

A PKI-based protocol for secure and practical online elections



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Lucie Langer, Axel Schmidt, Melanie Volkamer, Johannes Buchmann

Project *voteremote*



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Bundesministerium
für Wirtschaft
und Technologie



TECHNISCHE
UNIVERSITÄT
DARMSTADT

T · · · Systems · · ·

U N I K A S S E L
V E R S I T Ä T

PTB Physikalisch
Technische
Bundesanstalt
Braunschweig und Berlin

Security requirements



TECHNISCHE
UNIVERSITÄT
DARMSTADT

- Secrecy
 - Democracy
 - Accuracy
 - Fairness
 - Verifiability
-
- Receipt-freeness
 - Coercion-resistance

Additional requirements



TECHNISCHE
UNIVERSITÄT
DARMSTADT

- Scalability
- Robustness
- Usability
- ...

Security vs. usability



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Our goals and assumptions



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Goals:

- Meet basic security requirements
- Standard primitives
- Efficient implementation
- No “untappable channels”

Assumptions:

- Non-political elections
- Low-coercion scenario
- Reasonable adversary

Building blocks



TECHNISCHE
UNIVERSITÄT
DARMSTADT

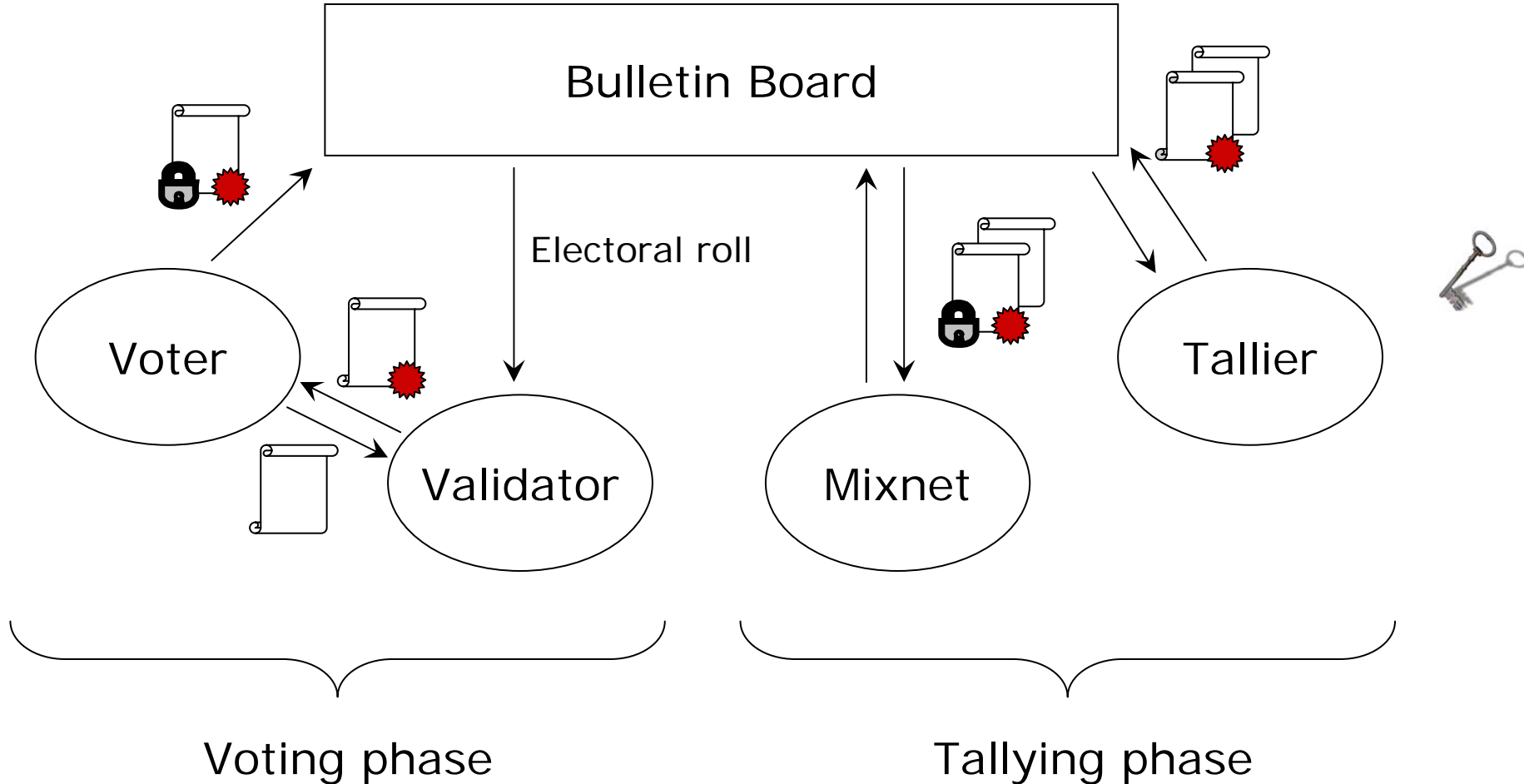
- Secure communication via TLS/SSL
- Trusted PKI
- Blind signatures
- Mixnet
- Bulletin Board

Players



- Voters
- Validator (trusted)
- Mixnet (trusted / verifiable)
- Bulletin Board (trusted)
- Tallier (verifiable)

Voting scheme



Analysis (1/2)



- Secrecy ✓
- Democracy ✓
- Accuracy ✓
- Fairness ✓

- Verifiability ?
- Receipt-freeness ?

- Coercion-resistance ⚡

Analysis (2/2)

- Probabilistic signatures: 

Individual verifiability 

Receipt-freeness 

- Deterministic signatures: 

Individual verifiability 

Receipt-freeness 

Consequences



- Basic security requirements met
- More complex primitives needed
 - to reconcile receipt-freeness and individual verifiability
 - to achieve coercion-resistance



Thank you!