Miraidon: MinRank Identification

Ryann Cartor[1] and Freeman Slaughter[2] *

[1] Clemson University, Clemson SC, USA
[2] University of South Florida, Tampa FL, USA
fslaughter@usf.edu

Abstract. We introduce *Miraidon*, a new family of MinRank-based post-quantum signature schemes built from a novel zero-knowledge proof system. Our primary construction, *Miraidon-S*, is a digital signature scheme with competitive public key and signature sizes, improved soundness parameters, and security based on the hardness of the MinRank problem. Building on this framework, we further construct *Miraidon-RS*, a ring signature scheme, and introduce *Miraidon-LRS*, the first linkable ring signature scheme based on the MinRank problem. We present concrete parameters and comparisons with contemporary lattice- and code-based ring and linkable ring signatures, showing that MinRank provides a promising foundation for efficient advanced post-quantum signature primitives.

Keywords: MinRank, zero-knowledge proof, signature scheme, linkable ring signature

1 Introduction

In our increasingly digital world, digital signatures play a fundamental role in ensuring the authenticity and integrity of communications. As quantum computing threatens many classical public-key primitives, the development of efficient and secure post-quantum signature schemes has become a core focus in modern cryptography. Beyond standard signatures, there is growing interest in multifunctional signature primitives that provide additional privacy or functionality guarantees. One important example is the notion of a ring signature, introduced in [48]. Ring signatures allow any legitimate member of a set of users to anonymously sign a message on behalf of the entire group, without revealing which member actually produced the signature. Ring Signatures do not require any prearranged groups among users; each member only needs a public key from a conventional signature scheme such as RSA.

As attention shifts to post-quantum protocols, interest in post-quantum ring signatures has followed. One such scheme is MR-DSS [17], which is a post-quantum ring signature scheme based on the MinRank problem.

The MinRank problem has long occupied an important role in post-quantum cryptography, both as a tool for cryptanalysis and as a candidate hard problem underlying secure cryptographic constructions. It first appeared first appeared in the cryptographic setting in [42] as an attack against the HFE multivariate cryptosystem. In this attack, as well as most of the MinRank attacks against public key cryptosystems, one searches for low-rank linear combinations of public equations in order to recover hidden algebraic structure associated with secret low-rank maps.

Beyond cryptanalysis, MinRank has attracted attention as a computational hardness assumption in its own right. The decisional version of MinRank was shown to be NP-complete [23], while both

* This research was supported by the National Science Foundation (Grant Number DMS-2342254).

theoretical and experimental evidence suggest that random instances are hard to solve in practice. Moreover, no known quantum algorithms provide a substantial asymptotic speedup for solving generic MinRank instances. These properties, combined with the extensive cryptanalytic study of the problem over the past two decades, make MinRank a compelling foundation for identification and signature schemes in the post-quantum setting.

Further supporting the view that MinRank is an attractive problem for cryptographic constructions, several MinRank-based schemes have been included in the NIST standardization process for additional digital signatures [47]. Now in its third round, the first round of the call included the MinRank-based signature schemes MIRA [6,5] and MiRitH [2,1], which merged to Mirath [3] in the second round. These schemes rely on different proofs of knowledge introduced in [33], both of which are based on the "MPC-in-the-Head" paradigm [39], where a single prover internally simulates the execution of a multi-party computation protocol.

1.1 Our Contribution

We design a novel MinRank signature scheme with competitive sizes and soundness errors. In this work, we introduce *Miraidon*, a novel MinRank-based signature framework with competitive signature and key sizes, as well as improved soundness parameters. Building on a new underlying zero-knowledge proof system, we develop *Miraidon-S*, a digital signature scheme whose security is proven against forgery attacks and whose parameters are chosen to withstand the best known attacks on the MinRank problem. We provide concrete parameter sets targeting NIST Security Levels I, III, and V, and show that the resulting schemes achieve competitive communication costs compared to existing post-quantum constructions. In particular, we compare favorably against MR-DSS [17], as well as several modern code-based signature schemes.

Beyond standard signatures, we extend our construction to obtain *Miraidon-RS*, a ring signature scheme derived from our MinRank framework. We further introduce *Miraidon-LRS*, to the best of our knowledge the first linkable ring signature scheme based on the MinRank problem. We present concrete parameter sets for both constructions and compare them against existing code-based and lattice-based ring and linkable ring signatures, demonstrating that our schemes are competitive with contemporary post-quantum alternatives in both efficiency and security.

1.2 Organization

The remainder of this paper is organized as follows. Section 2 reviews the necessary background on zero-knowledge proofs, identification schemes, digital signatures, ring signatures, and linkable ring signatures. Section 3 introduces the MinRank problem, surveys the most relevant attacks, and reviews prior MinRank-based cryptographic constructions. In Section 4, we present the zero-knowledge proof underlying Miraidon, prove its security properties, and describe several efficiency optimizations. Section 5 introduces Miraidon-S, including its algorithms, security analysis, concrete parameters, and performance evaluation. Section 6 extends the framework to the ring signature scheme Miraidon-RS and the linkable ring signature scheme Miraidon-LRS, together with parameter recommendations and comparisons to existing post-quantum constructions. Finally, Section 7 concludes the paper and outlines future work, while additional definitions and deferred proofs are provided in the Appendix.

2 Preliminaries

For q a prime power, let $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q^\star = \mathbb{F}_q \setminus \{0\}$. Then $\mathbb{F}_q^n$ is the set of length n vectors and $\mathbb{F}_q^{m\times n}$ the set of $m \times n$ matrices, both with entries in $\mathbb{F}_q$. We reserve GL_n for the group of $n \times n$ invertible matrices, without explicitly stating entries in $\mathbb{F}_q$. We let $[n]$ represent the set $\{1, 2, \ldots, n\}$ for $n \in \mathbb{N}$.

Let λ be a specified security parameter. We say that a function is negligible in λ if it vanishes faster than the inverse of any polynomial in λ. All algorithms are assumed to be probabilistic polynomial-time (PPT).

Let $\mathtt{com}$ denote a commitment function, which we model as a cryptographically secure hash function. We assume that $\mathtt{com}$ is both *hiding*, meaning that the commitment output reveals no information about the input, and *binding*, meaning that is it intractable to compute a different input that leads to an output collision.

2.1 Zero-Knowledge Proofs and Identification Protocols

Zero-Knowledge Proofs (ZKPs), as introduced in [37], allow a prover $\mathcal{P}$ to convince a verifier $\mathcal{V}$ that a statement is true without revealing any additional information beyond the validity of the statement itself. More formally, for a relation $\mathcal{R}$, the prover seeks to convince the verifier that there exists a witness w such that $(x; w) \in \mathcal{R}$ for a given statement x.

A ZKP may consist of multiple rounds of interaction between the prover and verifier, commonly referred to as the number of "passes" in the protocol. The standard definition of a Σ-protocol from [9] considers a 3-pass interactive proof. Since all protocols considered in this work are instead 5-pass protocols, we adapt the standard definitions accordingly. A generic example of a 5-pass ZKP is given in Algorithm 1.

Public: Relation $\mathcal{R}$, statement x
Private: Witness w such that $(x; w) \in \mathcal{R}$

PROVER		**VERIFIER**
$\mathtt{seed} \xleftarrow{\$} \{0,1\}^\lambda$		
$\mathtt{data}_1 \leftarrow \mathcal{A}(x, w, \mathtt{seed})$		
$\mathtt{com}_1 = \mathtt{com}(\mathtt{data}_1)$	$\xrightarrow{\mathtt{com}_1}$	
	$\xleftarrow{\mathtt{chal}_1}$	$\mathtt{chal}_1 \xleftarrow{\$} \mathcal{C}_1$
$\mathtt{data}_2 \leftarrow \mathcal{A}(\mathtt{data}_1, \mathtt{chal}_1)$		
$\mathtt{com}_2 = \mathtt{com}(\mathtt{data}_2)$	$\xrightarrow{\mathtt{com}_2}$	
	$\xleftarrow{\mathtt{chal}_2}$	$\mathtt{chal}_2 \xleftarrow{\$} \mathcal{C}_2$
$\mathtt{resp} \leftarrow \mathcal{A}(\mathtt{data}_1, \mathtt{chal}_1, \mathtt{data}_2, \mathtt{chal}_2)$	$\xrightarrow{\mathtt{resp}}$	
		return $\mathcal{V}(x, \mathtt{com}_1, \mathtt{chal}_1, \mathtt{com}_2, \mathtt{chal}_2, \mathtt{resp})$

Algorithm 1: The structure of a 5-pass zero-knowledge proof.

Definition 1 (Zero-Knowledge Proof). *An interactive protocol is a zero-knowledge proof for a relation $\mathcal{R}$ and challenge spaces $\mathcal{C}_1$ and $\mathcal{C}_2$ if it has the form of Algorithm 1 and the following holds:*

- ***Completeness****: If both parties are honest, then the verifier always accepts.*
- ***Soundness****: If there exists no witness w such that $(x; w) \in \mathcal{R}$, $\mathcal{V}$ accepts with negligible probability.*
- ***Zero-Knowledge****: There exists a PPT simulator algorithm $\mathcal{S}$ which can produce a transcript indistinguishable from a genuine interaction between $\mathcal{P}$ and $\mathcal{V}$ without access to witness w.*

It was first noted in [34] that one could generically transform zero-knowledge proofs into signature schemes by replacing the verifier's random challenge with a hash digest. This idea was leveraged in [32] to formalize identification schemes and proofs of knowledge. We follow the Fiat-Shamir framework to turn our MinRank ZKP presented in Algorithm 3 into a full-fledged non-interactive signature scheme.

The following definition from [26] is crucial for the protocols considered in this work, where the sizes of the challenge spaces are fixed such that $|\mathcal{C}_1| = q - 1$ and $|\mathcal{C}_2| = 2$.

Definition 2 ($(q-1,2)$-Identification Scheme). *A $(q-1,2)$-identification scheme is a 5-pass interactive protocol such that $\mathtt{chal}_1$ is selected from a set of cardinality $q-1$ (such as $\mathbb{F}_q \setminus \{0\}$), $\mathtt{chal}_2$ from a binary set (such as $\{0,1\}$), and the output of $\mathtt{com}$ appears indistinguishable from random.*

These $(q-1,2)$-identification schemes achieve a soundness error of $\frac{q}{2(q-1)}$, meaning that the probability a dishonest prover can successfully convince a verifier in a single round is $\frac{q}{2(q-1)}$. Additionally, these protocols satisfy a stronger type of soundness, the $(2,2)$-out-of-$(q-1,2)$-special soundness property: a witness can be extracted from two transcripts with distinct first challenges, where for each they receive both second challenge responses. [7,8].

2.2 Signatures, Ring Signatures, and Linkable Ring Signatures

The Fiat-Shamir heuristic [34] is a standard technique for converting an interactive proof into a non-interactive zero-knowledge argument by replacing the verifier's random coin tosses with values derived in a publicly verifiable manner. In this paradigm, the verifier's challenges may be generated deterministically by applying a cryptographic hash function to the protocol transcript:

$$\mathtt{chal}_1 = \mathtt{com}\,(x, \mathtt{com}_1, \mathtt{salt}).$$

In the Random Oracle Model (ROM), an idealized framework in which each unique input produces a truly random uniform output, this transformation preserves the soundness and zero-knowledge properties of the underlying protocol. This allows for the transformation from an interactive identification scheme to a non-interactive signature scheme, which will contain a key generation algorithm, signing algorithm, and verification algorithm.

Ring signatures are an advanced cryptographic primitive that permit any individual member of an ad-hoc group - the "ring" of users - to digitally sign a message on behalf of that group while remaining anonymous inside it. Formally introduced in [48], the protocol was conceptualized as a secure mechanism to leak a secret while eschewing a central group manager. Consequentially, this requires no central authority delegating private keys, no trusted setup, and no interactive coordination among the members. To generate a signature the signer collates the public keys of the other members, then leverages their private key to produce a zero-knowledge proof demonstrating that the signer is indeed a member of the specified group.

Linkable ring signatures, introduced in [43] though LSAG (Linkable Spontaneous Anonymous Group) signatures, extend this primitive by introducing a mechanism to detect duplicate uses of the same signing key. While unconditional anonymity is desirable in some contexts, enabling a single user to sign repeatedly in an indistinguishable way could be used to falsely create the illusion of consensus, or spend a digital asset twice. Linkable ring signatures resolve this by generating a deterministic linking tag (often called a "key image" in the field of cryptocurrencies) along with the signature. This tag– derived from the signer's private key– ensures that if two signatures are generated using the same key, they will produce identical linking tags, thereby exposing to any third party this repeat use.

The introduction of linkability greatly expands the applicability of ring signatures in decentralized protocols. Most notably, they are a critical construction to prevent double-spend attacks in cryptocurrencies, wherein a user attempts to spend the same coin twice analogously to spending two bills with identical serial numbers. In the Monero blockchain, linkable ring signatures are famously deployed as a core protocol, evolving through frameworks like MLSAG (Multilayered Linkable Spontaneous Anonymous Group) signatures and the highly optimized CLSAG (Compact Linkable Spontaneous Anonymous Group) signatures [46] constructions that obfuscate transaction histories while preventing double-spend. Beyond decentralized finance, linkable ring signatures have become indispensable for designing secure e-voting systems, as they ensure voter anonymity and ballot authenticity while preventing voters from casting duplicate ballots.

3 MinRank

The MinRank Problem is of particular interest in post-quantum cryptography because its presumed hardness against both classical and quantum adversaries has enabled the construction of efficient cryptographic primitives, including identification schemes, signature schemes, and public-key encryption systems. However, the MinRank problem admits a wide range of algebraic, combinatorial, and hybrid attacks. For certain parameter choices these algorithms can solve problem instances efficiently, making careful security analysis and parameter selection essential.

3.1 The MinRank Problem

Problem 1 (MinRank). Given $M_1, \ldots, M_k \in \mathbb{F}_q^{m \times n}$ and target rank $r \in \mathbb{N}$, find $a \in \mathbb{F}_q^k$ such that

$$\operatorname{rank}\left(\sum_{i=1}^{k} a_i M_i\right) \leq r.$$

Formally, we refer to this problem as $\mathrm{MinRank}(q, m, n, k, r)$, though we suppress the variables when they are clear. We also consider the decisional variant of the problem.

