Theoretical Computer Science 809 (2020) 372–383

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

A new encryption scheme for multivariate quadratic systems

Jiahui Chen [a], Jianting Ning [b,*], Jie Ling [a], Terry Shue Chien Lau [c], Yacheng Wang [d]

[a] *School of Computers, Guangdong University of Technology, Guangzhou 510006, China*
[b] *School of Mathematics and Computer Science, Fujian Normal University, China*
[c] *Temasek Laboratories, National University of Singapore, Singapore*
[d] *Department of Mathematical Informatics, University of Tokyo, Bunkyo-ku, Toyko, Japan*

ARTICLE INFO

Article history:
Received 19 October 2018
Received in revised form 24 November 2019
Accepted 29 December 2019
Available online 7 January 2020
Communicated by G. Yang

Keywords:
Multivariate public cryptography
Post-quantum cryptography
Encryption scheme
Rainbow

ABSTRACT

It is regarded as a difficult task to design a secure MPKC fundamental schemes such as an encryption scheme. In this paper we introduce a new central trapdoor for multivariate quadratic (MQ) public-key cryptosystems that allows for encryption, in contrast to time-tested MQ primitives such as Unbalanced Oil and Vinegar or Rainbow which only allow for signatures. The same as UOV or Rainbow, our construction is single field scheme where the central polynomial system is chosen to have a particular structure that enables efficient inversion. After applying this transformation, the plaintext can be recovered by solving a linear system. Our new central trapdoor can use to replace the broken extension field calculation trapdoor and simple matrix encryption trapdoor, thereafter, we use the minus and plus modifiers to inoculate our scheme against known attacks. It is highlight that our encryption scheme is a good explore in the area of multivariate cryptography. Finally, a straightforward Magma implementation confirms the efficient operation of the public key algorithms.

1. Introduction

In post-quantum era, with the emergence of the powerful quantum computers, traditional public key algorithms based on traditional number theory will be extremely vulnerable. Popular algorithms such as RSA, ECC, Elgamal will be broken in a polynomial time according to Shor's algorithm [40]. The increasing importance of research in this area has recently been emphasized by a number of authorities. For example, the American National Security Agency (NSA) has recommended governmental organizations to change their security infrastructures from schemes like RSA to post quantum schemes and the National Institute of Standards and Technologies (NIST) is preparing to standardize these schemes in December of 2016, where it published an open call for proposals for new post-quantum standards for some of the most critical security applications in digital communication infrastructure.

According to NIST standardization, one of the main candidates for this standardization is multivariate cryptography. Multivariate schemes are in general very fast and require only modest computational resources, which makes them attractive for the use on low cost devices like smart cards and RFID chips. Additionally, at least in the area of digital signatures, there

[*] Corresponding author.
E-mail address: jtning88@gmail.com (J. Ning).

https://doi.org/10.1016/j.tcs.2019.12.032

exists a large number of practical multivariate schemes such as PSfalsh [6], Gui [36], UOV [26], Rainbow [19] and MQDSS [10].

Traditionally, basing on the four basic schemes MI [29], HFE [31], STS [45] and UOV [26], the MQ public key cryptosystems are divided in four groups. The first two are known as mixed field and they use a ground field and an extension field to construct the trapdoor. The last two are single field systems, and the trapdoor is constructed only in one field with some specific structure. In addition, one uses the Plus method, the Minus method and the Perturbed method to modify MI and HFE. Therefore, there are many variant schemes, such as Sflash [1], C*-+ [34], PMI [15], PMI+ [16], HFE- [30], HFE+ [30], IPHFE [18], HFEv [26,18], Quartz [32] and so on. It is clear that secure MPKC schemes are extremely rare. Recently, researchers have proposed some new multivariate cryptosystems, such as HLY-2012 scheme [25], YTS-2013 scheme [47], ABC [43], matrix-based Rainbow [46], YTS-2014 scheme [48], cubic-ABC [17], ZHFE [37], RGB [39], HS-Sign [9]. However, we need more time to verify their securities. Also, current focus on MPKC is developing "advanced" cryptosystems, such as threshold ring signature scheme [35], proxy signature [42], identity-based signature [7] and online/offline signature [8].

It is regarded as a difficult task to design a secure MPKC fundamental schemes such as an encryption scheme or key exchange scheme. Encryption schemes have been the bane of multivariate quadratic cryptography. No MQ encryption scheme has withstood the test of time, while several MQ signature schemes have. For example, Porras et al. proposed a new central trapdoor which they call ZHFE [37]. Up until this point, the extension field polynomial in HFE-based cryptosystem required the number of nonzero coefficients to be small and its degree to be relatively low, so as to allow efficient root calculation. The idea of Porras et al. exchanges this single low-degree polynomial for a pair of high-degree polynomials that make up the central map. However, not to mention its few key generation space estimated by Zhang et al. [49], ZHFE has been broken by Daniel Cabarcas currently [5] by key recover attack. Another promising encryption scheme in the area of MPKC is the simply ABC Encryption proposed by Tao et al. [43]. Despite ABC may occur decryption failure, the trapdoor is relatively strong and is the most promising encryption scheme. Also, ABC has been broken by Liu et al. currently [28] by structural attack.

Recently, Szepieniec et al. proposed a new central trapdoor for multivariate quadratic systems, based on mixed-field operation call Extension Field Cancellation (EFC) [41]. Unlike other schemes in the mixed-field area such as HFE, its inversion is quite fast, since the plaintext can be recovered by solving a linear system. To sum up, assume the number of variate is n, the inversion is equation to solve a linear system with $2n$ variate in $2n$ equations, and the complexity is only $8n^3$.

So far as we know, ABC and EFC are the existing possible encryption scheme in MPKC, but they both have been broken currently. Due to this limitation, developing an other encryption scheme in this area is the most urgent thing.

Our contributions. We introduce a new central trapdoor for multivariate quadratic encryption schemes. Our proposal is a single-field scheme similar to the ABC proposal. However, our proposal is notably different from its predecessors, where the restriction on the quadratic number of variate of this central polynomial was key both to their efficiency and to their demise; our proposal allows arbitrary number of variate and in addition our scheme will have smaller private key size. Our proposal allows for encryption, in stark contrast to most other members of the HFE, UOV or Rainbow family.

Our scheme has some similarity with the current promising encryption schemes (ABC and EFC).

Like the ABC encryption scheme, decryption of a ciphertext consists of essentially solving linear systems. This linear system is parameterized by the particular ciphertext or message: every possible ciphertext or message implicitly defines a unique linear system. Knowledge of the private key allows the user to obtain the linear system efficiently, while the adversary who attacks the system without this crucial information has no advantage to solve the quadratic system.

