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

<table>
<thead>
<tr>
<th>univariate</th>
<th>multivariate</th>
</tr>
</thead>
<tbody>
<tr>
<td>quadratic</td>
<td>MFE [31, 11], multi-HFE [7, 4]</td>
</tr>
<tr>
<td>high degree</td>
<td>IC [13, 18]</td>
</tr>
<tr>
<td>variants</td>
<td>Sflash [1, 14], Quartz [29, 9], etc.</td>
</tr>
</tbody>
</table>

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

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

\[ \vdots \]

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

over 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 \( G : K^N \to K^N \):

\[ G(X_1, \ldots, X_N) = (G_1(X_1, \ldots, X_N), \ldots, G_N(X_1, \ldots, X_N))^t, \]

\[ G_1(X_1, \ldots, X_N) = \sum_{1 \leq i \leq j \leq N} \alpha_{ij}^{(1)} X_i X_j + \sum_{1 \leq i \leq N} \beta_i^{(1)} X_i + \gamma^{(1)}, \]

\[ \vdots \]

\[ G_N(X_1, \ldots, X_N) = \sum_{1 \leq i \leq j \leq N} \alpha_{ij}^{(N)} X_i X_j + \sum_{1 \leq i \leq N} \beta_i^{(N)} X_i + \gamma^{(N)}, \]

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

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

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

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 \( x = S^{-1}(z) \).
Cryptanalysis of multi-HFE

2.2 Efficiency

When $N$ is small enough, $G$ 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 $G$ is chosen randomly, the decryption by the Gröbner basis algorithm is not efficient. Then for such $N$, a special structure of $G$ 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 $(y_1, \ldots, y_n) \in k^n$ 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 $O(2^m(3.31^{3.62}/\log q))$ if $\log q \ll n$ 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 $1/2(q - 1)|\log D| + 2$ [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 $2 \leq \omega < 3$ 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 $n_1, n_2 \geq 1$, let $M_{n_1,n_2}(k)$ be the set of $n_1 \times n_2$ matrices of $k$ entries. Denote by $I_n \in M_{n,n}(k)$ the identity matrix and by $0_{n_1,n_2} \in M_{n_1,n_2}(k)$ the zero matrix. For simplicity, we write $M_n(k) := M_{n,n}(k)$ 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 $l \geq 1$, put

$$A^{(l)} := \left(a_{ij}^{(l)}\right)_{i,j}, \quad g^{(l)}(t) := c_0^{(l)} + c_1^{(l)} t + \cdots + c_d^{(l)} t^d.$$
Lemma 3.2.

For square matrices $A_1 \in M_{n_1}(k), \ldots, A_l \in M_{n_l}(k)$, $A_1 \oplus \cdots \oplus A_l$ means

$$A_1 \oplus \cdots \oplus A_l := \begin{pmatrix} A_1 \\ \vdots \\ A_l \end{pmatrix} \in M_{n_1+\cdots+n_l}(k).$$

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 $\{\theta_1, \ldots, \theta_r\}$ of $K$ over $k$ and a one-to-one map $\phi : k^n \to K^N$. For simplicity, suppose that $\phi$ is chosen such that $\phi(a_{11}, \ldots, a_{1N}, a_{21}, \ldots, a_{rN}) = (a_{11}\theta_1 + \cdots + a_{r1}\theta_r, \ldots, a_{1N}\theta_1 + \cdots + a_{rN}\theta_r)$. Let $L_N$ be a subset of $K^n$ with

$$L_N := \left\{ \begin{pmatrix} a_1, \ldots, a_N, a_1^q, \ldots, a_N^{q^{-1}} \end{pmatrix}^t \mid a_1, \ldots, a_N \in K \right\},$$

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

$$\Theta := \begin{pmatrix} \theta_1 I_N & \theta_2 I_N & \cdots & \theta_r I_N \\ \theta_1^q I_N & \theta_2^q I_N & \cdots & \theta_r^q I_N \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{q^{-1}} I_N & \theta_2^{q^{-1}} I_N & \cdots & \theta_r^{q^{-1}} I_N \end{pmatrix}.$$

Then the following lemma holds.