Problem 2 (Decisional MinRank). Let $E \in \mathbb{F}_q^{m \times n}$ of rank r and $a \in \mathbb{F}_q^k$ be selected uniformly at random. Given MinRank matrices $M_1, \ldots, M_k \in \mathbb{F}_q^{m \times n}$ and $D \in \mathbb{F}_q^{m \times n}$, distinguish if D was constructed as $D = E - \sum_{i=1}^{k} a_i M_i$, or sampled uniformly at random.

Denote the advantage of an adversary $\mathcal{A}$ in distinguishing $\mathrm{DMinRank}(q, m, n, k, r)$ from $1/2$ as $\mathrm{Adv}_{\mathcal{A}}^{DMR}(\lambda)$. We assume that $\mathrm{Adv}_{\mathcal{A}}^{DMR}(\lambda)$ is negligible, meaning that no computationally bounded adversary can successfully distinguish except by chance.

MinRank Algorithms The complexity of solving an instance of MinRank is determined by the MinRank algorithm and the choice of polynomial solvers. The following is a non-exhaustive list describing well-known techniques.

The most straight forward technique is brute force, in which one guesses coefficients $a_1, \ldots, a_k \in \mathbb{F}_q$, computes rank $\left(\sum_{i=1}^{k} a_i M_i\right)$, then determines if this value is less than or equal to r. This process is repeated until a valid solution is obtained. The complexity of this method is $q^k n^\omega$, where $2 \leq \omega \leq 3$ is the cost of matrix multiplication.

Combinatorial methods, such as Kernel Search, [38], were introduced to speed up exhaustive search. This method requires a user to guess $\lceil \frac{k}{m} \rceil$ kernel vectors v_i and solve

$$\sum_{j=1}^{k} a_j M_j v_i = 0$$

linearly for the unknown a_i values. Simultaneously guessing two kernel vectors of a rank r matrix takes on average approximately $q^{\lceil \frac{k}{m} \rceil r}$. Thus, this technique has complexity

$$\mathcal{O}\left(q^{\lceil \frac{k}{m} \rceil r}\left(k^\omega + n^\omega\right)\right).$$

The Support Minors method of MinRank, introduced in [12], considers the decomposition of the rank r target matrix $M := \sum_{i=0}^{k} a_i M_i$ into the product of two matrices $S \in \mathbb{F}_q^{m \times r}$ and $C \in \mathbb{F}_q^{r \times n}$ such that $SC = M$. By construction, the rowspace of C is the rowspace of M, and thus appending a row of M, call it ρ_j, to C results in an $(r+1) \times n$ matrix of rank r. This guarantees that every maximal minor of the matrix $\begin{pmatrix} \rho_j \\ C \end{pmatrix}$ is zero. The support minors modeling computes the maximal minors of such a matrix and solves the system for the a_i variables that appear in the row vectors ρ_j. The complexity of solving the MinRank problem using Support Minors Modeling can be estimated as

$$\min_{m' \leq m} 3(k-1)(r+1)\binom{m'}{r}^2 \binom{k+b-2}{b}^2 \tag{1}$$

where b is the smallest integer such that

$$\binom{m'}{r}\binom{k+b-2}{b} - 1 \leq \sum_{i=1}^{b} (-1)^{i+1} \binom{m'}{r+i}\binom{n+i-1}{i}\binom{k+b-i}{b-i}. \tag{2}$$

As indicated in Equation (1) above, the number of columns used can be optimized to lower the complexity of the attack. It is often the case that a larger value of b along with a smaller m' may result in a more efficient attack.

Other commonly considered MinRank algorithms include Big-K [28], Minors [31], and Kipnis and Shamir [42]. Different algorithms may be more efficient than others depending on the parameter regime. The complexity of solving an instance of MinRank can be assessed using CryptographicEstimators[1] [30], which provides complexity estimates for commonly used classical attacks.

[1] `https://github.com/Crypto-TII/CryptographicEstimators`

3.2 Known MinRank Signature Schemes

The Courtois MinRank identification scheme [29] is a zero-knowledge proof that enables a prover to demonstrate knowledge of a solution $a \in \mathbb{F}_q^k$ to the MinRank problem, Problem 1. This 3-pass protocol achieves a soundness error of $\frac{2}{3}$, and shares structural similarities to the code-based Stern identification scheme [52,51]. During execution, the prover commits to a random masking vector $b \in \mathbb{F}_q^k$, then, depending on the verifier's challenge, demonstrates knowledge of one of three branches: (i) a linear combination of the MinRank matrices $\{M_i\}_{i=1}^k$ formed from the random mask b, (ii) a shifted linear combination formed from $a + b$, or (iii) proof that their difference leads to a rank-r matrix. Standard witness extraction arguments certify that if a prover can consistently answer all three challenge branches, they must possess a valid witness a which yields a rank-r matrix, hence they know a solution to the MinRank problem. We recall the full protocol in Algorithm 2.

Courtois MinRank Zero-Knowledge Proof		
Public: $q, m, n, k, r \in \mathbb{N}$, $M_1, \ldots, M_k \in \mathbb{F}_q^{m \times n}$ **Private:** $a \in \mathbb{F}_q^k$ such that $E = \sum_{i=1}^{k} a_i M_i$ is rank r		
PROVER		**VERIFIER**
Sample $b \xleftarrow{\$} \mathbb{F}_q^k$, $X \xleftarrow{\$} \mathbb{F}_q^{m \times n}$, $(S, T) \xleftarrow{\$} (\mathrm{GL}_m, \mathrm{GL}_n)$ Set $N_1 = \sum_{i=1}^{k} b_i M_i$, $N_2 = N_1 + E$, $Z_i = S N_i T + X$ for $i = 1, 2$ Pick $(r_0, r_1, r_2) \xleftarrow{\$} (\{0,1\}^\lambda)^3$ Set $c_0 = \mathsf{com}(r_0, S, T, X)$ Set $c_i = \mathsf{com}(r_i, Z_i)$ for $i = 1, 2$	$\xrightarrow{(c_0, c_1, c_2)}$	
	$\xleftarrow{b}$	Pick $b \xleftarrow{\$} \{0, 1, 2\}$
If $b = 0$, set $\mathtt{resp} = \{r_1, r_2, Z_1, Z_2\}$ If $b = 1$, set $\mathtt{resp} = \{r_0, r_1, S, T, X, b\}$ If $b = 2$, set $\mathtt{resp} = \{r_0, r_2, S, T, X, a + b\}$	$\xrightarrow{\mathtt{resp}}$	
		If $b = 0$, accept if: $c_i \stackrel{?}{=} \mathsf{com}(r_i, Z_i)$ for $i = 1, 2$ and $\mathrm{rank}(Z_2 - Z_1) \stackrel{?}{=} r$. If $b = 1, 2$, recompute Z_b from $\mathtt{resp}$. Accept if: S, T are invertible, $c_0 \stackrel{?}{=} \mathsf{com}(r_0, S, T, X)$, and $c_b \stackrel{?}{=} \mathsf{com}(r_b, Z_b)$.

Algorithm 2: The zero-knowledge proof for MinRank introduced in [29].

Subsequently, a variant of 2 was introduced in [49] which reduces the soundness to $\frac{1}{2}$. Although this modification was proposed with the goal of minimizing signature sizes, later analysis has determined that the communication complexity of the two schemes are actually equivalent [17].

More recently, MR-DSS was introduced in [17], which achieves a soundness error of $\frac{1}{2}$ by leveraging the *Sigma protocol with helper* framework of [19]. By applying the *cut-and-choose* technique of [41] to eliminate the simulated helper from the final protocol transcript, MR-DSS attains more compact signature sizes. Building on this framework, the authors also propose a MinRank-based ring signature scheme, MRr-DSS. While [29] briefly observed that such a construction should be generically possible from the base protocol, no concrete instantiation or security analysis was provided; consequently, MRr-DSS appears to constitute the first explicit and rigorously analyzed MinRank ring signature scheme. Despite these advancements, the design of a *linkable* ring signature relying on the hardness of MinRank remains an open problem.

4 Miraidon: A MinRank Identification Scheme

We now present the Miraidon identification scheme in Algorithm 3. Structurally reminiscent to the code-based CVE scheme [24], Miraidon achieves a soundness error that approaches $\frac{1}{2}$ asymptotically as the field size q increases. Crucially, our construction yields significantly reduced signature and public key sizes compared to MR-DSS. Building upon this, we adapt the protocol into a signature scheme Miraidon-S, design a ring signature scheme Miraidon-RS, then instantiate the first MinRank-based linkable ring signature scheme Miraidon-LRS. A proof-of-concept Python implementation of Miraidon is publicly available on GitHub[2].

The zero-knowledge property of Miraidon critically relies on the observation that for uniformly sampled invertible S and T, the obfuscated $Q = SET$ is indistinguishable from a random matrix of rank r [29], thereby hiding the secret low-rank linear combination E. To establish soundness, we show that if a prover can successfully answer both second challenges for the same initial transcript, a valid witness to the MinRank problem can be extracted. Namely, assuming hash collisions are intractable, the prover demonstrates knowledge of S, T, X, Q such that

$$\sum_{i=1}^{k} v_i S M_i T = X + \xi Q,$$

where $\text{rank}\,(Q) = r$ by construction. After expressing the coefficient of v as an affine function of the challenge ξ, that is $v = u + \xi a$, by evaluating this as a polynomial we obtain

$$\begin{aligned} X + \xi Q &= \sum_{i=1}^{k} (u_i + \xi a_i) S M_i T \\ &= \sum_{i=1}^{k} u_i (S M_i T) + \xi \sum_{i=1}^{k} a_i (S M_i T). \end{aligned}$$

Equating coefficients, it must be that $Q = S\left(\sum_{i=1}^{k} a_i M_i\right) T$. Since Q was constrained to have rank r, and by the invertibility of S and T, it follows that $\text{rank}\left(\sum_{i=1}^{k} a_i M_i\right) = r$. therefore, the vector a constitutes a valid witness for the MinRank problem.

[2] `https://github.com/FreemanSlaughter/Miraidon`

The Miraidon Zero-Knowledge Proof		
Public: $q, m, n, k, r \in \mathbb{N}$, $M_1, \ldots, M_k \in \mathbb{F}_q^{m \times n}$ **Private:** $a \in \mathbb{F}_q^k$ such that $E = \sum_{i=1}^{k} a_i M_i$ is rank r		
PROVER		**VERIFIER**
Pick $\texttt{seed}_{ST} \xleftarrow{\$} \{0,1\}^{2\lambda}$		
Expand $\texttt{seed}_{ST} \to (S, T) \in (\mathrm{GL}_m, \mathrm{GL}_n)$		
Select random $u \xleftarrow{\$} \mathbb{F}_q^k$		
Set $X = \sum_{i=1}^{k} u_i (S M_i T)$		
Set $Q = SET$		
Solve $Q = LR$ for $L \in \mathbb{F}_q^{m \times r}$, $R \in \mathbb{F}_q^{r \times n}$		
Set $c_0 = \mathsf{com}(X, Q)$, $c_1 = \mathsf{com}(S, T)$	$\xrightarrow{(c_0, c_1)}$	
	$\xleftarrow{\xi}$	Sample $\xi \xleftarrow{\$} \mathbb{F}_q^\star$
Define $v = u + \xi a$		
Set $y = \mathsf{com}\left(\sum_{i=1}^{k} v_i (S M_i T)\right)$	$\xrightarrow{y}$	
	$\xleftarrow{b}$	Pick $b \xleftarrow{\$} \{0, 1\}$
If $b = 0$, set $\texttt{resp} = \{X, L, R\}$		
Else, set $\texttt{resp} = \{\texttt{seed}_{ST}, v\}$	$\xrightarrow{\texttt{resp}}$	
		If $b = 0$, set $Q = LR$ Accept if c_0 is valid and $y \stackrel{?}{=} \mathsf{com}(X + \xi Q)$ Else, expand $(S, T) \leftarrow \texttt{seed}_{ST}$ Accept if c_1 is valid and $y \stackrel{?}{=} \mathsf{com}\left(\sum_{i=1}^{k} v_i (S M_i T)\right)$

Algorithm 3: The Miraidon zero-knowledge proof for MinRank.

Theorem 1. *Algorithm 3 is complete.*

Proof. Suppose that the prover is honest. For $b = 0$, Q will indeed be rank at most r, so the commitments c_0 and y will match. Then in the case $b = 1$, the commitments c_1 and y will match, passing the verifier's checks. □

Theorem 2. *Algorithm 3 is sound.*

Proof. As Algorithm 3 is a $(q-1, 2)$-identification scheme, it is $(2, 2)$-out-of-$(q-1, 2)$ special sound, hence has a soundness error of $\frac{q}{2(q-1)}$. □

Theorem 3. *Algorithm 3 is zero-knowledge.*

Proof. We demonstrate this by creating a simulator algorithm $\mathcal{S}$ which behaves indistinguishably from a genuine interaction, but appears to pass always despite having no knowledge of a solution.

Suppose this simulator anticipates the challenge $b = 0$. In this case, they prepare $Q = LR$ as a random rank r, with no regard to if it is a linear combination of the M_i's, and sample a random X.

Commitment c_0 is formed honestly, but c_1 is set as a random string. When the verifier communicates ξ, then $\mathcal{S}$ sets $Y = \mathsf{com}\,(X + \xi Q)$. In this manner, they will be able to pass in the $b = 0$ branch.

On the other hand, suppose that the algorithm expects $b = 1$. Then $\mathcal{S}$ selects S, T, v randomly, then computes $Y = \mathsf{com}\left(\sum_{i=1}^{k} v_i S M_i T\right)$, which is genuinely a linear combination of the M_i's, but will not be rank r. They form c_1 honestly, but set c_0 to be a random string. As c_1 is formed per the protocol, this will result in them being able to pass the verifier's $b = 1$ challenge every time.