Like EFC encryptions scheme, decryption of a ciphertext consists of essentially solving linear systems. While Gaussian elimination is in this case guaranteed to find a solution, this solution need not be unique.

What's more, all the three schemes has an important problem of decryption failure.

Finally, compare with ABC and EFC, our encryption scheme have the following benefits:

1. Our scheme is not only based on single field but also allows to choose arbitrary number of variate.
2. Our scheme has much smaller key size.
3. Our scheme reduces the blow-up factor between plaintext and ciphertext size to a value of 1.27 (while that of both ABC and EFC is 2).
4. Our scheme has lower decryption failure rate.

Table 1 summarize the comparison.

2. Definition and concept

The basic objects of multivariate cryptography are systems of multivariate quadratic equations over a finite field K. Such a system of m questions in n variables is defined as

$$\begin{cases} \sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij}^{(1)}\cdot x_i\cdot x_j+\sum_{j=i}^{n}\beta_i^{(1)}\cdot x_i+\gamma_i^{(1)}=0\\ \dots\\ \sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij}^{(m)}\cdot x_i\cdot x_j+\sum_{j=i}^{n}\beta_i^{(m)}\cdot x_i+\gamma_i^{(m)}=0. \end{cases} \tag{1}$$

The security of multivariate cryptosystems is based on the MQ-Problem which is defined as follows:

Table 1
Comparison with two current promising MPKC encryption schemes.

	Our scheme	EFC	ABC
Field	single field	mixed field	single field
Parameter choosing	$m=n+1-a+s$ n chooses arbitrarily	$m=2n-a$ a is small	$m=2n$ n grows quadratically
Inversion of central map	linear	linear	linear
Blow-up factor	1.27	2	2
Decryption failure rate	$1/q^{s-a+1}$	$1/q^{n-a}$	$1/q$
Public key size	$m(n+2)(n+1)/2$	$m(n+2)(n+1)/2$	$m(n+2)(n+1)/2$
(80 bit security)	134KB	375KB	2MB
Private key size	m^2+n^2+mn+ $s(n+2)(n+1)/2$	$7n^2+n$	m^2+3n^2
(80 bit security)	53.9KB	48.8KB	162.5KB
Encryption	$\mathcal{O}(n^3)$	$\mathcal{O}(n^3)$	$\mathcal{O}(n^3)$
Decryption	$\mathcal{O}(q^a n^3)$	$\mathcal{O}(q^a n^3)$	$\mathcal{O}(n^3)$

Definition 1. Given m quadratic polynomials $p_1, \ldots, p_m$ in n variables over a finite field $\mathbb{F}$, find a vector $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ such that $p_1(\mathbf{x}) = \ldots = p_m(\mathbf{x}) = 0$.

This problem is proven to be NP-hard even for quadratic systems over the field of two elements [33].

However, for most of the existing multivariate public key cryptosystems, the coefficients of the public system P (P is a collection of m quadratic polynomials $p_1, \ldots, p_m$ in n variables) are not chosen randomly. Instead one starts with an easily invertible quadratic map F (called central map) and combines it with two invertible affine maps S and T to get a public key of the form $P = S \circ F \circ T$. Therefore, the security of the scheme is based not only on the MQ-Problem, but also on the IP-Problem (defined as follows).

Definition 2. The Problem of Isomorphism of Polynomials (abbreviated *IP Problem*) is the problem to find an isomorphism (S, T) from P to F, where P and F are two public sets of u quadratic equations, and S and T are isomorphic.

There is not much knowledge about the hardness of the IP-Problem, and this is the main obstacle for researchers to give security proofs for their multivariate public key cryptosystems.

Usually, a MPKC encryption scheme on finite field $\mathbb{F}_q$ is built as:

$$P = S \circ F \circ T$$

in which F is a set of m quadratic multivariate equations in n variables which is constructed in such a way that it is also easy to invert. S is an affine transformation from $\mathbb{F}_q^m$ to $\mathbb{F}_q^m$ and T is an affine transformation from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$.

Encryption: To encrypt a message $d \in \mathbb{F}_q^n$, one simply computes $c = P(d)$. The ciphertext of the message d is $c \in \mathbb{F}_q^m$.

Decryption: To decrypt the ciphertext $c \in \mathbb{F}_q^m$, one computes recursively $x = S^{-1}(c)$, $y = F^{-1}(x)$ and $d = T^{-1}(y)$. $d \in \mathbb{F}_q^n$ is the plaintext corresponding to the ciphertext c.

For multivariate encryption schemes, we have $m \leq n$, the pre-image of the vector y under the central map F and therefore the decrypted plaintext is unique.

3. Modifiers

In the area of MPKC, one usually applies modifiers to make the encryption scheme secure. For example, the “minus” method to inoculate basic trapdoors against these attacks.

3.1. Minus method

The Minus method was first proposed and discussed in [38] and was utilized by Patarin and Matsumoto in [34]. We will see the instance in the case of Matsumoto-Imai scheme that eliminates the possibility of the linearization equation attack, if the Minus number a is not too small.

The“minus” modifier, which removes one or more polynomials from the public key [34], is more than just a countermeasure against Patarin’s attack. The results by Ding et al. [20] indicates that this modifier is much better considered as a fundamental building block of multivariate quadratic cryptosystems rather than a mere patch. That is, not only does the first application of this modifier block Patarin’s linearization attack; every repeated application increments by one the rank of the quadratic form associated with the extension field polynomial, rendering the MinRank attack due to Kipnis and Shamir [27] as well as its subsequent improvement by Courtois [13] that much more infeasible. Furthermore, this rank increase in turn increases the degree of regularity of the system, resulting in a similarly infeasible algebraic attack.

The use of this modifier will increase the cost of performance. More precisely, the decryption algorithm must first guess the values of the missing polynomials before inverting the output transformation T. Under this guess, it can proceed to the inversion system of the center map F and compute the potential matching plaintext x. If $P(x) = c$, then the correct plaintext was found. If not, then the guess was wrong and the algorithm must start all over again with a new one.

Fortunately, once the number of dropped polynomials a is small enough, the correct plaintext can still be found with overwhelming probability, and the resulting performance is still competitive.

3.2. Plus modifier

The plus modifier is to add a few, say s, randomly chosen polynomial components to a given multivariate scheme, and then mixing them into the public key through an invertible affine transformation. Clearly the degree of the plus polynomials should be chosen to be the same as the underlying scheme.

We would like to point out that originally the main purpose of the plus modifier was not to improve the security of the original scheme associated with F, but rather to make the map F, which is not injective, into an injective map, so that it can be used for encryption.

