Security Analysis Against "A New Encryption Scheme for Multivariate Quadratic Systems"

Yasuhiko Ikematsu[1] and Shuhei Nakamura[2]

[1] Institute of Mathematics for Industry, Kyushu University, 744 Motooka, Nishi-ku,
Fukuoka 819-0395, Japan, ikematsu@imi.kyushu-u.ac.jp

[2] Department of Liberal Arts and Basic Sciences, Nihon University, Japan,
nakamura.shuhei@nihon-u.ac.jp

Abstract. Multivariate encryption schemes are public key encryption schemes using multivariate polynomials over finite fields. In 2020, Jiahui Chen et al. proposed a new multivariate encryption scheme. In order to construct the public key consisting of quadratic polynomials, they used the minus and plus modifiers to prevent known attacks, such as linear equations attack, minRank attack and algebraic attack. However, in this paper we show that even if such modifiers are used, an attack using linear algebra is valid for their scheme. In fact, our attack can break the claimed 80 and 128-bit parameters in the complexity of around 27 and 31 bits, respectively.

Keywords: Multivariate Public-Key Cryptography · Post-Quantum Cryptography · Encryption Schemes.

1 Introduction

Multivariate public key cryptography (MPKC) [7] is the public key cryptography using multivariate polynomials over finite fields and is considered one of the main candidates for Post-Quantum Cryptography (PQC) [1]. It has been studied for around 3 decades since the MI scheme [18], which is the first multivariate encryption scheme, was proposed in 1988. An important ingredient of MPKC is the so-called *central map* F. Namely, $F = (f_1, \ldots, f_m)$ is a map from $\mathbb{F}^n$ to $\mathbb{F}^m$ consisting of m multivariate quadratic polynomials $f_1, \ldots, f_m$ in n variables over a finite field $\mathbb{F}$ and has a property that the equation $F(x) = y$ ($y \in \mathbb{F}^m$) can be solved easily. In order to hide the structure of F, randomly choose two affine maps S and T and the public key is given by $P = T \circ F \circ S$. The security of MPKC is based on the so called *MQ-Problem* which asks for a solution to the system of quadratic equations. From a fact that MQ-Problem is proven to be an NP-hard problem even for quadratic polynomials over $\mathbb{F}_2$ [13], MPKC is considered having the potential to resist quantum computer attacks.

In the area of digital signatures, there exists a large number of practical multivariate signature schemes [9, 16, 21]. On the other hand, it is considered to be difficult to construct a secure multivariate encryption scheme. The MI encryption scheme [18] was broken by Patarin in 1995 [19] using the linear equations attack. After that, Patarin proposed a multivariate encryption scheme extending MI scheme, called HFE scheme [20]. However, by a series of subsequent researches [3, 5, 8, 10, 12, 14, 17], it was found that HFE scheme has a serious trade-off between efficiency and security. Currently, while ABC [23], EFC [22], HFERP [15] and EFLASH [6] are considered as secure multivariate encryption schemes, there exist tasks about their security analysis and key size.

In 2020, Jiahui Chen et al. proposed a new multivariate encryption scheme [4]. Each central map $F = (f_1, \ldots, f_m)$ used in [4] satisfies that the difference $f_i - f_j$ between two quadratic polynomials f_i and f_j is a degree-one polynomial. Also, they applied the minus and plus modifiers to the central map and constructed the public key P.

In this paper, we propose an attack against Chen et al.'s encryption scheme using the property that $f_i - f_j$ is of degree one. To be precise, we show that the vector space spanned by the public key P has degree-one polynomials. By applying such degree-one polynomials to the public key P, we can break Chen et al.'s encryption scheme. We also show that our attack can break the claimed 80 and 128-bit parameters in the complexity of around 27 and 31 bits, respectively.

Our paper is organized as follows: we briefly recall the general construction of multivariate encryption schemes and Chen et al.'s encryption scheme in Section 2. In Section 3, we propose our attack and give experimental results. Finally we conclude our paper in Section 4.

2 Preliminaries

In this section, we describe the general construction of multivariate encryption schemes and Chen et al.'s encryption scheme [4].

2.1 Multivariate public key cryptography

Let $\mathbb{F}$ be a finite field with q elements and n, m be positive integers.

