

Multivariate Public Key Cryptosystems

Yasufumi Hashimoto

Abstract This paper presents a survey on the multivariate public key cryptosystem (MPKC), which is a public key cryptosystem whose public key is a set of multivariate quadratic forms over a finite field.

Keywords Multivariate public key cryptosystem (MPKC) · Post-quantum cryptology

1 Introduction

A *Multivariate Public Key Cryptosystem (MPKC)* is a public key cryptosystem whose public key is a set of multivariate quadratic forms

$$\begin{aligned} f_1(x_1, \dots, x_n) &= \sum_{1 \leq i \leq j \leq n} a_{ij}^{(1)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(1)} x_i + c^{(1)}, \\ &\vdots \\ f_m(x_1, \dots, x_n) &= \sum_{1 \leq i \leq j \leq n} a_{ij}^{(m)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(m)} x_i + c^{(m)} \end{aligned} \quad (1)$$

over a finite field. It is known that MPKCs have advantage that the encryption (or signature verification) is faster than RSA and ECC [22]. Furthermore, since the problem of solving a system of multivariate nonlinear polynomial equations over a finite field of order 2 is NP-hard [48, 49], it has been expected that a secure cryptosystem can be constructed by a set of multivariate polynomials. Especially, after Shor [95] proposed polynomial time quantum algorithms for factoring integers and solving discrete logarithm problems, MPKCs have been considered as one of leading candidates of *Post-Quantum Cryptography* as well as the lattice-based cryptography,

Y. Hashimoto (✉)

Department of Mathematical Sciences, University of the Ryukyus, Nishihara-cho,
Okinawa 903-0213, Japan
e-mail: hashimoto@math.u-ryukyu.ac.jp

© Springer Nature Singapore Pte Ltd. 2018

T. Takagi et al. (eds.), *Mathematical Modelling for Next-Generation Cryptography*,
Mathematics for Industry 29, DOI 10.1007/978-981-10-5065-7_2

the code-based cryptography and the isogeny-based cryptography. In fact, MPKC is included in NIST's proposals of standardization of post-quantum cryptography [24, 72, 76].

This paper presents a survey on MPKC. In Sect. 2, we describe two early MPKCs called the *Matsumoto–Imai cryptosystem* (MI, C^*) [69] and the *Moon Letter cryptosystem* ($ML, TsuKIFM$) [105] proposed in 1980s and the general construction of MPKCs. While these early MPKCs were already broken [29, 52, 79], the construction of maps

$$F = T \circ G \circ S \quad (2)$$

has been used in most MPKCs, where S, T are secret invertible affine maps, G is a quadratic map to be feasibly inverted and F is a public quadratic map. The central map G essentially characterizes the corresponding MPKC. The security and the speed of decryption highly depend on G . Unfortunately, at the present time, there are few works on the security proof of MPKCs. On the other hand, there are various attacks on proposed MPKCs. Such works greatly help to build secure MPKCs by pointing out which properties of G yield vulnerabilities. In Sect. 3, we give outlines of major attacks on MPKCs to explain which properties of G yield vulnerabilities of the corresponding MPKC. In Sect. 4, we describe several famous MPKCs and discuss their security based on the descriptions in Sect. 3. Finally in Sect. 5, we conclude this paper by listing open problems on MPKCs for future developments.

2 Early MPKCs and General Construction

2.1 Early MPKCs

In this subsection, we describe two early MPKCs, the Matsumoto–Imai cryptosystem [69] and the Moon Letter cryptosystem [105].

Matsumoto–Imai's cryptosystem (MI, C^* [69]).

Let $n \geq 1$ be an integer, k a finite field of even characteristic, $q := \#k$, K an n -extension of k and $\{\theta_1, \dots, \theta_n\} \subset K$ a basis of K over k . Choose an integer $i \geq 1$ such that $\gcd(q^n - 1, q^i + 1) = 1$ and define the map $\mathcal{G} : K \rightarrow K$ by

$$\mathcal{G}(X) = X^{1+q^i}. \quad (3)$$

The *secret key* of this scheme is a pair of two invertible affine maps $S, T : k^n \rightarrow k^n$ and the *public key* is

$$F := T \circ \phi^{-1} \circ \mathcal{G} \circ \phi \circ S : k^n \rightarrow k^n, \quad (4)$$

where $\phi : k^n \rightarrow K$ is a one-to-one map, e.g., $\phi(x_1, \dots, x_n) = x_1\theta_1 + \dots + x_n\theta_n$ for $(x_1, \dots, x_n)^t \in k^n$. Since it holds

$$X^{q^i} = (x_1\theta_1 + \dots + x_n\theta_n)^{q^i} = x_1\theta_1^{q^i} + \dots + x_n\theta_n^{q^i}$$

for $X := x_1\theta_1 + \dots + x_n\theta_n \in K$, $\phi^{-1}(X^{q^i})$ is a set of linear forms of x_1, \dots, x_n over k and then the public key F is quadratic over k . For a given plaintext $x \in k^n$, the *ciphertext* is $y = F(x) \in k^n$. To *decrypt* y , first calculate $Z := \phi(T^{-1}(y)) \in K$ and compute $W := Z^l \in K$ where the integer l satisfies $(1 + q^i)l \equiv 1 \pmod{q^n - 1}$. The plaintext is $x = S^{-1}(\phi^{-1}(W))$.

Moon Letter cryptosystem (ML, TsuKIFM [105]).

Let $n \geq 1$ be an integer, k a finite field and $g_1(x), \dots, g_n(x)$ the quadratic forms of $x = (x_1, \dots, x_n)^t$ over k given by

$$\begin{aligned} g_1(x) &= (\text{linear form of } x_1), \\ g_2(x) &= x_2 \cdot (\text{linear form of } x_1) + (\text{quadratic form of } x_1), \\ g_3(x) &= x_3 \cdot (\text{linear form of } x_1, x_2) + (\text{quadratic form of } x_1, x_2), \\ &\vdots \\ g_n(x) &= x_n \cdot (\text{linear form of } x_1, \dots, x_{n-1}) + (\text{quadratic form of } x_1, \dots, x_{n-1}). \end{aligned} \tag{5}$$

The *secret key* is a pair of two invertible affine maps $S, T : k^n \rightarrow k^n$ and the quadratic map $G : k^n \rightarrow k^n$ given by $G(x) = (g_1(x), \dots, g_n(x))^t$. The *public key* is the quadratic map

$$F := T \circ G \circ S : k^n \rightarrow k^n. \tag{6}$$

For a given plaintext $x' \in k^n$, the *ciphertext* is $y = F(x') \in k^n$. To *decrypt* the cipher $y \in k^n$, first compute $z = (z_1, \dots, z_n)^t := T^{-1}(y)$ and find $x_1 \in k$ such that $g_1(x) = z_1$. Since $g_1(x)$ is a linear form of x_1 , x'_1 is recovered easily. Next find $x_2 \in k$ such that $g_2(x) = z_2$. Since $g_2(x)$ is a linear form of x_2 for a fixed x_1 , x_2 is recovered easily. Similarly, we can recover $x_3, \dots, x_n \in k$ such that $g_3(x) = z_3, \dots, g_n(x) = z_n$ recursively. The plaintext is $x' = S^{-1}(x_1, \dots, x_n)^t$.

Unfortunately, ML had not been known well since it was proposed on the paper [105] written in Japanese at 1986. Instead, Shamir's birational signature scheme [93] presented at Crypto 1993 has been well known. These two schemes are quite similar. In fact, the map G in Shamir's scheme is given by $m = n - 1$ and $G(x) = (g_2(x), \dots, g_n(x))^t$.

2.2 General Construction of MPKCs

Similar to MI and ML, most MPKCs have the structure $F := T \circ G \circ S$. We describe the general construction of MPKCs in this subsection.

Let $n, m \geq 1$ be integers, k a finite field and $q := \#k$. The *secret key* is a tuple of three maps (S, G, T) , where $S : k^n \rightarrow k^n$, $T : k^m \rightarrow k^m$ are invertible affine maps and $G : k^n \rightarrow k^m$ is a quadratic map that is *inverted feasibly*. The *public key* F is the convolution of these three maps S, G, T :

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

For a given plaintext $x \in k^n$, the *ciphertext* $y \in k^m$ is computed by $y = F(x)$. To *decrypt* y , find $z \in k^n$ such that $G(z) = T^{-1}(y)$. Then the plaintext is $x = S^{-1}(z)$. Since G is *inverted feasibly*, one can decrypt y efficiently.

Efficiency.

One of remarkable advantage of MPKCs is the speed of encryption (or signature verification). Under the naive implementation, the ciphertext $y = (y_1, \dots, y_m)^t \in k^m$ of a plaintext $x = (x_1, \dots, x_n)^t \in k^n$ is computed by

$$\begin{aligned} y_i = f_i(x) &= x_1 \cdot \left(a_{11}^{(i)} \cdot x_1 + a_{12}^{(i)} \cdot x_2 + \dots + a_{1n}^{(i)} \cdot x_n + b_1^{(i)} \right) \\ &\quad + x_2 \cdot \left(a_{22}^{(i)} \cdot x_2 + \dots + a_{2n}^{(i)} \cdot x_n + b_2^{(i)} \right) \\ &\quad + \dots \\ &\quad + x_n \cdot \left(a_{nn}^{(i)} \cdot x_n + b_n^{(i)} \right) + c_i, \quad (1 \leq i \leq m). \end{aligned}$$

It is clear that the numbers of multiplications and additions in this computation for each $1 \leq i \leq m$ are $\ll \frac{1}{2}n^2$. Such a computation is not best possible. In fact, there have been ideas to reduce the number of operations for several MPKCs by reducing the number of parameters in the public key [43, 85, 86]. Furthermore, the average speed of encryption can be improved if several plaintexts are encrypted simultaneously. As an example, we now study the situation that one encrypts $n + 1$ plaintexts $p_1, \dots, p_{n+1} \in k^n$. For $x = (x_1, \dots, x_n)^t \in k^n$, let $\bar{x} := (x_1, \dots, x_n, 1)^t \in k^{n+1}$ and denote by A_i an $(n + 1) \times (n + 1)$ matrix with

$$f_i(x) = \bar{x}^t A_i \bar{x},$$

for $1 \leq i \leq m$. Then we see that

$$\begin{pmatrix} f_i(p_1) \\ \vdots \\ f_i(p_{n+1}) \end{pmatrix} = \begin{pmatrix} \bar{p}_1^t \cdot (A_i \cdot P)_1 \\ \vdots \\ \bar{p}_{n+1}^t \cdot (A_i \cdot P)_{n+1} \end{pmatrix} \quad (7)$$

where $P := (\bar{p}_1, \dots, \bar{p}_{n+1})$ is the $(n+1) \times (n+1)$ matrix and $(*)_j$ is the j -th column vector. The Eq. (7) means that $(f_i(p_1), \dots, f_i(p_{n+1}))^t$ is computed by one multiplication $A_i \cdot P$ of $(n+1) \times (n+1)$ matrices and $n+1$ inner products of $(n+1)$ -vectors. Thus the number of operations for encrypting $n+1$ plaintexts is $\ll (n+1)^w m$, where $2 \leq w \leq 3$ is the exponent of the matrix multiplication algorithms (see e.g., [14, 28, 66, 98], $w = 2.3728 \dots$ is the presently best estimate [66]). It is smaller than the number of operations $O(n^3 m)$ by the naive computations.