4. The basic idea of our encryption scheme

Let $m = n + 1$ and $C \in \mathbb{F}_q^{m\times n}$ be a random matrix over the base field $\mathbb{F}_q$ with elements $c_{i,j}$, where $i = 1, ..m, j = 1.., n$. Conditionally we let the resultant square matrix $RC \in \mathbb{F}_q^{n\times n}$ whose elements are $rc_{i,j} = 2(c_{i+1,j} - c_{i,j})$ be invertible, where $i, j = 1, .., n$.

Then we define the central trapdoor as follows:

$$F : \mathbb{F}_q^n \to \mathbb{F}_q^m : x \mapsto (\sum(x_j - c_{i,j})^2, i = 1, ..m, j = 1.., n).$$

More precisely, F is constructed as follows:

$$\begin{cases} f_1 = (x_1 - c_{1,1})^2 + (x_2 - c_{1,2})^2 + ... + (x_n - c_{1,n})^2 \\ f_2 = (x_1 - c_{2,1})^2 + (x_2 - c_{2,2})^2 + ... + (x_n - c_{2,n})^2 \\ ... \\ f_m = (x_1 - c_{m,1})^2 + (x_2 - c_{m,2})^2 + ... + (x_n - c_{m,n})^2 \end{cases}$$

To see how we are able to invert $F(\mathrm{x}) = \mathrm{d}$, we are dealing with a system as follows:

$$\begin{cases} (x_1 - c_{1,1})^2 + (x_2 - c_{1,2})^2 + ... + (x_n - c_{1,n})^2 = d_1 \\ (x_1 - c_{2,1})^2 + (x_2 - c_{2,2})^2 + ... + (x_n - c_{2,n})^2 = d_2 \\ ... \\ (x_1 - c_{m,1})^2 + (x_2 - c_{m,2})^2 + ... + (x_n - c_{m,n})^2 = d_m \end{cases}$$

If we subtract the above j-th equation from the $(j$ + 1)-th equation, $j = 1, 2, ..., m$, we obtain :

$$\begin{cases} 2(c_{2,1} - c_{1,1})x_1 + ... + 2(c_{2,n} - c_{1,n})x_n + (c_{1,1}^2 - c_{2,1}^2) + ... + (c_{1,n}^2 - c_{2,n}^2) \\ = d_1 - d_2 \\ ... \\ 2(c_{m,1} - c_{m-1,1})x_1 + ... + 2(c_{m,n} - c_{m-1,n})x_n + ... + (c_{m-1,n}^2 - c_{m,n}^2) \\ = d_{m-1} - d_m \end{cases}$$

By subtract one by one we are dealing with a linear system. Since RC is invertible, we will have one solution by Gaussian elimination. In fact, this inversion process is extremely fast.

However, the trapdoor as described above is insecure. In particular, it is broken by linear equation attack, minRank attack or an algebraic attack using fast Grobner basis algorithms.

Below we discuss why this trapdoor is insecure.

Without loss of generality, let us see only one polynomial f_1 in the construction, where

$$f_1 = (x_1 - c_{1,1})^2 + (x_2 - c_{1,2})^2 + ... + (x_n - c_{1,n})^2,$$

if we use matrix to express it, we have

$$f_1 = \begin{bmatrix} x_1 & \cdots & x_n & 1 \end{bmatrix} \circ \left[\begin{array}{ccc|c} & & & 0\\ & I_n & & \vdots\\ & & & 0\\ \hline C_{1,1} & \cdots & C_{1,n} & 1 \end{array}\right] \cdot \left[\begin{array}{ccc|c} & & & 0\\ & I_n & & \vdots\\ & & & 0\\ \hline 0 & \cdots & 0 & 0 \end{array}\right]$$

$$\cdot \left[\begin{array}{ccc|c} & & & C_{1,1}\\ & I_n & & \vdots\\ & & & C_{1,n}\\ \hline 0 & \cdots & 0 & 1 \end{array}\right] \circ \begin{bmatrix} x_1\\ \vdots\\ x_n\\ 1 \end{bmatrix}.$$

Let

$$F_1 = \left[\begin{array}{ccc|c} & & & 0\\ & I_n & & \vdots\\ & & & 0\\ \hline C_{1,1} & \cdots & C_{1,n} & 1 \end{array}\right] \cdot \left[\begin{array}{ccc|c} & & & 0\\ & I_n & & \vdots\\ & & & 0\\ \hline 0 & \cdots & 0 & 0 \end{array}\right] \cdot \left[\begin{array}{ccc|c} & & & C_{1,1}\\ & I_n & & \vdots\\ & & & C_{1,n}\\ \hline 0 & \cdots & 0 & 1 \end{array}\right].$$

Similarly, we express $f_2, ..., f_m$ with matrices, we have $F_2, ..., F_m$.

Next, assume the affine map S is $\left[\begin{array}{cc} M_S & 0\\ \hline C_S & 1 \end{array}\right]$, we apply affine map S to $\{f_1, ..., f_m\}$, and get

$$S(F_1) = \left[\begin{array}{c|c} & 0\\ M_S & \vdots\\ & 0\\ \hline C_S & 1 \end{array}\right] \cdot F_1 \cdot \left[\begin{array}{ccc|c} & {M_S}^t & & {C_S}^t\\ \hline 0 & \cdots & 0 & 1 \end{array}\right]$$

$$= \left[\begin{array}{c|c} & 0\\ M_S & \vdots\\ & 0\\ \hline C_S + (C_{1,1}, ..., C_{1,n}) & 1 \end{array}\right] \cdot \left[\begin{array}{ccc|c} & & & 0\\ & I_n & & \vdots\\ & & & 0\\ \hline 0 & \cdot & 0 & 0 \end{array}\right]$$

$$\cdot \left[\begin{array}{ccc|c} & {M_S}^t & & {C_S}^t + (C_{1,1}, ..., C_{1,n})^t\\ \hline 0 & \cdots & 0 & 1 \end{array}\right]$$

$$= \left[\begin{array}{c|c} M_S \circ {M_S}^t & M_S \circ C_S + (C_{1,1}, ..., C_{1,n})^t\\ \hline \{C_S + (C_{1,1}, ..., C_{1,n})\} & \{C_S + (C_{1,1}, ..., C_{1,n})\}\\ \circ {M_S}^t & \cdot \{C_S + (C_{1,1}, ..., C_{1,n})\}^t \end{array}\right].$$

Next, assume the matrix expression of the public map p_1 is P, the matrix expression of the affine map T is $\left[\begin{array}{cc} M_T & 0\\ \hline C_T & 1 \end{array}\right]$, since $S(F_1) = P_1(T^{-1})$, and P_1 is public known, if we choose random M_T and C_T, we have some linear equations relate to M_S and C_S.

