ENFORCING CONFIDENTIALITY IN TORNADO CASH-BASED E-VOTING SYSTEMS

STEFANO BISTARELLI, IVAN MERCANTI AND FRANCESCO SANTINI
ENFORCING CONFIDENTIALITY IN TORNADO CASH-BASED E-VOTING SYSTEMS

AGENDA

- Background
- Model
- Satisfied Properties
- Conclusion
BACKGROUND

THE ERC20 STANDARD
OUR MODEL

FIRST STEP

Admin

Deploy

Handle

User Identification

DTV (ERC20) token

Documentation

Fail

User
**OUR MODEL**

**PSEUDO-ANONYMIZATION**

Admin

Deploy

TornadoCash-Relayer SC

Set

Deposit expired time

Deposit 0.0015 ETH and 1 DTV

Receive a Nonce

User
OUR MODEL

PSEUDO-ANONYMIZATION

Deploy

TornadoCash-Relayer SC

Provide the Nonce

Withdraw 0.0015 ETH and 1 DTV

Admin

Set

Deposit expired time

User
OUR MODEL

VOTE ENCRYPTION

Candidates

Register

Public keys

Encrypt vote

Voting SC

Encrypt

Send 1 DTV to vote

Vote Webpage

User
OUR MODEL

VOTE COUNTING

Candidates -> Reveal -> Private keys -> Get votes -> Voting SC

Voting SC

Decryption

Admin

Decrypted Votes -> Counting

Admin
SATISFIED PROPERTIES

OUR PROPERTIES

- Verifiability
- Uniqueness
- Integrity
- Counting
SATISFIED PROPERTIES

OUR PROPERTIES

- Privacy
- Authentication
- Confidentiality
SATISFIED PROPERTIES

OUR PROPERTIES

- Lack of evidence

- Reliability
CONCLUSION AND FUTURE WORK

- Enforcing Confidentiality E-voting system
- Use distributed public key
- Implement a Web dApp
- Enforce more properties: Lack of evidence
- Enforce authentication: OAuth and OpenID protocol
Enforcing Confidentiality in Tornado Cash-based E-voting Systems

Stefano Bistarelli, Ivan Mercanti and Francesco Santini

THANKS FOR THE ATTENTION. QUESTIONS?

Email: ivan.mercanti@unipg.it