Bern University
of Applied Sciences

Verifiable Electronic Elections:
Technical Solutions and Limits

Rolf Haenni

September 5th, 2014

Im Zentrum der Sicherheitsanforderungen steht die Verifizierbarkeit.

Bericht des Bundesrates zu Vote électronique
Schweizerischer Bundesrat, 2013

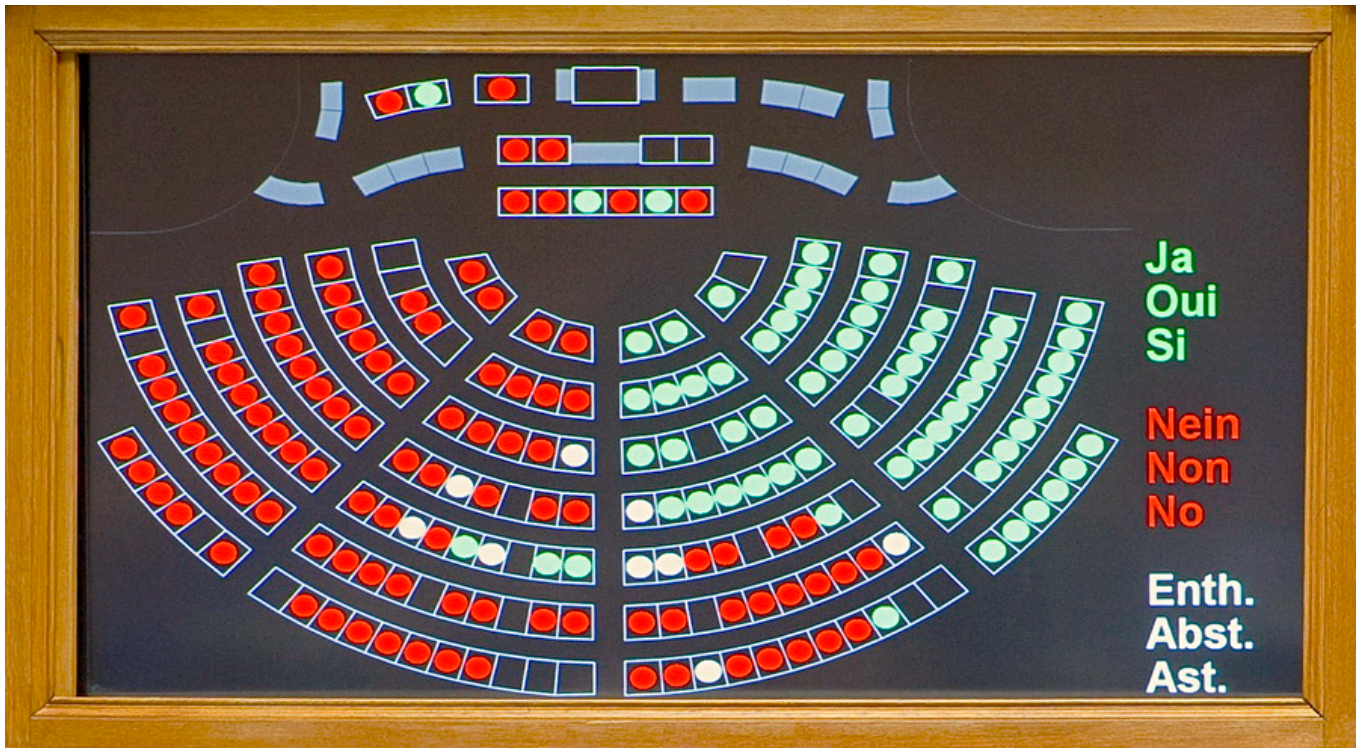
Overview

- Introduction
- The Mathematics of Verifiable Elections
- Individual Verifiability
- Universal Verifiability
- Conclusion

Introduction

One should verify the election, not the election system.

Ben Adida


Ja
Oui
Si
Nein
Non
No
Enth.
Abst.
Ast.

Bern University
of Applied Sciences

The Mathematics of Verifiable Elections

Exponentiation

$$z = b^x$$

Exponentiation

$$
\begin{aligned}
z &= b^x \\
&= \underbrace{b * b * \cdots * b}_{x \text{ times}}
\end{aligned}
$$

Exponentiation

$$
\begin{aligned}
z &= b^x \\
&= \underbrace{b * b * \cdots * b}_{x \text{ times}}
\end{aligned}
$$

Example: $z = 2^4 = 16$

Modular Exponentiation

Let n be a fixed number, for example $n = 5$

$$z = b^x \bmod n$$

Modular Exponentiation

Let n be a fixed number, for example $n = 5$

$$
\begin{aligned}
z &= b^x \bmod n \\
&= \underbrace{b * b * \cdots * b}_{x \text{ times}} \bmod n
\end{aligned}
$$

Modular Exponentiation

Let n be a fixed number, for example $n = 5$

$$z = b^x \bmod n$$
$$= \underbrace{b * b * \cdots * b}_{x \text{ times}} \bmod n$$

Example: $z = 2^4 \bmod 5 = 16 \bmod 5 = 1$

Fixed-Base Modular Exponentiation

Let b be a fixed number, for example $b = 2$

$$z = Exp(x) = b^x \bmod n$$

Fixed-Base Modular Exponentiation

Let b be a fixed number, for example $b = 2$

$$z = Exp(x) = b^x \bmod n$$

Example: $z = Exp(4) = 1$ for $b = 2$, $n = 5$

Very Large Numbers

If n and x are very large numbers ($>$300 digits), for example

$n =$ 161931481198080639220214033595931441094586304918402813506510547237223787775475425991443924977419330663170224569788019900180050114468430413908687329871251101280878786588515668012772798298511621634145464600626619548823238185390034868354933050128115662663653841842699535282987363300852550784188180264807606304297