Similarly, we consider $S(F_2), ..., S(F_m)$, we will get enough linear equations to solve M_S and C_S, together with M_T and C_T, we have equivalent partial private keys. More precisely, the total number of combined unknowns in the above linear equations is $N = n^3 + n^2 + n(n+1)/2 + n^2$ (we can treat the quadratic part of variables from M_s as a new variable). If we can select more than this number of linearly independent equations from $S(F_1) = P_1(T^{-1}), ..., S(F_m) = P_m(T^{-1})$, then solving the above system through linearization is easy. In fact, the total number of equations from this part is $(n+1)n^2$ under our design of trapdoor. However, once we use the minus method, there will not be enough equations to solve this problem. Know that the dropping polynomials can be relatively small, i.e., 2 is enough.

Furthermore, the minRank attack can work as follows:

Let $P = S \circ (f_1, \cdots, f_m) \circ T$.

Let $P_1, \cdots, P_n$ be the matrices associated to public key polynomials.

Let $F_1, \cdots, F_n$ be the matrices associated to central map polynomials.

Then we have $F_i - F_j = S \circ (T^{-1}(P_i - P_j) \circ (T^{-1})^{transpose})$, since the rank of matrix $F_i - F_j$ is two, so we can use minrank attack to break the encryption scheme.

Also, the grobner basis algorithms can work after we estimate this trapdoor.

Fortunately, the minus method can also solve these two problems. In Section 6, we will discuss why the minus method to avoid this insecurity.

5. Our new encryption scheme

Based on the above, we can summarize our new encryption scheme as follows:

Let $m = n + 1 - a + s$, F be a polynomial mapping whose components are $f_1, ..., f_{n+1} \in \mathbb{F}_q[x_1, ...x_n]$ as above. Randomly choose s quadratic polynomials $p_1, ..., p_s \in \mathbb{F}_q[x_1, ...x_n]$. Define three invertible affine transformations $S : \mathbb{F}_q^m \to \mathbb{F}_q^m, T : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Let the map $\overline{F}^{+-} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be as follows:

$$\overline{F}^{+-} = S \circ (f_1, .., f_{n+1-a}, p_1, ..., p_s) \circ T = (\overline{f}_1, ..., \overline{f}_m).$$

Then our encryption scheme has the following structure.

Public Key

The field $\mathbb{F}_q$ including its additive and multiplicative structure;

The $m = n + 1 - a + s$ quadratic polynomials $\overline{F}^{+-} = (\overline{f}_1, ..., \overline{f}_m)$.

Private Key

The matrix C, the degree two polynomials $p_1, ..., p_s$;

The two invertible affine transformations S and T.

Encryption

Given a plaintext $(x_1, ..., x_n) \in \mathbb{F}_q^n$, calculate $(y_1, ..., y_m) \in \mathbb{F}_q^m$ with the public polynomials:

$$(y_1, ..., y_m) = \overline{F}^{+-}(x_1, ..., x_n).$$

Decryption

To decrypt a message we execute the following steps:

1. Calculate $(z_1, ..., z_m) = S^{-1}(y_1, ..., y_m)$;
2. For each $\omega = (\omega_1, ..., \omega_a) \in \mathbb{F}_q^a$, compute

   $$u_\omega = (u_1, ..., u_n) = F^{-1}(z_1, ..., z_{n+1-a}, \omega_1, ..., \omega_a),$$

   and define $U = \{(\omega, u_\omega) | \omega \in \mathbb{F}_q^a\}$.
3. For each $(\omega, u_\omega) \in U$, check whether

   $$p_i(u_\omega) = z_{n+1-s+i}$$

   holds for all $i = 1, ..., s$. Keep each t_ω that satisfy these criteria and discard the rest. If s is large enough, we should have only one element left, mark this element as $(u'_1, ..., u'_n)$.
4. Calculate $(x_1, ..., x_n) = T^{-1}((u'_1, ..., u'_n))$ and we get the plaintext.

6. Discuss the dropping polynomials

In this section, we will discuss how to choose a proper number of dropping polynomials a so that the minus method can help our scheme secure.

In the previous section, we discuss why this trapdoor is insecure according to the linear equation attack and why the minus method can help to avoid it.

Below we focus mainly on the most efficient attack on our system: the algebraic attack using efficient Grobner basis algorithms such as Faugere's F4 or F5 [21] [22].

For the complexity of these algorithms, in [2], Bettale et al. asserted that, for a semi-regular system, the computational complexity of F$_4$ is bounded by $\mathcal{O}\left(\left(t\binom{n+d_{reg}-1}{d_{reg}}\right)^{\omega}\right)$, where n is the number of variables, t is the number of equations, ω is a linear algebra constant and $2 \leq \omega \leq 3$, in general we set $\omega = 2$ for lower bound complexity and $\omega = 3$ for upper bound complexity. d_{reg} is the degree of regularity of the system, which is the index of the first non-positive coefficient in the Hilbert series $S_{m,n}$ with

Table 2
Result of experiments with direct attack on our scheme.

Parameters	Time (ms)	Memory (MB)	D_{reg}
$q=3, n=19, a=4, s=4$	64	83	4
$q=3, n=19, a=6, s=6$	423	188	5
$q=3, n=19, a=8, s=8$	4271	412	6
$q=3, n=19, a=10, s=10$	39820	1059	6
$q=3, n=19, a=12, s=12$	120000	ooM	7

Table 3
Result of experiments with direct attack on our scheme.

Parameters	Time (ms)	Memory (MB)	D_{reg}
$q=3, n=59, a=3, s=3$	240	105.9	3
$q=3, n=59, a=4, s=4$	520	630	4
$q=3, n=59, a=6, s=6$	4130	2990	6
$q=3, n=59, a=8, s=8$	34740	ooM	8
$q=3, n=59, a=10, s=10$	120000	ooM	10

$$S_{m,n} = \frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n},$$

where d_i is the degree of the i-th equation.

The running time of efficient Grobner basis algorithms is dominated by Gaussian elimination in the matrix of coefficients associated with the monomials of degree of regularity D_{reg}. In particular, the number of monomials of this degree is given by $T=\binom{n}{D_{reg}}$. And the total complexity is calculated by τT^2 with $\tau=\binom{n}{q}$. For example, if we let $q=3, n=59$ and we need to make sure $D_{reg}\geq 8$ to achieve 80 bit security.

