Enhancing Ethereum's Security With LUMEN, Novel Zero-Knowledge Algorithms Generating Transparent and Efficient SNARKs Based on Hidden Order Groups

Quan, Yunjia (School: Charlotte Country Day School)

The cryptocurrency Ethereum utilizes zero-knowledge rollups (ZKR) to improve its scalability. ZKRs processes thousands of Ethereum transactions in a batch and uses zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge) to verify the validity of those transactions. zk-SNARKs rely on a trusted setup procedure, where a group of participants uses secret information about transactions to generate public information used by zk-SNARKs. However, this process introduces a security risk to Ethereum. Thus, researchers have been developing transparent zk-SNARKs that do not require a trusted setup. However, those transparent zk-SNARKs are often not as efficient as non-transparent zk-SNARKs. In this research, I developed LUMEN, a novel set of algorithms that includes a recursive polynomial commitment scheme and a new interactive polynomial oracle proof protocol, which is compiled into efficient and transparent zk-SNARKs with linear proof computation and verification time. Various techniques were creatively incorporated into LUMEN, including groups with hidden orders, Lagrange basis polynomials, witness-extended emulation, and an amortization strategy. Mathematical proofs show LUMEN's completeness, soundness, and zero-knowledge, and we implemented LUMEN in Python and Rust. LUMEN's efficiency, measured in proof size, surpasses DARK and zk-STARK (two of the most efficient transparent zk-SNARKs) by 8 and 37 times, respectively, and LUMEN's proof size is only 0.71KB more than Plonk, the most commonly used non-transparent zk-SNARKs. LUMEN is a promising solution to improve Ethereum's security while maintaining its efficiency, and the findings of the techniques that enabled LUMEN to be efficient and transparent can significantly benefit future work improving Ethereum.