# ZKExpress (2025.07)

Kurt Pan @ zkpunk.pro

July 25, 2025

## Contents

## 1 [PP25] Hobbit: Space-Efficient zkSNARK with Optimal Prover Time

## 2 [TMM25] Ring-LWR based Commitments and ZK-PoKs with Application to Verifiable Quantum-Safe Searchable Symmetric Encryption

## 3 [KLNO25] RoK and Roll Verifier-Efficient Random Projection for $\tilde{O}(\lambda)$-size Lattice Arguments

## 4 [Fu25] Improved Constant-Sized Polynomial Commitment Schemes Without Trusted Setup

## 5 [FDR+25] LegoLog: A configurable transparency log

## 6 [MRR25] Tree PCPs

## 7 [GSSB25] Efficiently parsing existing eID documents for zero-knowledge proofs

## 8 [XGBK25] FRIttata: Distributed Proof Generation of FRI-based SNARKs

We present the first horizontally scalable SNARK for general circuits that is both transparent and plausibly post-quantum (PQ) secure. This system adapts the distributed proof generation technique introduced in Pianist (IEEE S&P 2024), which achieves linear scalability by encoding witnesses using bivariate polynomials and committing to them using the KZG polynomial commitment scheme. While Pianist and other scalable SNARK systems offer strong performance profiles, they rely on trusted setup ceremonies and cryptographic assumptions that are not PQ secure, e.g., pairing-based primitives. In contrast, we present a bivariate polynomial commitment scheme based on FRI, achieving a transparent and plausibly PQ alternative. Distributed FRI has a high communication cost. Therefore, we introduce Fold-and-Batch, a customizable technique that applies partial folding locally be-

fore performing batched FRI centrally. We formally prove the security of our constructions and provide an implementation for three variants of distributed FRI with thorough performance evaluations. Our results show that Fold-and-Batch reduces communication overhead compared to existing distributed FRI approaches while preserving scalability and keeping proof sizes moderate. To our knowledge, this is the first horizontally scalable SNARK for general circuits that at the same time achieves transparency, plausible PQ security, with a tunable tradeoff between efficiency, verifier cost and communication.

## 9 [Lon25] Interstellar: GKR Protocol based Low Prover Cost Folding Scheme for Circuit Satisfiability

In this work, we present Interstellar, a novel folding and IVC framework built on a technique we call circuit interpolation, designed specifically for circuit satisfiability. By incorporating the GKR protocol, our approach avoids commitments to full computation traces and cross-term vectors, requiring instead only commitments to the actual circuit witness and optionally a small subset of intermediate gate values. This design significantly reduces the size of the vectors to be committed to in each folding step, which is an important advantage over existing schemes, as vector commitments typically incur costly group multi-scalar multiplications. Moreover, Interstellar is highly flexible. It can be extended naturally to handle high-degree and lookup gates, enable multi-instance folding, and support non-uniform IVC efficiently, making it well-suited for practical applications ranging from zkML to proving program execution for zkVMs. We instantiate our protocol with various vector/polynomial commitment schemes and provide detailed cost analyses, demonstrating substantial reductions in prover overhead compared to existing approaches.

## 10 [Ila25] Godel in Cryptography: Effectively Zero-Knowledge Proofs for NP with No Interaction, No Setup, and Perfect Soundness

Classical zero-knowledge proofs face the Goldreich-Oren impossibility: you cannot simultaneously achieve perfect soundness, non-interactivity, and zero-knowledge. This work circumvents this limitation by introducing a relaxed

zero-knowledge definition where instead of requiring a simulator to actually exist, they only require that one cannot prove a simulator doesn't exist (logical independence). The approach achieves all security properties of classical zero-knowledge with perfect soundness, no interaction, and no setup, enabling the removal of interaction and setup from existing zero-knowledge applications. The trade-off is that security becomes "game-based" rather than "simulation-based." The construction relies on two assumptions: non-interactive witness indistinguishable proofs exist (following from standard crypto assumptions) and the Krajcek-Pudlk conjecture that no optimal proof system exists (a major proof complexity conjecture related to Gdel's incompleteness). The technical approach creates a prover-verifier system where no simulator exists, but this non-existence is unprovable in strong logical systems like ZFC set theory. The bottom line is that this work effectively achieves the "impossible" combination of perfect soundness, non-interactivity, and zero-knowledge by cleverly relaxing what "zero-knowledge" means while preserving all practical security guarantees.