On the other hand, the size of a public key of MPKC is, in general, relatively larger than other cryptosystems. In fact, the number of coefficients of the quadratic forms in F is about $\frac{1}{2}n^2 m$, which means that, if n, m are around one hundred, the key size of public key is over several hundreds kilo bites under naive implementations. Then reducing key size is an important problem for MPKCs. Note that approaches to reduce the key size for several MPKCs are given in [43, 85, 86].

Security.

Since $F = T \circ G \circ S$, the quadratic forms in the public key F are given by

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix} = T \begin{pmatrix} g_1(S(x)) \\ \vdots \\ g_m(S(x)) \end{pmatrix}. \quad (8)$$

The roles of the secret affine maps S, T are to transform the map G inverted feasibly into the map F not inverted feasibly. Remark that, for most MPKCs, there are nontrivial S, T such that F can be inverted efficiently. For example, on ML, if $S = \begin{pmatrix} * & * \\ \cdot & \cdot \\ 0 & * \end{pmatrix}$ and $T = \begin{pmatrix} * & 0 \\ \cdot & \cdot \\ * & * \end{pmatrix}$, the quadratic forms $f_1(x), \dots, f_m(x)$ are also in the form (5), which are inverted recursively. We call such a bad pair (S, T) a *weak key*, and call a pair (S_1, T_1) an *equivalent key* if $(SS_1^{-1}, T_1^{-1}T)$ is a weak key. It is important to study which kind of (S, T) is weak, not to choose such weak keys as a secret key.

We also remark that several MPKCs are known to be insecure at all for arbitrary (S, T) . In fact, two early MPKCs were already broken [29, 52, 79]. We describe how to break them in the next subsection.

2.3 Attacks on Early MPKCs

Patarin's attack on MI [79].

For a plaintext $x = (x_1, \dots, x_n)^t \in k^n$ and the corresponding ciphertext $y = (y_1, \dots, y_n)^t \in k^n$, let $X := \phi(S^{-1}(x))$ and $Y := \phi(T^{-1}(y)) = X^{1+q^i}$. It is easy to see that

$$Y X^{q^{2i}} = Y^{q^i} X \left(= X^{1+q^i+q^{2i}} \right). \quad (9)$$

Since $\phi^{-1}(Y), \phi^{-1}(Y^{q^i})$ are sets of linear forms of y and $\phi^{-1}(X), \phi^{-1}(X^{q^{2i}})$ are those of x , there exist polynomials over k in the form

$$L(x, y) := \sum_{1 \leq i, j \leq n} \alpha_{ij} x_i y_j + \sum_{1 \leq i \leq n} \beta_i x_i + \sum_{1 \leq j \leq n} \gamma_j y_j + \delta \quad (10)$$

such that $L(x, y) = 0$ holds for arbitrary plaintext–ciphertext pairs (x, y) . To determine the coefficients $\alpha_{ij}, \beta_i, \gamma_j, \delta \in k$, prepare sufficiently many pairs (x, y) of the plaintext and ciphertext, substitute them into (10) to generate a system of linear equations of variables $\alpha_{ij}, \beta_i, \gamma_j, \delta$ and solve its system. Once the attacker finds polynomials in the form (10), he/she can get candidates of the plaintext $x = (x_1, \dots, x_n)^t$ by solving a system of linear equations derived from (10). It is known that the number of candidates of x given by this attack is $q^{\text{gcd}(i, n)} \leq q^{n/3}$, which is much smaller than $\#k^n = q^n$. \square

Hasegawa–Kaneko’s attack on ML [29, 52].

Let G_1, \dots, G_n be the coefficient matrices of $g_1(x), \dots, g_n(x)$, namely $g_i(x) = x^t G_i x + (\text{linear form})$. By the construction of g_i ’s, we see that

$$G_n = \begin{pmatrix} * & * \\ * & 0 \end{pmatrix}, \quad G_{n-1} = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}, \quad \dots$$

Since the coefficient matrices F_1, \dots, F_n of the public polynomials $f_1(x), \dots, f_n(x)$ are given by

$$\begin{pmatrix} F_1 \\ \vdots \\ F_n \end{pmatrix} = T \begin{pmatrix} S^t G_1 S \\ \vdots \\ S^t G_n S \end{pmatrix},$$

there exist constants $\alpha_1, \dots, \alpha_{n-1} \in k$ such that

$$\text{rank}(F_i - \alpha_i F_n) \leq n - 1, \quad \text{i.e.} \quad \det(F_i - \alpha_i F_n) = 0$$

for $1 \leq i \leq n - 1$. Then the attacker can find such α_i ’s by solving univariate polynomial equations. It is easy to see that such α_i ’s are partial information of T , which means that, once α ’s are recovered, the attacker can recover partial information of S easily. Further information of S, T can be recovered recursively. \square

3 Major Attacks

Section 2.3 describes attacks on the early MPKCs based on the property of G . Now we want to know *what kinds of G construct secure MPKCs*. Unfortunately, we do not have complete answers; there are no MPKCs with security proofs at the present time. On the other hand, there have been various works on cryptanalysis against proposed

MPKCs. These works give answers for *what kinds of G construct insecure MPKCs*, which are quite helpful to build secure MPKCs. In this section, we describe outlines of major attacks on MPKCs.

3.1 Direct Attacks

The *direct attack* is to find a common solution of multivariate quadratic equations

$$f_1(x_1, \dots, x_n) = y_1, \quad \dots, \quad f_m(x_1, \dots, x_n) = y_m \quad (11)$$

to recover the plaintext $x = (x_1, \dots, x_n)^t \in k^n$ of a ciphertext $y = (y_1, \dots, y_m)^t \in k^m$. The most naive approach is the *exhaustive search*, whose complexity is heuristically $O(q^{\min(m,n)} \cdot (\text{polyn.}))$. It is too heavy in general, and then the attacker requires better algorithms. Note that a faster algorithm was proposed in [16] for $q = 2$.

One of standard approaches for direct attacks is by computing the Gröbner basis of the polynomial system $\{f_1(x) - y_1, \dots, f_m(x) - y_m\}$. While the complexity of the original Gröbner basis algorithm by Buchberger [17] is $O(2^{2^n})$, there have been improved algorithms such like the F_4 - and F_5 -algorithms [5, 10, 44, 45]. It is known that the complexities of these algorithms depend on the *degree of regularity* d_{reg} of the corresponding polynomial system, in fact, the complexity of F_5 algorithm is $\ll m^{\binom{n+d_{\text{reg}}-1}{d_{\text{reg}}}}$. When the polynomial system is over-defined ($m > n$) and is *semi-regular*, d_{reg} coincides with the smallest degree of the non-positive coefficients of the polynomial $\frac{(1-t^2)^m}{(1-t)^n}$ [5]. This means that, if m is sufficiently larger than n , d_{reg} is small enough. Especially, when $m \gg \frac{1}{2}n^2$, this algorithm is in polynomial time. When the difference $m - n$ is small, one can reduce the complexity by mixing the exhaustive search with the Gröbner basis algorithm. This approach is called the *hybrid* approach. According to [10], its complexity is $O(2^{m(3.31-3.62/\log_2 q)})$ for $n = m$.

For under-defined systems ($n > m$), there are improved algorithms. When $n \geq \frac{1}{2}m(m+1)$, Cheng et al. [25] (see also [53, 65, 70]) proposed a polynomial time algorithm to find a solution x by reducing the problem of solving $\{f_1(x) = y_1, \dots, f_m(x) = y_m\}$ to the problem of finding a solution of

$$\begin{aligned} &(\text{quadratic form of } x_1) = 0, \\ &(\text{quadratic form of } x_1, x_2) = 0, \\ &\quad \vdots \\ &(\text{quadratic form of } x_1, \dots, x_m) = 0. \end{aligned} \quad (12)$$

It is clear that (12) can be solved recursively. Even if $n < \frac{1}{2}m(m+1)$, relatively efficient algorithms are proposed in [25, 104]. For example, if $n \geq \frac{1}{2}m(m+1) - \frac{1}{2}l(l+1)$ ($1 \leq l < m$), one can reduce the corresponding problem to the problem of

finding a solution of the system of l quadratic equations of l variables, which can be solved by the Gröbner basis algorithm more efficiently than the original system of quadratic equations.

In April 2015, the *MQ Challenge* [113] started. It is a challenge to solve a given system of multivariate quadratic equations chosen randomly for $m = 2n$, $n \sim 1.5m$ and $q = 2, 2^8, 31$. The records of this challenge have been renewed frequently, which shows that the algorithms for the direct attack have been developing quickly.

3.2 Rank Attacks

The *rank attack* is to recover T partially when the coefficient matrices of quadratic forms have special conditions on their ranks. Let G_1, \dots, G_m be the coefficient matrices of the quadratic forms $g_1(x), \dots, g_m(x)$ in the central map G , and F_1, \dots, F_m those of $f_1(x), \dots, f_m(x)$ in the public key F . Due to (8), we have

$$F_j = S^t \left(\sum_{1 \leq i \leq m} t_{ij} G_i \right) S, \quad (1 \leq j \leq m), \quad (13)$$

where t_{ij} 's are the entries in T . Then the rank of F_j coincides with the rank of $\sum_i t_{ij} G_i$. This means that, if there exist constants $c_1, \dots, c_m \in k$ such that the rank of $\sum_i c_i G_i$ is $r (< n)$, there exist constants $c'_1, \dots, c'_m \in k$ such that the rank of $\sum_i c'_i F_i$ is (at most) r . The rank attack recovers such constants c'_1, \dots, c'_m .