With these strategies, if the simulator knows which b challenge they will receive, they can appear to pass the verifier's challenges without knowing a MinRank solution - a matrix which is both a linear combination of the M_i's and low rank - while remaining indistinguishable from a genuine interaction. □

4.1 Optimizations

We now proceed with optimizations to the underlying MinRank zero-knowledge proof of Algorithm 3 after the application of the Fiat-Shamir paradigm. We consider seeds to be size λ and commitments to be size 2λ, and include a salt of length 2λ in the commitments to prevent collision attacks.

Fixed-Weight Challenges This optimization is most beneficial when the second-challenge responses have drastically different response sizes [36,53,20,21,27,13], which is the case with Miraidon. Consider the vector of second challenges, $b = (b^{(1)}, \ldots, b^{(t)})$, and let this vector have weight w, meaning there are w rounds where the verifier asks for $b^{(i)} = 1$, but $t - w$ rounds with $b^{(i)} = 0$. Since in the $b^{(i)} = 0$ branch the prover sends $(mn+(m+n)r)\log_2(q)$ bits, while in the $b^{(i)} = 1$ branch they send $2\lambda + k\log_2(q)$ bits, the weight w will be selected to reduce the communication cost. We choose w to be close to t, to reduce the communication to mostly a fixed-length seed and a length-k vector. This optimization maintains soundness, as was proven in [15].

Delaying Second Response Instead of communicating $y^{(i)}$ in each round i, the prover can send $Y = \mathsf{com}\left(y^{(1)}, \ldots, y^{(t)}\right)$, then the verifier can recompute Y after all t rounds.

Commitment Tree Since the verifier will always recompute one of the two commitments in each round, but the challenges are biased to often return $b^{(i)} = 1$, they must compute the majority of the $c_1^{(i)}$ commitments. Thus, the prover can instead commit to the digest $c_1 = \mathsf{com}\left(c_1^{(1)}, \ldots, c_1^{(t)}\right)$, reducing the cost of these t commitments down to a single one.

Place the initial commitments for each round $(c_0^{(i)}, c_1^{(i)})$ into tree structures. Define their commitment $c_1 = \mathsf{com}\left(c_1^{(1)}, \ldots, c_1^{(t)}\right)$, then let $I \subseteq [t]$ be the support of $(b^{(1)}, \ldots, b^{(t)})$. The verifier will be sent $c_1^{(i)}$ when $i \in I$, so communication can be reduced by only sending the commitment when necessary. In the case that $i \notin I$, the prover can include $c_1^{(i)}$ as part of the second response. Thus, the overall cost for the $b^{(i)} = 1$ branches together is

$$\underbrace{2\lambda}_{c_1} + \underbrace{2\lambda(t-w)}_{c_1^{(i)},\, i \notin I} = 2\lambda(1 + t - w).$$

For the $c_0^{(i)}$ commitments, we prepare a Merkle tree with c_0 as the root and $(c_0^{(1)}, \ldots, c_0^{(t)})$ as the leaves. The verifier can recompute $c_0^{(i)}$ with $i \notin I$ for themselves, so will ask for the Merkle proof

for these indices to ensure that the prover did indeed commit to them honestly. As there are $t-w$ rounds with $b^{(i)}=0$, sending these proofs requires $(t-w)\log_2(t)$ hash digests: $\log_2(t)$ digests for each of the $t-w$ leaves needing a proof. However, we can leverage the existence of common paths to reduce this to $(t-w)\log_2\left(\frac{t}{t-w}\right)$. So the total cost for the $b^{(i)}=0$ branches does not exceed

$$\underbrace{2\lambda}_{c_0} + \underbrace{2\lambda(t-w)\log_2\left(\frac{t}{t-w}\right)}_{\text{proof of } c_0^{(i)},\, i\notin I} = 2\lambda\left(1+(t-w)\log_2\left(\frac{t}{t-w}\right)\right).$$

Seed Tree In the precomputation stage of Algorithm 3, the prover samples $\mathtt{seed}_{LR}^{(i)}$ for rounds $i\in[t]$. We generate these seeds together, using a tree structure $\mathtt{Tree}$, with $(\mathtt{MSeed},\mathtt{Salt})$ as the root, where $\mathtt{MSeed}\xleftarrow{\$}\{0,1\}^\lambda$ is the master seed and $\mathtt{Salt}\xleftarrow{\$}\{0,1\}^{2\lambda}$ is a length 2λ random salt, per [25]. In this manner, the prover only needs communicate w seeds, one for each entry in the support of b, which can be compressed by instead sending all but $t-w$ seeds. So at most, the number of nodes that need to be shared is $(t-w)\log_2\left(\frac{t}{t-w}\right)$, thus sending all the seeds requires a total cost of

$$\lambda(t-w)\log_2\left(\frac{t}{t-w}\right).$$

Further Tree Improvements By [22], it is possible to compress tree structures even further. Both the seed and commitment trees together can be expressed in bits as

$$3\lambda\left\lfloor(t-w)\log_2\left(\frac{t}{t-w}\right)+\mathrm{wt}(t\text{ written in binary})-1\right\rfloor,$$

where we write out t as a binary string, then compute the number of non-zero entries in that string.

5 Miraidon-S: A MinRank Signature Scheme

Let $\mathtt{FS}_1$ be a Fiat-Shamir hash function with range $(\mathbb{F}_q^\star)^t$, and $\mathtt{FS}_2$ a second Fiat-Shamir hash function which outputs a length-t binary string with weight w. We then transform Miraidon into a signature scheme using these Fiat-Shamir hash functions, as illustrated in Algorithms 4 - 6.

5.1 Security Against Forgery Attacks

We first present two forgery attack methods in which a dishonest prover attempts to pass the verifier's check fraudulently. Both forgery attacks may be found in [14] and are derived from [40]; the first is specified for weighted challenges, while the second applies to general $(q-1,2)$-identification schemes.

In the first forgery, the dishonest prover attempts to guess either challenge in each round. If they are successful and they have guessed correctly in all rounds, then they fraudulently pass, so intuitively the probability of passing is the reciprocal of the probability that both challenges were correctly guessed, over all rounds.

Miraidon Signing Algorithm

Public: $q, m, n, k, r \in \mathbb{N}$, $M_1, \ldots, M_k \in \mathbb{F}_q^{m \times n}$, $\mathtt{msg}$

Private: $a \in \mathbb{F}_q^k$ such that $E = \sum_{i=1}^{k} a_i M_i$ is rank r

Sample $\mathtt{MSeed} \xleftarrow{\$} \{0,1\}^\lambda$, $\mathtt{Salt} \xleftarrow{\$} \{0,1\}^{2\lambda}$

$(\mathtt{seed}^{(1)}, \ldots, \mathtt{seed}^{(t)}) = \mathtt{SeedTree}(\mathtt{MSeed}, \mathtt{Salt})$

For $i \in [t]$:

- Sample $(u^{(i)}, S^{(i)}, T^{(i)}) \leftarrow \mathtt{seed}^{(i)}$
- Set $Q^{(i)} = S^{(i)} E T^{(i)}$
- Solve $Q^{(i)} = L^{(i)} R^{(i)}$ for $L^{(i)}, R^{(i)}$
- Set $X^{(i)} = \sum_{j=1}^{k} u_j^{(i)} (S^{(i)} M_j T^{(i)})$
- Set $c_0^{(i)} = \mathsf{com}\left(X^{(i)}, Q^{(i)}, \mathtt{Salt}, i\right)$
- Set $c_1^{(i)} = \mathsf{com}\left(S^{(i)}, T^{(i)}, \mathtt{Salt}, i\right)$

Create $\mathcal{T} = \mathtt{MerkleTree}(c_0^{(1)}, \ldots, c_0^{(t)})$

Set $c_0 = \mathtt{Root}_{\mathcal{T}}$, $c_1 = \mathsf{com}\left(c_1^{(1)}, \ldots, c_1^{(t)}\right)$

Gen $(\xi^{(1)}, \ldots, \xi^{(t)}) \leftarrow \mathtt{FS}_1(c_0, c_1, \mathtt{msg}, \mathtt{Salt})$

For $i \in [t]$:

- Set $v^{(i)} = u^{(i)} + \xi^{(i)} a$
- $y^{(i)} = \mathsf{com}\left(\sum_{j=1}^{k} v_j^{(i)} S^{(i)} M_j T^{(i)}\right)$

Set $Y = \mathsf{com}\left(y^{(1)}, \ldots, y^{(t)}\right)$

$\boldsymbol{b} \leftarrow \mathtt{FS}_2(c_0, c_1, \mathtt{msg}, \mathtt{Salt}, \{\xi^{(i)}\}_{i \in [t]}, Y)$

Set $I = \mathrm{supp}(\boldsymbol{b})$ for $b = (b^{(1)}, \ldots, b^{(t)})$

$\mathtt{Path} = \mathtt{SeedPath}(\mathtt{MSeed}, \mathtt{Salt}, I)$

For $i \notin I$:

- Set $\mathtt{resp}^{(i)} = (c_1^{(i)}, X^{(i)}, L^{(i)}, R^{(i)})$

For $i \in I$:

- Set $\mathtt{resp}^{(i)} = (v^{(i)})$

Compute $\mathtt{Proof} = \mathtt{MerkleProof}_{\mathcal{T}}(I^c)$

$\sigma = \{c_0, c_1, \mathtt{Salt}, Y, \mathtt{Path}, \mathtt{Proof}, \{\mathtt{resp}^{(i)}\}_{i \in [t]}\}$

Output signature σ

Algorithm 4: The Miraidon signature generation protocol.

Miraidon Key Generation Algorithm

Input: $\lambda \in \mathbb{N}$, $\mathtt{PRNG}$

Sample $(\mathtt{seed}_{pk}, \mathtt{seed}_{sk}) \xleftarrow{\$} (\{0,1\}^\lambda)^2$

Generate $(M_k^R \in \mathbb{F}_q^{m \times r}$,

$M_1, \ldots, M_{k-1} \in \mathbb{F}_q^{m \times n}) \xleftarrow{\$} \mathtt{PRNG}(\mathtt{seed}_{pk})$

Generate $K \in \mathbb{F}_q^{r \times (n-r)} \xleftarrow{\$} \mathtt{PRNG}(\mathtt{seed}_{sk})$

For $j \in [k]$, let $a \in \mathbb{F}_q^k$ be unique solution to

$$\mathrm{vec}(M_k^R K)_j = a_k^{-1} \left(\sum_{i=1}^{k-1} a_i (\delta_{i,j} - \mathrm{vec}(M_i^R K)_j) \right)$$

If no solution, return to top.

Compute $E^R = \sum_{i=1}^{k-1} a_i M_i^R + a_k M_k^R$

If rank $(E^R) \neq r$, return to top; else:

- Set $M_k^L = a_k^{-1} \left(E^R K - \sum_{i=1}^{k-1} a_i M_i^L \right)$

$\mathtt{PubKey} = (\mathtt{seed}_{pk}, \mathrm{vec}(M_k^L)_{k+1}, \ldots, \mathrm{vec}(M_k^L)_{m(n-r)})$

$\mathtt{PrivKey} = (\mathtt{seed}_{pk}, \mathtt{seed}_{sk})$

Algorithm 5: The Miraidon key generation procedure, from [50].

Miraidon Verification Algorithm

Public: $q, m, n, k, r \in \mathbb{N}$, $M_1, \ldots, M_k \in \mathbb{F}_q^{m \times n}$

Input: message $\mathtt{msg}$, signature σ

Generate $(\xi^{(1)}, \ldots, \xi^{(t)}) \leftarrow \mathtt{FS}_1(c_0, c_1, \mathtt{msg}, \mathtt{Salt})$

Generate $\boldsymbol{b} \leftarrow \mathtt{FS}_2(c_0, c_1, \mathtt{msg}, \mathtt{Salt}, \{\xi^{(i)}\}_{i=1}^{t}, Y)$

Set $I = \mathrm{supp}(b^{(1)}, \ldots, b^{(t)})$

Recompute $\{\mathtt{seed}^{(i)}\}_{i \in I} = \mathtt{FormTree}(\mathtt{Path}, \mathtt{Salt})$

For $i \notin I$:

- Set $Q^{(i)} = L^{(i)} R^{(i)}$
- Set $c_0^{(i)} = \mathsf{com}\left(X^{(i)}, Q^{(i)}, \mathtt{Salt}, i\right)$
- Set $y^{(i)} = \mathsf{com}\left(X^{(i)} + \xi^{(i)} Q^{(i)}\right)$

For $i \in I$:

- Sample $(S^{(i)}, T^{(i)}) \leftarrow \mathtt{seed}^{(i)}$
- Set $c_1^{(i)} = \mathsf{com}\left(S^{(i)}, T^{(i)}, \mathtt{Salt}, i\right)$
- Set $y^{(i)} = \mathsf{com}\left(\sum_{j=1}^{k} v_j^{(i)} S^{(i)} M_j T^{(i)}\right)$

Accept σ if:

- $c_0 = \mathsf{com}\left(c_0^{(1)}, \ldots, c_0^{(t)}\right)$
- $c_1 = \mathtt{VerifyTree}(\{c_1^{(i)}\}_{i \notin I}, \mathtt{Proof})$
- $Y = \mathsf{com}\left(y^{(1)}, \ldots, y^{(t)}\right)$

Else reject.

Algorithm 6: The Miraidon signature verification procedure.

Theorem 4 ([14], Proposition 1). *Consider a $(q-1,2)$-identification scheme with t rounds, w of which select the $b=1$ branch. An adversary can falsely convince the verifier if they can guess in advance either the first or second challenge (or both) correctly. Thus, selecting $0 \leq \alpha \leq t$ rounds, they can mount a forgery attack that on average runs in $O\left(\frac{1}{P(t,w,\alpha)}\right)$ time, where*

$$P(t,w,\alpha) = \sum_{j=\max(0,w+\alpha-t)}^{\min(w,\alpha)} \frac{\binom{\alpha}{j}\binom{t-\alpha}{w-j}}{\binom{t}{w}}(q-1)^{2j-\alpha-w},$$

after optimizing over α.

In [15], a stronger and more general forgery attack is presented. We describe the process below, detailed for Miraidon, along with the cost of the forgery.

