17/WAKU2-RLN-RELAY: Privacy-Preserving Peer-to-Peer Economic Spam Protection

Sanaz Taheri Boshrooyeh (Presenter)*

Oskar Thoren*

Barry Whitehat

Wei Jie Koh

Onur Kilic

Kobi Gurkan

*Vac Research and Development

*Status Research and Development, Singapore

Link to the paper:
https://github.com/vacp2p/research/blob/master/rln-research/Waku_RLN_Relay.pdf

Contents

- WAKU2
- WAKU2-RELAY: Privacy-preserving p2p transport protocol
- Spam issue in WAKU2-RELAY
- Privacy-Preservation and Spam protection
- State-of-the-art p2p spam protections
- WAKU2-RLN-RELAY: Privacy-Preserving Peer-to-Peer Economic Spam Protection
- Future work

WAKU2 [1]

- A family of modular, privacy-preserving peer-to-peer (p2p) protocols for private, secure, censorship resistant communication
- Suitable for resource restricted devices e.g., mobile phones
- WAKU2 protocols include:
  - **WAKU2-RELAY: privacy-preserving transport**
  - WAKU2-STORE: historical message storage
  - WAKU2-FILTER: light version of WAKU2-RELAY for bandwidth limited devices
  - **WAKU2-RLN-RELAY: spam-protected version of WAKU2-RELAY**
  - And many more …
- For the full list of RFCs is available in rfc.vac.dev

[1] https://rfc.vac.dev/spec/10/

WAKU2-RELAY [1]

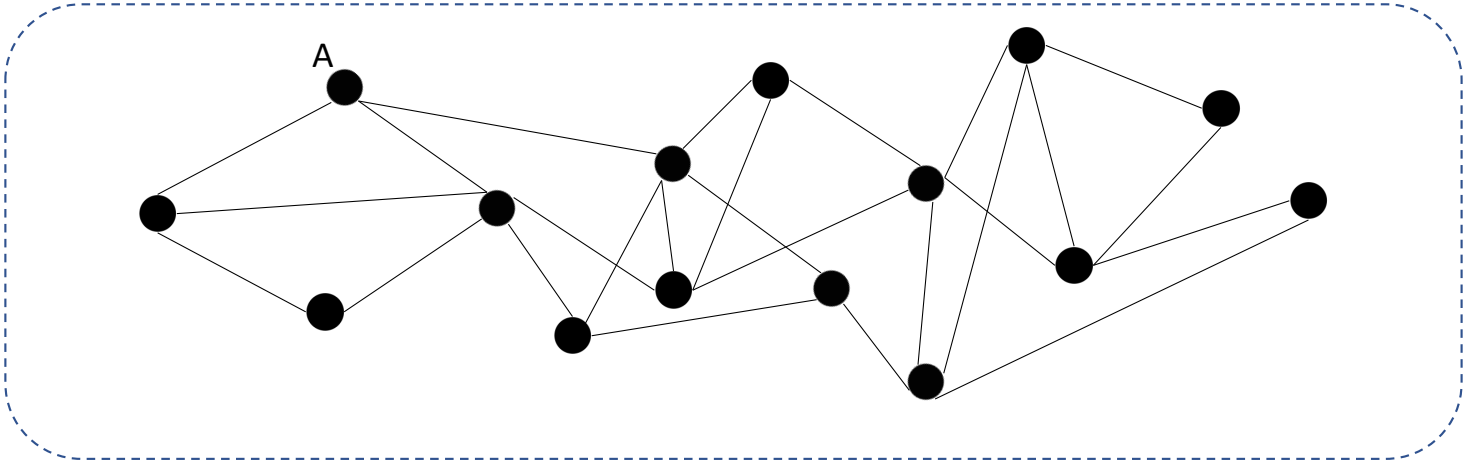
- Publisher-Subscriber Model
- Gossip-based Routing (extension of libp2p GossipSub-v1.1 [2])
- Anonymous and Privacy-Preserving

[1] https://rfc.vac.dev/spec/11/
[2] https://github.com/libp2p/specs/tree/master/pubsub/gossipsub

WAKU2-RELAY

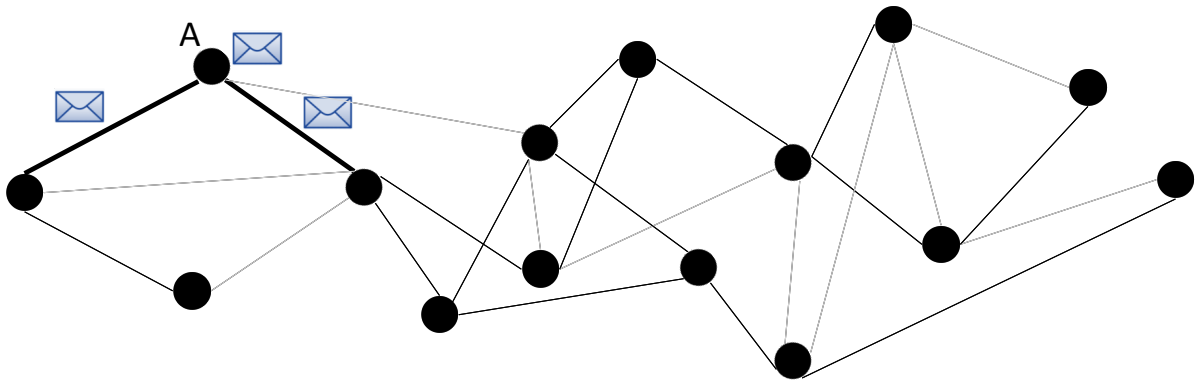
- Peers subscribed to the same topic form a mesh

Mesh of peers subscribed to the same topic



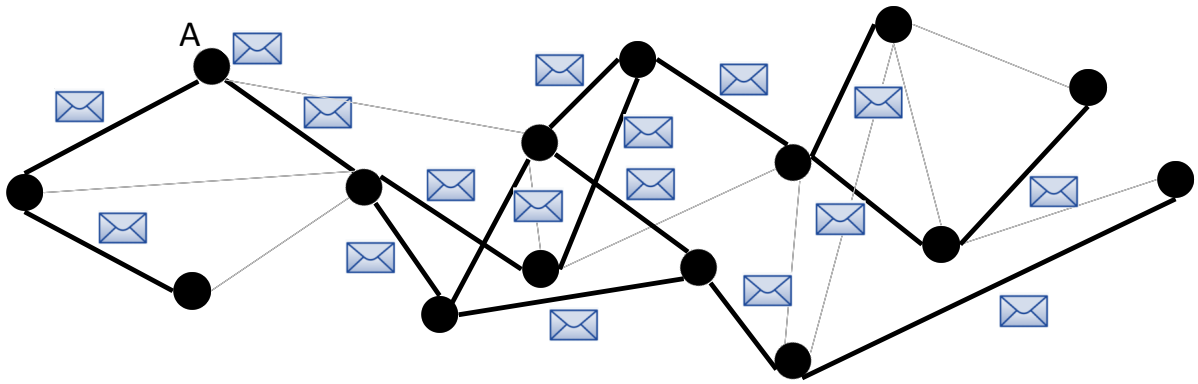
WAKU2-RELAY

- Peers subscribed to the same topic form a mesh
- Peers route messages by sending them to a subset of their connections



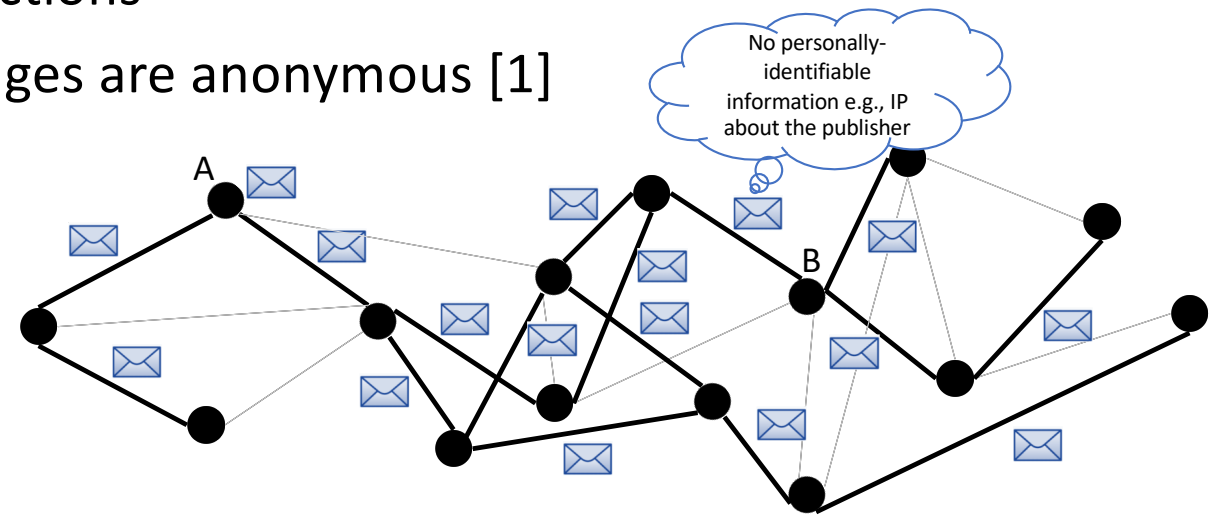
WAKU2-RELAY

- Peers subscribed to the same topic form a mesh
- Peers route messages by sending them to a subset of their connections



