ZKExpress (2025.09)

Kurt Pan @ ZKPunk

September 17, 2025

Contents

1 [DJJK+25] 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.

2 [WW25] 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 [HWW25] 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.

4 [WLXS+25] 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 (∼360 tps) 36× that of the state-of-the-art work (∼10 tps).

5 [AAAG25] 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.

6 [FNR25] 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.

7 [DHLM+25] 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.

8 [BDS25] 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.

9 [HSBB25] 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.

10 [BMMS25] 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.

11 [BMNW24b] Arc: Accumulation for Reed–Solomon Codes

homomorphic vector commitments
[BMNW24a]

12 [DO25] 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.

13 [RKW25] 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.

14 [CCYY25] 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.

References

[AAAG25] Hamza Abusalah, Gaspard Anthoine, Gennaro Avitabile, and Emanuele Giunta. *Lower Bounding Update Frequency in Short Accumulators and Vector Commitments*. Cryptology ePrint Archive, Paper 2025/1558. 2025 (cit. on p. 4).

[BDS25] Gustavo Banegas, Anaëlle Le Dévéhat, and Benjamin Smith. *Compressed verification for post-quantum signatures with long-term public keys*. Cryptology ePrint Archive, Paper 2025/1576. 2025 (cit. on p. 5).

[BMMS25] Anubhav Baweja, Pratyush Mishra, Tushar Mopuri, and Matan Shtepel. *Query-Optimal IOPPs for Linear-TIme Encodable Codes*. Cryptology ePrint Archive, Paper 2025/1588. 2025 (cit. on p. 5).

[BMNW24a] Benedikt Bünz, Pratyush Mishra, Wilson Nguyen, and William Wang. *Accumulation without Homomorphism*. Cryptology ePrint Archive, Paper 2024/474. 2024 (cit. on p. 6).

[BMNW24b] Benedikt Bünz, Pratyush Mishra, Wilson Nguyen, and William Wang. *Arc: Accumulation for Reed–Solomon Codes*. Cryptology ePrint Archive, Paper 2024/1731. 2024 (cit. on p. 6).

[CCYY25] Mingshu Cong, Sherman S. M. Chow, Siu Ming Yiu, and Tsz Hon Yuen. *Scalable zkSNARKs for Matrix Computations: A Generic Framework for Verifiable Deep Learning*. Cryptology ePrint Archive, Paper 2025/1646. 2025 (cit. on p. 7).

[DHLM+25] François Dupressoir, Andreas Hülsing, Cameron Low, Matthias Meijers, Charlotte Mylog, and Sabine Oechsner. *How Hard Can It Be to Formalize a Proof? Lessons from Formalizing CryptoBox Three Times in EasyCrypt*. Cryptology ePrint Archive, Paper 2025/1569. 2025 (cit. on p. 4).

[DJJK+25] Pratish Datta, Abhishek Jain, Zhengzhong Jin, Alexis Korb, Surya Mathialagan, and Amit Sahai. *Incrementally Verifiable Computation for NP from Standard Assumptions*. Cryptology ePrint Archive, Paper 2025/1546. 2025 (cit. on p. 2).

[DO25] Gökçe Düzyol and Kamil Otal. *Leveraging Smaller Finite Fields for More Efficient ZK-Friendly Hash Functions*. Cryptology ePrint Archive, Paper 2025/1593. 2025 (cit. on p. 6).

[FNR25] Sebastian Faller, Guilhem Niot, and Michael Reichle. *Lattice-based Threshold Blind Signatures*. Cryptology ePrint Archive, Paper 2025/1566. 2025 (cit. on p. 4).

[HSBB25] Hossein Hafezi, Alireza Shirzad, Benedikt Bünz, and Joseph Bonneau. *IronDict: Transparent Dictionaries from Polynomial Commitments*. Cryptology ePrint Archive, Paper 2025/1580. 2025 (cit. on p. 5).

[HWW25] Susan Hohenberger, Brent Waters, and David J. Wu. *Pairing-Based Aggregate Signatures without Random Oracles*. Cryptology ePrint Archive, Paper 2025/1548. 2025 (cit. on p. 3).

[RKW25] Daniel Römer, Gero Knoblauch, and Alexander Wiesmaier. *On GPU acceleration of PQC algorithms*. Cryptology ePrint Archive, Paper 2025/1596. 2025 (cit. on p. 7).

[WLXS+25] Chenke Wang, Yu Long, Xian Xu, Shi-Feng Sun, Yiqi Liu, and Dawu Gu. *UniCross: A Universal Cross-Chain Payment Protocol with On-demand Privacy and High Scalability*. Cryptology ePrint Archive, Paper 2025/1554. 2025 (cit. on p. 3).

[WW25] Brent Waters and David J. Wu. *Silent Threshold Cryptography from Pairings: Expressive Policies in the Plain Model*. Cryptology ePrint Archive, Paper 2025/1547. 2025 (cit. on p. 2).