Voting with coercion resistance and everlasting privacy using linkable ring signatures

Panagiotis Grontas, Aris Pagourtzis and Marianna Spyrakou

School of Electrical and Computer Engineering
National Technical University of Athens

May 23, 2024

ATHECRYPT 2024

Table of Contents

Contents

Ideal Properties of an Electronic Voting Scheme

- Verifiability
- Privacy
- Receipt freeness
- Coercion resistance

Overview

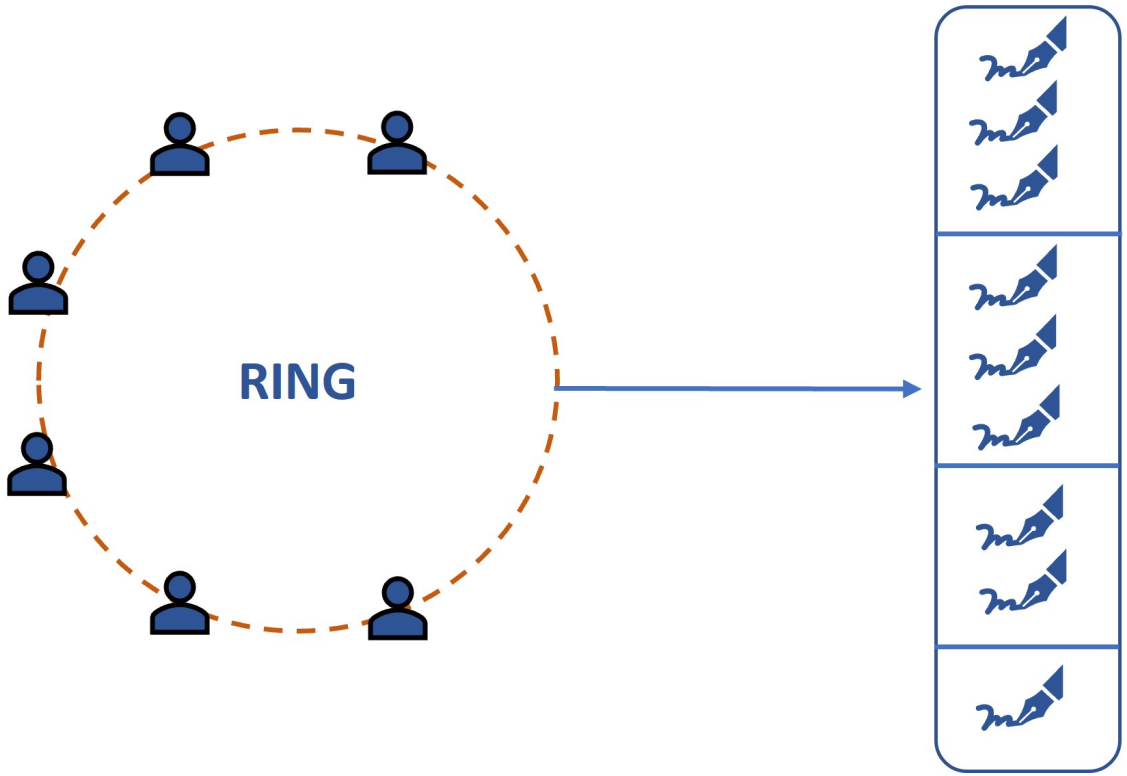
We propose a voting scheme that:

- provides **coercion resistance** ([JCJ05] framework)
- is based on **linkable ring signatures**
- provides **verifiability, ballot secrecy** and **everlasting privacy**

[JCJ05] Juels, Catalano, Jakobsson. Coercion-resistant electronic elections

Contents

Linkable Ring Signatures



- Ring Signatures [RST01]
- Linkable Ring Signatures [LWW04]

[RST01] Rivest, Shamir, Tauman. How to Leak a Secret

[LWW04] Liu, Wei, Wong. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups

Can we use linkable ring signatures in voting?

