AIMS Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 9(8): 22197–22212.
DOI: 10.3934/math.20241079
Received: 07 March 2024
Revised: 20 June 2024
Accepted: 02 July 2024
Published: 16 July 2024

Research article

Simple PKE schemes from the TSPEM problem

Limin Zhou[1,*] **and Qiuyang Wang**[2]

[1] Department of Mathematics, Shandong University of Aeronautics, Shandong, 256603, China

[2] School of Computer Science and Technology, Tianjin Key Laboratory of Autonomous Intellgience Technology and System. Tiangong University, Tianjin, 300387, China

[*] **Correspondence:** Email: zhoulimin.s@163.com.

Abstract: In the quantum era, the advent of quantum computers poses significant threats to the security of current cryptosystems. Therefore, designing quantum-resistant cryptoschemes becomes important to guarantee information security. This work concentrates on the development of the post-quantum public key encryption (PKE) scheme. Non-commutative cryptography (NCC) has entered the field of post-quantum cryptography. We utilize the TSPEM problem with asymmetric structures (which serve as a potential candiate for resisting quantum attacks) to construct two PKE schemes which are demonstrated to be CPA security under the DTSPEM assumption. By representing the plaintext as a matrix, these schemes can effectively encrypt a significant amount of information in a single operation. Assuming an equal amount of messages for encryption, the proposed schemes acheive superior efficiency compared to existing PKE schemes. Structurally, our systems exhibit a level of synchronization and coexistence due to the distinct public keys (P) and ciphertexts (C_1). The efficiency analysis is conducted by comparing known schemes from the aspect of specific cryptographic indicators. Generally, the proposed ones offer several advantages including provable security, high efficiency, potential quantum-resistant, and relative ease of implementation; along with synchronization and coexistence. Our investigation has established the feasibility of constructing PKE schemes based on the TSPEM problem, specifically for asymmetric communication scenarios. The preliminary results pave the way for further exploration of the TSPEM problem′s potential in developing other cryptosystems suitable for quantum computing environments.

Keywords: PKE; DTSPEM assumption; CPA-secure; quantum attack
Mathematics Subject Classification: 06D50

1. Introduction

In recent years, the development of new information sciences, such as quantum information science and the emergence of quantum computers have brought computing power capable of breaking classical cryptographic schemes. Since the pioneering works [1, 2], a new goal has been set: to build a general theory of security against quantum computers which pose a significant threat to current traditional cryptosystems. To address this challenge, cryptosystems should be based on mathematical problems that are intractable for quantum computers, making them resilient against quantum attacks. As a result, a large number of cryptoschemes have been developed and various cryptographic primitives have been designed to withstand quantum attacks.

Recent advances in quantum computing have shown the possibility of new types of attacks. To counter this, candidates for cryptographic schemes resistant to quantum computers have actually emerged, such as lattice-based schemes [3] and multivariate polynomial-based schemes [4]. Non-commutative cryptography (NCC), an abbreviation for cryptography based on non-commutative algebraic structures, has also entered the field of post-quantum cryptography. The mathematical platform of cryptography research, where "commutativity" has been extended to "noncommutativity", is a product of interdisciplinary development, including quantum computing, combinatorial group theory, computational complexity theory and so on. NCC schemes utilize more complex algebraic structures, making them more challenging to analyze and attack. The security of NCC schemes and their underlying methods, primitives, and structures are based on algebraic structures, such as groups, rings, semiring and matrix groups/rings. Among these, matrix groups/rings have been particularly promising.

The prevailing view [5–7] is that NCC can resist attacks from quantum computers. This is because no known quantum polynomial-time algorithms exist to solve NP-hard problems involved in non-commutative algebraic structures with well-established results [8–10]. The non-commutative algebraic structures enable the design of more intricate cryptoschemes with enhanced security features. Quantum computers struggle to efficiently solve non-commutative algebraic problems, making NCC a promising approach with a higher level of security and flexibility compared to traditional methods. The most significant advantage of NCC is its demonstrated resistance to quantum computer attacks. Several NCC schemes have already emerged (e.g., [5–7, 11–17]), showing the potential of NCC.

NCC systems have emerged as a promising defense against attackers wielding quantum computing power. This growing field has seen the development of numerous NCC schemes [11, 12, 14, 15] suitable for applications like asymmetric key exchange protocols in asymmetric ambience. However, constructing encryption schemes with asymmetric structures remains an open challenge. Similarly, building Elgamal-like PKE schemes within asymmetric cryptosystems presents significant difficulties.

NCC offers a potential approach to designing cryptoschemes by leveraging non-commutative algebraic structures, such as non-commutative groups and rings. These structures, defined by specific non-commutative operations, are inherently resistant to quantum attacks. Implementing NCC in an asymmetric setting, crucial for scenarios like cloud computing and the Internet of Things (IoT), presents a distinct challenge for asymmetric communication to transmit messages and necessitates new problem formulations. Despite the challenges, achievements have been made. In 2009, Wu [12] proposed an asymmetric group key agreement protocol. In 2018, Yu [13] utilized the matrix decomposition problem to analyze an asymmetric encryption scheme. Most recently, Wang [14] introduced an asymmetric computing key exchange protocol. In 2014, Mao [15] leveraged the ergodic matrix problem and the tensor decomposition problem to propose an NP-hard (non-deterministic polynomial time, NP) problem which was only suitable for a symmetric key exchange protocol as a candidate for quantum-resistant.

Specifically, in accordance with some sets with certain non-commutative operations like the matrix multiplication and tensor product, the knapsack problem, the tensor decomposition problem, the ergoric problem, and the inherent difficulty of NP-complete (NPC) problems [18–21], Mao [11] proposed the tensor and subset-product of the ergodic matrix (TSPEM) problem including the computational TSPEM (CTSPEM) problem and the decisional TSPEM (DTSPEM) problem, constructing an asymmetric TSPEM-based key exchange protocol as a candidate for resisting quantum attacks. The appeal of the TSPEM-based protocol [11] lies in its use in asymmetric settings and its potential to resist quantum computing due to its underlying algebraic structures and computational complexity. The TSPEM problem [11] has the potential to open new fields in NCC as quantum-resistant candidates in non-commutative environments.

The TSPEM problem can be effectively employed in asymmetric communication scenarios [11], such as cloud computing and IoT, where devices like communication between servers and mobile terminals. This approach presents a benefit: compared to traditional key establishment methods, at an equivalent security level, one participant (typically the mobile device) involved requires substantially less computational power and key storage space. The suitability of the TSPEM problem for establishing asymmetric-computing keys [11] is particularly evident in cloud computing and IoT applications, where communication often occurs between mobile devices with limited resources (like computational capability) and powerful servers. The asymmetric nature of the TSPEM problem leverages this disparity, allowing the mobile device to participate with minimal resource consumption for non-commutative circumstances.

