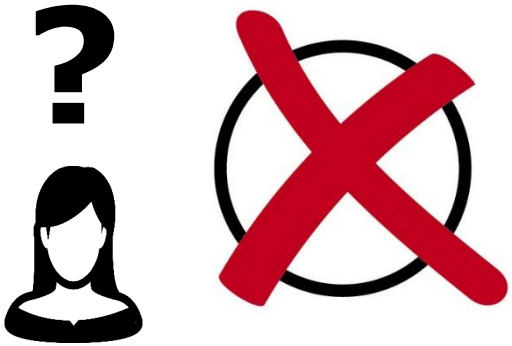
Usability of End-to-End Verifiable E-Voting Schemes

Karola Marky

TECHNISCHE UNIVERSITÄT DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

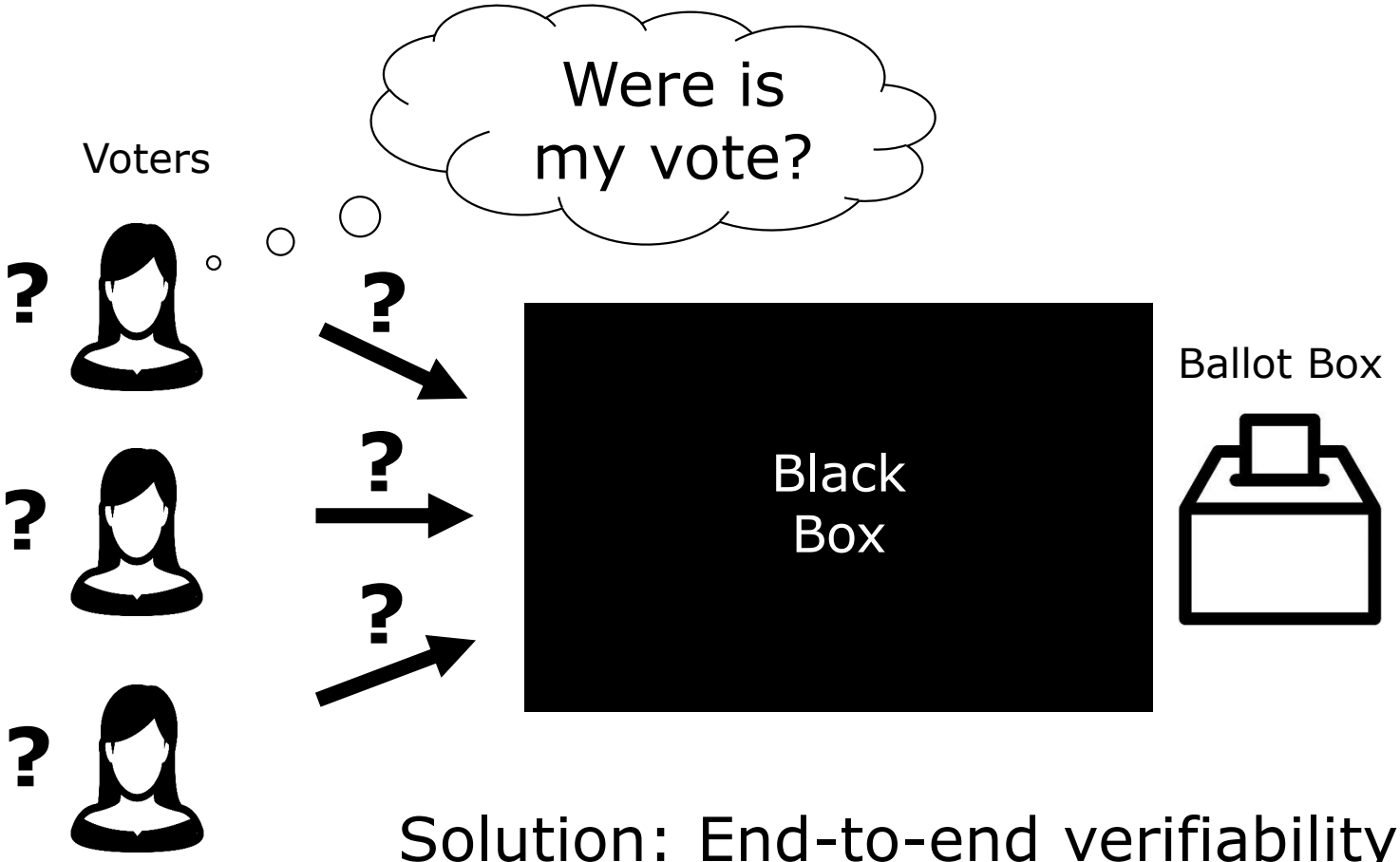
CRISP
Center for Research in Security and Privacy



SECUSO

- Security, Usability und Society
- Research group at TU Darmstadt
- Human Centered Security
- Interdisciplinary team

Motivation



Solution: End-to-end verifiability

End-to-end Verifiability

- Cast-as-intended

  Cast vote corresponds to the voter‘s intent

- Recorded-as-cast

  Recorded vote matches the cast vote

- Tallied-as-recorded

  All recorded votes are correctly included in the result

Cast-as-intended Verifiability (C-a-I)

- „Decryption“
  - E.g. Estonian system
- Challenge or cast
  - E.g. Benaloh Challenge
- Return Codes
  - E.g. Pretty Good Privacy
- Tracking Codes
  - E.g. Selene

Impact of Usability

- Attacker alters vote in secret
- Voting platform alters vote in secret
- Voting platform might malfunction

- Bad usability of C-a-I leads to
  - More successful attacks
  - Inaccurate election results

Usability (ISO 9241-11)

- Effectiveness

  Ability of users to complete their task.

