JSIAM Letters Vol.10 (2018) pp.21–24 ©2018 Japan Society for Industrial and Applied Mathematics JSIAM Letters

High-rank attack on HMFEv

Yasufumi Hashimoto[1]

[1] Department of Mathematical Sciences, University of the Ryukyus, 1 Senbaru, Nishihara-cho, Nakagami-gun, Okinawa, Japan

E-mail *hashimoto@math.u-ryukyu.ac.jp*

Received October 18, 2017, Accepted February 19, 2018

Abstract

HMFEv is a new multivariate signature scheme proposed at PQCrypto 2017. This is a vinegar variant of multi-HFE (Chen et al., 2008). While the original multi-HFE is known to be insecure against the direct attack (Huang et al., 2015), the min-rank attack (Bettale et al., 2013) and the attack using a diagonalization approach (Hashimoto, 2017), HMFEv is considered to be secure enough against these attacks. However, the security against the high-rank attack had not been studied at all. In the present paper, we study the structure of HMFEv and discuss its security against the high-rank attack.

Keywords HMFEv, high-rank attack, multivariate public key cryptosystem (MPKC), post-quantum cryptography

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

The multi-HFE [1] is one of public key cryptosystems whose public keys are sets of multivariate quadratic forms over finite fields. The quadratic forms in multi-HFE are generated by a set of multivariate quadratic forms over an extension field of the basic field. Unfortunately, the multi-HFE is known to be insecure against the direct attack [2], the min-rank attack [3] and the attack using a diagonalization approach [4].

Recently in PQCrypto 2017, a vinegar variant of multi-HFE, called HMFEv, was proposed by Petzoldt et al. [5]. This vinegar variant succeeds to enhance the security against the known attacks [2–4] and then HMFEv had been expected to be one of signature schemes, secure and efficient enough under suitable parameter selections [5] (see Table 1). However, the security against the high-rank attack had not been studied yet at all.

In this paper, we study the structure of HMFEv and discuss the security of HMFEv against the high-rank attack. Based on the results of our experiments given in Table 2, we can conclude that the security of HMFEv is much less than expected.

2. Multi-HFE and HMFEv

In this section, we describe the constructions of multi-HFE [1] and HMFEv [5].

2.1 Multi-HFE

Let $n, N, r \geq 1$ be integers with $n = Nr$ and q a power of prime. Denote by k a finite field of order q and K an r-extension of k. Define the quadratic map $\mathcal{G} : K^N \to K^N$ by

$$X = (X_1, \ldots, X_N)^t,$$
$$\mathcal{G}(X) = (\mathcal{G}_1(X), \ldots, \mathcal{G}_N(X))^t,$$
$$\mathcal{G}_l(X) = \sum_{1 \leq i \leq j \leq N} \alpha_{ij}^{(l)} X_i X_j + \sum_{1 \leq i \leq N} \beta_i^{(l)} X_i + \gamma^{(l)}$$

for $1 \leq l \leq N$, where $\alpha_{ij}^{(l)}, \beta_i^{(l)}, \gamma^{(l)} \in K$.

The *secret key* is a pair of two invertible affine maps $S, T : k^n \to k^n$ and the *public key* is the quadratic map $F : k^n \to k^n$ defined by $F := T \circ \phi_N^{-1} \circ \mathcal{G} \circ \phi_N \circ S$, where $\phi_N : k^n \to K^N$ is a one-to-one map.

In the multi-HFE, a plain-text $p \in k^n$ is *encrypted* by $c = F(p) \in k^n$, and the cipher-text $c \in k^n$ is *decrypted* as follows. First, compute $Z = (Z_1, \ldots, Z_N)^t := \phi_N(T^{-1}(c)) \in K^N$. Next, find a common solution $X \in K^N$ of the equations

$$\mathcal{G}_1(X) = Z_1, \quad \ldots, \quad \mathcal{G}_N(X) = Z_N. \tag{1}$$

The plain-text $p \in k^n$ is given by $S^{-1}(\phi_N^{-1}(X))$.

To find X with (1), one needs to solve a system of N quadratic equations of N variables. Since the complexity of solving it is in exponential for N (see e.g. [6, 7]), the number N can not be taken large.

2.2 HMFEv

Let $n, m, N, r, v \geq 1$ be integers with $m := Nr$, $n := m + v$ and q a power of prime. Denote by k the finite field of order q and K the r-extension of k. Define the map $\mathcal{G} : K^N \times k^v \to K^N$ by

$$X = (X_1, \ldots, X_N)^t, \quad u = (u_1, \ldots, u_v)^t,$$
$$\mathcal{G}(X, u) = (\mathcal{G}_1(X, u), \ldots, \mathcal{G}_N(X, u))^t,$$
$$\mathcal{G}_l(X, u) = \sum_{1 \leq i \leq j \leq N} \alpha_{ij}^{(l)} X_i X_j + \sum_{1 \leq i \leq N} \beta_i^{(l)}(u) X_i + \gamma^{(l)}(u) \tag{2}$$

for $1 \leq l \leq N$, where $\alpha_{ij}^{(l)} \in K$, $\beta_i^{(l)} : k^v \to K$ is an affine form and $\gamma^{(l)} : k^v \to K$ is a quadratic form.

The *secret key* is a pair of two invertible affine maps $S : k^n \to k^n$, $T : k^m \to k^m$ and the *public key* is the quadratic map $F : k^n \to k^m$ defined by

$$F := T \circ \phi_N^{-1} \circ \mathcal{G} \circ \phi_{N,v} \circ S,$$

where $\phi_N : k^m \to K^N$, $\phi_{N,v} : k^n \to K^N \times k^v$ are one-

Table 1. Parameter Selection of HMFEv [5].

q	n	m	N	r	v	Security
31	44	36	2	18	8	80bit
256	39	27	3	9	12	80bit
31	68	56	2	28	12	128bit
256	61	45	3	15	16	128bit
31	97	80	2	40	17	192bit
256	90	69	3	23	21	192bit
31	131	110	2	55	21	256bit
256	119	93	3	31	26	256bit

to-one maps.

In the signature scheme HMFEv, a given message $y \in k^m$ is *signed* as follows. First, compute $Z = (Z_1, \dots, Z_N)^t := \phi_N(T^{-1}(y))$ and choose $u \in k^v$. Next, find a common solution $X \in K^N$ of the equations

$$\mathcal{G}_1(X,u) = Z_1, \quad \dots, \quad \mathcal{G}_N(X,u) = Z_N. \tag{3}$$

The signature for $y \in k^m$ is $S^{-1}(\phi_{N,v}^{-1}(X,u))$. The signature $x \in k^n$ is *verified* if $F(x) = y$ holds.

To find X with (3), one needs to solve a system of N quadratic equations of N variables. Then, similar to the multi-HFE, the number N cannot be large since the complexity of solving it is exponential for N. In [5] (see Table 1), Petzeldt et al. selected the parameters of HMFEv with $N = 2, 3$ as a signature scheme secure and efficient enough for practical use.

We note that the constant parts of S, T do not contribute to enhance the security. In fact, for $s \in k^n$, $t \in k^m$, $S_0(x) := x + s$ and $T_0(y) := y + t$, the map $\phi_N \circ T_0 \circ G \circ S_0 \circ \phi_{N,v}^{-1}$ is also a quadratic map similar to (2). Then we can consider that S, T are linear maps without loss of generality.

3. Security analysis

In this section, we study the structure of HMFEv and discuss the security against the rank attacks. We first study the structures of polynomials in HMFEv.

3.1 Polynomials in HMFEv

For integers $n_1, n_2 \geq 1$ and a finite field k, let $\mathrm{M}_{n_1,n_2}(k)$ be the set of $n_1 \times n_2$ matrices of k-entries. Denote by $I_n \in \mathrm{M}_{n,n}(k)$ the identity matrix and by $0_{n_1,n_2} \in \mathrm{M}_{n_1,n_2}(k)$ the zero matrix. For simplicity, we write $\mathrm{M}_n(k) := \mathrm{M}_{n,n}(k)$ and $0_n := 0_{n,n}$. For an integer $l \geq 1$ and a matrix $A = (a_{ij})_{i,j}$, we denote by $A^{(l)} := \left(a_{ij}^l\right)_{i,j}$.