(1024 Bits),

$x = \ldots$

then

Property 1: One-Way Function

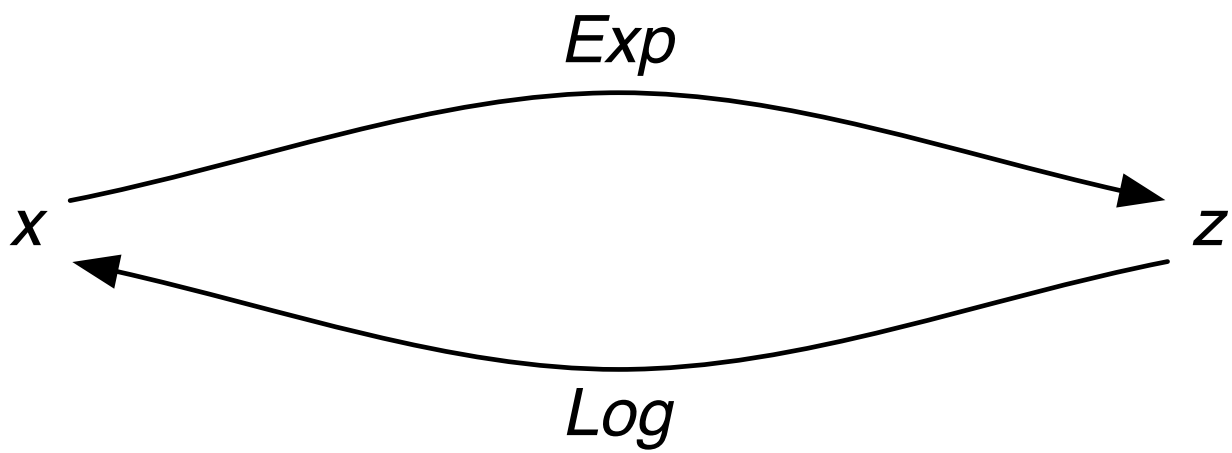
- $z = Exp(x)$ is still easy to compute

Property 1: One-Way Function

- $z = Exp(x)$ is still easy to compute
- $x = Log(z)$ is very hard to compute

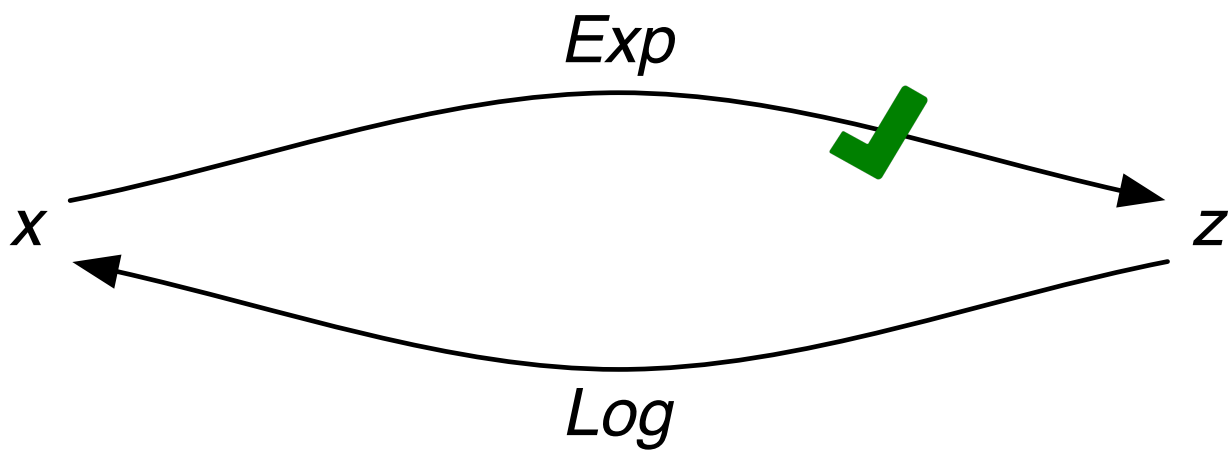
Property 1: One-Way Function

- $z = Exp(x)$ is still easy to compute
- $x = Log(z)$ is very hard to compute



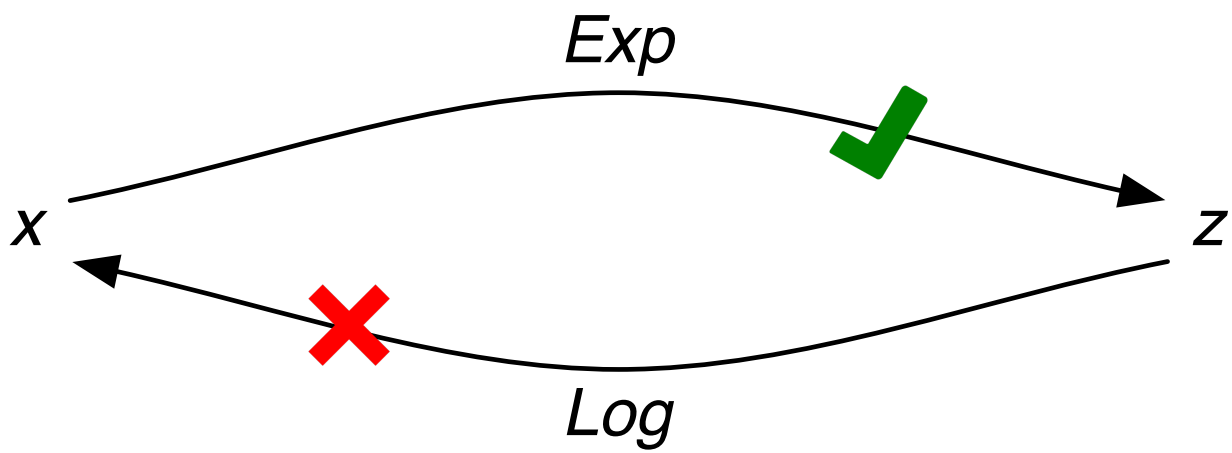
Property 1: One-Way Function

- $z = Exp(x)$ is still easy to compute
- $x = Log(z)$ is very hard to compute



Property 1: One-Way Function

- $z = Exp(x)$ is still easy to compute
- $x = Log(z)$ is very hard to compute



Property 2: Homomorphism

$$Exp(x) * Exp(y) = Exp(x + y)$$

Property 2: Homomorphism

$$Exp(x) * Exp(y) = Exp(x + y)$$

$$Exp(x)^y = Exp(x \cdot y)$$

Property 2: Homomorphism

$$Encrypt(x) * Encrypt(y) = Encrypt(x + y)$$

$$Encrypt(x)^y = Encrypt(x \cdot y)$$

Zero-Knowlegde Proofs

- Let n and x be very large numbers
- If I claim to know x such that $z = Exp(x)$, what can I do to make you believe me?

Zero-Knowlegde Proofs

- Let n and x be very large numbers
- If I claim to know x such that $z = Exp(x)$, what can I do to make you believe me?

- Option 1: Show you x and you check it

Zero-Knowlegde Proofs

- Let n and x be very large numbers
- If I claim to know x such that $z = Exp(x)$, what can I do to make you believe me?

- Option 1: Show you x and you check it

- Option 2: Compute a zero-knowledge proof

Zero-Knowlegde Proofs

- Let n and x be very large numbers
- If I claim to know x such that $z = Exp(x)$, what can I do to make you believe me?

- Option 1: Show you x and you check it

- Option 2: Compute a zero-knowledge proof
  - I give you a commitment $t = Exp(r)$ for a random value r
  - You give me a random challenge c
  - I give you my response $s = r + x \cdot c$
  - You check $Exp(s) = t \cdot z^c$

Applications in Electronic Voting

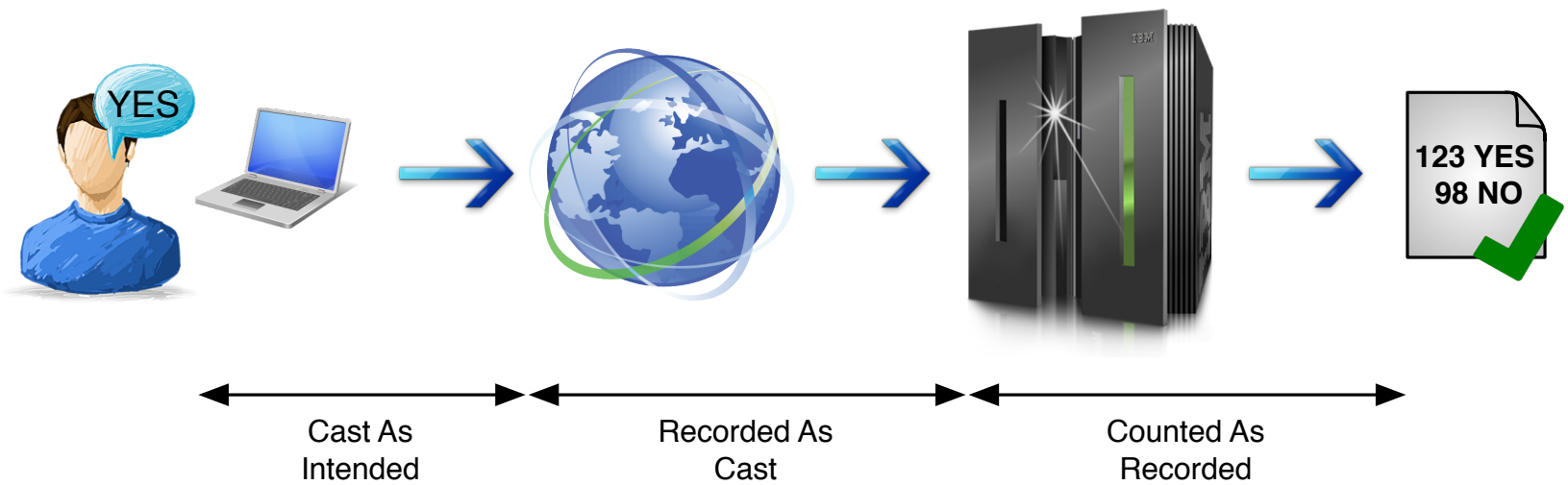
- Encrypting votes (ElGamal)
- Proving that an encrypted vote is either 0 or 1
- Summing up encrypted votes
- Computing verification codes from encrypted votes
- Re-encrypting an encrypted vote
- Shuffling a list of encrypted votes
- Proving that the re-encrytion and shuffling was done correctly
- Sharing the decryption key
- Decrypting votes with shared keys
- etc.

Individual Verifiability

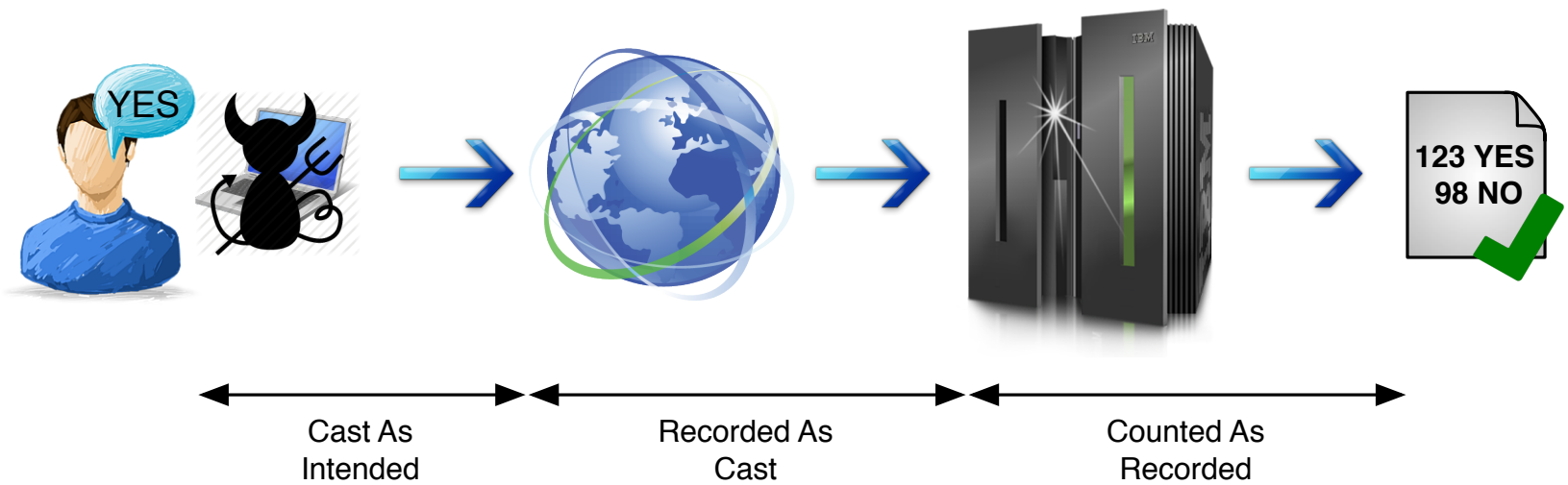
Die Stimmenden müssen die Möglichkeit haben, zu erkennen, ob ihre Stimme auf der Benutzerplattform oder auf dem Übertragungsweg manipuliert worden ist.

