PAPER *Special Section on Cryptography and Information Security*

Key Recovery Attacks on Multivariate Public Key Cryptosystems Derived from Quadratic Forms over an Extension Field

Yasufumi HASHIMOTO[†a), ***Member***

SUMMARY One of major ideas to design a multivariate public key cryptosystem (MPKC) is to generate its quadratic forms by a polynomial map over an extension field. In fact, Matsumoto-Imai's scheme (1988), HFE (Patarin, 1996), MFE (Wang et al., 2006) and multi-HFE (Chen et al., 2008) are constructed in this way and Sflash (Akkar et al., 2003), Quartz (Patarin et al., 2001), Gui (Petzoldt et al, 2015) are variants of these schemes. An advantage of such extension field type MPKCs is to reduce the numbers of variables and equations to be solved in the decryption process. In the present paper, we study the security of MPKCs whose quadratic forms are derived from a "quadratic" map over an extension field and propose a new attack on such MPKCs. Our attack recovers partial information of the secret affine maps in polynomial time when the field is of odd characteristic. Once such partial information is recovered, the attacker can find the plain-text for a given cipher-text by solving a system of quadratic equations over the extension field whose numbers of variables and equations are same to those of the system of quadratic equations used in the decryption process.

key words: *multivariate public-key cryptosystems (MPKC), post-quantum cryptography, extension field, quadratic forms*

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 equations over a finite field of order 2 is NP hard [14] and then MPKC has been expected as a cryptosystem resisting against attacks by quantum computers.

One of major ideas to design MPKCs is to generate quadratic forms by a polynomial map over an extension field. For example, the quadratic forms in Matsumoto-Imai's scheme [21] and Hidden Field Equations (HFE) [23] are derived from a univariate monomial/polynomial over an extension field, and those in MFE [27] and multi-HFE [8] are derived from a set of multivariate quadratic forms over an extension field. An advantage of such a construction is that one can reduce the numbers of variables and polynomials in the system of polynomial equations to be solved for decryption. Since, in general, the complexity of solving a system of polynomial equations highly depends on the numbers of variables and polynomials [5], [12], it is expected that an efficient scheme can be generated by such a construction.

However, most known schemes in this type are less secure than expected. In fact, Matsumoto-Imai's scheme and MFE are broken by the linearlization attacks [10], [22], Sflash [1] is broken by the differential attack [11] and (the original) HFE/multi-HFE have an unwelcome trade-off between efficiency and security (especially against the min-rank attack [6], [19]). These facts have made us suspect that such extension field type MPKCs might have structural vulnerabilities.

In the present paper, we study the security of general MPKCs whose quadratic forms are derived from a "quadratic" map over an extension field. As a result, we propose a new attack on such MPKCs for odd characteristic case to recover a quadratic map equivalent to the quadratic map to be used for decryption in polynomial time. While the complexity of the min-rank attack [6] highly depends on the numbers of variables and quadratic forms over the extension field, our attack does not (highly) depend on them. We actually succeeded to recover equivalent secret keys of examples of multi-HFE in about fifteen seconds on average, which were recovered in about nine days by the min-rank attack. This means that, at least for the "quadratic" case, the field extension approach is not practical for constructing secure and efficient MPKCs.

2. Multivariate Public Key Cryptosystems

2.1 General Construction of MPKCs

Let $n, m \geq 1$ be integers, k a finite field and q the order of k. The public key of a multivariate public key cryptosystem (MPKC) is given by a set of quadratic forms

$$f_1(x_1, \cdots, x_n) = \sum_{1\leq i\leq j\leq n} a_{ij}^{(1)} x_i x_j + \sum_{1\leq i\leq n} b_i^{(1)} x_i + c^{(1)},$$

$$\vdots$$

$$f_m(x_1, \cdots, x_n) = \sum_{1\leq i\leq j\leq n} a_{ij}^{(m)} x_i x_j + \sum_{1\leq i\leq n} b_i^{(m)} x_i + c^{(m)},$$

over k. Most MPKCs are described as follows.

Secret key. Two invertible affine maps $S : k^n \to k^n$, $T : k^m \to k^m$ and a quadratic map $G : k^n \to k^m$ inverted feasibly.

Public key. The quadratic map $F := T \circ G \circ S$.

$$F : k^n \xrightarrow{S} k^n \xrightarrow{G} k^m \xrightarrow{T} k^m.$$

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

Manuscript received March 19, 2016.
Manuscript revised June 14, 2016.

[†]The author is with the Department of Mathematical Sciences, University of the Ryukyus, Okinawa-ken, 903-0213 Japan.
a) E-mail: hashimoto@math.u-ryukyu.ac.jp

DOI: 10.1587/transfun.E100.A.18

Decryption. Compute $z := T^{-1}(c) \in k^m$ and find $w \in k^n$ such that $G(w) = z$. The plain-text is $p = S^{-1}(w) \in k^n$.

