# SnarkExpress

## (2025 Q4)

Edited by SurtPan @ ZKPunk

October 26, 2025

# Contents

# Chapter 1

# 2025.10

## 1.1 [BM25] 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.

## 1.2 [KKAŚ+25] 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.

## 1.3 [WZDW+25] Polylogarithmic Polynomial Commitment Scheme over Galois Rings

This paper introduces the first multilinear polynomial commitment scheme (PCS) over Galois rings achieving $\mathcal{O}\left(\log^2 n\right)$ 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 $\mathcal{O}\big(\log^2 n\big)$ 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 $\mathcal{O}\big(NM\log^2 n\big)$ to $\mathcal{O}\big(\log^2 n\big)$, prover time from $\mathcal{O}(NMn)$ to $\mathcal{O}(n)$, further enhancing efficiency.

## 1.4 [CYY25] 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.

## 1.5 [BGY25] 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.

## 1.6 [AAKT+25] 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.

## 1.7 [AAFK+25] 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.

## 1.8 [Kiy25] 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.

## 1.9 [GHKS+25] 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.

## 1.10 [GK25] 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].

## 1.11 [RR25] 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.

## 1.12 [AB25] 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.

## 1.13 [Liu25] 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 $n \geq 19$.

## 1.14 [Hio25] 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.

## 1.15 [Kon25] 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.

## 1.16 [FPST25] 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%.

## 1.17 [SKVP25] 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.

## 1.18 [GR25] 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.

## 1.19 [KPRR+25] 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.

## 1.20 [CMV25] Public-Key Encryption from the MinRank 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.

## 1.21 [HMOY25] 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.

## 1.22 [AMK25] 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.

## 1.23 [MSY25] 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 **SampPDQP** $\not\subseteq$ **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.

## 1.24 [ZLSZ+25] 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 $\Sigma$-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.

## 1.25 [Jan25] 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.

## 1.26 [BF25] 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.

## 1.27 [GKKP+25] 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.

## 1.28 [JBW25] 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.

## 1.29 [BCD25] 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 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.

## 1.30 [CSK25] 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 $\mathcal{O}(1)$ verifier work per certified batch with $\mathcal{O}(r+\alpha)$ 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.

## 1.31 [AFLL+25] 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.

## 1.32 [CH25] On the Quantum Equivalence between S|LWE⟩ and ISIS

In this paper, we investigate the equivalence between S|LWE⟩ and ISIS. We present the first fully generic reduction from ISIS to S|LWE⟩, valid even in the presence of errors in the underlying

algorithms. We then explore the reverse direction, introducing an inhomogeneous variant of C|LWE⟩, denoted IC|LWE⟩, and show that IC|LWE⟩ reduces to S|LWE⟩. Finally, we prove that, under certain recoverability conditions, an algorithm for ISIS can be transformed into one for S|LWE⟩. We instantiate this reverse reduction by tweaking a known algorithm for (I)SIS in order to construct quantum algorithm for S|LWE⟩ 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⟩ and ISIS, and we show both their strong connection as well as the remaining barriers for showing full equivalence.

## 1.33 [BHMV25] 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.

## 1.34 [LXYY+25] 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 $O(n^{4/3} + |C|)$, verification time $O(n + |C|)$, 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.

## 1.35 [ZZ25] 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.

## 1.36 [HACF25] 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.

## 1.37 [CDGV25] 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.

## 1.38 [KLR25] 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.

## 1.39 [GKKR+25] 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.

## 1.40 [ZOZ25] 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.

## 1.41 [QTW25] 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.

## 1.42 [ZGCP+25] HyperWolf: Lattice Polynomial Commitments with Standard Soundness

We present HyperWolf, a lattice-based, fully transparent polynomial commitment scheme (PCS) for univariate and multilinear polynomials. To the best of our knowledge, it is the first lattice PCS to simultaneously achieve logarithmic proof size and verification time with standard soundness under standard lattice assumptions over polynomial rings. Building on sublinear schemes such as Greyhound (CRYPTO'24) and BrakeDown (CRYPTO'23), we generalize the two-dimensional approach to a $k$-dimensional witness-folding recursion, yielding a $k$-round hyperdimensional proof. Each round folds the witness along one axis, reducing the tensor arity by one, giving overall cost $O(kN^{1/k})$;

choosing $k = \log N$ yields $O(\log N)$ verification time and proof size. For standard $\ell_2$ soundness, we give an exact Euclidean-norm proof tailored to lattice relations: we prove $\langle \vec{f}, \vec{f} \rangle$ mod $q$ via an inner-product argument and enforce a small-coefficient bound on $\|\vec{f}\|_\infty$ so that $\langle \vec{f}, \vec{f} \rangle$ mod $q = \langle \vec{f}, \vec{f} \rangle$ over $\mathbb{Z}$. Both sub-proofs admit the same structure for $O(\log N)$ complexity. We further compact the proof using a proof-of-proof IPA à la LaBRADOR (CRYPTO'23), attaining $O(\log \log \log N)$ while preserving logarithmic verification and linear proving. We also describe a candidate optimization that achieves $O(\log \log N)$ proofs without LaBRADOR. For $N = 2^{30}$, HyperWolf features a ∼53 KB proof size and, compared to Greyhound, reduces verifier work from $\Theta(\sqrt{N})$ to $\Theta(\log N)$, yielding 2 to 3 orders of magnitude improvement for large $N$ while maintaining comparable size.

## 1.43 [Che25] Symphony: Scalable SNARKs in the Random Oracle Model from Lattice-Based High-Arity Folding

We re-envision how to use folding, and introduce Symphony, the first folding-based SNARK that avoids embedding hashes in SNARK circuits. It is memory-efficient, parallelizable, streaming-friendly, plausibly post-quantum secure, with polylogarithmic proof size and verification, and a prover dominated by committing to the input witnesses. As part of our construction, we introduce a new lattice-based folding scheme that compresses a large number of NP-complete statements into one in a single shot, which may be of independent interest. Furthermore, we design a generic compiler that converts a folding scheme into a SNARK without embedding the Fiat-Shamir circuit into proven statements. Our evaluation shows its concrete efficiency, making Symphony a promising candidate for applications such as zkVM, proof of learning, and post-quantum aggregate signatures.

## 1.44 [HV25] A Simple and Efficient One-Shot Signature Scheme

In this work, we address the inefficiency of the Shmueli-Zhandry construction which signs messages bit-by-bit, resulting in signing keys of $\Theta(\lambda^4)$ qubits and signatures of size $\Theta(\lambda^3)$ bits for polynomially long messages, where $\lambda$ is the security parameter. We construct a new, simple, direct, and efficient one-shot signature scheme which can sign messages of any polynomial length using signing keys of $\Theta(\lambda^2)$ qubits and signatures of size $\Theta(\lambda^2)$ bits. We achieve corresponding savings in runtimes, in both the oracle model and the plain model. In addition, unlike the Shmueli-Zhandry construction, our scheme achieves perfect correctness. Our scheme also achieves strong signature incompressibility, which implies a public-key quantum fire scheme with perfect correctness among other applications, correcting an error in a recent work of Çakan, Goyal and Shmueli (QCrypt 2025) and recovering their applications.

