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

多変数多項式署名 Rainbow に対する新たな乱数固定のフォルト攻撃
New Fault Attack on Rainbow by Fixing Randomness

加藤　拓 *　　清村　優太郎 †　　高木　剛 *
Taku Kato　　Yutaro Kiyomura　　Tsuyoshi Takagi

キーワード　耐量子計算機暗号, ディジタル署名, Rainbow, フォルト攻撃

あらまし

量子計算機の実用化に備えて, 近年では耐量子計算機暗号 (PQC) の研究が盛んである. 耐量子計算機暗号の一つに, 多変数多項式暗号という多変数多項式求解 (MQ) 問題の困難性に依拠した暗号がある. その中でもディジタル署名 Rainbow [2] は NIST の PQC 標準化プロジェクトの第三ラウンド最終候補に選出されるなど注目されている [7]. Rainbow は他の耐量子性を持つディジタル署名に比べて短い署名長を持つという特徴がある.

Rainbow は UOV を多層化した方式であり, Rank attacks [1], UOV attack [5], RBS attack [3] など多くの暗号解析の研究がなされている. 近年ではこれらの暗号解析に加えて, 物理的な攻撃, 特にサイドチャネル攻撃やフォルト攻撃に関する研究も行われている. フォルト攻撃は, 署名アルゴリズムに対して, アルゴリズム中の計算に故障を起こすという, サイドチャネル攻撃の一種である. 多変数多項式暗号に対するフォルト攻撃として, Hashimoto ら [4] は, 中心写像の成分の変更, 乱数の固定の二つの攻撃モデルを提案した. Krämer ら [6] は, Hashimoto らの結果を UOV や Rainbow に適用した場合の攻撃について解析をした. Shim ら [8] は, Rainbow の署名生成の際に用いる乱数に対するフォルト攻撃を提案した. Shim らはフォルト攻撃によって得られた情報から, 秘密鍵と等価な鍵を得る手法を提案し, その手法の計算量を評価した. Hashimoto ら, Krämer ら, Shim らの攻撃は, 変数の個数に対して指数時間の計算量が必要であった.

本研究では Rainbow に対するフォルト攻撃による新たな鍵回復攻撃を提案する. フォルト攻撃のモデルとしては Rainbow の署名生成の際に乱数固定のフォルト攻撃を行なう場合を考える. 本研究の成果は大きく分けて二つである. 一つ目は, 全ての乱数を固定した場合の鍵回復攻撃である. この場合には, good key を利用した新たな鍵回復攻撃を提案する. 提案手法では多項式時間にて鍵回復攻撃が可能であることを示した. 二つ目の成果は, 一部の乱数を固定した場合の鍵回復攻撃である. この場合には, フォルト攻撃によって得られた情報を利用することにより, 既存の Rainbow の攻撃手法 (MinRank attack, HighRank attack, UOV attack, RBS attack, Intersection attack, NewMinRank attack) がより小さい計算量となることを示した. 攻撃をする乱数の個数に応じて, 計算量が最も小さくなる手法は変化する. 128 ビットセキュリティのパラメータにおいて, この提案手法を Shim らが用いた手法と比べた場合, 計算量が約 2^{20} 倍削減されることを示した.

参考文献

[1] Beullens, W.: Improved cryptanalysis of UOV and Rainbow. In: EUROCRYPT 2021. LNCS 12696, pp. 348 - 373 (2021)
[2] Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: ACNS 2005. LNCS 3531, pp. 164 - 175 (2005)
[3] Ding, J., Yang, B.Y., Chen, C.H.O., Chen, M.S., Cheng, C.M.: New differential-algebraic attacks and reparametrization of Rainbow. In: ACNS 2008. LNCS 5037, pp. 242 - 257 (2008)
[4] Hashimoto, Y., Takagi, T., Sakurai, K.: General fault attacks on multivariate public key cryptosystems. In: PQCrypto 2011. LNCS 7071, pp. 1 - 18 (2011)
[5] Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: CRYPTO 1998. LNCS 1462, pp. 257 - 266 (1998)
[6] Krämer, J., Loiero, M.: Fault attacks on UOV and Rainbow. In: COSADE 2019. LNCS 11421, pp. 193 - 214 (2019)
[7] NIST: Post-quantum cryptography, round3 submissions (2020), https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
[8] Shim, K.A., Koo, N.: Algebraic fault analysis of UOV and rainbow with the leakage of random vinegar values. IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2429 - 2439 (2020)

* 東京大学大学院 情報理工学系研究科 数理情報学専攻 〒 113–8656 東京都文京区本郷 7-3-1, Department of Mathematical Informatics, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan
† NTT 社会情報研究所 〒 180-8585 東京都武蔵野市緑町 3-9-11, NTT Social Informatics Laboratories, 3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585, Japan