2.2 Extension Field Type Scheme

There have been MPKCs whose quadratic map G is derived from a polynomial map over an extension field of k. In this subsection, we study such schemes.

Let $r \geq 1$ be a divisor of $\gcd(m, n)$, $N := n/r$, $M := m/r$ and K an extension field with $[K : k] = r$. In extension field type MPKCs, the map G is given by $G = \phi_M^{-1} \circ \mathcal{G} \circ \phi_N$ where $\phi_N : k^n \to K^N$ is a one-to-one map and $\mathcal{G} : K^N \to K^M$ is a polynomial map over K.

$$G : k^n \xrightarrow{\phi_N} K^N \xrightarrow{\mathcal{G}} K^M \xrightarrow{\phi_M^{-1}} k^m.$$

For example, in Matsumoto-Imai's scheme [21], q is even, $N = M = 1$ ($r = n$) and

$$\mathcal{G}(X) = X^{q^i+1},$$

where i is an integer with $\gcd(q^i + 1, q^n - 1) = 1$. The decryption is computed by $Y^\theta = G^{-1}(Y) = X$ with $\theta(q^i + 1) \equiv 1 \bmod q^n - 1$. Unfortunately, Patarin [22] proposed the linearlization attack to recover the message based on the relation $Y^{q^i} X = X^{q^{2i}} Y$. In HFE [23], the map $\mathcal{G}$ is given by

$$\mathcal{G}(X) = \sum_{0 \leq i \leq j \leq d} \alpha_{ij} X^{q^i+q^j} + \sum_{0 \leq i \leq j \leq d} \beta_i X^{q^i} + \gamma.$$

where $d \geq 1$ is an integer and $\alpha_{ij}, \beta_i, \gamma \in K$. The inversion of $\mathcal{G}$ is computed by the Berlekamp algorithm whose complexity depends on the degree of $\mathcal{G}$ (see e.g. Chapter 20 of [26]). Since the degree of $\mathcal{G}$ is at most $2q^d$, the numbers q, d cannot be too large. It is known that the complexity of the min-rank attack to recover (partial information of) T depends on d and is estimated by $O(\binom{n+d+2}{d+2}^w)$ where $2 \leq w < 3$ is the exponent of the Gaussian elimination [6], [19]. Then HFE with small d is not secure against the min-rank attack. Furthermore, it is also known that the Gr´obner basis algorithm can recover the message of HFE effectively if d is small [9], [13], [16]. In fact, the degree of regularity of the system $\{f_1(x) - y_1, \ldots, f_n(x) - y_n\}$ is bounded by $\frac{1}{2}(q-1)\lfloor \log_q (2q^d - 1) + 1 \rfloor + 2$ [9], [16]. This means that HFE is not secure when q and d are small.

In both Matsumoto-Imai's scheme and HFE, the polynomial map $\mathcal{G}$ is given by a univariate ($N = 1$) polynomial of higher degree. On the other hand, there have been MPKCs such that $\mathcal{G}$ is multivariate ($N > 1$) and quadratic, namely

$$\begin{aligned}&\mathcal{G}(X_1, \ldots, X_N)\\ &= (\mathcal{G}_1(X_1, \ldots, X_N), \ldots, \mathcal{G}_M(X_1, \ldots, X_N))^t\end{aligned}$$

is written by

$$\begin{aligned}&\mathcal{G}_l(X_1, \ldots, X_N)\\ &= \sum_{1 \leq i \leq j \leq N} \alpha_{ij}^{(l)} X_i X_j + \sum_{1 \leq i \leq N} \beta_i^{(l)} X_i + \gamma^{(l)}\end{aligned}$$

for $1 \leq l \leq M$. For example, MFE [27] is an extension field type MPKC such that $(N, M) = (12, 15)$ and $\mathcal{G}$ is a special type quadratic map to be inverted feasibly. In multi-HFE [8], $N = M$ are small enough and $\mathcal{G}$ is a randomly chosen quadratic map. Since $N, M \geq 1$ are small, the complexity of inverting $\mathcal{G}$ is not large (see Table 1 of [8] for the efficiency of multi-HFE). Unfortunately, MFE is also broken by the linearlization attack [10] and multi-HFE with small N is not secure against the min-rank attack [6]. In fact, the complexity is estimated by $O\left(\binom{n+N+1}{N+1}^{\omega}\right) = O\left(r^{(N+1)w}\right)$ in Proposition 13 of [6].

3. Proposed Attack

In this section, we propose our attack for odd q. Before describing it, we give several notations and lemmas as a preparation of our attack.

3.1 Preliminary

3.1.1 Finite Fields k and K

Recall that k is a finite field of order q and K is its r-extension. The following lemma holds.

Lemma 3.1: Let $a \in K$. Then we have
(i) $a \in K$ satisfies $a^q = a$ if and only if $a \in k$,
(ii) $a + a^q + \cdots + a^{q^{r-1}} \in k$.

