Coercion-Resistant Electronic Elections with Observer

Jörn Schweisgut

University of Giessen

Germany

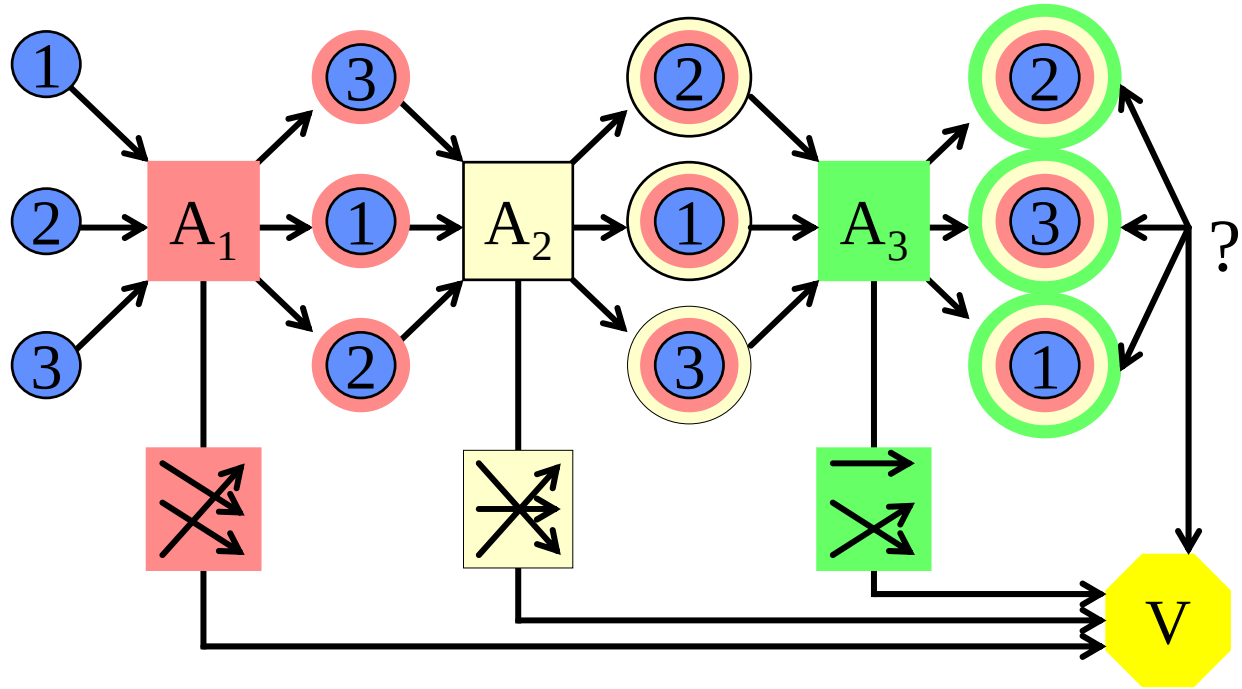
email: Joern.Schweisgut@math.uni-giessen.de

Overview

- **Hirt and Sako's Voting Scheme [HS00]**
- ***Observer:* A Tamper-Resistant Hardware Device**
- **Receipt-Free Electronic Voting with Observer**
- **Coercion-Resistance [JCJ05]**
- **Efficient Receipt-Free Electronic Voting with Observer [Sch06a]**
- **Coercion-Resistant Observer-based Electronic Voting [Sch06b]**
- **Use of an Observer – advantages**

© J. Schweisgut

Hirt and Sako's voting scheme [HS00]



Example with three candidates {1,2,3} and three authorities A_i

© J. Schweisgut

Observer: A Tamper-Resistant Hardware Device

Disadvantages of [HS00]

- requires a physically secure channel from each authority to each voter (impossible to achieve by encryption)
- not very efficient: designated-verifier and witness-indistinguishable proofs of correct permutation and re-encryption must be performed by each authority

Solution:

- an "**observer**" – a tamper-resistant hardware device in possession of the voter

© J. Schweisgut

Receipt-Free Electronic Voting with Observer

[Sch05]

- observer generates randomness and encrypts all candidate choices
- ciphertexts and designated-verifier proof are sent to the voter
- voter re-encrypts his choice and lets the observer digitally sign

receipt-free, *but* …

© J. Schweisgut

Coercion-Resistant Electronic Voting

The voter can be forced

a) to cast his vote randomly (**randomisation attack**)

b) to enable the coercer to vote instead of the voter (**impersonation attack**)

