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)