WAKU2-RELAY

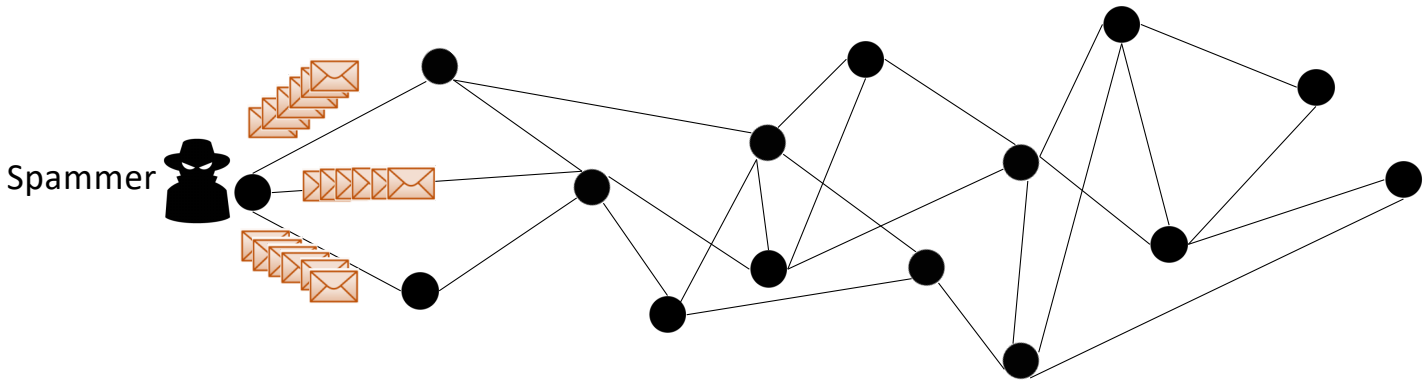
- Peers subscribed to the same topic form a mesh
- Peers route messages by sending them to a subset of their connections
- Messages are anonymous [1]



[1] https://rfc.vac.dev/spec/11/#security-analysis

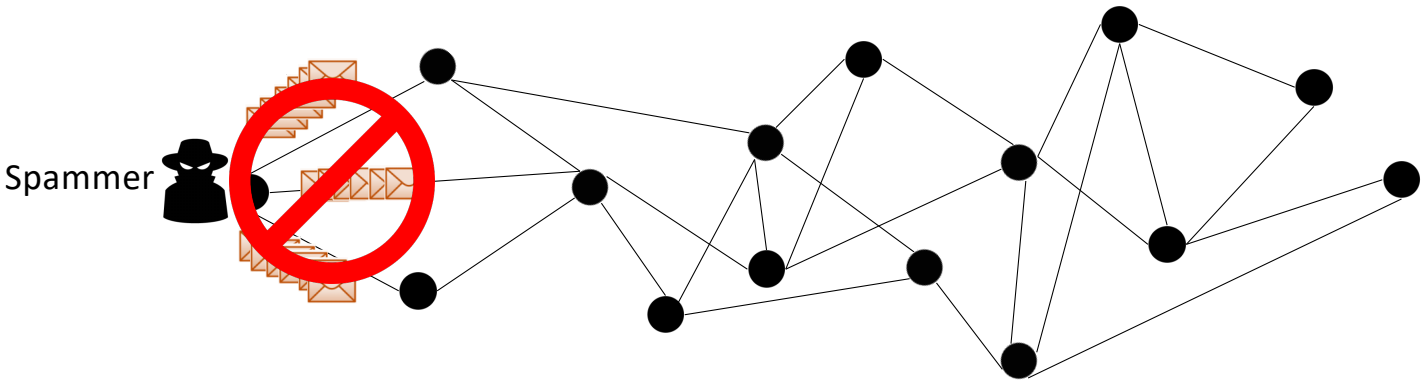
Spam issue in WAKU2-RELAY

- We define spammers as entities that publish a large number of messages in a short amount of time, and cause denial-of-service



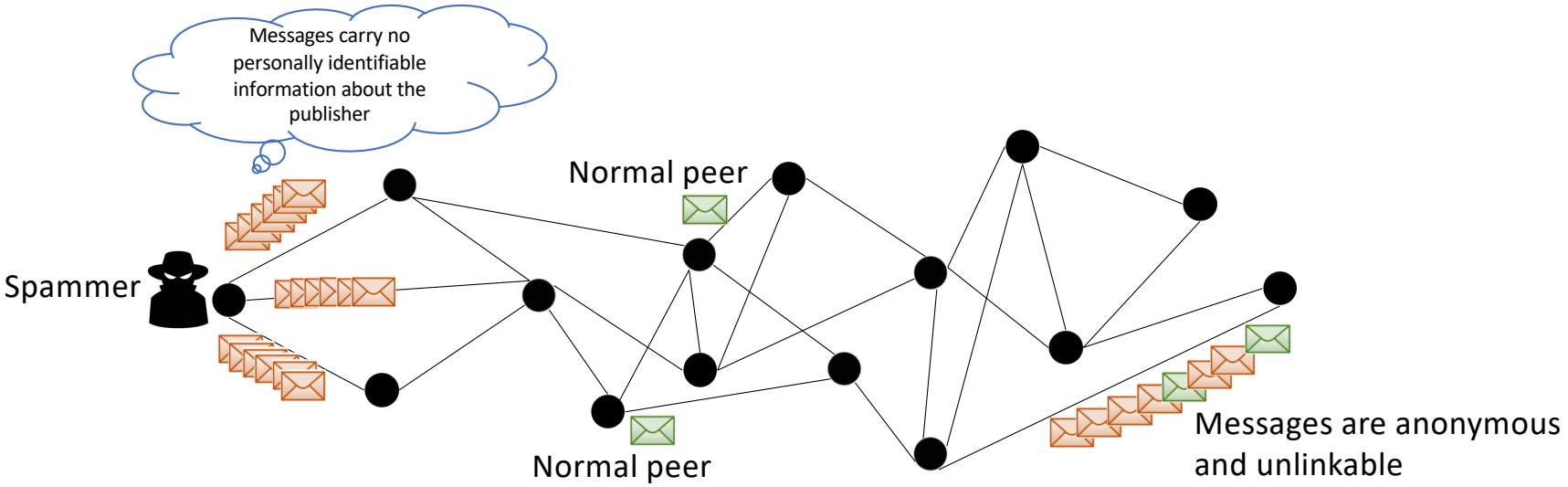
Spam issue in WAKU2-RELAY

- We define spammers as entities that publish a large number of messages in a short amount of time, and cause denial-of-service
- Spam Protection = Controlled Messaging Rate



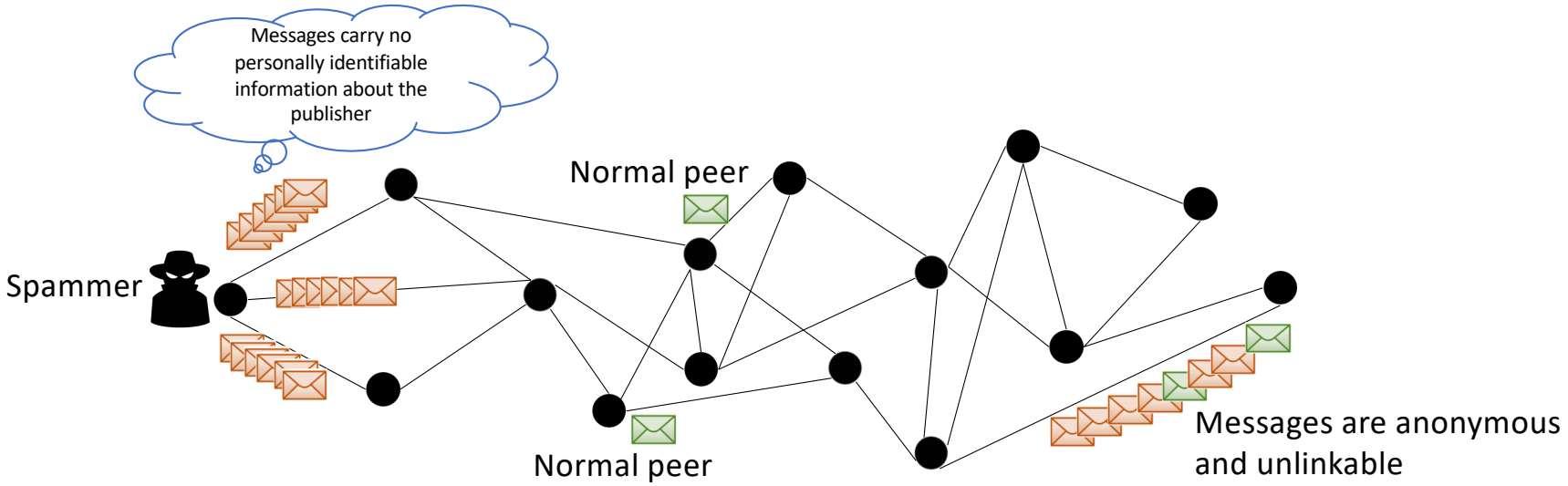
Privacy-Preservation and Spam protection

- Messages are anonymous: No Personally Identifiable information is available



Privacy-Preservation and Spam protection

- Messages are anonymous: No Personally Identifiable information is available
- Solutions like IP blocking are not effective



State-of-the-art p2p spam protections

- Proof-of-work [1] deployed by Whisper [2]
  - Computationally expensive
  - Not suitable for network of heterogeneous peers with limited resources
- Peer Scoring [3] in libp2p
  - Local to each peer
  - No global identification of spammer
  - Subject to inexpensive attacks using bots
  - Prone to censorship

[1] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Annual 456 international cryptology conference. Springer, 1992.
[2] https://eips.ethereum.org/eips/eip-627.
[3] https://github.com/libp2p/specs/blob/master/pubsub/gossipsub/gossipsub-v1.1.mdpeerscoring.