Inspired by work [11], we explore the application of the TSPEM problem to construct encryption schemes, and achieve the goal by incorporating Elgamal-like techniques and methods from the TSPEM problem. Rigorous analysis shows that the proposed PKE schemes are provably secure, highly efficient and potentially resistant to quantum attacks, and simultaneously provide positive responses to the challenges in post-quantum cryptography.

The basic security model for the PKE scheme was chosen-plaintext attack (CPA) security model [22] in which an adversary has access to an encryption oracle to try to "break" the scheme. The CPA security [22] is a very useful concept for the PKE scheme and sufficient for many encryption applications in the presence of some attackers, enabling it to be widely accepted as the standard security notion for encryption schemes. Notably, there exist many PKE schemes, such as those in [3, 4], that achieve CPA security. We will strive to design new CPA-secure PKE schemes based on [11].

Building upon [11], we utilize the TSPEM problem to construct two PKE schemes and analyze their CPA security based on the DTSPEM assumption and performance. Intuitively, the plaintexts are represented by matrices, allowing for the efficient encryption of a significant amount of information in a single operation. The efficiency is indeed achieved owing to the asymmetric algebraic structure of the TSPEM problem [11]. The two PKE schemes have interrelated structures and dissimilar public keys and ciphtertexts. On the one hand, the public key P of PKE I is different from that of PKE II, and their ciphertexts C_1 also differ. On the other hand, P of PKE I is regarded as C_1 of PKE II; and C_1 of PKE I is equivalent to P of PKE II. In essence, PKE I and PKE II are synchronized, coexistent, and complementary to each other, making them well-suited for asymmetric environments. Furthermore, from the standpoint of their algebraic structures and computational complexity, PKE *I* and PKE *II* exhibit promising potential for resisting quantum attacks.

The proposed PKE schemes are necessary for both theoretical and practical applications in modern non-commutative communication such as cloud computing and IoT. Their design has attracted much interest to construct NCC primitives as having potential candidates for post-quantum cryptography in non-commutative settings, which is supported by their inherent algebraic structures and computational complexity. Our current work focuses on the CPA security, leaving the investigation of more advanced attacks, such as chosen ciphertext attack (CCA) security, in future work. There might be other conceived cryptographic primitives based on the TSPEM problem, like signatures and key encapsulation mechanisms, not explore them here. Hitherto, developing new cryptosystems based on the TSPEM problem to resist quantum computing remains an active area of research. We will prioritize addressing these challenges in future work.

The remainder of the article is structured as follows. Section 2 provides some definitions and properties related to the TSPEM problem [11]. Section 3 introduces our PKE schemes and demonstrates their CPA security [22]. Section 4 analyzes the performance of our schemes. Conclusion is presented in Section 5.

2. Preliminaries

Let F_q denote a finite field. We represent $n \times n$ matrices over a finite field as $F_q^{n\times n}$. The symbol $\otimes$ denotes tensor-product operation in F_q. All computations are performed modulo q in F_q.

Review the TSPEM problem and its related NPC hard problems [11], the bounded knapsack problem, the tensor decomposition problem, and the ergodic matrix problem (EMP), along with their relative NPC problems as presented in [19, 20, 23].

Tensor of Matrix [20]. *Given two matrices $A = [a_{i,j}]_{m\times n}$ and $B = [b_{ij}]_{k\times l}$, tensor $(A \otimes B)_{mk\times nl}$ includes mk rows and nl columns, if it can be expressed as a block matrix, a block (i, j) in $(A \otimes B)_{mk\times nl}$ is a $k \times l$ matrix $a_{ij}B$. Some properties of the tensor product of matrices are given in F_q:*

1. $(A \otimes_q B) \otimes_q C = A \otimes_q (B \otimes_q C)$ (the properties of the tensor product can be expanded to more than three matrices);
2. $(A\otimes_q B)(C\otimes_q D) = AC\otimes_q CD)$, where the dimensions of A, B, C and D are $m_1\times n_1$, $m_2\times n_2$, $n_1\times n_3$, and $n_2 \times n_4$, respectively.

Ergodic Matrix [23]. *Given a matrix $Q \in F_q^{n\times n}$, for $\forall v \in F_q^n\backslash\{O\}$, if $\{Qv, Q^2v, \cdots, Q^{q^n}v\}$ just traverses $F_q^n\backslash\{O\}$, then Q is an ergodic matrix.*

The problem of subset-product of ergodic matrix (SPEM) and its variants, and the problem of tensor of ergodic matrix (TEM) and its difficulty refer to **Lemma 1.1–Lemma 1.4** [11].

Lemma 1.1. *Choose randomly $M \in F_q^{n\times m}\backslash\{O\}$, for the uniformly chosen random m matrix pairs $(X_1, Y_1), \cdots, (X_m, Y_m)$, where $X_i, Y_i \in F_q^{n\times m}\backslash\{O\}, i = 1, \cdots, m$, $(X_1 \otimes_q M \otimes Y_1, \cdots, X_m \otimes_q M \otimes Y_m)$ is known, solving M is difficult, and the difficulty is unaffected by a value of m.*

Lemma 1.2. *For an ergodic matrix $Q \in F_q^{n\times n}$, choose uniformly at random $M \in F_q^{n\times n}\backslash\{O\}$, $x_1, \cdot\cdot$*

$\cdot, x_m \in F_{q^n}$ and $y_1, \cdots, y_m \in F_{q^n}$. ($a$) $Q^{x_1} \otimes_q M \otimes_q Q^{y_1}$ is known to solve for x_1, y_1, and M; and (b) $(Q^{x_1} \otimes_q M \otimes_q Q^{y_1}, \cdots, Q^{x_m} \otimes_q M \otimes_q Q^{y_m})$ is known to solve for x_1, y_1, and M. Here, both (a) and (b) have the same difficulty.

Lemma 1.3. *For an ergodic matrix $Q \in F_q^{n\times n}$, choose uniformly at random $M \in F_q^{n\times n}\backslash\{O\}$, $x_1, \cdots, x_m \in F_{q^n}$, $y_1, \cdots, y_m \in F_{q^n}$ and $k, l \in F_{q^n}$. (a) $Q^{kx_1} \otimes_q M \otimes_q Q^{ly_1}$ is known to solve for k, l, and M; and (b) $(Q^{kx_1} \otimes_q M \otimes_q Q^{ly_1}, \cdots, Q^{kx_m} \otimes_q M \otimes_q Q^{ly_m})$ is known to solve for k, l, and M. The two problems have the same difficulty.*

Lemma 1.4. *For $m > 2n$, given an ergodic matrix $Q \in F_q^{n\times n}$, choose uniformly at random $x_1, \cdots, x_m \in F_{q^n}$ and $\tilde{x}_1, \cdots, \tilde{x}_m \in F_{q^n}$. Compute $Q_1 = Q^{x_1}, \cdots, Q_m = Q^{\tilde{x}_m}$ and $\tilde{Q}_1 = Q^{\tilde{x}_1}, \cdots, \tilde{Q}_m = Q^{\tilde{x}_m}$ in $F_q^{n\times n}$. Choose uniformly at random $r = (r_1, \cdots, r_m) \in \{0, 1\}^m, \|r\| \le poly(n)$ or the hamming weight is less than a given bound, when $(\prod_{i=1}^{m} Q_i^{r_i}, \prod_{i=1}^{m} \tilde{Q}_i^{r_i})$ is known, solving $r \in \{0, 1\}^m$ is difficult.*

Present the DTSPEM problem and assumption [11].