## 1.45 [ZGGX25] Quasar: Sublinear Accumulation Schemes for Multiple Instances

In this work, we present a novel accumulation scheme for multiple instances based on polynomial commitment schemes, achieving a theoretical verifier complexity that is sublinear in the number of instances. Technically, our scheme leverages partial evaluation of polynomials to replace random linear combinations, thereby minimizing the costly Commitment Random Linear Combination (CRC) operations on the verifier side. Building on this accumulation scheme, we introduce Quasar, a multi-instance IVC with small recursion overhead in practice. Notably, Quasar reduces the number of costly CRC operations in the recursive circuit from linear to quasi-linear, substantially improving practical performance. By instantiating Quasar with appropriate polynomial commitment schemes, it can achieve linear-time accumulation prover complexity, plausible post-quantum security, and support for parallelizable proving at each step.

## 1.46 [CFJW25] Unambiguous SNARGs for P from LWE with Applications to PPAD Hardness

We construct the first unambiguous succinct non-interactive arguments (SNARGs) for P and incrementally verifiable computation (IVC) for P from the polynomial hardness of learning with errors (LWE). Unambiguity guarantees that it is computationally hard to find two distinct accepting proofs for the same statement. As an application, we establish the first PPAD hardness result based on the polynomial hardness of LWE combined with a widely believed complexity assumption. Central to our approach is a new notion of rate-1 witness-unambiguous batch arguments for NP, which we give the first construction from the polynomial hardness of LWE.

## 1.47 [ZSVD25] Graeffe-Based Attacks on Poseidon and NTT Lower Bounds

We introduce the use of the Graeffe transform in univariate polynomial solving within this line of work. The proposed method streamlines the root recovery process in interpolation attacks and achieves several orders of magnitude acceleration in practical settings, enabling a new and more efficient class of attacks against Poseidon targeting round-reduced permutations and constrained input/output instances. We release open-source code and describe our method in detail, demonstrating substantial improvements over prior approaches: reductions in wall time by a factor of $2^{13}$ and in memory usage by a factor of $2^{4.5}$. Memory-access costs for NTTs turn out to be a dominant barrier in practice. And we prove that this cost increases at least as the 4/3-power of the input size (up to logarithmic factors), which suggests the commonly used pseudo-linear cost model may underestimate the true resource requirements. This behavior contrasts with multivariate equation solving, whose main bottleneck remains finite-field linear algebra. We argue that, when selecting parameters, designers

should account for interpolation-based attacks explicitly, since their practical hardness is determined by different, and sometimes stronger, resource constraints than those of multivariate techniques.

## 1.48 [RLHK+25] UPPR: Universal Privacy-Preserving Revocation

This paper introduces UPPR, a revocation mechanism for One-Show Verifiable Credentials (oVCs) and unlinkable Anonymous Credentials (ACs). Revocations are managed using per-credential Verifiable Random Function (VRF) tokens, which are published in a Bloom filter cascade on a blockchain. Holders prove non-revocation via a VRF proof for oVCs or a single Zero-Knowledge Proof for ACs. The construction prevents revocation status tracking, allows holders to stay offline, and hides issuer revocation behavior. We analyze the privacy properties of UPPR and provide a prototype implementation on Ethereum. Our implementation enables off-chain verification at no cost. On-chain checks cost 0.56-0.84 USD, while issuers pay only 0.00002-0.00005 USD per credential to refresh the revocation state.

## 1.49 [BP25] ALFOMs and the Moirai: Quantifying the Performance/Security Tradeoff for ZK-friendly Hash Functions

In this paper, we show that it is possible to build a simple yet efficient security argument based on a precise estimate of the so-called "algebraic degree" of a system of equations. Furthermore, we show that the increase of this quantity across rounds is tightly connected to the cost of the hash function in two different arithmetizations, namely AIR and R1CS. We precisely quantify this relation by introducing ALgebraic Figures Of Merit (ALFOMs) that capture how efficient a specific primitive (and in fact its round function) are at increasing the security per unit of cost. This new insight allows us to better understand sometimes puzzling performance differences between state-of-the-art hash functions in the R1CS and AIR cases, and to provide a fair and simple comparison of their round functions in this context. Furthermore, we present a new group of round functions we called the Moirai which allow us to explore what a round function providing optimal performance/security tradeoff could look like.

## 1.50 [BCK25] Golden: Lightweight Non-Interactive Distributed Key Generation

In this work, we present Golden, a non-interactive Distributed Key Generation (DKG) protocol. The core innovation of Golden is how it achieves publicly verifiability in a lightweight manner, allowing all participants to non-interactively verify that all other participants followed the protocol correctly. For this reason, Golden can be performed with only one round of (broadcast) communication. Non-interactive DKGs are important for distributed applications; as parties may go offline at any moment, reducing rounds of communication is a desirable feature. Golden outputs Shamir secret

shares of a field element $sk$
$inZ_p$ to all participants, and a public key $PK = g^{sk}$ that is a discrete-logarithm commitment to sk. Further, the security of Golden requires only the hardness of discrete-logarithm assumptions, and so can be used over any elliptic curve where these assumptions hold.

## 1.51 [Kos25] Hashing-friendly elliptic curves

The article introduces a new class of elliptic curves over finite fields, more appropriate for multiple hashing to them. Moreover, two explicit hashing-friendly Montgomery/twisted Edwards curves (of $\approx 128$ security bits) have been generated: one of CM discriminant $-7$, i.e., a GLV-friendly curve and one of huge CM discriminant, i.e., a CM-secure curve. The new elliptic curves are intentionally covered by so-called Klein's and Bring's curves of geometric genera 3 and 4, respectively. The latter are well studied in various algebraic geometry contexts, although they have not yet been (reasonably) applied in cryptography to the author's knowledge. Such a mathematical complication is justified, since conventional curves (from existing standards or of $j$-invariants 0, 1728) are seemingly less efficient for batch hashing.

