Discussion post for: Verifying RLN Proofs in Light Clients with Subtrees | Vac Research

cross-posted to: Light RLN Verifiers using a Tiered Commitment Tree - Vac Rearch Blog Posts - Vac

tl;dr: Implementation of a technique to decrease gas fees associated with a sparse Merkle tree on-chain, while simultaneously minimizing client-side requirements. This solution leverages the segmentation of root computation into subtrees. Notably utilized by projects like Penumbra and Polygon Miden, this approach also facilitates trustless availability of the Merkle tree root on-chain, even when using a zk-friendly hash function that is more costly within the EVM environment.

Can be used for Semaphore/RLN.