Proof. It is clear that $a^q = a$ for any $a \in k$. Since the number of solutions of the equation $x^q - x = 0$ is at most $q = \#k$, we see that (i) holds.

Let $b := a + a^q + \cdots + a^{q^{r-1}}$. Since $b^q = a^q + \cdots + a^{q^{r-1}} + a = b$, (ii) follows immediately from (i). □

3.1.2 Matrices of k and K

For integers $n_1, n_2 \geq 1$, 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 an integer $l \geq 1$, a matrix $A = (a_{ij})_{i,j}$ and a polynomial $g(t) = c_0 + c_1 t + \cdots + c_d t^d$, 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 $A_1 \in \mathrm{M}_{n_1}(k), \ldots, A_l \in \mathrm{M}_{n_l}(k)$, the direct sum $A_1 \oplus \cdots \oplus A_l$ means

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

Recall that $r = [K : k]$ and choose a basis $\{\theta_1, \ldots, \theta_r\}$ of K over k. Define the matrix

$$\Theta_N := \left(\theta_j^{q^{i-1}} I_N\right)_{1 \leq i,j \leq r} \in \mathrm{M}_n(K)$$

and the sets of matrices

$$\begin{aligned}\mathcal{A}_N &:= \left\{ \left(A_j^{(q^{i-1})} \right)_{1 \le i,j \le r} \,\middle|\, A_1, \dots, A_r \in \mathrm{M}_N(K) \right\},\\ \mathcal{B}_N &:= \left\{ \left(B_i^{(q^{j-1})} \right)_{1 \le i,j \le r} \,\middle|\, B_1, \dots, B_r \in \mathrm{M}_N(K) \right\},\\ \mathcal{C}_N &:= \left\{ \left(C_{(j-i \bmod r)+1}^{(q^{i-1})} \right)_{1 \le i,j \le r} \,\middle|\, C_1, \dots, C_r \in \mathrm{M}_N(K) \right\}.\end{aligned}$$

Then the following lemma holds.

Lemma 3.2: For any $N \ge 1$, we have

$$\begin{aligned}\mathcal{A}_N &= \Theta_N \cdot \mathrm{M}_n(k),\\ \mathcal{B}_N &= \mathrm{M}_n(k) \cdot \Theta_N^{-1}, \qquad (1)\\ \mathcal{C}_N &= \Theta_N \cdot \mathrm{M}_n(k) \cdot \Theta_N^{-1}.\end{aligned}$$

Proof. First, choose $A = (A_{ij})_{1 \le i,j \le r} \in \mathrm{M}_n(k)$ arbitrary. The (i,j)-block A'_{ij} of $\Theta_N A$ is

$$A'_{ij} = \theta_1^{q^{i-1}} A_{1j} + \cdots + \theta_r^{q^{i-1}} A_{rj}.$$

Since $A_{ij}^{(q)} = A_{ij}$, we have

$$A'_{ij} = (\theta_1 A_{1j} + \cdots + \theta_r A_{rj})^{(q^{i-1})} = (A'_{1j})^{(q^{i-1})}.$$

This means that $\Theta_N A \in \mathcal{A}_N$ and then $\Theta_N \cdot \mathrm{M}_n(k) \subset \mathcal{A}_N$.

Next, choose $B = (B_i^{(q^{j-1})})_{1 \le i,j \le r} \in \mathcal{B}_N$ arbitrary. The (i,j)-block B'_{ij} of $B\Theta_N$ is

$$B'_{ij} = B_i \theta_j + B_i^{(q)} \theta_j^q + \cdots + B_i^{(q^{r-1})} \theta_j^{q^{r-1}}.$$

Due to (ii) of Lemma 3.1, we see that $B'_{ij} \in \mathrm{M}_N(k)$. This means that $B\Theta_N \in \mathrm{M}_n(k)$ and then $\mathcal{B}_N \subset \mathrm{M}_n(k) \cdot \Theta_N^{-1}$.

Choose $C = \left(C_{(j-i \bmod r)+1}^{(q^{i-1})} \right)_{1 \le i,j \le r} \in \mathcal{C}_N$ arbitrary. The (i,j)-block C'_{ij} in $C \cdot \Theta_N$ is

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

This means that $C\Theta_N \in \mathcal{A}_N$ and then $\mathcal{C}_N \subset \mathcal{A}_N \cdot \Theta_N^{-1}$.

It is easy to see that all of the numbers of elements in the sets $\mathrm{M}_n(k)$, $\mathcal{A}_N$, $\mathcal{B}_N$ and $\mathcal{C}_N$ coincide with q^{n^2}. We thus conclude that this lemma holds. □

3.1.3 Diagonalization

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: (Lemma 4.1 of [17]) 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

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

(ii) If $P_1, P_2 \in \mathrm{M}_n(k)$ satisfy

$$P_1^{-1} H P_1 = P_2^{-1} H P_2 = C(h_1) \oplus \cdots \oplus C(h_l),$$

then there exist matrices $M_1 \in \mathrm{M}_{d_1}(k), \dots, M_l \in \mathrm{M}_{d_l}(k)$ such that

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

3.2 Quadratic Forms

In this subsection, we study the structure of the quadratic forms in the public key F when $\mathcal{G}$ is a quadratic map.