WAKU2-RLN-RELAY [1]

WAKU2-RLN-RELAY = WAKU2-RELAY + Rate Limiting Nullifiers (RLN)

- P2p solution
- Global spam protection
- Privacy preserving
- Efficient
- Economic incentives

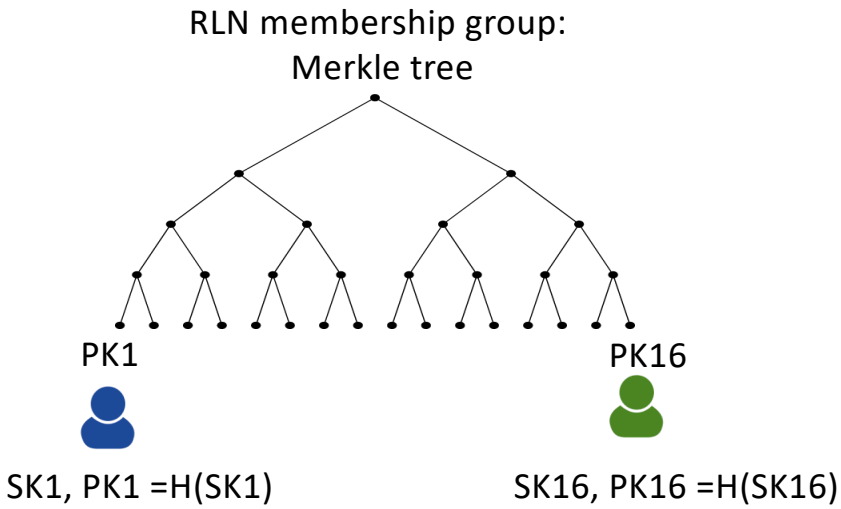
[1] https://rfc.vac.dev/spec/17/

RLN Primitive [1]

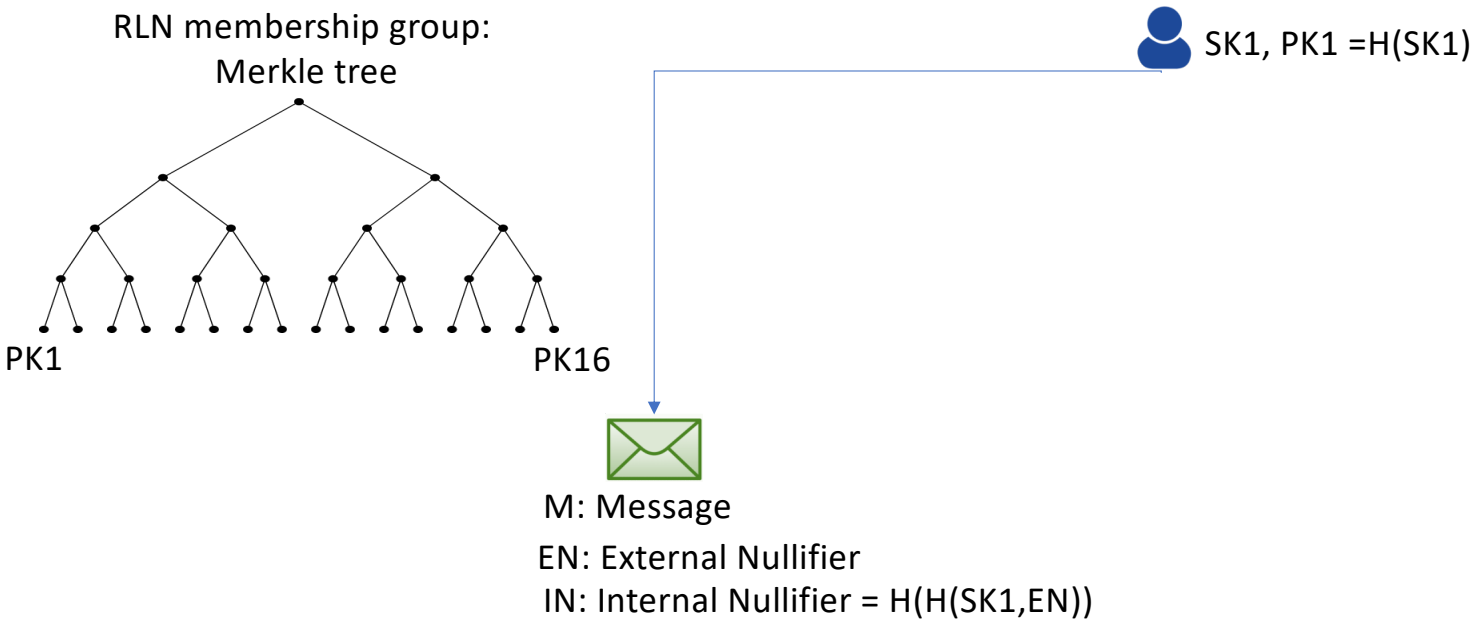
- RLN is a zero-knowledge and rate-limited signaling framework
- Each user can only send M messages for each External Nullifier
- External nullifier can be seen as a voting booth where each user can only cast one vote
- M and external nullifier are application dependent
- M=1 for this presentation

[1] https://ethresear.ch/t/semaphore-rln-rate-limiting-nullifier-for-spam-prevention-in-anonymous-p2p-setting/5009

