Cryptanalysis of Simple Matrix Scheme for Encryption

Chunsheng Gu

School of Computer Engineering, Jiangsu University of Technology,
Changzhou, 213001, China
{chunsheng_gu}@163.com

Abstract. Recently, Tao et al. presented a new simple and efficient multivariate pubic key encryption scheme based on matrix multiplication, which is called Simple Matrix Scheme or ABC. Using linearization method, we propose a polynomial time algorithm, which directly solves an equivalent private key from the public key of ABC. Furthermore, our attack can also be applied to the variants of ABC since these variants have the same algebraic structure as the ABC scheme. Therefore, the ABC cryptosystem and its variants are insecure.

Keywords: public key cryptography, multivariate pubic key, linearization attack, cryptanalysis

1 Introduction

Since Shor [1] presented a polynomial time quantum algorithm for integers factorization and discrete logarithm problem, the widely used public key encryption schemes such as RSA, DSA, and ECC [2–4] would become insecure once the quantum computer becomes a reality. This encourages researchers to study the new public key scheme in order to resist quantum computers attacks.

Multivariate public key cryptosystems (MPKC) are believed an alternative that can resist quantum computing attacks. This is because MPKC is based on a system of multivariate polynomials over a finite field that is an NP-hard problem [5, 6]. However, this does not mean that a public key scheme based on multivariate polynomials is secure. Many multivariate public key schemes have been broken in the past [7–10]. A major problem of all multivariate public key schemes is no security proof.

Recently, Tao et al. [11] presented a new simple and efficient multivariate pubic key encryption scheme based on matrix multiplication, which is called Simple Matrix Scheme or ABC. Subsequently, Ding, Petzoldt, and Wang [12] proposed an improved variant of ABC that introdces cubic polynomials, and claimed breaking this variant using algebraic attacks is at least as hard as solving a set of random quadratic equations. Very recently, Tao, Xiang, Petzoldt, and Ding [13] generalized the ABC scheme by using non-square matrices, instead of square matrices. To eliminate the decryption failures from ABC, Petzoldt, Ding, and Wang [14] described a new version of ABC, which uses tensor product of

matrices. However, Hashimoto [15] showed the security of this variant is much weaker than that of the origin ABC scheme. Furthermore, Peng, Tang, Chen, Wu, and Zhang [16] optimized the implementation of ABC by exploiting the power of modern x64 CPU to improve the efficiency.

In order to analyze the security of ABC and its variants, Moody, Perlner, and Smith-Tone [17] presented a structural key recovery attack using subspace differential invariants inherent to the ABC scheme. This attack takes time at least $O(q^s s^7 \log q)$ for ABC [1] and $O(sq^r n^3 \log q)$ for the improved ABC [12], where q, n, r, s were defined in the following scheme. If r, s are the security parameter or q is the exponential size of the security parameter, then the attack algorithm in [17] needs exponential time. Thus, the attack based on subspace differential invariants [17] did not completely break the ABC and its variants. Recently, Moody, Perlner, and Smith-Tone [18] further demonstrated that the cubic variant of ABC do not enhance the security of ABC. To the best of our knowledge, no polynomial time attacks were known before this work on the ABC and its variants.

Our main contribution is to prove that the ABC cryptosystem [11] and its variants [12, 13] are insecure. In this paper, we analyze the algebraic structure of ABC and transform this structure into a new algebraic mapping that is easy to apply with linearization techniques. Then using linearization equation technique, we present a polynomial time (i.e. $O(s^3 n^{12} \log q)$, or $O(s^3 n^9 \log q)$ by using attack method in Section 4) algorithm for ABC that solves an equivalent private key from its public key. Our key observation is that in order to implement the linearization attack for ABC, it is not necessary to use the higher-order linearization equations considered in [11–13], but only the cubic (or quadratic) linearization equations. That is, we can use a new linearization method to find an equivalent private key from the public key. Furthermore, since the variants in [12, 13] have the same algebraic structure as the ABC scheme, consequently the above attack can also generalize to these variants.

Organization. Section 2 describes the ABC cryptosystem. Section 3 provides the cryptanalysis of ABC. Section 4 presents the variants of ABC using rectangular matrix and its cryptanalysis. Section 5 describes the cubic ABC and its cryptanalysis. Section 6 draws conclusions.

2 ABC Cryptosystem

In this section, we briefly describe the ABC cryptosystem. For symbolic consistency, we adaptively use the following notations.

Let $\mathbb{F}$ be a finite field with q elements. Let $n, m, s \in \mathbb{N}$ be integers such that $n = s^2$ and $m = 2n$. Given a positive integer k, let $\mathbb{F}^k$ denote the set of all k-tuples of elements of $\mathbb{F}$. We use bold lower-case letters like $\mathbf{x}$ to denote column vectors, and the transpose of vectors like $\mathbf{x}^T$ to denote row vectors. We use bold upper-case letters like $\mathbf{A}$ to denote matrices, and represent a matrix by the column vector.

We denote the plaintext by $\mathbf{x} = (x_1, x_2, \cdots, x_n)^T \in \mathbb{F}^n$ and the ciphertext by $\mathbf{y} = (y_1, y_2, \cdots, y_m)^T \in \mathbb{F}^m$. The polynomial ring with n variables in $\mathbb{F}$ is denoted by $\mathbb{F}[x_1, \cdots, x_n]$.

Let $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$ and $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$ be two linear transformations, that is,

$$\mathcal{L}_1(x_1, x_2, \cdots, x_n) = \mathbf{L}_1\mathbf{x},$$
$$\mathcal{L}_2(y_1, y_2, \cdots, y_m) = \mathbf{L}_2\mathbf{y},$$

where $\mathbf{L}_1 \in \mathbb{F}^{n\times n}, \mathbf{L}_2 \in \mathbb{F}^{m\times m}$, $\mathbf{x} = (x_1, x_2, \cdots, x_n)^T$ and $\mathbf{y} = (y_1, y_2, \cdots, y_m)^T$.

Key Generation:

(1) Given $\mathbf{x} = (x_1, x_2, \cdots, x_n)^T$, choose the linear map $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$:

(1.1) Choose an invertible matrix $\mathbf{L}_1 \in \mathbb{F}^{n\times n}$ as the linear map $\mathcal{L}_1$.

(1.2) Compute $\overline{\mathbf{x}} = \mathbf{L}_1\mathbf{x}$, where $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n)^T$.

(2) Define the central map $\mathcal{F}$ over $\overline{\mathbf{x}}$:

(2.1) Given $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n)^T$, generate matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}$:

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,s} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,s} \\ \vdots & \vdots & \cdots & \vdots \\ a_{s,1} & a_{s,2} & \cdots & a_{s,s} \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,s} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,s} \\ \vdots & \vdots & \cdots & \vdots \\ b_{s,1} & b_{s,2} & \cdots & b_{s,s} \end{pmatrix},$$

$$\mathbf{C} = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,s} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,s} \\ \vdots & \vdots & \cdots & \vdots \\ c_{s,1} & c_{s,2} & \cdots & c_{s,s} \end{pmatrix},$$

where for $i, j \in [s]$, $a_{i,j} = \overline{x}_{(i-1)*s+j}$, and $b_{i,j}, c_{i,j}$ are randomly linear combinations of the set $\{\overline{x}_1, \cdots, \overline{x}_n\}$.

(2.2) Set $\mathbf{E}_1 = \mathbf{A} \cdot \mathbf{B}$ and $\mathbf{E}_2 = \mathbf{A} \cdot \mathbf{C}$.

