ULNERABILITY OF DIENE-THABET-YUSUF’S CUBIC MULTIVARIATE SIGNATURE SCHEME

Ryukyu Math. J., 34(2021), 1-4

VULNERABILITY OF DIENE-THABET-YUSUF'S CUBIC MULTIVARIATE SIGNATURE SCHEME *

Yasufumi Hashimoto

Abstract

In 2020, Diene, Thabet and Yusuf proposed a new multivariate signature scheme whose public key is a set of multivariate "cubic" polynomials over a finite field. In the present paper, we show how to recover its equivalent secret key.

Keywords. multivariate public-key cryptosystems, cubic polynomials

1 Introduction

A multivariate public key cryptosystem is a cryptosystem whose public key is a set of multivariate non-linear polynomials over a finite field, and has been considered to be a candidate of post-quantum cryptography. In fact, in NIST's standardization project of post-quantum cryptography, Rainbow [3] and GeMSS [2] were selected as a finalist and an alternative candidate respectively in the final (third) round [12].

Most multivariate public key cryptosystems, including these two signature schemes, are constructed by quadratic polynomials. One of the reasons why there have been few schemes with (over) cubic polynomials is that the number of coefficients in cubic polynomials is much more than that in quadratic polynomials and then the key size is much larger. While there might be a cubic type scheme which is secure enough to compensate for the disadvantage in efficiency, we do not have such schemes at the present time (see e.g. [9, 4, 10, 1, 11, 6, 7]). Recently, Diene-Thabet-Yusuf [5] proposed a multivariate signature scheme using cubic polynomials, whose signature generations are fast enough. However, such a structure for speeding up the signature generation has yielded a vulnerability. In the present paper, we show that how to recover its equivalent secret key of this signature scheme efficiently.

*Received November 30, 2021.

2 Diene-Thabet-Yusuf's signature scheme

We first describe the construction of Diene-Thabet-Yusuf's signature scheme [5].

Let q be a power of prime, $\mathbf{F}_q$ a finite field of order q and $r, m, n \geq 1$ integers with $m := r^2$, $n := 2r^2 = 2m$. Denote by $k_1(\mathbf{x}), \dots, k_n(\mathbf{x})$ linear polynomials of $\mathbf{x} = {}^t(x_1, \dots, x_n)$ and put

$$P = P(\mathbf{x}) := \begin{pmatrix} k_1(\mathbf{x}) \cdot k_{m+1}(\mathbf{x}) & k_{r+1}(\mathbf{x}) \cdot k_{m+r+1}(\mathbf{x}) & \cdots & k_{m-r+1}(\mathbf{x}) \cdot k_{n-r+1}(\mathbf{x}) \\ k_2(\mathbf{x}) \cdot k_{m+2}(\mathbf{x}) & k_{r+2}(\mathbf{x}) \cdot k_{m+r+2}(\mathbf{x}) & \cdots & k_{m-r+2}(\mathbf{x}) \cdot k_{n-r+2}(\mathbf{x}) \\ \vdots & \vdots & \ddots & \vdots \\ k_r(\mathbf{x}) \cdot k_{m+r}(\mathbf{x}) & k_{2r}(\mathbf{x}) \cdot k_{m+2r}(\mathbf{x}) & \cdots & k_m(\mathbf{x}) \cdot k_n(\mathbf{x}) \end{pmatrix}.$$

Generate an $r \times r$ matrix $M = M(\mathbf{x})$ whose entries are (constants or) linear polynomials of $\mathbf{x}$ such that the entries of M^{-1} are also (constants or) linear polynomials of $\mathbf{x}$. Define the cubic polynomial map $G : \mathbf{F}_q^n \to \mathbf{F}_q^m$, $G(\mathbf{x}) = {}^t(g_1(\mathbf{x}), \dots, g_m(\mathbf{x}))$ by

$$\begin{pmatrix} g_1(\mathbf{x}) & \cdots & g_{m-r+1}(\mathbf{x}) \\ \vdots & \ddots & \vdots \\ g_r(\mathbf{x}) & \cdots & g_m(\mathbf{x}) \end{pmatrix} = M(\mathbf{x}) \cdot P(\mathbf{x}).$$

Diene-Thabet-Yusuf's signature scheme is as follows [5].