1. Sample $\{\mathtt{seed}_{ST}^{(i)}\}_{i\in[t]}$, then guess first challenge vector $(\widetilde{\xi}^{(1)},\ldots,\widetilde{\xi}^{(t)})$ and weight $\alpha \geq w$ second challenge vector $(\widetilde{b}^{(1)},\ldots,\widetilde{b}^{(t)})$
2. For $i \in [t]$:
   (a) Sample $\mathtt{MSeed} \xleftarrow{\$} \{0,1\}^{\lambda}$ and $\mathtt{Salt} \xleftarrow{\$} \{0,1\}^{2\lambda}$; generate $\{\mathtt{seed}_{ST}^{(i)}\}_{i\in[t]}$ using PRNG
   (b) Reconstruct $S^{(i)} \in \mathrm{GL}_m$ and $T^{(i)} \in \mathrm{GL}_m$ from $\mathtt{seed}_{ST}^{(i)}$
   (c) Sample $v^{*(i)} \in \mathbb{F}_q^k$
   (d) Sample $L^{(i)} \in \mathbb{F}_q^{m\times r}$ and $R^{(i)} \in \mathbb{F}_q^{r\times n}$, then set $Q^{(i)} = L^{(i)}R^{(i)}$
   (e) Compute $X^{(i)} = \sum_{j=1}^{k} v_j^{*(i)}\left(S^{(i)}M_jT^{(i)}\right) - \widetilde{\xi}^{(i)}Q^{(i)}$
   (f) Set $c_0^{(i)} = \mathsf{com}\left(X^{(i)},L^{(i)},R^{(i)},\mathtt{Salt},i\right)$ and $c_1^{(i)} = \mathsf{com}\left(\mathtt{seed}_{ST}^{(i)},v^{*(i)},\mathtt{Salt},i\right)$
3. Compute c_0 as the root of the Merkle tree $\mathtt{MerkleTree}(c_0^{(1)},\ldots,c_0^{(t)})$ and $c_1 = \mathsf{com}\left(c_1^{(1)},\ldots,c_1^{(t)}\right)$, then generate $(\xi^{(1)},\ldots,\xi^{(t)}) \leftarrow \mathtt{FS}_1(c_0,c_1,\mathtt{msg},\mathtt{Salt})$
4. Let $S = \{i \in [t] \mid \widetilde{\xi}^{(i)} = \xi^{(i)}\}$; if $|S| \leq t^*$, restart from top
5. For $i \in S$, set $y^{(i)} = \mathsf{com}\left(\sum_{j=1}^{k} v_j^{*(i)}\left(S^{(i)}M_jT^{(i)}\right)\right)$; for $i \notin S$
   (a) If $\widetilde{b}^{(i)} = 0$: set $y^{(i)} = \mathsf{com}\left(X^{(i)} + \xi^{(i)}Q^{(i)}\right)$
   (b) If $\widetilde{b}^{(i)} = 1$: set $y^{(i)} = \mathsf{com}\left(\sum_{j=1}^{k} v_j^{*(i)}\left(S^{(i)}M_jT^{(i)}\right)\right)$
6. Set $Y = \mathsf{com}\left(y^{(1)},\ldots,y^{(t)}\right)$ then generate $(b^{(1)},\ldots,b^{(t)}) \leftarrow \mathtt{FS}_2(c_0,c_1,\mathtt{msg},\mathtt{Salt},\{\xi\}_{i\in[t]}Y)$
7. If $\widetilde{b}^{(i)} = b^{(i)}$ for all $i \notin S$, continue; else, return to Step 5
8. For each $i \in [t]$: if $b^{(i)} = 0$, set $\mathtt{resp}^{(i)} = \{X^{(i)},L^{(i)},R^{(i)}\}$; else, set $\mathtt{resp}^{(i)} = \{\mathtt{seed}_{ST}^{(i)},v^{*(i)}\}$.

Theorem 5 ([14], Proposition 2). *The forgery attack presented above runs in average time*

$$\min_{t^*\in\{0,\ldots,t\}}\left\{\frac{1}{P_1(t,t^*,q)} + \frac{1}{P_2(t,t^*,w,q)}\right\},$$

where

$$P_1(t,t^*,q) = \sum_{j=t^*}^{t}\binom{t}{j}\left(\frac{1}{q-1}\right)^j\left(1-\frac{1}{q-1}\right)^{t-j}$$

and

$$P_2(t,t^*,w,q) = \max_{\alpha\in\{w,\ldots,t\}} \sum_{j=t^*}^{t} \frac{\binom{t}{j}\left(\frac{1}{q-1}\right)^j\left(1-\frac{1}{q-1}\right)^{t-j}}{P_1(t,t^*,q)} \sum_{w^*=\max\{0,\alpha-j\}}^{\min\{t-j,\alpha\}} \frac{\binom{t-j}{w^*}\binom{j}{\alpha-w^*}\binom{j}{w-w^*}}{\binom{t}{\alpha}\binom{t}{w}}.$$

To ensure the forgery attack remain intractable, we compute the forgery attack cost for the parameters selected in Table 3, along with the optimal values of the number of rounds t, the fixed-weight w, and the forgery parameters t^* and α.

Level	q	m	n	k	r	t	w	t^*	α	Forgery Cost
I	127	10	10	43	4	180	121	36	129	128.29
III	257	12	12	45	6	317	248	47	264	192.05
V	509	13	13	50	7	512	435	56	457	256.14

Table 1: Parameters with regards to forgery attack.

5.2 Signature and Public Key Sizes

Signature Size: In total, we compute the signature size for a t rounds, w of which are in the $b^{(i)} = 1$ branch, to be:

$$|\sigma| = \underbrace{8\lambda}_{c_0,c_1,Y,\texttt{Salt}} + \underbrace{3\lambda\left\lfloor (t-w)\log_2\left(\frac{t}{t-w}\right) + \mathrm{wt}(t \text{ in binary}) - 1\right\rfloor}_{\texttt{SeedTree+MerkleProof}}$$
$$+ \underbrace{(t-w)\left(\underbrace{2\lambda}_{c_1^{(i)}} + \underbrace{(mn+(m+n)r)\cdot\log_2(q)}_{X^{(i)},\ L^{(i)},\ R^{(i)}}\right)}_{\texttt{resp}^{(i)} \text{ for } i\notin I} + \underbrace{w\left(\underbrace{k\cdot\log_2(q)}_{v^{(i)}}\right)}_{\texttt{resp}^{(i)} \text{ for } i\in I} \text{ bits.}$$

Public Key Size: For the public key, note that one can generate from a length-λ seed all the MinRank matrices except the last one $M_1,\ldots,M_{k-1} \in \mathbb{F}_q^{m\times n}$, then select randomly a $a \in \mathbb{F}_q^k$ and $E \in \mathbb{F}_q^{m\times n}$ of rank r. Defining $M_k = a_k^{-1}\left(E - \sum_{i=1}^{k-1} a_i M_i\right)$, this public key can be communicated in the cost of the seed plus the cost to communicate M_k, for a total of $\lambda + mn\log_2(q)$ bits [29]. In [17], it is shown that public keys can be compressed even further by reducing it via linear algebra, to $\lambda + (mn-k)\log_2(q)$ bits. In effect, they let $L \in \mathbb{F}_q^{k\times mn}$ be the matrix formed from stacking the vectorization of the M_i's, then row-reduce to obtain a $k\times k$ identity in L, thus only the remainder need be communicated.

This was improved upon by [50], which shows that if one splits $E \in \mathbb{F}_q^{m\times n}$ of rank r into left and right components, say $E = (E^{(L)} \mid E^{(R)})$ with $E^{(L)} \in \mathbb{F}_q^{m\times(n-r)}$ and $E^{(R)} \in \mathbb{F}_q^{m\times r}$, then with high probability E^R is rank r. Thus, there exists a unique $K \in \mathbb{F}_q^{r\times(n-r)}$ such that $E^{(L)} = E^{(R)}K$.

With this, one only needs to communicate the left part of M_k after the seed, for a total cost of $\lambda + m(n-r)\log_2(q)$ bits.

This can then be combined with the use of canonical forms to shrink the public key even more, specifically to $\lambda+(m(n-r)-k)\log_2(q)$ bits. The idea is to generate $M_1, \ldots, M_{k-1}$ according to this canonical form, so that the vectorization of $M_k^{(L)}$ starts with k zero entries, thus only the remainder need be sent. In this manner, when the MinRank matrices are packaged together into a matrix of vectorizations, the left portion form a $k \times k$ identity with a $1 \times k$ zero vector below. See Algorithm 5 for this procedure.

The public key can be recovered by regenerating $M_k^{(R)}$ and $M_1, \ldots, M_{k-1}$ from $\texttt{seed}_{pk}$, then forming $\text{vec}(M_k^L)$ by appending k zeros in front of the sent vector, $(\text{vec}(M_k^L)_{k+1}, \ldots, \text{vec}(M_k^L)_{m(n-r)})$. Thus, M_k is obtained. In this manner, the public key can be reduced to

$$|\texttt{Pubkey}| = \lambda + (m(n-r)-k) \cdot \log_2(q) \text{ bits.}$$

Private Key Size: The private key is simply $a \in \mathbb{F}_q^k$ such that $a_k \neq 0$. If using one of the less optimized public key algorithms above, this may be stored directly as $k \cdot \log_2(q)$, leading to sizes of 18, 25, and 34 B for the proposed parameter sets of Table 3. We prioritize the reduction of the public key, and thus select to use the optimizations of [50]. Therefore the private key is generated from two seeds, hence

$$|\texttt{Privkey}| = 2\lambda \text{ bits.}$$

This results in 32, 48, and 64 B private keys.

5.3 Miraidon Signature Parameters

We instantiate out scheme with parameter sets carefully selected to optimize efficiency while maintaining strict security margins against all known attacks. Table 2 summarizes the estimated time complexities for various attack methods for each parameter set, computed using CryptographicEstimators[3] [30]. For each, we determine some of the optimal algorithmic-specific parameters, such as the hybridization parameter [11], that minimize the adversary's effort. To ensure conservative security bounds, take the linear algebra exponent to be $\omega = 2$, estimating that the multiplication of two $n \times n$ matrices requires only $O(n^\omega)$ field operations. We subsequently benchmark our security estimated directly against the MR-DSS signature scheme and CROSS.

Table 3 reports the public key and signature sizes generated by each parameter set. Python scripts to reproduce these parameter derivations and signature size estimations are available in the Miraidon GitHub repository[4].

In Table 4, we benchmark the signature, public key, and private key sizes of Miraidon against select select post-quantum signature schemes, targeting NIST Security Level I. Specifically, we compare the Miraidon-S parameter set to MR-DSS and CROSS [10], a code-based signature scheme that advanced to Round 2 of the NIST standardization process for additional digital signatures. This comparative analysis demonstrates that Miraidon-S achieves a highly competitive profile, consistently yielding compact signatures and public keys. Indeed, Miraidon-S consistently reduces the signature sizes by approximately 25% compared to MR-DSS, with public keys half the size and private keys up to a third smaller. Compared to CROSS, the signature sizes are only marginally larger (6% larger minimally) but with public keys less than half the size.

[3] `https://github.com/Crypto-TII/CryptographicEstimators`
[4] `https://github.com/FreemanSlaughter/Miraidon`

	λ	q	m	n	k	r	SM(a,b,n')	KS(a)	BigK	BF(a)	M(a)
Miraidon	128	127	10	10	44	4	139(4,2,6)	149(4)	**136**	149(4)	-
	192	257	12	12	45	6	**200**(3,3,9)	204(3)	242	209(4)	-
	256	509	13	13	50	7	274(3,3,10)	**265**(3)	279	269(4)	-
MR-DSS [17]	128	16	16	16	143	4	166(8,2,8)	155(8)	219	162(9)	**150**(5)
	192	16	19	19	167	6	236(8,2,11)	227(8)	343	234(9)	**216**(9)
	256	16	22	22	254	6	301(11,1,11)	299(11)	416	307(12)	**278**(12)

Table 2: Estimated security of parameter sets, conservatively taking $\omega = 2$.
The considered attacks include Support Minors with n' columns and bi-degree b (SM(a,b,n')), Kernel Search (KS) [12], Big-k [28], Brute Force (BF), and Minors (M) [31].
We denote the hybridization parameter [11] as a.

Sec. Level	q	m	n	k	r	Signature (kB)	PubKey (B)
I	127	10	10	44	4	20.6	29.98
III	257	12	12	45	6	45.76	51.02
V	509	13	13	50	7	80.17	63.47

Table 3: Suggested parameters for NIST security I, III, and V.

Sec. Level	Work	Sig (kB)	PubKey (B)	PrivKey (B)
I	Miraidon	21	30	32
	MR-DSS	27	73	50
	CROSS	18	77	32
III	Miraidon	46	51	48
	MR-DSS	60	121	58
	CROSS	41	115	48
V	Miraidon	80	63	64
	MR-DSS	106	147	88
	CROSS	75	153	64

Table 4: A comparison of Miraidon against the MR-DSS [17] and CROSS [10] signature schemes.

6 A MinRank Ring Signature and Linkable Ring Signature

6.1 Miraidon-RS: A MinRank Ring Signature

We now present Miraidon-RS, our MinRank ring signature protocol. We refer to the appendix for the formal ring signature definitions and proofs. Following the construction from [17], we demonstrate that Algorithm 4 can be used to instantiate a ring signature. Let $\boldsymbol{M} = (M_1, \ldots, M_k) \in \mathbb{F}_q^{m \times n}$ be the public matrices in an instance of the MinRank problem, and consider a ring with ℓ users. For brevity, we introduce new notation to denote MinRank sums, namely $\langle a, \boldsymbol{M} \rangle = \sum_{i=1}^{k} a_i M_i$. To generate their public key, each ring member does the following: for $i \in [\ell]$

1. User $\mathcal{U}_i$ selects random private key $a^{(i)} \in \mathbb{F}_q^k$

2. Select a random rank-r matrix $E^{(i)} \in \mathbb{F}_q^{m \times n}$
3. Compute $R_i = E^{(i)} - \langle a^{(i)}, \boldsymbol{M} \rangle$; this $R_i \in \mathbb{F}_q^{m \times n}$ is the public key for user U_i. By Problem 2, this public key is indistinguishable from random.