## 11 [DMZ25] PlasmaFold: An Efficient and Scalable Layer 2 with Client-Side Proving

This paper introduces PlasmaFold, a novel L2 designed to overcome these limitations. PlasmaFold utilizes a hybrid architecture: an operator (aggregator) generates proofs on server side for the honest construction of blocks, while users maintain balance proofs on their own devices. This separation of concerns enables instant, non-interactive exits via balance proofs, while block proofs handle most of the validations, minimizing users costs. By leveraging Incrementally Verifiable Computation (IVC), PlasmaFold achieves concrete efficiency. Users can update their balance proofs within a browser in under 1 second per transaction using less than 1 GB of RAM. Furthermore, only the identities of users who have acknowledged data receipt are posted to L1, ensuring data availability with a minimal on-chain footprint. This design keeps L1 costs extremely low, enabling a theoretical throughput of over 14000 transactions per second.

## 12 [GSSS25] SLVer Bullet: Straight-Line Verification for Bulletproofs

Eagen proposed "straight-line verification" for checking elliptic curve group operations using only linear combinations in the base field, enabling efficient proofs in inner product argument systems and R1CS. Parker applied this method in FCMP++ for scalar multiplication verification. This work formalizes and improves Eagen's informal technique. Previous formalization attempts by Bassa had soundness issues - specifically, assumed rational solutions to polynomial systems that don't actually exist. The authors resolve this by working with verification equations that reduce to a simpler form. For three collinear points $P, Q, R$ on elliptic curve $\mathcal{E}$ with slope $\lambda$ and $x$-coordinates $X_P, X_Q, X_R$, the dependency relation $\lambda^2 = X_P + X_Q + X_R$ gives $dX_R = -dX_P - dX_Q$ for any derivation $d$ on function field $K(\mathcal{E})$. This allows further computational reductions. The method shifts verification costs from verifier to prover by replacing expensive field divisions with cheaper arithmetic using logarithmic derivatives - reducing to just one division operation total. The authors provide formal completeness and soundness analysis with improved error bounds. Applications include speeding up verification in Schnorr identification schemes, Bulletproofs, and cryptocurrencies like Monero and Salvium. The approach generically improves verifier computation in discrete-logarithm-based protocols.

## 13 [YLZ+25] HyperFond: A Transparent and Post-Quantum Distributed SNARK with Polylogarithmic Communication

In this paper, we introduce HyperFond , the first distributed SNARK that enjoys a transparent setup, post-quantum security and polylogarithmic communication cost, as well as the field-agnostic property (no reliance on specific choices of fields). To this end, we first propose a distributed proof system based on HyperPlonk (by Chen et al. in EUROCRYPT 2023). To instantiate the system, we then put forward a novel approach to distribute the multilinear polynomial commitment scheme in BaseFold (by Zeilberger et al. in CRYPTO 2024), and also present a trade-off between communication cost and proof size. In HyperFond , after committing to polynomial coefficients with quasilinear complexity, each sub-prover generates proofs with time linear in subcircuit size. We implement HyperFond using up to 16 ma-

chines. Experimental results demonstrate that the proving time of is 14.3 × faster than HyperPlonk instantiated with BaseFold. We also compare to deVirgo (by Xie et al. in CCS 2022), so far the only post-quantum distributed SNARK, and achieve a 1.89 × speedup.

## 14 [LZC+25] Shred-to-Shine Metamorphosis in Polynomial Commitment Evolution

We propose $\text{PIP}_{\text{FRI}}$ , an FRI-based MLPCS that unites the linear prover time of PCSs from encodable codes with the compact proofs and fast verification of Reed-Solomon (RS) PCSs. By cutting FFT and hash overhead for both committing and opening, $\text{PIP}_{\text{FRI}}$ runs 10× faster in prover than the RS-based DeepFold (Usenix Security'25) while retaining competitive proof size and verifier time, and beats Orion (Crypto'22) from linear codes by 3.5 -fold in prover speed while reducing proof size and verification time by 15 -fold. Its distributed version $\text{DePIP}_{\text{FRI}}$ delivers the first code-based distributed SNARK for arbitrary circuits over a single polynomial, and further achieves accountability. $\text{DePIP}_{\text{FRI}}$ outperforms DeVirgo (CCS'22)—the only prior code-based distributed MLPCS, limited to data-parallel circuits and lacking accountability—by 25× in prover time and 7× in communication, with the same number of provers. A central insight in both constructions is the shred-to-shine technique. It further yields a group-based MLPCS of independent interest, with 16× shorter structured reference string and 10× faster opening time than multilinear KZG (TCC'13).

