# SnarkExpress

## (2025 Q4)

Edited by KurtPan @ ZKPunk

October 15, 2025

# Contents

# Chapter 1

# 2025.10

## 1.1 Communications in Cryptology Volume 2, Issue 3

## 1.2 [cryptoeprint:2025/1762] Threshold Signatures from One-Way Functions

In this work, we show how to construct threshold signatures for any $t$ and $n$ from one way functions, thus establishing the latter as a necessary and sufficient computational assumption. Our protocol makes non-black box use of one-way functions, and can be generalized to other access structures, such as monotone policies.

## 1.3 [cryptoeprint:2025/1764] Keccacheck: towards a SNARK friendly Keccak

This paper introduces a new method, termed keccacheck, which builds upon sum-check with influence from GKR to create circuits that can batch-verify Keccak permutations with fewer than 4000 constraints per instance. Keccacheck achieves this by exploiting the logarithmic scaling of recursive verification of the sum-check protocol, reducing the computational cost of verifying large enough batches to be only slightly higher than evaluating the multilinear extension of the input and output states. Its performance becomes competitive for a batch containing 16 permutations and offers more than a 10x cost reduction for batches of 512 or more permutations. This approach enables new levels of efficiency for the ZK ecosystem, providing the performant storage proofs that are essential to light clients, cross-chain bridges, privacy-focused protocols, and roll-ups.

## 1.4 [cryptoeprint:2025/1767] Polylogarithmic Polynomial Commitment Scheme over Galois Rings

This paper introduces the first multilinear polynomial commitment scheme (PCS) over Galois rings achieving $\mathcal{O}(\log^2 n)$ verification cost. It achieves $\mathcal{O}(n \log n)$ committing time and $\mathcal{O}(n)$ evaluation opening prover time. This PCS can be used to construct zero-knowledge proofs for arithmetic circuits over Galois rings, facilitating verifiable computation in applications requiring proofs of polynomial ring operations (e.g., verifiable fully homomorphic encryption). First we construct random foldable linear codes over Galois rings with sufficient code distance and present a distance preservation theorem over Galois rings. Second we extend the Basefold commitment (Zeilberger et al., Crypto 2024) to multilinear polynomials over Galois rings. Our approach reduces proof size and verifier time from $\mathcal{O}(\sqrt{n})$ to $\mathcal{O}(\log^2 n)$ compared to Wei et al., PKC 2025. Furthermore, we give a batched multipoint openning protocol for evaluation phase that collapses the proof size and verifier time of $N$ polynomials at $M$ points from $\mathcal{O}(NM \log^2 n)$ to $\mathcal{O}(\log^2 n)$, prover time from $\mathcal{O}(NMn)$ to $\mathcal{O}(n)$, further enhancing efficiency.

## 1.5 [cryptoeprint:2025/1768] DualMatrix: Conquering zkSNARK for Large Matrix Multiplication

We present DualMatrix, a zkSNARK solution for large-scale matrix multiplication. Classical zkSNARK protocols typically underperform in data analytic contexts, hampered by the large size of datasets and the superlinear nature of matrix multiplication. DualMatrix excels in its scalability. The prover time of DualMatrix scales linearly with respect to the number of non-zero elements in the input matrices. For $n \times n$ matrix multiplication with $N$ non-zero elements across three input matrices, DualMatrix employs a structured reference string (SRS) of size $O(n)$, and achieves RAM usage of $O(N+n)$, transcript size of $O(\log n)$, prover time of $O(N+n)$, and verifier time of $O(\log n)$. The prover time, notably at $O(N+n)$ and surpassing all existing protocols, includes $O(N+n)$ field multiplications and $O(n)$ exponentiations and pairings within bilinear groups. These efficiencies make DualMatrix effective for linear algebra on large matrices common in real-world applications. We evaluated DualMatrix with $2^{15} \times 2^{15}$ input matrices each containing $1G$ non-zero integers, which necessitate $32T$ integer multiplications in naive matrix multiplication. DualMatrix recorded prover and verifier times of 150.84s and 0.56s, respectively. When applied to $1M \times 1M$ sparse matrices each containing $1G$ non-zero integers, it demonstrated prover and verifier times of $1,384.45$s and 0.67s. Our approach outperforms current zkSNARK solutions by successfully handling the large matrix multiplication task in experiment. We extend matrix operations from field matrices to group matrices, formalizing group matrix algebra. This mathematical advancement brings notable symmetries beneficial for high-dimensional elliptic curve cryptography. By leveraging the bilinear properties of our group matrix algebra in the context of the two-tier commitment scheme, DualMatrix achieves efficiency gains over previous matrix multiplication arguments. To accomplish this, we extend and enhance Bulletproofs to construct an inner product argument featuring a transparent setup and logarithmic verifier time.

## 1.6 [cryptoeprint:2025/1771] Batched & Non-interactive Blind Signatures from Lattices

We introduce a new generalization called non-interactive batched blind signatures (NIBBS). Our goal is to reduce the computation and communication costs for signers and receivers, by batching multiple blind signature queries. More precisely, we define the property of 'succinct communication' which requires that the communication cost from signer to receiver be independent of the batch size. NIBBS is very suitable for large-scale deployments requiring only minimal signer-side effort. We design a NIBBS scheme and prove its security based on the hardness of lattice assumptions (in the random oracle model). When instantiated with the low-depth PRF candidate "Crypto Dark Matter" (TCC '18) and the succinct lattice-based proof system for rank-1 constraint systems (Crypto '23), our final signature size is 308 KB with <1 KB communication.