The public key of a multivariate public key cryptosystem consists of m multivariate quadratic polynomials $P = (p_1, \ldots, p_m)$ in n variables $x_1, \ldots, x_n$ over the finite field $\mathbb{F}$. Each polynomial $p_k(x_1, \ldots, x_n)$ is in the form of

$$p_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} b_i x_i + c, \quad (1 \leq k \leq m) \tag{1}$$

where $a_{ij}, b_i, c \in \mathbb{F}$. The security of multivariate public key schemes is based on the so called *MQ-Problem* which asks for a solution of a given system of multivariate quadratic polynomials over the finite field $\mathbb{F}$. In fact, MQ-Problem is proven to be an NP-hard problem even for quadratic polynomials over $\mathbb{F}_2$ [13].

We introduce the general construction of multivariate encryption schemes. First, the most important ingredient is a so called *central map* $F : \mathbb{F}^n \to \mathbb{F}^m$, which is an easily invertible quadratic map. Namely, we can easily compute a solution of $F(x) = y$ for any element $y \in \mathbb{F}^m$. Second, in order to hide the structure of the central map F, we randomly choose two invertible affine (or linear) maps $T : \mathbb{F}^m \to \mathbb{F}^m$ and $S : \mathbb{F}^n \to \mathbb{F}^n$. Then the *public key* is given by

$$P = T \circ F \circ S : \mathbb{F}^n \to \mathbb{F}^m$$

and the *private key* is given by $\{T, F, S\}$. The following is the encryption/decryption process:

Encryption: For a plaintext (or its hash value) $\alpha \in \mathbb{F}^n$, the ciphertext is given by $\beta = P(\alpha) \in \mathbb{F}^m$.

Decryption: For a given ciphertext $\beta \in \mathbb{F}^m$, one computes recursively $\gamma = T^{-1}(\beta), \delta = F^{-1}(\gamma)$ and $\alpha' = S^{-1}(\delta)$. Then α' is the plaintext of the ciphertext β. Here δ is a solution to $F(x) = \gamma$.

2.2 Chen et al.'s Encryption Scheme

Here we describe the construction of Chen et al.'s encryption scheme [4]. For a matrix $C = (c_{i,j})_{i,j} \in \mathbb{F}^{(n+1)\times n}$, we define the polynomials $f_{C,1}, \dots, f_{C,n+1}$ in n variables $x_1, \dots, x_n$ as follows:

$$\begin{aligned} f_{C,1}(x_1, \dots, x_n) &:= (x_1 - c_{1,1})^2 + (x_2 - c_{1,2})^2 + \cdots + (x_n - c_{1,n})^2, \\ &\vdots \\ f_{C,n+1}(x_1, \dots, x_n) &:= (x_1 - c_{n+1,1})^2 + (x_2 - c_{n+1,2})^2 + \cdots + (x_n - c_{n+1,n})^2. \end{aligned}$$

We recall in the below that the polynomial map $F_C = (f_{C,1}, \dots, f_{C,n+1}) : \mathbb{F}^n \to \mathbb{F}^{n+1}$ is easily invertible. For an element $(d_1, \dots, d_{n+1}) \in \mathbb{F}^{n+1}$, we would like to solve the system of equations

$$f_{C,1}(x_1, \dots, x_n) = d_1, \dots, f_{C,n+1}(x_1, \dots, x_n) = d_{n+1}. \tag{2}$$

For any $1 \le i \le n$, we have

$$d_{i+1} - d_i = f_{C,i+1} - f_{C,i} = 2(c_{i,1} - c_{i+1,1})x_1 + \cdots + 2(c_{i,n} - c_{i+1,n})x_n + \sum_{j=1}^{n}(c_{i+1,j}^2 - c_{i,j}^2).$$

From this, we have the linear equations

$$\begin{pmatrix} d_2 - d_1 \\ d_3 - d_2 \\ \vdots \\ d_{n+1} - d_n \end{pmatrix} = C' \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} \sum_{j=1}^{n}(c_{2,j}^2 - c_{1,j}^2) \\ \sum_{j=1}^{n}(c_{3,j}^2 - c_{2,j}^2) \\ \vdots \\ \sum_{j=1}^{n}(c_{n+1,j}^2 - c_{n,j}^2) \end{pmatrix}, \tag{3}$$

where $C' := (2c_{i,j} - 2c_{i+1,j})_{i,j} \in \mathbb{F}^{n\times n}$. Thus if C' is invertible, then we can obtain the solution to (2) by solving the system of linear equations (3).