- Efficiency

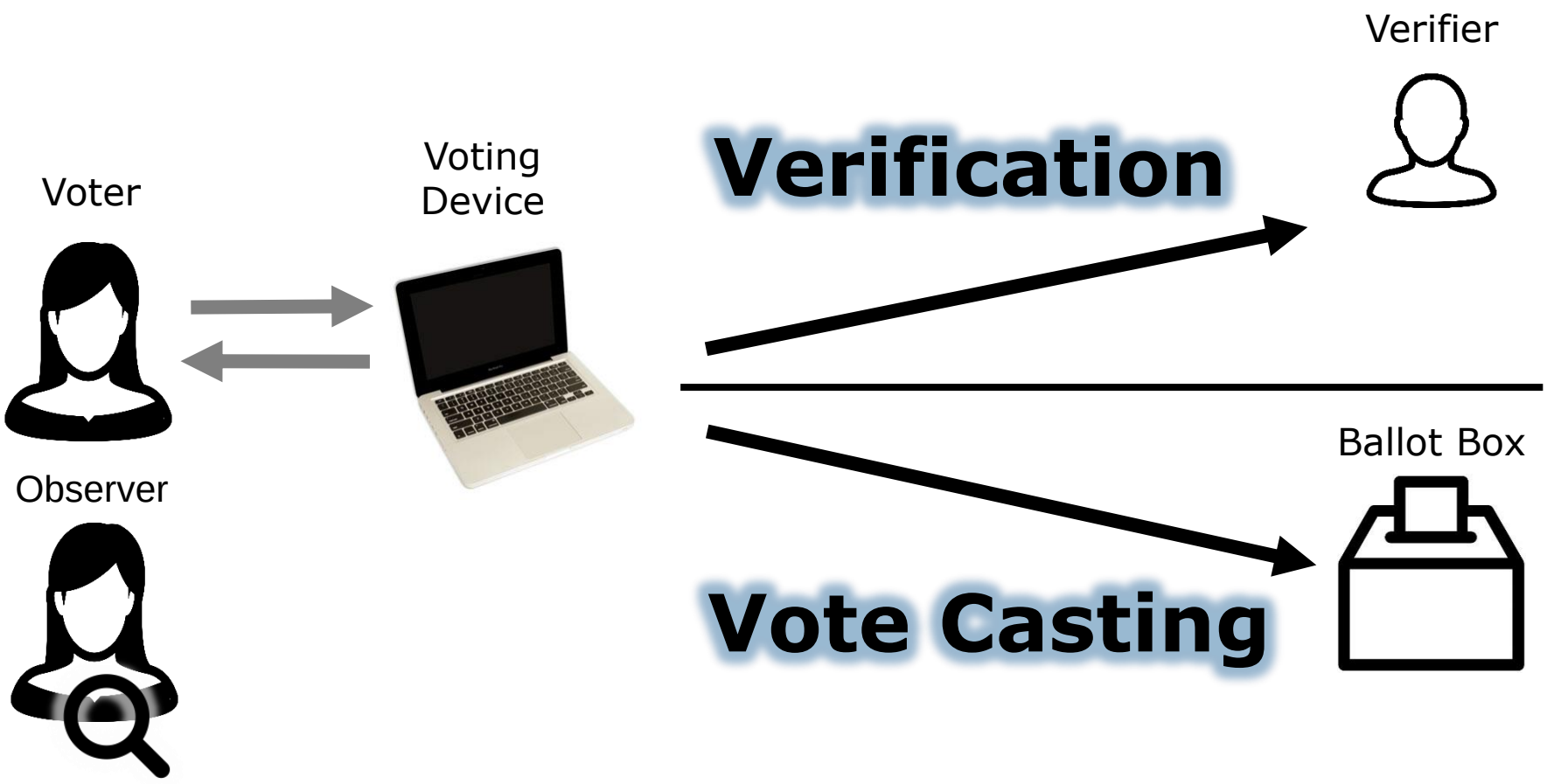
  Extent to which users consume resources to perform their task.

- Satisfaction

  Level of satisfaction users experience in performing their task.

Benaloh Challenge
User Study

Benaloh Challenge



3 Approaches

- Differences in the transfer of verification data
- Differences in the degree of voter involvement

Manual (Copy and Paste)

Automatic

Mobile (Scan of QR code)

Study Scenario

- German Federal Election 2017

3 Voting Websites

- Verifier
  - BSI
  - OSCE

Demo-Session
After workshop

- Verification devices
  - Android App

Study Design

- Lab study: 95 participants
- Between subjects
- Lab devices
- First-time voters: 17-22 years old

Procedure

- Explanation of the study
- Declaration of consent

Procedure

- Demographic questions:
  - Age
  - Gender
  - Occupation
  - Voting experience

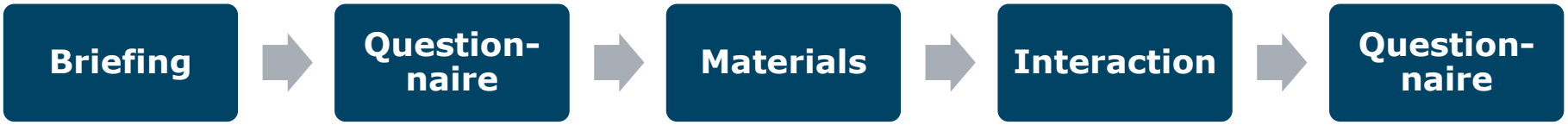
Procedure

- Internet voting document incl. login data
- Instructions
  - Mark party „SPD“
  - Verify vote using website / app
  - Mark party „GRÜNE“
  - Cast vote