However, the above result can only be used to check the system which is simi-regular. Since the original degree of regularity of our scheme is low, and since in our design we use the minus modifiers, the public key polynomial system of this trapdoor is not simi-regular at all.

So, to evaluate this degree of regularity, we carried out a number of experiments with MAGMA [4] v2.20-5, Tables 2 and 3 show the average results of our experiments to attack 1000 instances of our scheme for each set of parameters.

As Table 3 shows (ooM means that there occurs out of memory), the time and memory complexity increase as a grows. Also the memory increases as n grows which indicated that complexity is exponential. It is hard to evaluate how many dropping polynomials we should choose for the single field system. However, for the big systems, we can follow the results due to Ding et al. [20], who develop an upper bound for the degree of regularity of HFE systems. In this result, the degree of regularity D_{reg} is intricately depended on the rank r of the quadratic form associated with the extension field polynomial. More precisely, a application of the minus modifier effectively increases this rank by a. In addition, for small base fields, the degree of regularity is expected to lie near its upper bound:

$$D_{reg}\leq (q-1)(r+a)/2+2.$$

This argument can guide us to evaluate D_{reg} in a single quadratic form. So we will use this result to guide our choosing of a.

According to the theoretical and experiment analysis, we can see that the dropping polynomials a can be relatively small. Here we recommend $a\approx \log n+4$.

7. Discuss the failure rate

As long as the number of dropped polynomials a is small enough and the adding polynomials s is large enough, the correct plaintext will be found with overwhelming probability. In order for the decryption algorithm to produce the wrong plaintext upon decrypting the ciphertext, there must exist at least two guesses $g_1\in\mathbb{F}_q^a$ and $g_2\in\mathbb{F}_q^a$ such that both $(y;g_1)$ and $(y;g_2)$ are in the range of $\overline{F}$. It is statistically unlikely that there are multiple preimages. Under the simplifying heuristic that outputs of $\overline{F}$ are independent and uniformly distributed, which is certainly not the case but seems statistically close. More precisely, there are q^n distinct randomly distributed outputs of $\overline{F}$. So the probability that any two lie in any fixed particular coset of $\ker(\overline{F})$ is $1-(1-q^{-m})^{q^n}-q^{n-m}(1-q^{-m})^{q^n-1}$, which is approximately $q^{n-m}=q^{-s+a-1}$ when $m>n$. Consequently, as long as $a\ll s$, the probability of decryption failure remains astronomically small.

Only when a and s are quite approximate, is this probability noticeable; when s rises to practical values, this probability does indeed drop to zero.

To address decryption failures, we note that the probability estimate above is approximately q^{n-m}. We set a reasonable bound 2^B on the probability of decryption failure and may set $s=B/2lg(q)+a-1$ to achieve this bound.

8. Discuss the blow-up factor between plaintext and ciphertext

For all the previously proposed promising encryption schemes and their variants, i.e., ABC, CubicABC, ZHFE, EFC, the ciphertext is at least twice as large as the corresponding plaintext. In this section we analyze this blow-up factor and try to figure out the relationship between the parameter s and n.

To calculate this blow-up factor, we have

$$blow-up-factor = \frac{m}{n} = \frac{n+1-a+s}{n} = 1 + \frac{s-a+1}{n}.$$

According to the above analysis, $s-a+1$ affect the decryption failure rate and this should be large enough, since a can be as small as around $\log n$, to make a balance on the decryption failure rate and the blow-up factor, we recommend s should be one half of n.

Once we set an reasonable bound 2^B on the probability of decryption failure and may set $s = B/2lg(q) + a - 1$ to achieve this bound, the blow-up factor can be calculated as $1 + \frac{B}{2lg(q)n}$, which is obviously better than that of the current promising encryption schemes such as ABC or EFC.

9. Security analysis

There are three main cryptanalytic techniques that are applicable to multivariate cryptosystems. In a sense, all of these techniques are related to the rank. The MinRank key recovery attack has a complexity directly dependent on the Q-rank of the central map. The differential symmetry attack is relevant when the rank of the central map is minimal in the relevant algebra. The direct algebraic attack has a complexity dependent on the degree of regularity of the public key which is usually a linear function of the rank. We review each of these techniques.

9.1. MinRank

MinRank attack is based on the so-called MinRank problem [12] and an effective algorithm [24] which could solve this problem. The essence of the MinRank attack is finding a linear combination of the public multivariate polynomials' corresponding symmetric matrices which has minimum rank (precisely, it doesn't have to be the minimum rank but it should be less than the largest possible minimum rank).

Let H_i be the symmetric matrix representing the homogeneous quadratic part of the i-th public polynomial. In the MinRank attack one tries to find linear combinations $H = \sum_{i=1}^{m} \alpha_i H_i$ of the matrices representing the homogeneous quadratic parts of the public polynomials such that rank$(H) = r \le n$. While in the HighRank attack one tries to identify the variables appearing the lowest number of times in the central equations. To do this, one forms random linear combinations H of the matrices H_i, if H has nontrivial kernel, one checks if the solution set of equation $(\sum_{i=1}^{m} \lambda_i H_i) \cdot \ker H = 0$ has dimension $n - o$. In the case of our encryption scheme, one can find that all the matrices Q_i representing the homogeneous quadratic parts of the central equations have full rank n. And this prevents the MinRank attack. More precisely, the full rank rate in the associated central symmetric matrix is close to $\frac{q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)}{q^{n^2}}$ (equal to the full rank rate of random matrix).

Furthermore, let us consider a modified minRank attack can work as follows:

For the first $n+1-a$ matrices of both P and F,

Let $\overline{F}^{+-} = S \circ (f_1, \cdots, f_m) \circ T$.

Let $\overline{F}_1^{+-}, \cdots, \overline{F}_{n+1-a}^{+-}$ be the matrices associated to public key polynomials.

Let $F_1, \cdots, F_{n+1-a}$ be the matrices associated to central map polynomials.

we have $F_i - F_j = S' \circ (T^{-1} \circ (\overline{F}_i^{+-} - \overline{F}_j^{+-}) \circ (T^{-1})^{\mathrm{T}})$,

Since the rank of the first $n+1-a$ matrices $F_i - F_j$ is two, someone may argue that we can try to use minRank attack to break the encryption scheme.

However, in our construction, we drop a polynomials of our central map, thus the dropping polynomials increases the rank.

In fact, since the quadratic form associated with the central map is so sparse, the removal of one equation in general increases the rank by two.

