Panoramix

Addressing the Challenges of e-Voting Through Crypto Design

Thomas Zacharias

University of Edinburgh

29 November 2017

Scotland's Democratic Future: Exploring Electronic Voting

Scottish Government and University of Edinburgh

School of Informatics Workshop

When do we actually setup an electronic voting procedure?

- What is the extent of “digitilisation” of a traditional election protocol that qualifies as e-voting?

When do we actually setup an electronic voting procedure?

E-voting means the use of electronic means in one of the following three processes:

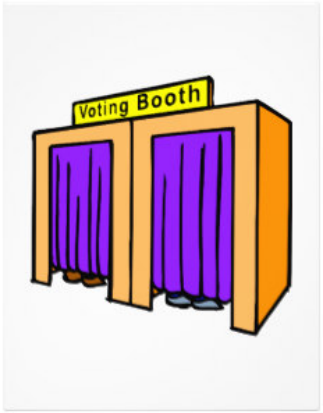
- Identification of voters
- Casting the vote
- Counting the vote

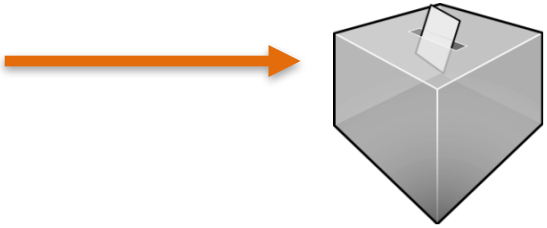
Source: https://www.e-voting.cc/en/it-elections/definitions/

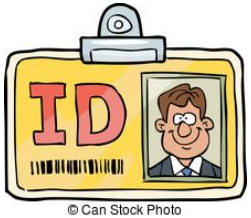
When do we actually setup an electronic voting procedure?

- What is the extent of “digitilisation” of a traditional election protocol that qualifies as e-voting?
  - Registration
  - Voting
  - Counting
  - Auditing

Replacing the human protocol with electronic procedures

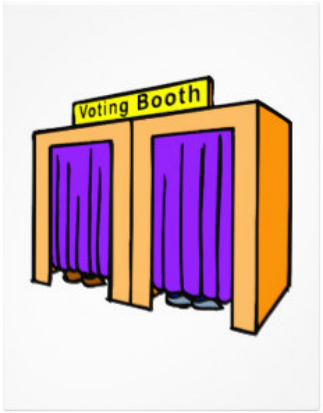


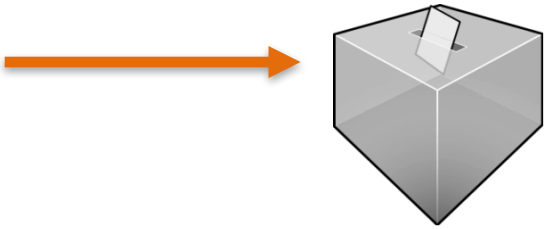


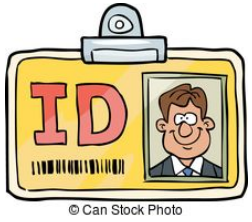


© Can Stock Photo

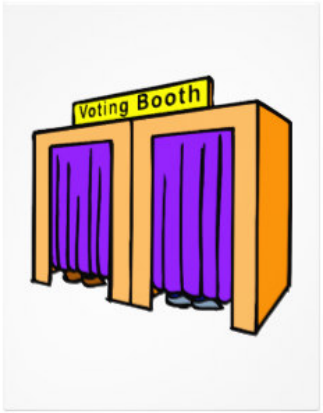
Replacing the human protocol with electronic procedures

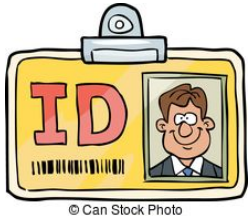




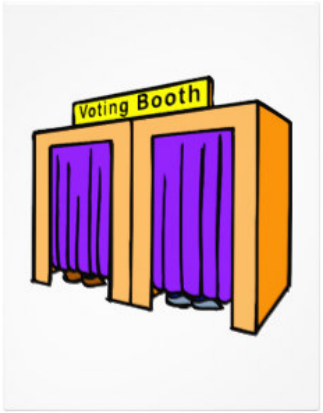


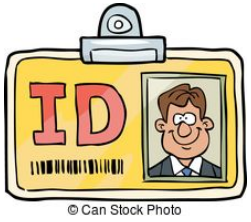
Replacing the human protocol with electronic procedures



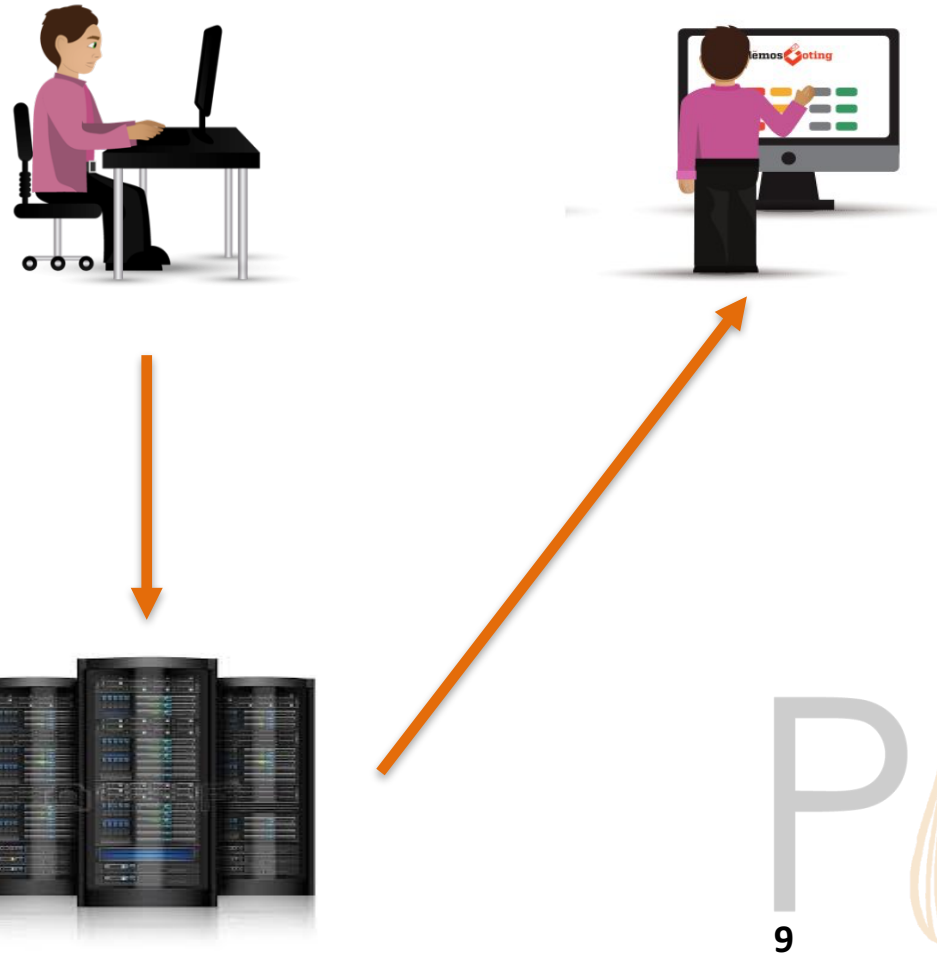


Replacing the human protocol with electronic procedures





Replacing the human protocol with electronic procedures



The benefits of e-voting

- Increase the participation of social groups that face considerable physical barriers.
- Increase the efficiency of the preparation of the election and the calculation of the final results.
- Reduce the financial cost of the elections (in long term).

