Saloomeh sayad Azari

[Review Your Choices: When Confirmation Pages Break Ballot Secrecy in Online Elections](#review)

[E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy](#evoting)

[Individual Verifiability with Return Codes: Manipulation Detection Efficacy](#individual)

1

Review Your Choices: When ConfirmationPages Break Ballot Secrecy in OnlineElections

James Brunet , Athanasios Demetri Pananos , and Aleksander Essex(B)  
Western University, London, Canada  
{jbrunet8,apananos,aessex}uwo.ca

**Background and Related Work**

• Ballot secrecy in online elections has been studied for active attacks like TLS subverting, exploiting vulnerabilities, or privileged access.

• Little research has explored passive attacks that focus on the lengths of exchanged messages.

• Volkamer and Krimmer's requirement that the e-voting system cannot deduce the vote or chosen candidates from transmitted voting protocol messages raises concerns.

**Research Question and Scope**

The study tested if ballot confirmation pages leak voter selection information, with Montreal-based Simply Voting being the only vendor with publicly accessible demonstrations.[1]

**Description of Simply Voting’s System**

• The system includes a ballot-casting process, a verification process, and a review and submission process.

• Potential side-channel attacks in the ballot-casting process include the length-based attack on a voter's selections when the names are sent as explicit, uncompressed text that was observed in the Voatz system [2]

**Methodology**

To test the hypothesis that a voter's choice correlates with the TLS record length of the ballot confirmation page, a large volume of requests was made to Simply Voting's servers. Instead of burdening resources, an application was designed to automatically log responses for analysis.

A testing system was developed, consisting of a Client Application and a Server Application, to simulate an online voting system. The system simulates an election where voters can vote for one or more offices, with each ballot representing an actual HTTP request.

The Client Application, developed using Python, Selenium WebDriver, Google Chrome, and Wireshark, interacts with the Server Application to request confirmation pages, capture network responses, parse TLS record length, and log candidate choice for statistical analysis.

**Township of Selwyn, Ward Lakefield Experiment1**

The 2018 municipal election confirmed page data, estimated encrypted vote probability using Multinomial Naive Bayes Model, and achieved 83% accuracy, precision, and recall in class classification.

**Township Experiment 2: Selwyn, Ward Ennismore**

The study used Python and scikit-learn for Multinomial Naive Bayes Model fitting, identifying 100% ballots associated with 11 possible combinations and detecting a limited voter information leak.

**Experiment 3: Town of Ajax, Ward 1**

The study utilized a Multinomial Naive Bayes Model to analyze the TLS record lengths of various candidate combinations, revealing that ballot secrecy can be compromised for all ballots.

**Mitigations**

SwissPost and Neuvote Systems' Mitigation Measures

• Avoid internet transmission of confirmation pages.

• Implement fixed-length responses to prevent fingerprinting attacks.[3]

• Implement uniformly random-length padding in response header.

• Ballot Secrecy Headers can be compromised by voter abstention, causing unique TLS record length.

Conclusion

• A model using the voter's vote confirmation page record length predicted the chosen candidate with 83% accuracy in a real-world mayoral contest.

The author believes that Using the network-observed TLS record length of the voter's vote confirmation page, predicted the winner of a recent real-world mayoral election. they said Our algorithm outperformed random guessing in more complex ballots.Then, we could still acquire limited information from a significant subset of ballots cast in an election in the form of certain combinations of candidates who were not voted for.

Our model validation results demonstrate that this performance gap is unlikely to be explained by sample variation.