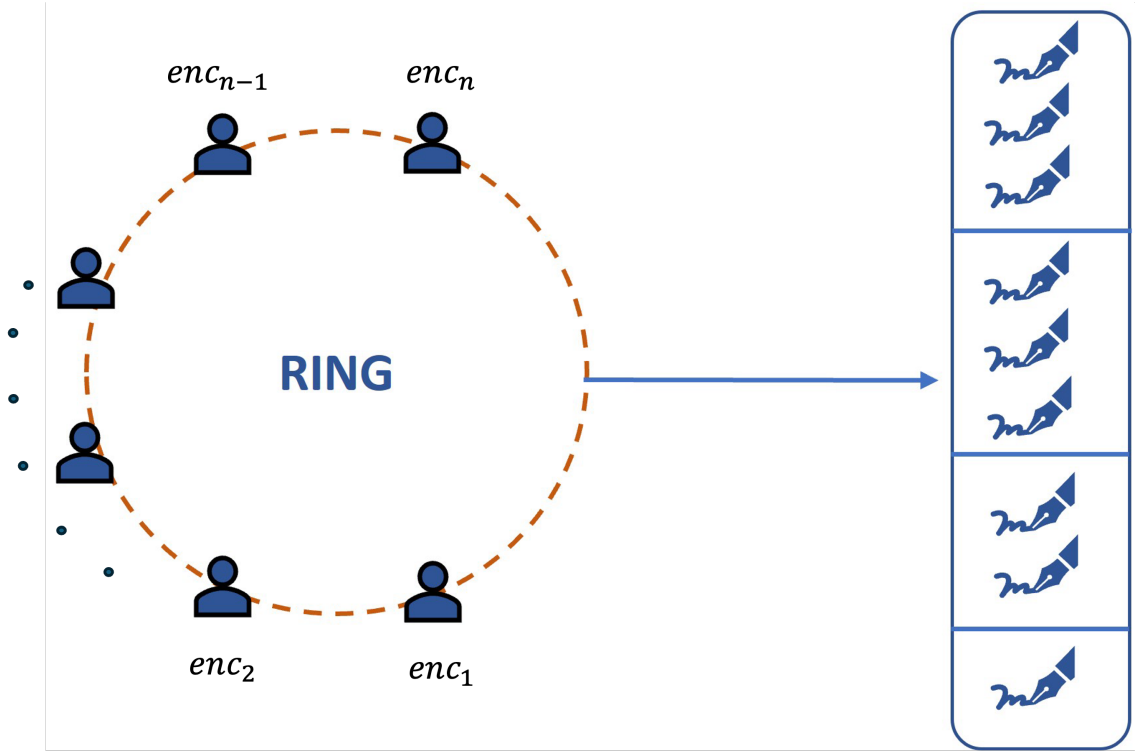
Properties achieved

- Verifiability
- Privacy
- Avoid double voting

Properties **not** achieved

- Receipt freeness
- Coercion resistance

Our LRS construction



- Signature scheme based on [LWW04], where the public credentials are encrypted values.
- Our signature is a proof of knowledge of the **secret credential** and of the **encryption randomness**.

LRS Signature

Properties

- **Unforgeability:** Noone besides the ring members is able to produce valid signatures.
- **Unconditional Anonymity:** Given a valid signature, noone can distinguish which ring member was the signer.
- **Linkability:** Two signatures from the same signer are linked.
- **Non-slanderability:** no one can create a valid signature that is linked with a given signature.

