Review of the Symbolic Models V1.3 of the Swiss Post Voting System V1.4

Saša Radomirović, Ioana Boureanu, and Steve Schneider
Surrey Centre for Cyber Security, University of Surrey, UK

24 July 2024

1 Scope and Methodology

We reviewed the changes and extensions made to the symbolic models and proofs of the Swiss Post Voting System's cryptographic protocols and their alignment with version 1.4 of the Swiss Post Voting System's specification. Our work falls into Scope 1 of the Federal Chancellery's (FCh's) Audit concept [AuC22], but *restricted to the Symbolic Proofs*. This means that evaluation of the protocols' *cryptographic proofs* are not in scope of this review, nor are computational cryptography concerns.

This review builds on our previous reviews [RBS22, RBS23].

Documents Reviewed and Supportive Material. Our report is based on the examination of the following files and documents:

- The documents comprising the symbolic models and proofs of the Swiss Post Voting System's cryptographic protocols and accompanying documentation [Mod] as published on 19 February 2024.
- Version 1.4.0 of the Swiss Post Voting System Specification [Spe24a] published on 19 February 2024.
- Version 1.4.1 of the Swiss Post Voting System Specification [Spe24b] published on 21 June 2024.
- E-voting catalogue of measures [CM23] published on 4 August 2023.

The symbolic models and documentation of the Swiss Post Voting System were downloaded from the public repository at the following URL: `https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation`. The links to the specific versions of the files we reviewed are given in the references.

Assessments Undertaken. Our work consisted of the following tasks.

1. Assessment of the alignment of v1.3 of the symbolic models (`Proverif` files [Mod]) with the version 1.4 of the Swiss e-voting protocol specification [Spe24a]. This is discussed in Section 2.
2. Verification of the most recent changes in v1.3 to the `Proverif` files [Mod] (as reported by their changelog). This is discussed in Section 3.
3. Assessment of the state of the symbolic models with respect to item A.12 of the E-voting catalogue of measures [CM23]. This is discussed in Section 4.

We used ProVerif version 2.05 to verify the correctness of the security claims.

2 Alignment between Symbolic Models v1.3 and E-voting Protocol Specification v1.4

We review the major changes that have been introduced in the Swiss e-voting specification between versions 1.3.2 and 1.4.0, and discuss whether and to which degree they have been implemented in the symbolic models. The changes between versions 1.4.0 and 1.4.1 of the e-voting specification do not affect the following observations and recommendations.

2.1 Setup Phase

In version v1.4 of the Swiss e-voting specification, the flow of the `SetupVoting` protocol and the setup of initial data in the so-called `Setup Component` have changed.

This has not led to any changes in any of the `Proverif` files, since this entire setup is not modelled as a protocol flow, but rather the data is a priori "assigned" to each protocol party (e.g., `CCRs`).

2.2 Algorithm 5.4 – `CreateVote`

This algorithm has been refactored to outsource the concatenation of contextual cryptographic parameters (called i_{aux}) to a new `GetHashContext` algorithm. This contextual data (i_{aux}) is an input in the exponentiation zero-knowledge proof (ZKP).

In the current version 1.3 of `Proverif` files, the model of the ZKP is based on an equational theory that is well-aligned with the protocol specification, except that contextual data (i_{aux}) is not included in the modelling of the ZKP's equational theory. We recommend[1] that the symbolic models change to include the i_{aux} data in the modelling of the exponentiation proof. Further, it would be desirable for the names of variables in the symbolic models to more closely align with those in the system specification for this ZKP.

[1] Jira EX-255

Other changes, such as those affecting write-in votes, are below the symbolic models' abstraction level. This means that the symbolic models do not model write-ins, so the changes in the protocol specifications linked to write-ins do not affect the symbolic models.

2.3 Algorithm 5.8 – `CreateLCCShare` & Algorithm 5.11 – `CreateLVCCShare`

These algorithms have been simplified (by removal of exponentiation proofs); this simplification is below the abstraction level of the symbolic models. I.e., the removal of the exponentiation proofs does not imply any change needed in the `Proverif` models.

In Algorithm 5.8, the specified output has been simplified. It now only consists of shares of the choice return codes, thus omitting the hashes of partial return codes from which the shares were computed. A change has been made in the Proverif files that makes the alignment between the models and specification easier to see and a helpful comment is given. A minor readability issue is the use of the `tild` function to represent exponentiation.

The `Proverif` model of Algorithm 5.11, including its changed outputs, remains well aligned with the v1.4. specifications.

