. In: E-VOTE-ID. Lecture Notes in Computer Science, vol. 10615, pp. 127–145. Springer (2017)
3. Dawson, J.E., Goré, R., Meumann, T.: Machine-checked reasoning about complex voting schemes using higher-order logic. In: VoteID. Lecture Notes in Computer Science, vol. 9269, pp. 142–158. Springer (2015)
4. Digital Elections Pty Ltd and Blitzm Systems: OSEV architecture diagram v1.1. http://www.elections.act.gov.au/__data/assets/pdf_file/0004/1659811/OSEV-Architecture-Diagram_v1_1.pdf (2020), accessed: 2022-07-14
5. Digital Elections Pty Ltd and Blitzm Systems: OSEV authentication sequence diagram v0.6.2. http://www.elections.act.gov.au/__data/assets/pdf_file/0005/1659812/OSEV-Authentication-Sequence-Diagram.pdf (2020), accessed: 2022-07-14
6. Digital Elections Pty Ltd and Blitzm Systems: OSEV check sequence diagram v0.6.0. http://www.elections.act.gov.au/__data/assets/pdf_file/0006/1659813/OSEV-Check-Sequence-Diagram.pdf (2020), accessed: 2022-07-14
7. Digital Elections Pty Ltd and Blitzm Systems: OSEV detailed requirements v1.2. http://www.elections.act.gov.au/__data/assets/pdf_file/0009/1659816/OSEV-Detailed-Requirements-v1_2.pdf (2020), accessed: 2022-07-14
8. Digital Elections Pty Ltd and Blitzm Systems: OSEV export sequence diagram v0.6.1. http://www.elections.act.gov.au/__data/assets/pdf_file/0010/1659817/OSEV-Export-Sequence-Diagram.pdf (2020), accessed: 2022-07-14
9. Digital Elections Pty Ltd and Blitzm Systems: OSEV register sequence diagram v0.6.1. http://www.elections.act.gov.au/__data/assets/pdf_file/0012/1659819/OSEV-Register-Sequence-Diagram.pdf (2020), accessed: 2022-07-14
10. Digital Elections Pty Ltd and Blitzm Systems: OSEV security summary v1.4. http://www.elections.act.gov.au/__data/assets/pdf_file/0007/1659823/OSEV_Security_Summary_v1_4_.pdf (2020), accessed: 2022-07-14

11. Digital Elections Pty Ltd and Blitzm Systems: OSEV system design v3.0. http://www.elections.act.gov.au/__data/assets/pdf_file/0005/1659821/OSEV-System-Design-v3_0.pdf (2020), accessed: 2022-07-14
12. Goré, R., Lebedeva, E.: Simulating STV hand-counting by computers considered harmful: A.C.T. In: E-VOTE-ID. Lecture Notes in Computer Science, vol. 10141, pp. 144–163. Springer (2016)
13. Goré, R., Meumann, T.: Proving the monotonicity criterion for a plurality vote-counting program as a step towards verified vote-counting. In: EVOTE. pp. 1–7. IEEE (2014)
14. Haenni, R., Dubuis, E., Koenig, R.E., Locher, P.: Chvote: Sixteen best practices and lessons learned. In: E-VOTE-ID. Lecture Notes in Computer Science, vol. 12455, pp. 95–111. Springer (2020)
15. Haines, T.: Review of the overseas e-voting (OSEV) system used in the Australian Capital Territory. Tech. rep., Australian National University (2022)
16. Haines, T., Rønne, P.B.: New standards for e-voting systems: Reflections on source code examinations. In: Financial Cryptography Workshops. Lecture Notes in Computer Science, vol. 12676, pp. 279–289. Springer (2021)
17. Moses, L.B., Goré, R., Levy, R., Pattinson, D., Tiwari, M.: No more excuses: Automated synthesis of practical and verifiable vote-counting programs for complex voting schemes. In: E-VOTE-ID. Lecture Notes in Computer Science, vol. 10615, pp. 66–83. Springer (2017)

The Diffusion of Electronic Voting for Participatory Budgeting Projects: Evidence from Ukraine

Dmytro Khutkyy[1][0000-0003-0786-2749]

[1] University of Tartu, Estonia
dmytro.khutkyy@ut.ee

Abstract. Electronic voting for participatory budgeting projects in Ukraine it is understudied. Therefore, the paper aims to investigate the patterns of diffusion of e-voting for participatory budgeting projects in Ukraine. This quantitative inquiry scrutinized data about 175 Ukrainian communities that have practiced e-participatory budgeting during 2017-2020 utilizing descriptive and inferential statistics, as well as ANOVA analysis of variance, bivariate and partial correlation analysis. It became evident that participatory budgeting e-voting diffusion vary greatly across Ukrainian communities. Overall, there are some indications of an ongoing digitalization of participatory budgeting voting, which cannot be stated with absolute certainty. The one definitely confirmed pattern of participatory budgeting e-voting diffusion in Ukrainian communities is that longer duration of participatory budgeting is associated with higher e-voting rates.

Keywords: Electronic Voting, Internet Voting, Participatory Budgeting.

1 E-Voting in Participatory Budgeting

According to the classic definition, participatory budgeting (further–'PB') is the process when ordinary citizens are mobilized into local meetings, where they learn about municipal budget, propose, and deliberate over policy projects, and vote on projects to be included in the yearly budget [1]. Its critical point is when locals vote for community development projects thereby exercising direct democracy. In the original model of PB such popular vote (in contrast to advisory consultations) is mandatory for authorities to implement. Thereby the authority over part of municipal budget is taken back from public officials to ordinary citizens empowering the latter. Electronic form of such voting (either in polling stations or via internet, labelled as 'e-voting' here) for PB projects was aimed to enhance digital transformation, decision-making processes, engagement of citizens, and public servants in the context of e-democracy [2]. Due to the similarities of digital uptake the patterns of e-voting for PB projects and for persons in elections may be similar. In Estonia, the wide diffusion of internet voting among the population required over three e-electoral cycles [3]. It is reasonable to surmise that in other countries and formats the pace of e-voting may be similar.

2 Patterns of Participatory Budgeting E-voting in Ukraine

The advance of PB e-voting in Ukraine is understudied. PB in the country is mostly viewed from the viewpoint of scale: funding amounts, submission rates, voter turnout etc. The Index of local democracy ranks major cities according to the performance of their e-participation instruments, including e-PB [4]. Deeper analysis of PB in Ukraine is usually limited to case studies [5]. The most comprehensive research of PB in Ukraine relies on data about 141 communities as of July 2019 [6]. That inquiry discovered the trend of digitalization of voting for PB projects. Yet, a more detailed and recent analysis of the PB e-voting scope and dynamics is missing. This paper aims to investigate the patterns of diffusion of e-voting for PB projects in Ukraine.

2.1 Questions and hypotheses

This inquiry aimed to find out answers to several open questions. What was the share of votes cast electronically of the total number of votes (e-voting share)? What was the dynamics of e-voting share change over time (e-voting share change)? What were the parameters linked with e-voting share and e-voting share change? No statistically significant association between independent and dependent variables was the null hypothesis. In Ukraine, settlements (unified administrative-territorial units) had rather dense population, while agglomerations (uniting several smaller villages or towns) had rather loose population. It was assumed that, due to the distance between constituent villages or towns, agglomerations were more inclined to use e-voting than settlements (hypothesis 1). As for bigger municipalities it was more feasible to engage voters online than offline it was assumed that the larger the population, the higher the percentage of e-voting (hypothesis 2). As digital uptake takes time, it was assumed that the longer the e-PB duration (the number of years of e-voting on an e-platform) the higher the e-voting share (hypothesis 3). Since bigger municipalities had more resources to launch PB e-voting earlier it was assumed that the bigger the settlement the longer the e-PB duration (hypothesis 4). It was reasonable to expect that e-voting share change was linked to population size and the e-PB duration. It was assumed that the bigger the population the higher the e-voting share increase (hypothesis 5) as well as the longer the e-PB duration the higher the e-voting share increase (hypothesis 6).

2.2 Research methodology

The study employed quantitative methods of data collection and analysis. The most vast and reliable PB voting data was available on the two most used e-PB platforms–e-DEM and Hromadskyi Project. The data was provided by organizations managing the e-platforms–EGAP and SocialBoost respectively. Data collection lasted during 2 June–2 July 2021. Population statistics was obtained from two sources–the national statistical yearbook for cities and the decentralization website for agglomerations. Data of up to 20 variables on the total of 175 communities was collected. For most communities, data was available for 2018-2020, therefore this timeframe was used for the study. Methods of analysis included the examination of descriptive and inferential statistics, ANOVA analysis of variance, bivariate and partial correlation analysis.

2.3 Empirical Findings

It was found that e-voting shares and e-voting share changes vary greatly. For 2018, the data was available for 88 communities with the sample error 4.83%, while for 2020– for 114 communities with the sample error 3.67%. Percentages range from 0.65% to 100% (with the median of 61.48%) in 2018 and from 0.22% to 100% (with the median of 85.6%) in 2020. 100% e-voting usually reflected the municipal policy that the voting for PB projects was allowed only in digital format.

To eliminate composition effect, statistics was calculated within the same communities over the 2018–2020-year period (by dividing the 2020 values by the 2018 values community-by-community). Data was available for 39 communities generating the sample error of 0.39. It was found that the minimal e-voting change over the three-year period was 0.18 (meaning that e-voting share decreased), the maximum e-voting change was 8.26 (meaning an over eight-fold increase), and the median e-voting change was 1.4 (indicating some increase on the margin of sample error).

To distinguish the change of e-voting before and after the pandemic, for communities with relevant data e-voting change during 2018–2019 was analyzed (by dividing the 2019 values by the 2018 values community-by-community). Data was available for 72 communities generating the sample error of 1.4. The results demonstrated that the minimal e-voting change over the two-year period was 0.28 (meaning that e-voting share decreased), the maximum e-voting change was 66.38 (meaning an over sixty-six-fold increase), and the median e-voting change was 1.04. The median e-voting change before the pandemic was unclear because of the high sample error.

Variance and correlation analyses found regularities refuting the null hypothesis.

The average share of e-voting in settlements was statistically significantly (at the level of 0.01) higher than in agglomerations–with the mean of 82% versus 54%, respectively and Eta equal to 0.410. However, settlements were on average more statistically significantly (at the level of 0.01) populated than agglomerations–with the mean of 134,429.33 versus 21,516.17, respectively and Eta equal to 0.217. Thereby, the higher e-voting share in settlements than in agglomerations may be due not to a denser, but rather to a bigger, or to a more technologically savvy urban population. Because of this, the hypothesis 1 cannot be neither refuted nor confirmed.

The share of e-voting in 2020 was positively connected with the population size in 2020–Pearson two-tailed correlation coefficient +0.212 statistically significant at the 0.05 level. However, if controlled for e-voting duration, this link disappeared (two-tailed partial correlation statistically insignificant at 0.05 level). This finding refutes the hypothesis 2.

E-voting share in 2020 was statistically significantly correlated with e-voting duration even if controlled for the population size in 2020 (two-tailed partial correlation +0.211 statistically significant at 0.05 level). This indicated that what really mattered for high e-voting share was longer history of e-PB. This confirmed the hypothesis 3.

Also, there was found no statistically significant association between the population size of settlements in 2018 and e-voting duration (two-tailed partial correlation statistically insignificant at 0.05 level). This means that not always bigger cities introduce PB e-voting earlier than smaller towns. This refuted hypothesis 4.

Finally, there was found no statistically significant association between the population size in 2018, e-voting duration, and e-voting share change (two-tailed partial correlations statistically insignificant at 0.05 level). Either 3 years of measurement for the sample of 39 settlements were insufficient to descry the possible regularity or such connection did not exist. In any case, these findings refute the hypotheses 5 and 6.

3 Conclusions on Participatory Budgeting E-Voting in Ukraine

The inquiry showed that PB e-voting diffusion vary considerably across Ukrainian communities–from 1% to 100% of e-voting. Both before and during the pandemic the median e-voting change was overall positive indicating the digitalization of PB voting. However, due to the high sample error this trend is not certain. The hypothesis 1 cannot be neither refuted nor confirmed–the revealed higher e-voting rates in settlements than in agglomerations may be explained either by a denser, or by a bigger, or by a more technologically savvy urban population. The hypothesis 2 about the link between e-voting share and population size was refuted–not always they were positively correlated. The hypothesis 3 was confirmed–the longer the e-PB duration the higher the e-voting share. The hypothesis 4 was refuted–not always bigger cities introduce PB e-voting earlier than smaller towns. The hypotheses 5 and 6 were refuted–neither bigger population nor longer the e-PB duration did not always predispose higher e-voting share increase. The principal definite pattern of PB e-voting diffusion in Ukraine is that longer duration of PB is associated with higher e-voting rates.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme.

References

1. Wampler, B.: Participation, representation, and social justice: Using participatory governance to transform representative democracy. Polity 44(4), 666–682 (2012), DOI: 10.1057/pol.2012.21.
2. Mærøe, A.R., Norta, A., Tsap, V., Pappel, I.: Increasing citizen participation in e-participatory budgeting processes. Journal of Information Technology & Politics, 18(2), 125-147, DOI: 10.1080/19331681.2020.1821421.
3. Vassil, K., Solvak, M., Vinkel, P., Trechsel, A.H., Alvarez, R.M.: The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. Government Information Quarterly, 33(3), 453–459, DOI: 10.1016/j.giq.2016.06.007.
4. CID: Index of local electronic democracy, https://cid.center/edemindex/.
5. PAUCI: Participatory budgeting on its way to openness: The results of support in ten communities during 2016–2018. Kyiv, Ukraine, (2019), https://cutt.ly/pKVD2od.
6. Khutkyy, D., Avramchenko, K.: Impact evaluation of participatory budgeting in Ukraine. Kyiv, Ukraine (2019), https://cutt.ly/vKVFiC2.

Adaptation of an i-voting scheme to Italian Elections for Citizens Abroad

Riccardo Longo[2][0000−0002−8739−3091], Umberto Morelli[1][0000−0003−2899−2227], Chiara Spadafora[2][0000−0003−3352−9210], and Alessandro Tomasi[1][0000−0002−3518−9400]

[1] Fondazione Bruno Kessler {umorelli,altomasi}@fbk.eu
[2] Università degli Studi di Trento {riccardo.longo,chiara.spadafora}@unitn.it

Abstract. We adapt the Araújo-Traoré protocol to Italian elections, with emphasis on anti-coercion measures. In this short paper we focus on a new method for managing anti-coercion credentials for each voter.

Keywords: i-voting · Coercion Resistance · e-Democracy · Verifiability.

1 Introduction

We report on work in progress of an adaptation of the ABRTY protocol [1,2] intended to address specific requirements of the Italian scenario.

First, the Italian Constitution allows voting from abroad - currently by postal vote, with an official experimentation of internet voting run in 2021 [4]. However, it has more stringent requirements than others, e.g., it does not allow early voting as in the U.S. [3]. Second, to access public digital services, Italian citizens are already widely using two eIDAS-notified [7] electronic identification schemes, reaching a High Level of Assurance. Third, vote selling and coercion due to organised crime are historically well-documented threats [5].

Our proposal is intended to guarantee the properties of *coercion-resistance* via the established mechanism of anti-coercion credentials (ACC) as in JCJ [10]; *end-to-end verifiability* and *ballot secrecy*, by encryption with a threshold modified ElGamal scheme [6], zero-knowledge proofs of ballot correctness, and verifiable shuffling and re-encryption [8].

In [2], a forged and a real ACC are distinguished by their private piece, x; this should be delivered over an untappable channel, memorized, and then typed by the voter, but being 20-30 ASCII characters long, it is impractical to remember [9]. To achieve a compromise between security and usability, a short PIN unmasking the ACC would be preferable; Neumann and Volkamer [11] therefore propose allowing voters to set their choice of PIN during the registration phase by being physically present in a controlled environment.

The physical presence of voters is difficult to reconcile with voters residing abroad. However, enabling voters to set their choice of PIN remotely would enable a coercion strategy. We therefore need to deliver a PIN threshold-generated by Registration Tellers (RT) to remote voters without interception by a coercer.

We assume that on a large scale it is very difficult to maintain active surveillance on sufficiently many voters to sway the results of an election, while it is

more practical to indirectly monitor them by requesting proofs of the voter's actions and the RTs' responses, e.g. a video. Therefore, we relax the untappable channel assumption assuming instead that gaps exist in the surveillance of the coercer, so a randomization of the response times makes it possible for a coerced voter to conceal communications and pass a forged response as the real one.

Our strategy is the following. During the Registration phase, the RTs send the ACC masked by a random value, of which the κ least significant digits are the PIN. After a first random time, the RTs send the mask to reveal the ACC; after a second, subsequent random time, the RTs send a Designated-Verifier Non-Interactive Zero-Knowledge Proof (DVNIZKP) to prove the correctness of the unmasked ACC. During the waiting periods, a coerced voter can exploit the surveillance gap to request a *forged* mask share from a trusted RT. Since a forged mask reveals a forged ACC, the voter can use it to evade coercion: if the voter received the real mask when not under active surveillance, they can feign to have never received it and pretend that the forged mask is the real one. The waiting period before receiving the DVNIZKP allows a coerced voter to exploit the DV secret key to construct a DVNIZKP that validates the forged mask.

2 Anti Coercion Credential (ACC)

Let $n_{\mathtt{RT}}$ be the number of RT that collaborate to generate and distribute the ACCs so that no single entity may generate a valid ACC, and only the voter may know the whole ACC, assuming that at least $n_{\mathtt{RT}} - t_{\mathtt{RT}}$ do not collude.

Let $\mathbb{G}$ be a cyclic group with prime order p where the q-SDH and SDDHI [1] problems are assumed to be hard. Let g_1, g_2, g_3, o be four generators of $\mathbb{G}$. The ACC for a voter $\mathcal{V}$ is the tuple $(A_\mathcal{V}, r_\mathcal{V}, x_\mathcal{V})$, with $A_\mathcal{V} = (g_1 g_3^{x_\mathcal{V}})^{\frac{1}{y+r_\mathcal{V}}}$, where $(A_\mathcal{V}, r_\mathcal{V})$ is public and y is the registration secret key, shared among the RTs and common for all ACCs in an election, associated to a public key $R = g_3^y$ that is used to verify the credentials with a DVNIZKP or during the tallying. Given a shared secret value z, z_i will identify the share of z owned by RT_i.

