Cryptanalysis of the Rank Preserving Signature

Nicolas Aragon[1], Maxime Bros[1], and Philippe Gaborit[1]

University of Limoges, CNRS, XLIM, UMR 7252, Limoges, France
{nicolas.aragon, maxime.bros, philippe.gaborit}@unilim.fr

Abstract. In code-based cryptography, the rank metric usually allows one to have smaller keys and signatures than the traditional Hamming metric. Recently, a new rank-based signature was proposed: Durandal [1]. It relies on the use of proofs of knowledge, namely the Schnorr-Lyubashevsky approach. The authors of the Rank Preserving Signature (RPS) [2] built upon this approach and proposed even smaller keys and signatures than Durandal.
In this talk, I will describe our attacks against the RPS scheme which break all sets of parameters proposed in [2].
More precisely, our attacks enable us to forge valid signatures in 2^{68} and 2^{47} operations for sets of parameters whose claimed securities are, respectively, 128 and 192 bits. In addition to this, we give a quantum adaptation of our attack which yields an attack on the last two sets of parameters given in [2].
Overall, our attacks highlight weaknesses of the RPS scheme and give new constraints when designing new parameter sets.
In order to describe the complexities of our attacks, this talk contains theoretical arguments together with experimental results.

Keywords: Rank-Metric based Cryptography · Post-Quantum Cryptography · Signature .

References

[1] Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. Durandal: a rank metric based signature scheme. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *LNCS*, pages 728–758. Springer, 2019.

[2] Terry Shue Chien Lau and Chik How Tan. Rank preserving code-based signature. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 846–851. IEEE, 2020.