Recent Developments in Multivariate Public Key Cryptosystems

Yasufumi Hashimoto

Abstract The multivariate signature schemes UOV, Rainbow, and HFEv- have been considered to be secure and efficient enough under suitable parameter selections. In fact, several second round candidates of NIST's standardization project of Post-Quantum Cryptography are based on these schemes. On the other hand, there are few multivariate encryption schemes expected to be practical and despite that, various new schemes have been proposed recently. In the present paper, we summarize multivariate schemes UOV, Rainbow, and (variants of) HFE generating the second round candidates and study the practicalities of several multivariate encryption schemes proposed recently.

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

1 Introduction

In 2016, NIST launched the standardization project of Post-Quantum Cryptography (NIST 2020). A lot of schemes were submitted to the first round of its project and 26 of them were chosen as the second round candidates in 2019 (NIST 2020). LUOV (Beullens et al. 2020), Rainbow (Ding et al. 2020) and GeMSS (Casanova et al. 2020) are multivariate signature schemes in the second round. These schemes are based on UOV (Kipnis et al. 1999; Patarin 1997), Rainbow (Ding et al. 2005), and HFEv- (Patarin et al. 2001), respectively, which were proposed before or around 2000 and have been still considered to be secure and efficient enough under suitable parameter

Y. Hashimoto (✉)

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

© The Author(s) 2021

T. Takagi et al. (eds.), *International Symposium on Mathematics, Quantum Theory, and Cryptography*, Mathematics for Industry 33,
https://doi.org/10.1007/978-981-15-5191-8_16

209

selections. On the other hand, there are few practical multivariate encryption schemes and despite that, various new schemes have been proposed in this decade.

The aim of this paper is to describe recent developments of multivariate public key cryptosystems, not yet presented in the previous paper (Hashimoto 2017). We first summarize in Sect. 2 the schemes UOV (Kipnis et al. 1999; Patarin 1997), Rainbow (Ding et al. 2005), and (variants of) HFE (Patarin 1996) with short surveys on the second round candidates LUOV (Beullens et al. 2020), Rainbow (Ding et al. 2020), and GeMSS (Casanova et al. 2020). Besides, we study in Sect. 3 the encryption schemes HFERP (Ikematsu et al. 2018), ZHFE (Porras et al. 2020), EFC (Szepieniec et al. 2016), and ABC (Tao et al. 2013) proposed recently, and show that the practicalities of these schemes are not much higher than the HFE variants for encryption, which are already known to be not too practical. Remark that MQDSS (Chen et al. 2016, 2020) is also a second round candidate and has been considered as a multivariate signature scheme since a set of randomly chosen multivariate quadratic forms is used in key generation, signature generation, and signature verification. However, it is based on Fiat–Shamir’s transform of the 5-pass identification scheme (Sakumoto et al. 2011) and is far from other multivariate schemes. We then avoid to study MQDSS in this paper.

2 UOV, Rainbow, and Variants of HFE

In this section, we describe UOV (Kipnis et al. 1999; Patarin 1997), Rainbow (Ding et al. 2005), and variants of HFE (Patarin 1996) and give short surveys on the second round candidates LUOV (Beullens et al. 2020), Rainbow (Ding et al. 2020), and GeMSS (Casanova et al. 2020) of NIST’s project (NIST 2020). We first propose the basic constructions of multivariate public key cryptosystems (MPKCS).

2.1 Basic Constructions of Multivariate Public Key Cryptosystems

Let $n, m \geq 1$ be integers, q a power of prime, and $\mathbf{F}_q$ a finite field of order q . Most MPKCSs are described as follows.

Secret key. Two invertible affine maps $S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$, $T : \mathbf{F}_q^m \rightarrow \mathbf{F}_q^m$ and a quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ to be inverted feasibly.

Public key. The quadratic map $F := T \circ G \circ S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

$$F : \mathbf{F}_q^n \xrightarrow{S} \mathbf{F}_q^n \xrightarrow{G} \mathbf{F}_q^m \xrightarrow{T} \mathbf{F}_q^m$$

Encryption scheme.

Encryption. For a plaintext $\mathbf{p} \in \mathbf{F}_q^n$, the ciphertext is $\mathbf{c} = F(\mathbf{p}) \in \mathbf{F}_q^m$.

Decryption. For a given ciphertext $\mathbf{c} \in \mathbf{F}_q^m$, compute $\mathbf{z} := T^{-1}(\mathbf{c})$ and find $\mathbf{y} \in \mathbf{F}_q^n$ with $G(\mathbf{y}) = \mathbf{z}$. Then the plaintext is $\mathbf{p} = S^{-1}(\mathbf{y})$.

Signature scheme.

Signature generation. For a message $\mathbf{m} \in \mathbf{F}_q^m$, compute $\mathbf{z} := T^{-1}(\mathbf{m})$ and find $\mathbf{y} \in \mathbf{F}_q^n$ with $G(\mathbf{y}) = \mathbf{z}$. Then the signature is $\mathbf{s} = S^{-1}(\mathbf{y})$.

Signature verification. The signature $\mathbf{s} \in \mathbf{F}_q^n$ is verified by $\mathbf{m} = F(\mathbf{s})$.

Efficiency. The encryption and signature verification are done by substituting $\mathbf{p}, \mathbf{s} \in \mathbf{F}_q^n$ into m quadratic forms of n variables. Their complexities are then $O(n^2m)$ for most MPKCs under naive implementations. Furthermore, it is known (Hashimoto 2017) that the complexities of encrypting n plaintexts and of verifying n signatures simultaneously are $O(n^w m)$, where $2 \leq w < 3$ is a linear algebra constant. The complexities of decryption and signature generation depend mainly on how to invert G . We will discuss them in the individual schemes.

Security. There are two types of attacks on MPKCs. One is the *direct attack* to recover the plaintext $\mathbf{p}$ of a given ciphertext $\mathbf{c}$ directly by solving a system of m quadratic equations $F(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_m(\mathbf{x})) = \mathbf{c}$ of n variables. The Gröbner basis attack is considered to be the most standard approach, and its complexity depends on the *degree* d_{reg} of *regularity* of the corresponding polynomial system $F(\mathbf{x}) - \mathbf{c}$. In general, d_{reg} is known to be smaller when the system is more over-defined ($m \gg n$) (Bardet et al. 2005). Furthermore, if q is small, the attacker will solve more efficiently by combining with the exhaustive search, which is called a *hybrid method* (Bettale et al. 2012). We also note that, if the system is massively under-defined ($n \gg m$), the attacker can find (at least) one of the solutions more effectively than the case of $n \sim m$ (Cheng et al. 2014; Kipnis et al. 1999; Miura et al. 2013; Tomae and Wolf 2012).

The other type is to recover partial information of the secret key (S, T) which is enough to invert F . In most known key recovery attacks on MPKCs, the attacker uses the property of the coefficient matrices of quadratic forms in G . Let $G_1, \dots, G_m, F_1, \dots, F_m$ be the coefficient matrices of $g_1(\mathbf{x}), \dots, g_m(\mathbf{x}), f_1(\mathbf{x}), \dots, f_m(\mathbf{x})$, respectively, i.e., $g_l(\mathbf{x}) = {}^t\mathbf{x}G_l\mathbf{x} + (\text{linear form})$ and $f_l(\mathbf{x}) = {}^t\mathbf{x}F_l\mathbf{x} + (\text{linear form})$ for $1 \leq l \leq m$. Since $F(\mathbf{x}) = T(G(S(\mathbf{x})))$, it holds

$$\begin{pmatrix} F_1 \\ \vdots \\ F_m \end{pmatrix} = T \begin{pmatrix} {}^tSG_1S \\ \vdots \\ {}^tSG_mS \end{pmatrix}. \quad (1)$$

This shows that, if $G_1, \dots, G_m$ have special properties, partial information S, T will be recovered by the public information $F_1, \dots, F_m$. How to recover and the complexity of the attack depend on $G_1, \dots, G_m$, and then we discuss them in the individual schemes.

2.2 UOV

Let $o, v \geq 1$ be integers and put $n := o + v$, $m := o$. The quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ is defined by

$$g_j(\mathbf{x}) = \sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+1}, \dots, x_n) \\ + (\text{quadratic form of } x_{o+1}, \dots, x_n), \quad (2)$$

for $1 \leq j \leq o$. UOV (Unbalanced Oil and Vinegar signature scheme, Patarin (1997), Kipnis et al. (1999)) is constructed as follows.

Secret key. An invertible affine map $S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$ and the quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ defined above.

Public key. The quadratic map $F := G \circ S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

Signature generation. For a message $\mathbf{m} = (m_1, \dots, m_o) \in \mathbf{F}_q^m$, choose $u_1, \dots, u_v \in \mathbf{F}_q$ randomly and find $y_1, \dots, y_o \in \mathbf{F}_q$ such that

$$g_1(y_1, \dots, y_o, u_1, \dots, u_v) = m_1, \quad \dots, \quad g_o(y_1, \dots, y_o, u_1, \dots, u_v) = m_o. \quad (3)$$

The signature is $\mathbf{s} = S^{-1}(y_1, \dots, y_o, u_1, \dots, u_v)$.