DTSPEM problem. *For $m > 2n \log q$, given an ergodic matrix $Q \in F_q^{n\times n}$, choose uniformly at random $x_1, \cdots, x_m \in F_{q^n}$ and $\tilde{x}_1, \cdots, \tilde{x}_m \in F_{q^n}$, compute $Q_1 = Q^{x_1}, \cdots, Q_m = Q^{x_m}$ and $\tilde{Q}_1 = Q^{\tilde{x}_1}, \cdots, \tilde{Q}_m = Q^{\tilde{x}_m}$ in $F_q^{n\times n}$. Choose uniformly at random $r = (r_1, \cdots, r_m) \in \{0, 1\}^m$ $(wt(r) = s)$ and $M \in F_q^{n\times n} \setminus \{\mathrm{O}\}$. If*

$$(Q_1^k \otimes_q M \otimes \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes \tilde{Q}_m^l, \prod_{i=1}^{m} Q_i^{r_i}, \prod_{i=1}^{m} \tilde{Q}_i^{r_i}, A \otimes_q B \otimes_q C)$$

are known, decide $A \otimes_q B \otimes_q C = \prod_{i=1}^{m} Q_i^{kr_i} \otimes_q M^s \otimes_q \prod_{i=1}^{m} \tilde{Q}_i^{lr_i}$ or not, where A, B, and C are chosen uniformly at random.

DTSPEM assumption. For sufficiently large security parameter n and a probability polynomial time (PPT) adversary $\mathcal{A}$,

$$\begin{aligned} &|Pr[(\mathcal{A}(P, F, f(n, l, M), g(r), A \otimes_q B \otimes_q C) = 1] - \\ &Pr[(\mathcal{A}(P, F, f(n, l, M), g(r), \prod_{i=1}^{m} Q_i^{nr_i} \otimes_q M^s \otimes_q \prod_{i=1}^{m} \tilde{Q}_i^{lr_i}) = 1]| \\ &\le negl(n) \end{aligned}$$

holds, where

$$\begin{aligned} f(n, l, M) &= (Q_1^n \otimes_q M \otimes \tilde{Q}_1^l, \cdots, Q_m^n \otimes_q M \otimes \tilde{Q}_m^l), \\ g(r) &= (\prod_{i=1}^{m} Q_i^{r_i}, \prod_{i=1}^{m} \tilde{Q}_i^{r_i}), \end{aligned}$$

and $negl(n)$ is a negligible function.

Definition 1.5 CPA security.

Given a PKE scheme $\coprod = (Gen, Enc, Dec)$ and a PPT adversary $\mathcal{A}$, define the CPA game $(PubK_{cpa,\coprod}(\mathcal{A}))$ between $\mathcal{A}$ and a challenger C as follows [22].

Setup. C runs the key generation algorithm $KeyGen$ to generate keys (pk, sk). C gives the public key pk to $\mathcal{A}$ and keeps sk as the private key.

Oracle access phase. $\mathcal{A}$ adaptively selects plaintexts of his choice and queries the encryption oracle access repeatedly with these chosen plaintexts. The oracle responds with the corresponding ciphertexts.

Challenge phase. $\mathcal{A}$ submits two different messages M_0, M_1 with $|M_0| = |M_1|$ to C who chooses randomly $b \in \{0, 1\}$ and then sends the challenge ciphertext $C^* = Enc_{pk}(M_b)$ to $\mathcal{A}$ who can access the encryption many times.

Guess phase. $\mathcal{A}$ tries to guess $b' \in \{0, 1\}$ of b. If $b' = b$, $\mathcal{A}$ wins the CPA game and outputs 1; otherwise, $\mathcal{A}$ fails and outputs 0.

If for any PPT $\mathcal{A}$, the *advantage* $Adv_{cpa,\coprod}(\mathcal{A})$ of $\mathcal{A}$ satisfies

$$Adv_{cpa,\coprod}(\mathcal{A}) = |Pr[b = b'] - \frac{1}{2}| \leq negl(n),$$

the scheme $\coprod$ achieves CPA security (or is CPA-secure), where $negl(n)$ is negligible, and n is a security parameter.

Parameter selection. The parameters are chosen the same as that in [11], e.g., $m > 2n \log q$, where the dimension of the ergodic matrix is n; the dimension of the basic field F_q is m. Employ reasonable parameters, e.g., $(q, n, m) = (2^8, 3, 80)$, and n is the security parameter.

3. The construction

We will construct two PKE schemes, PKE I and PKE II, and analyze their CPA security.

In PKE I and PKE II, take as input 1^n and output F_q with order q, F_{q^n} with order q^n, and $F_{q^n}\backslash\{0\}$ with order $q^n - 1$. All computations are modulo q, e.g., $\mod q$.

3.1. PKE I

Setup. Given an ergodic matrix $Q \in F_q^{n\times n}$, choose $x_1, \cdots, x_m \in F_{q^n}$ and $\tilde{x_1}, \cdots, \tilde{x_m} \in F_{q^n}$ at random uniformly. Then, compute $Q_1 = Q^{x_1}, \cdots, Q_m = Q^{x_m}$ (for each two in $Q_1 = Q^{x_1}, \cdots, Q_m = Q^{x_m}$ should be irreversible) and $\tilde{Q}_1 = Q^{\tilde{x_1}}, \cdots, \tilde{Q}_m = Q^{\tilde{x_m}}$ (for each two in $\tilde{Q}_1 = Q^{\tilde{x_1}}, \cdots, \tilde{Q}_m = Q^{\tilde{x_m}}$ should be irreversible) in $F_q^{n\times n}$, and take them as public parameters.

KeyGen. Let $P = (Q_1^k \otimes_q M \otimes_q \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes_q \tilde{Q}_m^l)$ be the public key associated with the private keys $k, l \in F_{q^n}$, and $M \in F_q^{n\times n}$. The pubic key is constructed as $pk = (q, F_q, F_{q^n}, F_q^{n\times n}, F_q^{n^3\times n^3}, Q, P)$.