Let $\{\theta_1, \dots, \theta_r\} \subset K$ be a basis of K over k and define $\Theta_N := \left(\theta_j^{q^{i-1}} \cdot I_N\right)_{1 \leq i,j \leq r} \in \mathrm{M}_m(K)$ and $\Theta_{N,v} := \begin{pmatrix} \Theta_N & \\ & I_v \end{pmatrix} \in \mathrm{M}_n(K)$. The one-to-one maps $\phi_N : k^m \to K^N$ and $\phi_{N,v} : k^n \to K^N \times k^v$ are given by the matrices Θ_N and $\Theta_{N,v}$ respectively. In fact, it holds

$$\phi_N = \psi_N^{-1} \circ \Theta_N, \quad \phi_{N,v} = \psi_{N,v}^{-1} \circ \Theta_{N,v}$$

for the two maps $\psi_N : K^N \to K^{Nr}$, $\psi_{N,v} : K^N \times k^v \to K^{Nr} \times k^v$ defined by

$$\begin{aligned}
&\psi_N(\alpha_1, \dots, \alpha_N) = \left(\alpha_1, \dots, \alpha_N, \alpha_1^q, \dots, \dots, \alpha_N^{q^{r-1}}\right)^t, \\
&\psi_{N,v}(\alpha_1, \dots, \alpha_N, u_1, \dots, u_v) \\
&\quad = \left(\alpha_1, \dots, \alpha_N, \alpha_1^q, \dots, \dots, \alpha_N^{q^{r-1}}, u_1, \dots, u_v\right)^t.
\end{aligned}$$

Then the public key F is described by

$$F = \left(T \circ \Theta_N^{-1}\right) \circ \left(\psi_N \circ \mathcal{G} \circ \psi_{N,v}^{-1}\right) \circ \left(\Theta_{N,v} \circ S\right),$$

namely

$$\begin{aligned}
F(x) &= (f_1(x), \dots, f_m(x))^t \\
&= \left(T \circ \Theta_N^{-1}\right) \cdot \left(\mathcal{G}_1\left(\phi_{N,v}(S(x))\right), \dots, \right. \\
&\quad \mathcal{G}_N\left(\phi_{N,v}(S(x))\right), \mathcal{G}_1\left(\phi_{N,v}(S(x))\right)^q, \dots, \\
&\quad \left. \mathcal{G}_N\left(\phi_{N,v}(S(x))\right)^{q^{r-1}}\right)^t.
\end{aligned} \tag{4}$$

When we express the polynomials $\mathcal{G}_1, \dots, \mathcal{G}_N$ by

$$\mathcal{G}_l(X,u) = (X^t, u^t) \begin{pmatrix} A_l & B_l \\ B_l^t & C_l \end{pmatrix} \begin{pmatrix} X \\ u \end{pmatrix} + (\text{linear form})$$

as quadratic forms of X, u with matrices $A_l \in \mathrm{M}_N(K)$, $B_l \in \mathrm{M}_{N,v}(K)$, $C_l \in \mathrm{M}_v(K)$, the polynomials $\mathcal{G}_1(X,u)$, $\dots, \mathcal{G}_N(X,u), \mathcal{G}_1(X,u)^q, \dots, \dots, \mathcal{G}_N(X,u)^{q^{r-1}}$ in (4) are written as quadratic polynomials of

$$\begin{aligned}
\bar{X} &:= \psi_{N,v}(X,u) \\
&= \left(X_1, \dots, X_N, X_1^q, \dots, \dots, X_N^{q^{r-1}}, u_1, \dots, u_v\right)^t
\end{aligned}$$

