ZKExpress (2025.08)

Kurt Pan @ ZKPunk

August 31, 2025

Contents

1 [FGR+25] Collaborative zkSNARKs with Sublinear Prover Time and Constant Proof Size 2

2 [BB25] Optimizing Backend Verification in zk-Rollup Architectures 3

3 [BBC+25] qedb: Expressive and Modular Verifiable Databases (without SNARKs) 3

4 [WKK+25] BACON: An Improved Vector Commitment Construction with Applications to Signatures 4

5 [WCT+25] AVPEU: Anonymous Verifiable Presentations with Extended Usability 4

6 [CFP25] When Can We Incrementally Prove Computations of Arbitrary Depth? 4

7 [BNNP25] Data Availability Sampling with Repair 5

8 [ACM+25] Coral: Fast Succinct Non-Interactive Zero-Knowledge CFG Proofs 6

9 [ADM+25] Efficient randomized strong 2-source non-malleable extractor for any linear min-entropy 6

10 [ESTR25] Design ZK-NR: A Post-Quantum Layered Protocol for Legally Explainable Zero-Knowledge Non-Repudiation Attestation 6

11 [SMX+25] TLShare: Private Authenticated MPC and FHE Inputs Over TLS **7**

12 [FZ25] zip: Reducing Proof Sizes for Hash-Based SNARGs **7**

13 [BCF+25] Time-Space Trade-Offs for Sumcheck **7**

14 [DYY25] PQ-STAR: Post-Quantum Stateless Auditable Rekeying **8**

15 [HM25] Tight Bounds on Uniform-Challenge Black-Box Reductions from Sigma Protocols **8**

16 [Fu25] Inner-Product Commitments Over Integers With Applications to Succinct Arguments **9**

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.

3 [BBC+25] qedb: Expressive and Modular Verifiable Databases (without SNARKs)

One of our primary contributions is a foundational framework that cleanly separates VDB logic from cryptographic instantiations. At its essence, it resembles other common information theoretic frameworks, such as Polynomial Interactive Oracle Proofs (PIOPs). At the same time it diverges from existing approaches by being slightly specialized for the database setting. We demonstrate how to instantiate our framework using modern pairing-based linear-map vector commitments and set accumulators. More in general, we show that our building blocks can be derived from extractable homomorphic polynomial commitments. Being modular, our approach permits alternative instantiations, such as with lattice-based polynomial commitments enabling post-quantum security.

4 [WKK+25] BACON: An Improved Vector Commitment Construction with Applications to Signatures

Inspired by the large-GGM based BAVC and the cGGM tree, this paper proposes BACON, a BAVC with aborts scheme by leveraging a large cGGM tree. BACON executes multiple instances of AVC in a single batch and enables an abort mechanism to probabilistically reduce the commitment size. We prove that BACON is secure under the ideal cipher model and the random oracle model. We also discuss the possible application of the proposed BACON, i.e., FAEST version 2. Furthermore, because the number of hash calls in a large cGGM tree is halved compared with that used in a large GGM tree, theoretically, our BACON is more efficient than the state-of-the-art BAVC scheme.

5 [WCT+25] AVPEU: Anonymous Verifiable Presentations with Extended Usability

In this paper, we present Anonymous Verifiable Presentations with Extended Usability (AVPEU), a novel framework that addresses this limitation (cannot effectively verify cross-domain credentials while maintaining anonymity.) through the introduction of a notary system. At the technical core of AVPEU lies our proposed randomizable message-hiding signature scheme. We provide both a generic construction of AVPEU and specific implementations based on Boneh-Boyen-Shacham (BBS), Camenisch-Lysyanskaya (CL), and Pointcheval-Sanders (PS) signature. Our experimental results demonstrate the feasibility of these schemes.

6 [CFP25] When Can We Incrementally Prove Computations of Arbitrary Depth?