The risks of e-voting

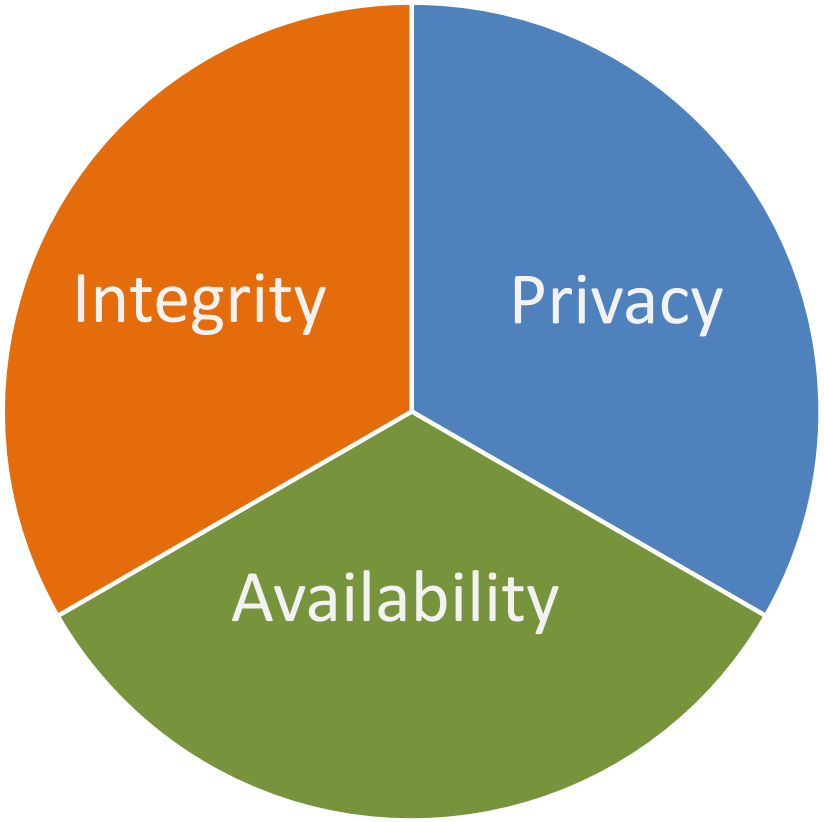
- Unauthorised intervention of third parties may cause denial of service.
- Large-scale manipulation by a small group of insiders.
- Lack of widely agreed standards for the election procedure (infrastructure, software).

The challenges of e-voting

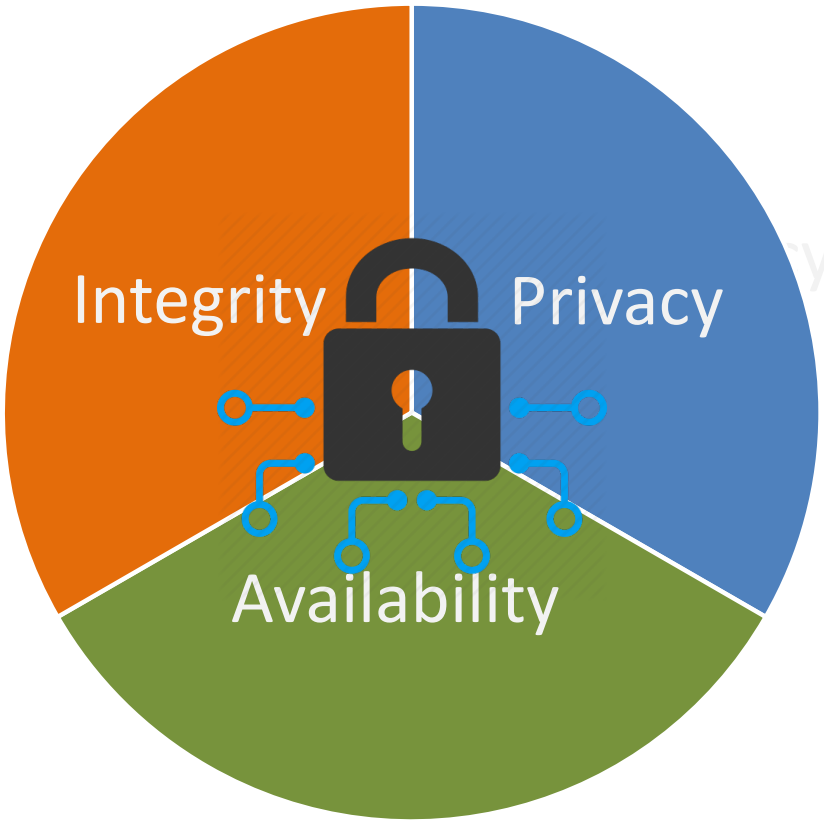
- At any point of replacing the traditional protocol with electronic means, extreme care in the algorithmic design, implementation, and execution oversight is required.

The challenges of e-voting

- Preserve the fundamental requirements of a voting system.



Addressing e-voting challenges via cryptographic tools



Modern cryptographic design

1. Understanding and formal definition of the studied notion.
2. Rigorous specification of the threat model.
3. Realisation via a well-described construction.
4. Mathematical proof of the construction's security under the defined threat model.

Modern cryptography in the real-world

- Secure internet communication (HTTPS over TLS/SSL, end-to-end encryption).
- Authentication (Digital signatures, password management).
- Privacy preservation (aggregate statistics, anonymous web browsing).
- Blockchain technologies (Bitcoin, Ethereum, smart contracts).

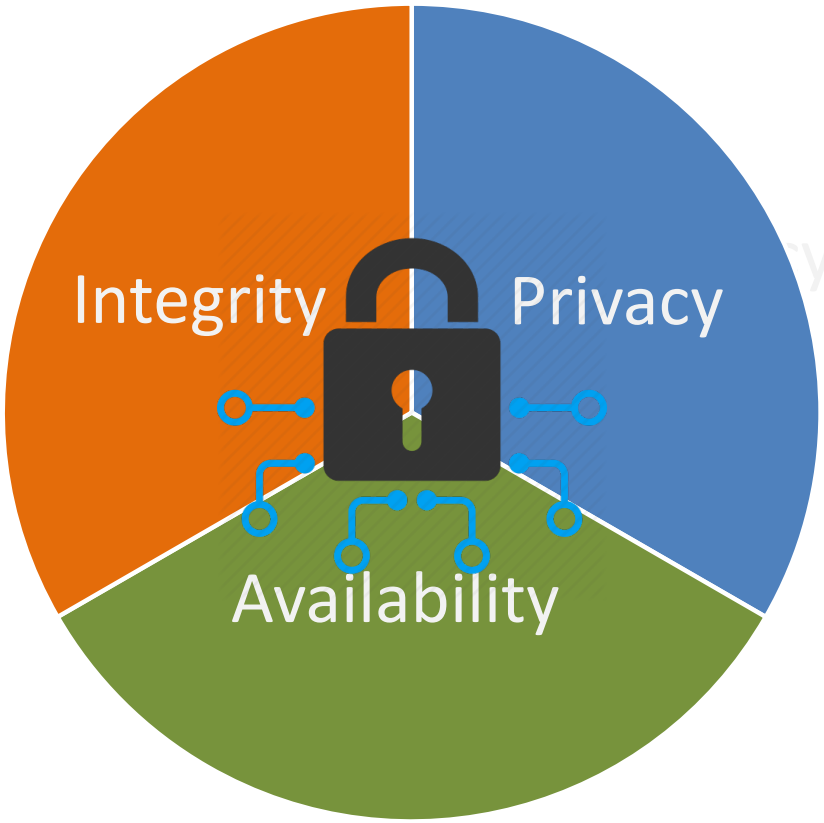
Modern cryptography in the real-world

- Secure web browsing.
- E-banking.
- E-mail.
- Privacy-preserving profile management.
- Secure messaging.
- Decentralised publicly verifiable transactions.

The necessity of cryptography for realising secure e-voting

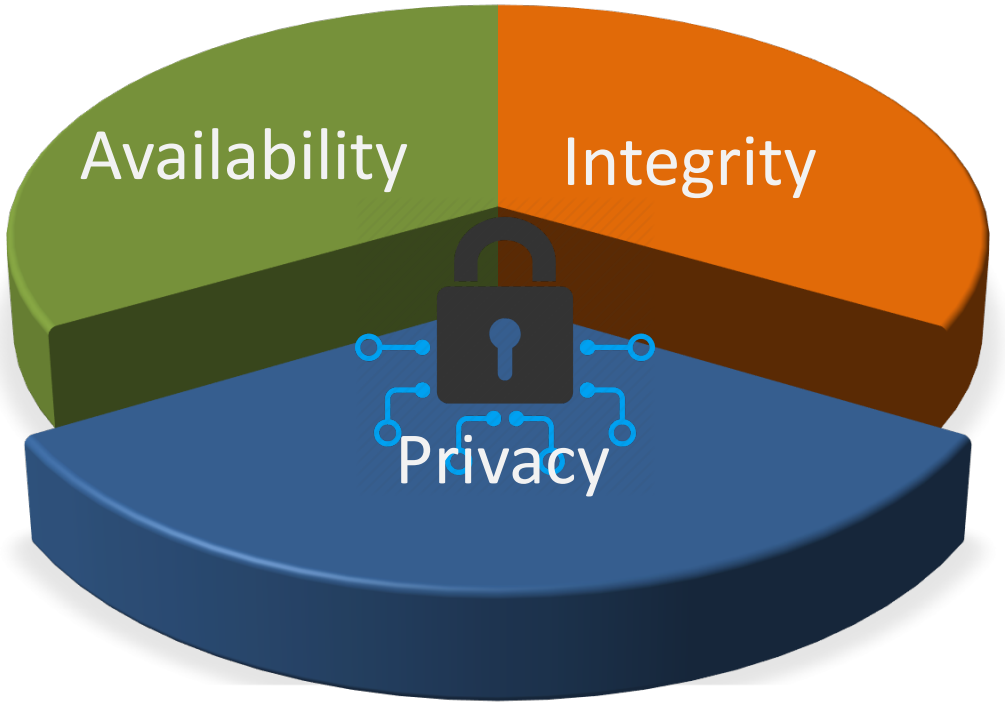
- Collecting, storing and/or communicating sensitive election data overtly, can easily jeopardise election security.
- Offline (on site): a vote collection device that keeps logs of unencrypted ballot casting can not protect voters' privacy when the logs are audited.
- Online: whenever two devices should interact, secure and authenticated communication must be applied to protect the exchanged data.

