A New Technique for Deniable Vote Updating: Intuitive, Efficient, and Secure

Najmeh Soroush
Johannes Muller, Ivan Pryvalov, Balázs Pejó

E-Vote-ID 2021
PhD Colloquium
October 2021

SnT
securityandtrust.lu

uni.lu
UNIVERSITÉ DU LUXEMBOURG

PhD Student

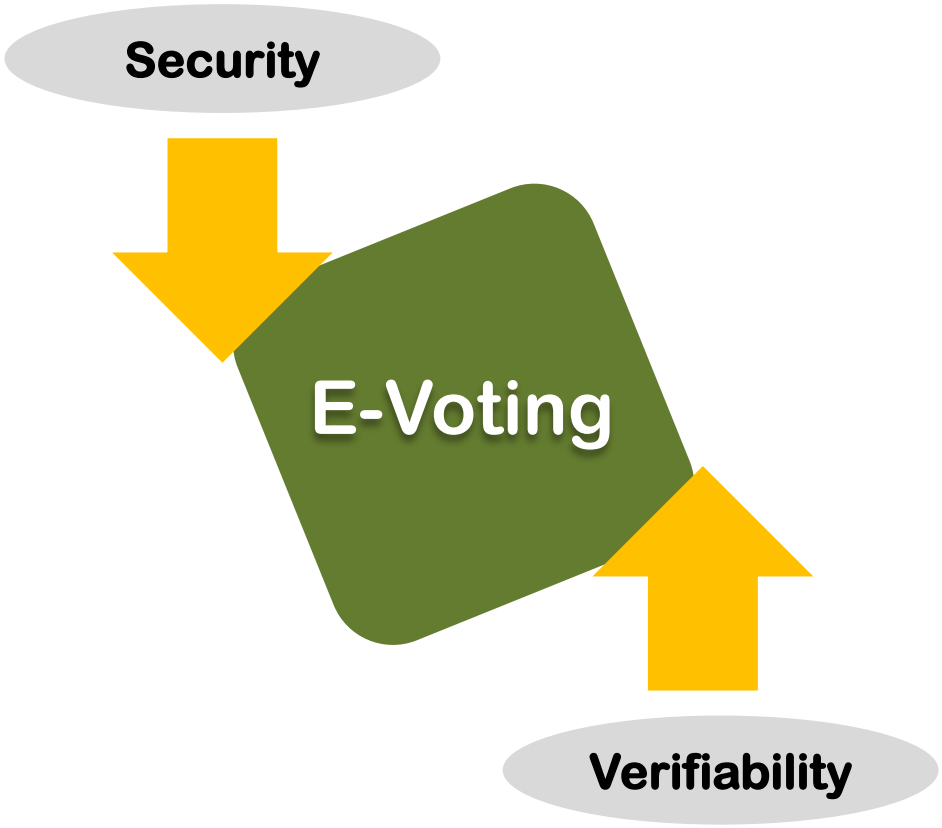
Functional Encryption

Zero-Knowledge Proof System

eVoting Protocols

Cryptographic Primitives

Verifiability



PhD Student

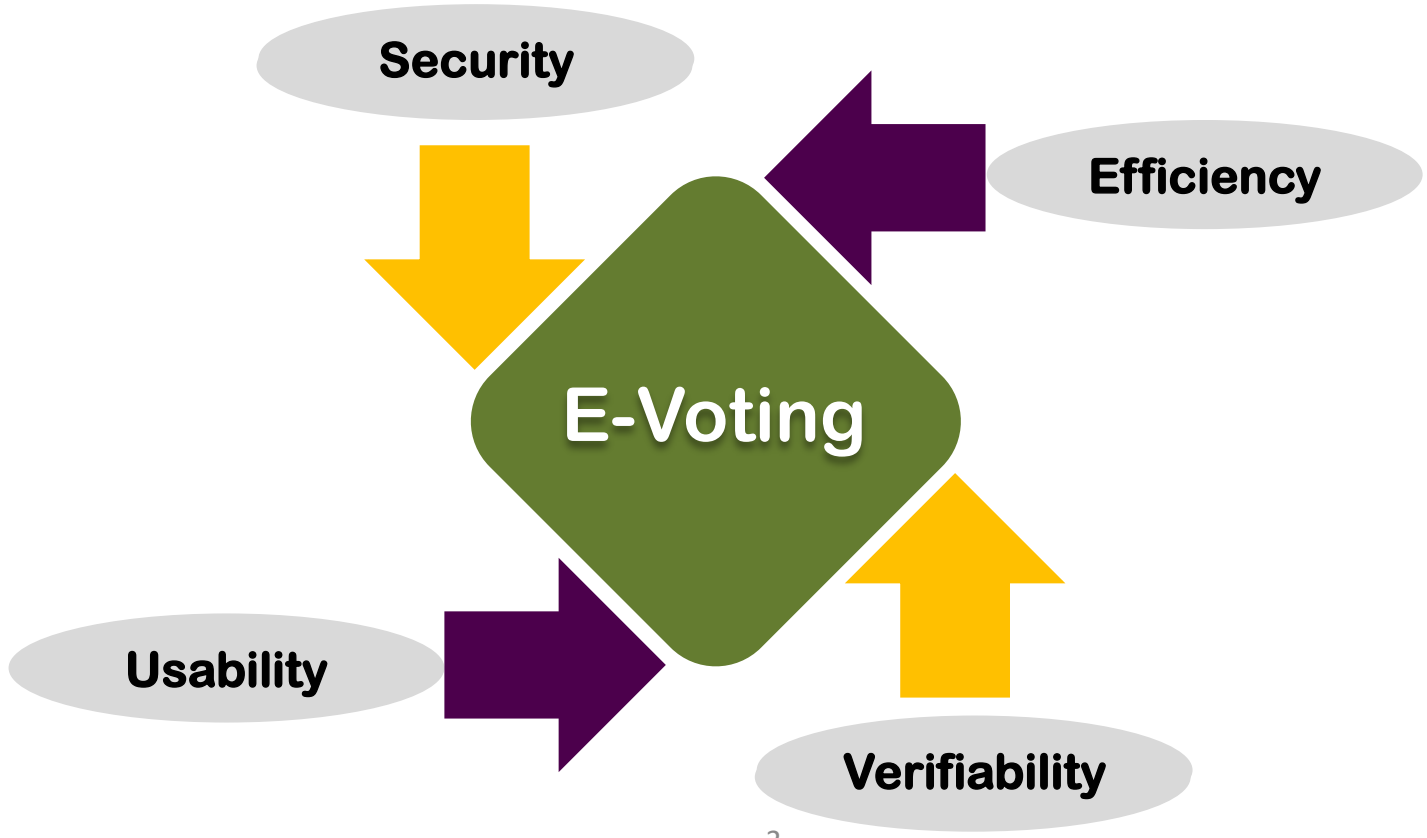
Functional Encryption