For example, on ML (Sects. 2.1, 2.3), G_n is of rank n and arbitrary linear sums of G_1, \dots, G_{n-1} are of rank $n - 1$. Then there exist $\alpha_1, \dots, \alpha_{n-1} \in k$ such that the rank of $F_i - \alpha_i F_n$ ($1 \leq i \leq n - 1$) is at most $n - 1$ and the attacker can recover T partially by these constants $\alpha_1, \dots, \alpha_{n-1}$.

There are two kinds of rank attacks. One is the *min-rank attack*, which is available if there exist $\beta_1, \dots, \beta_m \in k$ such that the rank r of $\sum_{1 \leq i \leq m} \beta_i G_i$ is small. The other is the *high-rank attack*, which is available if there exists a small integer $1 \leq l < m$, elements $\beta_1, \dots, \beta_{m-l} \in k$ and a series $\{i_1, \dots, i_{m-l}\} \subset \{1, \dots, m\}$ such that the rank of $\sum_{1 \leq j \leq m-l} \beta_j G_{i_j}$ is smaller than n .

When q is small, the rank attacks include exhaustive searches and their complexities are known to be $O(q^{r \lfloor \frac{m}{r} \rfloor} \cdot (\text{polyn.}))$ for the min-rank attack and $O(q^l \cdot (\text{polyn.}))$ for the high-rank attack [108]. On the other hand, when q is large, the attacker of the min-rank attack tries to find a solution of the system of polynomial equations of $(\alpha_1, \dots, \alpha_m)$ derived from the condition $\text{rank}(\sum_{1 \leq i \leq m} \alpha_i F_i) \leq r$. Since $\text{rank}(A) \leq r$ is equivalent that the determinants of all $(r + 1) \times (r + 1)$ minor matrices in A are zero, the corresponding equations are of degree (at most) $r + 1$. While solving a system of high degree equations is difficult in general, it can be done effectively by the Gröbner basis algorithm if r is small enough since the number of equations are much larger than the number of variables. In fact, its complexity is known to be $O\left(\binom{n+r+1}{r+1}^w\right)$ for $n = m$ under several good conditions (see [11, 64]).

3.3 Conjugation Attacks

Let H_1, H_2 be linear sums of F_1, \dots, F_m . Due to (13), we see that

$$H_1^{-1}H_2 = S^{-1}(Q_1^{-1}Q_2)S,$$

where Q_1, Q_2 are linear sums of G_1, \dots, G_m . If $Q_1^{-1}Q_2$ has special properties for conjugation, the attacker can recover S partially.

For example, the coefficient matrices G_1, \dots, G_m on the *oil and vinegar signature scheme* (OV) (Sect. 4.1.1, [81]) are expressed by $\begin{pmatrix} 0_m & * \\ * & *_{*m} \end{pmatrix}$, which means

$$H_1^{-1}H_2 = S^{-1} \begin{pmatrix} 0_m & * \\ * & *_{*m} \end{pmatrix} \begin{pmatrix} *_{*m} & * \\ * & 0_m \end{pmatrix} S = S^{-1} \begin{pmatrix} *_{*m} & * \\ 0 & *_{*m} \end{pmatrix} S.$$

By using the equation above, Kipnis and Shamir [63] proposed a polynomial time algorithm to recover S_1 such that $SS_1 = \begin{pmatrix} *_{*m} & * \\ 0_m & *_{*m} \end{pmatrix}$. Since $S = \begin{pmatrix} *_{*m} & * \\ 0 & *_{*m} \end{pmatrix}$ is a weak key, Kipnis–Shamir’s attack breaks OV.

This attack is also available on the signature scheme YTS (Sect. 4.3.2, [55, 111]) and on MPKCs derived from a quadratic map over an extension field (Sect. 4.2.4, [23, 59, 107]), since the coefficient matrices F_i ’s are respectively expressed by $S'(G'_i \otimes I_r)S$ with smaller matrix G'_i and $\tilde{S}' \begin{pmatrix} *_{*N} & & \\ & \ddots & \\ & & *_{*N} \end{pmatrix} \tilde{S}$ with a divisor $N \mid n$ and a matrix \tilde{S} over an extension field including the secret key S .

Remark that this attack cannot be used directly when the field is of even characteristic. When k is of even characteristic, the coefficient matrix H cannot be symmetric. Then, instead of H , the attacker will use the matrix $\hat{H} := H + H'$. Since \hat{H} is skew-symmetric ($\hat{H} + \hat{H}' = 0$), \hat{H} is not invertible when n is odd and the characteristic polynomial of $\hat{H}_1^{-1}\hat{H}_2$ is a square of a smaller degree polynomial when n is even (see e.g., [20, 40, 101]). Thus more delicate discussions are required for even characteristic cases.

3.4 Linearization Attacks

Recall that Patarin’s attack on MI (Sect. 2.3, [79]) recovers polynomials in the form

$$L(x, y) := \sum_{1 \leq i, j \leq n} \alpha_{ij} x_i y_j + \sum_{1 \leq i \leq n} \beta_i x_i + \sum_{1 \leq j \leq n} \gamma_j y_j + \delta \quad (14)$$

satisfying $L(x, y) = 0$ for arbitrary plaintext–ciphertext pairs (x, y) . The *linearization attack* is to recover such polynomials if there exist. Once the attacker obtains

such polynomials, he/she will get (candidates of) the plaintexts x of given ciphertexts y .

The basic approach to determine L is as follows. First, prepare sufficiently many plaintext–ciphertext pairs (x, y) . Next, generate a system of linear equations of the coefficients in L by the pairs (x, y) . Finally, solve the linear equations to determine the coefficients of L . The complexity of this attack depends on the number of monomials in L . For example, on MI, the complexity of the linearization attack is $O(n^{2w})$ since the number of monomials in (14) is $(n + 1)^2$.

Such an attack is extended to MFE [37, 107] and the simple matrix encryption scheme [99]. On MFE, there exist quadratic polynomials $h_1(y), \dots, h_{n+1}(y)$ such that

$$L(x, y) := \sum_{1 \leq i \leq n} x_i \cdot h_i(y) + h_{n+1}(y) \quad (15)$$

satisfies $L(x, y) = 0$ for any plaintext–ciphertext pairs (x, y) . Then the complexity of the linearization attack on MFE is not large. On the simple matrix encryption scheme, the complexity is sub-exponential time since the degrees of the polynomials corresponding to $h_1(y), \dots, h_{n+1}(y)$ are \sqrt{n} .

Remark that there are two ways to generate plaintext–ciphertext pairs (x, y) . One is by encrypting chosen plaintexts $x \in k^n$, and the other is by decrypting chosen ciphertexts $y \in k^m$. The former is a *chosen plaintext attack (CPA)* and the latter is a *chosen ciphertext attack (CCA)*. On MI and MFE, CPA is available. On the other hand, if the decryption map $\Psi : k^m \rightarrow k^n$ is not an inversion of F , namely $\Psi(F(x)) = x$ for $x \in k^n$ but $F(\Psi(y)) \neq y$ for sufficiently many $y \in k^m$, there is a possibility that CCA is available. In fact, CCA helps to recover the decryption map of ZHFE (Sect. 4.2.4, [60, 89]). Furthermore, if hidden information is used in the decryption algorithm, CCA might be able to recover such hidden information. Actually, the additional polynomials in Zhang–Tan’s variant [114, 115] can be recovered by CCA [57].

3.5 Differential Attacks

The *differential attack* is based on a *symmetric property* of the difference

$$Df(x, a) := f(x + a) - f(x) - f(a) + f(0),$$

for the polynomial map f associated with the corresponding MPKC. For example, Dubois et al. [41] proposed the differential attack on Sflash [1] (a variant of MI) by using the following symmetric relation:

$$D\mathcal{G}(\alpha X, a) + D\mathcal{G}(X, \alpha a) = (\alpha^{q^i} + \alpha)D\mathcal{G}(X, a), \quad (16)$$

where $\mathcal{G}(X) := X^{q^i+1}$ is the central map of MI. It is known that the differential attack is also available on l -IC and the internal perturbations of MI, HFE [42, 46, 47]. On the other hand, the security of HFE and its variations have been studied in [19, 32] and it was proved that HFEv- is secure against the differential attack.

3.6 Physical Attacks

Physical attacks, e.g., the *side channel attacks* and the *fault attacks*, have been studied for RSA [15, 62], ECC [13, 27, 30], Pairing [78], lattice- and code-based cryptosystems [2, 21, 71]. Also for MPKCs, there are several works on physical attacks.

Okeya et al. [77] proposed a *side channel attack* on Sflash [1] before Sflash was broken by the differential attack [41]. This attack can recover the random seed used for hashing in the process of signature generation. Furthermore, *fault attacks* on MPKCs was proposed at PQCrypto 2011 [61]. By comparing plaintext–ciphertext pairs given by a faulty map and those by the unfaulty (original) map, the attacker can recover the secret key S , T partially. It is known that the fault attack is available on most MPKCs under naive implementations. These works imply that MPKCs must be implemented carefully, not to be broken by physical attacks.

4 Proposed MPKCs

Until now, various MPKCs have been proposed. In this section, we describe famous MPKCs and discuss their security based on the descriptions of Sect. 3.

4.1 Stepwise Triangular Type

Recall that the central map G of ML (Sect. 2.1, [105]) is inverted recursively. While ML itself was already broken [52], the idea *decrypting step-by-step* is used in several MPKCs. We now give examples of MPKCs having the step-by-step structure.

4.1.1 Oil and Vinegar Signature Scheme

In the *Oil and Vinegar signature scheme (OV)* proposed by Patarin [81], $n = 2m$ and the quadratic map G is defined by

$$\begin{aligned}
g_j(x) = & \sum_{1 \leq i \leq m} x_i \cdot (\text{linear form of } x_{m+1}, \dots, x_n) \\
& + (\text{quadratic form of } x_{m+1}, \dots, x_n),
\end{aligned} \tag{17}$$

for $1 \leq j \leq m$. Remark that the affine map T is not necessary in OV since the polynomials in $T \circ G$ is also in the form (17). This scheme signs a message $y \in k^m$ as follows. First, choose $u_1, \dots, u_m \in k$ randomly and find $z_1, \dots, z_m \in k$ such that

$$\begin{aligned}
g_1(z_1, \dots, z_m, u_1, \dots, u_m) &= y_1, \\
&\vdots \\
g_m(z_1, \dots, z_m, u_1, \dots, u_m) &= y_m.
\end{aligned} \tag{18}$$

The signature of y is $x = S^{-1}(z_1, \dots, z_m, u_1, \dots, u_m)^t \in k^n$. By the definition of G , we see that (z_1, \dots, z_m) is given as a solution of m linear equations of m variables.

