Technology Innovation Institute

MR-DSS -- Smaller MinRank-based (Ring-)Signatures

Emanuele Bellini, Andre Esser,
Carlo Sanna, and Javier Verbel

https://eprint.iacr.org/2022/973.pdf

Cryptography
Research Center

tii.ae

Motivation

1. **Digital signature schemes**
   - Authenticity of digital messages.
   - Quantum secure → Against classical + quantum adversaries.
   - 3 schemes selected by NIST → - Dilithium, Falcon (Structured lattices)
     - SPHINCS+ (Hash-based)

2. **Demand** to diversify → **New NIST call for proposals**

3. **MinRank** problem:
   - Extensively study for cryptanalysis.
   - Simple, and easy to describe.
   - So far limited proposals based on the MinRank problem.

Our contribution

MR- DSS: A post-quantum MinRank-Based Digital Signature Scheme.

Previous MinRank-based signatures:

- **2001**: First MinRank-based signature scheme by N. Courtois. **[Cou21]**
  - ZK protocol with soundness 2/3 + Fiat-Shamir.
  - Allows for ring signatures.

- **MR- DSS:**
  - Built over Courtois' scheme.
  - Sigma protocols with helper [Beu20] + Fiat-Shamir
  - Soundness error to ½.
  - Signature and PK sizes smaller than Courtois'.

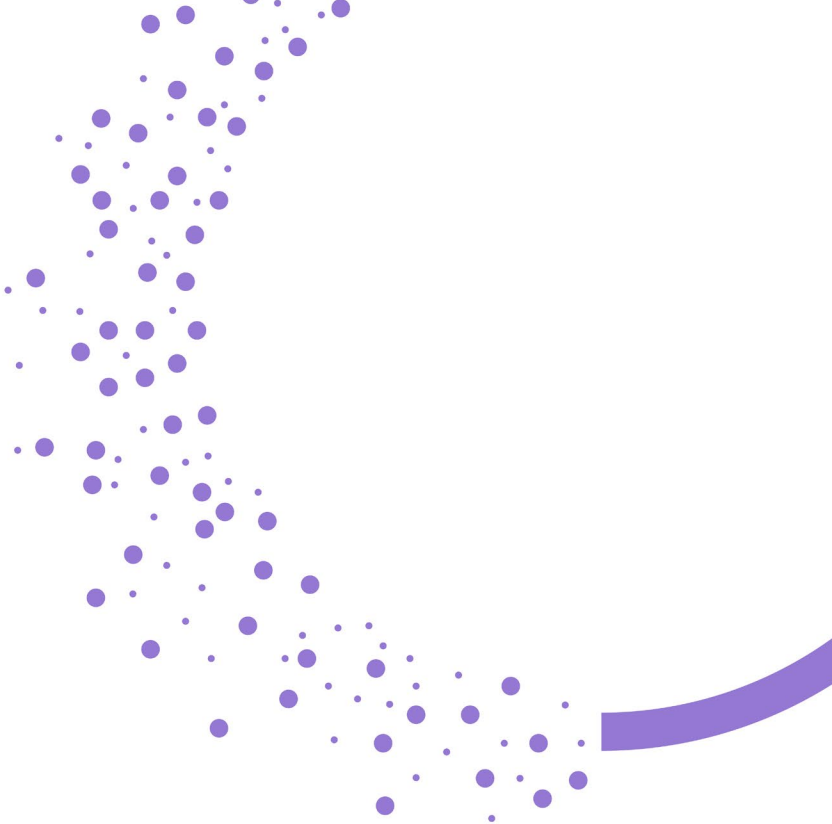
- **Concurrent work**: Signature scheme by Santoso, Ikematsu, Namura, and Yasuda.
  - **Different approach** + achieves **soundness error** of 1/2.

Outline

1. Preliminaries.
2. Our zero-knowledge protocol with Helper.
3. MR-DSS signature scheme.
4. Parameters.

Technology Innovation Institute

Preliminaries



tii.ae

Cryptography Research Center

The MinRank problem

Input: An integer r, and $k+1$ matrices $M_0, \dots, M_k \in \mathbb{F}_q^{m\ x\ n}$

Output: $\alpha_1, \dots, \alpha_k \in \mathbb{F}_q$ such than $rank(M_0 + \sum_{i=1}^{k} \alpha_i Mi) \leq r$