Procedure

- Screenrecording of devices
- Logging of time by software
- Observation

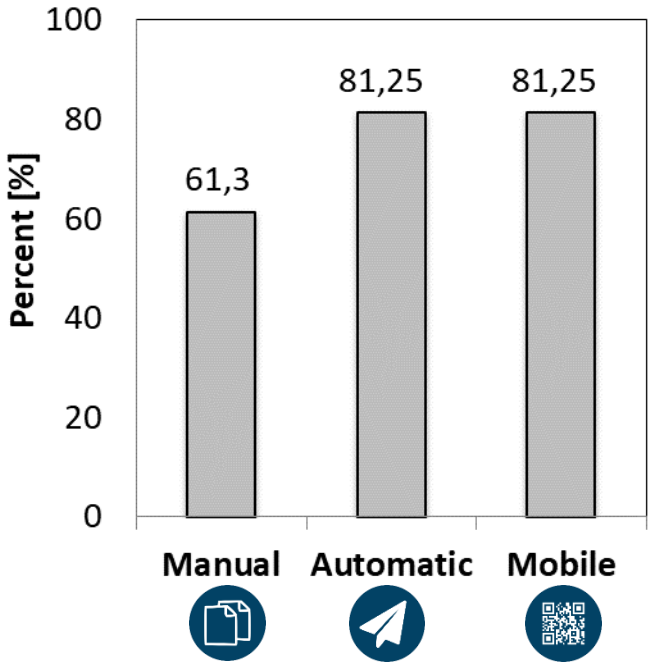
Procedure



- SUS questionnaire
- Additional questions

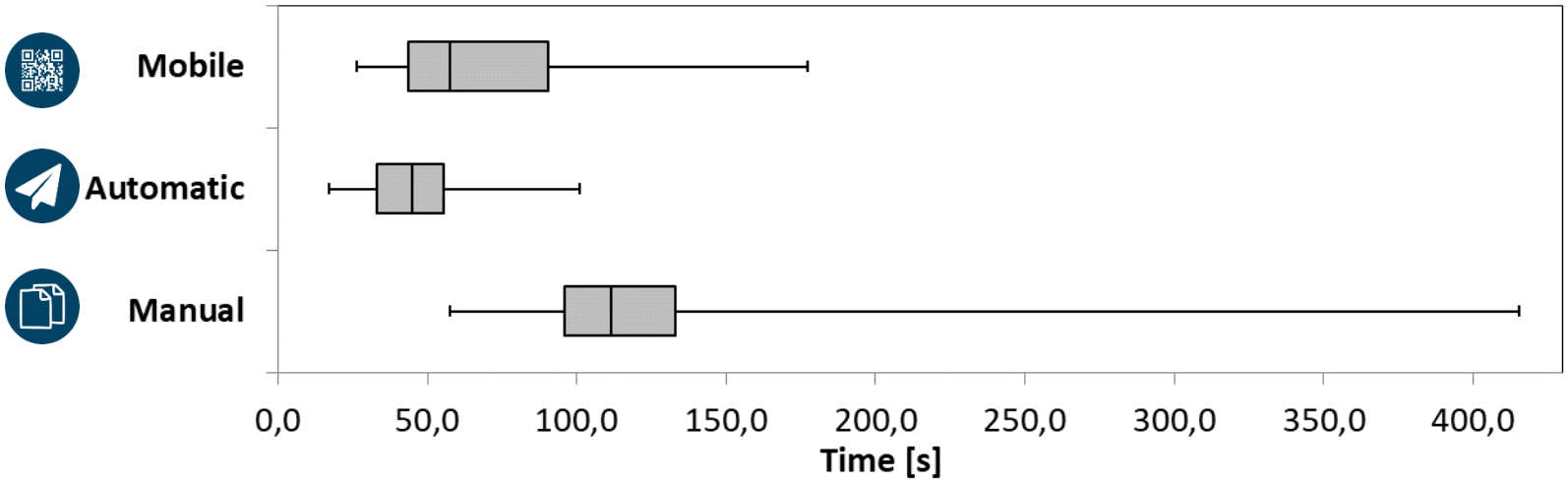
Collected Data: Effectiveness

- Completion rate
  - Share of subjects that verified successfully
- Determined by screenrecordings



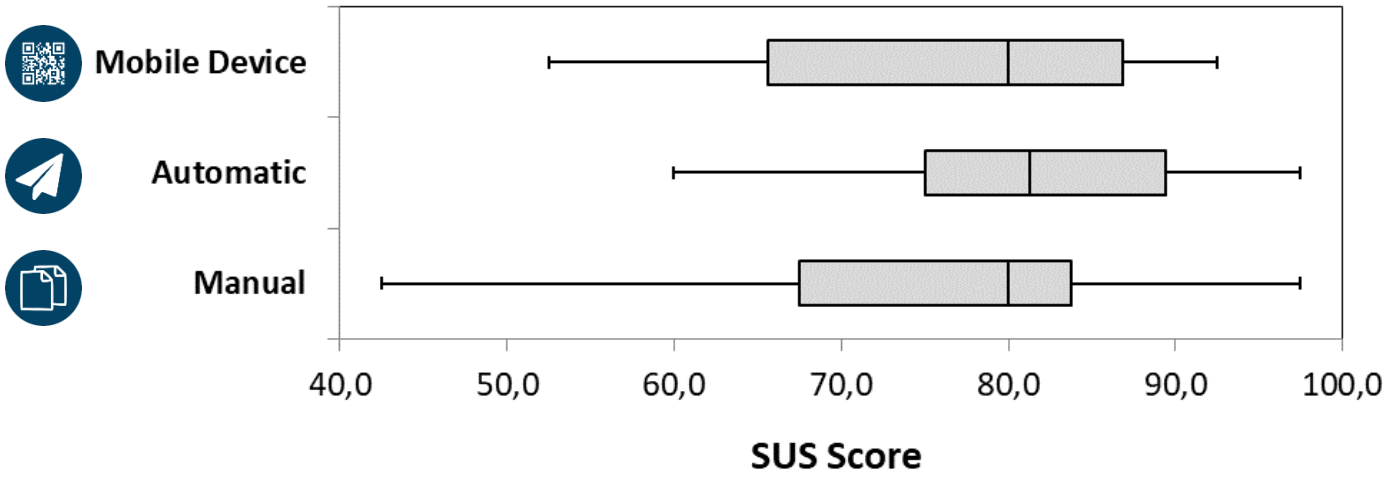
Collected Data: Efficiency

- Completion times:
  - Duration of the first successful verification
  - Logs by the software
  - Screenrecordings



Collected Data: Satisfaction

- System Usability Scale
  - 10 item questionnaire
  - SUS score from 0 up to 100



Collected Data: Additional

- Would you use the presented Internet voting system in a real Bundestag election?
- Would you use the presented verification option in a real Bundestag election?
- If you answered the question above affirmatively, how often would you perform verification?
- Did you experience any problems during vote verification?
- Did you experience any problems during vote casting?