Verordnung der BK über die elektronische Stimmabgabe, VEleS, 2013

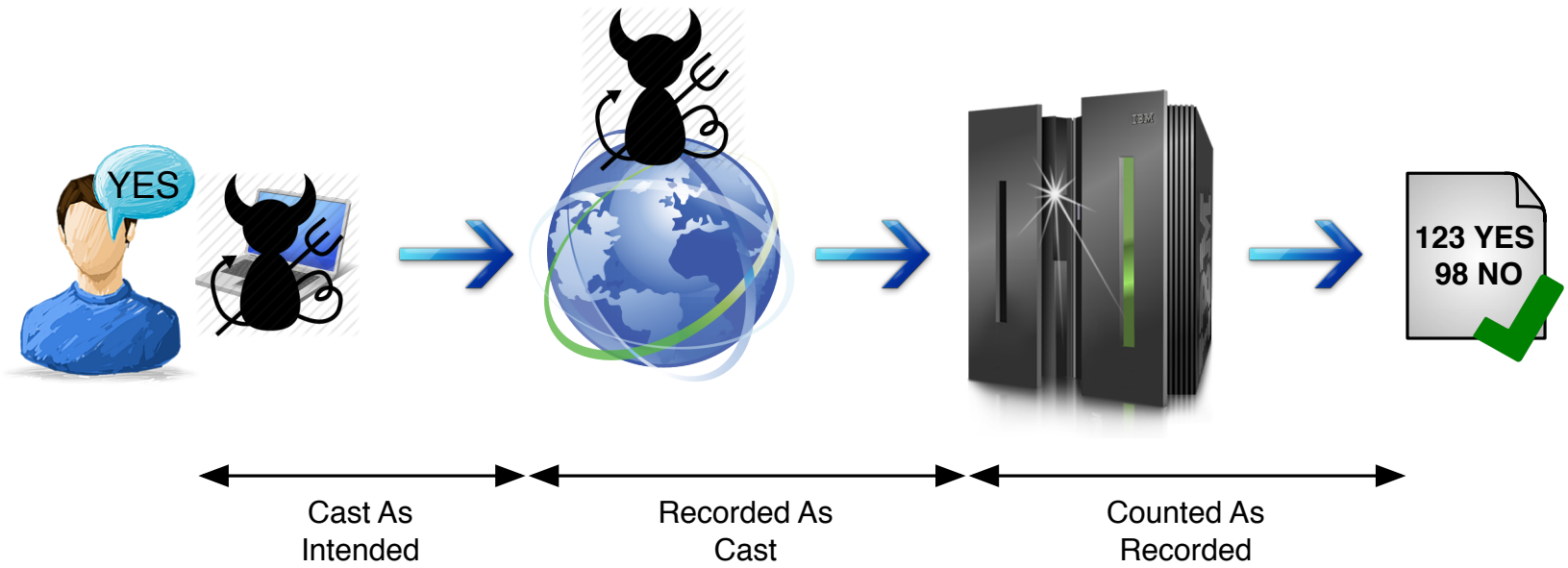
Trust Model


YES
123 YES
98 NO
Cast As
Intended
Recorded As
Cast
Counted As
Recorded

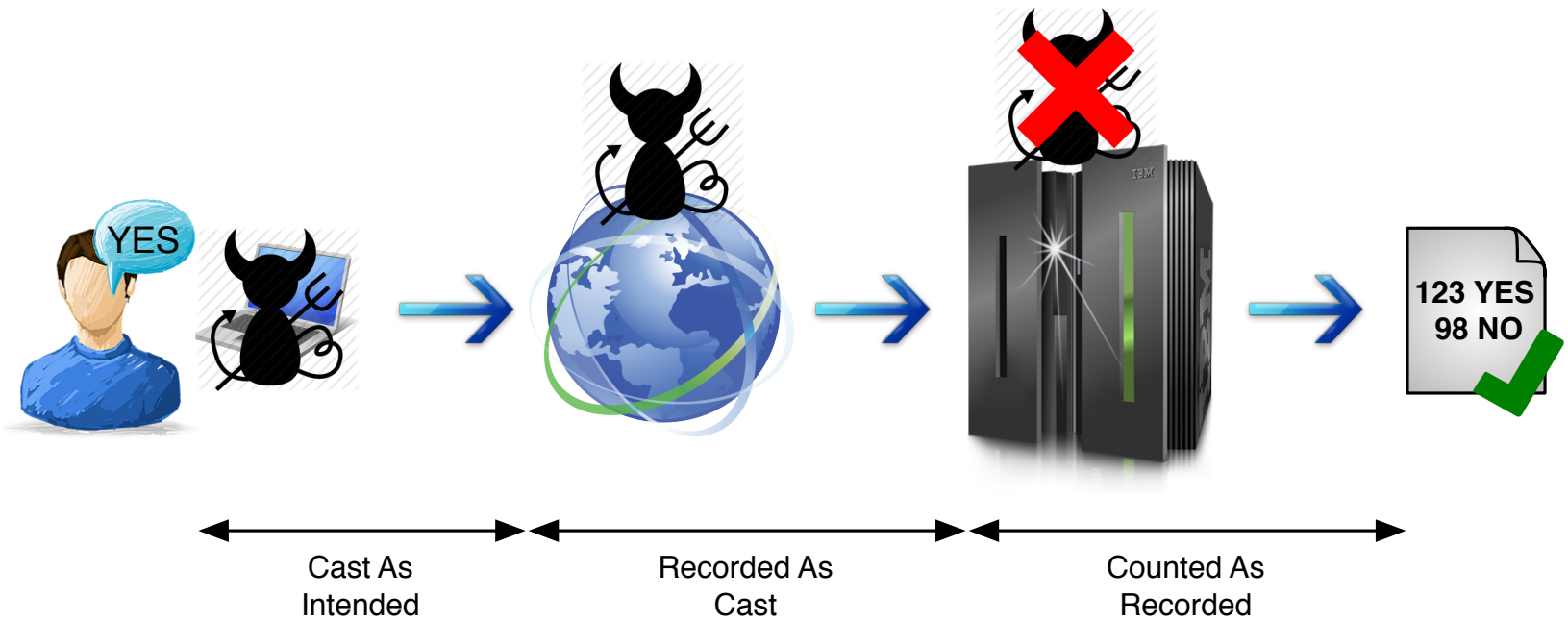
Trust Model


YES
123 YES
98 NO
Cast As
Intended
Recorded As
Cast
Counted As
Recorded

Trust Model


YES
123 YES
98 NO
Cast As
Intended
Recorded As
Cast
Counted As
Recorded

Trust Model


YES
123 YES
98 NO
Cast As
Intended
Recorded As
Cast
Counted As
Recorded

Individual Verifiability in Norway

- Differences to Switzerland
  - Citizens have a login for public services
  - Their mobile phone numbers are registered
  - The voting laws allow vote updates

Individual Verifiability in Norway

- Differences to Switzerland
  - Citizens have a login for public services
  - Their mobile phone numbers are registered
  - The voting laws allow vote updates
- Prior to an election, voters receive a code sheet
  - Different codes for each party/candidate
  - Different codes on each code sheet

Individual Verifiability in Norway

- Differences to Switzerland
  - Citizens have a login for public services
  - Their mobile phone numbers are registered
  - The voting laws allow vote updates
- Prior to an election, voters receive a code sheet
  - Different codes for each party/candidate
  - Different codes on each code sheet
- Vote verification
  - After voting, voters receive their verification codes by SMS
  - If the codes match with the ones on the code sheet, the vote has been recorded as intended
  - If something goes wrong, voters can try again

Individual Verifiability in Norway

- Differences to Switzerland
  - Citizens have a login for public services
  - Their mobile phone numbers are registered
  - The voting laws allow vote updates
- Prior to an election, voters receive a code sheet
  - Different codes for each party/candidate
  - Different codes on each code sheet
- Vote verification
  - After voting, voters receive their verification codes by SMS
  - If the codes match with the ones on the code sheet, the vote has been recorded as intended
  - If something goes wrong, voters can try again
- Verification codes are derived from the encrypted votes !