in the forms

$$\begin{aligned}
\mathcal{G}_l(X,u) &= \bar{X}^t \left(\begin{array}{ccc|c} A_l & & & B_l \\ & & 0_{m-N} & \\ & & & \\ \hline B_l^t & & & C_l \end{array}\right) \bar{X} \\
&\quad + (\text{linear form of } \bar{X}), \\
\mathcal{G}_l(X,u)^q &= \bar{X}^t \left(\begin{array}{ccc|c} 0_N & & & B_l^{(q)} \\ & A_l^{(q)} & & \\ & & 0_{m-2N} & \\ \hline & B_l^{(q)\,t} & & C_l^{(q)} \end{array}\right) \bar{X} \\
&\quad + (\text{linear form of } \bar{X}), \\
&\vdots \\
\mathcal{G}_l(X,u)^{q^{r-1}} &= \bar{X}^t \left(\begin{array}{ccc|c} 0_{m-N} & & & B_l^{(q^{r-1})} \\ & A_l^{(q^{r-1})} & & \\ \hline & B_l^{(q^{r-1})\,t} & & C_l^{(q^{r-1})} \end{array}\right) \bar{X} \\
&\quad + (\text{linear form of } \bar{X}).
\end{aligned} \tag{5}$$

This means that the quadratic forms in the public key are expressed by

$$f_l(x) = x^t F_l x + (\text{linear form of } x),$$

where

$$F_l = (\Theta_{N,v} S)^t \left(\begin{array}{ccc|c} *_N & & & * \\ & \ddots & & \vdots \\ & & *_N & * \\ \hline * & \cdots & * & *_v \end{array}\right) (\Theta_{N,v} S). \tag{6}$$

In the next two subsections, we discuss the security of HMFEv against the rank attacks based on these facts.

3.2 Min-rank attack

Let $F_1, \dots, F_m$ be the coefficient matrices of the quadratic forms $f_1(x), \dots, f_m(x)$ respectively. The *min-rank attack*, introduced by Kipnis-Shamir [8] and developed by Bettale et al. [3], is an attack to recover T (partially) by finding $\alpha_1, \dots, \alpha_m \in K$ such that the rank of $H := \alpha_1 F_1 + \cdots + \alpha_m F_m$ is at most R if there exist such $\alpha_1, \dots, \alpha_m \in K$ and an integer $1 \leq R < n$. For HMFEv, due to (4) and (5), we see that there exist such $\alpha_1, \dots, \alpha_m \in K$ with $R = N + v$ and H is one of the

following forms with high probability.

$$(\Theta_{N,v}S)^t\begin{pmatrix} *_N & & * \\ & 0_{m-N} & \\ * & & *_v \end{pmatrix}(\Theta_{N,v}S),$$

$$(\Theta_{N,v}S)^t\begin{pmatrix} 0_N & & & \\ & *_N & & * \\ & & 0_{m-2N} & \\ & * & & *_v \end{pmatrix}(\Theta_{N,v}S),$$

$$\ldots,(\Theta_{N,v}S)^t\begin{pmatrix} 0_{m-N} & \\ & *_{N+v} \end{pmatrix}(\Theta_{N,v}S).$$

Once such a matrix H is given, the attacker can recover keys equivalent to (S,T) easily (see [3]).

To find such $\alpha_1,\ldots,\alpha_m \in K$, the attacker generates a system of polynomial equations of m variables $z_1,\ldots,z_m$ derived from the condition that the rank of $H(z_1,\ldots,z_m) := z_1F_1+\cdots+z_mF_m$ is at most $N+v$ and solve it by, e.g., the Gröbner basis algorithm. Since the condition that the rank of A is at most R is equivalent that the determinants of arbitrary $(R+1)\times(R+1)$-minor matrices in A are zero, the min-rank attack requires to solve a system of polynomial equations of degree (at most) $N+v+1$ and of m variables. Based on the result in [3], the authors in [5] claimed that the complexity of the min-rank attack is $O\left(\binom{m+N+v+1}{N+v+1}^w\right)$ where $2\le w<3$ is an exponent of the Gaussian elimination. This means that, if one takes v sufficiently large, HMFEv is secure enough against the min-rank attack.

3.3 High-rank attack

The *high-rank attack*, introduced in [9, 10], is to find $\beta_1,\ldots,\beta_L \in K$ such that the rank of $P := F_m+\beta_1F_1+\cdots+\beta_LF_L$ is at most R if there exist such integers $1\le L,R<n$ and $\beta_1,\ldots,\beta_L\in K$. For HMFEv, recall that $F_1,\ldots,F_m$ are as written in (6). Due to (4) and (5), we see that the first N columns and lows of the central matrix in (6) are derived from linear sums of N polynomials $\mathcal{G}_1(X,u),\ldots,\mathcal{G}_N(X,u)$. Then, removing the contributions of such N polynomials, we can get a matrix of rank at most $n-N$. This means that the high-rank attack is available on HMFEv with $(L,R)=(N,n-N)$. We now describe how to recover an equivalent key of HMFEv.