2.4 Algorithm 6.1.1 – `GetMixnetInitialCiphertexts` & Algorithm 6.3 – `MixDecOnline`

Via the changes in these two algorithms, in version v1.4 of the specification, the flow of the `MixOnline` protocol in the tally phase has changed to first ensure that all control components have the same view of the initial ciphertexts (i.e., `hvc`s – hashes of cast votes) before the mixing starts.

The privacy models have been adapted to consider this flow at a substantial level of abstraction by introducing a consensus process (CCR_consensus). However, in the `Proverif` files the control components agree on the `hlVCC` values (i.e., which votes were confirmed) and not on the `hvc` values – hashes of cast votes, as per the specification. That means, that the agreement amongst control components in `Proverif` is weaker than in the specifications. It should be possible for the `Proverif` model to more closely follow the specifications, and we would recommend this change.[2]

The verifiability models have not been updated to reflect this change. Whilst this is a misalignment with the specification, it is sufficient for the purpose of the symbolic verification of individual and universal verifiability. However, such a misalignment unnecessarily complicates the assessment of the model's faithfulness to the specification.

[2] Jira EX-254

2.5 Algorithm 6.9 – `ProcessPlaintexts`

This algorithm replaces the old Algorithm 6.7 and has a new validity check on decrypted votes. The symbolic models have not been updated to reflect this. The privacy models are fixed to consider only one vote option while the verifiability models consider two options, and prevent the honest voter in the CreateVote phase from submitting an invalid vote, where the two options are the same.

We consider this level of abstraction to be appropriate.

3 Review of the `Proverif` Files with Respect to Their Changelog

Version 1.3 of the `Proverif` files is stated to have been verified with `Proverif` 2.05. We confirm that all files are successfully processed by `Proverif` 2.05 and the automatic verification returns the expected results.

We find the changelog to be an accurate description of the modifications to the `Proverif` files. Significant changes were made to the files modeling privacy to reflect the updated protocol flow in the `MixOnline` sub-protocol of [Spe24a] and to abstractly model the dispute resolver's `SendVoteAgreement` and `ConfirmVoteAgreement` algorithms.

It is stated in the symbolic models' changelog that the symbolic models are aligned with version 1.4 of the system specification. We confirm that the `Proverif` files are a good abstract model of version 1.4 of the specification.

However, as detailed in the previous section, some changes to the specification have not been reflected in the models which causes the alignment between the specification and the models to drift apart. We refer to our previous reviews for other areas of misalignment between the symbolic models and the specification, e.g., in that only the main protocol flows are modeled [RBS23].

4 State of the Proverif Files with Respect to Measure A.12

Measure A.12 of the Catalogue of Measures [CM23], which entails recommendations made in [RBS22], is planned for 2025 and has not been addressed in this version of the symbolic models.

References

[AuC22] *Audit concept v1.4 – For examining Swiss internet voting systems.* Swiss Federal Chancellery, 2022.

[CM23] Catalogue of measures by the Confederation and cantons, August 2023. `https://www.bk.admin.ch/bk/en/home/`

politische-rechte/e-voting/versuchsuebersicht.html. Accessed 2nd May 2024.

[Mod] Proverif Models of the Swiss Post Voting System. https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/documentation-1.6.0.0/Symbolic-models, commit 20d8d70723747305bda848c884b7febd07ddcba8, accessed 1st May 2024.

[RBS22] Saša Radomirović, Ioana Boureanu, and Steve Schneider. Review of the Symbolic Proofs for the Swiss Post Voting System's Cryptographic Protocols, October 2022. https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%201%20Final%20Report%20University%20of%20Surrey%2017.10.2022.pdf.download.pdf/Scope%201%20Final%20Report%20University%20of%20Surrey%2017.10.2022.pdf. Accessed 2nd May 2024.

[RBS23] Saša Radomirović, Ioana Boureanu, and Steve Schneider. Review of the Additions to the Symbolic Proofs Concerning the Authentication Subprotocol of the Swiss Post Voting System, June 2023. https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_August2023/Scope%201%20Final%20Report%20University%20of%20Surrey%2030.06.2023.pdf.download.pdf/Scope%201%20Final%20Report%20University%20of%20Surrey%2030.06.2023.pdf. Accessed 2nd May 2024.

[Spe24a] Swiss Post Voting System – System Specification. Version 1.4.0, February 2024. https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/documentation-1.6.0.0/System/System_Specification.pdf, commit 20d8d70723747305bda848c884b7febd07ddcba8, accessed 1st May 2024.

[Spe24b] Swiss Post Voting System – System Specification. Version 1.4.1. June 2024. https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/documentation-1.6.3.1/System/System_Specification.pdf. Accessed 24 July 2024.