CROSS-PLATFORM MOBILE APPLICATION FOR THE COTHORITY

Sacha Kozma
June 12, 2018

Decentralized and Distributed Systems lab, EPFL

Responsible Prof. Bryan Ford
Supervisor Linus Gasser
1 CPMAC Presentation
2 Improvements
3 Proof-of-Personhood Presentation
   PoP in CPMAC
4 Linkable Ring Signatures
5 BeerCoin Presentation
   Drawback
6 Demo
7 Conclusion
What is CPMAC?

iOS and Android application used for Cothority.
What is CPMAC?

iOS and Android application used for Cothority.

- Proof-of-Personhood
- CISC Identity Skipchain

Cothority applications

Conode
iOS and Android application used for Cothority.

Currently supported applications:

- Status
- Proof-of-Personhood
- Cisc Identity SkipChain

Built on top of NativeScript.
1 CPMAC Presentation
2 Improvements
3 Proof-of-Personhood
   Presentation
   PoP in CPMAC
4 Linkable Ring Signatures
5 BeerCoin
   Presentation
   Drawback
6 Demo
7 Conclusion
Work has been done on several points:

- PoP-Parties
  - Attendees support
  - Configuration sharing
- Usability
  - User Interface
  - Process simplifications
- New feature: BeerCoin
3 Proof-of-Personhood

Presentation

PoP in CPMAC

4 Linkable Ring Signatures

5 BeerCoin

Presentation

Drawback

6 Demo

7 Conclusion
Organizers agree on the party details
Proof-of-Personhood

Conodes

Organizers

Attendees
Proof-of-Personhood

Conodes

Organizers

Attendees
Proof-of-Personhood

Conodes

Organizers

Attendees
Proof-of-Personhood

Conodes

Organizers

Attendees
At the end of the party, the conodes generate:

\[ \text{Final statement} \]

And each attendee can generate:

\[ \text{Final statement} + \text{attendee’s key pair} = \text{PoP-Token} \]
1 CPMAC Presentation
2 Improvements
3 Proof-of-Personhood
   Presentation
   PoP in CPMAC
4 Linkable Ring Signatures
5 BeerCoin
   Presentation
   Drawback
6 Demo
7 Conclusion
Until now, CPMAC used PasteBin to share the party description to the other organizers.
Until now, CPMAC used PasteBin to share the party description to the other organizers.

This approach has drawbacks:

- Depends on third-party services
- Party description is publicly available
Until now, CPMAC used PasteBin to share the party description to the other organizers.

This approach has drawbacks:

- Depends on third-party services
- Party description is publicly available

Instead, adapt Cothority to use conodes!
Party description sharing with PasteBin

1. Upload party description
2. Send PasteBin link with QR Code
3. Fetch party description
Party description sharing with PasteBin

1) Upload party description

Organizer 1

PasteBin

Organizer 2
Party description sharing with PasteBin

1) Upload party description

2) Send PasteBin link with QR Code
Party description sharing with PasteBin

1) Upload party description

2) Send PasteBin link with QR Code

3) Fetch party description
PARTY DESCRIPTION SHARING WITH CONODES

1) Upload description
2) Description is propagated
3) Fetch party proposal
1) Upload description
1) Upload description

2) Description is propagated
Party description sharing with conodes

1) Upload description

2) Description is propagated

3) Fetch party proposal
1 CPMAC Presentation
2 Improvements
3 Proof-of-Personhood Presentation
4 PoP in CPMAC
4 Linkable Ring Signatures
5 BeerCoin Presentation
6 Drawback
6 Demo
7 Conclusion
Linkable Ring Signatures

Ring Signatures:

• Allow a user to sign on behalf of a group
• One can verify that someone from this group effectively signed the data
• But he cannot know which member precisely
Ring Signatures:

- Allow a user to sign on behalf of a group
- One can verify that someone from this group effectively signed the data
- But he cannot know which member precisely

Linkable Ring Signatures:

- Same as ring signatures
- But a linkage scope can be defined, and the verification process will then yield a tag, which is unique to the signer under that scope
A long-running joke at DEDIS!

BeerCoins are distributed in a group and each day/month/week they can have a beer. In CPMAC, it’s called a Bar.

It allows showing a simple example of what could be done with the current primitives implemented in CPMAC.
A long-running joke at DEDIS!

BeerCoins are distributed in a group and each day/month/week they can have a beer. In CPMAC, it’s called a Bar.

It allows showing a simple example of what could be done with the current primitives implemented in CPMAC.

Each member of the group gets a PoP-Token and the Bar uses linkable ring signatures to verify it.
In the case of BeerCoin, the scope should be unique for each Bar and each period:

\[
\text{scope} = \text{bar\_name} || \text{frequency} || \text{year} || \text{month} || \text{day}
\]

\[
frequency \in \{\text{daily, weekly, monthly}\}
\]
Linkable Ring Signatures: Client verification

Bar

QR Code [nonce, scope]

Generates and remembers the tag

Client

Signs with linkable ring signature

QR Code [signature]
1. CPMAC Presentation
2. Improvements
3. Proof-of-Personhood Presentation
   PoP in CPMAC
4. Linkable Ring Signatures
5. BeerCoin Presentation
   Drawback
6. Demo
7. Conclusion
Drawbacks

One major drawback comes from the association of QR Code with linkable ring signatures:

- Length of signatures is proportional to the number of member in the group
- But QR Code has fixed capacity

Actually, CPMAC could handle a maximum of 90 members per group.
Demo time!
CPMAC is increasingly becoming a large public app.
The primitives currently added allows some interesting applications:

- Voting system
- Online chat
- Authentication
- and many more
Questions ?