## 1.7 [cryptoeprint:2025/1773] Impossibility of VDFs in the ROM: The Complete Picture

This paper is concerned with the question whether Verifiable Delay Functions (VDFs), as introduced by Boneh et al. [CRYPTO 2018], can be constructed in the plain Random Oracle Model (ROM) without any computational assumptions. A first partial answer to this question is due to Mahmoody, Smith, and Wu [ICALP 2020], and rules out the existence of perfectly unique VDFs in the ROM. Building on this result, Guan, Riazanov, and Yuan [CRYPTO 2025] very recently demonstrated that even VDFs with computational uniqueness are impossible under a public-coin setup. However, the case of computationally unique VDFs with private-coin setup remained open. We close this gap by showing that even computationally expensive private-coin setup will not allow to construct VDFs in the ROM.

## 1.8 [cryptoeprint:2025/1782] On Verifiable Delay Functions from Time-Lock Puzzles

In this paper, we study the relationship between these two timed primitives. Our main result is a construction of "one-time" VDF from TLP using indistinguishability obfuscation (iO) and one-way functions (OWFs), where by "one-time" we mean that sequentiality of the VDF holds only against parallel adversaries that do not preprocess public parameters. Our VDF satisfies several desirable properties. For instance, we achieve perfectly sound and short proofs of $O(\lambda)$ bits, where $\lambda$ is the security parameter. Moreover, our construction is a trapdoor (one-time) VDF that can be easily extended to achieve interesting extra properties (defined in our paper) such as trapdoor-homomorphic and trapdoor-constrained evaluation. Finally, when combined with the results of Bitansky et al., [ITCS 2016], this yields one-time VDFs from any worst-case non-parallelizing language, iO and OWF. To the best of our knowledge, this is the first such construction that only relies on polynomial security.

## 1.9 [cryptoeprint:2025/1787] Four-round Statistical Non-malleable Zero-knowledge

We present a 4-round statistical non-malleable zero-knowledge (NMZK) argument in the plain model under standard hardness assumptions. Our construction can be based on any collision-resistant hash function and injective one-way function, and it guarantees simulation extractability in the delayed-input one-many setting. Before this work, 4-round constructions were known for computational NMZK but not for statistical NMZK.

## 1.10 [cryptoeprint:2025/1789] Olingo: Threshold Lattice Signatures with DKG and Identifiable Abort

We present Olingo, a framework for threshold lattice signatures that is the first to offer all desired properties for real-world implementations of quantum-secure threshold signatures: small keys and signatures, low communication and round complexity, non-interactive online signing, distributed key generation (DKG), and identifiable abort. Our starting point is the framework of Gur, Katz, and Silde (PQCrypto 2024). We change the underlying signature scheme to Raccoon (Katsumata et al., Crypto 2024), remove the trapdoor commitments, and apply numerous improvements and optimizations to achieve all the above properties. We provide detailed proofs of security for our new framework and present concrete parameters and benchmarks. At the 128-bit security level, for up to 1024 parties and supporting $2^{60}$ signatures, our scheme has 2.6 KB public keys and 9.7 KB signatures; while signing requires communication of 953 KB per party. Using the LaBRADOR proof system (Beullens and Seiler, Crypto 2023), this can be further reduced to 596 KB. An optimistic non-interactive version of our scheme requires only 83 KB communication per party.

## 1.11 [cryptoeprint:2025/1793] A note on the soundness of an optimized gemini variant

We give a formal analysis of the optimized variant of the gemini polynomial commitment scheme [BCHO22] used by the Aztec Network. Our work is motivated by an attack on a previous implementation [GL25].

## 1.12 [cryptoeprint:2025/1798] Threshold Blind Signatures from CDH

Threshold blind signature schemes (TBS) enhance blind signatures with a signing procedure distributed among up to n signers to reduce the risk attached to the compromise of the secret key. Blind signatures and TBS in pairing-free groups often rely on strong assumptions, e.g., the algebraic group model (AGM) or interactive assumptions. A recent line of work initiated by Chairattana-apirom, Tessaro and Zhu (Crypto'24), hereafter CTZ, manages to construct blind signatures in pairing-free groups in the random oracle model (ROM) without resorting to the AGM. While CTZ gives a construction from CDH, the scheme suffers from large signatures. Recent works have improved the efficiency, however at the cost of relying on a decisional assumption, namely DDH. In this work, we close this gap by giving an efficient blind signature in pairing-free groups proven secure under CDH in the ROM. Our signatures are of size 320 Byte which is an 32× improvement over CTZ's CDH-based construction. Further, we give the first TBS in pairing-free groups that does not rely on the AGM by thresholdizing our blind signature. Likewise, our TBS is proven secure under CDH in the ROM. To achieve this, our starting point is the efficient scheme introduced by Klooß, Reichle and Wagner (Asiacrypt'24). We manage to avoid the DDH assumption in the security argument by carefully hiding critical information from the user during the signing phase. At the cost of only 3 additional Zp elements in signature size, this allows us to prove security under CDH.

## 1.13 [cryptoeprint:2025/1802] Zyga: Optimized Zero-Knowledge Proofs with Dynamic Public Inputs

We present Zyga, a pairing-based zero-knowledge proof system optimized for privacy-preserving DeFi applications. Our main contribution is an enhancement of existing zkSNARK constructions that enables dynamic public input substitution during verification while maintaining privacy of witness components through one-sided encoding. The one-sided encoding aspect favors practical deployment constraints on Solana where G2 scalar multiplications are computationally expensive. Zyga separates private values (blinded through trusted setup) from public values (instantiated on-chain), enabling applications like private trading against current market rates without reproofing. We provide rigorous security analysis under discrete logarithm and q-Strong Diffie-Hellman assumptions, demonstrating computational soundness, zero-knowledge, and completeness. Performance analysis shows verification requires only 3 pairings with constant proof size, making it practical for blockchain deployment where transaction costs are critical.