Input. The public matrices $F_1,\ldots,F_m$.
Output. Invertible matrices $S'\in \mathrm{M}_n(k)$, $T'\in\mathrm{M}_m(k)$ such that $\phi_N\circ T'\circ F\circ S'\circ\phi_{N,v}^{-1}: K^N\times k^v\to K^N$ is a quadratic map similar to (2).

Step 1. Find $\beta_1,\ldots,\beta_N\in K$ such that $P := F_m+\beta_1F_1+\cdots+\beta_NF_N$.
Step 2. Find a matrix $Q\in\mathrm{M}_{n,N}(K)$ with $PQ=0_{n,N}$.
Step 3. Choose $Q_0\in\mathrm{M}_{n,v}(k)$ randomly and put $\tilde{Q} := (Q,Q^{(q)},\ldots,Q^{(q^{r-1})},Q_0)\in\mathrm{M}_n(k)\Theta_{N,v}^{-1}$. If $\tilde{Q}$ is not invertible, change Q,Q_0. Compute $F_l' := \tilde{Q}^tF_l\tilde{Q}$ for $1\le l\le m$.
Step 4. Find a matrix $W=(w_{ij})_{i,j}\in\mathrm{M}_{N,m}(K)$ with

$$F_i'' := \sum_{1\le j\le m} w_{ij}F_j' = \begin{pmatrix} *_N & & * \\ & 0_{m-N} & \\ * & & *_v \end{pmatrix}$$

for $1\le i\le N$. Put $\tilde{W} := \begin{pmatrix} W \\ W^{(q)} \\ \vdots \\ W^{(q^{r-1})} \end{pmatrix}\in\Theta_N\mathrm{M}_m(k)$. If $\tilde{W}$ is not invertible, change W.
Step 5. Output $S' := \tilde{Q}\Theta_{N,v}$ and $T' := \Theta_N^{-1}\tilde{W}$.

We explain why this attack recovers an equivalent key. As discussed before, there exist $\beta_1,\ldots,\beta_N\in K$ in Step 1 and we can easily check that P is one of the following forms with high probability.

$$\begin{aligned}&(\Theta_{N,v}S)^t\begin{pmatrix} 0_N & \\ & *_{n-N} \end{pmatrix}(\Theta_{N,v}S),\\ &(\Theta_{N,v}S)^t\begin{pmatrix} *_N & & * \\ & 0_N & \\ * & & *_{n-2N} \end{pmatrix}(\Theta_{N,v}S),\\ &\cdots,(\Theta_{N,v}S)^t\begin{pmatrix} *_{(r-1)N} & & * \\ & 0_N & \\ * & & *_v \end{pmatrix}(\Theta_{N,v}S).\end{aligned} \tag{7}$$

Since P is of rank at most $n-N$, there exists a matrix Q in Step 2 and it can be found by linear operations. Due to (7), we see that a matrix $\tilde{Q}=(Q,*)$ satisfies $\tilde{Q}^tP\tilde{Q}=\begin{pmatrix}0_N & \\ & *\end{pmatrix}$ and then $(\Theta_{N,v}S)\tilde{Q}$ is in the form $\begin{pmatrix}*_N & * \\ 0 & *\end{pmatrix}$ or its permutation. Lemma 3.2 in [4] tells that the matrix $\tilde{Q}$ in Step 3 is in $\mathrm{M}_n(k)\Theta_{N,v}^{-1}$ and $(\Theta_{N,v}S)\tilde{Q}\in\Theta_{N,v}\mathrm{M}_n(k)\Theta_{N,v}^{-1}$. Thus $(\Theta_{N,v}S)\tilde{Q}$ must be $\left(\begin{array}{ccc|c} *_N & & & * \\ & \ddots & & \vdots \\ & & *_N & * \\ \hline & & & *_v \end{array}\right)$ or its permutation. This means, due to (6), that $F_l' = \left(\begin{array}{ccc|c} *_N & & & * \\ & \ddots & & \vdots \\ & & *_N & * \\ \hline * & \cdots & * & *_v \end{array}\right)$ for $1\le l\le m$. Since F_l' is a linear sum of matrices similar to the coefficient matrices given in (5), a matrix W in Step 4 exists and it is found by linear operations. The matrices $F_1'',\ldots,F_N''$ are similar to the coefficient matrices of $\mathcal{G}_1(X,u),\ldots,\mathcal{G}_N(X,u)$. We thus conclude that (S',T') in Step 5 is an equivalent key. □