As already given in Sect. 3.3, an equivalent secret key of OV is recovered in polynomial time by Kipnis–Shamir’s attack [63] since the coefficient matrices of g_1, \dots, g_m are in the form $\begin{pmatrix} 0_m & * \\ * & *_{*m} \end{pmatrix}$ and $\begin{pmatrix} 0_m & * \\ * & *_{*m} \end{pmatrix}^{-1} \begin{pmatrix} 0_m & * \\ * & *_{*m} \end{pmatrix} = \begin{pmatrix} *_{*m} & * \\ 0 & *_{*m} \end{pmatrix}$. To enhance its security, Kipnis–Patarin–Goubin [65] proposed an arrangement of OV called the *Unbalanced Oil and Vinegar signature scheme (UOV)*. On this scheme, $n > 2m$ ($v := n - 2m$) and G is given as (17) for $1 \leq j \leq m$. The signature generation is almost same to the original OV. It is easy to see that $S = \begin{pmatrix} *_{*m} & * \\ 0 & *_{*m+v} \end{pmatrix}$ is a *weak key* of UOV.

Different to the original OV, Kipnis–Shamir’s attack is not available on UOV directly since the coefficient matrices are in the form $\begin{pmatrix} 0_m & * \\ * & *_{*m+v} \end{pmatrix}$ but $\begin{pmatrix} 0_m & * \\ * & *_{*m+v} \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0_m & * \\ * & *_{*m+v} \end{pmatrix} \neq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. Kipnis–Patarin–Goubin [65] also arrange Kipnis–Shamir’s attack to be available on UOV with the complexity $O(q^v \cdot (\text{polyn.}))$.

The advantage of UOV is that the signature generation is elementary and the security seems enough for $v \sim m$ ($n \sim 3m$). However, the key size is relatively larger than other MPKCs. We then need to reduce the key size of this scheme.

4.1.2 Rainbow

Rainbow [35] is the multi-layer version of UOV. For integers $o_1, \dots, o_l, v \geq 1$, put $m := o_1 + \dots + o_l, n := m + v$ and define G as follows:

$$\begin{aligned}
g_1(x), \dots, g_{o_1}(x) &= \sum_{1 \leq i \leq o_1} x_i \cdot (\text{linear form of } x_{o_1+1}, \dots, x_n) \\
&\quad + (\text{quadratic form of } x_{o_1+1}, \dots, x_n), \\
g_{o_1+1}(x), \dots, g_{o_1+o_2}(x) &= \sum_{o_1+1 \leq i \leq o_1+o_2} x_i \cdot (\text{linear form of } x_{o_1+o_2+1}, \dots, x_n) \\
&\quad + (\text{quadratic form of } x_{o_1+o_2+1}, \dots, x_n), \\
&\vdots \\
g_{o_1+\dots+o_{l-1}+1}(x), \dots, g_m(x) &= \sum_{o_1+\dots+o_{l-1}+1 \leq i \leq m} x_i \cdot (\text{linear form of } x_{m+1}, \dots, x_n) \\
&\quad + (\text{quadratic form of } x_{m+1}, \dots, x_n).
\end{aligned}$$

It is a generalization of ML and (U)OV. In fact, Rainbow with $l = n$, $o_1 = \dots = o_n = 1$ and $v = 0$ is almost same to ML and Rainbow with $l = 1$ is just the (U)OV.

To generate a signature, first choose $u_1, \dots, u_v \in k$ randomly and find $x_{o_1+\dots+o_{l-1}+1}, \dots, x_m \in k$ such that

$$\begin{aligned}
g_{o_1+\dots+o_{l-1}+1}(x_1, \dots, x_m, u_1, \dots, u_v) &= y_{o_1+\dots+o_{l-1}+1}, \\
&\vdots \\
g_m(x_1, \dots, x_m, u_1, \dots, u_v) &= y_m.
\end{aligned} \tag{19}$$

By the definition of G , the elements $x_{o_1+\dots+o_{l-1}+1}, \dots, x_m$ are given as a solution of a system of o_l linear equations of o_l variables. Other parameters $x_1, \dots, x_{o_1+\dots+o_{l-1}+1}$ can be found recursively.

The coefficient matrices of $g_1(x), \dots, g_m(x)$ are expressed by

$$\begin{aligned}
G_1, \dots, G_{o_1} &= \begin{pmatrix} 0_{o_1} & * \\ * & *_{n-o_1} \end{pmatrix}, \\
G_{o_1+1}, \dots, G_{o_1+o_2} &= \begin{pmatrix} 0_{o_1} & 0 & 0 \\ 0 & 0_{o_2} & * \\ 0 & * & *_{n-o_1-o_2} \end{pmatrix}, \\
&\vdots \\
G_{o_1+\dots+o_{l-1}+1}, \dots, G_m &= \begin{pmatrix} 0_{o_1+\dots+o_{l-1}} & 0 & 0 \\ 0 & 0_{o_l} & * \\ 0 & * & *_{o_l} \end{pmatrix}.
\end{aligned} \tag{20}$$

Then we see that a pair of $S = \begin{pmatrix} *_{o_1} & * \\ & \ddots \\ 0 & & *_{o_l} \end{pmatrix}$ and $T = \begin{pmatrix} *_{o_1} & * \\ & \ddots \\ 0 & & *_{o_l} \end{pmatrix}$ is a *weak key* of Rainbow. Due to (20), we see that the security against the high-rank attack is $O(q^{o_1} \cdot (\text{polyn.}))$, and the security against the min-rank attack is $O(q^{o_l+v} \cdot (\text{polyn.}))$.

Furthermore, since arbitrary linear sums of G_1, \dots, G_m are in the form $\begin{pmatrix} 0_{o_1} & * \\ * & *_{n-o_1} \end{pmatrix}$, (arranged) Kipnis–Shamir’s attack is available also on Rainbow and its complexity is $O(q^{n-2o_1} \cdot (\text{polyn.}))$.

The parameters of Rainbow are usually chosen by $l = 2$ and $o_1 \sim o_2 \sim v$. In this case, $n \sim 1.5m$ and the security against the rank attacks and Kipnis–Shamir’s attack is about $O(q^{o_1} \cdot (\text{polyn.}))$. Then Rainbow is considered to be secure enough under a suitable parameter selection and the key size is much less than UOV.

Note that there have been arrangements of Rainbow to reduce the key size. In TTS [108] and NC-Rainbow [109, 110, 112], the number of parameters in G is less than the original Rainbow and the signature generation is faster. In Cyclic Rainbow [85, 86], the number of parameters in F is less than the original Rainbow and the signature verification is faster. However, we should study the security of such arrangements carefully. For example, it is known that the security of Quaternion Rainbow over even characteristic field is almost 1/4 of the original Rainbow of similar size [54].

4.2 Extension Field Type

The central map of MI (Sect. 2.1, [69]) is constructed by a univariate monomial over an extension field. While MI was already broken, the idea *generating G over an extension field* is used for several MPKCs. The central map $G : k^n \rightarrow k^m$ of such an MPKC is generally described as follows.

Let $r \geq 1$ be a common divisor of n and m , $N := n/r$, $M := m/r$, K an r -extension of k and $\{\theta_1, \dots, \theta_r\} \subset K$ is a basis of K over k . Denote by $\phi_N : k^n \rightarrow K^N$ is a one-to-one map, e.g. $\phi_N(x_1, \dots, x_n) = (x_1\theta_1 + \dots + x_r\theta_r, \dots, x_{n-r+1}\theta_1 + \dots + x_n\theta_r)$ for $x_1, \dots, x_n \in k$, and define a polynomial map $\mathcal{G} : K^N \rightarrow K^M$ to be inverted feasibly. The central map G is constructed by $G := \phi_M^{-1} \circ \mathcal{G} \circ \phi_N$.

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

It is known that the polynomials $g_1(x), \dots, g_m(x)$ in $G(x)$ are quadratic forms of $x = (x_1, \dots, x_n)^t \in k^n$ over k if and only if the polynomials $\mathcal{G}_1(X), \dots, \mathcal{G}_M(X)$ in $\mathcal{G}(X)$ are quadratic forms of $\bar{X} := (X_1, \dots, X_N, X_1^q, \dots, X_N^{q^{r-1}})^t$ over K . It is because the one-to-one map ϕ_N is given by the matrix $\Theta_N := (\theta_j^{q^{i-1}} \cdot I_N)_{1 \leq i, j \leq r}$ where I_N is the identity matrix of size N . In fact, if $X = (X_1, \dots, X_N)^t := (x_1\theta_1 + \dots + x_r\theta_r, \dots, x_{n-r+1}\theta_1 + \dots + x_n\theta_r)^t$, it holds

$$\Theta_N x = \bar{X}.$$

Then F and G have the relation

$$F(x) = (T \circ \Theta_M^{-1}) \cdot \left(\mathcal{G}_1(\phi_N(S(x))), \dots, \mathcal{G}_N(\phi_N(S(x))), \right. \\ \left. \mathcal{G}_1(\phi_N(S(x)))^q, \dots, \mathcal{G}_N(\phi_N(S(x)))^{q^{r-1}} \right)^t,$$

and $\mathcal{G}_i(\phi_N(S(x)))^{q^j}$ is written by

$$\mathcal{G}_i(\phi_N(S(x)))^{q^j} = \bar{X}^t (\Theta_N S \Theta_N^{-1})^t G_i^{(q^j)} (\Theta_N S \Theta_N^{-1}) \bar{X} + (\text{linear form of } \bar{X})$$

for some $n \times n$ matrix $G_i^{(q^j)}$ with K -entries. The matrix $G_i^{(q^j)}$ is important for the security of the extension field type MPKCs.

In this subsection, we describe several examples of such MPKCs.

4.2.1 Hidden Field Equation (HFE)

Hidden Field Equation (HFE) proposed by Patarin [79] is constructed with $n = m = r$ (namely $N = M = 1$) and

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

where $1 \leq d \ll n$ is an integer and $\alpha_{ij}, \beta_i, \gamma \in K$. The decryption of HFE is obtained by solving a univariate polynomial equation $\mathcal{G}(X) - Y = 0$ of degree $D \leq 2q^d$. Its complexity is $O(D^3 + nD^2 \log q)$ by the Berlekamp algorithm [8, 9].