We now describe the ACC generation procedure [13,2][3]:

1. The RTs cooperatively generate the public key $V = g_1^{\xi_1} g_2^{\xi_2}$ for the Modified ElGamal Cryptosystem [10] with threshold $t_{\mathtt{RT}}$.
2. Using the same approach as [13], the RTs generate the secrets x, σ, r, y so that each RT_i owns only a share, but they can compute $E_V[(g_1 \cdot g_3^x)^{\frac{1}{y+r}}]$.
3. The value A is retrieved from $E_V[(g_1 \cdot g_3^x)^{\frac{1}{y+r}}]$ by threshold decryption, then every RT_i broadcasts the encryption $E_T^{\tilde{r}_i}[A]$ (where T is the public key of the TTs), so that they can be interpolated to obtain $E_T^{\tilde{r}}[A]$.
4. Each RT_i privately stores the tuple $\mathcal{T}_i = \left(r, x_i, \sigma_i, \tilde{r}_i, E_T^{\tilde{r}_i}[A]\right)$.
5. The tuple $\left(A, r, E_T^{\tilde{r}}[A], E_V^{\hat{r}}[g_1 \cdot g_3^x]\right)$ is called *public ACC* and is published on a Web Bulletin Board (WBB), associated to a pseudonymous identifier of $\mathcal{V}$.

To issue an ACC, to a voter $\mathcal{V}$ the following procedure is followed:

[3] The subscript $\mathcal{V}$ may be omitted when clear from context.

1. $\mathcal{V}$ generates uniformly at random the Designated Verifier private key $e_{\mathcal{V}} \in \mathbb{Z}_p$ and computes the corresponding public key $D_{\mathcal{V}} = g_2^{e_{\mathcal{V}}}$.
2. $\mathcal{V}$ uses an official electronic identification scheme to authenticate and request a pseudonymous credential associated to $D_{\mathcal{V}}$ that demonstrates $\mathcal{V}$'s right to vote (checked against the appropriate institutional registry).
3. Upon registration, $D_{\mathcal{V}}$ is linked to a public ACC and published on the WBB, so the tuple $\left(D_{\mathcal{V}}, A_{\mathcal{V}}, r_{\mathcal{V}}, E_T^{\tilde{r}_{\mathcal{V}}}[A_{\mathcal{V}}], E_V^{\tilde{r}_{\mathcal{V}}}[g_1 \cdot g_3^{x_{\mathcal{V}}}]\right)$ is publicly available.
4. Each RT_i uses $\tilde{r}_{i,\mathcal{V}}$ to compute a NIZKP $\Pi_{i,\mathcal{V}}$ that proves that $E_T^{\tilde{r}_{i,\mathcal{V}}}[A_{\mathcal{V}}]$ encrypts $A_{\mathcal{V}}$ and sends to $\mathcal{V}$ the tuple $(i, x_{i,\mathcal{V}} + \sigma_{i,\mathcal{V}}, E_T^{\tilde{r}_{i,\mathcal{V}}}[A_{\mathcal{V}}], \Pi_{i,\mathcal{V}})$.
5. With $t_{\mathtt{RT}}$ tuples, $\mathcal{V}$ can compute $x_{\mathcal{V}} + \sigma_{\mathcal{V}}$, and $E_T^{\tilde{r}_{\mathcal{V}}}[A_{\mathcal{V}}]$. Then $\mathcal{V}$ recovers from the WBB $r_{\mathcal{V}}, A_{\mathcal{V}}$, $E_T^{\tilde{r}_{\mathcal{V}}}[A_{\mathcal{V}}]$, verifies the proofs $\Pi_{i,\mathcal{V}}$ and the correctness of the ciphertext interpolation. $\mathcal{V}$ stores $(A_{\mathcal{V}}, r_{\mathcal{V}}, x_{\mathcal{V}} + \sigma_{\mathcal{V}})$ on the voting device.
6. Each RT_i waits for a randomized time interval then sends the share $(i, \sigma_{i,\mathcal{V}})$.
7. With $t_{\mathtt{RT}}$ tuples, $\mathcal{V}$ can compute $\sigma_{\mathcal{V}}$ which is split as: $\sigma_{\mathcal{V}} = \hat{\sigma}_{\mathcal{V}} \cdot 10^{\kappa} + \mathtt{PIN}_{\mathcal{V}}$. Then $\mathcal{V}$ memorizes $\mathtt{PIN}_{\mathcal{V}}$ and saves $\hat{\sigma}_{\mathcal{V}} \cdot 10^{\kappa}$ on the voting device.
8. $\mathcal{V}$ can request multiple times to receive again the shares $(i, \sigma_{i,\mathcal{V}})$, this allows to re-compute $\mathtt{PIN}_{\mathcal{V}}$ if it was forgotten.
9. To request a forged mask (to legitimize a forged PIN) $\mathcal{V}$ chooses $\mathtt{PIN}'_{\mathcal{V}} \neq \mathtt{PIN}_{\mathcal{V}}$, and computes $\sigma'_{\mathcal{V}} = \hat{\sigma}_{\mathcal{V}} \cdot 10^{\kappa} + \mathtt{PIN}'_{\mathcal{V}}$. $\mathcal{V}$ then selects a set I of size at least $n_{\mathtt{RT}} - t_{\mathtt{RT}} + 1$: the RT_i for $i \in I$ are trusted to collaborate with the evasion strategy. $\mathcal{V}$ uses the points $(0, \sigma'_{\mathcal{V}})$, $\{(j, \sigma_{j,\mathcal{V}})\}_{j \notin I}$ to interpolate a polynomial $p_{\sigma'_{\mathcal{V}}}$ of degree $t_{\mathtt{RT}}$ and computes the forged shares $\sigma'_{i,\mathcal{V}} = p_{\sigma'_{\mathcal{V}}}(i)$. Finally a request to receive again the shares is made, but each RT_i for $i \in I$ is privately instructed to respond with the forged share $(i, \sigma'_{i,\mathcal{V}})$, while the untrusted RTs respond normally. Note that once the forged shares have been computed, $\mathcal{V}$ can safely delete $\hat{\sigma}_{\mathcal{V}} \cdot 10^{\kappa}$ from the voting device (since the same value will be reconstructed from the forged shares) and pretend to not have received the mask yet (legitimizing the reception of the forged shares).

Once the mask has been sent to $\mathcal{V}$, the voter may verify the correctness of the ACC. After a randomized time, each RT_i sends to $\mathcal{V}$ a share of a DVNIZKP which, once reconstructed through interpolation, proves either the knowledge of $e_{\mathcal{V}} = \log_{g_2}(D_{\mathcal{V}})$ or the knowledge of $y = \log_{g_1 \cdot g_3^{x_{\mathcal{V}}} \cdot A_{\mathcal{V}}^{-r_{\mathcal{V}}}}(A_{\mathcal{V}}) = \log_{g_3}(R)$. The RTs can compute the shares of the proofs because they know the shares y_i of y, and $\mathcal{V}$ is convinced by the proof because $e_{\mathcal{V}}$ is kept private. On the other hand $\mathcal{V}$ can forge the proof for any PIN to fool a coercer using $e_{\mathcal{V}}$. We underline that the proof can be also used to verify that the PIN the voter remembers is correct: with a wrong PIN $\mathcal{V}$ retrieves the wrong $x_{\mathcal{V}}$ and the proof will not be verified.

To prevent RTs from *ballot stuffing* [12] by generating illegitimate credentials - i.e., valid credentials not associated to eligible voters - the values $E_T^{\tilde{r}_{\mathcal{V}}}[A_{\mathcal{V}}]$ published on the WBB are used to compute fingerprints [2] that identify legitimate ones. This procedure can be used to revoke credentials by marking the public ACC on the WBB as invalid; any corresponding vote will not be tallied. For other elections, the RTs can issue new credentials to eligible voters by changing only the public ACCs, not the private value $x_{\mathcal{V}}$, so voters may use the same PIN. This approach is particularly convenient for multiple concurrent elections.

3 Final Remarks

ACCs are interactively generated between RTs, therefore ACC are likely generated in advance rather than on the fly, and a certain number of spare ACCs may be pre-generated in case of revocation e.g., due to compromised voter devices. Voters may find it hard to trust a system in which more voting credentials are generated than actual eligible voters, in the name of service availability. One option could be to post the public ACCs on the WBB in advance, marked as un-assigned until associated with an authenticated voter.

Ideally, the masked ACC should be stored safely enough to guard against malicious exfiltration, but exportable without trace to allow a victim of coercion to vote from a separate device, recalling only their PIN. We leave considerations on PIN length and brute force countermeasures as implementation choices.

References

1. Araújo, R., Ben Rajeb, N., Robbana, R., Traoré, J., Youssfi, S.: Towards practical and secure coercion-resistant electronic elections. In: Cryptology and Network Security. Springer (2010). https://doi.org/10.1007/978-3-642-17619-7_20
2. Araújo, R., Traoré, J.: A practical coercion resistant voting scheme revisited. In: International Conference on E-Voting and Identity. pp. 193–209. Springer Berlin Heidelberg (2013). https://doi.org/10.1007/978-3-642-39185-9_12
3. Bifulco, R., Celotto, A., Olivetti, M.: Commentario alla Costituzione, vol. 1. UTET giuridica (2006)
4. Camera dei deputati: Comitato permanente sugli italiani nel mondo, audizione del dottor Vignali, https://webtv.camera.it/evento/21102
5. Desantis, V.: Il voto degli italiani all'estero: nuove criticità e vecchi problemi nella prospettiva del superamento del voto per corrispondenza. Federalismi.it (22) (2022)
6. Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Conference on the Theory and Application of Cryptology. pp. 307–315. Springer (1989). https://doi.org/10.1007/0-387-34805-0_28
7. Overview of pre-notified and notified eID schemes under eIDAS, https://ec.europa.eu/digital-building-blocks/wikis/x/iw3oAg
8. Groth, J.: A verifiable secret shuffle of homomorphic encryptions. Journal of Cryptology **23**(4), 546–579 (2010). https://doi.org/10.1007/s00145-010-9067-9
9. Huh, J.H., Kim, H., Bobba, R.B., Bashir, M.N., Beznosov, K.: On the memorability of system-generated PINs: Can chunking help? In: SOUPS 2015. pp. 197–209
10. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Towards Trustworthy Elections, LNCS, vol. 6000, pp. 37–63. Springer (2010). https://doi.org/10.1007/978-3-642-12980-3_2
11. Neumann, S., Volkamer, M.: Civitas and the real world: problems and solutions from a practical point of view. In: Seventh International Conference on Availability, Reliability and Security. IEEE (2012). https://doi.org/10.1109/ARES.2012.75
12. Puiggali, J., Chóliz, J., Guasch, S.: Best practices in internet voting. In: NIST: Workshop on UOCAVA Remote Voting Systems. Washington DC (2010)
13. Wang, H., Zhang, Y., Feng, D.: Short threshold signature schemes without random oracles. In: Progress in Cryptology - INDOCRYPT 2005. pp. 297–310. Springer Berlin Heidelberg (2005). https://doi.org/10.1007/11596219_24

Post-Election Audits in the Philippines

Carsten Schürmann

Center for Information Security and Trust
IT University of Copenhagen
carsten@itu.dk

Abstract. How do you observe the unobservable? The election technology in use in the Philippines are optical ballot scanners called Vote Counting Machines (VCMs) that scan, count, and transmit election results at the close of polls back to the national tallying center. Post-election audits called Random Manual Audits (RMAs) are required by law to take place prior to the result becoming final. In this paper, we explore the idea of replacing RMAs by Risk-Limiting Audits (RLAs) that are efficient, have a high chance of correcting an incorrect election outcome by the means of a recount, and can therefore strengthen public confidence in the election.

1 Introduction

How do you observe the unobservable? Election technologies handle voter information, ballots, and results in digital form. To observe the processing of a ballot requires the observer to follow the flow of electrons in a system that comprises billions of transistors and millions of lines of code. This is clearly impossible!

The Philippines uses election technologies for vote casting, vote counting, and also results transmission. A voter hand-marks a ballot paper by filling-in ovals with a black pen before putting it into a so-called *privacy sleeve* and proceeding to the vote counting machine (VCM) of the clustered precinct. A cluster precinct consists of several precincts and serves up to 800 voters. A VCM is an optical ballot scanner that stores and tabulates the results. Differently from other ballot scanners, the VCM produces also a VVPAT (voter verifiable paper audit trail) that is a printout of the interpretation of the ballot by the VCM. The voter is invited to check the VVPAT and deposits it then in a special VVPAT box. The Cast Vote Record, i.e. the interpretation of each ballot cast on the VCM in digital form, and other information such as configuration files and log files are stored on two SD cards, a main card and a backup card. After the poll closes, the VCM is used to transmit the results to various servers and produces multiple printouts of the election record (ER), i.e. national and local returns, and audit logs.

To assess *election integrity*, we should remind ourselves, that election integrity cannot be evaluated by inspecting the election technology alone. An optical ballot scanner, such as a VCM, may have software defects hidden deeply inside the system, or it may misbehave, because a malicious actor might have gained access

to the system prior to the election, for example through exploiting vulnerabilities, supply-chain, or other cyberattacks, and manipulated its software. What can be observed, however, is the evidence that is produced for and by the VCM: hand-marked paper ballots and the VVPAT. Both are voter-verified, the ballot papers are hand-marked by the voter, clearly representing the voter's intention, the VVPAT can be checked by the voter after the ballot has been scanned to ensure the that the scan was successful. To check this evidence, the Philippines Statistics Authority (PSA) conducts a Random Manual Audit (RMA) after every election as required by law.

In contrast, driven by the use of various election technologies in the U.S., post-election audits have become in recent years a major area of research, which includes the theory and statistics of post-election audits [3], as well as techniques to make the usable [4]. One technique that stands out are risk-limiting audits (RLAs) that are designed to confirm election results by drawing and inspecting random samples of ballots.

In this paper, we explore if the RMA could be implemented by a risk-limiting audit (RLA). In contrast to an RMA, which requires one ballot box per congressional district to be chosen randomly and recounted manually, an RLA will draw a sample of ballots at random based on the desired level of confidence. An RLA is one of the few if not the only auditing technique that will automatically correct an incorrect election result with high probability by triggering a full hand-count of all ballots if necessary. We consider two flavors of RLAs, ballot-polling audits and ballot-comparison audits.

Hypothesis: If the post-election audit for the Philippines general election would require an RLA instead of RMA, the audit of the election outcome would be more (1) expressive, (2) autocorrecting, and (3) more efficient, if we consider previous elections.

The paper is organized as follows. In Section 2, we summarize the state of post-election auditing in the Philippines and describe the legal framework and implementation of RMAs. We then introduce briefly RLAs in Section 3, before we consider and evaluate the impact of RLAs in the previous Philippines election in 2016 and 2022 in Section 4. Next, we assess results and conclude with Section 5.

2 Random Manual Audit

In this section, we describe the current situation in the Philippines, including the legal framework, the technique that is used to select at random a polling station in a congressional district, and finally the process of conducting the audit. With the introduction of VCMs into the voting process, *clustered precincts* were defined that comprise several "traditional" precincts, which means that up to 800 voters can use one and the same VCM.

2.1 The Legal Framework

The election law authorizing the use of an automated election system (AES) for the Philippines general election can be found in *Republic Act No. 9369*, approved

23 January 2007, which is an act amending Republic Act No. 8436, entitled "an act authorizing the commission on elections to use an automated election system in the May 11, 1998 national or local elections and in subsequent national and local electoral exercises, to encourage transparency, credibility, fairness and accuracy of elections, amending for the purpose Batas Pambansa Blg. 881, as amended, Republic Act No. 7166 and other related election laws, providing funds therefor and for other purposes.

Besides providing the legal justification for the use of technology, the law also governs the use of post-election audits, which are called Random Manual Audits (RMAs) in the Philippines. The relevant paragraph reads as follows:

> SEC 29. Random Manual Audit. - Where the AES is used, there shall be a random manual audit in one precinct per congressional district randomly chosen by the Commission in each province and city. Any difference between the automated and manual count will result in the determination of root cause and initiate a manual count for those precincts affected by the computer or procedural error.

There are 243 congressional districts in the Philippines.

To implement the provision of the law, the Commission on Elections (COMELEC) promulgated Resolution 10774 on March 23, 2022 amending Resolution 10738 promulgated on Dec. 9, 2021, entitled "In the Matter of the General Instructions for the Conduct of the Random Manual Audit (RMA) for the [May 9, 2022] Automated Synchronized National and Local Elections and Subsequent Elections Thereafter."

Resolution 10774 requires that "the actual number of precincts to be selected in a legislative district shall be determined by proportional allocation, that is, based on the number of clustered precincts a legislative district has in proportion to that of all the other legislative districts in the country."

The law states that the audit may take up to 45 days.

2.2 Election Results for 2022

We focus our attention to the presidential (see Table 1) and vice-presidential race (see Table 2). Results for the other 9 races can be found online.

