Tsinghua Science and Technology

Volume 21 | Issue 3 Article 10

2016

Cryptanalysis of Public Key Cryptosystems Based on Non-Abelian Factorization Problems

Jinhui Liu
Computer School of Wuhan University, Wuhan 430072, China.

Aiwan Fan
Computer School of Pingdingshan University, Pingdingshan 467001, China.

Jianwei Jia
Computer School of Wuhan University, Wuhan 430072, China.

Huanguo Zhang
Computer School of Wuhan University, Wuhan 430072, China.

Houzhen Wang
Computer School of Wuhan University, Wuhan 430072, China.

See next page for additional authors

Cryptanalysis of Public Key Cryptosystems Based on Non-Abelian Factorization Problems

Authors

Jinhui Liu, Aiwan Fan, Jianwei Jia, Huanguo Zhang, Houzhen Wang, and Shaowu Mao

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 10/11 pp344–351
Volume 21, Number 3, June 2016

Cryptanalysis of Public Key Cryptosystems Based on Non-Abelian Factorization Problems

Jinhui Liu, Aiwan Fan, Jianwei Jia, Huanguo Zhang*, Houzhen Wang, and Shaowu Mao

Abstract: Advances in quantum computers threaten to break public-key cryptosystems (e.g., RSA, ECC, and ElGamal), based on the hardness of factoring or taking a discrete logarithm. However, no quantum algorithms have yet been found for solving certain mathematical problems in non-commutative algebraic structures. Recently, two novel public-key encryption schemes, BKT-B cryptosystem and BKT-FO cryptosystem, based on factorization problems have been proposed at *Security and Communication Networks* in 2013. In this paper we show that these two schemes are vulnerable to structural attacks and linearization equations attacks, and that they only require polynomial time complexity to obtain messages from associated public keys. We conduct a detailed analysis of the two attack methods and show corresponding algorithmic descriptions and efficiency analyses. In addition, we provide some improvement suggestions for the two public-key encryption schemes.

Key words: cryptography; post-quantum cryptography; public key encryption; cryptanalysis; linear equations

1 Introduction

Most public key cryptosystems used today rely on the assumed difficulty of either integer factorization problem or discrete logarithm problem. However, there exists polynomial time quantum algorithms that solve the two problems. These reasons motivate researchers to develop a new family of cryptosystems that can resist quantum computer attacks, and are more efficient in terms of computation. At present, many cryptographers are working on the area of post-quantum computational cryptography[1–5], and are constructing alternative post-quantum (i.e., quantum-resistant) public-key cryptosystems from other mathematically intractable problems based on non-commutative algebraic structures[6–12].

Before going into details we would like to mention that non-Abelian algebraic structures have already been used in a cryptographic context. In recent decades, many public-key cryptosystems based on non-Abelian algebraic structures were proposed, such as cryptosystems based on inner automorphism groups, general linear groups, and braid groups[1, 11, 12]. However, this area is immature, and there are few practical and efficient non-commutative cryptosystems in use at present. In 2013, Gu et al.[12] proposed two public-key encryption schemes that use non-Abelian algebraic structures and gave affirmative answers to open questions proposed by Myasnikov et al.[13]

In this paper we analyze these two public-key cryptosystems based on non-Abelian factorization problems over non-commutative rings proposed in Ref. [12], i.e., the BKT-B cryptosystem and the BKT-FO cryptosystem. The two schemes are both vulnerable to a structural attack and a linearization equations attack. Using the two attack methods, we can extract the message from associated public keys with significant probability in a reasonable time, and we provide corresponding algorithmic descriptions and efficiency analyses for the two schemes.

• Jinhui Liu, Jianwei Jia, Huanguo Zhang, Houzhen Wang, and Shaowu Mao are with Computer School of Wuhan University, Wuhan 430072, China. E-mail: jh.liu@whu.edu.cn; jjwwhu@whu.edu.cn; liss@whu.edu.cn; wanghouzhen@126.com; sw.mao@whu.edu.cn.

• Aiwan Fan is with Computer School of Pingdingshan University, Pingdingshan 467001, China. E-mail: faw_1978@163.com.

* To whom correspondence should be addressed.

Manuscript received: 2016-01-20; accepted: 2016-03-17

The rest of this paper is organized as follows. Section 2 reviews necessary material for this paper, including the concepts of general linear groups and Kronecker products, as well as the factorization problem. Section 3 gives an overview of public-key cryptosystems based on non-Abelian factorization problems. Section 4 proposes two attack methods, shows corresponding algorithmic descriptions and efficiency analyses, and provides a toy example. At the end, Section 5 provides some concluding remarks and discusses possible lines of future work.

2 Preliminaries

In this paper, we use the following notations.

$\mathbb{F}_q$: a finite field of order q.

For an integer $k \geqslant 1$,

$\mathrm{GL}_k(\mathbb{F}_q)$: the set of $k \times k$ invertible matrices of $\mathbb{F}_q$-entries.

$M_k(\mathbb{F}_q)$: the set of $k \times k$ matrices of $\mathbb{F}_q$-entries.

$\boldsymbol{I}_k \in \mathrm{GL}_k(\mathbb{F}_q)$: the identity matrix.

For every matrix $\boldsymbol{P}$,

$\boldsymbol{P}^{\mathrm{T}}$: the transpose of $\boldsymbol{P}$.

For $\boldsymbol{P} = \begin{pmatrix} p_{11} & \cdots & p_{1k} \\ \vdots & \ddots & \vdots \\ p_{k1} & \cdots & p_{kk} \end{pmatrix} \in M_{k_1}(\mathbb{F}_q)$, $\boldsymbol{S} \in M_{k_2}(\mathbb{F}_q)$,

$$\boldsymbol{P} \otimes \boldsymbol{S} = \begin{pmatrix} p_{11}\boldsymbol{S} & \cdots & p_{1k}\boldsymbol{S} \\ \vdots & \ddots & \vdots \\ p_{k1}\boldsymbol{S} & \cdots & p_{kk}\boldsymbol{S} \end{pmatrix},$$

$\overrightarrow{\boldsymbol{P}} = (p_{11} \ \cdots \ p_{1k} \ p_{21} \ \cdots \ \cdots \ p_{kk}) \in \mathbb{F}_q^{1\times k^2}$.

The Kronecker product $\otimes$ has the following properties for matrices $\boldsymbol{P}, \boldsymbol{S}, \boldsymbol{T}, \boldsymbol{O}$, and $\boldsymbol{Z}$:

$$(\boldsymbol{P} \otimes \boldsymbol{S}) \otimes \boldsymbol{T} = \boldsymbol{P} \otimes (\boldsymbol{S} \otimes \boldsymbol{T});$$
$$\boldsymbol{P} \otimes (\boldsymbol{S} + \boldsymbol{T}) = (\boldsymbol{P} \otimes \boldsymbol{S}) + (\boldsymbol{P} \otimes \boldsymbol{T});$$
$$(\boldsymbol{P} \otimes \boldsymbol{S})^{\mathrm{T}} = \boldsymbol{P}^{\mathrm{T}} \otimes \boldsymbol{S}^{\mathrm{T}};$$
$$(\boldsymbol{P} \otimes \boldsymbol{S})(\boldsymbol{T} \otimes \boldsymbol{Z}) = \boldsymbol{PT} \otimes \boldsymbol{SZ}.$$