(2.3) Define the central map $\mathcal{F}$ over $\overline{\mathbf{x}}$:

$$\mathcal{F}(\overline{x}_1, \cdots, \overline{x}_n) = (f_1(\overline{x}_1, \cdots, \overline{x}_n), \cdots, f_m(\overline{x}_1, \cdots, \overline{x}_n)),$$

where for $i, j \in [s]$, $f_{(i-1)s+j}$ is the (i, j) element in $\mathbf{E}_1$, $f_{s^2+(i-1)s+j}$ is the (i, j) element in $\mathbf{E}_2$.

(2.4) Replacing $\overline{\mathbf{x}}$ with $\mathbf{L}_1\mathbf{x}$ for $\mathcal{F}$, generate the central map $\widetilde{\mathcal{F}}$ over $\mathbf{x}$:

$$\begin{aligned} \widetilde{\mathcal{F}}(x_1, \cdots, x_n) &= \mathcal{F}((\mathbf{L}_1\mathbf{x})^T) \\ &= (\mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n) \\ &= (\widetilde{f}_1(x_1, \cdots, x_n), \cdots, \widetilde{f}_m(x_1, \cdots, x_n)). \end{aligned}$$

(3) For $\widetilde{\mathcal{F}}(x_1,\cdots,x_n)$, choose the linear map $\mathcal{L}_2:\mathbb{F}^m\to\mathbb{F}^m$:

(3.1) Choose an invertible matrix $\mathbf{L}_2\in\mathbb{F}^{m\times m}$ as the linear map $\mathcal{L}_2$.
(3.2) Define the maps

$$\begin{aligned}\overline{\mathcal{F}}(x_1,\cdots,x_n)&=(\mathbf{L}_2(\widetilde{\mathcal{F}}(x_1,\cdots,x_n))^T)^T\\&=(\mathcal{L}_2\circ\widetilde{\mathcal{F}})(x_1,\cdots,x_n)\\&=(\mathcal{L}_2\circ\mathcal{F}\circ\mathcal{L}_1)(x_1,\cdots,x_n)\\&=(\overline{f}_1(x_1,\cdots,x_n),\cdots,\overline{f}_m(x_1,\cdots,x_n)).\end{aligned}$$

(4) Output the public key $pk=\{\overline{\mathcal{F}}=\mathcal{L}_2\circ\mathcal{F}\circ\mathcal{L}_1\}$ and the private key $sk=\{\mathbf{L}_1,\mathbf{L}_2,\mathbf{B},\mathbf{C}\}$.

Encryption: Given the public key pk and a message $\mathbf{d}=(d_1,d_2,\cdots,d_n)^T\in\mathbb{F}^n$, then the ciphertext is

$$\mathbf{y}^T=(y_1,y_2,\cdots,y_m)=\overline{\mathcal{F}}(d_1,d_2,\cdots,d_n).$$

Decryption: Given the secret key sk and a ciphertext $\mathbf{y}^T=(y_1,y_2,\cdots,y_m)$, one decrypts as follows:

(1) Compute $\overline{\mathbf{y}}^T=(\overline{y}_1,\overline{y}_2,\cdots,\overline{y}_m)=\mathcal{L}_2^{-1}(\mathbf{y}^T)=(\mathbf{L}_2^{-1}\mathbf{y})^T$, and set

$$\mathbf{E}_1=\begin{pmatrix}\overline{y}_1 & \overline{y}_2 & \cdots & \overline{y}_s\\ \overline{y}_{s+1} & \overline{y}_{s+2} & \cdots & \overline{y}_{2s}\\ \vdots & \vdots & \vdots & \vdots\\ \overline{y}_{(s-1)s+1} & \overline{y}_{(s-1)s+2} & \cdots & \overline{y}_{s^2}\end{pmatrix}\in\mathbb{F}^{s\times s},$$

$$\mathbf{E}_2=\begin{pmatrix}\overline{y}_{s^2+1} & \overline{y}_{s^2+2} & \cdots & \overline{y}_{s^2+s}\\ \overline{y}_{s^2+s+1} & \overline{y}_{s^2+s+2} & \cdots & \overline{y}_{s^2+2s}\\ \vdots & \vdots & \vdots & \vdots\\ \overline{y}_{s^2+(s-1)s+1} & \overline{y}_{s^2+(s-1)s+2} & \cdots & \overline{y}_{2s^2}\end{pmatrix}\in\mathbb{F}^{s\times s}.$$

(2) By $\mathbf{E}_1=\mathbf{AB}$ and $\mathbf{E}_2=\mathbf{AC}$, we consider the following cases:

– If $\mathbf{E}_1$ is invertible, then $\mathbf{BE}_1^{-1}\mathbf{E}_2=\mathbf{C}$. We get n linear equations with n unknowns $\overline{x}_1,\cdots,\overline{x}_n$.

– If $\mathbf{E}_2$ is invertible, but $\mathbf{E}_1$ is not invertible, then $\mathbf{CE}_2^{-1}\mathbf{E}_1=\mathbf{B}$. We also obtain n linear equations with n unknowns $\overline{x}_1,\cdots,\overline{x}_n$.

– If $\mathbf{E}_1,\mathbf{E}_2$ are not invertible, but $\mathbf{A}$ is invertible, then $\mathbf{A}^{-1}\mathbf{E}_1=\mathbf{B}$ and $\mathbf{A}^{-1}\mathbf{E}_2=\mathbf{C}$. We consider the elements of $\mathbf{A}^{-1}$ as the new variables, and end up with $m=2n$ linear equations in m unknowns. Then, we can eliminate the new variables to derive n linear equations in the $\overline{x}_1,\cdots,\overline{x}_n$.

– Otherwise, the decryption fails. Note that there exists an error for the decryption analysis of this case in ABC [1]. Because if the rank of $\mathbf{A}$ is r with $r<s$, then there exists a nonsigular matrix $\mathbf{W}$ such that $\mathbf{WA}=\begin{pmatrix}\mathbf{I}_{r\times r} & \mathbf{A}'_{r\times(s-r)}\\ \mathbf{0}_{(s-r)\times r} & \mathbf{0}_{(s-r)\times(s-r)}\end{pmatrix}$, instead of $\mathbf{WA}=\begin{pmatrix}\mathbf{I}_{r\times r} & \mathbf{0}_{r\times(s-r)}\\ \mathbf{0}_{(s-r)\times r} & \mathbf{0}_{(s-r)\times(s-r)}\end{pmatrix}$. Namely, $\mathbf{A}'_{r\times(s-r)}$ is generally not a "0" matrix.

(3)Given the above solution $\overline{\mathbf{x}}^T = (\overline{d}_1, \overline{d}_2, \cdots, \overline{d}_n)$, compute the plaintext

$$\mathbf{d}^T = (d_1, d_2, \cdots, d_n) = \mathcal{L}_1^{-1}(\overline{x}_1, \cdots, \overline{x}_n).$$

Remark 1. If $\mathbf{B}, \mathbf{C}$ are homogeneous linear combinations in $\{\overline{x}_1, \cdots, \overline{x}_n\}$, then one cannot solve a unique solution. For this case, authors provided a new encrypting step in [12] to determine which of multiple solutions is really a plaintext. Furthermore, in this case, the finite field $\mathbb{F}$ must be polynomial in n. Otherwise, the decryption time cannot be polynomial time in n.