Recall that the public map F is constructed by

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

where $S : k^n \to k^n, T : k^m \to k^m$ are invertible affine maps, $\mathcal{G} : K^N \to K^M$ is a quadratic map and $\phi_N : k^n \to K^N$ is a one-to-one map. Since

$$\phi_N = \psi_N^{-1} \circ \Theta_N \qquad (2)$$

where $\psi_N : K^N \to K^n$ is a map with $\psi_N(\alpha_1, \dots, \alpha_N) = (\alpha_1, \dots, \alpha_N, \alpha_1^q, \dots, \dots, \alpha_N^{q^{r-1}})^t$, the public key F is described by

$$F = (T \circ \Theta_M^{-1}) \circ (\psi_M \circ \mathcal{G} \circ \psi_N^{-1}) \circ (\Theta_N \circ S),$$

namely

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

Since $\mathcal{G}_1(X), \dots, \mathcal{G}_M(X)$ are quadratic forms of $X = (X_1, \dots, X_N)^t$, the polynomial $\mathcal{G}_j(X)^{q^{i-1}}$ is expressed by

$$\begin{aligned}\mathcal{G}_j(X)^{q^{i-1}} = &\bar{X}^t \left(0_{(i-1)N} \oplus G_j^{(q^{i-1})} \oplus 0_{n-iN} \right) \bar{X}\\ &+ (\text{linear form of } X^{(q^{i-1})}),\end{aligned}$$

where

$$\bar{X} := \psi_N(X) = (X_1, \dots, X_N, X_1^q, \dots, \dots, X_N^{q^{r-1}})^t$$

and $G_j \in \mathrm{M}_N(K)$ is the matrix with $\mathcal{G}_j(X) = X^t G_j X +$

(linear form of X). Then, due to Lemma 3.2, the quadratic forms $f_1(x), \dots, f_m(x)$ in the public key F are described by

$$\begin{aligned} f_l(x) =& x^t (\Theta_N S_0)^t \left(E_l \oplus \cdots \oplus E_l^{(q^{r-1})}\right) (\Theta_N S_0) x \\ & + \text{(linear form of } x\text{)}, \end{aligned} \tag{4}$$

where $S_0 \in \mathrm{M}_n(k)$ is the linear part of S (namely $S(x) = S_0 x + s$) and $E_1, \dots, E_m \in \mathrm{M}_N(K)$ are given by

$$\begin{aligned} &(E_1, \dots, E_m)^t \\ =&(T_0 \Theta_M^{-1})(G_1, \dots, G_M, 0_N, \dots, 0_N)^t, \end{aligned} \tag{5}$$

where $T_0 \in \mathrm{M}_m(k)$ is the linear part of T (namely $T(y) = T_0 y + t$).

3.3 Proposed Attack

According to the previous subsection, we see that the map

$$\phi_M \circ F \circ \phi_N^{-1} : K^N \to K^M$$

is described as a set of quadratic forms of $\bar{X} = (X_1, \dots, X_N, X_1^q, \dots, \dots, \dots, X_N^{q^{r-1}})^t$. Since the polynomials $\mathcal{G}_1(X), \dots, \mathcal{G}_M(X)$ in the map $\mathcal{G} : K^N \to K^M$ are quadratic forms of $X = (X_1, \dots, X_N)^t$, there exist $S' \in \mathrm{M}_n(k)$ and $T' \in \mathrm{M}_m(k)$ such that the map

$$\begin{aligned} &\phi_M \circ T' \circ F \circ S' \circ \phi_N^{-1} \\ &= (\phi_M \circ T' \circ \phi_M^{-1}) \circ (\phi_M \circ G \circ \phi_N^{-1}) \circ (\phi_N \circ S' \circ \phi_N^{-1}) \end{aligned}$$

is also a set of quadratic forms of $(X_1, \dots, X_N)$. Once such S' and T' are recovered, the attacker can obtain the desired message or a dummy signature by solving a system of M quadratic equations of N variables over K, not a system of m quadratic equations of n variables over k. This means that the advantage of extension field type construction is lost by S' and T'.

In this subsection, we propose an attack to recover such S' and T' when q is odd.

Proposed Attack

Input: Public key $F(x) = (f_1(x), \dots, f_m(x))^t$.

Output: Two invertible matrices $S' \in \mathrm{M}_n(k), T' \in \mathrm{M}_m(k)$ such that

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

is a quadratic map.