## 1.14 [cryptoeprint:2025/1807] Traceable Ring Signatures Revisited: Extended Definitions, $O(1)$ Tracing, and Efficient Log-Size Constructions

We revisit the syntax and security notions of TRS, and close this gap by defining extended linkability and extended exculpability. Building on these, we design a new framework of TRS from Pseudo-Random Functions (PRF) and Zero-Knowledge Proofs of Knowledge (ZKPoK) that supports $O(1)$ tracing, provided that both two signatures are valid. This constitutes a substantial improvement over existing approaches—all of which require $O(n)$ tracing with $n$ the size of the ring—and elevates TRS to a level of practicality and efficiency comparable to Linkable Ring Signatures (LRS), which have already achieved widespread deployment in practice. Finally, we instantiate our generic framework from the DDH assumption and leverage the Bulletproofs [S&P'18] to construct a TRS scheme with log-size signatures. The proposed scheme achieves highly optimized signature sizes in practice and remains compatible with most existing DLog-based systems. On Curve25519, the signature size is $(128 \cdot \log n + 736)$ bytes, which to our best knowledge is the shortest LRS scheme for a ring $n \geq 19$.

## 1.15 [cryptoeprint:2025/1811] Anchored Merkle Range Proof for Pedersen Commitments

We present a simple range-proof mechanism for Pedersen commitments that avoids pertransaction heavy ZK verification and pairings. The idea is to commit once to a Merkleized range table of points $\{(U, aX \cdot G)\}_{X \in \{1,\ldots,2^n\}}$ for a secret $a \in \mathbb{Z}_q$ and a public anchor $U = a \cdot B$. At transaction time, a prover shows set membership of the leaf ( $U, ax \cdot G$ ), proves via a Chaum-Pedersen DLEQ that $\log_B U = \log_C C'$ where $C' = a \cdot C$ and $C$ is the Pedersen commitment, and finally proves (Schnorr) that $C' - (ax \cdot G)$ lies in the $H$-direction. These three checks enforce $x$ to be the in-range value indexed by the Merkle leaf while preserving privacy. Verification costs a single Merkle proof plus a DLEQ and a Schnorr discrete-log proof over an elliptic curve group.

## 1.16 [cryptoeprint:2025/1813] Two-party ECDSA Signing at Constant Communication Overhead

In this work, we investigate whether the cost of two-party ECDSA signing can be brought within the realm of plain ECDSA signing. We answer the question in the affirmative for the case of communication complexity, by means of a new signing protocol. Our protocol consumes bandwidth linear in the security parameter, and hence the size of an ECDSA signature. Our scheme makes only blackbox use of generic tools—Oblivious Transfer during key generation, and any Pseudorandom Function when signing. While computation complexity is not asymptotically optimal, benchmarks of our protocol confirm that concrete costs are the lowest known for ECDSA signing. Our protocol is therefore the most concretely efficient in the literature on all fronts: bandwidth, computation, and rounds. On a technical level, our protocol is enabled by a novel Pseudorandom Correlation Function (PCF) for the Vector Oblivious Linear Evaluation correlation over a large ring. The PCF relies on one-way functions alone, and may be of independent interest. Our scheme supports standard extensions, such as pre-signing, and including backup servers for key shares in a $(2, n)$ configuration.

## 1.17 [cryptoeprint:2025/1819] New Straight-Line Extractable NIZKPs for Cryptographic Group Actions

This work introduces the GAO (Group Action Oriented) transform, a new generic compiler that produces straight-line extractable NIZKPs from Sigma protocols while significantly simplifying the analysis of the fixed-weight framework. The GAO transform is then optimized in two different ways, defining a collision predicate (yielding the Coll-GAO transform) and adopting a technique (Stretch-and-Compress) that can be applied to improve both GAO and Coll-GAO (yielding the SC-GAO and SC-Coll-GAO transforms). The practical advantages of the SC-Coll-GAO transform are theoretically motivated and concretely tested on the LESS digital signature, a code-based candidate that recently advanced to the second round of the NIST standardization process specifically purposed for post-quantum signatures. Remarkably, when compared to the Fiat-Shamir LESS baseline, SC-Coll-GAO incurs a computational cost increase by 50-60%, while signature sizes grow by only 10-20%.

## 1.18 [cryptoeprint:2025/1824] Coppercloud: Blind Server-Supported RSA Signatures

In this work, we introduce Coppercloud, a blind server-supported RSA signature scheme designed to enhance privacy in digital identity systems. Coppercloud enables a user to obtain a signature on a message, without revealing its content to the supporting server, while distributing the signing key between the user's device and the supporting server. We formalize the security requirements for blind server-supported signing by defining an ideal functionality, and prove that Coppercloud securely realizes this functionality in the Universal Composability (UC) model.

