On the modifier Q for multivariate signature schemes

Yasufumi Hashimoto *

Abstract

At PQCrypto 2021, Smith-Tone proposed a new modifier, called "Q", to construct a fast multivariate signature scheme from a known scheme. In the present paper, we propose an idea to weaken the security of this modifier.

Keywords. multivariate public-key cryptosystems, modifier Q

1 Multivariate signature scheme and Modifier Q

We first describe the basic construction of multivariate signature schemes and the modifier Q proposed in [4].

1.1 Basic constructions

Let $n, m \geq 1$ be integers, q a power of prime and $\mathbf{F}_q$ a finite field of order q. There have been various multivariate signature schemes and most of them are constructed as follows.

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 a quadratic map $F : \mathbf{F}_q^n \to \mathbf{F}_q^m$ to be inverted feasibly.

Public key. The quadratic map $P := T \circ F \circ S : \mathbf{F}_q^n \to \mathbf{F}_q^m$.

Signature generation. For a message $\mathbf{m} \in \mathbf{F}_q^m$, compute $\mathbf{z} := T^{-1}(\mathbf{m})$ and find $\mathbf{y} \in \mathbf{F}_q^n$ with $F(\mathbf{y}) = \mathbf{z}$. Then the signature is $\mathbf{s} = S^{-1}(\mathbf{y})$.

Signature verification. The signature $\mathbf{s} \in \mathbf{F}_q^n$ is verified by $\mathbf{m} = P(\mathbf{s})$.

1.2 Modifier Q

Smith-Tone's new modifier "Q" [4] is to construct a signature scheme from a known multivariate scheme in the following way.

Let $f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})$ be the quadratic polynomials of $\mathbf{x} = (x_1, \ldots, x_n)$ in $F(\mathbf{x})$ defined in §1.1. For a small integer $l \geq 1$, prepare the new variables $\mathbf{w} = (w_1, \ldots, w_l)$ and $\mathbf{z} = (z_{11}, \ldots, z_{1l}, z_{21}, \ldots, \ldots, z_{nl})$. Multiply $w_1, \ldots, w_l$ to the coefficients of $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ and put them $\tilde{f}_1(\mathbf{x}, \mathbf{w}), \ldots, \tilde{f}_m(\mathbf{x}, \mathbf{w})$. Replace $x_i w_k$ in $\tilde{f}$'s to z_{ik}, add linear sums of $\{x_i z_{jk} - x_j z_{ik}\}_{1 \leq i,j \leq n, 1 \leq k \leq l}$, $\{z_{ik} z_{jr} - z_{jk} z_{ir}\}_{1 \leq i,j \leq n, 1 \leq k,r \leq l}$, and put them $\hat{f}_1(\mathbf{x}, \mathbf{z}), \ldots, \hat{f}_m(\mathbf{x}, \mathbf{z})$. Define the quadratic maps $\tilde{F} : \mathbf{F}_q^{n+l} \to \mathbf{F}_q^m$ and $\hat{F} : \mathbf{F}_q^{(l+1)n} \to \mathbf{F}_q^m$ by $\tilde{F}(\mathbf{x}, \mathbf{w}) = (\tilde{f}_1(\mathbf{x}, \mathbf{w}), \ldots, \tilde{f}_m(\mathbf{x}, \mathbf{w}))$ and $\hat{F}(\mathbf{x}, \mathbf{z}) = (\hat{f}_1(\mathbf{x}, \mathbf{z}), \ldots, \hat{f}_m(\mathbf{x}, \mathbf{z}))$ respectively. The modifier Q is constructed as follows.

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

Secret key. Two invertible affine maps $\hat{S} : \mathbf{F}_q^{(l+1)n} \to \mathbf{F}_q^{(l+1)n}$, $T : \mathbf{F}_q^m \to \mathbf{F}_q^m$ and the quadratic map $\tilde{F} : \mathbf{F}_q^{n+l} \to \mathbf{F}_q^m$ defined above.