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

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

Take two linear sums W_1, W_2 of $F_1, \dots, F_m$ 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

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

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

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

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 $Q_0 \in \mathrm{M}_{M,m}(K)$ such that

$$Q_0 \begin{pmatrix} \hat{F}_1 \\ \vdots \\ \hat{F}_m \end{pmatrix} = \begin{pmatrix} \hat{E}_1 \oplus 0_{n-N} \\ \vdots \\ \hat{E}_M \oplus 0_{n-N} \end{pmatrix} \tag{6}$$

for some $\hat{E}_1, \dots, \hat{E}_M \in \mathrm{M}_N(K)$.

Step 7. If the matrix

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

is invertible, go to the next step. If not, go back to Step 6.

Step 8. Output $S' = P \Theta_N$ and $T' = \Theta_M^{-1} Q$.

We now explain why our attack is available. Due to the equation (4), we can write the matrix W by

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

for some $W_0 \in \mathrm{M}_N(K)$. Then 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, the polynomial $w_0(t)$ is

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

for some $0 \leq l \leq r-1$. According to Lemma 3.3, we see that there exists an invertible matrix $L \in \mathrm{M}_N(K)$ with $L^{-1} W_0^{(q^l)} L = C(w_0)$ and it holds

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

On the other hand, (i) of Lemma 3.3 tells that there exists an invertible matrix $P \in \mathrm{M}_n(K)$ with

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

It is easy to check that $P \in \mathrm{M}_n(k)\Theta_N^{-1}$ in Step 4 satisfies (10) by comparing the matrix WP with $P\left(C(w_0) \oplus \cdots \oplus C(w_0)^{(q^{r-1})}\right)$. Applying (7), (9), (10) into (ii) of Lemma 3.3, we get

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

for some invertible matrix $\tilde{S} \in \mathrm{M}_N(K)$, where

$$\sigma := \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix} \otimes I_N \in \mathrm{M}_n(k)$$

is a permutation matrix. Then the matrix $\hat{F}_l$ in Step 6 satisfies

$$\begin{aligned}\hat{F}_l =& P^t F_l P\\=&(\Theta_N S_0 P)^t \left(E_l \oplus \cdots \oplus E_l^{(q^{r-1})}\right)(\Theta_N S_0 P)\\=&\tilde{E}_l \oplus \cdots \oplus \tilde{E}_l^{(q^{r-1})}\end{aligned} \tag{12}$$

for some $\tilde{E}_l \in \mathrm{M}_N(K)$.

From the equations (4), (5) and Lemma 3.2, we see that

$$\begin{pmatrix} E_1 \oplus \cdots \oplus E_1^{(q^{r-1})} \\ \vdots \\ E_m \oplus \cdots \oplus E_m^{(q^{r-1})} \end{pmatrix} = (T_0\Theta_M^{-1})\begin{pmatrix} G_1 \oplus 0_{n-N} \\ \vdots \\ G_M \oplus 0_{n-N} \\ 0_N \oplus G_1^{(q)} \oplus 0_{n-2N} \\ \vdots \\ \vdots \\ 0_{n-N} \oplus G_M^{(q^{r-1})} \end{pmatrix}.$$

This means that, if the matrix Q_0 satisfies

$$\begin{aligned}Q_0 T_0 \Theta_M^{-1} =&(\tilde{T}, 0_{M,m-M}), \quad (0_M, \tilde{T}, 0_{M,m-2M}),\\&\ldots, \quad \text{or} \quad (0_{M,m-M}, \tilde{T})\end{aligned} \tag{13}$$

for some $\tilde{T} \in \mathrm{M}_M(K)$, the equation (6) holds for some $\hat{E}_1, \ldots, \hat{E}_M \in \mathrm{M}_N(K)$. Then the matrix Q_0 in Step 6 exists and it is found by the Gaussian elimination. From (13), we see that the matrix Q in Step 7 satisfies

$$QT_0\Theta_M^{-1} = \sigma^{l_1}\left(\tilde{T} \oplus \cdots \oplus \tilde{T}^{(q^{r-1})}\right) \tag{14}$$

for some $0 \leq l_1 \leq r-1$. Combining (4), (11) and (14), we can conclude that the map

$$\begin{aligned}&\phi_M \circ T' \circ F \circ S' \circ \phi_N^{-1}\\=&\psi_M^{-1} \circ (\Theta_M \circ T' \circ T \circ \Theta_M^{-1}) \circ (\psi_M \circ \mathcal{G} \circ \psi_N^{-1})\\&\circ (\Theta_N \circ S \circ S' \circ \Theta_N^{-1}) \circ \psi_N\\=&\psi_M^{-1} \circ (Q \circ T \circ \Theta_M^{-1}) \circ (\psi_M \circ \mathcal{G} \circ \psi_N^{-1})\\&\circ (\Theta_N \circ S \circ P) \circ \psi_N\end{aligned}$$

is a quadratic map from K^N to K^M. □

3.4 Complexity and Experiments

In this subsection, we estimate the complexity of our attack and describe experimental results.