## 1.52 [SGBK+25] Optimizing the Post Quantum Signature Scheme CROSS for Resource Constrained Devices

In this work, we propose two optimized implementations of the Codes and Restricted Objects Signature Scheme (CROSS) targeting the Cortex-M4 platform. One implementation targets the minimal possible stack size while the other trades some memory space for performance optimization using vectorization for some performance critical arithmetic operations. We show that all parameter sets fit within at maximum 24 kB of stack which corresponds to a reduction by a factor of 15 to 45 with respect to the reference implementation. The memory footprint of our implementation, taking the size of the binary and the signature also into account, is less than 128 kB. We additionally outline different stack reduction options which allow for a fine grained trade-off between memory footprint and performance of the algorithm. Notably, we also show that our memory optimizations alone have no significant impact on the signature verification of CROSS while we even achieve a speed-up factor of up to 1.7 when taking the stack and speed optimizations into account.

## 1.53 [WZZW+25] Attention is still what you need: Another Round of Exploring Shoup's GGM

In this work, we further investigate Shoup's GGM and identify novel limitations that have been previously overlooked. Specifically, to prevent generic algorithms from generating valid group elements without querying the oracle, the model typically employs sufficiently large encoding lengths. This leads to sparse encodings, a setting referred to as the sparse generic group model (sparse GGM).

In conclusion, our findings indicate that both feasibility and impossibility results in Shoup's GGM should be reinterpreted in a fine-grained manner, encouraging further exploration of cryptographic constructions and black-box separations in EC-GGM or dense GGM.

## 1.54 [GL25] Fully Homomorphic Encryption for Matrix Arithmetic

We propose an efficient fully homomorphic encryption (FHE) scheme tailored for matrix arithmetic based on the Ring-Learning with Errors (RLWE) problem. The proposed scheme naturally supports matrix multiplication, addition, and Hadamard multiplication for batched matrices of various sizes over both complex numbers and integers. Encrypted matrix multiplication is reduced to four matrix multiplications of ciphertext elements, without the need for expensive operations such as slot-to-coefficient conversion or ring switching. In addition, the scheme efficiently supports matrix transformations, including general and conjugate transpositions, as well as matrix rotations: inter-matrix rotations across batched matrices and intra-matrix rotations within rows and columns. Moreover, the proposed FHE scheme can be directly combined with existing bootstrapping algorithms. By eliminating the need for expensive operations such as repeated slot rotations and conversion between slot- and coefficient-encoding, the proposed construction achieves significant performance improvements. In our construction, encrypted multiplications of $n \times n$ matrices under slot encoding are decomposed into two parts: (1) matrix multiplication — four $n \times n$ matrix multiplications of ciphertext coefficients, and (2) key switching — with a total cost approximately 2–4 times that of Hadamard multiplication. We implemented the proposed scheme and utilized the FLINT library for the matrix multiplication component. Experimental results demonstrate that, even when leveraging highly optimized implementations, matrix multiplication remains the major cost, indicating that our construction substantially reduces auxiliary overheads and achieves strong overall efficiency.

## 1.55 [FTM25] zk-Cookies: Continuous Anonymous Authentication for the Web

In this paper, we propose Continuous Anonymous Authentication (CAA) schemes and give a concrete construction and applications for preventing credential sharing and theft. CAA schemes allow us to move the server-side collection, storage, and processing of these behavioral signals to the client while maintaining privacy and integrity. CAA schemes support, on the client side, a number of common behavioral analysis tests and analytics both for determining fraudulent behavior and updating security policies. We implement a prototype, zk-Cookies, which runs in the browser, and supports common behavioral signals such as IP address and geolocation history, browser fingerprinting, and page view history. Using this, we build a prototype application for age verification based on legacy credentials (like passports). We implement these checks efficiently in zk-SNARKs, and also show how to securely implement differentially private behavioral analytics in a zk-SNARK. The simplest version of our construction can perform the computation for an update in under 200 ms.

## 1.56 [ZJRY+25] GPV Preimage Sampling with Weak Smoothness and Its Applications to Lattice Signatures

In this work, we investigate the feasibility of *weak smoothness*, e.g. $\epsilon = O(\frac{1}{n})$ or even $O(1)$ in the GPV framework and present several positive results. First, we provide a theoretical security proof for GPV with weak smoothness under a new assumption. Then, we present Gaussian samplers that are compatible with the weak smoothness condition. As direct applications, we present two practical GPV signature instantiations based on a weak smoothness condition. Our first instantiation is a variant of Falcon achieving smaller size and higher security. The public key sizes are 21% to 28% smaller, and the signature sizes are 23.5% to 29% smaller than Falcon. We also showcase an NTRU-based GPV signature scheme that employs the Peikert sampler with weak smoothness. This offers a simple implementation while the security level is greatly lower. Nevertheless, at the NIST-3 security level, our scheme achieves a 49% reduction in size compared to Dilithium-3.

## 1.57 [NRT25] Adaptively-Secure Three-Round Threshold Schnorr from DL

We present the first adaptively-secure threshold Schnorr scheme in three rounds (two online, one offline) in the random oracle model under the DL assumption. Our result demonstrates that achieving both low round complexity and adaptive security is possible while preserving the (so far) minimal assumptions for Schnorr signatures. To achieve this, we introduce new techniques, including a novel use of an equivocal commitment scheme paired with a simulation-extractable NIZK, and a masking-based aggregated opening strategy for homomorphic commitments. Our work also makes several contributions that might be of independent interest, including a formalization of a strong adaptive security notion, a stronger commitment equivocation property, and an analysis of the simulation-extractability of the randomized Fischlin transformation.

## 1.58 [BFL25] Circuit-Succinct Algebraic Batch Arguments from Projective Functional Commitments

In this work, we give the first algebraic (pairing-based) construction of BARG that achieves proof size and online verifier runtime $O(\lambda \cdot |w|)$. We achieve our result by means of a compiler which builds a BARG generically from a projective chainable functional commitment (PCFC), which supports somewhere extraction, subvector projection, and functional openings. We then construct a PCFC from the standard MDDH assumption in bilinear groups by building on top of the functional commitment for circuits by Wee and Wu [Eurocrypt'24]. Our black-box transformation may be of independent interest for understanding the connection between functional commitments and BARGs and towards obtaining other algebraic constructions of the latter.

## 1.59 [YLCX+25] Robust and Scalable Lattice-Based Distributed Key Generation for Asynchronous Networks

This paper presents LADKG, a Lattice-Based Asynchronous Distributed Key Generation framework designed for post-quantum secure and scalable distributed systems. LADKG integrates Asynchronous Verifiable Short Secret Sharing (AV3S) with an Approximate Asynchronous Common Subset (AACS) protocol to achieve efficient key generation. By deferring verification and leveraging deterministic approximate agreement, LADKG reduces computational and communication overhead while maintaining security and robustness. Evaluations on geo-distributed AWS EC2 clusters demonstrate that LADKG is comparable or better than classical Asynchronous Distributed Key Generation (ADKG) schemes in scalability and efficiency. Under optimistic conditions with $n = 121$ nodes, completion is achieved in 45 seconds, ensuring robust key generation for post-quantum secure applications.