2.3 Drawing a Random Sample

The random sample of clustered precincts to be audited was chosen by software that was developed by the Philippines Statistical Authority (PSA) and reviewed by third parties.[1] As a result 757 clustered precincts were selected [2] in the presence of media and observers, out of which 746 ballot boxes were eventually audited and 27 were subjected to further verification, because the content

[1] See `https://www.manilatimes.net/2022/06/15/opinion/columns/random-manual-audit/1847437`

[2] See `https://comelec.gov.ph/?r=2022NLE/RandomManualAudit2022`

MARCOS, Ferdinand Jr. Romualdezos	31,629,783	58.77%
ROBREDO, Maria Leonor Gerona	15,035,773	27.94%
PACQUIAO, Emmanuel Dapidran	3,663,113	6.81%
DOMAGOSO, Francisco Moreno	1,933,909	3.59%
LACSON, Panfilo Morena	892,375	1.66%
MANGONDATO, Faisal Montay	301,629	0.56%
ABELLA, Ernesto Corpus	114,627	0.21%
DE GUZMAN, Leodegario Quitain	93,027	0.17%
GONZALES, Norberto Borja	90,656	0.17%
MONTEMAYOR, Jose Jr. Cabrera	60,592	0.11%
Total Votes	53,815,484	

Table 1. Presidential Race Philippines 2022

DUTERTE, Sara Zimmerman	32,208,417	61.53%
PANGILINAN, Francis Nepomuceno	9,329,207	17.82%
SOTTO, Vicente III Castelo	8,251,267	15.76%
ONG, Willie Tan	1,878,531	3.59%
ATIENZA, Jose Jr. Livioko	270,381	0.52%
LOPEZ, Emmanuel Sto Domingo	159,670	0.31%
BELLO, Walden Flores	100,827	0.19%
SERAPIO, Carlos Gelacio	90,989	0.17%
DAVID, Rizalito Yap	56,711	0.11%
Total Votes	52,346,000	

Table 2. Vice-Presidential Race Philippines 2022

of the ballot was damaged or ERs were missing. Although the software was carefully reviewed, some stakeholder groups publicly distrusted that the selection of clustered precincts was random.[3]

2.4 Conducting RMAs

An audit comprises a manual tally of all 11 contests on the ballot and judgments about what is a valid mark and what is not. Considering the voter turnout of about 83.07%, the expected number of ballots to be audited is around 503,071. The logistical effort for arranging an audit of this magnitude are immense. Ballot boxes must be transported to the Manila where the audit is executed, and since the ballot contains several races, a sort and count approach does not work.

[3] See `https://www.change.org/p/the-truth-petition-manifesto-exhorts-the-comelec-to-open-750-randomly-selected-ballot-boxes-for-manual-count-and-audit-of-sd-cards-sign-and-share-this-petition-now-click-here-bit-ly-truthpetitionph`

Instead, the information of the ballot is carefully recorded by other means, and an accuracy score is computed.

For the 2022 election, the accuracy score was determined to be 99.95928%. COMELEC reported[4] that out of 757, a total of 746 ballot boxes were audited. Some ballot boxes were no longer subjected to audit, while 27 are still subject to further verification of the Technological Evaluation Committee for the following reasons: mislabeled ballot boxes, with wet/torn ballots, and no printed and online election returns. The root cause of the discrepancies, we suspect, was due to a difference in interpretation of manual vs. automatic interpretation of the hand-marked ovals on the ballots.

3 Risk-Limiting Audit

A risk-limiting audit (RLA) [3] refers to a family of post-election auditing techniques that confirms a correct or corrects an incorrect election result with high probability, which is given by the risk-limit. It is a technique that reduces the trust in the correctness of the election result to the trust in the security of the evidence, usually hand-marked paper ballots, machine-marked paper ballots, or VVPATs.

The workings of the RLA and the reason why it works is best explained by an analogy[5]. If we were to determine if a large pot of soup is too salty, nobody would expect us to drink the entire pot: it is sufficient to stir the soup well and then take a spoonful. In the analogy, the soup represents all ballots, the spoon a sample, the "saltiness" the margin between winner and runner-up, and the tasting the verification. In a risk-limiting audit, the risk-limit defines how certain we want to be that the election result is correct, the size of the spoon is determined by statistics, and the stirring of the soup by picking a truly random sample. If the sample is not random, the result of the RLA will hold no truth.

If the RLA cannot confirm the election result, it triggers a full hand recount, and this recount will deliver the correct result. The RLA brings efficiency and, recognizing the challenges of stakeholder trust in smaller sample sizes, integrity to post-electoral audits. Different social choice functions require different techniques, for example, standard ballot-polling or ballot-comparison audits apply to first-past-the-post voting schemes, such as the one used in the Philippines, but there are also others that apply to the d'Hondt voting rule [5] and Single Transferable Vote (STV) systems [2].

3.1 Ballot-polling Audit

For a first-past-the-post system, the auditor conducting a ballot-polling audit selects a truly random sample of ballots and counts them. When the votes provide sufficient evidence that the election result is correct, the audit stops, otherwise

[4] See `https://www.pna.gov.ph/articles/1177078`

[5] Credit to Prof. Philip Stark, personal communication.

```
function draw_sample(totalvotes, samplesize, entropy):
  for i = 1 to samplesize:
      x = entropy ^ "," ^ i
      y = hash(x)
      z = lookup(y mod totalvotes)
      print(z)
  end
```

Fig. 1. Drawing a truly random sample

the sample size is increased until a full hand count of the ballot papers is triggered. Ballot-polling audits are not the most efficient audits, but they will work for any first-past-the-post election. A more efficient RLA is a ballot-comparison audit, which we discuss next.

3.2 Ballot-comparison Audit

Following [3], ballot-comparison audits confirm an election outcome by comparing hand counts to voting system counts for clusters of ballots. Comparison audits can be thought of as having two phases: (i) Check whether the reported subtotals for every cluster of ballots sum to the contest totals for every candidate. If they do not, the reported results are inconsistent; the audit cannot proceed. (ii) Spot-check the voting system subtotals against hand counts for randomly selected clusters, to assess whether the subtotals are sufficiently accurate to determine who won. If not, the audit has a large chance of requiring a full hand count.

3.3 Drawing a Random Sample

Whether ballot-polling or ballot-comparison audits, the math behind RLAs will determine the initial sample size to be drawn based on the risk-limit given. We present a technique in Figure 1 for drawing this sample, which is truly random and publicly verifiable: To draw the sample, entropy is collected, which is often done using ten-sided dice in conjunction with a cryptographically secure hash-function `hash`. The technique works well when ballots are identifiable. In the Philippines each ballot is uniquely identifiable by a barcode, which contains information such as the polling place identifier and a ballot serial number. Next, each ballot identifier is transcribed using the ballot manifest into the relevant precinct and serial number information (using the function `lookup`) and subsequently printed (using the function `print`), as outlined in the code below. Based on this information ballots should then be physically retrieved and checked.

The use of a cryptographically secure hash function guarantees that the algorithm is verifiable: If the manually generated entropy is known, anyone with

Fig. 2. Entropy collection

Legislative District/ City/ Municipality/ Province/ Region	Polling Place/ Address/ Barangay	Clustered Precincts	Ballot identifier
Maguindanao - first City of Cotabato Maguindanao Barmm	Lugay - Lugay Central School Kibatang St. Lugay - Lugay Bagua I Bagua	0155A, 0158A, 0161A, 0162A	295
Sulu - first Patikul Sulu Barmm	Kaumpang Elementary School Bangkal, Patikul Igasan	0060A, 0061A, 0062A, 0063A	137
...	...	...	...

Fig. 3. A sample list of ballots to be audited

a computer and limited programming skills can compute and verify that the set of audited ballots is correct.

For example, for the 2022 presidential race, where $53,815,484$ ballots were cast and a sample size of 49, we first collect entropy as displayed in Figure 2. The sample can be computed using `draw_sample(53815484, 49, "674987539")`. For illustration purposes, Figure 3 depicts a hypothetical output. Note that the right most column denotes the ballot to be checked in the clustered precinct identified in the third column. Different entropy generates different lists.

Note, that the method `draw_sample` could be used as an alternative to the way how precincts are selected in an RMA (see Section 2.3) that chooses a truly random sample of precincts among the $412,874$ used during the Philippines election. To use the method proposed here, generate new `entropy` and run `draw_sample(412874, 757, entropy)` with an appropriate `lookup` function that turns numeric precinct identifiers into precinct names. This method has several advantages over the method used in RMAs, the most important of

which being that the verification of the software or the software itself does not need to be trusted.

3.4 Executing the RLA

Executing an RLA is straightforward.

In the case of a ballot-polling audit, ballot after ballot is drawn following the sample set computed in the previous section. Once all ballots were retrieved, and it was determined that they statistically support the election result, the audit stops, otherwise, the RLA will increase the sample set to be audited.

In the case of a comparison-ballot audit, the ballot under audit is drawn and then compared against its digital interpretation in the cast vote record, which is originally stored on the SD cards of each VCM and later integrated into a comprehensive database.

Drawing a ballot implies that the auditors will need physical access to the hand-marked paper ballots or, alternatively, the VVPATs.

3.5 Correcting an Erroneous Outcome with an RLA

In the case that the election outcome is not confirmed the RLA algorithm may either increase the size of the sample or call immediately for a full hand-count. A full hand-count is easier and more efficient to organize and execute than to locate and verify each and every ballot individually. Recall, that the sample size depends on the margin between winner and runner-up and on the risk-limit. The greater the risk-limit, the smaller the sample size. A full hand-recount will determine the correct result and help identify the root cause for any discrepancy that might have occurred.

4 Evaluation

The conditions in the Philippines are well-suited for conducting either a ballot-polling or even a ballot-comparison audit against the cast vote record: Paper evidence is secured, voters appear to have confidence in the security of the paper trail, and there is already an understanding that audits are useful and should be conducted. The authorities could either audit the hand-marked paper ballots or the VVPATs. In general, we would recommend using the hand-marked paper ballots, because they most closely represent the intent of the voter, which renders the value of VVPATs redundant for the purpose of election integrity. We recognize of course that the VVPATs presented an efficient tool for voters to strengthen their confidence into that the VCMs interpreted their respective voting choices correctly.

Given a specified risk-limit, the efficiency with which an RLA could audit an election is determined by the margin between the winner and the runner-up. The wider the margin, the less evidence is needed to check the result, the smaller the sample of ballots to be audited. In contrast, the smaller the margin, the more

DUTERTE, Rodrigo	16,601,997	38.99%
ROXAS,Mar	9,978,175	23.43%
POE, Grace	9,100,991	21.37%
BINAY, Jejomar	5,416,140	12.72%
SANTIAGO, Miriam Defensor	1,455,532	3.42%
SENERES, Roy Sr. V.	25,779	0.06%
Total Votes	42,578,614	

Table 3. Presidential Race Philippines 2016

ballots need to be audited. This can also lead to the paradoxical case that for a given risk-limit the number of ballots that have to be audited exceed the number of ballots cast in the context.

For a better demonstration of these issues for the two different RLA methods discussed earlier, we present here also the election results for the 2016 Philippines elections, noting the margin for the 2016 election is 263,473 ballots (because of the vice presidential race), whereas the margin for the 2022 election is two orders of magnitudes larger, i.e. 16,594,010 ballots. The official results of the presidential and vice-presidential races are depicted in Table 3 and Table 4, respectively.

ROBREDO, Maria Leonor Gerona	14,418,817	35.11%
MARCOS, Ferdinand Jr. Romualdezos	14,155,344	34.47%
CAYETANO, Alan Peter	5,903,379	14.38%
ESCUDERO, Francis	4,931,962	12.01%
TRILLANES, Antonio	868,501	2.11%
HONASAN, Gregorio	788,881	1.92%
Total Votes	41,066,884	

Table 4. Vice Presidential Race Philippines 2016

We should expect that the sample size for 2016 is much larger than for 2022. Using the election auditing tools that Prof. Philip Stark offers on his webpage[6], we compute the different ballot sizes for a ballot-polling and ballot-comparison at different risk-limits. The results are summarized in Table 5 and Table 6, respectively. For 2022, if we compare the sample sizes of either RLA with the expected 503,071 ballots audited in the current elections, we observe that the RLAs are orders of magnitude more efficient. A ballot comparison audit, for example, requires only 49 ballots to audit while guaranteeing that an incorrect election outcome will be identified with a likelihood of 99.9%.

[6] See `https://www.stat.berkeley.edu/~stark/Vote/auditTools.htm#`

If we focus our attention to 2016, we note that the margin between winner and runner-up is very small. Consequently, we expect the sample size for either audit to be much larger than for 2022, and indeed it is. A ballot-polling audit still requires a substantial sample to be drawn, even if the risk limit is set to 10%. The comparison ballot audit, however, can yield 99.9% certainty that the outcome is correct, by only considering a sample of 2586 ballots.

Risk limit	2016	2022
10%	80,872	44
5%	105,169	57
2%	137,287	73
1%	161,583	85
0.1%	242,294	126

Table 5. Ballot-polling RLA. Sample sizes

Risk limit	2016	2022
10%	862	18
5%	1183	22
2%	1491	29
1%	1724	33
0.1%	2586	49

Table 6. Ballot-comparison RLA. Sample sizes

When comparing RMAs and RLAs, one key difference is that the random sample required to be inspected in an RLA may originate from any ballot box. Note, when doing a ballot comparison RLA, we do not have to recount the entire ballot box, all we have to do is to locate *the* ballot as specified by the RLA and compare it to its digital representation in the cast vote record. This means that in the worst case, with a risk-limit of 5%, in 2016, we would have to open 1,183 ballot boxes.

5 Conclusion

The requirement stipulated by the legal framework to audit election results that were produced using election technologies, such as VCM's, is a testimony for the Philippines to strive for transparent and verifiable elections. The Random Manual Audit (RMA) required by law is well-intended, but its efficiency and statistical relevance most likely could be further strengthened by considering ideas present in modern post-election technologies, such as risk-limiting audits.

To learn about the challenges of RLAs in the context of Philippines elections, the COMELEC could consult with the Philippines Statistical Authority (PSA) and derive a plan to run a RLA pilot in parallel the RMA for the next election. The logistics behind such an audit are challenging, especially when sample sizes are big.

In summary, an RLA works as follows: For a given risk limit, an RLA will, if the margin is suitably large, be an extremely efficient method to implement post-election auditing. If the margin is small, however, an RLA might even require a full hand count of all ballots, which may be justified if the desired risk-limit is small. If COMELEC ever considers implementing RLAs, the main question to be answered, is what is a suitable risk-limit and what kind of RLA should be used. Because of the availability of the cast vote record, a ballot comparison audit is possible, and should therefore be preferred.

As described, the sample sizes can be very small when conducting a risk-limiting audit, so small in fact, that voters may no longer trust the audit. Although the statistics is sound and the mathematics behind risk-limiting audits has been stress tested by several mathematicians, small sizes can give raise to distrust [1]. It is therefore advisable to evaluate to what extent voters trust the security of the paper trail and if they accept sample sizes that are as small as the ones described here.

References

1. Asmita Dalela, Oksana Kulyk, and Carsten Schürmann. Voter perceptions of trust in risk-limiting audits, 2021.
2. Floyd Everest, Michelle Blom, Philip B. Stark, Peter J. Stuckey, Vanessa Teague, and Damjan Vukcevic. Auditing ranked voting elections with dirichlet-tree models: First steps, 2022.
3. Mark Lindeman and Philip B. Stark. A gentle introduction to risk-limiting audits. *IEEE Security & Privacy*, 10(5):42–49, 2012.
4. Mayuri Sridhar and Ronald L. Rivest. k-cut: A simple approximately-uniform method for sampling ballots in post-election audits. In *Financial Cryptography Workshops*, 2019.
5. Philip B. Stark and Vanessa Teague. Verifiable european elections: Risk-limiting audits for D'Hondt and its relatives. *USENIX Journal of Election Technology and Systems (JETS)*, 1(3):18–39, December 2014.

Phd Colloquium

Domestic Decision-Making, Regional Linkages, and Cybersecurity Considerations: Implementation of Internet Voting in Russia, September 2021

Logan Carmichael[1,2] and Bogdan Romanov[1,3][0000-0001-8594-2387]

[1] Johan Skytte Institute of Political Studies, University of Tartu, Tartu, Estonia
[2] logan.emily.carmichael@ut.ee
[3] bogdan.romanov@ut.ee

Abstract. The research objective of the article is to explain why and how the Russian Federation implemented online voting in the case of the September 2021 national State Council elections. This case constitutes the first instance of large-scale, non-democratic, and legally binding elections with the use of i-voting. Hence, the paper provides answers to (1) why i-voting was introduced in the already state-controlled electoral context, (2) how Estonia, as a cradle of i-voting, affected the decision-making in Russia, and (3) how cybersecurity concerns were addressed by technology providers and engage in a discussion about cybersecurity not for users, but for officials. Our research design focuses on the instance of Russian online voting without going into further details of regional and capital city distinction and relies on the interview data. Results show that (1) the primary motivation underpinning the introduction of i-voting in Russia was regime stability, (2) Estonian successes in e-governance and i-voting did not impact decision-making in Russia, and (3) cybersecurity concerns around the i-voting technologies used in Russia were indeed present but were not central to decision-making. Findings have broader implications, the research fills in a gap in the literature surrounding the emergence of i-voting, as well as the relationship these processes have with existing, longer-term implementations in democratic states. At the same time, from the empirical viewpoint, the work sheds light on how topics in non-democracies can be studied.

Keywords: i-voting· cybersecurity· Russia · digital authoritarianism

1 Introduction

Electronic governance (e-governance), initially an undertaking in predominantly democratic states, has more recently become popular in some non-democratic regimes as well. This trend could be observed around 2015 [1; 2] when Internet penetration was no longer a uniquely democratic feature. As a result, this non-democratic shift led to the implementation of online participatory practices in autocratic states (e.g., China [3; 4], Egypt [5], post-soviet states, Kazakhstan [6], Kyrgyzstan [7], and others).

Even though the academic community noticed non-democratic interest in digital political technologies, some topics are overlooked, for instance, the recent online elections in Russia in September 2021. This is a continuation of previous trials in Moscow in 2019, however, this time opportunity to vote online was available in seven regions of Russia. Although limited in scale, this new i-voting precedent caused considerable discussions on the Internet, especially as tallying of online votes was exposed to be fraudulent [8]. Yet, the discussion did not draw any lessons or further implications for the i-voting implementation in Russia. This is an essential remark since March 14, 2022, online voting can be used in all elections in Russia.

Thus, the article's main research objective is to shed light on the rationale behind the introduction of i-voting in Russia, even though the party in power already controlled the electoral field. Secondly, this article explores how digital governance, i-voting, and cybersecurity success in neighboring Estonia impacted decision-making in Russia. Finally, this article aims to explain how aspects of cybersecurity were addressed.

2 Theoretical background and hypotheses

This paper employs twofold digital authoritarianism and a constructivist approach to the topics of i-voting and cybersecurity in Russia. Together, these two theoretical groundings provide a useful explanatory lens through which to examine these topics.

In its adoption of a digital authoritarianism approach, this paper employs various literature strands that refer to the use of the Internet and e-governance technologies in non-democratic contexts [9; 10]. The main contribution of the theoretical approach is that "…the use of the Internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties." [11, p. 2] With this backbone in mind, we will unpack the rationale behind implementing online voting in Russia. Additionally, the focus on political and social control would imply flawless cybersecurity of the deployed technology.