## 1.19 [cryptoeprint:2025/1826] Proofs of No Intrusion

We introduce Proofs of No Intrusion, which enable a classical client to remotely test whether a quantum server has been hacked and the client's data stolen. Crucially, the test does not destroy the data being tested, avoiding the need to store a backup elsewhere. We define and construct proofs of no intrusion for ciphertexts assuming fully homomorphic encryption. Additionally, we show how to equip several constructions of unclonable primitives with proofs of non-intrusion, such as unclonable decryption keys and signature tokens. Conceptually, proofs of non-intrusion can be defined for essentially any unclonable primitive. At the heart of our techniques is a new method for non-destructively testing coset states with classical communication. It can be viewed as a non-destructive proof of knowledge of a measurement result of the coset state.

## 1.20 [cryptoeprint:2025/1827] Blind ECDSA from the ECDSA Assumption

We design a protocol that ensures both unforgeability and blindness without introducing new computational assumptions and ensuring concurrent security. It involves zero-knowledge proofs based on the MPC-in-the-head paradigm for complex statements combining relations on encrypted elliptic curve points, their coordinates, and discrete logarithms.

## 1.21 [cryptoeprint:2025/1828] Block-Accumulate Codes: Accelerated Linear Codes for PCGs and ZK

We propose a generalized paradigm for building LPN-friendly codes with provable minimum distance. Roughly speaking, these codes are based on the idea of randomized turbo codes such as repeat accumulate codes. To prove their minimum distance, we present a generalized enumeration technique, which allows us to precisely compute the minimum distance for a broad class of codes. Although we do not prove their asymptotic behavior, the concrete parameters essentially give a linear-time encoder. Armed with these new techniques, we construct several novel codes, the most promising of which we call Block-Accumulate codes. Our original design goal was to construct codes that run efficiently on GPUs. Surprisingly, we find that our newly constructed codes are the fastest on both GPUs and CPUs, while at the same time achieve a better minimum distance. If we restrict our attention to codes with proofs, our code is 8× faster than state of the art on a CPU and 50× faster on a GPU. Even if we use aggressive parameters, our code is 3 and 20× faster, respectively. Under these parameters, this yields overall PCG speedups of 2.5× on the CPU and 15× on the GPU, achieving about 200 million OTs or binary Beaver triples per second on the GPU (excluding the one-time 10 ms GGM seed expansion). We expect similar improvements when applied to the ZK space.

## 1.22 [cryptoeprint:2025/1833] Public-Key Encryption from the Min-Rank Problem

We construct a public-key encryption scheme from the hardness of the (planted) MinRank problem over uniformly random instances. This corresponds to the hardness of decoding random linear rank-metric codes. Existing constructions of public-key encryption from such problems require hardness for structured instances arising from the masking of efficiently decodable codes. Central to our construction is the development of a new notion of duality for rank-metric codes.

## 1.23 [cryptoeprint:2025/1835] Who Verifies the Verifiers? Lessons Learned From Formally Verified Line-Point Zero-Knowledge

In this paper, we ask the question of how reliable are these machine-checked proofs by analyzing a formally verified implementation of the Line-Point Zero-Knowledge (LPZK) protocol (Dittmer, Eldefrawy, Graham-Lengrand, Lu, Ostrovsky and Pereira, CCS 2023). The implementation was developed in EasyCrypt and compiled into OCaml code that was claimed to be high-assurance, i.e., that offers the formal guarantees of guarantees of completeness, soundness, and zero knowledge. We show that despite these formal claims, the EasyCrypt model was flawed, and the implementation (supposed to be high-assurance) had critical security vulnerabilities. Concretely, we demonstrate that: 1) the EasyCrypt soundness proof was incorrectly done, allowing an attack on the scheme that leads honest verifiers into accepting false statements; and 2) the EasyCrypt formalization inherited a deficient model of zero knowledge for a class of non-interactive zero knowledge protocols that also allows the verifier to recover the witness. In addition, we demonstrate 3) a gap in the proof of the perfect zero knowledge property of the LPZK variant of Dittmer, Ishai, Lu and Ostrovsky (CCS 2022) that the EasyCrypt proof is based, which, depending on the interpretation of the protocol and security claim, could allow a malicious verifier to learn the witness. Our findings highlight the importance of scrutinizing machine-checked proofs, including their models and assumptions. We offer lessons learned for both users and reviewers of tools like EasyCrypt, aimed at improving the transparency, rigor, and accessibility of machine-checked proofs. By sharing our methodology and challenges, we hope to foster a culture of deeper engagement with formal verification in the cryptographic community.

## 1.24 [cryptoeprint:2025/1837] Proofs of quantum memory

In this paper, we introduce a new concept, proofs of quantum memory (PoQM). A PoQM is an interactive protocol between a classical probabilistic polynomial-time (PPT) verifier and a quantum polynomial-time (QPT) prover over a classical channel where the verifier can verify that the prover has possessed a quantum memory with a certain number of qubits during a specified period of time. PoQM generalize the notion of proofs of quantumness (PoQ) [Brakerski, Christiano, Mahadev, Vazirani, and Vidick, JACM 2021]. Our main contributions are a formal definition of PoQM and its constructions based on hardness of LWE. Specifically, we give two constructions of PoQM. The first is of a four-round and has negligible soundness error under subexponential-hardness of LWE. The second is of a polynomial-round and has inverse-polynomial soundness error under polynomial-hardness of LWE. As a lowerbound of PoQM, we also show that PoQM imply one-way puzzles. Moreover, a certain restricted version of PoQM implies quantum computation classical communication (QCCC) key exchange.