Individual Verifiability in Norway

- Trust assumptions
  - An attacker may either control the voter's computer or phone, but not both devices simultaneously
  - Voters no not use their phones for voting
  - Printing and postal services are trusted

Individual Verifiability in Norway

- Trust assumptions
  - An attacker may either control the voter's computer or phone, but not both devices simultaneously
  - Voters no not use their phones for voting
  - Printing and postal services are trusted
- Attacks against the voter's computer
  - Blocking the vote casting
  - Voting for another candidate
  - Stealing the voter's credentials for vote updating
  - Breaking the vote secrecy

Individual Verifiability in Norway

- Trust assumptions
  - An attacker may either control the voter's computer or phone, but not both devices simultaneously
  - Voters no not use their phones for voting
  - Printing and postal services are trusted
- Attacks against the voter's computer
  - Blocking the vote casting
  - Voting for another candidate
  - Stealing the voter's credentials for vote updating
  - Breaking the vote secrecy
- Attacks against the voter's phone
  - Blocking incoming SMS messages
  - Manipulating or generating incoming SMS messages

Individual Verifiability in Norway

- Trust assumptions
  - An attacker may either control the voter's computer or phone, but not both devices simultaneously
  - Voters no not use their phones for voting
  - Printing and postal services are trusted
- Attacks against the voter's computer
  - Blocking the vote casting
  - Voting for another candidate
  - **Stealing the voter's credentials for vote updating**
  - Breaking the vote secrecy
- Attacks against the voter's phone
  - **Blocking incoming SMS messages**
  - Manipulating or generating incoming SMS messages

Individual Verifiability in Norway

R. E. Koenig, R. Haenni, and P. Locher.
Attacking the verification code mechanism in the Norwegian internet voting system. *VoteID'13, 4th International Conference on E-Voting and Identity*, Guildford, U.K., 2013.

Individual Verifiability in Sitzerland

- The Norwegian verification mechanism can be adjusted to the "Swiss case"
  - Verification codes are displayed in the browser
  - Nothing is sent to the voter's phone
  - If something goes wrong, voters can vote on paper

Individual Verifiability in Sitzerland

- The Norwegian verification mechanism can be adjusted to the "Swiss case"
  - Verification codes are displayed in the browser
  - Nothing is sent to the voter's phone
  - If something goes wrong, voters can vote on paper
- Attacks against the voter's computer
  - Blocking the vote casting
  - Voting for another candidate
  - Blocking or manipulating incoming verification codes
  - Breaking the vote secrecy

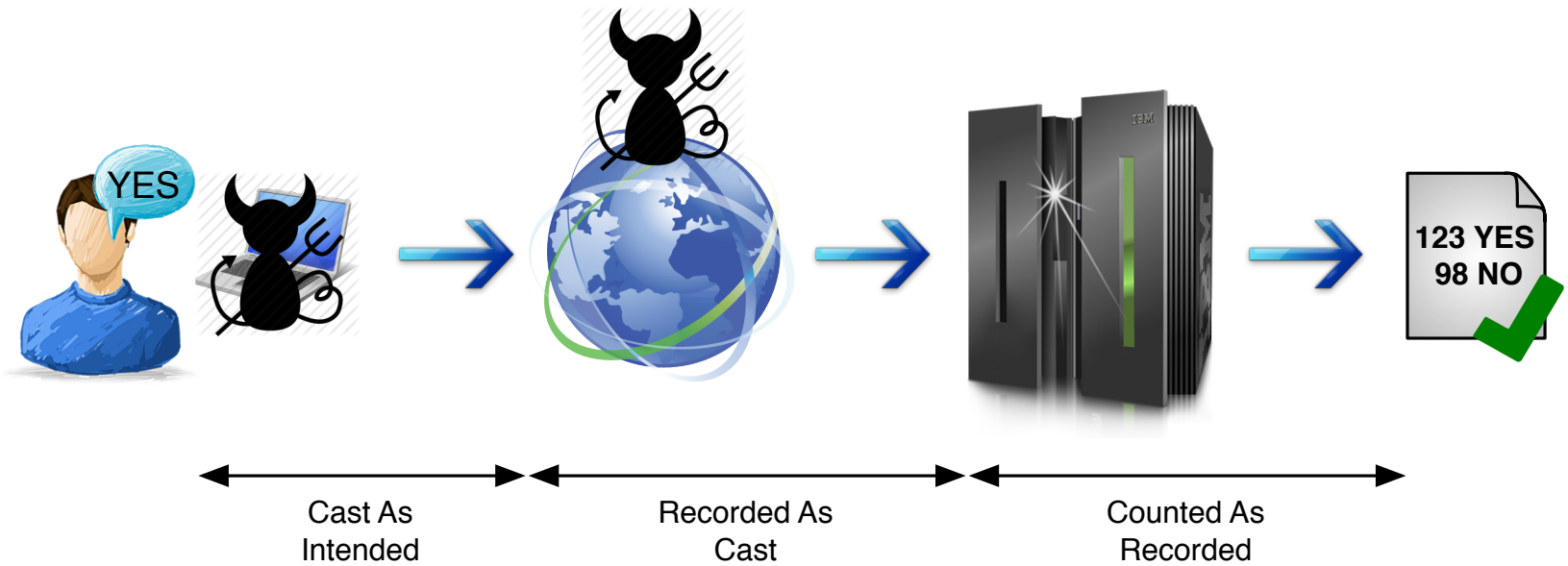
Bern University
of Applied Sciences

Universal Verifiability

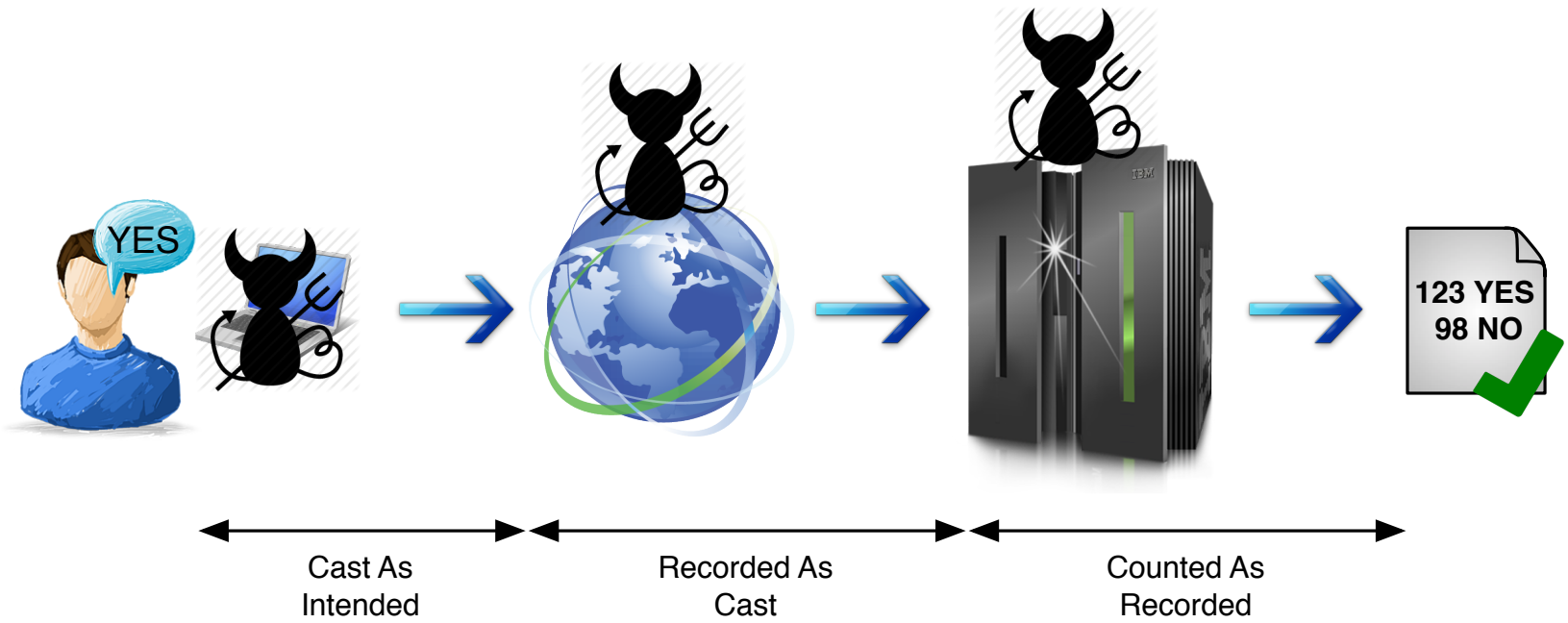
Zur universellen Verifizierung erhalten die Prüferinnen und Prüfer einen Beweis der korrekten Ergebnisermittlung. [...] Dazu müssen sie technische Hilfsmittel verwenden, die vom Rest des Systems unabhängig und isoliert sind.