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

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

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

where $a_i := a_{i1}\theta_1 + \cdots + a_{ri}\theta_r \in K$. Then $\Theta$ 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 $\psi(\Theta a) = (a_1, \ldots, a_N)^t = \phi(a)$. $\square$

For an integer $m \geq 1$, define the sets $A_m \subset M_{n,m}(K), B_m \subset M_{m,n}(K), C \subset M_n(K)$ of matrices as follows.

$$A_m := \left\{ \begin{pmatrix} A \\ A(q) \\ \vdots \\ A(q^{-1}) \end{pmatrix} \mid A \in M_{N,m}(K) \right\},$$

$$B_m := \left\{ \begin{pmatrix} B(q) & \cdots & B(q^{-1}) \end{pmatrix} \mid B \in M_{m,N}(K) \right\},$$

$$C := \left\{ \begin{pmatrix} C_{(j-i \mod r)+1} \end{pmatrix} \mid 1 \leq i, j \leq r \right\}.$$

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

$$A_m = \Theta \cdot M_{n,m}(k), \quad B_m = M_{m,n}(k) \cdot \Theta^{-1}, \quad C = \Theta \cdot M_n(k) \cdot \Theta^{-1}. \quad (2)$$
Proof. First, choose $A_1, \ldots, A_r \in M_{N,m}(k)$ 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 $\Theta \cdot M_{n,m}(k) \subset \mathcal{A}_m$. Since $(\#(\Theta \cdot M_{n,m}(k)) = \# \mathcal{A}_m = q^{mn}$, we obtain $\mathcal{A}_m = \Theta \cdot M_{n,m}(k)$.

Next, choose $B \in M_{m,n}(K)$ arbitrary. We have

$$(B, B^{(q)}, \ldots, B^{(q^{r-1})}) \Theta = (B \theta_1 + B^{(q)} \theta_1^q + \cdots + B^{(q^{r-1})} \theta_1^{q^{r-1}}, \ldots, B \theta_r + B^{(q)} \theta_r^q + \cdots + B^{(q^{r-1})} \theta_r^{q^{r-1}}).$$

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

$$(B \theta_l + B^{(q)} \theta_l^q + \cdots + B^{(q^{r-1})} \theta_l^{q^{r-1}})^{(q^{i-1})} = B \theta_l + B^{(q)} \theta_l^q + \cdots + B^{(q^{r-1})} \theta_l^{q^{r-1}}$$

for $1 \leq l \leq r$. It is well-known that $a \in K$ satisfies $a^q = a$ if and only if $a \in k$. This means that $B_m \cdot \Theta \subset M_{m,n}(k)$. It is clear that $\# B_m = \# (M_{m,n}(k) \cdot \Theta^{-1}) = q^{mn}$. We then obtain $B_m = M_{m,n}(k) \cdot \Theta^{-1}$.

Finally, choose $C_1, \ldots, C_r \in M_{n}(K)$ arbitrary and put $C := (C_{(j-i \mod r)+1})_{1 \leq i,j \leq r} \in C$. The $(i,j)$-block $C'_{ij}$ in $C \cdot \Theta$ is

$$C'_{ij} = C_{(j-i \mod r)+1} \theta_j + C_{(2-i \mod r)+1} \theta_j^q + \cdots + C_{(r-i \mod r)+1} \theta_j^{q^{r-1}} = (C_{ij})^{(q^{i-1})}.$$ 

This means that $C \cdot \Theta \subset \mathcal{A}_n = \Theta \cdot M_{n}(k)$. Since $\# C = \# (\Theta \cdot M_{n}(k) \cdot \Theta^{-1}) = q^{n^2}$, we obtain $C = \Theta \cdot M_{n}(k) \cdot \Theta^{-1}$. \hfill $\Box$

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

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

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 $H \in M_n(k)$, 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 $1 \leq i \leq l$. Then the following (i) and (ii) hold.

(i) There exists an invertible matrix $P \in M_n(k)$ such that $P^{-1} H P = C(h_1) \oplus \cdots \oplus C(h_l)$.

