Cryptanalysis of multi-HFE

Yasufumi Hashimoto *

Abstract

Multi-HFE (Chen et al., 2009) is one of cryptosystems whose public key is a set of multivariate quadratic forms over a finite field. Its quadratic forms are constructed by a set of multivariate quadratic forms over an extension field. Recently, Bettale et al. (2013) have studied the security of HFE and multi-HFE against the min-rank attack and found that multi-HFE is not more secure than HFE of similar size. In the present paper, we propose a new attack on multi-HFE by using a diagonalization approach. As a result, our attack can recover equivalent secret keys of multi-HFE in polynomial time for odd characteristic case. In fact, we experimentally succeeded to recover equivalent secret keys of several examples of multi-HFE in about fifteen seconds on average, which was recovered in about nine days by the min-rank attack.

Keywords. multivariate public-key cryptosystems, multi-HFE, post-quantum cryptography

1 Introduction

A multivariate public key cryptosystem (MPKC) is a cryptosystem whose public key is a set of multivariate quadratic forms over a finite field. It is known that the problem of finding a solution of a system of multivariate quadratic forms over a finite field is NP hard [19] and then MPKC has been expected as a candidate of Post-Quantum Cryptography.

One of major ideas to design MPKCs is to generate quadratic forms by a polynomial map over an extension field. Matsumoto-Imai's scheme [26] and Hidden Field Equations (HFE) [28] are representative schemes constructed in this way; in fact, their quadratic forms are derived from a high degree univariate monomial/polynomial over an extension field. Multi-HFE [7] is also one of such MPKCs, whose quadratic forms are constructed by a set of multivariate quadratic forms over an extension field. While its security against the Gröbner basis attack is considered to be enough [7], Bettale et al. [4] found that multi-HFE is not more secure than HFE of similar size against the min-rank attack. However, the complexity of the min-rank attack on multi-HFE [4] highly depends on the number of variables of quadratic forms over the extension field and then the min-rank attack is not feasible when its number is not small.

In the present paper, we propose a new attack on multi-HFE. Since the coefficient matrices of the quadratic forms in the public key of multi-HFE are described by linear transforms of diagonal type matrices, a key recovery attack using an approach similar to diagonalization of matrices is available for odd characteristic case. Our attack is much faster than the min-rank attack [4]. In fact, we succeeded to recover equivalent secret keys of an example of multi-HFE in about fifteen seconds on average, which was recovered in about nine days by the min-rank attack. Furthermore, different to the min-rank attack, the complexity of our attack does not

*Department of Mathematical Science, University of the Ryukyus/JST CREST

Table 1: Examples of MPKCs constructed by a polynomial map over an extension field

	univariate	multivariate
quadratic	Square [8, 5]	MFE [31, 11], multi-HFE [7, 4]
high degree	MI [26, 27], HFE [28], ZHFE [30]	lIC [13, 18]
variants	Sflash [1, 14], Quartz [29, 9], etc.	

depend on the number of variables of the quadratic forms over the extension field. This means that our attack can reduce the security of (not only multi-HFE but) most MPKCs constructed by a "quadratic" map over an extension field.

2 Multi-HFE

2.1 Construction

A multivariate public key cryptosystem (MPKC) is a cryptosystem whose public key is a set of multivariate quadratic forms

$$\begin{aligned} f_1(x_1,\cdots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)}, \\ &\vdots \\ f_m(x_1,\cdots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)}, \end{aligned}$$

over a finite field. We now describe the construction of multi-HFE.

Let $n, N, r \geq 1$ be integers with $Nr = n$ and q a power of prime. Denote by k a finite field of order q and K an extension field of k with $[K : k] = r$. Then multi-HFE is as follows.

Multi-HFE

Secret Keys: Two affine maps $S, T : k^n \to k^n$ and a quadratic map $\mathcal{G} : K^N \to K^N$:

$$\begin{aligned} \mathcal{G}(X_1,\ldots,X_N) &= (\mathcal{G}_1(X_1,\ldots,X_N),\ldots,\mathcal{G}_N(X_1,\ldots,X_N))^t, \\ \mathcal{G}_1(X_1,\ldots,X_N) &= \sum_{1\le i\le j\le N} \alpha_{ij}^{(1)} X_i X_j + \sum_{1\le i\le N} \beta_i^{(1)} X_i + \gamma^{(1)}, \\ &\vdots \\ \mathcal{G}_N(X_1,\ldots,X_N) &= \sum_{1\le i\le j\le N} \alpha_{ij}^{(N)} X_i X_j + \sum_{1\le i\le N} \beta_i^{(N)} X_i + \gamma^{(N)}, \end{aligned}$$

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

Public Key: The quadratic map $F := T \circ \phi^{-1} \circ \mathcal{G} \circ \phi \circ S : k^n \to k^n$, where $\phi : k^n \to K^N$ is a one-to-one map.

$$F : k^n \xrightarrow{S} k^n \xrightarrow{\phi} K^N \xrightarrow{\mathcal{G}} K^N \xrightarrow{\phi^{-1}} k^n \xrightarrow{T} k^n.$$

Encryption: For a plain-text $x \in k^n$, the cipher $y \in k^m$ is $y = F(x)$.

