Wuhan University Journal of Natural Sciences

2016, Vol.21 No.3, 209-213

Article ID 1007-1202(2016)03-0209-05

DOI 10.1007/s11859-016-1161-x

Cryptanalysis of Schemes Based on Pseudoinverse Matrix

□ **LIU Jinhui[1, 2], ZHANG Huanguo[1, 2†], JIA Jianwei[1, 2]**

1. School of Computer, Wuhan University, Wuhan 430072, Hubei, China;

2. Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan 430072, Hubei, China

Abstract: Advances in quantum computation threaten to break public key cryptosystems that are based on the difficulty of factorization or the difficulty of discrete logariths, although , no quantum algorithms have been found to be able to solve certain mathematical problems on non-commutative algebraic structures up to now. The proposed new quasi-inverse based cryptography scheme is vulnerable to a linear algebra attack based on the probable occurrence of weak keys in the generation process. In this paper, we illustrate that two of the quasi-inverse based cryptography are vulnerable to a structural attack and that it only requires polynomial time to obtain the equivalent keys for some given public keys. In addition, we conduct a detailed analysis on attack methods and provide some improved suggestions on these two schemes.

Key words: cryptography; post-quantum computational cryptography; key exchange protocol; cryptanalysis; matrix decomposition

CLC number: TP 305

Received date: 2015-09-23

Foundation item: Supported by the National Natural Science Foundation of China (61303212, 61170080, 61202386), the State Key Program of National Natural Science of China(61332019, U1135004), the Major Research Plan of the National Natural Science Foundation of China (91018008), Major State Basic Research Development Program of China (973 Program) (2014CB340600), the Natural Science Foundation of Hubei Province (2011CDB453, 2014CFB440)

Biography: LIU Jinhui, female, Ph.D. candidate, research direction: cryptography. E-mail:jh.liu@whu.edu.cn

† To whom correspondence should be addressed. E-mail: liss@ whu.edu.cn

0 Introduction

Most public key cryptosystems used today rely on the assumed difficulty of either factorization or discrete logarithms. However, the trustworthiness of these assumptions has been eroded by infactorization algorithms and by quantum algorithms that solve both problems. These are among the reasons that have motivated research into the development of a new family of cryptosystems that can resist quantum computer attacks with higher efficiency in computation. In recent years, cryptographers have been making efforts in the area of post-quantum computational cryptography[1-6]. They have also begun to construct alternative post-quantum (i.e., quantum-resistant) public key cryptosystems from other mathematically intractable problems[7-13].

Before describing details, we would like to mention that nonabelian algebraic structures have already been used in the cryptographic context. For a general introduction to non-commutative cryptography, we refer to Refs.[5, 6]. In this paper, we study cryptanalysis of two new quasi-inverse based cryptography proposed in Refs.[14, 15]. These two schemes are vulnerable to a linear algebra attack based on the probable occurrence of weak keys in the generation process. We illustrate that the scheme is insecure against a linear algebra attack. Using the linear algebra attack, we attempt to analyze the scheme so that we can obtain the equivalent keys from an associated public key with significant probability in a reasonable time. We then analyze the basic rationale for the linear algebra attack. We also propose an improved scheme that remedies the weakness of their schemes.

The rest of this paper is organized as follows. Section 1 reviews the necessary background materials. Section 2 gives an overview of the key exchange protocol based on the quasi-inverse matrix proposed in Refs.[14, 15]. Section 3 proposes an attack method, and describes the corresponding algorithmic description and efficiency analysis. Finally, Section 4 provides some concluding remarks and discusses possible lines of future work.

1 Preliminaries

In this paper, we use the following notation.

Let q be a power of a prime and F_q be a finite field. For an integer $k>1$, $\mathrm{GL}_k(F_q)$ is the set of $k\times k$ invertible matrices with entries in F_q, $M_k(F_q)$ is a set of $k\times k$ matrices with entries in F_q, $\boldsymbol{I}_k\in\mathrm{GL}_k(F_q)$ is the identity matrix and $\boldsymbol{O}_k$ is the $k\times k$ matrix with all-zero elements.

We introduce the concept of pseudo-inverse matrix and its properties without proofs.