Stretching the row of a matrix into one long row vector $\overrightarrow{\cdot}$ results in it having the following properties:

$$\overrightarrow{\alpha\boldsymbol{P} + \beta\boldsymbol{S}} = \alpha\overrightarrow{\boldsymbol{P}} + \beta\overrightarrow{\boldsymbol{S}},$$
$$(\overrightarrow{\boldsymbol{PO}})^{\mathrm{T}} = (\boldsymbol{P} \otimes \boldsymbol{I})(\overrightarrow{\boldsymbol{O}})^{\mathrm{T}},$$
$$(\overrightarrow{\boldsymbol{OS}})^{\mathrm{T}} = (\boldsymbol{I} \otimes \boldsymbol{S}^{\mathrm{T}})(\overrightarrow{\boldsymbol{O}})^{\mathrm{T}},$$
$$(\overrightarrow{\boldsymbol{POS}})^{\mathrm{T}} = (\boldsymbol{P} \otimes \boldsymbol{S}^{\mathrm{T}})(\overrightarrow{\boldsymbol{O}})^{\mathrm{T}}.$$

Definition 1 Factorization Problem (FP)[12, 13] Let $G = \mathrm{GL}_n(\mathbb{F}_q)$ (or $\mathrm{SL}_n(\mathbb{F}_q)$) be a finite group with identity $\boldsymbol{I}_n$. Let $\boldsymbol{M}, \boldsymbol{H} \in G$ be two random elements so that $<\boldsymbol{H}> \cap <\boldsymbol{M}> = \boldsymbol{I}_n$ and $\boldsymbol{HM} \neq \boldsymbol{MH}$. The factorization problem denoted by $\mathrm{FP}^{G}_{H;M}$ with respect to $G, \boldsymbol{H}$, and $\boldsymbol{M}$ is to split the given product $\boldsymbol{N} = \boldsymbol{H}^x\boldsymbol{M}^y \in G$ into a pair $(\boldsymbol{H}^x, \boldsymbol{M}^y) \in G^2$, where x and y are picked randomly.

3 Description of Schemes Based on the FP

In this section, we review the two schemes based on the FP proposed in Ref. [12].

3.1 BKT-B cryptosystem

KeyGen $\mathcal{K}$: Let κ be a system security. Let $G = \mathrm{GL}_n(\mathbb{F}_q)$ be a non-Abelian group with identity $\boldsymbol{I}_n$ and $|G| = \mathcal{O}(2^{2\kappa})$. Suppose that $\boldsymbol{H}, \boldsymbol{M} \in G$ are two non-commuting elements with orders $k, l = \mathcal{O}(2^{2\kappa})$ respectively and $<\boldsymbol{H}> \cap <\boldsymbol{M}> = \boldsymbol{I}_n$. Let the message space $\boldsymbol{m} = \{0,1\}^{\ell} \in \mathcal{M}$ be the set of all bit strings of length ℓ for any fixed $\ell \geqslant 2\kappa$, three collision-resistant hash functions $\pi : \mathcal{M} \to \mathbb{Z} \times \mathbb{Z}$, $\Phi : G \times G \to \mathcal{M}$, $\Psi : G \to \mathcal{M}$. Pick two integers x and y at random.

public key:

$$(\mathrm{GL}_n(\mathbb{F}_q), \mathcal{M}, \pi, \Phi, \Psi, \boldsymbol{H}, \boldsymbol{M}, \boldsymbol{N} = \boldsymbol{H}^x\boldsymbol{M}^y).$$

private key: (x, y).

Enc: (1) Alice chooses randomly $x_{\mathrm{r}}, y_{\mathrm{r}} \in \{0,1\}^{\kappa}$ and computes $\boldsymbol{A} = \boldsymbol{H}^{x_{\mathrm{r}}}\boldsymbol{N}\boldsymbol{M}^{y_{\mathrm{r}}}, \boldsymbol{B} = \Psi(\boldsymbol{A}) \oplus \boldsymbol{m}, (x_{\boldsymbol{B}}, y_{\boldsymbol{B}}) = \pi(\boldsymbol{B}), \boldsymbol{C} = \boldsymbol{H}^{x_{\boldsymbol{B}}}\boldsymbol{A}\boldsymbol{M}^{y_{\boldsymbol{B}}}, \boldsymbol{D} = \boldsymbol{H}^{x_{\mathrm{r}}+x_{\boldsymbol{B}}}\boldsymbol{M}^{y_{\mathrm{r}}+y_{\boldsymbol{B}}}, \boldsymbol{E} = \Phi(\boldsymbol{D}, \boldsymbol{C}) \oplus \boldsymbol{B}$. Then she sends $(\boldsymbol{D}, \boldsymbol{E})$ to Bob.

Dec: After receiving the ciphertext tuple $(\boldsymbol{D}, \boldsymbol{E})$, Bob performs the following steps with the private key pair $(\boldsymbol{H}^x, \boldsymbol{M}^y)$: $\boldsymbol{C}' = \boldsymbol{H}^x\boldsymbol{D}\boldsymbol{M}^y$, $\boldsymbol{B}' = \Phi(\boldsymbol{D}, \boldsymbol{C}') \oplus \boldsymbol{E}$, $(x_{\boldsymbol{B}'}, y_{\boldsymbol{B}'}) = \pi(\boldsymbol{B}')$, $\boldsymbol{A}' = \boldsymbol{H}^{-x_{\boldsymbol{B}'}}\boldsymbol{C}'\boldsymbol{M}^{y_{\boldsymbol{B}'}}$, $\boldsymbol{m}' = \Psi(\boldsymbol{A}') \oplus \boldsymbol{B}'$.

3.2 BKT-FO cryptosystem

KeyGen $\mathcal{K}$: Let κ be a system security. Let $G = \mathrm{GL}_n(\mathbb{F}_q)$ be a non-Abelian group with identity $\boldsymbol{I}_n$ and $|G| = \mathcal{O}(2^{2\kappa})$. Suppose that $\boldsymbol{H}, \boldsymbol{M} \in G$ are two non-commuting elements with orders $k, l = \mathcal{O}(2^{2\kappa})$ respectively and $<\boldsymbol{H}> \cap <\boldsymbol{M}> = \boldsymbol{I}_n$. Let the message space $\boldsymbol{m} = \{0,1\}^{\ell} \in \mathcal{M}$ be the set of all bit strings of length ℓ for any fixed $\ell \geqslant 2\kappa$, two random oracles $h_1 : G \to \{0,1\}^{\ell}$, $h_2 : \mathcal{M} \times G \to \{0,1\}^{2\kappa}$. Pick randomly two integers x and y.

public key: $(\mathrm{GL}_n(\mathbb{F}_q), \mathcal{M}, h_1, h_2, \boldsymbol{H}, \boldsymbol{M}, \boldsymbol{N}, \boldsymbol{N} = \boldsymbol{H}^x\boldsymbol{M}^y)$.

private key: (x, y).

Enc: Alice chooses randomly $\boldsymbol{R} \in G$ and computes $x'||y' = h_2(\boldsymbol{m}, \boldsymbol{R})$, $\boldsymbol{\tau}_1 = \boldsymbol{H}^{x'}\boldsymbol{N}\boldsymbol{M}^{y'}$, $\boldsymbol{\tau}_2 = \boldsymbol{H}^{x'}\boldsymbol{M}^{y'}\boldsymbol{R}$, $\boldsymbol{\tau}_3 = \boldsymbol{m} \oplus h_1(\boldsymbol{R})$. Then she sends $(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_3) \in G \times G \times \mathcal{M}$ to Bob.

Dec: After receiving the ciphertext triple $\boldsymbol{c} = (\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_3)$, Bob performs the following steps:

(1) Compute $\boldsymbol{R} = \boldsymbol{M}^y \boldsymbol{\tau}_1^{-1} \boldsymbol{H}^x \boldsymbol{\tau}_2$, $\boldsymbol{m} = \boldsymbol{\tau}_3 \oplus h_1(\boldsymbol{R})$, $x'||y' = h_2(\boldsymbol{m}, \boldsymbol{R})$.

(2) If $\boldsymbol{\tau}_2 = \boldsymbol{H}^{x'} \boldsymbol{M}^{y'} \boldsymbol{R}$, then output $\boldsymbol{m}$; otherwise, output $\perp$, which indicates the ciphertext is invalid.