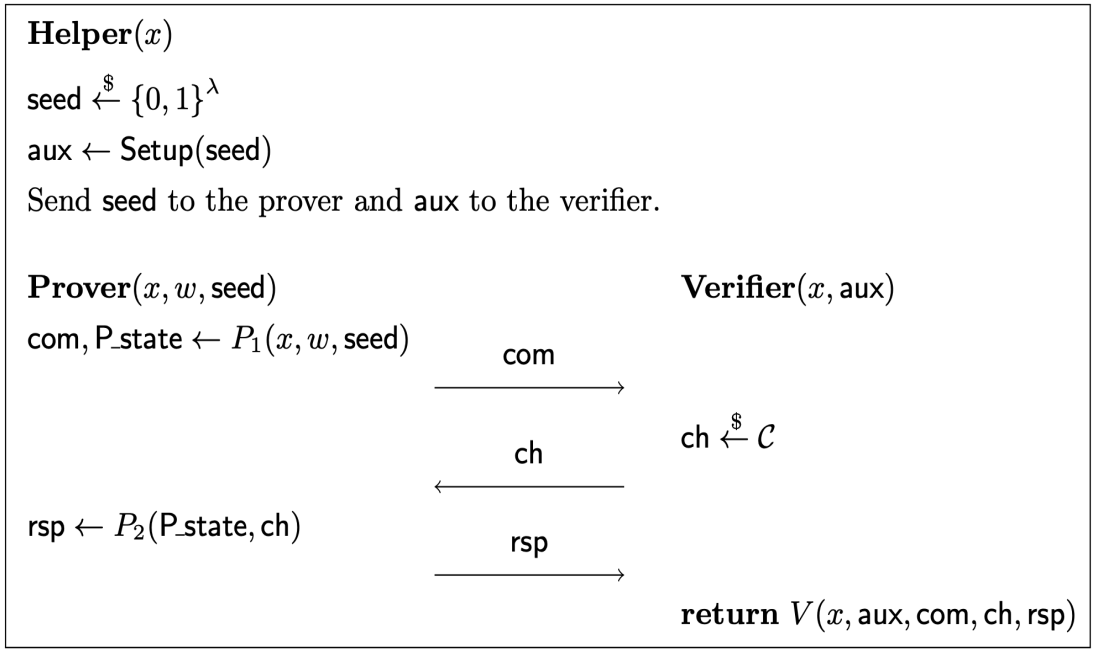
Features:

- NP- complete, and hard for random instances.
- Simple: Based on linear algebra computations.
- Extensively studied: Cryptanalysis of Rainbow, GeMSS, ROLLO, etc.
- Quantum secure.

A 3-pass sigma protocol with helper [Beu20]

- A protocol between the **Prover**(x, w) and the **Verifier**(x)
- **Goal**: Proof the knowledge w such that $(x, w) \in \mathcal{R}$.

The **Helper:** trusted by the **Prover** and the **Verifier.**



Accept or Reject ?

Security properties sigma protocol with Helper

1. **Correct:** A prover holding w is always accepted.

2. **2-special sound:** A witness w can be efficiently extracted

$$(x, aux, com\ \ , ch, rsp) \text{ and } \ (x, aux\ , com\ \ , ch', rsp').$$

3. HV-zero-knowledge: There exists an efficient simulator $\mathcal{S}(x)$ that produces transcripts indistinguishable from the ones by **Prover**(x, w).

Has soundness error p: Any efficient adversary $\mathcal{A}(1^{\lambda}, x)$ passes with prob. $\leq\ p + negl(\lambda)$.

Removing the Helper + Fiat-Shamir signatures

Cut-and-choose[KKW18]: A way to simulate the Helper

Prover(x, w):

for $i \in \{1, \dots, s\}$:

$seed_i \xleftarrow{\$} \{0,1\}^\lambda$

$aux_i \leftarrow Setup(seed_i)$

com_i and rsp_ias before

$com_i, aux_i \; \forall i$ →

← $I, \{ch_i\}_{i \in I}$

→ $\{seed_i\}_{i \notin I}, \{rsp_i\}_{i \in I}$

Verifier(x):

Sample $I \subset \{1, \dots, s\}, |I| = \tau$

Checks $aux_i = Setup(seed_i) \; \forall \; i \notin I$

Validates $(x, aux_i, com_i, ch_i, rsp_i)_{i \in I}$

Fiat-Shamir Transform:

Prover(x, w, msg):

com →

← $ch = H(com \,||\, msg)$

rsp →

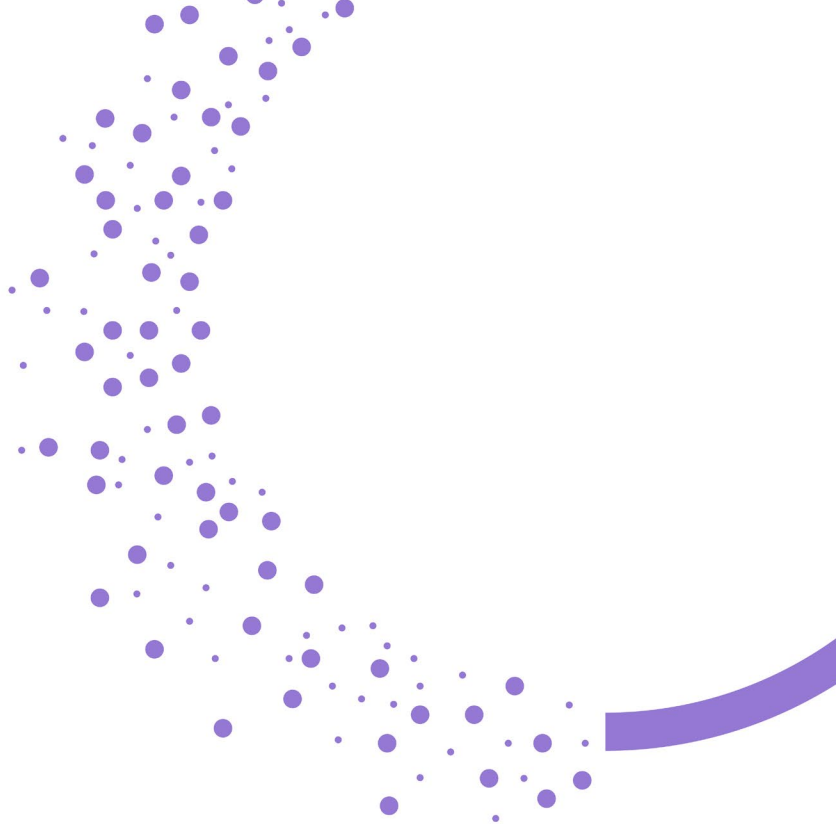
⟹

A signature for msg**:**

The Transcripts of the simulated protoc

Technology Innovation Institute

Our Zero-Knowledge Protocol with Helper



Cryptography Research Center

tii.ae

Our zero-knowledge protocol with Helper

$$(x, w) = ((M_0, \dots, M_k), (E, \alpha)) \text{ s.t : } \quad E \coloneqq M_0 + \Sigma_{i=1}^{k} \alpha_i M_i \ , \quad \text{and } rank(E) \leq r$$

Based on: $\forall \ T, S, \beta \quad TES = TM_0S - \underbrace{T\left(\sum_{i=1}^{k} \beta_i M_i\right)}_{\coloneqq N_1} S + \underbrace{T\left(\sum_{i=1}^{k} (\alpha_i + \beta_i) M_i\right)}_{\coloneqq N_2} S$

Our zero-knowledge protocol with Helper

$(x, w) = ((M_0, \dots, M_k), (E, \alpha))$ s.t : $E := M_0 + \Sigma_{i=1}^{k} \alpha_i M_i$, and $rank(E) \leq r$

Based on: $\forall\ T, S, \beta \quad TES = TM_0S - T\underbrace{\left(\sum_{i=1}^{k} \beta_i M_i\right)}_{:= N_1} S + T\underbrace{\left(\sum_{i=1}^{k} (\alpha_i + \beta_i) M_i\right)}_{:= N_2} S$

Helper: $(\beta, S, T) \leftarrow \text{PRG}(seed)$, and $com_0 = Com(S, T), com_1 = Com(T\ N_1 S)$

Prover$(M, (E, \alpha), seed)$:

$com = Com(T\ N_2 S)$

$\xrightarrow{com}$

$\xleftarrow{ch}$

$\xrightarrow{R}$

If $ch = 0$:

$(R_1, R_2) = (TN_1S, TN_2S)$

else:

$(R_1, R_2) = \big((S, T), \alpha + \beta\big)$

Verifier$(M, (com_0, com_1))$

$ch \xleftarrow{\$} \{0, 1\}$

If $ch = 0$:

$com_1 = Com(R_1)$ and $rank(R_2 - R_1) \leq r$?