Now we explain the key-generation of Chen et al.'s encryption scheme [4]. Let a, s be two positive integers and set $m := n + 1 - a + s$. First, randomly choose a matrix $C = (c_{i,j})_{i,j} \in \mathbb{F}^{(n+1)\times n}$ such that C' is invertible. Define the polynomials $F_C = (f_{C,1}, \dots, f_{C,n+1})$ as above. Next, randomly choose quadratic polynomials $g_1, \dots, g_s$ in n variables $x_1, \dots, x_n$ over $\mathbb{F}$. Then the central map is given by

$$F = (f_{C,1}, \dots, f_{C,n+1-a}, g_1, \dots, g_s) : \mathbb{F}^n \to \mathbb{F}^m.$$

Next, randomly choose invertible affine maps $S : \mathbb{F}^n \to \mathbb{F}^n$ and $T : \mathbb{F}^m \to \mathbb{F}^m$. Then the public key is the polynomial map $P := T \circ F \circ S$ and the secret key consists of $F_C = (f_{C,1}, \dots, f_{C,n+1})$, S and T.

Encryption: For a plaintext (or its hash value) $\alpha \in \mathbb{F}^n$, the ciphertext is given by $\beta = P(\alpha) \in \mathbb{F}^m$ by substituting into the public key P.

Decryption: For a given ciphertext $\beta \in \mathbb{F}^m$, first compute $\gamma = (\gamma_1, \dots, \gamma_m) := T^{-1}(\beta)$. Second, for an element $\gamma' = (\gamma'_1, \dots, \gamma'_a) \in \mathbb{F}^a$, solve the system of quadratic equations

$$f_{C,1}(x_1, \dots, x_n) = \gamma_1, \dots, f_{C,n+1-a}(x_1, \dots, x_n) = \gamma_{n+1-a},$$
$$f_{C,n+1-a+1}(x_1, \dots, x_n) = \gamma'_1, \dots, f_{C,n+1}(x_1, \dots, x_n) = \gamma'_a,$$

as explained above. Let $\delta = (\delta_1, \dots, \delta_n)$ be the solution. If we have

$$g_1(\delta) = \gamma_{n+1-a+1}, \dots, g_s(\delta) = \gamma_m,$$

then $\alpha' = S^{-1}(\delta)$ is the message of β. If not, re-choose another $\gamma' = (\gamma'_1, \dots, \gamma'_a) \in \mathbb{F}^a$.

The following table shows the two 80 and 128-bit security parameters (A) and (B) selected in [4].

Table 1. Selected parameters of Chen et al.'s scheme in [4] at 80 and 128-bits security levels. Here, q is the cardinality of the finite field $\mathbb{F}$.

	Security level	(q, n, a, s, m)	Public key (KB)	Secret key (KB)
(A)	80-bits	$(3, 59, 10, 25, 75)$	134	53.9
(B)	128-bits	$(3, 83, 12, 27, 99)$	345	108

3 Our Proposed Attack

In this section, we describe our proposed attack and apply it to the selected parameters in [4].

3.1 A property of the public key

Here we observe a property of the public key P.

Denote the polynomial $f_{C,i+1} - f_{C,i}$ by l_i for each $1 \leq i \leq n-a$. This l_i is a polynomial of degree-one from the definition of $f_{C,i}$. Moreover, the set $\{l_1, \dots, l_{n-a}\}$ is linearly independent since C' is invertible. Denote by $\mathrm{Span}_{\mathbb{F}}F$ the subspace in $\mathbb{F}[x_1, \dots, x_n]$ generated by the polynomials

$$\{f_{C,1}, \dots, f_{C,n+1-a}, g_1, \dots, g_s\}$$

in F over the finite field $\mathbb{F}$. It is clear that $\mathrm{Span}_{\mathbb{F}}F$ contains the set $\{l_1, \dots, l_{n-a}\}$. Therefore, $\mathrm{Span}_{\mathbb{F}}F$ has a linearly independent set of $n-a$ degree-one polynomials.

Let $\mathrm{Span}_{\mathbb{F}}P$ be the subspace in $\mathbb{F}[x_1, \dots, x_n]$ generated by the polynomials $P = \{p_1, \dots, p_m\}$ over $\mathbb{F}$. Since $P = T \circ F \circ S$ and S, T are invertible affine maps, it is easily shown that $\mathrm{Span}_{\mathbb{F}}P$ has a similar property. Namely, $\mathrm{Span}_{\mathbb{F}}P$ has a linearly independent set of $n-a$ degree-one polynomials. Therefore, an attacker can generate a linearly independent set of $n-a$ degree-one polynomials from the public key P.