Zero-Knowledge Proof System

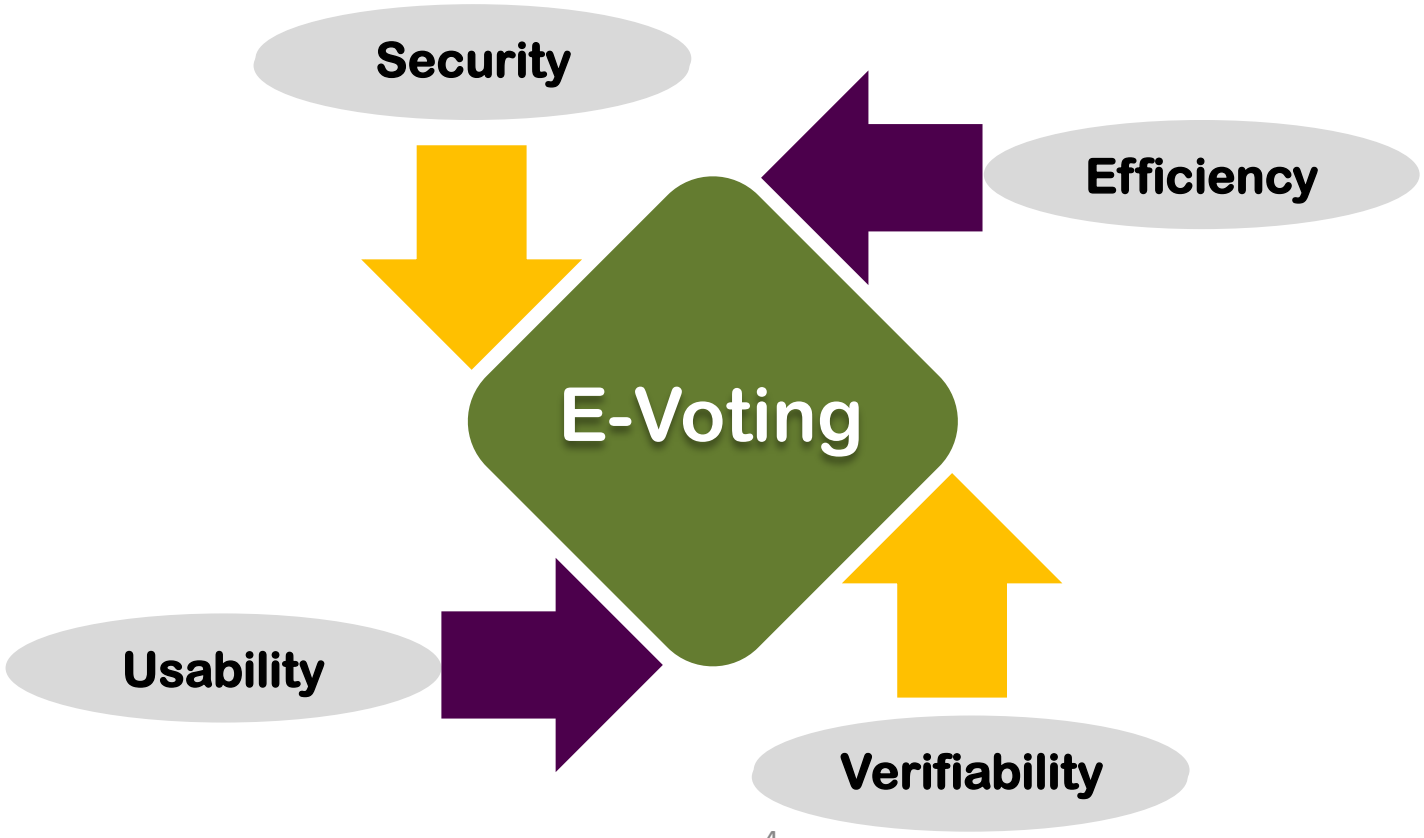
eVoting Protocols

Cryptographic Primitives

Verifiability



????
Secure verifiable Coercion-Resistance evoting Protocols



Coercion-Resistance Voting Protocol