(ii) If $P_1, P_2 \in M_n(k)$ 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 $M_1 \in M_{d_1}(k), \ldots, M_l \in M_{d_l}(k)$ such that $P_1^{-1} P_2 = M_1 \oplus \cdots \oplus M_l$. \hfill $\Box$
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 $F : k^n \rightarrow k^n$ is given by

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

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

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

Then, by the definition of $\psi$ and $G$, we see that

$$F(x) = (T \circ \Theta^{-1}) \cdot \begin{pmatrix} G_1((\Theta \circ S)x), \ldots, G_N((\Theta \circ S)x), G_1((\Theta \circ S)x)^q, \ldots, G_N((\Theta \circ S)x)^{q^r-1} \end{pmatrix}^t. \quad (3)$$

For $X = (X_1, \ldots, X_N)^t \in K^N$, let $\bar{X} := \psi^{-1}(X) = \left( X_1, \ldots, X_N, X_1^q, \ldots, X_N^{q^r-1} \right)^t \in L_N$. Since $G_1(X), \ldots, G_N(X)$ are quadratic forms, there exists matrices $G_1, \ldots, G_N \in M_N(K)$, low vectors $\beta_1, \ldots, \beta_N \in M_1(K)$ and constants $\gamma_1, \ldots, \gamma_N \in K$ such that

$$G_l(X) = X^t G_l X + \beta_l X + \gamma_l, \quad (1 \leq l \leq N).$$

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

$$G_l(X) = \bar{X}^t (G_l \oplus 0_{n-N}) \bar{X} + (\beta_l, 0_{1,n-N}) \bar{X} + \gamma_l,$$

$$G_l(X)^q = \bar{X}^t \left( 0_{1,N} \oplus G_l(q) \oplus 0_{1,n-2N} \right) \bar{X} + \left( 0_{1,N}, \beta_l(q), 0_{1,n-2N} \right) \bar{X} + \gamma_l^q,$$

$$\vdots$$

$$G_l(X)^{q^r-1} = \bar{X}^t \left( 0_{n-N} \oplus G_l(q^{r-1}) \right) \bar{X} + \left( 0_{1,n-N}, \beta_l(q^{r-1}) \right) \bar{X} + \gamma_l^{q^{r-1}}.$$

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

$$f_l(x) = x^t S_0^t \left( \Theta^t \left( E_l \oplus E_l(q) \oplus \cdots \oplus E_l(q^{r-1}) \right) \Theta S_0 x + \text{constant} \right)$$

$$+ x^t S_0^t \left( \Theta^t \left( E_l \oplus E_l(q) \oplus \cdots \oplus E_l(q^{r-1}) \right) \Theta s + s^t \Theta^t \left( E_l \oplus E_l(q) \oplus \cdots \oplus E_l(q^{r-1}) \right) S_0 x \right)$$

$$+ \left( b_l, b_l(q), \ldots, b_l(q^{r-1}) \right) \Theta S_0 x + \text{constant},$$

where $E_1, \ldots, E_n \in M_N(K)$ are matrices and $b_1, \ldots, b_n \in M_{1,N}(K)$ are low vectors given by

$$(E_1, \ldots, E_n)^t = (T_0 \Theta^{-1})(G_1, \ldots, G_N, 0_N)^t,$$

$$(b_1, \ldots, b_n)^t = (T_0 \Theta^{-1})(\beta_1, \ldots, \beta_N, 0_N)^t. \quad (6)$$

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 $F(x) = (f_1(x), \ldots, f_n(x))^t$ of multi-HFE.

**Output:** Two invertible matrices $S', T' \in M_n(k)$ such that

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

is a quadratic map.

**Step 1.** Let $F_1, \ldots, F_n \in M_n(k)$ be the symmetric matrices with

$$f_i(x) = x^t F_i x + \text{linear}.$$

Take two linear sums $W_1, W_2$ of $F_1, \ldots, F_n$ 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 $P_0 \in M_{n,N}(K)$ satisfying $w_0(W)P_0 = 0$ and put

$$P := \left( P_0, P_0^{(q)}, \ldots, P_0^{(q_{r-1})} \right) \in M_n(k) \cdot \Theta^{-1}.$$

**Step 5.** If $P$ is invertible, go to the next step. If not, go back to Step 4.

**Step 6.** Let $\hat{F}_i := P^t F_i P$. Find a matrix $Q_0 \in M_{n,n}(K)$ 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

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

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 $G$ is chosen randomly, the decryption without secret keys is as fast as the decryption with secret keys. Even if $G$ 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.