Definition 1 For every matrix (square or rectangular) $\boldsymbol{A}$ of real or complex elements, there is a unique matrix $\boldsymbol{A}^+$, called pseudo-inverse of $\boldsymbol{A}$, satisfying all of the four equations:

$$\boldsymbol{AA}^+\boldsymbol{A}=\boldsymbol{A};$$

$$\boldsymbol{A}^+\boldsymbol{AA}^+=\boldsymbol{A}^+;$$

$$(\boldsymbol{AA}^+)^{\mathrm{T}}=\boldsymbol{AA};$$

$$(\boldsymbol{A}^+\boldsymbol{A})^{\mathrm{T}}=\boldsymbol{A}^+\boldsymbol{A}.$$

Proposition 1 Given a matrix $\boldsymbol{A}\in\mathrm{GL}_{m\times n}(F_q)$,

if $m>n$ and $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$ is non-singular, then

$$\boldsymbol{A}^+=(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathrm{T}}$$

if $m<n$ and $\boldsymbol{AA}^{\mathrm{T}}$ is non-singular, then

$$\boldsymbol{A}^+=\boldsymbol{A}^{\mathrm{T}}(\boldsymbol{A}^{\mathrm{T}})^{-1}$$

Proposition 2 Let $\boldsymbol{A}\in\mathrm{GL}_{m\times n}(F_q)$ having $\mathrm{rank}(\boldsymbol{A})=k$ and the full rank factorization $\boldsymbol{A}=\boldsymbol{BC}$, where $\boldsymbol{B}\in\mathrm{GL}_{m\times k}(F_q)$ is the matrix of basic columns from $\boldsymbol{A}$ and $\boldsymbol{C}\in\mathrm{GL}_{r\times n}(F_q)$ is the matrix of non-zero rows from $\boldsymbol{E}_A$ ($\boldsymbol{E}_A$ is the unique reduced echelon form derived from $\boldsymbol{A}$ by means of row operations). The pseudo-inverse of $\boldsymbol{A}$ is defined by

$$\boldsymbol{A}^+=\boldsymbol{A}^{\mathrm{T}}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{AC}^{\mathrm{T}})^{-1}\boldsymbol{A}^{\mathrm{T}}$$

2 Description of Cryptography Based on Pseudo-Inverse Matrix

In this section, we briefly review the key exchange protocol based on pseudo-inverse matrix as follows.

2.1 The Key Exchange Protocol 1

The key exchange protocol 1 given in Ref. [14] can be summarized as follows:

Public Key: q,m,n

1) Alice generates a secret pseudo-invertible matrix $\boldsymbol{F}\in\mathrm{GL}_{m\times n}(F_q)$ and its pseudo-inverse $\boldsymbol{F}^+\in\mathrm{GL}_{n\times m}(F_q)$. She computes $\boldsymbol{X}=\boldsymbol{FF}^+$ and sends $\boldsymbol{X}$ to Bob.

2) Bob generates a secret pseudo-invertible matrix $\boldsymbol{G}\in\mathrm{GL}_{n\times m}(F_q)$ and its pseudo-inverse $\boldsymbol{G}^+\in\mathrm{GL}_{m\times n}(F_q)$. He computes $\boldsymbol{Y}=\boldsymbol{G}^+\boldsymbol{G}$ and a middle key $\boldsymbol{K}_{\mathrm{Bob}}=\boldsymbol{GX}$, then sends $\boldsymbol{Y}$ and $\boldsymbol{K}_{\mathrm{Bob}}$ to Alice.

3) Alice computes a middle key $\boldsymbol{K}_{\mathrm{Alice}}=\boldsymbol{YF}$, then sends $\boldsymbol{K}_{\mathrm{Alice}}$ to Bob.

4) Alice and Bob now share a secret key $\boldsymbol{K}=\boldsymbol{K}_{\mathrm{Bob}}$ $\boldsymbol{F}=\boldsymbol{GK}_{\mathrm{Alice}}$.

2.2 The Key Exchange Protocol 2

In this section, we briefly review the key exchange protocol based on pseudo-inverse matrix proposed in Ref.[15].

