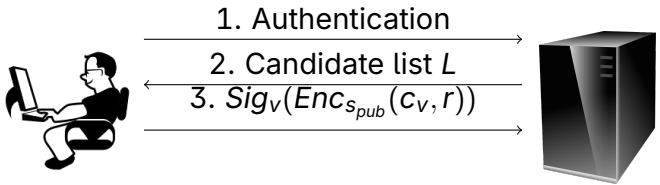
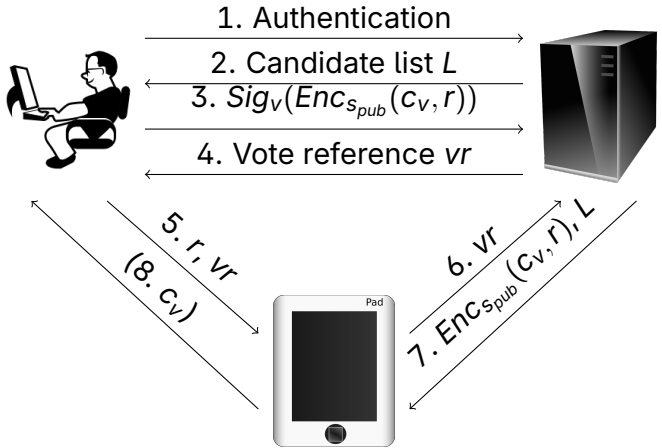
Zero-knowledge proofs in Estonian e-voting

Jan Willemson

Estonian Internet voting scheme 2013...2015

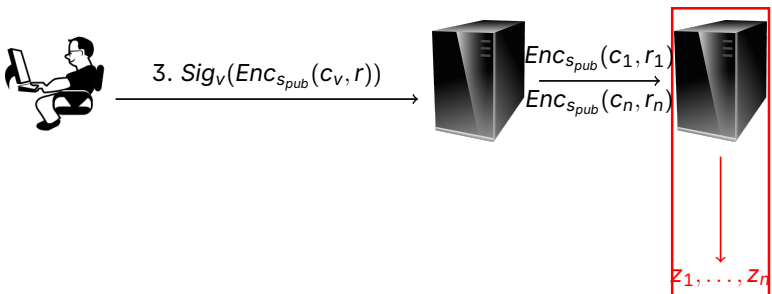


Estonian Internet voting scheme 2013…2015



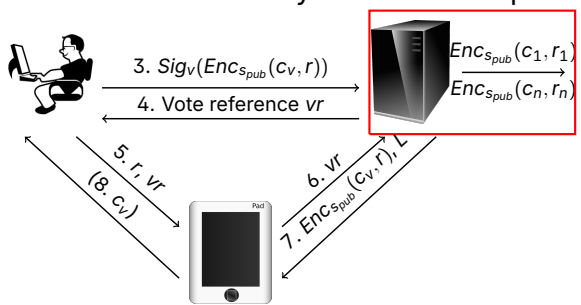
Shortcomings: tabulation integrity

- It is not possible to verify the correctness of the decryption.
- Compromised tabulation tool could change the result without anyone noticing.



Shortcomings: i-ballot box integrity

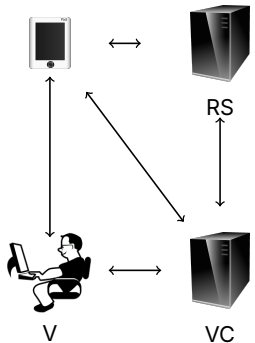
- Assuming the outer envelope (a.k.a. *signature*) can not be forged, ballot box stuffing and vote manipulation are practically unachievable.
- However, a malicious ballot box may choose to drop votes.