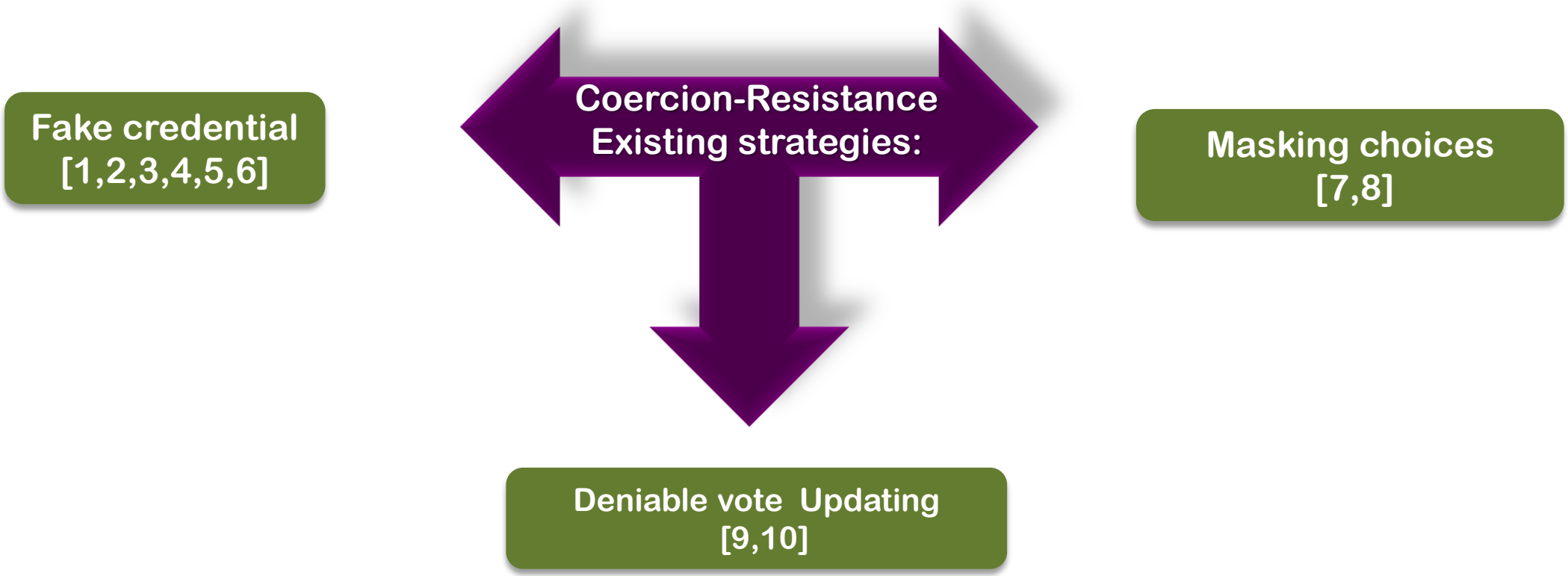
Obey the coercer and miss her chance to achieve her goal

NOT obey the coercer and getting the punishment

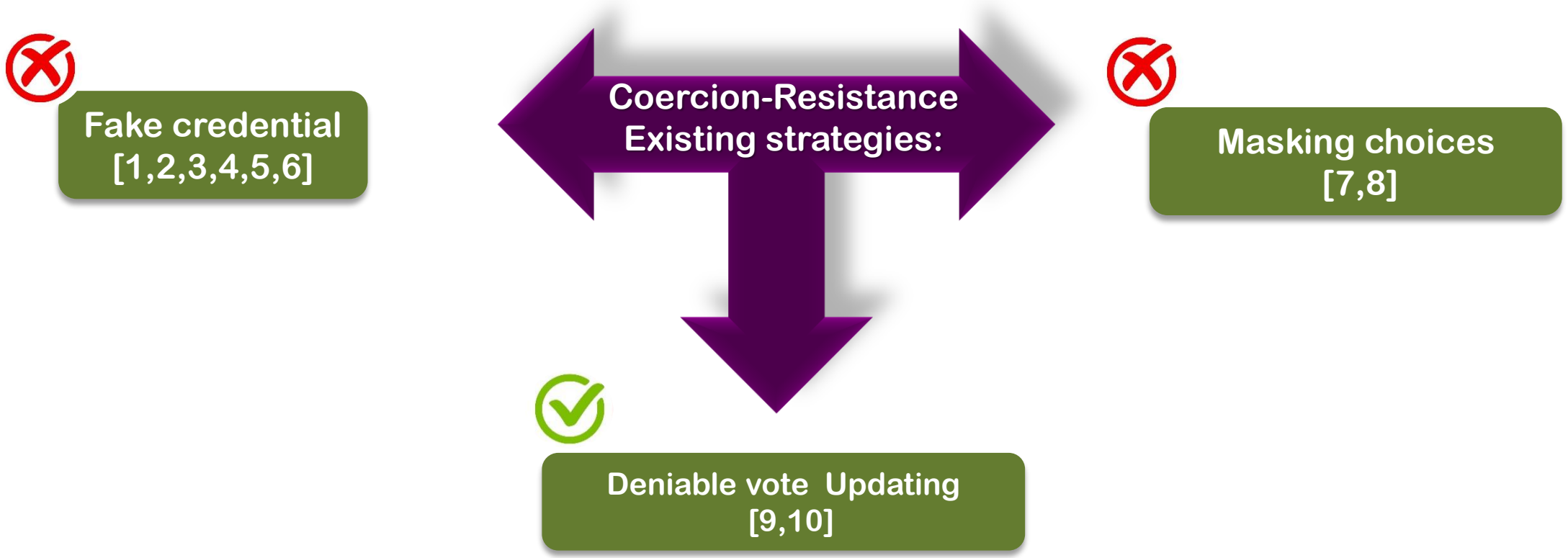
Run some counter-strategy instead of obeying the coercer

