ZKExpress (2025.08)

Kurt Pan @ ZKPunk

August 2, 2025

Contents

1 [FGR+25] Collaborative zkSNARKs with Sublinear Prover Time and Constant Proof Size

We propose a new collaborative zkSNARK scheme with $O\left(\frac{C}{n}\log\frac{C}{n}\right)$ prover time and $O(1)$ proof size with n servers for a circuit of size C. An adversary compromising less than $\frac{n}{4}$ servers cannot learn any information about the witness. The core of our technique lies in a new zkSNARK scheme for the Plonkish constraint system that is friendly to *packed secret sharing*. We utilize *bivariate polynomials* to avoid a large Fast Fourier Transform on the entire witness, which was the major bottleneck in prior work. We also construct permutation constraints based on logarithmic derivatives and univariate sumcheck to avoid the computation of prefix products. Finally, we build a bivariate polynomial commitment scheme that can be computed directly on packed secret shares. Experimental results show that for a circuit of size 2^{20}, with 128 servers, our scheme can accelerate the proof generation by 36.2× compared to running the zkSNARK on a single server. The prover time of our system is 25.9× faster than the prior work of zkSaaS. The proof size of our scheme is only 960 Bytes.

2 [BB25] Optimizing Backend Verification in zk-Rollup Architectures

This paper presents a comprehensive implementation of the Tokamak zkEVM verifier, specifically optimized for the BLS12-381 elliptic curve operations introduced by EIP-2537. We detail the complete verification architecture, from EVM compatible data formatting for pairing checks, multi-scalar multiplication (MSM), and elliptic curve addition, to the non-interactive protocol design between prover and verifier. Our key contribution lies in novel optimization techniques that substantially reduce on-chain verification costs. Through strategic polynomial aggregation and scalar factorization, we minimize G1 exponentiations from 40 to 31, achieving gas savings of 108,000 units per verification. Additionally, we introduce a dynamic barycentric interpolation method that replaces computationally intensive FFT operations, resulting in 92-95% gas reduction for sparse polynomial evaluations. We further present proof aggregation strategies that minimize precompile calls while maintaining the 128-bit security guarantees of BLS12-381.

References

[BB25] Mehdi Beriane and Muhammed Ali Bingol. Optimizing backend verification in zk-rollup architectures. Cryptology ePrint Archive, Paper 2025/1390, 2025. (In pages 1 and 2).

[FGR$^+$25] Zhiyong Fang, Sanjam Garg, Bhaskar Roberts, Wenxuan Wu, and Yupeng Zhang. Collaborative zkSNARKs with sublinear prover time and constant proof size. Cryptology ePrint Archive, Paper 2025/1388, 2025. (In page 1).