High-rank attack on HMFEv

Yasufumi Hashimoto

1. Introduction

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

Recently in PQCrypto 2017, a vinegar variant of multi-HFE (Chen et al., 2008). While the original multi-HFE is known to be insecure against the high-rank attack had not been studied yet at all. In the present paper, we study the structure of HMFEv and discuss its security against the high-rank attack.

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

2. Multi-HFE and HMFEv

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

2.1 Multi-HFE

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

$$X = (X_1, \ldots, X_N)^t,$$

$$G(X) = (G_1(X), \ldots, G_N(X))^t,$$

$$G_l(X) = \sum_{1 \leq i \leq j \leq N} \alpha^{(l)}_{ij} X_i X_j + \sum_{1 \leq i \leq N} \beta^{(l)}_{i} X_i + \gamma^{(l)}$$

for $1 \leq l \leq N$, where $\alpha^{(l)}_{ij}, \beta^{(l)}_{i}, \gamma^{(l)} \in K$.

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

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

$$G_l(X) = Z_l, \quad l \quad G_N(X) = Z_N.$$  

(1)

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

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

2.2 HMFEv

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

$$X = (X_1, \ldots, X_N)^t, \quad u = (u_1, \ldots, u_v)^t,$$

$$G(X, u) = (G_1(X, u), \ldots, G_N(X, u)),$$

$$G_l(X, u) = \sum_{1 \leq i \leq j \leq N} \alpha^{(l)}_{ij} X_i X_j + \sum_{1 \leq i \leq N} \beta^{(l)}_{i} X_i + \gamma^{(l)}(u)$$

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

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

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

\[
G_l(X, u) = Z_1, \quad \ldots, \quad G_N(X, u) = Z_N. \tag{3}
\]

The signature for \( y \in k^m \) is \( S^{-1}(\phi_N^{-1}(X, u)) \). The signature \( x \in k^m \) is verified if \( F(x) = y \) holds.

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

We note that the constant parts of \( S, T \) do not contribute to enhance the security. In fact, for \( s \in k^m, t \in k^N \), \( s_0(x) := x + s \) and \( t_0(y) := y + t \), the map \( \phi_N \circ t_0 \circ G \circ t_0 \circ \phi_N^{-1} \) is also a quadratic map similar to (2). Then we can consider that \( S, T \) are linear maps without loss of generality.

3. Security analysis

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

3.1 Polynomials in HMFev

For integers \( n_1, n_2 \geq 1 \) and a finite field \( k \), let \( M_{n_1,n_2}(k) \) 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 an integer \( l \geq 1 \) and a matrix \( A = (a_{i,j})_{i,j} \), we denote by \( A^{(l)} := (a_{i,j}^{(l)})_{i,j} \).

Let \( \{\theta_1, \ldots, \theta_t\} \subset K \) be a basis of \( K \) over \( k \) and define \( \Theta_N := (\theta_j^{-1} \cdot I_N)_{1 \leq i,j \leq t} \in M_{m,K} \) and \( \Theta_N,v := \left(\Theta_N \quad 0_{m-N} \right) \in M_{m,v,K} \). The one-to-one maps \( \phi_N : k^m \to K^N \) and \( \phi_{N,v} : k^m \to K^N \times k^v \) are given by the matrices \( \Theta_N \) and \( \Theta_N,v \), respectively. In fact, it holds

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

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

\[
\psi_N(\alpha_1, \ldots, \alpha_N) = (\alpha_1, \ldots, \alpha_N, \alpha_1^{q-1}, \ldots, \alpha_N^{q-1})^T, \\
\psi_{N,v}(\alpha_1, \ldots, \alpha_N, u_1, \ldots, u_v) = (\alpha_1, \ldots, \alpha_N, \alpha_1^{q-1}, \ldots, \alpha_N^{q-1}, u_1, \ldots, u_v)^T.
\]