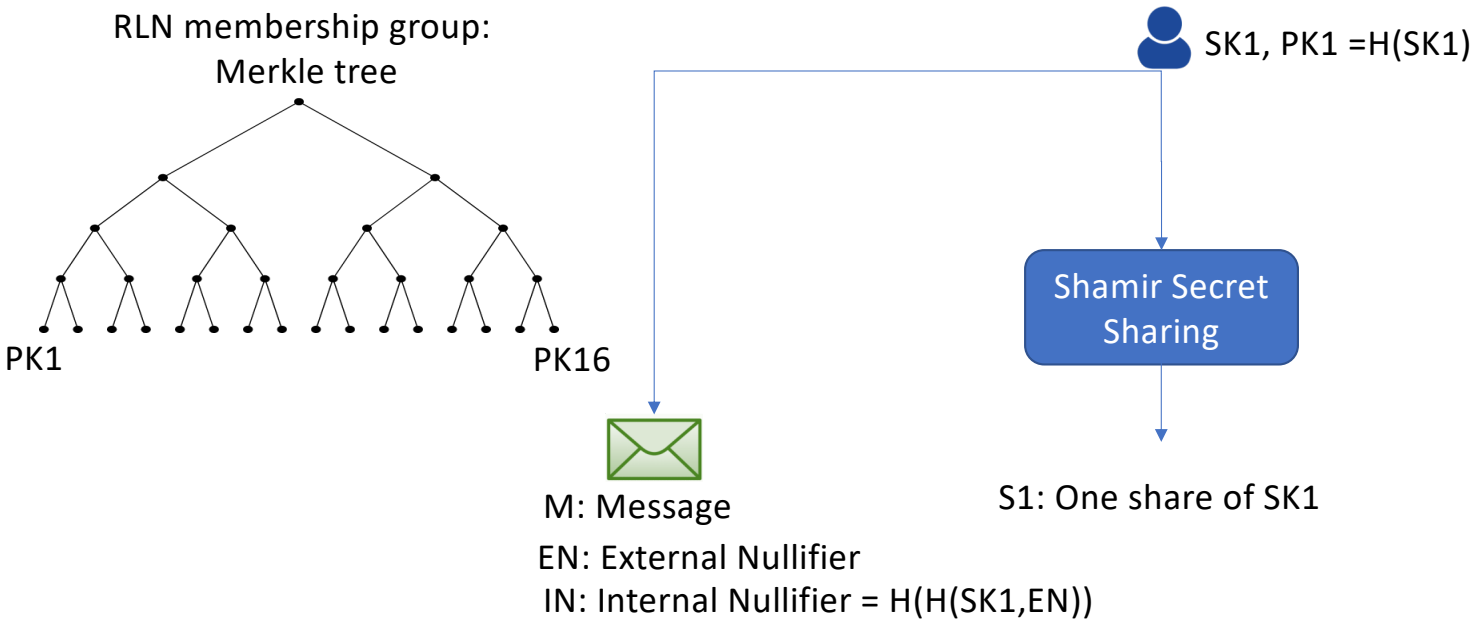
RLN Primitive: Membership Tree



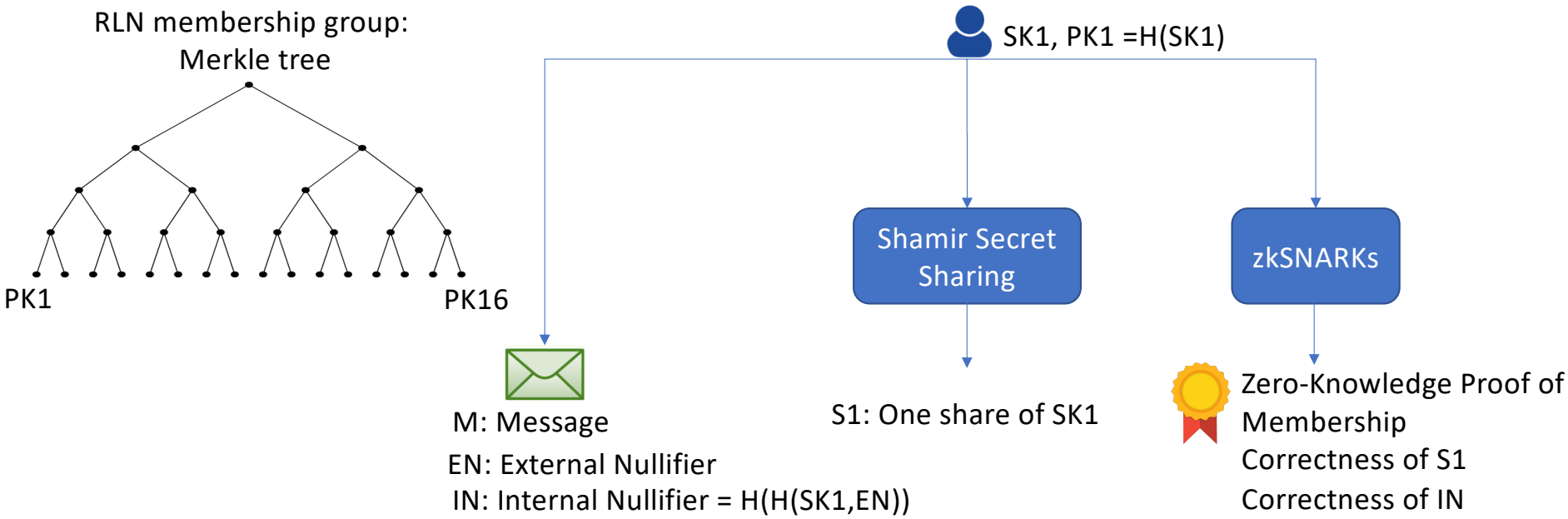
RLN Primitive: Signaling



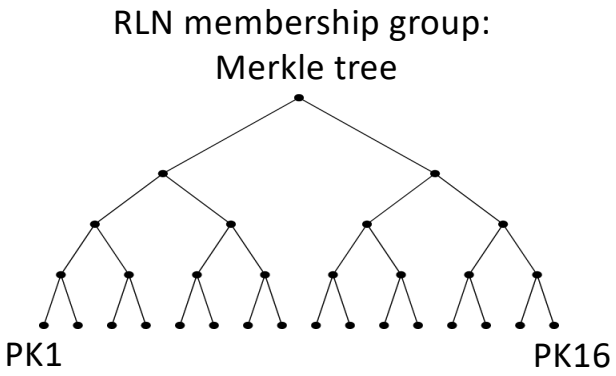
RLN Primitive: Signaling

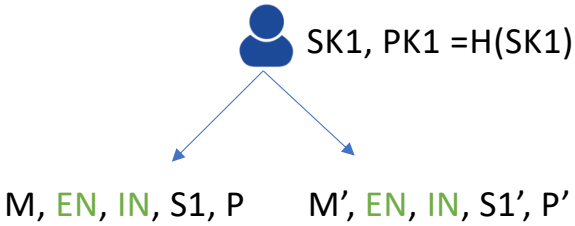


RLN Primitive: Signaling

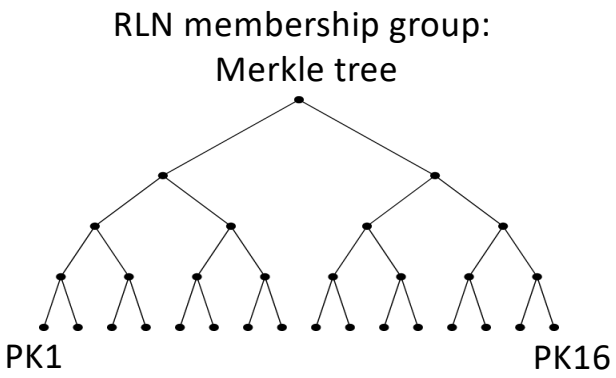


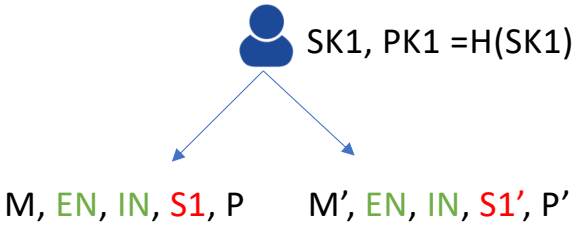
RLN Primitive: Detecting double signaling



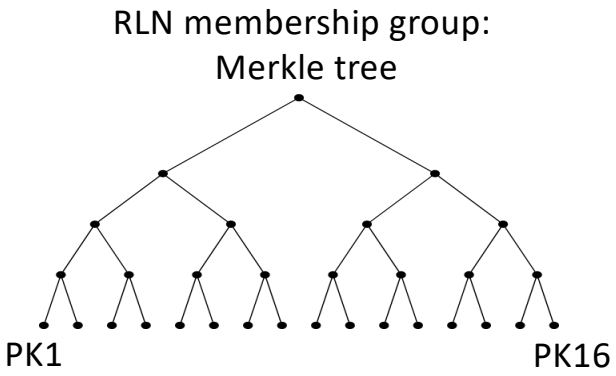


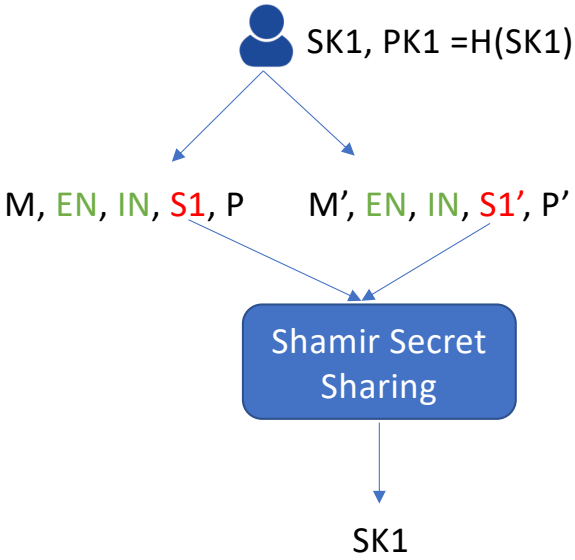
RLN Primitive: Detecting double signaling



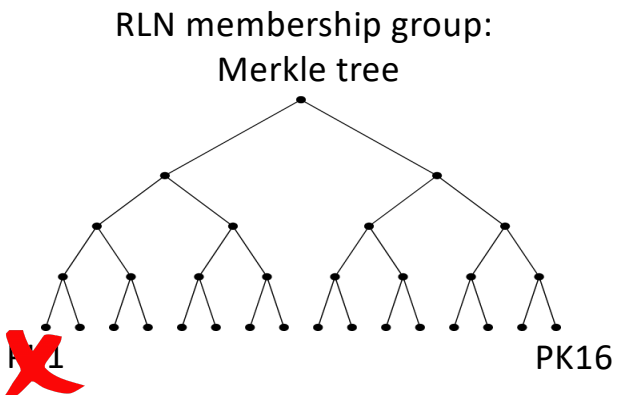


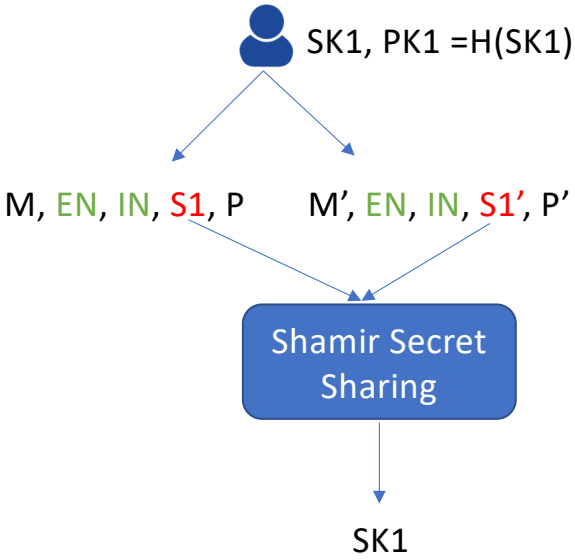
RLN Primitive: Detecting double signaling