Public key: $\boldsymbol{K}$

Private key: $\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{L}$

1) Alice chooses a uniformly random matrix $\boldsymbol{K}_1\in\mathrm{GL}_{m\times k}(F_q)$, $\boldsymbol{Q}\in\mathrm{GL}_{k\times k}(F_q)$ and finds $\boldsymbol{K}_2\in\mathrm{GL}_{k\times n}(F_q)$ ($k<n<m$) such that $\boldsymbol{K}_1\boldsymbol{K}_2=\boldsymbol{K}$. She computes $\boldsymbol{K}_{\mathrm{Alice}}=\boldsymbol{KK}^+\boldsymbol{K}_1\boldsymbol{Q}$ and $\boldsymbol{L}=\boldsymbol{Q}^{-1}\boldsymbol{K}_2$. Then she sends $\boldsymbol{K}_{\mathrm{Alice}}$ to Bob.

2) Bob chooses a matrix $\boldsymbol{M}\in\mathrm{GL}_{h\times m}(F_q)$, compues $\boldsymbol{K}_{\mathrm{Bob}}=\boldsymbol{MK}_{\mathrm{Alice}}$. Then he sends $\boldsymbol{K}_{\mathrm{Bob}}$ to Alice.

3) Thus, Alice and Bob end up with the same shared secret key $\boldsymbol{K}=\boldsymbol{K}_{\mathrm{Bob}}\boldsymbol{L}=\boldsymbol{MK}$.

3 The Key Recovery Attack

This section attempts to attack the two-key exchange protocols based on pseudo-inverse matrix mentioned above. The attack makes use of the elementary tools to show the structural vulnerabilities of the two-key exchange protocols.

3.1 Attack on the Key Exchange Protocol 1

We know that an attacker is observing the key exchange protocol 1 and he is able to get the information: $(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{K}_{\mathrm{Alice}},\boldsymbol{K}_{\mathrm{Bob}})$. He searches for a matrix $\tilde{\boldsymbol{F}}\in\mathrm{GL}_{m\times n}(F_q)$ such that

$$\begin{cases}\boldsymbol{XF}=\boldsymbol{F}\\ \boldsymbol{K}_{\mathrm{Alice}}=\boldsymbol{YF}\end{cases}\tag{1}$$

and $\mathrm{rank}(\tilde{\boldsymbol{F}})=n$. Then the proposed scheme 1 always has weakness. It remains to analyze the key agreement protocol 1,which can be done as follows.

Proposition 3 If an adversary can find a matrix $\tilde{\boldsymbol{F}}$ satisfying equations (1) and $\operatorname{rank}(\tilde{\boldsymbol{F}}) = n$, then the key exchange protocol 1 based on the pseudo-inverse matrix can be broken.

Proof If an adversary can find matrices $\tilde{\boldsymbol{F}}$ satisfying equations (1), then the key exchange protocol 1 based on pseudo-inverse matrix can be summarized as follows.

From $\boldsymbol{K}_{\text{Bob}} = \boldsymbol{GX}$ and $\boldsymbol{K}_{\text{Alice}} = \boldsymbol{Y}\tilde{\boldsymbol{F}}$, we have

$$\begin{aligned} \boldsymbol{K} &= \boldsymbol{G}\boldsymbol{K}_{\text{Alice}} \\ &= \boldsymbol{GY}\tilde{\boldsymbol{F}} \\ &= \boldsymbol{GY}\tilde{\boldsymbol{F}}\tilde{\boldsymbol{F}}^{+}\tilde{\boldsymbol{F}} \\ &= \boldsymbol{GYX}\tilde{\boldsymbol{F}} \\ &= \boldsymbol{G}\boldsymbol{G}^{+}\boldsymbol{GX}\tilde{\boldsymbol{F}} \\ &= \boldsymbol{GX}\tilde{\boldsymbol{F}} \end{aligned} \qquad (2)$$

The attacker thereby obtains the same shared secret key $\boldsymbol{K}$. This completes the proof.

Formally, the key recovery attack can be described by Algorithm 1. It takes as inputting the public key $(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{K}_{\text{Alice}}, \boldsymbol{K}_{\text{Bob}})$ and outputting the same shared secret key $\boldsymbol{K}$.