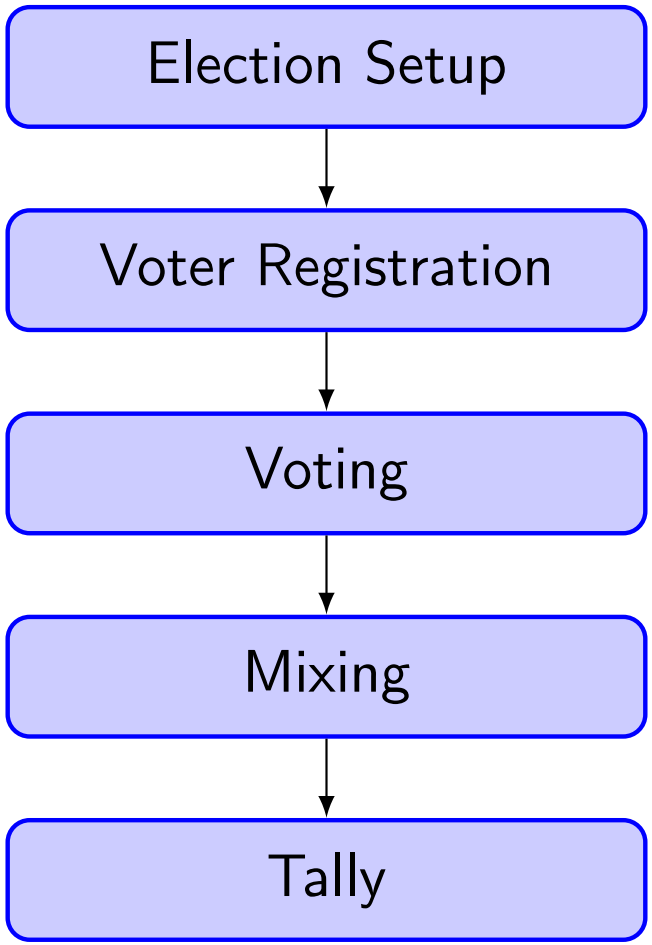
LRS Signature

Properties

- **Unforgeability** – Ensures verifiability
- **Unconditional Anonymity** – Achieves everlasting privacy
- **Linkability** – Avoids double voting
- **Non-slanderability** – Ensures that only the voter can update their vote.

Contents

Overview



Participating entities

- System supervisor

  Runs the Election Setupand publishes the public parameters required for the voting procedure to take place.

- Registration Authority (RA)
- Tallying Authority (TA)
- Voters (V)
- Bulletin Board (BB)

  Authenticated append- only ledger that contains all public election data.

Voter Registration

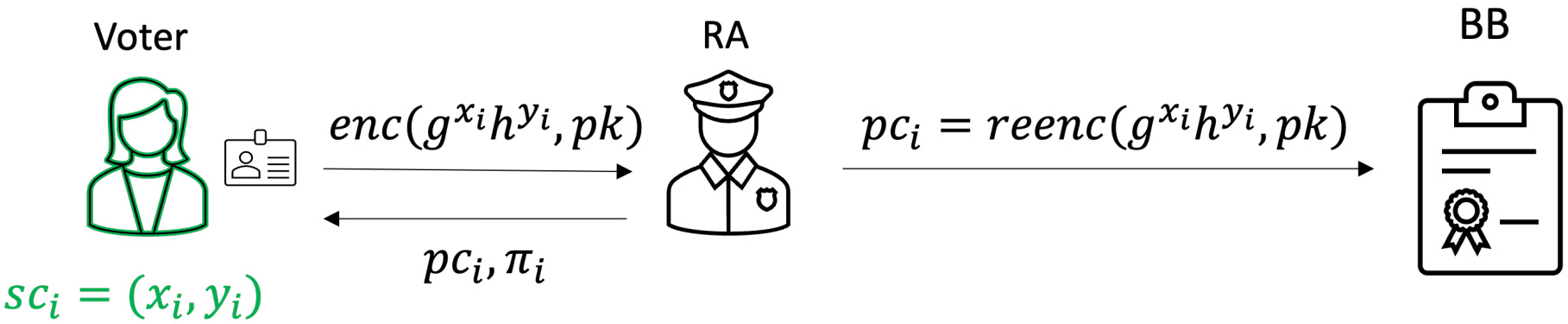


Figure 2: Registration Phase

After the registration phase

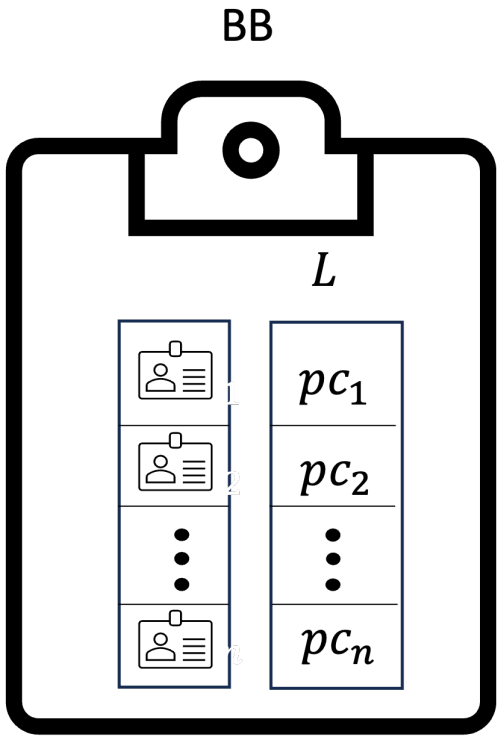


Figure 3: After the Registration phase the BB contains the list of eligible voters and a list L with their corresponding public credentials.