Decryption: First, compute $y' := T^{-1}(y)$ and put $Y' := \phi(y')$. Next, find $Z \in K^N$ with $G(Z) = Y'$. Finally, let $z := \phi^{-1}(Z)$ and compute $x = S^{-1}(z)$.

$$\boxed{N \text{ quadratic equations of } N \text{ variables over } K} \xrightarrow{\textbf{Multi-HFE}} \boxed{n \text{ quadratic equations of } n \text{ variables over } k}$$

2.2 Efficiency

When N is small enough, $\mathcal{G}$ is inverted efficiently by the Gröbner basis algorithm. See Table 1 of [7] for several examples of efficiency of multi-HFE with $N = 2, 3, 4$. However, when N is not small enough and $\mathcal{G}$ is chosen randomly, the decryption by the Gröbner basis algorithm is not efficient. Then for such N, a special structure of $\mathcal{G}$ like MFE [31, 11] is required for fast decryptions.

2.3 Security against known attacks

Direct attacks. The direct attack is to find a common solution $x \in k^n$ of $f_1(x) = y_1, \ldots, f_n(x) = y_n$ for a given cipher text $(y_1, \ldots, y_n)^t \in k^n$ directly. One of major approaches of the direct attack is by using the Gröbner basis algorithm [15, 16, 2, 3]. In [3], the complexity is estimated by $O(2^{m(3.31-3.62/\log_2 q)})$ if $\log_2 q \ll n$ and $\{f_1(x) - y_1, \ldots, f_n(x) - y_n\}$ is "semi-regular". On HFE, it is known that the "degree of regularity" of the system $\{f_1(x) - y_1, \ldots, f_n(x) - y_n\}$ is bounded by $\frac{1}{2}(q-1)\lceil \log D \rceil + 2$ [21, 10], where D is the degree of the central univariate polynomial of HFE over an extension field. This means that HFE with smaller q is less secure. For multi-HFE, while there have been less results compared with HFE, the authors of [7] claimed that the complexity against Gröbner basis attack is almost same to the random systems.

Min-Rank attacks. The min-rank attacks have been proposed by Kipnis-Shamir [23] for HFE and improved by Bettale-Faugère-Perret [4] for HFE and (generalized) multi-HFE. On HFE and multi-HFE, it is known that the coefficient matrices of the quadratic forms $F_1, \ldots, F_n$ are linear sums of matrices of small rank over K (its rank is at most N on multi-HFE given in §2.1,). The min-rank attack is to recover (partial information of) T by finding $\alpha_1, \ldots, \alpha_n \in K$ such that $\alpha_1 F_1 + \cdots + \alpha_n F_n$ is of small rank. In Proposition 13 and its proof of [4], the complexity of the min-rank attack is estimated by $O\left(\binom{n+N+1}{N+1}^{\omega}\right)$ under several conditions, where $2 \le \omega < 3$ is the exponent of the Gaussian elimination.

3 Proposed attacks on multi-HFE

In this section, we propose our attack on multi-HFE. First we prepare notations and several lemmas to explain our attack.

3.1 Notations and lemmas

For integers $n_1, n_2 \ge 1$, 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 a matrix $A = (a_{ij})_{i,j}$, a polynomial $g(t) = c_0 + c_1 t + \cdots + c_d t^d$ and an integer $l \ge 1$, put

$$A^{(l)} := \left(a_{ij}^l\right)_{i,j}, \qquad g^{(l)}(t) := c_0^l + c_1^l t + \cdots + c_d^l t^d.$$

For square matrices $A_1 \in \mathrm{M}_{n_1}(k), \dots, A_l \in \mathrm{M}_{n_l}(k)$, $A_1 \oplus \cdots \oplus A_l$ means

$$A_1 \oplus \cdots \oplus A_l := \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_l \end{pmatrix} \in \mathrm{M}_{n_1+\cdots+n_l}(k).$$

We now recall that $n, N, r \geq 1$ are integers with $n = Nr$, q is a power of prime, k is a finite field of order q and K is an extension field of k with $[K : k] = r$. Choose a basis $\{\theta_1, \dots, \theta_r\}$ of K over k and a one-to-one map $\phi : k^n \to K^N$. For simplicity, suppose that ϕ is chosen such that $\phi(a_{11}, \dots, a_{1N}, a_{21}, \dots, \dots, a_{rN}) = (a_{11}\theta_1 + \cdots + a_{r1}\theta_r, \dots, a_{1N}\theta_1 + \cdots + a_{rN}\theta_r)^t$. Let L_N be a subset of K^n with

$$L_N := \left\{ \left(a_1, \dots, a_N, a_1^q, \dots, \dots, a_N^{q^{r-1}}\right)^t \mid a_1, \dots, a_N \in K \right\},$$

$\psi : L_N \to K^N$ a one-to-one map with $\psi\left(a_1, \dots, a_N, a_1^q, \dots, \dots, a_N^{q^{r-1}}\right) = (a_1, \dots, a_N)^t$ and $\Theta \in \mathrm{M}_n(K)$ a matrix with

$$\Theta := \left(\theta_j^{q^{i-1}} I_N\right)_{1 \leq i,j \leq r} = \begin{pmatrix} \theta_1 I_N & \theta_2 I_N & \cdots & \theta_r I_N \\ \theta_1^q I_N & \theta_2^q I_N & \cdots & \theta_r^q I_N \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{q^{r-1}} I_N & \theta_2^{q^{r-1}} I_N & \cdots & \theta_r^{q^{r-1}} I_N \end{pmatrix}.$$

Then the following lemma holds.