3 Cryptanalysis of ABC

In this section, using linearization equation technique, we present a polynomial time algorithm that directly solves an equivalent private key from the public key of ABC. As a result, we break this ABC cryptosystem.

Theorem 1. Given the public key pk of the ABC cryptosystem, there exists a polynomial time algorithm which finds an equivalent secret key.

Proof. By $\overline{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1$, we have $\mathcal{L}_2^{-1} \circ \overline{\mathcal{F}} = \mathcal{F} \circ \mathcal{L}_1$. Hence,

$$\begin{aligned} &(\mathcal{L}_2^{-1} \circ \overline{\mathcal{F}})(x_1, \cdots, x_n) \\ &= (\mathbf{L}_2^{-1}(\overline{f}_1(x_1, \cdots, x_n), \cdots, \overline{f}_m(x_1, \cdots, x_n))^T)^T \\ &= (\mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T)^T \end{aligned}$$

where $y_j = \overline{f}_j(x_1, \cdots, x_n), j \in [m]$.

$$\begin{aligned} &(\mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n) \\ &= \mathcal{F}(\mathcal{L}_1(x_1, \cdots, x_n)) \\ &= \mathcal{F}((\mathbf{L}_1(x_1, \cdots, x_n)^T)^T) \\ &= \mathcal{F}(\overline{x}_1, \cdots, \overline{x}_n) \\ &= (f_1(\overline{x}_1, \cdots, \overline{x}_n), \cdots, f_m(\overline{x}_1, \cdots, \overline{x}_n)) \end{aligned}$$

Again by $\mathbf{E}_1 = \mathbf{AB}$ and $\mathbf{E}_2 = \mathbf{AC}$ and the definition of the central map $\mathcal{F}$, we have that $\mathbf{E}_1, \mathbf{E}_2, \mathbf{A}, \mathbf{B}, \mathbf{C}$ are defined in the variables $\{\overline{x}_1, \cdots, \overline{x}_n\}$.

In the following Claims 1-7, we construct a system of linear equations from the public key of ABC by applying linearization methods. Then, in Claim 8, we provide a polynomial time algorithm to solve this system of linear equations. Finally, in Claims 9-10, we show that an equivalent private key obtained from Claim 8 can decrypt an arbitrary ciphertext of ABC.

□

Claim 1. Suppose $\mathbf{L}_2^{-1} = \begin{pmatrix} v_{1,1} & \cdots & v_{1,m} \\ \vdots & \vdots & \vdots \\ v_{m,1} & \cdots & v_{m,m} \end{pmatrix}$, then $\overline{\mathbf{y}} = \mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T$.

Proof. By the definition of $\mathcal{L}_2$,

$$\begin{aligned}\overline{\mathbf{y}} &= (\mathcal{L}_2^{-1}(y_1, \cdots, y_m))^T \\ &= \mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T \\ &= (\sum_{j=1}^m v_{1,j}y_j, \cdots, \sum_{j=1}^m v_{m,j}y_j)^T.\end{aligned}$$

□

Claim 2. Suppose $\mathbf{L}_1 = \begin{pmatrix} u_{1,1} & \cdots & u_{1,n} \\ \vdots & \vdots & \vdots \\ u_{n,1} & \cdots & u_{n,n} \end{pmatrix}$, then $\overline{\mathbf{x}} = \mathbf{L}_1(x_1, \cdots, x_n)^T$.

Proof. By the definition of $\mathcal{L}_1$,

$$\begin{aligned}\overline{\mathbf{x}} &= (\mathcal{L}_1(x_1, \cdots, x_n))^T \\ &= \mathbf{L}_1(x_1, \cdots, x_n)^T \\ &= (\sum_{j=1}^n u_{1,j}x_j, \cdots, \sum_{j=1}^n u_{n,j}x_j)^T.\end{aligned}$$

□

According to the ABC cryptosystem, the entries $b_{i,j}, c_{i,j}, i, j \in [s]$ in $\mathbf{B}, \mathbf{C}$ are randomly linear combinations of $\{\overline{x}_1, \cdots, \overline{x}_n\}$. Without loss of generality, we assume $b_{i,j} = \sum_{k=1}^n b_{i,j,k}\overline{x}_k$ and $c_{i,j} = \sum_{k=1}^n c_{i,j,k}\overline{x}_k$

Therefore, by the definitions of $\mathbf{A}, \mathbf{B}, \mathbf{C}$, we obtain

$$\mathbf{A} = \begin{pmatrix} \overline{x}_1 & \overline{x}_2 & \cdots & \overline{x}_s \\ \overline{x}_{s+1} & \overline{x}_{s+2} & \cdots & \overline{x}_{2s} \\ \vdots & \vdots & \cdots & \vdots \\ \overline{x}_{(s-1)s+1} & \overline{x}_{(s-1)s+2} & \cdots & \overline{x}_{s^2} \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} \sum_{k=1}^n b_{1,1,k}\overline{x}_k & \sum_{k=1}^n b_{1,2,k}\overline{x}_k & \cdots & \sum_{k=1}^n b_{1,s,k}\overline{x}_k \\ \sum_{k=1}^n b_{2,1,k}\overline{x}_k & \sum_{k=1}^n b_{2,2,k}\overline{x}_k & \cdots & \sum_{k=1}^n b_{2,s,k}\overline{x}_k \\ \vdots & \vdots & \cdots & \vdots \\ \sum_{k=1}^n b_{s,1,k}\overline{x}_k & \sum_{k=1}^n b_{s,2,k}\overline{x}_k & \cdots & \sum_{k=1}^n b_{s,s,k}\overline{x}_k \end{pmatrix},$$

$$\mathbf{C} = \begin{pmatrix} \sum_{k=1}^n c_{1,1,k}\overline{x}_k & \sum_{k=1}^n c_{1,2,k}\overline{x}_k & \cdots & \sum_{k=1}^n c_{1,s,k}\overline{x}_k \\ \sum_{k=1}^n c_{2,1,k}\overline{x}_k & \sum_{k=1}^n c_{2,2,k}\overline{x}_k & \cdots & \sum_{k=1}^n c_{2,s,k}\overline{x}_k \\ \vdots & \vdots & \cdots & \vdots \\ \sum_{k=1}^n c_{s,1,k}\overline{x}_k & \sum_{k=1}^n c_{s,2,k}\overline{x}_k & \cdots & \sum_{k=1}^n c_{s,s,k}\overline{x}_k \end{pmatrix},$$

Claim 3. Suppose $\overline{\mathbf{y}}^T = \mathcal{L}_2^{-1}(y_1, \cdots, y_m)$, then

$$\mathbf{E}_1 = \begin{pmatrix} \overline{y}_1 & \overline{y}_2 & \cdots & \overline{y}_s \\ \overline{y}_{s+1} & \overline{y}_{s+2} & \cdots & \overline{y}_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{(s-1)s+1} & \overline{y}_{(s-1)s+2} & \cdots & \overline{y}_{s^2} \end{pmatrix},$$

$$\mathbf{E}_2 = \begin{pmatrix} \overline{y}_{s^2+1} & \overline{y}_{s^2+2} & \cdots & \overline{y}_{s^2+s} \\ \overline{y}_{s^2+s+1} & \overline{y}_{s^2+s+2} & \cdots & \overline{y}_{s^2+2s} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{s^2+(s-1)s+1} & \overline{y}_{s^2+(s-1)s+2} & \cdots & \overline{y}_{2s^2} \end{pmatrix}.$$

Proof. By the definition of $\mathbf{E}_1, \mathbf{E}_2$ and $\mathcal{F}$, the result directly follows.

