SnarkExpress

(2025 Q3)

Edited by KurtPan@ ZKPunk

October 15, 2025

Contents

Chapter 1

2025.07

1.1 [cryptoeprint:2025/1214] 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.

1.2 [cryptoeprint:2025/1216] 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).

1.3 [cryptoeprint:2025/1220] 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.

1.4 [cryptoeprint:2025/1233] 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.

1.5 [cryptoeprint:2025/1234] 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.

1.6 [cryptoeprint:2025/1252] 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.

1.7 [cryptoeprint:2025/1266] 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.

1.8 [cryptoeprint:2025/1269] Linear Prover IOPs in Log Star Rounds

Our main result is an IOP for a large class of Boolean circuits, with only $O\left(\log^*(S)\right)$ 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 $O\left(\log^*(S)\right)$. The protocol is both conceptually simpler, and strictly more efficient, than prior linear prover IOPs for Boolean circuits.

1.9 [cryptoeprint:2025/1271] 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.

1.10 [cryptoeprint:2025/1276] On Weak NIZKs, One-way Functions and Amplification

An $(\epsilon_{\mathrm{s}}, \epsilon_{\mathrm{zk}})$-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 ($\epsilon_{\mathrm{s}}, \epsilon_{\mathrm{zk}}$)-weak NIZK proof or argument for NP with $\epsilon_{\mathrm{zk}} + \sqrt{\epsilon_{\mathrm{s}}} < 1$ 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 $(\epsilon_{\mathrm{s}}, \epsilon_{\mathrm{zk}})$-weak NIZK proofs (with ϵ_{s} and ϵ_{zk} constants such that $\epsilon_{\mathrm{s}} + \epsilon_{\mathrm{zk}} < 1$) 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.

1.11 [FRIttata] 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.

1.12 [Interstellar] 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.

1.13 [Godel] 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 Krajícek-Pudlák conjecture that no optimal proof system exists (a major proof complexity conjecture related to Gödel'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.

1.14 [PlasmaFold] 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.

1.15 [SLVerBullet] 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 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.

1.16 [HyperFond] 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.

1.17 [Shred-to-Shine] Shred-to-Shine Metamorphosis in Polynomial Commitment Evolution

We propose $\mathrm{PIP}_{\mathrm{FRI}}$, 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, $\mathrm{PIP}_{\mathrm{FRI}}$ 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 DePIP $_{\mathrm{FRI}}$ delivers the first code-based distributed SNARK for arbitrary circuits over a single polynomial, and further achieves accountability. DePIP $_{\mathrm{FRI}}$ 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).

1.18 [cryptoeprint:2025/1364] A Framework for Witness Encryption from Linearly Verifiable SNARKs and Applications

In this work we make progress by designing a modular and extensible framework, which allows us to better understand existing schemes and further enables us to construct new witness encryption schemes. The framework is designed around simple but powerful building blocks that we refer to as "gadgets". Gadgets can be thought of as witness encryption schemes for small targeted relations (induced by linearly verifiable arguments) but they can be composed with each other to build larger, more expressive relations that are useful in applications. To highlight the power of our framework we methodically recover past results, improve upon them and even provide new feasibility results. The first application of our framework is a Registered Attribute-Based Encryption Scheme [Hohenberger et al. (Eurocrypt 23)] with linear sized common reference string (CRS). Our second application is a feasibility result for Registered Threshold Encryption (RTE) with succinct ciphertexts.

1.19 [cryptoeprint:2025/1366] NOPE: Strengthening domain authentication with succinct proofs

This paper describes the design, implementation, and experimental evaluation of NOPE, a new mechanism for server authentication that uses succinct proofs (for example, zero-knowledge proofs) to prove that a DNSSEC chain exists that links a public key to a specified domain.

1.20 [cryptoeprint:2025/1368] Post-Quantum Readiness in EdDSA Chains

In this work, we observe that blockchains employing EdDSA with RFC 8032-compliant key derivation (e.g., Sui, Solana, Near, Stellar, Aptos, Cosmos) possess an underexplored structural advantage. Specifically, EdDSA's hash-based deterministic secret key generation enables post-quantum zero-knowledge proofs of elliptic curve private key ownership, which can help switching to a quantum-safe algorithm proactively without requiring transfer of assets to new addresses. We demonstrate how Post-Quantum NIZKs can be constructed to prove knowledge of the "seed" used in EdDSA key derivation, enabling post-quantum-secure transaction authorization without altering addresses or disclosing elliptic curve data.