Then the public key \( F \) is described by

\[
F = (T \circ \Theta_N^{-1}) \circ (\psi_N \circ G \circ \psi_N^{-1}) \circ (\Theta_N,v \circ S),
\]

namely

\[
F(x) = (f_1(x), \ldots, f_m(x))^T = (T \circ \Theta_N^{-1}) \cdot (G_1(\phi_{N,v}(S(x))) \ldots, G_N(\phi_{N,v}(S(x))) \ldots, G_N(\phi_{N,v}(S(x)))^{q^{-1}})^T.
\]

When we express the polynomials \( G_1, \ldots, G_N \) by

\[
G_l(X, u) = (X^t, u^T) \left(\begin{array}{c} A_l \ B_l^T \\ C_l \end{array}\right) X^T \ u + (\text{linear form})
\]

as quadratic forms of \( X, u \) with matrices \( A_l \in M_{N,K}, B_l \in M_{N,v,K}, C_l \in M_{v,K} \), the polynomials \( G_l(X, u), \ldots, G_N(X, u), G_1(X, u)^q, \ldots, G_N(X, u)^{(q^t-1)} \) in (4) are written as quadratic polynomials

\[
X := \psi_N^{-1}(X, u)
\]

\[
= (X_1, \ldots, X_N, X_1^{q^{-1}}, \ldots, X_N^{q^{-1}}, u_1, \ldots, u_v)^T
\]

in the forms

\[
G_l(X, u) = X^t \left(\begin{array}{c} A_l \ 0_{m-N} \\ B_l^T \ C_l \end{array}\right) X + (\text{linear form of } X),
\]

\[
G_l(X, u)^q = X^t \left(\begin{array}{c} A_l^q \ 0_{m-N} \\ B_l^{q^t-1} \ C_l^{q^t-1} \end{array}\right) X + (\text{linear form of } X),
\]

\[
\vdots
\]

\[
G_l(X, u)^{(q^t-1)} = X^t \left(\begin{array}{c} A_l^{(q^t-1)} \ 0_{m-N} \\ B_l^{(q^t-1)} \ C_l^{(q^t-1)} \end{array}\right) X + (\text{linear form of } X).
\]

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

\[
f_l(x) = x^T F_l x + (\text{linear form of } x),
\]

where

\[
F_l := (\Theta_N,v S)^{lT} \left(\begin{array}{c} *^N \ 0^N \\ \vdots \ * \end{array}\right) (\Theta_N,v S).
\]

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

3.2 Min-rank attack

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

\[
(\Theta_{N,v} S)'^t \begin{pmatrix}
* & 0_{m-N} & * \\
* & * & * \\
0_{N} & * & * \\
* & 0_{m-2N} & * \\
* & * & *
\end{pmatrix} (\Theta_{N,v} S),
\]

\[
(\Theta_{N,v} S)'^t \begin{pmatrix}
0_N & * & * \\
* & 0_{N} & * \\
* & 0_{N} & * \\
* & 0_{N} & * \\
* & * & *
\end{pmatrix} (\Theta_{N,v} S),
\]

\[
\ldots, (\Theta_{N,v} S)'^t \begin{pmatrix}
0_{N} & * & * \\
* & 0_{N} & * \\
* & 0_{N} & * \\
* & 0_{N} & * \\
* & * & *
\end{pmatrix} (\Theta_{N,v} S).
\]

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

To find such \( \alpha_1, \ldots, \alpha_m \in K \), the attacker generates a system of polynomial equations of \( m \) variables \( z_1, \ldots, z_m \) derived from the condition that the rank of \( H(z_1, \ldots, z_m) := z_1 F_1 + \cdots + z_m F_m \) is at most \( N + v \) and solve it by, e.g., the Gr"obner basis algorithm. Since the condition that the rank of \( A \) is at most \( R \) is equivalent that the determinants of arbitrary \((R+1) \times (R+1)\)-minor matrices in \( A \) are zero, the min-rank attack requires to solve a system of polynomial equations of degree (at most) \( N + v + 1 \) and of \( m \) variables. Based on the result in [3], the authors in [5] claimed that the complexity of the min-rank attack is \( O\left(\binom{m+N+v+1}{N+v+1}\right)\) where \( 2 \leq w < 3 \) is an exponent of the Gaussian elimination. This means that, if one takes \( v \) sufficiently large, HMFEv is secure enough against the min-rank attack.