Signature verification. The signature $\mathbf{s} \in \mathbf{F}_q^n$ is verified by $\mathbf{m} = F(\mathbf{s})$.

Complexity of signature generation. Since (3) is a system of o linear equations of o variables, we see that the complexity of signature generation of UOV is $O(n^3)$.

Security. The most important attack on UOV is Kipnis–Shamir’s attack (Kipnis et al. 1999; Kipnis and Shamir 1998), which recovers an affine map S' such that

$SS' = \begin{pmatrix} * & o & * \\ 0 & * & v \end{pmatrix}$ by using the fact that $G_1, \dots, G_m$ are matrices having the forms of

$\begin{pmatrix} 0 & o & * \\ * & * & v \end{pmatrix}$. Its complexity is known to be $O(q^{\max(v-o, 0)} \cdot n^4)$ (Kipnis et al. 1999), and

then the parameter v must be sufficiently larger than o , namely n must be sufficiently larger than $2m$. This causes two inconveniences on UOV; one is that the sizes of keys are relatively large, and the other is that the approaches in Tomae and Wolf (2012), Cheng et al. (2014) weakens the security against the direct attacks a little. The later is easily covered by taking (n, m) a little larger. For the former, several approaches have been given until now. However, since some of key reduction approaches yield critical vulnerabilities (e.g., Hashimoto 2019; Peng and Tang 2018), the security of such UOVs must be studied quite carefully.

LUOV. LUOV (Beullens et al. 2020) is a signature scheme based on UOV and is a second round candidate of NIST’s project. It is constructed over a finite field of even characteristic field and the components and coefficients in S, G, F are elements of $\mathbf{F}_2$. The size of keys is smaller and the security against the direct attack is not too less than the original UOV. Remark that the security against Kipnis–Shamir’s attack

is $O(2^{v-o} \cdot n^4)$ and a new attack on LUOV was quite recently proposed in Ding et al. (2013). Then the parameters o, v should be taken larger than the original version. See Beullens et al. (2020) for the latest version.

2.3 Rainbow

Rainbow (Ding et al. 2005) is a multi-layer version of UOV. We now describe the two-layer version. Let $o_1, o_2, v \geq 1$ be integers and put $n = o_1 + o_2 + v$, $m = o_1 + o_2$. Define the quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ by

$$\begin{aligned} g_1(\mathbf{x}), \dots, g_{o_1}(\mathbf{x}) &= \sum_{1 \leq i \leq o_1} x_i \cdot (\text{linear form of } x_{o_1+1}, \dots, x_n) \\ &\quad + (\text{quadratic form of } x_{o_1+1}, \dots, x_n), \\ g_{o_1+1}(\mathbf{x}), \dots, g_m(\mathbf{x}) &= \sum_{o_1+1 \leq i \leq m} x_i \cdot (\text{linear form of } x_{m+1}, \dots, x_n) \\ &\quad + (\text{quadratic form of } x_{m+1}, \dots, x_n), \end{aligned} \quad (4)$$

Rainbow is constructed as follows.

Secret key. Two invertible affine maps $S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$, $T : \mathbf{F}_q^m \rightarrow \mathbf{F}_q^m$ and the quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ defined above.

Public key. The quadratic map $F := T \circ G \circ S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

Signature generation. For a message $\mathbf{m} \in \mathbf{F}_q^m$ to be signed, compute $\mathbf{z} = {}^t(z_1, \dots, z_m) := T^{-1}(\mathbf{m})$ and choose $u_1, \dots, u_v \in \mathbf{F}_q$ randomly. Find $y_{o_1+1}, \dots, y_m \in \mathbf{F}_q$ such that

$$g_{o_1+1}(y_1, \dots, y_m, u_1, \dots, u_v) = z_{o_1+1}, \quad \dots, \quad g_m(y_1, \dots, y_m, u_1, \dots, u_v) = z_m. \quad (5)$$

After that, find $y_1, \dots, y_{o_1} \in \mathbf{F}_q$ such that

$$g_1(y_1, \dots, y_m, u_1, \dots, u_v) = z_1, \quad \dots, \quad g_{o_1}(y_1, \dots, y_m, u_1, \dots, u_v) = z_{o_1}. \quad (6)$$

The signature is $\mathbf{s} = S^{-1}(y_1, \dots, y_m, u_1, \dots, u_v)$.

Signature verification. The signature $\mathbf{s} \in \mathbf{F}_q^n$ is verified by $\mathbf{m} = F(\mathbf{s})$.

Complexity of signature generation. Since (5) is a system of o_2 linear equations of o_2 variables and (6) is a system of o_1 linear equations of o_1 variables, we see that the complexity of signature generation is $O(n^3)$.

Security. Kipnis–Shamir’s attack and rank attacks are major attacks on Rainbow. Since $G_1, \dots, G_{o_1} = \begin{pmatrix} 0_{o_1} & * \\ * & *_{o_2+v} \end{pmatrix}$ and $G_{o_1+1}, \dots, G_m = \begin{pmatrix} 0_{o_1} & 0 & 0 \\ 0 & 0_{o_2} & * \\ 0 & * & *_{o_3} \end{pmatrix}$, the complexity of Kipnis–Shamir’s attack (Kipnis et al. 1999; Kipnis and Shamir 1998) on Rainbow is $O(q^{\max(o_2+v-o_1, 0)} \cdot n^4)$. Furthermore, by checking the ranks of $G_1, \dots, G_m$, we see that the complexities of min-rank attack and high-rank attack are $O(q^{o_2+v} \cdot n^4)$ and $O(q^{o_1} \cdot n^4)$, respectively (Yang and Chen 2005). Note that there have been several approaches to improve the efficiency of Rainbow. However, some of improvements are known to be insecure (e.g., Hashimoto 2019; Hashimoto et al. 2018; Peng and Tang 2018; Shim et al. 2017) and then the security of such efficient Rainbows must be studied carefully.

Rainbow on NIST’s project. Rainbow (Ding et al. 2020) in the second round of NIST’s project includes three versions; the standard Rainbow, the cyclic Rainbow, and the compressed Rainbow. The public keys and the numbers of arithmetics for signature verification for the later two Rainbows are smaller than the standard Rainbow. However, it is reported (Ding et al. 2020) that the verifications of the latter two versions are slower than the standard version. We consider that it is because the algorithms for verifications of the latter two versions are more complicated than the naive algorithm for the standard Rainbow. Better implementations are required for these arranged versions.

2.4 HFE

Let $n, m, d \geq 1$ be integers with $n = m, d < n$. Define $\mathcal{G} : \mathbf{F}_{q^n} \rightarrow \mathbf{F}_{q^n}$ by

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

where $\alpha_{ij}, \beta_i, \gamma \in \mathbf{F}_{q^n}$ and $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$ by $G := \phi^{-1} \circ \mathcal{G} \circ \phi$ where $\phi : \mathbf{F}_q^n \rightarrow \mathbf{F}_{q^n}$ is an $\mathbf{F}_q$ -isomorphism. HFE (Patarin 1996) is constructed as follows.

Secret key. Two invertible affine maps $S, T : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$ and $\mathcal{G} : \mathbf{F}_{q^n} \rightarrow \mathbf{F}_{q^n}$ defined above.

Public key. The quadratic map $F := T \circ G \circ S = T \circ \phi^{-1} \circ \mathcal{G} \circ \phi \circ S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$.

Encryption. For a plaintext $\mathbf{p} \in \mathbf{F}_q^n$, the ciphertext is $\mathbf{c} := F(\mathbf{p}) \in \mathbf{F}_q^n$.

Decryption. For a given ciphertext $\mathbf{c}$, compute $\mathbf{z} := T^{-1}(\mathbf{c})$ and put $Z := \phi(\mathbf{z})$. Find $Y \in \mathbf{F}_{q^n}$ with $\mathcal{G}(Y) = Z$ and put $\mathbf{y} := \phi^{-1}(Y)$. The plaintext is $\mathbf{p} = S^{-1}(\mathbf{y})$.

Complexity of decryption. Since $\mathcal{G}(Y) = Z$ is a univariate polynomial equation of degree at most $2q^d$ over $\mathbf{F}_{q^n}$, the complexity of finding Y is

$$O((\deg \mathcal{G}(X))^3 + n(\deg \mathcal{G}(X))^2 \log q) = O(q^{3d} + nq^{2d} \log q)$$

by the Berlekamp algorithm (Berlekamp 1967, 1970). Then the parameter d should be $d = O(\log_q n)$.

