Ryukyu Math. J., 31(2018), 1-5

ON THE SECURITY OF ZHANG-TAN'S VARIANTS OF MULTIVARIATE SIGNATURE SCHEMES *

Yasufumi HASHIMOTO

Abstract

Until now, various multivariate public key cryptosystems (MPKCs) have been proposed but some of them are known to be insecure. In IMACC 2015 and Inscrypt 2015, Zhang and Tan proposed new variants of MPKCs for signatures to enhance the security of the original schemes. However, Zhang-Tan's variants are much less secure than expected. In this paper, we describe an attack on Zhang-Tan's variants to recover a public key of the original scheme.

1 Introduction

After Shor [6] proposed polynomial-time algorithms to factor integers and to solve discrete logarithm problems by quantum computers, constructing cryptosystems secure against quantum attacks is one of big issues in cryptology. *Multivariate public key cryptosystems (MPKCs)*, public key cryptosystems whose public keys are sets of multivariate quadratic forms over finite fields, have been expected to be such cryptosystems. While various MPKCs have been proposed until now, some of them were broken soon after proposed or known to be much less secure than expected.

In IMACC 2015 and Inscrypt 2015, Zhang and Tan [9, 10] proposed a new idea to repair such insecure MPKCs for signatures. Their idea is adding several variables and terms for the additional variables on the original polynomials, and hiding several equations to eliminate the contributions of additional variables in the process of signature generation. They actually used this idea on already broken schemes MI-T [8] and YTS [7, 2] by adding HFE-like polynomials and claimed that this idea enhanced the security drastically. However, the hidden equations can be recovered by sufficiently many signatures and these equations tell us partial information of the secret key. In this paper, we describe how to recover the hidden equations and the secret key partially, and conclude that our attack removes the contributions of the additional variables and recovers a public key of the original scheme.

*Received November 30, 2018

2 Multivariate Public Key Cryptosystem

In this section, we describe the general construction of multivariate public key cryptosystems (MPKCs).

Let $n, m \geq 1$ be integers, k a finite field and $q := \#k$. Define a quadratic map $G : k^n \to k^m$ to be inverted feasibly, i.e. finding $\mathbf{x} \in k^n$ with $G(\mathbf{x}) = \mathbf{y}$ is feasible for any (or most) $\mathbf{y} \in k^m$. 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 the quadratic map $G : k^n \to k^m$. The *public key* is the convolution of these three maps

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

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

On a signature scheme, a signature $\mathbf{x} \in k^n$ for a given message $\mathbf{y} \in k^m$ is generated as follows. Find $\mathbf{z} \in k^n$ with $G(\mathbf{z}) = \mathbf{y}$ and compute $\mathbf{x} = S^{-1}(\mathbf{z})$. The signature $\mathbf{x} \in k^n$ for $\mathbf{y}$ is verified if $\mathbf{y} = F(\mathbf{x})$ holds.

3 Zhang-Tan's variant

In this section, we describe Zhang-Tan's variant [9, 10] on MPKC.

Let $n, n_0, m, l \geq 1$ be integers with $n = n_0 + l$ and $\mathbf{x} = {}^t(x_1, \ldots, x_n)$, $\mathbf{x}_1 = {}^t(x_1, \ldots, x_{n_0})$, $\mathbf{x}_2 = {}^t(x_{n_0+1}, \ldots, x_n)$ are variables. Define the quadratic maps $G : k^n \to k^m$, $H : k^n \to k^l$ by

$$\begin{aligned} G(\mathbf{x}) &= {}^t(g_1(\mathbf{x}), \ldots, g_m(\mathbf{x})), \\ H(\mathbf{x}) &= {}^t(h_1(\mathbf{x}), \ldots, h_l(\mathbf{x})), \end{aligned}$$

where $g_1(\mathbf{x}), \ldots, g_m(\mathbf{x})$ are quadratic forms of $\mathbf{x}_1$ and

$$\begin{aligned} h_i(\mathbf{x}) =& (\text{homogeneous quadratic form of } \mathbf{x}_2) \\ &+ \sum_{1 \leq j \leq l} x_{n_0+j} \cdot (\text{linear form of } \mathbf{x}_1), \qquad (1 \leq i \leq l). \end{aligned} \tag{1}$$