Verordnung der BK über die elektronische Stimmabgabe, VEleS, 2013

Trust Model


YES
123 YES
98 NO
Cast As
Intended
Recorded As
Cast
Counted As
Recorded

Trust Model

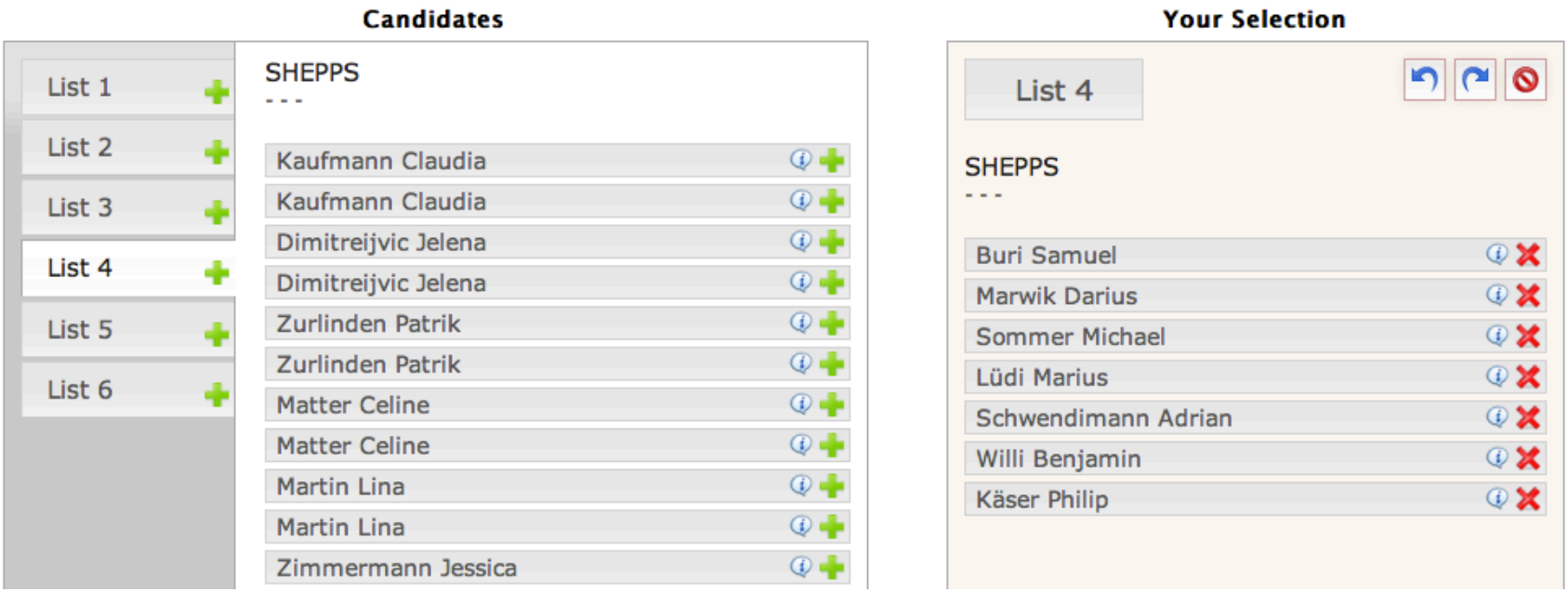

YES
123 YES
98 NO
Cast As
Intended
Recorded As
Cast
Counted As
Recorded

UNI VOTE

VSBFH Studierendenratswahl 2014

Key Entry > Vote > Confirmation

Please prepare your vote by dragging the preferred list and candidates from the left column to the ballot on the right-hand-side. You can cast the ballot whenever you are ready.



Universal Verifiability in UniVote

- Differences to cantonal and federal elections
  - Students have login for university services
  - Their e-mail addresses are registered
  - They are above-average computer users

Universal Verifiability in UniVote

- Differences to cantonal and federal elections
  - Students have login for university services
  - Their e-mail addresses are registered
  - They are above-average computer users
- Prior to an election, students need to register
  - They generate their own voting key
  - Nothing is printed on paper

Universal Verifiability in UniVote

- Differences to cantonal and federal elections
  - Students have login for university services
  - Their e-mail addresses are registered
  - They are above-average computer users
- Prior to an election, students need to register
  - They generate their own voting key
  - Nothing is printed on paper
- After voting, voters receive a receipt of their vote
  - QR-code displayed on screen
  - They can copy/paste the image or take a snapshot

Universal Verifiability in UniVote

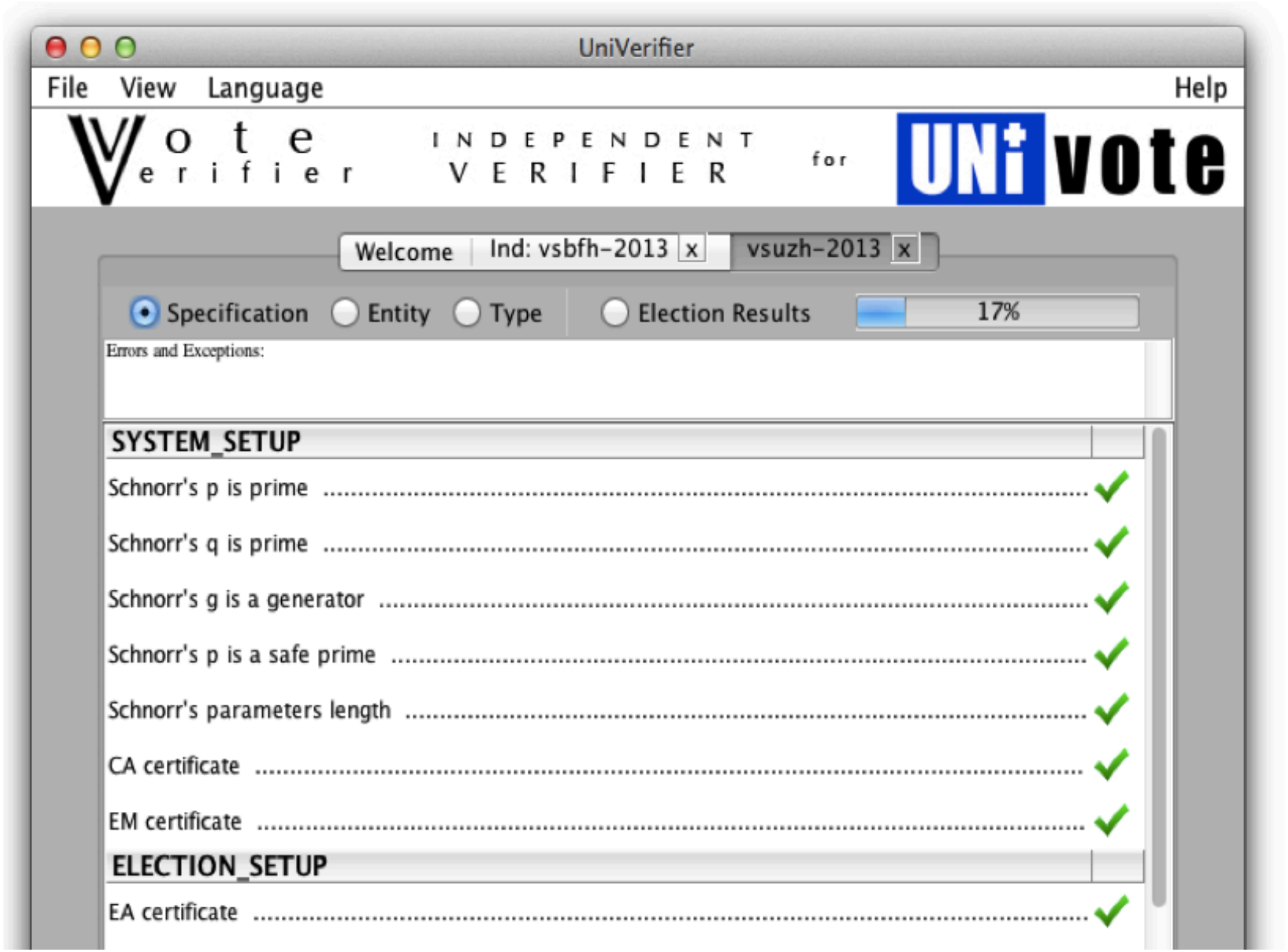
- Differences to cantonal and federal elections
  - Students have login for university services
  - Their e-mail addresses are registered
  - They are above-average computer users
- Prior to an election, students need to register
  - They generate their own voting key
  - Nothing is printed on paper
- After voting, voters receive a receipt of their vote
  - QR-code displayed on screen
  - They can copy/paste the image or take a snapshot
- After the election, all voters can check
  - The inclusion of their votes (using the QR-code)
  - The correctness of the final result