To sign, the user with index π will follow Algorithm 4, with the following changes: (i) instead of using private input $a^{(\pi)} \in \mathbb{F}_q^k$, they will use $(a^{(\pi)} \,||\, e^{(\pi)}) \in \mathbb{F}_q^{k+\ell}$ where $e^{(\pi)}$ is the π-th standard basis vector, and (ii) instead of using the MinRank matrices $\boldsymbol{M} = (M_1, \ldots, M_k)$, they will use $\mathcal{M} = (M_1, \ldots, M_k \,||\, R_1, \ldots, R_\ell)$. With these changes, the signing procedure results in a valid signature that demonstrates ring membership, which can be authenticated using the verification procedure in Algorithm 6. We present the underlying ZKP for this ring signature scheme in Algorithm 7; the ring signature itself will be formed by applying the Fiat-Shamir transform to this ZKP in parallel until the soundness error is below some specified tolerance. We suppress the signer's subscript π for readability.

Miraidon Ring Signature Zero-Knowledge Proof		
Public: $q, m, n, k, r \in \mathbb{N}$, $\mathcal{M} = (\boldsymbol{M} \,||\, \boldsymbol{R}) \in \mathbb{F}_q^{m \times (k+\ell)n}$ **Private:** $a \in \mathbb{F}_q^k$ and standard basis vector $e \in \mathbb{F}_q^\ell$ s.t. $E = \langle a, \boldsymbol{M} \rangle + \langle e, \boldsymbol{R} \rangle$ is rank r		
PROVER		**VERIFIER**
Pick $\texttt{seed}_{ST} \xleftarrow{\$} \{0,1\}^{2\lambda}$		
Form $\texttt{seed}_{ST} \to (S, T) \in (\mathrm{GL}_m, \mathrm{GL}_n)$		
Select random $u \xleftarrow{\$} \mathbb{F}_q^{k+\ell}$		
Set $X = \langle u, S\mathcal{M}T \rangle$ and $Q = SET$		
Solve $Q = LR$ for $L \in \mathbb{F}_q^{m \times r}$, $R \in \mathbb{F}_q^{r \times n}$		
Set $c_0 = \mathsf{com}(X, Q)$, $c_1 = \mathsf{com}(S, T)$	$\xrightarrow{(c_0, c_1)}$	
	$\xleftarrow{\xi}$	Sample $\xi \xleftarrow{\$} \mathbb{F}_q^*$
Define $v = u + \xi(a \,||\, e) \in \mathbb{F}_q^{k+\ell}$		
Set $y = \mathsf{com}(\langle v, S\mathcal{M}T \rangle)$	$\xrightarrow{y}$	
	$\xleftarrow{b}$	Pick $b \xleftarrow{\$} \{0,1\}$
If $b = 0$, set $\texttt{resp} = \{X, L, R\}$		
Else, set $\texttt{resp} = \{\texttt{seed}_{ST}, v\}$	$\xrightarrow{\texttt{resp}}$	
		If $b = 0$, set $Q = LR$
		Accept if c_0 is valid and $y \stackrel{?}{=} \mathsf{com}(X + \xi Q)$
		Else, expand $(S, T) \leftarrow \texttt{seed}_{ST}$
		Accept if c_1 is valid and $y \stackrel{?}{=} \mathsf{com}(\langle v, S\mathcal{M}T \rangle)$

Algorithm 7: The Miraidon ring signature zero-knowledge proof.

6.2 Miraidon-RS Parameters

Transitioning from the signature to ring signature setting results in only a marginal penalty to the communication overhead. Specifically, the cost to send the response vector v now requires $(k + \ell)\log_2(q)$ bits. For small ring sizes ℓ, this increase has a negligible impact on the total signature size, however appending the ring members' public keys expands the MinRank matrices from $(M_1, \ldots, M_k)$ to $(M_1, \ldots, M_k \,||\, R_1, \ldots, R_\ell)$. This expanded system increases the degrees of freedom,

directly improving the success probability of the Big-k attack algorithm. Consequently, this more effective attack avenue must be bounded in the security analysis.

Table 5 details the proposed parameter sets for Miraidon-RS, targeting NIST Security Level I for various ring sizes ℓ. We derive these sets by evaluating the time complexities of the algorithms listed in Table 6 against the expanded system of $k+\ell$ MinRank matrices. To ensure that the forgery cost remains intractable, we fix parameters $t = 180$ and $w = 121$ across all instances, resulting in $t^* = 36$ and $a = 129$.

When evaluating the security of the ring signature, we account for two primary strategies. In the first, the attacker targets a specific ring member $i \in [\ell]$ and attempts to solve the MinRank instance defined by $(M_1, \ldots, M_k \,||\, R_i)$. In the second, the attacker targets a subset of i members, and attempts to find i solutions for the combined instance $(M_1, \ldots, M_k \,||\, R_1, \ldots, R_i)$. We proactively mitigate both attack methods by requiring that all intermediate instances from parameters $(q, m, m, k+1, r)$ up to $(q, m, m, k+\ell, r)$ independently satisfy the necessary security threshold. The final claimed security is conservatively taken as the minimum of all instances.

$\log_2(\ell)$	q	m	n	$k+\ell$	r	Bit Sec.	Sig (kB)
2	127	10	10	$41+4$	4	133	20.71
3	127	11	11	$37+8$	5	133	23.33
4	127	12	12	$45+16$	5	132	26.73
5	127	13	13	$41+32$	6	131	31.14
6	127	16	16	$54+64$	7	138	43.88

Table 5: Parameters for the Miraidon ring signature scheme with ℓ members.

In the ring signature setting, Miraidon-RS achieves smaller signature sizes compared to MRr-DSS [17], the state-of-the-art construction relying on the MinRank problem, as can be seen in Table 6. Furthermore, its profile remains highly competitive even when benchmarked against post-quantum alternatives, including advanced lattice-based ring signatures. We note that Miraidon-RS is most effectively utilized with small-to-medium anonymity sets, e.g. with $\ell \leq 2^5$. As ℓ increases exponentially, the concatenation of MinRank matrices with public keys substantially enhances the capabilities of the Big-k attack algorithm; mitigating this necessitates an aggressive increase in matrix dimensions, which diminishes the scheme's baseline efficiency, hence Miraidon-RS is preferentially deployed in the $\ell \leq 2^5$ regime.

ℓ	2^2	2^3	2^4	2^5	2^6	Assumption	Sec.
Miraidon-RS	21	23	27	31	44	MinRank	128
MRr-DSS [17]	$27^\star$	27	27	32	36	MinRank	128
Falafl [21]	$30^\star$	30	$31^\star$	$32^\star$	32	MSIS/MLWE	128
Raptor [45]	5	10	20	40	80	SIS	100

Table 6: A comparison of ring signatures in kB. We denote estimated parameter sizes with a *.

6.3 Miraidon-LRS: A MinRank Linkable Ring Signature

we now introduce Miraidon-LRS, a novel linkable ring signature relying on the hardness of the MinRank problem. In standard linkable ring signature constructions, each signature is accompanied by a deterministically-derived linking tag, formed directly from the signing key. If this key is reused across signatures, there exists a public PPR algorithm to detect this reuse - generally, this is achieved by simple inspection. To formalize both membership and linkability into our Miraidon framework, we introduce the following computational problem:

Problem 3 (Compressed MinRank). Given $M_1, \ldots, M_k, N_1, \ldots, N_k \in \mathbb{F}_q^{m \times n}$ and target ranks $r_1, r_2 \in \mathbb{N}$, find $a \in \mathbb{F}_q^k$ such that

$$\text{rank}\left(\sum_{i=1}^{k} a_i M_i\right) \leq r_1 \text{ and } \text{rank}\left(\sum_{i=1}^{k} a_i N_i\right) \leq r_2.$$

We refer to this problem as $\text{CMinRank}(q, m, n, k, r_1, r_2)$.

It is straightforward to see that the Compressed MinRank Problem is at least as hard as the standard MinRank problem. Any PPT algorithm capable of solving Problem 3 can trivially take $N_i = 0$ for all $i \in [k]$, thus solving Problem 1 as well.

In our framework, the first MinRank instance establishes membership, identical to the standard ring signature setting, while the second enforces linkability. To create the linking tag, the signer selects a matrix $\widetilde{E} \in \mathbb{F}_q^{m \times n}$ of rank r_2 and defines the tag to be $\mathtt{tag} = \widetilde{E} - \langle a, \boldsymbol{M} \rangle \in \mathbb{F}_q^{m \times n}$, where $a \in \mathbb{F}_q^k$ is the signer's witness to the membership instance. An honest signer with knowledge of a can trivially compute a valid $\widetilde{E}$ to satisfy linkability; an adversary attempting to forge a link to an existing ring without knowledge of a is forced to solve an instance of the MinRank problem. Furthermore, by how `tag` was generated, it will appear undistinguishable from a random matrix.

Overall, the core zero-knowledge proof requires a prover to demonstrate knowledge of a witness pair $a \in \mathbb{F}_q^k$ and $e \in \mathbb{F}_q^\ell$ such that the membership combination $E = \langle a, \boldsymbol{M} \rangle + \langle e, \boldsymbol{R} \rangle$ is rank r_1 and the linkability combination $\widetilde{E} = \mathtt{tag} + \langle a, \boldsymbol{M} \rangle$ is rank r_2.

In canonical cryptocurrency applications such as Monero, preventing double-spend necessarily requires that the linking tags are deterministic computations of the signing key, with no randomness involved at all. Our proposed construction deviates slightly however, in that the linking tag depends on the signer's choice of the rank-r_2 matrix $\widetilde{E}$. Consequently, Miraidon-LRS achieves linkability under the assumption of honest tag generation; this paradigm has been termed "user-controlled linkability" in the literature [35], though has also been characterized as "opt-in linkability" in conference presentations and code-based linkable ring signatures by the second author. Throughout this work, we proceed under the premise that a prover who intends to produce linkable signatures executes the protocol faithfully, producing consistent tags.

We now formalize the operational algorithms for Miraidon-LRS: signature generation is detailed in Algorithm 8 and verification in Algorithm 9. We highlight that the fundamental ring signature, Miraidon-RS, can be trivially recovered by omitting the linking tag and all variables denoted with a tilde. Finally, Algorithm 10 describes the functional components of Miraidon-LRS and their interactions.

6.4 Miraidon-LRS Parameters

In Table 7 we select parameter sets for the Miraidon linkable ring signature. For this, we ensure that the bit security for solving the instances $\text{MinRank}(q, m, n, [k, k+\ell], r_1)$ and $\text{MinRank}(q, m, n, k, [r_2, 2r_2])$

Miraidon Linkable Ring Signature Signing Algorithm

Public: $q, m, n, k, r \in \mathbb{N}$, $\boldsymbol{M} = (M_1, \ldots, M_k) \in \mathbb{F}_q^{m \times kn}$,
$\boldsymbol{R} = (R_1, \ldots, R_\ell) \in \mathbb{F}_q^{m \times \ell n}$, $\mathcal{M} = (\boldsymbol{M} \,||\, \boldsymbol{R}) \in \mathbb{F}_q^{m \times (k+\ell) n}$, $\mathtt{msg}$
Private: $a \in \mathbb{F}_q^k$, $e \in \mathbb{F}_q^\ell$ s.t. $E = \langle a, \boldsymbol{M} \rangle + \langle e, \boldsymbol{R} \rangle$ is rank r_1,
$\widetilde{E} = \mathtt{tag} + \langle a, \boldsymbol{M} \rangle$ is rank r_2

Sample $\mathtt{MSeed} \xleftarrow{\$} \{0,1\}^\lambda$, $\mathtt{Salt} \xleftarrow{\$} \{0,1\}^{2\lambda}$
$(\mathtt{seed}^{(1)}, \ldots, \mathtt{seed}^{(t)}) = \mathtt{SeedTree}(\mathtt{MSeed}, \mathtt{Salt})$
For $i \in [t]$:
  Sample $(u^{(i)}, S^{(i)}, T^{(i)}) \leftarrow \mathtt{seed}^{(i)}$
  Set $Q^{(i)} = S^{(i)} E T^{(i)}$, $\widetilde{Q}^{(i)} = S^{(i)} \widetilde{E} T^{(i)}$
  Solve $Q^{(i)} = L^{(i)} R^{(i)}$ for $L^{(i)}, R^{(i)}$,
    $\widetilde{Q}^{(i)} = \widetilde{L}^{(i)} \widetilde{R}^{(i)}$ for $\widetilde{L}^{(i)}, \widetilde{R}^{(i)}$
  Set $X^{(i)} = \sum_{j=1}^{k+\ell} u_j^{(i)} \left(S^{(i)} \mathcal{M}_i T^{(i)} \right)$,
    $\widetilde{X}^{(i)} = \sum_{j=1}^{k} u_j^{(i)} \left(S^{(i)} \boldsymbol{M}_i T^{(i)} \right)$
  Set $c_0^{(i)} = \mathsf{com}\left(X^{(i)}, Q^{(i)}, \widetilde{X}^{(i)}, \widetilde{Q}^{(i)}, \mathtt{Salt}, i \right)$
  Set $c_1^{(i)} = \mathsf{com}\left(S^{(i)}, T^{(i)}, \mathtt{Salt}, i \right)$

Create $\mathcal{T} = \mathtt{MerkleTree}\left(c_0^{(1)}, \ldots, c_0^{(t)} \right)$, set $c_0 = \mathtt{Root}_{\mathcal{T}}$
$c_1 = \mathsf{com}\left(c_1^{(1)}, \ldots, c_1^{(t)} \right)$
Generate $(\xi^{(1)}, \ldots, \xi^{(t)}) \leftarrow \mathtt{FS}_1(c_0, c_1, \mathtt{msg}, \mathtt{Salt})$
For $i = 1, \ldots, t$:
  Set $v^{(i)} = u^{(i)} + \xi^{(i)} (a \,||\, e)$,
  $W^{(i)} = \langle v^{(i)}, S^{(i)} \mathcal{M} T^{(i)} \rangle$,
  $\widetilde{W}^{(i)} = S^{(i)} \left(\xi \cdot \mathtt{tag} + \langle v^{(i)}, \boldsymbol{M} \rangle \right) T^{(i)}$
  $y^{(i)} = \mathsf{com}\left(W, \widetilde{W} \right)$
Set $Y = \mathsf{com}\left(y^{(1)}, \ldots, y^{(t)} \right)$

$\boldsymbol{b} \leftarrow \mathtt{FS}_2\left(c_0, c_1, \mathtt{msg}, \mathtt{Salt}, \{\xi^{(i)}\}_{i \in [t]}, Y \right)$
Set $I = \mathrm{supp}(\boldsymbol{b})$, $\mathtt{Path} = \mathtt{SeedPath}(\mathtt{MSeed}, \mathtt{Salt}, I)$
For $i \notin I$:
  Set $\mathtt{resp}^{(i)} = \left(c_1^{(i)}, X^{(i)}, L^{(i)}, R^{(i)}, \widetilde{X}^{(i)}, \widetilde{L}^{(i)}, \widetilde{R}^{(i)} \right)$
For $i \in I$:
  Set $\mathtt{resp}^{(i)} = (v^{(i)})$
Compute $\mathtt{Proof} = \mathtt{MerkleProof}_{\mathcal{T}}(I^c)$
$\sigma = \{c_0, c_1, \mathtt{Salt}, Y, \mathtt{Path}, \mathtt{Proof}, \{\mathtt{resp}^{(i)}\}_{i \in [t]}, \mathtt{tag}\}$
Output signature σ

Algorithm 8: The Miraidon linkable ring signature generation protocol.

