SCIENCE CHINA
Information Sciences

• RESEARCH PAPERS •

June 2011 Vol. 54 No. 6: 1161–1171
doi: 10.1007/s11432-011-4262-3

Extended multivariate public key cryptosystems with secure encryption function

WANG HouZhen[1,2], ZHANG HuanGuo[1,2]*, WANG ZhangYi[1,2] & TANG Ming[1,2]

[1]*The Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Computer, Wuhan University, Wuhan* 430079*, China;*
[2]*State Key Laboratory of Software Engineering, Wuhan University, Wuhan* 430072*, China*

Received May 1, 2010; accepted December 31, 2010

Abstract Advances in quantum computers pose great threats on the currently used public key cryptographic algorithms such as RSA and ECC. As a promising candidate secure against attackers equipped with quantum computational power, multivariate public key cryptosystems (MPKCs) have attracted increasing attention in recently years. Unfortunately, the existing MPKCs can only be used as a multivariate signature scheme, and it remains unknown how to construct an efficient MPKC enabling secure encryption. Furthermore, some multivariate signature schemes have been shown insecure in recent years, and it is also not trivial to build MPKC which can serve as a secure signature scheme. By employing the basic MQ-trapdoors, this paper proposes a novel MPKC and shows how it can be used as a multivariate signature scheme and a multivariate encryption scheme, respectively. The goal is achieved by incorporating our new hash authentication techniques and some modification methods such as the Shamir's minus method. Thorough analysis shows that our schemes are secure and efficient. Our MPKC gives a positive response to the challenges in multivariate public key cryptography.

Keywords cryptography, post-quantum cryptography, MQ problem, hash function

Citation Wang H Z, Zhang H G, Wang Z Y, et al. Extended multivariate public key cryptosystems with secure encryption function. Sci China Inf Sci, 2011, 54: 1161–1171, doi: 10.1007/s11432-011-4262-3

1 Introduction

Public key cryptography is an important tool for nowadays information society. Quantum computers have recently emerged as a threat to the modern public key cryptosystems. In 1994, Shor [1] presented polynomial-time algorithms for factoring integers and computing discrete logarithms on a quantum computer. This means that once a practical quantum computer is built, the most widely used public key cryptosystems (including RSA, ElGamal and ECC) will be no longer secure. The significant experimental results achieved thus far are the 7-qubit quantum computer built by IBM in 2001 [2], and 16-qubit quantum computer built by D-wave in 2007 and increased to 48-qubit in 2008 [3, 4]. Noting that the popular ECCs are implemented in finite cyclic groups in the size of about 160 bits [5], one may envision that the secure threats from quantum computers become increasingly realistic. Therefore, it is very essential to investigate alternative public key cryptosystems, i.e., post-quantum cryptosystems to withstand attacks from one equipped with quantum computation capacity in the near future.

*Corresponding author (email: liss@whu.edu.cn)

Great efforts have been devoted to post-quantum cryptography in the last decade. For instance, the International Workshop on Post-Quantum Cryptography has successfully held three meetings: PQCrypto-2006, PQCrypto2008 and PQCrypto2010. In the last ten years, as a promising candidate of post-quantum cryptosystems, multivariate public key cryptosystems (MPKCs) have recently received much attention. In addition to the strong security against quantum computing based attacks, MPKC schemes are usually much more efficient in computation than number theoretic-based schemes. Indeed, in the large body of proposed MPKC proposals, many are very suitable for "small" ubiquitous computing devices with limited computation capacity, e.g., embedded device, active RFID tags and mobile ad hoc networks [6].

In spite of the enjoyable advantages, more efforts are required to develop MPKCs for wide deployment in practice. Indeed, existing MPKCs can only be used as a multivariate signature scheme, and how to construct secure and efficient MPKCs enabling a secure multivariate encryption scheme remains an open problem. Furthermore, some multivariate signature schemes have been shown insecure in recent years, and it is also not trivial to build MPKC as a secure signature scheme. To response to these challenges for practical deployment of MPKCs, we propose a novel extended MPKC and show how it can be used to encrypt and sign messages, respectively. The goal is achieved by incorporating our novel hash authentication techniques and some modification methods into the basic MQ-trapdoors. Thorough analysis shows that our schemes are secure and efficient. These desirable features render our MPKC a promising solution to withstand quantum attacks without significant cost, applicable to even low-end device.

The remainder of this paper is organized as follows. Section 2 reviews MPKCs and summarizes the notations used throughout the paper. We describe a novel extended multivariate cryptosystem (EMC), and propose the EMC encryption scheme and the EMC signature scheme in section 3. Section 4 analyzes the security of our proposals. We implement three practical instances and evaluate their performance in section 5. Section 6 concludes the paper.

2 Preliminaries

2.1 Notations and conventions

For clarity, Table 1 summarizes the main notations and conventions used in the paper.

