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

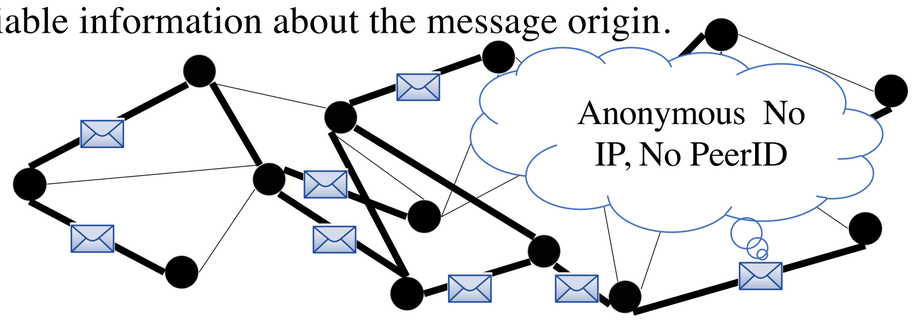
Wei Jie Koh
Independent
contact@kohweijie.com

Onur Kilic
Unaffiliated
onurkilic@protonmail.com

Kobi Gurkan
cLabs
me@kobi.one

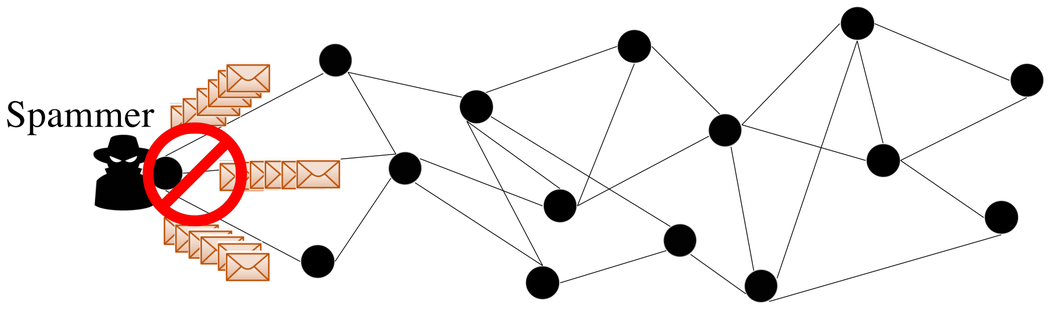
WAKU-RELAY: Anonymous P2P Gossip-Based Routing

WAKU-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.