Addressing e-voting challenges via cryptographic tools



Addressing e-voting challenges via cryptographic tools:

Privacy

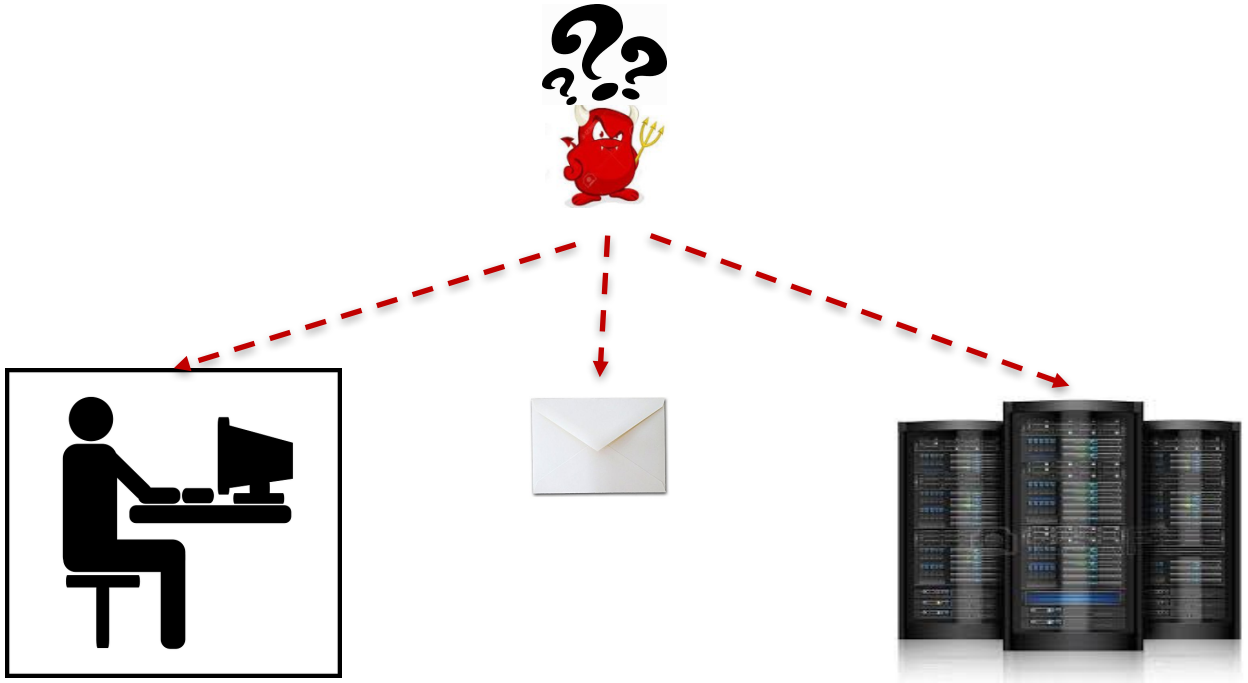


Ballot secrecy

- Encryption realises the concept of a “digital envelope”.
  - The voter’s selection is cryptographically “sealed”.
  - An attacker can not obtain information about the encryption’s content (vote selection).

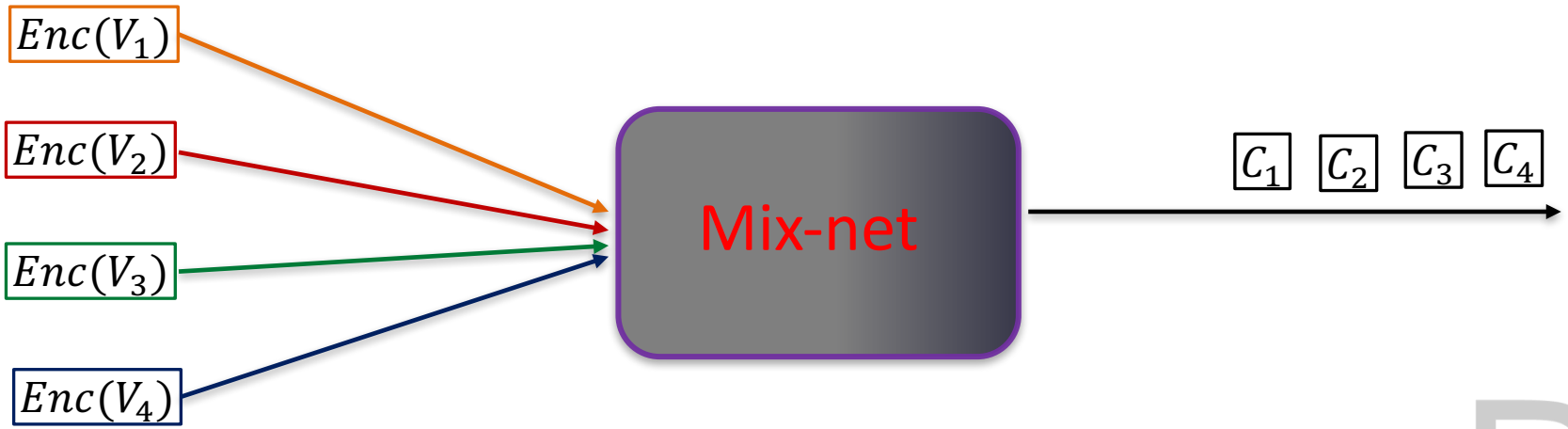
Voter-vote Unlinkability

- At some point of the election process, the votes must be anonymised, to prevent coercion and vote-selling.



Voter-vote Unlinkability

- Mix-nets: a powerful cryptographic primitive realising vote shuffling in a digital ballot box.



$$\{C_1, C_2, C_3, C_4\} = \{Enc(V_1), Enc(V_2), Enc(V_3), Enc(V_4)\}$$

Voter-vote Unlinkability

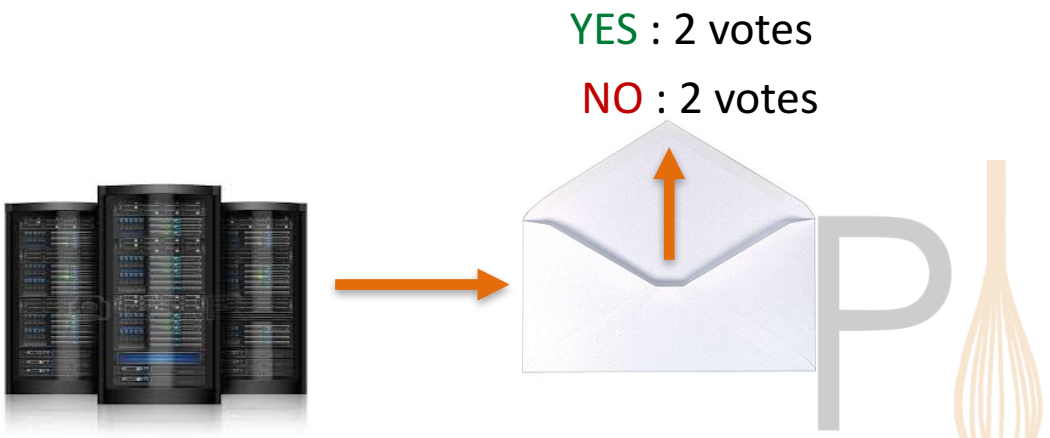
- Additive homomorphic tally: a mathematical property of special encryption schemes (E.g. ElGamal, Paillier) that allow for the counting of votes in encrypted manner.