2.2 Description of MPKCs

A function F from $\mathbb{F}_q^n$ to $\mathbb{F}_q^m$ is defined by m quadratic polynomials in n variables, and coefficients are in $\mathbb{F}_q$, called the *central map* and its components called *central polynomials*. In most MPKCs, the public key is a map $P\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$, and obtained by hiding the cental map $F = (f_1, \ldots, f_m)$ via composition with two affine maps U, T, that is,

$$P = (p_1, \ldots, p_m) = T \circ F \circ U,$$

where $\circ$ denotes the composition of functions. We usually write, for $1 \leqslant j \leqslant k \leqslant n, 1 \leqslant i \leqslant m$,

$$p_i(x_1, \ldots, x_n) = \sum_{1 \leqslant j \leqslant k \leqslant n} c_{ijk} x_j x_k + \sum_{j=1}^{n} b_{ij} x_j + a_i, \tag{1}$$

where a_i is usually normalized to zero and coefficients $c_{ijk}, b_{ij} \in \mathbb{F}_q$.

In any given scheme, the central map F is usually chosen from a certain class of quadratic maps whose inverse can be computed efficiently. Then F is masked by two full-rank affine maps U, T such that the public map $P = T \circ F \circ U$ appears a random quadratic map. Note that P's inverse is difficult for one who does not know T and U. The key of an MPKC scheme is the design of the central map. The public key consists of the polynomials in P. In practice, it is always the collection of the coefficients of the p_i's. The secret key consists of the information in U, T and F, that is, U^{-1}, T^{-1} and F^{-1} (sometimes F can be discarded). This key generation paradigm is similar to that of most NP-hard problem based crypto-

Table 1 List of symbols

Symbol	Meaning
$\mathbb{F}_q$	a degree k extension of the field $\{0,1\}$, where $q=2^k$.
$\mathbb{F}_q^n$	n-dimensional vectorspace over $\mathbb{F}_q$.
$\mathbb{F}_{q^n}$	a degree n extension of the field $\mathbb{F}_q$.
$H(\cdot)$	a standard hash function such as SHA-1.
$H_k(\cdot)$	an operation extracting the first k bits of $H(\cdot)$ and mapping the bitstring into an element in $\mathbb{F}_q$.
$a\|\|b$	concatenation of variables a and b.
δ	the number of extended input variables of public key, where $0 \leqslant \delta < n$.
μ	the number of increased equations of the central map for the "encrypt" operation ($0 \leqslant \mu < \delta$), and the number of deleted equations of the central map for the "sign" operation ($-\delta < \mu \leqslant 0$).

systems such as McEliece cryptosystem [7]. Encryption and decryption processes are shown in Figure 2.

2.3 A survey of MPKCs

The security of MPKC schemes essentially depends on the two hard computational problems. One is based on solving a set of randomly chosen nonlinear multivariate polynomial equations over a finite field (called MQ problem). This problem is known to be NP-hard [8]; that is, given a ciphertext $y_1,\ldots,y_m$, finding a plaintext solution $x_1,\cdots,x_n$ from quadratic equations of formula (1) is computationally infeasible. Consequently, randomly chosen quadratic equations over finite field $\mathbb{F}_q$ like (1) is a one-way function. However, in order to allow legitimate users to easily decrypt the ciphertext, the central map F is not randomly chosen. Hence, two affine bijective transformations U,T are employed to mask the central map F as a hard one, i.e., the public key $P=T\circ F\circ U$. Here, P and F are the isomorphism of polynomials (IP). Clearly, if an attacker can find U and T from P, then the according MPKC is broken. However, to finish this task requires the attacker to solve the so-called IP-problem which has been shown to be NP-complete [9].

Generally speaking, MQ-problem and IP-problem cannot completely guarantee the security of MPKCs. By now, all basic trapdoors (including MIA, HFE, OV and STS) are insecure, and must be modified using some effective measures for enhancing their security. Wolf [10] summarized ten modifications. In these methods, only the minus method "–" proposed by Shamir [11] is believed to be secure and efficient. The idea of minus method is to enhance the security of basic multivariate schemes by removing the last r coordinates from the public key or its central map. Accordingly, the resulting MPKC as an encryption scheme runs q^r times slower than the original scheme.

Apart from Shamir's minus method, the plus method "+" and the Vinegar method "v" are believed to be slightly more secure, while the Homogenising method "h" has no effect on the security of the original scheme. The subfield method "/" and the branching method "$\perp$" are now known to be insecure. As to the Fixing method "f", the Sparse polynomials "s", the Internal perturbation "i" and the Masking "m", it remains unknown whether they have security effect on the original MPKC scheme.

With some modifications and enhancing approaches, dozens of variants have been derived from the four basic MQ trapdoors. However, most of these variants can only be used for signing messages. Furthermore, their security has been seriously challenged and many efficient attacks have been found [12]. Hence, there is a rather pressing need to investigate new MQ-trapdoors or new enhancing methodologies to construct MPKCs allowing secure encryption and signature. This observation motivates our work in this paper.