□

Claim 4. Suppose $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{E}_1, \mathbf{E}_2$ are defined as above. Then we can generate the system of m quadratic equations in variables $\overline{x}_1, \cdots, \overline{x}_n$ and $\overline{y}_1, \cdots, \overline{y}_m$.

Proof. Using $\mathbf{E}_1 = \mathbf{A} \cdot \mathbf{B}$ and $\mathbf{E}_2 = \mathbf{A} \cdot \mathbf{C}$, the result directly follows.

□

Claim 5. Given the system of m quadratic equations in Claim 4, then we can generate the system of m quadratic equations in variables $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$.

Proof. By Claims 1 and 2, $\overline{\mathbf{y}} = \mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T$ and $\overline{\mathbf{x}} = \mathbf{L}_1(x_1, \cdots, x_n)^T$.

Thus, for the system of quadratic equations in Claim 4, we can get the result by replacing $\overline{x}_1, \cdots, \overline{x}_n$ and $\overline{y}_1, \cdots, \overline{y}_m$ with the corresponding entries in $\mathbf{L}_1(x_1, \cdots, x_n)^T$ and $\mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T$.

Without loss of generality, we denote by $\widetilde{\mathbf{E}}_1 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{B}}$ and $\widetilde{\mathbf{E}}_2 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{C}}$ this new system in variables $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$.

□

Since one can generate arbitrary number of plaintext and ciphertext pairs for any public key cryptosystem. Consequently, when we consider $\mathbf{x}, \mathbf{y}$ as known variables, and $\{b_{i,j,k}, c_{i,j,k}, i, j \in [s], k \in [n]\}$, $\{u_{i,j}, i, j \in [n]\}$, and $\{v_{i,j}, i, j \in [m]\}$ as unknown variables, we can establish a new system of equations.

Claim 6. Given $\widetilde{\mathbf{E}}_1 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{B}}$ and $\widetilde{\mathbf{E}}_2 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{C}}$ in Claim 5, and a set of plaintext-ciphertext pairs $\{x_1, \cdots, x_n\}$ and $\{y_1, \cdots, y_m\}$ generated by the public key of ABC, then the system of equations becomes a system of cubic equations in $3n^2 + m^2$ unknown variables $\{b_{i,j,k}, c_{i,j,k}, i, j \in [s], k \in [n]\}$, $\{u_{i,j}, i, j \in [n]\}$, and $\{v_{i,j}, i, j \in [m]\}$.

Proof. It is easy to verify that the number of unknown variables $\{b_{i,j,k}, c_{i,j,k}, i, j \in [s], k \in [n]\}$, $\{u_{i,j}, i, j \in [n]\}$, and $\{v_{i,j}, i, j \in [m]\}$ is $3n^2 + m^2$. Similarly, it is not difficult to verify this system is cubic equations over these unknown variables.

□

Claim 7. Given the system of cubic equations in Claim 6, then using relinearization technique in variables $\{b_{i,j,k}, c_{i,j,k}, i, j \in [s], k \in [n]\}$, $\{u_{i,j}, i, j \in [n]\}$, and $\{v_{i,j}, i, j \in [m]\}$, the system becomes a system of linear equations with $2sn^4 + m^2$ unknown variables that have the form $b_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$, or $c_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$, or $\{v_{i,j}, i, j \in [m]\}$.

Proof. By Claim 5, we have the following system in variables $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$.

$$\begin{cases} \widetilde{\mathbf{E}}_1 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{B}} \\ \widetilde{\mathbf{E}}_2 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{C}} \end{cases} \tag{1}$$

By $\mathbf{E}_1 = \mathbf{AB}$ and Claim 2, we get the $(1,1)$ element of $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$ as follows:

$$\begin{aligned} (\widetilde{\mathbf{A}}\widetilde{\mathbf{B}})_{1,1} &= \sum_{k=1}^{n} b_{1,1,k}\overline{x}_k\overline{x}_1 + \sum_{k=1}^{n} b_{1,2,k}\overline{x}_k\overline{x}_2 + \cdots + \sum_{k=1}^{n} b_{1,s,k}\overline{x}_k\overline{x}_s \\ &= \sum_{k=1}^{n} b_{1,1,k}(\sum_{j=1}^{n} u_{k,j}x_j \sum_{j=1}^{n} u_{1,j}x_j) + \\ &\quad \sum_{k=1}^{n} b_{1,2,k}(\sum_{j=1}^{n} u_{k,j}x_j \sum_{j=1}^{n} u_{2,j}x_j) + \\ &\quad \cdots + \\ &\quad \sum_{k=1}^{n} b_{1,s,k}(\sum_{j=1}^{n} u_{k,j}x_j \sum_{j=1}^{n} u_{s,j}x_j) \end{aligned}$$

It is easy to see that for the variables $\{b_{i,j,k}, i,j \in [s], k \in [n]\}$, $\{u_{i,j}, i,j \in [n]\}$, there are $s \times n \times (n^2) = sn^3$ different cubic terms in the $(1,1)$ element of $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$. So, the total number of different cubic terms in $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$ are sn^4.

Thus, from the perspective of unknown variables in $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{L}_1$, any cubic term in these elements of $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$ and $\widetilde{\mathbf{A}}\widetilde{\mathbf{C}}$ must be of the form $b_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$ or $c_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$. As a result, there are at most $2 \times sn^4 = 2sn^4$ different cubic terms in the right side $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$ and $\widetilde{\mathbf{A}}\widetilde{\mathbf{C}}$ of the system (1).

For the left side $\widetilde{\mathbf{E}}_1, \widetilde{\mathbf{E}}_2$ of the system (1), we have the linear terms with m^2 unknown variables in $\mathbf{L}_2^{-1}$.

Consequently, the total number of unknown variables generated by relinearization method is $2sn^4 + m^2$.

□

In the following, we first present Algorithm 1 that runs in the polynomial time to solve the linear system (1). Then, we show the solution returned by Algorithm 1 is an equivalent private key.

Claim 8. Given the relinearization system of equations with $2sn^4 + m^2$ unknowns in Claim 7, there exists a polynomial time algorithm, which finds a feasible solution for the unknown variables $\{b_{i,j,k}, c_{i,j,k}, i,j \in [s], k \in [n]\}$, $\{u_{i,j}, i,j \in [n]\}$, and $\{v_{i,j}, i,j \in [m]\}$.

Proof. By Claim 7, we obtain the relinearization system of equations with $2sn^4 + m^2$ unknown variables. These unknown variables are all of the form $b_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}, c_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}, i,j \in [s], k \in [n], i_1, i_2, j_1, j_2 \in [n]$, and $\{v_{i,j}, i,j \in [m]\}$.

Since there are $2sn^4 + m^2$ unknown variables, we require $2sn^4 + m^2$ linear equations. Again, using a pair of plaintext-ciphertext, we can get m linear equations over unknown variables. So, we can construct the relinearization system of equations by using $sn^3 + m$ plaintext-ciphertext pairs.

Assume the linear system of equations is $\mathbf{Dz} = \mathbf{0}$ with $f = 2sn^4 + m^2$ unknown variables. Algorithm 1 solves $\mathbf{Dz} = \mathbf{0}$ and generates an equivalent private key as follows.

Algorithm 1 Solving the linear system to find an equivalent private key.

Input: The linear system of equations $\mathbf{Dz} = \mathbf{0}$ with $f = 2sn^4+m^2$ unknown variables, where z_t is of the form $b_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$, $c_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$, v_{i_3,j_3}.