Algorithm 1 Solve the shared key $\boldsymbol{K}$

```
1. Input $(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{K}_{\text{Alice}}, \boldsymbol{K}_{\text{Bob}})$
2. Solve the homogeneous linear equations in $2mn$
   equations with $mn$ unknowns of $\boldsymbol{F}$:
   $\boldsymbol{XF} = \boldsymbol{F}, \boldsymbol{K}_{\text{Alice}} = \boldsymbol{YF}$.
3. Pick a random solution matrix $\tilde{\boldsymbol{F}}$ until rank $(\tilde{\boldsymbol{F}}) = n$.
4. Compute $\boldsymbol{K} = \boldsymbol{K}_{\text{Bob}}\tilde{\boldsymbol{F}}$.
5. Output $\boldsymbol{K}$.
```

According to the above discussions, let us make a performance evaluation on Algorithm 1. The classical techniques for matrix multiplication/inversion in F_q take about $O(n^{\omega}(\log q)^2)$ bit operations, since the best known algorithm for the product of two $n \times n$ matrices requires $O(n^{\omega})(\omega \approx 2.3755)$ F_q operations and each F_q operation needs $O(\log^2 q)$ bit operations[15-17]. The complexity for Algorithm 1 can be mainly concluded as follows.

Step 2 is to solve $2mn$ linear equations in mn variables and then its complexity is about $O(2mn\,(mn)^{\omega-1})$. Now, if we neglect small constant factors, the key recovery attack against the key agreement protocol 1 based on the pseudo-inverse matrix can be completed with a complexity of $O((mn)^{\omega}\log^2 q)$.

A Toy Example

In order to illustrate the steps in our cryptanalysis over $\mathrm{GL}_{2\times 2}(F_q)$, we give the following toy example. Let $q = 7$ and consider the field F_q.

Since the following information is known:

$$\boldsymbol{X} = \begin{pmatrix} 6 & 5 & 6 \\ 5 & 3 & 5 \\ 6 & 5 & 6 \end{pmatrix}, \boldsymbol{Y} = \begin{pmatrix} 2 & 5 & 6 \\ 5 & 2 & 1 \\ 6 & 1 & 4 \end{pmatrix}$$

$$\boldsymbol{K}_{\text{Alice}} = \begin{pmatrix} 4 \\ 3 \\ 5 \end{pmatrix}, \boldsymbol{K}_{\text{Bob}} = (1 \quad 2 \quad 1)$$

The private key

$$\boldsymbol{F} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \boldsymbol{F}^{+} = (6 \quad 5 \quad 6), \boldsymbol{G} = (3 \quad 4 \quad 2), \boldsymbol{G}^{+} = \begin{pmatrix} 3 \\ 4 \\ 2 \end{pmatrix}$$

We now illustrate the structural attack processes.

Due to

$$\boldsymbol{XF} = \boldsymbol{F}, \boldsymbol{K}_{\text{Alice}} = \boldsymbol{YF},$$

we have a solution

$$\boldsymbol{F} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$$

that means the shared secret key $\boldsymbol{K} = \boldsymbol{K}_{\text{Bob}}\boldsymbol{F} = 6$.

3.2 Attack on the Key Exchange Protocol 2

The attack makes use of the elementary tools mentioned above and this is intended to show the structural vulnerabilities of the system. For the key exchange protocol 2 based on pseudo-inverse matrix, we know that an attacker can get the information $(\boldsymbol{K}_{\text{Alice}}, \boldsymbol{K}_{\text{Bob}})$, where $\boldsymbol{K}_{\text{Bob}} = \boldsymbol{MK}_{\text{Alice}}$. Then we have

$$\begin{aligned} &\boldsymbol{K}_{m\times n} \\ &= \boldsymbol{P}_{m\times m} \begin{pmatrix} \boldsymbol{I}_r & \boldsymbol{O}_{r\times(k-r)} & \boldsymbol{O}_{r\times(n-k)} \\ \boldsymbol{O}_{(n-r)\times r} & \boldsymbol{O}_{(n-r)\times(k-r)} & \boldsymbol{O}_{(n-r)\times(n-k)} \\ \boldsymbol{O}_{(m-n)\times r} & \boldsymbol{O}_{(m-n)\times(k-r)} & \boldsymbol{O}_{(m-n)\times(n-k)} \end{pmatrix} \boldsymbol{Q}_{n\times n} \\ &= \boldsymbol{P} \begin{pmatrix} \boldsymbol{I}_r & \boldsymbol{O}_{r\times(k-r)} \\ \boldsymbol{O}_{(k-r)\times r} & \boldsymbol{O}_{(k-r)\times(k-r)} \\ \boldsymbol{O}_{(m-k)\times r} & \boldsymbol{O}_{(m-k)\times(k-r)} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_r & \boldsymbol{O} & \boldsymbol{O} \\ \boldsymbol{I}_{(k-r)\times r} & \boldsymbol{O} & \boldsymbol{O} \end{pmatrix} \boldsymbol{Q} \end{aligned}$$