## 1.25 [cryptoeprint:2025/1839] Lattice-Based zk-SNARKs with Hybrid Verification Technique

In this work, we propose a new notion of a hybrid verification mechanism. Here, the prover generates a proof that can be verified by a designated verifier. For this proof, the designated verifier can generate auxiliary information with its secret key. The combination of this proof and the auxiliary information allows any public verifier to verify the proof without any other information. We also introduce necessary security notions and mechanisms to identify a cheating designated verifier or the prover. Our hybrid verification zkSNARK construction is based on module lattices and adapts the zkSNARK construction by Ishai et al. (CCS 2021). In this construction, the designated verifier is required only once after proof generation to create the publicly verifiable proof. Our construction achieves a small constant-size proof and fast verification time, which is linear in the statement size.

## 1.26 [cryptoeprint:2025/1840] Quantum Cryptography and Hardness of Non-Collapsing Measurements

In this paper, we base OWPuzzs on hardness of non-collapsing measurements. To that end, we introduce a new complexity class, **SampPDQP**, which is a sampling version of the decision class **PDQP** introduced in [Aaronson, Bouland, Fitzsimons, and Lee, ITCS 2016]. We show that if **SampPDQP** is hard on average for quantum polynomial time, then OWPuzzs exist. We also show that if $\mathbf{SampPDQP} \not\subseteq \mathbf{SampBQP}$, then auxiliary-input OWPuzzs exist. **SampPDQP** is the class of sampling problems that can be solved by a classical polynomial-time deterministic algorithm that can make a single query to a non-collapsing measurement oracle, which is a ”magical” oracle that can sample measurement results on quantum states without collapsing the states. Such non-collapsing measurements are highly unphysical operations that should be hard to realize in quantum polynomial-time, and therefore our assumptions on which OWPuzzs are based seem extremely plausible. Moreover, our assumptions do not seem to imply OWFs, because the possibility of inverting classical functions would not be helpful to realize quantum non-collapsing measurements. We also study upperbounds of the hardness of **SampPDQP**. We introduce a new primitive, distributional collision-resistant puzzles (dCRPuzzs), which are a natural quantum analogue of distributional collision-resistant hashing [Dubrov and Ishai, STOC 2006]. We show that dCRPuzzs imply average-case hardness of **SampPDQP** (and therefore OWPuzzs as well). We also show that two-message honest-statistically-hiding commitments with classical communication and one-shot message authentication codes (MACs), which are a privately-verifiable version of one-shot signatures [Amos, Georgiou, Kiayias, Zhandry, STOC 2020], imply dCRPuzzs.

## 1.27 [cryptoeprint:2025/1841] Pegasus and PegaRing: Efficient (Ring) Signatures from Sigma-Protocols for Power Residue PRFs with (Q)ROM Security

In this work, we present a novel commit-and-open Σ-protocol based on the Legendre and power residue PRFs. Our construction leverages the oblivious linear evaluation (OLE) correlations inherent in PRF evaluations and requires only black-box access to a tree-PRG-based vector commitment. By applying the standard Fiat-Shamir transform, we obtain a post-quantum signature scheme, Pegasus, which achieves short signature sizes (6025 to 7878 bytes) with efficient signing (3.910 to 19.438 ms) and verification times (3.942 to 18.999 ms). Furthermore, by pre-computing the commitment phase, the online response time can be reduced to as little as 0.047 to 0.721 ms. We prove the security of Pegasus in both the classical random oracle model (ROM) and the quantum random oracle model (QROM), filling a gap left by prior PRF-based signature schemes. We further develop a ring signature scheme, PegaRing, that preserves the three-move commit-and-open structure of Pegasus. Compared to previous PRF-based ring signature called DualRing-PRF (ACISP 2024), PegaRing reduces the constant communication overhead by more than half and achieves significantly faster signing and verification. For a ring size of 1024, PegaRing yields signatures of 29 to 32 KB, with signing times of 8 to 44 ms, and verification times of 6 to 31 ms, depending on the parameters. Finally, we prove the security of PegaRing in both the ROM and the QROM, which is, to the best of our knowledge, the first symmetric-key primitives-based ring signature with practical performances and provable QROM security.

## 1.28 [cryptoeprint:2025/1844] Bird of Prey: Practical Signature Combiners Preserving Strong Unforgeability

This work introduces three practical combiners that preserve strong unforgeability and all BUFF (beyond unforgeability features) properties. Each combiner is tailored to a specific class of classical signature schemes capturing all broadly used schemes that are strongly unforgeable. Remarkably, all combiners can be instantiated with any post-quantum signature scheme in a black-box way making deployment practical and significantly less error prone. The proposed solutions are further highly efficient and have signatures that are at most the size of the (insecure) concatenation combiner. For instance, our most efficient combiner enables the combination of EdDSA with ML-DSA, yielding a signature size that is smaller than the sum of an individual EdDSA signature and an individual ML-DSA signature. Additionally, we identify a novel signature property that we call random-message validity and show that it can be used to replace the BUFF transform with the more efficient Pornin-Stern transform. The notion may be of independent interest.

## 1.29 [cryptoeprint:2025/1846] The Order of Hashing in Fiat-Shamir Schemes

Our work investigates whether there are advisable or imprudent input orders for hashing in Fiat-Shamir signatures. We examine Fiat-Shamir signatures with plain and nested hashing using Merkle-Damgård or sponge-based hash functions. We analyze these constructions in both classical and quantum settings. As part of our investigations, we introduce new security properties following the idea of quantum-annoyance of Eaton and Stebila (PQCrypto 2021), called annoyance for user exposure and signature forgeries. These properties ensure that an adversary against the hash function cannot gain a significant advantage when attempting to extend a successful attack on a single signature forgery to multiple users or to multiple forgeries of a single user. Instead, the adversary must create extra forgeries from scratch. Based on our analysis, we derive a simple rule: When using Fiat-Shamir signatures, one should hash the commitment before the message; all other inputs may be ordered arbitrarily.