Output: An equivalent private key.

1: Using Gaussian Elimination method, transform $\mathbf{Dz} = \mathbf{0}$ into the following form:

$$\begin{pmatrix} \mathbf{I}_{w\times w} & \mathbf{0}_{w\times(f-w)} \\ \mathbf{0}_{(f-w)\times w} & \mathbf{I}_{(f-w)\times(f-w)} \end{pmatrix} \begin{pmatrix} \mathbf{z}_S \\ \mathbf{z}_{\overline{S}} \end{pmatrix} = \begin{pmatrix} \mathbf{U}_{w\times(f-w)}\mathbf{z}_{\overline{S}} \\ \mathbf{z}_{\overline{S}} \end{pmatrix}, \tag{2}$$

where $S \cup \overline{S} = [f]$, and $\mathbf{U}_{w\times(f-w)} \in \mathbb{F}^{w\times(f-w)}$.

2: Without loss of generality, assume $\mathbf{z}_S = (z_1, \cdots, z_w)^T$, $\mathbf{z}_{\overline{S}} = (z_{w+1}, \cdots, z_f)^T$. Randomly set $\mathbf{z}_{\overline{S}} = (\alpha_{w+1}, \cdots, \alpha_f)^T$ such that $\alpha_t \in \mathbb{F}\backslash\{0\}, t = w+1, \cdots, f$.

3: By the system (2), we compute $\mathbf{z}_S = \mathbf{U}_{w\times(f-w)}\mathbf{z}_{\overline{S}} = \mathbf{U}_{w\times(f-w)}(\alpha_{w+1}, \cdots, \alpha_f)^T$. Let $\mathbf{z}_S = (\alpha_1, \cdots, \alpha_w)^T$.

4: Choose an arbitrary non-univariate $z_t, t \in [f]$, such as $z_t = b_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$. Without loss of generality, we randomly set $u_{i_1,j_1} = \beta_{i_1,j_1} \in \mathbb{F}\backslash\{0\}$. For any other forms of z_t, e.g. $z_t = c_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$, or $b_{i,j,k}u_{i_1,j_1}$, or $b_{i,j,k}$ et al., we deal with z_t similarly.

5: If u_{i_1,j_1} appears in $z_\gamma, \gamma \in [f]$, e.g. $z_\gamma = c_{i',j',k'}u_{i_1,j_1}u_{i'_2,j'_2}$, then we replace z_γ with $\beta_{i_1,j_1}c_{i',j',k'}u_{i'_2,j'_2}$ and override a new unknown variable $z_\gamma = c_{i',j',k'}u_{i'_2,j'_2} = \alpha_\gamma \times \beta^{-1}_{i_1,j_1}$. We similarly deal with any other forms.

6: If there exists a non-univariate $z_t, t \in [f]$ with quadratic or cubic in the unknown variables $\{b_{i,j,k}, c_{i,j,k}, i,j \in [s], k \in [n]\}$, $\{u_{i,j}, i,j \in [n]\}$, then goto 4.

7: **return** a feasible solution for the unknown variables $\{b_{i,j,k}, c_{i,j,k}, i,j \in [s], k \in [n]\}$, $\{u_{i,j}, i,j \in [n]\}$, and $\{v_{i,j}, i,j \in [m]\}$.

Time analysis of Algorithm 1: Given the linear system $\mathbf{Dz} = \mathbf{0}$ with $f = 2sn^4 + m^2$ unknown variables:

Step 1: The Gaussian Elimination method costs time $O(f^3 \log q) = O(s^3n^{12} \log q)$.

Step 2: Setting $\mathbf{z}_{\overline{S}}$ costs time $O(f \log q) = O(sn^4 \log q)$.

Step 3: Computing $\mathbf{z}_S$ costs time $O(f^2 \log q)$.

Step 4: Choosing an arbitrary non-univariate $z_t, t \in [f]$ costs time $O(f \log q)$.

Step 5: Scanning and overriding $z_\gamma, \gamma \in [f]$ requires time $O(f \log q)$.

Step 6: By Claim 6, there exist $3n^2+m^2$ unknown variables $\{b_{i,j,k}, c_{i,j,k}, i,j \in [s], k \in [n]\}$, $\{u_{i,j}, i,j \in [n]\}$, and $\{v_{i,j}, i,j \in [m]\}$. However, only $3n^2$ unknown variables appear in non-univariate $z_t, t \in [f]$. Hence the number of "goto" Step 4 is at most $3n^2$. On the other hand, checking whether there exists a non-univariate $z_t, t \in [f]$ takes time $O(f)$. So, this substep requires time at most $3n^2 \times O(f \log q) = O(sn^6 \log q)$.

Thus, Algorithm 1 runs in time $O(s^3n^{12} \log q)$.

□

Claim 9. The probability that $\mathbf{L}_1$ obtained by Algorithm 1 is not invertible is $\frac{1}{q}$.

Proof. Assume $\mathbf{L}_1$ consists of $\{u_{i,j}, i,j \in [n]\}$ returned by Algorithm 1. Since for a random matrix $\mathbf{L} \in \mathbb{F}^{n\times n}$, the probability $\det(\mathbf{L}) = 0$ is $\frac{1}{|\mathbb{F}|} = \frac{1}{q}$. Without loss of generality, we can assume $\{u_{i,j}, i,j \in [n]\}$ are random elements in $\mathbb{F}$. So, the probability $\det(\mathbf{L}_1) = 0$ is also $\frac{1}{q}$.

□

Claim 10. Given a feasible solution for $\{b_{i,j,k}, c_{i,j,k}, i,j \in [s], k \in [n]\}$, $\{u_{i,j}, i,j \in [n]\}$, and $\{v_{i,j}, i,j \in [m]\}$ returned by Algorithm 1, one can generate an equivalent private key $\{\mathbf{B}, \mathbf{C}, \mathbf{L}_1, \mathbf{L}_2^{-1}\}$, and correctly decrypt ciphertexts in the ABC cryptosystem.

Proof. By Claim 9, the probability $\mathbf{L}_1$ is invertible is $1 - \frac{1}{q}$. So, if $\mathbf{L}_1$ is not invertible, we reuse Algorithm 1 to generate a new feasible solution. Without loss of generality, assume $\mathbf{L}_1$ is invertible.

Since $\mathbf{L}_2^{-1}$ itself is already in the form of inverse matrix, it is not required invertible. Of course, the probability that $\mathbf{L}_2^{-1}$ is invertible is also $1 - \frac{1}{q}$.

Thus, $\{\mathbf{B}, \mathbf{C}, \mathbf{L}_1, \mathbf{L}_2^{-1}\}$ can be used an equivalent private key.

Consequently, given an arbitrary ciphertext of ABC, we can decrypt it into the plaintext using the private key $\{\mathbf{B}, \mathbf{C}, \mathbf{L}_1, \mathbf{L}_2^{-1}\}$ obtained by Algorithm 1.

□

Remark 2. Note that by $\overline{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1$ and plaintext-ciphertext pairs generated by the public key, we can directly construct a system of quartic equations on unknown variables, and get an equivalent secret key by directly applying linearization method. In this case, the linearization system has $2sn^4m^2$ unknown variables. We can solve this linearization system by similarly using Algorithm 1.

4 ABC using rectangular matrix and Cryptanalysis

In the ABC cryptosystem, there are two shortcomings: (1) the probability of decryption failure is relatively large; (2) the decryption algorithm is less efficient.