Security. Let $\{\theta_1, \dots, \theta_n\}$ be a basis of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ and $\Theta := (\theta_j^{q^{i-1}})_{1 \leq i, j \leq n}$. It is easy to see that $\Theta \mathbf{x} = {}^t(\phi(\mathbf{x}), \phi(\mathbf{x})^q, \dots, \phi(\mathbf{x})^{q^{n-1}}) := {}^t(X, X^q, \dots, X^{q^{n-1}})$. Since $F = (T \circ \phi^{-1}) \circ \mathcal{G} \circ (\phi \circ S)$, we have

$$\begin{pmatrix} F_1 \\ \vdots \\ F_n \end{pmatrix} = (T \cdot \Theta^{-1}) \begin{pmatrix} {}^t(\Theta S) \mathcal{G}^{(0)} (\Theta S) \\ \vdots \\ {}^t(\Theta S) \mathcal{G}^{(n-1)} (\Theta S) \end{pmatrix}, \quad (7)$$

where $\bar{X} := \Theta \mathbf{x}$ and $\mathcal{G}^{(i)}$ is an $n \times n$ matrix over $\mathbf{F}_{q^n}$ such that $\mathcal{G}(X)^{q^i} = {}^t \bar{X} \mathcal{G}^{(i)} \bar{X} +$ (linear form of $\bar{X}$). This means that there exist $a_1, \dots, a_n \in \mathbf{F}_{q^n}$ such that

$$a_1 F_1 + \dots + a_n F_n = {}^t(\Theta S) \mathcal{G}^{(0)} (\Theta S) = {}^t(\Theta S) \begin{pmatrix} *_{d+1} & \\ & 0_{n-d-1} \end{pmatrix} (\Theta S), \quad (8)$$

and then $\text{rank}(a_1 F_1 + \dots + a_n F_n) \leq d + 1$. The *min-rank attack* (Bettale et al. 2013; Kipnis and Shamir 1999) is an attack to recover such $(a_1, \dots, a_n)$ and its complexity is estimated by $O\left(\binom{n+d+2}{d+2}^w\right) = O(n^{(d+2)w})$ under the assumption that a variant of Fröberg conjecture holds, where $2 \leq w \leq 3$ is a linear algebra constant. It is not difficult to check that the tuple $(a_1, \dots, a_n)$ gives partial information of $T \Theta^{-1}$ and, once such a tuple is recovered, the attacker can recover partial information of ΘS , which is enough to decrypt arbitrary ciphertexts by elementary linear algebraic approaches. Since $d = O(\log_q n)$, the security of HFE is $n^{O(\log_q n)}$. Then the original HFE has been considered to be impractical. We also note that the security against Gröbner basis attack has been studied well (see e.g., Ding et al. 2011; Dubois and Gamma 2020; Faugère 2003; Granboulan et al. 2020; Huang et al. 2018). It is known that the rank condition (8) gives an upper bound of the degree d_{reg} of regularity of the polynomial system $F(\mathbf{x}) = \mathbf{c}$, in fact, $d_{\text{reg}} \leq \frac{1}{2}(q-1)(d+2)$ holds for HFE (Ding et al. 2011).

2.5 Variants of HFE

There have been various variants of HFE. In this subsection, we describe four major variants “plus (+)”, “minus (−)”, “vinegar (v)”, and “projection (p)”.

Plus (+). The “plus (+)” is a variant to add several polynomials on G . Let $r_+ \geq 1$ be an integer and $h_1(\mathbf{x}), \dots, h_{r_+}(\mathbf{x})$ random quadratic forms of $\mathbf{x}$. For the map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ of the original scheme, define $G_+ : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^{m+r_+}$ by $G_+(\mathbf{x}) := {}^t(g_1(\mathbf{x}), \dots, g_m(\mathbf{x}), h_1(\mathbf{x}), \dots, h_{r_+}(\mathbf{x}))$. The public key $F_+ : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^{m+r_+}$ of the plus

is $F_+ := T_+ \circ G_+ \circ S$ where $T_+ : \mathbf{F}_q^{m+r_+} \rightarrow \mathbf{F}_q^{m+r_+}$ is an invertible affine map. It is mainly used for encryption when $m \geq n$. The decryption is as follows.

Decryption. For the ciphertext $\mathbf{c} \in \mathbf{F}_q^{m+r_+}$, compute $\mathbf{z} = (z_1, \dots, z_{m+r_+}) := T_+^{-1}(\mathbf{c})$. Find $\mathbf{y} \in \mathbf{F}_q^n$ with $G(\mathbf{y}) = {}^t(z_1, \dots, z_m)$ and verify whether ${}^t(h_1(\mathbf{y}), \dots, h_{u_+}(\mathbf{y})) = {}^t(z_{m+1}, \dots, z_{m+r_+})$. If it holds, the plaintext is $\mathbf{p} = S^{-1}(\mathbf{y})$. If not, try it again by another $\mathbf{y}$.

Complexity of decryption. If $m \geq n$, the number of $\mathbf{y}$ with $G(\mathbf{y}) = \mathbf{z}$ is (probably) small. Then the complexity of decryption of “plus” is not much larger than the original scheme.

Security. It is easy to see that an equation similar to (8) holds for the “plus” of HFE. Then the complexity of the min-rank attack on HFE+ is similar to the original HFE.

Minus (−). The “minus (−)” is to reduce several polynomials in F . Let $r_- \geq 1$ be an integer. For the public key $F : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ of the original scheme, the public key $F_- : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^{m-r_-}$ of the minus is generated by $F_-(x) = {}^t(f_1(x), \dots, f_{m-r_-}(x))$. It is mainly used for the signature scheme when $n \geq m$. The signature generation is as follows.

Signature generation. For a message $\mathbf{m} = {}^t(m_1, \dots, m_{m-r_-}) \in \mathbf{F}_q^{m-r_-}$ to be signed, choose $u_1, \dots, u_{r_-} \in \mathbf{F}_q$ randomly and let $\tilde{\mathbf{m}} := {}^t(m_1, \dots, m_{m-r_-}, u_1, \dots, u_{r_-})$. Find $\mathbf{s} \in \mathbf{F}_q^n$ with $F(\mathbf{s}) = \tilde{\mathbf{m}}$. If there exists such an $\mathbf{s}$, the signature is $\mathbf{s}$. If not, change $u_1, \dots, u_{r_-}$ and repeat until such an $\mathbf{s}$ appears.

Complexities of signature generation. When $n \geq m$, the probability that $\mathbf{s}$ does not exist is considered to be not large. Then the complexity of the signature generation of the “minus” is not much larger than the original scheme.

Security. For the minus, it is easy to see that there exists an $(n - r_-) \times n$ matrix T_- such that

$$\begin{pmatrix} F_1 \\ \vdots \\ F_{n-r_-} \end{pmatrix} = (T_- \cdot \Theta^{-1}) \begin{pmatrix} {}^t(\Theta S) \mathcal{G}^{(0)}(\Theta S) \\ \vdots \\ {}^t(\Theta S) \mathcal{G}^{(n-1)}(\Theta S) \end{pmatrix}. \quad (9)$$

Then one can eliminate the contributions of $n - r_- - 1$ matrices in the right hand side by taking a linear combination of $F_1, \dots, F_{n-r_-}$, namely there exist $a_1, \dots, a_{n-r_-}$, $b_0, \dots, b_{r_-} \in \mathbf{F}_{q^n}$ such that

$$\begin{aligned} a_1 F_1 + \dots + a_{n-r_-} F_{n-r_-} &= b_0 {}^t(\Theta S) \mathcal{G}^{(0)}(\Theta S) + \dots + b_{r_-} {}^t(\Theta S) \mathcal{G}^{(r_-)}(\Theta S) \\ &= {}^t(\Theta S) \begin{pmatrix} *_{d+r_-+1} \\ 0_{n-d-r_-+1} \end{pmatrix} (\Theta S). \end{aligned}$$

The min-rank attack is thus available on HFE- and its complexity can be estimated by $O\left(\binom{n+d+r_-+2}{d+r_-+2}^w\right) = O(n^{(d+r_-+2)w})$. This means that the “minus” enhances the security of HFE (see also Vates and Smith-Tone 2017).

Vinegar (v). The “vinegar (v)” is to add several variables on G . Let $r_v \geq 1$ be an integer. For the map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ of the original scheme, define $G_v : \mathbf{F}_q^{n+r_v} \rightarrow \mathbf{F}_q^m$

such that $G_v(x_1, \dots, x_n, u_1, \dots, u_{r_v})$ is inverted similarly to $G(\mathbf{x})$ for any (or most) $u_1, \dots, u_{r_v} \in \mathbf{F}_q$. For example, the map G_v of HFEv is given by $G_v := \phi_{-1} \circ \mathcal{G}_v \circ \phi_v$, where $\phi_v : \mathbf{F}_q^{n+r_v} \rightarrow \mathbf{F}_{q^n} \times \mathbf{F}_{q^v}^{r_v}$ is an $\mathbf{F}_q$ -isomorphism and $\mathcal{G}_v : \mathbf{F}_{q^n} \times \mathbf{F}_{q^v}^{r_v} \rightarrow \mathbf{F}_{q^n}$ is the following polynomial map.

$$\begin{aligned} \mathcal{G}_v(X, x_{n+1}, \dots, x_{n+r_v}) = & \sum_{0 \leq i, j \leq d} \alpha_{ij} X^{q^i + q^j} + \sum_{0 \leq i \leq d} X^{q^i} \cdot (\text{linear form of } x_{n+1}, \dots, x_{n+r_v}) \\ & + (\text{quadratic form of } x_{n+1}, \dots, x_{n+r_v}). \end{aligned}$$

The public key $F_v : \mathbf{F}_q^{n+r_v} \rightarrow \mathbf{F}_q^n$ of the vinegar is $F_v := T \circ G_v \circ S_v$ where $S_v : \mathbf{F}_q^{n+r_v} \rightarrow \mathbf{F}_q^{n+r_v}$ is an invertible affine map. It is mainly used for signature when $n \geq m$. The signature generation is as follows.

