# MinRank in the Head: Short Signatures from Zero-Knowledge Proofs

Gora Adj, Luis Rivera-Zamarripa, Javier Verbel

Technology Innovation Institute, UAE
{gora.adj,luis.zamarripa,javier.verbel}@tii.ae

We present a new digital signature scheme based on the MinRank problem. MinRank is a decoding problem in the rank metric for matrices. It is NP-complete and has been extensively studied, and because no known quantum algorithm improves over classical algorithms, assuming its hardness seems to be reasonable when designing secure post-quantum schemes.

Our MinRank-based signature scheme is built from a zero-knowledge interactive identification scheme (IDS) that proves knowledge of a solution of a Minrank instance. The IDS is, in turn, obtained via the MPC-in-the-head paradigm.

**The IDS.** Using the kipnis-Shamir modeling [5], we formulate the MinRank problem for a target rank $r$ as follows. Given a tuple $\boldsymbol{M} = (M_0, M_1, \dots, M_k)$ of $(n \times n)$-matrices over a field $\mathbb{F}_q$ of $q$ elements, find a vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_k)^T$ in $\mathbb{F}_q^k$ and a matrix $K \in \mathbb{F}_q^{r\times(n-r)}$, such that

$$M_0^L + \sum\nolimits_{i=1}^{k} \alpha_i M_i^L = -\left(M_0^R + \sum\nolimits_{i=1}^{k} \alpha_i M_i^R\right) \cdot K, \tag{1}$$

where, for $i \in [0, k]$, $M_i^L$ is the matrix consisting of the $(n-r)$ first columns of $M_i$, and $M_i^R$ is the remaining $r$ columns. Denote Eq. (1) as $\boldsymbol{M}_{\boldsymbol{\alpha}}^L = \boldsymbol{M}_{\boldsymbol{\alpha}}^R K$.

We construct the underlying N-party MPC protocol of our IDS by generalizing the Nof-Baum verification protocol of multiplication triples in [3], by which our work is inspired, to the matrix triple $(K, \boldsymbol{M}_{\boldsymbol{\alpha}}^R, \boldsymbol{M}_{\boldsymbol{\alpha}}^L)$. With this, we obtain a 5-pass zero-knowledge IDS scheme that enjoys a soundness error of $\varepsilon = \frac{1}{N} + \frac{N-1}{q^n N}$.

**Security of the IDS.** Considering the state-of-the-art algorithms for solving the MinRank problem, we suggest parameter sets for each of the NIST's security categories I, III, and V, i.e., targeting 143, 207, and 273 bits of security, respectively. On the other hand, to meet a security level of a category $\Lambda \in \{\text{I,III,V}\}$ in the IDS, one has to repeat the IDS protocol for $\tau$ rounds, where $\tau$ is such that $\lfloor 1/\varepsilon^\tau \rfloor$ runs of the protocol have the same bit complexity as $\Lambda$.

**The Signature scheme.** To turn our IDS into a non-interactive protocol, which then will result in a signature scheme, we apply the generalized Fiat-Shamir transform for canonical 5-pass IDS protocols.

**Security of the Signature scheme.** Since applying the Fiat-Shamir transform slightly harms the soundness of 5-pass protocols [4], the forgery cost that has to be considered is

$$C(\tau, q, n, N) = \min_{0\le k\le\tau} \left\{ \frac{1}{\sum_{i=k}^{\tau} \left(\frac{1}{q^n}\right)^i \left(1 - \frac{1}{q^n}\right)^{\tau-i} \binom{\tau}{i}} + N^{\tau-k} \right\}. \tag{2}$$

**Parameters and sizes.** In Table 1, where $\lambda$ denotes the security parameter, we propose parameter sets which, in addition to IDS security requirements, takes into account the forgery cost of the signature scheme given in Eq. (2).

Table 2 shows the signature and public key sizes of our scheme compared with Courtois's scheme [2], MR-DSS [1]. Now, compared with the schemes selected by NIST for standardization, our scheme for category I, for instance, offers signatures 15% (*resp.* 39%) shorter than the short (*resp.* fast) version of SPHINCS+, and 2.5 times larger than Dilithium, which security is based on a structured problem from lattices, while our scheme is based on random Minrank instances.

| Set | Variant | $\lambda$ (bits) | $q$ | $n$ | $k$ | $r$ | $N$ | $\tau$ | Bit security | Maximum signature size |
|---|---|---|---|---|---|---|---|---|---|---|
| Ia | Fast<br>Short | 128 | 16 | 15 | 79 | 6 | 16<br>256 | 34<br>18 | 144 | 10364<br>6695 |
| Ib | Fast<br>Short | 128 | 16 | 16 | 142 | 4 | 16<br>256 | 34<br>18 | 155 | 11758<br>7422 |
| IIIa | Fast<br>Short | 192 | 16 | 19 | 115 | 8 | 16<br>256 | 51<br>27 | 207 | 24114<br>14832 |
| IIIb | Fast<br>Short | 192 | 16 | 19 | 167 | 6 | 16<br>256 | 51<br>27 | 229 | 24930<br>15858 |
| Va | Fast<br>Short | 256 | 16 | 21 | 192 | 7 | 16<br>256 | 67<br>35 | 273 | 40827<br>25934 |
| Vb | Fast<br>Short | 256 | 16 | 22 | 254 | 6 | 16<br>256 | 67<br>35 | 295 | 44211<br>27667 |

**Table 1.** Parameter sets for the MinRank MPC-in-the-head signature scheme.

| Set | Signature (KB) | | | Public key (B) | | |
|---|---|---|---|---|---|---|
| | Courtois | MR-DSS | This work | Courtois | MR-DSS | This work |
| Ib | 65 | 27 | 7.2 | 144 | 73 | 73 |
| IIIb | 135 | 60 | 15.4 | 205 | 121 | 121 |
| Vb | 248 | 106 | 27 | 274 | 147 | 147 |

**Table 2.** Size comparison of MinRank-based signature schemes.

## References

1. Bellini, E., Esser, A., Sanna, C., Verbel, J.: MR-DSS – smaller MinRank-based (ring-)signatures. Cryptology ePrint Archive, Paper 2022/973 (2022), https://eprint.iacr.org/2022/973
2. Courtois, N.T.: Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Advances in cryptology—ASIACRYPT 2001 (Gold Coast), vol. 2248, pp. 402–421 (2001)
3. Feneuil, T., Joux, A., Rivain, M.: Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs. Cryptology ePrint Archive, Paper 2022/188 (2022), https://eprint.iacr.org/2022/188
4. Kales, D., Zaverucha, G.: An attack on some signature schemes constructed from five-pass identification schemes. In: Cryptology and Network Security. pp. 3–22. Springer International Publishing, Cham (2020)
5. 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)