Study Results

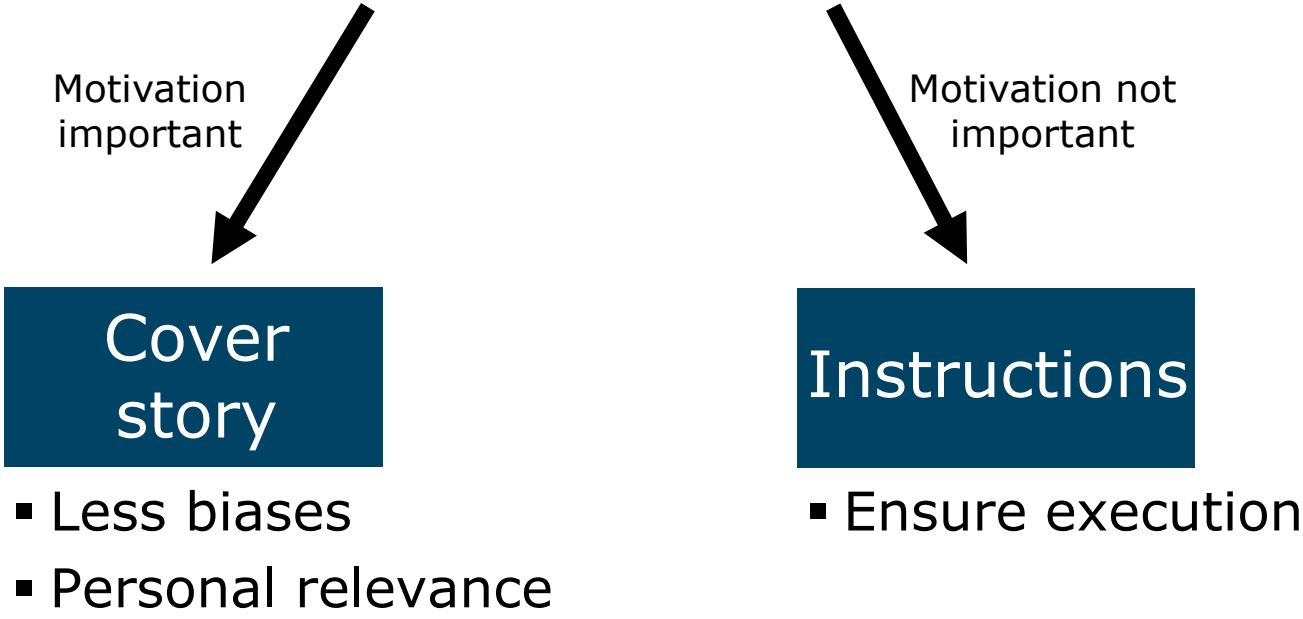
			
Ø – SUS	75,4	79,4	75,8
Completion rate	61,3 %	81,25 %	81,25 %
Ø – Time	131 s	47 s	61 s

Automatic is better than manual

Mobile is better than manual

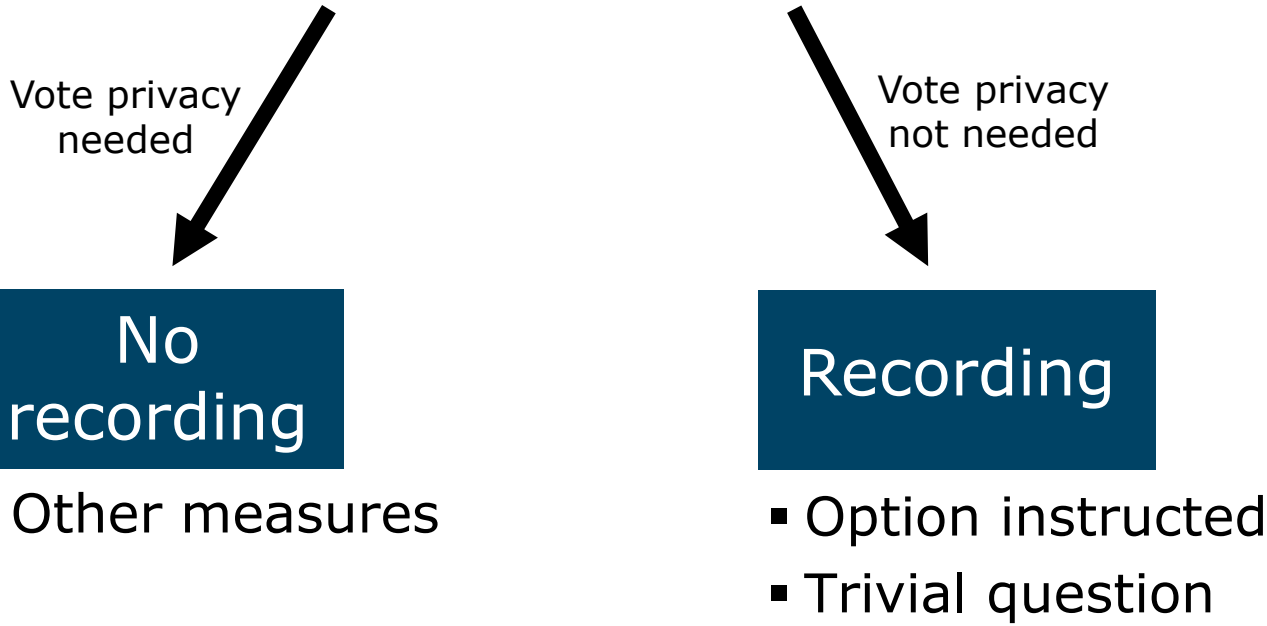
Lessons Learned – Motivation

- Participants have to be motivated to execute a task
- Usability does not include motivation



Lessons Learned – Vote Privacy

- Concerns the votes of the study participants
- Recording and observation break vote privacy



Lessons Learned - Effectiveness

- Actual comparison of data hardly detectable
  - Screenrecordings are not sufficient
  - Self reporting not reliable

Next Steps

- Long-term goal: Further research on c-a-i usability
- Next step: Evaluation of code voting vs. Benaloh
- Next-next step: Evaluation of other c-a-i approaches
  - Literature search for cast-as-intended approaches
  - Overview of available approaches
  - Classification of approaches

Discussion

- Mixing of understandability and usability
  - How can those concepts be seperated?
- Measuring of effectiveness
  - Are there other approaches to completion rates?
- Challenges in evaluation
  - Are there further challenges not mentioned in this presentation?