Voter achieves her own goal

the coercer should not able to distinguish whether the coerced voter followed his instructions or ran the counter-strategy



[1] Aleksander Essex, Jeremy Clark, and Urs Hengartner. Cobra: Toward Concurrent Ballot Authorization for Internet Voting.
[2] Roberto Araujo, Amira Barki, Solenn Brunet, and Jacques Traore. Remote Electronic Voting Can Be Ecient, Veriable and Coercion-Resistant.
[3] Jeremy Clark and Urs Hengartner. Selections: Internet Voting with Over-the- Shoulder Coercion-Resistance.
[4] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: Toward a Secure Voting System.
[5] Michael Schl apfer, Rolf Haenni, Reto E. Koenig, and Oliver Spycher. Ecient Vote Authorization in Coercion-Resistant Internet Voting.
[6] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections.
[7] Michael Backes, Martin Gagne, and Malte Skoruppa. Using mobile device communication to trengthen e-Voting protocols.
[8] Roland Wen and Richard Buckland. Masked Ballot Voting for Receipt-Free Online Elections.
[9] Wouter Lueks, I~nigo Querejeta-Azurmendi, and Carmela Troncoso. VoteAgain: A Scalable Coercion-Resistant Voting System
[10] Oksana Kulyk, Vanessa Teague, and Melanie Volkamer. Extending Helios Towards Private Eligibility Veriability.



[1] Aleksander Essex, Jeremy Clark, and Urs Hengartner. Cobra: Toward Concurrent Ballot Authorization for Internet Voting.
[2] Roberto Araujo, Amira Barki, Solenn Brunet, and Jacques Traore. Remote Electronic Voting Can Be Ecient, Veriable and Coercion-Resistant.
[3] Jeremy Clark and Urs Hengartner. Selections: Internet Voting with Over-the- Shoulder Coercion-Resistance.
[4] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: Toward a Secure Voting System.
[5] Michael Schl□apfer, Rolf Haenni, Reto E. Koenig, and Oliver Spycher. Ecient Vote Authorization in Coercion-Resistant Internet Voting.
[6] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections.
[7] Michael Backes, Martin Gagne, and Malte Skoruppa. Using mobile device communication to trengthen e-Voting protocols.
[8] Roland Wen and Richard Buckland. Masked Ballot Voting for Receipt-Free Online Elections.
[9] Wouter Lueks, I~nigo Querejeta-Azurmendi, and Carmela Troncoso. VoteAgain: A Scalable Coercion-Resistant Voting System
[10] Oksana Kulyk, Vanessa Teague, and Melanie Volkamer. Extending Helios Towards Private Eligibility Veriability.

Fake credential
[1,2,3,4,5,6]

Coercion-Resistance
Existing strategies:

Masking choices
[7,8]

Deniable vote Updating
[9,10]

Enables each voter to overwrite her previously submitted ballot, that she may have cast under coercion

[9] Quadratic Complexity in the number of voters

[10] Cumbersome for human voter

[9] Wouter Lueks, I˜nigo Querejeta-Azurmendi, and Carmela Troncoso. VoteAgain: A Scalable Coercion-Resistant Voting System
[10] Oksana Kulyk, Vanessa Teague, and Melanie Volkamer. Extending Helios Towards Private Eligibility Veriability.