Suppose that G, H are inverted feasibly, i.e. finding $\mathbf{x}_1 \in k^{n_0}$ with $G(\mathbf{x}_1) = \mathbf{y}$ is feasible for any (or most) $\mathbf{y} \in k^m$ and finding $\mathbf{x}_2 \in k^l$ with $H(\mathbf{x}_1, \mathbf{x}_2) = 0$ is also feasible for any (or most) $\mathbf{x}_1 \in k^{n_0}$. In [9, 10], G is the central map of MI-T [8] or YTS [7] and H is given by an HFE-like polynomial.

Zhang-Tan's variant is given as follows.

Secret key. Two invertible affine maps $S : k^n \to k^n$, $T : k^m \to k^m$, a linear map $T_1 : k^l \to k^m$ and the quadratic maps $G : k^n \to k^m$, $H : k^n \to k^l$ defined above.

Public key. The quadratic map $F : k^n \to k^m$ defined by

$$F := (T \circ G + T_1 \circ H) \circ S.$$

Signature generation. For a message $\mathbf{y} \in k^m$ to be signed, find $\mathbf{z}_1 \in k^{n_0}$ with $G(\mathbf{z}_1) = T^{-1}(\mathbf{y})$, and $\mathbf{z}_2 \in k^l$ with $H(\mathbf{z}_1, \mathbf{z}_2) = 0$. The signature is $\mathbf{w} = S^{-1}(\mathbf{z}_1, \mathbf{z}_2)$.

Signature verification. The signature $\mathbf{w}$ is verified if $F(\mathbf{w}) = \mathbf{y}$ holds.

Since $G(\mathbf{x})$ is a set of quadratic forms of $\mathbf{x}_1$ and is constructed to be inverted feasibly, $\mathbf{z}_1$ is found feasibly. Similarly, finding $\mathbf{z}_2$ is also feasible. Note that H is constructed such that $H(\mathbf{x}_1, 0) = 0$ for any $\mathbf{x}_1$. Then $\mathbf{z}_2 = 0$ is acceptable in the process of signature generation if there are no non-trivial $\mathbf{z}_2$ for a given $\mathbf{z}_1$.

4 On the security of Zhang-Tan's variant

In this section, we propose our attack to reduce the problem of solving $F(\mathbf{x}) = \mathbf{y}$ to the problem of solving $F_0(\mathbf{x}_1) = \mathbf{y}_1$ where $F_0 := T \circ G \circ S_0$ is a public key of the original scheme derived from G, where $S_0 : k^{n_0} \to k^{n_0}$ is an invertible affine map. For simplicity, we assume that S is a linear map.

First, recall that one finds $\mathbf{z}_1, \mathbf{z}_2$ with $H(\mathbf{z}_1, \mathbf{z}_2) = 0$ in the process of signature generation, and the signature $\mathbf{w}$ satisfies $(\mathbf{z}_1, \mathbf{z}_2) = S(\mathbf{w})$. Then $H \circ S(\mathbf{w}) = 0$ holds for any signature $\mathbf{w}$ generated by the corresponding Zhang-Tan's variant. This means that there are l-linearly independent quadratic forms $u_1(\mathbf{x}), \ldots, u_l(\mathbf{x})$ with $u_i(\mathbf{w}) = 0$ for any signature $\mathbf{w}$ and these quadratic forms are linear sums of $h_1(S(\mathbf{x})), \ldots, h_l(S(\mathbf{x}))$. Since h_i is a quadratic form of n variables, we can recover $u_1(\mathbf{x}), \ldots, u_l(\mathbf{x})$ by $N \gg \frac{1}{2}n(n+1)$ signatures.