1. Cardillo, A., Akinyokun, N., Essex, A.: Online voting in Ontario municipal elections: a conflict of legal principles and technology? In: Krimmer, R., et al. (eds.)  
   E-Vote-ID 2019. LNCS, vol. 11759, pp. 67–82. Springer, Cham (2019). https://doi.  
   org/10.1007/978-3-030-30625-0\_5
2. Specter, M.A., Koppel, J., Weitzner, D.: The ballot is busted before the blockchain:  
   a security analysis of Voatz, the first internet voting application used in US. Federal  
   elections. In: 29th USENIX Security Symposium (USENIX Security 2020), pp.  
   1535–1553 (2020)
3. Gellert, K., Jager, T., Lyu, L., Neuschulten, T.: On fingerprinting attacks and  
   length-hiding encryption. In: Galbraith, S.D. (ed.) CT-RSA 2022. LNCS, vol.  
   13161, pp. 345–369. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-  
   95312-6\_15

Citation /Reference: Use **APA** format

Brunet, J., Pananos, A. D., & Essex, A. (2022, September). Review Your Choices: When Confirmation Pages Break Ballot Secrecy in Online Elections. In *International Joint Conference on Electronic Voting* (pp. 36-52). Cham: Springer International Publishing.‏

**2**

E-Voting with Blockchain: An E-Voting Protocol  
with Decentralisation and Voter Privacy

Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis  
ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom  
Email: *f*Freya.SheerHardwick.2016, Apostolos.Gioulis.2015*g*@live.rhul.ac.uk, *f*r.n.akram, k.markantonakis*g*@rhul.ac.uk

Modern democracies rely on voting, including traditional ballet-based and e-voting, to combat voter apathy, particularly among younger tech-savvy generations[1]. Robust e-voting schemes require transparency, accuracy, suitability, system integrity, and authority distribution.

Blockchain technology, a distributed network of interconnected nodes, allows users to remain anonymous and has the potential to make e-voting more acceptable and reliable. Its distributed ledger contains the full history of transactions, and no single authority controls the network.[2,3]

PROTOCOL

The proposed e-voting protocol uses a blockchain-based system to allow voters to change their minds and cancel votes. The protocol uses a transparent ballot box as a network of equals, with each voter acting as a node. A Central Authority verifies eligibility and uses application-dependent methods. Ballots are digital representations of physical ballots, sealed if not revealed. The voter's public key, Vipriv, serves as the signature validating key, and their new commitment represents their choice.

**Protocol Phases**

Initial phase: The process involves determining election rules, initializing the CA, blockchain, and protocols, making decisions on protocol phases, publicizing rules, providing eligible voters, generating signature keys, initializing the blockchain with a genesis block, and tying the blockchain to a specific election to prevent disputes.

Preparation phase:The voter authenticates with the Central Authority (CA) using the e-voting platform's client application. The CA determines voter eligibility using the initialization phase's list of eligible voters. If eligible, Vi's client generates a public key pair, Vipub, and a digital commitment, dci. Both are sent for signature, using a blinding signature scheme.

Voting phase: The voting phase involves voters constructing and broadcasting their votes, collecting, validating, and inserting them into the blockchain. Valid votes must be cast by the vote owner, validated by the CA's signature, and adhere to predefined structure.

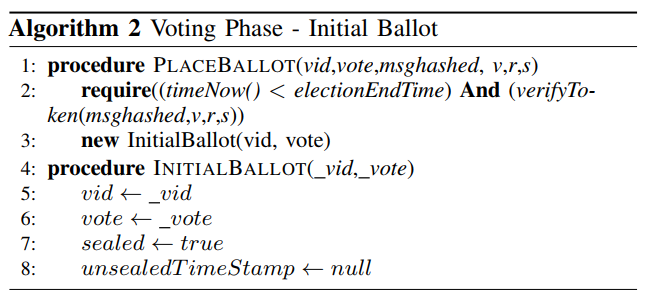
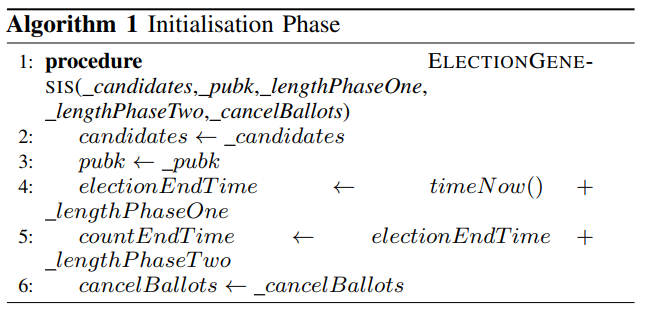
Counting phase: voters reveal their final choice by broadcasting a ballot opening message, obi, containing their final vote VID, commitment value, and signature. Network nodes collect messages and verify signatures. Voters broadcast messages to peers, including vote in count, ensuring equal results.