1.21 [cryptoeprint:2025/1373] A Zero-Knowledge Proof for the Syndrome Decoding Problem in the Lee Metric

The syndrome decoding problem is one of the NP-complete problems lying at the foundation of code-based cryptography. The variant thereof where the distance between vectors is measured with respect to the Lee metric, rather than the more commonly used Hamming metric, has been analyzed recently in several works due to its potential relevance for building more efficient code-based cryptosystems. The purpose of this article is to present a zero-knowledge proof of knowledge for this variant of the problem.

1.22 [cryptoeprint:2025/1374] An Attack to Universally Composable Commitments from Malicious Physically Uncloneable Functions and how to Avoid it

In this work, we explore the possibility of unconditionally secure universally composable (UC) commitments, a very relevant cryptographic primitive in the context of secure multi-party computation. To this end, we assume the existence of Physically Uncloneable Functions (PUFs), a hardware security assumption that has been proven useful for securely achieving diverse tasks. In prior work [ASIACRYPT 2013, LNCS, vol. 8270, pp. 100–119] it was shown that a protocol for unconditional

UC-secure commitments can be constructed even when the PUFs are malicious. Here, we report an attack to this protocol, as well as a few more issues that we identified in its construction. To address them, first we revise some of the previous PUF properties, and introduce new properties and tools that allow us to rigorously develop and present the security proofs. Second, we propose two different ways for making the commitment scheme secure against the attack we found. The first involves considering a new model where the creator of a PUF is notified whenever the PUF is queried and the second involves restricting adversaries to only being able to create stateless malicious PUFs. Finally, we analyze the efficiency of our schemes and show that our constructions are advantageous in this respect compared to the original proposal.

Chapter 2

2025.08

2.1 [cryptoeprint:2025/1388] 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.

2.2 [cryptoeprint:2025/1390] 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.

2.3 [cryptoeprint:2025/1408] 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.

2.4 [cryptoeprint:2025/1411] 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.

2.5 [cryptoeprint:2025/1412] 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.

2.6 [cryptoeprint:2025/1413] 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 few—an 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.

2.7 [cryptoeprint:2025/1414] 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).

2.8 [cryptoeprint:2025/1420] 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 object—such as fields in Web API responses or in JSON Web Tokens——to 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.

2.9 [cryptoeprint:2025/1421] 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).

2.10 [cryptoeprint:2025/1422] 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 protocol achieves semantic interpretability by structurally separating contextual proofs from bounded explanations, while maintaining cryptographic soundness under the Universal Composability framework.

2.11 [cryptoeprint:2025/1434] 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.

2.12 [cryptoeprint:2025/1446] 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.

2.13 [cryptoeprint:2025/1473] 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.

2.14 [cryptoeprint:2025/1489] 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.

2.15 [cryptoeprint:2025/1535] 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 adversary's 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 results—namely, 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 games—combinatorial 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.

2.16 [cryptoeprint:2025/1536] 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.

Chapter 3

2025.09

3.1 [cryptoeprint:2025/1546] Incrementally Verifiable Computation for NP from Standard Assumptions

In this work, we observe that the Gentry-Wichs barrier can be overcome for IVC for NP. We show the following two results: - Assuming subexponential $i\mathcal{O}$ and LWE (or bilinear maps), we construct IVC for all NP with proof size $\mathsf{poly}(|x_i|, \log T)$. - Assuming subexponential $i\mathcal{O}$ and injective PRGs, we construct IVC for trapdoor IVC languages where the proof-size is $\mathsf{poly}(\log T)$. Informally, an IVC language has a trapdoor if there exists a (not necessarily easy to find) polynomial-sized circuit that determines if a configuration x_i is reachable from x_0 in i steps.