Lemma 3.1. *The matrix Θ gives a one-to-one map from k^n to L_N and it holds $\phi = \psi \circ \Theta$.*

Proof. For $a = (a_{11}, \dots, a_{1N}, a_{21}, \dots, \dots, a_{rN})^t \in k^n$, we have

$$\Theta a = (a_1, \dots, a_N, a_1^q, \dots, \dots, a_N^{q^{r-1}})^t, \tag{1}$$

where $a_i := a_{1i}\theta_1 + \cdots + a_{ri}\theta_r \in K$. Then Θ gives a map from k^n to L_N and we can easily check that it is one-to-one. Furthermore, due to (1), we have $\psi(\Theta a) = (a_1, \dots, a_N)^t = \phi(a)$. □

For an integer $m \geq 1$, define the sets $\mathcal{A}_m \subset \mathrm{M}_{n,m}(K), \mathcal{B}_m \subset \mathrm{M}_{m,n}(K), \mathcal{C} \subset \mathrm{M}_n(K)$ of matrices as follows.

$$\mathcal{A}_m := \left\{ \begin{pmatrix} A \\ A^{(q)} \\ \vdots \\ A^{(q^{r-1})} \end{pmatrix} \middle| \; A \in \mathrm{M}_{N,m}(K) \right\},$$

$$\mathcal{B}_m := \left\{ \left(B, B^{(q)}, \cdots, B^{(q^{r-1})}\right) \middle| \; B \in \mathrm{M}_{m,N}(K) \right\},$$

$$\mathcal{C} := \left\{ \left(C_{(j-i \bmod r)+1}^{(q^{i-1})}\right)_{1 \leq i,j \leq r} = \begin{pmatrix} C_1 & C_2 & \cdots & C_r \\ C_r^{(q)} & C_1^{(q)} & \cdots & C_{r-1}^{(q)} \\ \vdots & \vdots & \ddots & \vdots \\ C_2^{(q^{r-1})} & C_3^{(q^{r-1})} & \cdots & C_1^{(q^{r-1})} \end{pmatrix} \middle| \; C_1, \dots, C_r \in \mathrm{M}_N(K) \right\},$$

Lemma 3.2. *For any $m \geq 1$, we have*

$$\mathcal{A}_m = \Theta \cdot \mathrm{M}_{n,m}(k), \qquad \mathcal{B}_m = \mathrm{M}_{m,n}(k) \cdot \Theta^{-1}, \qquad \mathcal{C} = \Theta \cdot \mathrm{M}_n(k) \cdot \Theta^{-1}. \tag{2}$$

Proof. First, choose $A_1, \dots, A_r \in \mathrm{M}_{N,m}(k)$ arbitrary. We have

$$\Theta \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_r \end{pmatrix} = \begin{pmatrix} A_1\theta_1 + \cdots + A_r\theta_r \\ A_1\theta_1^q + \cdots + A_r\theta_r^q \\ \vdots \\ A_1\theta_1^{q^{r-1}} + \cdots + A_r\theta_r^{q^{r-1}} \end{pmatrix} = \begin{pmatrix} A_1\theta_1 + \cdots + A_r\theta_r \\ (A_1\theta_1 + \cdots + A_r\theta_r)^{(q)} \\ \vdots \\ (A_1\theta_1 + \cdots + A_r\theta_r)^{(q^{r-1})} \end{pmatrix}.$$

This means that $\Theta \cdot \mathrm{M}_{n,m}(k) \subset \mathcal{A}_m$. Since $\#(\Theta \cdot \mathrm{M}_{n,m}(k)) = \#\mathcal{A}_m = q^{mn}$, we obtain $\mathcal{A}_m = \Theta \cdot \mathrm{M}_{n,m}(k)$.

Next, choose $B \in \mathrm{M}_{m,N}(K)$ arbitrary. We have

$$\begin{aligned}\left(B, B^{(q)}, \cdots, B^{(q^{r-1})}\right)\Theta =& \Big(B\theta_1 + B^{(q)}\theta_1^q + \cdots + B^{(q^{r-1})}\theta_1^{q^{r-1}}, \dots \\ & \dots, B\theta_r + B^{(q)}\theta_r^q + \cdots + B^{(q^{r-1})}\theta_r^{q^{r-1}}\Big).\end{aligned}$$

Since $B^{(q^r)} = B$ and $\theta_l^{q^r} = \theta_l$, we see that

$$\begin{aligned}\left(B\theta_l + B^{(q)}\theta_l^q + \cdots + B^{(q^{r-1})}\theta_l^{q^{r-1}}\right)^{(q)} =& B^{(q)}\theta_l^q + \cdots + B^{(q^{r-1})}\theta_l^{q^{r-1}} + B\theta_l \\ =& B\theta_l + B^{(q)}\theta_l^q + \cdots + B^{(q^{r-1})}\theta_l^{q^{r-1}}\end{aligned}$$

for $1 \le l \le r$. It is well-known that $a \in K$ satisfies $a^q = a$ if and only if $a \in k$. This means that $\mathcal{B}_m \cdot \Theta \subset \mathrm{M}_{m,n}(k)$. It is clear that $\#\mathcal{B}_m = \#\left(\mathrm{M}_{m,n}(k) \cdot \Theta^{-1}\right) = q^{mn}$. We then obtain $\mathcal{B}_m = \mathrm{M}_{m,n}(k) \cdot \Theta^{-1}$.

