Privacy-Preserving Spam-Protected Gossip-Based Routing

Sanaz Taheri
Vac Research and Development
sanaz@status.im

Oskar Thoren
Vac Research and Development
oskar@status.im

Barry Whitehat
Unaffiliated
barrywhitehat@protonmail.com

Wei Jie Koh
Independent
contact@kohweijie.com

Onur Kilic
Unaffiliated
onurkilic@protonmail.com

Kobi Gurkan
cLabs
me@kobi.one

## WAKU2-RELAY: Anonymous P2P Gossip-Based Routing

WAKU2-RELAY [1] follows a publisher-subscriber messaging model with gossip-based routing (extension of libp2p GossipSub-v1.1 [2])
Messages are anonymous i.e. protocol message headers carry no personally identifiable information about the message origin

Anonymous
No IP, No
PeerID
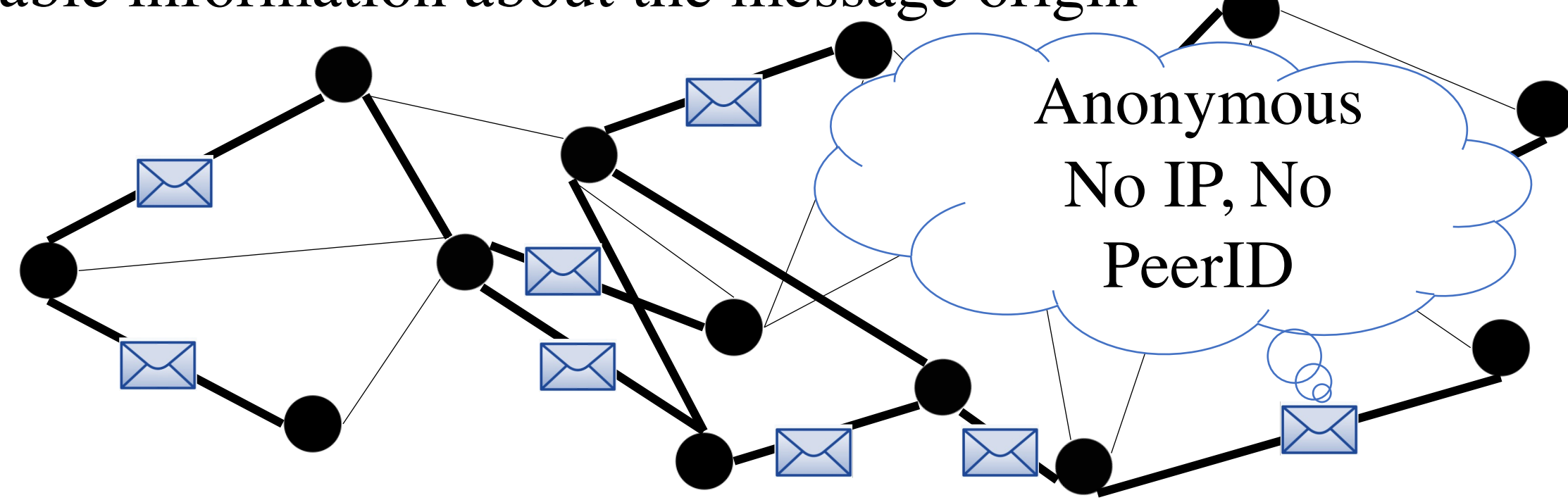
Spam and Denial-of-Service Attack