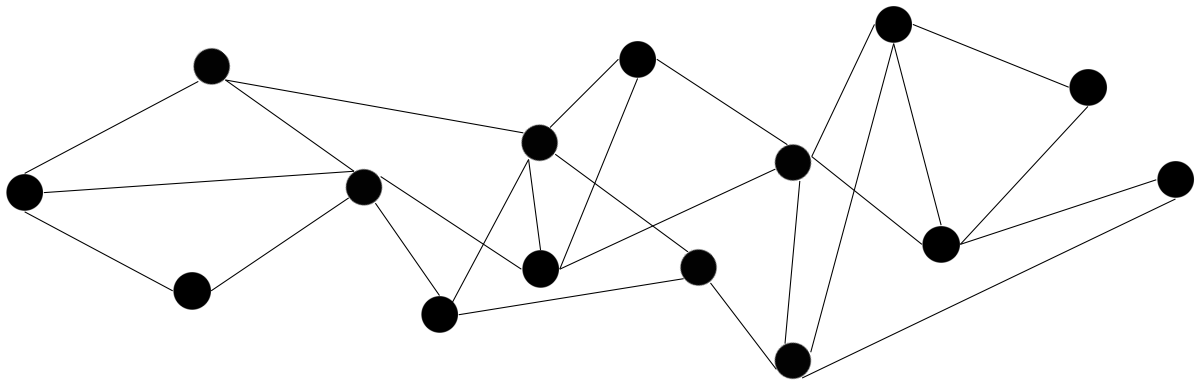
RLN Primitive: Detecting double signaling



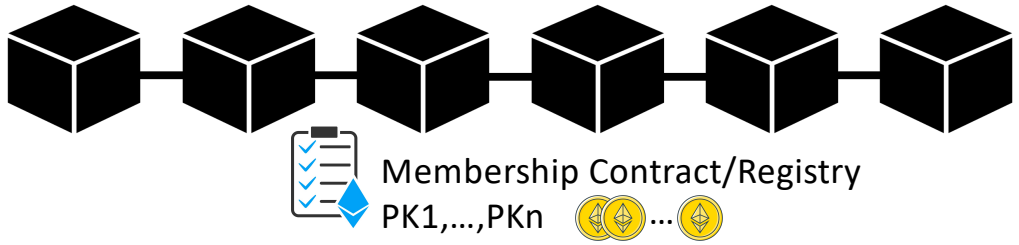


WAKU2-RLN-RELAY

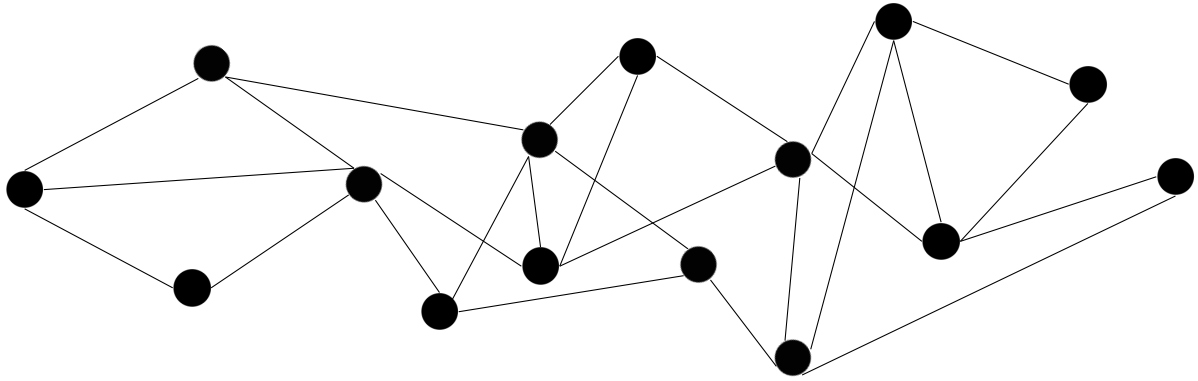
RLN group = Peers subscribed to the same topic e.g., waku-rln-relay



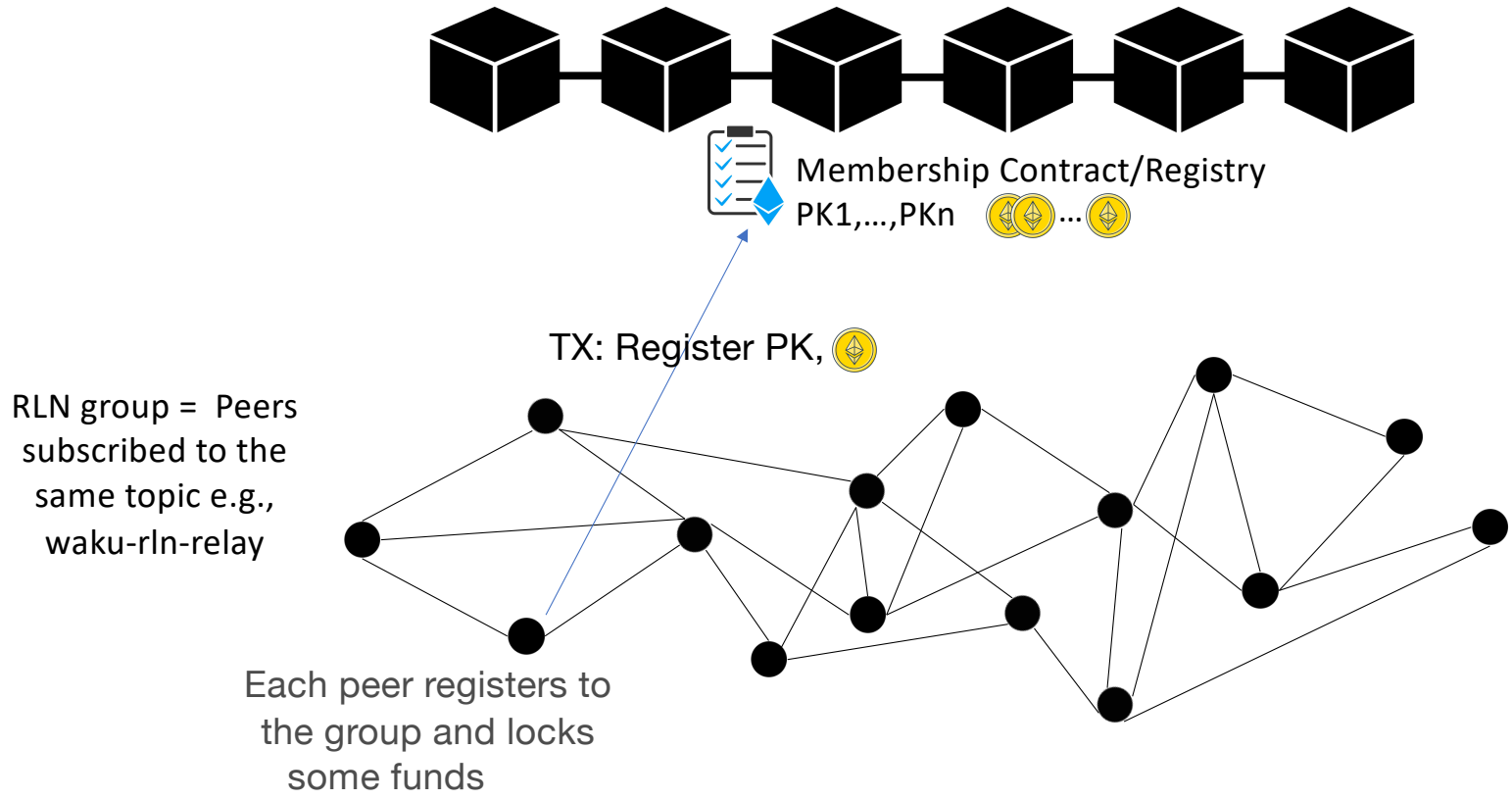
WAKU2-RLN-RELAY: Registration



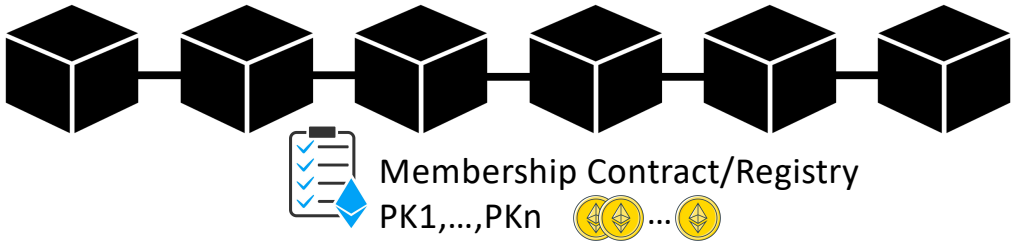
RLN group = Peers subscribed to the same topic e.g., waku-rln-relay