## References


[DMZ25] Pierre Daix-Moreux and Chengru Zhang. PlasmaFold: An efficient and scalable layer 2 with client-side proving. Cryptology ePrint Archive, Paper 2025/1300, 2025. (In pages 2 and 5).

[FDR+25] Vivian Fang, Emma Dauterman, Akshay Ravoor, Akshit Dewan, and Raluca Ada Popa. LegoLog: A configurable transparency log. Cryptology ePrint Archive, Paper 2025/1234, 2025. (In pages 1 and 3).

[Fu25] Shihui Fu. Improved constant-sized polynomial commitment schemes without trusted setup. Cryptology ePrint Archive, Paper 2025/1233, 2025. (In pages 1 and 3).

[GSSB25] Tom Godden, Ruben De Smet, Kris Steenhaut, and An Braeken. Efficiently parsing existing eID documents for zero-knowledge proofs. Cryptology ePrint Archive, Paper 2025/1266, 2025. (In pages 1 and 3).

[GSSS25] Brandon Goodell, Rigo Salazar, Freeman Slaughter, and Luke Szramowski. SLVer bullet: Straight-line verification for bulletproofs. Cryptology ePrint Archive, Paper 2025/1345, 2025. (In pages 2 and 6).

[Ila25] Rahul Ilango. Gdel in cryptography: Effectively zero-knowledge proofs for NP with no interaction, no setup, and perfect soundness. Cryptology ePrint Archive, Paper 2025/1296, 2025. (In pages 1 and 4).

[KLNO25] Michael Kloo, Russell W. F. Lai, Ngoc Khanh Nguyen, and Micha Osadnik. RoK and roll verifier-efficient random projection for $\tilde{O}(\lambda)$-size lattice arguments. Cryptology ePrint Archive, Paper 2025/1220, 2025. (In pages 1 and 3).

[Lon25] Jieyi Long. Interstellar: GKR protocol based low prover cost folding scheme for circuit satisfiability. Cryptology ePrint Archive, Paper 2025/1294, 2025. (In pages 1 and 4).

[LZC+25] Weihan Li, Zongyang Zhang, Sherman S. M. Chow, Yanpei Guo, Boyuan Gao, Xuyang Song, Yi Deng, and Jianwei Liu. Shred-to-shine metamorphosis in polynomial commitment evolution. Cryptology ePrint Archive, Paper 2025/1354, 2025. (In pages 2 and 7).

[MRR25] Tamer Mour, Alon Rosen, and Ron Rothblum. Tree PCPs. Cryptology ePrint Archive, Paper 2025/1252, 2025. (In pages 1 and 3).

[PP25] Christodoulos Pappas and Dimitrios Papadopoulos. Hobbit: Space-efficient zkSNARK with optimal prover time. Cryptology ePrint Archive, Paper 2025/1214, 2025. (In pages 1 and 3).

[TMM25] Debadrita Talapatra, Nimish Mishra, and Debdeep Mukhopadhyay. Ring-LWR based commitments and ZK-PoKs with application to verifiable quantum-safe searchable symmetric encryption. Cryptology ePrint Archive, Paper 2025/1216, 2025. (In pages 1 and 3).

[XGBK25] Hua Xu, Mariana Gama, Emad Heydari Beni, and Jiayi Kang. FRIttata: Distributed proof generation of FRI-based SNARKs. Cryptology ePrint Archive, Paper 2025/1285, 2025. (In pages 1 and 3).

[YLZ+25] Yuanzhuo Yu, Mengling Liu, Yuncong Zhang, Shi-Feng Sun, Tianyi Ma, Man Ho Au, and Dawu Gu. HyperFond: A transparent and post-quantum distributed SNARK with polylogarithmic communication. Cryptology ePrint Archive, Paper 2025/1349, 2025. (In pages 2 and 6).