3.2 [cryptoeprint:2025/1547] Silent Threshold Cryptography from Pairings: Expressive Policies in the Plain Model

In this work, we introduce a new pairing-based approach for constructing threshold signatures and encryption schemes with silent setup. On the one hand, our techniques directly allow us to support expressive policies like monotone Boolean formulas in addition to thresholds. On the other hand, we only rely on basic algebraic tools (i.e., a simple cross-term cancellation strategy), which yields constructions with shorter signatures and ciphertexts compared to previous pairing-based constructions. As an added bonus, we can also prove (static) security under q-type assumptions in the plain model. Concretely, the signature size in our distributed threshold signature scheme is 3 group elements and the ciphertext size in our distributed threshold encryption scheme is 4 group elements (together with a short tag).

3.3 [cryptoeprint:2025/1548] Pairing-Based Aggregate Signatures without Random Oracles

In this work, we focus on simple aggregate signatures in the plain model. We construct a pairing-based aggregate signature scheme that supports aggregating an a priori bounded number of signatures N. The size of the aggregate signature is just two group elements. Security relies on the (bilateral) computational Diffie-Hellman (CDH) problem in a pairing group. To our knowledge, this is the first group-based aggregate signature in the plain model where (1) there is no restriction on what type of signatures can be aggregated; (2) the aggregated signature contains a constant number of group elements; and (3) security is based on static falsifiable assumptions in the plain model. The limitation of our scheme is that our scheme relies on a set of public parameters (whose size scales with N) and individual signatures (before aggregation) also have size that scale with N. Essentially, individual signatures contain some additional hints to enable aggregation. Our starting point is a new notion of slotted aggregate signatures. Here, each signature is associated with a "slot" and we only support aggregating signatures associated with distinct slots. We then show how to generically lift a slotted aggregate signature scheme into a standard aggregate signature scheme at the cost of increasing the size of the original signatures.

3.4 [cryptoeprint:2025/1554] UniCross: A Universal Cross-Chain Payment Protocol with On-demand Privacy and High Scalability

This paper proposes a universal cross-chain payment framework. This framework enables payments across a wide range of blockchains since it is independent of any specific blockchain features. Moreover, this framework provides on-demand privacy and high scalability. To instantiate the framework, we introduce UniCross, a novel universal cross-chain payment protocol. Concretely, we utilize the ring learning with errors (RLWE)-based encryption scheme and propose a new non-interactive zero-knowledge (NIZK) protocol, named HybridProof, to construct UniCross. We formally define the security of the universal cross-chain payment framework and prove the universal composability (UC) security of UniCross. The proof-of-concept implementation and evaluation demonstrate that (1) UniCross consumes up to 78% and 94% less communication and computation cost than the state-of-the-art work; (2) UniCross achieves a throughput ($\sim$360 tps) 36× that of the state-of-the-art work ($\sim$10 tps).

3.5 [cryptoeprint:2025/1558] Lower Bounding Update Frequency in Short Accumulators and Vector Commitments

We study the inherent limitations of additive accumulators and updatable vector commitments (VCs) with constant-size digest (i.e., independent of the number of committed elements). Specifically, we prove two lower bounds on the expected number of membership proofs that must be updated when a *single* element is added (or updated) in such data structures. Our results imply that when the digest bit length approaches the concrete security level, then the expected number of proofs invalidated due to an append operation for a digest committing to n elements is nearly maximal: $n - \mathsf{negl}(\lambda)$ in the case of exponential-size universes, and $n - o(n)$ for super-polynomial universes. Our results have significant implications for stateless blockchain designs relying on constant-size VCs, suggesting that the overhead of frequent proof updates may offset the benefits of reducing global state storage.

3.6 [cryptoeprint:2025/1566] Lattice-based Threshold Blind Signatures

We present the first construction of a threshold blind signature secure in the post-quantum setting, based on lattices. We prove its security under an interactive variant of the SIS assumption introduced in [Agrawal et al., CCS'22]. Our construction has a reasonable overhead of a factor of roughly 1.4 X to 2.5 X in signature size over comparable non-threshold blind signatures over lattices under heuristic but natural assumptions.

3.7 [cryptoeprint:2025/1569] How Hard Can It Be to Formalize a Proof? Lessons from Formalizing CryptoBox Three Times in EasyCrypt

We present a new security proof for the generic construction of a PKAE scheme from a NIKE and AE scheme, written in a code-based, game-playing style à la Bellare and Rogaway, and compare it to the same proof written in the style of state-separating proofs, a methodology for developing modular game-playing security proofs. Additionally, we explore a third “blended” style designed to avoid anticipated difficulties with the formalization. Our findings suggest that the choice of definition style impacts proof complexity—including, we argue, in detailed pen-and-paper proofs—with trade-offs depending on the proof writer’s goals.