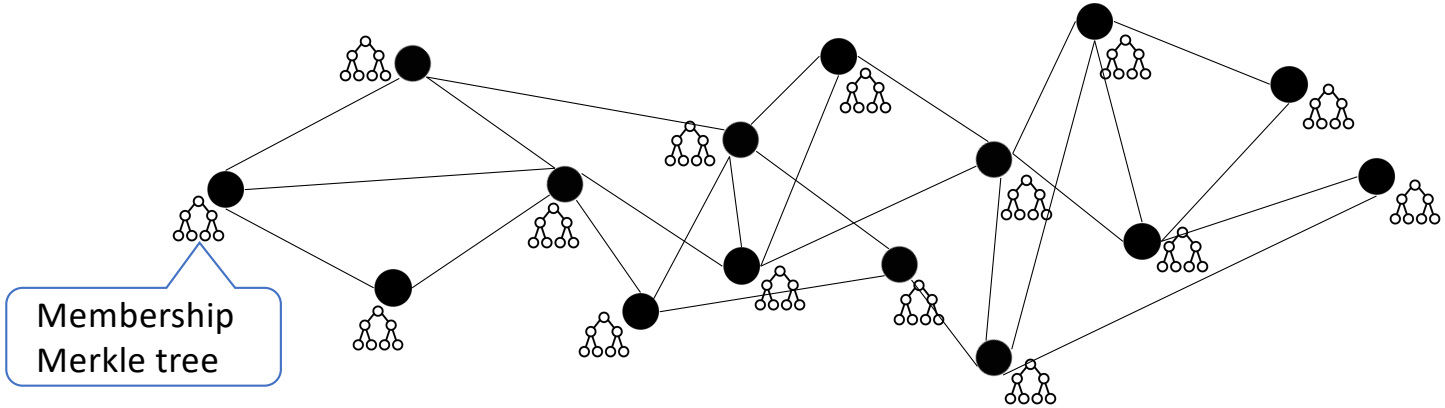


WAKU2-RLNR-ELAY: Registration

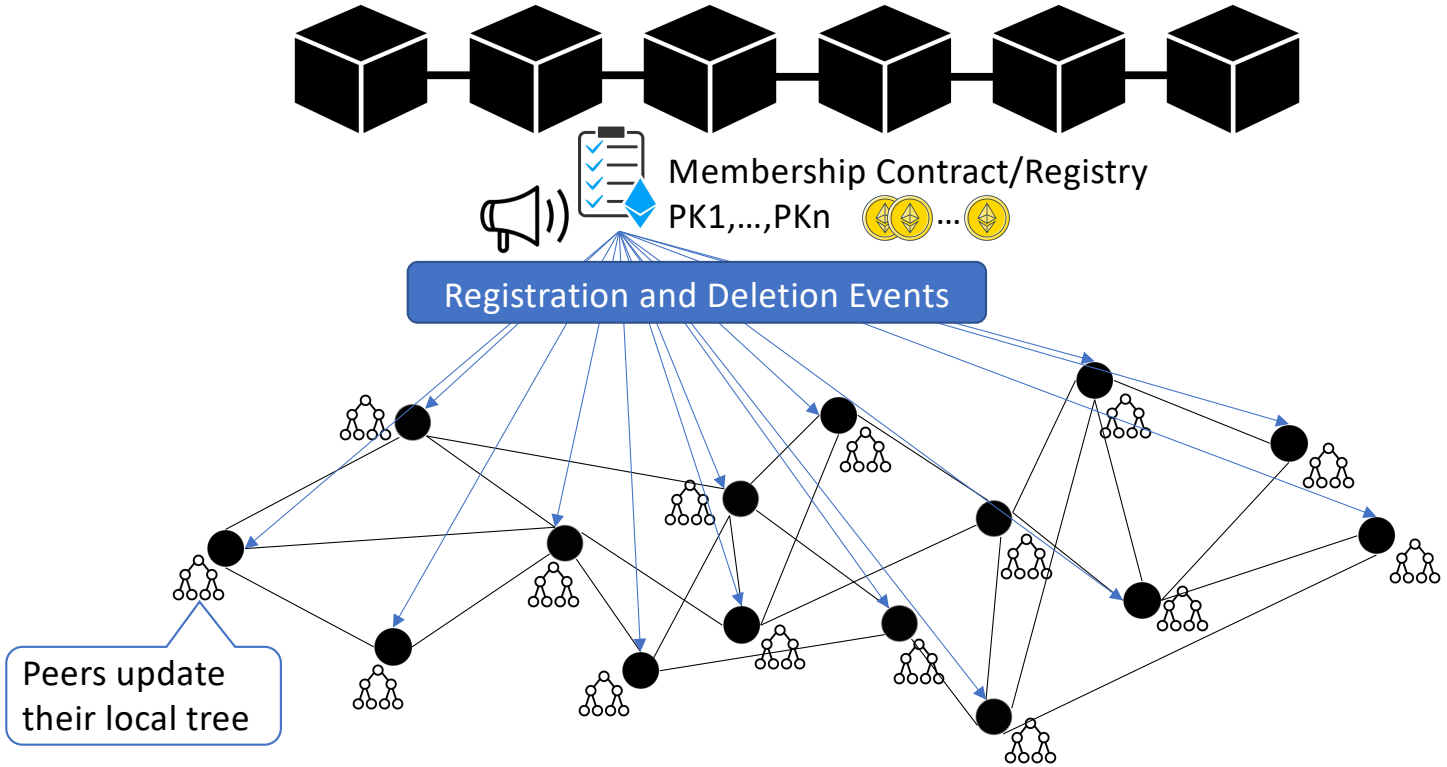


WAKU2-RLN-RELAY: Registration



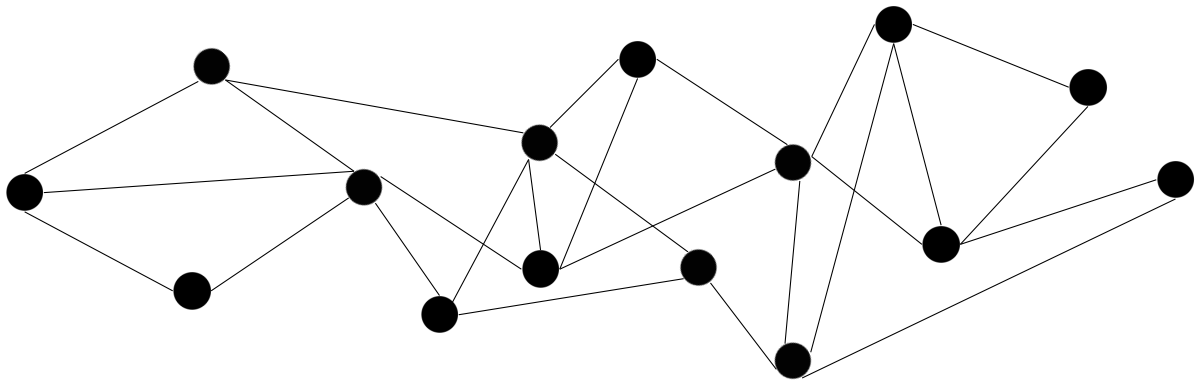


WAKU2-RLN-RELAY: Registration



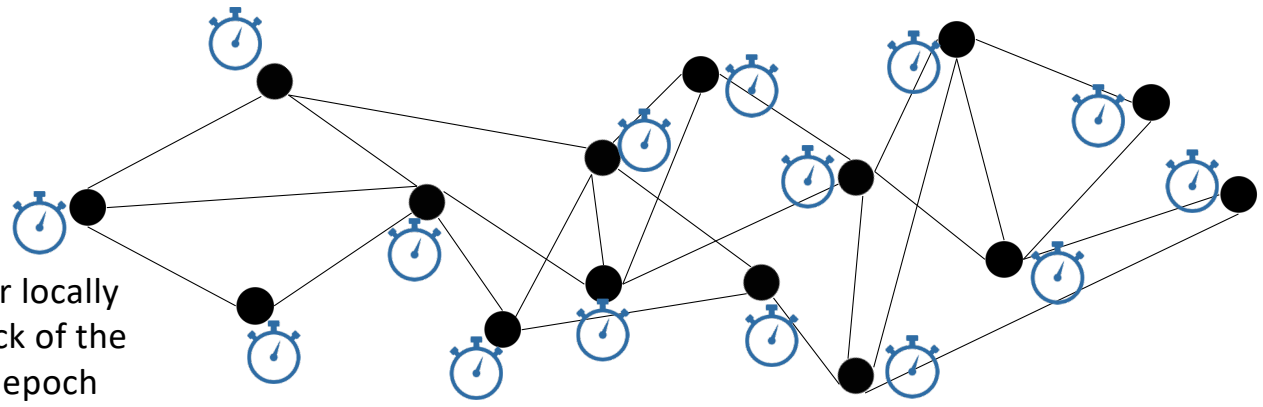
WAKU2-RLN-RELAY: External Nullifier

External Nullifier = Epoch = the number of T seconds that elapsed since the Unix epoch.
Messaging rate is limited to 1 per epoch.



