Improving the Support Minors Modeling on a MinRank instance on a small field

Alban Gilard

LITIS, Université de Rouen Normandie

Abstract. The MinRank problem is ubiquitous in multivariate and rank-based cryptography. It is at the core of various algebraic attacks, and the security of the MIRA and MiRitH signature schemes, submitted to the first round of the NIST call for Additional Digital Signature Schemes, is based on a Zero-Knowledge Proof of Knowledge of a solution to a random MinRank instance. The Support Minors (SM) technique is considered as one of the most efficient algebraic attacks on MinRank, and the parameters of the MIRA and MiRitH schemes are chosen according to the complexity of the SM method, using an hybrid strategy that reduces the solving of a cryptographic instance to the solving of several smaller instances.

In this talk, we analyse the complexity of solving the support-minors modeling. Usually, we solve this problem by applying the Wiedemann algorithm on a Macaulay matrix of the SM system, which turns out to be sparse, but these matrices have in fact a very specific structure that we study deeper. We then use these results to give a combinatoric version of this algorithm which can be better on instances defined on small fields. For MiRith, it results in a gain of approximatively 4 security bits for some parameters sets. Especially, the security level of Va parameters is reduced from 274 to 270 bits of security.

This research was funded by the French Agence Nationale de la Recherche and plan France 2030 program under Grant ANR-22-PETQ-0008 PQ-TLS. This is a joint work with Magali Bardet.

Keywords: MinRank · Support-Minors Modeling · Macaulay Matrices · Algebraic cryptanalysis · Wiedemann Algorithm

References

1. Magali Bardet and Manon Bertin. Improvement of Algebraic Attacks for Solving Superdetermined MinRank Instances. In Jung Hee Cheon and Thomas Johansson, editors, *Post-Quantum Cryptography 2022*, volume 13512 of *LNCS*, pages 107–123, Cham, September 2022. Springer International Publishing.
2. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In *Advances in Cryptology - ASIACRYPT 2020, International Conference on the Theory and Application of Cryptology and Information Security, 2020. Proceedings*, pages 507–536, 2020.