Finally, choose $C_1, \dots, C_r \in \mathrm{M}_N(K)$ arbitrary and put $C := \left(C_{(j-i \bmod r)+1}^{(q^{i-1})}\right)_{1 \le i,j \le r} \in \mathcal{C}$. The (i,j)-block C'_{ij} in $C \cdot \Theta$ is

$$\begin{aligned} C'_{ij} =& C_{(1-i \bmod r)+1}^{(q^{i-1})}\theta_j + C_{(2-i \bmod r)+1}^{(q^{i-1})}\theta_j^q + \cdots + C_{r-i+1}^{(q^{i-1})}\theta_j^{q^{r-1}} \\ =& \left(C_1\theta_j + \cdots + C_r\theta_j^{q^{r-1}}\right)^{(q^{i-1})} = (C'_{1j})^{(q^{i-1})}. \end{aligned}$$

This means that $\mathcal{C} \cdot \Theta \subset \mathcal{A}_n = \Theta \cdot \mathrm{M}_n(k)$. Since $\#\mathcal{C} = \#\left(\Theta \cdot \mathrm{M}_n(k) \cdot \Theta^{-1}\right) = q^{n^2}$, we obtain $\mathcal{C} = \Theta \cdot \mathrm{M}_n(k) \cdot \Theta^{-1}$. $\square$

For a monic polynomial $h(t) = c_0 + c_1 t + \cdots + c_{d-1}t^{d-1} + t^d$ of degree d, let

$$C(h) := \begin{pmatrix} 0 & \cdots & 0 & -c_0 \\ 1 & & 0 & -c_1 \\ & \ddots & & \vdots \\ 0 & & 1 & -c_{d-1} \end{pmatrix}.$$

The matrix $C(h)$ is called the companion matrix of $h(t)$. Then the following lemma holds.

Lemma 3.3. *(see [22]) For a matrix $H \in \mathrm{M}_n(k)$, let $h(t) := \det(t \cdot I_n - H)$ be the characteristic polynomial of H and $h(t) = h_1(t) \cdots h_l(t)$ is the factorization of $h(t)$ over k. Suppose that $h(t)$ is square free and put $d_i := \deg(h_i(t))$ for $1 \le i \le l$. Then the following (i) and (ii) hold.*
(i) There exists an invertible matrix $P \in \mathrm{M}_n(k)$ such that

$$P^{-1}HP = C(h_1) \oplus \cdots \oplus C(h_l).$$

(ii) If $P_1, P_2 \in \mathrm{M}_n(k)$ satisfy $P_1^{-1}HP_1 = P_2^{-1}HP_2 = C(h_1) \oplus \cdots \oplus C(h_l)$, then there exist matrices $M_1 \in \mathrm{M}_{d_1}(k), \dots, M_l \in \mathrm{M}_{d_l}(k)$ such that

$$P_1^{-1}P_2 = M_1 \oplus \cdots \oplus M_l.$$

$\square$

3.2 Quadratic forms in multi-HFE

In this subsection, we study the structure of the quadratic forms in multi-HFE.

Recall that the public key of multi-HFE is a quadratic map $F : k^n \to k^n$ is given by

$$F = T \circ \phi^{-1} \circ \mathcal{G} \circ \phi \circ S,$$

where $S, T : k^n \to k^n$ are invertible affine maps, $\mathcal{G} : K^N \to K^N$ is a quadratic map and $\phi : k^n \to K^N$ is a one-to-one map. Due to Lemma 3.1, we have

$$F = (T \circ \Theta^{-1}) \circ (\psi^{-1} \circ \mathcal{G} \circ \psi) \circ (\Theta \circ S).$$

Then, by the definition of ψ and $\mathcal{G}$, we see that

$$\begin{aligned} F(x) =&(T \circ \Theta^{-1})\cdot \\ &\left(\mathcal{G}_1\left((\Theta \circ S)x\right), \dots, \mathcal{G}_N\left((\Theta \circ S)x\right), \mathcal{G}_1\left((\Theta \circ S)x\right)^q, \dots, \dots, \mathcal{G}_N\left((\Theta \circ S)x\right)^{q^{r-1}}\right)^t. \end{aligned} \tag{3}$$

For $X = (X_1, \dots, X_N)^t \in K^N$, let $\bar{X} := \psi^{-1}(X) = \left(X_1, \dots, X_N, X_1^q, \dots, \dots, X_N^{q^{r-1}}\right)^t \in L_N$. Since $\mathcal{G}_1(X), \dots, \mathcal{G}_N(X)$ are quadratic forms, there exists matrices $G_1, \dots, G_N \in \mathrm{M}_N(K)$, low vectors $\beta_1, \dots, \beta_N \in \mathrm{M}_{1,N}(K)$ and constants $\gamma_1, \dots, \gamma_N \in K$ such that

$$\mathcal{G}_l(X) = X^t G_l X + \beta_l X + \gamma_l, \quad (1 \le l \le N).$$

Then the polynomials $\mathcal{G}_l(X), \mathcal{G}_l(X)^q, \dots, \mathcal{G}_l(X)^{q^{r-1}}$ are expressed as quadratic forms of $\bar{X}$ as follows.