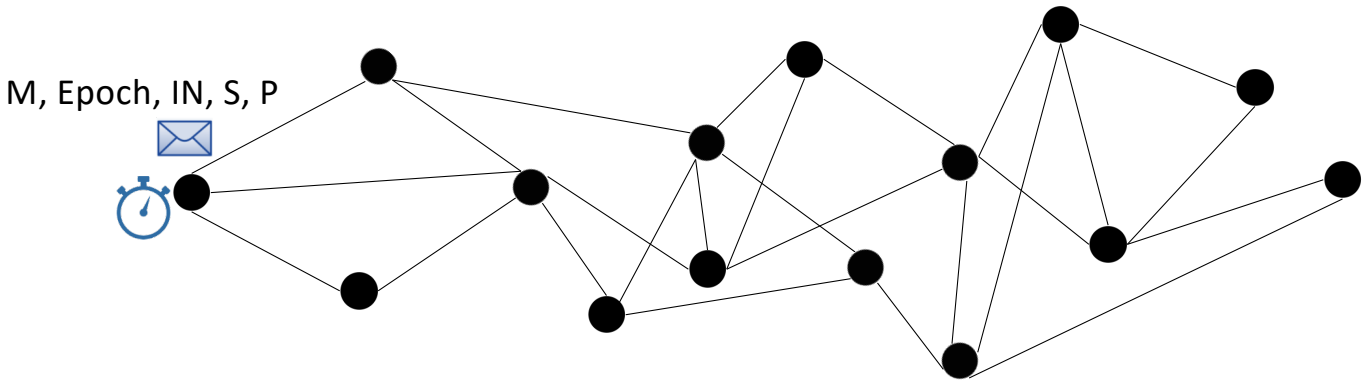
WAKU2-RLN-RELAY: External Nullifier

External Nullifier = Epoch = the number of T seconds that elapsed since the Unix epoch.
Messaging rate is limited to 1 per epoch.