Signature generation. For a message $\mathbf{m} \in \mathbf{F}_q^m$ to be signed, compute $\mathbf{z} := T^{-1}(\mathbf{m})$. Choose $u_1, \dots, u_{r_v} \in \mathbf{F}_q$ randomly, and find $\mathbf{y} \in \mathbf{F}_q^n$ with $G_v(\mathbf{y}, u_1, \dots, u_{r_v}) = \mathbf{z}$. If such an $\mathbf{y}$ does not exist, change $u_1, \dots, u_{r_v}$ and try again. The signature is $\mathbf{s} = S_v^{-1}(\mathbf{y}, u_1, \dots, u_{r_v})$.

Complexity of signature generation. Since $\mathbf{y}$ is found similarly to the original scheme, the complexity of finding $\mathbf{y}$ is almost the same as the original scheme. If $n \geq m$, the probability that $\mathbf{y}$ does not exist is considered to be not too large. Then the complexity of the “vinegar” is not too larger than the original scheme.

Security. For HFEv, we see that $\mathcal{G}_v(X, x_{n+1}, \dots, x_{n+r_v}) = {}^t\bar{X}_v \left(\frac{*_{d+1} \mid *}{* \mid *_{r_v}} \right) \bar{X}_v + (\text{linear form of } \bar{X}_v)$, where $\bar{X}_v = {}^t(X, \dots, X^{q^{n-1}}, x_{n+1}, \dots, x_{n+r_v})$. Then there exist $a_1, \dots, a_n \in \mathbf{F}_{q^n}$ such that

$$a_1 F_1 + \dots + a_n F_n = {}^t \left(\begin{pmatrix} \Theta & \\ & I_{r_v} \end{pmatrix} S_v \right) \left(\frac{*_{d+1} \mid *}{* \mid *_{r_v}} \right) \left(\begin{pmatrix} \Theta & \\ & I_{r_v} \end{pmatrix} S_v \right).$$

Since the rank of the matrix in the right hand side above is at most $d + r_v + 1$, the security of HFEv against the min-rank attack is estimated by $O((\frac{n+d+r_v+2}{d+r_v+2})^w) = O(n^{(d+r_v+2)w})$.

Projection (p). The “projection” is to reduce several variables of the polynomials in F . Let $r_p \geq 1$ be an integer and $u_1, \dots, u_{r_p} \in \mathbf{F}_q$. For the public key $F : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ of the original scheme, the public key $F_p : \mathbf{F}_q^{n-r_p} \rightarrow \mathbf{F}_q^m$ of the projection is generated by $F_p(x_1, \dots, x_{n-r_p}) := F(x_1, \dots, x_{n-r_p}, u_1, \dots, u_{r_p})$. It is mainly used for encryption when $m \geq n$. The decryption is as follows.

Decryption. For the ciphertext $\mathbf{c} \in \mathbf{F}_q^m$, find $\mathbf{p} \in \mathbf{F}_q^n$ with $F(\mathbf{p}) = \mathbf{c}$ similarly to the original scheme. If $\mathbf{p} = (*, \dots, *, u_1, \dots, u_{r_p})$, the plaintext is $\tilde{\mathbf{p}} := (p_1, \dots, p_{n-r_p}) \in \mathbf{F}_q^{n-r_p}$. If not, try it again by another $\mathbf{p}$.

Complexities of decryption. If $m \geq n$, the number of $\mathbf{p}$ with $F(\mathbf{p}) = \mathbf{c}$ is (probably) not too large. Then the complexity of decryption of the “projection” is not much larger than the original scheme.

Security. For the projection of HFE, we see that there exist $a_1, \dots, a_n \in \mathbf{F}_{q^n}$ such that

$$a_1 F_1 + \dots + a_n F_n = {}^t(\Theta \tilde{S}) \begin{pmatrix} *_{d+1} \\ 0_{n-d-1} \end{pmatrix} (\Theta \tilde{S}),$$

where $\tilde{S}$ is an $n \times (n - r_p)$ matrix with $S = (\tilde{S}, *)$. Then the min-rank attack is available and its complexity is almost the same as the original scheme.

The most successful variant of HFE is probably the signature scheme **HFEv-** (Patarin et al. 2001), a combination of “minus” and “vinegar” of HFE, since the security against the min-rank attack is enhanced drastically without slowing down the signature generation. In fact, **GeMSS** (Casanova et al. 2020) based on HFEv- was chosen as a second round candidate of NIST’s project (NIST 2020). There are three kinds of GeMSS, called GeMSS, BlueGeMSS, and RedGeMSS. The major difference among these three GeMSSs is the degree of $\mathcal{G}_v$; the degrees are $513 (= 2^9 + 1)$, $129 (= 2^7 + 1)$, $17 (= 2^4 + 1)$, i.e., d ’s are 10, 8, 5, respectively. Of course, the signature generation of RedGeMSS is fastest and the BlueGeMSS is the next. Furthermore, the securities against the min-rank attack are enough if r_- , r_v are sufficiently large. On the other hand, as pointed out in Hashimoto (2018) for HMFev (Petzoldt et al. 2017) (the vinegar of multi-HFE (Chen et al. 2020)), the minus and the vinegar do not enhance the security against the high-rank attack. Though critical vulnerabilities of HFE variants against the high-rank attack have not been reported until now, we consider that an HFEv- with smaller d has a higher risk against the high-rank attack.

We recall that **Sflash** (Akkar et al. 2003) (a minus of Matsumoto–Imai’s scheme (Matsumoto and Imai 1988) is a signature scheme selected by NESSIE (Preneel 2020) and broken by a differential attack (Fouque et al. 2005). Recently, its projections called **Pflash** (Cartor and Smith-Tone 2017; Smith-Tone et al. 2015) and **Eflash** (Cartor and Smith-Tone 2018) were proposed. Pflash is a signature scheme with $r_p < r_-$ and Eflash is an encryption scheme with $r_p > r_-$. The complexities of signature generation and decryption are about $q^{\min(r_p, r_-)}$ times of Matsumoto–Imai’s scheme (Matsumoto and Imai 1988) and then we should take r_-, r_p by $\min(r_p, r_-) = O(\log_q n)$. It has been considered that the differential attack is not available on these schemes, and the security against the min-rank attack highly depends on r_- . The security of Eflash is thus $n^{O(\log_q n)}$. Similarly for the encryption scheme HFEp- with $r_p > r_-$, it is easy to see that the complexity of decryption is about q^{r_-} times of the original HFE and the complexity of the min-rank attack is roughly estimated by $O(n^{(3d+r_-+2)w})$. Since $3d + r_- = O(\log_q n)$, its security is also $n^{O(\log_q n)}$.

3 New Encryption Schemes

In this section, we study the encryption schemes HFERP (Ikematsu et al. 2018), ZHFE (Porrás et al. 2020), EFC (Szepieniec et al. 2016), and ABC (Tao et al. 2013, 2015) proposed recently.

3.1 HFERP

HFERP (Ikematsu et al. 2018) is an encryption scheme constructed by a “plus” and “projection” of a combination of HFE and Rainbow. We first describe a one-layer version HFERP without “plus” and “projection”.

Let $v, o, l, d_0 \geq 1$ be integers, $n := v + o$ and $m := v + o + l$. Define the map $\mathcal{G}_0 : \mathbf{F}_{q^v} \rightarrow \mathbf{F}_{q^v}$ by

$$\mathcal{G}_0(X) := \sum_{0 \leq i \leq j \leq d_0} \alpha_{ij} X^{q^i + q^j} + \sum_{0 \leq i \leq d_0} \beta_i X^{q^i} + \gamma,$$

where $\alpha_{ij}, \beta_i, \gamma \in \mathbf{F}_{q^v}$. The quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ is given as follows.

$$\begin{aligned} {}^t(g_1(\mathbf{x}), \dots, g_v(\mathbf{x})) &= (\phi_0^{-1} \circ \mathcal{G}_0 \circ \phi_0)(\mathbf{x}_0), \\ g_{v+1}(\mathbf{x}), \dots, g_m(\mathbf{x}) &= \sum_{v+1 \leq i \leq n} x_i \cdot (\text{linear form of } \mathbf{x}_0) + (\text{quadratic form of } \mathbf{x}_0), \end{aligned}$$

where $\phi_0 : \mathbf{F}_q^v \rightarrow \mathbf{F}_{q^v}$ is an $\mathbf{F}_q$ -isomorphism and $\mathbf{x}_0 = {}^t(x_1, \dots, x_v)$. HFERP (without “plus”, “projection”) is constructed as follows.