Without lost of generation, we can let $P' = \{P_i\} = \{\overline{F}_{i+1}^{+-} - \overline{F}_i^{+-}\}$, $F' = \{F_i'\} = \{F_{i+1} - F_i\}$ with $i = 1, \ldots, m-1$. And we let S' be a $(m-1) \times (m-1)$ matrix corresponded to the matrix S.

Now we consider these P as our public key and the corresponding private key is S', F', T.

To focus on only the first $n-a$ matrices of our central map, we found the concept of equivalent public key proposed in [44] can help. Below we will give our analysis.

We express an actions of π by the following $(m-1) \times (m-1)$ matrix as follows:

$$\pi = \begin{bmatrix} I_{(n-a)\times(n-a)} & 0_{(s)\times(s)} \\ 0_{(s)\times(s)} & 0_{(n-a)\times(n-a)} \end{bmatrix}.$$

Let $R = \pi \circ S'$, and let $f = R \circ (T^{-1} \circ P \circ (T^{-1})^{\mathrm{T}})$.

Consider $R = \pi \circ S'$, then $R : \mathbb{F}_q^{m-1} \to \mathbb{F}_q^{m-1}$ is $n - a$ $\mathbb{F}_q$-linear. Then $R \circ f \circ T$ is said to be equivalent to our public key.

Then to see the impact of the dropping a polynomials, we need to find another equivalent public key with linear map being $m - 1$ $\mathbb{F}_q$-linear.

As we know by the proposition 2 in [14], if we let $ker(R)$ be the kernel of R, and let $\overline{\pi}(x) = \prod_{r \in ker(R)}(x - r)$, then there exists a nonsingular linear map $\overline{R}$ from $\mathbb{F}_q^{m-1}$ to $\mathbb{F}_q^{m-1}$ such that $Rx = \overline{R}\overline{\pi}x$.

Then, $P^* = \overline{R} \circ \overline{\pi} \circ f \circ T \circ x$ is equivalent to our public key P, and the corresponding private key is $\overline{R}$, $\overline{\pi} \circ f$ and T with $\overline{R}$ be $m - 1$ $\mathbb{F}_q$-linear.

Now we consider the new central map $\overline{f} = \overline{\pi} \circ f$ with $\overline{\pi}(x) = \prod_{r \in ker(R)}(x - r)$, by the result of [3], we need to find symmetric matrices $(H_1, ..., H_{m-1})$ such that $\overline{f}_i = \overline{x}H_i\overline{x}^{\mathrm{T}}$, where $(H_1, ..., H_{m-1}) = (M_{m-1}F'_1M^{\mathrm{T}}_{m-1}, ..., M_{m-1}F'_{m-1}M^{\mathrm{T}}_{m-1})M^{-1}_{m-1}$, where M_{m-1} is a matrix need to be discussed. Finally the minRank of our construction is now turning into the rank of $M_{m-1}F'_iM^{\mathrm{T}}_{m-1}M^{-1}_{m-1}$ with $i = 1, ..., n - a$.

When we consider our central map, we see that F'_i has rank 2. If we assume that r is uniformly between a and $m - 1 - a$, then M_{m-1} has minRank $2(a + 1)$.

Finally, by the analysis in [23], the complexity of solving this MinRank problem is given by $\mathcal{O}\left(\binom{m + d_{reg}}{d_{reg}}^{\omega}\right)$ where d_{reg} is already discuss above and ω is the linear algebra constant.

9.2. Differential techniques

A second class of attacks that has proven effective against big field schemes is the family of differential attacks involving the recovery of a symmetric relation to remove the minus modifier, or as a tool for accessing a low Q-rank. The discrete differential of a function $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is the bivariate function

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

The differential operation D is linear and acts in many ways like a derivative; i.e., the differential of a $\mathbb{F}_q$-quadratic map is $\mathbb{F}_q$-bilinear, the differential of a $\mathbb{F}_q$-cubic function is $\mathbb{F}_q$-bi-quadratic, etc.

Differential attacks have been the basis of several cryptanalyses. The two basic techniques are linear differential symmetry attacks and differential invariant attacks. Linear differential symmetry attacks attempt to find linear maps L that “factor through” the differential of the central map in an interesting way. Specifically, the goal is to find maps L satisfying

$$Df(La, x) + Df(a, Lx) = \Lambda_L Df(a, x).$$

If such a map can be found, it allows one to “remove” the minus modifier by discovering new linear combinations of the central maps that are linearly independent of the public key.

The above attack has broken SFLASH, it works efficiently for big field scheme (only one variate). For single field scheme, the differential attacks need to be modified. We express the differential as an n-tuple of differential coordinate forms in the following way: $[Df(a, x)]_i = a^T Df_i x$, where Df_i is a symmetric matrix representation of the action on the ith coordinate of the bilinear differential. In such way, the differential techniques try to find the invariant space of the public key. Specifically, if a large subspace of the public key has the property that the matrices representing the functions as quadratic form map a particular subspace V simultaneously into another subspace W of the same dimension, then any projection producing two full rank differentials Df_1 and Df_2 allow one an advantage in recovering V, since V is left invariant by $Df_1 Df_2^{-1}$. Then this modified differential attack model, the invariant attacks, use the low rank structure on a large subspace of the public key to enhance the linear algebra search version of MinRank. However, as we have mentioned above, our scheme prevents the MinRank attack.

9.3. Algebraic attacks

There are many algebraic attack algorithms working on MPKCs, such as XL [11] and Gröbner Basis algorithms such as F_4, and F_5. The idea of direct attack on our scheme is to add $n - m$ linear equations. In this way, the number of variables can be reduced to m so as to create a determined system. On the other hand, a system with n variables and m equations is expected to have $q^{(n-m)}$ solutions on average. Therefore, adding a total of $n - m$ linear equations will lead to one solution on average. Repeating this experiment a few times, we will find at least one solution.

As we have mentioned in Section 6, our scheme now can protect algebraic attacks once we choose the proper number of dropping polynomials.

10. Complexity

The public key consists of m quadratic polynomials in n variables. Thus the number of coefficients from $\mathbb{F}_q$ in the public key is $m \times (n + 2)(n + 1)/2$. However, we note that there is a considerable amount of redundancy in the public key which we expect can be exploited to produce smaller keys such as using cyclic modifier or equivalent key.

Table 4
Parameters and performance of our scheme at the 80-bit and 128-bit quantum security levels.

Scheme and Parameters	PK (KB)	SK (KB)	enc. (ms)	dec. (ms)	Blow-up Factor	Dec. Failure
(q=3, n=59, a=10, s=25)	134	53.9	43	124192	1.27	2^{-32}
(q=3, n=83, a=12, s=27)	345	108	187	782912	1.19	2^{-32}

The private key consists of two linear transformations S and T, the matrix C, along with s random polynomials. This amounts to $m^2+n^2+mn+s(n+2)(n+1)/2$.