To overcome these shortcomings, Tao et al. proposed a variant scheme of ABC in [12] that uses rectangular matrices. Since this improved scheme preserves the same algebraic structure as the basic ABC scheme [11], as a result, the attack method described above can also be applied to this variant. In the following, we first give the ABC using rectangular matrix in [12], and then provide cryptanalysis for this variant.

4.1 ABC using rectangular matrix

Let $\mathbb{F}$ be a finite field with q elements, and $r, s, u, v, m, n \in \mathbb{N}$ be integers such that $m = s \cdot (u + v)$, $s \geq r$ and $(n - r(u + v - s)) \cdot (n - r(u + v - s) + 1) \leq 2m$.

Key Generation:

(1) Given $\mathbf{x} = (x_1, x_2, \cdots, x_n)^T$, choose the linear map $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$:

(1.1) Choose an invertible matrix $\mathbf{L}_1 \in \mathbb{F}^{n\times n}$ as the linear map $\mathcal{L}_1$.

(1.2) Compute $\overline{\mathbf{x}} = \mathbf{L}_1\mathbf{x}$, where $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n)^T$.

(2) Define the central map $\mathcal{F}$ over $\overline{x}$:

(2.1) Given $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n)^T$, generate matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}$:

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,r} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,r} \\ \vdots & \vdots & \cdots & \vdots \\ a_{s,1} & a_{s,2} & \cdots & a_{s,r} \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,u} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,u} \\ \vdots & \vdots & \cdots & \vdots \\ b_{r,1} & b_{r,2} & \cdots & b_{r,u} \end{pmatrix},$$

$$\mathbf{C} = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,v} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,v} \\ \vdots & \vdots & \cdots & \vdots \\ c_{r,1} & c_{r,2} & \cdots & c_{r,v} \end{pmatrix},$$

where the elements $a_{i,j}$ in $\mathbf{A}$ are randomly chosen from the set $\{\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n\}$, and the elements $b_{i,j}, c_{i,j}$ in $\mathbf{B}, \mathbf{C}$ are randomly linear combinations of the set $\{\overline{x}_1, \cdots, \overline{x}_n\}$, respectively.

(2.2) Set $\mathbf{E}_1 = \mathbf{A} \cdot \mathbf{B}$ and $\mathbf{E}_2 = \mathbf{A} \cdot \mathbf{C}$.

(2.3) Define the central map $\mathcal{F}$ over $\overline{\mathbf{x}}$:

$$\mathcal{F}(\overline{x}_1, \cdots, \overline{x}_n) = (f_1(\overline{x}_1, \cdots, \overline{x}_n), \cdots, f_m(\overline{x}_1, \cdots, \overline{x}_n)),$$

where for $i \in [s], j \in [u]$, $f_{(i-1)u+j}$ is the (i,j) element in $\mathbf{E}_1$, and for $i \in [s], j \in [v]$, $f_{su+(i-1)v+j}$ is the (i,j) element in $\mathbf{E}_2$.

(2.4) Replacing $\overline{\mathbf{x}}$ with $\mathbf{L}_1\mathbf{x}$ for $\mathcal{F}$, generate the central map $\widetilde{\mathcal{F}}$ over $\mathbf{x}$:

$$\begin{aligned} \widetilde{\mathcal{F}}(x_1, \cdots, x_n) &= (\mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n) \\ &= (\widetilde{f}_1(x_1, \cdots, x_n), \cdots, \widetilde{f}_m(x_1, \cdots, x_n)). \end{aligned}$$

(3) For $\widetilde{\mathcal{F}}(x_1, \cdots, x_n)$, choose the linear map $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$:

(3.1) Choose an invertible matrix $\mathbf{L}_2 \in \mathbb{F}^{m \times m}$ as the linear map $\mathcal{L}_2$.

(3.2) Define the maps

$$\begin{aligned} \overline{\mathcal{F}}(x_1, \cdots, x_n) &= (\mathcal{L}_2 \circ \widetilde{\mathcal{F}})(x_1, \cdots, x_n) \\ &= (\mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n) \\ &= (\overline{f}_1(x_1, \cdots, x_n), \cdots, \overline{f}_m(x_1, \cdots, x_n)). \end{aligned}$$

(4) Output the public key $pk = \{\overline{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1\}$ and the private key $sk = \{\mathbf{L}_1, \mathbf{L}_2, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$.

Note that $\mathbf{A}$ in the private key is not required when decrypting a ciphertext of ABC with rectangular matrices.

Encryption: Given the public key pk and a message $\mathbf{d}^T = (d_1, d_2, \cdots, d_n) \in \mathbb{F}^n$, then the ciphertext is

$$\mathbf{y}^T = (y_1, y_2, \cdots, y_m) = \overline{\mathcal{F}}(d_1, d_2, \cdots, d_n).$$

Decryption: Given the secret key sk and a ciphertext $\mathbf{y}^T = (y_1, y_2, \cdots, y_m)$, one decrypts as follows:

(1) Compute $\overline{\mathbf{y}}^T = (\overline{y}_1, \overline{y}_2, \cdots, \overline{y}_m) = \mathcal{L}_2^{-1}(\mathbf{y}) = (\mathbf{L}_2^{-1}\mathbf{y})^T$, and set

$$\mathbf{E}_1 = \begin{pmatrix} \overline{y}_1 & \overline{y}_2 & \cdots & \overline{y}_u \\ \overline{y}_{u+1} & \overline{y}_{u+2} & \cdots & \overline{y}_{2u} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{(s-1)u+1} & \overline{y}_{(s-1)u+2} & \cdots & \overline{y}_{su} \end{pmatrix} \in \mathbb{F}^{s\times u},$$

$$\mathbf{E}_2 = \begin{pmatrix} \overline{y}_{su+1} & \overline{y}_{su+2} & \cdots & \overline{y}_{su+v} \\ \overline{y}_{su+v+1} & \overline{y}_{su+v+2} & \cdots & \overline{y}_{su+2v} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{su+(s-1)v+1} & \overline{y}_{su+(s-1)v+2} & \cdots & \overline{y}_{su+sv} \end{pmatrix} \in \mathbb{F}^{s\times v}.$$

(2) By $\mathbf{E}_1 = \mathbf{AB}$ and $\mathbf{E}_2 = \mathbf{AC}$, we find a plaintext vector $\overline{\mathbf{x}} \in \mathbb{F}^n$ such that $\mathcal{F}(\overline{\mathbf{x}}) = \overline{\mathbf{y}}^T$ as follows:

- If the rank of $\mathbf{A}$ is r, then there exists an $r \times s$ matrix $\mathbf{W}$ such that $\mathbf{W} \times \mathbf{A} = \mathbf{I}$, where $\mathbf{I}$ is the $r \times r$ identity matrix. First, by $\mathbf{E}_1 = \mathbf{AB}$ and $\mathbf{E}_2 = \mathbf{AC}$, we get $\mathbf{W} \times \mathbf{E}_1 = \mathbf{B}$ and $\mathbf{W} \times \mathbf{E}_2 = \mathbf{C}$, and generate $r(u+v)$ linear equations in $rs+n$ unknown variables when considering the elements of $\mathbf{W}$ as unknown variables. Then, we eliminate rs unknown variables of $\mathbf{W}$ from these equations, and get about $r(u+v-s)$ linear equations in unknown variables $\{\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n\}$. Finally, using Gaussian elimination and Relinearization algorithm [19], we find a solution $\overline{\mathbf{x}}^T = (\overline{d}_1, \overline{d}_2, \cdots, \overline{d}_n)$.
- In the rank of $\mathbf{A}$ is less than r, decryption remains an open problem.