Encrypt. To encrypt a message $\tilde{M} \in F_q^{n^3\times n^3}$ using pk, first choose $r = (r_1, \cdots, r_m) \in \{0, 1\}^m$ at random uniformly, and then compute

$$C_1 = (\prod_{i=1}^{m} Q_i^{r_i}, \prod_{i=1}^{m} \tilde{Q}_i^{r_i}),$$

$$C_2 = \tilde{M} + \prod_{i=1}^{m} (Q_i^k \otimes_q M \otimes_q \tilde{Q}_i^l)^{r_i}.$$

Output the ciphertext $C = (C_1, C_2)$.

Decrypt. To decrypt $C = (C_1, C_2)$ with the private keys $k,\ l \in F_{q^n}$, and $M \in F_q^{n\times n}$, compute

$$\tilde{M} = C_2 - \prod_{i=1}^{m} (Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^{r_i})^l$$

using known $C_1 = (\prod_{i=1}^{m} Q_i^{r_i},\ \prod_{i=1}^{m} \tilde{Q}_i^{r_i})$.

Correctness. If PKE I is run honestly, the plaintext $\tilde{M}$ can be recovered successfully.

Based on the form of $C_1 = (\prod_{i=1}^{m} Q_i^{r_i},\ \prod_{i=1}^{m} \tilde{Q}_i^{r_i})$, compute

$$\begin{aligned} C_1' &= (\prod_{i=1}^{m} Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q (\prod_{i=1}^{m} \tilde{Q}_i^{r_i})^l \\ &= \prod_{i=1}^{m} (Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^{r_i})^l \end{aligned}$$

using the private keys $k, l \in F_{q^n}$, and $M \in F_q^{n\times n}$. This allows us to further obtain

$$\begin{aligned} C_2 - C_1' &= (\tilde{M} + \prod_{i=1}^{m} (Q_i^k \otimes_q M \otimes_q \tilde{Q}_i^l)^{r_i}) \\ &\quad - \prod_{i=1}^{m} (Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^{r_i})^l \\ &= (\tilde{M} + \prod_{i=1}^{m} (Q_i^k)^{r_i} \otimes_q M^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^l)^{r_i}) \\ &\quad - \prod_{i=1}^{m} (Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^{r_i})^l \\ &= \tilde{M} \end{aligned}$$

with $wt(r) = \lfloor \frac{m}{2} \rfloor$.

3.2. Security analysis of PKE I

Theorem 3.1 proves the CPA security of PKE I.

Theorem 3.1 *If the DTSPEM problem is hard for a PPT adversary $\mathcal{A}$, PKE I is CPA-secure.*

Proof. Let $\coprod$ denote PKE I. We prove that $\coprod$ achieves indistinguishable encryptions for an adversary $\mathcal{A}$, which implies that PKE I is CPA-secure. In the CPA game ($PubK_{cpa}(\mathcal{A})$) between $\mathcal{A}$ and the challenger C, $\mathcal{A}$ can make an arbitrary number of encryption queries and is given a challenge ciphertext for the distinguishability test.

If $\mathcal{A}$ can successfully break the CPA security of the PKE I, this implies that $\mathcal{A}$ has a non-negligible advantage in distinguishing ciphertexts. By exploiting this advantage during the CPA game, C can then interact with $\mathcal{A}$ to solve the DTSPEM problem with a non-negligible probability of success.

Setup. C runs $KeyGen(1^n)$ to generate the public key $P = (Q_1^k \otimes_q M \otimes_q \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes_q \tilde{Q}_m^l)$ to $\mathcal{A}$ and keeps $k, l \in F_{q^n}$, and $M \in F_q^{n\times n}$ as the private keys.

Oracle access. $\mathcal{A}$ is allowed to access the encryption oracles for any plaintext $\tilde{M}' \in F_q^{n^3\times n^3}$ of choice. Upon submitting a message, $\mathcal{A}$ receives either the corresponding ciphertext C' or $\perp$ (indicating an invalid query) as his accessed result. In other words, $\mathcal{A}$ submits the selected plaintexts to access encrypted oracles many times and obtains the corresponding results.

During the challenge stage, $\mathcal{A}$ can receive a 2-tuple $C = (C_1, C_2)$ where C_2 either equals the challenge ciphertext C_2^* below or a random value R uniformly chosen from $F_q^{n^3\times n^3}$. C performs the following challenge.

Challenge. C runs $KeyGen(1^n)$ to get the system parameters $(F_q, F_{q^n}, F_q^{n\times n}, F_q^{n^3\times n^3}, q, Q)$, selects randomly $k,\ l,\ k',\ l' \in F_{q^n}, M,\ M' \in F_q^{n\times n}$ and sets

$$\begin{aligned} C_1 &= (\prod_{i=1}^{m} Q_i^{r_i} \prod_{i=1}^{m} \tilde{Q}_i^{r_i}), \\ P &= (Q_1^k \otimes_q M \otimes_q \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes_q \tilde{Q}_m^l), \\ C_3 &= \prod_{i=1}^{m} (Q_i^k)^{r_i} \otimes_q M^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^l)^{r_i}, \\ (C_3 &= \prod_{i=1}^{m} (Q_i^{k'} \otimes_q M' \otimes_q \tilde{Q}_i^{l'})^{r_i} \\ &= \prod_{i=1}^{m} (Q_i^{k'})^{r_i} \otimes_q (M')^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^{l'})^{r_i}). \end{aligned}$$

Let $pk = (q, F_q, F_{q^n}, F_q^{n\times n}, F_q^{n^3\times n^3}, Q, P)$, $\mathcal{A}$ executes $\mathcal{A}(pk)$ to output two equal-length plaintexts $\tilde{M}_0,\ \tilde{M}_1 \in F_q^{n^3\times n^3} \backslash \{O\}$, and submits $\tilde{M}_0$, $\tilde{M}_1$ to C who chooses randomly $b \in \{0, 1\}$ and encrypts $\tilde{M}_b$ to get the challenge ciphertext $C^* = Enc_{pk}(\tilde{M}_b) = (C_1^*, C_2^*)$ which is then sent back to $\mathcal{A}$, where

$$\begin{aligned} C_1^* &= (\prod_{i=1}^{m} Q_i^{r_i},\ \prod_{i=1}^{m} \tilde{Q}_i^{r_i}), \\ C_2^* &= C_3 + \tilde{M}_b, \\ C_3 &= \prod_{i=1}^{m} (Q_i^k)^{r_i} \otimes_q M^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^l)^{r_i}, \\ (C_3 &= \prod_{i=1}^{m} (Q_i^{k'} \otimes_q M' \otimes_q \tilde{Q}_i^{l'})^{r_i}). \end{aligned}$$

C gives C^* to $\mathcal{A}$ and obtains $\mathcal{A}$'s output b' of b. If $b = b'$, C outputs 1; otherwise, C outputs 0.