4 Weakness of Schemes Based on the FP

In this section, we analyze two public key cryptosystems based on non-Abelian factorization problems.

4.1 Structural attack

The attack is able to get the information: $(\boldsymbol{M}, \boldsymbol{H}, \boldsymbol{D} = \boldsymbol{H}^{x_{\mathrm{r}}+x_B} \boldsymbol{M}^{y_{\mathrm{r}}+y_B}, \boldsymbol{N} = \boldsymbol{H}^x \boldsymbol{M}^y, \boldsymbol{E}, \Phi, \Psi, \pi)$. If an adversary can find matrices $(\boldsymbol{X}, \boldsymbol{Y})$ such that

$$\begin{cases} \boldsymbol{XH} = \boldsymbol{HX}; \\ \boldsymbol{YM} = \boldsymbol{MY}; \\ \boldsymbol{N} = \boldsymbol{XY} \end{cases} \tag{1}$$

the proposed BKT-B cryptosystem always had weakness.

Using Proposition 2, the linear Eq. (1) can be transformed into

$$\begin{cases} (\boldsymbol{I}_n \otimes \boldsymbol{H}^{\mathrm{T}} - \boldsymbol{H} \otimes \boldsymbol{I}_n)\overrightarrow{\boldsymbol{X}^{-1}}^{\mathrm{T}} = \boldsymbol{0}; \\ (\boldsymbol{M} \otimes \boldsymbol{I}_n) - (\boldsymbol{I}_n \otimes \boldsymbol{M}^{\mathrm{T}})\overrightarrow{\boldsymbol{Y}}^{\mathrm{T}} = \boldsymbol{0}; \\ (\boldsymbol{I}_n \otimes \boldsymbol{N}^{\mathrm{T}})\overrightarrow{\boldsymbol{X}^{-1}}^{\mathrm{T}} - (\boldsymbol{I}_n \otimes \boldsymbol{I}_n)\overrightarrow{\boldsymbol{Y}}^{\mathrm{T}} = \boldsymbol{0} \end{cases} \tag{2}$$

Let $\boldsymbol{Q} =$

$$\begin{pmatrix} (\boldsymbol{H} \otimes \boldsymbol{I}_n) - (\boldsymbol{I}_n \otimes \boldsymbol{H}^{\mathrm{T}}) & \boldsymbol{0} \\ \boldsymbol{0} & (\boldsymbol{M} \otimes \boldsymbol{I}_n) - (\boldsymbol{I}_n \otimes \boldsymbol{M}^{\mathrm{T}}) \\ \boldsymbol{I}_n \otimes \boldsymbol{N}^{\mathrm{T}} & -(\boldsymbol{I}_n \otimes \boldsymbol{I}_n) \end{pmatrix},$$

$\boldsymbol{x} = (\overrightarrow{\boldsymbol{X}^{-1}}, \overrightarrow{\boldsymbol{Y}})^{\mathrm{T}}$, where $\det(\boldsymbol{X}) \neq 0$, $\overrightarrow{\boldsymbol{X}^{-1}}$ and $\overrightarrow{\boldsymbol{Y}}$ are the stretches of matrices $\boldsymbol{X}^{-1}$ and $\boldsymbol{Y}$ respectively, $\otimes$ represents the Kronecker product, and $\boldsymbol{I}_n$ is an $n \times n$ identity. It remains to analyze the BKT-B cryptosystem as follows.

Proposition 1 If an adversary can find any matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$ satisfying Eq. (1), the BKT-B cryptosystem can be broken .

Proof If $\mathcal{A}$ finds matrices $\widetilde{\boldsymbol{X}}$ and $\widetilde{\boldsymbol{Y}}$ satisfying Eq. (1), according to $\widetilde{\boldsymbol{X}}\boldsymbol{H} = \boldsymbol{H}\widetilde{\boldsymbol{X}}$ and $\widetilde{\boldsymbol{Y}}\boldsymbol{M} = \boldsymbol{M}\widetilde{\boldsymbol{Y}}$, $\mathcal{A}$ has

$$\widetilde{\boldsymbol{Y}}\boldsymbol{M}^2 = \boldsymbol{M}\widetilde{\boldsymbol{Y}}\boldsymbol{M} = \boldsymbol{M}(\widetilde{\boldsymbol{Y}}\boldsymbol{M}) = \boldsymbol{M}(\boldsymbol{M}\widetilde{\boldsymbol{Y}}) = \boldsymbol{M}^2\widetilde{\boldsymbol{Y}},$$

hence $\widetilde{\boldsymbol{Y}}\boldsymbol{M}^k = \boldsymbol{M}^k\widetilde{\boldsymbol{Y}}, \widetilde{\boldsymbol{X}}\boldsymbol{H}^k = \boldsymbol{H}^k\widetilde{\boldsymbol{X}}$ for every integer k and

$$\begin{aligned} \widetilde{\boldsymbol{X}}\boldsymbol{D}\widetilde{\boldsymbol{Y}} =& \widetilde{\boldsymbol{X}}\boldsymbol{H}^{x_{\mathrm{r}}+x_B}\boldsymbol{M}^{y_{\mathrm{r}}+y_B}\widetilde{\boldsymbol{Y}} = \\ & \boldsymbol{H}^{x_{\mathrm{r}}+x_B}\widetilde{\boldsymbol{X}}\widetilde{\boldsymbol{Y}}\boldsymbol{M}^{y_{\mathrm{r}}+y_B} = \\ & \boldsymbol{H}^{x_{\mathrm{r}}+x_B}\mathbf{N}\mathbf{M}^{y_{\mathrm{r}}+y_B} = \\ & \boldsymbol{H}^{(x_{\mathrm{r}}+x_B)}\boldsymbol{H}^x\boldsymbol{M}^y\boldsymbol{M}^{(y_{\mathrm{r}}+y_B)} = \\ & \boldsymbol{H}^{x+(x_{\mathrm{r}}+x_B)}\boldsymbol{M}^{y+(y_{\mathrm{r}}+y_B)} = \boldsymbol{C} \end{aligned} \tag{3}$$

Because $(\boldsymbol{M}, \boldsymbol{H}, \boldsymbol{D}, \boldsymbol{N}, \boldsymbol{E}, \Phi, \Psi, \pi)$ are known information, $\boldsymbol{B}$, $x_{\boldsymbol{B}}$, and $y_{\boldsymbol{B}}$ can be solved in the following form:

$$\boldsymbol{B} = \boldsymbol{E} \oplus \Phi(\boldsymbol{D}, \widetilde{\boldsymbol{X}}\boldsymbol{D}\widetilde{\boldsymbol{Y}}),$$

$$(x_{\boldsymbol{B}}, y_{\boldsymbol{B}}) = \pi(\boldsymbol{B}).$$

The matrix $\boldsymbol{A}$ can be computed as follows:

$$\boldsymbol{A} = \boldsymbol{H}^{-x_{\boldsymbol{B}}}\boldsymbol{C}\boldsymbol{M}^{-y_{\boldsymbol{B}}}.$$

Hence the message

$$\boldsymbol{m} = \boldsymbol{B} \oplus \Psi(\boldsymbol{A})$$

is obtained, that is, the BKT-B cryptosystem is broken. This completes the proof.

Algorithm 1 is the method to calculate the message $\boldsymbol{m}$.