3.4.1 Complexity

Step 1 includes several basic operations of $n \times n$ matrices over k. Then its complexity is estimated by $\ll n^3(\log q)^2$ if one uses naive algorithms for multiplications of elements of k and matrices over k.

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). The numbers of field operations of these computations are known to be $\ll n^3$ by Keller-Gehrig's algorithm [18] and $\ll n^3 + n^2 \log q^r$ by Berlekamp's algorithm [3], [4] respectively. Then the complexity of Step 2 is $\ll (r^2n^3 + r^3n^2 \log q) \cdot (\log q)^2$.

It is well known that the probability that a randomly chosen polynomial of degree N is irreducible is about N^{-1} [20]. In our case, while it is difficult to prove that W_0 given in Step 2 is distributed randomly, Table 1, which is based on the result of 10,000 times experiments, shows that the probability that $w_0(t)$ satisfies the condition in **Step 3** is about N^{-1}. Then the attacker will repeat Step 1–3 about N times on average.

Step 4 is for finding a kernel matrix of $w_0(W)$. Before computing the kernel, we need to compute $W^2, W^3, \ldots, W^N$ for determining $w_0(W)$. Furthermore, the number of operations to compute the kernel is known to be $\ll n^3$ [2]. Then the complexity of **Step 4** is $\ll Nn^3 \cdot r^2(\log q)^2 = n^4 r(\log q)^2$. **Step 5** is for checking invertibility of an $n \times n$ matrix over K with the complexity $\ll n^3 \cdot r^2(\log q)^2$.

In **Step 6**, the attacker computes $2m$ times multiplication of $n \times n$ matrices over K to compute $\hat{F}$ and use the Gaussian elimination to find Q_0. Then the complexity of Step 6 is $\ll m \cdot n^3 \cdot r^2(\log q)^2$. **Step 7** is for checking

Table 1 Probability (%) that $\det(t \cdot I_N - W_0)$ is irreducible for $q = 31$.

N	2	3	4	5	6	7
Prob.	49.2	33.4	25.2	19.5	17.4	13.7

8	9	10	11	12	$\cdots$
12.7	11.2	9.9	9.0	8.2	$\cdots$

Table 2 Experiments of our attack for $q = 31$.

n	N	r	min-rank	our attack
30	3	10	1h38m	1.01s
33	3	11	—	1.57s
36	3	12	—	1.75s
39	3	13	—	3.82s
42	3	14	—	6.58s
45	3	15	2d1h	5.08s
48	3	16	—	7.26s
51	3	17	—	11.4s
54	3	18	9d16h	14.5s
57	3	19	—	19.6s
60	3	20	—	26.3s
50	5	10	—	7.58s
55	5	11	—	10.7s
60	5	12	—	12.9s
65	5	13	—	24.8s
70	5	14	—	46.4s
75	5	15	—	38.8s
80	5	16	—	64.7s
85	5	17	—	83.3s
90	5	18	—	103s
72	3	24	—	61.8s
72	4	18	—	43.0s
72	6	12	—	27.9s
72	8	9	—	23.9s
72	9	8	—	25.5s
72	12	6	—	16.2s
72	18	4	—	4.16s
72	24	3	—	2.44s

invertibility and then its complexity is $\ll m^3 \cdot r^2(\log q)^2$.

We thus conclude that the total complexity of our attack is roughly estimated by $\ll (r^2n^3 + r^3n^2 \log q)(\log q)^2 \cdot N + rn^4(\log q)^2 + n^3mr^2(\log q)^2 + m^3r^2(\log q)^2 \sim (rn^4 + r^2n^3 \log q + r^2n^3m + r^2m^3)(\log q)^2$ on average. When N and M are similar and q is not much larger than 2^N, it is $O\left(n^4r^2(\log q)^2\right)$, namely our attack works in polynomial time, and it is faster than the min-rank attack $\binom{n+N+1}{N+1}^w$ [6] especially for large N.

3.4.2 Experiments

We implemented our attack by using Magma [7] ver.2.15-10 on Windows 7, Core-i7 2.67 GHz and succeeded to recover equivalent secret keys. Table 2 describes the running times of our attack for $q = 31$ and $N = M$. We also attach on Table 2 the running times of the min-rank attack given in [6] by using Magma ver.2.16-10 on 2.93 GHz Intel® Xeon® CPU. This table shows that our attack can recover equivalent keys much faster than the min-rank attack for $N = 3$ and is able to recover them also for larger N with feasible running times. We thus claim that the extension field type MPKCs with quadratic $\mathcal{G}$ is vulnerable against our attack and our attack works much faster than the min-rank attack.