First, we revisit the security analysis, in the unbounded-depth regime, of the canonical construction of IVC based on the recursive composition of SNARKs. We extend this analysis to include SNARKs that are straightline extractable in the algebraic group model (AGM) and some additional oracle model. As a consequence of our result, we obtain novel instantiations of IVC for unbounded-depth computations based on AGM-based SNARKs, such as Groth16 or Marlin, to name a fewan important class of SNARKs

not captured by similar analyses in prior work [Chiesa et al. TCC 2024]. Second, we consider incremental proof systems for arbitrary depth computations in which full-blown extractability is not necessary. We study under what conditions they can be instantiated from the recursive composition of "plain" building blocks (SNARKs, folding, accumulation schemes), that is without requiring special straightline extractability. We introduce incremental functional commitments (incremental FC), a primitive that allows one to commit to a large data D and later prove a function $f(D)$. The key aspect is that both the committing and proving functionalities operate incrementally, processing D in a streaming, piece-by-piece manner. Also, like in standard FCs, their security property is a form of evaluation binding, a notion that is weaker than knowledge-soundness (it states that it is hard to produce two valid proofs for the same commitment and two distinct outputs). Our second main result consists of a construction of incremental FCs based on recursive composition of SNARKs and its security analysis, which shows that arbitrarily deep compositions of primitives with non-straightline extractors do not suffer from inherent security limitations.

7 [BNNP25] Data Availability Sampling with Repair

First, we provide a new definitional framework that formalizes the notion of repair, along with the security guarantees that a DAS scheme must provide. Second, we propose a new DAS scheme designed with efficient repair in mind, based on locally-correctable multiplicity codes. To facilitate using these codes, we introduce a new multivariate polynomial commitment scheme that (i) supports efficient openings of partial derivatives of a committed polynomial, (ii) supports fast batch opening proof generation at many points, and (iii) has an algorithm to recompute (repair) opening proofs at a point from only a few other proofs. The proposed scheme improves upon the state-of-the-art Ethereum Fulu DAS scheme, slated for deployment in late 2025/early 2026, in storage overhead, repair bandwidth and coordination, while only slightly increasing dispersal cost and sampling bandwidth. Our techniques readily carry over to data availability schemes based on verifiable information dispersal (VID).

8 [ACM+25] Coral: Fast Succinct Non-Interactive Zero-Knowledge CFG Proofs

We introduce Coral, a system for proving in zero- knowledge that a committed byte stream corresponds to a structured object in accordance to a Context Free Grammar. Once a prover establishes the validity of the parsed object with Coral, they can selectively prove facts about the objectsuch as fields in Web API responses or in JSON Web Tokensto third parties or blockchains. Coral reduces the problem of correct parsing to a few simple checks over a left-child right-sibling tree and introduces a novel segmented memory abstraction that unifies and extends prior constructions for RAM in zkSNARKs.

9 [ADM+25] Efficient randomized strong 2-source non-malleable extractor for any linear min-entropy

In this work, we construct a two-source non-malleable extractor in the Common Reference String (CRS) model, where a random low-degree polynomial is sampled once and made accessible to independent random sources, the distinguisher, and the tamperer. Our results advance the state of non-malleable cryptographic primitives, with applications in secure storage, leakage-resilient cryptography, and privacy amplification. By eliminating the need for strong computational hardness assumptions, our techniques provide a more foundational and widely applicable method for randomness extraction. We also show, that the requirements on CRS for our application are so mild that the CRS can be sampled with party computation even when one of the parties is malicious (setting in which establishing unbiased coins is impossible).

10 [ESTR25] Design ZK-NR: A Post-Quantum Layered Protocol for Legally Explainable Zero-Knowledge Non-Repudiation Attestation

This article presents the architectural design of Zero Knowledge Non-Repudiation (ZK-NR), a layered cryptographic protocol enabling post-quantum secure, legally interpretable, and verifiably non-repudiable attestations. Built upon STARK-based zero-knowledge proofs, hybrid post-quantum signatures, and entropy-accumulating ledger anchoring, ZK-NR satisfies the structural properties of both the Q2CSI framework and the NIZK-E model. The proto-

col achieves semantic interpretability by structurally separating contextual proofs from bounded explanations, while maintaining cryptographic soundness under the Universal Composability framework.