For the security of HFE, it has been reported that F of HFE with small d is inverted efficiently by the Gröbner basis attack [45]. It is known that the degree of regularity of the corresponding polynomial system is bounded by $\frac{1}{2}(q-1)[\log_q(2q^d-1)+1]+2$ [34, 50]. Furthermore, since the coefficient matrix of \mathcal{G} as a quadratic form of \bar{X} is in the form $\binom{*_{d+1}}{d+2}$, the min-rank attack is also available on HFE and its complexity is $\binom{n+d+2}{d+2}^w \ll n^{(d+2)w}$ [11, 64].

From these facts, we see that both the decryption speed and the security of HFE are exponential of d , namely HFE has a serious trade-off between efficiency and security. Thus HFE itself has been considered to be impractical. In Sect. 4.2.2, we describe arrangements of MI and HFE to enhance the security.

4.2.2 Variants of MI and HFE

The *minus* ($-$) variant is to hide several polynomials in G , namely, for $G : k^n \rightarrow k^m$ with $G(x) = (g_1(x), \dots, g_m(x))^t$, the minus $G_- : k^n \rightarrow k^{m-l}$ ($1 \leq l < m$) is defined by $G_-(x) := (g_1(x), \dots, g_{m-l}(x))$. This is mainly used for signature schemes. To generate the signature, choose $u_1, \dots, u_l \in k$ randomly and find $x \in k^n$ such that $G(x) = (y_1, \dots, y_{m-l}, u_1, \dots, u_l)^t$. Sflash [1], selected by NESSIE project

[90], is a minus variant of MI. Unfortunately, the differential attack can recover the hidden polynomials of Sflash [41, 46].

The *plus* (+) variant is to add several polynomials, namely the central map of plus is $G_+ = (g_1(x), \dots, g_m(x), h_1(x), \dots, h_l(x))$ where $l \geq 1$ is an integer and h_i 's are quadratic forms chosen randomly. To decrypt $\tilde{y} = (y_1, \dots, y_{m+l})^t \in k^{m+l}$, one finds $x \in k^n$ such that $G(x) = y = (y_1, \dots, y_m)^t$ and verifies whether $(h_1(x), \dots, h_l(x)) = (y_{m+1}, \dots, y_{m+l})$. When $m \geq n$, the decryption of the plus variant is (probably) not too slower than the original scheme since the number of solutions of $G(x) = y$ is not many. On the other hand, when $n > m$, it is much slower since the equation $G(x) = y$ will have many solutions. See [82] for the security of $MI\pm$ (the plus variant of $MI-$).

The *vinegar* (v) variant is to add several variables. When the quadratic forms in $G(x) := (g_1(x), \dots, g_m(x))^t$ are given by

$$g_l(x) := \sum_{1 \leq i \leq j \leq n} a_{ij}^{(l)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(l)} x_i + c^{(l)},$$

the quadratic forms in a vinegar variant $G_v(x) := (\hat{g}_1(\tilde{x}), \dots, \hat{g}_m(\tilde{x}))$ are defined by

$$\hat{g}_l(\tilde{x}) := \sum_{1 \leq i \leq j \leq n} a_{ij}^{(l)} x_i x_j + \sum_{1 \leq i \leq n} v_i^{(l)}(x_{n+1}, \dots, x_{n+l}) x_i + w^{(l)}(x_{n+1}, \dots, x_{n+r}),$$

where $r \geq 1$ is an integer, x_{n+1}, \dots, x_{n+r} are additional variables, $\tilde{x} := (x_1, \dots, x_{n+r})^t$, $v_i^{(l)}$ is a linear form and $w^{(l)}$ is a quadratic form such that for any $(u_1, \dots, u_r) \in k^r$, $\{\hat{g}_l(x_1, \dots, x_n, u_1, \dots, u_r)\}_{1 \leq l \leq m}$ is equivalent to the original G . HFEv- is the vinegar variant of HFE-, and has been considered to be secure enough under suitable parameter selections (e.g., Quartz, Gui [31, 65, 80, 83, 87, 102]). Recently, Zhang and Tan proposed a new variant similar to the vinegar [114, 115]. However, the vinegar terms can be recovered easily by a chosen ciphertext attack [57].

The *projection* (p) is to reduce several variables from the quadratic forms. When the original G is given by $\{g_l(x_1, \dots, x_n)\}_{1 \leq l \leq m}$, the projection G_p is $\{g_l(x_1, \dots, x_{n-r}, u_1, \dots, u_r)\}_{1 \leq l \leq m}$ with constants $u_1, \dots, u_r \in k$. It is known that the differential attack is not available on the projection of $MI-$ (called *PFLASH*) [96], despite the signature generation is slower than Sflash.

The *internal perturbation* (IP) [33] and the *piece in hand* (PH) [106] are randomizations of G . It is known that these variants improve the security against the Gröbner basis attack [36, 106]. However, their security should be studied carefully. In fact, the differential attack removes the perturbation on PMI (IP of MI) [46] and the linearization attack recovers additional polynomials in the 2-layer version of PH [74].

4.2.3 ZHFE

ZHFE [89] is an encryption scheme with $(N, M) = (1, 2)$. The simplest version is as follows. Let $D \geq 1$ be an integer, $\mathcal{G}_1(X), \mathcal{G}_2(X)$ quadratic forms of \tilde{X} such that

$$\Psi(X) := X \cdot \mathcal{G}_1(X) + X^q \cdot \mathcal{G}_2(X)$$

is of degree at most D and $\mathcal{G} : K \rightarrow K^2$ the map with $\mathcal{G}(X) := (\mathcal{G}_1(X), \mathcal{G}_2(X))$. To find $X \in K$ with $\mathcal{G}_1(X) = Y_1$ and $\mathcal{G}_2(X) = Y_2$ in the decryption process, one solves the univariate equation

$$\begin{aligned} \Psi(X, (Y_1, Y_2)) &:= \Psi(X) - XY_1 - X^q Y_2 \\ &= X \cdot (\mathcal{G}_1(X) - Y_1) + X^q \cdot (\mathcal{G}_2(X) - Y_2) = 0 \end{aligned} \quad (21)$$

of degree at most D . Similar to HFE, the complexity of the decryption is $O(D^3 + nD^2 \log q)$ by the Berlekamp algorithm.

The security of ZHFE against the attacks available on HFE has been studied in [84, 89, 116]. These works claimed that ZHFE is more secure than HFE against the direct attacks, the min-rank attacks and the differential attack. However, a *chosen ciphertext attack* can reduce the security of ZHFE to the security of HFE against the min-rank attack [60]. This means that, similar to HFE, ZHFE has a serious trade-off between efficiency and security.

4.2.4 Multivariate ($N > 1$) Version

The maps \mathcal{G} for MI, HFE, and ZHFE are given by univariate polynomials, namely $N = 1$. Other than these scheme, there are MPKCs with $N > 1$. For example, MFE [107] is an extension field type MPKC with $(N, M) = (12, 15)$ and \mathcal{G} has a special structure to be inverted feasibly. In multi-HFE [23], $N (= M)$ is small and the polynomials in \mathcal{G} are quadratic forms chosen randomly. The map \mathcal{G} for l -IC [38] is a set of multivariate higher degree monomials similar to MI.

Unfortunately, these MPKCs are known to be impractical. In fact, MFE was broken by the linearization attack [37] and the l -IC was broken by the differential attack [47]. For multi-HFE, since $\mathcal{G}_i(X) = \tilde{X}^t \begin{pmatrix} *N \\ *N \end{pmatrix} \tilde{X} + (\text{linear form})$, the min-rank attack [11] is available and its complexity is $O\left(\binom{n+N+1}{N+1}^\omega\right) = O(r^{(N+1)w})$. Furthermore, the extension field type MPKCs with quadratic \mathcal{G} and odd q are broken by the conjugation attack [59] since the public quadratic forms are in the form $f_i(x) =$

$$x^t (\Theta_N S)^t \begin{pmatrix} *N & & \\ & \ddots & \\ & & *N \end{pmatrix} (\Theta_N S)x + (\text{linear form}).$$

4.2.5 Noncommutative Version

In Sects. 3.2.1–4, we describe MPKCs whose central maps are derived from polynomial maps over extension *fields*. Such constructions can be generalized to *rings*, not necessarily fields. In fact, there have been several MPKCs constructed on non-commutative rings [54, 103, 109, 110, 112]. However, we cannot recommend such constructions strongly since the following theorem is well-known (see e.g. [6]).

The Artin–Wedderburn theorem. A ring \mathcal{R} is a semi-simple if and only if there exist integers $n_1, \dots, n_l \geq 1$ and division rings K_1, \dots, K_l such that

$$\mathcal{R} \simeq M_{n_1}(K_1) \oplus \dots \oplus M_{n_l}(K_l),$$

where $M_n(K)$ is the ring of $n \times n$ matrices of K -entries.

Furthermore, due to Wedderburn’s theorem, we see that, if a semi-simple ring \mathcal{R} is finite, then the rings K_1, \dots, K_l are commutative. For example, let

$$\mathcal{R} := \{a_1\sigma_1 + \dots + a_5\sigma_5 \mid a_1, \dots, a_5 \in k\}$$

be a ring over k with $q \equiv 1 \pmod{3}$ and $\sigma_1 := \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$, $\sigma_2 := \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, $\sigma_3 := \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, $\sigma_4 := \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$, $\sigma_5 := \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. Define $\delta_1, \dots, \delta_5 \in \mathcal{R}$ by

$$\begin{pmatrix} \delta_1 \\ \delta_2 \\ \delta_3 \\ \delta_4 \\ \delta_5 \end{pmatrix} := 3^{-1} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \\ -1 & -1 & -1 & \alpha - 1 & \alpha^2 - 1 \\ -1 & -1 & -1 & \alpha^2 - 1 & \alpha - 1 \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \sigma_4 \\ \sigma_5 \end{pmatrix},$$

where $\alpha \in \mathcal{R}$ satisfies $\alpha \neq 1$, $\alpha^3 = 1$. It is easy to see that the elements $\delta_1, \dots, \delta_5$ have the following multiplicative relations:

$$\begin{array}{lllll} \delta_1\delta_1 = \delta_1, & \delta_1\delta_2 = 0, & \delta_1\delta_3 = 0, & \delta_1\delta_4 = 0, & \delta_1\delta_5 = 0, \\ \delta_2\delta_1 = 0, & \delta_2\delta_2 = \delta_3, & \delta_2\delta_3 = 0, & \delta_2\delta_4 = \delta_4, & \delta_2\delta_5 = 0, \\ \delta_3\delta_1 = 0, & \delta_3\delta_2 = 0, & \delta_3\delta_3 = \delta_2, & \delta_3\delta_4 = 0, & \delta_3\delta_5 = \delta_5, \\ \delta_4\delta_1 = 0, & \delta_4\delta_2 = 0, & \delta_4\delta_3 = \delta_5, & \delta_4\delta_4 = 0, & \delta_4\delta_5 = \delta_2, \\ \delta_5\delta_1 = 0, & \delta_5\delta_2 = \delta_4, & \delta_5\delta_3 = 0, & \delta_5\delta_4 = \delta_3, & \delta_5\delta_5 = 0. \end{array}$$

This means that $\mathcal{R} \simeq k \oplus M_2(k)$ and, if one generates G from quadratic forms over \mathcal{R} , the corresponding MPKC has a risk to be broken by rank attacks or conjugation attacks.