Secret key. Two invertible affine maps $S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n, T : \mathbf{F}_q^m \rightarrow \mathbf{F}_q^m$ and the quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

Public key. The quadratic map $F := T \circ G \circ S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

Encryption. For a plaintext $\mathbf{p} \in \mathbf{F}_q^n$, the ciphertext is $\mathbf{c} = F(\mathbf{p}) \in \mathbf{F}_q^m$.

Decryption. For a given ciphertext $\mathbf{c}$, compute $\mathbf{z} = {}^t(z_1, \dots, z_m) := T^{-1}(\mathbf{c})$. Let $Z_0 := \phi_0(z_1, \dots, z_v) \in \mathbf{F}_{q^v}$ and find $Y_0 \in \mathbf{F}_{q^v}$ such that $\mathcal{G}_0(Y_0) = Z_0$. Put $(y_1, \dots, y_v) := \phi_0^{-1}(Y_0) \in \mathbf{F}_q^v$ and find $y_{v+1}, \dots, y_n \in \mathbf{F}_q$ with

$$g_{v+1}(y_1, \dots, y_v, y_{v+1}, \dots, y_n) = z_{v+1}, \quad \dots, \quad g_m(y_1, \dots, y_v, y_{v+1}, \dots, y_n) = z_m. \quad (10)$$

The plaintext is $\mathbf{p} = S^{-1}(y_1, \dots, y_n)$.

Complexity of decryption. Since the degree of $\mathcal{G}_0(X)$ is at most $2q^{d_0}$, the complexity of finding Y_0 is $O(q^{3d_0} + vq^{2d_0} \log q)$ by Berlekamp’s algorithm. We see that (10) is a system of $o + l$ linear equations of o variables. We thus conclude that the total

complexity of decryption is $O(q^{3d_0} + vq^{2d_0} \log q + n^3)$. The parameter d_0 should be taken by $d_0 = O(\log_q n)$.

Security. Let $\{\theta_1, \dots, \theta_v\}$ be a basis of $\mathbf{F}_{q^v}$ over $\mathbf{F}_q$ and $\Theta_0 := \left(\theta_j^{q^{i-1}} \right)_{1 \leq i, j \leq v}$. By the definition of G, F , we see that

$$\begin{pmatrix} F_1 \\ \vdots \\ F_m \end{pmatrix} = T \cdot \begin{pmatrix} \Theta_0^{-1} & \\ & I_{o+l} \end{pmatrix} \begin{pmatrix} {}^tS \begin{pmatrix} {}^t\Theta_0 \mathcal{G}_0^{(0)} \Theta_0 & \\ & 0_o \end{pmatrix} S \\ \vdots \\ {}^tS \begin{pmatrix} {}^t\Theta_0 \mathcal{G}_0^{(v-1)} \Theta_0 & \\ & 0_o \end{pmatrix} S \\ {}^tS \begin{pmatrix} *_{\nu} & * \\ * & 0_o \end{pmatrix} S \\ \vdots \\ {}^tS \begin{pmatrix} *_{\nu} & * \\ * & 0_o \end{pmatrix} S \end{pmatrix}$$

and then there exist $a_1, \dots, a_m \in \mathbf{F}_{q^v}$ such that

$$a_1 F_1 + \dots + a_m F_m = {}^tS \begin{pmatrix} {}^t\Theta_0 \mathcal{G}_0^{(0)} \Theta_0 & \\ & 0_o \end{pmatrix} S = {}^tS {}^t \begin{pmatrix} \Theta_0 & \\ & I_o \end{pmatrix} \begin{pmatrix} *_{d_0+1} & \\ & 0_{n-d_0-1} \end{pmatrix} \begin{pmatrix} \Theta_0 & \\ & I_o \end{pmatrix} S.$$

The min-rank attack is thus available on HFERP and its complexity can be estimated by $O\left(\binom{m+d_0+2}{d_0+2}^w\right) = O(m^{(d_0+2)w})$ (Ikematsu et al. 2018). This situation is similar for its plus and projection. Since $d_0 = O(\log_q n)$, the security of HFERP is $n^{O(\log_q n)}$, which is almost the same as HFE. For the minus, we can easily check that the complexity of decryption is at most q^{r_-} times of the original HFERP and the security against the min-rank attack is $O\left(\binom{m+d_0+2}{d_0+r_-+2}^w\right) = O(m^{(d_0+r_-+2)w})$. This means that the security of HFERP- is also $n^{O(\log_q n)}$.

3.2 ZHFE

ZHFE (Porrás et al. 2020) is an encryption scheme constructed by two univariate polynomials over an extension field. In this subsection, we study the simplest version of ZHFE since the structure of the original version is not far from the simplest version.

Let $n, m, D \geq 1$ be integers with $m = 2n$ and define the quadratic forms $\mathcal{G}_1(X)$, $\mathcal{G}_2(X)$ of $\tilde{X} = {}^t(X, X^q, \dots, X^{q^{n-1}})$ such that the degree of $\Psi(X) := X^q \cdot \mathcal{G}_1(X) + X \cdot \mathcal{G}_2(X)$ is at most D . It is easy to see that the coefficient matrices $\mathcal{G}_1^{(0)}, \mathcal{G}_2^{(0)}$ of $\mathcal{G}_1(X), \mathcal{G}_2(X)$ as quadratic forms of $\tilde{X}$ are

$$\mathcal{G}_1^{(0)} = \left(\begin{array}{c|ccc} * & d+1 & * & \dots & * \\ * & 0 & 0 & \dots & 0 \\ \vdots & \vdots & 0 & & \\ * & 0 & & & \end{array} \middle| \begin{array}{c} * & \dots & * \\ 0 & \dots & 0 \\ \mathbf{0} & & \end{array} \right), \quad \mathcal{G}_2^{(0)} = \left(\begin{array}{c|ccc} * & d+1 & 0 & \dots & 0 \\ 0 & * & * & & * \\ \vdots & \vdots & 0 & & \\ 0 & * & & & \end{array} \middle| \begin{array}{c} 0 & \dots & 0 \\ * & & * \\ \mathbf{0} & & \\ 0 & & \end{array} \right), \quad (11)$$

where $d := \lceil \log_q \frac{D-q}{2} \rceil$. Denote by $\phi_2 : \mathbf{F}_q^m \rightarrow \mathbf{F}_{q^n}^2$ an $\mathbf{F}_q$ -isomorphism and $\mathcal{G}(X) := (\mathcal{G}_1(X), \mathcal{G}_2(X))$. ZHFE is constructed as follows.

Secret key. Two invertible affine maps $S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$, $T : \mathbf{F}_q^m \rightarrow \mathbf{F}_q^m$ and the quadratic map $G := \phi_2^{-1} \circ \mathcal{G} \circ \phi : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

Public key. The quadratic map $F := T \circ G \circ S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

Encryption. For a plaintext $\mathbf{p} \in \mathbf{F}_q^n$, the ciphertext is $\mathbf{c} = F(\mathbf{p}) \in \mathbf{F}_q^m$.

Decryption. For a given ciphertext $\mathbf{c} \in \mathbf{F}_q^m$, compute $\mathbf{z} := T^{-1}(\mathbf{c})$. Let $(Z_1, Z_2) := \phi_2(\mathbf{z}) \in \mathbf{F}_{q^n}^2$, and find $Y \in \mathbf{F}_{q^n}$ such that $\Psi(Y) - Y^q \cdot Z_1 - Y \cdot Z_2 = 0$. Verify whether $\mathcal{G}_1(Y) = Z_1$, $\mathcal{G}_2(Y) = Z_2$ hold and put $\mathbf{y} := \phi^{-1}(Y) \in \mathbf{F}_q^n$. The plaintext is $\mathbf{p} = S^{-1}(\mathbf{y})$.

Complexity of decryption. Since $\Psi(Y) - Y^q \cdot Z_1 - Y \cdot Z_2 = Y^q \cdot (\mathcal{G}_1(Y) - Z_1) + Y \cdot (\mathcal{G}_2(Y) - Z_2)$, at least one of Y satisfies $\mathcal{G}_1(Y) = Z_1$, $\mathcal{G}_2(Y) = Z_2$ if $\mathbf{z} \in G(\mathbf{F}_{q^n})$. The complexity of decryption is $O(D^3 + nD^2 \log q) = O(q^{3d} + nq^{2d} \log q)$ by Berlekamp's algorithm. The parameter d should be $d = O(\log_q n)$.