3 Extended multivariate public key cryptosystems

The key idea of EMC schemes is to increase a secret transformation L defined in subsection 3.1 in the outermost layer of the original MQ-trapdoor framework (Figure 1). More precisely, we use the map L and some modifications to hide the basic MQ-trapdoors into a larger algorithm space; that is, we change the original public key $P:\mathbb{F}^n\to\mathbb{F}^n$ into $P':\mathbb{F}^{n+\delta}\to\mathbb{F}^{n+\mu}(\delta>\mu)$. Accordingly, the asymmetry of input

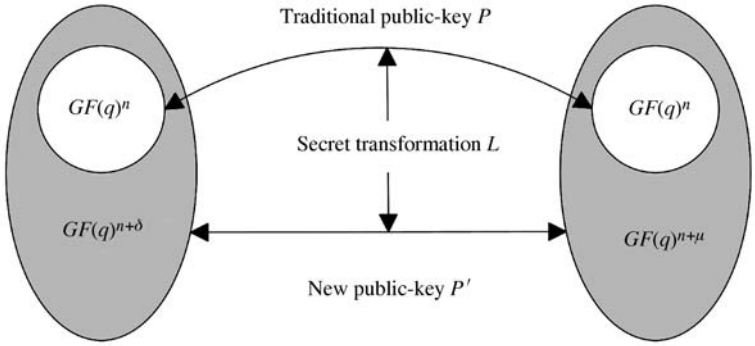

Figure 1 Illustration of design ideas for new schemes.

and output space can effectively demolish some potential mathematical properties of the original public key P.

3.1 Extended multivariate public key cryptosystems

We first define a Tame map $\Gamma : \mathbb{F}^n \to \mathbb{F}^n$,

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n-1} \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 + g_1(x_1) \\ \vdots \\ x_{n-1} + g_{n-2}(x_1, \ldots, x_{n-2}) \\ x_n + g_{n-1}(x_1, \ldots, x_{n-2}, x_{n-1}) \end{pmatrix}, \tag{2}$$

where g_i are arbitrary polynomials. Obviously, Γ can be easily inverted assuming that the g_i are known [12]. However, from the perspective of cryptography, a Tame map cannot be directly used to construct an MPKC scheme because of some linear relationships between its input and output vector.

Next, we construct a hash-based tame transformation, also called an HT transformation. An HT transformation is defined by $L : \mathbb{F}_q^n \to \mathbb{F}_q^n$,

$$\begin{cases} \begin{pmatrix} y_1 \\ \vdots \\ y_{n-\delta} \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n-\delta} \end{pmatrix} + \alpha_1, \\ \begin{pmatrix} y_{n-\delta+1} \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_{n-\delta+1} \\ \vdots \\ x_n \end{pmatrix} + D \cdot \begin{pmatrix} x_{n+1} \\ \vdots \\ x_{n+\delta} \end{pmatrix} + B \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n-\delta} \end{pmatrix} + \alpha_2, \end{cases} \tag{3}$$

where α_1, α_2 are $(n-\delta)$-dimension vector and $(n-\delta)$-dimension vector respectively; $(n-\delta) \times (n-\delta)$ matrix A and $\delta \times \delta$ diagonal matrix D must be full-rank; B is a $\delta \times (n-\delta)$ random matrix B; other corresponding coefficients are randomly chosen in $\mathbb{F}_q$; in addition, the extended variables $x_{n+i} (1 \leqslant i \leqslant \delta)$ are defined by

$$x_{n+i} = H_k(x_1 || x_2 || \cdots || x_{n-\delta+i-1}). \tag{4}$$

Obviously, L is also bijective (but not linear) like (2). We can compute the preimage $x = L^{-1}(y)$ as easily as $y = L(x)$, but it is difficult to write x explicitly as a function of y variable because of the nonlinear property of hash function. In addition, if we look upon the δ extended variables $x_{n+1}, \ldots, x_{n+\delta}$ as the new variables identified with the first n variables $x_1, \ldots, x_n$. Then L can be seen as a compression map from $\mathbb{F}_q^{n+\delta}$ to $\mathbb{F}_q^n$, that is,

$$(y_1, \ldots, y_n) = L(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+\delta}).$$

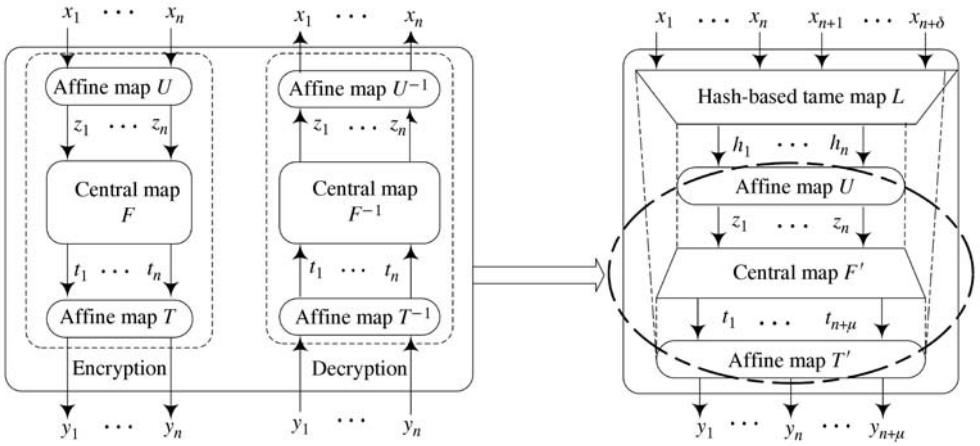

Figure 2 Structure comparison between traditional MPKC and EMC.