Third party auditability

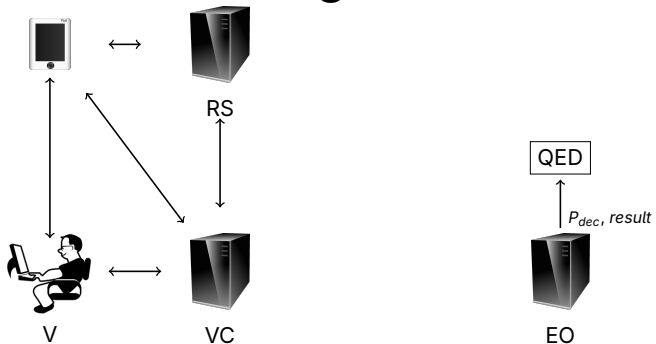
- We want to allow a third party auditor to verify i-ballot box properties in a privacy preserving manner.
  - The auditor should be able to check the eligibility, well-formedness and tallied-as-recorded properties.
  - We need assurance that there is no invisible way to drop votes.
- If the integrity of the vote collection can be audited, it becomes possible to outsource this procedure.
- The verifiability of the correct tabulation would increase the trustworthiness of the voting result.

IVXV (2017…): The Big Picture



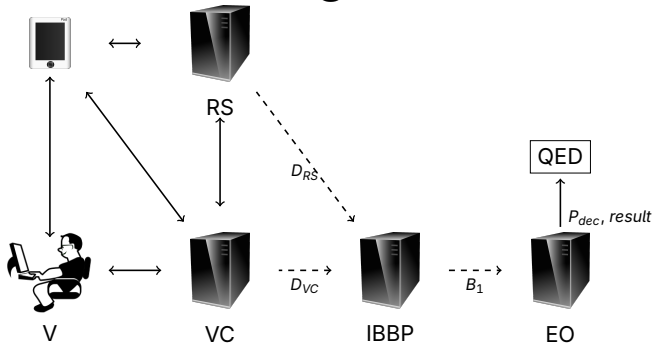
- Vote Collector shall register each vote to an independently hosted Registration Service.
- The consistency shall be audited both by voters and auditors.

IVXV (2017…): The Big Picture



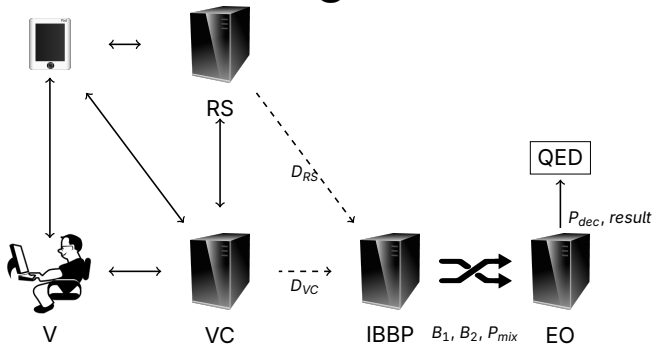
- The tabulation application shall provide a proof of correct decryption for each ballot.

IVXV (2017…): The Big Picture



- The i-ballot box processor audits the vote collection and anonymizes votes for the tabulation.

IVXV (2017…): The Big Picture



- In order to provide an external auditor with access to both digitally signed votes and decryption proofs, a verifiable re-encryption mix-net (Verificatum) was applied.

IVXV and ZK 2017…2025

- ZK proof of correct mixing.
- ZK proof of correct decryption.

IVXV and ZK 2017…2025

- ZK proof of correct mixing.
- ZK proof of correct decryption.
- But who can verify these proofs?
  - Input to mixing still contains private data (personalizable cryptograms), so these proofs can only be verified by NDA-bound auditors.
  - Decryption result together with its input and output can, in principle, be public

IVXV and ZK 2017…2025

- ZK proof of correct mixing.
- ZK proof of correct decryption.
- But who can verify these proofs?
  - Input to mixing still contains private data (personalizable cryptograms), so these proofs can only be verified by NDA-bound auditors.
  - Decryption result together with its input and output can, in principle, be public
  - … unless someone has managed to manipulate their vote so that the decryption output will leak something.

ZK to the rescue again!

- In order to prevent decryption output from leaking, we would like to audit the ballots at the time of submission.
- However, the ballots are encrypted.
- Still, we can force the voting application (even a self-written one!) to provide a ZK proof that the ballot takes a value in the predefined list of candidates.
- This feature will be implemented for 2027 Parliamentary elections.

Thank you!

- Questions?

cybernetica
Cybernetica
cybernetica_ee
Cybernetica