11 [SMX+25] TLShare: Private Authenticated MPC and FHE Inputs Over TLS

We introduce TLShare, a framework that extracts authenticated data from a TLS connection and imports it into secure multiparty computation (MPC) or fully homomorphic encryption (FHE), without requiring server-side changes or exposing client credentials. Unlike prior work, TLShare allows the payload itself, not just a predicate about it, to serve as private input to secure downstream computation. TLShare supports combining verifiable inputs across multiple clients and servers, enabling new applications such as privacy-preserving financial risk assessment and collaborative analytics. We design three protocols for TLShare: one for MPC using verifiable secret sharing, and two for FHE using interactive and non-interactive zero-knowledge proofs, each ensuring input authenticity, integrity, and end-to-end privacy. We evaluate all three protocols of TLShare over both LAN and WAN settings, comparing their trade-offs and demonstrating their practicality.

12 [FZ25] zip: Reducing Proof Sizes for Hash-Based SNARGs

We present a non-recursive proof compression technique to reduce the size of hash-based succinct arguments. The technique is black-box in the underlying succinct arguments, requires no trusted setup, can be instantiated from standard assumptions (and even when P=NP !) and is concretely efficient.

13 [BCF+25] Time-Space Trade-Offs for Sumcheck

We study time-space tradeoffs for the prover of the sumcheck protocol in the streaming model, and provide upper and lower bounds that tightly characterize the efficiency achievable by the prover.

14 [DYY25] PQ-STAR: Post-Quantum Stateless Auditable Rekeying

We introduce Post-Quantum Stateless Auditable Rekeying (PQ-STAR), a novel post-quantum secure stateless rekeying scheme with audit support. PQ-STAR is presented in three variants of increasing security guarantees: (i) Plain PQ-STAR lets an authorized auditor decrypt and verify selected ciphertexts; (ii) Commitment-based PQ-STAR with the additional binding guarantee from the commitments, preventing a malicious sender from potentially claiming a random or wrong session key. (iii) Zero-knowledge PQ-STAR equips each session key with a signature-based zero-knowledge proof (ZKP), which proves that the session key was derived honestly, without ever revealing the secret preimage. We formally prove that all variants achieve key-uniqueness, index-hiding, and forward-secrecy, even if a probabilistic polynomial-time (PPT) adversary arbitrarily learns many past session keys.

15 [HM25] Tight Bounds on Uniform-Challenge Black-Box Reductions from Sigma Protocols

In this work, we show that this quadratic loss is inherent for two natural classes of reductions. For interactive protocols, we prove it for uniform-challenge, black-box reductions, which query the adversary using uniformly sampled challenges. For non-interactive protocols (i.e., in the random-oracle model), we prove it for weakly programmable, black-box reductions, which answer the adversarys oracle queries with uniformly sampled outputs. Applying our bounds to the reductions from Schnorr identification and signatures to discrete logarithm yields lower bounds that match known positive resultsnamely, the classical worst-case reduction of Pointcheval and Stern (Journal of Cryptology, 2000) and the higher-moment reduction of Rotem and Segev (Journal of Cryptology, 2024). Our approach reduces the analysis of such reductions to the values of simple hitting gamescombinatorial games that we introduce. Bounding these games is our main technical contribution, and we believe these bounds can enable more modular proofs of related results.

16 [Fu25] Inner-Product Commitments Over Integers With Applications to Succinct Arguments

Due to the significant applicability of inner-product arguments (IPA) in constructing succinct proof systems, in this work, we extend them to work natively in the integer setting. We introduce and construct inner-product commitment schemes over integers that allow a prover to open two committed integer vectors to a claimed inner product. The commitment size is constant and the verification proof size is logarithmic in the vector length. The construction significantly improves the slackness parameter of witness extraction, surpassing the existing state-of-the-art approach. Our construction is based on the folding techniques for Pedersen commitments defined originally over $\mathbb{Z}_p$. Building upon our IPAs, we first present a novel batchable argument of knowledge of nonnegativity of exponents that can be used to further reduce the proof size of Dew-PCS (Arun et al., PKC 2023). Second, we present a construction for range proofs that allows for extremely efficient batch verification of a large number of range proofs over much larger intervals. We also provide a succinct zero-knowledge argument of knowledge with a logarithmic-size proof for more general arithmetic circuit satisfiability over integers.