Backup Slides

Benaloh Challenge

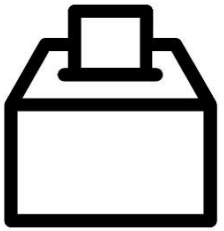
Benaloh Challenge

Verifier

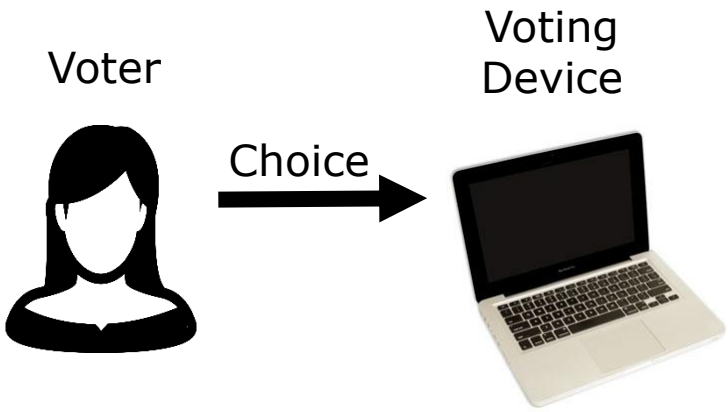
Voter

Voting Device

Ballot Box

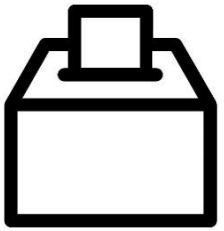


Benaloh Challenge

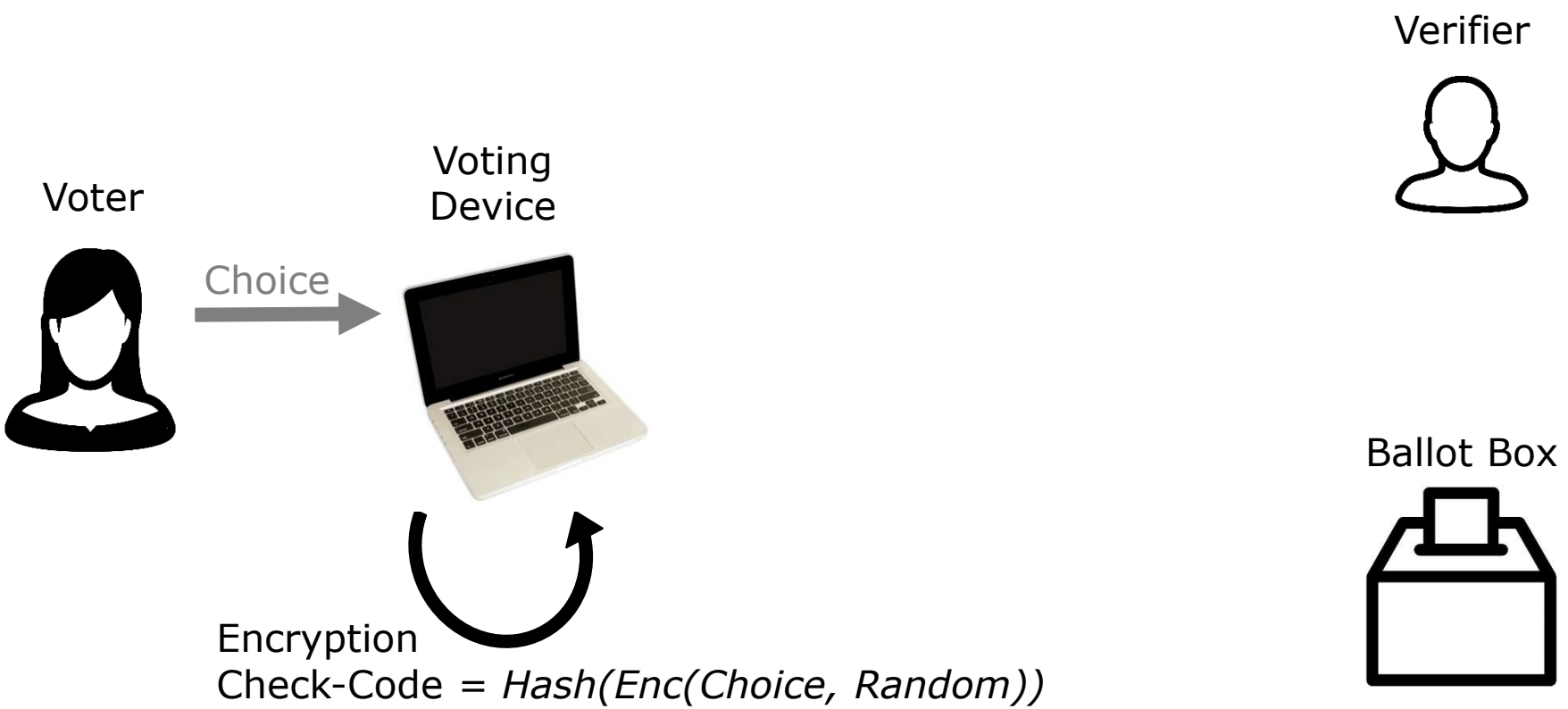


Verifier

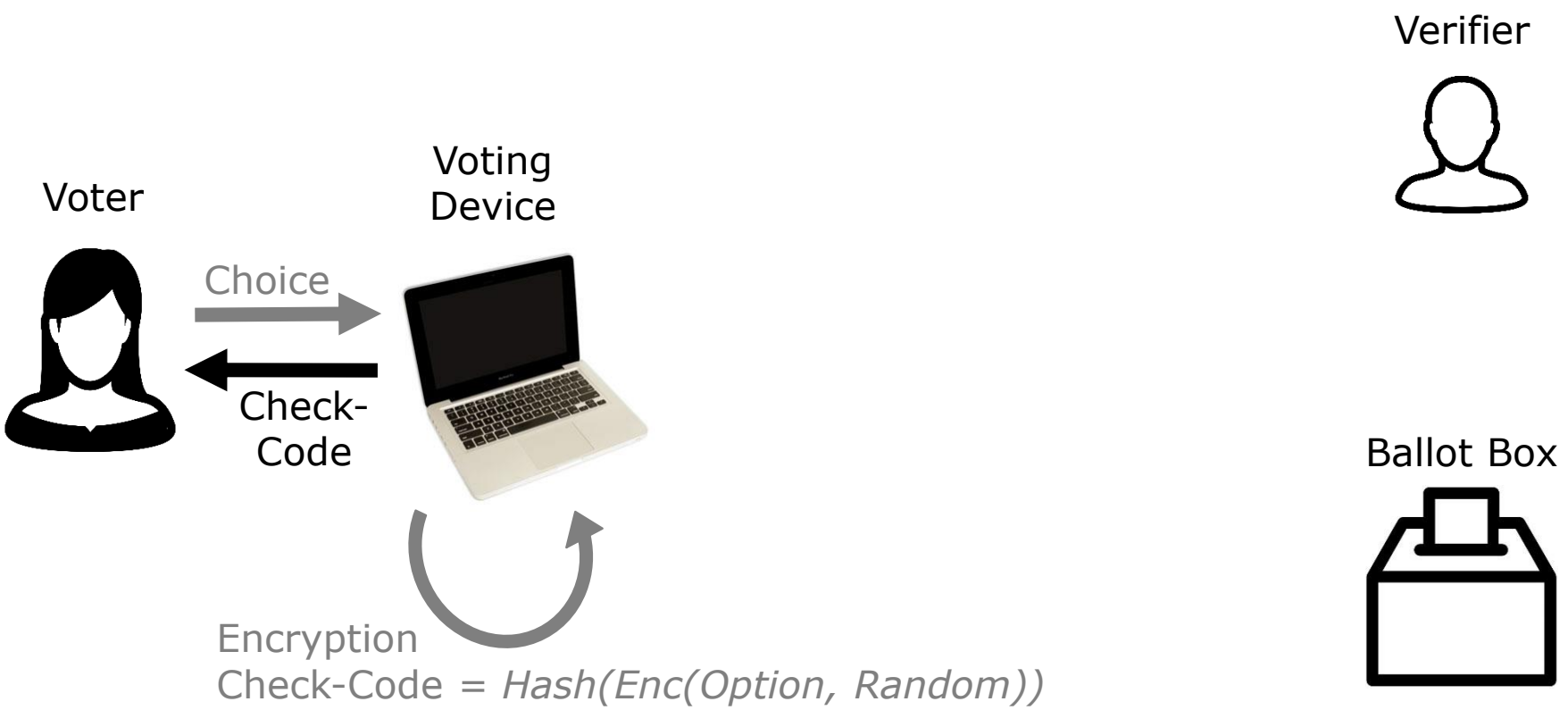
Ballot Box



