On the security of Diene-Thabet-Yusuf's cubic multivariate signature scheme

Yasufumi Hashimoto *

Abstract

Diene, Thabet and Yusuf recently proposed a new multivariate signature scheme whose public key is a set of multivariate cubic polynomials over a finite field. This paper studies its security.

Keywords. multivariate public-key cryptosystems, cubic polynomials

1 Diene-Thabet-Yusuf's signature scheme

This paper studies the security of Diene-Thabet-Yusuf's signature scheme [3] proposed recently. We first describe its construction.

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 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 [3].

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

*Department of Mathematical Science, University of the Ryukyus, hashimoto@math.u-ryukyu.ac.jp

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 $O(n^3)$.

2 On the security of DTY signature scheme

We now study the security of 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 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 Kipnis-Shamir's attack on the (balanced) oil-vinegar signature scheme [2, 1] is available for $(h_1(\mathbf{x}), \dots, h_m(\mathbf{x}))$ and it recovers 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

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

We thus conclude that the attacker can generate dummy signatures for arbitrary messages feasibly and this signature scheme is not secure enough.

Acknowledgments. The author was supported by JST CREST no. JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

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

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

[3] A. Diene, S.A. Thabet, Y. Yusuf, A multivariate signature based on block matrix multiplication, Preprints **2020**, 2020040392, doi: 10.20944/preprints202004.0392.v1.