$$Enc(X) \cdot Enc(Y) = Enc(X + Y)$$

Voter-vote Unlinkability

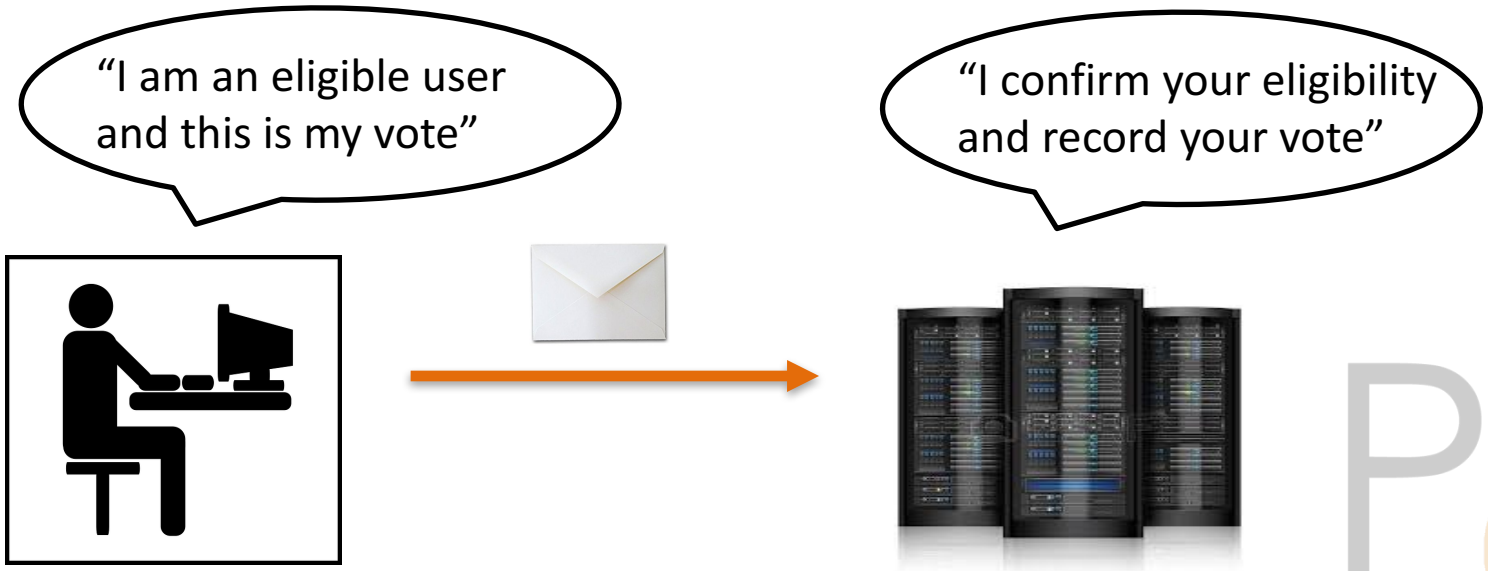
- Additive homomorphic tally: a mathematical property of special encryption schemes (E.g. ElGamal, Paillier) that allow for the counting of votes in encrypted manner.

$$Enc(X) \cdot Enc(Y) = Enc(X + Y)$$



Voter-vote Unlinkability

- Anonymous authentication: the voter proves her eligibility via a one-show anonymous credential (e.g. blind signature of the voter's ballot).

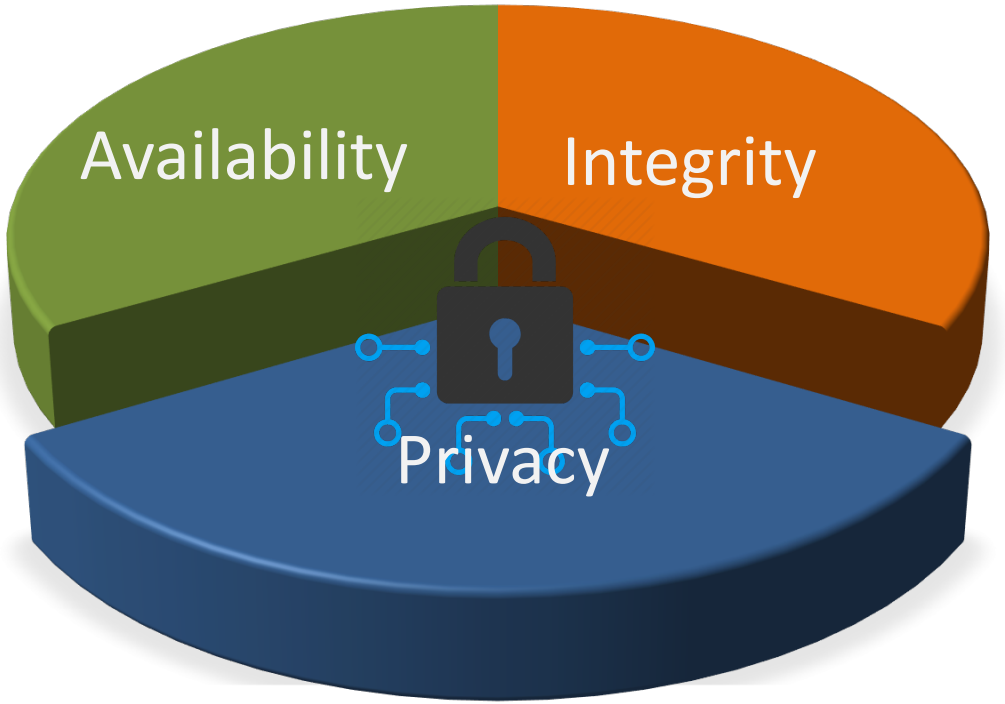


Coercion resistance

- Concerns about coercion in other types of remote voting (e.g. postal voting) also apply to internet voting.
- In cases where postal voting is allowed, internet voting could be used, supporting multiple voting as a coercion countermeasure (Estonian e-voting).

Addressing e-voting challenges via cryptographic tools:

Privacy



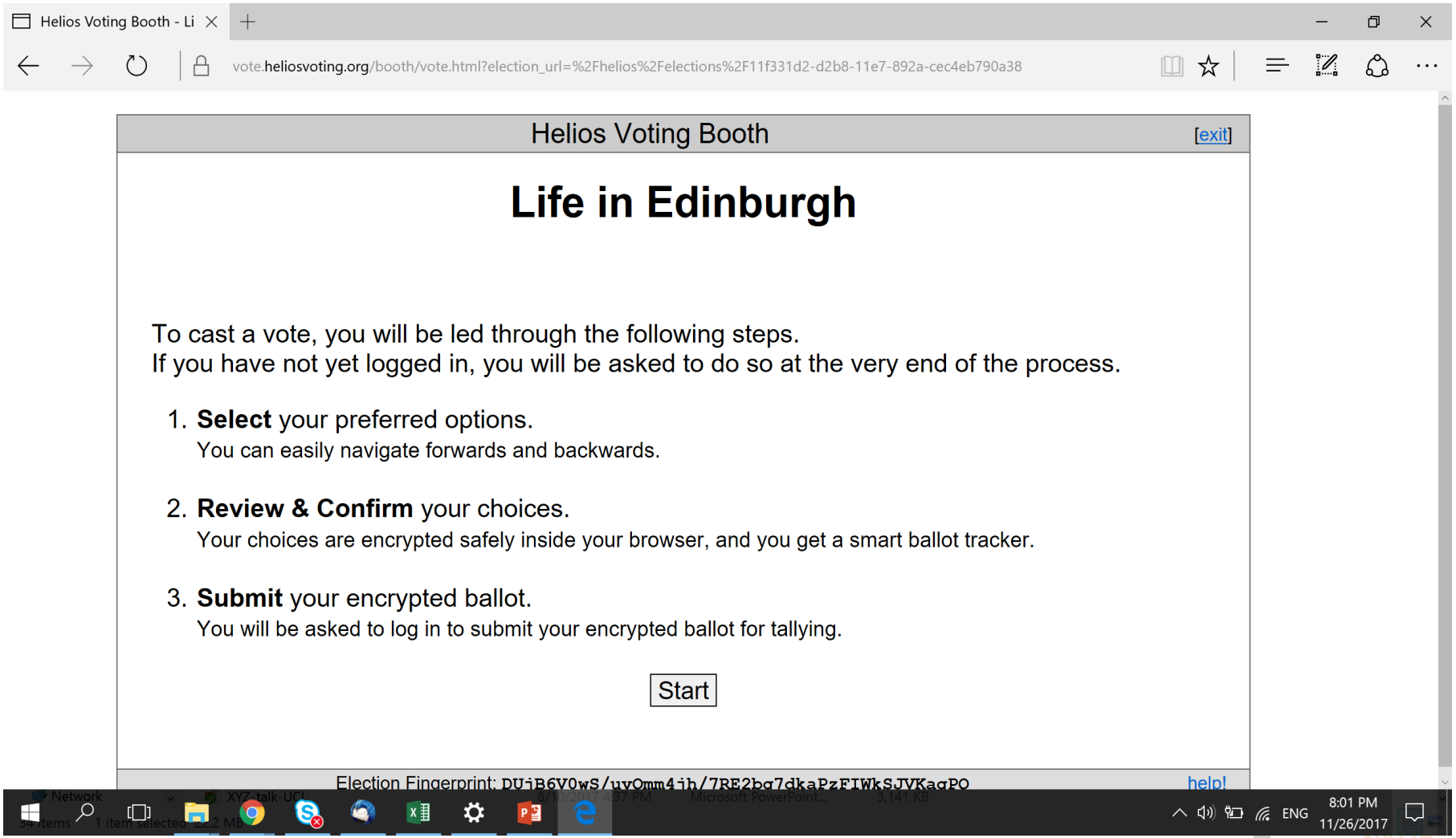
Addressing e-voting challenges via cryptographic tools:

Availability

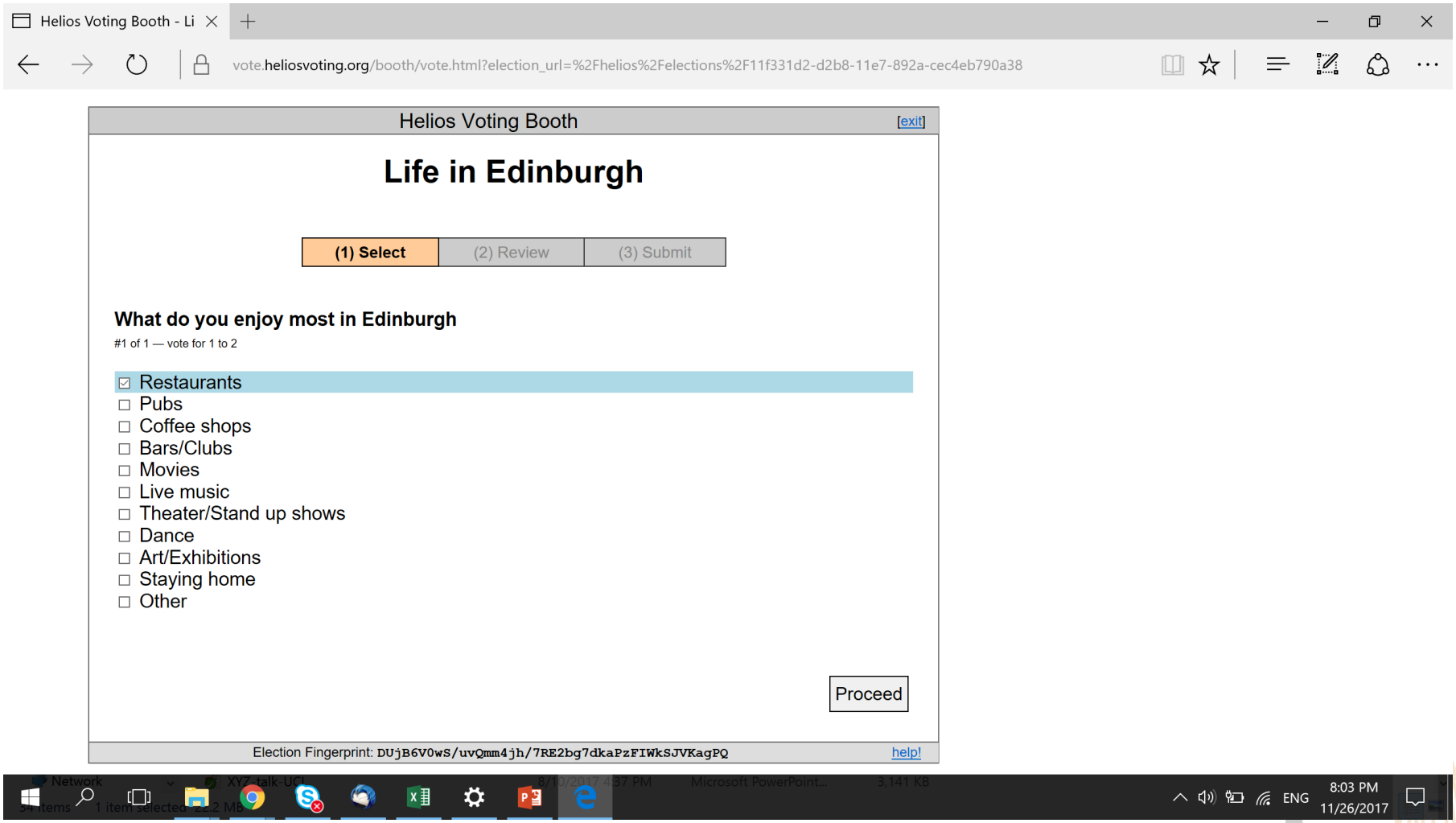
Usability: making e-voting feasible for every citizen

- When ballot encoding is applied during vote casting, the voter interacts via a user-friendly interface in a designated voting device, or their browser.
- Basic familiarity with a standard operating system (e.g., Windows, iOS, Android) or web browser (e.g., Edge/Explorer, Safari, Chrome, Firefox) is the only required background.

Usability: making e-voting feasible for every citizen



Usability: making e-voting feasible for every citizen



Usability: making e-voting feasible for every citizen

Usability: making e-voting feasible for every citizen

- When code-voting is applied, the voter obtains a ballot with a pre-encoding of the election options (vote-code).

Usability: making e-voting feasible for every citizen

What is your stance on the potential of adopting e-voting for national elections?

Serial number: **100**	
1	VERY POSITIVE
4	POSITIVE
5	NEUTRAL
2	NEGATIVE
3	VERY NEGATIVE

Usability: making e-voting feasible for every citizen

- When code-voting is applied, the voter obtains a ballot with a list of random cryptographic pre-encoding of the election options (vote-code).
- The voter simply submits the vote-code that correspond to her option selection, which can be done in lightwight electronic devices.

Usability: making e-voting feasible for every citizen

Serial number: **100**
Vote-code: **5**

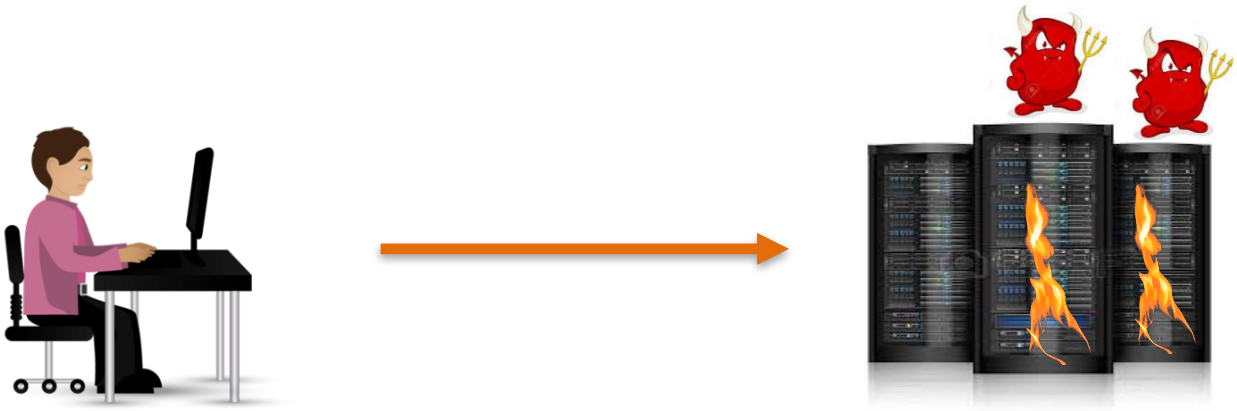
Serial number: **100**	
1	VERY POSITIVE
4	POSITIVE
5	NEUTRAL
2	NEGATIVE
3	VERY NEGATIVE

Usability: making e-voting feasible for every citizen

- When code-voting is applied, the voter obtains a ballot with a list of random cryptographic pre-encoding of the election options (vote-code).
- The voter simply submits the vote-code that correspond to her option selection, which can be done in any electronic device with internet access.
- In case the voting device is trusted for privacy, vote casting can run via a user-friendly interface.

