ARTEMIS

SOLVING THE SECURE PLATFORM PROBLEM FOR THE HELIOS E-VOTING SYSTEM

Bachelor thesis - Mike Boss

WELCOME

TO

MYTHOLOGY 101!

Zeus

Apollo

Helios

Artemis

Belenios

MYTH OF
SECURE E-VOTING

SECURITY?

SECURITY?

Verifiability

SECURITY?

Verifiability

+

Privacy

E-VOTING SYSTEM

1. Vote creation
2. Vote submission
3. Tally

E-VOTING SYSTEM

1. Vote creation
2. Vote submission
3. Tally

E-VOTING SYSTEM

1. Vote creation
2. Vote submission
3. Tally

E-VOTING SYSTEM

1. Vote creation
2. Vote submission
3. Tally

3. Tally

HOMOMORPHIC TALLYING

$$\{1\}_k + \{0\}_k + \{1\}_k = \{2\}_k$$

ZKP: 0 or 1

3. Tally

RE-ENCRYPTION MIX-NET

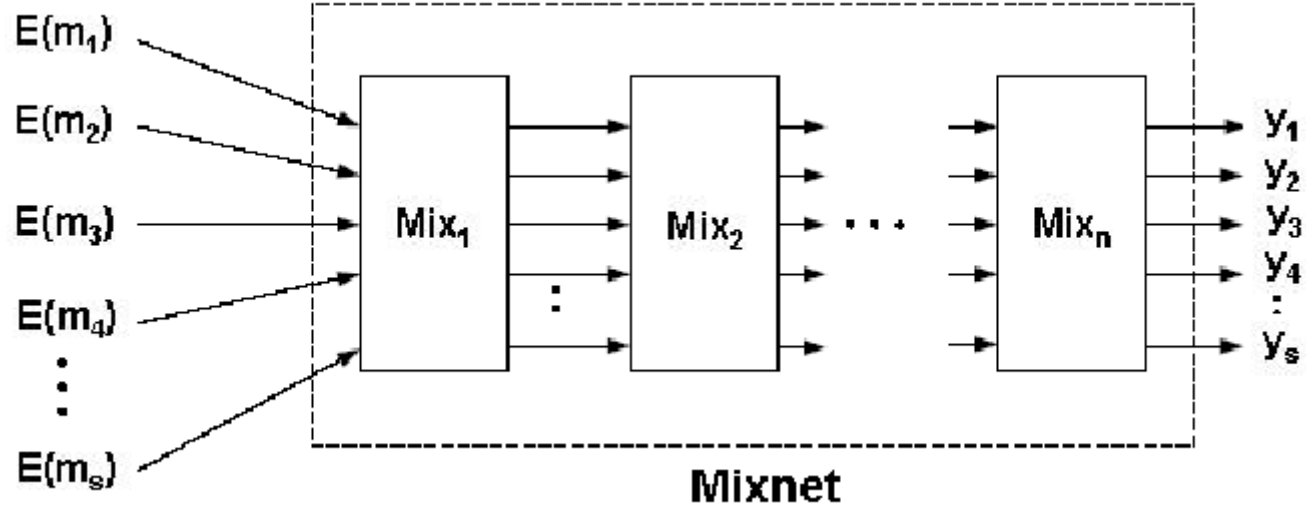
3. Tally

RE-ENCRYPTION MIX-NET

3. Tally

RE-ENCRYPTION MIX-NET

RE-ENCRYPTION MIX-NET



FIRST THERE WAS

HELIOS

1. Vote creation	Benaloh Challenge
2. Vote submission	Just send
3. Tally	Homomorphic tallying

BENALOH CHALLENGE

(Voter-initiated-audit)

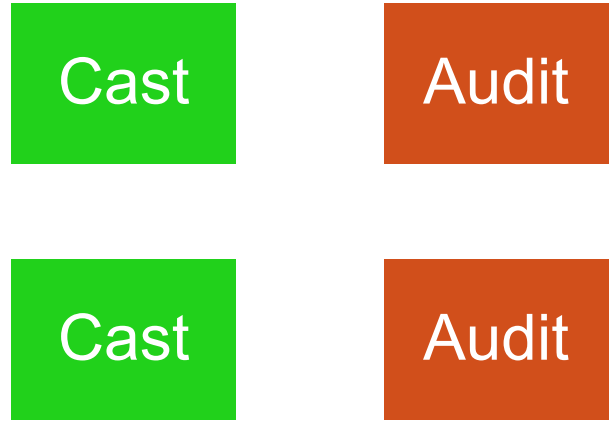
$$\{Alice\}_k$$

Cast

Audit

BENALOH CHALLENGE

(Voter-initiated-audit)