By the construction (1) of H, we see that the polynomials $u_i(\mathbf{x})$ are written by

$$u_i(\mathbf{x}) = {}^t\mathbf{x}\, {}^tS \begin{pmatrix} 0_{n_0} & * \\ * & *_l \end{pmatrix} S\mathbf{x} + (\text{linear form})$$

for $1 \le i \le l$. This is similar to the quadratic form in UOV [5, 3] and then, once $u_1(\mathbf{x}), \ldots, u_l(\mathbf{x})$ are given, the attacker can recover an invertible linear map $S_1 : k^n \to k^n$ with $SS_1 = \begin{pmatrix} *_{n_0} & * \\ 0 & *_l \end{pmatrix}$ by Kipnis-Shamir's attack on UOV [4, 3] in time $O(q^{\max(0, l-n_0)} \cdot (\text{polyn.}))$.

Since $\bar{F} := F \circ S_1 = (T \circ G + T_1 \circ H) \circ (S \circ S_1)$ and $SS_1 = \begin{pmatrix} S_0 & * \\ 0 & *_l \end{pmatrix}$ with some $n_0 \times n_0$ matrix S_0, we see that $H \circ (S \circ S_0)$ is a set of quadratic forms as given in (1). Then we have $\bar{F}(\mathbf{x}_1, 0) = (T \circ G \circ S_0)(\mathbf{x}_1)$, which is a public key of the original scheme derived from G. We thus conclude that Zhang-Tan's variant does not protect the original scheme strongly.

Our attack is summarized as follows.

Step 1. Let N be an integer sufficiently larger than $\frac{1}{2}n(n+1)$. Choose N messages $\mathbf{y}_1, \ldots, \mathbf{y}_N \in k^m$ randomly, and generate signatures $\mathbf{w}_1, \ldots, \mathbf{w}_N \in k^n$ for $\mathbf{y}_1, \ldots, \mathbf{y}_N \in k^m$ respectively.

Step 2. Find l linearly independent quadratic forms $u_1(\mathbf{x}), \ldots, u_l(\mathbf{x})$ with $u_i(\mathbf{w}_j) = 0$ for any $1 \leq j \leq N$.

Step 3. Find an invertible linear map $S_1 : k^n \to k^n$ with

$$u_i(S_1(\mathbf{x})) = {}^t\mathbf{x} \begin{pmatrix} 0_{n_0} & * \\ * & *_l \end{pmatrix} \mathbf{x} + (\text{linear form})$$

for $1 \leq i \leq l$ by Kipnis-Shamir's attack [4, 3].

Step 4. Let $\bar{F} := F \circ S_1$. Then $\bar{F}(\mathbf{x}_1, 0)$ is a public key of the original scheme.

As already explained, the complexity of Step 3 is $O(q^{\max(0,l-n_0)} \cdot (\text{polyn.}))$. It is easy to see that the complexities of other steps of our attack are in polynomial time. Then the total complexity of our attack is $O(q^{\max(0,l-n_0)} \cdot (\text{polyn.}))$, which is much less than $O(q^l \cdot (\text{polyn.}))$ expected by Zhang and Tan [9, 10]. This means that l must be sufficiently larger than n_0, namely the number n of variables in Zhang-Tan's variant must be sufficiently larger than twice of the number n_0 of the variables in the original scheme. This situation is similar to UOV [3], and we can consider that Zhang-Tan's variant does not have an advantage over UOV. Furthermore, the complexity $O(q^{\max(0,l-n_0)} \cdot (\text{polyn.}))$ might be improved if H has a special structure. For example, when H is given by an HFE-like polynomial [9, 10], the rank attack [1] will reduce the complexity. We thus conclude that Zhang-Tan's variant is not practical at all.

Acknowledgment. This work was supported by JST CREST Grant Number JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

[1] L. Bettale, J.C. Faugere, L. Perret, Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic, Designs, Codes and Cryptography **69** (2013), pp.1-52.

[2] 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.

[3] 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.

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

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

[6] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing **26** (1997), pp.1484–1509.

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

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

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

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

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