*Protocol Analysis*

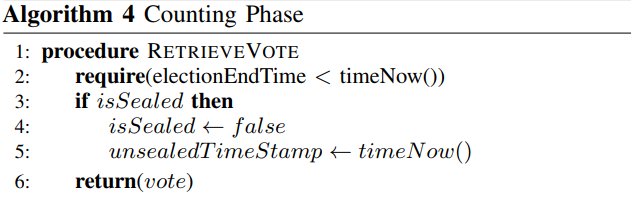
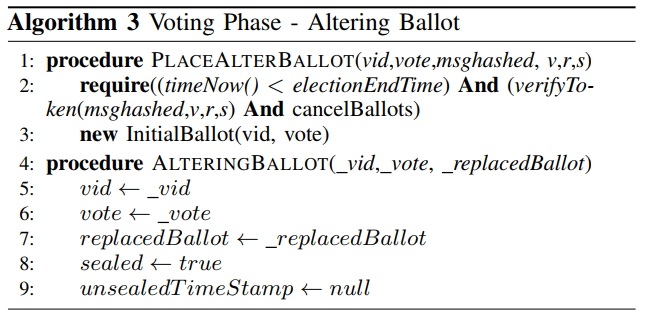
The protocol ensures eligibility, privacy, fairness, and verification of election results. Eligible voters must have a valid ballot and signature from the Central Authority. A blind signature scheme prevents party identification. Centralization and fraud prevention are key concerns. A multisignature scheme and permissioned blockchain could enhance security.

*Implementation*  
The implementation of a private network using Ethereum blockchain API is chosen due to its widespread popularity and potential for comparison with similar protocols. Computational expenses, expressed as 'gas', impact design choices in Ethereum applications. Nodes aim to maximize profits by determining transaction worth above computational cost. In a private network, nodes have other stakes, such as the right to vote, but computation still has attached costs. Ethical concerns arise when charging voters for the right to vote, but a gateway node sponsored by election hosts could circumvent this issue.

the initialisation phase of an election, a genesis contract is placed on the blockchain using Algorithm 1. This contract contains information for validating ballots, ensuring no ballots are placed after time, without a signed token, and prohibiting alteration ballots. It also contains public information like candidate list and election timing.



To place a ballot on the blockchain, voters must first communicate with the CA for a signed token, and then submit the token's component parts, as splitting them costs too much gas. A voter must submit a unique VID and message token to uniquely mark their vote on the blockchain. The message token is verified by the public key and the current time is checked. Only after these requirements are met can the ballot be created, sealed, and the unsealedtimeStamp null. The contract is then pushed to the blockchain(.algorithm 2)

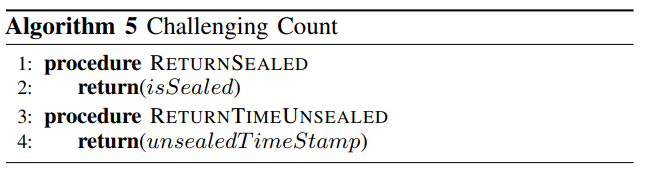


The process for altering a ballot (Algorithm 3) involves a voter with a signed token, a candidate's unique VID, and the previous ballot's address. Validation is not done until the counting phase due to Solidity's lack of support for transaction extrapolation and the decision not to store addresses of previous ballots due to computational costs

The message token is verified by the election's public key, the current time is checked, and election rules are verified. Only after these requirements are met can a ballot be created, with the VID and vote set, the ballot sealed, and the unsealedtimeStamp null

The Counting Phase involves retrieving votes from the ballot, marking them unsealed if they're the first time, and recording the retrieval time. The VID of the vote is publicly available, and altering bids can be checked for validity before counting. Security is ensured by private blockchain access to this information. .(algoritm 4)