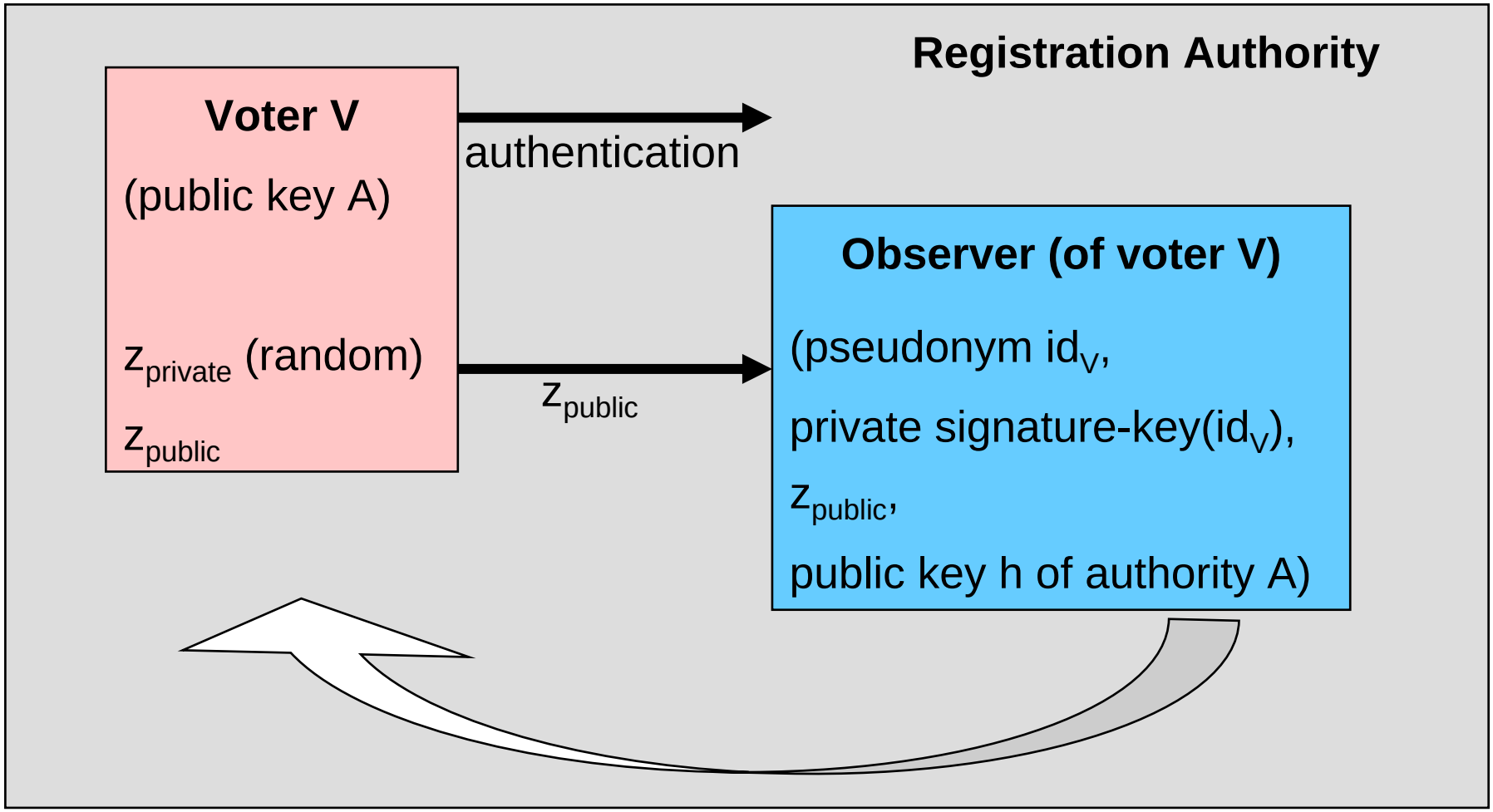
c) to refrain from voting (**abstention attack**)

[JCJ05]