Security. Let $\{\theta_1, \dots, \theta_n\}$ be a basis of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ and $\Theta_2 := (\theta_j^{q^{i-1}} \cdot I_2)_{1 \leq i, j \leq n}$. We can easily check that

$$\begin{pmatrix} F_1 \\ \vdots \\ F_m \end{pmatrix} = T \Theta_2^{-1} \begin{pmatrix} {}^t(\Theta S) \mathcal{G}_1^{(0)}(\Theta S) \\ {}^t(\Theta S) \mathcal{G}_2^{(0)}(\Theta S) \\ {}^t(\Theta S) \mathcal{G}_1^{(1)}(\Theta S) \\ \vdots \\ {}^t(\Theta S) \mathcal{G}_2^{(n-1)}(\Theta S) \end{pmatrix}$$

and then there exist $a_1, \dots, a_m \in \mathbf{F}_{q^n}$ such that

$$a_1 F_1 + \dots + a_m F_m = {}^t(\Theta S) \mathcal{G}_1^{(0)}(\Theta S).$$

Since $\text{rank} \mathcal{G}_1^{(0)} \leq d + 2$ due to (11), the min-rank attack is available on ZHFE and its complexity can be estimated by $O(\binom{m+d+3}{d+3}^w) = O(m^{(d+3)w})$ (Cabarcas et al. 2017; Perlne and Smith-Tone 2016). Since $d = O(\log_q n)$, the security of ZHFE is also $n^{O(\log_q n)}$.

We note that the plus and projection do not enhance the security. For the minus, we see that there exist $a_1, \dots, a_{m-r_-}, b_0, \dots, b_{r_-} \in \mathbf{F}_{q^n}$ such that

$$\begin{aligned}
& a_1 F_1 + \cdots + a_{m-r_-} F_{m-r_-} \\
& = b_0 {}^t(\Theta S) \mathcal{G}_1^{(0)}(\Theta S) + b_1 {}^t(\Theta S) \mathcal{G}_2^{(0)}(\Theta S) + \cdots + b_{r_-} {}^t(\Theta S) \mathcal{G}_{(r_- \bmod 2)+1}^{(\lfloor r_-/2 \rfloor)}(\Theta S) \\
& = {}^t(\Theta S) \begin{pmatrix} *_{\lceil \frac{r_-}{2} \rceil + 1} & * & * \\ * & *_{d-(r_- \bmod 2)} & 0 \\ * & 0 & 0 \end{pmatrix} (\Theta S).
\end{aligned}$$

Since the rank of the matrix above is $d + r_- + 2$, the complexity of the min-rank attack is $O\left(\binom{m+d+3}{d+r_-+3}^w\right) = O((2n)^{(d+r_-+3)w})$. However, the complexity of decryption is at most q^{r_-} times of the original ZHFE, and then the security of ZHFE- is also $n^{O(\log_q n)}$. Remark that (Perlne and Smith-Tone 2016) proposed a minus of ZHFE without slowing down the decryption by using a singular-type ZHFE. However, by studying the structure of such a ZHFE- carefully, we can easily check that such a minus does not enhance the security against the min-rank attack at all.

3.3 EFC

EFC (Szepieniec et al. 2016) is an encryption scheme constructed from the fact that an extension field can be expressed by a set of matrices.

Let $n, m \geq 1$ be integers with $m = 2n$, $h(t)$ an irreducible univariate polynomial over $\mathbf{F}_q$ and H an $n \times n$ matrix whose characteristic polynomial is $h(t)$. It is easy to see that $\mathcal{H} := \{a_0 I_n + a_1 H + \cdots + a_{n-1} H^{n-1} \mid a_0, \dots, a_{n-1} \in \mathbf{F}_q\}$ is isomorphic to $\mathbf{F}_q[t]/\langle h(t) \rangle \simeq \mathbf{F}_{q^n}$. Choose $A_1, \dots, A_m \in \mathcal{H}$ and define the map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ by

$$\begin{aligned}
{}^t(g_1(\mathbf{x}), g_3(\mathbf{x}), \dots, g_{m-1}(\mathbf{x})) &= (x_1 A_1 + x_2 A_3 + \cdots + x_{m-1} A_n) \mathbf{x}, \\
{}^t(g_2(\mathbf{x}), g_4(\mathbf{x}), \dots, g_m(\mathbf{x})) &= (x_1 A_2 + x_2 A_4 + \cdots + x_m A_n) \mathbf{x}.
\end{aligned}$$

EFC (Szepieniec et al. 2016) is constructed as follows.

Secret key. Two invertible affine maps $S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$, $T : \mathbf{F}_q^m \rightarrow \mathbf{F}_q^m$ and the quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ (i.e., the matrices $A_1, \dots, A_m$) defined above.

Public key. The quadratic map $F := T \circ G \circ S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

Encryption. For a plaintext $\mathbf{p} \in \mathbf{F}_q^n$, the ciphertext is $\mathbf{c} = F(\mathbf{p}) \in \mathbf{F}_q^m$.

Decryption. For a given ciphertext $\mathbf{c}$, compute $\mathbf{z} = {}^t(z_1, \dots, z_m) := T^{-1}(\mathbf{c})$. Solve a system of linear equations given by

$$\begin{aligned}
& (x_1 A_1 + x_2 A_3 + \cdots + x_n A_{m-1}) {}^t(z_2, z_4, \dots, z_m) \\
& = (x_1 A_2 + x_2 A_4 + \cdots + x_n A_m) {}^t(z_1, z_3, \dots, z_{m-1}),
\end{aligned} \tag{12}$$

and find a solution $\mathbf{y}$ of (12) satisfying $G(\mathbf{y}) = \mathbf{z}$. The plaintext is $\mathbf{p} = S^{-1}(\mathbf{y})$.

Complexity of decryption. Since $\mathcal{H}$ is commutative, it holds

$$\begin{aligned}
& (x_1 A_2 + x_2 A_4 + \cdots + x_n A_m)^t (g_1(\mathbf{x}), g_3(\mathbf{x}), \dots, g_{m-1}(\mathbf{x})) \\
&= (x_1 A_1 + x_2 A_3 + \cdots + x_n A_{m-1})^t (g_2(\mathbf{x}), g_4(\mathbf{x}), \dots, g_m(\mathbf{x})).
\end{aligned}$$

Then at least one of solutions of (12) satisfies $G(\mathbf{y}) = \mathbf{z}$ if $\mathbf{z} \in G(\mathbf{F}_q^n)$. The equation (12) is written by $(z_1 B_1 + \cdots + z_m B_m) \mathbf{x} = 0$ with $n \times n$ matrices $B_1, \dots, B_m$ are $n \times n$ derived from $A_1, \dots, A_m$. The complexity of decryption is thus $O(n^3)$.

Note that, since the map G in EFC is over-defined, the complexity of the “plus” and the “projection” is almost the same as the original EFC and that of the “minus” is at most q^{t-} times of the original EFC.

Security. It is already known that the original EFC is insecure against the linearization attack (Szepieniec et al. 2016). We now study the security of EFC- against the min-rank attack. Let $\theta \in \mathbf{F}_{q^n}$ be a root of $h(t)$, choose a basis of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ by $\{\theta_1, \dots, \theta_n\} = \{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ and put $\Theta := \left(\theta_j^{q^{i-1}} \right)_{1 \leq i, j \leq n}$. Suppose that H is a companion matrix of $h(t)$. Since $A_1, \dots, A_m \in \mathcal{H}$, there exist linear forms $L_1(\mathbf{x}), \dots, L_m(\mathbf{x})$ of $\mathbf{x}$ over $\mathbf{F}_q$ such that

$$\begin{aligned}
x_1 A_1 + x_2 A_3 + \cdots + x_n A_{m-1} &= L_1(\mathbf{x}) I_n + L_3(\mathbf{x}) H + \cdots + L_{m-1}(\mathbf{x}) H^{n-1}, \\
x_1 A_2 + x_2 A_4 + \cdots + x_n A_m &= L_2(\mathbf{x}) I_n + L_4(\mathbf{x}) H + \cdots + L_m(\mathbf{x}) H^{n-1}.
\end{aligned}$$

Denote by

$$\begin{aligned}
\mathcal{G}_1(X) &:= g_1(\mathbf{x})\theta_1 + g_3(\mathbf{x})\theta_2 + \cdots + g_{m-1}(\mathbf{x})\theta_n, \\
\mathcal{G}_2(X) &:= g_2(\mathbf{x})\theta_1 + g_4(\mathbf{x})\theta_2 + \cdots + g_m(\mathbf{x})\theta_n, \\
\mathcal{L}_1(X) &:= L_1(\mathbf{x})\theta_1 + L_3(\mathbf{x})\theta_2 + \cdots + L_{m-1}(\mathbf{x})\theta_n, \\
\mathcal{L}_2(X) &:= L_2(\mathbf{x})\theta_1 + L_4(\mathbf{x})\theta_2 + \cdots + L_m(\mathbf{x})\theta_n,
\end{aligned}$$

where $X := \phi(\mathbf{x}) = x_1\theta_1 + \cdots + x_n\theta_n$. It is easy to see that $\mathcal{G}_1(X), \mathcal{G}_2(X)$ are quadratic forms and $\mathcal{L}_1(X), \mathcal{L}_2(X)$ are linear forms of $\bar{X} = \Theta \mathbf{x} = {}^t(X, X^q, \dots, X^{q^{n-1}})$. By the definition of G , we see that

$$\begin{aligned}
\Theta^t(g_1(\mathbf{x}), g_3(\mathbf{x}), \dots, g_{m-1}(\mathbf{x})) &= \left(\sum_{1 \leq i \leq n} L_{2i-1}(\mathbf{x}) (\Theta H \Theta^{-1})^{i-1} \right) (\Theta \mathbf{x}), \\
\Theta^t(g_2(\mathbf{x}), g_4(\mathbf{x}), \dots, g_m(\mathbf{x})) &= \left(\sum_{1 \leq i \leq n} L_{2i}(\mathbf{x}) (\Theta H \Theta^{-1})^{i-1} \right) (\Theta \mathbf{x}).
\end{aligned} \tag{13}$$