## 1.60 [BGCR+25] Fully Adaptive FROST in the Algebraic Group Model From Falsifiable Assumptions

We present the first round-optimal Schnorr threshold signature scheme that achieves full adaptive security against algebraic adversaries, relying solely on the Algebraic One-More Discrete Log (AOMDL) assumption. Our scheme, FaFROST, builds on the FROST framework preserving its two-round signing structure and communication efficiency. By avoiding binding commitments to partial public keys, FaFROST circumvents the recent impossibility results from CRYPTO'25 and requires no reliance on the newly introduced, tailor-made LDVR assumption. This establishes that round-optimal, adaptively secure Schnorr threshold signatures are achievable under well-established algebraic assumptions.

## 1.61 [BCLT+25] Adaptively Secure Partially Non-Interactive Threshold Schnorr Signatures in the AGM

In this paper, we present ms-FROST. Our scheme is partially non-interactive and supports any t - 1 $<$ n adaptive corruptions, where n is the number of signers and t is the signing threshold. Its security relies on the algebraic one-more discrete logarithm (AOMDL) assumption, the algebraic group model (AGM), and the random oracle model (ROM). Further, it achieves the strongest security notion (TS-UF-4) in the security hierarchy of Bellare et al. (CRYPTO 2022). To justify our use of the algebraic group model, we show an impossibility result: We rule out any black-box algebraic security reduction in the ROM from AOMDL to the adaptive TS-UF-0 security of ms-FROST.

## 1.62 [Sak25] Aggregate Signatures Tightly Secure under Adaptive Corruptions

We propose the first aggregate signature scheme tightly secure under adaptive corruptions using pairings. An aggregate signature includes two source group elements of bilinear groups plus a bit vector whose length is equal to the number of single-signer signatures being aggregated. To construct a scheme, we employ a technique from quasi-adaptive non-interactive zero-knowledge arguments. Our construction can be seen as modularization and tightness improvement of Libert et al.'s threshold signature scheme supporting signature aggregation (Theoretical Computer Science 645) in a non-threshold setting.

## 1.63 [CTHK25] Linear-time and Logarithmically-sound Permutation and Multiset SNARKs

We present new arguments with linear-time provers and logarithmic soundness, without auxiliary commitments. Prior work achieving logarithmic soundness error arithmetizes the permutation as a product of several multilinear polynomials, a formulation chosen for compatibility with the classic Sumcheck PIOP. A simpler alternative treats permutations as multilinear extensions of their permutation matrices. While this formulation was previously believed to require quadratic prover time, we show that this overhead can be eliminated by taking a linear-algebraic perspective. This viewpoint has a key advantage: partially evaluating the multilinear polynomial of the permutation requires no additional field operations and amounts to applying the inverse permutation to the verifier's challenge vector. This makes the step essentially free in terms of algebraic cost, unlike in prior approaches. Compared to concurrent work BiPerm (Bünz et al., ePrint Archive, 2025), our scheme requires no permutation preprocessing and supports prover-supplied permutations. We show a sparsity-aware PCS like Dory (Lee, TCC, 2021) can compile our PIOP to a SNARK such that the resulting SNARK prover still runs in time $O(n)$. Our construction is the first logarithmically-sound SNARK with an $O(n)$-time prover for both permutation and multiset checks. We further prove a matching optimal prover lower bound, and we identify specific permutations that can be evaluated by the verifier in $O(\text{polylog}(n))$-time. The ability to evaluate these permutations in $O(\text{polylog}(n))$ time allows the verifier to avoid relying on prover-supplied commitments or evaluation proofs. As a result, we obtain the first logarithmically sound, field-agnostic SNARK with an $O(n)$-time prover in this setting.

## 1.64 [TKKS+25]Cryptographic Personas: Responsible Pseudonyms Without De-Anonymization

We present cryptographic personas, an approach for facilitating access to pseudonymous speech within communities without enabling abuse. In systems equipped with cryptographic personas, users are

able to authenticate to the service provider under new, unlinkable personas at will and post messages under those personas. When users violate community norms, their ability to post anonymously can be revoked. We develop two significant improvements to existing work on anonymous banning systems that make it possible to integrate cryptographic personas into real-time applications like group messaging: we show how to push expensive proof generation into an offline phase and find a way to optimize server-side overhead using recent proof folding techniques.

## 1.65 [CHT25] Tight Security for BBS Signatures

On the positive end, we show a novel tight reduction for BBS in the case where each message is signed at most once–this case covers in particular the common practical use case which derandomizes signing. On the negative end, we use a meta-reduction argument to prove that if we allow generating multiple signatures for the same message, then *no* algebraic reduction to $q$-SDH (and its variants) can be tight.

# Chapter 2

# ESORICS 2025

## 2.1 [ZZSD+26] Extending Groth16 for Disjunctive Statements

In this paper, we mainly focus on the disjunctive statements of Groth16, and we propose a Groth16 variant—CompGroth16, which provides a framework for Groth16 to prove the disjunctive statements that consist of a mix of algebraic and arithmetic components. Specifically, we could directly combine CompGroth16 with varSigma Σ-protocol or even CompGroth16 with CompGroth16 just like the logical composition of varSigma Σ-protocols. From this, we can gain many good properties, such as broader expression, better prover's efficiency and shorter CRS. In addition, for the combination of CompGroth16 and varSigma Σ-protocol, we also present two representative application scenarios to demonstrate the practicality of our construction.

## 2.2 [PH26; PH25] Formalisation of the KZG Polynomial Commitment Schemes in EasyCrypt

In this paper, we present formally verified proofs of the popular KZG Polynomial Commitment Schemes (PCSs), including the security proofs for the properties of correctness, polynomial binding, evaluation binding and hiding. Polynomial commitment schemes have various applications in cryptography and computer science, including verifiable computation, blockchain and cryptocurrencies, secure multi-party computation as well as in the construction of ZK-SNARKs. To validate security, we utilise EasyCrypt, an interactive theorem prover that allows for formal verification of cryptographic primitives and protocols. This approach enforces correct proofs which cover all required cases and formalising assumptions reducing the risk of overlooked vulnerabilities. This formalisation validates the current understanding of KZG's PCSs as secure while clarifying various issues in the original claims.

## 2.3 [WZDW+26] Polylogarithmic Polynomial Commitment Scheme over Galois Rings

This paper introduces the first multilinear polynomial commitment scheme (PCS) over Galois rings achieving $\mathcal{O}\left(\log^2 n\right)$ 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 zeroknowledge 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 $\mathcal{O}\left(\log^2 n\right)$ compared to Wei et al., PKC 2025. Furthermore, we give a batched multipoint opening protocol for evaluation phase that collapses the proof size and verifier time of $N$ polynomials at $M$ points from $\mathcal{O}\left(NM \log^2 n\right)$ to $\mathcal{O}\left(\log^2 n\right)$, prover time from $\mathcal{O}(NMn)$ to $\mathcal{O}(n)$, further enhancing efficiency.

