SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

A study of the Kipnis-Shamir approach against the Rainbow signature scheme

Yasuhiko Ikematsu* Shuhei Nakamura †

Keywords: MinRank problem, Multivariate public key cryptography, Rainbow

Abstract

Rainbow is a multivariate signature scheme proposed by Ding et al. [3] in 2005. Due to its efficiency, the Rainbow scheme gets attention in the area of post-quantum cryptography (PQC) [1]. In fact, the Rainbow scheme is selected as a finalist candidate of NIST PQC standardization project [4]. The security of the Rainbow scheme mainly relates to the multivariate quadratic (MQ) problem and the MinRank problem. The MinRank problem is a problem to find a low-rank matrix by computing a linear combination from a set of matrices over a finite field and is known to be NP-hard. The Kipnis-Shamir (KS) approach [5] is one of the major approach to solve the MinRank problem. It tries to find a target low-rank matrix by solving the polynomial system (called KS system) obtained by treating kernel vectors of the target low-rank matrix as variables. Recently, Verbel et al. [6] gave a tighter complexity estimation for KS approach in 2019. They constructed explicit syzygies by focusing on the bilinear structure of KS system associated to random instances of the MinRank problem. In this paper, we consider the instances coming from the Rainbow scheme and study their complexity estimation. Moreover, we apply our result to the rectangular MinRank attack proposed by Beullens [2] in 2020.

References

[1] Bernstein, D.J., Buchmann J. and Dahmen, E. eds.: 'Post-Quantum Cryptography', Springer, 2009.

[2] Beullens W.: 'Improved Cryptanalysis of UOV and Rainbow', EUROCRYPT 2021, LNCS 12696, pp. 348–373, Springer

[3] Ding, J., Schmidt, D.S.: 'Rainbow, a new multivariate polynomial signature scheme', ACNS 2005, LNCS 3531, pp.164–175, Springer

[4] Ding, J., Chen, M.S., Petzoldt, A., Schmidt, D.S., Yang, B.Y.: 'Rainbow', Technical report, National Institute of Standards and Technology, *Post-Quantum Cryptography*, ⟨https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-3-submissions⟩

[5] Kipnis A., Shamir A.: 'Cryptanalysis of the hfe public key cryptosystem by relinearization', CRYPTO 99, LNCS 1666, pp. 19–30, Springer

[6] Verbel J.A, Baena J., Daniel Cabarcas D., Perlner R.A, Smith-Tone D.: 'On the Complexity of "Superdetermined" Minrank Instances', PQCrypto 2019, LNCS 11505, pp. 167–186, Springer

* Institute of Mathematics for Industry, Kyushu University 744, Motooka, Nishi-ku, Fukuoka 819–0395, Japan. ikematsu@imi.kyushu-u.ac.jp

† Department of Liberal Arts and Basic Sciences, Nihon University, 1-2-1 Izumi-cho, Narashino, Chiba 275-8575, Japan. nakamura.shuhei@nihon-u.ac.jp