- new notion of security: **coercion-resistance**

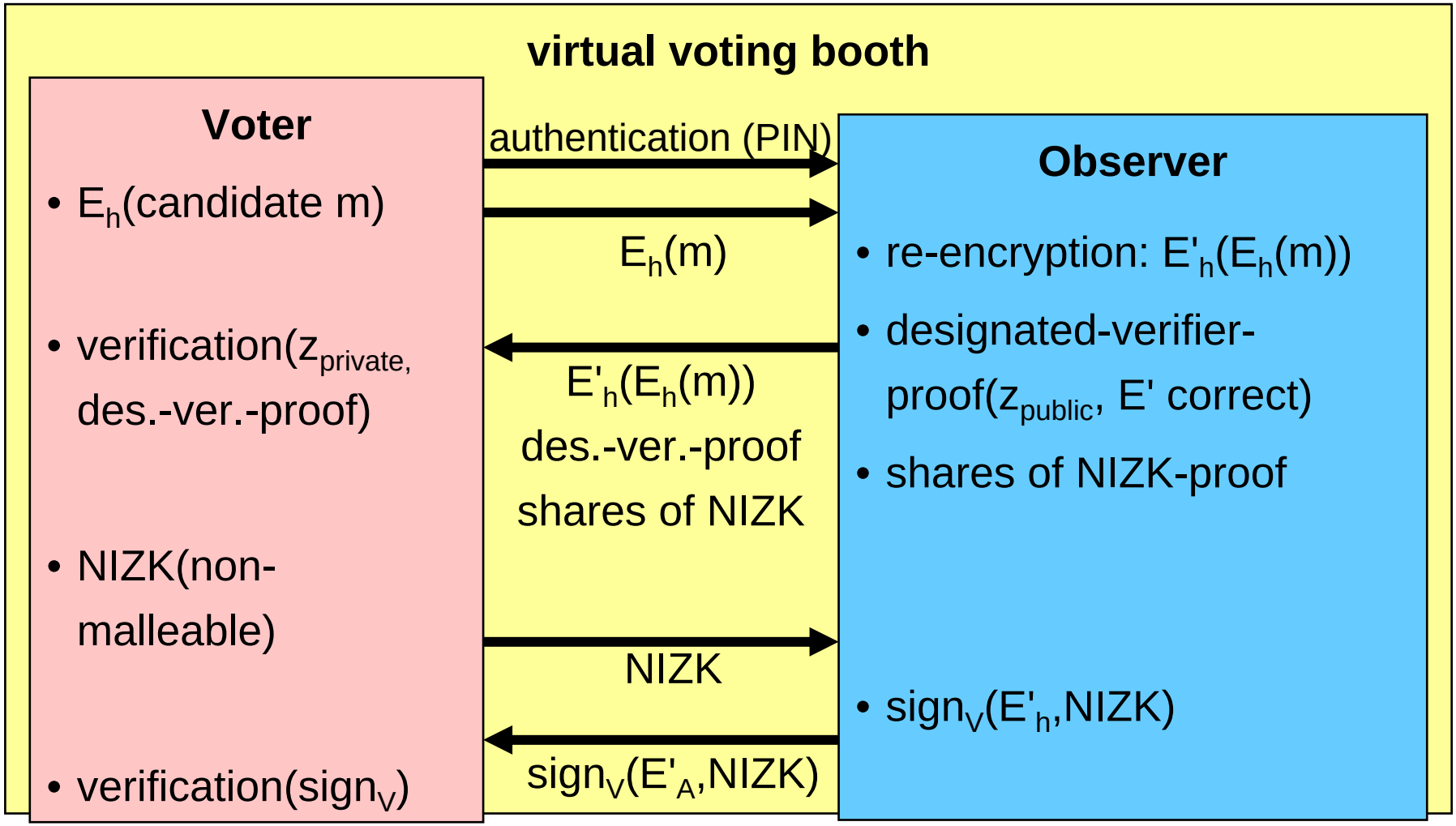
© J. Schweisgut