### 3.3 High-rank attack

The high-rank attack, introduced in [9,10], is to find \( \beta_1, \ldots, \beta_L \in K \) such that the rank of \( P := F_m + \beta_1 F_1 + \cdots + \beta_L F_L \) is at most \( R \) if there exist such integers \( 1 \leq L, R < n \) and \( \beta_1, \ldots, \beta_L \in K \). For HMFEv, recall that \( F_1, \ldots, F_m \) are as written in (6). Due to (4) and (5), we see that the first \( N \) columns and rows of the central matrix in (6) are derived from linear sums of \( N \) polynomials \( G_1(X,u), \ldots, G_N(X,u) \). Then, removing the contributions of such \( N \) polynomials, we can get a matrix of rank at most \( n - N \). This means that the high-rank attack is available on HMFEv with \((L,R) = ((N,n-s)\). We now describe how to recover an equivalent key of HMFEv.

**Input.** The public matrices \( F_1, \ldots, F_m \).

**Output.** Invertible matrices \( S' \in M_m(k) \), \( T' \in M_m(k) \) such that \( \phi_N \circ T' \circ F \circ S' \circ \phi_N^{-1} : K^N \times k^N \rightarrow K^N \) is a quadratic map similar to (2).

**Step 1.** Find \( \beta_1, \ldots, \beta_N \in K \) such that \( P := F_m + \beta_1 F_1 + \cdots + \beta_N F_N \).

**Step 2.** Find a matrix \( Q \in M_n,N(k) \) with \( PQ = 0_{n,N} \).

**Step 3.** Choose \( Q_0 \in M_{n,N}(k) \) randomly and put \( \tilde{Q} := (Q,Q(q), \ldots, Q(q^{N-1}),Q_0) \in M_n(k)^{N+1} \). If \( \tilde{Q} \) is not invertible, change \( Q, Q_0 \). Compute \( F'_i := \tilde{Q} F_i \tilde{Q} \) for \( 1 \leq l \leq m \).

**Step 4.** Find a matrix \( W \in M_m(k) \) with

\[
W' := \sum_{1 \leq j \leq m} w_{ij} F'_j = \begin{pmatrix}
* & 0_{m-N} & * \\
* & * & * \\
0_N & * & * \\
* & 0_{m-2N} & * \\
* & * & *
\end{pmatrix} \in \Theta_N M_m(k). \]

for \( 1 \leq i \leq N \). Put \( \tilde{W} := \begin{pmatrix}
w_{i+N} & \cdots & w_{i+N}\end{pmatrix} \in \Theta_N M_m(k) \). If \( \tilde{W} \) is not invertible, change \( W \).

**Step 5.** Output \( S' := \tilde{Q} \Theta_{N,v} \) and \( T' := \Theta_{N,v}^{-1} \tilde{W} \).

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

\[
(\Theta_{N,v} S)'^t \begin{pmatrix}
0_N & *_{N-1} & * \\
* & * & * \\
0_N & *_{N-1} & * \\
* & 0_{N-2N} & * \\
* & * & *
\end{pmatrix} (\Theta_{N,v} S),
\]

\[
(\Theta_{N,v} S)'^t \begin{pmatrix}
* & 0_{N} & * \\
* & * & * \\
* & 0_{N} & * \\
* & 0_{N} & * \\
* & * & *
\end{pmatrix} (\Theta_{N,v} S),
\]

\[
\ldots, (\Theta_{N,v} S)'^t \begin{pmatrix}
* & 0_{N} & * \\
* & * & * \\
* & 0_{N} & * \\
* & 0_{N} & * \\
* & * & *
\end{pmatrix} (\Theta_{N,v} S).
\]