Voting

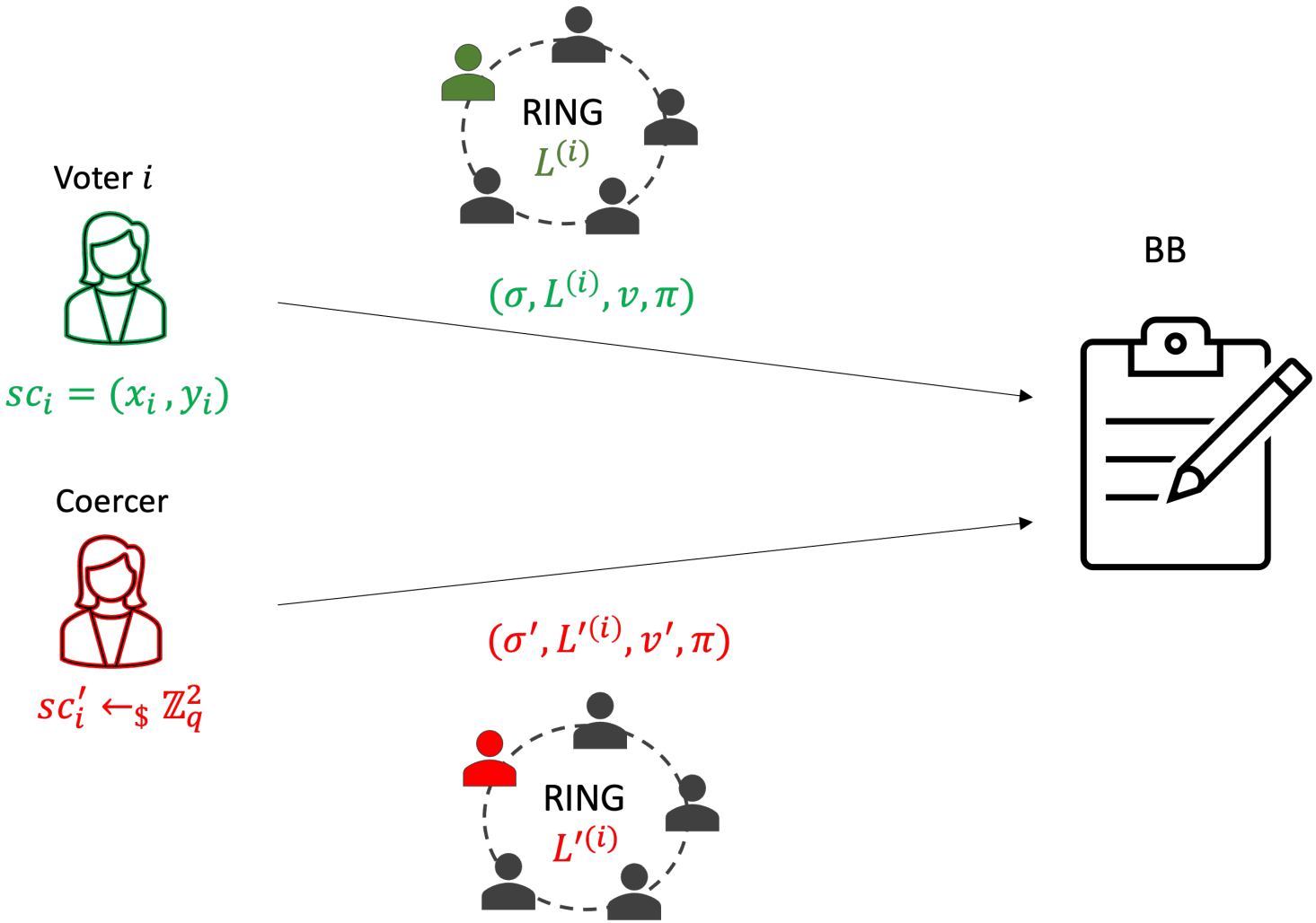


Figure 4: Voting Phase

Mixing

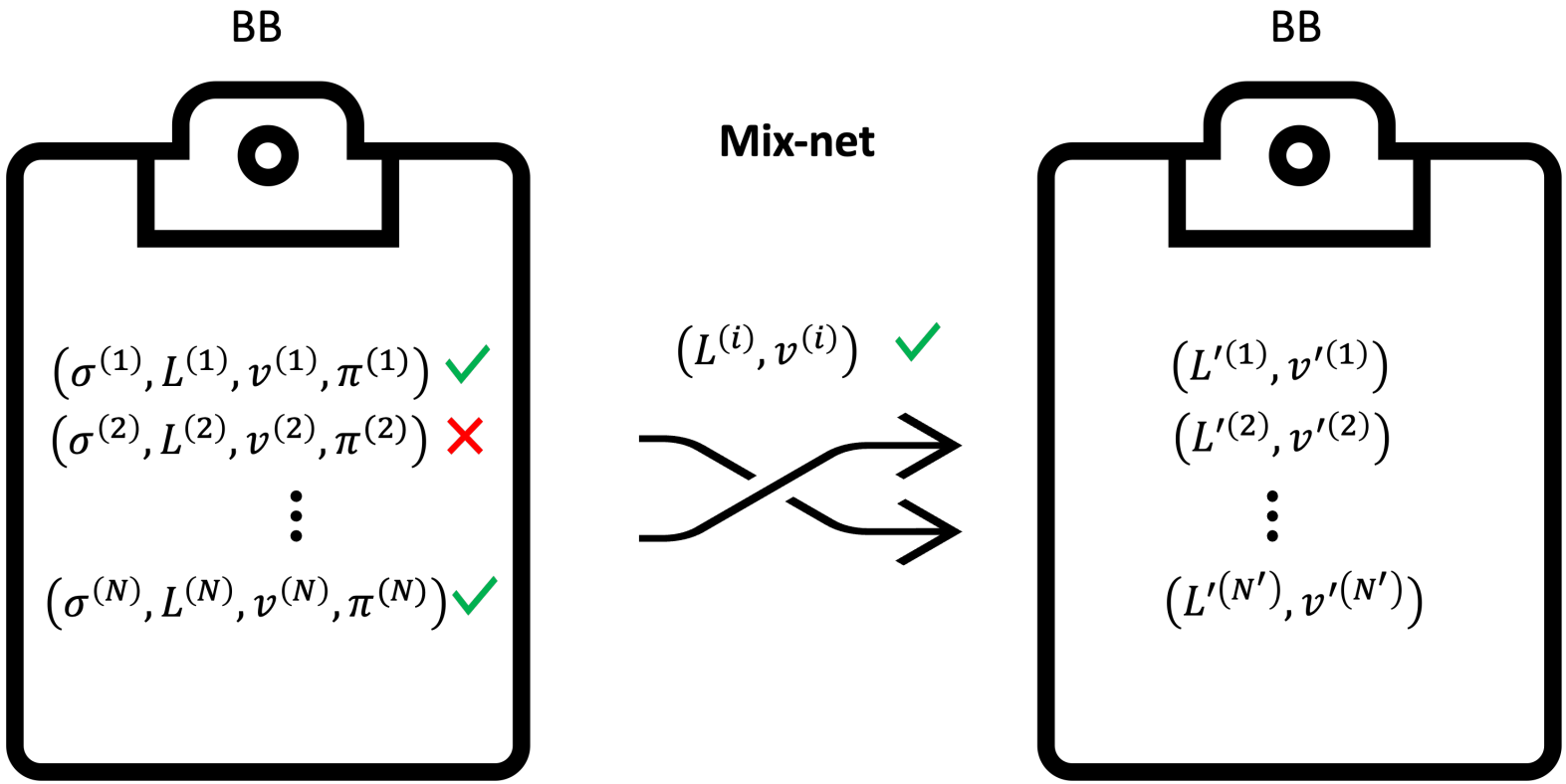


Figure 5: Mixing Phase

Tally

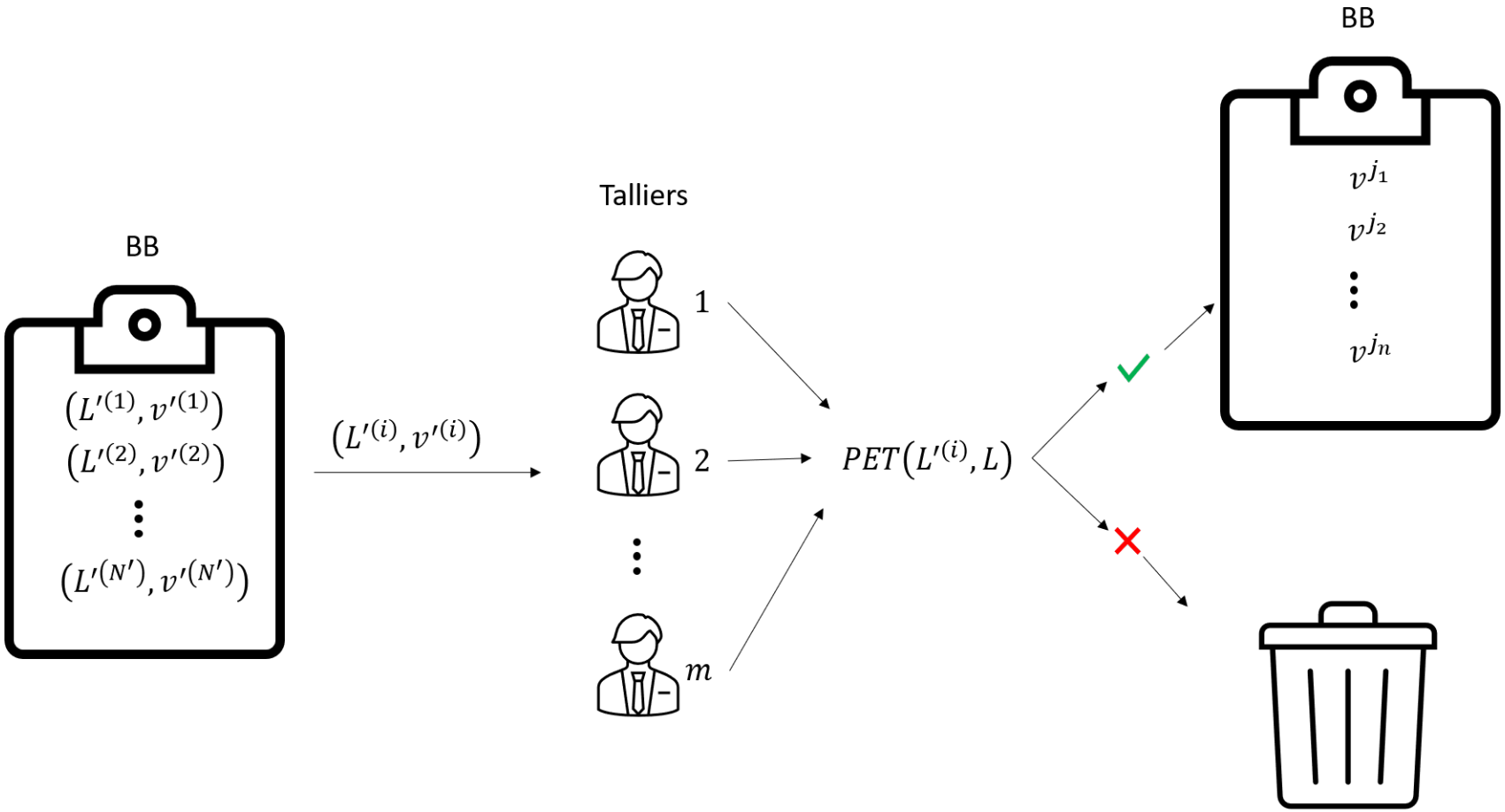


Figure 6: Tally

Security Properties

Individual & Universal **Verifiability**: Are achieved by the NIZK proofs provided by the voters, the registration and tallying authorities.

Security Properties

Individual & Universal **Verifiability**:
Are achieved by the NIZK proofs provided by the voters, the registration and tallying authorities.

Coercion Resistance:
The coercer doesn't know if their attack succeeded. It is indistinguishable whether the credential given was real or fake.

Security Properties

Individual & Universal **Verifiability**:
Are achieved by the NIZK proofs provided by the voters, the registration and tallying authorities.