The generic construction of the new public key is

$$P' = (p'_1, \ldots, p'_n) = P \circ L = T \circ F \circ U \circ L. \tag{5}$$

The new public key P' is in the form of multivariate quadratic polynomials from $\mathbb{F}_q^{n+\delta}$ to $\mathbb{F}_q^n$. In practice, this is always the collection of the coefficients of the p'_i's. The corresponding secret key consists of L^{-1}, U^{-1}, T^{-1} and F^{-1}. In addition, from the theoretical point of view, we can be free to choose one of the four basic MQ-trapdoors discussed in section 2.

Due to the special construction of the new scheme, we call our scheme the EMC (extended multivariate cryptosystems) scheme.

3.2 Constructing encryption scheme

The new encryption scheme is called HTTP (Hash-based tame and plus) encryption scheme, which combines an HT transformation L like (3) and the plus method "+" (cf. Figure 2) as follows:

The secret parameters. We randomly choose three maps: two affine bijective maps $U : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $T : \mathbb{F}_q^{n+\mu} \to \mathbb{F}_q^{n+\mu}$, and an HT transformation $L : \mathbb{F}_q^{n+\delta} \to \mathbb{F}_q^n$. Furthermore, we find their respective inverse maps U^{-1}, T^{-1} and L^{-1}. In addition, we need to choose an appropriate central map $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ from the four basic MQ-trapdoors (see section 2). Consequently, the private key consists of the information U^{-1}, T^{-1}, L^{-1} and F^{-1}. Here, the size of F^{-1} depends on the MQ-trapdoor used.

The public parameters. By (5), the public map P' can be obtained by the composition of the above four private maps. Applying the plus method to the central map F, exampled by adding the μ randomly chosen quadratic polynomials ($0 \leqslant \mu < n$), we have

$$F' = F \circ U \circ L = (f'_1, \ldots, f'_n), \quad F'^{+} = (f'_1, \ldots, f'_n, f'_{n+1}, \ldots, f'_{n+\mu}).$$

Accordingly, the public key of the HTTP encryption scheme $P'^{+} : \mathbb{F}_q^{n+\delta} \to \mathbb{F}_q^{n+\mu}$ can be obtained by

$$P'^{+}(x_1, \ldots, x_{n+\delta}) = T \circ F'^{+} = (p_1, \ldots, p_{n+\mu}).$$

In addition, the public key also includes the field structure of $\mathbb{F}_q$ and the standard hash function used.

The encryption process. Given a plaintext $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. We first calculate the extended variables

$$x_{n+i} = H_k(x_1 || x_2 || \cdots || x_{n-\delta+i-1}), 1 \leqslant i \leqslant \delta$$

and apply the public polynomials P'^{+} to encrypt the plaintext. Then the corresponding ciphertext is easily obtained by

$$(y_1, \ldots, y_{n+\mu}) = P'^{+}(x_1, \ldots, x_{n+\delta}).$$

The decryption process. To decrypt the ciphertext $(y_1, \ldots, y_{n+\mu})$, we successively execute the following steps:

Step 1. Compute $(t_1, \ldots, t_{n+\mu}) = T^{-1}(y_1, \ldots, y_{n+\mu})$, and then discard the μ redundant values $t_{n+1}, \ldots, t_{n+\mu}$ to produce an n-dimensional vector $(t_1, \ldots, t_n)$.

Step 2. Compute $(z_1, \ldots, z_n) = F^{-1}(t_1, \ldots, t_n)$.

Step 3. Compute $(h_1, \ldots, h_n) = U^{-1}(z_1, \ldots, z_n)$.

Step 4. Finally, the plaintext can be obtained by $(x_1, \ldots, x_n) = L^{-1}(h_1, \ldots, h_n)$.

Compared with the decryption process of the traditional multivariate public key cryptosystems, it is apparent that the HTTP scheme only increases a linear multiplication with regard to L^{-1}.

3.3 Constructing signature scheme

Contrary to the HTTP encryption scheme, our new signature scheme is called HTTM scheme, which is combined with the Shamir's minus method [11] as follows:

The secret parameters. We randomly choose two affine bijective maps U, T from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ and an HT transformation L from $\mathbb{F}_q^{n+\delta}$ to $\mathbb{F}_q^n$, and find their inverse map U^{-1}, T^{-1} and L^{-1} respectively. In addition, we need to choose an appropriate central map $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ from the four basic MQ-trapdoors (see section 2). Consequently, the private key consists of the information U^{-1}, T^{-1}, L^{-1} and F^{-1}, where the size of F^{-1} depends on the MQ-trapdoor used.