3.8 [cryptoeprint:2025/1576] Compressed verification for post-quantum signatures with long-term public keys

A method to replace large public keys in GPV-style signatures with smaller, private verification keys. This significantly reduces verifier storage and runtime while preserving security. Applied to the conservative, short-signature schemes Wave and Squirrels.

3.9 [cryptoeprint:2025/1580] IronDict: Transparent Dictionaries from Polynomial Commitments

We present IronDict, a transparent dictionary construction based on polynomial commitment schemes. Transparent dictionaries enable an untrusted server to maintain a mutable dictionary and provably serve clients lookup queries. Our construction makes black-box use of a generic multilinear polynomial commitment scheme and inherits its security notions, i.e. binding and zero-knowledge. We implement our construction with the recent KZH scheme and find that a dictionary with 1 billion entries can be verified on a consumer-grade laptop in 35 ms, a 300× improvement over the state of the art, while also achieving 150,000× smaller proofs (8 KB). In addition, our construction ensures perfect privacy with concretely efficient costs for both the client and the server. We also show fast-forwarding techniques based on incremental verifiable computation (IVC) and checkpoints to enable even faster client auditing.

3.10 [cryptoeprint:2025/1588] Query-Optimal IOPPs for Linear-TIme Encodable Codes

We present the first IOPP for a linear-time encodable code that achieves linear prover time and $O(\lambda)$ query complexity, for a broad range of security parameters λ. No prior work is able to simultaneously achieve this efficiency: it either supports linear-time encodable codes but with worse query complexity [FICS; ePrint 2025], or achieves $O(\lambda)$ query complexity but only for quasilinear-time encodable codes [Minzer, Zheng; FOCS 2025]. Furthermore, we prove a matching lower bound that shows that the query complexity of our IOPP is asymptotically optimal (up to additive factors) for codes with constant rate. We obtain our result by tackling a ubiquitous subproblem in IOPP constructions: checking that a batch of claims hold. Our novel solution to this subproblem is twofold. First, we observe that it is often sufficient to ensure that, with all but negligible probability, most of the claims hold. Next, we devise a new ‘lossy batching’ technique which convinces a verifier of the foregoing promise with lower query complexity than that required to convince it that all the claims hold. This method differs significantly from the line-versus-point test used to achieve query-optimal IOPPs (for quasilinear-time encodable codes) in prior work [Minzer, Zheng; FOCS 2025], and may be of independent interest. Our IOPP can handle all codes that support efficient codeswitching [Ron-Zewi, Rothblum; JACM 2024], including several linear-time encodable codes. Via standard techniques, our IOPP can be used to construct the first (to the best of our knowledge) IOP for NP with $O(n)$ prover time and $O(\lambda)$ query complexity. We additionally show that our IOPP (and by extension the foregoing IOP) is round-by-round tree-extractable and hence can be used to construct a SNARK in the random oracle model with $O(n)$ prover time and $O(\lambda \log n)$ proof size.

[cryptoeprint:2024/474]

3.11 [cryptoeprint:2025/1593] Leveraging Smaller Finite Fields for More Efficient ZK-Friendly Hash Functions

In this paper, we examine the applicability of the generalized subfield construction and the possibility of improvements on ZK-friendly hash functions. As a case study, we focus on a recent ZK-friendly hash function Vision Mark-32 presented by Ashur et al. in [IACR Preprint 2024/633]. In particular, instead of using a 24×24 MDS matrix over $\mathbb{F}_{2^{32}}$ for a 24×1 column input over $\{0,1\}^{32}$, we suggest separating the 24×1 column input over $\{0,1\}^{32}$ into four 24×1 subcolumns over $\{0,1\}^{8}$ and then using a 24×24 MDS matrix over $\mathbb{F}_{2^8}$ for each subcolumn. This method still keeps the maximum diffusion property without any compromise and provides simplicity and efficiency. For example, it is possible to significantly decrease the required LUT values to 265 from about 9200 and FF values to 102 from about 4600 for the hardware implementation. We also highlight that we do not need any additional tricks such as NTT for field multiplications. We also push the theoretical boundaries of the generalized subfield construction to see how much small finite fields we can use, examine the arithmetization complexity, and discuss its applicability to other ZK-friendly hash functions.