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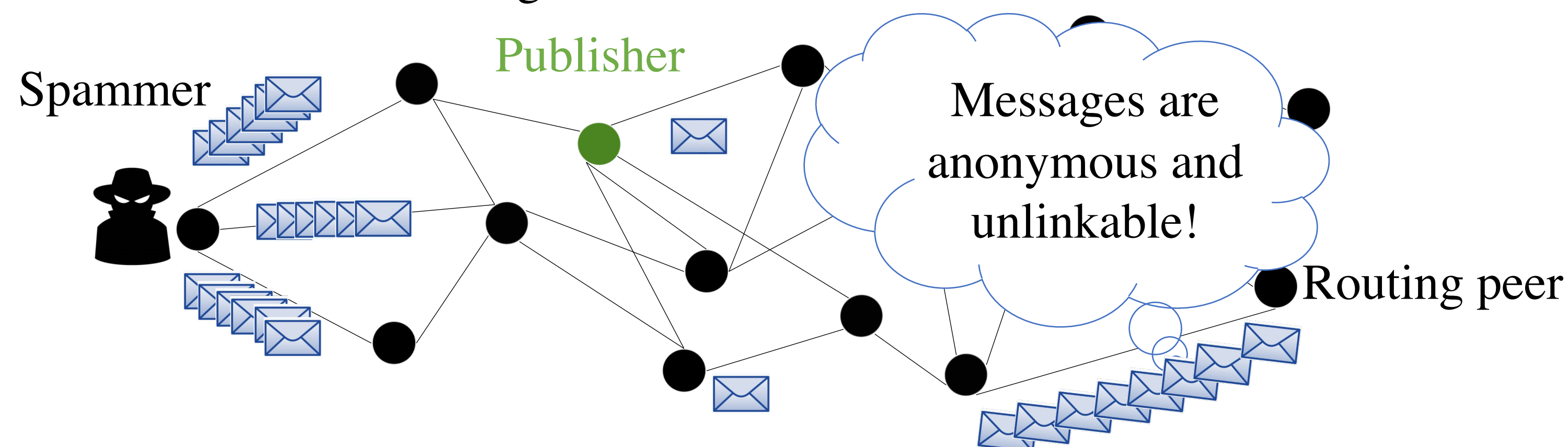Spam Protection = Controlled Messaging Rate
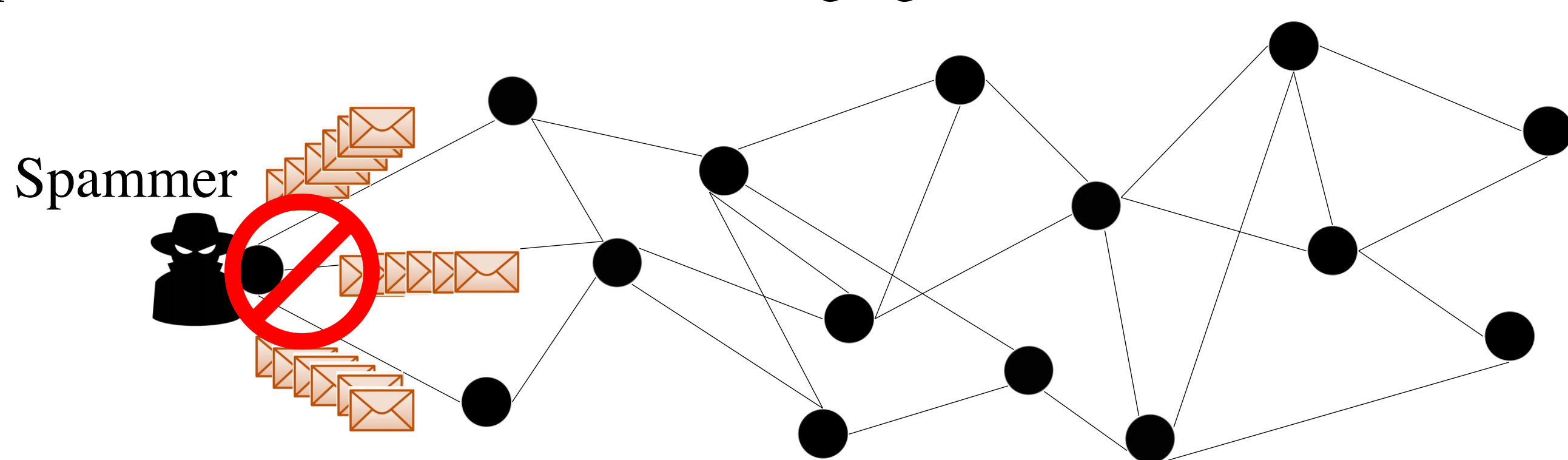
Spammer

Global Spam Protection and Anonymity

Routing peers can not distinguish between spam messages and non-spam messages.
Solutions like IP blocking are not effective.

Spammer

Publisher

Messages are anonymous and unlinkable!