The public parameters. The public map P' can be obtained by the composition of the above four maps. Once we apply the Shamir's minus method to P', exampled by deleting the last $|\mu|$ components, we will have a new map of the EMC signature scheme $P'^{-} : \mathbb{F}_q^{n+\delta} \to \mathbb{F}_q^{n-|\mu|}$ defined by

$$P'^{-}(x_1, \ldots, x_{n+\delta}) = (p_1, \ldots, p_{n-|\mu|}).$$

Of course, the public key also includes the field structure of $\mathbb{F}_q$ and the standard hash function used.

The signing process. Let the message (or its hash value) be $Y^{-} = (y_1, \ldots, y_{n-|\mu|})$ in $\mathbb{F}_q^{n-|\mu|}$. Then a signer first chooses μ random elements $y_{n-|\mu|+1}, \ldots, y_n \in \mathbb{F}_q$, which are appended to Y^{-} to obtain $Y = (y_1, \ldots, y_n)$ in $\mathbb{F}_q^n$. To obtain the valid signature X, he (or she) successively executes the following steps:

Step 1. Compute $(t_1, \ldots, t_{n+\mu}) = T^{-1}(y_1, \ldots, y_{n-|\mu|})$, and then choose the $|\mu|$ random values $t_{n-|\mu|+1}$, $\ldots, t_n$ to produce an n-dimensional vector $(t_1, \ldots, t_n)$.

Step 2. Compute $(z_1, \ldots, z_n) = F^{-1}(t_1, \ldots, t_n)$.

Step 3. Compute $(h_1, \ldots, h_n) = U^{-1}(z_1, \ldots, z_n)$.

Step 4. Finally, the corresponding signature can be obtained by $(x_1, \ldots, x_{n+\delta}) = L^{-1}(h_1, \ldots, h_n)$.

The verifying process. Anyone who receives the message Y^{-} and its signature $X = (x_1, \ldots, x_{n+\delta})$ first applies the public hash function to check if necessary

$$x_{n+i} = H_k(x_1||x_2||\cdots||x_{n-\delta+i-1}), 1 \leqslant i \leqslant \delta. \tag{V1}$$

If equality holds, then he (or she) continues to check

$$P'^{-}(X) = Y^{-}. \tag{V2}$$

We can conclude that a signature X of Y^{-} is valid if and only if the two conditions (V1) and (V2) are simultaneously satisfied. Due to the use of hash function, the (V1) is called the *hash authentication checking*. The checking method in (V2) is the same as the traditional MPKC's. Of course, steps (V1) and (V2) can be permuted. It is not required that they are executed in the order shown above.

We will discuss that in section 4, both (V1) and (V2) offer double-protection for the security of the HTTM signature scheme.

4 Security analysis

Several major methods have been developed to attack the traditional MPKCs. They can be roughly grouped into the following two categories: structure-based attacks and general attacks [12]. In subsection 4.1 we discuss the security of our schemes under general attacks. In subsection 4.2, we pay attention to how to resist structure-based attack methods using our schemes, mainly including linearization equations attack and differential attack for EMC schemes with the MI-trapdoor scheme as the central map. Finally, the precise security estimate of the HTTP and HTTM schemes is provided in subsections 4.3 and 4.4.

4.1 General attacks

The most natural ideal of attack on any public-key cryptosystem is to find a plaintext x for a given ciphertext y without using any information beyond the public key itself. In the case of MPKCs, the intention is equivalent to solving an instance of the MQ problem over a finite field. However, this problem is known to be NP-hard, when restricted to quadratic equations over $GF(2)$ [8] and over any finite field [9]. Several major methods based on Gröbner bases have been developed to solve the MQ problem, including the XL algorithm based on the Gröbner basis method [13], F4 and F5 algorithms [14], and DR algorithm [15], but these algorithms are exponential in time and memory [16]. Generally speaking, these attacks can be easily avoided by choosing appropriate scale parameters.

The construction of our new schemes is essentially the same as the traditional MQ-trapdoors like (6). The only difference is that the transformation U is replaced by U' $(= U \circ L)$, the combination of an affine bijective map and an HT transformation. It is obvious that U' is also a bijective map. More precisely, the generic construction of our schemes has the canonical decomposition of most MPKC's as follows:

$$P' = (p'_1, \ldots, p'_n) = T \circ F \circ U \circ L \overset{\text{def } U' = U \circ L}{=\!=\!=} T \circ F \circ U'. \tag{6}$$

For the EMC cryptosystems, we transform the original public key $P : \mathbb{F}_q^n \to \mathbb{F}_q^n$ into the new public key $P' : \mathbb{F}_q^{n+\delta} \to \mathbb{F}_q^n$ using an HT map L, obtained by $P' = P \circ L$, where $P = T \circ F \circ U$ (see section 3). According to [9], how to find P and L from P' is an IP problem and is NP-hard. Merging an HT transformation into the traditional MPKCs is equivalent to increasing the number of input variables, which is difficult to be eliminated by the attacker because of the hash-value relationship like (4) among these input variables. It is obviously more difficult to find a preimage x from the new public key P' than from the original public key P.