Fault tolerance: protecting the election's liveness

- Threshold cryptography in combination with a distributed system architecture allows for a secure and uninterrupted election access and execution, even when a substantial amount of election servers is not available.

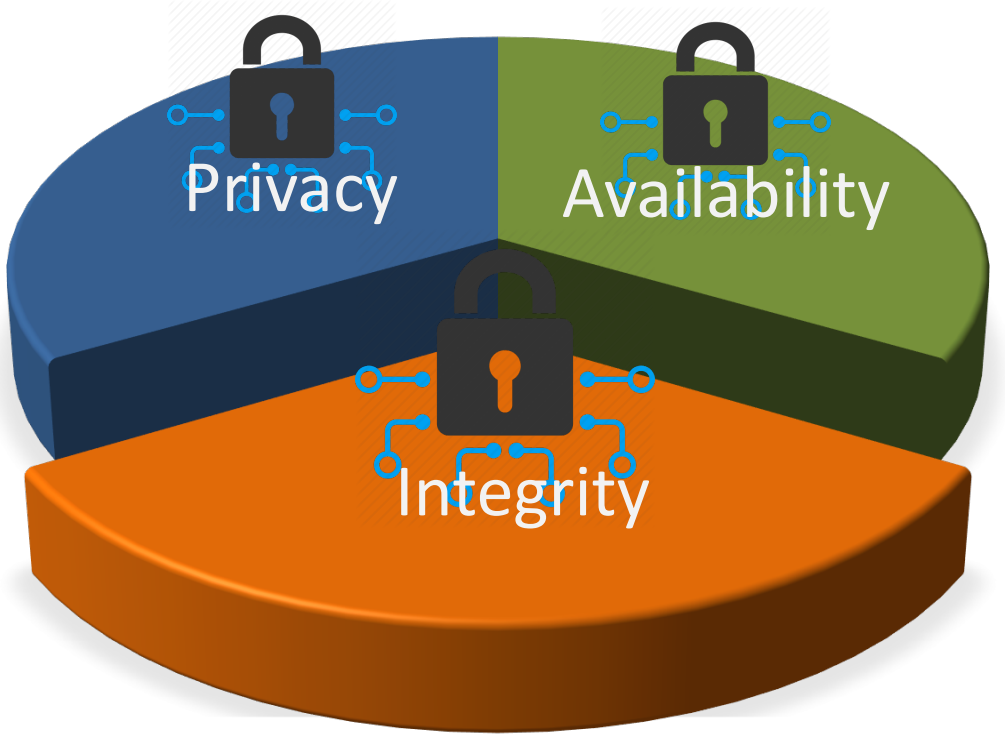


Addressing e-voting challenges via cryptographic tools:

Availability

Addressing e-voting challenges via cryptographic tools:

Integrity



Eligibility

- The authentication/registration authority is equipped with the algorithm that specifies the set of eligible voters.
  - Digital signatures: each voter has an ID-card with an embedded signing key (Estonia).
  - Password-based: the authentication server(s) maintains a cryptographic hash table with all the passwords that correspond to eligible voters.

End-to-end verifiability

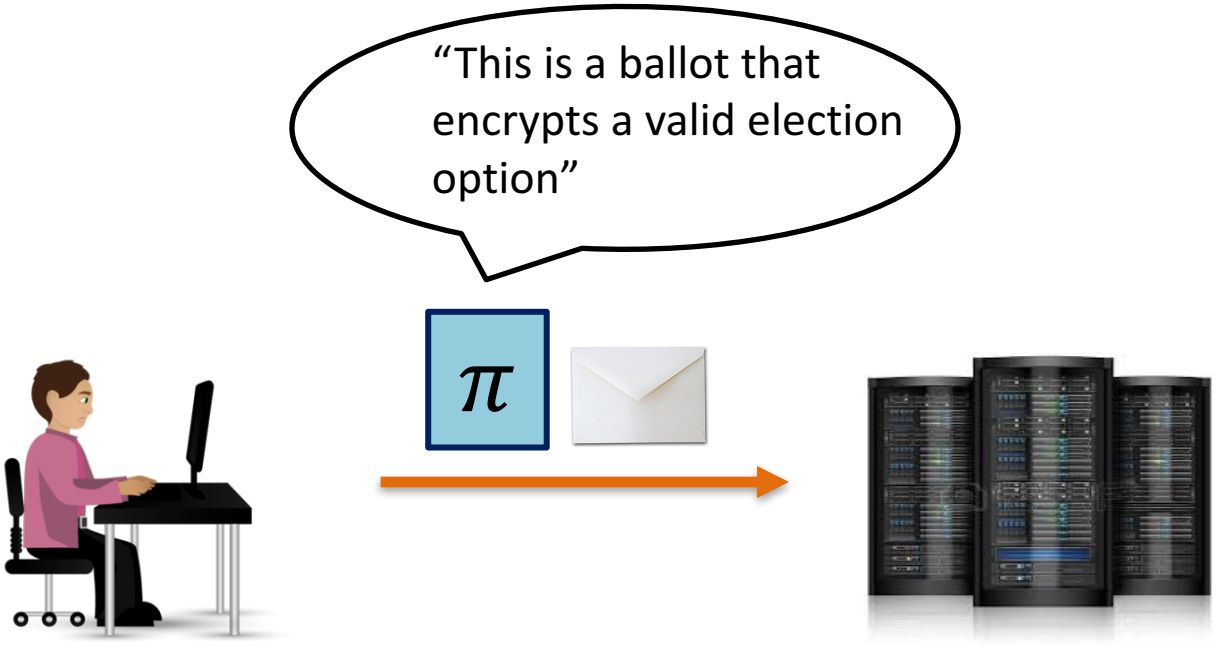
- **Universal level:** Any party can verify the correctness of the election transcript.

End-to-end verifiability

- **Individual level:** The voters obtain some audit data in order to verify themselves that their votes were:
  - **Cast-as-intended**
  - **Recorded-as-cast**
  - **Tallied-as-recorded**

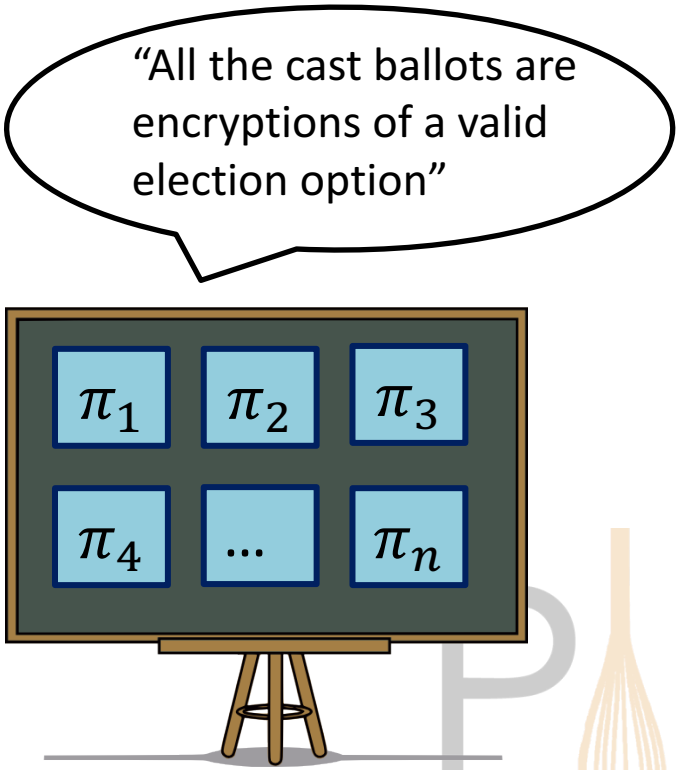
Universal Verifiability

- Every step of the election procedure is associated with a cryptographic proof of its execution.