Nodes on the blockchain can examine the blockchain, retrieve information like the VID, and contest whether a ballot was opened early or not included in the count, allowing them to challenge the count.



conclusion

E-voting, as addressed in the paper, is a viable answer to the youthful tech-savvy population's lack of interest in voting. A potential approach for making e-voting more open, transparent, and independently auditable would be to base it on blockchain technology. This article investigates the possibilities of blockchain technology and its application in an e-voting scheme. The paper suggests and then implements an e-voting mechanism. The article describes the implementation and related performance metrics, as well as the obstacles offered by the blockchain platform for developing a sophisticated application such as e-voting.

The authors identify various flaws and propose two potential next steps for improving the underlying platform (blockchain technology) to accommodate e-voting and other related applications. Blockchain technology holds a lot of promise, but it may not attain its full potential in its current state. A concerted effort is required in fundamental blockchain technology research to increase its features and support for complicated apps that can run within the blockchain network.

1. L. C. Schaupp and L. Carter, “E-voting: from apathy to adoption,” *Journal of Enterprise Information Management*, vol. 18, no. 5, pp. 586–601, 2005
2. T. Moura and A. Gomes, “Blockchain voting and its effects on election transparency and voter confidence,” in *Proceedings of the 18th Annual International Conference on Digital Government Research*, ser. dg.o ’17. New York, NY, USA: ACM, 2017, pp. 574–575. [Online]. Available:  
   <http://doi.acm.org/10.1145/3085228.3085263>
3. P. McCorry, S. F. Shahandashti, and F. Hao, “A smart contract for boardroom voting with maximum voter privacy,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2017, pp. 357–375

Citation /Reference: Use **APA** format

Hardwick, F. S., ApostolosGioulis, R. N. A., & Markantonakis, K. (2018). E-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy.‏

**3**

Individual Verifiability with ReturnCodes: Manipulation Detection Efficacy

Paul Tim Th¨ urw¨ achter1, Melanie Volkamer1(B), and Oksana Kulyk

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

Cryptographic end-to-end verifiability helps detect election integrity violations, but individual verifiability is challenging for voters. User studies evaluate voters' ability to detect manipulation in electronic voting systems and attack types. A study by Kulyk et al. at E-Vote-ID 2021 showed that QR-code-based code voting should be used in certain elections, as it avoids reliance on trustworthy clients and positively affects manipulation detection rates.[1]

Studies on verifiable voting systems have shown mixed results on their effectiveness in e-voting systems. Some systems show high-efficiency rates, while others show mixed results. Empirical experiments are crucial for understanding security. A code-voting approach aims to reduce trust in vote secrecy, but limited evaluations have been conducted.

The paper explores the use of blockchain technology in e-voting to address voter disinterest among young tech-savvy voters. It proposes a scheme and measures performance, highlighting challenges such as individual verifiability and detection rates varying from 100% for easy manipulation to 10% for difficult ones.[1]

The study examines the Swiss voting system's vulnerability to difficult-to-detect attacks, focusing on the improvement proposed by Kulyk et al. at E-Vote-ID 2021. A user study found the improved version significantly improved manipulation detection, indicating its potential for use in certain elections.[2]

Studies on human aspects of verifiable voting systems reveal mixed results, with some finding voters cannot verify their votes correctly. Check codes show high verification efficiency rates, but only 56% can detect attacks. Empirical experiments are crucial for understanding e-voting system security and usability, but limited evaluations of verification in code-voting systems have been conducted.