4.3 Other MPKCs

In this subsection, we describe two MPKCs as examples not classified in neither the stepwise type nor the extension field type.

4.3.1 ABC Encryption Scheme

In the *ABC (or Simple Matrix) encryption scheme* proposed by Tao et al. [99], the central map G is generated by products among three matrices A, B, C . It is generalized as follows. Let $n, m \geq 1$ be integers with $m := 2n$, \mathcal{R} a ring over k with $[\mathcal{R} : k] = n$ and $\{\xi_1, \dots, \xi_n\} \subset \mathcal{R}$ is a basis of \mathcal{R} over k . Denote by $\phi : k^n \rightarrow \mathcal{R}, \phi_2 : k^m \rightarrow \mathcal{R}^2$ one-to-one maps, e.g. $\phi(x_1, \dots, x_n) = x_1\xi_1 + \dots + x_n\xi_n$ and $\phi_2(y_1, \dots, y_m) = (y_1\xi_1 + \dots + y_n\xi_n, y_{n+1}\xi_1 + \dots + y_m\xi_n)$ for $x_1, \dots, x_n, y_1, \dots, y_m \in k$, and $\mathcal{B}, \mathcal{C} : k^n \rightarrow k^n$ linear maps. For $x \in k^n$, put $A = A(x) := \phi(x)$, $B = B(x) := \phi(\mathcal{B}(x))$, $C = C(x) := \phi(\mathcal{C}(x))$, $E_1 = E_1(x) := A \cdot B$, $E_2 = E_2(x) := A \cdot C$ and $E(x) := (E_1(x), E_2(x))$. The central map $G : k^n \rightarrow k^m$ is defined by

$$G := \phi_2^{-1} \circ E \circ \phi.$$

For $Y_1, Y_2 \in \mathcal{R}$, one finds $x \in k^n$ with $E_1(x) = Y_1$ and $E_2(x) = Y_2$ by solving a system of linear equations derived from $C(x) = B(x)Y_1^{-1}Y_2$ or $B(x) = C(x)Y_2^{-1}Y_1$.

It is easy to see that the original ABC encryption scheme [99] is just same to the case that $\mathcal{R} = M_r(k)$ with $r^2 = n$, and the *extension field cancelation (EFC)* [97] is essentially expressed as an ABC encryption scheme in the case that \mathcal{R} is an n extension field of k .

The decryption of this scheme is simple and quite efficient. However, the decryption fails when A is not invertible. Especially, the probability of decryption failure for the original ABC encryption scheme [99] is about q^{-1} , which is not negligible. To reduce the probability of decryption failure, several arrangements have been proposed, e.g., taking q large, using rectangular matrices instead of A, B, C et al. [100], using a tensor type matrix as S [88]. However, the security for such arrangements should be studied carefully. It was shown that the tensor type S is a weak key [56].

For the security, it is known that the min-rank attack and the linearization attack are available on this encryption scheme. For the original ABC [99], the complexities of these attacks are $O(q^{2r} \cdot (\text{polyn.}))$ and $O((m \binom{n+r}{r})^w)$ respectively. Furthermore, Moody et al. [73] proposed another attack on this scheme with the complexity $O(q^{r+4} \cdot (\text{polyn.}))$. Then this encryption scheme (presently) has a sub-exponential time security of n . For EFC, it is known that the linearization attack can recover plaintexts easily. To prevent it, the authors of [97] recommended to use the minus and the projection of EFC. In [39], the cubic version of ABC was proposed; the polynomials in A are quadratic and then those in F, G are cubic. Though the security against the direct attack is improved, the security against the linearization attack is almost same to the original ABC.

4.3.2 YTS

YTS is a signature scheme proposed by Yasuda–Takagi–Sakurai [111] over a finite field of odd characteristic and by Zhang–Tan [115] over a field of even characteristic. We now describe the odd characteristic version.

Let $r \geq 1$ be an integer, $n := r^2$ and $m := r(r+1)/2$. Denote by $\phi : k^n \rightarrow M_r(k)$, $\psi : k^m \rightarrow \text{SM}_r(k)$ one-to-one maps, where $\text{SM}_r(k)$ is the set of $r \times r$ symmetric matrices over k . Define two maps $\mathcal{G}_1, \mathcal{G}_2 : M_r(k) \rightarrow \text{SM}_r(k)$ by $\mathcal{G}_1(X) := X^t X$ and $\mathcal{G}_2(X) := X^t B^t \begin{pmatrix} I_{r-1} & \\ & \delta \end{pmatrix} B X$, where $\delta \in k$ is not a square of any elements in k and $B \in M_r(k)$ is an invertible matrix. The central maps $G_1, G_2 : k^n \rightarrow k^m$ are given by

$$G_i := \psi^{-1} \circ \mathcal{G}_i \circ \phi, \quad (i = 1, 2).$$

The public key is two maps $F_1, F_2 : k^n \rightarrow k^m$ with $F_i := T \circ G_i \circ S$ and the signature $x \in k^n$ for a message $y \in k^m$ is verified if either $F_1(x) = y_1$ or $F_2(x) = y_2$ holds. It is known that, for any $Y \in \text{SM}_r(k)$, there exists $X \in M_r(k)$ such that either $X^t X = Y$, $X^t \begin{pmatrix} I_{r-1} & \\ & \delta \end{pmatrix} X = Y$ holds and such X can be found feasibly [68]. This fact is used for signature generation. While the signature generation is fast, the security is not enough. Since the quadratic forms in G_i are quite sparse, an equivalent secret key can be recovered in sub-exponential time by the min-rank attack [111] and in polynomial time by the conjugation attack [55].

5 Open Problems

We conclude this paper by giving several open problems on MPKC.

1. Are there MPKCs with security proofs?

There have been several works on provable security of MPKCs [18, 92]. However, they seem still far from the security proof of proposed MPKCs. We expect that, if such an MPKC would be proposed, it could help future developments of MPKCs.

2. Which schemes are polynomial systems suitable for?

It has been considered that there are good multivariate *signature schemes*, which seem secure and efficient enough under suitable parameter selections. For example, Rainbow is one of them despite the key size is relatively large. On the other hand, there seem to be few good *encryption schemes*, except the schemes proposed recently and not yet analyzed enough. That is (maybe) because constructing a good one-to-one map by nonlinear polynomial systems is not easy. Other than signature schemes and encryption schemes, a multi-receiver signcryption scheme [67], an identity-based signature scheme [94], a public key identification schemes [91] and a stream cipher [7] were proposed. We consider that we should analyze more to use them in practice.

3. Why quadratic? How about higher (≥ 3) degree polynomials?

For most MPKCs, F and G are sets of quadratic forms. One of the reasons that quadratic forms are mainly used in MPKCs is that higher degree polynomials have much more coefficients, which lacks efficiency. On the other hand, there have been several MPKCs with cubic F and G (e.g., [39, 65, 75]). It has been considered that one of the advantage of “cubic” construction is to avoid attacks based on the properties of coefficient matrices. However, the attacker can get a quadratic map by taking a difference $\Delta_C F(x) := F(x + C) - F(x) = T \circ \Delta_C G \circ S$, and he/she may be able to find vulnerabilities in the coefficient matrices in $\Delta_C F(x)$. For example, in the cubic version of UOV described in Sect. 9 of [65], we can easily check that $\Delta_C F$ is equivalent to a public key of the original UOV, which means that the security of cubic version UOV is almost same to the security against the key recovery attack on the original UOV. Furthermore, another cubic version of UOV [75] was broken easily [58]. We thus consider that, to construct a cubic version of MPKC, one should study the security and efficiency carefully.

4. Are MPKCs really “Post-Quantum”?

MPKCs have been expected to be secure against quantum attacks. However, the proposed attacks on MPKCs are only by the classical computers and there are few works on the security against quantum attacks. The complexities of the proposed attacks might be improved if the attacker could implement such attacks on the quantum computers. For example, by using Grover’s algorithm [51], the attacker will reduce the complexities of the attacks including the exhaustive search, e.g., the high-rank attacks on small fields. Furthermore, it is known that, on the isogeny-based cryptosystem, the security against the quantum attacks is less than the security against the attacks by the classical computers [12, 26]. We consider that (the possibility of) quantum attacks on MPKCs must be studied in near future.

5. How about relations with other NP-complete/hard problems.

It is known that the problem of finding a solution of a system of multivariate nonlinear polynomial equations over a finite field of order 2 is NP-hard, and the correspondence between this problem and the SAT problem is given by $xy \leftrightarrow x \wedge y$, $xy + x + y \leftrightarrow x \vee y$ and $x + 1 \leftrightarrow \neg x$ [48, 49]. By using this correspondence, Bard et al. [3, 4] proposed an algorithm to solve a system of multivariate quadratic equations by the SAT-solver. We consider that studying the security of MPKCs in the view of other NP-complete/hard problems is quite interesting.