Specifically, the constructivist approach enacted here would borrow from constructivist theory in international relations, emphasizing the centrality of ideation and experiences in behavior, interactions, and political decision-making [12]. Although this paper looks at i-voting as an inherently domestic undertaking in Russia, it is an endeavor with international ramifications, as traditional understandings of jurisdiction become quickly blurred in cyberspace and the digital world. Ciolan [13] has written specifically about how a constructivist approach is useful to the study of cybersecurity because involved stakeholders are "trying to impose their ideas regarding the way of constructing the future type of cyberspace" [13, p. 131]. This broad premise extends to i-voting and governance decisions surrounding the implementation of i-voting.

Leaving literature review aside, we derived the following hypotheses from the current state-of-the-art:

H1: Online voting was implemented solely as a tool for regime stability via electoral fraud and results manipulation

This assumption stems directly from the digital authoritarianism theory, which entails that all digital and technological alterations are caused because of regime instability. However, the case of the September 2021 elections could have more than one explanation. COVID-19 could be another reason behind the i-voting introduction since autocracies care about their population as a source of legitimacy. That is why autocracies might be more reactive due to the 'autocratic advantage' [14] in protecting their citizens [15; 16]. Or it could be a consequent step in developing the e-governance ecosystem in Russia, which could be traced from Medvedev's presidential term in 2008-2012.

H2: Regional competition between Estonia and Russia did play a crucial role in the establishment of online voting

Taking into account all the perturbations in Russia-Estonia relationships, we assume that Estonia could, in a form of collaboration or competition, incentivize further development of e-governance in Russia. Either Russian officials could refer for help to the Estonian side, or maybe there were discourses which hinted that Russia was driven by a desire to prove to be on par with a digitally advanced neighbor. This assumption is supported by the digital authoritarianism paradigm, which emphasizes regime maintenance, and here, this collaboration/competition would give Russia more international legitimacy as a capable state.

H3: Cybersecurity concerns were at the core of decision-making regarding the online voting implementation

Since it is not the first online voting trial in Russia, but the first on such a large scale, we would expect decision-makers and providers of the technology to think through the cybersecurity aspect of the elections. Especially after the cases in which elections were hijacked from the outside of a state, conducting elections. Additionally, as described in the literature, Russia has a unique approach toward cyberspace and, thus cybersecurity, so this question should be among the first priorities.

As a result, these three hypotheses will expose genuine rationales behind the implementation of online voting in the case of the 2021 elections; analyze the role of Estonia in the decision-making process; and finally, will shed more light on the perception of cybersecurity in Russia, which is expected to be different from the democratic one.

3 Methodology

The research employs a qualitative empirical design, which consists of semi-structured interviews. The semi-structured expert interviews will help us to gather domain knowledge from people inside of Russia, people specializing in Russia, and experts outside of Russia. By employing semi-structured interviews, we could gain nuanced insight into these ideas and experiences surrounding i-voting and cybersecurity issues. As a result, we will have corpora of texts, which could prove or falsify our hypotheses. Since hypotheses cover different topics, we applied purposive sampling [17] to cover every assumption. As a result, we pinpointed three groups of respondents with a different number of people in each, see Table 1.

Table 1. The list of interviewees from different areas of expertise.

Group name	Quantity	Affiliation
Political scientists	**4**	Universities in Russia, Finland
I-Voting practitioners/ decision-makers	**4**	State Information System, National election committee, University of Tartu
Cybersecurity practitioners	**2**	Cybernetica, e-Governance Academy

As a remark, we would like to address the question of our respondents' anonymity since we are working with a susceptible topic. First, respondents were asked to sign an informed consent form, in which they could choose to stay anonymous or allow us to mention their names. Secondly, despite the answer in the form, we anonymized all interview audio recordings and stored them in a secured and different folder from the one with consent forms. Lastly, we sent transcripts to the respondents for their approval.

4 Results

This paper has shed light on Russian internet voting processes, the decision-making behind its implementation, how it has been impacted by regional players and trends, and the cybersecurity of i-voting technologies in the September 2021 elections.

Firstly, it has examined the role of regime stability in the decision to implement i-voting in Russia, finding that indeed considerations such as the possibility to manipulate electoral outcomes digitally, cost efficiency for the incumbent, and the lack of in-person voting interactions aimed to prevent political violence or protests all offer compelling motivations for the Russian authorities.

Secondly, it has been found that Estonia's early and pervasive adoption of e-governance practices and, specifically, i-voting did not impact Russian decision-making around the implementation of i-voting on the grounds of regional competition; rather, Russia may have seen Estonia as a benchmark in this space but crafted its system, with distinct i-voting technologies. Rather than regional competition between Russia and Estonia, this paper suggests regional cooperation on digital governance between Russia and other non-democratic regimes in the region.

Finally, this paper examined cybersecurity concerns with Russian i-voting technologies, discovering linkages between cybersecurity and the previously outlined regime stability. The degree to which Russian authorities feared interference with their elections is not necessarily represented in the cybersecurity mechanisms protecting i-voting technologies. Concerns with authentication and with source code that lacks transparency were not addressed and left the possibility of electoral manipulation, indicating that cybersecurity concerns were not at the forefront of decision-making for Russian authorities; rather, there is the possibility that they were intentionally neglected, in some capacities, for the purpose of regime stability. In outlining these interconnected topics of i-voting, regime stability, and cybersecurity, this paper has also illuminated interesting trends in i-voting practices and diffusions in a non-democratic context, providing novel directions for future research on these topics.

References

1. Kabanov, Y., Romanov, B.: Interaction Between the Internet and the Political Regime: An Empirical Study (1995–2015). Digital Transformation and Global Society. pp. 282–291. Springer International Publishing, Cham (2017).
2. Karlsson, M.: Carrots and sticks: internet governance in non-democratic regimes. IJEG. 6, 179 (2013). https://doi.org/10.1504/IJEG.2013.058405.
3. Deng, J., Liu, P.: Consultative Authoritarianism: The Drafting of China's Internet Security Law and E-Commerce Law. Journal of Contemporary China. 26, 679–695 (2017). https://doi.org/10.1080/10670564.2017.1305488.
4. Kornreich, Y.: Authoritarian responsiveness: Online consultation with "issue publics" in China. Governance. 32, 547–564 (2019). https://doi.org/10.1111/gove.12393.
5. ELKheshin, S., Saleeb, N.: Assessing the Adoption of E-government Using Tam Model: Case of Egypt. IJMIT. 12, 1–14 (2020). https://doi.org/10.5121/ijmit.2020.12101.
6. Amanbek, Y., Balgayev, I., Batyrkhanov, K., Tan, M.: Adoption of e-Government in the Republic of Kazakhstan. JOItmC. 6, 46 (2020). https://doi.org/10.3390/joitmc6030046.
7. Sheranova, A.: Cheating the Machine: E-voting Practices in Kyrgyzstan's Local Elections. European Review. 28, 793–809 (2020). https://doi.org/10.1017/S1062798720000241.
8. Jiménez, R., Thurner, S., Pericchi, L.R., Klimek, P.: Fraud Detection, Electoral. In: Balakrishnan, N., Colton, T., Everitt, B., Piegorsch, W., Ruggeri, F., and Teugels, J.L. (eds.) Wiley StatsRef: Statistics Reference Online. pp. 1–10. Wiley (2018). https://doi.org/10.1002/9781118445112.stat08006.
9. Cebul, M., Pinckney, J.: Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution. 24 (2021).
10. Dragu, T., Lupu, Y.: Digital Authoritarianism and the Future of Human Rights. Int Org. 75, 991–1017 (2021). https://doi.org/10.1017/S0020818320000624.
11. Yayboke, E., Brannen, S.: A Strategic Approach to Digital Authoritarianism. 12 (2020).
12. Theys, S.: Introducing Constructivism in International Relations Theory. International Relations. 4 (2018).
13. Ciolan, I.M.: Defining Cybersecurity as the Security Issue of the Twenty First Century. A Constructivist Approach. 17 (2014).
14. Schwartz, J.: Compensating for the 'Authoritarian Advantage' in Crisis Response: A Comparative Case Study of SARS Pandemic Responses in China and Taiwan. J OF CHIN POLIT SCI. 17, 313–331 (2012). https://doi.org/10.1007/s11366-012-9204-4.
15. Cepaluni, G., Dorsch, M.T., Branyiczki, R.: Political Regimes and Deaths in the Early Stages of the COVID-19 Pandemic. 49 (2020).
16. Cheibub, J.A., Hong, J.Y.J., Przeworski, A.: Rights and Deaths: Government Reactions to the Pandemic. SocArXiv (2020). https://doi.org/10.31235/osf.io/fte84.
17. Turner, D.: Qualitative Interview Design: A Practical Guide for Novice Investigators. TQR. (2014). https://doi.org/10.46743/2160-3715/2010.1178.

Secure postal voting

Henri Devillez

UCLouvain, Crypto Group, Belgium

Abstract. There has been several recent attempts to enhance postal voting systems with the technologies of end-to-end voting systems to obtain the best of both worlds. Our contribution is two fold. We first propose a postal voting protocol that uses ballots interpretable by the voters, and then we give a security model in a simpler variant of the universally composable model (SUC) for which our protocol is provably secure.

1 Motivation and limitations

At the present time, the most common form of remote voting used in practice is postal voting. Despite its extreme simplicity, this naive system guarantees the remote elector that their vote is cast as intended through an human-readable format of the ballot and does not give any evidence of their choice after the ballot has been posted. However, the voter has no way to verify that their ballot has reached an election office and has been correctly counted in the tally. On the other end, there has been a lot of efforts to design verifiable electronic election systems with the use of cryptography.

Recently, there have been attempts to bring together these two approaches and keep the best of both worlds [1]. In this draft, we provide a protocol achieving these goals and an intuitive functionality in the universally composable model [2] capturing the desired privacy and verifiablity properties of vote-by-mail, for which our protocol is provably secure. We restrict ourselves to a strict setting in which ballots are downloaded and printed by the voter (hence preventing the use of special types of papers) and ballots cast by the voters are human-readable.

2 High level view of the protocol

We consider a protocol for remote elections in a vote-by-mail setting with approval voting ballots. By approval voting, we mean that given a list of candidates, a voter can choose to approve any subset of these candidates.

The election is overseen by a party called the election authorities (EA). This party sets the parameters of the election p, which consists in the list of valid voters, the list of candidates for which one can vote, the numbers of talliers.

Ballots are generated by an independent server, the ballots issuer (BI). When a voter asks the server for a ballot, the voter authenticates to the server (with an electronic ID for example) and receives a blank ballot. This blank ballot contains

a sheet with an unpredictable voting token and a list of candidate that the voter has to fill. The voter will then send this ballot to the election office (EO). The ballot also contains a sheet of codes and a note sheet. For each choice, the voter copies the code corresponding to their choices on the note sheet, then destroys the codes sheet. All the codes are also encrypted by the ballots issuer using a public key of a threshold encryption scheme run by the talliers. The encryptions of each of those codes are sent to the talliers, each time with the corresponding choice and an hash of the voting token associated to the voter and the choice.

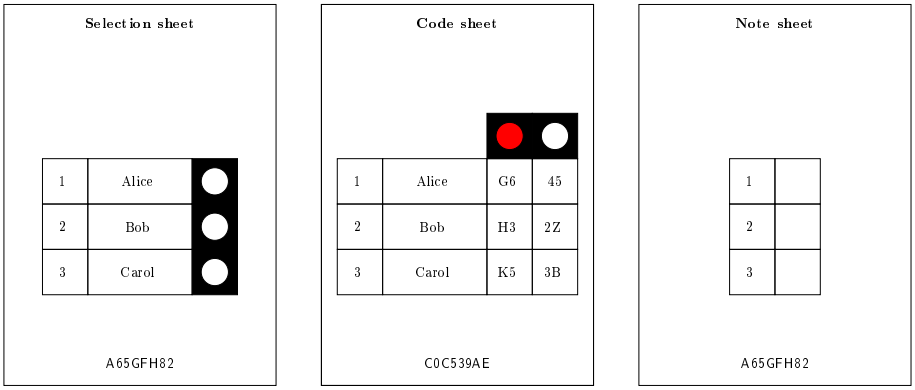


Fig. 1. example of ballot

During the tallying phase, the election office interacts with the talliers to compute the result of the election that can be published once every ballot has been counted. To do so, the election office sends to each tallier a hash of the voting token and the choices written on the ballot. The talliers recovers the corresponding choices and encryptions received from the ballot issuer. Hence each tallier can independently compute the tally of the election and if they all agree on the result, they decrypt together the codes matching each selected choice. These codes are then sent to a verification server (VS). Voters can later connect to this server to receive the decrypted codes and compare them with the codes they saved when they voted. As long as it is difficult to guess the code of the other choices, the voter has a guarantee that their choices have been correctly recorded and counted if they see the right codes when they interact with the verification server.

3 Security

We introduce a simulation-based security definition in a simpler variant of the universally composable model (SUC)[2] for the security of postal voting protocols. As usual in this framework, we define a trusted third party which would give natural security guarantees if it happened to exist. A protocol is secure if for

any adversary $\mathcal{A}$ against the protocol, there exists an adversary $\mathcal{S}$ (also called the simulator) such that a real execution of the protocol with the adversary $\mathcal{A}$ is indistinguishable from an ideal execution of the protocol with the trusted third party with $\mathcal{S}$.

In the ideal world, we define the ideal postal voting functionality as follows. Voters send their votes to this functionality instead of the election office and receive from it the output of the verification procedure at the end of the election.

Secure Postal Voting functionality

Setup Phase

When receiving a command $\mathsf{setup}(\mathsf{p})$ from EA, forwards the election parameters p to every voter and the simulator. In particular, p contains a probability $\mathsf{p\_limit}$ which is an upper bound on the probability of success of adversary changing the vote of a voter without him noticing anything. Then, assign to each voter a random distinct string handle. For each handle, keep in memory $\mathsf{ballots}^{\mathsf{cast}}_{\mathsf{handle}} = \{\}$ and $\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}} = \{\}$. Also, send to the simulator the mapping between the corrupted voters and their handle.

If the simulator replies with a command abort, send abort to EA. Otherwise if the simulator replies with a command $\mathsf{continue}$, enter the Voting phase.

Voting phase

- When receiving a $\mathsf{vote}(\mathsf{id}, \mathsf{v})$ command from the voter with identity id, append v to $\mathsf{ballots}^{\mathsf{cast}}_{\mathsf{handle}}$ and $\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}}$ where handle is linked to id.
- When receiving a $\mathsf{vote}(\mathsf{id}, \mathsf{v})$ command from the simulator, append v to $\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}}$ where handle is associated to id.
- If the postal channel is corrupted, the functionality has two additional commands. When receiving a command $\mathsf{get\_vote}(\mathsf{id}, \mathsf{i})$ from the simulator, send to the simulator the i-th vote v in the list $\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}}$. When receiving a command $\mathsf{modify\_vote}(\mathsf{id}, \mathsf{i}, \mathsf{new_v})$, modify the i-th vote in the list $\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}}$ into $\mathsf{new\_v}$. If $\mathsf{new\_v} = \perp$, drop the ballot instead.
- When receiving a $\mathsf{stop\_vote}$, enter in the Tallying phase.

Tallying phase

- When entering the $\mathsf{tallying}$ phase, send to the simulator a list of pairs of handle and the corresponding $\mathsf{vote}^{\mathsf{counted}}_{\mathsf{handle}}$.
- When receiving a command $\mathsf{modify\_ballot}(\mathsf{handle}, \mathsf{i}, \mathsf{new\_v})$ from the simulator, update the i-th vote of $\mathsf{vote}^{\mathsf{counted}}_{\mathsf{handle}}$ into $\mathsf{new\_v}$. If $\mathsf{new\_v} = \perp$, drop the ballot instead.
- When receiving a command abort from the simulator, send a message abort to EA.
- When receiving a command $\mathsf{publish}$ from the simulator, send to the dummy EA and to every voter the result of the election. The result r of the election is computed as follows:
  1. Set $r = \{\}$

2. For each handle, append $\perp$ to r if $|\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}}| \neq 1$. Otherwise append v to r where v is the unique vote of $\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}}$.

Then enter in the Verification phase.

Verification phase

For every voter, send a command verify(id) to the simulator. The simulator sends one of the following command in return:

- When receiving a command verification_fail from the simulator, send cheat to the voter with identity id.
- When receiving a command verification_success(p_success) from the simulator, ignore the command if p_success $>$ p_limit. Otherwise, send honest to the voter with identity id with probability p_success or cheat with probability $1 -$ p_success
- When receiving a command ballot_based from the simulator, send to the voter with identity id either:
  - cheat if the votes computed with $\mathsf{ballots}^{\mathsf{cast}}_{\mathsf{handle}}$ and $\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}}$ are not the same
  - nothing_received if $\mathsf{ballots}_{\mathsf{cast}} = \mathsf{ballots}_{\mathsf{counted}} = \{\}$
  - honest otherwise

Intuitively, every voter has an handle hiding their identity. The functionality will later know the vote of each handle but the mapping between the handles and the voters' id will remain secret, hence preserving the privacy (except for the corrupted voters or the leak caused by the postal channel corruption).

Regarding the individual verifiability of the election, the variables $\mathsf{ballots}^{\mathsf{cast}}_{\mathsf{handle}}$ and $\mathsf{ballots}^{\mathsf{counted}}_{\mathsf{handle}}$ respectively represent the voter's ballots that are cast by the voter and counted in the tallying procedure. These might be different because of the adversarial behavior, but in that case the voter will receive a cheat message with a probability at least p_limit.