Routing peer

Related Works

Proof-of-work [3] deployed by Whisper [4]
- Computationally expensive
- Not suitable for network of heterogeneous peers with limited resources

Peer Scoring [2] in libp2p
- Local to each peer
- No global identification of spammer
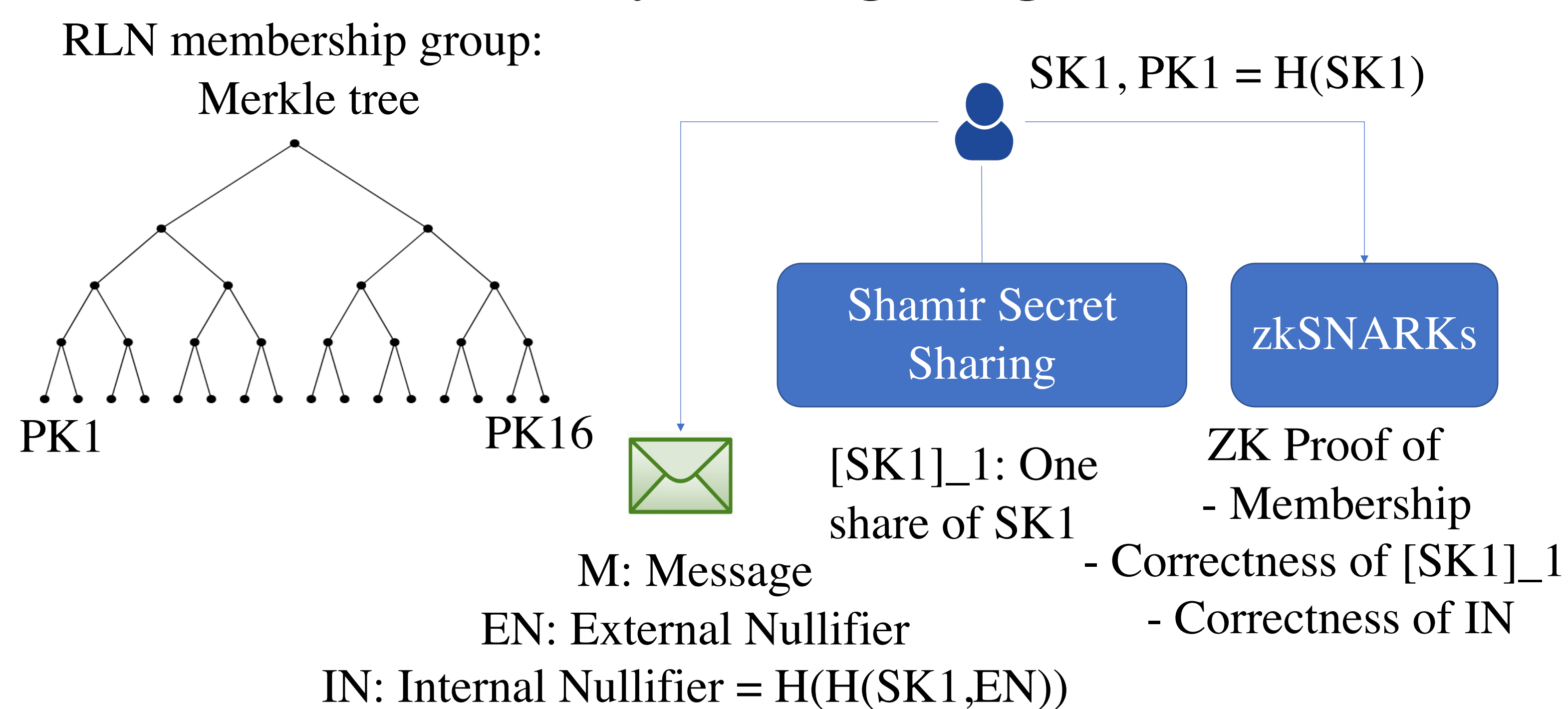- Subject to inexpensive attacks using bots