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

References

1. M.L. Akkar, N. Courtois, L. Goubin, R. Duteuil, A fast and secure implementation of Sflash, in *PKC’03*. LNCS, vol. 2567 (2003), pp. 267–278

2. R.M. Avanzi, S. Hoerder, D. Page, M. Tunstall, Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. *J. Crypt. Eng.* **1**, 271–281 (2011)
3. G.V. Bard, *Algebraic Cryptanalysis* (Springer, Dordrecht, 2009)
4. G.V. Bard, N.T. Courtois, C. Jefferson, Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over $GF(2)$ via SAT-Solvers, <https://eprint.iacr.org/2007/024.pdf>
5. M. Bardet, J.C. Faugère, B. Salvy, B.Y. Yang, Asymptotic expansion of the degree of regularity for semi-regular systems of equations, in *MEGA'05* (2005)
6. J.A. Beachy, *Introductory Lectures on Rings and Modules* (Cambridge University Press, Cambridge, 1999)
7. C. Berbain, H. Gilbert, J. Patarin, QUAD: a practical stream cipher with provable security, in *Eurocrypt'06*. LNCS, vol. 4004 (2006), pp. 109–128
8. E.R. Berlekamp, Factoring polynomials over finite fields. *Bell Syst. Tech. J.* **46**, 1853–1859 (1967)
9. E.R. Berlekamp, Factoring polynomials over large finite fields. *Math. Comput.* **24**, 713–735 (1970)
10. L. Bettale, J.C. Faugère, L. Perret, Solving polynomial systems over finite fields: Improved analysis of the hybrid approach. *ISSAC 2012*, 67–74 (2012)
11. L. Bettale, J.C. Faugère, L. Perret, Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Des. Codes Crypt.* **69**, 1–52 (2013)
12. J.F. Biasse, D. Jao, A. Sankar, A quantum algorithm for computing isogenies between supersingular elliptic curves, in *Indocrypt'14*. LNCS, vol. 8885 (2014), pp. 428–442
13. I. Biehl, B. Meyer, V. Müller, Differential fault attacks on elliptic curve cryptosystems, in *Crypto'00*. LNCS, vol. 2000 (1880), pp. 131–146
14. D. Bini, M. Capovani, F. Romani, G. Lotti, $O(n^{2.7799})$ complexity for $n \times n$ approximate matrix multiplication. *Inf. Process. Lett.* **8**, 234–235 (1979)
15. D. Boneh, R.A. DeMillo, R.J. Lipton, On the importance of checking cryptographic protocols for faults, in *Eurocrypt'97*. LNCS, vol. 1233 (1997), pp. 37–51
16. C. Bouillaguet, H.C. Chen, C.M. Cheng, T. Chou, R. Niederhagen, A. Shamir, B.Y. Yang, Fast exhaustive search for polynomial systems in F_2 , in *CHES'10*. LNCS, vol. 6225 (2010), pp. 203–218
17. B. Buchberger, A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bull.* **10**, 19–29 (1976)
18. S. Bulygin, A. Petzoldt, J. Buchmann, Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks, in *Indocrypt'10*. LNCS, vol. 6498 (2010), pp. 17–32
19. R. Cartor, R. Gipson, D. Smith-Tone, J. Vates, On the differential security of the HFEv-signature primitive, in *PQCrypto'16*. LNCS, vol. 9606 (2016), pp. 162–181
20. A. Cayley, Sur les déterminants gauches (On skew determinants). *Crelle's J.* **38**, 93–96 (1847)
21. P.L. Cayrel, P. Dusart, Fault injection's sensitivity of the McEliece PKC, in *Proceedings of 5th International Conference on Future Information Technology* (2010), pp. 1–6
22. A.I.T. Chen, M.S. Chen, T.R. Chen, C.M. Chen, J. Ding, E.L.H. Kuo, F.Y.S. Lee, B.Y. Yang, “SSE implementation of multivariate PKCs on modern x86 CPUs, in *CHES'09*. LNCS, vol. 5747 (2009), pp. 33–48
23. 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>
24. L. Chen, S. Jordan, Y.K. Liu, D. Moody, R. Reralta, R. Perlner, D. Smith-Tone, Report on post-quantum cryptography, in *National Institute of Standards and Technology Internal Report*, vol. 8105 (2016), http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf
25. C.M. Cheng, Y. Hashimoto, H. Miura, T. Takagi, A polynomial-time algorithm for solving a class of underdetermined multivariate quadratic equations over fields of odd characteristics, in *PQCrypto'14*. LNCS, vol. 8772 (2014), pp. 40–58
26. A. Childs, D. Jao, V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.* **8**, 1–29 (2014)

27. M. Ciet, M. Joye, Elliptic curve cryptosystems in the presence of permanent and transient faults. *Des. Codes Crypt.* **36**, 33–43 (2005)
28. D. Coppersmith, S. Winograd, Matrix multiplication via arithmetic progressions. *J. Symb. Comput.* **9**, 251–280 (1990)
29. D. Coppersmith, J. Stern, S. Vaudenay, Attacks on the birational permutation signature schemes, in *Crypto'93*. LNCS, vol. 773 (1994), pp. 435–443
30. J.S. Coron, Resistance against differential power analysis for elliptic curve cryptosystems, in *CHES'99*. LNCS, vol. 1717 (1999), pp. 292–302
31. N.T. Courtois, M. Daum, P. Felke, On the security of HFE, HFEv- and Quartz, in *PKC'03*. LNCS, vol. 2567 (2003), pp. 337–350
32. T. Daniels, D. Smith-Tone, Differential properties of the HFE cryptosystem, in *PQCrypto'14*. LNCS, vol. 8772 (2014), pp. 59–75
33. J. Ding, A new variant of the Matsumoto-Imai cryptosystem through perturbation, in *PKC'04*. LNCS, vol. 2947 (2004), pp. 305–318
34. J. Ding, T.J. Hodges, Inverting HFE systems is quasi-polynomial for all fields, in *Crypto'11*. LNCS, vol. 6841 (2011), pp. 724–742
35. J. Ding, D. Schmidt, Rainbow, a new multivariate polynomial signature scheme, in *ACNS'05*. LNCS, vol. 3531 (2005), pp. 164–175
36. J. Ding, J.E. Gower, D. Schmidt, C. Wolf, Z. Yin, Complexity estimates for the F_4 attack on the perturbed Matsumoto-Imai cryptosystem, in *10th IMA International Conference on Cryptography and coding*. LNCS, vol. 3796 (2005), pp. 262–277
37. J. Ding, L. Hu, X. Nie, J. Li, J. Wagner, High order linearization equation (HOLE) attack on multivariate public key cryptosystems, in *PKC'07*. LNCS, vol. 4450 (2007), pp. 233–248
38. J. Ding, C. Wolf, B.Y. Yang, l -invertible cycles for multivariate quadratic (MQ) public key cryptography, in *PKC'07*. LNCS, vol. 4450 (2007), pp. 266–281
39. J. Ding, A. Petzoldt, L.C. Wang, The cubic simple matrix encryption scheme, in *PQC'14*. LNCS, vol. 8772 (2014), pp. 76–87
40. D.Z. Doković, On the product of two alternating matrices. *Amer. Math. Monthly* **98**, 935–936 (1991)
41. V. Dubois, P.A. Fouque, A. Shamir, J. Stern, Practical cryptanalysis of SFLASH, in *Crypto'07*. LNCS, vol. 4622 (2007), pp. 1–12
42. V. Dubois, L. Granboulan, J. Stern, Cryptanalysis of HFE with internal perturbation, in *PKC'07*. LNCS, vol. 4450 (2007), pp. 249–265
43. D.H. Duong, A. Petzoldt, T. Takagi, Reducing the key size of the SRP encryption scheme, in *ACISP'16*. LNCS, vol. 9723 (2016), pp. 427–434
44. J.C. Faugère, A new efficient algorithm for computing Grobner bases (F_4). *J. Pure Appl. Algebra* **139**, 61–88 (1999)
45. J.C. Faugère, A. Joux, Algebraic cryptanalysis of Hidden Field Equations (HFE) using Gröbner bases, in *Crypto'03*. LNCS, vol. 2729 (2003), pp. 44–60
46. P.A. Fouque, L. Granboulan, J. Stern, Differential cryptanalysis for multivariate schemes, in *Eurocrypt'05*. LNCS, vol. 3494 (2005), pp. 341–353
47. P.A. Fouque, G. Macario-Rat, L. Perret, J. Stern, Total break of the l -IC signature scheme, in *PKC'08*. LNCS, vol. 4939 (2008), pp. 1–17
48. A.S. Fraenkel, Y. Yesha, Complexity of problems in games, graphs and algebraic equations. *Discret. Appl. Math.* **1**, 15–30 (1979)
49. M.R. Garey, D.S. Johnson, *Computers and Intractability, A Guide to the Theory of NP-completeness* (W.H. Freeman, New York, 1979)
50. L. Granboulan, A. Joux, J. Stern, Inverting HFE is quasipolynomial, in *Crypto'06*, LNCS, vol. 4117 (2006), pp. 345–356
51. L.K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings 28th Annual ACM Symposium on the Theory of Computing* (1996) pp. 212–219
52. S. Hasegawa, T. Kaneko, An attacking method for a public-key cryptosystem based on the difficulty of solving a system of non-linear equations (in Japanese), in *Proceedings of 10th SITA*, vol. JA5-3 (1987)