Since $\Theta H \Theta^{-1} = \text{diag}(\theta, \theta^q, \dots, \theta^{q^{n-1}})$ (e.g., Horn et al. 1985), we have $\mathcal{G}_1(X) = \mathcal{L}_1(X) \cdot X$, $\mathcal{G}_2(X) = \mathcal{L}_2(X) \cdot X$ due to (13). This means that the map G is written by $G = \phi_2^{-1} \circ \mathcal{G} \circ \phi$ where $\mathcal{G}(X) = (\mathcal{G}_1(X), \mathcal{G}_2(X)) = (\mathcal{L}_1(X) \cdot X, \mathcal{L}_2(X) \cdot X)$, and it holds

$$\begin{pmatrix} F_1 \\ \vdots \\ F_m \end{pmatrix} = T \Theta_2^{-1} \begin{pmatrix} {}^t(\Theta S) \mathcal{G}_1^{(0)}(\Theta S) \\ {}^t(\Theta S) \mathcal{G}_2^{(0)}(\Theta S) \\ {}^t(\Theta S) \mathcal{G}_1^{(1)}(\Theta S) \\ \vdots \\ {}^t(\Theta S) \mathcal{G}_2^{(n-1)}(\Theta S) \end{pmatrix}.$$

Then, for EFC-, there exist $a_1, \dots, a_{m-r_-}, b_0, \dots, b_{r_-} \in \mathbf{F}_{q^n}$ such that

$$\begin{aligned} & a_1 F_1 + \dots + a_{m-r_-} F_{m-r_-} \\ &= b_0 {}^t(\Theta S) \mathcal{G}_1^{(0)}(\Theta S) + b_1 {}^t(\Theta S) \mathcal{G}_2^{(0)}(\Theta S) + \dots + b_{r_-} {}^t(\Theta S) \mathcal{G}_{(r_- \bmod 2)+1}^{(\lfloor r_-/2 \rfloor)}(\Theta S) \\ &= {}^t(\Theta S) \begin{pmatrix} *_{1+\lfloor \frac{r_-}{2} \rfloor} * \\ * \end{pmatrix} (\Theta S). \end{aligned}$$

Since the rank of the matrix above is at most $2\lfloor \frac{r_-}{2} \rfloor + 2$, the min-rank attack is available on EFC- and its complexity can be estimated by $O\left(\binom{2n-r_-+2\lfloor \frac{r_-}{2} \rfloor+3}{3+2\lfloor \frac{r_-}{2} \rfloor}^w\right) = O((2n)^{(r_-+3)w})$. Since $r_- = O(\log_q n)$, the security of EFC- is also $n^{O(\log_q n)}$. This situation is similar to the “plus” and “projection” of EFC-.

3.4 ABC

ABC (Tao et al. 2013, 2015) is an encryption scheme constructed by three polynomial matrices A, B, C . Let $r, n, m \geq 1$ be integers with $n = r^2, m = 2r^2$. For $\mathbf{x} = (x_1, \dots, x_n)$, define the $r \times r$ matrices $A(\mathbf{x}), B(\mathbf{x}), C(\mathbf{x}), E_1(\mathbf{x}), E_2(\mathbf{x})$ by $A(\mathbf{x}) := (x_{j+r(i-1)})_{1 \leq i, j \leq r}$, $B(\mathbf{x}) := (b_{ij}(\mathbf{x}))_{1 \leq i, j \leq r}$, $C(\mathbf{x}) := (c_{ij}(\mathbf{x}))_{1 \leq i, j \leq r}$, $E_1(\mathbf{x}) := A(\mathbf{x})B(\mathbf{x})$ and $E_2(\mathbf{x}) := A(\mathbf{x})C(\mathbf{x})$, where $b_{ij}(\mathbf{x}), c_{ij}(\mathbf{x})$ are linear forms of $\mathbf{x}$. The quadratic map $G : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$ is generated by $E_1(\mathbf{x}) = (g_{j+r(i-1)}(\mathbf{x}))_{1 \leq i, j \leq r}$ and $E_2(\mathbf{x}) = (g_{n+j+r(i-1)}(\mathbf{x}))_{1 \leq i, j \leq r}$. The encryption scheme ABC (Tao et al. 2013) is constructed as follows.

Secret key. Two invertible affine maps $S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n, T : \mathbf{F}_q^m \rightarrow \mathbf{F}_q^m$ and the quadratic map G defined above.

Public key. The quadratic map $F := T \circ G \circ S : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^m$.

Encryption. For a plaintext $\mathbf{p} \in \mathbf{F}_q^n$, the ciphertext is $\mathbf{c} = F(\mathbf{p}) \in \mathbf{F}_q^m$.

Decryption. For a given ciphertext $\mathbf{c}$, compute $\mathbf{z} = (z_1, \dots, z_m) := T^{-1}(\mathbf{c})$ and put $Z_1 := (z_{j+r(i-1)})_{1 \leq i, j \leq r}, Z_2 := (z_{n+j+r(i-1)})_{1 \leq i, j \leq r}$. Find $\mathbf{y} \in \mathbf{F}_q^n$ such that

$$B(\mathbf{y}) = C(\mathbf{y})Z_2^{-1}Z_1. \quad (14)$$

If Z_2 is not invertible, replace (14) into $B(\mathbf{y})Z_1^{-1}Z_2 = C(\mathbf{y})$. The plaintext is $\mathbf{p} = S^{-1}(\mathbf{y})$.

Complexity of decryption. The equation (14) yields a system of n linear equations of n variables. Then the complexity of decryption is $O(n^3)$. Remark that the decryption fails if $A(S(\mathbf{p}))$ is not invertible and its probability is about q^{-1} .

Security. It is easy to check that the coefficient matrix G_1 of the first polynomial $g_1(\mathbf{x})$ in $G(\mathbf{x})$ is $G_1 = \begin{pmatrix} * & * \\ * & 0_{n-r} \end{pmatrix}$. Then the min-rank attack is available and its complexity is $O(q^{2r} \cdot n^4)$ (Tao et al. 2013). Moody et. al. (Moody et al. 2014, 2017) proposed an asymptotically optimal attack with the complexity $O(q^{r+2} \cdot n^4)$ based on the structure of subspace differential invariants. Recently, Liu (Liu et al. 2018) proposed a key recovery attack by solving a system of linear equations derived from the construction of the polynomials, and extended its key recovery attack to the rectangular ABC (Tao et al. 2015) and Cubic ABC (Ding et al. 2014). They claimed that the complexities of these attacks are with the complexity $O(n^{2w})$, which is critical for the security of ABC schemes. On the other hand, one of the anonymous reviewers on the present paper claimed in his/her report that its attack seems doubtful. He/She may present his/her opinion somewhere in the near future.

Table 1 Signature schemes

	$\#\{\text{var.}\}$	$\#\{\text{polyn.}\}$	Sig. gen.	Security
UOV	$o + v$	o	n^3	$q^{v-o} n^4$ (KS)
Rainbow	$o_1 + o_2 + v$	$o_1 + o_2$	n^3	$q^{\min(o_2+v-o_1, o_1)} n^4$ (KS, HR)
HFEv-	$n + r_v$	$n - r_-$	q^{3d}	$n^{(d+r_-+r_v+2)w}$ (MR)

Table 2 Encryption schemes

	$\#\{\text{var.}\}$	$\#\{\text{polyn.}\}$	Decrypt.	Security
HFE var.	$n - r_p$	$n + r_+ - r_-$	q^{3d+r_-}	$n^{(d+r_-+2)w}$ (MR)
Eflash	$n - r_p$	$n - r_-$	$q^{r-} n^3$	$n^{(r_-+3)w}$ (MR)
HFERP var.	$n - r_p$	$n + l + r_+ - r_-$	$q^{3d_0+r_-}$	$(n + l)^{(d_0+r_-+2)w}$ (MR)
ZHFE var.	$n - r_p$	$2n + r_+ - r_-$	q^{3d+r_-}	$(2n)^{(d+r_-+3)w}$ (MR)
EFC var.	$n - r_p$	$2n + r_+ - r_-$	$q^{r-} n^3$	$(2n)^{(r_-+3)w}$ (MR)
ABC	r^2	$2r^2$	n^3	n^{2w} (Liu et. al.)

4 Conclusion

In Sect. 2, we describe the multivariate schemes UOV, Rainbow, HFE variants and the corresponding second round candidates of NIST's project. In Sect. 3, we discuss the practicalities of several new multivariate encryption schemes proposed recently. Tables 1 and 2 are rough sketches of the complexities of decryption/signature generation and the major attacks for the corresponding schemes. Remark that there are various other attacks concerned for implementations.