$$\begin{aligned} \mathcal{G}_l(X) =&\bar{X}^t(G_l \oplus 0_{n-N})\bar{X} + (\beta_l, 0_{1,n-N})\bar{X} + \gamma_l, \\ \mathcal{G}_l(X)^q =&\bar{X}^t\left(0_{1,N} \oplus G_l^{(q)} \oplus 0_{1,n-2N}\right)\bar{X} + \left(0_{1,N}, \beta_l^{(q)}, 0_{1,n-2N}\right)\bar{X} + \gamma_l^q, \\ &\vdots \\ \mathcal{G}_l(X)^{q^{r-1}} =&\bar{X}^t\left(0_{n-N} \oplus G_l^{(q^{r-1})}\right)\bar{X} + \left(0_{1,n-N}, \beta_l^{(q^{r-1})}\right)\bar{X} + \gamma_l^{q^{r-1}}. \end{aligned} \tag{4}$$

Since the affine maps S, T are given by $Sx = S_0x + s, Ty = T_0y + t$ with matrices $S_0, T_0 \in \mathrm{M}_n(k)$ and column vectors $s, t \in \mathrm{M}_{n,1}(k)$, the quadratic forms $f_1(x), \dots, f_n(x)$ in the public key F are described as follows.

$$\begin{aligned} f_l(x) =&x^t S_0^t \Theta^t \left(E_l \oplus E_l^{(q)} \oplus \cdots \oplus E_l^{(q^{r-1})}\right)\Theta S_0 x \\ &+ x^t S_0^t \Theta^t \left(E_l \oplus E_l^{(q)} \oplus \cdots \oplus E_l^{(q^{r-1})}\right)\Theta s + s^t \Theta^t \left(E_l \oplus E_l^{(q)} \oplus \cdots \oplus E_l^{(q^{r-1})}\right) S_0 x \\ &+ \left(b_l, b_l^{(q)}, \dots, b_l^{(q^{r-1})}\right)\Theta S_0 x + (\text{constant}), \end{aligned} \tag{5}$$

where $E_1, \dots, E_n \in \mathrm{M}_N(K)$ are matrices and $b_1, \dots, b_n \in \mathrm{M}_{1,N}(K)$ are low vectors given by

$$\begin{aligned} (E_1, \dots, E_n)^t =&(T_0\Theta^{-1})(G_1, \dots, G_N, 0_N, \dots, 0_N)^t, \\ (b_1, \dots, b_n)^t =&(T_0\Theta^{-1})(\beta_1, \dots, \beta_N, 0_N, \dots, 0_N)^t. \end{aligned} \tag{6}$$

3.3 Proposed attack on multi-HFE

We now propose our attack on multi-HFE for odd characteristic case as follows.

Proposed Attack on multi-HFE

Input: Public key $F(x) = (f_1(x), \dots, f_n(x))^t$ of multi-HFE.
Output: Two invertible matrices $S', T' \in \mathrm{M}_n(k)$ such that

$$\phi \circ T' \circ F \circ S' \circ \phi^{-1} : K^N \to K^N$$

is a quadratic map.

Step 1. Let $F_1, \dots, F_n \in \mathrm{M}_n(k)$ be the symmetric matrices with

$$f_l(x) = x^t F_l x + (\text{linear}).$$

Take two linear sums W_1, W_2 of $F_1, \dots, F_n$ such that W_1 is invertible and put

$$W := W_1^{-1} W_2.$$

Step 2. Compute the characteristic polynomial $w(t) := \det(t \cdot I_n - W)$ of W and factor $w(t)$ over K. Choose a polynomial $w_0(t)$ of degree N such that

$$w(t) = w_0(t) w_0^{(q)}(t) \cdots w_0^{(q^{r-1})}(t).$$

Step 3. If $w(t)$ is square free and $w_0(t)$ is irreducible, go to the next step. If not, go back to Step 1.
Step 4. Find a matrix $P_0 \in \mathrm{M}_{n,N}(K)$ satisfying $w_0(W)P_0 = 0$ and put

$$P := \left(P_0, P_0^{(q)}, \cdots, P_0^{(q^{r-1})}\right) \in \mathrm{M}_n(k) \cdot \Theta^{-1}.$$

Step 5. If P is invertible, go to the next step. If not, go back to Step 4.
Step 6. Let $\hat{F}_l := P^t F_l P$. Find a matrix $Q_0 \in \mathrm{M}_{N,n}(K)$ with

$$Q_0 \begin{pmatrix} \hat{F}_1 \\ \vdots \\ \hat{F}_n \end{pmatrix} = \begin{pmatrix} \hat{E}_1 \oplus 0_{n-N} \\ \vdots \\ \hat{E}_N \oplus 0_{n-N} \end{pmatrix}.$$

Step 7. If

$$Q := \begin{pmatrix} Q_0 \\ Q_0^{(q)} \\ \vdots \\ Q_0^{(q^{r-1})} \end{pmatrix} \in \Theta \cdot \mathrm{M}_n(k)$$

is invertible, go to the next step. If not, go back to Step 7.
Step 8. Output $S' = P\Theta$ and $T' = \Theta^{-1} Q$.

Once S', T' are recovered, the problem of inverting F is reduced to the problem of finding a common solution of N quadratic equations of N variables. This means that, if $\mathcal{G}$ is chosen randomly, the decryption without secret keys is as fast as the decryption with secret keys. Even if $\mathcal{G}$ has a special structure for fast decryptions, the security is much less than expected since solving N equations of N variables is much faster than solving n equations of n variables in general.

$$\boxed{n \text{ quadratic equations of } n \text{ variables over } k}$$

$$\xrightarrow{\textbf{Our Attack}} \boxed{N \text{ quadratic equations of } N \text{ variables over } K}$$

We now explain why our attack is available.