Since \( P \) is of rank at most \( n - N \), there exists a matrix \( Q \) in Step 2 and it can be found by linear operations. Due to (7), we see that a matrix \( \tilde{Q} = (Q,*)* \) satisfies \( \tilde{Q} P \tilde{Q} = \begin{pmatrix}
0_N & * \\
* & *
\end{pmatrix} \) and then \((\Theta_{N,v} S)\tilde{Q} \) is in the form \begin{pmatrix}
* & * \\
* & *
\end{pmatrix} \) or its permutation. Lemma 3.2 in [4] tells that the matrix \( \tilde{Q} \) in Step 3 is in \( M_{n,k}(\Theta_{N,v}) \). Thus \((\Theta_{N,v} S)\tilde{Q} \) must be \begin{pmatrix}
* & * \\
* & *
\end{pmatrix} \) or its permutation. This means, due to (6), that \( F'_i = \begin{pmatrix}
* & * \\
* & *
\end{pmatrix} \) for \( 1 \leq i \leq m \). Since \( F'_i \) is a linear sum of matrices similar to the coefficient matrices given in (5), a matrix \( W \) in Step 4 exists and it is found by linear operations. The matrices \( F'_i, \ldots, F'_m \) are similar to the coefficient matrices \( G_1(X,u), \ldots, G_N(X,u) \). We thus conclude that \((S',T') \) in Step 5 is an equivalent key. 

It is easy to see that Step 2-5 require only linear operations. Then the complexity of Step 1 is important in this attack. To find \( \beta_1, \ldots, N \in K \) in Step 1, we state a system of polynomial equations of \( N \) variables \( y_1, \ldots, y_N \) derived from the condition that the rank of \( P(y_1, \ldots, y_N) := F_m + y_1 F_1 + \cdots + y_N F_N \) is at most \( n - N \) and solve it by, e.g., the Gr"obner basis algorithm. Since this condition is equivalent the determinants of arbitrary \((n-N+1) \times (n-N+1)\)-minor matrices of \( P(y_1, \ldots, y_N) \) are zero, the attacker needs to solve a system of polynomial equations of degree at most \( n - N + 1 \) and of \( N \) variables. Then we can consider that the complexity of the high-rank attack on HMFEv highly depends on \( N \) and the contribution of \( v \) for the security seems not too much.

Note that, for integers \( M_1, N_1, d \geq 1 \) with \( M_1 \geq N_1 \) and a semi-regular system of polynomials \( \{p_1(x), \ldots, p_{M_1}(x)\} \) of \( N_1 \)-variables and of degree \( d \), it is known (e.g. [6,7]) that the complexity of the Gr"obner basis algorithm on this polynomial system is bounded by \( \mathcal{O}\left(\binom{N_1+d_{eig}}{N_1}\right)^{w} \), where \( d_{eig} \) is a constant, called the degree of regularity, given by the index of the first non-zero.
positive coefficient of the univariate polynomial \( C(t) := (1-t^d)M_1(1-t)^{-N_1} \). This means that, if \( M_1 \) is sufficiently larger than \( N_1 \), we have \( d_{\text{sec}} = d \). We thus expect that the complexity of the high-rank attack on HMFEv is

\[
O \left( \left( \frac{n+1}{N} \right)^w \right)
\]

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

3.4 Experiments of the high-rank attack

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

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

We also remark that, if \( q \) is even, we use \( F_1 + F_1^T \) instead of the matrix \( F_1 \). The matrix \( F_1 + F_1^T \) is symmetric and skew-symmetric since the field \( k \) is of even characteristic. It is known (e.g. [13]) that the determinant of a skew-symmetric matrix is zero when the size of the matrix is odd and is a square when that is even. We then have to arrange our attack based on this fact. Fortunately, the arrangement for even characteristic cases was already discussed in [3] for the min-rank attack and we can apply it also for the high-rank attack.

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

4. Conclusion

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

Acknowledgments

The author was supported by JST CREST no. JP-MJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181. He would like to thank the anonymous referee(s) for reading the previous draft carefully and giving helpful comments.

References