where $\boldsymbol{P}$ and $\boldsymbol{Q}$ are $m \times m, n \times n$ permutation matrices, respectively. Let

thus we can get a matrix decomposition such that $\boldsymbol{K} = \boldsymbol{K}_1\boldsymbol{K}_2$.

$$\boldsymbol{K}_1=\boldsymbol{P}_{m\times m}\begin{pmatrix}\boldsymbol{I}_r & \boldsymbol{O}_{r\times(k-r)}\\ \boldsymbol{O}_{(k-r)\times r} & \boldsymbol{O}_{(k-r)\times(k-r)}\\ \boldsymbol{O}_{(m-k)\times r} & \boldsymbol{O}_{(m-k)\times(k-r)}\end{pmatrix},$$

$$\boldsymbol{K}_2=\begin{pmatrix}\boldsymbol{I}_r & \boldsymbol{O}_{r\times(k-r)} & \boldsymbol{O}_{r\times(n-k)}\\ \boldsymbol{I}_{(k-r)\times r} & \boldsymbol{O}_{(k-r)\times(k-r)} & \boldsymbol{O}_{(k-r)\times(n-k)}\end{pmatrix}\boldsymbol{Q}_{n\times n}$$

Remark 1 It is easy to see that $\boldsymbol{K}_1$ and $\boldsymbol{K}_2$ are not unique. For example,

$$\boldsymbol{K}_1=\boldsymbol{P}_{m\times m}\begin{pmatrix}\boldsymbol{I}_r & \boldsymbol{O}_{r\times(k-r)}\\ \boldsymbol{O}_{(k-r)\times r} & \boldsymbol{O}_{(k-r)\times(k-r)}\\ \boldsymbol{O}_{(m-k)\times r} & \boldsymbol{O}_{(m-k)\times(k-r)}\end{pmatrix},$$

$$\boldsymbol{K}_2=\begin{pmatrix}\boldsymbol{I}_r & \boldsymbol{O}_{r\times(k-r)} & \boldsymbol{O}_{r\times(n-k)}\\ \boldsymbol{O}_{(k-r)\times r} & \boldsymbol{O}_{(k-r)\times(k-r)} & \boldsymbol{O}_{(k-r)\times(n-k)}\end{pmatrix}\boldsymbol{Q}_{n\times n}$$

It remains to analyze the key agreement protocol 2 based on pseudo-inverse matrix, which can be done as follows.

Proposition 4 If an adversary can find a pair of matrix $(\boldsymbol{K}_1,\boldsymbol{K}_2)$ satisfying the following equations (3) and $\boldsymbol{Q}\in \mathrm{GL}_k(F_q)$, then the key exchange protocol 2 based on pseudo-inverse matrix can be broken.

Proof By Proposition 2, we can get $\boldsymbol{K}^+$. If an adversary can find matrices $\tilde{\boldsymbol{K}}_1,\tilde{\boldsymbol{K}}_2$ and $\tilde{\boldsymbol{Q}}\in \mathrm{GL}_k(F_q)$ satisfying

$$\begin{cases}\boldsymbol{K}=\boldsymbol{K}_1\boldsymbol{K}_2\\ \boldsymbol{K}_{\text{Alice}}=\boldsymbol{K}\boldsymbol{K}^+\boldsymbol{K}_1\boldsymbol{Q}\end{cases} \tag{3}$$

then the key exchange protocol 2 based on pseudo-inverse matrix can be attacked as follows.