Fake credential
[1,2,3,4,5,6]

Coercion-Resistance Existing strategies:

Masking choices
[7,8]

Deniable vote Updating
[9,10]

Enables each voter to overwrite her previously submitted ballot, that she may have cast under coercion

[9] Quadratic Complexity in the number of voters

[10] Cumbersome for human voter

Our Contribution

- ✓ Voters can deniably update their votes in an intuitive way.
- ✓ End-to-end verifiability and vote privacy are provably guaranteed without any additional trust assumptions besides the standards.
- ✓ Large-scale real-world elections can be realized efficiently.

Main Idea for Deniable Vote Updating

Cryptographic Primitevs:

IND-CPA -Secure Public Key Encryption Scheme :
Which support re-Encryption

Zero-Knowledge Proof Of Knowledge:
Which support Disjuction predicates

One Way Function :

Deniable Vote Updating eVoting Protocol:

Voter : $(Pk_{evoter}\ ,\ Sk_{evoter})$

$[Pk_{voter}, CT_0 = Enc(PK_{election}, 0)]$ (CT_1, π_1) (CT_2, π_2) (CT_3, π_3) (CT_i, π_i) (CT_{i+1}, π_{i+1})

$$\pi\ :\ P(x, w) = TRUE$$

$$[(CT_{i+1} = Enc(PK_{election}, vote)]$$

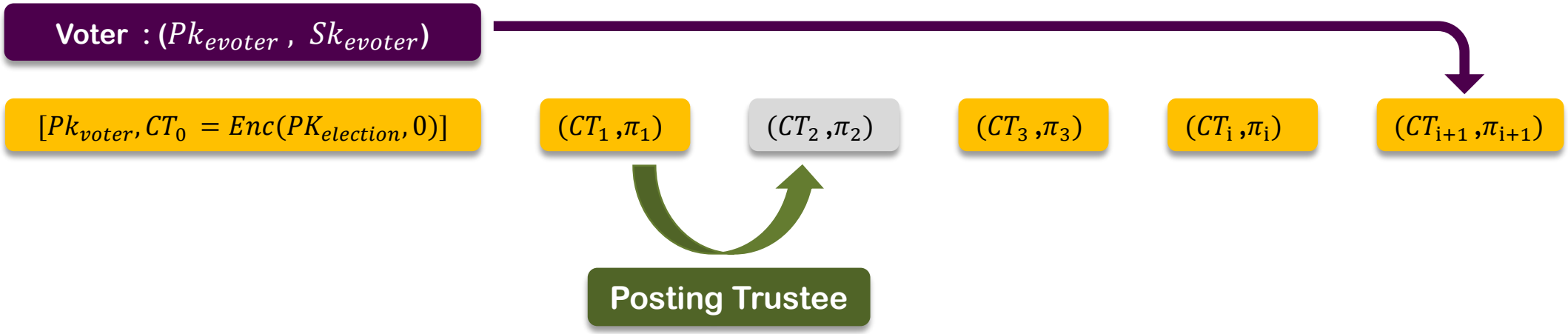
AND

$$[Proof\ Of\ Knowledge\ (Sk_{evoter})]$$

OR

$$[(CT_{i+1} = re - Enc(PK_{election}, (CT_i)]$$

Deniable Vote Updating eVoting Protocol:



$$\pi\ :\ P(x, w) = TRUE$$

$$[(CT_{i+1} = Enc(PK_{election}, vote)]$$

AND

$$[Proof\ Of\ Knowledge\ \ (Sk_{evoter})]$$

OR

$$[(CT_{i+1} = re - Enc(PK_{election}, (CT_i)]$$

Deniable Vote Updating eVoting Protocol:

Voter : $(Pk_{evoter}, Sk_{evoter})$

$[Pk_{voter}, CT_0 = Enc(PK_{election}, 0)]$ (CT_1, π_1) (CT_2, π_2) (CT_3, π_3) (CT_i, π_i) (CT_{i+1}, π_{i+1})

Tally

Defrential Privacy:

Indistinguishable

Deniable Vote Updating eVoting Protocol:

- Security
- Practical efficiency
- Intuitive counter strategy.

Futur Steps

- Combine with other evoting Scheme
- More efficient ZK such as NIWI (bilinear map)
- Instantiation in Post-Quantum primitives

we're all in this together