If $C_2^* = \tilde{M}_b + \prod_{i=1}^{m} (Q_i^k)^{r_i} \otimes_q M^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^l)^{r_i}$, then C^* is the valid encryption of $\tilde{M}_b$ with the correct distribution (as $C_3 = \prod_{i=1}^{m} (Q_i^k)^{r_i} \otimes_q M^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^l)^{r_i}$ is a TSPEM problem tuple). In the case, $\mathcal{A}$ wins with a probability of $P[PubK_{cpa,\prod}(\mathcal{A}) = 1]$.

When C_3 (like $C_3 = \prod_{i=1}^{m}(Q_i^{k'} \otimes_q M' \otimes_q \tilde{Q}_i^{l'})^{r_i}$) is random uniformly in $F_q^{n^3 \times n^3}$, the challenge ciphertext C^* is independent of b from $\mathcal{A}'$s view. If C^* is randomly chosen from $F_q^{n^3 \times n^3} \times F_q^{n^3 \times n^3}$, there exists three cases.

Suppose that $\mathcal{A}$ receives a ciphertext $(C_1', C_2') \neq (C_1^*, C_2^*)$, where $(C_1', C_2') \in F_q^{n^3 \times n^3} \times F_q^{n^3 \times n^3}$ is uniformly distributed.

Case 1. Suppose that $(C_1', C_2') = (C_1^*, C_2')$ which means that $C_2' \neq C_2^*$. After receiving (C_1^*, C_2'), $\mathcal{A}$ attempts to compute

$$\tilde{M}_b' = C_2' - \prod_{i=1}^{m}(Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q \prod_{i=1}^{m}(\tilde{Q}_i{}^{r_i})^l.$$

Because $\mathcal{A}$ knows nothing about the private key k, l, M (according to lemma 1.2 and 1.3), he cannot obtain $\tilde{M}_b$ from C_1^* (since C_1^* has no relation to $\tilde{M}_b$). Therefore, C_2' is a random element which leads to (C_1^*, C_2') also being random.

Case 2. Suppose that $(C_1', C_2') = (C_1', C_2^*)$ which implies that $C_1^* \neq C_1'$. Although $\mathcal{A}$ knows C_2^*, he cannot know $\tilde{M}_b$ from C_2^* under the DTSPEM assumption. In addition, C_1' is inherently random for $\mathcal{A}$. Consequently, (C_1', C_2^*) is a random element.

Case 3. We introduce a modified version of $\coprod$, denoted by $\tilde{\coprod}$, where *KenGen* is exact as that in $\coprod$. In $\tilde{\coprod}$, to encrypt a message $\tilde{M}_b \in F_q^{n^3 \times n^3} \backslash \{O\}$ using the public key $pk = (F_q, F_{q^n}, F_q^{n \times n}, F_q^{n^3 \times n^3}, q, Q, P)$, first select k', $l' \in F_{q^n}$, and $M' \in F_q^{n \times n}$ at random uniformly, and output the ciphertext

$$(C_1', C_2') = ((\prod_{i=1}^{m} Q_i^{r_i},\ \prod_{i=1}^{m} \tilde{Q}_i^{r_i}), \tilde{M}_b + \prod_{i=1}^{m}(Q_i^{k'} \otimes_q M' \otimes_q \tilde{Q}_i^{l'})^{r_i}),$$

where $C_3 = \prod_{i=1}^{m}(Q_i^{k'} \otimes_q M' \otimes_q \tilde{Q}_i^{l'})^{r_i}$.

In $\tilde{\coprod}$, $\tilde{M}_b + \coprod_{i=1}^{m}(Q_i^{k'} \otimes_q M' \otimes_q \tilde{Q}_i^{l'})^{r_i}$ is a random element which is independent of $\tilde{M}_b$. (If k' and l' are chosen uniformly at random in F_{q^n} and $M' \in F_q^{n \times n}$ is at random uniformly, then $\prod_{i=1}^{m}(Q_i^{k'} \otimes_q M' \otimes_q \tilde{Q}_i^{l'})^{r_i}$ is random uniformly in $F_q^{n^3 \times n^3}$). Additionally, the first element, $(\prod_{i=1}^{m} Q_i^{r_i},\ \prod_{i=1}^{m} \tilde{Q}_i^{r_i})$, is not associative with $\tilde{M}_b$. As a result, the ciphertext (C_1', C_2') is independent of $\tilde{M}_b$ in $\tilde{\coprod}$ and has no connection with $\tilde{M}_b$.

As discussed above, $\mathcal{A}$ knows nothing about $\tilde{M}_b$ from (C_1', C_2') since C_1' contains no information about $\tilde{M}_b$ and C_2' is a random element in $F_q^{n^3 \times n^3}$ with k', $l' \in F_{q^n}$, $M' \in F_q^{n \times n}$ chosen at random. Namely, if

$$\begin{aligned} C_3 &= \prod_{i=1}^{m}(Q_i^{k'} \otimes_q M' \otimes_q \tilde{Q}_i^{l'})^{r_i} \\ &= \prod_{i=1}^{m}(Q_i^{k'})^{r_i} \otimes_q (M')^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m}(\tilde{Q}_i^{l'})^{r_i}, \end{aligned}$$

then $C_2' = C_3 + \tilde{M}_b$ becomes completely random from $\mathcal{A}'$s view. In short, (C_1', C_2') is independent of $\tilde{M}_b$ and reveals nothing about $\tilde{M}_b$. Therefore, in all three cases (case 1, case 2, and case 3), (C_1', C_2') appears random to $\mathcal{A}$. At this point, if $\mathcal{A}$ wins with a probability of $P[Pub_{cpa,\coprod_{1,2,3}}(\mathcal{A}) = 1]$, we have

$$P[Pub_{cpa,\coprod_{1,2,3}}(\mathcal{A}) = 1] = \frac{1}{2}.$$

Guess. $\mathcal{A}$ attempts to guess $\tilde{M}_b, b \in \{0,1\}$ corresponding to C^*. To achieve this, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ of b. Two scenarios exist.