Secret key: Two invertible affine maps $S : \mathbf{F}_q^n \to \mathbf{F}_q^n$, $T : \mathbf{F}_q^m \to \mathbf{F}_q^m$ and polynomial matrices P, M.

Public key: The cubic polynomial map

$$F := T \circ G \circ S : \mathbf{F}_q^n \to \mathbf{F}_q^m.$$

Signature generation: For a message $\mathbf{m} \in \mathbf{F}_q^m$, compute $\mathbf{y} = (y_1, \dots, y_m) := T^{-1}(\mathbf{m})$. Next choose $u_1, \dots, u_m \in \mathbf{F}_q$ randomly and find $\mathbf{x} \in \mathbf{F}_q^n$ satisfying

$$M(\mathbf{x})^{-1} \cdot \begin{pmatrix} y_1 & \cdots & y_{m-r+1} \\ \vdots & \ddots & \vdots \\ y_r & \cdots & y_m \end{pmatrix} = \begin{pmatrix} u_1 \cdot k_1(\mathbf{x}) & \cdots & u_{m-r+1} \cdot k_{m-r+1}(\mathbf{x}) \\ \vdots & \ddots & \vdots \\ u_r \cdot k_r(\mathbf{x}) & \cdots & u_m \cdot k_m(\mathbf{x}) \end{pmatrix},$$
$$(k_{m+1}(\mathbf{x}), \dots, k_{2m}(\mathbf{x})) = (u_1, \dots, u_m).$$

The signature for the message $\mathbf{m}$ is $\mathbf{s} = S^{-1}(\mathbf{x})$.

Signature verification: Verify whether $F(\mathbf{s}) = \mathbf{m}$ holds.

Since M is generated such that the entries of $M(\mathbf{x})^{-1}$ are (constants or) linear polynomials, the signature generation requires only solving a system of n linear equations of n variables. The complexity of the signature generation is thus $O(n^3)$.

3 Key recovery attack on DTY signature scheme

We now propose our key recovery attack on Diene-Thabet-Yusuf's signature scheme.

Let $K : \mathbf{F}_q^n \to \mathbf{F}_q^n$ be the linear map with $K(\mathbf{x}) = (k_1(\mathbf{x}), \dots, k_n(\mathbf{x}))$, $\tilde{P} : \mathbf{F}_q^n \to \mathbf{F}_q^m$ the quadratic polynomial map with

$$\tilde{P}(\mathbf{x}) = {}^t\!(p_1(\mathbf{x}), \dots, p_m(\mathbf{x})) := {}^t\!(x_1 \cdot x_{m+1}, \dots, x_m \cdot x_n)$$

and $\tilde{M}(\mathbf{x}) := \begin{pmatrix} M(\mathbf{x}) & & \\ & \ddots & \\ & & M(\mathbf{x}) \end{pmatrix}$. It is easy to see that

$$G(\mathbf{x}) = \tilde{M}(\mathbf{x})\tilde{P}(K(\mathbf{x})),$$

and then

$$F(\mathbf{x}) = (T\tilde{M}(\mathbf{x}))\tilde{P}((K(S(\mathbf{x}))).$$

Since T, K, S are affine maps and the entries of $\tilde{M}^{-1}$ are (constants or) linear polynomials of $\mathbf{x}$, there exist an $m \times m$ matrix $L = L(\mathbf{x})$ whose entries are (constants or) linear polynomials and quadratic polynomials $h_1(\mathbf{x}), \dots, h_m(\mathbf{x})$ such that

$$L(\mathbf{x})F(\mathbf{x}) = {}^t\!(h_1(\mathbf{x}), \dots, h_m(\mathbf{x})).$$

