Rate-Limiting Nullifier

A ZK Gadget to Prevent Spam in Anonymous Environments

Tyler [ AtHeartEngineer ]
Privacy and Scaling Explorations Team
Rate-Limiting Nullifier TLDR

Semaphore Groups [Registry]

Shamir’s Secret Sharing [SSS]

Time / Event Delineation [Epoch]

Registration [Anonymity Set]

Signaling [Sending Messages]

Secret Recovery / Slashing [Using SSS]
Registration

[ Binary Merkle Tree of Identity Commitments ]

- Secret Key
- Poseidon Hash
- Identity Commitment

Membership
Merkle Tree

IDn  IDn+1  IDn+2  IDn+3
Signaling
(ex: Generating a Proof to Send a Message)

- Epoch [public]
- Message [public]
- Secret Key
- RLN Circuit Generates proof [zk-snark]
- ZK Proof
  - Epoch
  - Message
  - Membership
  - Secret Share
ELI12 Shamir’s Secret Sharing Secret

\[ f(x) = mx + b \]
ELI12 Shamir’s Secret Sharing
Random Point

\[ f(x) = mx + b \]
ELI12 Shamir’s Secret Sharing
Share Generation

\[ f(x) = mx + b \]
ELI12 Shamir’s Secret Sharing
Single Share

\[ f(x) = mx + b \]
ELI12 Shamir’s Secret Sharing
Secret Recovery

\[ f(x) = mx + b \]
ELI12 Shamir’s Secret Sharing
Secret Recovery

\[ f(x) = mx + b \]
ELI12 Shamir’s Secret Sharing
Beyond Linear

(0,516)
Secret

Share

Share

Share

Random Point
[ Derived From Epoch ]
RLN Circom Circuit

- Epoch
- Poseidon Hash
- RLN Identifier
- a1
- Poseidon Hash
- Nullifier
- Message
- Poseidon Hash
- Secret Key
- Poseidon Hash
- Identity Commitment
- Membership Merkle Tree
- IDn
- IDn+1
- IDn+2
- IDn+3
Use Cases

- Anonymous Messaging [ chat / email ]
  - $N$ message(s) per minute

- Auctions [ ebay / defi ]
  - $N$ bid(s) per user

- Bulletin-Board [ reddit / twitter ]
  - $N$ comment(s) per post

- Denial of Service Attack Prevention [ cloudflare ]
  - $N$ request(s) per second

Tools

- RLNjs
- Circom circuits
- Zerokit (Rust library by the Vac team)

github.com/Rate-Limiting-Nullifier
Documentation / Libraries
Thank you!

Tyler [ AtHeartEngineer ]
Privacy & Scaling Explorations

Questions?