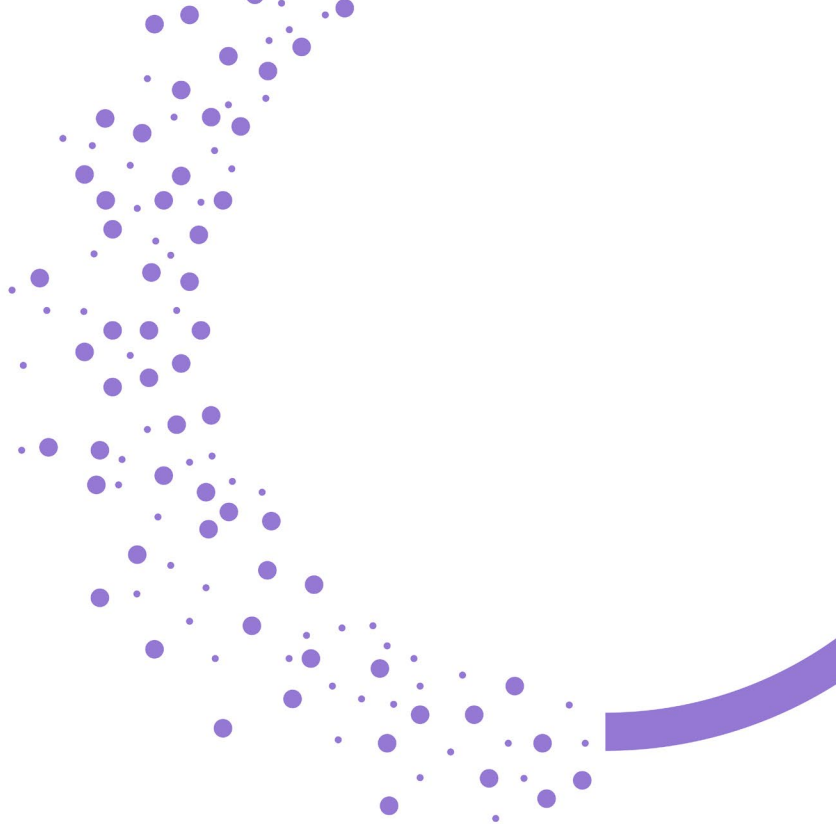
else:

Recompute N_2 from R_2, and T, S for R_1

$com_0 = Com(R_1)$ and $com = Com($ $N_2 S)$

Technology Innovation Institute

MR-DSS signature scheme



Cryptography Research Center

tii.ae

The Signature Scheme

1. **KeyGen:** $M_1, \dots, M_k, E, \alpha$ are random, with $rank(E) \leq r$
   - PK: $M = (M_0, \dots, M_k)$, where $M_0 \coloneqq E + \Sigma_{i=1}^{k} \alpha_i \, Mi$
   - SK $= (E, \alpha)$

2. **Optimizations:**

   - **Smaller PK:** We force k zeros coordinates of M_0.

$$mn \log(q) \Longrightarrow (mn - k) \log(q)$$

   - **Send rank-r matrix**: $(TN_1S, TN_2S - TN_1S)$ instead of (TN_1S, TN_2S)

$$mn \log(q) \Longrightarrow r(m + n) \log(q)$$

The Ring-Signature Scheme

Ring Signatures:

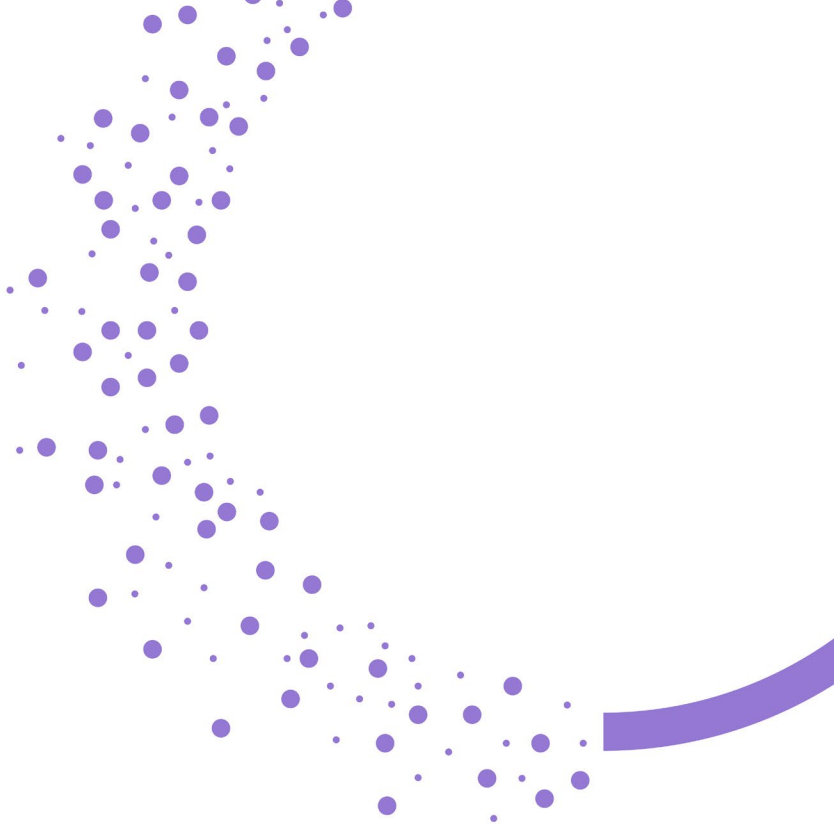
- A **ring** with $\boldsymbol{u}$ user is a set $\mathcal{R} := (PK_1, \dots, PK_u)$.
- A **member** of $\mathcal{R}$ is a holder SK_i for some i.
- Any member of $\mathcal{R}$ can sing a given message.
- Anyone with $\mathcal{R}$ can verify a signature.
- **Anonymity:** The identity of the signer remains secret within $\mathcal{R}$.