(3) Compute the plaintext $(d_1, d_2, \cdots, d_n) = \mathcal{L}_1^{-1}(\overline{d}_1, \overline{d}_2, \cdots, \overline{d}_n)$.

4.2 Cryptanalysis

For this improved scheme, $\mathbf{A}, \mathbf{B}, \mathbf{C}$ are the rectangular matrices, instead of the square matrices in the origin ABC scheme. Furthermore, each element of $\mathbf{A}$ in this variant is randomly chosen from $\{\overline{x}_1, \cdots, \overline{x}_n\}$, whereas each element of $\mathbf{A}$ in ABC is ordered from $\{\overline{x}_1, \cdots, \overline{x}_n\}$. Namely, we can directly write out the elements of $\mathbf{A}$ according to $\{\overline{x}_1, \cdots, \overline{x}_n\}$ for ABC, but we cannot achieve this for its variant.

However, by the definition of $\mathbf{A}, \mathbf{B}, \mathbf{C}$, we observe that if we substitute $\{\overline{x}_1, \cdots, \overline{x}_n\}$ with $\mathbf{L}_1\mathbf{x}$ for the elements of $\mathbf{A}, \mathbf{B}, \mathbf{C}$, then $\widetilde{\mathbf{A}}, \widetilde{\mathbf{B}}, \widetilde{\mathbf{C}}$ generated by this method are defined in the variables $\{x_1, \cdots, x_n\}$. As a result, we do not need to know in advance how the elements of $\mathbf{A}$ choose from $\{\overline{x}_1, \cdots, \overline{x}_n\}$. Furthermore, the above attack for ABC does not matter about matrix shape. Hence, we can generalize the above attack to this variant.

Theorem 2. Given the public key pk of ABC using rectangular matrix, there exists a polynomial time algorithm which finds an equivalent secret key.

Proof. By $\overline{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1$, we have $\mathcal{L}_2^{-1} \circ \overline{\mathcal{F}} = \mathcal{F} \circ \mathcal{L}_1 = \widetilde{\mathcal{F}}$. Hence,

$$(\mathcal{L}_2^{-1} \circ \overline{\mathcal{F}})(x_1, \cdots, x_n) = (\mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T)^T$$

where $y_j = \overline{f}_j(x_1, \cdots, x_n), j \in [m]$.

$$\begin{aligned}(\mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n) &= \widetilde{\mathcal{F}}(x_1, \cdots, x_n) \\ &= (\widetilde{f}_1(x_1, \cdots, x_n), \cdots, \widetilde{f}_m(x_1, \cdots, x_n))\end{aligned}$$

Again by $\mathbf{E}_1 = \mathbf{AB}$ and $\mathbf{E}_2 = \mathbf{AC}$ and the definition of the central map $\mathcal{F}$, we have that $\mathbf{E}_1, \mathbf{E}_2, \mathbf{A}, \mathbf{B}, \mathbf{C}$ are defined in the variables $\{\overline{x}_1, \cdots, \overline{x}_n\}$.

Replacing $\overline{\mathbf{x}}$ with $\mathbf{L}_1\mathbf{x}$, we have the following system in the variables $x_1, \cdots, x_n$:

$$\begin{cases}\mathbf{E}_1 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{B}} \\ \mathbf{E}_2 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{C}}\end{cases} \tag{3}$$

On the other hand, given $\overline{\mathbf{y}}^T = (\overline{y}_1, \overline{y}_2, \cdots, \overline{y}_m) = \mathcal{L}_2^{-1}(\mathbf{y})$, we have

$$\mathbf{E}_1 = \begin{pmatrix} \overline{y}_1 & \overline{y}_2 & \cdots & \overline{y}_u \\ \overline{y}_{u+1} & \overline{y}_{u+2} & \cdots & \overline{y}_{2u} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{(s-1)u+1} & \overline{y}_{(s-1)u+2} & \cdots & \overline{y}_{su} \end{pmatrix} \in \mathbb{F}^{s \times u},$$

$$\mathbf{E}_2 = \begin{pmatrix} \overline{y}_{su+1} & \overline{y}_{su+2} & \cdots & \overline{y}_{su+v} \\ \overline{y}_{su+v+1} & \overline{y}_{su+v+2} & \cdots & \overline{y}_{su+2v} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{su+(s-1)v+1} & \overline{y}_{su+(s-1)v+2} & \cdots & \overline{y}_{su+sv} \end{pmatrix} \in \mathbb{F}^{s \times v}.$$

Replacing $\overline{\mathbf{y}}$ with $\mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T$, we get the following system in the variables $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$:

$$\begin{cases}\widetilde{\mathbf{E}}_1 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{B}} \\ \widetilde{\mathbf{E}}_2 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{C}}\end{cases} \tag{4}$$

In the following proof, we first give two claims about the elements of $\widetilde{\mathbf{A}}, \widetilde{\mathbf{B}}, \widetilde{\mathbf{C}}$ in the equation (4).

Claim 11. The elements $\widetilde{a}_{i,j}$ in $\widetilde{\mathbf{A}}$ can be represented linear combination of the set $\{x_1, \cdots, x_n\}$.

Proof. Since the elements $a_{i,j}, i \in [s], j \in [r]$ in $\mathbf{A}$ are randomly chosen from the set $\{\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n\}$, without loss of generality, assume $a_{i,j} = \overline{x}_t, t \in [n]$.

By $\overline{\mathbf{x}} = \mathbf{L}_1\mathbf{x}$, we have $\overline{x}_t = \sum_{k=1}^{n} u_{t,k}x_k$.

So, $a_{i,j} = \sum_{k=1}^{n} u_{t,k}x_k$. Namely, $\widetilde{a}_{i,j} = \sum_{k=1}^{n} \widetilde{a}_{i,j,k}x_k$ with $\widetilde{a}_{i,j,k} = u_{t,k}$. The result follows.

□

Claim 12. The elements $\widetilde{b}_{i,j}, \widetilde{c}_{i,j}$ in $\widetilde{\mathbf{B}}, \widetilde{\mathbf{C}}$ can be represented linear combination of the set $\{x_1, \cdots, x_n\}$.

Proof. Since the elements $b_{i,j}$ in $\mathbf{B}$ are randomly linear combinations of the set $\{\overline{x}_1, \cdots, \overline{x}_n\}$, without loss of generality, assume $b_{i,j} = \sum_{t=1}^{n} b_{i,j,t}\overline{x}_t$.

By $\overline{\mathbf{x}} = \mathbf{L}_1\mathbf{x}$, we have $b_{i,j} = \sum_{t=1}^{n} b_{i,j,t} \sum_{k=1}^{n} u_{t,k}x_k$.

We arrange $b_{i,j}$ and write it as $\widetilde{b}_{i,j} = \sum_{k=1}^{n} \widetilde{b}_{i,j,k}x_k$, where $\widetilde{b}_{i,j,k} = \sum_{t=1}^{n} b_{i,j,t}u_{t,k}$.

Similarly, we can obtain $\widetilde{c}_{i,j} = \sum_{k=1}^{n} \widetilde{c}_{i,j,k}x_k$, where $\widetilde{c}_{i,j,k} = \sum_{t=1}^{n} c_{i,j,t}u_{t,k}$.