3.12 [cryptoeprint:2025/1596] On GPU acceleration of PQC algorithms

This paper investigates their acceleration using GPUs. We implemented Dilithium, FrodoKEM, and SPHINCS+ on GPUs using CUDA and benchmarked them together with an existing GPU implementation of Kyber on a Tesla A100 and on a RTX 2070 Super. Dilithium performed convincingly on both GPUs, achieving speed-ups in key generation, signing, and verify by factors of around 820, 2,724 and 2,609 on the A100 and 198, 714 and 802 on the RTX 2070 using the optimal batch sizes. SPHINCS+ achieved speed-ups by factors of around 715, 4,114 and 5,915 on the A100 and 193, 193 and 134 on the RTX 2070. FrodoKEM's key generation, encapsulation, and decapsulation on the A100 were accelerated by factors of 9,989, 4,726, and 3,566. It performed speed-up factors of 107, 108, and 206 on the RTX 2070, respectively. We compared to Kyber's acceleration factors of 476, 513 and 1782 on the A100 and 18.5, 17.4 and 184.5 on the RTX 2070. In addition, we investigated the effect of using a variable set of CUDA streams for FrodoKEM. Here, using 8 streams, a speedup of another 2% could be achieved.

3.13 [cryptoeprint:2025/1646] Scalable zkSNARKs for Matrix Computations: A Generic Framework for Verifiable Deep Learning

Sublinear proof sizes have recently become feasible in verifiable machine learning (VML), yet no approach achieves the trio of strictly linear prover time, logarithmic proof size and verification time, and architecture privacy. Hurdles persist because we lack a succinct commitment to the full neural network and a framework for heterogeneous models, leaving verification dependent on architecture knowledge. Existing limits motivate our new approach: a unified proof-composition framework that casts VML as the design of zero-knowledge succinct non-interactive arguments of knowledge (zkSNARKs) for matrix computations. Representing neural networks with linear and non-linear layers as a directed acyclic graph of atomic matrix operations enables topology-aware composition without revealing the graph. Modeled this way, we split proving into a reduction layer and a compression layer that attests to the reduction with a proof of proof. At the reduction layer, inspired by reduction of knowledge (Crypto '23), root-node proofs are reduced to leaf-node proofs under an interface standardized for heterogeneous linear and non-linear operations. Next, a recursive zkSNARK compresses the transcript into a single proof while preserving architecture privacy. Complexity-wise, for a matrix expression with M atomic operations on $n \times n$ matrices, the prover runs in $O(Mn^2)$ time while proof size and verification time are $O(\log(Mn))$, outperforming known VML systems. Honed for this framework, we formalize relations directly in matrices or vectors—a more intuitive form for VML than traditional polynomials. Our LiteBullet proof, an inner-product proof based on folding and its connection to sumcheck (Crypto '21), yields a polynomial-free alternative. With these ingredients, we reconcile heterogeneity, zero-knowledge, succinctness, and architecture privacy in a single VML system.

3.14 [cryptoeprint:2025/1653] Distributed SNARK via folding schemes

In this paper, we propose a novel distributed SNARK system constructed by compiling distributed PIOP with additively homomorphic polynomial commitment, rather than distributed polynomial commitment. The core technical component is distributed SumFold, which folds multiple sum-check instances into one. After the folding process, only one prover is required to perform polynomial commitment openings. It facilitates compilation with SamaritanPCS, which is a recently proposed additively homomorphic multilinear polynomial commitment scheme. The resulting SNARK system is specifically optimized for data-parallel circuits. Compared to prior HyperPlonk-based distributed proof systems (e.g., Hyperpianist and Cirrus), our construction achieves improvements in both proof size and prover time.