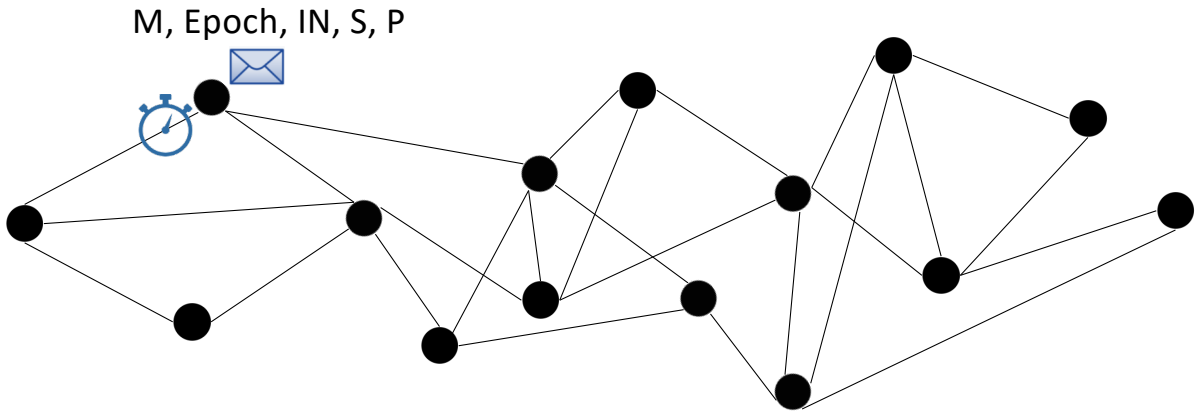


Each peer locally keeps track of the current epoch

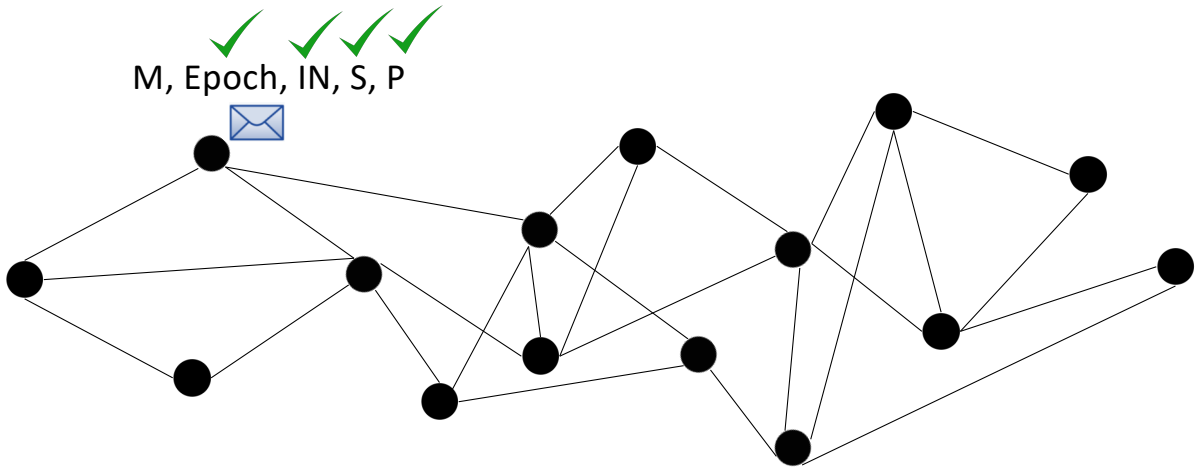
WAKU2-RLN-RELAY: Publishing



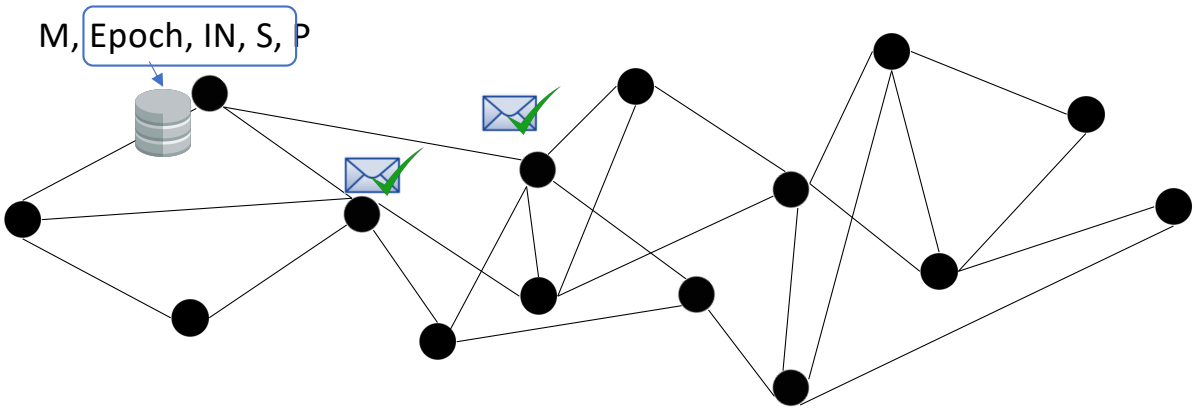
WAKU2-RLN-RELAY: Routing



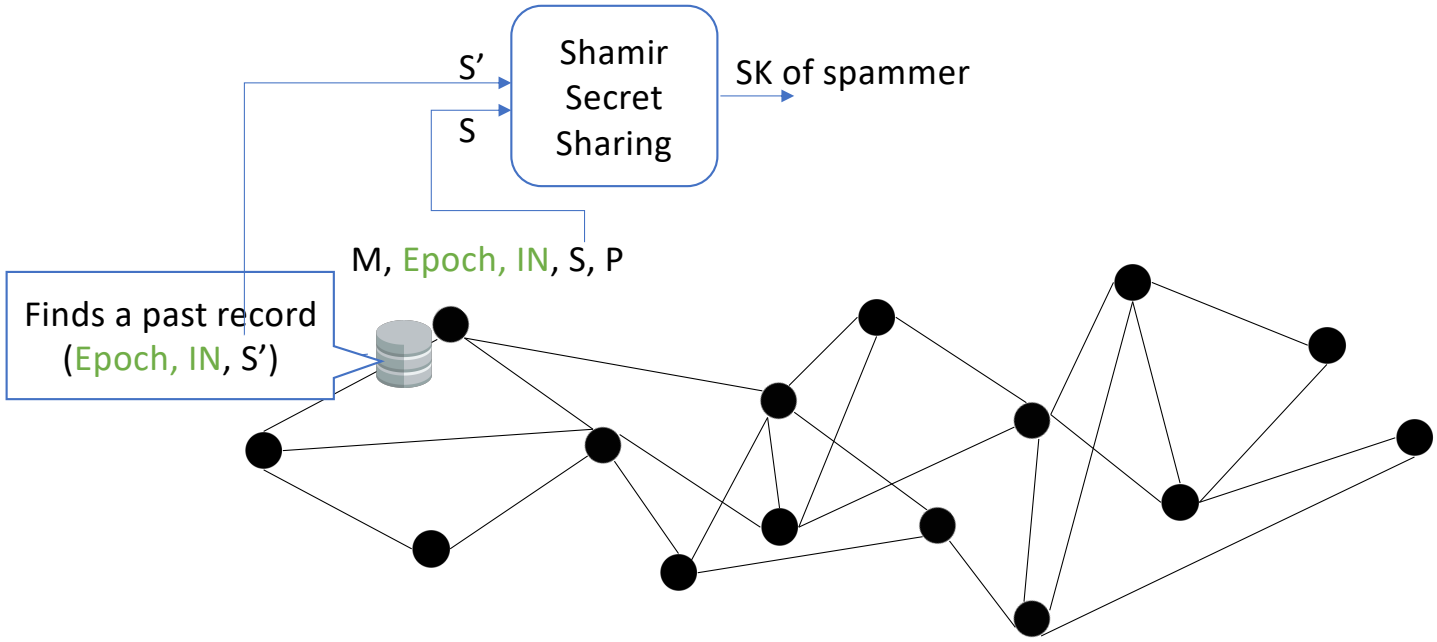
WAKU2-RLN-RELAY: Routing



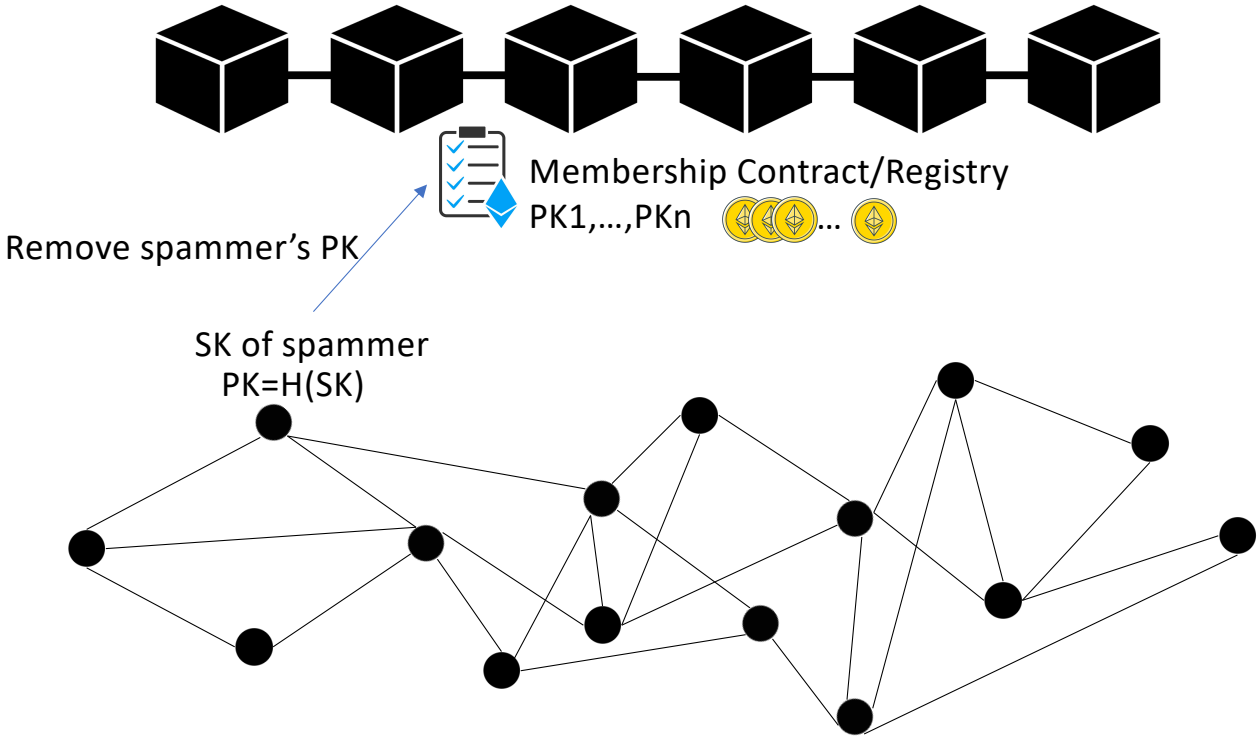
WAKU2-RLN-RELAY: Routing



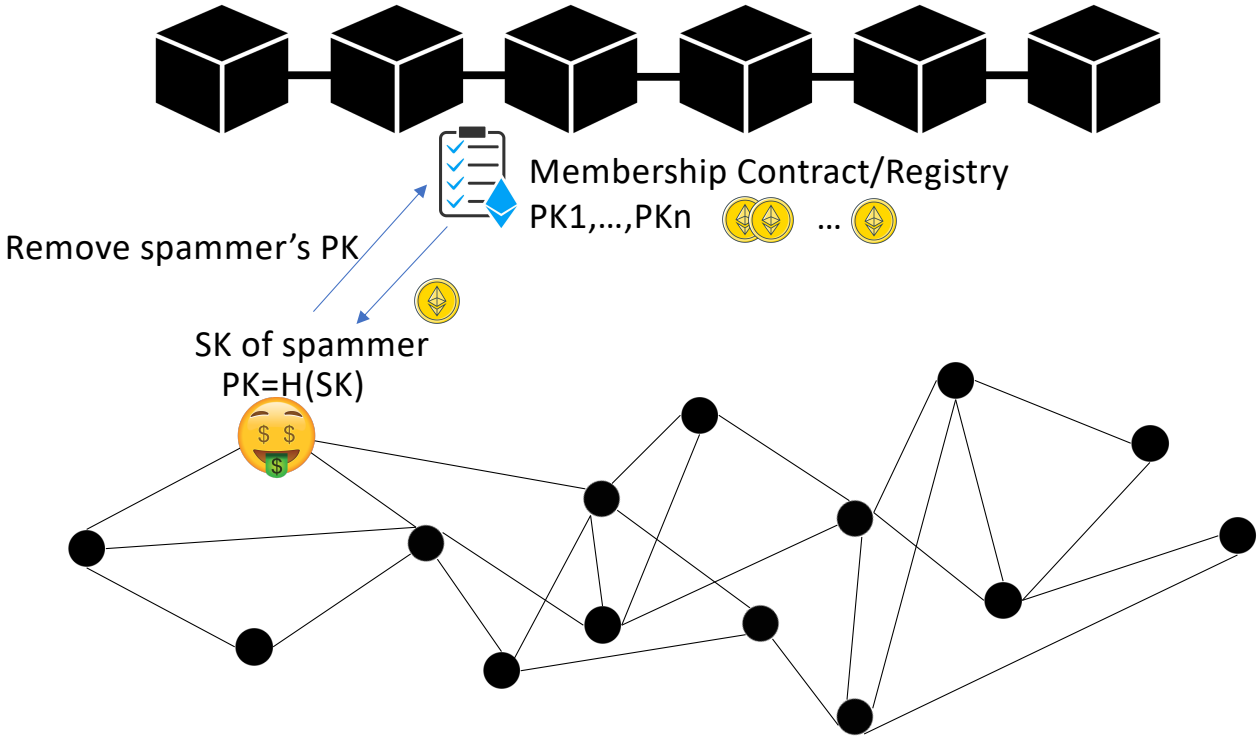
WAKU2-RLN-RELAY: Slashing



WAKU2-RLN-RELAY: Slashing



WAKU2-RLN-RELAY: Slashing



Future work

- Benchmarking
- Storage-efficient Merkle tree storage
  - P2p network of full-nodes and light-nodes
  - Partial view of Merkle tree
- Real-time removal of spammers using off-chain/p2p solutions
- Cost-effective way of member insertion and deletion using layer 2 solutions

References

- Waku-rln-relay specs: https://rfc.vac.dev/spec/17/
- Waku-rln-relay paper: https://github.com/vacp2p/research/blob/master/rln-research/Waku_RLN_Relay.pdf
- Vac post on Waku-rln-relay: https://vac.dev/rln-relay
- Nim-Waku implementation: https://github.com/status-im/nim-waku
- js-Waku implementation: https://github.com/status-im/js-waku
- RLN Ethereum research post: https://ethresear.ch/t/semaphore-rln-rate-limiting-nullifier-for-spam-prevention-in-anonymous-p2p-setting/5009
- RLN medium post: https://medium.com/privacy-scaling-explorations/rate-limiting-nullifier-a-spam-protection-mechanism-for-anonymous-environments-bbe4006a57d
- RLN circuits: https://github.com/appliedzkp/rln
- RLN circuits spec: https://hackmd.io/7GR5Vi28Rz2EpEmLK0E0Aw
- RLN in Rust: https://github.com/kilic/rln

Thank you