# Chapter 3

# Communications in Cryptology Volume 2, Issue 3

## 3.1 [SR25] Towards Post-Quantum Bitcoin Blockchain using Dilithium Signature

In this work, we analyze the potential replacement of the ECDSA signature, the current signature in Bitcoin, with Dilithium, which is a post-quantum digital signature. This replacement will have a significant impact on many protocols within the Bitcoin ecosystem. The ECDSA algorithms are not only utilized for transaction signing and verification but also in wallet management. Bitcoin operates on a pseudonymous system rather than complete anonymity. To enhance privacy protection, the Bitcoin community has adopted a special type of (hierarchical) deterministic wallet as outlined in Bitcoin Improvement Proposal 32 (BIP32). We have constructed deterministic wallets by first designing DilithiumRK, a signature scheme with rerandomizable keys from Dilithium. Subsequently, we conducted a thorough security analysis and successful implementation of DilithiumRK.

## 3.2 [HHI25] Practical Batch Proofs of Exponentiation

In this work, we introduce two batch PoEs that outperform both proposals of Rotem and we evaluate their practicality. First, we show that the two batch PoEs of Rotem can be combined to improve the overall efficiency by at least a factor of two. Second, we revisit the work of Bellare, Garay and Rabin (EUROCRYPT 1998) on batch verification of digital signatures and show that, under the low order assumption, their bucket test can be securely adapted to the setting of groups of unknown order. The resulting batch PoE quickly outperforms the state of the art in the expected number of group multiplications with the growing number of instances, and it decreases the cost of batching by an order of magnitude already for hundreds of thousands of instances. Importantly, it is the first batch PoE that significantly decreases both the proof size and complexity of verification.

## 3.3 [GBKS+25] Blind zkSNARKs: for Private Proof Delegation and Verifiable Computation over Encrypted Data

In this paper, we show for the first time it is practical to privately delegate proof generation of zkSNARKs to a single server for computations of up to $2^{20}$ R1CS constraints. We achieve this by computing zkSNARK proof generation over homomorphic ciphertexts, an approach we call blind zkSNARKs. We formalize the concept of blind proofs, analyze their cryptographic properties and show that the resulting blind zkSNARKs remain sound when compiled using BCS compilation. Our work follows the framework proposed by Garg et al. (Crypto'24) and improves the instantiation presented by Aranha et al. (Asiacrypt'24), which implements only the FRI subprotocol. By delegating proof generation, we are able to reduce client computation time from 10 minutes to mere seconds, while server computation time remains limited to 20 minutes. We also propose a practical construction for vCOED supporting constraint sizes four orders of magnitude larger than the current state-of-the-art verifiable FHE-based approaches. These results are achieved by optimizing Fractal for the GBFV homomorphic encryption scheme, including a novel method for making homomorphic NTT evaluation packing-friendly by computing it in two dimensions. Furthermore, we make the proofs publicly verifiable by appending a zero-knowledge Proof of Decryption (PoD). We propose a new construction for PoDs optimized for low proof generation time, exploiting modulus and ring switching in GBFV and using the Schwartz-Zippel lemma for proof batching; these techniques might be of independent interest. Finally, we implement the latter protocol in C and report on execution time and proof sizes.

## 3.4 [MBSB+25] Keyed-Verification Anonymous Credentials with Highly Efficient Partial Disclosure

Our first construction adapts the approach of Fuchsbauer, Hanser and Slamanig (JoC'19), which achieved constant-size credential presentation in a publicly verifiable setting using their proposed structure-preserving signatures on equivalence classes (SPS-EQ) and set commitment schemes, to the KVAC setting. We introduce structure-preserving message authentication codes on equivalence classes (SP-MAC-EQ) and designated-verifier set commitments (DVSC), resulting in a KVAC system with constant-size credentials (2 group elements) and presentations (5 group elements). To avoid the bilinear groups and pairing operations required by SP-MAC-EQ, our second construction uses a homomorphic MAC with a simplified DVSC. While this sacrifices constant-size credentials (n+2 group elements, where n is the number of attributes), it retains constant-size presentations (2 group elements) in a pairingless setting.

## 3.5 [DH25] zkMaP: Zero-Knowledge Succinct Non-Interactive Matrix Multiplication Proofs

We introduce zkMaP (Zero-Knowledge Succinct Non-Interactive Matrix Multiplication Proofs), a novel non-interactive zero-knowledge proof system for verifying matrix multiplication with significant improvements in efficiency and scalability. Our protocol leverages KZG polynomial commitments and an innovative inner-product reduction technique to reduce the verification of n x n matrix multiplication to a single pairing equation, thereby enabling constant-time verification independent of the matrix size. In particular, zkMaP requires only two pairing operations and produces proofs as small as 320 bytes, yielding a 96 percent reduction in proof size compared to prior schemes.

## 3.6 [OPS25b; OPS25a] Who Verifies the Verifiers? Lessons Learned From Formally Verified Line-Point 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.

## 3.7 [MP25b; MP25a] 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.

# Bibliography


[AAFK+25] Hamza Abusalah, Karen Azari, Dario Fiore, Chethan Kamath, and Erkan Tairi. *On Verifiable Delay Functions from Time-Lock Puzzles*. Cryptology ePrint Archive, Paper 2025/1782. 2025 (cit. on p. 8).

[AAKT+25] Hamza Abusalah, Karen Azari, Chethan Kamath, Erkan Tairi, and Maximilian von Consbruch. *Impossibility of VDFs in the ROM: The Complete Picture*. Cryptology ePrint Archive, Paper 2025/1773. 2025 (cit. on p. 8).

[AB25] Tiiago A. O. Alves and Vitor Py Braga. *Zyga: Optimized Zero-Knowledge Proofs with Dynamic Public Inputs*. Cryptology ePrint Archive, Paper 2025/1802. 2025 (cit. on p. 10).

[AFLL+25] Martin R. Albrecht, Joël Felderhoff, Russell W. F. Lai, Oleksandra Lapiha, and Ivy K. Y. Woo. *A Gaussian Leftover Hash Lemma for Modules over Number Fields*. Cryptology ePrint Archive, Paper 2025/1852. 2025 (cit. on p. 17).

[AMK25] Supriya Adhikary, Puja Mondal, and Angshuman Karmakar. *Lattice-Based zk-SNARKs with Hybrid Verification Technique*. Cryptology ePrint Archive, Paper 2025/1839. 2025 (cit. on p. 13).