Working with Algorithm 1, we do a performance evaluation. Suppose that the rank of the $3n^2 \times 2n^2$ coefficient matrix $\boldsymbol{Q}$ is r, where $0 < r \leqslant 2n^2$ by employing the method of Gauss elimination. If $r = 2n^2$, then the matrix $\boldsymbol{Q}$ has full column rank, i.e., $\boldsymbol{x} = \boldsymbol{0}$. There is at least one solution to Eq. (1), namely, the private keys, thus $0 < r < 2n^2$. Since the classical techniques for matrix multiplication/inversion in $\mathrm{GL}_n(\mathbb{F}_q)$ take about $\mathcal{O}(n^\omega \log^2 q)$ bit operations, where the best known algorithm for the product of two $n \times n$ matrices requires $\mathcal{O}(n^\omega)$ $\mathbb{F}_q$ operations and each $\mathbb{F}_q$ operation needs $\mathcal{O}(\log^2 q)$ bit operations[14–16], where $\omega \approx 2.3755$. Hence the bit complexity of the Algorithm 1 can be analyzed in Table 1.

If we ignore small constant factors, a structural attack against the BKT-B cryptosystem can be concluded with a bit complexity of $\mathcal{O}(n^{2\omega} \log^2 q)$.

For the BKT-FO cryptosystem, $\mathcal{A}$ is able to get the information:

$$(G, \mathcal{M}, h_1, h_2, \boldsymbol{H}, \boldsymbol{M}, \boldsymbol{N} = \boldsymbol{H}^x\boldsymbol{M}^y, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_3).$$

Algorithm 1 Solve the message $\boldsymbol{m}$ of the BKT-B cryptosystem

1: **Input** $(\boldsymbol{M}, \boldsymbol{H}, \boldsymbol{D}, \boldsymbol{N}, \boldsymbol{E}, \Phi, \Psi, \pi)$;
2: Solve the homogeneous linear equations in the $2n^2$ entries of $\boldsymbol{x}$: $\boldsymbol{Q}\boldsymbol{x} = O$;
3: Fix a basis for the solution space $\boldsymbol{x} = (\overrightarrow{\boldsymbol{X}^{-1}}, \overrightarrow{\boldsymbol{Y}})^{\mathrm{T}}$, pick random vector $\boldsymbol{x}$ and transform $\overrightarrow{\boldsymbol{X}^{-1}}$ and $\overrightarrow{\boldsymbol{Y}}$ to the matrices $\boldsymbol{X}^{-1}$ and $\boldsymbol{Y}$ until $\boldsymbol{X}^{-1}$ is invertible;
4: Compute $\boldsymbol{C} = \boldsymbol{XDY}$;
5: Reckon $\boldsymbol{B} = \boldsymbol{E} \oplus \Phi(\boldsymbol{D}, \boldsymbol{C})$;
6: Compute $(x_{\boldsymbol{B}}, y_{\boldsymbol{B}}) = \pi(\boldsymbol{B})$;
7: Calculate $\boldsymbol{A} = \boldsymbol{H}^{-x_{\boldsymbol{B}}}\boldsymbol{C}\boldsymbol{M}^{-y_{\boldsymbol{B}}}$ and the message $\boldsymbol{m} = \boldsymbol{B} \oplus \Psi(\boldsymbol{A})$;
8: Return $\boldsymbol{m}$.

Table 1 Computation cost of Algorithm 1.

Comp. content	Comp. cost	Explanation
$\boldsymbol{Qx}=\boldsymbol{0}$	$\mathcal{O}(3n^2(2n^2)^{\omega-1}\log^2 q)$	$3n^2$ equations in $2n^2$ variables
$\boldsymbol{x}$	$\mathcal{O}(n^2(2n^2-r)^{\omega-1}\log^2 q)$	An invertible solution
$\boldsymbol{C}=\boldsymbol{XDY}$	$\mathcal{O}(3n^{\omega})$	2 multiplications, 1 inversion
$\boldsymbol{A}=\boldsymbol{H}^{-x_B}\boldsymbol{CM}^{-y_B}$	$\mathcal{O}(2n^{\omega})$	2 multiplications

If $\mathcal{A}$ can find any $(\boldsymbol{X},\boldsymbol{Y})$ satisfying Eq. (1), then the proposed scheme BKT-FO cryptosystem is vulnerable. It remains to analyze the BKT-FO cryptosystem as follows.

Proposition 2 If an adversary $\mathcal{A}$ can find any matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$ satisfying Eq. (1), then the BKT-FO cryptosystem can be broken .

Proof If $\mathcal{A}$ can find matrices $\widetilde{\boldsymbol{X}},\widetilde{\boldsymbol{Y}}$ satisfying Eq. (1), according to $\widetilde{\boldsymbol{X}}\boldsymbol{H}=\boldsymbol{H}\widetilde{\boldsymbol{X}}$, $\widetilde{\boldsymbol{Y}}\boldsymbol{M}=\boldsymbol{M}\widetilde{\boldsymbol{Y}}$, $\boldsymbol{N}=\widetilde{\boldsymbol{X}}\widetilde{\boldsymbol{Y}}$, $\mathcal{A}$ gets $\widetilde{\boldsymbol{X}}\boldsymbol{H}^{-1}=\boldsymbol{H}^{-1}\widetilde{\boldsymbol{X}}$, $\widetilde{\boldsymbol{Y}}\boldsymbol{M}^{-1}=\boldsymbol{M}^{-1}\widetilde{\boldsymbol{Y}}$, $\widetilde{\boldsymbol{X}}(\boldsymbol{H}^{-1})^k=(\boldsymbol{H}^{-1})^k\widetilde{\boldsymbol{X}}$, and $\widetilde{\boldsymbol{Y}}(\boldsymbol{M}^{-1})^k=(\boldsymbol{M}^{-1})^k\widetilde{\boldsymbol{Y}}$ for every integer k. Then

$$\begin{aligned}\widetilde{\boldsymbol{Y}}\boldsymbol{\tau}_1^{-1}\widetilde{\boldsymbol{X}}\boldsymbol{\tau}_2 =&\widetilde{\boldsymbol{Y}}(\boldsymbol{H}^{x'}\mathbf{N}\mathbf{M}^{y'})^{-1}\widetilde{\boldsymbol{X}}\boldsymbol{\tau}_2=\\ &\widetilde{\boldsymbol{Y}}\boldsymbol{M}^{-y'}\boldsymbol{N}^{-1}\boldsymbol{H}^{-x'}\widetilde{\boldsymbol{X}}\boldsymbol{\tau}_2=\\ &\boldsymbol{M}^{-y'}\widetilde{\boldsymbol{Y}}\boldsymbol{N}^{-1}\widetilde{\boldsymbol{X}}\boldsymbol{H}^{-x'}\boldsymbol{\tau}_2=\\ &\boldsymbol{M}^{-y'}\widetilde{\boldsymbol{Y}}(\widetilde{\boldsymbol{X}}\widetilde{\boldsymbol{Y}})^{-1}\widetilde{\boldsymbol{X}}\boldsymbol{H}^{-x'}\boldsymbol{\tau}_2=\\ &\boldsymbol{M}^{-y'}\boldsymbol{I}\boldsymbol{H}^{-x'}\boldsymbol{\tau}_2=\\ &\boldsymbol{M}^{-y'}\boldsymbol{H}^{-x'}\boldsymbol{\tau}_2=\\ &\boldsymbol{M}^{-y'}\boldsymbol{H}^{-x'}\boldsymbol{H}^{x'}\boldsymbol{M}^{y'}\boldsymbol{R}=\boldsymbol{R}\end{aligned}\tag{4}$$

Because $(h_1,\boldsymbol{\tau}_3)$ are known information, the message

$$\boldsymbol{m}=\boldsymbol{\tau}_3\oplus h_1(\widetilde{\boldsymbol{Y}}\boldsymbol{\tau}_1^{-1}\widetilde{\boldsymbol{X}}\boldsymbol{\tau}_2)$$

is obtained, that is, the BKT-FO cryptosystem is broken. This completes the proof.

The method to calculate message $\boldsymbol{m}$ in the BKT-FO cryptosystem can be concluded in Algorithm 2.

