Improving Support-Minors rank attacks: applications to G*e*MSS and Rainbow.

John Baena[1], **Pierre Briaud**[2,3], Daniel Cabarcas[1], Ray Perlner[4], Daniel Smith-Tone[4,5] and Javier Verbel[6]

[1] Universidad Nacional de Colombia, Colombia
[2] Sorbonne Universités, UPMC Univ Paris 06
[3] Inria, Team COSMIQ, Paris, France
pierre.briaud@inria.fr
[4] National Institute of Standards and Technology, USA
[5] University of Louisville, USA
[6] Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE

The Support-Minors (SM) method [1] has opened new routes to attack multivariate schemes with rank properties that were previously impossible to exploit, as shown by the recent attacks of [4] and [2] on the NIST candidates G*e*MSS and Rainbow respectively.

In this paper, we study this SM approach more in depth, which allows us first to propose a greatly improved attack on G*e*MSS and also to define a more realistic cost model to evaluate the memory complexity of an XL strategy on the SM system using the Block-Wiedemann algorithm. Our new attack on G*e*MSS makes it completely unfeasible to repair the scheme by simply increasing the size of its parameters or even applying the projection technique from [3], as the signing time would be increased in a considerable way. Also, in our refined cost model, the rectangular MinRank attack from [2] does indeed reduce the security of all round 3 Rainbow parameter sets below their targeted security strengths.

References

1. 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)
2. Beullens, W.: Improved cryptanalysis of UOV and Rainbow. In: Canteaut, A., Standaert, F.X. (eds.) Advances in Cryptology – EUROCRYPT 2021. pp. 348–373. Springer International Publishing, Cham (2021)
3. Øygarden, M., Smith-Tone, D., Verbel, J.: On the effect of projection on rank attacks in multivariate cryptography. In: Cheon, J.H., Tillich, J.P. (eds.) Post-Quantum Cryptography. pp. 98–113. Springer International Publishing, Cham (2021)
4. Tao, C., Petzoldt, A., Ding, J.: Efficient key recovery for all HFE signature variants. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology – CRYPTO 2021. pp. 70–93. Springer International Publishing, Cham (2021)