On the security of new vinegar-like variant of multivariate signature scheme

Yasufumi Hashimoto *

Abstract

In IMACC 2015 and Inscrypt 2015, Zhang and Tan proposed new vinegar-like variants of multivariate signature schemes. While their aims were to enhance the security of broken schemes, the security is much less than expected. In this note, we describe how to recover a public key of the original scheme.

Keywords. multivariate public-key cryptosystems, new vinegar-like variant

1 Introduction

In IMACC 2015 and Inscrypt 2015, Zhang and Tan [6, 7] proposed new vinegar-like variants of MI-T [5] and YTS [4] of even characteristic field. It was claimed that, while the original schemes were already broken [6, 1], their variants were secure enough. However, the security is much less than expected. In this note, we describe how to recover a public key of the original scheme.

2 Multivariate Public Key Cryptosystem

In this section, we describe multivariate public key cryptosystems (MPKCs) in general.

Let $n, m \geq 1$ be integers, k a finite field and $q := \#k$. The *secret key* is a tuple of three maps (S, G, T), where $S : k^n \to k^n$, $T : k^m \to k^m$ are invertible affine maps and $G : k^n \to k^m$ is a quadratic map *inverted feasibly*. The *public key* is the convolution of these three maps

$$F := T \circ G \circ S : k^n \to k^m.$$

On the encryption scheme, the *cipher* $y \in k^m$ for a given plain-text $x \in k^n$ is computed by $y = F(x)$. To *decrypt* y, find $z \in k^n$ such that $G(z) = T^{-1}(y)$. Then the plain-text is $x = S^{-1}(z)$. Since G is *inverted feasibly*, one can decrypt y feasibly.

On the signature scheme, the signature generation of $y \in k^m$ is similar to the decryption in the encryption scheme. The signature $x \in k^n$ for y is *verified* by $y = F(x)$.

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

3 New vinegar-like variant

In this section, we describe Zhang-Tan's a new vinegar-like variant [6, 7].

Let $l, d \geq 1$ be integers and K an l-extension of k. Define the maps $\mathcal{G}_1 : K^2 \to K$ and $G_1 : k^{n+l} \to k^l$ by

$$\mathcal{G}_1(X_1, X_2) := \sum_{0 \leq i \leq j \leq d} a_{ij} X_2^{q^i+q^j} + \sum_{\substack{0 \leq i \leq d \\ 0 \leq j \leq l-1}} b_{ij} X_1^{q^j} X_2^{q^i} + \sum_{0 \leq i \leq d} c_i X_2^{q^i},$$

$$G_1 := \phi^{-1} \circ \mathcal{G}_1 \circ \phi_2 \circ (T_1 \oplus I_l),$$

where $a_{ij}, b_{ij}, c_i \in K$, $\phi : k^l \to K$, $\phi_2 : k^{2l} \to K^2$ are one-to-one maps and $T_1 : k^n \to k^l$ is a linear map. For a quadratic map $G : k^n \to k^m$ inverted feasibly, the map $\hat{G} : k^{n+l} \to k^m$ is given as follows.

$$\hat{G}(x) = G(\mathrm{x}_1) + T_2 G_1(x),$$

where $\mathrm{x}_1 = (x_1, \ldots, x_n)^t$ for $x = (x_1, \ldots, x_{n+l})^t$ and $T_2 : k^l \to k^m$ is an invertible linear map. Zhang-Tan's new vinegar-like variant [6, 7] is as follows.

Secret key. Two affine maps $\hat{S} : k^{n+l} \to k^{n+l}$, $T : k^m \to k^m$, a quadratic map $G : k^n \to k^m$ inverted feasibly, the map $\mathcal{G}_1 : K^2 \to K$ and linear maps T_1, T_2.

Public key. The quadratic map

$$\hat{F} := T \circ \hat{G} \circ \hat{S} : k^{n+l} \to k^m.$$

Signature generation. Let $y \in k^n$ be a message to be signed. First compute $z := T^{-1}(y)$, Next, find $\mathbf{w}_1 \in k^n$ with $G(\mathbf{w}_1) = z$, and $\mathbf{w}_2 \in k^l$ with $G_1(\mathbf{w}_1, \mathbf{w}_2) = 0$. The signature is $x = \hat{S}^{-1}\left(\begin{smallmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \end{smallmatrix}\right)$.

Signature verification. Verify whether $\hat{F}(x) = y$ holds.

Note that $\mathbf{w}_2$ with $G_1(\mathbf{w}_1, \mathbf{w}_2) = 0$ is computed by a univariate polynomial equation derived from $\mathcal{G}_1$ of degree at most $2q^d$. If there are no non-trivial solution, $X_2 = 0$ is acceptable as a solution.