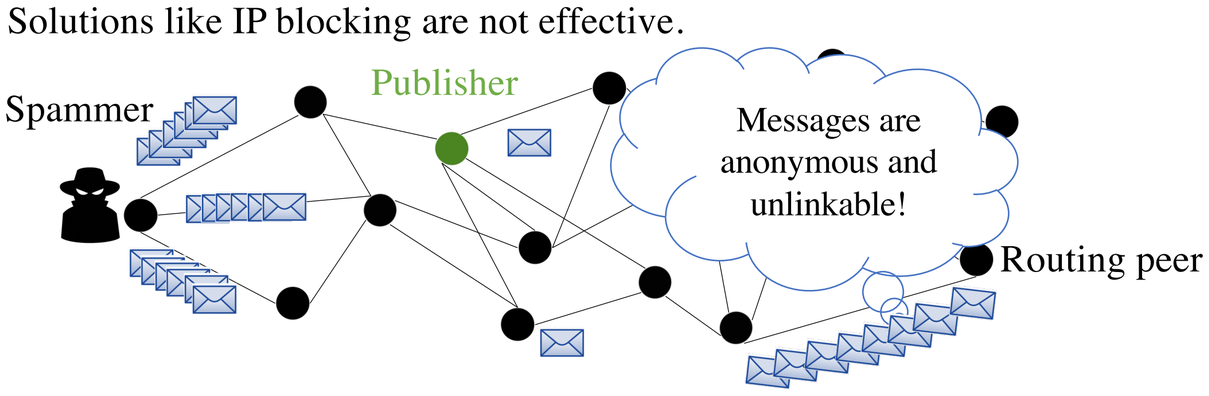
Spam and Denial-of-Service Attack

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



Global Spam Protection and Anonymity

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



State-of-the-art Spam Protection Methods

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

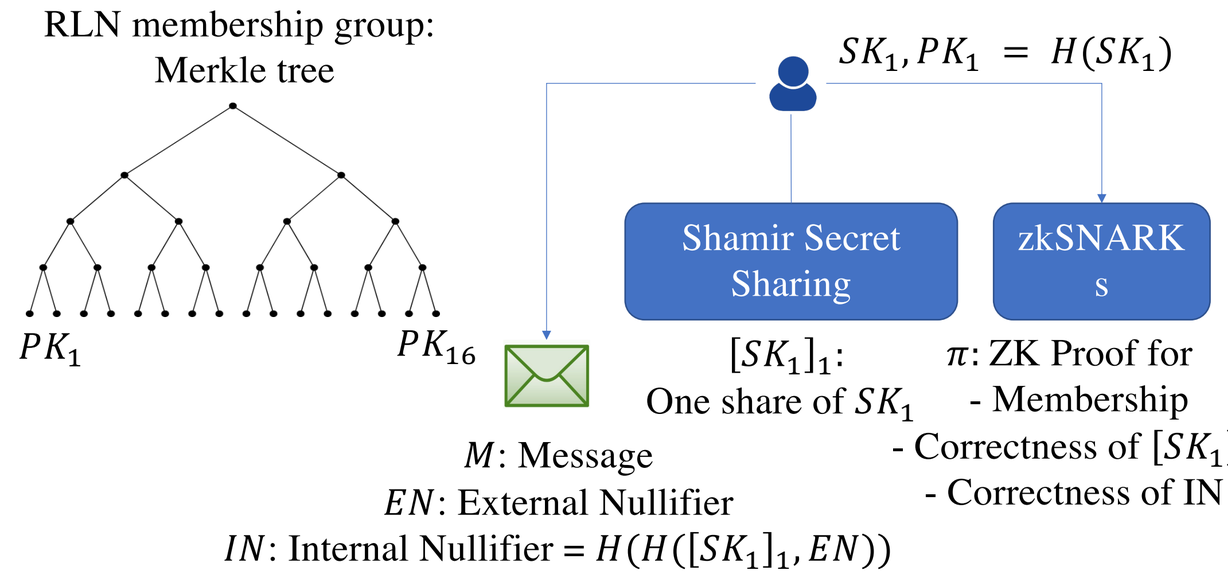
Peer Scoring [2] in libp2p
- Local to each peer
- No global identification of spammer
- Subject to inexpensive attacks using bots

WAKU-RLN-RELAY: Anonymous and P2P Global Spam Protection Made Possible

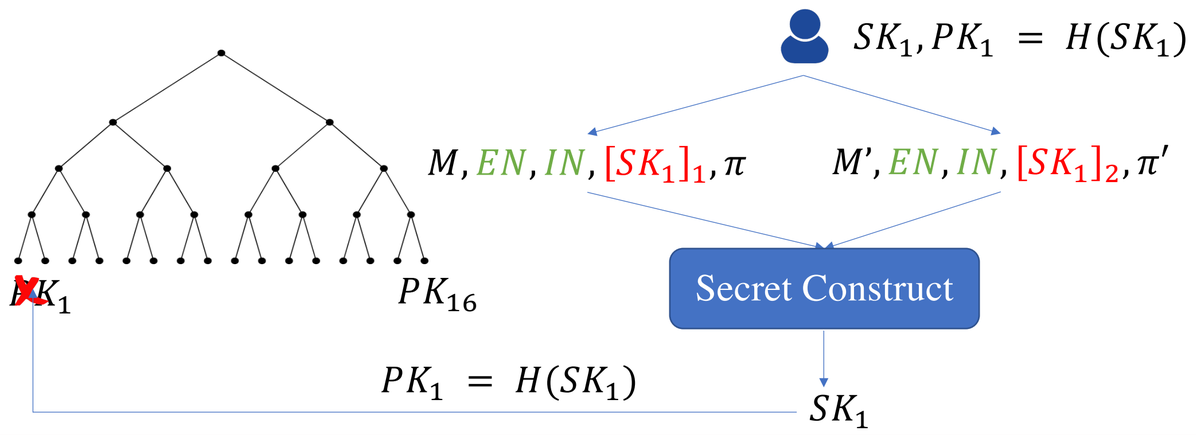
WAKU-RLN-RELAY [6] features an **Efficient & Anonymous P2P Global Spam Protection** by integrating the novel construct of *Rate Limiting Nullifiers (RLN)* [5] into the WAKU-RELAY protocol. The final result is a spam-protected gossip-based routing protocol that additionally provides:
- A protocol-level solution
- Sybil attack mitigation
- Built-in economic incentives where spammers are financially punished and those who find spammers are rewarded