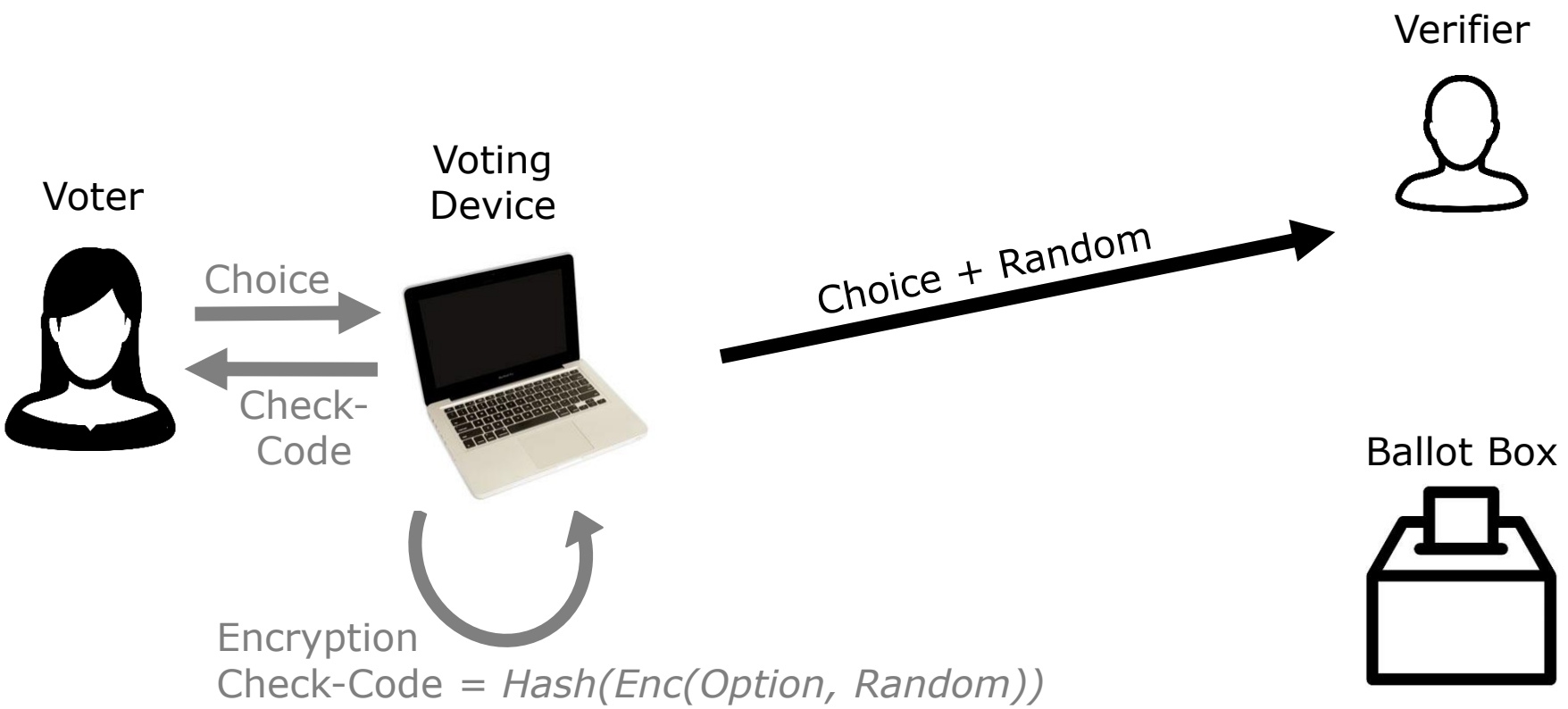
Benaloh Challenge



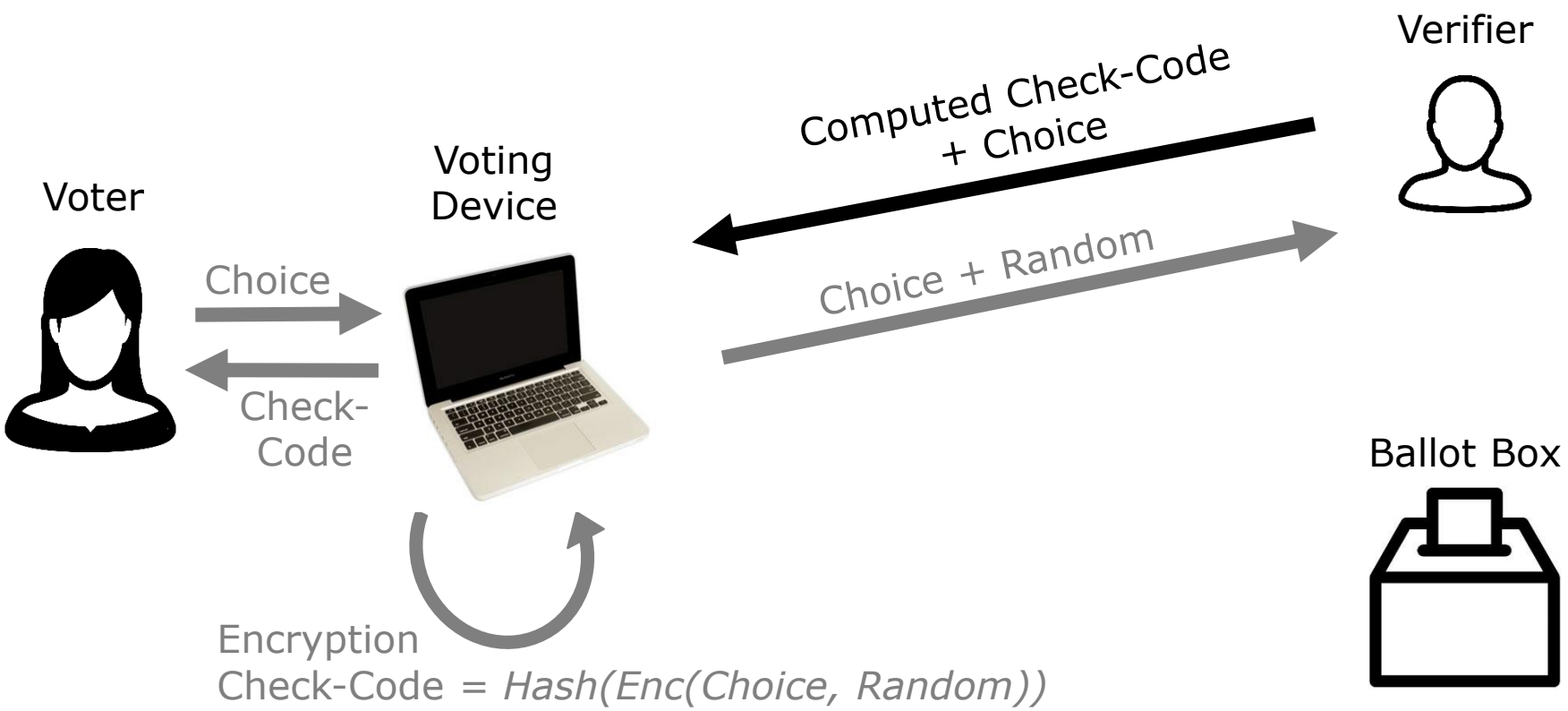
Benaloh Challenge



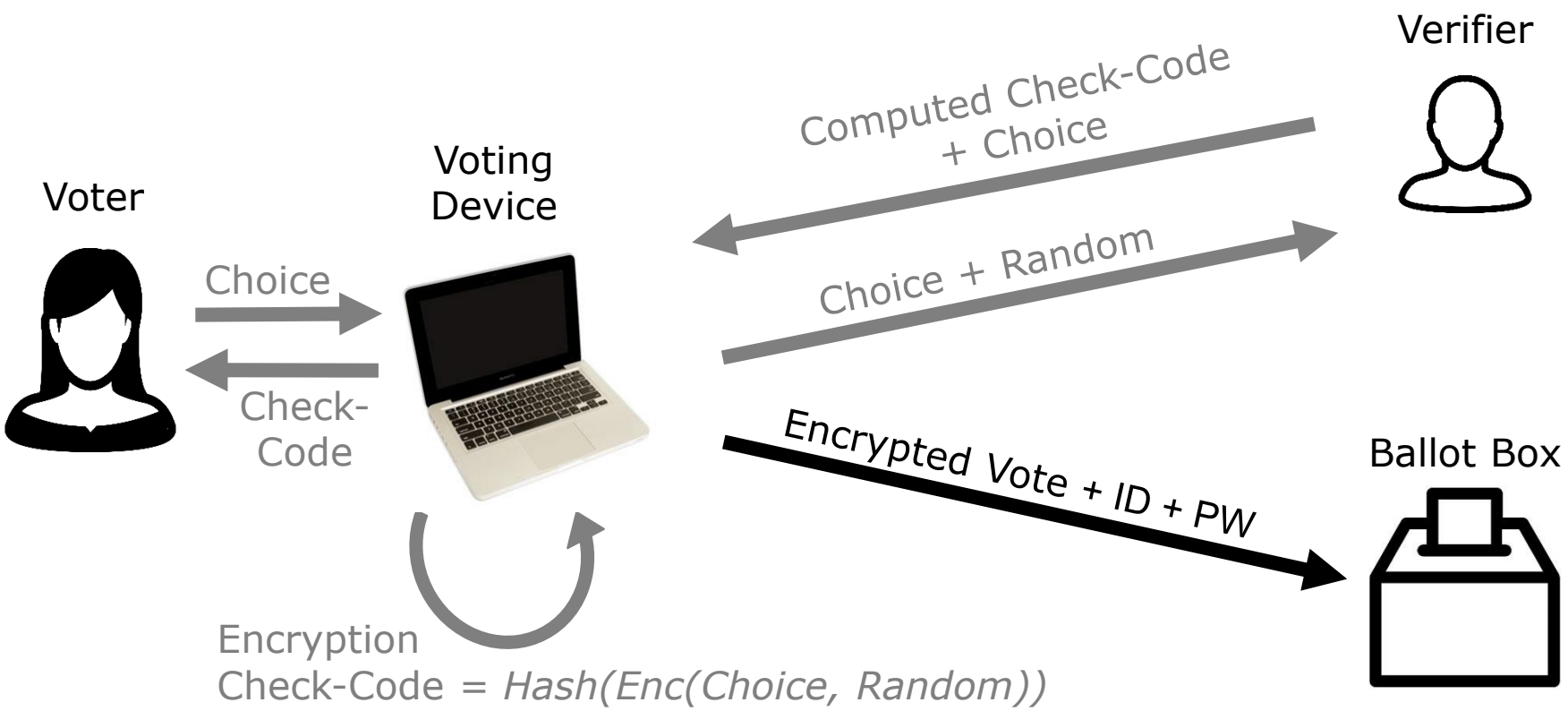
Benaloh Challenge



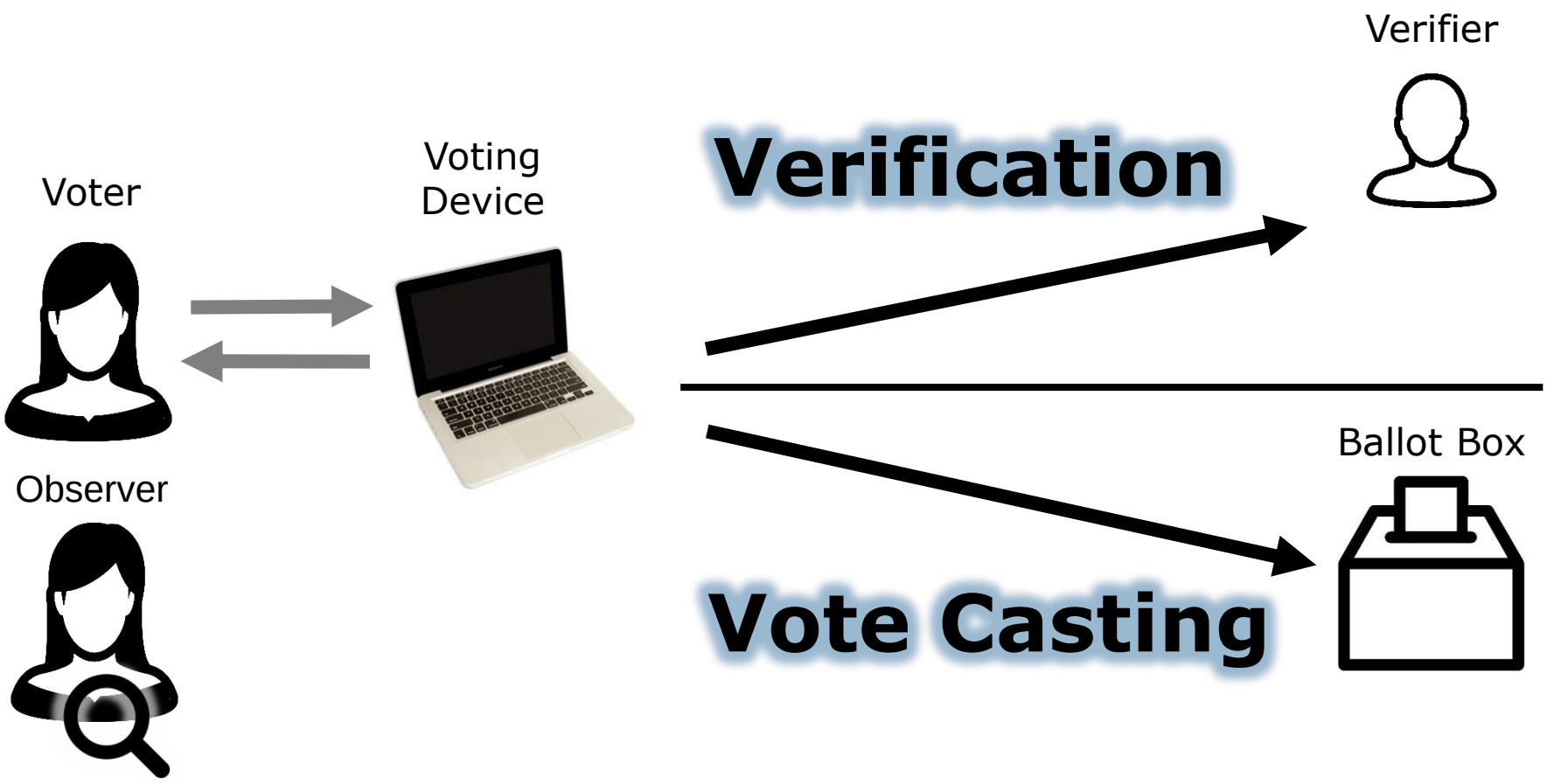
Benaloh Challenge



Benaloh Challenge



Benaloh Challenge



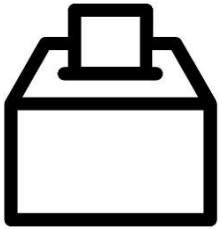
Code Voting