From $\boldsymbol{K}=\tilde{\boldsymbol{K}}_1\tilde{\boldsymbol{K}}_2, \boldsymbol{K}_{\text{Alice}}=\boldsymbol{K}\boldsymbol{K}^+\tilde{\boldsymbol{K}}_1\tilde{\boldsymbol{Q}}$ and $\tilde{\boldsymbol{L}}=\tilde{\boldsymbol{Q}}^{-1}\tilde{\boldsymbol{K}}_2$, then

$$\begin{aligned}\boldsymbol{K}_{\text{Alice}}\boldsymbol{L}&=\boldsymbol{K}\boldsymbol{K}^+\boldsymbol{K}_1\boldsymbol{Q}\boldsymbol{Q}^{-1}\boldsymbol{K}_2=\boldsymbol{K}\\ &=\boldsymbol{K}\boldsymbol{K}^+\tilde{\boldsymbol{K}}_1\tilde{\boldsymbol{Q}}\tilde{\boldsymbol{Q}}^{-1}\tilde{\boldsymbol{K}}_2=\boldsymbol{K}_{\text{Alice}}\tilde{\boldsymbol{L}}\end{aligned}$$

Thus the same shared secret key

$$\begin{aligned}\boldsymbol{K}&=\boldsymbol{M}\boldsymbol{K}_{\text{Alice}}\boldsymbol{L}\\ &=\boldsymbol{M}\boldsymbol{K}\boldsymbol{K}^+\tilde{\boldsymbol{K}}_1\tilde{\boldsymbol{Q}}\boldsymbol{L}\\ &=\boldsymbol{M}\boldsymbol{K}_{\text{Alice}}\tilde{\boldsymbol{L}}\\ &=\boldsymbol{M}\boldsymbol{K}\end{aligned}$$

The attacker thereby obtains the same shared secret key $\boldsymbol{K}$. This completes the proof.

Formally, the key recovery attack can be described by Algorithm 2. It takes as inputting the information $(\boldsymbol{K},\boldsymbol{K}_{\text{Alice}},\boldsymbol{K}_{\text{Bob}})$ and outputting the same shared secret key $\boldsymbol{K}$.

Algorithm 2 Solve the shared key $\boldsymbol{K}$

```
1. Input $(\boldsymbol{K},\boldsymbol{K}_{\text{Alice}},\boldsymbol{K}_{\text{Bob}})$
2. Compute $\boldsymbol{K}^+$
3. Solve a matrix decomposition $\boldsymbol{K}=\tilde{\boldsymbol{K}}_1\tilde{\boldsymbol{K}}_2$
4. Solve the linear equations in $mk$ equations with $k^2$ unknowns of $\tilde{\boldsymbol{Q}}:\boldsymbol{K}_{\text{Alice}}=\boldsymbol{K}\boldsymbol{K}^+\tilde{\boldsymbol{K}}_1\tilde{\boldsymbol{Q}}$.
5. Pick randomly a matrix $\tilde{\boldsymbol{Q}}$, if $\tilde{\boldsymbol{Q}}$ is invertible, then compute $\tilde{\boldsymbol{L}}=\tilde{\boldsymbol{Q}}^{-1}\tilde{\boldsymbol{K}}_2$, if not, go to step 4.
6. Compute $\boldsymbol{K}=\boldsymbol{K}_{\text{Alice}}\tilde{\boldsymbol{L}}$.
7. Output $\boldsymbol{K}$.
```

Remark 2 The probability of an invertible matrix over finite field F_q is about $1-1/q$. When q is big, we can obtain the equivalent keys from an associated public key with significant probability.

In the following we estimate the complexity of Algorithm 2 in terms of F_q operations.

In Step 2, $\boldsymbol{K}^+$ is computed by Proposition 2. Then the complexity is about $O((mn)^{\omega})$. Step 3 is to compute a matrix decomposition $\boldsymbol{K}=\tilde{\boldsymbol{K}}_1\tilde{\boldsymbol{K}}_2$. It is roughly estimated by $O((mn)^{\omega})$. Step 3 is to solve mk linear equations in k^2 variables and then its complexity is about $\leqslant O(mkk^{2\omega-2})$. Thus, we conclude that the total complexity of Algorithm 2 is about $O(\max\{mk^{2\omega-1}, (mn)^{\omega}\})$.