Table 2: Probability (%) that $\det(t \cdot I_N - W_0)$ is irreducible for $q = 31$

N	2	3	4	5	6	7	8	9	10	$\cdots$
Prob.	49.2	33.4	25.2	19.5	17.4	13.7	12.7	11.2	9.9	$\cdots$

The equation (5) gives

$$F_l = (\Theta S_0)^t \left(E_l \oplus \cdots \oplus E_l^{(q^{r-1})}\right)(\Theta S_0),$$

the matrix W is written by

$$W = (\Theta S_0)^{-1} \left(W_0 \oplus \cdots \oplus W_0^{(q^{r-1})}\right)(\Theta S_0) \tag{7}$$

for some $W_0 \in \mathrm{M}_N(K)$ and the polynomial $w(t)$ is

$$w(t) = \det(t \cdot I_N - W_0) \cdots \det\left(t \cdot I_N - W_0^{(q^{r-1})}\right).$$

If $\det(t \cdot I_N - W_0)$ is irreducible, we have

$$w_0(t) = \det\left(t \cdot I_N - W_0^{(q^l)}\right) \tag{8}$$

for some $0 \leq l \leq r-1$. Then it is easy to see that there exists $L \in \mathrm{M}_N(K)$ with $L^{-1}W_0^{(q^l)}L = C(w_0)$ and it holds

$$\begin{aligned}&\left(\sigma^l\left(L \oplus \cdots \oplus L^{(q^{r-1})}\right)\right)^{-1}\left(W_0 \oplus \cdots \oplus W_0^{(q^{r-1})}\right)\left(\sigma^l\left(L \oplus \cdots \oplus L^{(q^{r-1})}\right)\right)\\ &= C(w_0) \oplus \cdots \oplus C(w_0)^{(q^{r-1})},\end{aligned} \tag{9}$$

where $\sigma := \begin{pmatrix} & I_N & & \\ & & \ddots & \\ & & & I_N \\ I_N & & & \end{pmatrix} \in \mathrm{M}_n(k)$ is a permutation matrix. On the other hand, due to (i) of Lemma 3.3, we see that there exists an invertible matrix $P \in \mathrm{M}_n(K)$ such that

$$P^{-1}WP = C(w_0) \oplus \cdots \oplus C(w_0)^{(q^{r-1})} \tag{10}$$

and it is easy to check that P in Step 4 satisfies (10). Applying (7), (9), (10) into (ii) of Lemma 3.3, we get

$$\Theta S_0 P = \sigma^l \left(\tilde{S} \oplus \cdots \oplus \tilde{S}^{(q^{r-1})}\right), \tag{11}$$

for some invertible matrix $\tilde{S} \in \mathrm{M}_N(K)$. Then the matrix $\hat{F}_l$ in Step 6 is given by

$$\hat{F}_l = P^t F_l P = (\Theta S_0 P)^t \left(E_l \oplus \cdots \oplus E_l^{(q^{r-1})}\right)(\Theta S_0 P) = \hat{E}_l \oplus \cdots \oplus \hat{E}_l^{(q^{r-1})} \tag{12}$$

for some $\hat{E}_l \in \mathrm{M}_N(K)$. Due to (6), we see that there exists Q_0 in Step 7 and it is found by the Gaussian elimination. It is easy to see that Q in Step 8 satisfies

$$QT_0\Theta^{-1} = \sigma^{l_1}\left(\tilde{T} \oplus \cdots \oplus \tilde{T}^{(q^{r-1})}\right) \tag{13}$$

for some $0 \leq l_1 \leq r-1$ and $\tilde{T} \in \mathrm{M}_N(K)$. Combining (5), (11) and (13), we can conclude that the map

$$\begin{aligned}\phi \circ T' \circ F \circ S' \circ \phi^{-1} &= \psi \circ (\Theta \circ T' \circ T \circ \Theta^{-1}) \circ (\psi^{-1} \circ \mathcal{G} \circ \psi) \circ (\Theta \circ S \circ S' \circ \Theta^{-1}) \circ \psi^{-1}\\ &= \psi \circ (Q \circ T \circ \Theta^{-1}) \circ (\psi^{-1} \circ \mathcal{G} \circ \psi) \circ (\Theta \circ S \circ P) \circ \psi^{-1}\end{aligned}$$

is a quadratic map from K^N to K^N. $\square$

Table 3: Experimental results of our attack for $q = 31$

n	N	r	min-rank attack	our attack
30	3	10	37.2bit (1h38m)	1.23s
45	3	15	42.5bit (2d1h)	4.96s
54	3	18	44.8bit (9d16h)	15.0s
60	3	20	46.3bit	22.3s
75	3	25	49.2bit	75.5s
40	4	10	48.5bit	3.37s
60	4	15	55.1bit	15.6s
72	4	18	58.2bit	45.5s
50	5	10	59.9bit	7.65s
60	5	12	63.4bit	12.8s
75	5	15	67.9bit	33.9s
60	6	10	71.3bit	15.0s
72	6	12	75.4bit	40.6s
70	7	10	82.7bit	38.9s
72	8	9	91.0bit	38.0s
72	9	8	98.3bit	41.7s
70	10	7	104.bit	34.7s

Complexity. In Step 1, the attacker takes several basic computations of $n \times n$ matrices over k and then the complexity of Step 1 is $\ll n^3$. Step 2 is for computing the characteristic polynomial of $n \times n$ matrix W and factoring a polynomial $w(t)$ of degree n over K (r-extension of k). Then the complexity of Step 2 is $\ll n^3 \cdot r$.