Miraidon Linkable Ring Signature Verification Algorithm

Public: $q, m, n, k, r \in \mathbb{N}$, $\boldsymbol{M} = (M_1, \ldots, M_k) \in \mathbb{F}_q^{m \times kn}$,
$\boldsymbol{R} = (R_1, \ldots, R_\ell) \in \mathbb{F}_q^{m \times \ell n}$, $\mathcal{M} = (\boldsymbol{M} \,||\, \boldsymbol{R}) \in \mathbb{F}_q^{m \times (k+\ell) n}$
Input: message $\mathtt{msg}$, signature σ

Generate $(\xi^{(1)}, \ldots, \xi^{(t)}) \leftarrow \mathtt{FS}_1(c_0, c_1, \mathtt{msg}, \mathtt{Salt})$
Generate $(b^{(1)}, \ldots, b^{(t)}) \leftarrow \mathtt{FS}_2(c_0, c_1, \mathtt{msg}, \mathtt{Salt}, \{\xi^{(i)}\}_{i \in [t]}, Y)$
Set $I = \mathrm{supp}(b^{(1)}, \ldots, b^{(t)})$
Recompute $\{\mathtt{seed}^{(i)}\}_{i \in I} = \mathtt{FormTree}(\mathtt{Path}, \mathtt{Salt})$
For $i \notin I$:
  Set $Q^{(i)} = L^{(i)} R^{(i)}$ and $\widetilde{Q}^{(i)} = S^{(i)} \widetilde{E} T^{(i)}$
  Set $c_0^{(i)} = \mathsf{com}\left(X^{(i)}, Q^{(i)}, \widetilde{X}^{(i)}, \widetilde{Q}^{(i)}, \mathtt{Salt}, i \right)$
  Set $y^{(i)} = \mathsf{com}\left(X^{(i)} + \xi^{(i)} Q^{(i)},\ \widetilde{X}^{(i)} + \xi^{(i)} \widetilde{Q}^{(i)} \right)$
For $i \in I$:
  Sample $(S^{(i)}, T^{(i)}) \leftarrow \mathtt{seed}^{(i)}$
  Set $c_1^{(i)} = \mathsf{com}\left(S^{(i)}, T^{(i)}, \mathtt{Salt}, i \right)$
  Set $y^{(i)} = \mathsf{com}\left(\langle v^{(i)}, S^{(i)} \mathcal{M} T^{(i)} \rangle,\ S^{(i)} \left(\xi \cdot \mathtt{tag} + \langle v^{(i)}, \boldsymbol{M} \rangle \right) T^{(i)} \right)$
Accept σ if:
  $c_0 = \mathsf{com}\left(c_0^{(1)}, \ldots, c_0^{(t)} \right)$
  $c_1 = \mathtt{VerifyTree}\left(\{c_1^{(i)}\}_{i \notin I}, \mathtt{Proof} \right)$
  $Y = \mathsf{com}\left(y^{(1)}, \ldots, y^{(t)} \right)$
Else: reject

Algorithm 9: The Miraidon linkable ring signature verification procedure.

$\mathtt{PubParam}$: $\mathtt{pp} = (q, m, n, k, r, N) \in \mathbb{N}^6$, $\boldsymbol{M} = (M_1, \ldots, M_k) \in \mathbb{F}_q^{m \times kn}$

$\mathtt{KeyGen}(\mathtt{pp}, \{\mathcal{U}_i\}_{i=1}^N) \to (\mathtt{sk}, \mathtt{pk})$
  For $i = 1, \ldots, \ell$, user $\mathcal{U}_i$ does:
    Sample individual secret keys $a^{(i)} \in \mathbb{F}_q^k$ and $E^{(i)} \in \mathbb{F}_q^{m \times n}$ of rank r_1
    Set $R_i = E^{(i)} - \langle a^{(i)}, \boldsymbol{M} \rangle$
  Form the ring public key $\mathtt{pk} = \boldsymbol{R} = (R_1, \ldots, R_\ell) \in \mathbb{F}_q^{m \times \ell n}$
  Signer $\mathcal{U}_\pi$ sets the ring secret key $\mathtt{sk} = a^{(\pi)} \in \mathbb{F}_q^k$

$\mathtt{Sign}(\mathtt{pp}, \mathtt{sk}, \mathtt{pk}) \to \sigma$
  Signer $\mathcal{U}_\pi$ does:
    Sample $\widetilde{E} \in \mathbb{F}_q^{m \times n}$ of rank r_2, calculate $\mathtt{tag} = \widetilde{E} - \langle a^{(\pi)}, \boldsymbol{M} \rangle$
  Implement Algorithm 8 with $\mathtt{input} = (\mathtt{pp}, \mathtt{pk}, \mathtt{tag})$ and $\mathtt{sk}$
  Set transcript to be τ; define $\sigma = (\tau, \mathtt{tag})$ and output LRS σ

$\mathtt{Verify}(\mathtt{input}, \sigma) \to \{0, 1\}$
  Recompute τ using Algorithm 9, verify if τ is valid transcript
  Output 1, else output 0

$\mathtt{Link}(\mathtt{input}, \sigma, \sigma') \to \{0, 1\}$
  Parse $\sigma = (\tau, \mathtt{tag})$ and $\sigma' = (\tau', \mathtt{tag}')$
  Ensure that σ and σ' are valid using τ and τ', verify that $\mathtt{tag} = \mathtt{tag}'$
  Output 1, else output 0

Algorithm 10: The functions of the Miraidon protocol.

(for linkability; see Appendix B) are all at or above 128, where we use brackets to denote that all parameter sets contained in the interval should each be hard.

$\log_2(\ell)$	q	m	n	$k+\ell$	r_1	r_2	Signature (kB)
2	127	15	15	$121+4$	4	3	53.90
3	127	15	15	$121+8$	4	3	54.33
4	127	15	15	$121+16$	4	3	55.17
5	127	15	15	$121+32$	4	3	56.18
6	127	16	16	$105+64$	4	4	64.12

Table 7: Parameters for the Miraidon linkable ring signature scheme with ℓ members.

We compare Miraidon-LRS to some of the most advanced lattice- and code-based linkable ring signature schemes in Table 8. Note that this work concentrates on rings of size 64 or fewer, which is the parameter regime inhabited by cryptocurrencies: pre-FCMP+ upgrade, Monero utilizes 32-member rings to implement their linkable ring signatures. We highlight that for medium-to-small ring sizes, Miraidon-LRS tends to perform better than the other protocols we consider. We include Linkable Raptor [45], as Miraidon-LRS achieves better signatures for larger ring sizes.

ℓ	2^2	2^3	2^4	2^5	2^6	Assumption	Sec.
Miraidon-LRS	54	54	55	56	64	MinRank	128
Liu & Wang [44]	-	-	66	-	-	SDP	80
BLO18 [16]	-	83	-	306	-	MSIS/MLWE	128
Lattice RingCT [4]	$28^\star$	44	87	171	340	R-SIS	100
Linkable Raptor [45]	$7^\star$	$12^\star$	$22^\star$	$43^\star$	83	SIS	100

Table 8: A comparison of various linkable ring signatures in kB.
* denotes approximated parameters

7 Conclusions and Future Work

As the transition to post-quantum cryptography accelerates, the development of efficient and secure signature primitives has become increasingly important. In particular, advanced anonymity-preserving primitives such as ring signatures and linkable ring signatures play a central role in applications including privacy-preserving authentication, anonymous cryptocurrencies, and decentralized identity systems. While substantial progress has been made in lattice- and code-based cryptography, comparatively fewer advanced signature constructions have been developed from the MinRank problem, despite its strong security foundations and growing relevance in post-quantum cryptography.

In this work, we introduced Miraidon, a novel MinRank-based framework for post-quantum cryptography, and use it to construct efficient advanced signature primitives. Building on this new zero-knowledge proof system, we develop Miraidon-S, a post-quantum signature scheme with

competitive parameters and communication costs. We further extend this framework to obtain Miraidon-RS, a ring signature scheme achieving smaller signature sizes than both MR-DSS and several contemporary lattice-based constructions. Finally, we introduced Miraidon-LRS, the first linkable ring signature scheme based on the MinRank problem, which is comparable to state-of-the-art lattice-based alternatives.

Several directions for future work remain open. In particular, further parameter optimization may lead to additional reductions in signature and public key sizes. Improvements to the techniques of [50] would be especially valuable, as they could reduce public key sizes essentially for free. Another promising avenue is the development of a traceable ring signature scheme based on the MinRank problem, where malicious reuse of a signing key not only reveals that two signatures are linked, but also identifies the identity of the signer within the ring.

A Security Definitions

We now give the formal definitions involving ring signatures, which may be found in [18]. We recall that λ is the security parameter.

Definition 3. *For security parameter λ, a ring signature consists of three polynomial-time algorithms:*

1. $\mathtt{KeyGen}(1^\lambda) \to (\mathtt{pk}, \mathtt{sk})$*, taking public parameters and outputting a public/secret key pair.*
2. $\mathtt{Sign}(\mathtt{pk}_R, \mathtt{sk}_i, \mathtt{msg}) \to \sigma$*, accepting the ring's public key $\mathtt{pk}_R = (\mathtt{pk}_1, \ldots, \mathtt{pk}_N)$ for $N \geq 2$ distinct individual public keys, the secret key $\mathtt{sk}_i$ corresponding to $\mathtt{pk}_i \in \mathtt{pk}_R$, and a message $\mathtt{msg}$, then producing signature σ.*
3. $\mathtt{Verify}(\mathtt{pk}_R, \mathtt{msg}, \sigma) \to \{0, 1\}$*, checking a signature σ is valid from the public key and $\mathtt{msg}$.*

This scheme is correct if, for all set of outputs $\{\mathtt{pk}_i, \mathtt{sk}_i\}_{i=1}^N$ from $\mathtt{KeyGen}(1^\lambda)$, we have:

$$\mathtt{Verify}(\mathtt{pk}_R, \mathtt{msg}, \mathtt{Sign}(\mathtt{pk}_R, \mathtt{sk}_i, \mathtt{msg})) = 1.$$

Definition 4. *A linkable ring signature scheme satisfies anonymity if for any PPT adversary $\mathcal{A}$, the advantage in the following game is negligible in λ:*

1. ***Setup:*** *The challenger generates a pool of key pairs $\{\mathtt{pk}_i, \mathtt{sk}_i\}_{i=1}^N$ and provides $\mathtt{pk}_R = (\mathtt{pk}_1, \ldots, \mathtt{pk}_N)$ to $\mathcal{A}$, who is given arbitrary access to a signing oracle $\mathcal{O}_{sign}(\mathtt{pk}_R, \mathtt{sk}_i, \mathtt{msg})$.*
2. ***Challenge:*** *$\mathcal{A}$ outputs a message $\mathtt{msg}^*$, a ring $\mathtt{pk}_R^*$, and two public keys $\mathtt{pk}_{i_0}, \mathtt{pk}_{i_1} \in \mathtt{pk}_R^*$.*
3. ***Signing:*** *The challenger samples a bit $b \leftarrow \{0, 1\}$, computes $\sigma^* = \mathtt{Sign}(\mathtt{pk}_R^*, \mathtt{sk}_{i_b}, \mathtt{msg}^*)$, and provides σ^* to $\mathcal{A}$.*
4. ***Output:*** *$\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$, and wins if $b = b'$.*

We say that $(\mathtt{KeyGen}, \mathtt{Sign}, \mathtt{Verify})$ achieves anonymity if, for any polynomial N, $\mathcal{A}$'s success probability in the long run $Adv_{\mathcal{A}}^{anon}(\lambda) = |Pr[b' = b] - 1/2|$ is negligible.

Definition 5. *A linkable ring signature scheme is existentially unforgeable under chosen-message attacks (EUF-CMA) if for any PPT adversary $\mathcal{A}$, the probability of winning the following game is negligible in λ:*

1. ***Setup:*** *The challenger generates a pool of key pairs $\{\mathtt{pk}_i, \mathtt{sk}_i\}_{i=1}^N$. $\mathcal{A}$ is given $\mathtt{pk}_R = (\mathtt{pk}_1, \ldots, \mathtt{pk}_N)$ and access to $\mathcal{O}_{sign}$.*

2. ***Output:*** *$\mathcal{A}$ outputs a tuple $(\mathtt{pk}_R^*, \mathtt{msg}^*, \sigma^*)$.*

$\mathcal{A}$ wins if: $\mathtt{Verify}(\mathtt{pk}_R^*, \mathtt{msg}^*, \sigma^*) = 1$ and σ^* was not the output of a query to $\mathcal{O}_{sign}$ on inputs $(\mathtt{pk}_R^*, -, \mathtt{msg}^*)$.

We now upgrade these definitions to a linkable ring signature.