The EMC scheme can be understood from the following aspects. 1) It can be seen as an essentially improved scheme of the traditional MPKCs. 2) For the HTTM signature scheme, it can also be seen as a novel hash-based signature scheme like the Merkle tree scheme [17], which is equivalent to hiding an HT transformation L defined in this paper with the MQ problem and IP problem. Furthermore, contrary to our scheme, the private key of other hash-based signature schemes has limited lifetime. 3) The structure of the MPKCs scheme would be similar to the McEliece-type cryptosystems [7]. From coding point of view, the HT map L can be viewed as an encode process, similarly, its inverse L^{-1} is also considered as a fast decode process. Thus our key idea is to hide L with a bijective nonlinear map P combined with the IP problem, that is, $P' = P \circ L$.

By now, multivariate public key cryptosystems are currently believed to be resistant to quantum computing based attacks. According to our analysis, the EMC scheme belongs to the MPKC scheme and thus can also be post-quantum. Consequently, we can construct a class of quantum resistant public key systems by choosing different central maps and hash functions.

4.2 Structure-based attacks

We next show how to resist structure-based attack using our schemes. When using the MI-trapdoor scheme [18] as the central map, the cryptanalysis methods are mainly including linearization equations attack for the HTTP encryption scheme and differential attack for the HTTM signature scheme.

4.2.1 *Linearization equations attack for the HTTP scheme*

Linearization equations attack used to cryptanalyse the C^* scheme was proposed in 1995 by Patarin [19]. This attack relies on the use of the public key P to generate a large set of equations in the plaintext indeterminates $x_1, x_2, \ldots, x_n$ and the ciphertext indeterminates $y_1, y_2, \ldots, y_n$. The equations to be generated in this attack all have the "bilinear" form

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\gamma_{ij}x_iy_j + \sum_{i=1}^{n}\delta_i x_i + \sum_{i=1}^{n}\epsilon_i + \eta = 0. \tag{7}$$

It is shown in [19] that the linear equations in $\gamma_{ij}, \delta_i, \epsilon_i$ and η provided by a sufficient number of P input-output pairs allow to recover these unknown coefficients, and that once this has been done, the obtained vector space of solutions can be used to compute the inverse by P of any $\mathbb{F}_q^n$ element Y at the expense of solving a small linear system. The complexity of the attack is approximately $\mathcal{O}(n^6)$.

By section 3, we know that the HT transformation L is a nonlinear bijective function with regard to input variables $x_1, \ldots, x_n$ (but its degree is unknown by the properties of hash function). In other words, L further increases the nonlinear degree of MPKCs. Our experiments show that, for a large number of system parameters chosen such as the HTTP^{v1} scheme in Table 2, there only exists a trivial solution for the linear equations with regard to the all coefficients of (7) constructed by a sufficiently large number of P' input-output pairs.

4.2.2 *Differential attack for the HTTM scheme*

Dubois et al. [20] proposed a practical attack on the C^{*-} signature scheme. The attack only needs the public key and consumes about one second to forge a signature for any message, after a one-time computation of several minutes. The attack uses a specific multiplicative property of the differential of the public key of a C^{*-} scheme. The differential of the internal quadratic function $F(X) = X^{q^\theta+1}$ is symmetric bilinear in $\mathbb{F}_{q^n}$, and is defined by $DF(a, x)$:

$$DF(a, x) = F(x + a) - F(a) - F(x) + F(0) = ax^{q^\theta} + a^{q^\theta}x.$$

This map has a very specific multiplicative property: for all $\xi \in \mathbb{F}_{q^n}$, we have

$$DF(\xi a, x) + DF(a, \xi x) = (\xi + \xi^{q^\theta})DF(a, x).$$

Due to the linearity of the DP operator, the differential function of public key P is $DP(a, x) = T \circ DF(U(a), U(x))$. Then

$$\begin{aligned} DP(\xi a, x) + DP(a, \xi x) &= T \circ DF(\xi \cdot U(a), U(x)) + T \circ DF(U(a), \xi \cdot U(x)) \\ &= T \circ (\xi + \xi^{q^\theta}) \circ T^{-1} \circ DP(a, x). \end{aligned} \tag{8}$$

Let $P_\Pi = T_\Pi \circ F \circ U$ be the public key of the C^{*-} scheme. Then we can find the non-trivial map N_ξ such that

$$P'_\Pi = P_\Pi \circ N_\xi = T_\Pi \circ M_\xi \circ F \circ U,$$

where N_ξ and M_ξ denote two linear maps with regard to ξ (see [20, 21]).

Let us consider the special case $\xi \in \mathbb{F}_{q^n}$. It is obvious that T_Π and $T_\Pi \circ M_\xi$ are non-trivial. Therefore, in the sets P_Π and P'_Π the internal quadratic coordinates of $F \circ U$ are mixed with two different linear combinations, T_Π and $T_\Pi \circ M_\xi$. We hope that for some value $\xi \in \mathbb{F}_{q^n}$, μ equations in the set P'_Π together with P_Π will recover a valid C^* public key P''. For each choice of μ equations, the success probability is approximately $1 - 1/q$. Then, it remains to apply Patarin's linearization attack [19] to this new P'', but by subsection 4.2.1, the MI system combined with the HT map L can avoid the linearization attack. Thus we can now say that the HTTM signature scheme is secure.