3.5 Remarks on Even Characteristic Cases

When q is odd, we can choose symmetric matrices $F_1, \ldots, F_n$ as coefficient matrices of the quadratic forms. However, if q is even, F_l cannot be symmetric and we should use $F_l + F_l^t$ instead of F_l. It is easy to see that these matrices are symmetric and their diagonal entries 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 and 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

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

where $\mathfrak{S}_N$ is the set of all permutations among $1, \ldots, N$. Now, let $i_j := \sigma^{-1}(j)$ for a given $\sigma \in \mathfrak{S}_N$ and $1 \leq j \leq N$. Since $j = \sigma(i_j)$ and $\{i_1, \ldots, i_N\} = \{1, \ldots, N\}$, we have

$$\begin{aligned} &x_{1\sigma^{-1}(1)}x_{2\sigma^{-1}(2)}\cdots x_{N\sigma^{-1}(N)} \\ =&x_{\sigma(i_1)i_1}x_{\sigma(i_2)i_2}\cdots x_{\sigma(i_N)i_N} \\ =&x_{\sigma(1)1}x_{\sigma(2)2}\cdots x_{\sigma(N)N} \end{aligned} \tag{16}$$

From the equation (16) and the assumption that X is symmetric, we see that

$$\begin{aligned} &x_{1\sigma^{-1}(1)}x_{2\sigma^{-1}(2)}\cdots x_{N\sigma^{-1}(N)} \\ =&x_{1\sigma(1)}x_{2\sigma(2)}\cdots x_{N\sigma(N)}. \end{aligned} \tag{17}$$

The equation (17) means that, since the right hand side of (15) includes both the terms corresponding to σ and σ^{-1} if $\sigma^2 \neq \mathrm{id}$, the terms corresponding to σ with $\sigma^2 \neq \mathrm{id}$ vanish when k is of even characteristic. Furthermore, since $x_{11}, \ldots, x_{NN}$ are zero, we have

$$\det X = \sum_{\sigma\in\mathfrak{S}_N^{(2)}} x_{1\sigma(1)}x_{2\sigma(2)}\cdots x_{N\sigma(N)}, \tag{18}$$

where

$$\mathfrak{S}_N^{(2)} := \{\sigma \in \mathfrak{S}_N \mid \sigma^2 = \mathrm{id}, \sigma(i) \neq i, 1 \leq \forall i \leq N\}.$$

When N is odd, it is clear that $\mathfrak{S}_N^{(2)}$ is empty and then (i) holds. When N is even, there are pairs $(i_1, j_1), \ldots, (i_{N/2}, j_{N/2})$ such that $\sigma(i_l) = j_l$, $\sigma(j_l) = i_l$ and $\{i_1, \ldots, i_{N/2}, j_1, \ldots, j_{N/2}\} = \{1, \ldots, N\}$ for any $\sigma \in \mathfrak{S}_N^{(2)}$. Thus we have

$$\begin{aligned} \det X &= \sum_{\sigma\in\mathfrak{S}_N^{(2)}} \left(x_{i_1j_1}\cdots x_{i_{N/2}j_{N/2}}\right)^2 \\ &=\left(\sum_{\sigma\in\mathfrak{S}_N^{(2)}} x_{i_1j_1}\cdots x_{i_{N/2}j_{N/2}}\right)^2, \end{aligned} \tag{19}$$

where $\{(i_1, j_1), \ldots, (i_{N/2}, j_{N/2})\}$ depends on σ. Thus

(ii) follows immediately from (19) and the fact that $\det(tI_N - A^{-1}B) = (\det A)^{-1}\det(tA - B)$. □

This lemma shows that our attack given in §3.3 cannot be used directly for even characteristic cases, because 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 need to arrange our attack for even characteristic cases in the future.

4. Conclusion

In the present paper, we propose an attack on general extension field type MPKCs with quadratic $\mathcal{G}$ for odd characteristic cases. Our attack can recover partial information S', T' of the secret affine maps S, T in polynomial time. Once S', T' are recovered, the attacker can find the plain-text for a given cipher-text by solving a system of M quadratic equations of N variables. Though, in general, solving such a system of quadratic equations is in exponential time for N, M, it is almost same to inverting $\mathcal{G}$ in the decryption process and is much faster than inverting F directly. This implies that the advantage of such a construction of MPKC was lost at least the case that $\mathcal{G}$ is quadratic and q is odd. While our attack is not presently available on even characteristic cases, it might be improved in near future. We thus cannot recommend extension field type MPKCs derived from a quadratic map as a practical MPKC.

Acknowledgment

The author would like to thank the anonymous reviewers for reading the previous draft of this paper carefully and giving helpful comments to improve it. He is supported by CREST, JST and JSPS Grant-in-Aid for Young Scientists (B) no. 26800020.

References

[1] M.-L. Akkar, N.T. Courtois, R. Duteuil, and L. Goubin, "A fast and secure implementation of Sflash," Public Key Cryptography, PKC 2003, Lecture Notes in Computer Science, vol.2567, pp.267–278, Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.