[Sch06a] - Registration



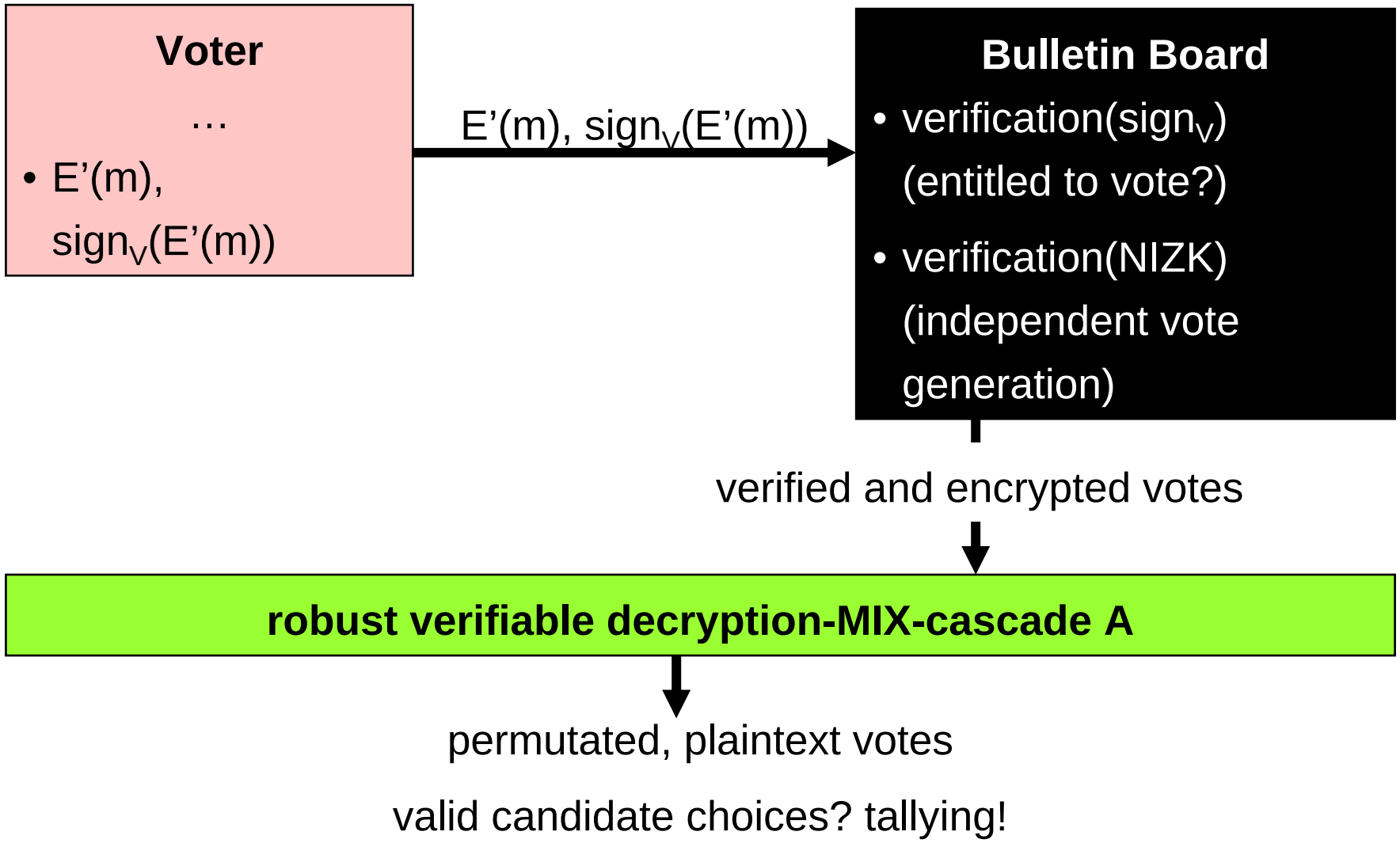
© J. Schweisgut

Voting-phase (Overview)