Furthermore, we also illustrate how to resist the differential attack using HTTM scheme. Essentially, the generic construction of our EMC schemes is the same as the traditional MQ-trapdoors, that is,

$$P' = P \circ L = (T \circ F \circ U) \circ L \overset{\texttt{def } U'=U\circ L}{=\!=\!=\!=\!=\!=} T \circ F \circ U'. \tag{9}$$

By the nonlinear property of HT map L, obviously, U' in (9) is also a nonlinear map. Then $\forall x, \xi \in \mathbb{F}_{q^n}$, we have

$$\xi \circ U'(x) \not\equiv U'(\xi x).$$

Therefor the differential function DP' of the public key P' must also satisfy

$$\begin{aligned} DP'(\xi a, x) + DP'(a, \xi x) &= T \circ DF(\xi \cdot U'(a), U'(x)) + T \circ DF(U'(a), \xi \cdot U'(x)) \\ &\not\equiv T \circ (\xi + \xi^{q^\theta}) \circ T^{-1}(DP'(a, x)). \end{aligned} \tag{10}$$

Expression (10) shows that by increasing L, one can powerfully demolish the specific multiplicative property of MI scheme like (8) and effectively avoid differential cryptanalysis.

4.3 The security of HTTP encryption scheme

The structure-based attack type relies solely on the specific structures of the corresponding multivariate public key schemes. The preliminary security analysis suggests that we can choose any one of the four basic MQ-trapdoors (see section 2) as the central map F of our proposed EMC schemes. As space is limited, we do not intend to discuss each scheme based on a basic MQ-trapdoor in detail. However, we have shown that the original public key P was disguised as our new public key P' by an HT map L, and how to find P and L from P' is a computationally intractable problem. The "Chemical Synthesis" of the HT map and traditional MQ-trapdoors offers double security protection for the EMC schemes. Hence the EMC schemes, including signature and encryption schemes, can effectively resist all known attacks for the original public key P (see subsection 4.2).

For the HTTP encryption scheme, let $\mathcal{O}(T_{n+\mu})$ denote the complexity of finding a plaintext $X' = (x'_1, \ldots, x'_{n+\delta})$ of given ciphertext Y such that $P'(X') = Y$. According to the asymmetric characteristic of P''s input-output space, there are about $q^{\delta-\mu}$ values X' satisfying $P'(X') = Y$. Thus the complexity of finding unique legitimate ciphertext X' is approximately $\mathcal{O}(T_{n+\mu} \cdot q^{\delta-\mu})$, which, in practice is replaced by conservative security level

$$C_{\text{encrypt}} = \mathcal{O}\Big(\min\big\{T_{n+\mu},\ q^{\delta-\mu}\big\}\Big). \tag{11}$$

4.4 The security of HTTM signature scheme

Contrary to the HTTP scheme, from the security analysis above, the public key P' of the HTTM signature scheme can also resist all known structure-based cryptanalysis techniques of the original public key P. Consequently, we let $\mathcal{O}(T_{n-|\mu|})$ $(-\delta < \mu \leqslant 0)$ denote the complexity of forging a signature $X' = (x'_1, \ldots, x'_{n+\delta})$ of given message Y by finding the multivariate quadratic equations $P'(X') = Y$ (i.e., passing (V2) in the verifying process). In addition, the success probability of randomly finding an X' satisfying (4) is approximately $1/q^\delta$. Thus the complexity of finding a signature X' simultaneously satisfying (V1) and (V2) in the verifying process is approximately $\mathcal{O}(T_{n+\mu} \cdot q^\delta)$. Furthermore, according to the results of the minus method, for a given message Y, the complexity of X' simultaneously satisfying $P'(X') = Y$ and being the unique legitimate signature is approximately $\mathcal{O}(q^{\delta-|\mu|})$. In practice, we have also proposed the conservative security level of the HTTM scheme as follows:

$$C_{\text{sign}} = \mathcal{O}\Big(\min\big\{T_{n-|\mu|},\ q^{\min\{\delta,\ \delta-|\mu|\}}\big\}\Big). \tag{12}$$

Table 2 Comparison with SFLASH signature schemes

Version	n	δ	μ	k	Public key size (KB)	Private key size (KB)
HTTP^{v1}	20	17	6	8	18.8	3.9
HTTM^{v1}	31	10	−5	8	22.9	4.9
HTT^{v1}	31	16	0	8	35.6	5.8
SFLASH^{v2}	37	–	−11	7	15.4	2.45
SFLASH^{v3}	67	–	−11	7	112.3	7.8

5 Practical-sized instances and performance evaluations

In order to facilitate the discussion, we next denote the our proposed EMC schemes by EMC(n, δ, μ, k), where the parameters k, δ and μ have been defined in Table 1, and n is the number of dimensions of the central map $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$. For the parameter μ, if $\mu < 0$, then the scheme can be only used as signing. Conversely, if $\mu > 0$, then it can be only used as encrypting. Of course, when $\mu = 0$, it can be used to both sign and encrypt a message (but generally not recommended).

