ZKEXPress (2025.07)

Kurt Pan @ ZKPunk

July 25, 2025

Contents

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

In this work, we introduce Hobbit, the only existing space-efficient zkSNARK that achieves optimal prover time $O(|C|)$ for an arithmetic circuit C. At the same time, Hobbit is the first transparent and plausibly post-quantum secure construction of its kind. Moreover, our experimental evaluation shows that Hobbit outperforms all prior general-purpose space-efficient zkSNARKs in the literature across four different applications (arbitrary arithmetic circuits, inference of pruned Multi-Layer Perceptron, batch AES128 evaluation, and select-andaggregate SQL query) by $\times 8 - \times 56$ in terms or prover time while requiring up to $\times 23$ less total space. At a technical level, we introduce two new building blocks that may be of independent interest: (i) the first sumcheck protocol for products of polynomials with optimal prover time in the streaming setting, and (ii) a novel multi-linear plausibly post-quantum polynomial commitment that outperforms all prior works in prover time (and can be tuned to work in a space-efficient manner). We build Hobbit by combining the above with a modified version of

HyperPlonk, providing an explicit routine to stream access to the circuit evaluation.

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

In this work, we propose a zero-knowledge proof of knowledge using the Ring Learning with Rounding (RLWR) assumption for an interesting and useful class of statements: linear relations on polynomials. We begin by proposing, to the best of our knowledge, the first efficient commitment scheme in literature based on the hardness of RLWR assumption. We establish two properties on RLWR that aid in the construction of our commitments: (i) closure under addition with double rounding, and (ii) closure under multiplication with a short polynomial. Building upon our RLWR commitment scheme, we consequently design a RLWR based Σ_2 protocol for proving knowledge of a single committed message under linear relations with public polynomials. As an use-case of our proposed Σ_2 protocol, we showcase a construction of a quantum-safe Searchable Symmetric Encryption (SSE) scheme by plugging a prior LWR based SSE scheme from (EuroS&P 2023) with our Σ_2 protocol. Concretely, using our Σ_2 protocol for linear relations, we prove the correctness of an encrypted search result in a zero-knowledge manner. We implement our verifiable SSE framework and show that the overhead of an extra verification round is negligible (0.0023 seconds) and retains the asymptotic query execution time complexity of the original SSE scheme. Our work establishes results on zero-knowledge proof systems that can be of independent interest. By shifting the setting from RLWE to RLWR, we gain significant (i) efficiency improvements in terms of communication complexity by $O(M)$ (since some prior works on RLWE require rejection sampling by a factor of M), as well as (ii) very short proof size (8.4 KB) and tighter parameters (since RLWR does not explicitly manipulate error polynomials like RLWE).

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

We introduce RoK and Roll, the first lattice-based SNARK that breaks the quadratic barrier, achieving communication complexity of $\tilde{O}(\lambda)$ together

with a succinct verification time. The protocol significantly improves upon the state of the art of fully-succinct argument systems established by "'RoK, Paper, SISsors'" (RPS) [ASIACRYPT'24] and hinges on two key innovations, presented as reductions of knowledge (RoKs): *Structured random projections*: We introduce a new technique for structured random projections that allows us to reduce the witness dimensions while approximately preserving its ℓ_2 norm and maintaining the desired tensor structure. In order to maintain succinct communication and verification, the projected image is further committed and adjoined to the original relation. This procedure is recursively repeated until dimension of the intermediate witness becomes poly(λ), i.e. independent of the original witness length. *Unstructured random projection*: When the witness is sufficiently small, we let the unstructured projection (over coefficients $\mathbb{Z}_q$) be sent in plain, as in LaBRADOR [CRYPTO'23]. We observe, however, that the strategy from prior works to immediately lift the projection claim to $\mathcal{R}_q$, and into our relation, would impose a quadratic communication cost. Instead, we gradually batch-and-lift the projection a the tower of intermediate ring extensions. This reduces the communication cost to $\tilde{O}(\lambda)$ while maintaining a succinct verification time. These two techniques, combined with existing RoKs from RPS, yield a succinct argument system with communication complexity $\tilde{O}(\lambda)$ and succinct verification for structured linear relations.

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

In this work, we address this challenge by presenting a set of novel batching and aggregation techniques tailored for proofs of knowledge of ranges in GUOs. These techniques may also be of independent interest and are readily applicable to enhance and shorten other existing schemes in GUOs. Consequently, by applying these techniques, we immediately achieve an improved PCS with an evaluation proof consisting of only 10 group elements—an impressive 85% reduction. To our knowledge, this represents the shortest PCS in the transparent setting. Thus compiling known information-theoretic proof systems using our improved PCS yields highly compact transparent argument systems when instantiated in a class group, which is more practical than prior constant-sized schemes.

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

We present the first configurable transparency log design, LegoLog, which we implement and empirically evaluate end- to-end for three specialized transparency logs. We also show that LegoLog can express six different applications, and we compare the asymptotic complexity of LegoLog and existing transparency logs tailored to individual applications. We find that configurability does not come at the cost of performance: LegoLog can capture a variety of applications while performing comparably to existing, special-purpose transparency logs.