WAKU2-RLN-RELAY

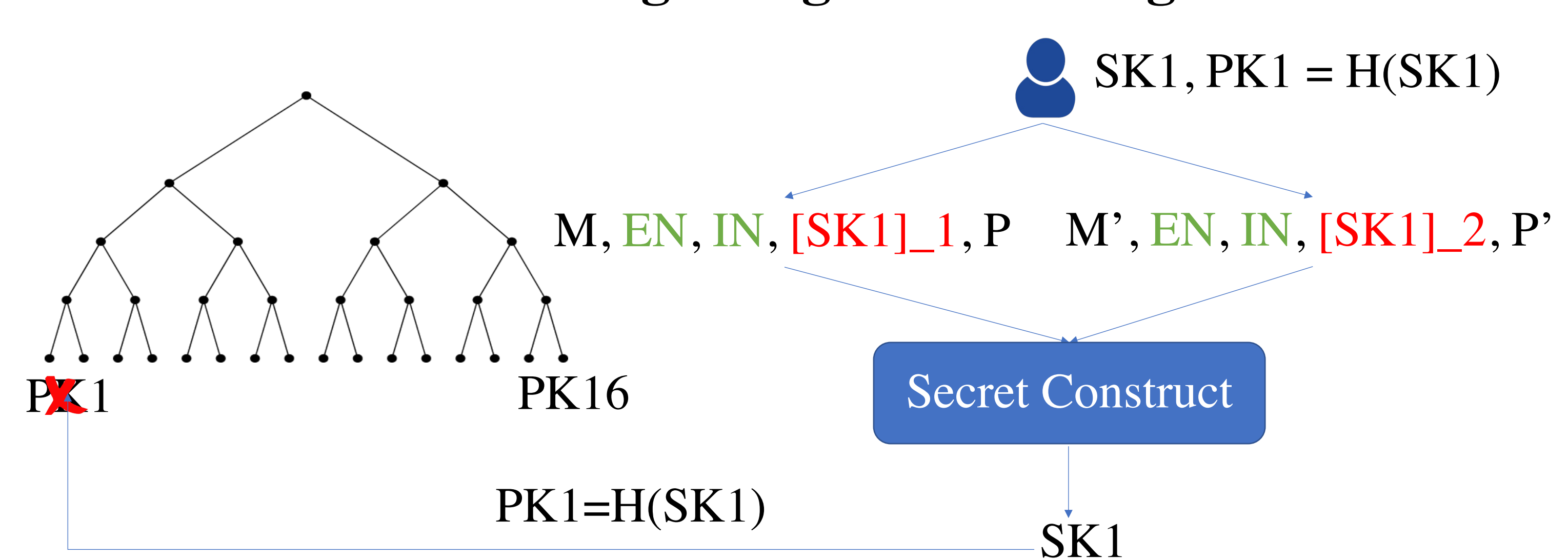WAKU2-RLN-RELAY [6] = WAKU2-RELAY + Rate Limiting Nullifiers [5]
- A protocol-level solution
- Computationally efficient and suitable for resource-restricted devices
- Privacy-preserving
- Global spam protection
- Sybil attack mitigation
- Built-in economic incentives where spammers are financially punished and those who find spammers are rewarded.

RLN: Rate Limiting Nullifier

Anonymous Signaling

RLN membership group: Merkle tree

SK1, PK1 = H(SK1)

Shamir Secret Sharing

zkSNARKS

$[SK1]\_1$: One share of SK1

ZK Proof of
- Membership
- Correctness of $[SK1]\_1$
- Correctness of IN

M: Message
EN: External Nullifier
IN: Internal Nullifier = H(H(SK1,EN))

Double Signaling and Slashing

SK1, PK1 = H(SK1)