4 Conclusion

We present two cryptanalysis of two key agreement protocols based on pseudo-inverse matrix by showing that these two schemes are vulnerable to a linear algebra attack, respectively. We illustrate that the two-key agreement protocols based on pseudo-inverse matrix are insecure in the sense that an attacker who is able to solve the linear equations with high efficiency can break the two schemes. We propose an improved scheme and discuss the enhanced security features that provide good protection against the aforementioned attack. The question whether there exist groups in which a key agreement protocol based on pseudo-inverse matrix is secure remains open. When designing a key agreement protocols based on pseudo-inverse matrix on other groups, the considerations of this paper must be taken into account. Another open question concerns whether it is possible to use several nonabelian algebraic structures to construct a public key cryptosystem with the potential to resist attacks from known quantum algorithms.

References

[1] Zhang H G, Han W B, Lai X J, *et al*. Survey on cyberspace security [J]. *Science China Information Sciences*, 2015, **58**(11): 1-43.

[2] Gu L, Wang L, Ota K, *et al*. New public key cryptosystems based on non-Abelian factorization problems [J]. *Security and Communication Networks*, 2013, **6**(7): 912-922.

[3] Armknecht F, Gagliardoni T, Katzenbeisser S, *et al*. General impossibility of group homomorphic encryption in the quantum world [C] // *Public Key Crypto* 2014, *LNCS* 8383. Heidelberg: Springer-Verlag, 2014: 556-573.

[4] Mao S W, Zhang H G, Wu W Q, *et al*. A resistant quantum key exchange protocol and its corresponding encryption scheme [J]. *China Communications*, 2014,**11**(9):131-141.

[5] Tsaban B. Polynomial-Time solutions of computational problems in noncommutative-algebraic cryptography [J]. *Journal of Cryptology*, 2015, **28**(3): 601-622.

[6] Zhang H G, Liu J H, Jia J W, *et al*. A survey on applications of matrix decomposition in cryptography [J]. *Journal of Cryptologic Research*, 2014, **1**(4): 341-357 (Ch).

[7] Han Y, Yue Z, Fang D, *et al*. New multivariate-based certificateless hybrid signcryption scheme for multi-recipient [J]. *Wuhan University Journal of Natural Sciences*, 2014, **19**(5): 433-440.

[8] Wang H Z, Zhang H G, Wang Z Y, *et al*. Extended multivariate public key cryptosystems with secure encryption function [J]. *Science China Information Sciences*, 2011, **54**(6): 1161-1171.

[9] Mao S, Zhang H, Wu W, *et al*. Multi-bit LWE-based encryption scheme without decryption errors [J]. *International Journal of Embedded Systems*, 2016, **8**(1): 24-33.

[10] Braun J, Buchmann J, Mullan C, *et al*. Long term confidentiality: A survey [J]. *Designs*, *Codes and Cryptography*, 2014, **71**(3): 459-478.

[11] Wu W Q, Zhang H G, Wu S M, *et al*. A new cryptosystem based on line algebra [J]. *Journal of Wuhan University* (*Natural Sciences Edition*), 2014, **57**(1):1-12 (Ch).

[12] Albrecht M R, Faugere J C, Fitzpatrick R, *et al*. Practical cryptanalysis of a public-key encryption scheme based on new multivariate quadratic assumptions [C] // *PKC*2014, *LNCS* 8383. Heidelberg: Springer-Verlag, 2014: 446-464.

[13] Wu W Q, Zhang H G, Wang H Z, *et al*. A public key cryptosystem based on data complexity under quantum environment [J]. *Science China Information Sciences*, 2015, **58**(11): 1-11.

[14] Nguyen T D, Dang V H. Quasi-inverse based cryptography [C] // *Computational Science and Its Applications–ICCSA* 2013, *LNCS*7974. Heidelberg: Springer-Verlag, 2013: 629-642.

[15] Van D H, Thuc N D. Pseudoinverse matrix over finite field and its applications [C] // *Information Science and Applications*, *LNCS* 339. Heidelberg: Springer-Verlag, 2015: 491-498.

[16] Gashkov S B, Sergeev I S. Complexity of computation in finite fields [J]. *Journal of Mathematical Sciences*, 2013, **191**(5): 661-685.

[17] Arne S, Mulders T. Fast algorithms for linear algebra modulo *N* [C] // *Algorithms-ESA*'98, *LNCS*1461. Heidelberg: Springer-Verlag, 1998: 139-150.

□