# On the security of HMFEv

Yasufumi Hashimoto *

**Abstract**

In this short report, we study the security of the new multivariate signature scheme HMFEv proposed at PQCrypto 2017.

**Keywords.** HMFEv, multivariate public-key cryptosystem (MPKC)

## 1 Introduction

In PQCrypto 2017, a new multivariate signature scheme HMFEv was proposed [8]. It is a vinegar variant of multi-HFE [4]. While the multi-HFE is known to be insecure against the direct attack [6], the min-rank attack [1] and the attack using a diagonalization approach [5], HMFEv is considered to be secure against these attacks and efficient enough.

In this short report, we study the structure of HMFEv and give experimental results of the high-rank attack on HMFEv with parameters selected in [8].

## 2 HMFEv

The signature scheme HMFEv [8] is constructed as follows.

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

$$\mathcal{G}_l(X, u) = \sum_{1 \leq i \leq j \leq N} \alpha_{ij}^{(l)} X_i X_j + \sum_{1 \leq i \leq N} \beta_i^{(l)}(u) X_i + \gamma^{(l)}(u), \quad (1 \leq l \leq N),$$

where $X = (X_1, \ldots, X_N)^t \in K^N$, $u \in k^v$, $\mathcal{G}(X, u) = (\mathcal{G}_1(X, u), \ldots, \mathcal{G}_N(X, u))^t$, $\alpha_{ij}^{(l)} \in K$, $\beta_i^{(l)} : k^v \to K$ is an affine form and $\gamma^{(l)} : k^v \to K$ is a quadratic form.

The *secret key* is invertible affine maps $S : k^n \to k^n$, $T : k^m \to k^m$ and the *public key* is the quadratic map

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

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

A given signature $y \in k^m$ is *signed* as follows. First, compute $Z = (z_1, \ldots, z_N)^t := \phi_N(T^{-1}(y))$ and choose $u \in k^v$. Next find $X \in K^N$ such that

$$\mathcal{G}_1(X, u) = z_1, \quad \ldots, \quad \mathcal{G}_N(X, u) = z_N. \tag{1}$$

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

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 exponential for $N$, the number $N$ cannot be large. Petzoldt et al. [8] selected the following parameters for practical use.

*Department of Mathematical Science, University of the Ryukyus, e-mail: hashimoto@math.u-ryukyu.ac.jp

Table 1: Parameter Selection of HMFEv [8]

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

## 3 Proposed attack

We first give several notations and study the structure of polynomials in HMFEv.

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 $l \geq 1$ and a matrix $A = (a_{ij})_{i,j}$, put $A^{(l)} := \left(a_{ij}^l\right)_{i,j}$.

Let $\{\theta_1, \dots, \theta_r\} \subset K$ be a basis of $K$ over $k$ and

$$\Theta_N := \left(\theta_j^{q^{i-1}} I_N\right)_{1 \leq i,j \leq r} \in \mathrm{M}_m(K), \qquad \Theta_{N,v} := \begin{pmatrix} \Theta_N & \\ & I_v \end{pmatrix} \in \mathrm{M}_n(K).$$

It is known that the one-to-one maps $\phi_N, \phi_{N,v}$ are given by the matrices $\Theta_N, \Theta_{N,v}$. In fact, it is easy to see that

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

where $\psi_N : K^N \to K^{Nr}$, $\psi_{N,v} : K^N \times k^v \to K^{Nr} \times k^v$ are maps with

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

Then the public key $F$ is described by

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

namely

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

When we express $\mathcal{G}_1(X,u), \dots, \mathcal{G}_N(X,u)$ by

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

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

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

in the forms

$$\mathcal{G}_l(X,u) = \bar{X}^t \left(\begin{array}{cc|c} A_l & & B_l \\ & 0_{n-N} & \\ \hline & B_l^t & C_l \end{array}\right) \bar{X} + (\text{linear form of } \bar{X}),$$