It is easy to see that Step 2-5 require only linear operations. Then the complexity of Step 1 is important in this attack. To find $\beta_1,\ldots,\beta_N$ in Step 1, we state a system of polynomial equations of N variables $y_1,\ldots,y_N$ derived from the condition that the rank of $P(y_1,\ldots,y_N) := F_m+y_1F_1+\cdots+y_NF_N$ is at most $n-N$ and solve it by, e.g., the Gröbner basis algorithm. Since this condition is equivalent that the determinants of arbitrary $(n-N+1)\times(n-N+1)$-minor matrices of $P(y_1,\ldots,y_N)$ are zero, the attacker needs to solve a system of polynomial equations of degree at most $n-N+1$ and of N variables. Then we can consider that the complexity of the high-rank attack on HMFEv highly depends on N and the contribution of v for the security seems not too much.

Note that, for integers $M_1,N_1,d\ge 1$ with $M_1\ge N_1$ and a *semi-regular* system of polynomials $\{p_1(x),\ldots,p_{M_1}(x)\}$ of N_1-variables and of degree d, it is known (e.g. [6,7]) that the complexity of the Gröbner basis algorithm on this polynomial system is bounded by $O\left(\binom{N_1+d_{\mathrm{reg}}}{N_1}^w\right)$, where d_{reg} is a constant, called the *degree of regularity*, given by the index of the first non-

Table 2. Running times of high-rank attack on HMFEv.

q	n	m	N	r	v	Time	(Security)
31	44	36	2	18	8	2.20s	(80bit)
256	39	27	3	9	12	13.2s	(80bit)
31	68	56	2	28	12	19.1s	(128bit)
256	61	45	3	15	16	261s	(128bit)
31	97	80	2	40	17	113s	(192bit)
256	90	69	3	23	21	—	(192bit)
31	131	110	2	55	21	701s	(256bit)
256	119	93	3	31	26	—	(256bit)

positive coefficient of the univariate polynomial $C(t) := (1-t^d)^{M_1}(1-t)^{-N_1}$. This means that, if M_1 is sufficiently larger than N_1, we have $d_{\mathrm{reg}} = d$. We thus expect that the complexity of the high-rank attack on HMFEv is

$$O\left(\binom{n+1}{N}^w\right) \tag{8}$$

since $(N_1, d) = (N, n-N+1)$ for the polynomial system in the high-rank attack and M_1 can be taken at most $\binom{n}{n-N+1}^2$. Remark that (8) is the number of operations on K and then the real running time seems at most $(r \log q)^2$ times larger than (8). While, on this paper, we avoid to give a concrete proof for the estimate (8) of the high-rank attack, we consider that (8) is not far from the real complexity of the high-rank attack.

3.4 Experiments of the high-rank attack

We implemented the high-rank attack on HMFEv by Magma [11] ver.2.22-3 on Windows 8.1, Core(TM)i7-4800MQ, 2.70GHz for the parameters in Table 1 ([5]). In our implementation, we first choose an integer M sufficiently larger than N, and generate M equations of N variables $(y_1, \ldots, y_N)$ by the determinants of $(n-N+1) \times (n-N+1)$ minor matrices of $P(y_1, \ldots, y_N)$. Next, we find a common solution $(y_1, \ldots, y_N) = (\beta_1, \ldots, \beta_N)$ of such M equations by the Gröbner basis algorithm. Finally, we check whether the rank of $P(\beta_1, \ldots, \beta_N)$ is at most $n-N$.

Remark that the Gaussian elimination is not efficient to compute a determinant of a polynomial matrix of large size. We then used an algorithm introduced in [12] instead of the Gaussian elimination for computations of polynomial matrices.