53. Y. Hashimoto, Algorithms to solve massively under-defined systems of multivariate quadratic equations. *IEICE Trans. Fundam.* **E94-A**, 1257–1262 (2011)
54. Y. Hashimoto, Cryptanalysis of the quaternion rainbow, in *IWSEC'13*. LNCS, vol. 8231 (2013), pp. 244–257
55. Y. Hashimoto, Cryptanalysis of the multivariate signature scheme proposed in PQCrypto 2013, in *PQCrypto'14*, LNCS, vol. 8772 (2014), pp. 108–125. *IEICE Trans. Fundam.* **99-A**, 58–65 (2016)
56. Y. Hashimoto, A note on tensor simple matrix encryption scheme, <http://eprint.iacr.org/2016/065>
57. Y. Hashimoto, On the security of new vinegar-like variant of multivariate signature scheme, <http://eprint.iacr.org/2016/787>
58. Y. Hashimoto, On the security of cubic UOV, <http://eprint.iacr.org/2016/788>
59. Y. Hashimoto, Key recovery attacks on multivariate public key cryptosystems derived from quadratic forms over an extension field. *IEICE Tans. Fundam.* **100-A**, 18–25 (2017)
60. Y. Hashimoto, Chosen ciphertext attack on ZHFE. *JSIAM Lett.* (2017). To appear
61. Y. Hashimoto, T. Takagi, K. Sakurai, General fault attacks on multivariate public key cryptosystems, in *PQC'11*. LNCS, vol. 7071 (2011), pp. 1–18
62. M. Joye, A.K. Lenstra, J.J. Quisquater, Chinese remaindering based cryptosystems in the presence of faults. *J. Cryptol.* **12**, 241–245 (1999)
63. A. Kipnis, A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, in *Crypto'98*. LNCS, vol. 1462 (1998), pp. 257–267
64. A. Kipnis, A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, in *Crypto'99*. LNCS, vol. 1666 (1999), pp. 19–30
65. A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, in *Eurocrypt'99*. LNCS, vol. 1592 (1999), pp. 206–222, extended in [www.citeseer/231623.html](http://www.citeseer.231623.html), 2003-06-11
66. F. Le Gall, Powers of tensors and fast matrix multiplication, in *ISSAC'14, Proceedings of the 39th ISSAC* (2014), pp. 296–303
67. H. Li, X. Chen, L. Pang, W. Shi, Quantum attack-resistant certificateless multi-receiver sign-encryption scheme. *PLoS ONE* **8**(6), e49141 (2013)
68. R. Lidl, H. Niederreiter, *Finite Fields* (Addison-Wesley, London, 1983)
69. T. Matsumoto, H. Imai, Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, in *Eurocrypt'88*. LNCS, vol. 330 (1988), pp. 419–453
70. H. Miura, Y. Hashimoto, T. Takagi, Extended algorithm for solving underdefined multivariate quadratic equations, in *PQCrypto'13*, LNCS, vol. 7932 (2013), pp. 118–135. *IEICE Trans. Fundam.* **E97-A**, 1418–1425 (2014)
71. H.G. Molter, R. Overbeck, A. Shoufan, F. Strenzke, E. Tews, Side channels in the McEliece PKC, in *PQC'08*. LNCS, vol. 5299 (2008), pp. 216–229
72. D. Moody, Post-quantum cryptography: NIST's plan for the future, in *NIST Announcement in PQCrypto'16* (2016), https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf
73. D. Moody, R. Perlner, D. Smith-Tone, An asymptotically optimal structural attack on the ABC multivariate encryption scheme, in *PQC'14*. LNCS, vol. 8772 (2014), pp. 180–196
74. X. Nie, A. Petzoldt, J. Buchmann, Cryptanalysis of 2-layer nonlinear piece in hand method, in *CD-ARES'13*. LNCS, vol. 8128 (2013), pp. 91–104
75. X. Nie, B. Liu, H. Xiong, G. Lu, Cubic unbalance oil and vinegar signature scheme, in *Inscrypt'15*. LNCS, vol. 9589 (2015), pp. 47–56
76. NIST, Submission requirements and evaluation criteria for the Post-Quantum Cryptography standardization process (2016), <http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf>
77. K. Okeya, T. Takagi, C. Vuillaume, On the importance of protecting Δ in SFLASH against side channel attacks. *IEICE Trans.* **88-A**, 123–131 (2005)
78. D. Page, F. Vercauteren, A fault attack on pairing-based cryptography. *IEEE Trans. Comput.* **55**, 1075–1080 (2006)

79. J. Patarin, Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88, in *Crypto '95*. LNCS, vol. 963 (1995), pp. 248–261
80. J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, *Eurocrypt'96*. LNCS, vol. 1070 (1996), pp. 33–48
81. J. Patarin, The oil and vinegar signature scheme, in *The Dagstuhl Workshop on Cryptography* (1997)
82. J. Patarin, L. Goubin, N.T. Courtois, $C * -+$ and HM: variations around two schemes of T. Matsumoto and H. Imai, in *Asiacrypt'98*. LNCS, vol. 1514 (1998), pp. 35–49
83. J. Patarin, N. Courtois, L. Goubin, QUARTZ, 128-bit long digital signatures, in *CT-RSA'01*. LNCS, vol. 2020 (2001), pp. 282–297
84. R. Perlner, D. Smith-Tone, Security analysis and key modification for ZHFE, in *PQCrypto'16*. LNCS, vol. 9606 (2016), pp. 197–212
85. A. Petzoldt, S. Bulygin, J.A. Buchmann, CyclicRainbow - a multivariate signature scheme with a partially cyclic public key, in *IndoCrypt'10*. LNCS, vol. 6498 (2010), pp. 33–48
86. A. Petzoldt, S. Bulygin, J.A. Buchmann, Fast verification for improved versions of the UOV and Rainbow signature schemes, in *PQC'13*. LNCS, vol. 7932 (2013), pp. 188–202
87. A. Petzoldt, M.S. Chen, B.Y. Yang, C. Tao, J. Ding, Design principles for HFEv- based multivariate signature schemes, in *Asiacrypt'15*. LNCS, vol. 9452 (2015), pp. 311–334
88. A. Petzoldt, J. Ding, L.C. Wang, Eliminating decryption failures from the simple matrix encryption scheme (2016), <http://eprint.iacr.org/2016/010>
89. J. Porras, J. Baena, J. Ding, ZHFE, a new multivariate public key encryption scheme, in *PQCrypto'14*. LNCS, vol. 8772 (2014), pp. 229–245
90. B. Preneel, NISSIE Project Announces Final Selection of Crypto Algorithms, https://www.cosic.esat.kuleuven.be/nissie/deliverables/press_release_feb27.pdf
91. K. Sakumoto, T. Shirai, H. Hiwatari, Public-key identification schemes based on multivariate quadratic polynomials, in *Crypto'11*. LNCS, vol. 6841 (2011), pp. 706–723
92. K. Sakumoto, T. Shirai, H. Hiwatari, On provable security of UOV and HFE signature schemes against Chosen-Message Attack, in *PQCrypto'11*. LNCS, vol. 7071 (2011), pp. 68–82
93. A. Shamir, Efficient signature schemes based on birational permutations, in *Crypto '93*. LNCS, vol. 773 (1983), pp. 1–12
94. W. Shen, S. Tang, L. Xu, IBUOV, A provably secure Identity-Based UOV Signature Scheme, in *Proceeding CSE'13* (2013), pp. 388–395
95. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997)
96. D. Smith-Tone, M.-S. Chen, B.-Y. Yang, PFLASH - secure asymmetric signatures on smart cards, in *Lightweight Cryptography Workshop* (2015), <http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session3-smith-tone-paper.pdf>
97. A. Szeponiec, J. Ding, B. Preneel, Extension field cancellation: a new central trapdoor for multivariate quadratic systems, in *PQC'16*. LNCS, vol. 9606 (2016), pp. 182–196
98. V. Strassen, Gaussian elimination is not optimal. *Numer. Math.* **13**, 354–356 (1969)
99. C. Tao, A. Diene, S. Tang, J. Ding, Simple matrix scheme for encryption, in *PQCrypto 2013*. LNCS, vol. 7932 (2013), pp. 231–242
100. C. Tao, H. Xiang, A. Petzoldt, J. Ding, Simple Matrix - a multivariate public key cryptosystem (MPKC) for encryption. *Finite Fields Appl.* **35**, 352–368 (2015)
101. O. Taussky, H. Zassenhaus, On the similarity transformation between a matrix and its transpose. *Pac. J. Math.* **9**, 893–896 (1959)
102. R. Terada, E.R. Andrade, Comparison of two signature schemes based on the MQ problem and Quartz. *IEICE Trans. Fundam.* **99-A**, 2527–2538 (2016)
103. E. Thomae, Quo vadis quaternion? Cryptanalysis of Rainbow over non-commutative rings, in *SCN'12*. LNCS, vol. 7485 (2012), pp. 361–373
104. E. Thomae, C. Wolf, Solving underdetermined systems of multivariate quadratic equations revisited, in *PKC'12*. LNCS, vol. 7293 (2012), pp. 156–171
105. S. Tsujii, K. Kurosawa, T. Itoh, A. Fujioka, T. Matsumoto, A public-key cryptosystem based on the difficulty of solving a system of non-linear equations. *IEICE Trans. Inf. Syst. (Japanese Edition)*, **J69-D**, pp. 1963–1970 (1986)

106. S. Tsujii, K. Tadaki, R. Fujita, Proposal for Piece in Hand Matrix: general concept for enhancing security of multivariate public key cryptosystems. *IEICE Trans.* **90-A**, 992–999 (2007)
107. L.C. Wang, B.Y. Yang, Y.H. Hu, F. Lai, A “medium-field” multivariate public-key encryption scheme, in *CT-RSA’06*. LNCS, vol. 3860 (2006), pp. 132–149
108. B.Y. Yang, J.M. Chen, Building secure tame-like multivariate public-key cryptosystems: the new TTS, in *ACISP’05*. LNCS, vol. 3574 (2005), pp. 518–531
109. T. Yasuda, K. Sakurai, A security analysis of uniformly-layered rainbow defined over non-commutative rings. *Pac. J. Math. Ind.* **6**, 81–89 (2014)
110. T. Yasuda, K. Sakurai, T. Takagi, Reducing the key size of Rainbow using non-commutative rings, in *CT-RSA’12*. LNCS, vol. 7178 (2012), pp. 68–83
111. T. Yasuda, T. Takagi, K. Sakurai, Multivariate signature scheme using quadratic forms. in *PQCrypto’13*. LNCS, vol. 7932 (2013), pp. 243–258
112. T. Yasuda, T. Takagi, K. Sakurai, Security of multivariate signature scheme using non-commutative rings. *IEICE Trans.* **97-A**, 245–252 (2014)
113. T. Yasuda, X. Dahan, Y.-J. Huang, T. Takagi, K. Sakurai, MQ Challenge: hardness evaluation of solving multivariate quadratic problems, in *The NIST Workshop on Cybersecurity in a Post-Quantum World, Washington, D.C.*, April 2–3 (2015), <https://www.mqchallenge.org/>
114. W. Zhang, C.H. Tan, MI-T-HFE, A new multivariate signature scheme, in *IMACC’15*. LNCS, vol. 9496 (2015), pp. 43–56
115. W. Zhang, C.H. Tan, A secure variant of Yasuda, Takagi and Sakurai’s signature scheme, in *Inscrypt’15*. LNCS, vol. 9589 (2015), pp. 75–89
116. W. Zhang, C.H. Tan, On the security and key generation of the ZHFE encryption scheme, in *IWSEC’16*. LNCS, vol. 9836 (2016), pp. 289–304

Mathematical Modelling for Next-Generation

Cryptography

CREST Crypto-Math Project

Takagi, T.; Wakayama, M.; Tanaka, K.; Kunihiro, N.;

Kimoto, K.; Duong, D.H. (Eds.)

2018, VIII, 368 p. 23 illus., 6 illus. in color., Hardcover

ISBN: 978-981-10-5064-0