© J. Schweisgut

Voting-phase, Tallying



© J. Schweisgut

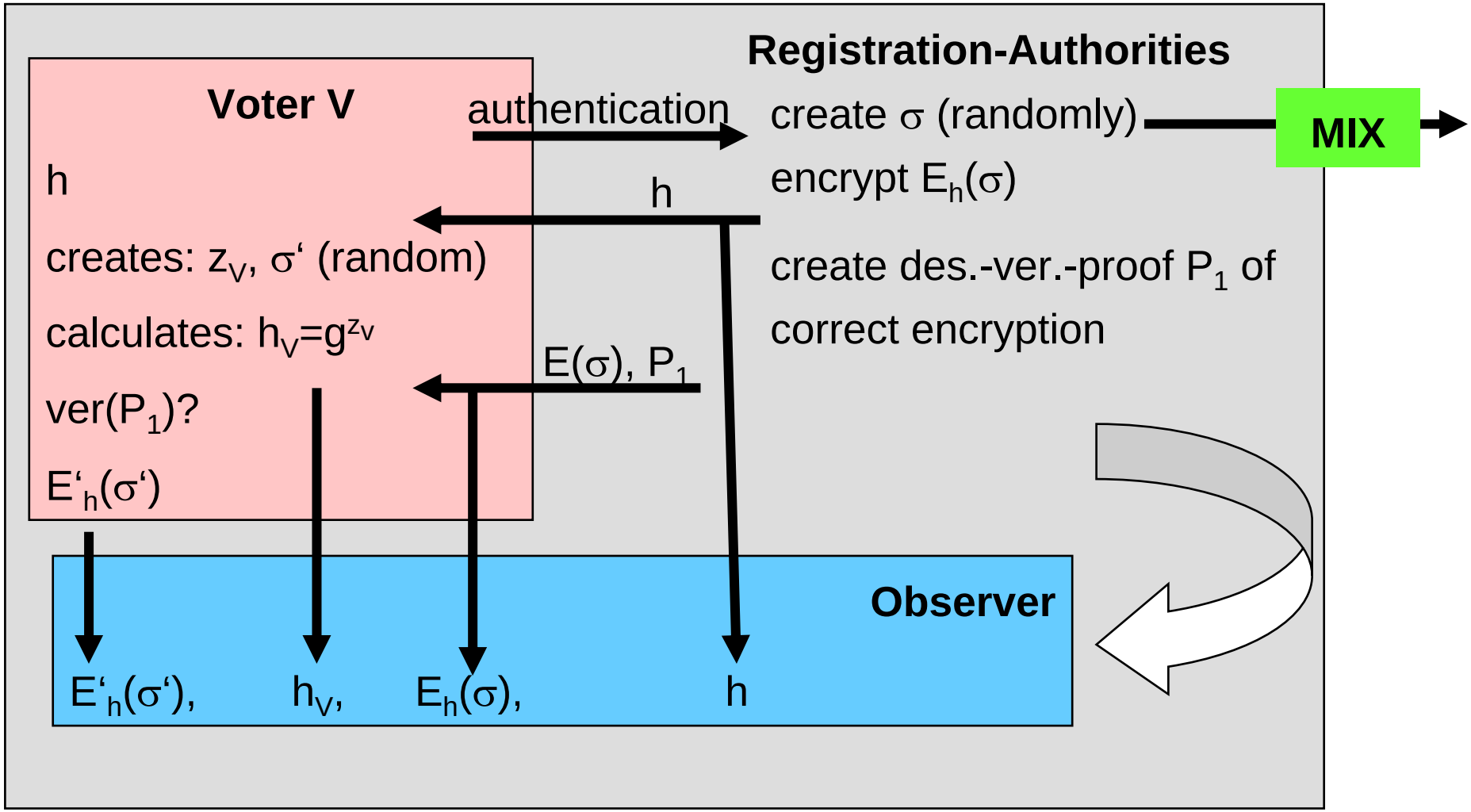
Coercion-resistance?

- receipt-free (if there are no write-in ballots)
- secure against randomisation-attack
- secure against impersonation-attack:

  PINs for observer
  - correct PIN → correct ballot generation
  - any other ‘PIN’ with spurious des.-ver. secret $z_{private}$ → false ballot generation and forged des.-ver.-proof
- abstention attack: possible