1. Run *KeyGen* to get $(q, F_q, F_{q^n}, F_q^{n\times n}, F_q^{n^3\times n^3}, Q)$, select $x_1, \cdots, x_m, \tilde{x}_1, \cdots, \tilde{x}_m, k, l \in F_{q^n}, M \in F_q^{n\times n}$ and set

$$\begin{aligned} P &= (Q_1^k \otimes_q M \otimes_q \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes_q \tilde{Q}_m^l), \\ C_1 &= (\prod_{i=1}^{m} Q_i^{r_i}, \ \prod_{i=1}^{m} \tilde{Q}_i^{r_i}), \\ C_3 &= \prod_{i=1}^{m} (Q_i^k)^{r_i} \otimes_q M^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^l)^{r_i}, \\ C_2 &= C_3 + \tilde{M}_b. \end{aligned}$$

The public key is constructed as $pk = (q, F_q, F_{q^n}, F_q^{n\times n}, F_q^{n^3\times n^3}, Q, P)$, and the ciphertext is (C_1, C_2). In this scenario, $\mathcal{A}'$s view is identical to that in the real game $PubK_{cpa,\coprod}(n)$. If $b' = b$, C outputs 1. This implies that $C_3 = \prod_{i=1}^{m} (Q_i^k)^{r_i} \otimes_q M^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^l)^{r_i}$. We have that

$$Pr[\mathcal{A}(F_q, Q, P, C_1, C_3) = 1] = P[PubK_{cpa,\coprod}(\mathcal{A}) = 1].$$

2. Run *KeyGen* to get $(q, F_q, F_{q^n}, F_q^{n\times n}, F_q^{n^3\times n^3}, Q)$, select $x_1, \cdots, x_m, \tilde{x}_1, \cdots, \tilde{x}_m, k, l \in F_{q^n}, M \in F_q^{n\times n}$ and set

$$\begin{aligned} P &= (Q_1^k \otimes_q M \otimes_q \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes_q \tilde{Q}_m^l), \\ C_1 &= (\prod_{i=1}^{m} Q_i^{r_i}, \ \prod_{i=1}^{m} \tilde{Q}_i^{r_i}), \\ C_2 &= C_3 + \tilde{M}_b, \end{aligned}$$

where $C_2 \in F_q^{n^3\times n^3}$ is at random in all three cases (case 1, 2 and case 3). The public key is constructed as $pk = (q, F_q, F_{q^n}, F_q^{n\times n}, F_q^{n^3\times n^3}, Q, P)$, and the ciphertext is (C_1, C_2).

In this scenario, the view of $\mathcal{A}$ is exactly the same as $\mathcal{A}'$s view in all three cases, we have that

$$P[\mathcal{A}(F_q, Q, P, C_1, A \otimes B \otimes Z) = 1] = P[Pub_{cpa,\coprod_{1,2,3}}(\mathcal{A}) = 1] = \frac{1}{2},$$

where A, B, and $Z \in F_q^{n^3\times n^3}$ are random elements.

Under the DTSPEM assumption, there exists a $negl(n)$ such that

$$|P[\mathcal{A}(F_q, Q, P, C_1, A \otimes B \otimes Z) = 1] - Pr[\mathcal{A}(F_q, Q, P, C_1, C_3) = 1]| \leq negl(n).$$

Putting the above altogether, it follows that

$$Adv_{cpa,\coprod} = |P[b = b'] - \frac{1}{2}| \leq negl(n).$$

According to the definition of CPA security, PKE I is CPA-secure for any PPT $\mathcal{A}$ under the DTSPEM assumption.

This completes the proof of Theorem 3.1. □

3.3. PKE II

Setup. Given an ergodic matrix $Q \in F_q^{n\times n}$, select $x_1, \cdots, x_m \in F_{q^n}$ and $\tilde{x_1}, \cdots, \tilde{x_m} \in F_{q^n}$ uniformly at random. Then, compute $Q_1 = Q^{x_1}, \cdots, Q_m = Q^{x_m}$ (for each two in $Q_1 = Q^{x_1}, \cdots, Q_m = Q^{x_m}$ should be irreversible) and $\tilde{Q}_1 = Q^{\tilde{x_1}}, \cdots, \tilde{Q}_m = Q^{\tilde{x_m}}$ (for each two in $\tilde{Q}_1 = Q^{\tilde{x_1}}, \cdots, \tilde{Q}_m = Q^{\tilde{x_m}}$ should be irreversible) in $F_q^{n\times n}$, and take them as public parameters.

KeyGen. Let $P = (\prod_{i=1}^{m} Q_i^{r_i}, \prod_{i=1}^{m} \tilde{Q}_i^{r_i})$ be the public key associated with the private key $r = (r_1, \cdots, r_m) \in \{0,1\}^m$ $(wt(r) = \lfloor \frac{m}{2} \rfloor)$.

Encrypt. To encrypt $\tilde{M} \in F_q^{n^3\times n^3}$, choose at random uniformly k, $l \in F_{q^n}$, and $M \in F_q^{n\times n}$, and compute

$$C_1 = (Q_1^k \otimes_q M \otimes_q \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes_q \tilde{Q}_m^l),$$
$$C_2 = \tilde{M} + \prod_{i=1}^{m} (Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^{\ r_i})^l.$$

Output the ciphertext $C = (C_1, C_2)$.

Decrypt. To decrypt $C = (C_1, C_2)$ with the private key $r = (r_1, \cdots, r_m) \in \{0,1\}^m$ $(wt(r) = \lfloor \frac{m}{2} \rfloor)$, compute

$$\tilde{M} = C_2 - \prod_{i=1}^{m} (Q_i^k \otimes_q M \otimes_q \tilde{Q}_i^l)^{r_i}$$

using known $C_1 = (Q_1^k \otimes_q M \otimes_q \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes_q \tilde{Q}_m^l)$.

Correctness. If PKE II is run honestly, the plaintext $\tilde{M}$ can be recovered successfully.

Based on the form of C_1:

$$C_1 = (Q_1^k \otimes_q M \otimes_q \tilde{Q}_1^l, \cdots, Q_m^k \otimes_q M \otimes_q \tilde{Q}_m^l),$$

compute

$$C_1' = \prod_{i=1}^{m} (Q_i^k \otimes_q M \otimes_q \tilde{Q}_i^l)^{r_i}$$

using the private key $r = (r_1, \cdots, r_m) \in \{0,1\}^m$ $(wt(r) = \lfloor \frac{m}{2} \rfloor)$. This allows us to further obtain

$$
\begin{aligned}
C_2 - C_1' &= (\tilde{M} + \prod_{i=1}^{m} (Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i{}^{r_i})^l) \\
&- \prod_{i=1}^{m} (Q_i^k \otimes_q M \otimes_q \tilde{Q}_i^l)^{r_i} \\
&= (\tilde{M} + \prod_{i=1}^{m} (Q_i^{r_i})^k \otimes_q M^{\llcorner \frac{m}{2} \lrcorner} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i{}^{r_i})^l) \\
&- (\prod_{i=1}^{m} (Q_i^{kr_i}) \otimes_q M^{\sum_{i=1}^{m} r_i} \otimes_q \prod_{i=1}^{m} (\tilde{Q}_i^{lr_i})) \\
&= \tilde{M}
\end{aligned}
$$

with $wt(r) = \lfloor \frac{m}{2} \rfloor$.

3.4. Security analysis of PKE II

Theorem 3.2 presents the CPA security of PKE *II*.

Theorem 3.2 *If the DTSPEM problem is hard for a PPT $\mathcal{A}$, then PKE II is CPA-secure.*

Proof. The proof of Theorem 3.2 is similar to that of Theorem 3.1, we omit it here. □

4. Performance analysis

This section mainly provides a comparative analysis of security, computation, and storage cost between our schemes and several representative PKE schemes. Tables 1 and 2 compare ours with the PKE scheme [3] based on the learning with errors problem and the ergodic matrix-based PKE scheme [21].

It is common knowledge that any intricate problem with small parameters can be addressed through certain attacks. The size of m (not too small) [11] determines efficiency and security. From the practical perspective, we can select appropriate parameters for the implementation of the proposed schemes, e.g., employing $(q, n, m) = (2^8, 3, 80)$. The operations of our schemes mainly refer to matrix multiplication. and tensor-product. Both of them need $O(m)$ matrix multiplications and $2m + 2$ tensor products or so, thereby they possess high efficiency and ease of implementation in hardware and software, making it suitable for utilization in smart systems.

Computational complexity is measured by the number of multiplication operations over F_q. Specifically, *Pub.cost* refers to the computational overhead of generating a public key P, and other items can be treated similarly; $\log^2 q$ denotes the computational overhead of multiplication of two integers in F_q. Storage overhead stands for the size of system elements, where *priv.size* represents the size of the private key, and similarly for other items. *Com.alg.* is an abbreviation for a computational algorithm.

We compare PKE *I* with PKE *II* in Table 1 and Table 2. The *Pub.size* with $O(n^7 \log q)$ of PKE *I* is much bigger than $o(n^2 \log q)$ of PKE *II*. The *Priv.size*, $O(n^2 \log q)$ of PKE *I* is bigger than $O(n \log q)$ of PKE *II*. *Cipher.size* of PKE *II* is much bigger than that in PKE *I*. The *plain.size* of PKE *I* is the same as PKE II's. The $Pub.cost$ and $Dec.cost$ of PKE II can be expressed by $O(n^4 \log q)$, smaller than $O(n^5 \log^2 q)$ in PKE I. The $Enc.cost$, $O(n^5 \log^2 q)$ in PKE II is bigger than $O(n^4 \log q)$ of PKE I. These results indicate that their structures are interconnected.

As shown from Tables 1 and 2, compared to schemes [3, 21], our proposed ones offer certain advantages in terms of computational and storage efficiency. Specifically, the storage overhead (e.g., $Pub.size$, $Priv.size$, and $Cipher.size$) and computational complexity (e.g., $Pub.cost, Enc.cost$, and $Dec.cost$) in [3] seem to be lower than those of PKE I and PKE II. However, it is not so. While [3] can encrypt only one bit of plaintext at a time, both PKE I and PKE II can encrypt $n^6 \log q$ bits in a single operation. Consequently, encrypting $n^6 \log q$ bits utilizing [3] would require $n^6 \log q$ executions whereas PKE I and PKE II would only necessitate a single execution. Namely, the proposed schemes can encrypt more information at once, increasing the encryption quality compared to [3]. It is clear that both computing complexity and storage overhead in [3] are higher than those of PKE I and PKE II when encrypting the same amount of messages, making PKE I and PKE II much more efficient than [3]. The $Pub.size$ ($4n^2 \log 2$) and $Priv.size$ ($2(n-1)\log 2$) in [21] are similar to those of PKE II, but smaller than those of PKE I. Other parameters including $Cipher.size$, $Plain.size$, $Pub.cost$, $Enc.cost$, and $Dec.cost$ in [21] are much smaller than those of PKE I and PKE II owing to their different domains. The analysis indicates that our schemes overcome the serious defect of the classic scheme with encryption of less plaintexts one time by enabling the encryption of larger plaintexts in a single operation, resulting in greatly improved efficiency.

Based on different assumptions, while our schemes and [3] achieve CPA security, [21] likely provides only weak security such as opposing brute force attack and simultaneous equations attack, and not sure whether it is CPA-secure. The security [21] is limited to theoretical analysis and has not been realized in practice, especially considering resistance against quantum attacks. While [3] offers resistance against quantum attacks, PKE I and PKE II can only be considered candidates for quantum-resistant cryptography. In general, our schemes outperform [3, 21] and achieve superior efficiency in terms of computation and storage while maintaining comparable or stronger security guarantees. This analysis highlights theoretical efficiency measures when evaluating cryptographic schemes. Practically, while PKE I and PKE II can be implemented in an asymmetric setting, it is unknown whether [3, 21] can be applied in such a setting. Leave the research for future work.

Table 1. Comparison of performance between PKE schemes.

System	$Pub.size$	$Priv.size$	$Cipher.size$	$Plain.size$	$Pub.cost$
[3]	$2(n+1)n\log^2 q$	$n\log q$	$n\log^2 q + \log q$	1	$2n^2\log^3 q$
[21]	$4n^2\log 2$	$2(n-1)\log 2$	$n^2\log 2$	$n^2\log 2$	$2^n\log^2 2$
$PKE\ I$	$(2n\log q+1)n^6\log q$	$(2n+n^2)\log q$	$(2+n^4)n^2\log q$	$n^6\log q$	$O(n^5\log^2 q)$
$PKE\ II$	$2n^2\log q$	$2n\log q + 1$	$(2n\log q+2)n^6\log q$	$n^6\log q$	$O(n^4\log q)$

Table 2. Comparison of performance between PKE schemes.

$System$	$Enc.cost$	$Dec.cost$	$Resist.Quantum$	$Assumption$	$CPA - secure$
[3]	$2n^2 \log^2 q$	$n \log^2 q$	Yes	$Lattice$	Yes
[21]	$2(n+1)n^2 \log^2 2$	$2(n+1)n^2 \log^2 2$	No	$TEMP$	No
$PKE\ I$	$O(n^4 \log q)$	$O(n^5 \log^2 q)$	$Open$	$DTSPEM$	Yes
$PKE\ II$	$O(n^5 \log^2 q)$	$O(n^4 \log q)$	$Open$	$DTSPEM$	Yes

5. Conclusions

The rise of quantum computers has significantly heightened the need for cryptosystems resistant to quantum attacks. To ensure the security of future information applications, further development in post-quantum cryptography is crucial. We present two PKE schemes based on the TSPEM problem which can be regarded as a promising candidate for resisting quantum attacks due to its inherent algebraic structures and computational complexity. We formally prove their CPA security under the DTSPEM assumption [11]. Finally, the efficiency of their execution is analyzed.

The inherent efficiency of matrix operations in both software and hardware contributes significantly to the high performance of the proposed schemes. The efficient encryption of large plaintexts in a single operation is allowed by the TSPEM problem′s structure. As highlighted earlier, our schemes yield several good features: security can be reduced to the hard DTSPEM problem, scalable security parameters, high efficiency, ease of implementation, and potential resistance to quantum attacks, as well as the unique synchronization and coexistence. These characteristics make the proposed ones well-suited for various applications, such as the IoT, asymmetric cryptography, cloud computing, and potentially even quantum computing environments.