PUD

Voter

Voting Device

Ballot Box



PUD

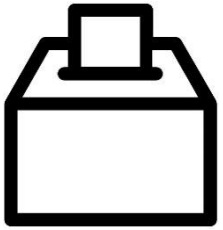
Code Sheet

ID: 34919	ID: 34919	ID: 34919
Fred Rubble	28502	93448
John Citizen	23983	62104
Jane Doe	45982	12937
Mary Hill	83410	89129
Joe Smith	29311	13812
–	94340	83429

Voter

Voting Device

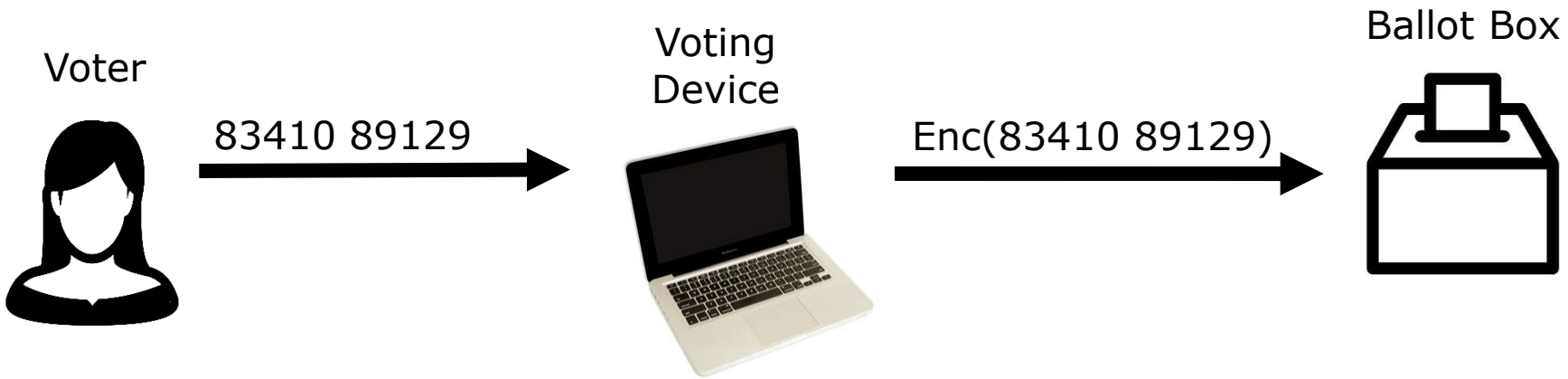
Ballot Box



PUD

Code Sheet

ID: 34919	ID: 34919	ID: 34919
Fred Rubble	28502	93448
John Citizen	23983	62104
Jane Doe	45982	12937
Mary Hill	83410	89129
Joe Smith	29311	13812
–	94340	83429



PUD

Code Sheet

ID: 34919	ID: 34919	ID: 34919
Fred Rubble	28502	93448
John Citizen	23983	62104
Jane Doe	45982	12937
Mary Hill	83410	89129
Joe Smith	29311	13812
–	94340	83429