We can easily check that one can find such an L in polynomial time and the quadratic polynomials $h_1(\mathbf{x}), \dots, h_m(\mathbf{x})$ are linear sums of $p_1((K(S(\mathbf{x}))), \dots,$ $p_m((K(S(\mathbf{x})))$. Then the coefficient matrices of $h_1(\mathbf{x}), \dots, h_m(\mathbf{x})$ are in the forms

$${}^t\!(KS) \begin{pmatrix} 0_m & * \\ * & 0_m \end{pmatrix} (KS).$$

This means that the polynomials $h_1(\mathbf{x}), \dots, h_m(\mathbf{x})$ are the balanced oil-vinegar type and then that Kipnis-Shamir's attack on the (balanced) oil-vinegar signature scheme [13, 8, 9] is available for $(h_1(\mathbf{x}), \dots, h_m(\mathbf{x}))$. We can recover a linear map $S_1 : \mathbf{F}_q^n \to \mathbf{F}_q^n$ satisfying

$$(KS)S_1 = \begin{pmatrix} *_m & * \\ 0 & *_m \end{pmatrix}$$

in polynomial time. It is easy to see that the quadratic polynomials in $L(\mathbf{x})F(S_1(\mathbf{x}))$ are in the forms

$${}^t\mathbf{x} \begin{pmatrix} 0_m & * \\ * & *_m \end{pmatrix} \mathbf{x} + (\text{linear polynomial of } \mathbf{x}).$$

This is equivalent to the polynomials in the balanced oil-vinegar signature scheme [13]. We thus conclude that the attacker can generate dummy signatures for arbitrary messages feasibly and this signature scheme is not secure at all.

Acknowledgments. The author was supported by JST CREST no. JPMJCR2113 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

[1] J. Baena, D. Cabarcas, D.E. Escudero, K. Khathuria, J. Verbel, *Rank analysis of cubic multivariate cryptosystems*, PQCrypto'18, LNCS **10786** (2018), pp. 355–374.

[2] A. Casanova, J.C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem, *GeMSS: A Great Multivariate Short Signature, Rainbow Signature*, `https://www-polsys.lip6.fr/Links/NIST/GeMSS.html`.

[3] J. Ding, M.-S. Chen. A. Petzoldt, D. Schmidt, B.-Y. Yang, M. Kannwischer J. Patarin, *Rainbow Signature*, `https://www.pqcrainbow.org/`.

[4] J. Ding, A. Petzoldt, L.-C. Wang, *The cubic simple matrix encryption scheme*, PQCrypto'14, LNCS **8772** (2014), pp. 76–87.

[5] A. Diene, S.A. Thabet, Y. Yusuf, *A multivariate signature based on block matrix multiplication*, `https://www.preprints.org/manuscript/202004.0392/v1`, 2020.

[6] D.H. Duong, A. Petzoldt, Y. Wang, T. Takagi, *Revisiting the cubic UOV signature scheme*, ICISC'16, Springer LNCS **10157** (2016), pp. 223–238.

[7] Y. Hashimoto, *Weaknesses of cubic UOV and its variants*, Ryukyu Mathematical Journal **30** (2017), pp. 1–7.

[8] A. Kipnis, A. Shamir, *Cryptanalysis of the oil and vinegar signature scheme*, Crypto'98, LNCS **1462** (1998), pp. 257–267.

[9] A. Kipnis, J. Patarin, L. Goubin, *Unbalanced oil and vinegar signature schemes*, Eurocrypt'99, LNCS **1592** (1999), pp. 206–222, extended in `http://www.goubin.fr/papers/OILLONG.PDF`, 2003.

[10] D. Moody, R. Perlner, D. Smith-Tone, *Improved attacks for characteristic-2 parameters of the cubic ABC simple matrix encryption scheme*, PQCrypto'17, LNCS **10346** (2017), pp. 255–271.

[11] X. Nie, B. Liu, H. Xiong, G. Lu, *Cubic unbalance oil and vinegar signature scheme*, Inscrypt 2015, Springer LNCS **9589** (2015), pp. 47–56.

[12] NIST, *Post-Quantum Cryptography Standardization, Round 3 Submissions*, `https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions`.

[13] J. Patarin, *The Oil and Vinegar Signature Scheme*, the Dagstuhl Workshop on Cryptography, 1997.

Department of Mathematical Sciences,
Faculty of Science,
University of the Ryukyus,
Senbaru 1, Nishihara, Okinawa 903-0213
JAPAN