From the security analysis above, in Table 2, we propose three EMC schemes of at least 80-bit security level, which are called HTTP^{v1}, HTTM^{v1} and HTT^{v1}. Note that the central map F in (5) still uses the MI-type trapdoor, and the hash function uses SHA-256. We summarize the parameters in Table 2.

The key size of these schemes is slightly greater than SFLASH^{v2} in [20], but it can be vastly superior to SFLASH^{v2} [22]. The concrete computing process of the above schemes is the same as the SFLASH family. Roughly speaking, their efficiency is roughly the same as that of SFLASH^{v2}.

6 Conclusions

In this paper, we introduce the hash authentication techniques and combine it with the traditional MQ-trapdoors to yield a novel extend multivariate public key cryptosystem. Security analysis shows that the extended schemes can resist all the known attacks. By using our new framework and some modification methods, we can construct not only secure and efficient signature scheme but also encryption scheme. As an instance, with the MI-type basic trapdoor, we illustrated how to enhance the security of the traditional MPKCs using our new framework. Of course, the central map can also choose the other MQ-trapdoors. If the original MPKC scheme is secure in our new framework, then the corresponding extended schemes can offer double security protections for signing/encrypting messages. For instance, one can use our extended framework and currently secure MPKCs, e.g., Rainbow, TTS, HEFv-, to construct a class of quantum resistant MPKC schemes.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos. 60970115, 60970116, 61003267, 61003268, 61003214), and the Major Research Plan of the National Natural Science Foundation of China (Grant No. 91018008).

References

1 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput, 1997, 6: 1484–1509

2 Vandersypen L M K, Steffen M, Breyta G, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 2001, 414: 883–887

3 Guan H M. Progress in quantum computers abroad, information security challenges and countermeasures. Comput Secur, 2009, 4: 1–5

4 Fu X Q, Bao W S, Zhou C. Speeding up implementation for Shor's factorization quantum. Chinese Sci Bull, 2010, 55: 322–327

5 Wu Q H, Mu Y, Susilo W, et al. Asymmetric group key agreement. In: Eurocrypt 2009, LNCS, Vol. 5479. Berlin: Springer-Verlag, 2009. 153–170
6 Wu Q H, Domingo-Ferrer J, González-Nicolás U. Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications. IEEE Trans Veh Technol, 2010, 2: 559–573
7 Li Y, Deng R, Wang X. The equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Trans Inf Theory, 1994, 44: 271–273
8 Garey M, Johnson D. Computers and Intractability, a Guide to the Theory of NP-Completeness. New York: Freeman, 1979. 128–130
9 Patarin J. Hidden field equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Proceedings of Eurocrypt 1996, LNCS, Vol. 1070. Berlin: Springer-Verlag, 1996. 33–48
10 Wolf C. Multivariate quadratic polynomials in public key cryptography. Katholieke Universiteit Leuven, 2005
11 Shamir A. Efficient signature schemes based on birational permutations. In: Proceedings of Crypto 1993, LNCS, Vol. 773. Berlin: Springer-Verlag, 1993. 1–12
12 Wang H Z, Zhang H G, Guan H M. Multivariate algebra theory and its application in cryptography. J Beijing Univ Technol, 2010, 5: 9–17
13 Coutrtois N T, Klimov A, Patarin J, et al. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: Proceedings of Eurocrypt 2000, LNCS, Vol. 1807. Berlin: Springer-Verlag, 2000. 392–407
14 Faugere J C. A new efficient algorithm for computing Grobner bases without reduction to zero (F5). In: Proceedings of ISSAC 2002 LNCS, Vol. 2518. Berlin: Springer-Verlag, 2002. 75–83
15 Tang X J, Feng Y. Applying dixon resultants in cryptography. J Softw, 2007, 7: 1738–1745
16 Wang H Z, Zhang H G, et al. Design theory and method of multivariate hash function. Sci China Inf Sci, 2010, 53: 1977–1987
17 Merkle R C. A certified digital signature. In: Proceedings of CRYPTO1989. LNCS, Vol. 435. Berlin: Springer-Verlag, 1989. 218–238
18 Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature verification and message encryption. In: Proceedings of Eurocryp 1988, LNCS, Vol. 330. Berlin: Springer-Verlag, 1988. 419–453
19 Patarin J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 1988. In: Proceedings of Crypto 1995, LNCS, Vol. 963. Berlin: Springer-Verlag, 1995. 248–261
20 Dubois V, Fouque P A, Shamir A, et al. Practical cryptanalysis of SFLASH. In: Proceedings of Crypto 2007, LNCS, Vol. 4622. Berlin: Springer-Verlag, 2007. 1–12
21 Wang H Z, Zhang H G, et al. A new perturbation algorithm and enhancing security of SFLASH signature scheme. Sci China Inf Sci, 2010, 53: 760–768
22 Akkar M, Courtois N. A fast and secure implementation of SFLASH. In: Proceedings of PKC 2003, LNCS, Vol. 2567. Berlin: Springer-Verlag, 2003. 267–278