Definition 6. *Formally, a linkable ring signature is a ring signature from Definition 3, plus one additional polynomial-time algorithm:*

1. *$\mathtt{Link}(\mathtt{pk}_R, \mathtt{msg}_1, \sigma_1, \mathtt{msg}_2, \sigma_2) \to \{0, 1\}$, using the public key, two messages $\mathtt{msg}_1, \mathtt{msg}_2$, and two signatures σ_1, σ_2 such that $\mathtt{Verify}(\mathtt{pk}_R, \mathtt{msg}_i, \sigma_i) = 1$ for $i = 1, 2$, this algorithm outputs 1 if σ_1 and σ_2 were signed using the same secret key.*

Definition 7. *A linkable ring signature scheme is linking correct if for $N \geq 2$, any set of key pairs $\{\mathtt{pk}_i, \mathtt{sk}_i\}_{i=1}^N$ generated by $\mathtt{KeyGen}(1^\lambda)$, given the ring's public key $\mathtt{pk}_R = (\mathtt{pk}_1, \ldots, \mathtt{pk}_N)$, the following holds:*

1. ***Linking Correctness:*** *For $i, j \in [N]$ and messages $\mathtt{msg}_1, \mathtt{msg}_2$, let $\sigma_1 = \mathtt{Sign}(\mathtt{pk}_R, \mathtt{sk}_i, \mathtt{msg}_1)$ and $\sigma_2 = \mathtt{Sign}(\mathtt{pk}_R, \mathtt{sk}_j, \mathtt{msg}_2)$. Then:*

$$\mathtt{Link}(\mathtt{pk}_R, \mathtt{msg}_1, \sigma_1, \mathtt{msg}_2, \sigma_2) = 1 \iff i = j$$

Definition 8. *A linkable ring signature scheme satisfies linkability if for any PPT adversary $\mathcal{A}$, the probability of winning the following game is negligible in λ: $\mathcal{A}$ is given access to $\mathtt{KeyGen}(1^\lambda)$ and outputs a ring $\mathtt{pk}_R^*$ of size N, alongside a set of $N+1$ valid message-signature pairs $\{(\mathtt{msg}_k, \sigma_k)\}_{k=1}^{N+1}$.*

$\mathcal{A}$ wins if:

1. *For all $k \in [N+1]$, $\mathtt{Verify}(\mathtt{pk}_R^*, \mathtt{msg}_k, \sigma_k) = 1$.*
2. *For all distinct $i, j \in [N+1]$, $\mathtt{Link}(\mathtt{pk}_R^*, \mathtt{msg}_i, \sigma_i, \mathtt{msg}_j, \sigma_j) = 0$.*

Definition 9. *A linkable ring signature scheme satisfies non-frameability if for any PPT adversary $\mathcal{A}$, the probability of winning the following game is negligible in λ:*

1. ***Setup:*** *The challenger generates a pool of key pairs $\{(\mathtt{pk}_i, \mathtt{sk}_i)\}_{i=1}^N$. $\mathcal{A}$ has access to $\mathcal{O}_{sign}$ and $\mathcal{O}_{corrupt}$, where $\mathcal{O}_{sign}(\mathtt{pk}_R, \mathtt{sk}_i, \mathtt{msg})$ returns a valid signature from user i on message $\mathtt{msg}$, and $\mathcal{O}_{corrupt}(i)$ returns the secret key $\mathtt{sk}_i$*
2. ***Output:*** *$\mathcal{A}$ outputs a ring $\mathtt{pk}_R^*$, a message $\mathtt{msg}^*$, and a forged signature σ^*.*

$\mathcal{A}$ wins if:

1. *$\mathtt{Verify}(\mathtt{pk}_R^*, \mathtt{msg}^*, \sigma^*) = 1$.*
2. *There exists an honest user $\mathtt{pk}_i \in \mathtt{pk}_R^*$ such that a previous query to $\mathcal{O}_{sign}$ returned σ' for message $\mathtt{msg}'$ on behalf of $\mathtt{pk}_i$, with*

$$\mathtt{Link}(\mathtt{pk}_R^*, \mathtt{msg}^*, \sigma^*, \mathtt{msg}', \sigma') = 1.$$

3. *The signature σ^* was not strictly the output of $\mathcal{O}_{sign}$.*

Remark 1. Note that we do not give a proof of existential unforgeability, as this follows from linkability and nonframeability [34].

B Security Proofs

Theorem 6. *Our linkable ring signature scheme achieves correctness.*

Proof. The correctness of `Sign` follows from the correctness of the underlying identification protocol, due to the application of the Fiat-Shamir heuristic: so we always have that $\texttt{Verify}(\texttt{pk}_R, \texttt{msg}, \sigma) = 1$ for any genuine $(\texttt{msg}, \sigma)$.

To see that it is linking correct, note that if σ and σ' were generated by the same user who is honestly behaving according to protocol, then `Link` returns 1. □

Theorem 7. *Our linkable ring signature scheme satisfies anonymity in the ROM, assuming Problem 2 is hard.*

Proof. For anonymity, we show that the signature reveals no information about which member signed it, assuming the adversary does not already know the secret key and has not seen a prior signature from the same user. We prove this via a sequence of indistinguishable games. Let P_X denote the probability that $\mathcal{A}$ guesses correctly $b' = b$ in Game X.

Game A (Legitimate): This is the true anonymity game from Definition 4. The challenger computes $\texttt{tag}^* = \widetilde{E}_b - \langle a_b, \boldsymbol{M} \rangle$ with $\text{rank}\left(\widetilde{E}_b\right) \leq r_2$, then executes the true signing algorithm to produce σ^*. Then $P_A = \Pr[b' = b \text{ in Game A}]$.

Game B (Simulated): In this game, the challenger $\mathcal{C}$ still uses the secret key a_b for the linking tag, but invokes the zero-knowledge simulator $\mathcal{S}$ for the signature. This simulator accepts $\boldsymbol{M}$, message $\texttt{msg}^*$, and tag $\texttt{tag}^*$ to produce signature σ^*_{sim} without knowledge of a_b.

As this simulated proof is indistinguishable from a genuine proof, any noticeable differences between Game A and Game B lead to an advantage is breaking the zero-knowledgeness of the underlying proof:

$$|P_A - P_B| \leq \text{Adv}^{zk}_{\mathcal{A}}(\lambda).$$

Game C (Random Tag): Now, $\mathcal{C}$ samples a random linking tag. Instead of computing $\texttt{tag}^*$ from a_b, they select it uniformly at random from $\mathbb{F}_q^{m \times n}$, then run $\mathcal{S}$. The simulator outputs σ^*_{sim}.

If $\mathcal{A}$ can distinguish Game B from Game C, then they have an advantage in violating Problem 2, contrary to our assumptions. That is,

$$|P_B - P_C| \leq \text{Adv}^{DMR}_{\mathcal{A}}(\lambda).$$

Overall, since Game C produces a random signature and linking tag - neither of which depend on the challenger's bit b or the secret key a_b - the adversary's advantage in guessing b in Game C is exactly chance, so $P_C = \frac{1}{2}$. Thus,

$$\text{Adv}^{anon}_{\mathcal{A}}(\lambda) = \left| P_A - \frac{1}{2} \right| \leq |P_A - P_B| + |P_B - P_C| = \text{Adv}^{zk}_{\mathcal{A}}(\lambda) + \text{Adv}^{DMR}_{\mathcal{A}}(\lambda).$$

Since the zero-knowledge advantage and the Decisional MinRank advantage are negligible for any PPT adversary, our scheme achieves linkable anonymity. □

Theorem 8. *Our linkable ring signature scheme realizes linkability in the ROM.*

Proof. We demonstrate linkability by showing it is difficult for an adversary to produce two valid signatures with the same linking tag, but distinct secret keys.

Let $\mathcal{A}$ denote an adversary capable of breaking linkability in Algorithm 8. That is, per Definition 8, they can produce tuples $(\mathtt{msg}_1, \sigma_1)$ and $(\mathtt{msg}_2, \sigma_2)$ satisfying $\mathtt{Verify}(\mathtt{pk}_R, \mathtt{msg}_i, \sigma_i) = 1$ for $i = 1, 2$, and $\mathtt{Link}(\mathtt{pk}_R, \mathtt{msg}_1, \sigma_1, \mathtt{msg}_2, \sigma_2) = 1$.

Let $\mathcal{P}_{gen}$ denote genuine parameters produced by a legitimate honest user, while $\mathcal{P}_{sim}$ are parameters generated by the simulator algorithm $\mathcal{S}$. By the zero-knowledge property of the identification protocol, no $\mathcal{A}$ can determine which is which, except by chance. Note that for $\mathcal{P}_{sim}$, the extractor algorithm can recover $a_1 \neq a_2$ such that for $i = 1, 2$ the following holds: $\widetilde{E}_i = \mathtt{tag}_i + \langle a_i, \boldsymbol{M} \rangle$ is r_2.

As we suppose $\mathcal{A}$ can violate linkability, we assume $\mathtt{tag}_1 = \mathtt{tag}_2$, thus $\langle a_1, \boldsymbol{M} \rangle - \widetilde{E}_1 \neq \langle a_2, \boldsymbol{M} \rangle - \widetilde{E}_2$. To break linkability, it must be that $\widetilde{E}_1 - \widetilde{E}_2 = \langle a_1 - a_2, \boldsymbol{M} \rangle$, implying

$$\operatorname{rank}\left(\langle a_1 - a_2, \boldsymbol{M} \rangle\right) = \operatorname{rank}\left(\widetilde{E}_1 - \widetilde{E}_2\right) \leq \operatorname{rank}\left(\widetilde{E}_1\right) + \operatorname{rank}\left(\widetilde{E}_2\right) = 2r_2.$$

Hence this adversary can break the MinRank problem, as they output non-zero $a = a_i - a_j$ which results in a linear combination of rank at most $2r_2$, in contradiction to our assumptions. □

A consequence of this proof is that is prudent to select parameters such that the MinRank instance of rank r_2 and rank $2r_2$ are both hard.

Theorem 9. *Our linkable ring signature scheme satisfies nonframeability, assuming MinRank*$(q, m, n, k+\ell, r_1)$ *and MinRank*$(q, m, n, k, 2r_2)$ *are hard.*

Proof. Nonframeability ensures that an adversary cannot forge a signature to frame an honest user, constructing a valid signature with the same linking tag. We show that a PPT $\mathcal{A}$ breaking nonframeability leads to solving a MinRank instance.

Setup: Suppose an algorithm $\mathcal{B}$ sets up the game by generating public parameters and N key pairs.

Setup: $\mathcal{A}$ outputs a forged signature σ^* from $\mathtt{msg}^*$ on $\boldsymbol{M}$ that frames user i, so their tag matches. That is, $\mathtt{tag}^* = \mathtt{tag}_i = \widetilde{E}_i - \langle a_i, \boldsymbol{M} \rangle$ such that $\widetilde{E}_i$ is rank r_2.

Since σ^* is a valid proof, an the underlying zero-knowledge proof is simulation-extractable, $\mathcal{B}$ rewinds to extract a witness (a^*, e^*). This witness must satisfy $\mathtt{tag}^* = \widetilde{E}^* - \langle a^*, \boldsymbol{M} \rangle$ such that $\widetilde{E}^*$ is rank r_2, and $E^* = \langle a^*, \boldsymbol{M} \rangle + \langle e^*, \boldsymbol{R} \rangle$ such that E^* is rank r_1. From this, we have two cases:

Case A: The extracted key is also the legitimate key, $a^* = a_i$. As $\mathcal{A}$ never queried the corruption oracle, this means they must have extracted the secret key from the public parameters and transcript, computing it directly from the pubkey relation $E^* = \langle a^*, \boldsymbol{M} \rangle + \langle e^*, \boldsymbol{R} \rangle$. In effect, they have solved an instance of $\text{MinRank}(q, m, (k+\ell)n, k+\ell, r_1)$.

Case B: There is a collision and $a^* \neq a_i$. Let this difference be called a, which is non-zero. We can rearrange the tag equation above and take the rank to see that

$$\operatorname{rank}\left(\langle a, \boldsymbol{M} \rangle\right) = \operatorname{rank}\left(\widetilde{E}^* - \widetilde{E}_i\right) \leq \operatorname{rank}\left(\widetilde{E}^*\right) + \operatorname{rank}\left(\widetilde{E}_i\right) \leq 2r_2.$$

That is, they have solved an instance of $\text{MinRank}(q, m, kn, k, 2r_2)$.

In both cases, an adversary capable of violating nonframeability can also solve an instance of the MinRank problem, a feat that we consider intractable from PPT algorithms.

