DoS-Resistant Protocols in Ethereum: WHISK and Homomorphic Sortition

Privacy-Enhanced Leader Election for Blockchain Systems

Author: Tomas Krajci Supervisor: doc. Ing. Ivan Homoliak, Ph.D. Year: 2025

1. Introduction:

Modern proof-of-stake blockchains rely on leader election to determine who can propose the next block. However, exposing validator identities before block production creates Denial-of-Service (DoS) vulnerabilities.

We explore two privacy-preserving approaches — WHISK and Homomorphic Sortition — that protect and mitigate these DoS vulnerabilities by hiding the proposer until the block is finalized.

2. WHISK Protocol:

WHISK introduces a shuffle-based protocol using SNARKs to hide validator selection behind a cryptographic mixnet.

Key Features:
-Trackers are randomized commitments: (rG, k·rG)
-SNARK proof ensures correct shuffle of tracker list
-Validators prove ownership of shuffled trackers via DLEQ proofs
-Identity is bound to commitment com(k) = kG

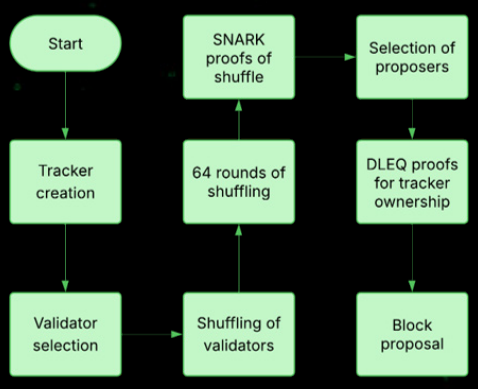

Figure 1. - Whisk protocol flow

Figure 3. – Sortition protocol flow

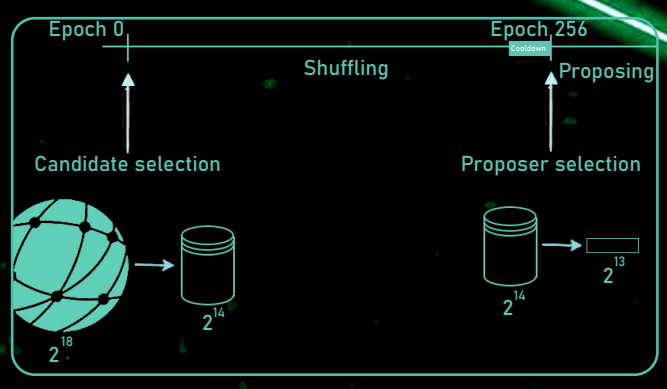

Figure 2. - Whisk Protocol flow

3. Homomorphic Sortition:

The Homomorphic Sortition protocol leverages Fully Homomorphic Encryption (FHE) to privately select a winner from a set of candidates.
All computation, including comparison and selection, happens on encrypted data — meaning no party learns the outcome unless they're the winner.

Key Features:
-Stake-weighted fairness: Selection probability is proportional to a process's stake.
-Privacy-preserving: Leader identity remains secret unless voluntarily revealed.
-Uses Threshold FHE (ThFHE) for secure encrypted computation.

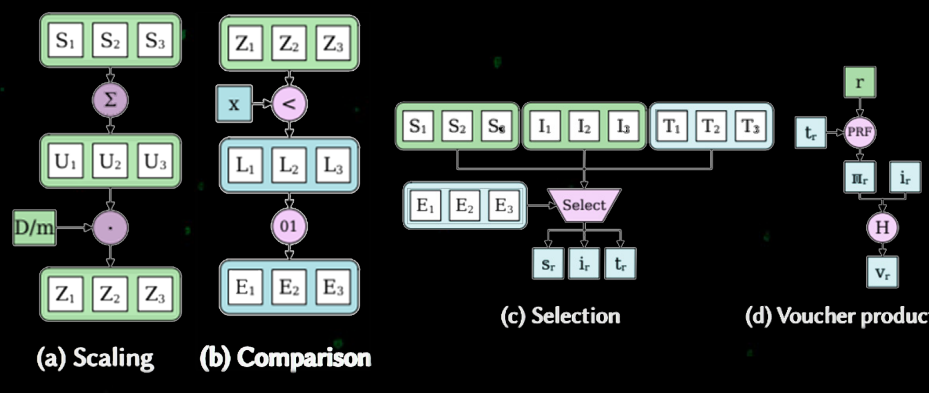

Figure 4., 5., 6. – Sortition protocol parts

4. Practical Contributions:

- Implemented and evaluated two SSLE protocols: WHISK (shuffle-based) and Homomorphic Sortition (FHE-based)

- Designed and validated a SNARK-based proof system for verifiable shuffling

- Analyzed performance overhead of both protocols (computation, communication, state size)

Feature	WHISK	Homomorphic Sortition
Privacy Guarantee	High (shuffle-based)	Very High (full FHE protection)
Identity Revelation	Only when block is proposed	Only after voucher decryption
Proof Mechanism	SNARKs	Threshold Fully Homomorphic Encryption (ThFHE)
Computation Cost	Moderate (ZK proof generation)	High (encrypted comparisons and PRF)
Communication Overhead	Moderate (proofs per shuffle)	Medium (partial decryptions needed)

Table 1. - WHISK and Sortition comparison

5. Conclusions:

-WHISK and Homomorphic Sortition both mitigate targeted DoS risks in Ethereum-like PoS blockchains.
-WHISK offers lower computation overhead but requires continuous proofs.
-Homomorphic Sortition provides stronger privacy at the cost of high computation.
-Future work: scaling FHE-based circuits and hybrid designs combining shuffle + FHE

6. References:

Luciano Freitas, Andrei Tonkikh, Adda-AkramBendoukha, Sara Tucci-Piergiovanni, RenaudSirdey, Oana Stan, and Petr Kuznetsov. Homo-morphic sortition – single secret leader electionfor PoS blockchains. Cryptology ePrint Archive,-Paper 2023/113, 2023.
Dan Boneh, Saba Eskandarian, Lucjan Hanzlik,and Nicola Greco. Single secret leader election,2020.
Antoine Toulme, Justin Drake, Dankrad Feist,Gottfried Herold, Dmitry Khovratovich, MaryMaller, and Mark Simkin. Whisk: A practicalshuffle-based ssle protocol for ethereum. https://hackmd.io/@asn-d6/HyD3Yjp2Y, 2020.

Excel@FIT 2025

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY