Tsinghua Science and Technology

Volume 21 | Issue 3 Article 6

2016

New Public-Key Cryptosystem Based on the Morphism of Polynomials Problem

Houzhen Wang
the Computer School of Wuhan University, Wuhan 430079, China and the State Key Laboratory of Cryptology, Beijing 100878, China.

Huanguo Zhang
the Computer School of Wuhan University, Wuhan 430079, China.

Shaowu Mao
the Computer School of Wuhan University, Wuhan 430079, China.

Wanqing Wu
the Computer School of Wuhan University, Wuhan 430079, China.

Liqiang Zhang
the Computer School of Wuhan University, Wuhan 430079, China.

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 06/11 pp302–311
Volume 21, Number 3, June 2016

New Public-Key Cryptosystem Based on the Morphism of Polynomials Problem

Houzhen Wang, Huanguo Zhang, Shaowu Mao, Wanqing Wu, and Liqiang Zhang*

Abstract: During the last two decades, there has been intensive and fast development in Multivariate Public Key Cryptography (MPKC), which is considered to be an important candidate for post-quantum cryptography. However, it is universally regarded as a difficult task, as in the Knapsack cryptosystems, to design a secure MPKC scheme (especially an encryption scheme) employing the existing trapdoor construction. In this paper, we propose a new key-exchange scheme and an MPKC scheme based on the Morphism of Polynomials (MP) problem. The security of the proposed schemes is provably reducible to the conjectured intractability of a new difficult problem, namely the Decisional Multivariate Diffie-Hellman (DMDH) problem derived from the MP problem. The proposed key agreement is one of several non-number-theory-based protocols, and is a candidate for use in the post-quantum era. More importantly, by slightly modifying the protocol, we offer an original approach to designing a secure MPKC scheme. Furthermore, the proposed encryption scheme achieves a good tradeoff between security and efficiency, and seems competitive with traditional MPKC schemes.

Key words: public key cryptosystem; key exchange; Multivariate Public Key Cryptography (MPKC); Morphism of Polynomials (MP) problem

1 Introduction

Public Key Cryptosystems (PKC) have fundamentally changed our modern communication systems and become an important tool for information society. This revolutionary idea was firstly introduced by Diffie and Hellman in their landmark paper, "*New directions in cryptography*", in 1976[1]. The Diffie-Hellman key exchange protocol allows two entities to establish a shared secret key via a public communication channel. This common secret key is subsequently applied to carry out a variety of cryptographic purposes such as efficient symmetric encryption and entity authentication. In the past 30 years, the basic Diffie-Hellman protocol has been considered to be one of the most practical cryptographic primitives, and has been studied extensively. Some improved protocols, such as the MQV protocol[2, 3], have become the international standards and been widely applied to many fields in the real world, including the Internet and e-commerce.

Since the advent of the Diffie-Hellman protocol, many PKC schemes have been proposed and subsequently broken. Most of the successful PKCs are based on number theory. For example, the difficulty of factorization of an integer with large prime factors led to the RSA scheme and its variants. Also the difficulty of the discrete logarithm problem generated the Diffie-Hellman like schemes such as ElGamal and ECC.

Motivation. These public key schemes are widely used, but have two obvious drawbacks. The first comes from the challenge of rapid development of quantum computing. In 1997, Shor[4] proposed

• Houzhen Wang is with the Computer School of Wuhan University, Wuhan 430079, China and the State Key Laboratory of Cryptology, Beijing 100878, China. E-mail: whz@whu.edu.cn.
• Huanguo Zhang, Shaowu Mao, Wanqing Wu, and Liqiang Zhang are with the Computer School of Wuhan University, Wuhan 430079, China. E-mail: liss@whu.edu.cn.
∗ To whom correspondence should be addressed.
Manuscript received: 2016-02-09; accepted: 2016-03-07

quantum polynomial-time algorithms for factoring integers and computing discrete logarithms. This means that once a sufficiently powerful quantum computer is built, the most widely used public key schemes, including RSA, ElGamal, ECC, and their corresponding key agreement protocols, will no longer be secure. The second drawback is that these number-theory-based schemes are not suitable for application in small computing devices, such as low-cost smart cards and active RFID tags, with limited computing capacity.

Hence it is of great interest and importance to construct non-number-theory-based, faster, and secure key exchange protocols and PKCs.

Related work. In recent years, the research on post-quantum cryptography[5] has received a lot of attention, with its main object to find alternative PKCs against the quantum computing attack. Multivariate Public Key Cryptography (MPKC) is considered to be a competitive candidate for post-quantum cryptography. Meanwhile it is well known that MPKC schemes are in general much more computationally efficient than number-theory-based PKC's[6]. Most existing MPKC schemes are based on the MQ problem and the Isomorphism of Polynomials (IP) problem, which will be introduced in Section 2. The MQ problem is NP-hard[7, 8]. It is worth mentioning that we can obtain some excellent cryptographic schemes by using the difficulty of the MQ problem directly, e.g., a stream cipher scheme[9], a hash function[10], and a public key identification scheme[11]. Up to now, we have not known whether the IP problem is an NP-hard problem. Also many IP-based cryptosystems, including SFLASH, HFE, TTM, and some of their variants[6, 12–16], have been broken, because the special structure of the central function made the corresponding IP problem no longer random. Although there are several MPKC proposals that are not considered to be broken yet (HFE and UOV[17], for instance), like the Knapsack cryptosystems, it is generally regarded as a difficult problem to design a secure MPKC scheme (especially encryption scheme) employing existing trapdoor construction.

Some efforts have been also made to construct alternative secure key exchange protocols that are not based on number theory. The results, however, are far from encouraging. In 1999, Anshel et al.[18] proposed a key agreement based on non-Abelian groups, and subsequently presented a variant using the braid group[19]; these two protocols were broken in Refs. [20, 21]. Similarly, a key agreement based on the braid group was proposed by Ko et al.[22] and proved to be insecure in Refs. [20, 23]. Boucher et al.[24] proposed a new key exchange and encryption scheme based on the so-called non-commutative skew polynomials, whereafter, an efficient attack was discovered by Dubois and Kammerer[25]. The other systems that are worth mentioning are the quantum-key agreement protocols proposed by Bennet and Brassard[26, 27]. However, from our perspective, these quantum protocols are still high-cost, and can hardly achieve the protocols without a classical channel. Indeed one of our aims is to construct a faster secure key-exchange protocol based on a non-number-theory problem.

Main contributions. We propose a Diffie-Hellman-like key-exchange scheme and an MPKC scheme employing a Morphism of Polynomials (MP) problem. Our proposed schemes have the following features.

(1) The key-exchange protocol is based on a variant of the MP problem similar to the Diffie-Hellman problem, which also proved to be secure in the presence of an eavesdropper. We propose practical-sized parameters which provide 14 400 bits of exchanged information, with a complexity of roughly 2^{24} binary operations for performing the protocol. Our encryption scheme is constructed from this protocol, and bears some similarity to the ElGamal scheme.

(2) The MPKC encryption scheme is non-deterministic and has also proved to be CPA-secure like ElGamal. For each session, the ciphertext relies on both of the corresponding plaintexts and an MQ function chosen at random in the shared key space.

(3) We propose a truly original approach to designing the secure MPKC scheme in the construction of our encryption scheme. Moreover, the key exchange protocol and encryption scheme are also considered to be a promising candidate for post-quantum era.

Paper organization. The remainder of this paper is organized as follows. In Section 2, we introduce several notations and new difficulty assumptions, which will be used in our constructions. In Section 3 we propose a Diffie-Hellman-type key-exchange protocol and a new MPKC scheme. Section 4 is dedicated to a simple security proof and security evaluation against several possible attack methods. In Section 5 we give the theoretical operating characteristics of our schemes

and a practical-sized instance. Finally, we conclude our work and suggest possible improvements in Section 6.

2 Preliminaries

The notations used throughout this paper are as follows. Let $\mathbb{F}_q$ be a finite field with q elements, $\mathcal{M}_n(\mathbb{F}_q)$ be a set of $n \times n$ matrices whose components are in $\mathbb{F}_q$, and let $\boldsymbol{I}_n$ be an $n \times n$ identity matrix. For any set $\mathcal{S}$, $a \in_R \mathcal{S}$ denotes that a is uniformly and randomly selected from $\mathcal{S}$, and for $s \in \mathcal{S}$, we write $\Pr[a = s]$ to denote the probability that any a is equal to s. As usual, $\boldsymbol{x} = (x_1, \ldots, x_n)$ represents an n-dimensional row vector.

2.1 Multivariate quadratic systems and related problems

Definition 1 (The MQ Function) We denote by $\mathcal{MQ}(n, m, \mathbb{F}_q)$ a family of multivariate quadratic functions,

$$\boldsymbol{F}(\boldsymbol{x}) = (f_1(\boldsymbol{x}), \ldots, f_m(\boldsymbol{x})),$$
$$f_i(\boldsymbol{x}) = \sum_{j \leqslant k}^{n} \alpha_{i,j,k} x_j x_k + \sum_{j}^{n} \beta_{i,j} x_j + \gamma_i,$$

where $\alpha_{i,j,k}, \beta_{i,j}, \gamma_i \in \mathbb{F}_q$ for $i = 1, \ldots, m$.

Given an instance $\boldsymbol{F} \in_R \mathcal{MQ}(n, m, \mathbb{F}_q)$ and a vector $\boldsymbol{y}_0 \in \mathbb{F}_q^m$, the so-called MQ problem is to find a solution $\boldsymbol{x}_0 \in \mathbb{F}_q^n$ such that $\boldsymbol{F}(\boldsymbol{x}_0) = \boldsymbol{y}_0$. The MQ problem is well known to be an NP-hard problem, even when restricted to quadratic equations over $\mathbb{F}_2$[7] and over any finite field[8]. Some cryptographic schemes can be constructed only from this problem such as Refs. [9, 11].

The security of existing MPKC schemes relies not only on the MQ problem but also on an IP problem defined as follows:

Definition 2 (IP Problem) Given any $\boldsymbol{F}$ and $\boldsymbol{G}$ in $\mathcal{MQ}(n, m, \mathbb{F}_q)$, find, if any, a pair of invertible affine transformations $(\boldsymbol{T}, \boldsymbol{U})$ such that

$$\boldsymbol{G} = \boldsymbol{T} \circ \boldsymbol{F} \circ \boldsymbol{U} \tag{1}$$

where "$\circ$" denotes the composition of functions.

The general method of building an MPKC scheme is to construct an *invertible* MQ function $\boldsymbol{F}$, called a central function, and then hide this central function by employing two invertible affine transformations $\boldsymbol{T}$ and $\boldsymbol{U}$. The composition $\boldsymbol{T} \circ \boldsymbol{F} \circ \boldsymbol{U}$ will be used as a public key and the pair $(\boldsymbol{T}, \boldsymbol{U})$ is considered to be a secret key. That is, the IP problem is usually used for an embedded trapdoor.

The IP problem originated by trying to recovering the secret keys for an MPKC scheme (such as the C* scheme[28]), and IP cryptosystems were first introduced by Patarin[29]. During the blossom of MPKCs, many IP-based cryptosystems were proposed, including the SFLASH scheme, the HFE scheme, the OV scheme, the TTM scheme, and some of their variants (see Ref. [6]). Nevertheless, most of these schemes have been broken, because the special structure of the central function made the corresponding IP problem no longer random. More efforts were devoted to this direction, e.g., Refs. [30–34], but so far no polynomial time algorithms that attack the general IP problem are known.

In this paper, we propose a new key exchange protocol and public key encryption scheme based on a more general IP-type problem that is when affine transformations $\boldsymbol{T}$ and $\boldsymbol{U}$ as in Eq. (1) are not necessary bijective; this is called an MP problem. This problem has been proven to be NP-hard for any finite field by Patarin et al.[35] Thus Patarin et al. advised designing cryptographic schemes using the MP problem, but meanwhile they also think that this very general construction is not very practical, and it may be more difficult to design cryptographic algorithms from MP than from IP.

In addition, it is the linear variant of IP-type that is usually used in practice. More precisely, the $\boldsymbol{T}$ and $\boldsymbol{U}$ in Definition 2 are both linear transformations. Faugère and Perret[33] pointed out that any method solving a variant of IP can be easily transformed into a method solving IP. For the case of MP, according to the results in Ref. [35], a linear variant of an MP problem is still hard. Thus in the rest of the paper, we substitute affine transformations for linear ones. That is to say, $\boldsymbol{T}$ and $\boldsymbol{U}$ like Eq. (1) will be both seen as square matrices over $\mathbb{F}_q$.

2.2 Proposed difficult problems

Our proposed cryptographic hardness assumptions are based on the following result.

Theorem 1 Let $f(\boldsymbol{T}) = a_n \boldsymbol{T}^n + a_{n-1} \boldsymbol{T}^{n-1} + \cdots + a_1 \boldsymbol{T} + a_0 \boldsymbol{I}_n$ and

$$\mathcal{K}_T = \{f(\boldsymbol{T}) \mid \forall\, \boldsymbol{T} \in \mathcal{M}_n(\mathbb{F}_q), a_i \in \mathbb{F}_q, 0 \leqslant i \leqslant n\}.$$

Let $|\mathcal{K}_T|$ denote the number of elements of the set $\mathcal{K}_T$ and d be the degree of the minimal polynomial $m(x)$ of matrix $\boldsymbol{T}$, then:

(1) for any two elements $\boldsymbol{T}_a$ and $\boldsymbol{T}_\mathrm{b}$ in $\mathcal{K}_T$, $\boldsymbol{T}_a$ and $\boldsymbol{T}_\mathrm{b}$ satisfy the multiplication commutative law, that is $\boldsymbol{T}_a \boldsymbol{T}_\mathrm{b} = \boldsymbol{T}_\mathrm{b} \boldsymbol{T}_a$;

(2) $|\mathcal{K}_T| = q^d$.

Proof The proof of (1) follows immediately from the properties of a matrix polynomial. As to (2), note

that since $m(\boldsymbol{T}) = 0$, the matrix polynomial $f(\boldsymbol{T})$ can be changed into a matrix polynomial with the degree less than or equal to $d-1$. We can define by

$$f(\boldsymbol{T}) = a'_{d-1}\boldsymbol{T}^{d-1} + a'_{d-2}\boldsymbol{T}^{d-2} + \cdots + a'_1\boldsymbol{T} + a'_0\boldsymbol{I}_n,$$

where each a'_i can be viewed as a function with respect to $a_0, a_1, \ldots, a_n$.

Let us now prove uniqueness. Assume that

$$f^{(1)}(\boldsymbol{T}) = a^{(1)}_{d-1}\boldsymbol{T}^{d-1} + a^{(1)}_{d-2}\boldsymbol{T}^{d-2} + \cdots + a^{(1)}_1\boldsymbol{T} + a^{(1)}_0\boldsymbol{I}_n$$

and

$$f^{(2)}(\boldsymbol{T}) = a^{(2)}_{d-1}\boldsymbol{T}^{d-1} + a^{(2)}_{d-2}\boldsymbol{T}^{d-2} + \cdots + a^{(2)}_1\boldsymbol{T} + a^{(2)}_0\boldsymbol{I}_n,$$

where $a^{(1)}_i, a^{(2)}_i \in_R \mathbb{F}_q$, $0 \leqslant i \leqslant d-1$.

If $f^{(1)}(\boldsymbol{T}) = f^{(2)}(\boldsymbol{T})$, then we have

$$g(\boldsymbol{T}) = f^{(1)}(\boldsymbol{T}) - f^{(2)}(\boldsymbol{T}) = \sum_{i=0}^{d-1}(a^{(1)}_i - a^{(2)}_i)\boldsymbol{T}^i = 0,$$

where $\boldsymbol{T}^0 = \boldsymbol{I}_n$.

It is clear that $g(x)$ is an annihilating polynomial of matrix $\boldsymbol{T}$ and must satisfy $m(x)|g(x)$. The degree of both polynomials meets $\deg(m(x)) > \deg(g(x))$. We conclude that the condition $m(x)|g(x)$ holds if and only if $g(x) \equiv 0$; that is, $a^{(1)}_i = a^{(2)}_i$ for $0 \leqslant i \leqslant d-1$. In other words, any matrix $\boldsymbol{T}' \in \mathcal{K}_T$ can be uniquely expressed by a d-dimensional vector $(a'_0, a'_1, \ldots, a'_{d-1})$. Furthermore, the d-dimensional vector $(a'_0, a'_1, \ldots, a'_{d-1}) \in \mathbb{F}_q^d$ has q^d possible values. Thus we have $|\mathcal{K}_T| = q^d$. ■

Note that the matrix $\boldsymbol{T}$ is called a *seed matrix*, and the corresponding $\mathcal{K}_T$ is a *key space* in the above Theorem. We will show in Section 3 that the key space of our proposed cryptographic scheme is $\mathcal{K}_T \cup \mathcal{K}_U$, which is generated by two *singular* seed matrices $\boldsymbol{T} \in_R \mathcal{M}_m(\mathbb{F}_q)$ and $\boldsymbol{U} \in_R \mathcal{M}_n(\mathbb{F}_q)$. Now we assume that

$$\begin{aligned} \boldsymbol{G}_x &= \boldsymbol{T}_x \circ \boldsymbol{F} \circ \boldsymbol{U}_x, \\ \boldsymbol{G}_y &= \boldsymbol{T}_y \circ \boldsymbol{F} \circ \boldsymbol{U}_y, \\ \boldsymbol{G}_{xy} &= \boldsymbol{T}_x\boldsymbol{T}_y \circ \boldsymbol{F} \circ \boldsymbol{U}_x\boldsymbol{U}_y \end{aligned} \tag{2}$$

where $\boldsymbol{F} \in_R \mathcal{MQ}(n, m, \mathbb{F}_q)$, $\boldsymbol{T}_x, \boldsymbol{T}_y \in_R \mathcal{K}_T$, and $\boldsymbol{U}_x$, $\boldsymbol{U}_y \in_R \mathcal{K}_U$.

In addition, we denote the shared key space in Section 3.1 by

$$\mathcal{SK} = \{\boldsymbol{T}_z \circ \boldsymbol{F} \circ \boldsymbol{U}_z \mid \boldsymbol{T}_z \in \mathcal{K}_T \text{ and } \boldsymbol{U}_z \in \mathcal{K}_U\} \tag{3}$$

and let $\boldsymbol{G}_z$ be a random MQ function in $\mathcal{SK}$ that can be obtained by $\boldsymbol{G}_z = \boldsymbol{T}_z \circ \boldsymbol{F} \circ \boldsymbol{U}_z$ for $\boldsymbol{T}_z \in_R \mathcal{K}_T$ and $\boldsymbol{U}_z \in_R \mathcal{K}_U$.

The security of our key exchange protocol and PKC scheme involves the difficulty of the following problems.

(1) The Computational Multivariate Diffie-Hellman (CMDH) problem:

Instance: Given a triple $(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y)$,

Objective: Find the MQ function $\boldsymbol{G}_{xy}$ such that $\boldsymbol{G}_{xy} = \boldsymbol{T}_x\boldsymbol{T}_y \circ \boldsymbol{F} \circ \boldsymbol{U}_x\boldsymbol{U}_y$ as in Eq. (2).

(2) The Decisional Multivariate Diffie-Hellman (DMDH) problem:

Instance: Given a 4-tuple $(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_z)$,

Objective: Decide whether $\boldsymbol{G}_z = \boldsymbol{G}_{xy}$ as in Eq. (2).

The relationship among these problems, including the MP problem, is similar to the case of the CDH problem, the DDH problem, and the DL problem. That is, we do not know whether CMDH and DMDH belong to an NP-type problem. From the security proof in Section 4, our proposed schemes can achieve the expected security level based on the premise that MP and DMDH are computationally hard. That is the following two hardness assumptions:

Definition 3 (MP Assumption) For all Probabilistic Polynomial-Time (PPT) algorithms $\mathcal{A}$, there exists a negligible function negl such that

$$\Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x) = (\boldsymbol{T}_x, \boldsymbol{U}_x)] \leqslant \text{negl}(\lambda),$$

where λ denotes a security parameter.

Definition 4 (DMDH Assumption) We say that a DMDH problem is hard if for all PPT algorithms $\mathcal{A}$, there exists a negligible function negl such that

$$\begin{aligned} &|\Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_z) = 1] - \\ &\Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_{xy}) = 1]| \leqslant \text{negl}(\lambda), \end{aligned}$$

where λ denotes a security parameter.

3 Cryptosystem Using an MP Problem

In this section, we propose a key-exchange agreement and a PKC scheme based on the MP problem and the CMDH problem.

3.1 Key-exchange protocol

Let $\mathcal{G}$ be a PPT algorithm that, upon input of a security parameter 1^λ, outputs a 4-tuple $(\mathbb{F}_q, \boldsymbol{T}, \boldsymbol{U}, \boldsymbol{F})$, where $\boldsymbol{F} \in_R \mathcal{MQ}(n, m, \mathbb{F}_q)$, and two singular matrices $\boldsymbol{T} \in_R \mathcal{M}_m(\mathbb{F}_q)$ and $\boldsymbol{U} \in_R \mathcal{M}_n(\mathbb{F}_q)$ of which the degrees of the minimal polynomials are attained in m and n, respectively. Now we describe a Diffie-Hellman-like key agreement protocol between Alice and Bob as follows:

(1) Alice runs $\mathcal{G}(1^\lambda)$ to obtain $(\mathbb{F}_q, \boldsymbol{T}, \boldsymbol{U}, \boldsymbol{F})$.

(2) Alice chooses $\boldsymbol{T}_\text{a} \in \mathcal{K}_T$ and $\boldsymbol{U}_\text{a} \in \mathcal{K}_U$ at random and computes $\boldsymbol{G}_\text{a} = \boldsymbol{T}_\text{a} \circ \boldsymbol{F} \circ \boldsymbol{U}_\text{a}$.

(3) Alice sends $(\mathbb{F}_q, \boldsymbol{T}, \boldsymbol{U}, \boldsymbol{F}, \boldsymbol{G}_\text{a})$ to Bob.

(4) Bob receives $(\mathbb{F}_q, \boldsymbol{T}, \boldsymbol{U}, \boldsymbol{F}, \boldsymbol{G}_\text{a})$. He chooses $\boldsymbol{T}_\text{b} \in \mathcal{K}_T$ and $\boldsymbol{U}_\text{b} \in \mathcal{K}_U$ at random and computes $\boldsymbol{G}_\text{b} =$

$\boldsymbol{T}_\mathrm{b} \circ \boldsymbol{F} \circ \boldsymbol{U}_\mathrm{b}$. Bob sends $\boldsymbol{G}_\mathrm{b}$ to Alice and computes the shared key $k_\mathrm{B} := \boldsymbol{G}_\mathrm{ab} = \boldsymbol{T}_\mathrm{b} \circ \boldsymbol{G}_\mathrm{a} \circ \boldsymbol{U}_\mathrm{b}$.

(5) Alice receives $\boldsymbol{G}_\mathrm{b}$ and computes the shared key $k_\mathrm{A} := \boldsymbol{G}_\mathrm{ba} = \boldsymbol{T}_\mathrm{a} \circ \boldsymbol{G}_\mathrm{b} \circ \boldsymbol{U}_\mathrm{a}$.

Proof of correctness: By Theorem 1, $\boldsymbol{T}_\mathrm{a}$ and $\boldsymbol{T}_\mathrm{b}$ commute (resp. $\boldsymbol{U}_\mathrm{a}$ and $\boldsymbol{U}_\mathrm{b}$), Thus we have $\boldsymbol{G}_\mathrm{ba} = \boldsymbol{T}_\mathrm{a} \circ \boldsymbol{G}_\mathrm{b} \circ \boldsymbol{U}_\mathrm{a} = \boldsymbol{T}_\mathrm{a} \circ (\boldsymbol{T}_\mathrm{b} \circ \boldsymbol{F} \circ \boldsymbol{U}_\mathrm{b}) \circ \boldsymbol{U}_\mathrm{a} = \boldsymbol{T}_\mathrm{a} \circ \boldsymbol{T}_\mathrm{b} \circ \boldsymbol{F} \circ \boldsymbol{U}_\mathrm{b} \circ \boldsymbol{U}_\mathrm{a} = \boldsymbol{T}_\mathrm{b} \circ (\boldsymbol{T}_\mathrm{a} \circ \boldsymbol{F} \circ \boldsymbol{U}_\mathrm{a}) \circ \boldsymbol{U}_\mathrm{b} = \boldsymbol{T}_\mathrm{b} \circ \boldsymbol{G}_\mathrm{a} \circ \boldsymbol{U}_\mathrm{b} = \boldsymbol{G}_\mathrm{ab}$.

Consequently, Alice and Bob successfully establish a common session key $\mathrm{sk} = k_\mathrm{A} = k_\mathrm{B}$, which is an MQ function in $\mathcal{MQ}(n, m, \mathbb{F}_q)$.

Remark 1. In the above protocol, we assume that Alice generates $(\mathbb{F}_q, \boldsymbol{T}, \boldsymbol{U}, \boldsymbol{F})$ and sends it to Bob as her first message. In fact, $(\mathbb{F}_q, \boldsymbol{T}, \boldsymbol{U}, \boldsymbol{F})$, as the system parameter, can also be publicly known by two parties. Thus Alice only needs to send $\boldsymbol{G}_\mathrm{a}$, and Bob needs not wait for Alice's message $\boldsymbol{G}_\mathrm{a}$ before computing and sending $\boldsymbol{G}_\mathrm{b}$.

3.2 Public key encryption scheme

Let $H : \mathcal{SK} \to \{0,1\}^\ell$ be an ideal hash function from a shared key space like Eq. (3) to the message space. By employing the key-exchange protocol in Section 3.1, we construct a new MPKC scheme as follows:

(1) Key generation:

(a) Alice runs $\mathcal{G}(1^\lambda)$ to obtain $(\mathbb{F}_q, \boldsymbol{T}, \boldsymbol{U}, \boldsymbol{F})$.

(b) Alice chooses $\boldsymbol{T}_\mathrm{a} \in \mathcal{K}_T$ and $\boldsymbol{U}_\mathrm{a} \in \mathcal{K}_U$ at random, and computes $\boldsymbol{G}_\mathrm{a} = \boldsymbol{T}_\mathrm{a} \circ \boldsymbol{F} \circ \boldsymbol{U}_\mathrm{a}$.

(c) Public key is $\boldsymbol{G}_\mathrm{a}$ and private key is $(\boldsymbol{T}_\mathrm{a}, \boldsymbol{U}_\mathrm{a})$.

(2) Encryption: Bob uses Alice's public key $\boldsymbol{G}_\mathrm{a}$ to encrypt a message $\boldsymbol{M} \in \{0,1\}^\ell$.

(a) Bob chooses $\boldsymbol{T}_k \in \mathcal{K}_T$ and $\boldsymbol{U}_k \in \mathcal{K}_U$ at random and computes $\boldsymbol{G}_{\mathrm{a}k} = \boldsymbol{T}_k \circ \boldsymbol{G}_\mathrm{a} \circ \boldsymbol{U}_k$.

(b) Bob computes $\boldsymbol{G}_k = \boldsymbol{T}_k \circ \boldsymbol{F} \circ \boldsymbol{U}_k$ and $\boldsymbol{C} = \boldsymbol{M} \oplus H(\boldsymbol{G}_{\mathrm{a}k})$.

(c) Ciphertext is $(\boldsymbol{G}_k, \boldsymbol{C})$.

(3) Decryption: Alice uses the private key $(\boldsymbol{T}_\mathrm{a}, \boldsymbol{U}_\mathrm{a})$ to decrypt the ciphertext $(\boldsymbol{G}_k, \boldsymbol{C})$.

(a) Alice uses $(\boldsymbol{T}_\mathrm{a}, \boldsymbol{U}_\mathrm{a})$ to compute $\boldsymbol{G}_{k\mathrm{a}} = \boldsymbol{T}_\mathrm{a} \circ \boldsymbol{G}_k \circ \boldsymbol{U}_\mathrm{a}$.

(b) Then Alice computes $\boldsymbol{M} = \boldsymbol{C} \oplus H(\boldsymbol{G}_{k\mathrm{a}})$.

It is not hard to see that the encryption scheme is correct: Since $\boldsymbol{T}_\mathrm{a}$ and $\boldsymbol{T}_k$ commute (respectively, $\boldsymbol{U}_\mathrm{a}$ and $\boldsymbol{U}_k$), Alice obtains $\boldsymbol{G}_{k\mathrm{a}} = \boldsymbol{T}_\mathrm{a}\boldsymbol{T}_k \circ \boldsymbol{F} \circ \boldsymbol{U}_k\boldsymbol{U}_\mathrm{a} = \boldsymbol{G}_{\mathrm{a}k}$ and hence $\boldsymbol{C} \oplus H(\boldsymbol{G}_{k\mathrm{a}}) = \boldsymbol{C} \oplus H(\boldsymbol{G}_{\mathrm{a}k}) = \big(\boldsymbol{M} \oplus H(\boldsymbol{G}_{\mathrm{a}k})\big) \oplus H(\boldsymbol{G}_{\mathrm{a}k}) = \boldsymbol{M}$.

4 Security Analysis

In this section, we analyze the security of the proposed key-exchange protocol and encryption scheme.

4.1 Security proof

We next prove the security of our key agreement protocol in the presence of an eavesdropper. The proof method is similar to that of Katz and Lindell[36]. We first give some formalization definitions. Let Π denote a key-exchange protocol, $\mathcal{A}$ an adversary, and λ the security parameter. We define the following key-exchange experiment $\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda)$:

(1) Two parties holding the security parameter 1^λ execute protocol Π. This execution generates a transcript **trans** including all the messages sent by the parties, and a key k established by each of the parties.

(2) A bit $b \leftarrow \{0,1\}$ is chosen at random. If $b = 0$ then choose a bit string $\hat{k} \leftarrow \{0,1\}^\lambda$ uniformly at random, and if $b = 1$ set $\hat{k} := k$.

(3) $\mathcal{A}$ is given **trans** and $\hat{k}$, and outputs a bit b'.

(4) We say that $\mathcal{A}$ succeeds if $b' = b$, and is denoted by $\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda) = 1$.

Note that $\mathcal{A}$ being given the **trans** implies that he (or she) eavesdrops on the entire execution of the protocol. We say that $\mathcal{A}$ breaks Π successfully if he (or she) can correctly determine the key k and a completely random bit string $\hat{k}$. On the contrary, we conclude that Π is secure if the adversary succeeds with probability that at most negligibly greater than 1/2. That is the following security definition:

Definition 5 A key exchange protocol Π is secure in the presence of eavesdropping adversaries if for all PPT adversaries $\mathcal{A}$ there exists a negligible function negl such that

$$\Pr[\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda) = 1] \leqslant \frac{1}{2} + \mathrm{negl}(\lambda).$$

We especially emphasize that our following proof is *less rigorous*. The main reason is that Definition 5 requires the output key to be indistinguishable from a completely random bit string, but we are only able to prove that the shared key established by two parties is indistinguishable from a random element of $\mathcal{SK}$ as Eq. (3). For now, we let $\widehat{\mathrm{KE}}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda)$ denote a modified experiment where if $b = 0$, the adversary $\mathcal{A}$ is given $\hat{k} \leftarrow \boldsymbol{G}_z$ instead of a random string, where $\boldsymbol{G}_z$ is chosen uniformly at random in $\mathcal{SK}$.

Let us now prove the security of the proposed protocol under the DMDH assumption.

Theorem 2 Based on the DMDH assumption, the proposed key exchange protocol is secure in the

presence of an eavesdropper (with respect to the modified experiment $\widehat{\mathrm{KE}}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda)$).

Proof Let $\mathcal{A}$ be a PPT adversary. Since $\Pr[b = 0] = \Pr[b = 1] = 1/2$, we can obtain the inequality like Formula (4).

$$\begin{aligned}
&\Pr[\widehat{\mathrm{KE}}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda) = 1] = \\
&\Pr[\widehat{\mathrm{KE}}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda) = 1 \wedge b = 1] + \\
&\Pr[\widehat{\mathrm{KE}}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda) = 1 \wedge b = 0] = \\
&\frac{1}{2} \cdot \Pr[\widehat{\mathrm{KE}}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda) = 1 \mid b = 1] + \\
&\frac{1}{2} \cdot \Pr[\widehat{\mathrm{KE}}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda) = 1 \mid b = 0] = \\
&\frac{1}{2} \cdot \Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_{xy}) = 1] + \\
&\frac{1}{2} \cdot \Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_z) = 0] = \\
&\frac{1}{2} \cdot \Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_{xy}) = 1] + \\
&\frac{1}{2} \cdot (1 - \Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_z) = 1]) = \\
&\frac{1}{2} + \frac{1}{2} \cdot (\Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_{xy}) = 1] - \\
&\Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_z) = 1]) \leqslant \\
&\frac{1}{2} + \frac{1}{2} \cdot |\Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_{xy}) = 1] - \\
&\Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_z) = 1]|
\end{aligned} \tag{4}$$

Assume that the DMDH problem is hard. By Definition 4, there exists a negligible function negl such that

$$|\Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_z) = 1] - \Pr[\mathcal{A}(\boldsymbol{F}, \boldsymbol{G}_x, \boldsymbol{G}_y, \boldsymbol{G}_{xy}) = 1]| \leqslant \mathrm{negl}(\lambda).$$

We conclude that

$$\Pr[\widehat{\mathrm{KE}}^{\mathrm{eav}}_{\mathcal{A},\Pi}(\lambda) = 1] \leqslant \frac{1}{2} + \frac{1}{2} \cdot \mathrm{negl}(\lambda),$$

which completes the proof. ■

Like the relationship between the Diffie-Hellman protocol and the ElGamal scheme, the new encryption scheme directly derives from the the proposed key-exchange protocol. We already analyzed the security of our proposed protocol. In fact, the new proposed encryption scheme is also CPA-secure, just like ElGamal, which will be stated in Theorem 3. Due to the limitations of space, proof details are omitted. A similar proof for the ElGamal encryption scheme can be found in Ref. [36].

Theorem 3 Based on the DMDH assumption, the proposed public-key encryption scheme is secure under a Chosen Plaintext Attack (CPA).

4.2 Possible attacks and complexity

The proposed schemes are similar to the Diffie-Hellman protocol and the ElGamal scheme in design, and have the following properties:

(1) Like the original Diffie-Hellman protocol, our key-exchange protocol is also insecure against active adversaries. In particular, it succumbs to *the well-known person-in-the-middle attack*. The reason comes from the lack of authentication of the temporary exchange public keys. In fact, it can be modified by digital signature or PKI-based techniques. However, this is outside of the scope of the paper.

(2) Our encryption schemes, like ElGamal, must use a different ephemeral key $(\boldsymbol{T}_k, U_k) \in \mathcal{K}_T \times \mathcal{K}_U$ for every session. If the same key $(\boldsymbol{T}_k, U_k)$ is used to encrypt M_1 and M_2 whose corresponding ciphertexts are (G_k, C_1) and (G_k, C_2), then M_2 can be easily obtained from (G_k, C_1, C_2) because $H(G_{k\mathrm{a}}) = M_1 \oplus C_1 = M_2 \oplus C_2$.

(3) By Section 4.1, the problem of breaking our schemes is equivalent to solving the MP problem and the CMDH problem, as breaking the Diffie-Hellman key-exchange scheme and the ElGamal scheme is equivalent to solving DL and CDH.

We now look at two natural attacks to evaluate the base problems: the MP problem and the proposed CMDH problem.

The first attack is to directly find the private key pair $(\boldsymbol{T}_{\mathrm{a}}, \boldsymbol{U}_{\mathrm{a}})$ from $\boldsymbol{G}_{\mathrm{a}}$ and $(\boldsymbol{T}_{\mathrm{b}}, \boldsymbol{U}_{\mathrm{b}})$ from $\boldsymbol{G}_{\mathrm{b}}$ for computing $\boldsymbol{G}_{\mathrm{ab}}$. We next consider how to recover $(\boldsymbol{T}_{\mathrm{a}}, \boldsymbol{U}_{\mathrm{a}})$ from $\boldsymbol{G}_{\mathrm{a}}$. Let $\boldsymbol{T}_{\mathrm{a}} = \sum_{i=1}^{m} \alpha_i \boldsymbol{T}^i + \alpha_0 \boldsymbol{I}_m$ and $\boldsymbol{U}_{\mathrm{a}} = \sum_{i=1}^{n} \beta_i \boldsymbol{U}^i + \beta_0 \boldsymbol{I}_n$ (In general, α_0 and β_0 are equal to 0 in order to assure that $\boldsymbol{T}_{\mathrm{a}}$ and $\boldsymbol{U}_{\mathrm{a}}$ are both singular, the same as $\boldsymbol{T}$ and $\boldsymbol{U}$). It is obvious that for any $\boldsymbol{x} \in \mathbb{F}_q^n$, we have

$$\boldsymbol{G}_{\mathrm{a}}(\boldsymbol{x}) - \boldsymbol{T}_{\mathrm{a}} \circ \boldsymbol{F} \circ \boldsymbol{U}_{\mathrm{a}}(\boldsymbol{x}) \equiv 0 \tag{5}$$

and can obtain the following q^n cubic equations with respect to $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ by substituting all $\boldsymbol{x} \in \mathbb{F}_q^n$ into Eq. (5).

$$\sum_{j,k,t} \xi^{(1)}_{ijkt} \alpha_j \beta_k \beta_t + \sum_{j,k} \xi^{(2)}_{ijk} \alpha_j \beta_k + \sum_{j,k} \xi^{(3)}_{ijk} \beta_j \beta_k + \sum_{j} \xi^{(4)}_{ij} \alpha_j + \sum_{j} \xi^{(5)}_{ij} \beta_j + \xi^{(6)}_{i} = 0 \tag{6}$$

where $1 \leqslant i \leqslant q^n$ and all coefficients are in $\mathbb{F}_q$.

Note that if one can choose

$$N = mn^2 + mn + \frac{n(n+1)}{2} + m + n$$

linearly independent equations from Eq. (6), then solving such an *overdefined* nonlinear system is easy by linearization[37], and the complexity is only $\mathcal{O}(N^6)$. However, the construction of such linearly independent equations is in essence an exhaustive search process, and thus it is not feasible. In fact, since $\boldsymbol{F}$ and $(\boldsymbol{T}_{\mathrm{a}}, \boldsymbol{T}_{\mathrm{b}})$ are both chosen at random, the problem of finding $(\boldsymbol{T}_{\mathrm{a}}, \boldsymbol{U}_{\mathrm{a}})$ from $\boldsymbol{G}_{\mathrm{a}}$ is viewed as a random instance of the *reduced* MP problem. The only difference is that the number of unknown variables of Eq. (6) is $m+n$; but it is m^2+n^2 for the general MP problem (to the best of our knowledge, the complexity of the only exhaustive search algorithm for solving this problem is about $\mathcal{O}(q^{n^2})$), and thus the expected complexity of recovering the private key attack is $\mathcal{O}(q^n)$.

The second attack is to find equivalent keys. Note that solutions to the MP problem are in fact not unique; we say that $(\boldsymbol{T}, \boldsymbol{U})$ and $(\boldsymbol{T}', \boldsymbol{U}')$ are equivalent keys of the MP problem derived from $\boldsymbol{F}$ if

$$\boldsymbol{T} \circ \boldsymbol{F} \circ \boldsymbol{U} = \boldsymbol{T}' \circ \boldsymbol{F} \circ \boldsymbol{U}'.$$

From the point of view of an attacker, we can see clearly that the first attack method is more difficult than recovering equivalent keys. For such analogous decompositions including product of polynomials and matrices, it is fairly difficult to recover *precisely* the corresponding unknown factors. Relatively speaking, an equivalent keys attack is always more feasible. Indeed, this is evidenced by the successful attack of some pioneering schemes such as the braid Diffie-Hellman scheme[23], SFLASH[34], and NSP[25].

Before discussing the equivalent key attack in the proposed schemes, we first introduce an important Lemma[38] as follows:

Lemma 1 Let the matrix $\boldsymbol{A} \in_R \mathcal{M}_n(\mathbb{F}_q)$ be given. Then the number of the solutions $\boldsymbol{X}$ of the equation $\boldsymbol{AX} = \boldsymbol{XA}$ satisfies

(1) $N_{\mathrm{A}}(n,q) = q^{n^2}$ when $\boldsymbol{A} = \boldsymbol{0}$ or $\boldsymbol{I}_n$, otherwise

(2) $q^n \leqslant N_{\mathrm{A}}(n,q) \leqslant q^{(n-1)^2+1}$.

The equivalent keys attack with our notations is that if an attacker can find an equivalent key pair $(\boldsymbol{T}'_{\mathrm{a}}, \boldsymbol{U}'_{\mathrm{a}})$ such that $\boldsymbol{G}_{\mathrm{a}} = \boldsymbol{T}'_{\mathrm{a}} \circ \boldsymbol{F} \circ \boldsymbol{U}'_{\mathrm{a}}$, and $\boldsymbol{T}'_{\mathrm{a}}$ and $\boldsymbol{T}_{\mathrm{b}}$ commute (respectively, $\boldsymbol{U}'_{\mathrm{a}}$ and $\boldsymbol{U}_{\mathrm{b}}$), then he (or she) can compute

$$\begin{aligned} \boldsymbol{T}'_{\mathrm{a}} \circ \boldsymbol{G}_{\mathrm{b}} \circ \boldsymbol{U}'_{\mathrm{a}} =& \boldsymbol{T}'_{\mathrm{a}} \circ (\boldsymbol{T}_{\mathrm{b}} \circ \boldsymbol{F} \circ \boldsymbol{U}_{\mathrm{b}}) \circ \boldsymbol{U}'_{\mathrm{a}} = \\ & \boldsymbol{T}_{\mathrm{b}} \circ (\boldsymbol{T}'_{\mathrm{a}} \circ \boldsymbol{F} \circ \boldsymbol{U}'_{\mathrm{a}}) \circ \boldsymbol{U}_{\mathrm{b}} = \\ & \boldsymbol{T}_{\mathrm{b}} \circ \boldsymbol{G}_{\mathrm{a}} \circ \boldsymbol{U}_{\mathrm{b}} = \boldsymbol{G}_{\mathrm{ab}} \end{aligned} \tag{7}$$

Let $\boldsymbol{U}'_{\mathrm{a}}$ be given and satisfy $\boldsymbol{U}'_{\mathrm{a}}\boldsymbol{U}_{\mathrm{b}} = \boldsymbol{U}_{\mathrm{b}}\boldsymbol{U}'_{\mathrm{a}}$. We know that finding $\boldsymbol{T}'_{\mathrm{a}}$ such that

$$\boldsymbol{G}_{\mathrm{a}}(\boldsymbol{x}) - \boldsymbol{T}'_{\mathrm{a}} \circ \boldsymbol{F} \circ \boldsymbol{U}'_{\mathrm{a}}(\boldsymbol{x}) = 0$$

is very easy for enough $\boldsymbol{x} \in \mathbb{F}_q^n$ if $\boldsymbol{T}'_{\mathrm{a}}$ exists. Clearly, that if such $\boldsymbol{T}'_{\mathrm{a}}$ exists and commutes with $\boldsymbol{T}_{\mathrm{b}}$, then the attacker succeeds. On the premise that $\boldsymbol{T}'_{\mathrm{a}}$ exists, according to Eq. (7) and Lemma 1, the success probability is

$$\Pr[\boldsymbol{T}'_{\mathrm{a}} | \boldsymbol{T}'_{\mathrm{a}}\boldsymbol{T}_{\mathrm{b}} = \boldsymbol{T}_{\mathrm{b}}\boldsymbol{T}'_{\mathrm{a}}] = \frac{N_{\boldsymbol{T}_{\mathrm{b}}}(m,q)}{q^{m^2}} \leqslant \frac{q^{(m-1)^2+1}}{q^{m^2}} \to 0 \tag{8}$$

where $N_{\boldsymbol{T}_{\mathrm{b}}}(m,q) \leqslant q^{(m-1)^2+1}$ because the private key $\boldsymbol{T}_{\mathrm{b}}$ is not equal to $\boldsymbol{0}$ or $\boldsymbol{I}_n$ in practice.

The security of our proposed schemes is based on the MP problem, only the exhaustive search algorithm is known to solve MP. But the complexity estimate provided for the IP problem is based on the TF algorithm[35], which is $\mathcal{O}(q^{n/2})$ for the C^* scheme[28], and $\mathcal{O}(q^{3n/2})$ for any central function in $\mathcal{MQ}(n,m,\mathbb{F}_q)$. Consequently, a conservative security estimate of our proposed schemes is at least $\mathcal{O}(q^{n/2})$.

Remark 2. Compared with the existing MPKC construction, the overriding advantage is that the central map in our construction is not required to be invertible, and thus can be chosen at random. There is also a drawback in that the matrices of the two sides we generated are not completely random in $\mathcal{M}_m(\mathbb{F}_q)$ or $\mathcal{M}_n(\mathbb{F}_q)$. That is to say, the security of our schemes is based on the reduced MP problem, but which is intractable like the above discussion.

5 Efficiency Analysis

In this section, we discuss the implementation details of the proposed encryption scheme, including sizes and implementation computation complexity.

Recall that the system parameter of our encryption scheme is $(\mathbb{F}_q, \boldsymbol{F}, \boldsymbol{T}, \boldsymbol{U})$, where $\boldsymbol{F} \in_R \mathcal{MQ}(n,m,\mathbb{F}_q)$, and two nonsingular matrices, $\boldsymbol{T} \in_R \mathcal{M}_m(\mathbb{F}_q)$ and $\boldsymbol{U} \in_R \mathcal{M}_n(\mathbb{F}_q)$, of which the degree of the minimal polynomial is attained in m and n, respectively. We can denote the proposed encryption scheme by a triple $(\mathbb{F}_q, n, m)$. The following discussions are about the implementation details of our encryption scheme, which is summarized in Table 1.

(1) The private key $\boldsymbol{T}_{\mathrm{a}}$ can be generated by an m-dimensional vector in $\mathbb{F}_q^m$ by Theorem 1, and $\boldsymbol{U}_{\mathrm{a}}$ by a corresponding n-dimensional vector in $\mathbb{F}_q^n$. Thus in practical, the size of the private key is only $(m+n)\log q$ bits.

(2) The size of the public key $\boldsymbol{G}_{\mathrm{a}}$ is at most $n(n+3)m\log q/2$ bits.

Table 1 The operating characteristics of our scheme.

	$(\mathbb{F}_q, n, m)$	$(\mathbb{F}_{2^{16}}, 12, 10)$
Plaintext	$(m+n)\log q$ bits	352 bits
Ciphertext	$n(n+3)mq/2 + (m+n)\log q$ bits	14 752 bits
Private key	$(m+n)\log q$ bits	352 bits
Public key	$n(n+3)m\log q/2$ bits	14 400 bits
Encryption	$\mathcal{O}(mn^4)$	162 878 Muls[a]
Decryption	$\mathcal{O}(mn^4)$	132 120 Muls[a]
Security	$\mathcal{O}(q^{n/2})$	2^{96}

Note: Muls[a] denotes the number of multiplication operation over $\mathbb{F}_{2^{16}}$.

(3) In order to obtain better security, we may set the bit length ℓ of $H(\boldsymbol{G}_{\mathrm{ak}})$ equal to $(m+n)\log q$, and thus the message length is also $(m+n)\log q$. That is equal to the size of the private key.

(4) Since the size of $\boldsymbol{G}_k$ is the same as that of $\boldsymbol{G}_{\mathrm{a}}$, the bit size of ciphertext $(\boldsymbol{G}_k, \boldsymbol{C})$ is equal to $n(n+3)m\log q/2 + (m+n)\log q$.

(5) The implementation of the scheme only involves in multiplication and addition in $\mathbb{F}_q$. In comparison with the cost of multiplication operations, addition operations are considered negligible. Thus we only compute multiplications in the following analysis.

- The key generation step consists in the generation of the matrices $(\boldsymbol{T}_{\mathrm{a}}, \boldsymbol{T}_{\mathrm{b}})$ and the creation of the MQ function $\boldsymbol{G}_{\mathrm{a}} = \boldsymbol{T}_{\mathrm{a}} \circ \boldsymbol{F} \circ \boldsymbol{U}_{\mathrm{a}}$. We know that the product of two $n \times n$ matrices requires n^3 multiplications in the worse case (in fact, the best known algorithm is $\mathcal{O}(n^c)$, where $c \simeq 2.3755$). So the first part has a complexity of $m^4 + m + n^4 + n$ multiplications in $\mathbb{F}_q$. The second part is
$$\Big((n+n^2)\frac{n(n+1)}{2} + n^2\Big)m + \frac{n(n+3)m}{2}m.$$
Hence the overall complexity is $\mathcal{O}(mn^4)$.
- The cost of the encryption step is the same as that of the key generation process. The decryption step only needs to construct the MQ function $\boldsymbol{G}_{k\mathrm{a}}$. Thus the complexity of these two steps is also $\mathcal{O}(mn^4)$.

Note that only $(m+n)\log q$ bits are encrypted at a time, which leads to the serious message expansion. Table 1 shows that it is close to a multiple of 40 for the proposed instance. Meanwhile, we know that public-key schemes are used essentially for identification and key management; thus, the scheme still has certain value in practice.

We propose a practical encryption scheme employing $(\mathbb{F}_{2^{16}}, 12, 10)$. As shown in Table 1, the time complexity of the best-known algorithms to break this instance is estimated to be more than 2^{80}. The encryption speed is about 2^{18} multiplications in $\mathbb{F}_{2^{16}}$, which is roughly estimated to be 2^{24} binary operations. And the corresponding decryption speed is roughly 2^{23}. As for the key size, the proposed scheme is greater than that of the ElGamal scheme. This is also a common shortcoming of all MPKC schemes, but compared with some classical MPKC schemes such as the SFLASH signature standard[39] (which has been fully broken[13, 34]), the key size of the proposed scheme is clearly smaller.

6 Conclusion and Future Work

In this paper we propose a new key-exchange protocol and a public-key cryptosystem based on the MP problem. The security of these two schemes is provably reducible to solving the base problem, the DMDH problem. Meanwhile these schemes are also viewed as a candidate for the post-quantum era with the quantum computing security. More importantly, we offer an original approach to design the MPKC scheme. Overall our proposed schemes achieve a good tradeoff between security, efficiency, and key size, and seem to be competitive with existing approaches.

As a further study, some possible improvements of our cryptographic schemes are:

(1) This paper introduces two new difficult problems, CMDH and DMDH. The relationship between them is similar to the relationship among DL, CDH, and DDH. That is, if MP can be easily solved, then CMDH can be easily solved, and that if one can solve CMDH then one can solve DMDH as well. But how to prove the converses is still an open problem. In particular, the practical hardness of CMDH and DMDH deserves a focused discussion of its own.

(2) A new MPKC signature scheme is left to study because we do not yet have such a scheme based on our new approach yet.

(3) The new technique of commuting matrices over a finite field is worth of deep study, for the key generation. To support our ideas, we briefly adopt the matrix polynomial method for commuting; but the key space seems to be a bit too small.

(4) We may try to increase the length of a plaintext block for reducing the message expansion. For example, perhaps we could directly remove the hash function $H\colon \mathcal{SK} \to \{0,1\}^{\ell}$ from our encryption scheme in Section 3.2, where

message M is encoded in an MQ function in $\mathcal{MQ}(n, m, \mathbb{F}_q)$. Then the message expansion is only double that of ElGamal. In brief, on the basis of the higher security offered by our scheme, how to reduce the message expansion deserves more attention.

Acknowledgment

The authors would like to thank anonymous referees for their valuable comments. This work was supported by the National Natural Science Foundation of China (Nos. 61303212, 61303024, 61170080, 61501333, 61303024, and 61332019) and the Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-14-002).

References

[1] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. on Info. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[2] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, An efficient protocol for authenticated key agreement, *Designs, Codes and Cryptography*, vol. 28, no. 2, pp. 119–134, 2003.

[3] K. Hu, J. Xue, C. Hu, R. Ma, and Z. Li, An improved ID-based group key agreement protocol, *Tsinghua Science and Technology*, vol. 19, no. 5, pp. 421–428, 2014.

[4] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Computer*, vol. 26, no. 5, pp. 1484–1509, 1997.

[5] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Springer-Verlag, 2009.

[6] J. T. Ding, J. E. Gower, and D. S. Schmidt, *Multivariate Public Key Cryptosystems*. Springer-Verlag, 2006.

[7] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. Freeman, 1979.

[8] J. Patarin and L. Goubin, Trapdoor one-way permutations and multivariate polynomials, in *Proc. ICICS1997*, 1997, pp. 356–368.

[9] C. Berbain, H. Gilbert, and J. Patarin, QUAD: A practical stream cipher with provable security, in *Proc. EUROCRYPT2006*, 2006, pp. 109–128.

[10] H. Z. Wang, H. G. Zhang, and Q. H. Wu, Design theory and method of multivariate hash function, *SCIENCE CHINA Information Sciences*, no. 10, pp. 1977–1987, 2010.

[11] K. Sakumoto, T. Shirai, and H. Hiwatari, Public-key identification schemes based on multivariate quadratic polynomials, in *Proc. CRYPTO2011*, 2011, pp. 706–723.

[12] O. Billet and M. R. Gilles, Cryptanalysis of the square cryptosystems, in *Proc. ASIACRYPT 2009*, 2009, pp. 451–468.

[13] V. Dubois, P. A. Fouque, A. Shamir, and J. Stern, Practical cryptanalysis of SFLASH, in *Proc. Crypto2007*, 2007, pp. 1–12.

[14] L. Goubin and N. T. Courtois, Cryptanalysis of the TTM cryptosystem, in *Proc. ASIACRYPT2000*, 2000, pp. 44–57.

[15] C. D. Tao, A. Diene, S. H. Tang, and J. T. Ding, A simple matrix scheme for encryption, in *PQC2013*, 2013, pp. 231–242.

[16] H. Z. Wang and H. G. Zhang, Extended multivariate public key cryptosystems with secure encrytion fuction, *SCIENCE CHINA Information Sciences*, no. 6, pp. 1161–1171, 2011.

[17] K. Sakumoto, T. Shirai, and H. Hiwatari, On provable security of UOV and HFE signature schemes against Chosen-Message attack, in *Proc. PQC2011*, 2011, pp. 68–82.

[18] I. Anshel, M. Anshel, and D. Goldfeld, An algebraic method for public-key cryptography, *Math Research Letters*, 1999, vol. 6, no. 3, pp. 287–291

[19] I. Anshel, M. Anshel, and D. Goldfeld, New key agreement protocols in braid group cryptography, in *Proc. CT-RSA2001*, 2001, pp. 1–15

[20] A. Myasnikov, V. Shpilrain, and A. Ushakov, A practical attack on a Braid group based cryptographic protocol, in *Proc. Crypto2005*, 2005, pp. 86–96.

[21] A. Myasnikov and A. Ushakov, Length based attack and Braid groups: Cryptanalysis of Anshel-Anshel-Goldfeld Key exchange protocol, in *Proc. PKC2007*, 2007, pp. 76–88

[22] K. Ko, S. Lee, J. Cheon, J. Han, J. Kang, and C. Park, New pulic-key cryptosystem using Braid groups, in *Proc. Crypto2000*, 2000, pp. 166–183.

[23] J. H. Cheon and B. Jun, A polynomial time algorithm for the Braid Diffie-Hellman conjugacy problem, in *Proc. Crypto2003*, 2003, pp. 212–215.

[24] D. Boucher, P. Gaborit, W. Geiselmann, O. Ruatta, and F. Ulmer, Key exchange and encryption schemes based on non-commutative skew polynomials, in *Proc. PQCrypto2010*, 2010, pp. 126–141.

[25] V. Dubois and J. G. Kammerer, Cryptanalysis of cryptosystems based on non-commutative skew polynomials, in *Proc. PKC 2011*, 2011, pp. 459–472.

[26] C. H. Bennett and G. Brassard, An update on quantum cryptography, in *Proc. CRYPTO1984*, 1984, pp. 475–480.

[27] C. Bennett, Quantum cryptography using any two nonorthoganol states, *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, 1992.

[28] T. Matsumoto and H. Imai, Public quadratic polynomial-tuples for efficient signature verification and message encryption, in *Proc. EUROCRYPT1988*, 1988, pp. 419–453.

[29] J. Patarin, Hidden field equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms, in *Proc. EUROCRYPT1996*, 1996, pp. 33–48.

[30] C. Bouillaguet, J. C. Faugère, P. A. Fouque, and L. Perret, Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem, in *Porc. PKC2011*, 2011, pp. 473–493.

[31] L. Francoise and F. Ludovic, Polynomial equivalence problems and applications to multivariate cryptosystems, in *Proc. INDOCRYPT 2003*, 2003, pp. 235–251.

[32] D. Lin, J. C. Faugère, L. Perret, and T. Wang, On enumeration of polynomial equivalence classes and their application to MPKC, *Finite Fields and Their Applications*, vol. 18, no. 2, pp. 283–302, 2012.
[33] J. C. Faugère and L. Perret, Polynomial equivalence problems: Algorithmic and theoretical aspects, in *Proc. EUROCRYPT2006*, 2006, pp. 30–47.
[34] P. A. Fouque, G. Macario-Rat, and J. Stern, Key recovery on hidden monomial multivariate schemes, in *Proc. EUROCRYPT2008*, 2008, pp. 19–30.
[35] J. Patarin, L. Goubin, and N. Courtois, Improved algorithms for isomorphisms of polynomials, in *Proc. EUROCRYPT1998*, 1998, pp. 184–200.
[36] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman & Hall/CRC, 2007.
[37] N. Courtois and J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, in *Proc. Asiacrypt 2002*, 2002, pp. 267–287.
[38] H. Jin, Struction of matrices space exchangeable for given matrix, *Mathematical Theory and Applications*, vol. 21, no. 3, pp. 40–44 , 2001.
[39] M. Akkar and N, Courtois, A fast and secure implementation of SFLASH, in *Proc. PKC2003*, 2003, pp. 267–278.

Houzhen Wang is currently an assistant professor in the Computer School, Wuhan University, China. He received the PhD degree from Wuhan University in 2010. From 2015 to 2016, he was a visiting researcher at the University of Victoria. His research interests include cryptography and information security.

Huanguo Zhang is currently a professor and PhD supervisor in the Computer School, Wuhan University, China. He received the BS degree from Xidian University in 1970. His main research interests include information security, cryptography, and trusted computing.

Shaowu Mao is a PhD student in the Computer School, Wuhan University, China. He received the MS degree from Wuhan University in 2011. His current research interests include cryptography and information security.

Wanqing Wu is a PhD student in the Computer School, Wuhan University, China. He received the MS degree from Hebei University in 2008. His current research interests include cryptography and information security.

Liqiang Zhang is currently an assistant professor in the Computer School, Wuhan University, China. He received the PhD degree from Wuhan University in 2008. His research interests include trust computing and information security.