Table 1 shows that practical signature schemes can be implemented easily since signatures can be generated in polynomial time and the proposed attacks are in exponential time. On the other hand, Table 2 shows that the issues on the practicality of HFE variants have not been eliminated on the new encryption schemes. While selecting parameters for 80-, 100-, 120-bit securities on such encryption schemes might be possible, they will not be able to follow the future inflation of security levels. Further drastic approaches will be required to construct practical multivariate encryption schemes.

Acknowledgements The author would like to thank the anonymous reviewer(s) for reading the previous draft and giving helpful comments. He was supported by JST CREST no.JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

- 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
- 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)
- E.R. Berlekamp, Factoring polynomials over finite fields. *Bell Syst. Tech. J.* **46**, 1853–1859 (1967)
- E.R. Berlekamp, Factoring polynomials over large finite fields. *Math. Comput.* **24**, 713–735 (1970)
- L. Bettale, J.C. Faugère, L. Perret, Solving polynomial systems over finite fields: improved analysis of the hybrid approach. *ISSAC 2012*, 67–74 (2012)
- L. Bettale, J.C. Faugère, L. Perret, Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes Cryptogr.* **69**, 1–52 (2013)
- W. Beullens, B. Preneel, A. Szepieniec, F. Vercauteren, LUOV, an MQ signature scheme, <https://www.esat.kuleuven.be/cosic/pqcrypto/luov/>
- D. Cabarcas, D. Smith-Tone, J.A. Verbel, Key recovery attack for ZHFE, in *PQCrypto'17*. LNCS, vol. 10346 (2017), pp. 289–308
- R. Cartor, D. Smith-Tone, An updated security analysis of PFLASH, in *PQCrypto'17*. LNCS, vol. 10346 (2017), pp. 241–254
- R. Cartor, D. Smith-Tone, EFLASH: a new multivariate encryption scheme, in *SAC'18*. LNCS, vol. 11349 (2018), pp. 281–299
- A. Casanova, J.C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem, GeMSS: a great multivariate short signature, <https://www.polsys.lip6.fr/Links/NIST/GeMSS.html>
- 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>
- M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, P. Schwabe, From 5-pass MQ-based identification to MQ-based signatures, in *Asiacrypt'16*. LNCS, vol. 10032 (2016), pp. 135–165

- M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, P. Schwabe, MQDSS, Post-quantum signature, <http://mqdss.org/contact.html>
- 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
- J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Rainbow-Round2.zip>
- J. Ding, T.J. Hodges, Inverting HFE systems is quasi-polynomial for all fields, in *Crypto'11*. LNCS, vol. 6841 (2011), pp. 724–742
- J. Ding, A. Petzoldt, L.-C. Wang, The cubic simple matrix encryption scheme, in *PQCrypto'14*. LNCS, vol. 8772 (2014), pp. 76–87
- J. Ding, D. Schmidt, Rainbow, a new multivariate polynomial signature scheme, in *ACNS'05*. LNCS, vol. 3531 (2005), pp. 164–175
- J. Ding, Z. Zhang, J. Deaton, K. Schmidt, Vishakha, A new attack on the LUOV schemes, in *Second PQC Standardization Conference* (2019), <https://csrc.nist.gov/events/2019/second-pqc-standardization-conference>
- V. Dubois, N. Gama, The degree of regularity of HFE systems, in *Asiacrypt'10*. LNCS, vol. 6477 (2010), pp. 557–576
- J.C. Faugère, A new efficient algorithm for computing Grobner bases (F_4). *J. Pure Appl. Algebra* **139**, 61–88 (1999)
- 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
- P.A. Fouque, L. Granboulan, J. Stern, Differential cryptanalysis for multivariate schemes, in *Eurocrypt'05*. LNCS, vol. 3494 (2005), pp. 341–353
- L. Granboulan, A. Joux, J. Stern, Inverting HFE is quasipolynomial, in *Crypto'06*. LNCS, vol. 4117 (2006), pp. 345–356
- Y. Hashimoto, Multivariate public key cryptosystems, in *Mathematical Modelling for Next-Generation Cryptography* (Springer, Berlin, 2017), pp. 17–42
- Y. Hashimoto, High-rank attack on HMFev. *JSIAM Lett.* **10**, 21–24 (2018)
- Y. Hashimoto, Key recovery attack on Circulant UOV/Rainbow. *JSIAM Lett.* **11**, 45–48 (2019)
- Y. Hashimoto, Y. Ikematsu, T. Takagi, Chosen message attack on multivariate signature ELSA at Asiacrypt, in *IWSEC'18*. LNCS, vol. 11049 (2018), pp. 3–18
- R.A. Horn, R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, 1985)
- M.-D.A. Huang, M. Kusters, Y. Yang, S.L. Yeo, On the last fall degree of zero-dimensional Weil descent systems. *J. Symb. Comput.* **87**, 207–226 (2018)
- Y. Ikematsu, R.A. Perlner, D. Smith-Tone, T. Takagi, J. Vates, HFERP - a new multivariate encryption scheme, in *PQCrypto'18*. LNCS, vol. 10786 (2018), pp. 396–416
- A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, in *Eurocrypt'99*. LNCS, vol. 1592 (1999), pp. 206–222, extended in <http://www.goubin.fr/papers/OILLONG.PDF> (2003)
- A. Kipnis, A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, in *Crypto'99*. LNCS, vol. 1666 (1999), pp. 19–30
- A. Kipnis, A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, in *Crypto'98*. LNCS, vol. 1462 (1998), pp. 257–267
- J. Liu, Y. Yu, B. Yang, J. Jia, S. Wang, H. Wang, Structural key recovery of simple matrix encryption scheme family. *Comput. J.* **61**, 1880–1896 (2018)
- 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
- H. Miura, Y. Hashimoto, T. Takagi, Extended algorithm for solving underdefined multivariate quadratic equations, in *PQCrypto'13*. LNCS, vol. 7932 (2013), pp. 118–135
- D. Moody, R. Perlner, D. Smith-Tone, An asymptotically optimal structural attack on the ABC multivariate encryption scheme, in *PQCrypto'14*. LNCS, vol. 8772 (2014), pp. 180–196

- D. Moody, R. Perlner, D. Smith-Tone, Improved attacks for characteristic-2 parameters of the cubic ABC simple matrix encryption scheme, in *PQCrypto'17*. LNCS, vol. 10346 (2017), pp. 255–271
- NIST, Post-quantum cryptography standardization, <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization>
- NIST, Post-quantum cryptography, round 2 submissions, <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions>
- J. Patarin, Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88, in *Crypto'95*. LNCS, vol. 963 (1995), pp. 248–261
- J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, in *Eurocrypt'96*. LNCS, vol. 1070 (1996), pp. 33–48
- J. Patarin, The oil and vinegar signature scheme, in *the Dagstuhl Workshop on Cryptography* (1997)
- J. Patarin, N. Courtois, L. Goubin, Quartz, 128-bit long digital signatures, in *CT-RSA'01*. LNCS, vol. 2001 (2020), pp. 282–297
- Z. Peng, S. Tang, Circulant UOV: a new UOV variant with shorter private key and faster signature generation. *KSII Trans. Int. Inf. Syst.* **12**, 1376–1395 (2018)
- R. Perlner, D. Smith-Tone, Security analysis and key modification for ZHFE, in *PQCrypto'16*. LNCS, vol. 9606 (2016), pp. 197–212
- A. Petzoldt, M.S. Chen, J. Ding, B.Y. Yang, HMFev - An efficient multivariate signature scheme, in *PQCrypto 2017*. LNCS, vol. 10346 (2017), pp. 205–223
- J. Porras, J. Baena, J. Ding, ZHFE, a new multivariate public key encryption scheme, in *PQCrypto'14*. LNCS, vol. 8772 (2014), pp. 229–245
- B. Preneel, NESSIE project announces final selection of crypto algorithms, https://www.cosic.esat.kuleuven.be/nessie/deliverables/press_release_feb27.pdf
- 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
- K.-A. Shim, C.-M. Park, N. Koo, An existential unforgeable signature scheme based on multivariate quadratic equations, in *Asiacrypt'17*. LNCS, vol. 10624 (2017), pp. 37–64
- 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>
- A. Szepieniec, 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
- C. Tao, A. Diene, S. Tang, J. Ding, Simple matrix scheme for encryption, in *PQCrypto 2013*. LNCS, vol. 7932 (2013), pp. 231–242
- C. Tao, H. Xiang, A. Petzoldt, J. Ding, Simple matrix - a multivariate public key cryptosystem (MPKC) for encryption. *Finite Fields Their Appl.* **35**, 352–368 (2015)
- E. Tomae, C. Wolf, Solving underdetermined systems of multivariate quadratic equations revisited, in *PKC'12*. LNCS, vol. 7293 (2012), pp. 156–171
- J. Vates, D. Smith-Tone, Key recovery attack for all parameters of HFE-, in *PQCrypto'17*. LNCS, vol. 10346 (2017), pp. 272–288
- 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

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.