We now explain why our attack is available.
Table 2: Probability (%) that $\det(t \cdot I_N - W_0)$ is irreducible for $q = 31$

<table>
<thead>
<tr>
<th>$N$</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>$\cdots$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prob.</td>
<td>49.2</td>
<td>33.4</td>
<td>25.2</td>
<td>19.5</td>
<td>17.4</td>
<td>13.7</td>
<td>12.7</td>
<td>11.2</td>
<td>9.9</td>
<td>$\cdots$</td>
</tr>
</tbody>
</table>

The equation (5) gives

$$F_l = (\Theta S_0)^t \left( E_t \oplus \cdots \oplus E_1^{(q^r-1)} \right) (\Theta S_0),$$

the matrix $W$ is written by

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

(7)

for some $W_0 \in M_N(K)$ 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

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

(8)

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

$$\left(\sigma^t \left( L \oplus \cdots \oplus L^{(q^r-1)} \right) \right)^{-1} \left( W_0 \oplus \cdots \oplus W_0^{(q^r-1)} \right) \left( \sigma^t \left( L \oplus \cdots \oplus L^{(q^r-1)} \right) \right) = C(w_0) \oplus \cdots \oplus C(w_0)^{(q^r-1)},$$

(9)

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

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

(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

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

(11)

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

$$\tilde{F}_l = P^t F_l P = (\Theta S_0 P)^t \left( E_t \oplus \cdots \oplus E_1^{(q^r-1)} \right) (\Theta S_0 P) = \tilde{E}_l \oplus \cdots \oplus \tilde{E}_1^{(q^r-1)}$$

(12)

for some $\tilde{E}_l \in M_N(K)$. 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

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

(13)

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

$$\phi \circ T' \circ F \circ S' \circ \phi^{-1} = \psi \circ (\Theta \circ T' \circ T \circ \Theta^{-1}) \circ (\psi^{-1} \circ G \circ \psi) \circ (\Theta \circ S \circ S' \circ \Theta^{-1}) \circ \psi^{-1}$$

$$= \psi \circ (Q \circ T \circ \Theta^{-1}) \circ (\psi^{-1} \circ G \circ \psi) \circ (\Theta \circ S \circ P \circ \Theta^{-1}) \circ \psi^{-1}$$

is a quadratic map from $K^N$ to $K^N$. □
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 \( \left( \frac{n+N+1}{N+1} \right)^\omega \) 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

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

Table 3: Experimental results of our attack for \( q = 31 \)
Cryptanalysis of multi-HFE

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 $A, B \in M_N(k)$ 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 $X = (x_{ij})_{1 \leq i, j \leq N} \in M_N(k)$ is given by
$$ \det X = \sum_{\sigma \in \mathfrak{S}_N} x_{1\sigma(1)}x_{2\sigma(2)} \cdots x_{N\sigma(N)}, $$
where $\mathfrak{S}_N$ is the set of permutations among $1, \ldots, N$. It is easy to see that
$$ x_{1\sigma^{-1}(1)}x_{2\sigma^{-1}(2)} \cdots x_{N\sigma^{-1}(N)} = x_{\sigma(1)}x_{\sigma(2)} \cdots x_{\sigma(N)}N. $$
Then, when $X$ is symmetric and its diagonal entries are zero, we have
$$ \det X = \sum_{\sigma \in \mathfrak{S}_N^{(2)}} x_{1\sigma(1)}x_{2\sigma(2)} \cdots x_{N\sigma(N)}, $$
where $\mathfrak{S}_N^{(2)} := \{ \sigma \in \mathfrak{S}_N \mid \sigma^2 = \text{id}, \sigma(i) \neq i, 1 \leq \forall i \leq N \}$. 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 $\sigma \in \mathfrak{S}_N^{(2)}$,
$$ x_{1\sigma(1)} \cdots x_{N\sigma(N)} = \left( x_{i_1j_1} \cdots x_{i_N/2j_N/2} \right)^2. $$
Since $k$ is of even characteristic, we have
$$ \det X = \left( \sum_{\sigma \in \mathfrak{S}_N^{(2)}} x_{i_1j_1} \cdots x_{i_N/2j_N/2} \right)^2, $$
where $\{i_1, j_1, \ldots, (i_N/2, j_N/2)\}$ depends on $\sigma$. Since $\det (tI_N - A^{-1}B) = (\det A)^{-1} \det (tA - B)$, (ii) follows immediately from (16). \qed

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.
Cryptanalysis of multi-HFE

References