3.2 Our attack

Let $d = (d_1, \dots, d_m) \in \mathbb{F}^m$ be a ciphertext. We would like to solve the system of m quadratic equations

$$p_1(x_1, \dots, x_n) = d_1, \dots, p_m(x_1, \dots, x_n) = d_m \tag{4}$$

in n variables without the secret key.

Step 1: We solve the system of linear equations in variables $a_1, \dots, a_m$

$$\sum_{i=1}^{m} a_i \cdot \mathrm{Quad}(p_i) = 0,$$

where $\mathrm{Quad}(p_i)$ means the quadratic part of p_i.

Step 2: From what we discussed in 3.1, we can see that the kernel of this system is of dimension $n-a$. Choose a basis $\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n-a)} \in \mathbb{F}^m$ of the kernel. Then we can obtain $n-a$ linearly independent degree-one polynomials

$$\begin{aligned} r_1(x_1, \dots, x_n) &:= \mathbf{a}_1^{(1)} p_1 + \cdots + \mathbf{a}_m^{(1)} p_m, \\ &\vdots \\ r_{n-a}(x_1, \dots, x_n) &:= \mathbf{a}_1^{(n-a)} p_1 + \cdots + \mathbf{a}_m^{(n-a)} p_m. \end{aligned}$$

Step 3: From (4), we have the linear equations

$$\begin{aligned} r_1(x_1,\ldots,x_n) &= \mathbf{a}_1^{(1)}d_1+\cdots+\mathbf{a}_m^{(1)}d_m,\\ &\vdots\\ r_{n-a}(x_1,\ldots,x_n) &= \mathbf{a}_1^{(n-a)}d_1+\cdots+\mathbf{a}_m^{(n-a)}d_m. \end{aligned}$$

By substituting the linear equations into (4), we have a system of $m-(n-a)=s+1$ quadratic equations in a-variables. Using the brute force, we can solve the quadratic system and its solution is equal to the solution of (4), namely, the plaintext of the ciphertext d.

The complexity of Step 1 is that of solving the linear system with size m. Thus it is $\mathcal{O}(m^3)$. We can ignore the complexity of Step 2. In Step 3, its complexity is dominated by solving a system of $(s+1)$ quadratic equations in a-variables, which is done by the brute force. Thus it is $\mathcal{O}(q^a\cdot(s+1)a^2)$, where q is the cardinality of $\mathbb{F}$. Note that we can also use a Gröbner basis algorithm such as F4 [11] to solve the quadratic system in Step 3. We will use F4 algorithm in our experiments and its complexity is lower than that of the brute force.

As a result, the complexity of our attack is $\mathcal{O}(m^3)+\mathcal{O}(q^a\cdot(s+1)a^2)$ at most.

Remark 1. Our analysis implies that the direct attack can break Chen et al.'s scheme in the almost same complexity as that of our attack.

3.3 Apply our attack to the parameters (A) and (B) in Table 1

The claimed 80-bits parameter (A) is $(q,n,a,s,m)=(3,59,10,25,75)$. Thus the complexity of our attack against (A) is $75^3+3^{10}\cdot 26\cdot 10^2=2^{27.19}$. Moreover, the complexity of our attack against the claimed 128-bits parameter (B) is $99^3+3^{12}\cdot 28\cdot 12^2=2^{30.99}$.

The following table is our experimental results. Table 2 presents the average timing of 10 experiments for each parameter. The experiments were performed using Magma V2.24-4 [3] on CPU 1.6GHz Intel Core i5. Here we used F4 algorithm [11] to solve the quadratic system in Step 3.

Table 2. Experimental results for our attack in Section 3.2 at two claimed 80 and 128-bit parameters (A) and (B) of Chen et al.'s scheme in [4]

	Security level	(q,n,a,s,m)	Our attack (s)
(A)	80-bits	$(3,59,10,25,75)$	0.05
(B)	128-bits	$(3,83,12,27,99)$	0.18

4 Conclusion

In this paper, we studied the security against Chen et al.'s encryption scheme [4]. We showed that the vector space spanned by the quadratic polynomials in the public key P has degree-one polynomials. By applying such degree-one polynomials to the public key P, we can break Chen et al.'s encryption scheme [4]. Our attack can break the claimed 80 and 128-bit security parameters in [4] in the complexity of around 27 and 31 bits, respectively.