[BCD25] Benedikt Bünz, Jessica Chen, and Zachary DeStefano. *Linear*-Time Permutation Check*. Cryptology ePrint Archive, Paper 2025/1850. 2025 (cit. on p. 16).

[BCK25] Benedikt Bünz, Kevin Choi, and Chelsea Komlo. *Golden: Lightweight Non-Interactive Distributed Key Generation*. Cryptology ePrint Archive, Paper 2025/1924. 2025 (cit. on p. 24).

[BCLT+25] Renas Bacho, Yanbo Chen, Julian Loss, Stefano Tessaro, and Chenzhi Zhu. *Adaptively Secure Partially Non-Interactive Threshold Schnorr Signatures in the AGM*. Cryptology ePrint Archive, Paper 2025/1953. 2025 (cit. on p. 28).

[BF25] Barbara Jiabao Benedikt and Marc Fischlin. *The Order of Hashing in Fiat-Shamir Schemes*. Cryptology ePrint Archive, Paper 2025/1846. 2025 (cit. on p. 15).

[BFL25] David Balbás, Dario Fiore, and Russell W. F. Lai. *Circuit-Succinct Algebraic Batch Arguments from Projective Functional Commitments*. Cryptology ePrint Archive, Paper 2025/1943. 2025 (cit. on p. 27).

[BGCR+25] Ruben Baecker, Paul Gerhart, Davide Li Calsi, Luigi Russo, Dominique Schröder, and Arkady Yerukhimovich. *Fully Adaptive FROST in the Algebraic Group Model From Falsifiable Assumptions*. Cryptology ePrint Archive, Paper 2025/1950. 2025 (cit. on p. 28).

[BGY25] Foteini Baldimtsi, Rishab Goyal, and Aayush Yadav. *Batched & Non-interactive Blind Signatures from Lattices*. Cryptology ePrint Archive, Paper 2025/1771. 2025 (cit. on p. 7).

[BHMV25] Samuel Bouaziz–Ermann, Minki Hhan, Garazi Muguruza, and Quoc-Huy Vu. *On Limits on the Provable Consequences of Quantum Pseudorandomness*. Cryptology ePrint Archive, Paper 2025/1863. 2025 (cit. on p. 18).

[BM25] Pedro Branco and Giulio Malavolta. *Threshold Signatures from One-Way Functions*. Cryptology ePrint Archive, Paper 2025/1762. 2025 (cit. on p. 6).

[BP25] Aurélien Boeuf and Léo Perrin. *ALFOMs and the Moirai: Quantifying the Performance/Security Tradeoff for ZK-friendly Hash Functions*. Cryptology ePrint Archive, Paper 2025/1920. 2025 (cit. on p. 24).

[CDGV25] Alain Couvreur, Thomas Debris-Alazard, Philippe Gaborit, and Adrien Vinçotte. *MIRANDA: short signatures from a leakage-free full-domain-hash scheme*. Cryptology ePrint Archive, Paper 2025/1878. 2025 (cit. on p. 19).

[CFJW25] Liyan Chen, Cody Freitag, Zhengzhong Jin, and Daniel Wichs. *Unambiguous SNARGs for P from LWE with Applications to PPAD Hardness*. Cryptology ePrint Archive, Paper 2025/1913. 2025 (cit. on p. 23).

[CH25] André Chailloux and Paul Hermouet. *On the Quantum Equivalence between S|LWE> and ISIS*. Cryptology ePrint Archive, Paper 2025/1857. 2025 (cit. on p. 17).

[Che25] Binyi Chen. *Symphony: Scalable SNARKs in the Random Oracle Model from Lattice-Based High-Arity Folding*. Cryptology ePrint Archive, Paper 2025/1905. 2025 (cit. on p. 22).

[CHT25] Rutchathon Chairattana-Apirom, Dennis Hofheinz, and Stefano Tessaro. *Tight Security for BBS Signatures*. Cryptology ePrint Archive, Paper 2025/1973. 2025 (cit. on p. 30).

[CMV25] Rohit Chatterjee, Changrui Mu, and Prashant Nalini Vasudevan. *Public-Key Encryption from the MinRank Problem*. Cryptology ePrint Archive, Paper 2025/1833. 2025 (cit. on p. 13).

[CSK25] Seunghyun Cho, Eunyoung Seo, and Young-Sik Kim. *Locally Recoverable Data Availability Sampling*. Cryptology ePrint Archive, Paper 2025/1851. 2025 (cit. on p. 17).

[CTHK25] Bing-Jyue Chen, Lilia Tang, David Heath, and Daniel Kang. *Linear-time and Logarithmically-sound Permutation and Multiset SNARKs*. Cryptology ePrint Archive, Paper 2025/1967. 2025 (cit. on p. 29).

[CYY25] Mingshu Cong, Tsz Hon Yuen, and Siu-Ming Yiu. *DualMatrix: Conquering zkSNARK for Large Matrix Multiplication*. Cryptology ePrint Archive, Paper 2025/1768. 2025 (cit. on p. 7).

[DH25] Biniyam Deressa and M. Anwar Hasan. "zkMaP: Zero-Knowledge Succinct Non-Interactive Matrix Multiplication Proofs". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). ISSN: 3006-5496 (cit. on p. 35).

[FPST25] Andrea Flamini, Federico Pintore, Edoardo Signorini, and Giovanni Tognolini. *New Straight-Line Extractable NIZKPs for Cryptographic Group Actions*. Cryptology ePrint Archive, Paper 2025/1819. 2025 (cit. on p. 11).

[FTM25] Alexander Frolov, Hal Triedman, and Ian Miers. *zk-Cookies: Continuous Anonymous Authentication for the Web*. Cryptology ePrint Archive, Paper 2025/1938. 2025 (cit. on p. 26).

[GBKS+25] Mariana Gama, Emad Heydari Beni, Jiayi Kang, Jannik Spiessens, and Frederik Vercauteren. "Blind zkSNARKs: for Private Proof Delegation and Verifiable Computation over Encrypted Data". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). ISSN: 3006-5496 (cit. on p. 34).

[GHKS+25] Kamil Doruk Gur, Patrick Hough, Jonathan Katz, Caroline Sandsbråten, and Tjerand Silde. *Olingo: Threshold Lattice Signatures with DKG and Identifiable Abort*. Cryptology ePrint Archive, Paper 2025/1789. 2025 (cit. on p. 9).

[GK25] Ariel Gabizon and Nishat Koti. *A note on the soundness of an optimized* gemini *variant*. Cryptology ePrint Archive, Paper 2025/1793. 2025 (cit. on p. 9).

[GKKP+25] Anindya Ganguly, Angshuman Karmakar, Suparna Kundu, Debranjan Pal, and Sumanta Sarkar. *Revisiting Lattice-based Non-interactive Blind Signature*. Cryptology ePrint Archive, Paper 2025/1848. 2025 (cit. on p. 16).