MRr-DSS:

- A fixed random public set $M = (M_0, \dots, M_k) \in \mathbb{F}^{m \times n}$.
- (PK, SK) = $(R, (E, \alpha))$, where $R := -E + M_0 + \Sigma_{i=1}^{k} \alpha_i M_i$, $rank(E) \leq r$
- The vector $(1, \alpha_1, \dots, \alpha_k, 0, \dots, 0, 1, 0, \dots, 0)$ is a solution to
- MinRank with : $(M_0, M_1, \dots, M_k, R_1, \dots, R_{j-1}, R, R_{j+1}, \dots, R_u)$
- From α we produce a signature for the ring $(R_1, \dots, R_{j-1}, R, R_{j+1}, \dots, R_u)$.

Technology Innovation Institute

Parameters



Cryptography Research Center

tii.ae

Attacks on the MinRank problem

We want $\alpha \in \mathbb{F}^k$ such that: $E := M_0 + \Sigma_{i=1}^{k} \alpha_i M_i \in \mathbb{F}^{m \times n}$, and $rank(E) \leq r$

1. Kernel Search: Guess $\lceil \frac{k}{m} \rceil$ L.I vectors in $kernel(E)$.

2. Support Minors [BBCGPSTV20]: Rows of $M_0 + \Sigma_{i=1}^{k} \alpha_i M_i \in \text{Row} - \text{Space of } C \in \mathbb{F}^{r \times n}$.

3. Hybrid approach [BBBGT22] : Guess $l_v < r$ of the $\alpha_i's$, and $a < \lceil \frac{k}{m} \rceil$ vectors in $kernel(E)$.

$$MinRank\ (m \times n, k, r) = q^{l_v + ar}\ MinRank(m \times (n - a), k - am - l_v, r)$$

4. $k + 1 < (m - r)(n - r)$ to get uniqueness of α.

5. $m(n - r) - k + 1$ big enough to avoid the "big-m" attack [Cou01].

Removing the Helper and the Signature Scheme

Cat	λ	q	m/n	k	r	Alg.	Bit complexity
I	128	16	16	142	4	KS	158
III	192	16	19	167	6	KS	231
V	256	16	22	254	6	SM	295

Bit complexity of proposed parameters

Cat	Signature size (KB)		PK size (B)	
	Courtois's	MR-DSS	Courtois's	MR-DSS
I	65	**27**	144	**73**
III	135	**60**	205	**121**
V	248	**106**	274	**147**

Signature and pk size comparisons, $s = 2\lambda$ and $\tau = \lambda$.

Performance ring-signatures small rings.

#users (u)	2^3	2^4	2^5	2^6	2^7	Assumption	Security
MRr-DSS	27	27	32	36	45	MinRank	Cat I
[KKW18]	-	-	-	250	-	LOWMC	Cat V
Raptor[LZ19]	10	-	-	81	-	MSIS/MLWE	100 bit
[EZSLL19]	19	-	-	31	-	MSIS/MLWE	Cat II
Falafl [BKP20]	30	-	-	32	-	MSIS/MLWE	Cat I
Calamari[BKP20]	5	-	-	8	-	CSIDH	128 bit
LESS[BBNPS22]	11	-	-	14	-	Code Equiv.	128 bit

Comparison ring signature size (in KB).

Conclusions and future work

Conclusions:

1. We proposed MR-DSS: A signature scheme based on MinRank problem.

- 3-pass ZK proof + Fiat-Shamir transform.
- Its ZK protocol has soundness error of $\frac{1}{2}$.
- It improves by a factor >2 sig. size of Courtois's scheme.
- It is quantum-secure.
- An interesting alternative for ring-signatures.

Future work:

1. ZK protocol for MinRank with smaller soundness.

2. Trapdoor MinRank-based signatures.

Technology Innovation Institute

Thank you!

Questions?