## 1.30 [cryptoeprint:2025/1848] Revisiting Lattice-based Non-interactive Blind Signature

Later, Zhang et al. introduced another lattice-based construction in ProvSec 2024, and proved its security under the standard module short integer solution (MSIS) assumption. We analyse the security of the latter scheme. In the random oracle model, we show that it fails to achieve both nonce blindness and receiver blindness. We present explicit attacks where an adversary breaks both properties with probability 1. Our attack is based on a crucial observation that uncovers a flaw in the design. Specifically, this flaw allows an attacker to link a message-signature pair with its presignature-nonce pair. In addition, we also identify a flaw in the unforgeability proof. Finally, we suggest a modification to address the issue, which is similar to Baldimtsi et al. construction, and its security relies again on the non-standard rOM-ISIS assumption. This work again raises the question of the feasibility of achieving NIBS from standard assumptions.

## 1.31 [cryptoeprint:2025/1849] CoBBl: Dynamic constraint generation for SNARKs

This paper presents a compiler and proof system, CoBBl, that combines the benefits of CPU emulation and direct translation: it takes advantage of program-specific optimizations, but doesn't pay for an unnecessary state representation or unexecuted computation. COBBL outper- forms CirC, a state-of-the-art direct translator, by 1˘30× on compile time and 26˘350× on prover time, and outperforms Jolt, a state-of-the-art CPU emulator, on prover time by 1.1˘1.8× on Jolt-friendly benchmarks, and up to 100× on other benchmarks.

## 1.32 [cryptoeprint:2025/1850] Linear*-Time Permutation Check

Permutation and lookup arguments are at the core of most deployed SNARK protocols today. Most modern techniques for performing them require a grand product check. This requires either committing to large field elements (E.g. in Plonk) or using GKR (E.g. in Spartan) which has worse verifier cost and proof size. Sadly, both have a soundness error that grows linearly with the input size. We present two permutation arguments that have $\mathrm{polylog}(n)/|\mathbb{F}|$ soundness error – for reasonable input size $n = 2^{32}$ and field size $|\mathbb{F}| = 2^{128}$, the soundness error improves significantly from $2^{-96}$ to $2^{-120}$. Moreover, the arguments achieve $\log(n)$ verification cost and proof size without ever needing to commit to anything beyond the witness. BiPerm only requires the prover to perform $O(n)$ field operations on top of committing to the witness, but at the cost of limiting the choices of PCS. We show a stronger construction, MulPerm, which has no restriction on the PCS choice and its prover performs essentially linear field operations, $n \cdot \tilde{O}(\sqrt{\log(n)})$. Our permutation arguments generalize to lookups. We demonstrate how our arguments can be used to improve SNARK systems such as HyperPlonk and Spartan, and build a GKR-based protocol for proving non-uniform circuits.

## 1.33 [cryptoeprint:2025/1851] Locally Recoverable Data Availability Sampling

We propose Locally Recoverable Data Availability Sampling (LR-DAS), which upgrades binary, threshold-based availability to graded verification by leveraging optimal locally recoverable codes (e.g., Tamo-Barg). Local groups of size $r+\alpha$ serve as atomic certification units: once $r$ verified openings fix a degree- $< r$ local polynomial, the entire group is certified and accumulates monotonically toward global availability. We formalize a locality-aware commitment with a single algebraic local-global link that binds every accepted local proof to a unique global codeword, preventing cross-group splicing. Our verifier admits a two-tier IOP view (local RSmembership, global TB-proximity, one DEEP-style linking query). We instantiate this with (i) a two-layer KZG design and (ii) a transparent FRI/IOPP stack. Both support batched multi-point openings and cross-block random-weight aggregation, yielding $\mathbb{O}(1)$ verifier work per certified batch with $\mathbb{O}(r+\alpha)$ field payload per block. Security is captured by graded soundness against missing-fraction and missing-group adversaries with explicit overshoot bounds. A lightweight proof-of-custody layer-one unpredictable global opening at publish time plus periodic batched local checks-composes seamlessly to enforce possession without altering the core pipeline. Empirically and analytically, LR-DAS certifies availability with fewer samples than required for global recovery under the same encoding, providing a practical univariate alternative to multivariate repair-based DAS while retaining succinct proofs and a simple prover/verifier pipeline. Design levers $(r, \alpha)$ allow tuning responsiveness versus distance, and the transparent instantiation offers a post-quantum-ready option.

## 1.34 [cryptoeprint:2025/1852] A Gaussian Leftover Hash Lemma for Modules over Number Fields

Leftover Hash Lemma (LHL) states that $\mathbf{X} \cdot \mathbf{v}$ for a Gaussian $\mathbf{v}$ is an essentially independent Gaussian sample. It has seen numerous applications in cryptography for hiding sensitive distributions of $\mathbf{v}$. We generalise the Gaussian LHL initially stated over $\mathbb{Z}$ by Agrawal, Gentry, Halevi, and Sahai (2013) to modules over number fields. Our results have a sub-linear dependency on the degree of the number field and require only polynomial norm growth: $\|\mathbf{v}\|/\|\mathbf{X}\|$. To this end, we also prove when $\mathbf{X}$ is surjective (assuming the Generalised Riemann Hypothesis) and give bounds on the smoothing parameter of the kernel of $\mathbf{X}$. We also establish when the resulting distribution is independent of the geometry of $\mathbf{X}$ and establish the hardness of the $k$-SIS and $k$-LWE problems over modules ($k$-MSIS/$k$-MLWE) based on the hardness of SIS and LWE over modules (MSIS/MLWE) respectively, which was assumed without proof in prior works.