All in all, the TSPEM problem will become one promising foundamental tool for constructing post-quantum cryptoschemes in the future. Our schemes acts as a foundation for designing other TSPEM-based cryptosystems like key encapsulation mechanisms, authentication key exchange protocols, and signatures, which are promising candidates for cryptosystems resistant to quantum attacks. Despite the proposed ones can achieve CPA security for certain applications, they do not satisfy stronger CCA security [22]. However, our results can likely be modified to CCA-secure PKE schemes by incorporating appropriate cryptographic transformation technologies or primitives. The TSPEM problem will lead to more efficient PKE schemes, CCA-secure KEMs, and leakage-resistant CCA-secure PKE schemes suitable for quantum computing circumstances. Future research will fruitfully explore these issues further by constructing TSPEM-based cryptosystems with higher-lever security features.

Author contributions

Limin Zhou: Resource, Ideals, Conceptualization, Methodology, Investigation, Writing-original draft, Data computation, Performance analysis, Validation; Qiuyan Wang: Writing-review and editing, Formal analysis, Software, Technical and presentational advice, Funding acquisition, Supervision. All authors have read and approved the final version of the article for publication.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Acknowledgement

This work is partially supported by the Science and Technology Development Fund of Tianjin Education Commission for Higher Education, No. 2020KJ112, KYOD1817, Haihe Lab. of ITAI (Grant number: 22HHXCJC00002).

References

1. L. K. Grover, A fast quantum mechanical algorithm for database search, *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, ACM*, (1996), 212–219. https://doi.org/10.1145/237814.237866
2. P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Review*, (1999), 303–332. https://doi.org/10.1137/S0036144598347011
3. O. Regev, On lattices, learning with errors, random linear codes and cryptography, *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, May, (2005), 84–93. https://doi.org/10.1145/1060590.1060603
4. H. Z. Wang, H. G. Zhang, Z. Y. Wang, M. Tang, Extended multivariate public key cryptosystems with secure encryption function, *Sci. China Inform. Sci.*, **54** (2011), 1161–1171. https://doi.org/10.1007/s11432-011-4262-3
5. M. Eftekhari, A diffie-hellman key exchange protocol using matrices over non-commutative rings, *Groups Complex. Crypt.*, **4** (2012), 167–176. https://doi.org/10.1515/gcc-2012-0001
6. A. G. Myasnikov, V. Shpilrain, A. Ushakov, Non-Commutative Cryptography and Complexity of Group-Theoretic Problems, No. 177. Providence, RI, *USA: American Mathematical Society*, (2011), 41–111. Available from: https://dl.acm.org/doi/abs/10.5555/2161874
7. Z. F. Chao, New Directions of Modern Cryptography, *CRC Press*, (2012), 233–322. Available from: https://dl.acm.org/doi/abs/10.5555/2490637
8. D. J. Bernstein, T. Lange, Post-quantum cryptography, *Nature*, **549** (2017), 188–194. https://doi.org/10.1038/nature23461
9. R. A. Perlner, D. A. Cooper, Quantum resistant public key cryptography: A survey, *Proceed ings of the 8th Symposium on Identity and Trust on the Internet, ACM*, (2009), 85–93. https://doi.org/10.1145/1527017.1527028
10. T. Okamoto, K. Tanaka, S. Uchiyama, Quantum public-key cryptosystems, *Advances in Cryptology-CRYPTO 2000, Springer Berlin Heidelberg*, (2000), 147–165. https://doi.org/10.1007/3-540-44598-6

11. S. W. Mao, H. G. Zhang, W. Q. Wu, H. Z. Wang, An asymmetric-computing key exchange protocol, *Advances in Cryptology 2014, ChinaCrypt*, (2014), 135–149.
12. Q. H. Wu, Y. Mu, W. Susilo, B. Qin, D. F. Josep, Asymmetric group key agreement, In: Eurocrypt 2009, *LNCS, Berlin: Springer-Verlag*, **5479** (2009), 153–170. https://doi.org/10.1007/978-3-642-01001-9
13. Z. Yu, C. Gu, Z. Jing, Q. Cai, Y. Luo, Y. Wang, Cryptanalysis of an asymmetric cipher protocol using a matrix decomposition problem: revisited, *Multimed. Tools Appl.*, **77** (2018), 11307–11320. https:// doi.org/10.1007/s11042-017-5535-7
14. H. Wang, J. Wen, J. Liu, H. Zhang, ACKE: Asymmetric computing key exchange protocol for IoT environments, In: *IEEE Internet Things*, **10** (2023), 18273–18281. http://doi.org/10.1109/JIOT.2023.3279283
15. S. W. Mao, H. G. Zhang, W. Wu, J. Liu, S. Li, H. Wang, A resistant quantum key exchange protocol and its corresponding encryption scheme, *China Commun.*, **11** (2014), 124–134. http://doi.org/10.1109/CC.2014.6969777
16. A. Mihalkovich, E. Sakalauskas, K. Luksy, Key exchange protocol defined over a non-commuting group based on an NP-complete decisional problem, *Symmetry*, **12** (2020), 1–16. https://doi.org/10.3390/sym12091389
17. D. Boucher, P. Gaborit, W. Geiselmann, Key exchange and encryption schemes based on non-commutative skew polynomials, *International Workshop on Post-Quantum cryptography, Berlin, Heidelberg: Springer Berlin Heidelberg, Lecture Notes in Computer Science*, (2010), 126–141. https://doi.org/10.1007/978-3-642-12929-2
18. K. Dudziski, S. Walukiewicz, Exact methods for the knapsack problem and its generalizations, *Eur. J. Oper. Res.*, **28** (1987), 3–21. https://doi.org/10.1016/0377-2217(87)90165-2
19. J. Li, D. Wan, On the subset sum problem over finite fields, *Finite Fields Th. App.*, **14** (2008), 911–929. https://doi.org/10.1016/j.ffa.2008.05.003
20. C. J. Hillar, L. H. Lim, Most tensor problem are NP-hard, *J. ACM (JACM)*, September, **60** (2013), 1–39. https://doi.org/10.1145/2512329
21. S. H. Pei, Y. Z. Zhao, H. W. Zhao, Construct public key encryption scheme using ergodic matrices over GF(2), *International Conference on Theory and Applications of Models of Computation, Springer Berlin Heidelberg*, (2007), 181–188. https://doi.org/10.1007/978-3-540-72504-6
22. J. Katz, Y. Lindell, Introduction to Modern Cryptography: Principles and Protocols, *CRC Press*, (2007), 336–337. https://doi.org/10.1201/9781420010756
23. J. J. Zheng, P. J. Guo, S. G. Chun, A novel public key cryptosystem based on ergodic matrix over GF(2), *2012 International Conference on Computer Science and Service System, IEEE*, (2012), 845–848. https://doi.org/10.1109/CSSS.2012.216

AIMS Press