Table 1 indicates that a structural attack against the BKT-FO cryptosystem can be finished with a bit complexity of $\mathcal{O}(n^{2\omega}\log^2 q)$ without small constant factors.

Algorithm 2 Solve the message m of the BKT-FO cryptosystem

1: **Input** $(h_1,h_2,\boldsymbol{H},\boldsymbol{M},\boldsymbol{N},\boldsymbol{\tau}_1,\boldsymbol{\tau}_2,\boldsymbol{\tau}_3)$;
2: Solve $\boldsymbol{X}^{-1},\boldsymbol{Y}$ by steps 2&3 in Algorithm 1;
3: Compute $\boldsymbol{R}=\boldsymbol{Y}\boldsymbol{\tau}_1^{-1}\boldsymbol{X}\boldsymbol{\tau}_2$;
4: Calculate the message $\boldsymbol{m}=\boldsymbol{\tau}_3\oplus h_1(\boldsymbol{R})$;
5: Return $\boldsymbol{m}$.

4.2 Linearization equations attack

For any $\boldsymbol{V}\in \mathrm{GL}_n(\mathbb{F}_q)$, there exists a corresponding minimum polynomial $f_{\min \boldsymbol{V}}(x)$ such that $f_{\min \boldsymbol{V}}(\boldsymbol{V})=\boldsymbol{0}$. The characteristic polynomial $f_{\boldsymbol{V}}(x)$ of $\boldsymbol{V}$ satisfies

$$f_{\boldsymbol{V}}(x)=\det(x\boldsymbol{I}_n-\boldsymbol{V})=$$
$$v_n x^n+v_{n-1}x^{n-1}+\cdots+v_1x+v_0,$$

where $v_i\in\mathbb{F}_q$. According to the Hamilton-Cayley Theorem,

$$f_{\boldsymbol{V}}(\boldsymbol{V})=v_n\boldsymbol{V}^n+v_{n-1}\boldsymbol{V}^{n-1}+\cdots+v_1\boldsymbol{V}+v_0\boldsymbol{I}_n=\boldsymbol{0}.$$

and

$$\boldsymbol{V}^{-1}=-\frac{v_n}{v_0}\boldsymbol{V}^{n-1}-\frac{v_{n-1}}{v_0}\boldsymbol{V}^{n-2}-\ldots-\frac{v_1}{v_0}\boldsymbol{I}_n.$$

Hence for the matrix $\boldsymbol{A}$, $\boldsymbol{A}^k(k\in\mathbb{Z})$ can be linearly represented by the set $\mathcal{B}=\{\boldsymbol{I},\boldsymbol{A},\ldots,\boldsymbol{A}^{n-1}\}$. That means, $\boldsymbol{H}^{-x}$ can be linearly represented by the set $\{\boldsymbol{I},\boldsymbol{H},\ldots,\boldsymbol{H}^{n-1}\}$ and $\boldsymbol{M}^y$ can be linearly represented by the set $\{\boldsymbol{I},\boldsymbol{M},\ldots,\boldsymbol{M}^{n-1}\}$.

Let

$$\begin{cases}\boldsymbol{X}=\boldsymbol{H}^{-x}=\sum\limits_{i=0}^{n-1}a_i\boldsymbol{H}^i,\\ \boldsymbol{Y}=\boldsymbol{M}^{y}=\sum\limits_{j=0}^{n-1}b_j\boldsymbol{M}^j,\\ \sum\limits_{i=0}^{n-1}a_i\boldsymbol{H}^i\boldsymbol{N}=\sum\limits_{j=0}^{n-1}b_j\boldsymbol{M}^j\end{cases}\tag{5}$$

where $\boldsymbol{H}^{-x}\boldsymbol{N}=\boldsymbol{M}^y,\boldsymbol{N}=\boldsymbol{X}^{-1}\boldsymbol{Y},a_i,b_j\in\mathbb{F}_q$, and $\boldsymbol{X}$ is invertible.

Equation (5) is equivalent to solving a system of n^2 equations with $2n$ variables and can be expressed by

$$\boldsymbol{L}\boldsymbol{x}=\boldsymbol{0}\tag{6}$$

where

$$\boldsymbol{L}=((\overrightarrow{\boldsymbol{H}^0\boldsymbol{N}})^{\mathrm{T}},\ldots,(\overrightarrow{\boldsymbol{H}^{n-1}\boldsymbol{N}})^{\mathrm{T}},\ldots,-(\overrightarrow{\boldsymbol{M}^{n-1}})^{\mathrm{T}}),$$
$$\boldsymbol{x}=(a_0,\ldots,a_{n-1},b_0,\ldots,b_{n-1})^{\mathrm{T}}_{2n\times 1}.$$

Then the proposed BKT-B cryptosystem and BKT-FO cryptosystem always are vulnerable, which can be analyzed as follows.

Proposition 3 If an adversary can find matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$ satisfying Eq. (5), then the BKT-B and BKT-FO cryptosystems can be broken.

Proof If an adversary can find matrices $\widetilde{\boldsymbol{X}}=\sum\limits_{i=0}^{n-1}a_i\boldsymbol{H}^i$ and $\widetilde{\boldsymbol{Y}}=\sum\limits_{j=0}^{n-1}b_j\boldsymbol{M}^j$ satisfying Eq. (5), then $\widetilde{\boldsymbol{Y}}\boldsymbol{M}=\boldsymbol{M}\widetilde{\boldsymbol{Y}}$, $\widetilde{\boldsymbol{X}}^{-1}\boldsymbol{H}=\boldsymbol{H}\widetilde{\boldsymbol{X}}^{-1}$, $\widetilde{\boldsymbol{X}}^{-1}\boldsymbol{H}^i=\boldsymbol{H}^i\widetilde{\boldsymbol{X}}^{-1}$, and $\widetilde{\boldsymbol{Y}}\boldsymbol{M}^j=\boldsymbol{M}^j\widetilde{\boldsymbol{Y}}$ for every integers i and j.

For the BKT-B cryptosystem,

$$\widetilde{\boldsymbol{X}}^{-1}\boldsymbol{D}\widetilde{\boldsymbol{Y}}=(\sum_{i=0}^{n-1}a_i\boldsymbol{H}^i)^{-1}\boldsymbol{H}^{x_{\mathrm{r}}+x_B}\boldsymbol{M}^{y_{\mathrm{r}}+y_B}(\sum_{j=0}^{n-1}b_j\boldsymbol{M}^j)=$$

$$\boldsymbol{H}^{x_{\mathrm{r}}+x_{\boldsymbol{B}}}(\sum_{i=0}^{n-1}a_i\boldsymbol{H}^i)^{-1}(\sum_{j=0}^{n-1}b_j\boldsymbol{M}^j)\boldsymbol{M}^{y_{\mathrm{r}}+y_{\boldsymbol{B}}}=$$
$$\boldsymbol{H}^{x_{\mathrm{r}}+x_{\boldsymbol{B}}}\boldsymbol{N}\boldsymbol{M}^{y_{\mathrm{r}}+y_{\boldsymbol{B}}}=$$
$$\boldsymbol{H}^{x_{\mathrm{r}}+x_{\boldsymbol{B}}}\boldsymbol{H}^{x}\boldsymbol{M}^{y}\boldsymbol{M}^{y_{\mathrm{r}}+y_{\boldsymbol{B}}}=\boldsymbol{C} \tag{7}$$

According to the solving process of the message $\boldsymbol{m}$ in Proposition 1, the BKT-B cryptosystem is broken.

