

# Review of the Symbolic Models V1.4 of the Swiss Post Voting System V1.5

Saša Radomirović<sup>1</sup>, Ioana Boureanu<sup>2</sup>, and Steve Schneider<sup>2</sup>

<sup>1</sup> Heriot-Watt University, Edinburgh, UK

<sup>2</sup> Surrey Centre for Cyber Security, University of Surrey, UK

17 December 2025

## 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 1.5.2 of the Swiss Post Voting System’s specification [Sys25]. Our work falls into Scope 1 of the Federal Chancellery’s (FCh’s) Audit concept [AuC25], 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, RBS24].

**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 in June 2025.
- Versions 1.5.0 and 1.5.2 of the Swiss Post Voting System Specification [Sys25] published in June 2025 and October 2025, respectively.
- E-voting catalogue of measures [CM23] published in 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. Review of the most recent changes to the Proverif models [Mod] with respect to their changelog. This is discussed in Section 2.

2. Review of the models with respect to previous recommendations made and 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 3.
3. Overall assessment of the models. This is discussed in Section 4.

## 2 Review of the Proverif files with respect to their changelog

We find the changelog to be an accurate description of the modifications to the Proverif files. The following subsections summarise and confirm the changes made to each of the Proverif files.

### 2.1 Verifiability Models

#### Individual-Verifiability-2CCRs-n=4-psi=1.pv

Significant improvements were made to the model. The encryption of partial Choice Return Codes with  $pk_{CCR}$  was added, and the zero-knowledge proofs were extended to include  $r2$ ,  $pk_{CCR}$ , and  $vc\_id$ , thereby improving their faithfulness to the specification. The modelling of decryption was also refined: `DecMerge` was removed and replaced with the more general `PartialDec()`, and `mergepk` was replaced with `t_ekeypair()`, `mergePKSK()`, and `mergePKPK`. Moreover, the lists  $L_{decPCC}$ ,  $L_{sentVotes}$ , and  $L_{confirmedVotes}$  were remodelled in a more faithful way, and the computation of  $hhlVCC\_id$  was improved by adding  $vc\_id$ . The `dishonest_CCR_log()` process was also aligned with the agreement procedure, so that it now requires voting-phase evidence, thus strengthening individual verifiability. Overall, this model has implemented most recommendations and does more faithfully reflect the specification.

#### Individual-Verifiability-2CCRs-n=4-psi=2.pv

The same family of changes was carried out when  $\psi = 2$  selections out of  $n = 4$  options can be voted for. In particular, this variant incorporates the updated zero-knowledge proof equations and CCR processes, in line with the changelog found online.

#### Universal-Verifiability-2CCMs-n=4-psi=2.pv

For the universal verifiability case, the partial decryption modelling was cleaned up by removing `PDec1` and `PDec2` and replacing them with `PartialDec`, `Dec`, and `t_ekeypair(..)`. The modelling of lists was also made more faithful and consistent across decryption steps. These changes ensure that the universal verifiability proofs are better aligned with the voting specification, and overall this model, too, implements most of the suggestions made in 2024.

## 2.2 Privacy Models

### `Vote_privacy_CCM1.pv`

This is the model where CCM1 is assumed to be trustworthy. The 2025 version of the model incorporates several corrections and alignments that improve on the 2024 version. Variable names were harmonised (`lvcc_j_id` replacing `lvcc_id_j` and `hlvcc_j_id` replacing `hlvcc_id_j`), removing an albeit minor source of confusion across processes. No structural change was necessary to relocate ZKP verification into the setup component, since the symbolic model already performed verification there; as a result, the specification and model are now better aligned.

Collectively, these changes increase internal consistency, make the processes executable in the intended traces, and thus improve the privacy analysis.

### `Vote_privacy_CCM2-3-4.pv`

This is the complementary model where at least one of the CCMs is assumed to be trustworthy. The same family of improvements as above were applied, with special attention to the execution paths when CCM2-3-4 is honest. Small but necessary adjustments were introduced in the CCM1 and CCM2\_3.4 processes to ensure that honest-mix configurations progress without deadlocks or unreachable branches.

In addition, an execution bug in the CCR process was fixed: a previously unsatisfiable precondition guarded an `insert ConfirmedVotes(j,vcid,B)` command, preventing it from ever firing; the corrected guard now makes the insertion executable under its intended conditions.

Together with the variable-name harmonisation, these modifications bring the 2025 variant into closer agreement with the intended privacy guarantees while preserving executability and trace completeness in honest scenarios.

## 3 Review of previous recommendations and state with respect to Measure A.12

Measure A.12 of the Catalogue of Measures [CM23], which entails recommendations made in [RBS22], is planned for a future release and has not been fully addressed in this version of the symbolic models. We summarise the state of the models with respect to our 2024 findings [RBS24] and the Catalogue of Measures [CM23] in Table 1.