[2] P. Bürgisser, M. Karpinski, and T. Lickteig, "Some computational problems in linear algebra as hard as matrix multiplication," Comput. Complex., vol.1, no.2, pp.131–155, 1991.

[3] E.R. Berlekamp, "Factoring polynomials over finite fields," Bell Syst. Tech. J., vol.46, no.8, pp.1853–1859, 1967.

[4] E.R. Berlekamp, "Factoring polynomials over large finite fields," Math. Comput., vol.24, no.111, pp.713–713, 1970.

[5] L. Bettale, J.-C. Faugère, and L. Perret, "Solving polynomial systems over finite fields," Proc. 37th International Symposium on Symbolic and Algebraic Computation, ISSAC'12, pp.67–74, 2012.

[6] L. Bettale, J.-C. Faugère, and L. Perret, "Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic," Des. Codes Cryptogr., vol.69, no.1, pp.1–52, 2013.

[7] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," J. Symb. Comput., vol.24, no.3-4, pp.235–265, 1997.

[8] 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

[9] J. Ding and T.J. Hodges, "Inverting HFE systems is quasi-polynomial for all fields," Advances in Cryptology, CRYPTO 2011, Lecture Notes in Computer Science, vol.6841, pp.724–742, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[10] J. Ding, L. Hu, X. Nie, J. Li, and J. Wagner, "High order linearization equation (HOLE) attack on multivariate public key cryptosystems," Public Key Cryptography, PKC 2007, Lecture Notes in Computer Science, vol.4450 pp.233–248, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[11] V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern, "Practical cryptanalysis of SFLASH," Advances in Cryptology, CRYPTO 2007, Lecture Notes in Computer Science, vol.4622, pp.1–12, 2007.

[12] J.-C. Faugére, "A new efficient algorithm for computing Gröbner bases (F_4)," J. Pure Appl. Algebra., vol.139, no.1-3, pp.61–88, 1999.

[13] J.-C. Faugère and A. Joux, "Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases," Advances in Cryptology, CRYPTO 2003, Lecture Notes in Computer Science, vol.2729, pp.44–60, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

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

[15] J.V.Z. Gathen and D. Panario, "Factoring polynomials over finite fields: A survey," J. Symb. Comput., vol.31, no.1-2, pp.3–17, 2001.

[16] L. Granboulan, A. Joux, and J. Stern, "Inverting HFE is quasipolynomial," Advances in Cryptology, CRYPTO 2006, Lecture Notes in Computer Science, vol.4117, pp.345–356, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[17] Y. Hashimoto, "Cryptanalysis of the multivariate signature scheme proposed in PQCrypto 2013," IEICE Trans. Fundamentals, vol.E99-A, no.1, pp.58–65, 2016.

[18] W. Keller-Gehrig, "Fast algorithms for the characteristics polynomial," Theor. Comput. Sci., vol.36, pp.309–317, 1985.

[19] A. Kipnis and A. Shamir, "Cryptanalysis of the HFE public key cryptosystem by relinearization," Advances in Cryptology, CRYPTO'99, Lecture Notes in Computer Science, vol.1666, pp.19–30, Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

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

[21] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," Advances in Cryptology, EUROCRYPT'88, Lecture Notes in Computer Science, vol.330, pp.419–453, 1988.

[22] J. Patarin, "Cryptanalysis of the Matsumoto and Imai public key scheme of eurocrypt'88," Advances in Cryptology, CRYPT0'95, Lecture Notes in Computer Science, vol.963, pp.248–261, Springer Berlin Heidelberg, Berlin, Heidelberg, 1995.

[23] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Science, vol.1070, pp.33–48, Springer Berlin Heidelberg, Berlin, Heidelberg, 1996.

[24] J. Patarin, N. Courtois, and L. Goubin, "QUARTZ, 128-bit long digital signatures," Topics in Cryptology, CT-RSA 2001, Lecture Notes in Computer Science, vol.2020, pp.282–297, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001.

[25] A. Petzoldt, M.-S. Chen, B.-Y. Yang, C. Tao, and J. Ding, "Design principles for HFEv- based multivariate signature schemes," Advances in Cryptology, ASIACRYPT 2015, Lecture Notes in Computer Science, vol.9452, pp.311–334, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[26] V. Shoup, A Computational Introduction to Number Theory and Algebra, Second ed., Cambridge Univ. Press, 2009.

[27] L.-C. Wang, B.-Y. Yang, Y.-H. Hu, and F. Lai, "A "Medium-field" multivariate public-key encryption scheme," Topics in Cryptology, CT-RSA 2006, Lecture Notes in Computer Science, vol.3860, pp.132–149, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

Yasufumi Hashimoto received the Ph.D. degree in mathematics from Kyushu University, Fukuoka, Japan, in 2006. He is currently an associate professor of Department of Mathematical Sciences, University of the Ryukyus. His research interests include cryptography, number theory and representation theory.