References

1. Adj, G., Barbero, S., Bellini, E., Esser, A., Rivera-Zamarripa, L., Sanna, C., Verbel, J.A., Zweydinger, F.: MiRitH - MinRank in the Head. https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures, accessed: 2026-05-15
2. Adj, G., Barbero, S., Bellini, E., Esser, A., Rivera-Zamarripa, L., Sanna, C., Verbel, J.A., Zweydinger, F.: MiRitH: Efficient Post-Quantum Signatures from MinRank in the Head. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2024**, 304–328 (2024), https://api.semanticscholar.org/CorpusID:264559629
3. Adj, G., Barbero, S., Bellini, E., Esser, A., Rivera-Zamarripa, L., Sanna, C., Verbel, J.A., Zweydinger, F., Aragon, N., Bardet, M., Bidoux, L., Chi-Domínguez, J., Dyseryn, V., Feneuil, T., Gaborit, P., Neveu, R., Rivain, M., Tillich, J.P.: Mirath. https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures, accessed: 2026-05-15
4. Alberto Torres, W.A., Steinfeld, R., Sakzad, A., Liu, J.K., Kuchta, V., Bhattacharjee, N., Au, M.H., Cheng, J.: Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0). In: Susilo, W., Yang, G. (eds.) Information Security and Privacy. pp. 558–576. Springer International Publishing, Cham (2018)
5. Aragon, N., Bardet, M., Bidoux, L., Chi-Domínguez, J., Dyseryn, V., Feneuil, T., Gaborit, P., Neveu, R., Rivain, M., Tillich, J.P.: MIRA. https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures, accessed: 2026-05-15
6. Aragon, N., Bidoux, L., Chi-Domínguez, J., Feneuil, T., Gaborit, P., Neveu, R., Rivain, M.: MIRA: a Digital Signature Scheme Based on the MinRank Problem and the MPC-in-the-Head Paradigm. CoRR **abs/2307.08575** (2023). https://doi.org/10.48550/ARXIV.2307.08575, https://doi.org/10.48550/arXiv.2307.08575
7. Attema, T., Cramer, R., Kohl, L.: A Compressed Σ-Protocol Theory for Lattices. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part II. pp. 549–579. Lecture Notes in Computer Science, Springer (2021). https://doi.org/10.1007/978-3-030-84245-1_19, https://doi.org/10.1007/978-3-030-84245-1_19
8. Attema, T., Fehr, S., Klooß, M.: Fiat-Shamir Transformation of Multi-Round Interactive Proofs. In: Kiltz, E., Vaikuntanathan, V. (eds.) Theory of Cryptography - 20th International Conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, Proceedings, Part I. pp. 113–142. Lecture Notes in Computer Science, Springer (2022). https://doi.org/10.1007/978-3-031-22318-1_5, https://doi.org/10.1007/978-3-031-22318-1_5
9. Babai, L.: Trading Group Theory for Randomness. In: Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing. p. 421–429. STOC '85, Association for Computing Machinery, New York, NY, USA (1985). https://doi.org/10.1145/22145.22192, https://doi.org/10.1145/22145.22192
10. Baldi, M., Barenghi, A., Bitzer, S., Karl, P., Manganiello, F., Pavoni, A., Pelosi, G., Santini, P., Schupp, J., Slaughter, F., Wachter-Zeh, A., Weger, V.: CROSS: Codes and Restricted Objects Signature Scheme. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/CROSS-spec-web.pdf, accessed: 26-Jan-2025
11. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Tillich, J.P.: Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem. Des. Codes Cryptography **91**(11), 3671–3707 (Jul 2023). https://doi.org/10.1007/s10623-023-01265-x, https://doi.org/10.1007/s10623-023-01265-x
12. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R., Smith-Tone, D., Tillich, J.P., Verbel, J.: Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 507–536. Springer International Publishing, Cham (2020)
13. Barenghi, A., Biasse, J.F., Persichetti, E., Santini, P.: LESS-FM: Fine-Tuning Signatures from the Code Equivalence Problem. In: Cheon, J.H., Tillich, J.P. (eds.) Post-Quantum Cryptography. pp. 23–43. Springer International Publishing, Cham (2021)

14. Battagliola, M., Longo, R., Pintore, F., Signorini, E., Tognolini, G.: A Revision of CROSS Security: Proofs and Attacks for Multi-Round Fiat-Shamir Signatures. Cryptology ePrint Archive, Paper 2025/127 (2025), https://eprint.iacr.org/2025/127
15. Battagliola, M., Longo, R., Pintore, F., Signorini, E., Tognolini, G.: Security of Fixed-Weight Repetitions of Special-Sound Multi-Round Interactive Proofs. Des. Codes Cryptogr. **93**(10), 4323–4353 (2025). https://doi.org/10.1007/S10623-025-01686-W, https://doi.org/10.1007/s10623-025-01686-w
16. Baum, C., Lin, H., Oechsner, S.: Towards Practical Lattice-Based One-Time Linkable Ring Signatures. In: Naccache, D., Xu, S., Qing, S., Samarati, P., Blanc, G., Lu, R., Zhang, Z., Meddahi, A. (eds.) Information and Communications Security. pp. 303–322. Springer International Publishing, Cham (2018)
17. Bellini, E., Esser, A., Sanna, C., Verbel, J.A.: MR-DSS - Smaller MinRank-Based (Ring-)Signatures. In: Cheon, J.H., Johansson, T. (eds.) Post-Quantum Cryptography - 13th International Workshop, PQCrypto 2022, Virtual Event, September 28-30, 2022, Proceedings. pp. 144–169. Lecture Notes in Computer Science, Springer (2022). https://doi.org/10.1007/978-3-031-17234-2_8, https://doi.org/10.1007/978-3-031-17234-2_8
18. Bender, A., Katz, J., Morselli, R.: Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles. In: Halevi, S., Rabin, T. (eds.) Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings. pp. 60–79. Lecture Notes in Computer Science, Springer (2006). https://doi.org/10.1007/11681878_4, https://doi.org/10.1007/11681878_4
19. Beullens, W.: Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020. pp. 183–211. Springer International Publishing, Cham (2020)
20. Beullens, W., Dobson, S., Katsumata, S., Lai, Y.F., Pintore, F.: Group Signatures and More from Isogenies and Lattices: Generic, Simple, and Efficient. In: Advances in Cryptology – EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 – June 3, 2022, Proceedings, Part II. p. 95–126. Springer-Verlag, Berlin, Heidelberg (2022). https://doi.org/10.1007/978-3-031-07085-3_4, https://doi.org/10.1007/978-3-031-07085-3_4
21. Beullens, W., Katsumata, S., Pintore, F.: Calamari and Falafl: Logarithmic (Linkable) Ring Signatures from Isogenies and Lattices. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 464–492. Springer International Publishing, Cham (2020)
22. Borin, G., Persichetti, E., Pintore, F., Reijnders, K., Santini, P.: A Guide to the Design of Digital Signatures based on Cryptographic Group Actions. J. Cryptol. **38**(3), 23 (2025). https://doi.org/10.1007/S00145-025-09542-9, https://doi.org/10.1007/s00145-025-09542-9
23. Buss, J.F., Frandsen, G.S., Shallit, J.O.: The Computational Complexity of Some Problems of Linear Algebra. J. Comput. Syst. Sci. **58**(3), 572–596 (1999). https://doi.org/10.1006/JCSS.1998.1608, https://doi.org/10.1006/jcss.1998.1608
24. Cayrel, P.L., Véron, P., El Yousfi Alaoui, S.M.: A Zero-Knowledge Identification Scheme Based on the q-ary SD Problem. In: SAC'2010. SAC'2010, vol. 6544, pp. 171–186. Springer, Waterloo, Canada (Aug 2010). https://doi.org/10.1007/978-3-642-19574-7_12, https://inria.hal.science/hal-00674249
25. Chailloux, A., Etinski, S.: On the (in)Security of Optimized Stern-Like Signature Schemes. Des. Codes Cryptogr. **92**(3), 803–832 (2024). https://doi.org/10.1007/S10623-023-01329-Y, https://doi.org/10.1007/s10623-023-01329-y
26. Chen, M., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: From 5-Pass MQ-Based Identification to MQ-Based Signatures. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II. pp. 135–165. Lecture Notes in Computer Science (2016). https://doi.org/10.1007/978-3-662-53890-6_5, https://doi.org/10.1007/978-3-662-53890-6_5

27. Chou, T., Niederhagen, R., Persichetti, E., Randrianarisoa, T.H., Reijnders, K., Samardjiska, S., Trimoska, M.: Take Your MEDS: Digital Signatures from Matrix Code Equivalence. In: El Mrabet, N., De Feo, L., Duquesne, S. (eds.) Progress in Cryptology - AFRICACRYPT 2023. pp. 28–52. Springer Nature Switzerland, Cham (2023)
28. COURTOIS, N.: La Sécurité des Primitives Cryptographiques Basées sur des Problèmes Algébriques Multivariables MQ, IP, MinRank, HFE. Ph.D. thesis, Université de Paris 6 - Pierre et Marie Curie (2001), https://api.semanticscholar.org/CorpusID:190348026
29. Courtois, N.T.: Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank. In: Boyd, C. (ed.) Advances in Cryptology — ASIACRYPT 2001. pp. 402–421. Springer Berlin Heidelberg, Berlin, Heidelberg (2001)
30. Esser, A., Verbel, J.A., Zweydinger, F., Bellini, E.: SoK: CryptographicEstimators - a Software Library for Cryptographic Hardness Estimation. In: AsiaCCS. {ACM} (2024)
31. Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J.: Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology. In: ISSAC 2010 - 35th International Symposium on Symbolic and Algebraic Computation. pp. 257–264. ACM, Munich, Germany (Jul 2010). https://doi.org/10.1145/1837934.1837984, https://hal.science/hal-01057840
32. Feige, U., Fiat, A., Shamir, A.: Zero-Knowledge Proofs of Identity. In: Association for Computing Machinery. pp. 210–217 (01 1987). https://doi.org/10.1145/28395.28419
33. Feneuil, T.: Building MPCitH-Based Signatures from MQ, MinRank, and Rank SD. In: Applied Cryptography and Network Security: 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5–8, 2024, Proceedings, Part I. p. 403–431. Springer-Verlag, Berlin, Heidelberg (2024). https://doi.org/10.1007/978-3-031-54770-6_16, https://doi.org/10.1007/978-3-031-54770-6_16
34. Fiat, A., Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Proceedings on Advances in Cryptology—CRYPTO '86. p. 186–194. Springer-Verlag, Berlin, Heidelberg (1987)
35. Fiore, D., Garms, L., Kolonelos, D., Soriente, C., Tucker, I.: Ring Signatures with User-Controlled Linkability. In: Computer Security – ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part II. p. 405–426. Springer-Verlag, Berlin, Heidelberg (2022). https://doi.org/10.1007/978-3-031-17146-8_20, https://doi.org/10.1007/978-3-031-17146-8_20
36. Ghantous, W., Pintore, F., Veroni, M.: Efficiency of SIDH-based Signatures (Yes, SIDH). Journal of Mathematical Cryptology **18**(1), 20230023 (2024). https://doi.org/doi:10.1515/jmc-2023-0023, https://doi.org/10.1515/jmc-2023-0023
37. Goldwasser, S., Micali, S., Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing **18**(1), 186–208 (1989). https://doi.org/10.1137/0218012, https://doi.org/10.1137/0218012
38. Goubin, L., Courtois, N.T.: Cryptanalysis of the TTM Cryptosystem. In: Okamoto, T. (ed.) Advances in Cryptology — ASIACRYPT 2000. pp. 44–57. Springer Berlin Heidelberg, Berlin, Heidelberg (2000)
39. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Zero-Knowledge from Secure Multiparty Computation. In: Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing. p. 21–30. STOC '07, Association for Computing Machinery, New York, NY, USA (2007). https://doi.org/10.1145/1250790.1250794, https://doi.org/10.1145/1250790.1250794
40. Kales, D., Zaverucha, G.: An Attack on Some Signature Schemes Constructed from Five-Pass Identification Schemes. In: Krenn, S., Schulmann, H., Vaudenay, S. (eds.) Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings. pp. 3–22. Lecture Notes in Computer Science, Springer (2020). https://doi.org/10.1007/978-3-030-65411-5_1, https://doi.org/10.1007/978-3-030-65411-5_1
41. Katz, J., Kolesnikov, V., Wang, X.: Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures. In: Lie, D., Mannan, M., Backes, M., Wang, X. (eds.) Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON,

Canada, October 15-19, 2018. pp. 525–537. ACM (2018). https://doi.org/10.1145/3243734.3243805, https://doi.org/10.1145/3243734.3243805
42. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Wiener, M. (ed.) Advances in Cryptology — CRYPTO' 99. pp. 19–30. Springer Berlin Heidelberg, Berlin, Heidelberg (1999)
43. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) Information Security and Privacy: 9th Australasian Conference, ACISP 2004, Sydney, Australia, July 13-15, 2004. Proceedings. pp. 325–335. Lecture Notes in Computer Science, Springer (2004). https://doi.org/10.1007/978-3-540-27800-9_28, https://doi.org/10.1007/978-3-540-27800-9_28
44. Liu, X., Wang, L.P.: A Postquantum Linkable Ring Signature Scheme from Coding Theory. Security and Communication Networks **2023**, 1–12 (12 2023). https://doi.org/10.1155/2023/1794053
45. Lu, X., Au, M.H., Zhang, Z.: Raptor: A Practical Lattice-Based (Linkable) Ring Signature. In: Deng, R.H., Gauthier-Umaña, V., Ochoa, M., Yung, M. (eds.) Applied Cryptography and Network Security. pp. 110–130. Springer International Publishing, Cham (2019)
46. monero.how: Monero Privacy Explained: Ring Signatures, Stealth Addresses, and RingCT. https://www.monero.how/tutorial-monero-privacy-ring-signatures-stealth-addresses-ringct, accessed: 2026-05-17
47. NIST: Post-Quantum Cryptography: Additional Digital Signature Schemes. https://csrc.nist.gov/projects/pqc-dig-sig/round-3-additional-signatures, accessed: 2026-05-15
48. Rivest, R.L., Shamir, A., Tauman, Y.: How to Leak a Secret. In: Boyd, C. (ed.) Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings. pp. 552–565. Lecture Notes in Computer Science, Springer (2001). https://doi.org/10.1007/3-540-45682-1_32, https://doi.org/10.1007/3-540-45682-1_32
49. Santoso, B., Ikematsu, Y., Nakamura, S., Yasuda, T.: Three-Pass Identification Scheme Based on MinRank Problem with Half Cheating Probability. In: 2022 International Symposium on Information Theory and Its Applications (ISITA). pp. 59–63 (2022)
50. Scala, A.J.D., Sanna, C.: Smaller Public Keys for MinRank-Based Schemes. Journal of Mathematical Cryptology **19**(1), 20240008 (2025). https://doi.org/doi:10.1515/jmc-2024-0008, https://doi.org/10.1515/jmc-2024-0008
51. Stern, J.: A New Paradigm for Public Key Identification. IEEE Transactions on Information Theory **42**(6), 1757–1768 (1996). https://doi.org/10.1109/18.556672, https://ieeexplore.ieee.org/document/556672
52. Stern, J.: A New Identification Scheme Based on Syndrome Decoding. In: Stinson, D.R. (ed.) Advances in Cryptology — CRYPTO' 93. pp. 13–21. Springer Berlin Heidelberg, Berlin, Heidelberg (1994), https://doi.org/10.1007/3-540-48329-2_2
53. Tang, G., Duong, D.H., Joux, A., Plantard, T., Qiao, Y., Susilo, W.: Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022. pp. 582–612. Springer International Publishing, Cham (2022)