It is well known that the probability that randomly chosen polynomial of degree N is irreducible is about N^{-1} [24]. In this case, while it is difficult to prove that W_0 is distributed randomly since W_1, W_2 are symmetric, Table 2 shows that its probability seems about N^{-1}.

Step 4 is for finding kernel matrix of $w_0(W)$ and then its complexity is $\ll n^3 \cdot r$. In Step 6 and 7, the attacker takes the Gaussian eliminations and basic linear operations $n \times n$ matrices over K.

We thus conclude that the total complexity of our attack is $\ll n^3 r \cdot N \ll n^4$ on average.

Experiments. In Table 3, we compare our attack with the min-rank attack [4] for $q = 31$. In this table, "min-rank attack" means the complexity $\binom{n+N+1}{N+1}^{\omega}$ of the min-rank attack (see Proposition 13 and its proof of [4]) with $\omega = 2.4$ and the experimental results in Table 5 of [4] by using Magma [25] ver.2.16-10 on 2.93 GHz Intel® Xeon® CPU, and "our attack" means the average of the running times of 100 times experiments of our attack by using Magma [25] ver.2.15-10 on Windows 7, Core-i7 2.67GHz. Table 3 shows that our attack is much faster than the min-rank attack and it is feasible also for larger N.

3.4 Remarks on even characteristic cases

When q is odd, we can choose symmetric matrices $F_1, \ldots, F_n$ as coefficient matrices of quadratic forms in the public key F. On the other hand, F_l cannot be symmetric when q is even. Then we should use $F_l + F_l^t$ instead of F_l when q is even. It is easy to see that these matrices are symmetric and their diagonal entries matrices are zero. For such matrices, the following lemma holds.

Lemma 3.4. *Let k be a finite field of even characteristic, $N \geq 1$ an integer and $A, B \in \mathrm{M}_N(k)$ symmetric matrices. Suppose that the diagonal entries of A, B are zero. Then we have*
(i) if N is odd then $\det A = \det B = 0$.
(ii) if N is even and $\det A \neq 0$, *then the polynomial* $\det(t \cdot I_N - A^{-1}B)$ *is a square of another polynomial of degree $N/2$.*

Proof. When k is of even characteristic, the determinant of the matrix $X = (x_{ij})_{1 \leq i,j \leq N} \in \mathrm{M}_N(k)$ is given by

$$\det X = \sum_{\sigma \in \mathfrak{S}_N} x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{N\sigma(N)}, \tag{14}$$

where $\mathfrak{S}_N$ is the set of permutations among $1, \ldots, N$. It is easy to see that

$$x_{1\sigma^{-1}(1)} x_{2\sigma^{-1}(2)} \cdots x_{N\sigma^{-1}(N)} = x_{\sigma(1)1} x_{\sigma(2)2} \cdots x_{\sigma(N)N}.$$

Then, when X is symmetric and its diagonal entries are zero, we have

$$\det X = \sum_{\sigma \in \mathfrak{S}_N^{(2)}} x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{N\sigma(N)}, \tag{15}$$

where $\mathfrak{S}_N^{(2)} := \{\sigma \in \mathfrak{S}_N \mid \sigma^2 = \mathrm{id}, \sigma(i) \neq i, 1 \leq \forall i \leq N\}$. For a permutation $\sigma \in \mathfrak{S}_N^{(2)}$, there exist pairs $(i_1, j_1), \ldots, (i_s, j_s)$ such that $\sigma(i_l) = j_l$, $\sigma(j_l) = i_l$, $\{i_1, j_1, \ldots, i_s, j_s\} = \{1, \ldots, N\}$ and $i_1, j_1, \ldots, i_s, j_s$ are distinct to each other When N is odd, there are no such pairs. This means that $\mathfrak{S}_N^{(2)}$ is empty and then (i) holds. When N is even, there are such pairs and, for $\sigma \in \mathfrak{S}_N^{(2)}$,

$$x_{1\sigma(1)} \cdots x_{N\sigma(N)} = \left(x_{i_1 j_1} \cdots x_{i_{N/2} j_{N/2}}\right)^2.$$

Since k is of even characteristic, we have

$$\det X = \left(\sum_{\sigma \in \mathfrak{S}_N^{(2)}} x_{i_1 j_1} \cdots x_{i_{N/2} j_{N/2}}\right)^2, \tag{16}$$

where $\{(i_1, j_1), \ldots, (i_{N/2}, j_{N/2})\}$ depends on σ. Since $\det(tI_N - A^{-1}B) = (\det A)^{-1} \det(tA - B)$, (ii) follows immediately from (16). $\square$

This lemma shows that our attack on multi-HFE given in §3.3 cannot be used for even characteristic cases directly, since W_2 in Step 1 cannot be invertible when N is odd and $w_0(t)$ in Step 3 cannot be irreducible when N is even. We will arrange it in the future.