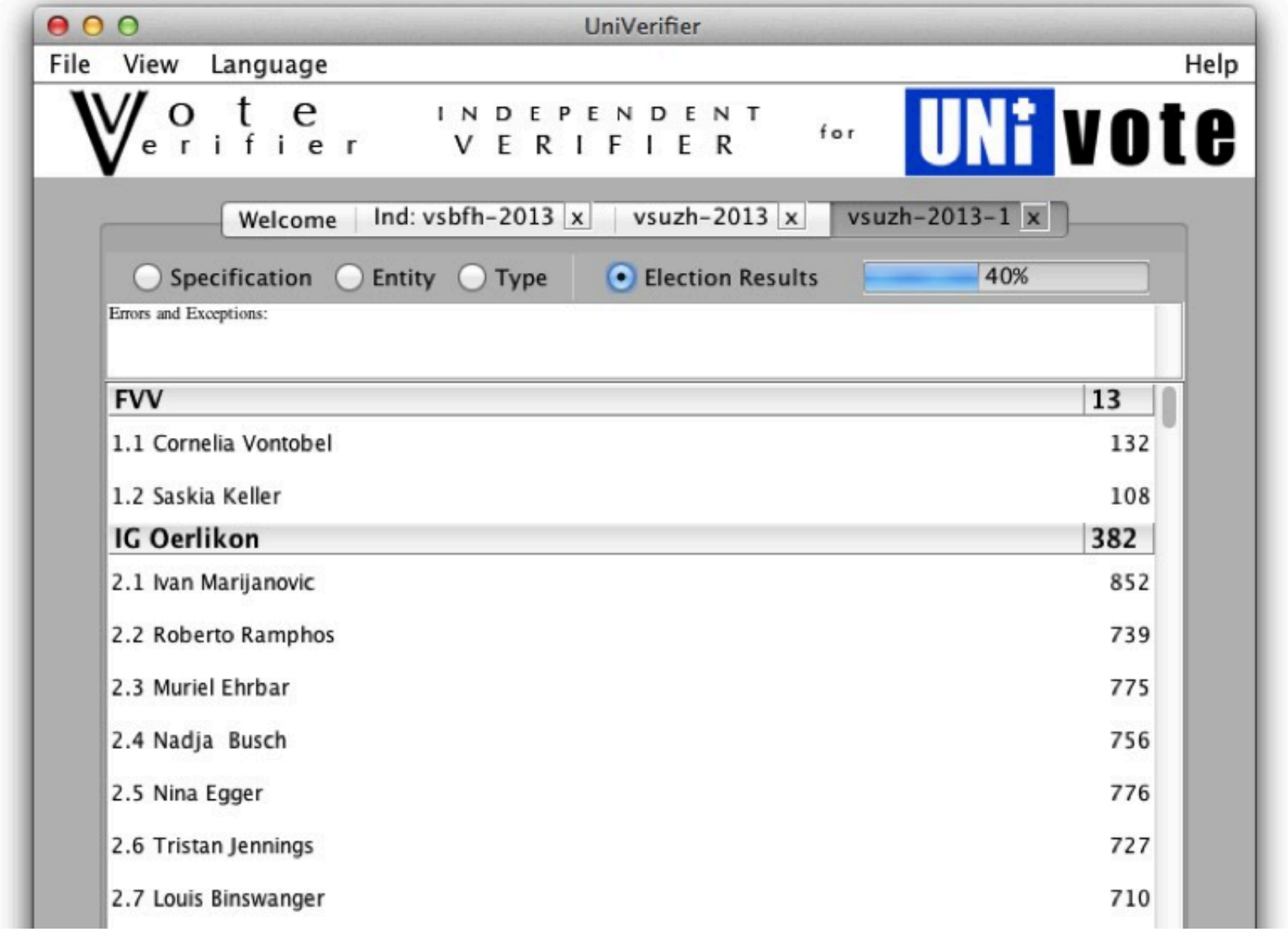
Universal Verifiability in UniVote

- The election data is published on the public bulletin board
  - System and election setup
  - List of candidates
  - List of voters and their voting keys
  - Anonymized list of voting keys (with zero-knowledge proof)
  - Encrypted votes (with zero-knowledge proofs)
  - Shuffled encrypted votes (with zero-knowledge proof)
  - Partial decryptions (with zero-knowledge proofs)
  - Decrypted votes
  - Final result

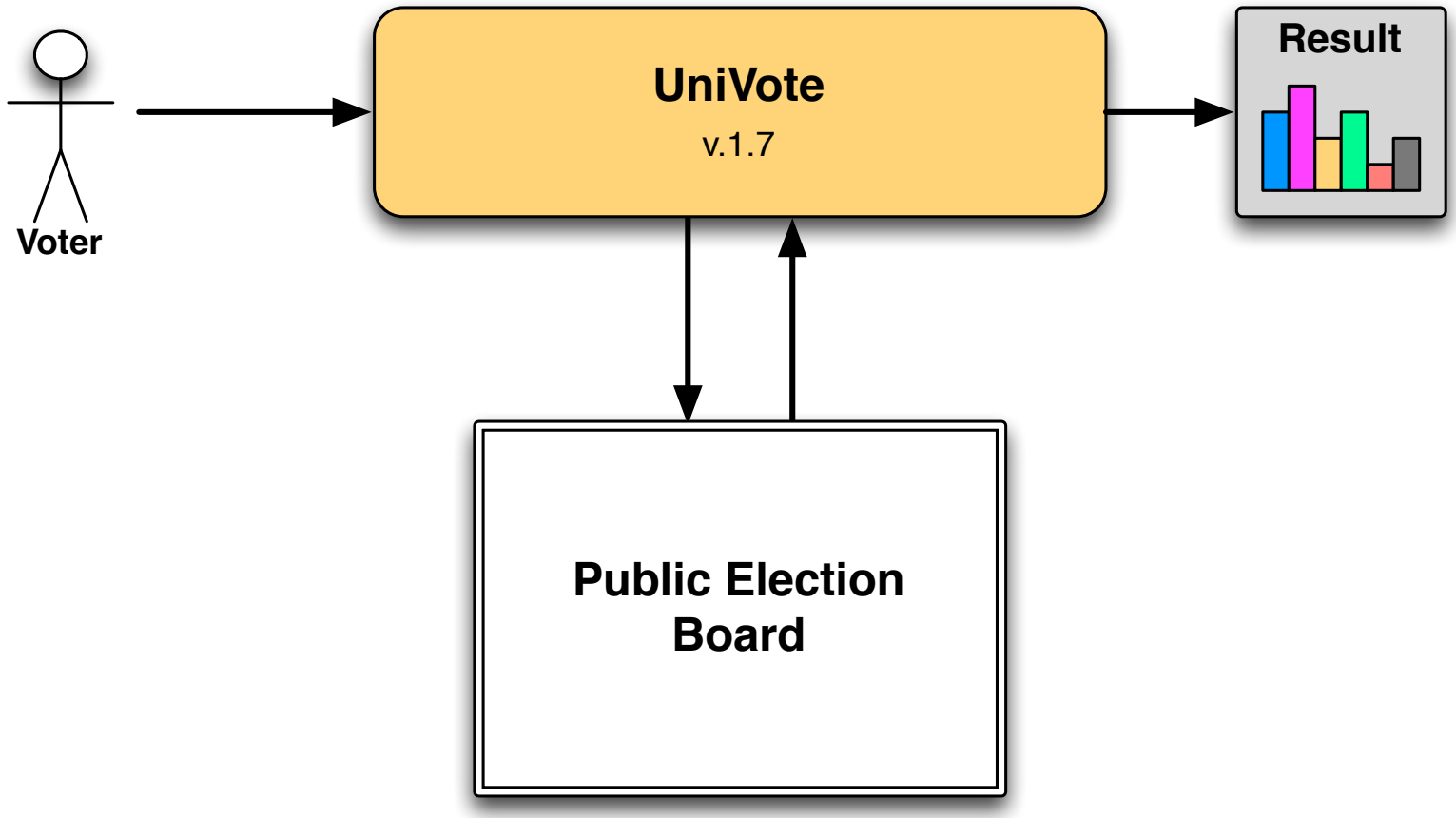
Universal Verifiability in UniVote

- The election data is published on the public bulletin board
  - System and election setup
  - List of candidates
  - List of voters and their voting keys
  - Anonymized list of voting keys (with zero-knowledge proof)
  - Encrypted votes (with zero-knowledge proofs)
  - Shuffled encrypted votes (with zero-knowledge proof)
  - Partial decryptions (with zero-knowledge proofs)
  - Decrypted votes
  - Final result
- An independent software is needed to verify the election result