Given this functionality, we can prove that the protocol sketched in Section 2 satisfies the following property:

Definition 1 (Secure postal voting). *A PVP $\mathcal{V}$ is secure if for any adversary $\mathcal{A}$, there exists an ideal adversary $\mathcal{S}$ such that for any environment $\mathcal{E}$, the probability that the environment distinguishes between the execution of the real protocol and an interaction with the ideal postal voting functionality is negligible. In this game, at most one of these sets of official parties is corrupted:* {EO *and all but one tallier*}, {BI} *and* {VS}. *Any number of voters and the postal channel can be corrupted.*

References

1. Benaloh, J.: Strobe-voting: Send two, receive one ballot encoding. In: International Joint Conference on Electronic Voting. pp. 33–46. Springer (2021)
2. Canetti, R., Cohen, A., Lindell, Y.: A simpler variant of universally composable security for standard multiparty computation. In: Annual Cryptology Conference. pp. 3–22. Springer (2015)

Moving Forward by Looking Back:

Learning From Unsuccessful E-voting Projects in Europe

Leo Fel[1][0000-0002-5896-0640]

[1] University of Luxembourg, Esch-sur-Alzette, Luxembourg
leo.fel@uni.lu

Abstract. Unsuccessful e-voting projects are more common than successful ones, yet they are underrepresented in the e-voting literature. Therefore, an interdisciplinary research proposal is offered to highlight the importance of failed e-voting endeavours by investigating the causes and consequences of failure. Besides answering why European e-voting projects are prone to fail rather than succeed, special attention is paid to the impact of that kind of outcome on future e-voting initiatives and to the examination of the state-of-the-art e-voting solutions and experiences that may overcome detected failures in the future. Towards that end, four case studies (Germany, Netherlands, Norway, UK) will be conducted to uncover context-specific and common failure sources. Ultimately, underlining the project's policy dimension, recommendations for policymakers will be formulated to improve the process of e-voting evaluation and implementation.

Keywords: e-voting, failure, interdisciplinary research.

1 Introduction

Many European countries have been trying to boost citizen participation in the electoral process by introducing technology in what is still considered to be "the realm of pen and paper". Besides improving turnout, particularly among previously underrepresented segments of the electorate, technology utilization also demonstrates potential benefits in enabling more accurate vote counts and creating an easy and convenient voting experience.

Nevertheless, successful e-voting[1] projects are an exception rather than a common phenomenon. In Europe, Estonia is the first and only country that has implemented e-voting completely, while Belgium and France have implemented it partially. In contrast, countries with long democratic traditions such as Germany, the Netherlands, Norway, and the UK[2] cancelled or did not continue with the implementation [7]. It is worth noting that Switzerland is currently in the process of reintroducing i-voting trials [1]. Despite that fact, a vast majority of e-voting research focuses on projects – particularly Estonian

[1] In this paper, electronic voting (e-voting) is defined as 'the use of electronic means to cast and/or count the vote' [2]. In this context, if not stated otherwise, e-voting refers to on-site e-voting and internet voting (i-voting).

[2] Alongside them are, for instance, Finland, Ireland and Italy. In the context of this research proposal, emphasis is given to case studies of the four countries mentioned above.

and Swiss – which are, although more or less successful, still uncommon in the general e-voting landscape.
This consideration urges us to concentrate on the prevailing e-voting project outcome – failure – that may be even more crucial for e-voting introduction in Europe than the few successful examples. At the very least, failure is as crucial as success and thus deserving of in-depth study.

2 Project relevance

Democracies with long traditions of free and fair elections, such as Germany, the Netherlands, Norway, and the UK, all at one point launched e-voting projects that, suddenly faced with various challenges, ultimately failed. Proclaimed reasons for what the literature calls abandonment, cancellation and/or discontinuation of e-voting[3] in the subject countries can be summarized as (a) trust issues and security concerns raised by various social groups, particularly civil society and experts [5, 7, 8] and (b) non-compliance of employed technological solutions with established legal requirements [7, 8].
E-voting failures are, in essence, policy failures, studied in more detail by Howlett [6]. Policy failures are of various types (program, process, and political issues); they occur in different stages of the policy cycle (agenda setting, formulation, decision-making, implementation, and evaluation phase); and they have several dimensions (extent, avoidability, visibility, intentionality, duration, and intensity). By internalizing that a failure is a complex, multifaceted phenomenon, it is possible to scratch beneath the surface to uncover other causes of e-voting failures apart from those officially declared. For instance, security concerns triggered by inadequate e-voting solutions might have deeper roots in the lack of sufficient funds or incompetence of those responsible for its development.
Revisiting unsuccessful e-voting projects in Germany, the Netherlands, Norway, and the UK is relevant for several reasons. First, failed e-voting efforts transcend boundaries and influence others who look attentively at public policy outcomes in role model countries. Second, this 'discourage effect' may hinder or block new e-voting initiatives. Third, e-voting trials and deployment are the best way to improve e-voting solutions and generate new knowledge. Fourth, this orientation is in line with recent research suggestions, which encourage the investigation of reasons for e-voting abandonment and conducting comparative case studies [3]. Lastly, recommendations based on failure examples can support policymakers who seek sound empirical findings to decide whether to reintroduce e-voting projects.

3 Research design

The proposed research aims to illuminate the causes and consequences of e-voting projects failures in Europe. Therefore, the research question is: *Why are e-voting projects in European democracies prone to fail rather than succeed?* Two additional sub-

[3] "E-voting failures" refers to all of those three and other similar phrases.

questions are: (1) *To what extent do those failures influence new e-voting initiatives in the subject countries and the rest of Europe?* (2) *Could some of the obstacles from previous e-voting projects be overcome with the help of state-of-the-art e-voting solutions and experiences?*

The project is designed in the form of a small-C comparative case study research including Germany, Netherlands, Norway and UK [4]. Factors such as type of e-voting, implementation phase, the scale of implementation, and proclaimed reasons for failures are different across cases, whereas the outcome is identical. What is more, selected cases are considered significant in the European context, and are a solid point of departure by offering an amount of existing literature, documents, and other valuable pieces of information.

When it comes to data collection, the first phase will be conducted as desk research to collect existing research and other data collections (e. g. legal documents, reports, feasibility studies, media content). The second phase is fieldwork in the form of semi-structured interviews with relevant stakeholders (politicians, election officials, activists, researchers, judges). Within-case evidence will be combined with cross-case analysis to point out the strengths of both.

Interdisciplinarity is a distinctive characteristic of this project situated at the intersection between political science, law, and computer science. The project emphasises the institutional level of e-voting implementation, understanding e-voting as a failed public policy that needs to be analysed retrospectively. Political analysis is also beneficial in exposing the impact of e-voting failures on further e-voting initiatives. Not forgetting that elections are subject to regulation, e-voting legal frameworks will be assessed and mutually compared, while relevant case law will be studied. As e-voting is tech-driven, computer science will be employed to provide a deeper insight into technical vulnerabilities and to examine the possibilities of recent technology in overcoming detected limitations.

4 Expected outcome and significance

This interdisciplinary project will contribute to mapping common and context-specific causes of e-voting failures in the European context. That will help better understand all the challenges policymakers encounter when designing public policies on new technologies, particularly those linking democratic processes with technology. Last but not least, policy recommendations will be formulated for a sensible e-voting evaluation and implementation.

References

1. Ch.ch, ://www.ch.ch/en/votes-and-elections/e-voting, last accessed 2022/6/20.
2. Council of Europe, Committee of Ministers: Recommendation CM Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (2017).
3. Darmawan, I.: E-voting adoption in many countries: A literature review. Asian Journal of Comparative Politics 6(4), 482-504 (2021).

4. Gerring, J.: Case Study Research: Principles and Practices. 2nd edn. Cambridge University Press, Cambridge (2017).
5. Goos, K., Beckert, B., Lindner, R.: Electronic, Internet-Based Voting. In: Lindner, R., Aichholzer, G., Hennen, L. (eds.) Electronic Democracy in Europe. Springer, Cham (2016).
6. Howlett, M.: The lessons of failure: learning and blame avoidance in public policy-making. International Political Science Review 33(5), 539–555 (2012).
7. Risnanto, S., Rahim, Y.B.A., Herman, N.S., Abdurrohman.: E-voting readiness mapping for general election implementation. Journal of Theoretical and Applied Information Technology 98(20), 3280-3290 (2020).
8. Vegas, C., Barrat, J.: Overview of Current State of E-voting Worldwide. In: Hao, F., Ryan, P.Y.A. (eds.) Real-World Electronic Voting: Design, Analysis and Deployment. 1st ed. CRC Press, Boca Raton (2016).

SoK: Secure E-voting with Everlasting Privacy

Rafieh Mosaheb

SnT, University of Luxembourg, rafieh.mosaheb@uni.lu

Abstract. In this work, we systematically analyze all e-voting protocols designed to provide everlasting privacy. Our main focus is to illustrate their relations and to identify the research problems which have or have not been solved in this area.

Keywords: electronic voting · everlasting privacy · protocol analysis.

1 Introduction

In all elections, it is crucial to ensure that the final election result correctly reflects the votes chosen by the voters. Moreover, voters' individual votes must remain secret so that the final result is not biased by those who are afraid to express their own will freely. In order to guarantee these two fundamental properties, modern *secure* e-voting protocols strive for (end-to-end) verifiability and (vote) privacy. In order to guarantee verifiability, some information about the voters' individual choices needs to be public. Since, at the same time, vote privacy must not be jeopardized, essentially all verifiable e-voting systems used in practice today (e.g., Helios [8] or Belenios [3]) employ the following approach: voters encrypt their votes under the talliers' public key, publish the resulting ciphertexts, and the talliers use their secret key to process these ciphertexts to obtain the final result. Now, the problem is that secrecy of all public-key encryption schemes deployed in these systems (e.g., ElGamal) is based on certain computational hardness assumptions (e.g., decisional Diffie-Hellman) that ensure vote privacy at the time of the election, but not necessarily in the long run. A future adversary, who learns from public data of past elections which ciphertext belongs to which voter, may therefore exploit novel (previously unknown) algorithms or more powerful machines (e.g., quantum computers) to efficiently solve the underlying hardness assumptions and thus break privacy of voters retrospectively. As explained above, such a risk is unacceptable for many real-world elections.

Fortunately, in order to ensure that vote privacy remains preserved in the future, numerous e-voting protocols have been proposed in the academic literature (e.g., [1, 2, 9, 10, 4]). These protocols strive for what is called *everlasting privacy*. This property ensures that privacy is protected *unconditionally* so that even a computationally unbounded adversary is not able to learn how individual voters voted. Most of the e-voting protocols mentioned above actually aim for a weaker notion of everlasting privacy. In fact, these protocols are designed to

guarantee unconditional privacy towards any external adversary who can access all public election data but who is not able to monitor the whole communication network. This relaxed notion of everlasting privacy is called *practical everlasting privacy* [5]. It accurately models the overall threat scenario of a future adversary who knows all public material required to verify an election and who is able to break any computational hardness assumption.

In the next sections, we explain our methodology and then describe our key findings.

2 Methodology

We use the following approach to systematically analyze the state-of-the-art in secure e-voting with everlasting privacy:

1. We study the academic literature to find all relevant existing protocols in this field.
2. We classify existing protocols according to how they (intend to) provide everlasting privacy technically. Moreover, we illuminate how different protocols depend on each other.
3. We analyze which existing protocols are practically efficient and guarantee public verifiability as well as (practical) everlasting privacy under realistic assumptions. To this end, we investigate which protocols actually achieve the properties they were designed for originally, and we critically reflect on the assumptions that existing protocols make.
4. Based on our analysis in the previous steps, we identify which research problems have already been solved and which ones are still open.

We collected 25 existing e-voting protocols designed for secure e-voting with everlasting privacy, however, for the sake of limited space we refer interested readers to the full paper.

3 Our Classification

We propose a classification that captures all existing e-voting protocols aiming for everlasting privacy. We identify two different classes of existing protocols, B-ANON and B-ID. In B-ANON, everlasting privacy reduces to publishing ballots anonymously. On the contrary, in B-ID, where public ballots are identifiable, everlasting privacy is based on the privacy-preserving technique to tally ballots. We argued in the full paper that the general approach taken in B-ID is superior to the one in B-ANON; in short: B-ID $>$ B-ANON. We observe that the two main classes B-ANON and B-ID essentially differ in two aspects: (1) the method used to ensure everlasting privacy as well as the phases when the respective method is applied, and (2) the technique employed to guarantee public verifiability.

4 Solved and problems

4.1 Solved problems

We discover that in both classes, B-ID and B-ANON, there exist reasonable protocols for secure e-voting with everlasting privacy under the respective assumptions made in these classes. For everlasting privacy, all of these protocols consider future adversaries that are not active during an election. We distinguish between those protocols that can handle simple ballot types (e.g., where voters can choose one candidate) and those which can handle arbitrary ballot types (e.g., where voters can rank candidates).

Observation 1 (Simple ballot types) *In B-ID, there exist two secure approaches that can handle simple ballot types: the one based on [1] and the one based on the homomorphic version of [2]. While [2] offers everlasting privacy towards the public (i.e, practical everlasting privacy), [1] additionally offers everlasting privacy towards a threshold of talliers.*

Observation 2 (Arbitrary ballot types) *In B-ID, there exists one secure approach that can handle arbitrary ballot types, the one based on the mix net version of [2]. In B-ANON, there exist two reasonably secure approaches that can handle arbitrary ballot types [3, 4]. These protocols offer practical everlasting privacy.*

All of the approaches mentioned before are sufficiently efficient for large-scale elections. In particular, Belenios [3] has already been deployed in many real-world elections.

4.2 Open problems

The most important open problems are:

1. *Formal protocol analysis:* While the cryptographic components of the promising approaches [1, 2, 4] have been analyzed in-depth, it is an open problem to formally analyze these proposals on the *protocol* level. It is also an open problem to formally analyze everlasting privacy of Belenios [4].
2. *Deployable e-voting system:* While Belenios [3], which is in B-ANON, can be deployed for real-world elections, it is an open problem to develop a full-fledged deployable e-voting system that realizes one of the promising approaches [1, 2] in the superior class B-ID.
3. *Weaker trust for arbitrary ballot types:* All promising approaches that can handle arbitrary ballot types [2, 4, 3] require that all election authorities or all talliers are trusted for everlasting privacy. It is an open problem to mitigate trust on the authorities in terms of everlasting privacy for arbitrary ballot types.
4. *Receipt-freeness:* In all of the promising approaches [1, 2, 4, 3], some evidence is created on the voters' devices that can serve as a proof for how the voter voted. It is an open problem to securely and efficiently improve [1, 2, 4, 3] so that they are free of such receipts.

From our point of view, the first two open problems (formal protocol analysis and development of a deployable system in B-ID) are the most pressing ones. We note that for automated verification, there exist appropriate symbolic definitions to address the first open problem, for example [5] for everlasting privacy and [6] for verifiability/accountability; recent advances [7] facilitate applying these definitions in a joint verification platform.

5 Conclusion

We demonstrated that there exist four promising approaches [1, 2, 4, 3] among the numerous proposals for secure e-voting with everlasting privacy. These solutions offer the potential to guarantee everlasting privacy in real elections. These approaches significantly differ in the assumptions that they need to make for everlasting privacy. While [4, 3] need to assume that voters submit their ballots anonymously, the other two approaches can avoid this often unrealistic assumption. Therefore, [1, 2] are preferable whenever distributing the trustee is feasible.

We identified two important open problems, one of theoretical and the other one of practical nature. First, it is fundamental to formally analyze the security of all promising protocols [1, 2, 4, 3]. Second, it is desirable to realize the two strongest proposals [1, 2] so that they can be deployed to guarantee everlasting privacy of elections in the real world, not only in theory.

References

1. Cramer, R., Franklin, Matthew K., Schoenmakers, B., Yung, M.: Multi-Autority Secret-Ballot Elections with Linear Work. In: EUROCRYPT 1996, pp. 72–83.
2. Cuvelier, E., Pereira, O., Peters, T.: Election Verifiability or Ballot Privacy: Do We Need to Choose?. In: ESORICS 2013, pp. 481–498.
3. Cortier, V., Gaudry, P., Glondu, S.: Belenios: A Simple Private and Verifiable Electronic Voting System. In: Foundations of Security, Protocols, and Equational Reasoning 2019, Springer, pp. 214–238.
4. Locher, P., Haenni, R.: Verifiable Internet Elections with Everlasting Privacy and Minimal Trust. In: VoteID 2015, pp. 74–91.
5. Arapinis, M., Cortier, V., Kremer, S., Ryan, M.: Practical Everlasting Privacy. In: POST 2013, pp. 21–40.
6. Morio, K., Künnemann, R.: Verifying Accountability for Unbounded Sets of Participants. In: 34th IEEE Computer Security Foundations Symposium, CSF 2021, pp. 1–16.
7. Cheval, V., Jacomme, C., Kremer, S., Künnemann, R.: SAPIC+: Protocol Verifiers of the World, Unite!. In: USENIX Security Symposium, 2022.
8. Adida, B.: Helios: Web-based Open-Audit Voting. In: USENIX Security 2008, pp. 335–348.
9. Moran, T., Naor, M.: Split-ballot voting: everlasting privacy with distributed trust. In: ACM CCS 2007, pp. 246–255.
10. Buchmann, J., Demirel, D., Van de Graaf, J.: Towards a Publicly-Verifiable Mix-Net Providing Everlasting Privacy. In: FC 2013, Revised Selected Papers, pp. 197–204.

Code Voting for Swiss Internet Voting

Florian Moser[1][0000−0003−2268−2367]

ETH Zürich, Switzerland moserfl@ethz.ch

1 Introduction

Switzerland is attempting to introduce an internet voting channel, with serious efforts starting as early as 2001 [7]. However, a clear solution has not yet been established: Switzerland has seen multiple systems come and go [8,5,13], along with three major revisions of its applicable law [9].

As Switzerland attempts to re-introduce internet voting, Swiss Post has the only viable system in reach. It is based on a system once distributed by Scytl [21]. While it was gradually extended over time, the core mechanisms remained the same [1,12,25]. As did the feedback: Critics regret low implementation quality [19,17,18] and very complex proofs and specification [20,28,10].

We believe the complexity of the protocol is indeed a serious issue that reduces implementation quality, makes reviews hard, and ultimately also undermines full trust in the system. But redesigning the protocol based on the same assumptions and same mechanisms will likely not result in a much simpler protocol; this has been attempted by experienced researchers in 2017 in the form of CHVote [14,3], which also turned out to be complex.

2 Code Voting

We propose tackling the complexity using code voting [11,23,4]. In code voting, each voting option is associated with a voting code. For each voter, these voting codes are then randomly permuted into voter-specific voting codes. To cast a vote, the voter submits the appropriate voting code.

If the voting server and network are untrusted, as it is the case in the Swiss setting, submitted voting codes are attributable to individual voters. To remedy this issue, code voting may be used with a privacy-preserving tally mechanism (e.g. verified shuffle), by mapping cast voting codes to ciphertext representing the voting choice. The same authority already responsible for generating the voter-specific permutation of the voting codes can generate the appropriate lookup.