Public key. The quadratic map $\hat{P} := T \circ \hat{F} \circ \hat{S} : \mathbf{F}_q^{(l+1)n} \to \mathbf{F}_q^m$.

Signature generation. For a message $\mathbf{m} \in \mathbf{F}_q^m$, compute $\mathbf{u} = T^{-1}(\mathbf{m})$. Choose $\mathbf{w} \in \mathbf{F}_q^l$ randomly and find $\mathbf{y} \in \mathbf{F}_q^n$ with $\tilde{F}(\mathbf{y}, \mathbf{w}) = \mathbf{u}$. The signature is $\mathbf{s} = S^{-1}(\mathbf{y}, \mathbf{y} \otimes \mathbf{w}) \in \mathbf{F}_q^{(l+1)n}$.

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

Since $(\mathbf{x}, \mathbf{z}) = (\mathbf{y}, \mathbf{y} \otimes \mathbf{w})$ in the signature generation satisfies

$$x_i z_{jk} - x_j z_{ik} = 0, \qquad z_{ik} z_{jr} - z_{jk} z_{ir} = 0 \tag{1}$$

for $1 \le i, j \le n, 1 \le k, r \le l$, these terms in $\hat{f}_1(\mathbf{x}, \mathbf{z}), \ldots, \hat{f}_m(\mathbf{x}, \mathbf{z})$ vanish and the signature $\mathbf{s} = S^{-1}(\mathbf{y}, \mathbf{y} \otimes \mathbf{w})$ satisfies $\hat{P}(\mathbf{s}) = \mathbf{m}$. While such hidden equations (1) contribute to speed up the signature generation, they give a big hint to break the modifier Q such as the hidden equations in Zhang-Tan's variant [5, 6, 1] and ELSA [3, 2]. In the next section, we describe how to weaken the security of this modifier.

2 Proposed attack

Let $u_{ijk}(\mathbf{x}, \mathbf{z}) := x_i z_{jk} - x_j z_{ik}$ and $v_{ijkr}(\mathbf{x}, \mathbf{z}) := z_{ik} z_{jr} - z_{jk} z_{ir}$ for $1 \le i, j \le n$, $1 \le k, r \le l$. Due to (1), we see that any signature $\mathbf{s}$ satisfies $u_{ijk}(\hat{S}(\mathbf{s})) = 0$ and $v_{ijkr}(\hat{S}(\mathbf{s})) = 0$. Then, if the attacker has sufficiently many (probably more than $\frac{1}{2}(l+1)n((l+1)n+1)$) signatures, he/she can recover linearly independent quadratic polynomials $h_1(\mathbf{x}, \mathbf{z}), \ldots, h_M(\mathbf{x}, \mathbf{z})$, which are expected to be linear sums of $u_{ijk}(\hat{S}(\mathbf{x}, \mathbf{z}))$ and $v_{ijkr}(\hat{S}(\mathbf{x}, \mathbf{z}))$. Note that M is the number of $u_{ijk}(\mathbf{x}, \mathbf{z})$ and $v_{ijkr}(\mathbf{x}, \mathbf{z})$, namely $M = \frac{1}{4} l(l+1)n(n+1)$. These polynomials will help the attacker to break Q in the following ways.

1. Direct attack. The direct attack is to generate a dummy signature for a given message $\mathbf{m} \in \mathbf{F}_q^m$ by solving the system $\{\hat{P}(\mathbf{x}, \mathbf{z}) = \mathbf{m}\}$ of quadratic equations directly. If the attacker has $h_1, \ldots, h_M$, he/she can generate it by solving the system $\{\hat{P}(\mathbf{x}, \mathbf{z}) = \mathbf{m}, h_1(\mathbf{x}, \mathbf{z}) = 0, \ldots, h_M(\mathbf{x}, \mathbf{z}) = 0\}$. It is (probably) more efficient than the direct attack without h's.