For the BKT-FO cryptosystem,

$$\widetilde{\boldsymbol{Y}}\boldsymbol{\tau}_1^{-1}\widetilde{\boldsymbol{X}}^{-1}\boldsymbol{\tau}_2=\widetilde{\boldsymbol{Y}}(\boldsymbol{H}^{x'}\boldsymbol{N}\boldsymbol{M}^{y'})^{-1}\widetilde{\boldsymbol{X}}^{-1}\boldsymbol{\tau}_2=$$
$$(\sum_{j=0}^{n-1}b_j\boldsymbol{M}^j)\boldsymbol{M}^{-y'}\boldsymbol{N}^{-1}\boldsymbol{H}^{-x'}(\sum_{i=0}^{n-1}a_i\boldsymbol{H}^i)^{-1}\boldsymbol{\tau}_2=$$
$$\boldsymbol{M}^{-y'}(\sum_{j=0}^{n-1}b_j\boldsymbol{M}^j)\boldsymbol{N}^{-1}(\sum_{i=0}^{n-1}a_i\boldsymbol{H}^i)^{-1}\boldsymbol{H}^{-x'}\boldsymbol{\tau}_2=$$
$$\boldsymbol{M}^{-y'}(\sum_{j=0}^{n-1}b_j\boldsymbol{M}^j)((\sum_{i=0}^{n-1}a_i\boldsymbol{H}^i)^{-1}\cdot$$
$$(\sum_{j=0}^{n-1}b_j\boldsymbol{M}^j))^{-1}(\sum_{i=0}^{n-1}a_i\boldsymbol{H}^i)^{-1}\boldsymbol{H}^{-x'}\boldsymbol{\tau}_2=$$
$$\boldsymbol{M}^{-y'}\boldsymbol{H}^{-x'}\boldsymbol{\tau}_2=$$
$$\boldsymbol{M}^{-y'}\boldsymbol{H}^{-x'}\boldsymbol{H}^{x'}\boldsymbol{M}^{y'}\boldsymbol{R}=\boldsymbol{R} \tag{8}$$

Because $(h_1,\boldsymbol{\tau}_3)$ are known, the message $\boldsymbol{m}=\boldsymbol{\tau}_3\oplus h_1(\boldsymbol{R})$ is obtained, that is, the BKT-FO cryptosystem is broken. This completes the proof.

Formally, the linearization equations attack on the BKT-B cryptosystem can be described by Algorithm 3.

The complexity for Algorithm 3 can be concluded in Table 2.

If we ignore small constant factors, then a linearization equations attack against the BKT-B cryptosystem can be finished with a bit complexity of $\mathcal{O}(n^{\omega+1}\log^2 q)$.

Algorithm 3 Solve the message m of the BKT-B cryptosystem

1: **Input** $(\boldsymbol{M},\boldsymbol{H},\boldsymbol{D},\boldsymbol{N},\boldsymbol{E},\Phi,\Psi,\pi)$;
2: Solve the following homogeneous linear equations in the $2n$ entries of the unknown vector $\boldsymbol{x}$: $\boldsymbol{L}\boldsymbol{x}=\boldsymbol{0}$;
3: Fix a basis for the solution space. Pick random solutions $\boldsymbol{x}$ until $\boldsymbol{X}=\sum_{i=0}^{n-1}a_i\boldsymbol{H}^i$ is invertible and compute $\boldsymbol{Y}=\sum_{i=0}^{n-1}b_i\boldsymbol{M}^i$;
4: Compute $\boldsymbol{C}=\boldsymbol{X}^{-1}\boldsymbol{D}\boldsymbol{Y},\boldsymbol{B}=\boldsymbol{E}\oplus\Phi(\boldsymbol{D},\boldsymbol{C}),(x_{\boldsymbol{B}},y_{\boldsymbol{B}})=\pi(\boldsymbol{B})$;
5: Calculate $\boldsymbol{A}=\boldsymbol{H}^{-x_{\boldsymbol{B}}}\boldsymbol{C}\boldsymbol{M}^{-y_{\boldsymbol{B}}}$;
6: The message $\boldsymbol{m}=\boldsymbol{B}\oplus\Psi(\boldsymbol{A})$;
7: Return $\boldsymbol{m}$.

Table 2 Computation cost of Algorithm 3.

Comp. content	Comp. cost	Explanation
$\boldsymbol{L}\boldsymbol{x}=\boldsymbol{0}$	$\mathcal{O}(n^2(2n)^{\omega-1}\log^2 q)$	n^2 equations in $2n$ variables
Solutions $\boldsymbol{x}$	$\mathcal{O}(2n(2n-r)^{\omega-1}\log^2 q)$	An invertible solution
Matrix $\boldsymbol{X}$	$\mathcal{O}((n-2)n^{\omega}\log^2 q)$	$\sum_{i=0}^{n-1}a_i\boldsymbol{H}^i$
Matrix $\boldsymbol{Y}$	$\mathcal{O}(2n^{\omega}\log^2 q)$	$\boldsymbol{X}^{-1}\boldsymbol{N}$

The method to calculate the message $\boldsymbol{m}$ of the BKT-FO cryptosystem can be concluded in Algorithm 4.

Table 2 indicates that a linearization equations attack against the BKT-FO cryptosystem can be finished with a complexity of $\mathcal{O}(n^{\omega+1}\log^2 q)$ without small constant factors.

4.3 Practical implementations for algorithms and a toy example

The computation costs of Algorithms 1 and 2 are almost the same, ignoring some small constants, and the computation costs of Algorithms 3 and 4 are smaller. We conduct our experiments on a 2.6 GHz Intel processor PC by Magma, with different parameters for Algorithm 1, the analysis results are given in Table 3.

We use a toy example to illustrate the attack methods over $\mathrm{GL}_3(\mathbb{F}_{2^{16}})$ in our cryptanalysis and the common information

$$\boldsymbol{H}=\begin{pmatrix}3421 & 14\,524 & 29\,952\\ 48\,988 & 24\,774 & 4993\\ 23\,688 & 29\,935 & 33\,266\end{pmatrix},$$
$$\boldsymbol{M}=\begin{pmatrix}24\,771 & 63\,557 & 612\\ 33\,158 & 24\,778 & 681\\ 962 & 57\,792 & 6149\end{pmatrix},$$

Algorithm 4 Solve the message m of the BKT-FO cryptosystem

1: **Input** $(h_1,h_2,\boldsymbol{H},\boldsymbol{M},\boldsymbol{N},\boldsymbol{\tau}_1,\boldsymbol{\tau}_2,\boldsymbol{\tau}_3)$;
2: Solve $\boldsymbol{X}^{-1},\boldsymbol{Y}$ by steps 2-3 in Algorithm 3;
3: Compute $\boldsymbol{R}=\boldsymbol{Y}\boldsymbol{\tau}_1^{-1}\boldsymbol{X}^{-1}\boldsymbol{\tau}_2$;
4: Calculate the message $\boldsymbol{m}=\boldsymbol{\tau}_3\oplus h_1(\boldsymbol{R})$;
5: Return $\boldsymbol{m}$.

Table 3 Complexity of algorithms.

q	n	Bit complexity		Attack time of Algorithm 1 (s)
		Algorithms 1 and 2	Algorithms 3 and 4	
2^8	10	$2^{30.0}$	$2^{21.3}$	0.016
2^{10}	10	$2^{31.6}$	$2^{22.4}$	0.031
2^{10}	20	$2^{27.2}$	$2^{21.2}$	1.912
2^{11}	50	$2^{33.7}$	$2^{26.0}$	387.782
2^{11}	100	$2^{38.5}$	$2^{29.3}$	30 345.860

$$\boldsymbol{N}=\begin{pmatrix} 9875 & 13\,949 & 7190 \\ 55\,586 & 26\,542 & 5567 \\ 51\,977 & 48\,759 & 60\,026 \end{pmatrix}.$$

The private keys $x = 120$, $y = 1125$.