The most computationally intensive part of the key generation algorithm is the polynomial multiplication part which is similar to other basic MPKC schemes. The total time complexity of the key generation to $\mathcal{O}(n^3)$.

Encryption consists of evaluating m quadratic polynomials in n variables. This comes down to two time steps with unlimited parallelism. Without parallelism, however, each of the $m \times (n(n-1)+2n)$ base field operations must be executed sequentially and the time complexity is therefore $\mathcal{O}(n^3)$.

Decryption consists of the following steps for q^a different guesses, which may be executed in parallel if the resources are available:

1. Inversion of S, which requires m^2 operations;
2. A Gaussian elimination of some n^3 operations;
3. Pruning, which has an almost constant expected running time.
4. Inversion of T requiring some n^2 operations;

Thus, decryption has an expected running time of $\mathcal{O}(q^a n^3)$. While this expression does involve an exponential factor, the exponent is rather small: on the recommend of $a \approx \log n$, decryption is still practically speaking a polynomial-time algorithm. See Table 1 to view the summary of above.

11. Practical parameters for our scheme

According to the above analysis in Section 7, 6, 8 and Section 10, we suggest the parameter set $q=3, n=59, a=10, s=25$ for 80 bit security and $q=3, a=12, n=83, s=27$ for 128 bit security.

12. Running time of our scheme

To further show the efficiency of our scheme, we run our scheme in MAGMA V2.19, with the hardware and software below: a workstation with a Dual XEON Quad Core 2.27 GHz processor, 24 GB of main random access memory and the operation system is Scientific Linux 5.11 (Boron). The result is summarized in Table 4.

13. Conclusions

In this chapter, we propose a new idea for trapdoor in MQ cryptosystems in order to use the benefits of polynomials substraction. After our construction, the plaintext can be obtained by solving a linear system. We anticipate several known attacks and use the minus modifiers to inoculate our trapdoor against these attacks, and finally get an efficient encryption scheme. We estimate parameters associated with 80 bits of security from the running time of an algebraic attack and offer some experimental validation of its complexity. Our implementation confirms the correctness of our schemes as well as their practical efficiency. Encryption can be done in only a few milliseconds, however, due to the missing information from the minus modifier, decryption takes several seconds.

The minus modifier is an obvious candidate for improvement. When it is necessary for security, any number of dropped polynomials constitutes an large cost on the decryption function because its running time is exponential in this number. In the future work, we will concentrate in other modifiers that can enhance the security, i.e., Oil and Vinegar modifier. Since it is obvious that any alternative modifier that has the same effect on security but reduce the need for exhaustive search can drastically accelerate decryption.

Declaration of competing interest

The authors claim that there is no conflict of interest.

Acknowledgement

This work is supported by the Key Areas Research and Development Program of Guangdong Province (grant 2019B010139002), the National Natural Science Foundation of China (61972094 and 61902079), the Shanghai Natural Science Foundation Project (grant 18ZR1417300) and the project of Guangzhou Science and Technology (grant 201902020006 and 201902020007). We also would like to thank Yacheng Wang from University of Tokyo, who help us discuss the attacks on our scheme and the evaluation of the degree of regularity.

References

[1] M. Akkar, N. Courtois, R. Duteuil, L. Goubin, A fast and secure implementation of sflash, in: Public Key Cryptography - PKC 2003, 6th International Workshop on Theory and Practice in Public Key Cryptography, Miami, FL, USA, January 6-8, 2003, Proceedings, 2003, pp. 267–278.

[2] L. Bettale, J. Faugère, L. Perret, Hybrid approach for solving multivariate systems over finite fields, J. Math. Cryptol. 3 (3) (2009) 177–197, https://doi.org/10.1515/JMC.2009.009.

[3] L. Bettale, J.-C. Faugère, L. Perret, Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic, Des. Codes Cryptogr. 69 (1) (Oct 2013) 1–52, https://doi.org/10.1007/s10623-012-9617-2.

[4] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, J. Symb. Comput. 24 (3–4) (1997) 235–265, http://www.sciencedirect.com/science/article/pii/S074771719690125X.

[5] D. Cabarcas, D. Smith-Tone, J.A. Verbel, Key Recovery Attack for ZHFE, Springer International Publishing, Cham, 2017, pp. 289–308.

[6] R. Cartor, D. Smith-Tone, An Updated Security Analysis of PFLASH, Springer International Publishing, Cham, 2017, pp. 241–254.

[7] J. Chen, J. Ling, J. Ning, J. Ding, Identity-based signature schemes for multivariate public key cryptosystems, Comput. J. 62 (8) (2019) 1132–1147, https://doi.org/10.1093/comjnl/bxz013.

[8] J. Chen, S. Tang, D. He, Y. Tan, Online/offline signature based on uov in wireless sensor networks, Wirel. Netw. 23 (6) (Aug 2017) 1719–1730, https://doi.org/10.1007/s11276-016-1245-8.

[9] J. Chen, S. Tang, X. Zhang, Hs-sign: a security enhanced uov signature scheme based on hyper-sphere, KSII Trans. Int. Inf. Syst. 11 (6) (2017) 3166–3187.

[10] M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, P. Schwabe, From 5-pass mq-based identification to mq-based signatures, in: J.H. Cheon, T. Takagi (Eds.), Advances in Cryptology – ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016, pp. 135–165.

[11] N. Courtois, A. Klimov, J. Patarin, et al., Efficient algorithms for solving overdefined systems of multivariate polynomial equations, in: B. Preneel (Ed.), Advances in Cryptology -EUROCRYPT 2000, in: Lecture Notes in Computer Science., vol. 1807, Springer Berlin Heidelberg, 2000, pp. 392–407.

[12] N.T. Courtois, Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001, pp. 402–421.

[13] N.T. Courtois, The Security of Hidden Field Equations (HFE), Springer Berlin Heidelberg, Berlin, Heidelberg, 2001, pp. 266–281.

[14] T. Daniels, D. Smith-Tone, Differential properties of the hfe cryptosystem, in: M. Mosca (Ed.), Post-Quantum Cryptography, Springer International Publishing, Cham, 2014, pp. 59–75.

[15] J. Ding, A new variant of the matsumoto-imai cryptosystem through perturbation, in: Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004, 2004, pp. 305–318.

[16] J. Ding, J.E. Gower, Inoculating multivariate schemes against differential attacks, in: Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings, 2006, pp. 290–301.