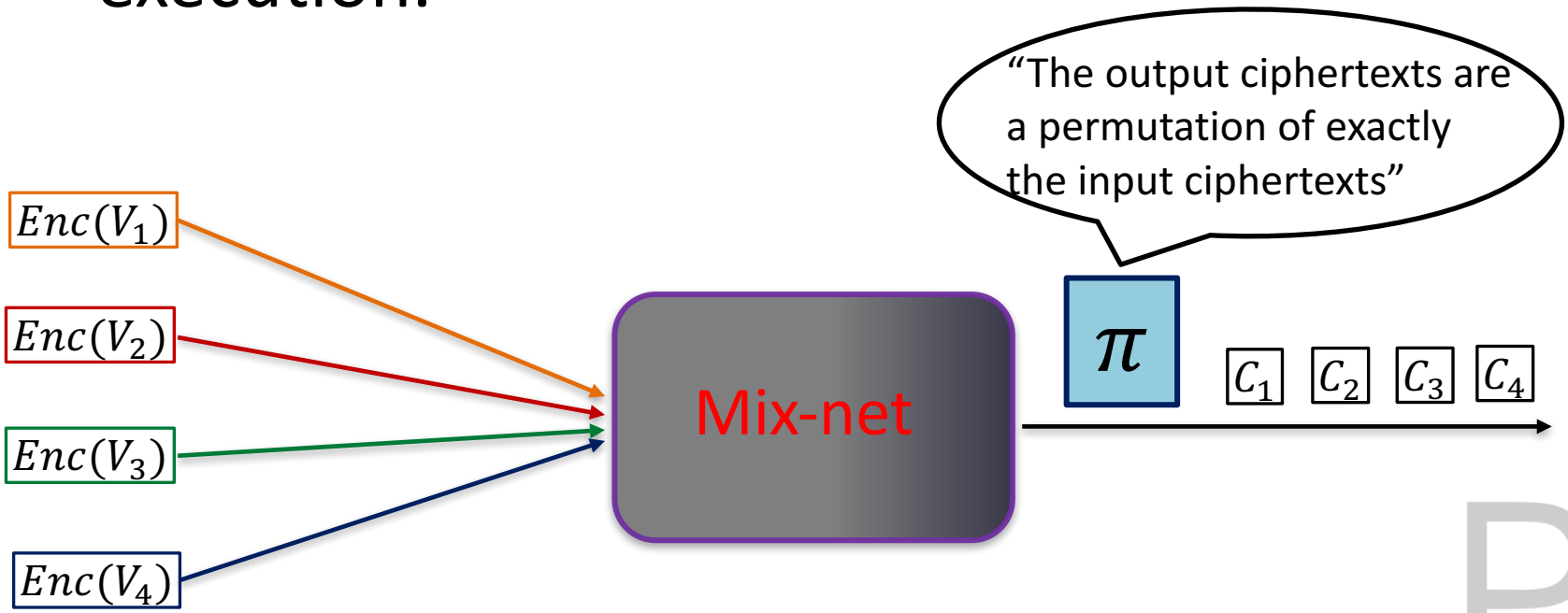
Universal Verifiability

- Every step of the election procedure is associated with a cryptographic proof of its execution.



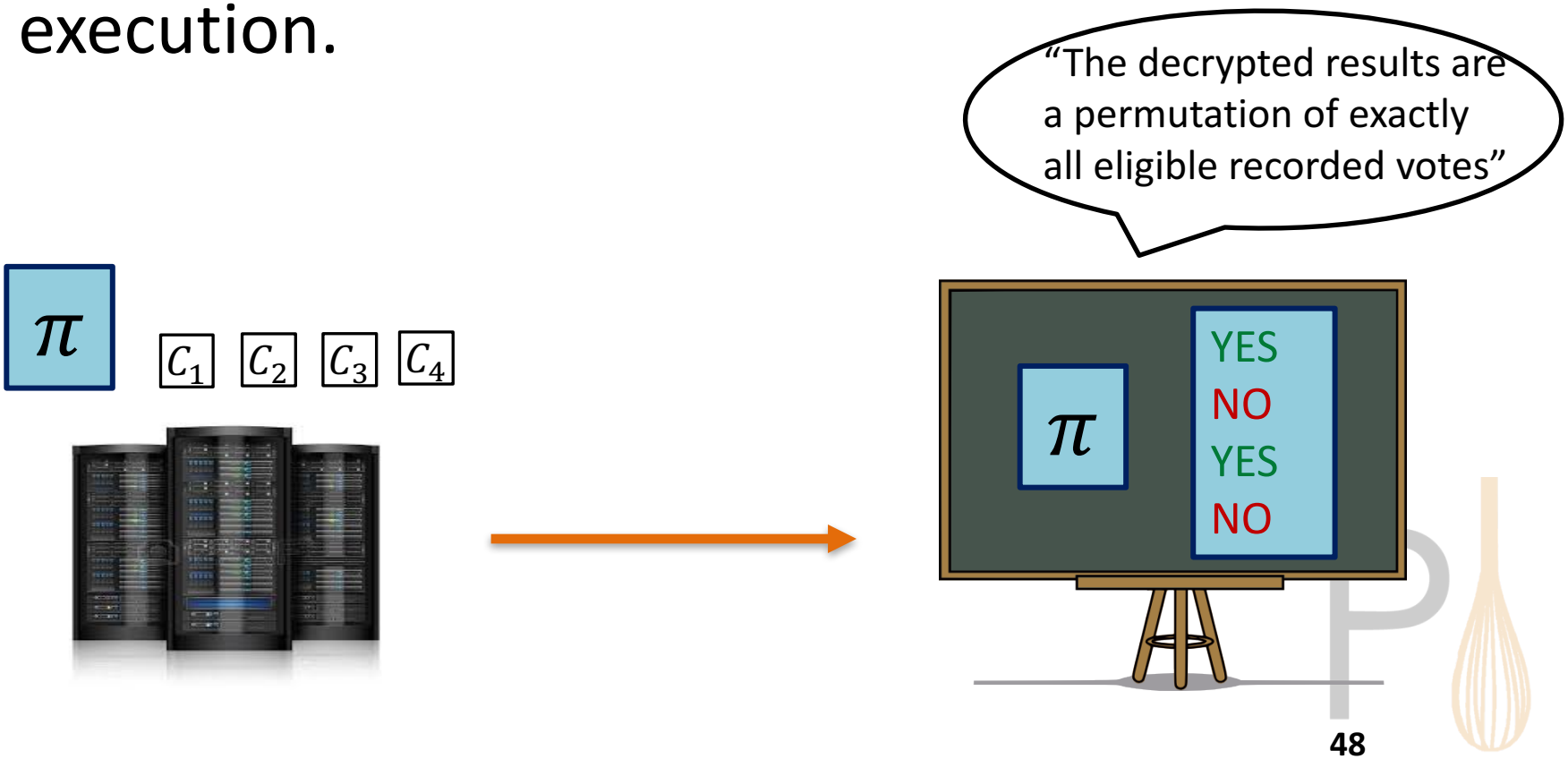
Universal Verifiability

- Every step of the election procedure is associated with a cryptographic proof of its execution.



Universal Verifiability

- Every step of the election procedure is associated with a cryptographic proof of its execution.



Universal Verifiability

- Each proof satisfies soundness (invalid statements will not be accepted) and prevents any malicious party from leaking information about the associated sensitive data (zero-knowledge proofs).
- The sequence of cryptographic proofs constitutes a verifiable election transcript that is posted in a publicly accessible web site (bulletin board) for auditing while preserving election privacy.

Individual Verifiability

- State-of-the-art e-voting systems support elaborate verification mechanism that allow the voter to challenge the correct encoding of their vote.
  1. Ballot encryption: audit the validity of the voting device by randomly checking the local cryptographic operations.
  2. Code-voting: audit the honest of the ballot preparation authorities by randomly checking the consistency of the encoding of the election options.

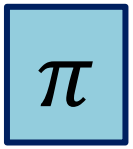
Accountability

- The e-voting system should provide a mechanism provides undeniable evidence of which entity is responsible for an incorrect execution.