BOOTH AUDIT => SECURITY 

BOOTH AUDIT => SECURITY 

LOCAL AUDIT => SECURITY ✕

HELIOS

HELIOS

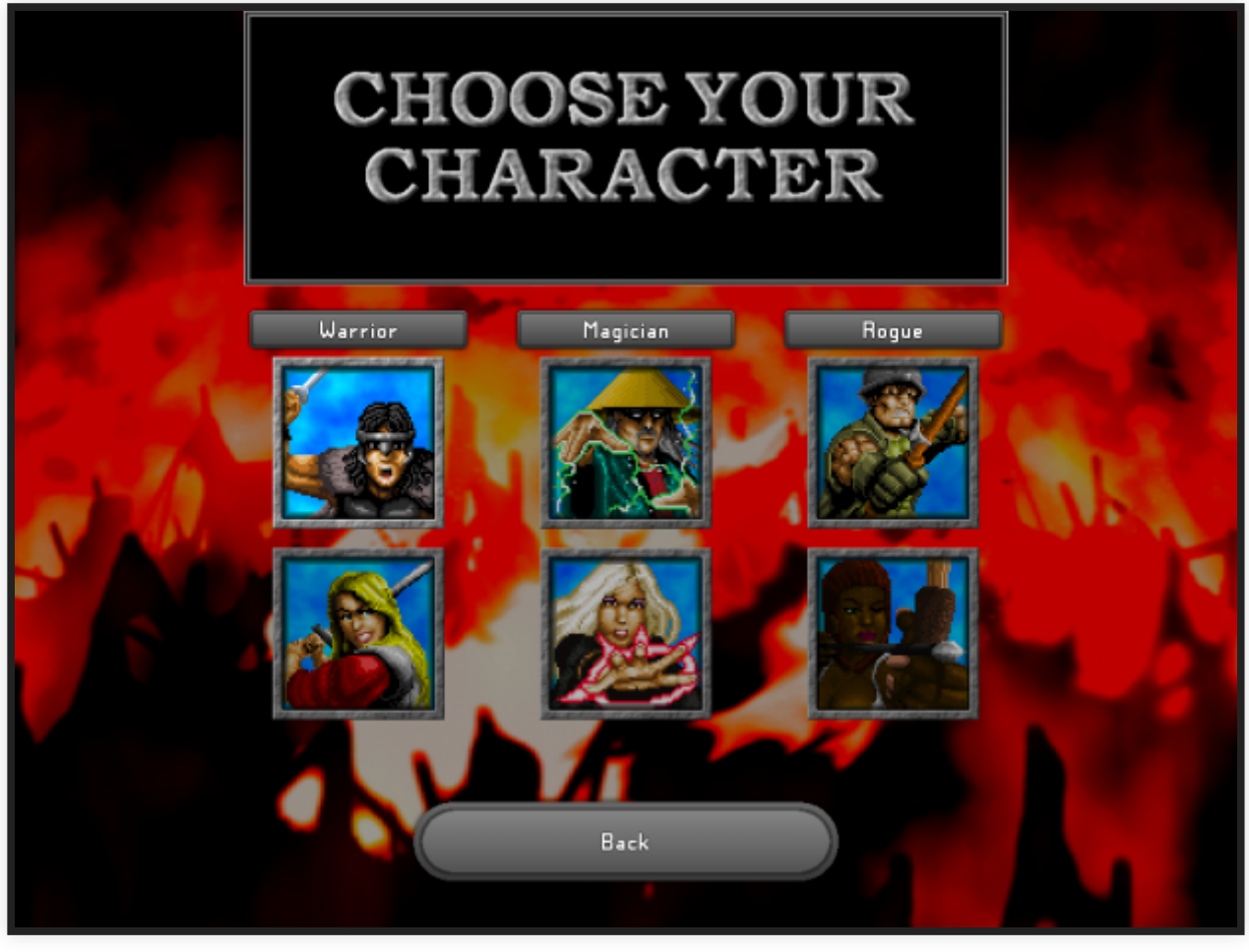
HELIOS

HELIOS

HELIOS


A
ARTEMIS

PLAYERS



PLAYERS

1. Voting terminal 
2. Active voting assistant 
3. Voting assistant(s) 

4. Tallying authority
5. Registrar

PLAYERS

1. Voting terminal 
2. Active voting assistant 
3. Voting assistant(s) 

4. Tallying authority
5. Registrar

PLAYERS

1. Voting terminal 
2. Active voting assistant 
3. Voting assistant(s) 

4. Tallying authority
5. Registrar

PLAYERS

1. Voting terminal 
2. Active voting assistant 
3. Voting assistant(s) 

4. Tallying authority
5. Registrar

PLAYERS

1. Voting terminal 
2. Active voting assistant 
3. Voting assistant(s) 

4. Tallying authority
5. Registrar

PLAYERS

1. Voting terminal 
2. Active voting assistant 
3. Voting assistant(s) 

4. Tallying authority
5. Registrar

1. VOTE CREATION

1. **Audit on multiple devices** => Security
2. **Interactive creation of indirection** => Privacy

INDIRECTION

Alice	↔	🟩	🟦	↔	l7ngr2d
Bob	↔	🟥	🟥	↔	l02JfTp
Charlie	↔	🟦	🟩	↔	d38Gnd

Problem

 can tell which ballot  submitted

Problem

 can tell which ballot  submitted

Solution

RE-ENCRYPTION

-  for privacy
-  for receipt-freeness

RE-ENCRYPTION

1.  →  →  :

$\{1\}_k^1$ ↔ 

$\{0\}_k^1$ ↔ 

2.  → 

$\{0\}_k^2$

3.  → 

$\{0\}_k^3$

2. VOTE SUBMISSION

TWO AUTHORITES

4. Registrar
5. Tallying authority

TWO AUTHORITES

- Against ballot stuffing
- Against malicious voting terminal

REGISTRAR

sends to all voters

1. Cast codes
2. Lock-in code

SUBMITTING A VOTE

Enter **cast code** => ☑ ? => Enter **lock-in code**

WHY ☑ ?

💻 switches ballot with entered cast code

WHY ☑ ?

💻 switches ballot with entered cast code

Enter lock-in code only if same ballot

3. TALLY

Mix-net => No change

Homomorphic tally => ZKP's invalid ✗

3. TALLY

Mix-net => No change

Homomorphic tally => ZKP's invalid ✗

Groth-Sahai proofs re-randomizable ✓

CONCLUSION

ARTEMIS

PRIVAPOLLO

Multiple devices

Indirection

BELENIOSRF

Re-encryption

Receipt-freeness

PROTOCOL

- Security + Privacy
- Receipt-freeness
- More election modes than BeleniosVS
- Easier to implement

- Benaloh Challenge

IMPLEMENATION

- Functional

- Helios code base
- Not finished