3.15 [cryptoeprint:2025/1663] IVC in the Open-and-sign Random Oracle Model

To mitigate the theoretical challenges, we present the Open-and-Sign Random Oracle Model (osROM) as an extension to the signed random oracle of Chiesa and Tromer (ICS '10). This model, while strictly harder to instantiate than the Random Oracle Model, allows the design of protocols that can efficiently verify calls to the oracle and support straight-line extractors. As a result, IVC constructions in the osROM can be shown to have provable security for polynomial depths of computation. Under our new model, we construct a framework to build secure IVC schemes from simple non-interactive reductions of knowledge. Our construction natively supports cycles of elliptic curves in the style of Ben-Sasson et al. (CRYPTO '14), thus answering the practical challenge outlined above. Finally, we analyze the HyperNova (CRYPTO '24) IVC scheme in the osROM and show that it is secure over a two-cycle of elliptic curves, for polynomial depths of computation.

3.16 [cryptoeprint:2025/1698] SNARK Lower Bounds via Communication Complexity

We initiate the study of lower bounding the verification time of Succinct Non-interactive ARguments of Knowledge (SNARKs) built in the Polynomial Interactive Oracle Proof + Polynomial Commitment Scheme paradigm. The verification time of these SNARKs is generally dominated by the polynomial commitment scheme, and so we want to understand if polynomial commitment schemes admit lower bounds on the verification time. By recognizing that polynomial commitment schemes are also often built by applying cryptography to some information-theoretic core protocol, we seek to separate this core from the cryptography in a way that meaningfully captures the verification time required by the polynomial commitment scheme verifier. We provide strong evidence that several polynomial commitment schemes have (nearly) optimal verifier times. Our evidence comes from connecting polynomial commitment schemes to certain information-theoretic protocols known as communication protocols from the field of communication complexity, a link which we believe to be of independent interest. Through this lens, we model the verifier work in the cryptographic protocols as information (i.e., number of bits) exchanged between parties in the communication protocols, allowing us to leverage lower bounds from communication complexity. These lower bounds give strong evidence that the verifier time in these polynomial commitment schemes must be at least the number of bits exchanged in the communication protocol. We extract the communication protocol cores of three polynomial commitment schemes and lower bound the bits exchanged in these cores. The lower bounds we obtain match (up to poly-logarithmic factors) the best-known (asymptotic) verification times of the polynomial commitment schemes we examine in this work. Specifically, we show that for univariate/multilinear polynomials of size $N = 2^n$: - the communication core of Hyrax PCS (Wahby et al., S&P 2016) requires $\Omega(\sqrt{N})$ bits to be exchanged; - the communication core of Bulletproofs PCS (Bootle et al., EUROCRYPT 2016; Bünz et al., S&P 2018) requires $\Omega(N)$ bits to be exchanged; and - the communication core of Dory PCS (Lee, TCC 2021) requires $\Omega(\log(N))$ bits to be exchanged. Our results strongly suggest a negative answer to a longstanding open question on whether the Bulletproofs verifier can be made sublinear time.

3.17 [cryptoeprint:2025/1709] The zkVot Protocol: A Distributed Computation Protocol for Censorship Resistant Anonymous Voting

zkVot is a client side trustless distributed computation protocol that utilizes zero knowledge proving technology. It is designed to achieve anonymous and censorship resistant voting while ensuring scalability.

3.18 [cryptoeprint:2025/1712] The Syndrome-Space Lens: A Complete Resolution of Proximity Gaps for Reed-Solomon Codes

We resolve the Correlated Agreement (CA) problem for Reed-Solomon codes up to the information-theoretic capacity limit by introducing a fundamental change of basis: from the traditional evaluation domain to the syndrome space. Viewed through this "Syndrome-Space Lens," the problem of proximity testing transforms into a transparent question of linear-algebraic geometry: a single affine line of syndromes traversing a family of low-dimensional subspaces. This new perspective makes a sharp phase transition at the capacity boundary visible, allowing for a complete characterization of the problem's behavior across all parameter regimes, yielding short, self-contained proofs.

3.19 [cryptoeprint:2025/1715] UltraMixer: A Compliant Zero-Knowledge Privacy Layer for Tokenized Real-World Assets

We present UltraMixer, a noncustodial privacy layer natively compatible with ERC-3643. Compliance is enforced at the boundary via zero-knowledge proofs of whitelist membership, while in-mixer transfers and atomic trades operate over commitments with nullifiers to prevent double-spend. A generalized UTXO encoding supports heterogeneous assets (fungible and non-fungible) under a unified commitment scheme. For selective disclosure, UltraMixer provides a verdict-only Δ-Window Proof of Holding that attests to continuous ownership across a time interval without revealing balances, identities, or linkages. Gas-aware batching and composable emergency controls (pause, freeze/unfreeze, force-transfer) preserve practicality and governance. The resulting architecture delivers regulator-compatible confidentiality for permissioned RWA markets.