[GKKR+25] Lorenzo Grassi, Dmitry Khovratovic, Katharina Koschatko, Christian Rechberger, Markus Schofnegger, and Verena Schröppel. *Poseidon2b: A Binary Field Version of Poseidon2*. Cryptology ePrint Archive, Paper 2025/1893. 2025 (cit. on p. 20).

[GL25] Craig Gentry and Yongwoo Lee. *Fully Homomorphic Encryption for Matrix Arithmetic*. Cryptology ePrint Archive, Paper 2025/1935. 2025 (cit. on p. 26).

[GR25] Vipul Goyal and Justin Raizes. *Proofs of No Intrusion*. Cryptology ePrint Archive, Paper 2025/1826. 2025 (cit. on p. 12).

[HACF25] Hossein Hafezi, Gaspard Anthoine, Matteo Campanelli, and Dario Fiore. *SoK: Lookup Table Arguments*. Cryptology ePrint Archive, Paper 2025/1876. 2025 (cit. on p. 19).

[HHI25] Charlotte Hoffmann, Pavel Hubáček, and Svetlana Ivanova. "Practical Batch Proofs of Exponentiation". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). ISSN: 3006-5496 (cit. on p. 33).

[Hio25] Leona Hioki. *Anchored Merkle Range Proof for Pedersen Commitments*. Cryptology ePrint Archive, Paper 2025/1811. 2025 (cit. on p. 11).

[HMOY25] Minki Hhan, Tomoyuki Morimae, Yasuaki Okinaka, and Takashi Yamakawa. *Proofs of quantum memory*. Cryptology ePrint Archive, Paper 2025/1837. 2025 (cit. on p. 13).

[HV25] Andrew Huang and Vinod Vaikuntanathan. *A Simple and Efficient One-Shot Signature Scheme*. Cryptology ePrint Archive, Paper 2025/1906. 2025 (cit. on p. 22).

[Jan25] Jonas Janneck. *Bird of Prey: Practical Signature Combiners Preserving Strong Unforgeability*. Cryptology ePrint Archive, Paper 2025/1844. 2025 (cit. on p. 15).

[JBW25] Kunming Jiang, Fraser Brown, and Riad S. Wahby. *CoBBl: Dynamic constraint generation for SNARKs*. Cryptology ePrint Archive, Paper 2025/1849. 2025 (cit. on p. 16).

[Kiy25] Susumu Kiyoshima. *Four-round Statistical Non-malleable Zero-knowledge*. Cryptology ePrint Archive, Paper 2025/1787. 2025 (cit. on p. 9).

[KKAŚ+25] Marcin Kostrzewa, Matthew Klein, Ara Adkins, Grzegorz Świrski, and Wojciech Żmuda. *Keccacheck: towards a SNARK friendly Keccak*. Cryptology ePrint Archive, Paper 2025/1764. 2025 (cit. on p. 6).

[KLR25] Michael Klooß, Russell W. F. Lai, and Michael Reichle. *Blind Signatures from Arguments of Inequality*. Cryptology ePrint Archive, Paper 2025/1886. 2025 (cit. on p. 20).

[Kon25] Yashvanth Kondi. *Two-party ECDSA Signing at Constant Communication Overhead*. Cryptology ePrint Archive, Paper 2025/1813. 2025 (cit. on p. 11).

[Kos25] Dimitri Koshelev. *Hashing-friendly elliptic curves*. Cryptology ePrint Archive, Paper 2025/1926. 2025 (cit. on p. 25).

[KPRR+25] Vladimir Kolesnikov, Stanislav Peceny, Rahul Rachuri, Srinivasan Raghuraman, Peter Rindal, and Harshal Shah. *Block-Accumulate Codes: Accelerated Linear Codes for PCGs and ZK*. Cryptology ePrint Archive, Paper 2025/1828. 2025 (cit. on p. 12).

[Liu25] Xiangyu Liu. *Traceable Ring Signatures Revisited: Extended Definitions, $O(1)$ Tracing, and Efficient Log-Size Constructions*. Cryptology ePrint Archive, Paper 2025/1807. 2025 (cit. on p. 10).

[LXYY+25] Zhe Li, Chaoping Xing, Yizhou Yao, Chen Yuan, and Mengmeng Zhou. *Succinct Line-Point Zero-Knowledge Arguments from Homomorphic Secret Sharing*. Cryptology ePrint Archive, Paper 2025/1866. 2025 (cit. on p. 18).

[MBSB+25] Omid Mirzamohammadi, Jan Bobolz, Mahdi Sedaghat, Emad Heydari Beni, Aysajan Abidin, Dave Singelée, and Bart Preneel. "Keyed-Verification Anonymous Credentials with Highly Efficient Partial Disclosure". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). ISSN: 3006-5496 (cit. on p. 34).

[MP25a] Jules Maire and Alan Pulval-Dady. *Blind ECDSA from the ECDSA Assumption*. Cryptology ePrint Archive, Paper 2025/1827. 2025 (cit. on p. 35).

[MP25b] Jules Maire and Alan Pulval-Dady. "Blind ECDSA from the ECDSA Assumption". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). ISSN: 3006-5496 (cit. on p. 35).

[MSY25] Tomoyuki Morimae, Yuki Shirakawa, and Takashi Yamakawa. *Quantum Cryptography and Hardness of Non-Collapsing Measurements*. Cryptology ePrint Archive, Paper 2025/1840. 2025 (cit. on p. 14).

[NRT25] Guilhem Niot, Michael Reichle, and Kaoru Takemure. *Adaptively-Secure Three-Round Threshold Schnorr from DL*. Cryptology ePrint Archive, Paper 2025/1941. 2025 (cit. on p. 27).

[OPS25a] Sabine Oechsner, Vitor Pereira, and Peter Scholl. *Who Verifies the Verifiers? Lessons Learned From Formally Verified Line-Point Zero-Knowledge*. Cryptology ePrint Archive, Paper 2025/1835. 2025 (cit. on p. 35).

[OPS25b] Sabine Oechsner, Vitor Pereira, and Peter Scholl. "Who Verifies the Verifiers? Lessons Learned From Formally Verified Line-Point Zero-Knowledge". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). ISSN: 3006-5496 (cit. on p. 35).

[PH25] Palak and Thomas Haines. *Formalisation of the KZG polynomial commitment schemes in EasyCrypt*. Cryptology ePrint Archive, Paper 2025/1972. 2025 (cit. on p. 31).