Rate Limiting Nullifier

Anonymous Signaling

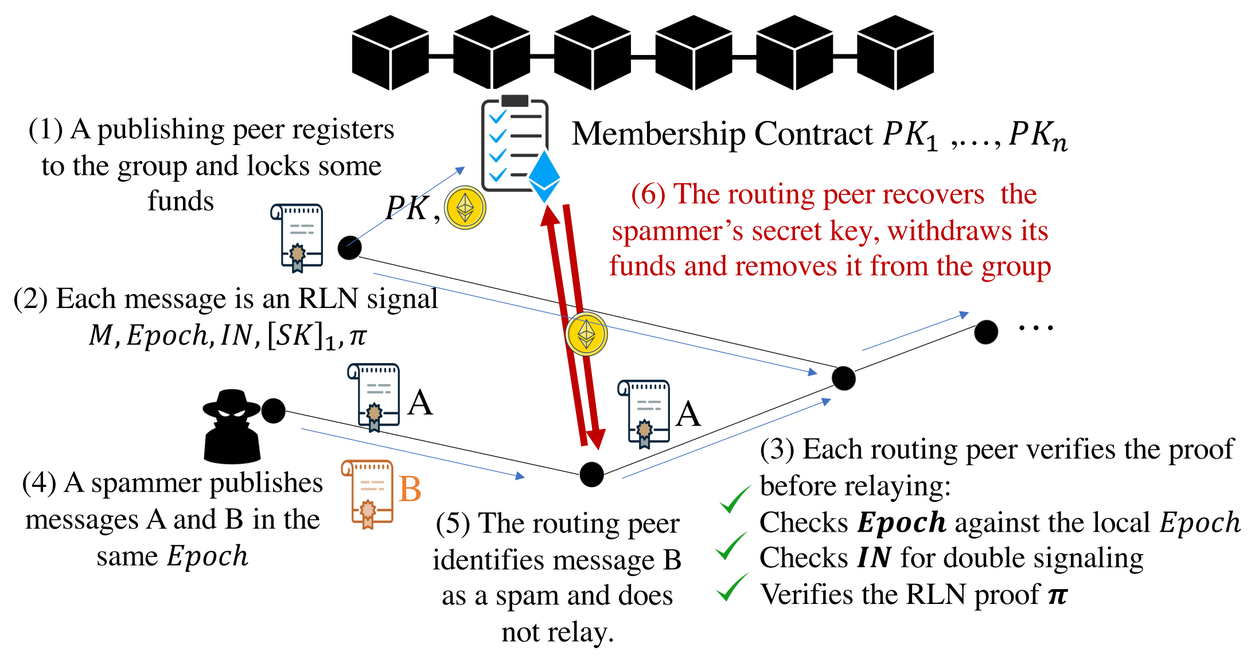


Double Signaling and Slashing



Routing Protocol Construction

RLN group: Peers subscribed to the same topic.
External Nullifier/Epoch: the number of T seconds that elapsed since the Unix epoch event. 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.



Future Work

- Benchmarking
- Efficient Merkle tree maintenance
  - 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. WAKU-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. WAKU-RLN-RELAY specifications, https://rfc.vac.dev/spec/17