M, EN, IN, [SK1]_1, P   M', EN, IN, [SK1]_2, P'
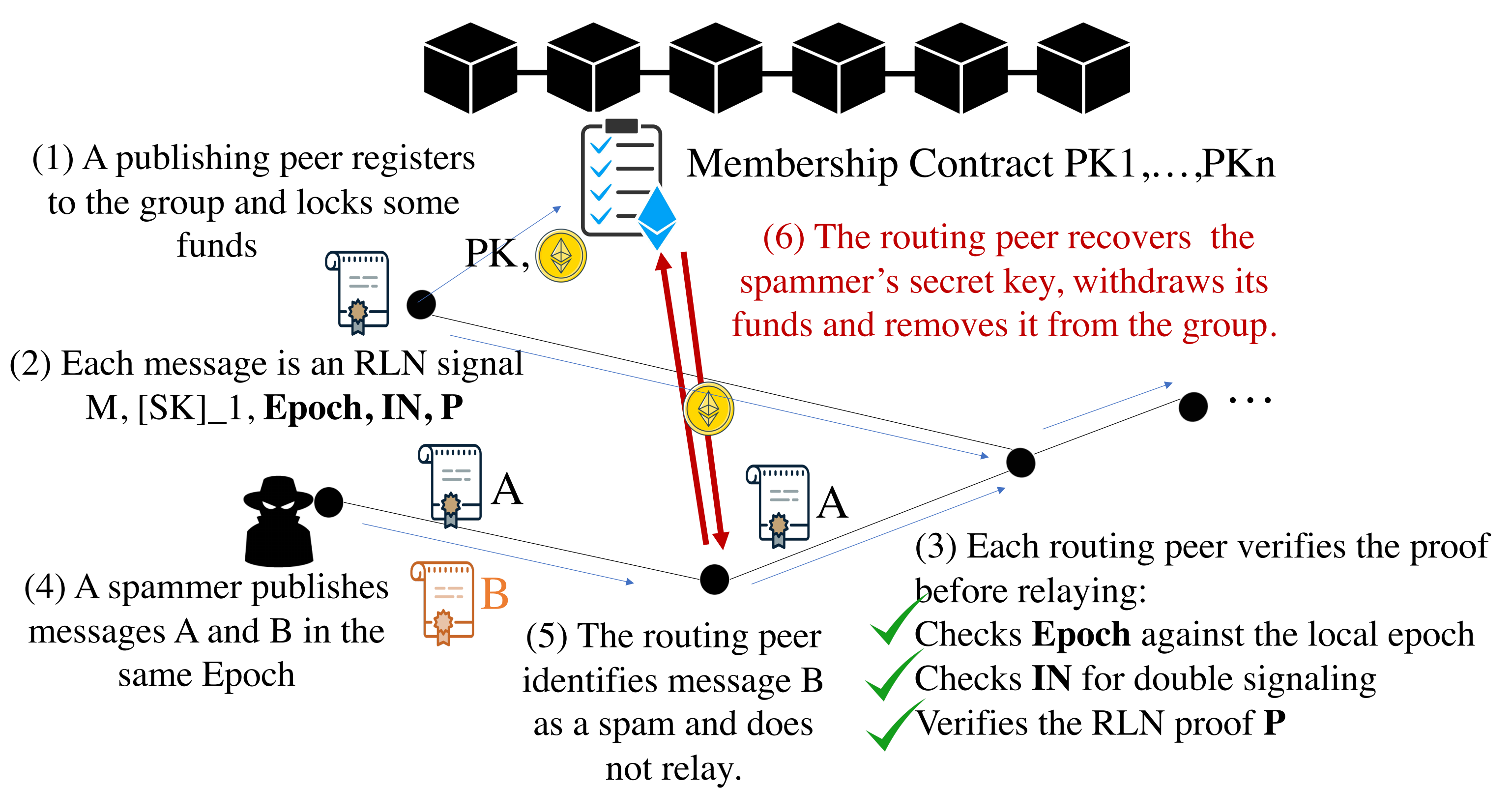
Secret Construct

PK1=H(SK1)

SK1

WAKU2-RLN-RELAY: Spam-Protected Gossip--Based Routing

RLN group: Peers subscribed to the same topic
External Nullifier/Epoch: the number of T seconds that elapsed since the Unix epoch. Each peer locally keeps track of the current epoch.
Messaging rate: 1 per Epoch.
Merkle Tree: Peers construct and update the Membership Merkle tree locally using events emitted from the membership contract.

(1) A publishing peer registers to the group and locks some funds

Membership Contract PK1,…,PKn

PK,

(6) The routing peer recovers the spammer's secret key, withdraws its funds and removes it from the group.

(2) Each message is an RLN signal M, [SK]_1, **Epoch, IN, P**

A

A

(4) A spammer publishes messages A and B in the same Epoch

B

(5) The routing peer identifies message B as a spam and does not relay.

(3) Each routing peer verifies the proof before relaying:
✓ Checks **Epoch** against the local epoch
✓ Checks **IN** for double signaling
✓ Verifies the RLN proof **P**

Future Works

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
1. WAKU2-RELAY specifications, https://rfc.vac.dev/spec/11
2. Vyzovitis D, Napora Y, McCormick D, Dias D, Psaras Y. GossipSub: Attack-resilient message propagation in the Filecoin and ETH2. 0 networks. arXiv preprint arXiv:2007.02754. 2020 Jul 6.
3. C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in Annual international cryptology conference. Springer, 1992.
4. Whisper https://eips.ethereum.org/eips/eip-627
5. RLN specifications, https://rfc.vac.dev/spec/32
6. WAKU2-RLN-RELAY specifications, https://rfc.vac.dev/spec/17