[PH26] Palak and Thomas Haines. "Formalisation of the KZG Polynomial Commitment Schemes in EasyCrypt". In: *Computer Security – ESORICS 2025*. Ed. by Vincent Nicomette, Abdelmalek Benzekri, Nora Boulahia-Cuppens, and Jaideep Vaidya. Cham: Springer Nature Switzerland, 2026, pp. 303–320. ISBN: 978-3-032-07891-9 (cit. on p. 31).

[QTW25] Willy Quach, LaKyah Tyner, and Daniel Wichs. *Unique NIZKs and Steganography Detection*. Cryptology ePrint Archive, Paper 2025/1898. 2025 (cit. on p. 21).

[RLHK+25] Leandro Rometsch, Philipp-Florens Lehwalder, Anh-Tu Hoang, Dominik Kaaser, and Stefan Schulte. *UPPR: Universal Privacy-Preserving Revocation*. Cryptology ePrint Archive, Paper 2025/1919. 2025 (cit. on p. 24).

[RR25] Michael Reichle and Zoé Reinke. *Threshold Blind Signatures from CDH*. Cryptology ePrint Archive, Paper 2025/1798. 2025 (cit. on p. 9).

[Sak25] Yusuke Sakai. *Aggregate Signatures Tightly Secure under Adaptive Corruptions*. Cryptology ePrint Archive, Paper 2025/1955. 2025 (cit. on p. 29).

[SGBK+25] Jonas Schupp, Marco Gianvecchio, Alessandro Barenghi, Patrick Karl, Gerardo Pelosi, and Georg Sigl. *Optimizing the Post Quantum Signature Scheme CROSS for Resource Constrained Devices*. Cryptology ePrint Archive, Paper 2025/1928. 2025 (cit. on p. 25).

[SKVP25] Nikita Snetkov, Mihkel Jaas Karu, Jelizaveta Vakarjuk, and Alisa Pankova. *Coppercloud: Blind Server-Supported RSA Signatures*. Cryptology ePrint Archive, Paper 2025/1824. 2025 (cit. on p. 12).

[SR25] Michel Seck and Adeline Roux-Langlois. "Towards Post-Quantum Bitcoin Blockchain using Dilithium Signature". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). ISSN: 3006-5496 (cit. on p. 33).

[TKKS+25] Rachel Thomas, Oliwia Kempinski, Hari Kailad, Emma Margaret Shroyer, Ian Miers, and Gabriel Kaptchuk. *Cryptographic Personas: Responsible Pseudonyms Without De-Anonymization*. Cryptology ePrint Archive, Paper 2025/1969. 2025 (cit. on p. 29).

[WZDW+25] Zhuo Wu, Xinxuan Zhang, Yi Deng, Yuanju Wei, Zhongliang Zhang, and Liuyu Yang. *Polylogarithmic Polynomial Commitment Scheme over Galois Rings*. Cryptology ePrint Archive, Paper 2025/1767. 2025 (cit. on p. 6).

[WZDW+26] Zhuo Wu, Xinxuan Zhang, Yi Deng, Yuanju Wei, Zhongliang Zhang, and Liuyu Yang. "Polylogarithmic Polynomial Commitment Scheme over Galois Rings". In: *Computer Security – ESORICS 2025*. Ed. by Vincent Nicomette, Abdelmalek Benzekri, Nora Boulahia-Cuppens, and Jaideep Vaidya. Cham: Springer Nature Switzerland, 2026, pp. 400–420. ISBN: 978-3-032-07891-9 (cit. on p. 32).

[WZZW+25] Taiyu Wang, Cong Zhang, Hong-Sheng Zhou, Xin Wang, Pengfei Chen, Wenli Wang, Kui Ren, and Chun Chen. *Attention is still what you need: Another Round of Exploring Shoup's GGM*. Cryptology ePrint Archive, Paper 2025/1930. 2025 (cit. on p. 25).

[YLCX+25] Linghe Yang, Jian Liu, Jingyi Cui, Guangquan Xu, Mingzi Zuo, Lei Zhang, and Zhongshan Li. *Robust and Scalable Lattice-Based Distributed Key Generation for Asynchronous Networks*. Cryptology ePrint Archive, Paper 2025/1946. 2025 (cit. on p. 28).

[ZGCP+25] Lizhen Zhang, Shang Gao, Sherman S. M. Chow, Kurt Pan, and Bin Xiao. *HyperWolf: Lattice Polynomial Commitments with Standard Soundness*. Cryptology ePrint Archive, Paper 2025/1903. 2025 (cit. on p. 21).

[ZGGX25] Tianyu Zheng, Shang Gao, Yu Guo, and Bin Xiao. *Quasar: Sublinear Accumulation Schemes for Multiple Instances*. Cryptology ePrint Archive, Paper 2025/1912. 2025 (cit. on p. 23).

[ZJRY+25] Shiduo Zhang, Huiwen Jia, Delong Ran, Yang Yu, Yu Yu, and Xiaoyun Wang. *GPV Preimage Sampling with Weak Smoothness and Its Applications to Lattice Signatures*. Cryptology ePrint Archive, Paper 2025/1940. 2025 (cit. on p. 27).

[ZLSZ+25] Xinyu Zhang, Ziyi Li, Ron Steinfeld, Raymond K. Zhao, Joseph K. Liu, and Tsz Hon Yuen. *Pegasus and PegaRing: Efficient (Ring) Signatures from Sigma-Protocols for Power Residue PRFs with (Q)ROM Security*. Cryptology ePrint Archive, Paper 2025/1841. 2025 (cit. on p. 14).

[ZOZ25] Tianyu Zhang, Yupeng Ouyang, and Yupeng Zhang. *Dynark: Making Groth16 Dynamic*. Cryptology ePrint Archive, Paper 2025/1897. 2025 (cit. on p. 20).

[ZSVD25] Ziyu Zhao, Antonio Sanso, Giuseppe Vitto, and Jintai Ding. *Graeffe-Based Attacks on Poseidon and NTT Lower Bounds*. Cryptology ePrint Archive, Paper 2025/1916. 2025 (cit. on p. 23).

[ZZ25] Jipeng Zhang and Jiaheng Zhang. *Vectorized Falcon-Sign Implementations using SSE2, AVX2, AVX-512F, NEON, and RVV*. Cryptology ePrint Archive, Paper 2025/1867. 2025 (cit. on p. 19).

[ZZSD+26] Xudong Zhu, Xinxuan Zhang, Xuyang Song, Yi Deng, Yuanju Wei, and Liuyu Yang. "Extending Groth16 for Disjunctive Statements". In: *Computer Security – ESORICS 2025*. Ed. by Vincent Nicomette, Abdelmalek Benzekri, Nora Boulahia-Cuppens, and Jaideep Vaidya. Cham: Springer Nature Switzerland, 2026, pp. 506–527. ISBN: 978-3-032-07891-9 (cit. on p. 31).