[17] J. Ding, A. Petzoldt, L. Wang, The cubic simple matrix encryption scheme, in: Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014, Proceedings, 2014, pp. 76–87.

[18] J. Ding, D. Schmidt, Cryptanalysis of hfev and internal perturbation of HFE, in: Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, 2005, pp. 288–301.

[19] J. Ding, D. Schmidt, Rainbow, a new multivariable polynomial signature scheme, in: Applied Cryptography and Network Security, Springer, 2005, pp. 164–175.

[20] J. Ding, B.-Y. Yang, Degree of Regularity for HFEv and HFEv-, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 52–66.

[21] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F_4), J. Pure Appl. Algebra 139 (1999) 61–88, http://www.sciencedirect.com/science/article/pii/S0022404999000055.

[22] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in: ACM ISSAC 2002, 2002, pp. 75–83.

[23] J.-C. Faugre, M.S.E. Din, P.-J. Spaenlehauer, On the complexity of the generalized minrank problem, J. Symb. Comput. 55 (2013) 30–58, http://www.sciencedirect.com/science/article/pii/S0747717113000485.

[24] L. Goubin, N.T. Courtois, Cryptanalysis of the TTM Cryptosystem, Springer Berlin Heidelberg, Berlin, Heidelberg, 2000, pp. 44–57.

[25] Y. Huang, F. Liu, B. Yang, Public-key cryptography from new multivariate quadratic assumptions, in: Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012, Proceedings, 2012, pp. 190–205.

[26] A. Kipnis, J. Patarin, L. Goubin, Unbalanced Oil and Vinegar signature schemes, in: J. Stern (Ed.), Advances in Cryptology -EUROCRYPT 99, in: Lecture Notes in Computer Science, vol. 1592, Springer Berlin Heidelberg, 1999, pp. 206–222.

[27] A. Kipnis, A. Shamir, Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization, Springer Berlin Heidelberg, Berlin, Heidelberg, 1999, pp. 19–30.

[28] J. Liu, Y. Yu, B. Yang, J. Jia, S. Wang, H. Wang, Structural key recovery of simple matrix encryption scheme family, Comput. J. 61 (12) (2018) 1880–1896.

[29] T. Matsumoto, H. Imai, Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, in: D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, C. Günther (Eds.), Advances in Cryptology -EUROCRYPT 98, in: Lecture Notes in Computer Science., vol. 330, Springer Berlin Heidelberg, 1988, pp. 419–453.

[30] J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, in: Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding, 1996, pp. 33–48.

[31] J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, in: U. Maurer (Ed.), Advances in Cryptology EUROCRYPT 96, in: Lecture Notes in Computer Science, vol. 1070, Springer Berlin Heidelberg, 1996, pp. 33–48.

[32] J. Patarin, N. Courtois, L. Goubin, Quartz, 128-bit long digital signatures, in: Topics in Cryptology - CT-RSA 2001, the Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8–12, 2001, Proceedings, 2001, pp. 282–297.

[33] J. Patarin, L. Goubin, Trapdoor one-way permutations and multivariate polynomials, in: Information and Communications Security, 1997, pp. 356–368.

[34] J. Patarin, L. Goubin, N. Courtois, C^{*}_{-+} and HM: variations around two schemes of T. Matsumoto and H. Imai, in: Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China, October 18–22, 1998, Proceedings, 1998, pp. 35–49.

[35] A. Petzoldt, S. Bulygin, J.A. Buchmann, A multivariate based threshold ring signature scheme, Appl. Algebra Eng. Commun. Comput. 24 (3–4) (2013) 255–275, https://doi.org/10.1007/s00200-013-0190-3.

[36] A. Petzoldt, M.-S. Chen, B.-Y. Yang, C. Tao, J. Ding, Design principles for hfev- based multivariate signature schemes, https://doi.org/10.1007/978-3-662-48797-6_14, 2015.

[37] J. Porras, J. Baena, J. Ding, Zhfe, a new multivariate public key encryption scheme, in: Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014, Proceedings, 2014, pp. 229–245.

[38] A. Shamir, Efficient signature schemes based on birational permutations, in: D.R. Stinson (Ed.), Advances in Cryptology — CRYPTO' 93: 13th Annual International Cryptology Conference Santa Barbara, California, USA, August 22–26, 1993, Proceedings, Springer Berlin Heidelberg, Berlin, Heidelberg, 1994, pp. 1–12.

[39] W. Shen, S. Tang, Rgb, a mixed multivariate signature scheme, Comput. J. 59 (4) (2016) 439–451, https://doi.org/10.1093/comjnl/bxv056.

[40] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (5) (1997) 1484–1509.

[41] A. Szepieniec, J. Ding, B. Preneel, Extension Field Cancellation: A New Central Trapdoor for Multivariate Quadratic Systems, Springer International Publishing, Cham, 2016, pp. 182–196.

[42] S. Tang, L. Xu, Towards provably secure proxy signature scheme based on isomorphisms of polynomials, Future Gener. Comput. Syst. 30 (2014) 91–97, http://www.sciencedirect.com/science/article/pii/S0167739X13001179.

[43] C. Tao, A. Diene, S. Tang, J. Ding, Simple matrix scheme for encryption, in: Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013, Proceedings, 2013, pp. 231–242.

[44] E. Thomae, C. Wolf, Cryptanalysis of enhanced tts, sts and all its variants, or: why cross-terms are important, in: A. Mitrokotsa, S. Vaudenay (Eds.), Progress in Cryptology - AFRICACRYPT 2012, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 188–202.

[45] C. Wolf, A. Braeken, B. Preneel, On the security of stepwise triangular systems, Des. Codes Cryptogr. 40 (3) (2006) 285–302, https://doi.org/10.1007/s10623-006-0015-5.

[46] T. Yasuda, J. Ding, T. Takagi, K. Sakurai, A variant of rainbow with shorter secret key and faster signature generation, in: Proceedings of the First ACM Workshop on Asia Public-Key Cryptography, AsiaPKC'13, Hangzhou, China, May 8, 2013, 2013, pp. 57–62.

[47] T. Yasuda, T. Takagi, K. Sakurai, Multivariate signature scheme using quadratic forms, in: Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013, Proceedings, 2013, pp. 243–258.

[48] T. Yasuda, T. Takagi, K. Sakurai, Efficient variant of rainbow using sparse secret keys, J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl. 5 (3) (2014) 3–13, http://isyou.info/jowua/papers/jowua-v5n3-1.pdf.

[49] W. Zhang, C.H. Tan, On the Security and Key Generation of the ZHFE Encryption Scheme, Springer International Publishing, Cham, 2016, pp. 289–304.