With code voting, the voter's device needs not be trusted for privacy, as the voting option is already entered in an encrypted form. Additionally, code voting promises to reach a notion of everlasting privacy, as, by the voter-specific permutation, the voter-specific voting codes are a perfect encryption of the voting options.

Code voting also allows using simpler and fewer cryptographic operations. If voter-specific encryption keys are generated by multiple authorities, the voter-specific permutations are applied one after the other. If the vote is sent over an

insecure network, the voter's device no longer needs to encrypt, but can simply forward the voting code. Consequentially, the voter no longer needs to enter a security-level appropriate encryption key, the expectedly much shorter voting codes suffice.[1] The validation of the vote is trivial, as valid voting codes are public information. To implement return codes, a voter-specific lookup, mapping each voting code to the appropriate return code, is sufficient.

For the voter, the process of casting a vote changes: Instead of entering the voting option, they now have to enter the corresponding voting code. It is our understanding, strengthened by corresponding communications with the Swiss chancellery, that the current Swiss law does not forbid code voting. An extension of the Swiss Post Protocol incorporating code voting has been shown to not reduce general usability [29].

3 Proofs

The proposed code voting scheme needs to be proven secure. Swiss law [9] mandates computational and symbolic proofs of four high-level properties, that we decompose into provable formal definitions while respecting Swiss particularities (for example, the availability of multiple voting channels).

Individual verifiability is defined to hold by Swiss law when voters are given exactly one of two proofs: Voters who participate electronically are given a proof that the vote has been registered successfully by the server, exactly as cast. Voters who did not participate electronically can request a proof that their vote has not been registered by the server [6, article 5.2, appendix 2.5]. The literature usually only refers to the first proof as individual verifiability (see [24,15,3]). We cover the second proof with an additional property we call *Participation Verifiability*; a new term, as we are not aware of this property being used in the literature.[2][3] We guarantee the "registered successfully" part by proving *Vote Verifiability* that ensures all votes represent valid voting options.[4]

Universal Verifiability is defined to hold when the auditors are given a proof that the result is composed out of all, and only out of, successfully registered votes [6, article 5.3, appendix 2.6]. This property is consistent with its use in literature (see [24,15,3]), although Swiss law only requires it to hold for auditors.

Vote Secrecy is defined to hold if the plaintext vote cannot be attributed to the voter, and *Fairness* ensures the attacker does not learn partial election results before the official tally [6, article 7, appendix 2.7]. While this intuition matches the literature, established privacy definitions such as BPRIV or Benaloh do not apply to return-code based schemes [2,28]. Further, we are not aware of any formal definition or proof of fairness; although depending on how both properties are formally defined, privacy might imply fairness.

[1] The voting codes need only be long enough to represent all voting choices.
[2] The property remains unproven for CHVote [3] and the Swiss Post protocol [22].
[3] The property was however discussed as part of Selections [27].
[4] This property is also referred to as ballot verifiability [3] or vote compliance [22].

Authentication is defined to hold when the attacker cannot insert votes without controlling the voter [6, appendix 2.8]. In the literature, this property is usually referred to as *Eligibility Verification* (see [16,26,15,3]). Implicitly, the law also requires that voters must only cast and confirm a single vote, which we refer to as *Eligibility Uniqueness*, as in the verifiability analysis of CHVote [3].

We introduce the formal definitions free from potentially complex protocol-specific syntax. This enables fruitful discussions over whether the definitions indeed capture the security notions implied by the Swiss law, while not limiting the discussions to experts of the concrete protocol. Further, we aim for as consistent definitions as possible. This makes it easier to think about whether all necessary properties have been captured; and it allows to simplify the proofs (e.g. by reusing game hops of similar properties). As another way to simplify the proofs, we aim to encapsulate the privacy-preserving tally mechanism and prove it separately.

4 References

[1] Allepuz, J.P., Castelló, S.G.: Cast-as-intended verification in Norway. In: Proc. 5th Conf. Electron. Voting. pp. 49–63. Citeseer (2012)

[2] Bernhard, D., Cortier, V., Galindo, D., Pereira, O., Warinschi, B.: Sok: A comprehensive analysis of game-based ballot privacy definitions. In: 2015 IEEE Symposium on Security and Privacy. pp. 499–516. IEEE (2015)

[3] Bernhard, D., Cortier, V., Gaudry, P., Turuani, M., Warinschi, B.: Verifiability analysis of CHVote. report, Bernhard, David and Cortier, Véronique and Gaudry, Pierrick and Turuani, Mathieu and Warinschi, Bogdan (2018)

[4] Budurushi, J., Neumann, S., Olembo, M.M., Volkamer, M.: Pretty understandable democracy-a secure and understandable internet voting scheme. In: 2013 International Conference on Availability, Reliability and Security. pp. 198–207. IEEE (2013)

[5] Bundeskanzlei, S.: Bundeskanzlei nimmt Standortbestimmung zum E-Voting vor. (March 2019)

[6] Bundeskanzlei, S.: Vorentwurf Verordnung der BK über die elektronische Stimmabgabe(VEleS) (April 2021)

[7] Bundesrat, S.: Bericht über den Vote électronique: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte. report, Schweizerischer Bundesrat (February 2002)

[8] Bundesrat, S.: Nationalratswahlen mit dem elektronischen Stimmkanal (August 2015)

[9] Bundesrat, S.: Vorentwurf Verordnung über die politischen Rechte(VPR) (April 2021)

[10] Bundesrat, S.: E-Voting: Ergebnisse der ersten unabhängigen Überprüfung liegen vor (April 2022)

[11] Chaum, D.: Sure Vote: Technical Overview. In: Proceedings of the workshop on trustworthy elections (WOTE 2001) (2001)

[12] Galindo, D., Guasch, S., Puiggali, J.: 2015 Neuchâtel's cast-as-intended verification mechanism. In: International Conference on E-Voting and Identity. pp. 3–18. Springer (2015)
[13] et canton de Genève, R.: Elections fédérales 2019: le canal de vote électronique ne sera pas proposé. (June 2019)
[14] Haenni, R., Koenig, R.E., Locher, P., Dubuis, E.: CHVote System Specification. IACR Cryptol. ePrint Arch. **2017**, 325 (2017)
[15] Jonker, H., Mauw, S., Pang, J.: Privacy and verifiability in voting systems: Methods, developments and trends. Computer Science Review **10**, 1–30 (2013)
[16] Kremer, S., Ryan, M., Smyth, B.: Election verifiability in electronic voting protocols. In: European Symposium on Research in Computer Security. pp. 389–404. Springer (2010)
[17] Locher, P., Haenni, R., Koenig, Reto E, B.F.: Analysis of the Cryptographic Implementation of the Swiss Post Voting Protocol. report, Berner Fachhochschule (July 2019)
[18] Locher, P., Haenni, R., Koenig, R.E., Dubuis, Eric, B.F.: Examination of the Swiss Post Internet Voting System. report, Berner Fachhochschule (March 2022)
[19] Østvold, B.M., Karlsen, E.K.: Public Review of E-Voting Source Code: Lessons learnt from E-Vote 2011. Norsk informatikkonferanse (2012)
[20] Pereira, O., Teague, V.: Report on the SwissPost-Scytl e-voting system, trusted-server version. report, Pereira, Olivier and Teague, Vanessa (July 2019)
[21] Post, S.: Ein E-Voting-System für die Schweiz aus der Schweiz (June 2020)
[22] Post, S.: Protocol of the Swiss Post Voting System: Computational Proof of Complete Verifiability and Privacy. Version 0.9.10. report, Schweizerische Post (July 2021)
[23] Ryan, P.Y., Teague, V.: Pretty good democracy. In: International Workshop on Security Protocols. pp. 111–130. Springer (2009)
[24] Sako, K., Kilian, J.: Receipt-free mix-type voting scheme. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 393–403. Springer (1995)
[25] Scytl: Swiss Online Voting Protocol. report, Scytl (2018)
[26] Smyth, B., Ryan, M., Kremer, S., Kourjieh, M.: Towards automatic analysis of election verifiability properties. In: Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security. pp. 146–163. Springer (2010)
[27] Spycher, O.: Trustworthy internet voting: defeating powerful coercers and vote-buyers. Ph.D. thesis, University of Fribourg, Switzerland (2015)
[28] Thomas Haines, Olivier Pereira, V.T.: Report on the Swiss Post e-Voting System. report, Thomas Haines, Olivier Pereira, Vanessa Teague (March 2022)
[29] Volkamer, M., Kulyk, O., Ludwig, J., Fuhrberg, N.: Increasing security without decreasing usability: A comparison of various verifiable voting systems. In: Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). pp. 233–252 (2022)

Impact of Technological Factor on Cloud Computing adoption for Electoral Data Management in Nigeria; a mediating effect of Environmental factor

Abigail Udoma [0000-0002-3499-7115]

[1] De Montfort University, Leicester, United Kingdom
abigailudoma2@gmail.com

Abstract. This study was carried out to ascertain the impact of technological factor on the adoption of cloud computing for electoral data management in Nigeria with consideration to the mediating impact of environmental factors. This study adopted inferential research design Three important stakeholders were engaged as target participants which included members of the general public who are of voting age (18 years and above), members of civil society organizations (CSOs) engaged in election monitoring; and INEC personnel. The study's data collection was through questionnaire and then analysed with the Structural equation model (SEM) AMOS of the SPSS. The results revealed that Technological factors significantly and positively affect cloud-based computing adoption in Nigeria electoral system, and that environmental factor partially, positively and significantly mediate in the relationship between Technological factors and cloud-based computing adoption in Nigeria electoral system, it was then concluded, among others, that an increase in the technological factors of cloud computing such as security, privacy, reliability and desirability would result to significant increase in the chances of adoption of the cloud computing technology, it was therefore recommended among others, that cloud computing service provider should ensure the security, reliability and desirability values of their services are maintained and constantly improved as such would increase the chances of government agencies like INEC demanding and adopting their services.

Keywords: Technological, Environmental factors, adoption, cloud computing

1 Introduction

The Independent National Electoral Commission (INEC) of Nigeria has been tasked with the primary responsibility of holding free and fair elections. So, the commission must use internationally known best practices such as the deployment of suitable data collecting, storage and dissemination technology. The commission is allowed to use any technology it deems necessary to carry out its core mandate of organizing free, fair, and credible elections in order to guarantee the long-term stability of Nigeria's democracy [1].

Therefore, it is critically crucial that cloud computing infrastructure be considered if INEC is to play a critical role in re-establishing trust in the Nigeria electoral system and in the Nigeria, government following the events of previous elections, and if elections are to be free, fair, and credible in accordance with globally accepted best practices. Thus, INEC must seek to prioritize the use of a comprehensive, secured, inclusive and transparent technology in the voting, collation, and transmission of election results as well as assertive communication to the general public on the use of this technology for voting, collation and transmission of results. To suggest a solution to this concern, this research study examine possibility of solving this problem by assessing the possible impacts of technological factors on the adoption of the cloud computing system in the Nigeria electoral system and the possible mediating impact of environmental factors.

2 Conceptual Frameworks

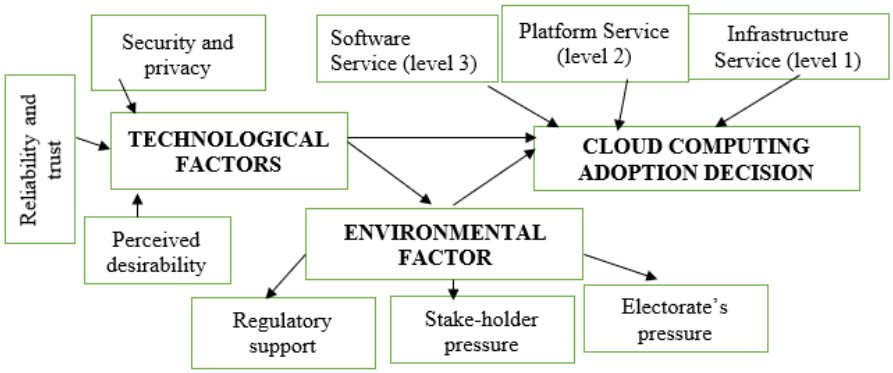


Fig. 1. Conceptual framework of the relationship between technological factor and cloud computing adoption with mediating impact of environmental factor

3 Methodology

This study adopted inferential research design which involves investigating cause-and-effect relationships. This involve determining the relationship between two variables in the case of this study we are concerned with assessing the impact of technological factors on cloud computing adoption and also to determine whether environmental factor mediate between impacts of technological factors on cloud computing adoption.

Three important stakeholders were engaged as target participants. (1) members of the public; the main criterion for selection was nationality (Nigerian) and age (voting age of 18 years and above) (2) members of civil society organizations (CSOs) engaged in election monitoring; and (3) INEC personnel. As a result, the study's data collection was confined to the capital Abuja. The homogeneous sampling method was used to identify individuals with common traits or a collection of shared features. In total, 600 respondents were sampled and used in the survey, and the stakeholder breakdown is as

follows: 300 individuals & households (electorate), 150 INEC employees and 150 CSO.

Questionnaire was used as research instrument and it contain two different section, section one contains questions on social demographical variables of the respondents while section two contain questions on technological factors, environmental factors and adoption of cloud computing. The questionnaire is self-administered and was completed by the respondents independently. The questionnaire has a variety of questions that were evaluated using 5 points Likert scale. The questionnaire is intended to gather data from three stakeholders sampled which included general population, civil society organizations, and INEC personnel.

The Structural equation model (SEM) AMOS of the SPSS was used for data analysis. Explanatory factor analysis was used to ascertain the number of latent variables. Confirmatory factor analysis was conducted to confirm the measurement model which involves the reliability and validity test while structural model was used to test the relationship between the model variables.

4 Results

CMIN/df	GFI	AGF	CFI	TLI	RMSEA	RMR
3.16	0.941	0.912	0.962	0.951	0.063	0.033
Good	Good	Good	Good	Good	Good	Good

Table 1. Model Fit Parameters

Group (levels)	*Construct*	*Path Coefficient*	*P value*	*Effect Size*	*Conclusion*
Level1: (IAAS)	TF	0.133	0.002	0.0016	Positive, Weak and Significant Impact
Level2: (PAAS)	TF	0.377	0.000	0.375	Positive, Strong and Significant Impact
Level3: (SAAS)	TF	0.391	0.000	0.215	Positive, Moderate and Significant Impact

$P < 0.05$ is significant and $p>0.05$ is insignificant.

Table 2. SEM, AMOS output after bootstrapping considering different cloud computing adoption level and the technological factor constructs

- H1: Technological factors significantly and positively affect the decision to adopt cloud-based computing in Nigeria electoral system:

This hypothesis is segregated into three sub-sections to capture the three level of cloud computing adoption and they are stated as follow:

- H1a: Technological factors significantly and positively affect cloud-based computing adoption level 1 in Nigeria electoral system

- H1b: Technological factors significantly and positively affect cloud-based computing adoption level 2 in Nigeria electoral system
- H1c: Technological factors significantly and positively affect cloud-based computing adoption level 3 in Nigeria electoral system

From Table 4 it is observed that at level one, the relationship between technological factor and cloud computing adoption is positive, with path coefficient of 0.133, weak with effect size 0.0016 (less than 0.15) and significant with p-value of 0.002 less than 0.05, thus the alternate hypothesis is accepted which stated that technological factors positively and significantly affect the adoption of first level cloud computing system into Nigeria electoral system. At level 2, it was observed from Table 4 that the relationship between technological factor and adoption of second level cloud computing is positive, with path coefficient of 0.377, strong, with effect size 0.375 (greater than 0.55) and significant with p-value of 0.000 less than 0.05, thus the alternate hypothesis is accepted which stated that technological factors positively and significantly affect the adoption of second level cloud computing system into Nigeria electoral system. At level 3, it was observed from Table 4 that the relationship between technological factor and adoption of third level cloud computing is positive, with path coefficient of 0.391, moderate, with effect size of 0.215 (less than 0.35 but greater than 0.15) and significant, with p-value of 0.000 less than 0.05, thus the alternate hypothesis is accepted which stated that technological factors positively and significantly affect the adoption of third level cloud computing system into Nigeria electoral system.

Hypothesis	*Relation*	*Path weight*	*p-value*	*Conclusion*
H2	TF → CCADecision	0.384	0.000	Positive and significant
	TF → EF → CCADecision	0.065	0.000	Partial mediation effect

$P < 0.05$ is significant and $p>0.05$ is insignificant.

Table 3. path weights and significance levels for the mediating effect

- H2: Environmental factor significantly mediate in the relationship between technological factor and cloud computing adoption in Nigeria electoral data maangement

The second hypothesis as shown in Table 5 revealed that the direct relationship between technological factor and cloud computing adoption is positive with path weight estimate of 0.384 and significant with p-value of 0.000 (less than 0.05) and the indirect relationship between technological factor and cloud computing adoption with mediating effect of environmental factor is also positive and significant with path weight estimate value of 0.065 and p-value of 0.000. Thus, this result implies that the environmental factor played a partial mediating role in the relationship between technological factor and cloud computing adoption, therefore alternate hypothesis is accepted which states that environmental factor has a significant but partial mediating impact on the relationship between technological factor and cloud computing adoption in Nigerian electoral system

5 Conclusion and recommendation

Based on the results and finding of this study, the following conclusion were drowned; one, It was concluded that the INEC official, CSOs and electorate agree that cloud computing technology is secured, reliable and suitable for INEC adoption for data management because they believe it is the solution to the problem of election data manipulation and rigging common experience in Nigeria elections. It was recommended that cloud computing service provider should ensure that the security; reliability and desirability values of their services are maintained and constantly improved as such would increase the chances of government agencies like INEC to demand and adopt their services.

References.

1. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. (2011), "Cloud computing, the business perspective"Decision support systems, 51 (1) 176-189

Is the JCJ voting system really coercion-resistant?