4.3.1 A toy example for Algorithm 1

Because $(\boldsymbol{M}, \boldsymbol{H}, \boldsymbol{D}, \boldsymbol{N}, \boldsymbol{E}, \Phi, \Psi, \pi)$ are known information and $\boldsymbol{D}=\begin{pmatrix} 42\,425 & 9239 & 24\,147 \\ 64\,572 & 680 & 17\,698 \\ 27\,871 & 31\,097 & 9494 \end{pmatrix}$, $\mathcal{A}$ calculates a basis for solution space $\boldsymbol{Qx}=\boldsymbol{0}$, where $\operatorname{rank}(\boldsymbol{Q}) = 17$, the matrix

$$\boldsymbol{Q}=\begin{pmatrix}
0 & 48\,988 & 23\,688 & 14\,524 & 0 & 0 & 29\,952 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
14\,524 & 28\,059 & 29\,935 & 0 & 14\,524 & 0 & 0 & 29\,952 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
29\,952 & 4993 & 36\,015 & 0 & 0 & 14\,524 & 0 & 0 & 29\,952 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
48\,988 & 0 & 0 & 28\,059 & 48\,988 & 23\,688 & 4993 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 48\,988 & 0 & 14\,524 & 0 & 29\,935 & 0 & 4993 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 48\,988 & 29\,952 & 4993 & 57\,652 & 0 & 0 & 4993 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
23\,688 & 0 & 0 & 29\,935 & 0 & 0 & 36\,015 & 48\,988 & 23\,688 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 23\,688 & 0 & 0 & 29\,935 & 0 & 14\,524 & 57\,652 & 29\,935 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 23\,688 & 0 & 0 & 29\,935 & 29\,952 & 4993 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 33\,158 & 962 & 63\,557 & 0 & 0 & 612 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 63\,557 & 9 & 57\,792 & 0 & 63\,557 & 0 & 0 & 612 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 612 & 681 & 30\,918 & 0 & 0 & 63\,557 & 0 & 0 & 612 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 33\,158 & 0 & 0 & 9 & 33\,158 & 962 & 681 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 33\,158 & 0 & 63\,557 & 0 & 57\,792 & 0 & 681 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 33\,158 & 612 & 681 & 30\,927 & 0 & 0 & 681 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 962 & 0 & 0 & 57\,792 & 0 & 0 & 30\,918 & 33\,158 & 962 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 962 & 0 & 0 & 57\,792 & 0 & 63\,557 & 30\,927 & 57\,792 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 962 & 0 & 0 & 57\,792 & 612 & 681 & 0 \\
9875 & 55\,586 & 51\,977 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
13\,949 & 26\,542 & 48\,759 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7190 & 5567 & 60\,026 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 9875 & 55\,586 & 51\,977 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 13\,949 & 26\,542 & 48\,759 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 7190 & 5567 & 60\,026 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 9875 & 55\,586 & 51\,977 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 13\,949 & 26\,542 & 48\,759 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 7190 & 5567 & 60\,026 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix},$$

and the basis

$$\varepsilon = (\,64\,580\ 28\,100\ 38\,450\ 24\,075\ 19\,014\ 2982\ 19\,161\ 4460\ 57\,772\ 31\,773\ 35\,855\ 10\,138\ 9807\ 44\,461\ 25\,898\ 15\,835\ 7172\ 44\,148\,).$$

Transform the vector $\boldsymbol{\varepsilon}$ to matrices

$$\widetilde{\boldsymbol{X}^{-1}}=\begin{pmatrix} 64\,580 & 28\,100 & 38\,450 \\ 24\,075 & 19\,014 & 2982 \\ 19\,161 & 4460 & 57\,772 \end{pmatrix}$$

and

$$\widetilde{\boldsymbol{Y}}_1=\begin{pmatrix} 31\,773 & 35\,855 & 10\,138 \\ 9807 & 44\,461 & 25\,898 \\ 15\,835 & 7172 & 44\,148 \end{pmatrix}.$$

$$\widetilde{\boldsymbol{X}}=\widetilde{\boldsymbol{X}^{-1}}^{-1}=\begin{pmatrix} 16\,286 & 2287 & 2776 \\ 12\,155 & 3519 & 495 \\ 20\,088 & 43\,293 & 35\,662 \end{pmatrix}.$$

Hence

$$\boldsymbol{C}=\widetilde{\boldsymbol{X}}\boldsymbol{D}\widetilde{\boldsymbol{Y}}=\begin{pmatrix} 3418 & 10\,960 & 52\,722 \\ 58\,639 & 22\,085 & 44\,909 \\ 56\,051 & 26\,831 & 10\,092 \end{pmatrix}.$$

After having $\boldsymbol{C}$, $\mathcal{A}$ computes $\boldsymbol{B}, \pi(\boldsymbol{B})$, where

$$\boldsymbol{B}=\boldsymbol{E}\oplus\Phi(\boldsymbol{D},\widetilde{\boldsymbol{X}}\boldsymbol{D}\widetilde{\boldsymbol{Y}}),(x_{\boldsymbol{B}},y_{\boldsymbol{B}})=\pi(\boldsymbol{B}).$$

Then gets $\boldsymbol{A}=\boldsymbol{H}^{-x_{\boldsymbol{B}}}\boldsymbol{C}\boldsymbol{M}^{-y_{\boldsymbol{B}}}$. So the message $\boldsymbol{m}=\boldsymbol{B}\oplus\Psi(\boldsymbol{A})$ is obtained which means that the BKT-B cryptosystem is broken.

4.3.2 A toy example for Algorithm 2

According to Algorithm 1 and known information $(h_1, h_2, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_3)$, where

$$\boldsymbol{\tau}_1=\begin{pmatrix} 16\,661 & 4562 & 53\,485 \\ 36\,267 & 64\,901 & 56\,769 \\ 55\,817 & 39\,613 & 13\,843 \end{pmatrix},$$

$$\boldsymbol{\tau}_2=\begin{pmatrix} 60\,941 & 28\,560 & 61\,390 \\ 14\,734 & 52\,931 & 63\,284 \\ 133 & 10\,153 & 11\,102 \end{pmatrix}.$$

Compute

$$\boldsymbol{R}=\widetilde{\boldsymbol{Y}}\boldsymbol{\tau}_1^{-1}\widetilde{\boldsymbol{X}}\boldsymbol{\tau}_2=\begin{pmatrix} 27\,883 & 14\,708 & 31\,279 \\ 56\,670 & 27\,265 & 62\,455 \\ 45\,956 & 58\,153 & 44\,262 \end{pmatrix}.$$

Because $(h_1, \boldsymbol{\tau}_3)$ is known, the message

$$\boldsymbol{m}=\boldsymbol{\tau}_3\oplus h_1(\boldsymbol{R}).$$

4.3.3 A toy example for Algorithm 3

Due to Eq. (6),

$$\boldsymbol{L}=\begin{pmatrix} 9875 & 44\,997 & 7555 & 1 & 24\,771 & 9535 \\ 13\,949 & 3737 & 60\,725 & 0 & 63\,557 & 47\,241 \\ 7190 & 25\,436 & 8230 & 0 & 612 & 58\,536 \\ 55\,586 & 52\,760 & 44\,771 & 0 & 33\,158 & 44\,338 \\ 26\,542 & 15\,975 & 8660 & 1 & 24\,778 & 56\,842 \\ 5567 & 35\,683 & 22\,906 & 0 & 681 & 59\,597 \\ 51\,977 & 15\,154 & 65\,222 & 0 & 962 & 47\,207 \\ 48\,759 & 13\,015 & 44\,349 & 0 & 57\,792 & 20\,832 \\ 60\,026 & 32\,626 & 8488 & 1 & 6149 & 41\,522 \end{pmatrix}.$$

Solving $\boldsymbol{Lx} = \boldsymbol{0}$ by employing the method of Gauss elimination, $\mathcal{A}$ gets a basis for the solution space $\boldsymbol{\varepsilon} =$ (11 657 51 808 25 403 21 630 21 033 1).