Acknowledgemants. This work was supported by JST CREST Grant Number JPMJCR14D6 and JSPS KAKENHI Grant Number 19K20266.

References

1. D.J. Bernstein, J. Buchmann, E. Dahmen (Eds.): Post-Quantum Cryptography. Springer, 2009.
2. W. Bosma, J. Cannon, C. Playoust: The Magma algebra system. I. The user language. J. Symbolic Comput. 24, 3-4 (1997), pp. 235 - 265.
3. L. Bettale, J. C. Faugère, L. Perret: Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic, Designs, Codes and Cryptography. Volume 69, Issue 1, pp 1–52, Springer 2013.
4. Jiahui Chen, Jie Ling, Jianting Ning, Terry Shue Chien Lau, Yacheng Wang: A New Encryption Scheme for Multivariate Quadratic Systems. Theoretical Computer Science (2020)
5. N. Courtois: The security of hidden field equations (HFE). In Naccache, C., editor, Progress in cryptology, CT-RSA, volume 2020 of LNCS, pages 266–281. Springer 2001.
6. R. Cartor, D. Smith-Tone, EFLASH: A new multivariate encryption scheme, SAC 2018, LNCS vol. 11349, pp.281–299. Springer 2018.
7. J. Ding, J. E. Gower, D. S. Schmidt: Multivariate Public Key Cryptosystems. Springer, 2006.
8. J. Ding, T. J. Hodges, Inverting HFE Systems is Quasi-Polynomial for All Fields, Crypto 2011, LNCS 6841, pp.724–742. Springer 2011.
9. J. Ding, D. S. Schmidt: Rainbow, a new multivariate polynomial signature scheme. ACNS 2005, LNCS vol. 3531, pp. 164–175. Springer 2005.
10. V. Dubois, N. Gamma, The Degree of Regularity of HFE Systems, Asiacrypt 2010, LNCS 6477, pp.557–576. Springer 2010.
11. J.C. Faugère: A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139, pp. 61-88 (1999).
12. J.C. Faugère, A. Joux, Algebraic cryptanalysis of Hidden Field Equations (HFE) using Groöbner bases, Crypto 2003, LNCS 2729, pp.44–60. Springer 2003.
13. M. R. Garey and D. S. Johnson: Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company 1979.
14. L. Granboulan, A. Joux, J. Stern: Inverting HFE is quasipolynomial, Crypto 2006, LNCS 4117, pp.345–356. Springer 2006.
15. Yasuhiko Ikematsu, Ray Perlner, Daniel Smith-Tone, Tsuyoshi Takagi and Jeremy Vates: HFERP - A New Multivariate Encryption Scheme. PQCrypto 2018. LNCS vol. 10786, pp. 396-416. Springer 2018.

16. A. Kipnis, L. Patarin, L. Goubin: Unbalanced Oil and Vinegar Schemes. EUROCRYPT 1999, LNCS vol. 1592, pp. 206–222. Springer 1999.
17. A. Kipnis, A. Shamir: Cryptanalysis of the HFE public key cryptosystem by relinearization. In Wiener, M., editor, Advances in Cryptology – CRYPTO'99, volume 1666 of LNCS, pages 19–30, Springer 1999.
18. T. Matsumoto, H. Imai: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. EUROCRYPT 1988. LNCS vol. 330, pp. 419-453. Springer 1988.
19. J. Patarin: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88. CRYPTO 1995, LNCS vol. 963, pp. 248-261. Springer, 1995.
20. J. Patarin: Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. EUROCRYPT, LNCS vol. 1070, pp. 33 - 48. Springer, 1996.
21. A. Petzoldt, M.S. Chen, B.Y. Yang, C. Tao, J. Ding: Design Principles for HFEv-based Signature Schemes. ASIACRYPT 2015 - Part I, LNCS vol. 9452, pp. 311 - 334. Springer 2015.
22. A. Szepieniec, J. Ding, B. Preneel: Extension Field Cancellation: a New Central Trapdoor for Multivariate Quadratic Systems. In PQCrypto 2016, volume 9606 of LNCS, pages 182–196, Springer 2016.
23. C. Tao, A. Diene, S. Tang, J. Ding: Simple matrix scheme for encryption. In PQCrypto 2013, volume 7932 of LNCS, pages 231–242, Springer 2013.