3.20 [cryptoeprint:2025/1723] Space-Deniable Proofs

We introduce and construct a new proof system called Non-interactive Arguments of Knowledge or Space (NArKoS), where a space bounded prover can convince a verifier they know a secret, while having access to sufficient space allows one to forge indistinguishable proofs without the secret. An application of NArKoS are space-deniable proofs, which are proofs of knowledge (say for authentication in access control) that are sound when executed by a lightweight device like a smart-card or an RFID chip that cannot have much storage, but are deniable (in the strong sense of online deniability) as the verifier, like a card reader, can efficiently forge such proofs. We construct NArKoS in the random oracle model using an OR-proof combining a sigma protocol (for the proof of knowledge of the secret) with a new proof system called simulatable Proof of Transient Space (simPoTS). We give two different constructions of simPoTS, one based on labelling graphs with high pebbling complexity, a technique used in the construction of memory-hard functions and proofs of space, and a more practical construction based on the verifiable space-hard functions from TCC'24 where a prover must compute a root of a sparse polynomial. In both cases, the main challenge is making the proofs efficiently simulatable.

3.21 [cryptoeprint:2025/1724] Efficient Aggregate Anonymous Credentials for Decentralized Identity

In this paper, we first introduce what we call aggregate tag-based signatures and describe an efficient instantiation. We then leverage the latter together with structure-preserving signatures and signatures of knowledge to construct an efficient aggregate anonymous credential scheme. We finally, formally evaluate the security of the proposed schemes and run benchmarks to showcase the practicality of the resulting scheme and its relevance for decentralized identity applications.

3.22 [cryptoeprint:2025/1732] Zero-Knowledge AI Inference with High Precision

In this work, we present ZIP, an efficient and precise commit and prove zero-knowledge SNARK for AIaaS inference (both linear and non-linear layers) that natively supports IEEE-754 double-precision floating-point semantics while addressing reliability and privacy challenges inherent in AIaaS. At its core, ZIP introduces a novel relative-error-driven technique that efficiently proves the correctness of complex non-linear layers in AI inference computations without any loss of precision, and hardens existing lookup-table and range proofs with novel arithmetic constraints to defend against malicious provers. We implement ZIP and evaluate it on standard datasets (e.g., MNIST, UTKFace, and SST-2). Our experimental results show, for non-linear activation functions, ZIP reduces circuit size by up to three orders of magnitude while maintaining the full precision required by modern AI workloads.

3.23 [cryptoeprint:2025/1741] Full L1 On-Chain ZK-STARK+PQC Verification on Solana: A Measurement Study

This work investigates whether a fully on-chain pipeline that verifies both a ZK-STARK and a post-quantum signature can operate within Solana L1's compute and memory constraints. Our prototype adapts Winterfell 0.12 with a dedicated SHA-256 hashv syscall path to reduce hashing overhead, suppresses inlining in FRI hotspots to respect SBF (Solana BPF) stack limits, and uses a custom bump allocator synchronized with requested heap frames.

3.24 [cryptoeprint:2025/1759] Plonk is Simulation Extractable in ROM Under Falsifiable Assumptions

Solving a long-standing open problem, Faonio, Fiore, and Russo proved that the widely used Plonk zk-SNARK is simulation extractable. However, their proof assumes both the random oracle model (ROM) and the algebraic group model. We prove that the same holds in the ROM under falsifiable assumptions. We combine the template of Faust et al., who proved that simulation extractability follows from knowledge soundness, (weak) unique response, and trapdoorless zero-knowledge, with the recent result of Lipmaa, Parisella, and Siim (Crypto 2025), who proved that Plonk has knowledge soundness in the ROM under falsifiable assumptions. For this, we prove that Plonk satisfies new variants of the weak unique response and trapdoorless zero-knowledge properties. We prove that several commonly used gadgets, like the linearization trick, are not trapdoorless zero-knowledge when considered as independent commit-and-prove zk-SNARKs.