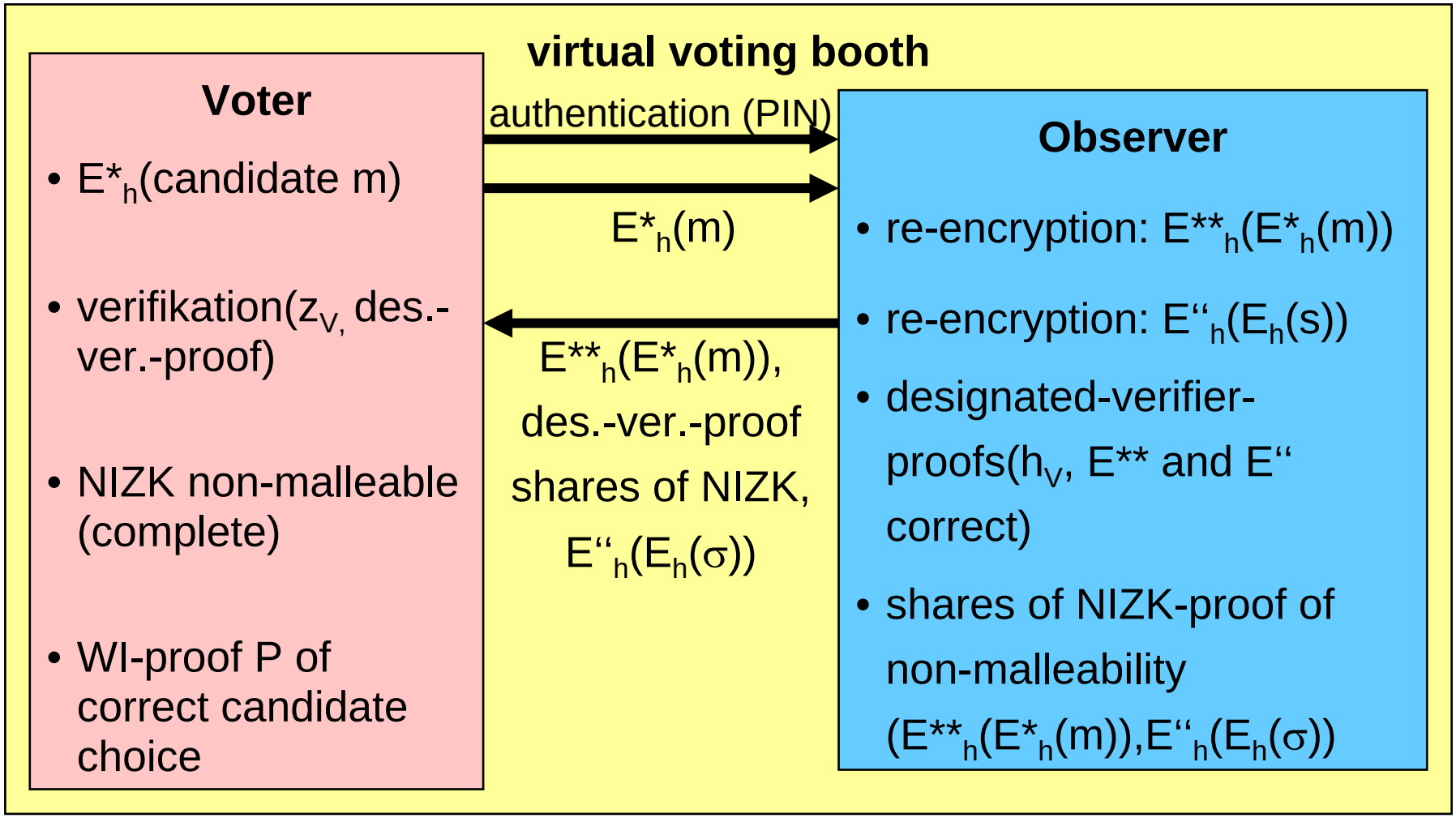
© J. Schweisgut

[Sch06b] - Registration



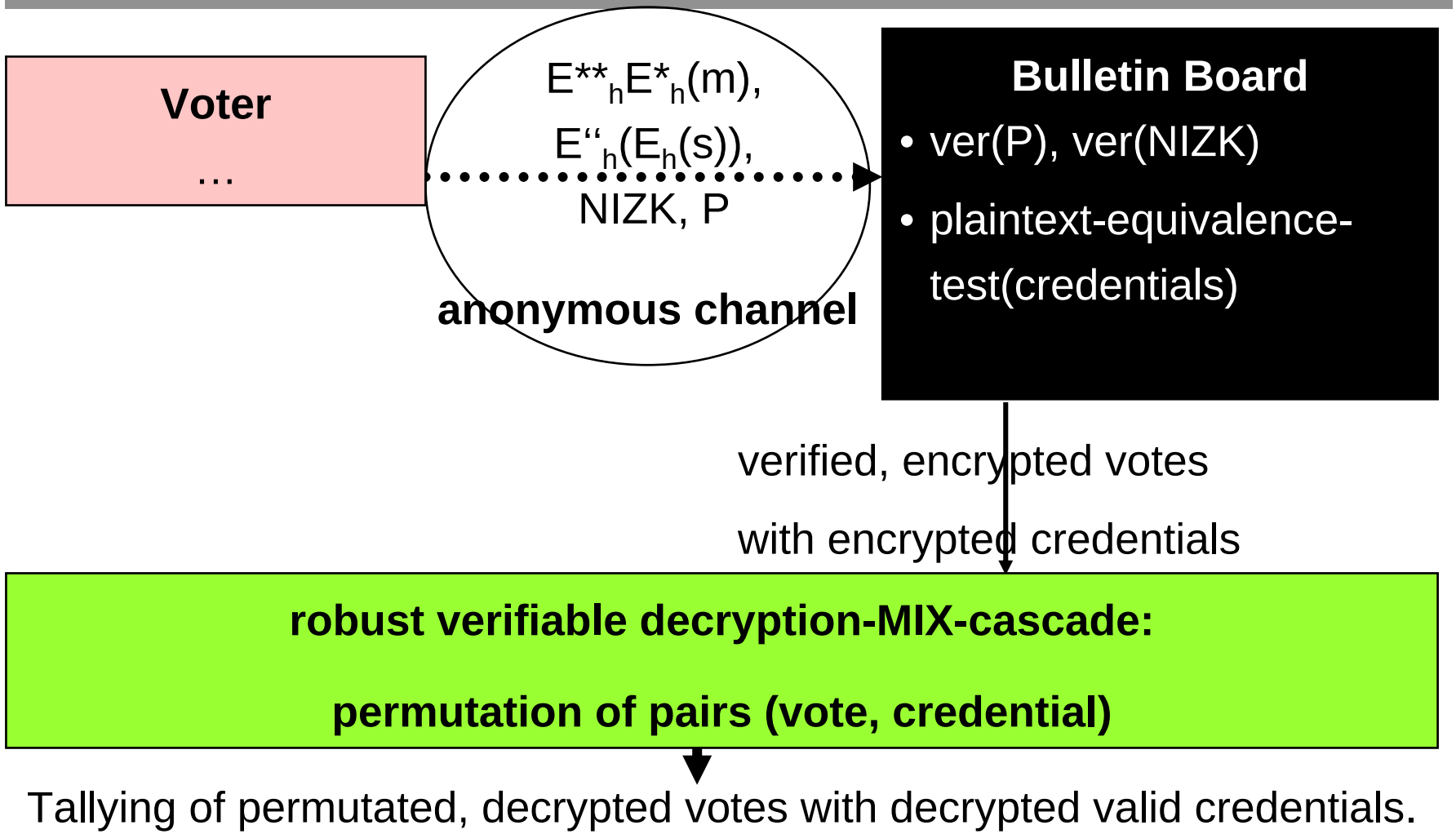
© J. Schweisgut

Voting-phase (Overview)



© J. Schweisgut

Voting-phase, Tallying



© J. Schweisgut

Properties

- no unrealistic assumptions (like a physically secure channel)
- receipt-free
- independent vote generation (non-malleability)
- coercion-resistance (no randomisation-attack, no impersonation-attack, no abstention-attack)
- permanent secrecy of votes if
  - voter does not give away his correct credential prior to the tallying
  - anonymous channel is not only secured by computational secure encryption but also by organisational arrangements (public voting booths)

© J. Schweisgut

Use of an Observer – advantages

- different approach to a coercion-resistant voting-scheme
- no unrealistic assumptions (like a physically secure channel)
- permits permanent secrecy of votes
- efficient receipt-free, but not coercion-resistant voting [Sch06a]

© J. Schweisgut

Literature

- **[JCJ05]** **A. Juels, D. Catalano, M. Jakobsson. *Coercion-Resistant Electronic Elections*. WPES '05**
- **[Sch05]** **J. Schweisgut. *Elektronische Wahlen mit Observer*. GI-Kryptotag September 2005, Darmstadt.**
- **[Sch06a]** **J. Schweisgut. *Effiziente Elektronische Wahlen mit Observer*. GI Sicherheit 2006, Magdeburg.**
- **[Sch06b]** **J. Schweisgut. *Coercion-Resistant Electronic Elections with Observer*. 2nd International Workshop on Electronic Voting 2006, Bregenz.**

© J. Schweisgut