2. Rank attack I. Since the coefficient matrices of $u_{ijk}(\hat{S}(\mathbf{x}, \mathbf{z}))$, $v_{ijkr}(\hat{S}(\mathbf{x}, \mathbf{z}))$ are of rank 4, there exist $a_1, \ldots, a_M \in \mathbf{F}_q$ such that the coefficient matrix of

$$a_1 h_1(\mathbf{x}, \mathbf{z}) + \cdots + a_M h_M(\mathbf{x}, \mathbf{z}) =: b(\mathbf{x}, \mathbf{z})$$

is of rank 4. It is easy to see that such a polynomial $b(\mathbf{x}, \mathbf{z})$ is a (permutation of) linear sum of $u_{121}(\hat{S}(\mathbf{x}, \mathbf{z})), \ldots, u_{12l}(\hat{S}(\mathbf{x}, \mathbf{z}))$. Then the invertible transform $S_1 : \mathbf{F}_q^{(l+1)n} \to \mathbf{F}_q^{(l+1)n}$ satisfying

$$b(S_1(\mathbf{x}, \mathbf{z})) = x_1 \cdot (\text{linear form of } z_{21}, \ldots, z_{2l}) + x_2 \cdot (\text{linear form of } z_{11}, \ldots, z_{1l})$$

gives partial information of the secret key $\hat{S}$.

3. Rank attack II. For some choice of F, the attacker can recover the secret key more efficiently

than "Rank attack I". For example, in QSTS [4], the quadratic map F is defined by

$$\begin{aligned} f_1(\mathbf{x}) =& (\text{quadratic form of } x_1), \\ f_2(\mathbf{x}) =& (\text{quadratic form of } x_1, x_2), \\ & \vdots \\ f_n(\mathbf{x}) =& (\text{quadratic form of } x_1, \ldots, x_n). \end{aligned}$$

It is easy to see that

$$\tilde{f}_1(\mathbf{x}, \mathbf{z}) = x_1 \cdot (\text{quadratic form of } z_{11}, \ldots, z_{1l}) + (\text{linear sum of } u_{ijk}(\mathbf{x}, \mathbf{z}) \text{ and } v_{ijkr}(\mathbf{x}, \mathbf{z})).$$

Since the coefficient matrix of the former term in the right hand side above is of rank 2, we see that there exist $a_1, \ldots, a_{n+M} \in \mathbf{F}_q$ such that the coefficient matrix of

$$a_1\hat{p}_1(\mathbf{x}, \mathbf{z}) + \cdots + a_n\hat{p}_n(\mathbf{x}, \mathbf{z}) + a_{n+1}h_1(\mathbf{x}, \mathbf{z}) + \cdots + a_{n+M}h_M(\mathbf{x}, \mathbf{z}) =: c(\mathbf{x}, \mathbf{z})$$

is of rank 2. Then the attacker can obtain partial information of the secret key $\hat{S}$ by recovering an invertible linear map S_2 satisfying

$$c(S_2(\mathbf{x}, \mathbf{z})) = x_1 \cdot (\text{quadratic form of } z_{11}, \ldots, z_{1l}).$$

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

References

[1] Y. Hashimoto, On the security of Zhang-Tan's variants of multivariate signature schemes, Ryukyu Math. J. **31** (2018), pp.1–5.

[2] Y. Hashimoto, Y. Ikematsu, T. Takagi, Chosen message attack on multivariate signature ELSA at Asiacrypt 2017, J. Information Processing, **27** (2019), pp.517–524.

[3] K.-A. Shim, C.-M. Park and N. Koo, An existential unforgeable signature scheme based on multivariate quadratic equations, Asiacrypt'17, LNCS **10624** (2017), 37–64.

[4] D. Smith-Tone, New Practical Multivariate Signatures from a Nonlinear Modifier, PQCrypto'21, LNCS **12841** (2021), pp. 79–97.

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

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