4 Recovering a public key of the original scheme

We now give an attack to recover a public key of the original scheme from the public key of vinegar variant.

Step 1. Choose sufficiently many messages $y_1, \ldots, y_N \in k^m$ randomly and generate their signatures $x_1, \ldots, x_N \in k^{n+l}$. Find l linearly independent quadratic forms $h_1(x), \ldots, h_t(x)$ such that $h_i(x_j) = 0$ for any $1 \leq j \leq N$.

Due to the equation $G_1(\mathbf{w}_1, \mathbf{w}_2) = 0$ in the signature generation, we see that there exist such l-linearly independent quadratic forms and they are linear sums of the quadratic forms in $G_1(S(x))$. Since the number of the coefficients of $h_i(x)$ is about $\frac{1}{2}(n+l)^2$, we need $N \gg \frac{1}{2}(n+l)^2$.

Step 2. Find an $l \times n$ matrix M such that

$$h_i\left(\begin{pmatrix} I_n & \\ M & I_l \end{pmatrix} x\right) = \sum_{1 \le i \le n} x_i \cdot (\text{linear form of } x_{n+1}, \ldots, x_{n+l}) + (\text{quadratic form of } x_{n+1}, \ldots, x_{n+l}) \tag{1}$$

for $1 \le i \le l$.

By the construction of $\mathcal{G}_1$ and G_1, we see that the coefficient matrices of the quadratic forms in G_1 are in the form $\left(\begin{smallmatrix} 0_n & * \\ * & *_l \end{smallmatrix}\right)$. Then Kipnis-Shamir's attack on the (unbalanced) oil-vinegar signature scheme [3, 2] can recover M with the complexity $O(q^{\max(l-n,0)} \cdot (\text{polyn.}))$ and M satisfies

$$\hat{S}\begin{pmatrix} I_n & \\ M & I_l \end{pmatrix} = \begin{pmatrix} *_n & * \\ 0 & *_l \end{pmatrix}. \tag{2}$$

Step 3. Let $f'_i(x) := f_i\left(\left(\begin{smallmatrix} I_n & \\ M & I_l \end{smallmatrix}\right)x\right)$ and $h'_i(x) := h_i\left(\left(\begin{smallmatrix} I_n & \\ M & I_l \end{smallmatrix}\right)x\right)$. Find an $n \times l$ matrix B such that the polynomials $f''_1(x), \ldots, f''_n(x)$ given by

$$\left(f''_1(x), \ldots, f''_n(x)\right)^t := (I_n, B_1)\left(f'_1(x), \ldots, f'_n(x), h'_1(x), \ldots, h'_l(x)\right)^t$$

are quadratic forms of $x_1, \ldots, x_n$.

Since G is a set of quadratic forms of $x_1, \ldots, x_n$, G_1 is a set of quadratic forms of $x_1, \ldots, x_{n+l}$ in the form (1) and M satisfies (2), there exists such a matrix B. It is easy to see that the set $(f''_1(x), \ldots, f''_n(x))^t$ is a public key of the original scheme. □

5 Conclusion

In this note, we describe how to recover the original scheme from Zhang-Tan's new vinegar-like variant. Its complexity is roughly estimated by $O(q^{\max(l-n,0)} \cdot (\text{polyn.}))$. This means that the security of this variant is much less than expected ($O(q^l)$, [7]), and one must take l sufficiently larger than n. We thus conclude that this variant is not practical.

Acknowledgment. This work was supported by CREST, JST and JSPS Grant-in-Aid for Young Scientists (B) no. 26800020.

References

[1] Y. Hashimoto, Cryptanalysis of the multivariate signature scheme proposed in PQCrypto 2013, PQCrypto'14, LNCS **8772** (2014), pp.108–125, IEICE Trans. Fundamentals, **99-A** (2016), pp.58–65.

[2] A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, Eurocrypt'99, LNCS **1592** (1999), pp.206–222, extended in citeseer/231623.html, 2003-06-11.

[3] A. Kipnis, A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, Crypto'98, LNCS **1462** (1998), pp.257–266.

[4] T. Yasuda, T. Takagi, K. Sakurai, Multivariate signature scheme using quadratic forms. PQCrypto'13, LNCS **7932** (2013), pp.243–258.

[5] W. Zhang, C.H. Tan, A new perturbed Matsumoto-Imai signature scheme, AsiaPKC'14, Proc. 2nd ACM Workshop on AsiaPKC (2014), pp.43–48.

[6] W. Zhang, C.H. Tan, MI-T-HFE, A new multivariate signature scheme, IMACC'15, LNCS **9496**, (2015), pp.43–56.

[7] W. Zhang, C.H. Tan, A secure variant of Yasuda, Takagi and Sakurai's signature scheme, Inscrypt'15, LNCS **9589** (2015), pp.75-89