Coercion Resistance:
The coercer doesn't know if their attack succeeded. It is indistinguishable whether the credential given was real or fake.

Ballot Secrecy:
is achieved by the anonymity of the ring signature, the encryption of the candidate preference and the distributed tally mechanism.

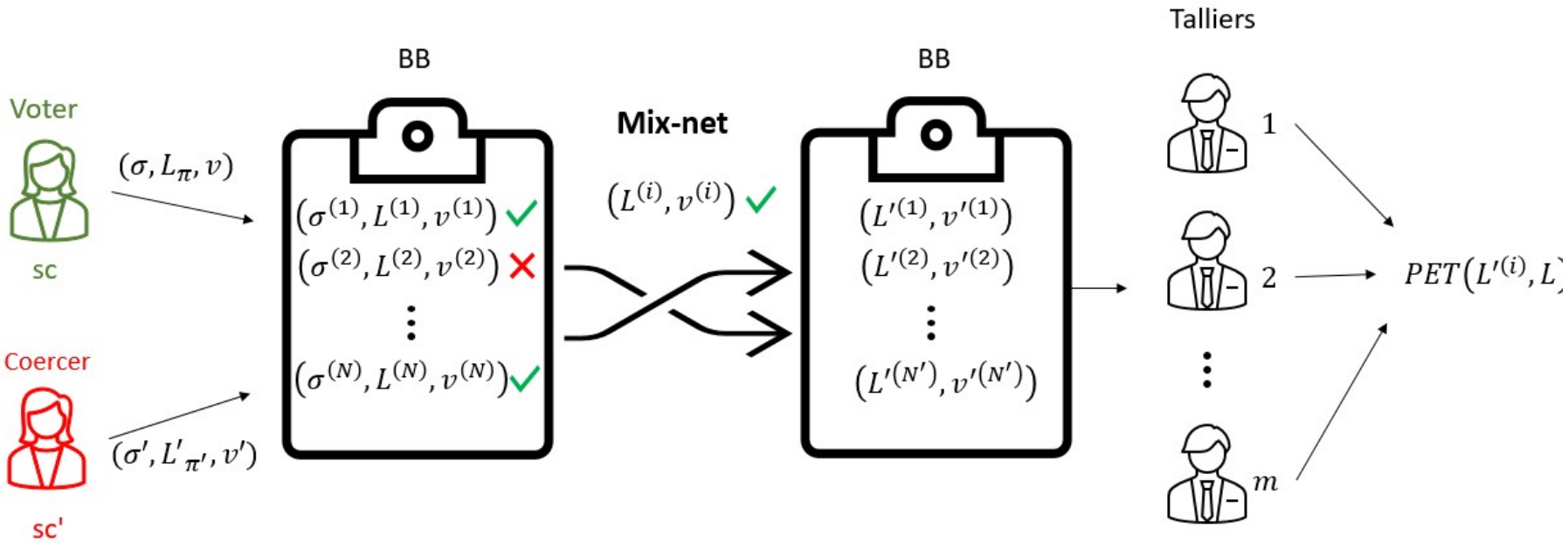
Security Properties

Individual & Universal **Verifiability**:
Are achieved by the NIZK proofs provided by the voters, the registration and tallying authorities.

Coercion Resistance:
The coercer doesn't know if their attack succeeded. It is indistinguishable whether the credential given was real or fake.

Ballot Secrecy:
is achieved by the anonymity of the ring signature, the encryption of the candidate preference and the distributed tally mechanism.

Everlasting Privacy:
is achieved by the unconditional anonymity property of our LRS.


Voter
sc
Coercer
sc'
(σ, L_π, v)
$(\sigma', L'_{\pi'}, v')$
BB
$(\sigma^{(1)}, L^{(1)}, v^{(1)})$
$(\sigma^{(2)}, L^{(2)}, v^{(2)})$
$(\sigma^{(N)}, L^{(N)}, v^{(N)})$
Mix-net
$(L^{(i)}, v^{(i)})$
BB
$(L'^{(1)}, v'^{(1)})$
$(L'^{(2)}, v'^{(2)})$
$(L'^{(N')}, v'^{(N')})$
Talliers
1
2
m
$PET(L'^{(i)}, L$


Thank you!