## 1.35 [cryptoeprint:2025/1857] On the Quantum Equivalence between S$|$LWE$\rangle$ and ISIS

In this paper, we investigate the equivalence between S$|$LWE$\rangle$ and ISIS. We present the first fully generic reduction from ISIS to S$|$LWE$\rangle$, valid even in the presence of errors in the underlying algorithms. We then explore the reverse direction, introducing an inhomogeneous variant of C$|$LWE$\rangle$, denoted IC$|$LWE$\rangle$, and show that IC$|$LWE$\rangle$ reduces to S$|$LWE$\rangle$. Finally, we prove that, under certain recoverability conditions, an algorithm for ISIS can be transformed into one for S$|$LWE$\rangle$. We instantiate this reverse reduction by tweaking a known algorithm for (I)SIS in order to construct quantum algorithm for S$|$LWE$\rangle$ when the alphabet size q is a small power of 2, recovering some results of Bai et al. [BJK+ 25]. Our results thus clarify the landscape of reductions between S$|$LWE$\rangle$ and ISIS, and we show both their strong connection as well as the remaining barriers for showing full equivalence.

## 1.36 [cryptoeprint:2025/1863] On Limits on the Provable Consequences of Quantum Pseudorandomness

We study new oracle worlds where one form of quantum pseudorandomness exists but another does not, under certain assumptions or constraints, and we provide potential directions toward achieving full black-box separation. More precisely: - We give a unitary oracle relative to which PRFSGs exist, but PRUs without using ancilla do not. This can be extended to general PRUs if a structural property of the PRU algorithm can be proven. Assuming a conjecture similar to an isoperimetric inequality, we show a unitary oracle world where log-length output PRFSGs exist, but proving the existence of quantum-computable pseudorandom generators (QPRGs) with negligible correctness error is as hard as proving that BQP $\neq$ QCMA. This result suggests that the inverse-polynomial error in the state-of-the-art construction of QPRGs from log-length PRSGs is inherent. Assuming the same conjecture, we prove that some natural methods of constructing super-log-length output PRSGs from log-length output PRFSGs are impossible. This partly complements the known hardness of shrinking the PRSG output lengths. Along the way, we also discuss other potential approaches to extend the PRSG output lengths. All our worlds are based on (variants of) oracles that output Haar-random quantum states for each bit string, which can be viewed as a quantum version of the random oracle model, where output strings are replaced by quantum states. Our results highlight technical difficulties when dealing with ancillary registers, measurements, and adaptivity in the quantum setting. As one of our key technical tools, we show an intriguing gentle behavior of intermediate measurements in algorithms producing outcome states with high purity, which may be of independent interest.

## 1.37 [cryptoeprint:2025/1866] Succinct Line-Point Zero-Knowledge Arguments from Homomorphic Secret Sharing

In this work, we beat the proof size barrier and propose *succinct LPZK arguments*, by distilling techniques from orthogonal studies on homomorphic secret sharing and succinct garbling. Specifically, under variants of group/lattice-based assumptions, we show the followings: i) There exist succinct LPZK arguments with common reference string (CRS) size $O(n^{2/3})$, proof size $O(n^{2/3})$, prover time $O(n^{4/3} + |\mathcal{C}|)$, verification time $O(n + |\mathcal{C}|)$, and negligible soundness error, where both the prover and the verifier executions and be run in a streaming fashion. ii) The above proof size can be further optimized to $O(1)$, at the cost of a larger CRS size $O(n)$, and prover time increased to $O(n^2 + |\mathcal{C}|)$. In general, our succinct LPZK arguments pave a new way for building designated-verifier zero-knowledge succinct non-interactive arguments of knowledge (dv-zkSNARKs), and new interesting features (e.g., streaming, constant sized proof with CRS size not proportional to the circuit size) are obtained for the first time along the way.

## 1.38 [cryptoeprint:2025/1867] Vectorized Falcon-Sign Implementations using SSE2, AVX2, AVX-512F, NEON, and RVV

We design a vectorized version of the BaseSample and provide optimized implementations across six different instruction sets: SSE2, AVX2, AVX-512F, NEON, RISC-V Vector (RVV), and RV64IM. The AVX2 implementation, for instance, achieves an 8.4× speedup over prior work. Additionally, we optimize the FFT/iFFT operations using RVV and RV64D. For the RVV implementation, we introduce a new method using strided load/store instructions, with 4+4 and 4+5 layer merging strategies for Falcon-512 and Falcon-1024, respectively, resulting in a speedup of more than 4×. Finally, we present the results of our optimized implementations across eight different instruction sets for signature generation of Falcon. For instance, our AVX2, AVX-512F, and RV64GCVB implementations achieve performance improvements of 23%, 36%, and 59%, respectively, for signature generation of Falcon-512.

## 1.39 [cryptoeprint:2025/1876] SoK: Lookup Table Arguments

In this work, we systematize the design of lookup arguments and the cryptographic primitives they rely on. We introduce a unified and modular framework that covers standard, projective, indexed, vector, and decomposable lookups. We classify existing protocols by proof technique—multiset equality, Logup-based, accumulators, and subvector extraction (matrix–vector)—as well as by composition style. We survey and evaluate existing protocols along dimensions such as prover cost, dependence on table size, and compatibility with recursive proofs. From this analysis, we distill lessons and guidelines for choosing lookup constructions in practice and highlight the benefits and limitations of emerging directions in literature, such as preprocessing and decomposability.