We also remark that, if q is even, we use $F_l + F_l^t$ instead of the coefficient matrix F_l. The matrix $F_l + F_l^t$ is symmetric and skew-symmetric since the field k is of even characteristic. It is known (e.g. [13]) that the determinant of a skew-symmetric matrix is zero when the size of the matrix is odd and is a square when that is even. We then have to arrange our attack based on this fact. Fortunately, the arrangement for even characteristic cases was already discussed in [3] for the min-rank attack and we can apply it also for the high-rank attack.

We describe the running times of the high-rank attack in Table 2 by taking $M = 3$ for $(q, N) = (31, 2)$ and $M = 10$ for $(q, N) = (256, 3)$. These results show that HMFEv with $N = 2$ is not secure at all. While the complexities for the cases of $N = 3$ is much more than the cases of $N = 2$, we can consider that the security is far from $80 \sim 256$ bit. Though one requires a larger N to generate a secure HMFEv, it lacks the efficiency of signature generation.

4. Conclusion

The signature scheme HMFEv is a vinegar variant of multi-HFE. It is known [5] that, if the vinegar parameter v is larger, HMFEv against the min-rank attack is exponentially more secure. However, the security against the high-rank attack does not highly depend on v and then HMFEv with the parameters selected in [5] (Table 1) is much less secure than expected. While HMFEv with larger N is secure enough, it lacks the efficiency of the signature generation. We thus conclude that this scheme has a serious trade-off between the security and efficiency.

Acknowledgments

The author was supported by JST CREST no. JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181. He would like to thank the anonymous referee(s) for reading the previous draft carefully and giving helpful comments.

References

[1] C.H.O. Chen, M.S. Chen, J. Ding, F. Werner and B.Y. Yang, Odd-char multivariate hidden field equations, http://eprint.iacr.org/2008/543, 2008.

[2] M.D.A. Huang, M. Kosters, Y. Yang and S.L. Yeo, On the last fall degree of zero-dimensional Weil descent systems, arXiv:1505.02532 [math.AC], 2015.

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

[4] Y. Hashimoto, Key recovery attacks on multivariate public key cryptosystems derived from quadratic forms over an extension field, IEICE Trans. Fundamentals, **100-A** (2017), 18–25.

[5] A. Petzoldt, M.S. Chen, J. Ding and B.Y. Yang, HMFEv - An efficient multivariate signature scheme, in: Proc. of PQCrypto 2017, T. Lange, T. Takagi eds., LNCS, Vol. 10346, pp. 205–223, Springer-Verlag, Cham, 2017.

[6] M. Bardet, J.C. Faugère, B. Salvy and B.Y. Yang, Asymptotic expansion of the degree of regularity for semi-regular systems of equations, MEGA'05 (2005).

[7] L. Bettale, J.C. Faugère and L. Perret, Solving polynomial systems over finite fields: Improved analysis of the hybrid approach, in: Proc. of ISSAC 2012, J. van der Hoeven and M. van Hoeij eds., pp.67–74, ACM, New York, 2012.

[8] A. Kipnis and A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, in: Proc. of CRYPTO 1999, M. Wiener eds., LNCS, Vol. 1666, pp.19–30, Springer-Verlag, Berlin, 1999.

[9] S. Hasegawa and T. Kaneko, An attacking method for a public-key cryptosystem based on the difficulty of solving a system of non-linear equations (in Japanese), in: Proc. of 10th Symposium on Information Theory and Its Applications, JA5-3, 1987.

[10] D. Coppersmith, J. Stern and S. Vaudenay, Attacks on the birational permutation signature schemes, in: Proc. of CRYPTO 1993, D.R. Stinson eds., LNCS, Vol. 773, pp.435–443, Springer-Verlag, Berlin, 1994.

[11] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput. **24** (1997), 235–265.

[12] E. V. Krishnamurthy, Error-free polynomial matrix computations, Texts and Monographs in Computer Science, Springer-Verlag, New York, 1985.

[13] A. Cayley, Sur les determinants gauches (On skew determinants), J. Reine Angew. Math. **38** (1849), 93–96.