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

$$\vdots$$

$$\mathcal{G}_l(X,u)^{q^{r-1}} = \bar{X}^t \left(\begin{array}{cc|c} 0_{n-N} & & \\ & A_l^{(q^{r-1})} & B_l^{(q^{r-1})} \\ \hline & {B_l^{(q^{r-1})}}^t & C_l^{(q^{r-1})} \end{array}\right) \bar{X} + (\text{linear form of } \bar{X}).$$

This means that the public quadratic forms are expressed by

$$f_l(x) = x^t(\Theta_{N,v}S)^t \left(\begin{array}{ccc|c} *_N & & & * \\ & \ddots & & \vdots \\ & & *_N & * \\ \hline * & \cdots & * & *_v \end{array}\right) (\Theta_{N,v}S)x + (\text{linear form of } x),$$

and we see that there exist $\delta_1, \ldots, \delta_N \in K$ such that

$$f_m(x) + \delta_1 f_1(x) + \cdots + \delta_N f_N(x) = x^t(\Theta_{N,v}S)^t \begin{pmatrix} 0_N & \\ & *_{n-N} \end{pmatrix} (\Theta_{N,v}S)x + (\text{linear form}).$$

Our attack is to try to find $\delta_1, \ldots, \delta_N \in K$ such that the rank of

$$H := F_m + \delta_1 F_1 + \cdots + \delta_N F_N$$

is at most $n - N$, where $F_l \in \mathrm{M}_n(k)$ is the coefficient matrix of $f_l(x)$. We can consider that, if $\mathrm{rank} H \leq n - N$, $H$ is written by one of the following forms with high probability.

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

$$\cdots, \quad (\Theta_{N,v}S)^t \begin{pmatrix} *_{(r-1)N} & & * \\ & 0_N & \\ * & & *_v \end{pmatrix} (\Theta_{N,v}S)$$

Once such a matrix $H$ is recovered, the attacker can recover keys equivalent to $(S, T)$ easily.

To find such $\delta_1, \ldots, \delta_N$, we state a system of polynomial equations of $N$ variables $y_1, \ldots, y_N$ derived from the condition that the rank of

$$H(y_1, \ldots, y_N) := F_m + y_1 F_1 + \cdots + y_N F_N$$

is at most $n - N$ and solve it. It is known that, for a matrix $A$ and an integer $l$, the condition that $\mathrm{rank} A \leq l$ is equivalent that the determinants of arbitrary $(l+1) \times (l+1)$ minor matrices of $A$ are zero. In our attack, we choose an integer $N_1$ sufficiently larger than $N$, state $N_1$ equations of $N$ variables $(y_1, \ldots, y_N)$ by the determinants of $(n - N + 1) \times (n - N + 1)$ minor matrices of $H(y_1, \ldots, y_N)$, find a common solution $(y_1, \ldots, y_N) = (\delta_1, \ldots, \delta_N)$ of such $N_1$ equations by the Gröbner basis algorithm and check whether $\mathrm{rank} H(\delta_1, \ldots, \delta_N) \leq n - N$.

We implemented this approach on Magma [2] ver.2.22-3 on Windows 8.1, Core(TM)i7-4800MQ, 2.70GHz for the parameter selections given in Table 1. In this implements, we

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

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

choose $N_1 = 3$ for $(q, N) = (31, 2)$ and $N_1 = 10$ for $(q, N) = (256, 3)$, and use an approach given in [7] to compute the determinants of polynomial matrices. We remark that, if $q$ is even, we use $F_l + F_l^t$ instead of the coefficient matrix $F_l$, and then we make a minor arrangement for our attack based on the fact 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 (e.g. [3]).

The running times of our attack are given in Table 2. These results show that HMFEv for $N = 2$ 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, 128, 192 or 256 bit.

**Acknowledgment.** The author was supported by JST CREST no.JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

## References

[1] 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.

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

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

[4] 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.

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

[6] M.D.A. Huang, M. Kosters, Y. Yang, S.L. Yeo, On the last fall degree of zero-dimensional Weil descent systems, https://arxiv.org/abs/1505.02532 (2015).

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

[8] A. Petzoldt, M.S. Chen, J. Ding, B.Y. Yang, HMFEv - An efficient multivariate signature scheme, PQCrypto 2017, LNCS **10346** (2017), pp. 205–223.