Véronique Cortier, Pierrick Gaudry, Quentin Yang

Université de Lorraine, Inria, CNRS

Abstract. Coercion-resistance is a security property of electronic voting, often considered as a must-have for high-stake elections. The JCJ voting scheme, proposed in 2005, is still the reference when designing a coercion-resistant protocol. We highlight a weakness in JCJ that is also present in all the systems following its general structure. It comes from the procedure that precedes the tally, where the trustees remove the ballots that should not be counted. This phase leaks more information than necessary, leading to potential threats for the coerced voters. Fixing this leads to the notion of *cleansing-hiding*, that we apply to form a variant of JCJ that we call CHide. This is a shorter version of [5].

1 Introduction

Internet voting allows to take part into an election without being physically present. It is used for politically-binding elections in several countries. For such contexts, coercion is an important threat which occurs when an attacker forces a voter to vote in a specific way, using a threat or a reward. It is known to exist in traditional elections, but an electronic voting solution which is not designed to tackle it could allow the attacker to coerce a larger number of voters, or to gain a more convincing evidence that the coerced voters actually obeyed.

A famous protocol designed to counter coercion was proposed in 2005 [6], along with a formalization of the notion which allows to give security arguments. It is called the JCJ protocol and remains the reference on coercion-resistance. We unveil that a phase (that we name the *cleansing phase*) of JCJ leaks some information that can be exploited by the coercer. We provide an example where this allows to fully break coercion-resistance. This highlights that, in general, the attacker has a non-negligible advantage by exploiting the leakage. All the variants and improvements on JCJ that we know of are also affected.

We propose a modification of JCJ, that we call CHide, and that is not subject to this weakness. The key modification is the introduction of a *cleansing hiding* procedure, that replaces the original leaky phase. As a consequence, in CHide, the adversary can only learn minimal information from the cleansing phase. Of course, each step comes with a zero-knowledge proof (ZKP) that the expected operation has been performed, so that anyone can check that the result of the election is correct.

2 Unveiling a Shortcoming in JCJ

We present a vulnerability in the JCJ scheme and discuss its impact.

2.1 Leakage in case of revoting

For a verifiable voting system which uses a public board, it seems unavoidable to leak the total number n_r of received ballots. The number n_v of valid ballots is also leaked unless more sophisticated tally methods are used [2, 7]. However, JCJ leaks more information in case of revoting, namely n_r the number ot revotes and even the complete distribution of revotes per credential. This leakage occurs during the *cleansing phase*, where duplicated and unauthorized credentials are removed, and can be exploited by a coercer to detect when a coerced voter disobeys. Indeed, there is no reason to assume that revoting is independent from the choice of candidate, as it is often due to voters changing their mind between candidates, for instance after a late announcements in the press.

Attacking coercion-resistance. We consider an extreme case, with two candidates such that voters voting for A do not revote while voters voting for B always revote once. Let r_A (resp. r_B) the number of votes for A (resp. B). Due to the distribution of voting behaviors that we consider, the number of revotes corresponds to the number of votes for B sent by the honest voters.

Assume now that Alice wants to vote for B but is instructed by her coercer to vote for A (or abstain): if Alice obeys, the coercer observes $r_B = n_r$ and if she disobeys and casts one ballot for B, the coercer observes that $r_B = n_r + 1$. Hence the coercer detects when Alice disobeys, which breaks coercion-resistance.

One could argue that Alice should follow a different strategy and cast one ballot (resp. two) when she votes for A (resp. B). In this case, a similar attack is possible when she wants to vote for A but is instructed to vote for B.

Discussion. The distribution considered above is very contrived. But as soon as the distribution of revotes is not independent from the distribution of votes per candidate, the coercer will learn some information, and hence detect when a voter disobeys with some non negligible advantage.

2.2 More noise is needed

A known issue of JCJ is that fake ballots should be randomly added, in order to hide to a coercer that the ballot cast under coercion has been removed. In JCJ, this "noise" comes from honest voters sending ballots with an invalid credential, but this source alone may not be sufficient. A natural approach is to have the authorities add a random number of dummies, as proposed in [9] (to mitigate a leakage during the tally). This noise made of fake ballots should however be calibrated carefully since the computation overhead of additional ballots is important. In a context where revoting is a well spread behavior, it could be judicious to rely on revoting, at least partially, as an additional source of noise. This is however not possible in JCJ since the two sources of noise can be distinguished.

3 CHide: A Cleansing-Hiding Variant of JCJ

We propose a modification of JCJ, where the cleansing phase is replaced by an MPC protocol that does not leak any extra information.

3.1 Cyrptographic primitives

ElGamal encryption scheme. We use the ElGamal encryption scheme on elliptic curves, which is convenient for its efficiency and homomorphic property. If (g, h) is the public key, we encrypt m by computing $(g^r, g^m h^r)$ with some random r. To decrypt, we need m to be taken in a small list of valid messages. An important special case is $\{0, 1\}$, when the MPC primitives we mention below can be applied. For a general message m, we use the bit-wise encryption of m, which is the list of the encryptions of the bits of a binary encoding of m.
Logical operations on encrypted bits. There are verifiable MPC protocols that allow to jointly perform logical operations on encrypted bits, without revealing the cleartexts to anyone. The main building block we use is the `CGate` protocol [8], that allows to compute an encryption of a logical and (a conjunction) of the encrypted bits given in input. Combining this with the homomorphic property of ElGamal encryption, we designed various protocols for all the logical operations on bits, and ultimately for realizing any function; see [4] for a more extensive description of the protocols we use. In CHide, we especially use the `Eq` (equality test) and the `Or` (disjunction) protocols that work on encrypted bits. The `Eq` protocol is extended to bit-wise encrypted data, by computing the conjunction of all the equality tests on encrypted bits.

3.2 Description of the CHide protocol

Setup phase. In the setup phase of CHide, the voters receive a credential. A bitwise encryption of the credential is published in the public board.

Voting phase. During this phase, the voters encrypt their vote as well as each bit of their credential. They also prove the knowledge of the plaintexts and that all encryptions are linked.

Cleansing and tallying phase. Once the voting phase is finished, the election trustees get the list of ballots published on the board. They run an MPC procedure on them, which allows to add an encrypted bit of validity to each ballot. Afterwards, the ballots are shuffled and the validity bit is decrypted, so that only the number of total and invalid ballots is revealed.

Efficiency considerations. In terms of computational and communication costs, the CHide system is slightly less efficient, but still in the same ballpark as JCJ. The encrypted credentials are now formed by κ ciphertexts instead of a single one, where κ is the security parameter. This factor is probably affordable by the authorities whose task is highly parallel. For the voters, the computational load increases but the total cost for realistic parameters is around a thousand exponentiations, which should be a matter of seconds with a standard implementation in Javascript running within a modern browser.

For the talliers, the cleansing phase is more complex than the one in JCJ, but still requires a number of exponentiations that grows quadratically with the number of ballots received on the board. The main difference is that due to the MPC tools, the number of communication rounds between them is no longer constant, but becomes logarithmic in the number of ballots.

4 Discussion

We conclude by discussing two other coercion-resistance protocols, which also have their own leakages.

We start with the AFT scheme presented in [1]. Its main feature is that it has a linear time complexity for the cleansing and tallying phase. While it uses different cryptographic primitives from JCJ, it has a similar structure. Assuming that the cryptography is perfect, we remark that both the number of duplicated and unauthorized credentials are revealed during the protocol, just as in JCJ. In addition, it is possible to deduce, by observing the board, the complete distribution of revote per credential. In JCJ, this information is only available during the tally, when it is no longer possible to submit a ballot. Hence, in the AFT scheme, the adversary may exploit this information to submit ballots in a specific way. Consequently, it provides a coercion-resistance level which is very similar to JCJ, but slightly (but strictly) weaker.

Another interesting example is Civitas [3], a scheme considered as equivalent to JCJ, but that actually leaks more information. First, it provides the same leakage as the AFT protocol: the number of revotes for each ballot can be directly deduced from the board. Furthermore, in order to mitigate the (still quadratic) cost of the cleansing, it proposes to group voters by blocks: each credential is publicly assigned to one block, and the voter indicates their block in clear when casting their ballot. Compared to JCJ, the adversary still learns how many revotes each ballot has and how many invalid ballots there is, but also has access to this information block by block, which leads to a stricly weaker security.

References

1. R. Araújo, S. Foulle, and J. Traoré. A practical and secure coercion-resistant scheme for remote elections. In *Frontiers of Electronic Voting*. IBFI, 2007.
2. J. Benaloh, T. Moran, L. Naish, K. Ramchen, and V. Teague. Shuffle-sum: coercion-resistant verifiable tallying for STV voting. *IEEE Trans. Inf. Forensics Secur.*, 2009.
3. M. Clarkson, S. Chong, and A. Myers. Civitas: Toward a Secure Voting System. In *S&P'08*. IEEE Computer Society, 2008.
4. V. Cortier, P. Gaudry, and Q. Yang. A toolbox for verifiable tally-hiding e-voting systems. Cryptology ePrint Archive, Report 2021/491, 2021. `https://ia.cr/2021/491`.
5. V. Cortier, P. Gaudry, and Q. Yang. Is the JCJ voting system really coercion-resistant? Cryptology ePrint Archive, Paper 2022/430, 2022. `https://eprint.iacr.org/2022/430`.
6. A. Juels, D. Catalano, and M. Jakobsson. Coercion-Resistant Electronic Elections. In *ACM Workshop on Privacy in the Electronic Society (WPES'05)*. ACM, 2005.
7. R. Küsters, J. Liedtke, J. Müller, D. Rausch, and A. Vogt. Ordinos: A Verifiable Tally-Hiding E-Voting System. In *EuroS&P'20*. IEEE Computer Society, 2020.
8. B. Schoenmakers and P. Tuyls. Practical Two-Party Computation Based on the Conditional Gate. In *Advances in Cryptology (ASIACRYPT'04)*. Springer, 2004.
9. O. Spycher, R. E. Koenig, R. Haenni, and M. Schläpfer. A New Approach towards Coercion-Resistant Remote E-Voting in Linear Time. In *15th International Conference on Financial Cryptography and Data Security (FC'11)*. Springer, 2011.

Demo and Poster Session

The highly secure anonymous e-voting system of the Czech Pirate Party

Tomáš Martínek[1][0000−0002−5217−3240] and Lukáš Forýtek[2][0000-0002-2453-4483]

[1] Department of Information Engineering, Faculty of Economics a Management, Czech University of Life Sciences Prague, Czech Republic
martinekt@pef.czu.cz
[2] Department of International and Diplomatic Studies, Faculty of International Relations, Prague University of Economics and Business, Czech Republic

Abstract. The article describes the open-source e-voting system of the Czech Pirate Party including the applications, their modifications and interconnection. Overall, it provides an insight into the highly credible, secure and anonymous voting system used for intra-party direct democracy by the Czech governing party.

Keywords: Internet voting, E-voting, E-democracy, Open-Source.

1 Introduction of the electronic voting system of the Pirates

1.1 The Czech Pirate Party

The Czech Pirate Party [15] is a centrist liberal progressive political party, founded in 2009, inspired by the Swedish Pirate Party. In the parliamentary election to the Chamber of Deputies in 2017, the Czech Pirate Party gained 10.79 per cent of the votes gaining 22 mandates for the first time. The lead author of this article also received one of the mandates. Since 2021 the Pirates have been the governing party in the Czech Republic. The leader of the Czech Pirate Party Ivan Bartoš is the Deputy Prime Minister for Digitalization and the Minister of Regional Development. On 9th September 2022, the Czech Pirate Party had 1193 members [1].

1.2 Systems for intra-party voting of the Czech Pirate Party

The Czech Pirates accent the digitalization, therefore respecting intra-party democracy they have been enabling all discussions and votings online using their systems since their establishment.

Since 2016 the Czech Pirate Party has been using the secure and anonymized Helios system for secret ballots. Combined with other systems of the party, this is a unique electronic voting system that has no comparison among Czech political parties.

Personal voting is available exclusively to the party members. Every member must be accepted by a public vote of the local board in an online forum [4]. Afterwards, each member is verified by an authorized person showing an ID or passport check.

The Forum of the Czech Pirate Party is a general discussion platform that enables the membership base to have free or facilitated discussions and some types of meetings. Technically, this is the phpBB system [9] which is run by the Technical Department on the party servers [4].
The Octopus (Chobotnice) is a system for managing people and teams (regional associations, bodies, etc.). The Octopus is used for the administration of personal registers in compliance with the GDPR. Specifically, it allows the mass management of people and teams, implementation of the agenda of identity verification, registration of supporters and acceptance of members, management of applications and payments of membership fees [3].
The Profile is an application where the members, registered supporters, candidates, volunteers and newsletter subscribers manage their personal information and public profiles, and submit their requests for registration or identity verification. The application is a data source for the Octopus system [2].
The People (the Directory) is a system that provides a public overview of bodies and teams in the party and their members. The Directory is linked to the Octopus and Profile systems [1]. The Octopus, Profile and People systems were developed by the Technical Department of the Czech Pirate Party.
The Auth (the Keycloak) is a central authentication point for other applications of the Pirates. Technically, this is the *Keycloak* system [8] in version 17 which is run by the Technical Department on the party servers and which is linked up to the Octopus system [7].
The LDAP is used as a backend for the Auth. Technically, this is the *OpenLDAP* system [6] which is run by the Technical Department on the party servers.
The Helios [10] is a system for the online secret ballot; however, the ballot is verifiable. Technically, the Helios system is run by the Technical Department on the party servers. Current version 3.1.4 is modified by linking up to the Keycloak for login, to the Octopus for user list integration and other security modifications. The modified version is still open-source and it is stored on the Pirates' GitLab. [5]
Other party technologies related to voting. For HTTPS, the third-party service *Let's Encrypt* is used [12]. The Postfix system is used to create e-mail aliases of the party members in the form "firstname.surname@pirati.cz", where they can receive the information about the election and which is also run by the Technical Department on the party servers. More information on the technical systems is available on the Pirate Wiki [14].

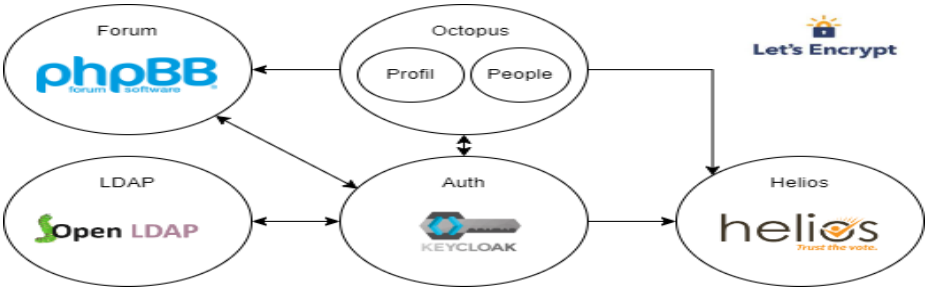


Fig. 1. Simplified scheme of the e-voting system of the Czech Pirate Party

1.3 The intra-party voting process of the Czech Pirate Party

The publicly available discussion and party meetings take place on the online forum of the Czech Pirate Party. The Pirates set an example of using direct democracy, therefore the delegate system is not used for elections, as in other Czech political parties, but all members of the given district can vote. The members usually belong to several levels of districts. The lowest level is the local forum, the middle level is the regional forum corresponding territorially to one of the 14 regions of the Czech Republic, and the highest level is the national forum, which includes all members of the party.

The elected representatives of a certain part or the entire membership base usually vote publicly on the forum of the Czech Pirate Party [4]. For example, a vote of the regional board on the admission of a new member. Personal elections and other important votes are decided by all members of the given district by direct secret electronic ballot.

For calling a vote public support is usually obtained through the forum. Similarly, also for personal elections, the forum is used to get a nomination, where it is possible to get support by supporting a specific nomination post using the "Thanks" functionality of the phpBB forum which displays the names of forum users who support a specific post. In order to start a meeting or a nomination, it is necessary to obtain the support of a group of members. The required member group amount is determined as twice the square root of the number of members in the area.

$$a = 2 * \sqrt{x} \tag{1}$$

a represents a required number of the group of members who supports the proposal

x represents a total number of members of the district

For negotiations that have already started, the required number of the group of members is halved.

In the case of personal elections, members who get the support of a given group of members by the deadline and at the same time accept a nomination or complete a nomination speech can run for the election.

The secret ballot in the voting system of the Czech Pirate Party

The party voting system is usually a two-round system. In the first round, it is possible to vote for none or all options that are acceptable to the voter. All those who receive more than half of the votes go into the second round. The second round is already a majority voting where the voters can choose one or none of the options. The winning option in the second round will be the one that receives the most votes. In case of a draw, the option with the higher support in the first round wins.

At least three trustees are appointed for the election, usually from among the particular departments and forum board. The trustees are responsible for deciphering the voting results. The Helios system itself is the basic automated trustee. Each trustee generates its key pair and uploads the public key to the Helios system [10]. If the results need to be decrypted each trustee uses his private key. The list of voters is uploaded automatically from the party systems after the selection of the district of the members who can vote.

The members are informed about the vote by e-mail, or by a mass SMS. Voting of the Czech Pirate Party can take place after the log-in of the members via the Auth Piráti system [7] using the Keycloak to the Helios party system [10] which takes data from the Octopus party system. The voting takes place on a predetermined date, usually from Friday at 10 a.m. to Monday at 10 p.m.

2 Discussion and conclusion

2.1 Important secret electronic votings of the Czech Pirate Party

The Czech Pirate Party emphasizes direct democracy, thus votings take place quite often. It is not only the election of the board, candidates, and others, but members can also call for a vote to remove them from the party positions. For example, the party statutes changes and other changes are voted on by a referendum. As this is a unique case in the Czech political environment, some votes are closely followed by the national media. The most watched cases are usually the elections of the party leader or, by contrast, calls for the removal of a certain person from a position in a party. In November 2021, all members voted on the entry of the Czech Pirate Party into the coalition government, which was closely followed by the media.

2.2 Conclusion

In contrast to other Czech political parties which vote and make decisions through delegates, or postal ballots, the Pirates allow all members to make decisions online. To increase the credibility, the Pirates exclusively use open-source solutions, making their modifications and applications available on their Gitlab [13]. The e-voting system which is used by the Pirates is comfortable even for mobile voting and guarantees a high degree of credibility, security, and anonymity for qualified decision-making in terms of direct democracy.