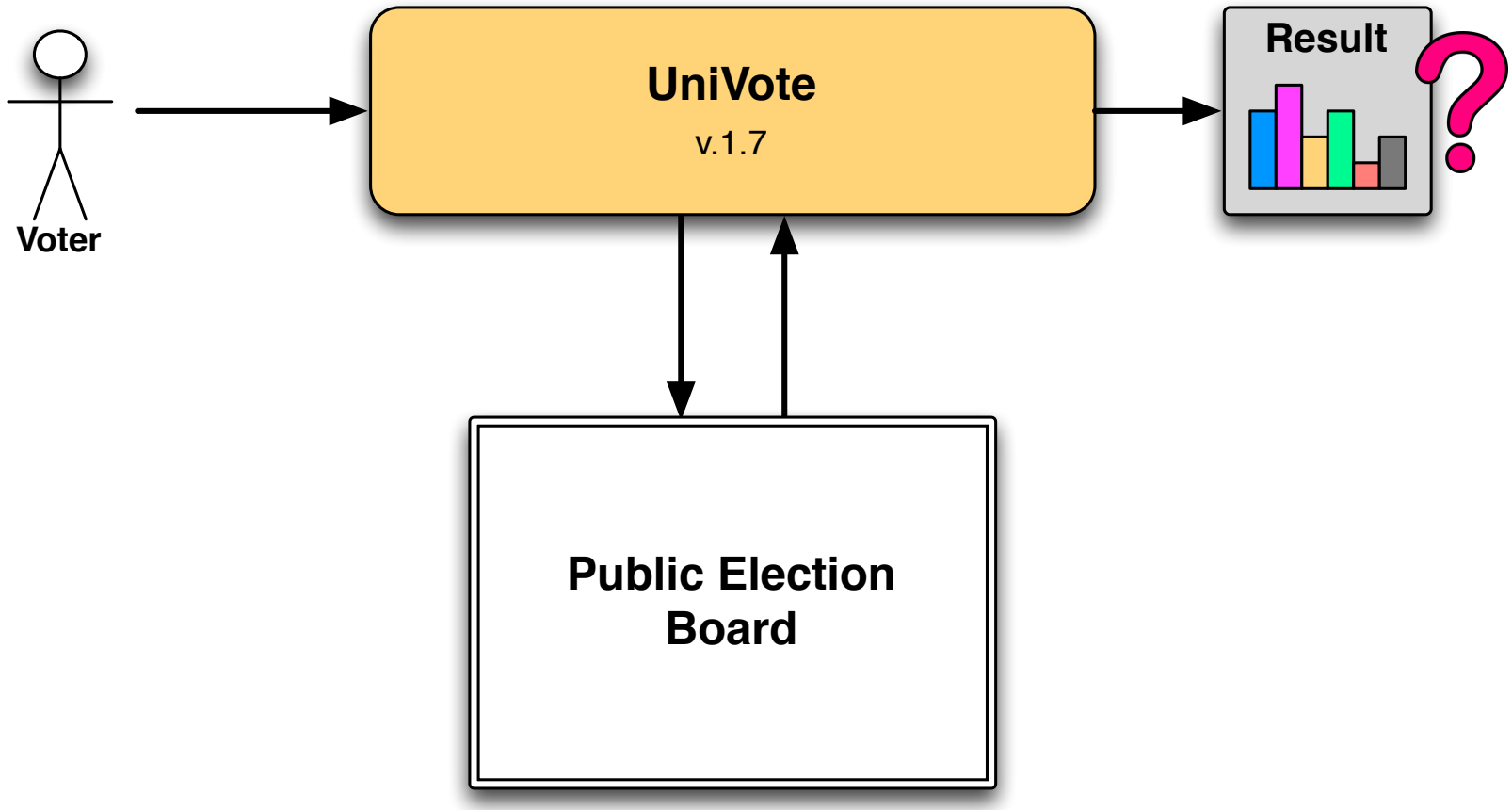

UniVerifier
File View Language Help
Vote Verifier
INDEPENDENT VERIFIER for
UNIvote
Welcome
Ind: vsbfh-2013 x
vsuzh-2013 x
Specification
Entity
Type
Election Results
17%
Errors and Exceptions:
SYSTEM_SETUP
Schnorr's p is prime
Schnorr's q is prime
Schnorr's g is a generator
Schnorr's p is a safe prime
Schnorr's parameters length
CA certificate
EM certificate
ELECTION_SETUP
EA certificate


UniVerifier
File View Language Help
Vote Verifier
INDEPENDENT VERIFIER for UNIvote
Welcome
Ind: vsbfh-2013 x
vsuzh-2013 x
vsuzh-2013-1 x
Specification
Entity
Type
Election Results
40%
Errors and Exceptions:
FVV 13
1.1 Cornelia Vontobel 132
1.2 Saskia Keller 108
IG Oerlikon 382
2.1 Ivan Marijanovic 852
2.2 Roberto Ramphos 739
2.3 Muriel Ehrbar 775
2.4 Nadja Busch 756
2.5 Nina Egger 776
2.6 Tristan Jennings 727
2.7 Louis Binswanger 710