**3 Background  
3.1 Swiss Electronic Voting System**

The Swiss voting system uses a postal service to send voters an individual code sheet, which contains an initialization code, check codes for each voting option, confirmation code, and finalization code. The system generates an election-specific election key pair for each voter, with the private key deduced from the initialization code. Voters open an election webpage, manually enter their initialization code, select their voting option, and compare the code with the one on the polling sheet. If the check is correct, voters receive a finalization code, which they must verify to ensure their vote is stored as intended. The voting scheme provides individual verifiability, but there are shortcomings in universal verifiability due to the implementation of cryptographic primitives.[3]

**3.2 E-Vote-ID-2021-Proposal**

Kulyk et al. proposed an extension of the Swiss voting system to include individual voting codes for each option. This would eliminate the need for a trustworthy voting client. Instead, voters could cast a vote using camera-equipped smartphones by scanning a QR code. The authors also integrated voting material and election web pages, introducing voting cards with QR codes on the front and back pages. The proposal is referred to as the 'E-Vote-ID-2021-proposal'.[2]

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

Kulyk et al.'s study enhanced the voting process by providing a URL to the election webpage in both text and QR-code format, placing a QR-code on polling sheets, adding a tick-box for verification, and modifying user interfaces to increase security.

The study explored online voting channels, discussing forums, company information, setup, and security evaluations. A 9-minute video describing the vote casting process was chosen, covering all steps and supporting calls.

<https://youtu.be/Yj7yz437OEc>

**5 Methodology**

The proposed improved scheme improves security and usability, but the effectiveness of manipulation-detection efficacy remains a question.

The study aims to determine the performance of the improved proposal with and without a descriptive video.

Participants were randomly assigned to a no-video group and a video group, receiving study materials in envelopes.

Participants were instructed to open an envelope, read a study letter and role card, and then read the voting material.

The study aimed to evaluate the usability of an online voting system, which may be considered deceptive.

**6 Results**

-The study found that 32 out of 50 participants detected manipulation, with 65.4% in the video group and 62.5% in the no-video group.

-Both groups had significantly higher detection rates than the original system

-No significant differences were found between the no-video-group and video-group

-Out of 31 participants who read the voting materials beforehand, 23 detected and reported the manipulation, compared to 47.4% of those who did not.

-24 out of 34 participants who watched the video fully or read the voting materials before voting were able to detect manipulation.

**7 Discussion**

The E-Vote-ID-2021-proposal outperforms the original system in detection manipulation rates (62.5% to 10%).

It is recommended for elections and polls in Switzerland and other election contexts with simple ballots.

However, increasing the manipulation rate requires additional measures such as awareness raising for verifiability and understanding why voting material received via postal service can be trusted but not necessary.

Participants who read voting materials only as they voted were more likely to follow instructions and missing manipulation.

The study evaluates manipulation-detection efficacy in verifiable electronic voting using a mock election.

Code voting can enhance the security and usability of online voting systems, but further research is needed to understand the impact of interventions on manipulation-detection efficacy, as verifiable schemes only provide secrecy if the client is trustworthy.

**Conclusion**

Verifiable voting schemes are the standard for online voting for political elections, but they only provide vote secrecy if the client is trustworthy. Code voting can address this issue by making the system usable and increasing manipulation-detection efficacy.

Authers belive that Combining code-voting with verifiable techniques can boost security while decreasing usability. There is, nevertheless, room for improvement, and a video intervention describing how to vote may not considerably enhance this percentage. More research is needed to understand how treatments affect manipulation-detection efficacy.

1. Kulyk, O., Volkamer, M., M¨ uller, M., Renaud, K.: Towards improving the efficacyof code-based verification in internet voting. In: Bernhard, M., et al. (eds.) FC2020. LNCS, vol. 12063, pp. 291–309. Springer, Cham (2020). https://doi.org/10.  
   1007/978-3-030-54455-3 21
2. Kulyk, O., Ludwig, J., Volkamer, M., Koenig, R.E., Locher, P.: Usable verifiable secrecy-preserving e-voting. In: Electronic Voting: 6th International Joint Conference, E-Vote-ID. University of Tartu Press (2021)
3. Haines, T., Lewis, S.J., Pereira, O., Teague, V.: How not to prove your election outcome. In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 644–660. IEEE (2020)

Citation /Reference: Use **APA** format

Thürwächter, P. T., Volkamer, M., & Kulyk, O. (2022, September). Individual Verifiability with Return Codes: Manipulation Detection Efficacy. In *International Joint Conference on Electronic Voting* (pp. 139-156). Cham: Springer International Publishing.‏