References

1. Lidé Piráti, https://lide.pirati.cz, last accessed 2022/09/09.
2. Profil Piráti, https://profil.pirati.cz, last accessed 2022/09/09.
3. Chobotnice Piráti, https://chobotnice.pirati.cz, last accessed 2022/09/09.
4. Fórum České pirátské strany, https://forum.pirati.cz, last accessed 2022/09/09.
5. Piráti: Helios Server, https://gitlab.pirati.cz/to/helios-server, last accessed 2022/09/11.
6. OpenLDAP, https://www.openldap.org/, last accessed 2022/09/09.
7. Auth Piráti, https://auth.pirati.cz/, last accessed 2022/09/09.
8. Keycloak.org, https://www.keycloak.org/, last accessed 2022/09/09.
9. phpBB, https://www.phpbb.com/, last accessed 2022/09/09.
10. Helios Piráti, https://helios.pirati.cz/, last accessed 2022/09/09.
11. Helios, https://vote.heliosvoting.org/, last accessed 2022/09/09.
12. Let’s Encrypt, https://letsencrypt.org/, last accessed 2022/09/09.
13. Pirátský GitLab, https://gitlab.pirati.cz/, last accessed 2022/09/11.
14. Piráti: Přehled technických systémů, https://wiki.pirati.cz/to/technicke-systemy, last accessed 2022/09/09.
15. Piráti, http://www.pirati.cz/, last accessed 2022/09/09.

Electis.app White Paper

Electis.io

Abstract. The Electis voting App (Electis.app) is a web application built using Django and ElectionGuard SDK). The latter comes with homomorphic encryption and end-to-end verifiable proof of ballots and tally (initially designed for US election machines. In addition, Electis.app relies on the Tezos blockchain to generate proof of the election via a smart contract. Finally, it uses IPFS decentralized storage to share the proof and ballots with voters to allow them to verify the election was not violated. This document dives into the overall architecture of the e-voting platform and discusses the application'sapplication's key features and how the election is decentralized.

1 Software Architecture

The Electis e-voting platform is separated into three core apps, electeez_auth, djelectionguard, and djectionguard_tezos. All user-related authentication and account management for the e-voting platform is handled within the ""electeez_auth"" app. The contest-related functionalities are managed in the ""djelectionguard"" app, and finally, all Tezos-related functionalities are in the ""djelectionguard_tezos"" app[1].

1.1 User Authentication

Django's inbuilt user authentication is utilized for the user account management and authentication system. The user model is extended from Django's AbstractUser to include the username and email, and a token model was added for verification (to verify unique users). To sign up, a user needs to do is to insert their email and password. Then, A user object is created in the database, and a token is generated for the user, set to expire after 30 days. A URL-safe token is generated and stored for later verification using python's inbuilt secrets library. When a user activates a verification link with the generated token, a crosscheck occurs in the token database. If not expired, the user is logged in, and the account is marked as active. Users can also reset their passwords, which is done by using the provided functionalities from Django.contrib.auth.urls. An extended feature in Electis.app is the ability to log in using One-Time Passwords (OTP).

During contest creation, when the moderator of the election shares the voters' email list, an account is created for any email address that does not have an account registered. An OTP is shared with users via email to use and log in to the platform and participate in the contest they were invited to vote in. In addition, a second level of identification through SMS is also available, requiring the voter to enter their phone number after

[1] Tezos. “Tezos White Paper”. Tezos Agora Wiki (Link)

signing up or receiving the OTP and then confirming the second password they receive via SMS.

1.2 ElectionGuard extension

ElectionGuard[2], which was designed for voting machines (within the existing infrastructure used in elections), is extended in Electis.app to organize a secure remote e-election. The following sections in this chapter will explain the entire flow of the extension.

Configuring an Election

In step 1, the user shares the basic details of the election, and a manifest is created in JSON format and parsed into an election description. Election Builder is instantiated and generates the public-private key pairs, readying for the key ceremony. The manifest includes contest- related information, such as name, ballot details, candidates, etc.

Key Ceremony

The key ceremony is the process of sharing the encryption keys for the contest. Before the election is opened, a fixed number of guardians pre-determined by the mediators must hold the private keys to decrypt the election results later. To account for potentially missing guardians, the quorum count can be less than the total number of guardians.

Each guardian has a unique id and sequence to generate their public-private key pair, where they will hold their private and all guardians' public keys. They will need to verify the key backup with all the keys they hold. If the verification fails, the guardian whose key doesn't match will perform a key challenge and share the unencrypted key with all guardians to verify. If it fails to verify, the guardian with the corrupted key is replaced with a new one (Electionguard Python). Once verified, the joint public keys are published for the election. Although ElectionGuard can organize elections without the key ceremony[3], it is recommended to increase the security of the election.

Encrypted Ballots

Once the election is opened for participants to share their vote, a client-side encrypted ballot is created; it first verifies that the ballot is well formed against the Election Metadata and generates a master nonce value as a secret when encrypting the ballot as CiphertextBallot.

As mentioned before, ElectionGuard uses homomorphic encryption and Non-Interactive Zero-Knowledge proof (Electionguard Python Documentation[4]). The proof is used to show that the encryption is either an encryption of zero or one for each selection on the ballot, or the sum of all encrypted ballots is equal to the selection limit

---

2 ElectionGuard Structure (Link)

3 Electionguard Python Documentation. "Key Ceremony." *GitHub*. (Link)

4 Electionguard Python Documentation. "Encrypt Ballots." *GitHub*. (Link)

on the contest. A verification code is then generated to share with the voters that they can use later to verify the tallying. The homomorphic property allows the encrypted votes to be combined to form encrypted tallies. First, the public guardian keys are combined into a single public key to encrypt the ballots. Then, at the end of the election, ideally, the guardians use their private key to decrypt each tally partially. In the end, the partial decryption is combined to form verifiable decryptions of the tallies (Electionguard Python Documentation).

Homomorphic Properties

The votes are encrypted using an exponential form of the ElGamal cryptosystem by selecting a random nonce and forming a pair. Then, the secret key's guardians, or multiple guardians, can decrypt the message (ElectionGuard). This allows it to have additively homomorphic properties.

Component-wise product of two encrypted messages would be the encryption of the sum of the two messages. Hence, all the encryptions of a single option across ballots can be multiplied to form the encryption of the sum of the individual values. The individual values are on ballots that select that option and zero. Otherwise, the sum is the tally of votes for that option, and the product of the individuation encryptions is an encryption of the tally (ElectionGuard).

Non-Interactive Zero-Knowledge (NIZK) Proofs

Four techniques are used in ElectionGuard to provide numerous proofs about encryption keys, ballots, and tallies. These techniques ensure keys are correctly chosen, the ballots are properly formed, and finally, the decrypted tally matches the claimed values.

- A Schnorr proof - allows a holder of an ElGamal secret key to interactively prove possession of the secret key without revealing it.
- A Chaum-Pedersen proof - allows ElGamal encryption to be interactively proven to decrypt to a particular value without revealing the nonce used for encryption or the secret decryption key.
- The Cramer-Damgard-Schoenmakers technique - enables a disjunction to be interactively proven without revealing which disjunct is true.
- The Flat-Shamir heuristic - converts interactive proofs into non-interactive ones. (ElectionGuard)

Cast and Spoiled Ballots

A key feature to be implemented soon in the Electis.app development roadmap is the "Benaloh Challenge" [1]. When voters create the ballots, they must be either cast or spoiled. When each ballot is loaded into the memory and verified to be correct using the proofs mentioned above, the ballot is submitted and can be either identified as cast or spoiled. The cast ballot is combined into CiphertextTally, whereas spoiled ballots are cached for later decryption (Electionguard Python Documentation[5]).

[5] Electionguard Python Documentation. "Cast and Spoil Ballots." *GitHub*. (Link)

Decrypting the Tally

When the election is closed, the encrypted ballots and proofs that the ballots are well formed are shared as artifacts. Each option's encryptions are homomorphically combined to form encryption of the total number of times that each option was selected. Finally, the combined encryption is decrypted to generate the election tally. No individual cast ballots are decrypted. To decrypt the combined encryption, a specific decryption share of the decryption is computed for each guardian. During this process, the spoiled ballots are also decrypted and shared, as it is verifiable in the same way that the aggregate ballot of tallies is decrypted. This allows voters to explicitly generate challenge ballots which they can later use to verify the authenticity of the election (Electionguard Python Documentation[6]).

1.3 Voter Participation Tracking

Electis.app can let election moderators track voter participation. It stores and checks whether the voter received the email with the OTP link or not and whether the voter cast it. If required, moderators can also request new OTP links for voters and share that with the voter manually.

1.4 Decentralization of the election

In the beginning, when the contest is set up, a smart contract for the election is created that holds all the election-related information, including the link to the InterPlanetary File System (IPFS) network. The published ballots by ElectionGuard at the end are published on IPFS storage. The smart contract created should be managed by the moderator of the election and should have its unique wallet. The smart contract holds all information such as, but not limited to, when and what time the contest was opened and closed, what it was about, the election manifesto, public keys, who the candidates were, the moderators, the guardians, etc.

IPFS Storage

In the last stage of the election, the artifacts are ready to be published when the contest has been tallied and decrypted. Hence, the moderator can initiate the action to publish all artifacts created by ElectionGuard and upload them on IPFS decentralized storage. The uploaded files include the encrypted casted ballots, spoiled ballots, proofs, and the encrypted and decrypted tally. Once the file is uploaded, the cryptographic hash is received, and later, anyone can look up the file using the unique fingerprint to download and verify the election. A transaction is made in the smart contract to update the storage to include the fingerprint and store the actual close time and final election tally.

What Smart Contracts Enable

---

[6] Electionguard Python Documentation. "Decryption." *GitHub* (Link)

While it is shared, the smart contract can function as a legal document to prove the election has met all the requirements. In addition, it also enables it to trigger actions depending on the output of the election. Actions based on the election result can be automated while keeping it transparent and secure.

1.5 Universal and Personal Verification

Elections should provide both privacy and integrity, i.e., enable everyone to audit the election results while not having to go transparent on their votes and forgetting about anonymity. We already know that with threshold encryption, there would be no way to decrypt the individual ballots as it would require combining all the private keys the guardians hold to run the decryption protocol. Along with the proofs prepared by the ElectionGuard SDK, Electis.app also uses the Fiat-Shamir Heuristic to verify the final tally. The process for the proof is public and verifiable.

With the proof of the results, voters receive their code (bulletin number), which they can use to verify that their casted ballot is counted in the final tally. All encrypted ballots are uploaded to the IPFS decentralized storage. At the end of a vote, the unique ID of their ballot and the unique ID of the election is shared with the voter. We use the email/login info as a key to present the election details and allow the user to check if their vote was considered. A hash of the encrypted ballot is provided to the voter after casting their vote, which the voter can compare to the hash of the encrypted ballot stored on IPFS under the correspondent bulletin ID. This double-check (bulletin ID and hash) provides a full personal identification.

Additionally, any voter can redo the tallying once the Guardians share the decryption keys publicly. This universal verification feature is a priority in our development roadmap and will soon be implemented. This, in combination with the "Benaloh challenge", offers full end-to- end verifiability. Trust in the central server's operations is then guaranteed by the trust in the in-flows (through the Benaloh challenge) and out-flows (through personal and universal verification) to and from the server.

2 Bibliography

1. Benaloh, J.: Simple verifiable elections. In: EVT 6. p. 5 (2006).

Verifiability of Scytl's voting system for government elections

Scytl Election Technologies SLU
08021 Barcelona, Spain
www.scytl.com

Scytl's online voting system has been a pioneer in the introduction of verifiability in online voting schemes for political elections. Starting from 2004 in Switzerland (Neuchâtel), Scytl's voting system included voting receipts [1], allowing voters to check that their vote was present in the final tally. In Norway, in 2011 and 2013, Scytl's online voting system introduced cast-as-intended individual verifiability for the first time in a national election using return codes [2], and counted-as-recorded verifiability using universal verifiable Mix-nets [3,4]. In 2015, Scytl's voting system implemented a second verification mechanism designed for the State of New South Wales (Australia), based on a cast and decrypt approach (decryption of the vote in a trusted environment accessible by phone) [5]. This mechanism was improved in 2019 State election by using a mobile verification application. Also in 2015, Scytl's individual verifiability (return codes) was adopted in Switzerland (Neuchâtel) and achieved in 2017 the Swiss certification for individual verifiable systems [6]. Currently, Scytl's online voting system has been selected by 41 local authorities for the 2022 Ontario municipal elections in Canada.

In the demo session, Scytl will show the verifiability mechanisms present in the online voting system that will be available in these Canadian municipal elections.

1. Puiggalí, J., Morales-Rocha, V.: Independent voter verifiability for remote electronic voting. In: Proceedings of International Conference on Security and Cryptography (SECRYPT '07), pp. 333–336, Barcelona (2007).
2. Puiggalí, J., Guasch, S.: Universally verifiable efficient re-encryption mixnet. In: Electronic Voting 2010 (EVOTE 2010), 4th International Conference, LNI, vol. 167, pp. 241–254, Austria (2010).
3. Puiggalí, J., Guasch, S.: Cast-as-intended verification in Norway. In: 5th International Conference on Electronic Voting 2012, (EVOTE 2012), LNI, vol. 205, pp. 49–63, Austria (2012).
4. Wikström, D.: A sender verifiable mix-net and a new proof of a shuffle. In: Proceedings of the 11th International Conference on Theory and Application of Cryptology and Information Security. pp. 273–292. ASIACRYPT'05, Springer-Verlag, Berlin, Heidelberg (2005).
5. Brightwell, I., Cucurull, J., Galindo, D., Guasch, S. An overview of the iVote 2015 voting system. Tech. rep. New South Wales Electoral Commission (2015).
6. Scytl News - https://www.scytl.com/news/scytl-swiss-post-online-voting-solution-first-switzerland-certified-50-voters/

E-Voting Wasm Cryptography

David Ruescas and Eduardo Robles

Sequent
david,edu@sequentech.io
http://https://sequentech.io/

Abstract. The Sequent Voting Platform is an open-source E2EV internet voting system currently used in private organisations and non-legally binding elections of public organisations. The system employs standard cryptographic techniques following in the steps of well-established voting schemes proposed in the academic literature.

We demo core cryptographic components that are being developed for the next generation of Sequent's platform. The main novelty demonstrated is the execution of (heavyweight) cryptographic operations in the browser, in a performant way. Potential applications of this technique are listed and possible benefits for security, privacy and verifiability are suggested.

Keywords: evoting · cryptography · webassembly.

1 Introduction

Like many other systems proposed in the literature, the closest ancestor in Sequent's genealogy tree is Helios[1] in its original mixnet variant. The most significant departures from that Helios design are the use of a threshold distributed key generation mechanism, described in Pedersen[2] and featured in CGS[3] and Distributed Helios[4], and the use of a Terelius-Wikstrom[5] style mixnet rather than the Sako-Kilian[6] one. Other systems with which Sequent shares techniques are Wombat[7] and CHVote[9].

Research and development into Sequent's next generation system is currently underway. Part of this effort has been centred around the use of Rust[10] as a core technology. One of the interesting aspects of this technology is its ability to target WebAssembly[11] through the LLVM[12] toolchain.

Internet voting systems require the use of a client component with which voters select and encrypt their votes, typically in a browser. In the past, these components have been written in javascript or related languages. These components replicate some of the cryptography (for example, ElGamal encryption) that later processes votes in the backend. The initial motivating factor for our investigation of Rust's WebAssembly target was the possibility of merging this overlapping cryptography into a single unified codebase. But there are further interesting possibilities.

2 Applications

2.1 Vote casting

Voting client software can reuse common cryptography packaged in a library compiled to wasm, eliminating duplication.

Suggested benefits

- Security: A unified code base reduces the likelihood of mismatches between client and server cryptography, and reduces the attack surface. The amount of code that needs to be audited is also reduced.
- Performance: Higher performance compared to javascript implementations.

2.2 Ballot verification

Ballot verifiers implementing the Benaloh challenge can reuse common cryptography packaged in a library compiled to wasm, eliminating duplication.

Suggested benefits

As above.

2.3 Election verification

Election verification, usually carried out by specialised software that must be downloaded and configured, can be executed in the browser with no installation.

Suggested benefits

- Verifiability: Making election verification procedures significantly more usable can achieve higher rates of exercised verification, moving the "universal" part of universal verifiability closer to practice.

Note that achieving performant implementations in this use case is particularly difficult as election verification involves compute intensive operations that a priori seem impossible in a browser. We have not listed performance as a benefit here as we are comparing with non-browser, native implementations; in other words, performance is a must-have rather than a benefit for this use case.

2.4 Trustee protocols

Running full trustee nodes on the browser with reduced deployment, administration and training costs.

Suggested benefits

Real world experience has taught us that one of the barriers to running mixnet-based elections with a larger number of independent trustees is the cost that these trustees must incur in terms of deployment, administration and training. This is especially true for elections with fewer resources in human capital and infrastructure. As a result, it is not always easy to procure independent trustees to assume this important responsiblity.

Any objective that is presumably achieved through distribution into independent trustees could be achieved to a greater degree when some of the costs of this distribution are reduced. For example:

- Privacy: Ballot secrecy safeguards achieved through the distribution of private key material and mixing permutations would be achieved to a higher degree if more trustees participate.
- Security: Correctness safeguards achieved through distribution of mixing and tallying would be achieved to a higher degree if more trustees participate.

See previous section regarding performance as a benefit.

References

1. Ben Adida. Helios: Web-based Open-Audit Voting.
2. Torben Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing.
3. Ronald Cramer, Rosario Gennaro, Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme.
4. Véronique Cortier, David Galindo, Stéphane Glondu, Malika Izabachène. Distributed ElGamal à la Pedersen: Application to Helios.
5. Björn Terelius, Douglas Wikström. Proofs of Restricted Shuffles.
6. Kazue Sako, Joe Kilian. Receipt-free mix-type voting scheme — a practical solution to the implementation of a voting booth.
7. Wombat Voting https://wombat.factcenter.org/
8. Niko Farhi. An Implementation of Dual (Paper and Cryptographic) Voting System. http://www.cs.tau.ac.il/ amnon/Students/niko.farhi.pdf
9. Rolf Haenni, Reto E. Koenig, Philipp Locher, Eric Dubuis. CHVote Protocol Specification. https://eprint.iacr.org/2017/325
10. https://www.rust-lang.org/
11. https://webassembly.org/
12. https://llvm.org/