## 1.40 [cryptoeprint:2025/1878] MIRANDA: short signatures from a leakage-free full-domain-hash scheme

We present Miranda, the first family of full-domain-hash signatures based on matrix codes. This signature scheme fulfils the paradigm of Gentry, Peikert and Vaikuntanathan (GPV), which gives strong security guarantees. Our trapdoor is very simple and generic: if we propose it with matrix codes, it can actually be instantiated in many other ways since it only involves a subcode of a decodable code (or lattice) in a unique decoding regime of parameters. Though Miranda signing algorithm relies on a decoding task where there is exactly one solution, there are many possible signatures given a message to sign and we ensure that signatures are not leaking information on their underlying trapdoor by means of a very simple procedure involving the drawing of a small number of uniform bits. In particular Miranda does not use a rejection sampling procedure which makes its implementation a very simple task contrary to other GPV-like signatures schemes such as Falcon or even Wave. We instantiate Miranda with the famous family of Gabidulin codes represented as spaces of matrices and we study thoroughly its security (in the EUF-CMA security model). For 128 bits of classical security, the signature sizes are as low as 90 bytes and the public key sizes are in the order of 2.6 megabytes.

## 1.41 [cryptoeprint:2025/1886] Blind Signatures from Arguments of Inequality

We give the first lattice-based blind signature that is concurrently-secure based on the Fiat-Shamir paradigm. - We give the first pairing-free blind signature that is concurrently-secure under the discrete logarithm assumption (without the algebraic group model). On a technical level, our work is inspired by the recent proofs of inequality technique (Klooß and Reichle, Crypto'25). This technique relies on statistical puncturing of the verification key. We explore the technique in the computational regime and develop new proof and design techniques to tackle the challenges encountered along the way.

## 1.42 [cryptoeprint:2025/1893] Poseidon2b: A Binary Field Version of Poseidon2

We present Poseidon2b, a version of Poseidon2 defined over binary extension fields. It is specifically designed to inherit many of the circuit-friendly properties of its prime field version, and to be used together with binary extension field proving systems such as Binius. Benchmarking demonstrates the merits around proof size, proving time, and especially verification time. We also revisit recent attacks on Poseidon and Poseidon2 and discuss their applicability in the binary field extension setting, in addition to analyzing attack vectors that were not applicable in the prime field setting. In particular, we lay special focus on algebraic cryptanalysis and subspace trails, techniques which resulted in attacks on initial versions of Poseidon defined over binary extension fields.

## 1.43 [cryptoeprint:2025/1897] Dynark: Making Groth16 Dynamic

In this paper, we introduce DYNARK, a dynamic zkSNARK scheme that can update the proof in sublinear time when the change of the witness is small. DYNARK is built on top of the seminal zkSNARK protocol of Groth, 2016. In the semi-dynamic setting, for an R1CS of size $n$, after a preprocessing of $O(n \log n)$ group operations on the original witness, it only takes $O(d)$ group operations and $O(d \log^2 d)$ field operations to update the proof for a new witness with distance $d$ from the original witness, which is nearly optimal. In the fully-dynamic setting, the update time of DYNARK is $O(d\sqrt{n \log n})$ group operations and $O(d \log^2 d)$ field operations. Both the proof size and the verifier time are $O(1)$, which are exactly the same as Groth16. Compared to the scheme in a prior work by Wang et al. 2024, we reduce the proof size from $O(\sqrt{n})$ to $O(1)$ without relying on pairing product arguments or another zkSNARK, and the update time and the verifier time of DYNARK are faster in practice. Experimental results show that for $n = 2^{20}$, after a one-time preprocessing of 74.3 seconds, it merely takes 3 milliseconds to update the proof in our semi-dynamic zkSNARK for $d = 1$, and 60 milliseconds to update the proof in our fully-dynamic zkSNARK. These are 1433× and 73× faster than Groth16, respectively. The proof size is 192 bytes and the verifier time is 4.4 milliseconds. The system is fully compatible with any existing deployment of Groth16 without changing the trusted setup, the proof and the verification algorithm.

## 1.44 [cryptoeprint:2025/1898] Unique NIZKs and Steganography Detection

In this work, following Lepinski, Micali, and shelat (TCC '05), we consider the following relaxed notion of unique NIZKs (UNIZKs): - We only require (computationally) unique proofs for NP statements with a (computationally) unique witness; an adversary that can produce two distinct proofs must also know two distinct witnesses. - We consider NIZKs with prover setup, where a potentially malicious prover initially publishes a public key $\mathsf{pk}$ and keeps a corresponding secret key $\mathsf{sk}$, which it uses to produce arbitrarily many NIZK proofs $\pi$ in the future. While the public key $\mathsf{pk}$

is not required to be unique, once it is fixed, all the subsequent proofs $\pi$ that the prover can produce should be unique. We show that both of these relaxations are needed to avoid witness encryption. Prior work constructed such UNIZKs under the quadratic residuosity assumption, and it remained an open problem to do so under any other assumptions. Here, we give a new construction of UNIZKs under the learning with errors (LWE) assumption. We also identify and fix a subtle circularity issue in the prior work. UNIZKs are a non-interactive version of steganography-free zero-knowledge of Abdolmaleki et al. (TCC '22). As an application of UNIZKs, we get a general steganography detection mechanism that can passively monitor arbitrary functionalities to detect steganographic leakage.