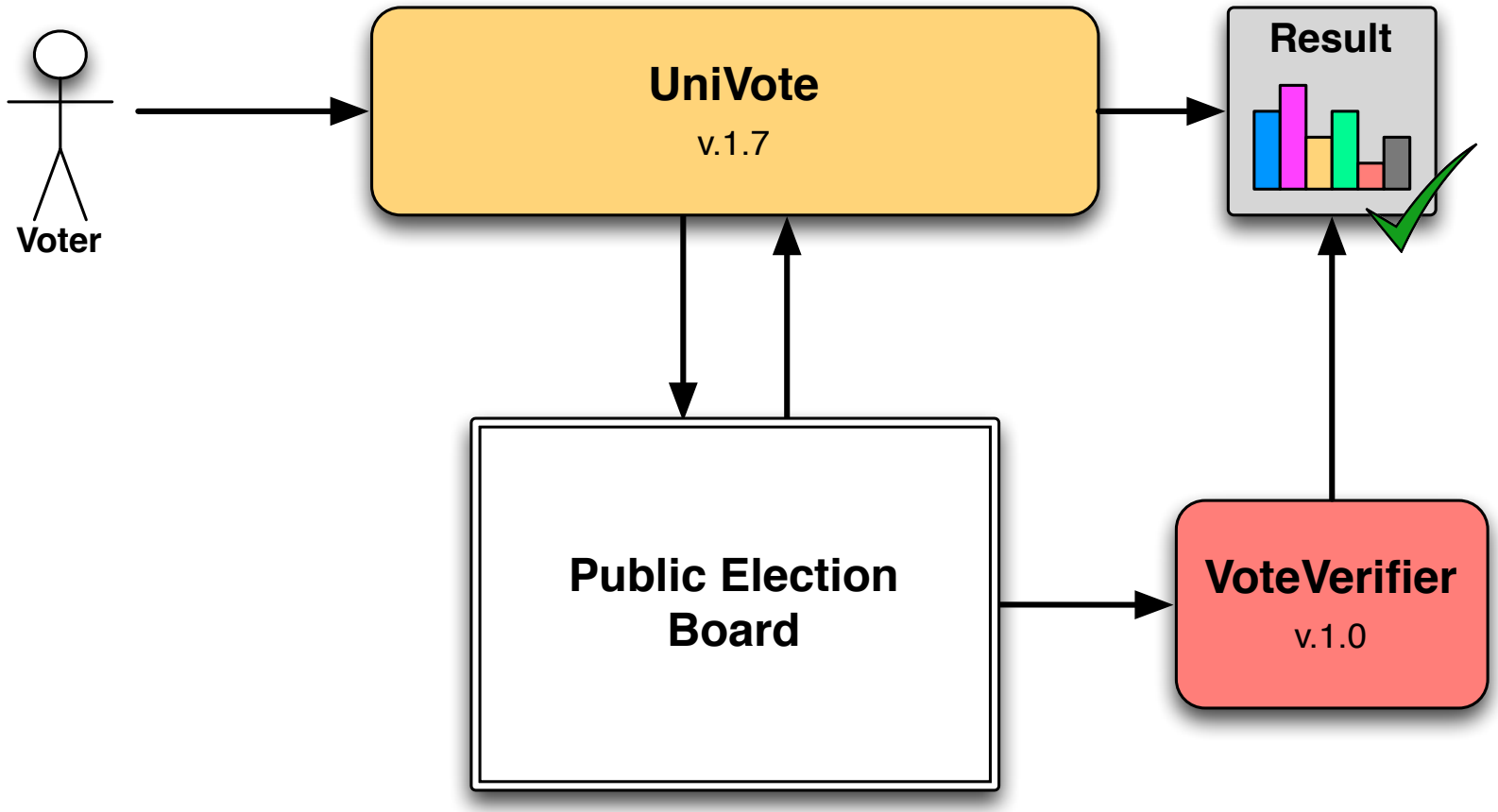
Public Bulletin Board



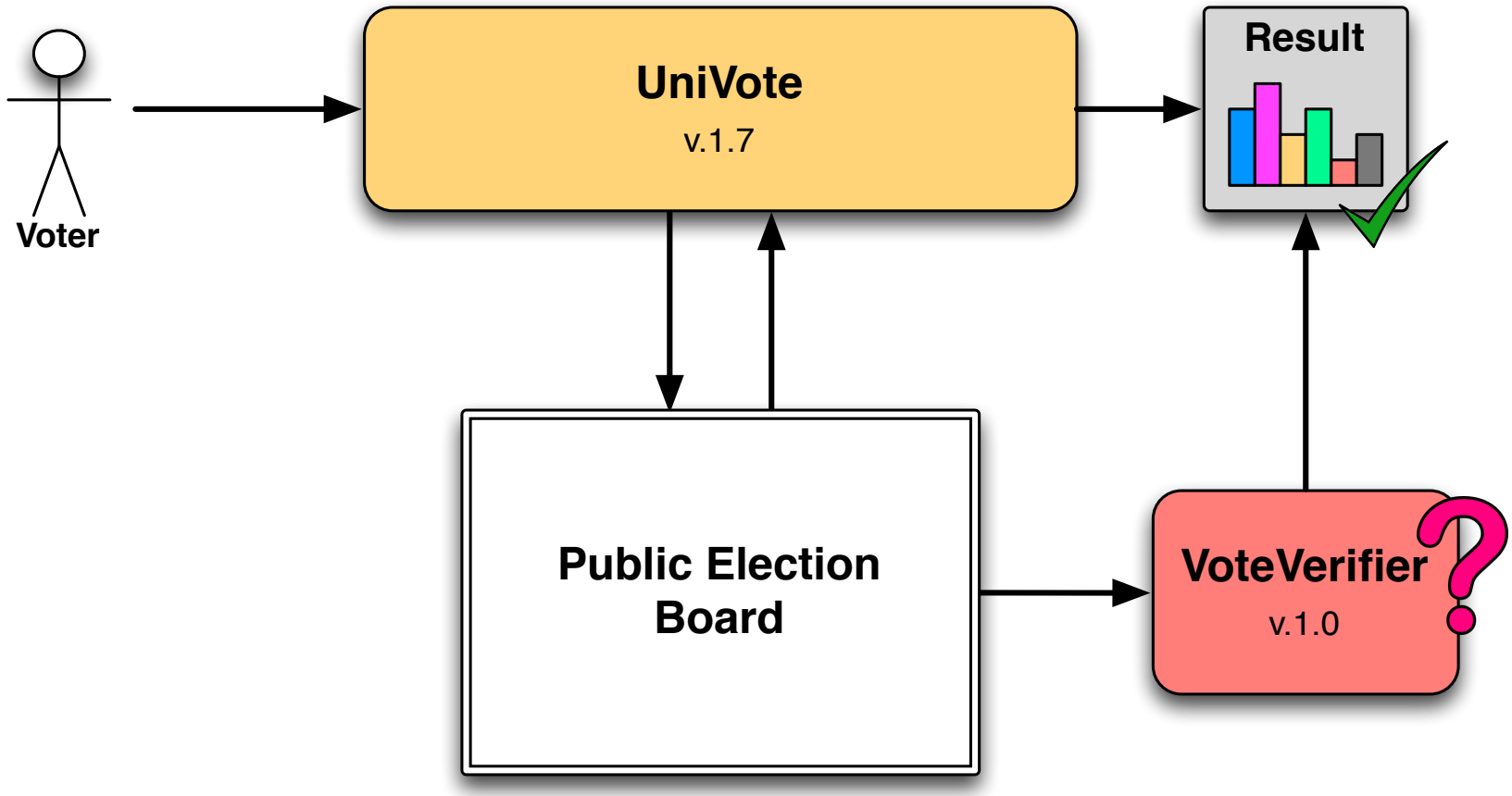
Public Bulletin Board



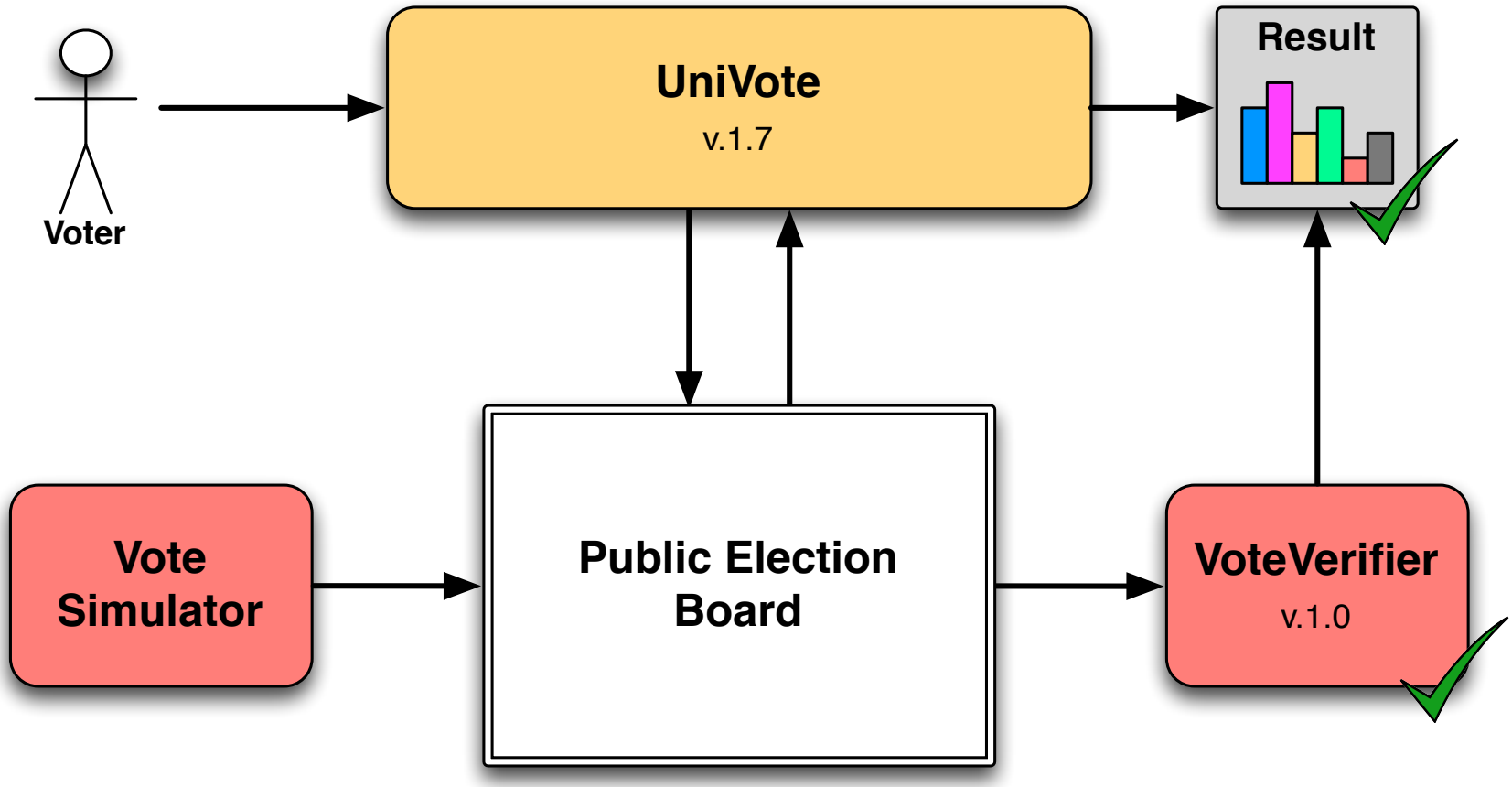
Public Bulletin Board



Public Bulletin Board



Public Bulletin Board



Conclusion

Conclusion

- Second-generation systems need to provide verifiability

Conclusion

- Second-generation systems need to provide verifiability
- There are technical solutions and implementations
  - Individual verifiability: Norway
  - Universal verifiability: UniVote (and some others)

Conclusion

- Second-generation systems need to provide verifiability
- There are technical solutions and implementations
  - Individual verifiability: Norway
  - Universal verifiability: UniVote (and some others)
- Challenges
  - Complexity of some approaches
  - Cryptography in web browsers (JavaScript)
  - Usability and voter education
  - Vote secrecy on insecure platform
  - Voting buying and coercion

See

http://www.voteid15.org