4 Conclusion

We propose a new attack on multi-HFE to recover equivalent secret keys for odd characteristic cases, which is much faster than the the min-rank attack [4]. While our attack is not presently available for even characteristic cases, we can claim that MPKCs derived from a "quadratic" map over an extension field cannot be recommended for practical use.

Acknowledgment. The author is partially supported by JSPS Grant-in-Aid for Young Scientists (B) no. 26800020.

References

[1] M.L. Akkar, N. Courtois, L. Goubin, R. Duteuil, A fast and secure implementation of Sflash, PKC'03, LNCS **2567** (2003), pp.267–278.

[2] M. Bardet, J.C. Faugère, B. Salvy, B.Y. Yang, Asymptotic Expansion of the Degree of Regularity for Semi-Regular Systems of Equations, MEGA'05 (2005).

[3] L. Bettale, J.C. Faugère, L. Perret, Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach, ISSAC 2012 (2012), pp.67–74.

[4] 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.

[5] O. Billet and G. Macario-Rat: Cryptanalysis of the Square cryptosystems, Asiacrypt'09, LNCS **5912** (2009), pp.451-468.

[6] A.I.T. Chen, M.S. Chen, T.R. Chen, C.M. Chen, J. Ding, E.L.H. Kuo, F.Y.S. Lee, B.Y. Yang, SSE Implementation of Multivariate PKCs on Modern x86 CPUs, CHES'09, LNCS **5747** (2009), pp.33–48.

[7] C.H.O. Chen, M.S. Chen, J. Ding, F. Werner, B.Y. Yang, Odd-char multivariate Hidden Field Equations, http://eprint.iacr.org/2008/543.

[8] C. Clough, J. Baena, J. Ding, B.-Y. Yang, and M.-S. Chen: Square, a new multivariate encryption scheme, CT-RSA'09, LNCS **5473** (2009) pp.252-264.

[9] N.T. Courtois, M. Daum, P. Felke, On the security of HFE, HFEv- and Quartz, PKC'03, LNCS **2567** (2003), pp.337–350.

[10] J. Ding, T. J. Hodges, Inverting HFE systems is quasi-polynomial for all fields, Crypto'11, LNCS **6841** (2011), pp.724–742.

[11] J. Ding, L. Hu, X. Nie, J. Li, and J. Wagner: High Order Linearization Equation (HOLE) attack on multivariate public key cryptosystems, PKC'07, LNCS **4450** (2007), pp.233-248.

[12] J. Ding, D. Schmidt, Rainbow, a new multivariate polynomial signature scheme, ACNS'05, LNCS **3531** (2005), pp.164–175.

[13] J. Ding, C. Wolf, B.Y. Yang, $l-$invertible cycles for Multivariate Quadratic (MQ) public key cryptography, PKC'07, LNCS **4450** (2007), pp.266–281.

[14] V. Dubois, P.A. Fouque, A. Shamir, J. Stern, Practical cryptanalysis of SFLASH, Crypto'07, LNCS **4622** (2007), pp.1–12.

[15] J.C. Faugère, A new efficient algorithm for computing Grobner bases (F_4), J. Pure and Applied Algebra **139** (1999), pp.61–88.

[16] J.C. Faugère, A. Joux, Algebraic cryptanalysis of Hidden Field Equations (HFE) using Grobner bases, Crypto'03, LNCS **2729** (2003), pp.44–60.

[17] J.C. Faugère, F. Levy-dit-Vehel, L. Perret, Cryptanalysis of MinRank, Crypto'08, LNCS **5157** (2008), pp.280–296.

[18] P.A. Fouque, G. Macario-Rat, L. Perret, J. Stern, Total break of the $l-$IC signature scheme, PKC'08, LNCS **4939** (2008), pp.1–17.

[19] M.R. Garey, D.S. Johnson, Computers and Intractability, A Guide to the Theory of NP-completeness, W.H. Freeman, 1979.

[20] J. Gathen, D. Panario, Factoring Polynomials Over Finite Fields: A Survey, J. Symbolic Computation **31** (2001), pp.3–17.

[21] L. Granboulan, A. Joux, J. Stern, Inverting HFE is quasipolynomial, Crypto'06, LNCS **4117**, pp.345–356.

[22] Y. Hashimoto, Cryptanalysis of the multivariate sigature scheme proposed in PQCrypto 2013, PQCrypto'14, LNCS **8772**, (2014), pp.108–125.

[23] A. Kipnis, A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, Crypto'99, LNCS **1666** (1999), pp.19–30.

[24] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, 1983.

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

[26] T. Matsumoto, H. Imai, Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, Eurocrypt'88, LNCS **330** (1988), pp.419–453.

[27] J. Patarin, Cryptoanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88, Crypto'95, LNCS **963** (1995), pp.248–261.

[28] J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, Eurocrypt'96, LNCS **1070** (1996), pp.33–48.

[29] , J. Patarin, N. Courtois, L. Goubin, QUARTZ, 128-bit long digital signatures, CT-RSA'01, LNCS **2020**, pp.282-297.

[30] J. Porras, J. Baena, and J. Ding, ZHFE, a new multivariate public key encryption scheme, PQCrypto'14, LNCS **8772**, pp.229-245.

[31] L.C. Wang, B.Y. Yang, Y.H. Hu, and F. Lai, A "medium-field" multivariate public-key encryption scheme, CT-RSA'06, LNCS **3860** (2006), pp.132-149.