Then

$$\widetilde{\boldsymbol{X}^{-1}} = 11\,657\boldsymbol{I}_3 + 51\,808\boldsymbol{H} + 25\,403\boldsymbol{H}^2 = \begin{pmatrix} 16\,679 & 20\,105 & 54\,846 \\ 25\,576 & 2072 & 27\,888 \\ 17\,709 & 22\,531 & 14\,548 \end{pmatrix},$$

$$\widetilde{\boldsymbol{X}} = \widetilde{\boldsymbol{X}^{-1}}^{-1} = \begin{pmatrix} 38\,828 & 31\,740 & 1025 \\ 9569 & 6994 & 23\,489 \\ 53\,184 & 27\,780 & 51\,390 \end{pmatrix},$$

$$\widetilde{\boldsymbol{Y}}_2 = 21\,630\boldsymbol{I}_3 + 21\,033\boldsymbol{M} + \boldsymbol{M}^2 = \begin{pmatrix} 33\,004 & 24\,540 & 13\,628 \\ 65\,186 & 39\,086 & 65\,011 \\ 36\,484 & 23\,678 & 58\,083 \end{pmatrix}.$$

Hence $\mathcal{A}$ gets

$$\boldsymbol{C} = \widetilde{\boldsymbol{X}}\boldsymbol{D}\widetilde{\boldsymbol{Y}} = \begin{pmatrix} 3418 & 10\,960 & 52\,722 \\ 58\,639 & 22\,085 & 44\,909 \\ 56\,051 & 26\,831 & 10\,092 \end{pmatrix}.$$

After having $\boldsymbol{C}$, $\mathcal{A}$ computes the message $\boldsymbol{m} = \boldsymbol{B} \oplus \Psi(\boldsymbol{A})$ which is the same as Algorithm 1.

4.3.4 A toy example for Algorithm 4

The known information $(h_1, h_2, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_3)$ is the same as Algorithm 2. By using $\widetilde{\boldsymbol{X}^{-1}}$ and $\widetilde{\boldsymbol{Y}}$ of Algorithm 3, $\mathcal{A}$ computes

$$\boldsymbol{R} = \widetilde{\boldsymbol{Y}}\boldsymbol{\tau}_1^{-1}\widetilde{\boldsymbol{X}^{-1}}\boldsymbol{\tau}_2 = \begin{pmatrix} 27\,883 & 14\,708 & 31\,279 \\ 56\,670 & 27\,265 & 62\,455 \\ 45\,956 & 58\,153 & 44\,262 \end{pmatrix}.$$

Hence the message

$$\boldsymbol{m} = \boldsymbol{\tau}_3 \oplus h_1(\boldsymbol{R})$$

is obtained, which means that the BKT-FO cryptosystem is broken.

5 Conclusion

In this paper, we showed that two public key cryptosystems based on non-Abelian factorization problems are insecure in the sense that an attacker who is able to solve the homogeneous linear equations with high efficiency in a given general linear group, is also able to break the two schemes. Moreover, other attack methods can also be of use in studying the two schemes. The question whether there exist other groups on which the two schemes are secure remains open. When designing a public key cryptosystem based on non-Abelian factorization problems on other groups, the considerations of the previous section must be taken into account. How to make a public key cryptosystem based on non-Abelian algebraic structures, which has the potential to resist known quantum attacks, also remains open.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Nos. 61303212, 61170080, 61202386, 61332019, U1135004, and 91018008), the National Key Basic Research and Development (973) Program of China (No. 2014CB340600), and the Natural Science Foundation of Hubei Province (Nos. 2011CDB453 and 2014CFB440)

References

[1] Z. Cao, *New Directions of Modern Cryptography*. CRC Press, 2012.

[2] M. Mosca, *Post-Quantum Cryptography*. Springer International Publishing, 2014.

[3] P. Gaborit, *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2013.

[4] S. Ling, D. H. Phan, D. Stehl'e, R. Steinfeld, Hardness of k-LWE and applications in traitor tracing, in *Proc. Advances in Cryptology-CRYPTO*, Santa Barbara, CA, USA, 2014, pp. 315–334.

[5] H. Zhang, J. Liu, J. Jia, S. Mao, and W. Wu, A survey on applications of matrix decomposition in cryptography, *Journal of Cryptologic Research*, vol. 9, no. 1, pp. 341–357, 2014.

[6] H. Wang, H. Zhang, Z. Wang, and M. Tang, Extended multivariate public key cryptosystems with secure encryption function, *SCIENCE CHINA Information Sciences*, vol. 54, no. 6, pp. 1161–1171, 2011.

[7] S. Mao, H. Zhang, W. Wu, J. Liu, and H. Wang, A resistant quantum key exchange protocol and its corresponding encryption scheme, *China Communications*, vol. 11, no. 9, pp. 131–141, 2014.

[8] Y. Yang, S. Zhang, J. Yang, J. Li, and Z. Li, Targeted fully homomorphic encryption based on a double decryption algorithm for polynomials, *Tsinghua Science and Technology*, vol. 19, no. 5, pp. 478–485, 2014.

[9] T. Boaz, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, *Journal of Cryptology*, vol. 28, no. 3, pp. 601–622 , 2015.

[10] S. Wang, Y. Zhu, D. Ma, and R. Feng, Lattice-based key exchange on small integer solution problem, *SCIENCE CHINA Information Sciences*, vol. 57, no. 11, pp. 1–12, 2014.

[11] M. Habeeb, D. Kahrobaei, C. Koupparis, and V. Shpilrain, Public key exchange using semidirect product of (semi)groups, in *Proceedings of ACNS 2013*, 2013.

[12] L. Gu, L. Wang, K. Ota, M. Dong, Z. Cao, and Y. Yang, New public key cryptosystems based on non-Abelian factorization problems, *Security and Communication Networks*, vol. 6, no. 7, pp. 912–922, 2013.

[13] A. Myasnikov, V. Shpilrain, and A. Ushakov, *Noncommutative Cryptography and Complexity of Grouptheoretic Problems*. American Mathematical Society, 2011.

[14] S. Gashkov and I. Sergeev, Complexity of computation in finite fields, *Journal of Mathematical Sciences*, vol. 191, no. 5, pp. 661–685, 2013.

[15] L. Bettale, J. C. Faug'ere, L. Perret, Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic, *Designs, Codes and Cryptography*, vol. 69, no. 1, pp. 1–52, 2013.

[16] L. Gu and S. Zheng, Conjugacy systems based on Nonabelian factorization problems and their applications in cryptography, *Journal of Applied Mathematics*, vol. 52, no. 2, pp. 1–9, 2014.

Jinhui Liu is a PhD candidate at the School of Computer of Wuhan University. She graduated from Wuhan University in 2013 with a master degree. Her research interests include cryptography and information security.

Aiwan Fan is an associate professor at the Computer School of Pingdingshan University. He graduated from Xidian University in 2007 with a master degree. His research interests include cryptography and information security.

Jianwei Jia is a PhD candidate at the School of Computer of Wuhan University. He graduated from Wuhan University in 2013 with a master degree. His research interests include cryptography and information security.

Huanguo Zhang is a currently professor and PhD supervisor at the School of Computer of Wuhan University. He graduated from Xidian University in 1970 with a bachelor degree. His research interests include information security and trusted computing.

Houzhen Wang received the PhD degree in information security from Wuhan University in 2011. He is currently a lecturer at the School of Computer of Wuhan University. His research interests include cryptography and information security.

Shaowu Mao is a PhD candidate at the School of Computer of Wuhan University. He graduated from Wuhan University in 2011 with a master degree. His research interests include cryptography and information security.