6 [MRR25] Tree PCPs

Inspired by tree codes (Schulman, STOC'93), we propose tree PCPs; these are PCPs that evolve as the computation progresses so that a proof for time t is obtained by appending a short string to the end of the proof for time $t-1$. At any given time, the tree PCP can be locally queried to verify the entire computation so far. We construct tree PCPs for non-deterministic space-s computation, where at time step t, the proof only grows by an additional $poly(s, \log(t))$ bits, and the number of queries made by the verifier to the overall proof is $poly(s) \cdot t^{\epsilon}$, for an arbitrary constant $\epsilon > 0$. Tree PCPs are well-suited to proving correctness of ongoing computation that unfolds over time. They may be thought of as an information-theoretic analog of the cryptographic notion of incrementally verifiable computation (Valiant, TCC'08). In the random oracle model, tree PCPs can be compiled to realize a variant of incrementally verifiable computation where the prover is allowed a small number of queries to a large evolving state. This yields the first construction of (a natural variant of) IVC in the random oracle model.

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

In this article, we propose an R1CS protocol to efficiently parse and extract fields from existing European National Identity Cards, with an implementation for the Belgian BeID. The protocol is able to prove correct extraction of a date-of-birth field in 22 seconds on a consumer device, with verification taking 230 milliseconds. With this, we aim to provide EU citizens with a

practical solution to the privacy and security risks that arise when one has to prove their authenticity or authority to a third party.

8 [ARZR25] Linear Prover IOPs in Log Star Rounds

Our main result is an IOP for a large class of Boolean circuits, with only $O(\log^*(S))$ rounds, where $\log^*$ denotes the iterated logarithm function (and S is the circuit size). The prover has linear size $O(S)$ and the verifier runs in time polylog (S) and has query complexity $O(\log^*(S))$. The protocol is both conceptually simpler, and strictly more efficient, than prior linear prover IOPs for Boolean circuits.

9 [Ozm25] Applications Of Zero-Knowledge Proofs On Bitcoin

This paper explores how zero-knowledge proofs can enhance Bitcoin's functionality and privacy. First, we consider Proof-of-Reserve schemes: by using zk-STARKs, a custodian can prove its Bitcoin holdings are more than a predefined threshold X, without revealing addresses or actual balances. We outline a STARK-based protocol for Bitcoin UTXOs and discuss its efficiency. Second, we examine ZK Light Clients, where a mobile or lightweight device verifies Bitcoin's proof-of-work chain using succinct proofs. We propose a protocol for generating and verifying a STARK-based proof of a chain of block headers, enabling trust-minimized client operation. Third, we explore Privacy-Preserving Rollups via BitVM: leveraging BitVM, we design a conceptual rollup that keeps transaction data confidential using zero-knowledge proofs. In each case, we analyze security, compare with existing approaches, and discuss implementation considerations. Our contributions include the design of concrete protocols adapted to Bitcoin's UTXO model and an assessment of their practicality. The results suggest that while ZK proofs can bring powerful features (e.g., on-chain reserve audits, trustless light clients, and private layer-2 execution) to Bitcoin, each application requires careful trade-offs in efficiency and trust assumptions.

10 [CHK25] On Weak NIZKs, One-way Functions and Amplification

An $(\epsilon_s, \epsilon_{zk})$-weak non-interactive zero knowledge (NIZK) argument has soundness error at most ϵ_s and zeroknowledge error at most ϵ_{zk}. We show that as long as NP is hard in the worst case, the existence of an $(\epsilon_s, \epsilon_{zk})$-weak NIZK proof or argument for NP with $\epsilon_{zk} + \sqrt{\epsilon_s} < 1$ implies the existence of one-way functions. To obtain this result, we introduce and analyze a strong version of universal approximation that may be of independent interest. As an application, we obtain NIZK amplification theorems based on very mild worst-case complexity assumptions. Specifically, [Bitansky-Geier, CRYPTO'24] showed that $(\epsilon_s, \epsilon_{zk})$-weak NIZK proofs (with ϵ_s and ϵ_{zk} constants such that $\epsilon_s + \epsilon_{zk} < 1$) can be amplified to make their errors negligible, but needed to assume the existence of one-way functions. Our results can be used to remove the additional one-way function assumption and obtain NIZK amplification theorems that are (almost) unconditional; only requiring the mild worst-case assumption that if NP $\subseteq$ ioP/poly, then NP $\subseteq$ BPP.

11 [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 before 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.

12 [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.

13 [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.

14 [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.

15 [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 formaliza-

tion 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 λ 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.

16 [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 machines. 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.

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

We propose PIP_{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, PIP_{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

[ARZR25] Noor Athamnah, Noga Ron-Zewi, and Ron D. Rothblum. Linear prover IOPs in log star rounds. Cryptology ePrint Archive, Paper 2025/1269, 2025. (In pages 1 and 6).

[CHK25] Suvradip Chakraborty, James Hulett, and Dakshita Khurana. On weak NIZKs, one-way functions and amplification. Cryptology ePrint Archive, Paper 2025/1276, 2025. (In pages 1 and 7).

[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 9).

[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 5).

[Fu25] Shihui Fu. Improved constant-sized polynomial commitment schemes without trusted setup. Cryptology ePrint Archive, Paper 2025/1233, 2025. (In pages 1 and 4).

[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 5).

[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 9).

[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 2 and 8).

[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 2 and 8).

[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 11).

[MRR25] Tamer Mour, Alon Rosen, and Ron Rothblum. Tree PCPs. Cryptology ePrint Archive, Paper 2025/1252, 2025. (In pages 1 and 5).

[Ozm25] Yusuf Ozmi. Applications of zero-knowledge proofs on bitcoin. Cryptology ePrint Archive, Paper 2025/1271, 2025. (In pages 1 and 6).

[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 2).

[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 2 and 7).

[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 10).