References

[ACM+25] Sebastian Angel, Sofa Celi, Elizabeth Margolin, Pratyush Mishra, Martin Sander, and Jess Woods. Coral: Fast succinct non-interactive zero-knowledge CFG proofs. Cryptology ePrint Archive, Paper 2025/1420, 2025. (In pages 1 and 6).

[ADM+25] Divesh Aggarwal, Pranjal Dutta, Saswata Mukherjee, Satyajeet Nagargoje, and Maciej Obremski. Efficient randomized strong 2-source non-malleable extractor for any linear min-entropy. Cryptology ePrint Archive, Paper 2025/1421, 2025. (In pages 1 and 6).

[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 3).

[BBC+25] Vincenzo Botta, Simone Bottoni, Matteo Campanelli, Emanuele Ragnoli, and Alberto Trombetta. qedb: Expressive and modu-

lar verifiable databases (without SNARKs). Cryptology ePrint Archive, Paper 2025/1408, 2025. (In pages 1 and 3).

[BCF+25] Anubhav Baweja, Alessandro Chiesa, Elisabetta Fedele, Giacomo Fenzi, Pratyush Mishra, Tushar Mopuri, and Andrew Zitek-Estrada. Time-space trade-offs for sumcheck. Cryptology ePrint Archive, Paper 2025/1473, 2025. (In pages 2 and 7).

[BNNP25] Dan Boneh, Joachim Neu, Valeria Nikolaenko, and Aditi Partap. Data availability sampling with repair. Cryptology ePrint Archive, Paper 2025/1414, 2025. (In pages 1 and 5).

[CFP25] Matteo Campanelli, Dario Fiore, and Mahak Pancholi. When can we incrementally prove computations of arbitrary depth? Cryptology ePrint Archive, Paper 2025/1413, 2025. (In pages 1 and 4).

[DYY25] Shlomi Dolev, Avraham Yagudaev, and Moti Yung. PQ-STAR: Post-quantum stateless auditable rekeying. Cryptology ePrint Archive, Paper 2025/1489, 2025. (In pages 2 and 8).

[ESTR25] Minka Mi Nguidjoi Thierry Emmanuel, Mani Onana Flavien Serge, Djotio Ndi Thomas, and Atsa Etoundi Roger. Design ZK-NR: A post-quantum layered protocol for legally explainable zero-knowledge non-repudiation attestation. Cryptology ePrint Archive, Paper 2025/1422, 2025. (In pages 1 and 6).

[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 pages 1 and 2).

[Fu25] Shihui Fu. Inner-product commitments over integers with applications to succinct arguments. Cryptology ePrint Archive, Paper 2025/1536, 2025. (In pages 2 and 9).

[FZ25] Giacomo Fenzi and Yuwen Zhang. zip: Reducing proof sizes for hash-based SNARGs. Cryptology ePrint Archive, Paper 2025/1446, 2025. (In pages 2 and 7).

[HM25] Iftach Haitner and Nikolaos Makriyannis. Tight bounds on uniform-challenge black-box reductions from sigma protocols. Cryptology ePrint Archive, Paper 2025/1535, 2025. (In pages 2 and 8).

[SMX+25] Manuel B. Santos, Dimitris Mouris, Xiang Xie, Miguel de Vega, and Andrei Lapets. TLShare: Private authenticated MPC and FHE inputs over TLS. Cryptology ePrint Archive, Paper 2025/1434, 2025. (In pages 2 and 7).

[WCT+25] Yalan Wang, Liqun Chen, Yangguang Tian, Long Meng, and Christopher J.P. Newton. AVPEU: Anonymous verifiable presentations with extended usability. Cryptology ePrint Archive, Paper 2025/1412, 2025. (In pages 1 and 4).

[WKK+25] Yalan Wang, Bryan Kumara, Harsh Kasyap, Liqun Chen, Sumanta Sarkar, Christopher J.P. Newton, Carsten Maple, and Ugur Ilker Atmaca. BACON: An improved vector commitment construction with applications to signatures. Cryptology ePrint Archive, Paper 2025/1411, 2025. (In pages 1 and 4).