Issue	2025 Status	Notes
<b>Setup Phase</b> SetupVoting flow not modelled; initial data is simply assigned.	not addressed	2025 models still treat setup as pre-assigned data, no explicit protocol flow; this may be OK for now, according to discussions in meetings.
<b>Algorithm 5.4 CreateVote</b> Contextual data ( <code>iaux</code> ) missing from ZKP model.	partially addressed	ZKPs extended with $r2$ , $pk_{CCR}$ , and $vc.id$ for more faithful modelling, but <code>iaux</code> still absent.
<b>Algorithms 6.1.1 &amp; 6.3 Mixnet Initial Ciphertexts / MixDecOnline</b> Models consensus on $hlVCC$ (confirmed votes) instead of $hvc$ (hashes of cast votes).	not addressed	2025 models still use $hlVCC$ ; no $hvc$ -level consensus introduced.
<b>Faithfulness &amp; Alignment (lists, dishonest CCR log)</b> Misalignment in <code>dishonest_CCR_log()</code> , weak modelling of lists.	addressed	2025 models fix <code>dishonest_CCR_log()</code> alignment, strengthen individual verifiability, and improve modelling of $L_{decPCC}$ , $L_{sentVotes}$ , $L_{confirmedVotes}$ .
<b>Measure A.12</b> Further develop symbolic proof of cryptographic protocol compliance.	pending	This is planned for future work.

Table 1: The 2025 symbolic models in the light of the 2024 report [RBS24].

## 4 Overall assessment of the models

Version 1.4 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 report here on two minor issues that we have found in our overall inspection of the models.

### 4.1 Missing traces

We have found the following issue in the 2025 model, but it also affects the 2024 models.

In the Individual-Verifiability models, the `VerifP` reduction models a correct zero-knowledge proof (ZKP) by defining when a ZKP proof is correct (by returning `true`). This reduction is used exactly once in the `ProcessVoteCheck` function, which in turn is used in the CCR process. The `ProcessVoteCheck` function always returns `true`, regardless of the result of `VerifP`. For instance, in the 2025 (and likewise in the 2024) models we find:

```
letfun ProcessVoteCheck(ELpk:public_ekey,pkCCR:public_ekey,
                       VCid:vc_id,B:bitstring) =
  let (xE1:bitstring, xE2:bitstring, xKVCId: public_ekey,
       xP:bitstring) = B in
  let Ok1 = VerifP(ELpk,pkCCR,xKVCId,VCid,xE1,xE2,xP) in
  true.
```

Thus, although the value of `VerifP` is computed and bound to `Ok1`, it is never checked. The consequence is that `ProcessVoteCheck` will always succeed, even if the ZKP were incorrect. This undermines the intended faithful modelling of the ballot verification step.

### 4.2 Administrative vs Electoral Board Keys

The symbolic models related to verifiability use the term `ABsk` to represent, presumably, the electoral board members' private key. This should be changed to `EBsk`, unless it is chosen on purpose to refer the the administrative board in which case this should be clarified. The system specification documents do not refer to an administrative board. However, other documents in the Swiss Post's collection additionally refer to (cantonal) administrators, e.g., the operations documents [Ope25] and a distinction between the administrative board and the electoral board is made in risk assessments of some cantons, e.g., [Can25].

## References

- [AuC25] *Audit concept v1.6 – For examining Swiss internet voting systems*. Swiss Federal Chancellery, 2025.

- [Can25] Risikoportfolio, 2025. [https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting/Bewilligungsverfahren-Dokumentation-Weiterentwicklung/\\_jcr\\_content/Par/sgch\\_downloadlist/DownloadListPar/sgch\\_download\\_1784384766.ocFile/E-Voting%20-%20Risikoportfolio.pdf](https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting/Bewilligungsverfahren-Dokumentation-Weiterentwicklung/_jcr_content/Par/sgch_downloadlist/DownloadListPar/sgch_download_1784384766.ocFile/E-Voting%20-%20Risikoportfolio.pdf).
- [CM23] Catalogue of measures by the Confederation and cantons, August 2023. <https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsubersicht.html>. Accessed 8 November 2024.
- [Mod] Proverif Models of the Swiss Post Voting System. <https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/documentation-1.7.0.0/Symbolic-models>, accessed 7th August 2025.
- [Ope25] Operations, 2025. <https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/documentation-1.7.0.0/Operations>.
- [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](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](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.
- [RBS24] Saša Radomirović, Ioana Boureanu, and Steve Schneider. Review of the Symbolic Models V1.3 of the Swiss Post Voting System V1.4, August 2024. [https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E\\_Voting/Examination\\_reports\\_August2024/Scope%201%20Final%20Report%20University%20of%20Surrey%2024.07.2024.pdf.download.pdf/Scope%201%20Final%20Report%20University%20of%20Surrey%2024.07.2024.pdf](https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_August2024/Scope%201%20Final%20Report%20University%20of%20Surrey%2024.07.2024.pdf.download.pdf/Scope%201%20Final%20Report%20University%20of%20Surrey%2024.07.2024.pdf).
- [Sys25] Swiss Post Voting System – System Specification. June 2025. Version 1.5.2. <https://gitlab.com/swisspost-evoting/e-voting/>

e-voting-documentation/-/blob/documentation-1.7.2.0/  
System/System\_Specification.pdf. Accessed 4th November 2025.