Accountability example: authenticated communication

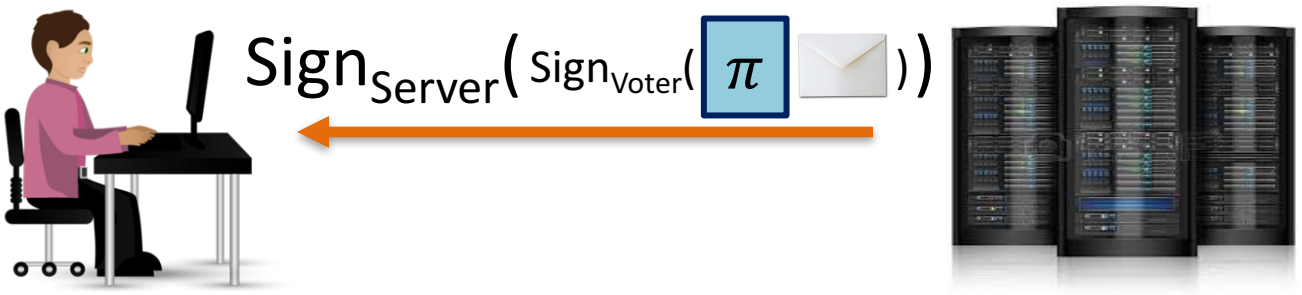
Accountability example: authenticated communication

- The voter signs her ballot.

$\text{Sign}_{\text{Voter}}($  $)$

Accountability example: authenticated communication

- The voter signs her ballot.
- The vote collection server replies with a signature on the received data.



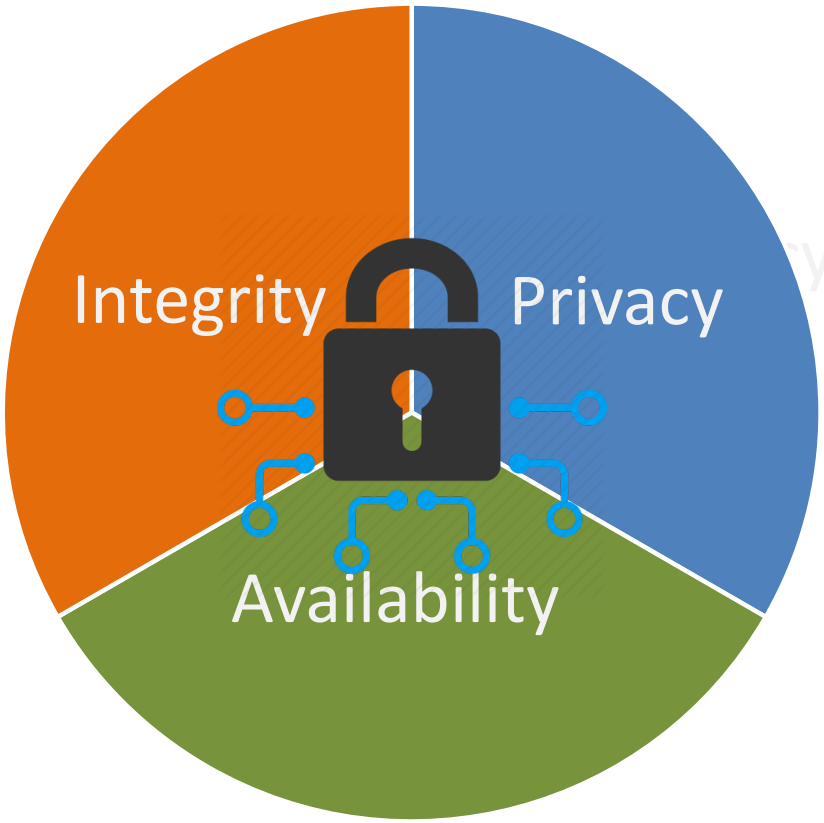
Accountability example: authenticated communication

- The voter signs her ballot.
- The vote collection server replies with a signature on the received data.
- If an authority is realized by a distributed subsystem, then malicious nodes can be blacklisted.

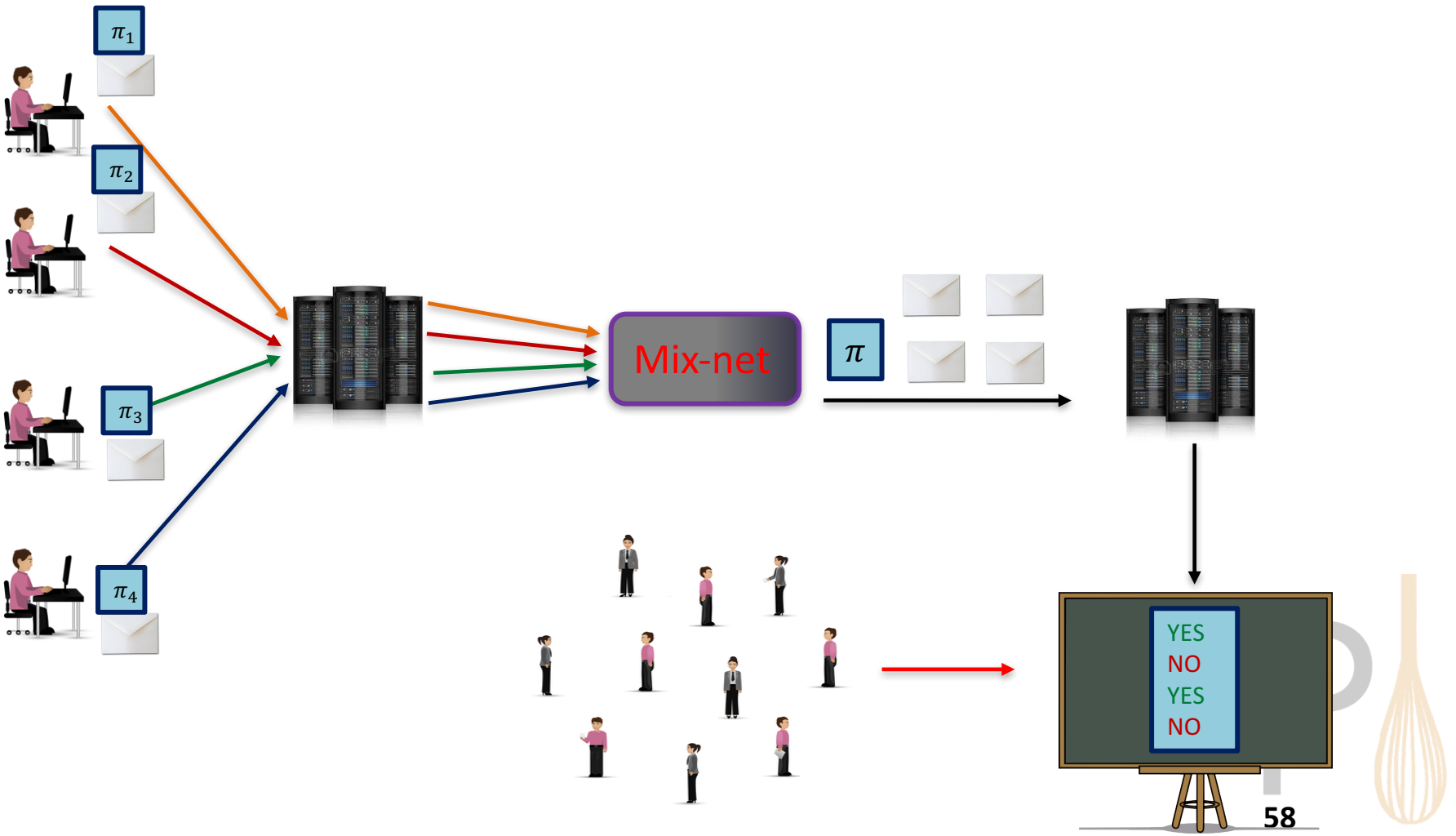
Accountability example: posting on the bulleting board

- The authorities commit to the validity of their data.
  - The election public key is posted prior to the voting period.
  - The ballot preparation authorities provide cryptographic proofs of proper encoding of the election options (Code-voting) .
  - The tallying authorities post cryptographic proofs of correct decryption and election tally.

Addressing e-voting challenges via cryptographic tools



Addressing e-voting challenges via cryptographic tools



Is crypto enough to guarantee secure e-voting?

The importance of the human factor

- Cryptographic tools provide a solid background, but do not suffice.
- Active participation of the stakeholders is crucial.
  - Verification mechanisms are meaningless if not even a small ratio of voters are willing to verify (or outsource verification to a trusted party).
  - The trustees should audit the correct publishing of the election public key to protect voters' privacy.
- A formally analysed human protocol and e-voting cryptographic design should be side-by-side.

Thank you!!!

Panoramix

Addressing the Challenges of e-Voting Through Crypto Design

Thomas Zacharias

University of Edinburgh

29 November 2017

Scotland's Democratic Future: Exploring Electronic Voting

Scottish Government and University of Edinburgh

School of Informatics Workshop