□

The proof of Theorem 2 continue:

In the following, we first analyze the $(1,1)$ element of $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$ as follows:

$$\begin{aligned}(\widetilde{\mathbf{A}}\widetilde{\mathbf{B}})_{1,1} &= \sum_{j=1}^{r} \widetilde{a}_{1,j}\widetilde{b}_{j,1} \\ &= \sum_{j=1}^{r} (\sum_{k=1}^{n} \widetilde{a}_{1,j,k}x_k)(\sum_{k=1}^{n} \widetilde{b}_{j,1,k}x_k)\end{aligned}$$

It is easy to verify that there are rn^2 different quadratic terms $\widetilde{a}_{1,j,k_1}\widetilde{b}_{j,1,k_2}$ in $(\widetilde{\mathbf{A}}\widetilde{\mathbf{B}})_{1,1}$. So, there are $su \times rn^2$ different quadratic terms in $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$.

Similarly, there are also $sv \times rn^2$ different quadratic terms in $\widetilde{\mathbf{A}}\widetilde{\mathbf{C}}$.

Now, we can construct a system of linear equations with $s(u+v) \times rn^2 + m^2$ unknown variables from the public key of the variant by applying linearization methods, and solve an equivalent private key by using Algorithm 1 in Claim 8.

Furthermore, solving an equivalent private key takes time at most $(s(u+v) \times rn^2 + m^2)^3 \log q = O(r^3m^3n^6 \log q)$.

This completes the proof of Theorem 2.

□

Notice that the above equivalent private key only includes $\mathcal{L}_2^{-1}$ and $\widetilde{\mathcal{F}}$. So, one no longer uses the linear inverse transformation $\mathcal{L}_1^{-1}$ when decrypting a ciphertext.

Remark 3. (1)If we require the equivalent private key obtained by Theorem 2 can generate the public key of the variant, then we need to directly build the linearization system from $\overline{\mathcal{F}} = \mathcal{L}_2 \circ \widetilde{\mathcal{F}}$ and add the coefficient equations in $\overline{\mathcal{F}} = \mathcal{L}_2 \circ \widetilde{\mathcal{F}}$ into the linearization system. It is not difficult to verify that there are $rn^2(su + sv)m^2 = rn^2m^3$ different cubic terms in this case. Similarly, we can solve this linearization system by using Algorithm 1 in Claim 8. (2)When $s = r = u = v$, the variant becomes the origin ABC scheme. Namely, the origin ABC scheme is a special case of the variant. So, the origin ABC scheme can

also be broken by using the attack method in this section. Furthermore, when applying the attack method in this section to ABC, there only exists $2sn^3 + m^2$ different quadratic terms. Consequently, the time complexity of attacking ABC will reduce to $O(s^3n^9 \log q)$.

5 Cubic ABC and Cryptanalysis

To improve the security of ABC, Ding, Petzoldt, and Wang [13] describe a cubic ABC. In this improved version, the elements of $\mathbf{A}$ are setting as random quadratic polynomials. However, the cubic ABC scheme has the same structure of ABC. As a result, we can also break the cubic ABC scheme using similar method attacking ABC.

5.1 Cubic ABC

Let $n, m, s \in \mathbb{N}$ be integers such that $n = s^2$ and $m = 2n$. We denote the plaintext by $(x_1, x_2, \cdots, x_n) \in \mathbb{F}^n$ and the ciphertext by $(y_1, y_2, \cdots, y_m) \in \mathbb{F}^m$.

Key Generation:

(1) Given $\mathbf{x} = (x_1, x_2, \cdots, x_n)^T$, choose the linear map $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$:

(1.1) Choose an invertible matrix $\mathbf{L}_1 \in \mathbb{F}^{n\times n}$ as the linear map $\mathcal{L}_1$.

(1.2) Compute $\overline{\mathbf{x}} = \mathbf{L}_1\mathbf{x}$, where $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n)^T$.

(2) Define the central map $\mathcal{F}$ over $\overline{\mathbf{x}}$:

(2.1) Given $\overline{\mathbf{x}} = (\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n)^T$, generate matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}$:

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,s} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,s} \\ \vdots & \vdots & \cdots & \vdots \\ a_{s,1} & a_{s,2} & \cdots & a_{s,s} \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,s} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,s} \\ \vdots & \vdots & \cdots & \vdots \\ b_{s,1} & b_{s,2} & \cdots & b_{s,s} \end{pmatrix},$$

$$\mathbf{C} = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,s} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,s} \\ \vdots & \vdots & \cdots & \vdots \\ c_{s,1} & c_{s,2} & \cdots & c_{s,s} \end{pmatrix},$$

where $a_{i,j}, i, j \in [s]$ are random quadratic polynomials in $\{\overline{x}_1, \cdots, \overline{x}_n\}$, and $b_{i,j}, c_{i,j}, i, j \in [s]$ are randomly linear combinations in $\{\overline{x}_1, \cdots, \overline{x}_n\}$.

(2.2) Set $\mathbf{E}_1 = \mathbf{A} \cdot \mathbf{B}$ and $\mathbf{E}_2 = \mathbf{A} \cdot \mathbf{C}$.

(2.3) Define the central map $\mathcal{F}$ over $\overline{x}$:

$$\mathcal{F}(\overline{x}_1, \cdots, \overline{x}_n) = (f_1(\overline{x}_1, \cdots, \overline{x}_n), \cdots, f_m(\overline{x}_1, \cdots, \overline{x}_n)),$$

where for $i, j \in [s]$, $f_{(i-1)s+j}$ is the (i, j) element in $\mathbf{E}_1$, $f_{s^2+(i-1)s+j}$ is the (i, j) element in $\mathbf{E}_2$.

(2.4) Replacing $\overline{\mathbf{x}}$ with $\mathbf{L}_1\mathbf{x}$ for $\mathcal{F}$, generate the central map $\widetilde{\mathcal{F}}$ over $\mathbf{x}$:

$$\begin{aligned}\widetilde{\mathcal{F}}(x_1, \cdots, x_n) &= (\mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n) \\ &= (\widetilde{f}_1(x_1, \cdots, x_n), \cdots, \widetilde{f}_m(x_1, \cdots, x_n)).\end{aligned}$$

(3) For $\widetilde{\mathcal{F}}(x_1, \cdots, x_n)$, choose the linear map $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$:

(3.1) Choose an invertible matrix $\mathbf{L}_2 \in \mathbb{F}^{m\times m}$ as the linear map $\mathcal{L}_2$.

(3.2) Define the maps

$$\begin{aligned}\overline{\mathcal{F}}(x_1, \cdots, x_n) &= (\mathcal{L}_2 \circ \widetilde{\mathcal{F}})(x_1, \cdots, x_n) \\ &= (\mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n) \\ &= (\overline{f}_1(x_1, \cdots, x_n), \cdots, \overline{f}_m(x_1, \cdots, x_n)).\end{aligned}$$

(4) Output the public key $pk = \{\overline{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1\}$ and the private key $sk = \{\mathbf{L}_1, \mathbf{L}_2, \mathbf{B}, \mathbf{C}\}$.

Encryption: Given the public key pk and a message $\mathbf{d}^T = (d_1, d_2, \cdots, d_n) \in \mathbb{F}^n$, then the ciphertext is

$$\mathbf{y}^T = (y_1, y_2, \cdots, y_m) = \overline{\mathcal{F}}(d_1, d_2, \cdots, d_n).$$

Decryption: Given the secret key sk and a ciphertext $\mathbf{y}^T = (y_1, y_2, \cdots, y_m)$, one decrypts as follows:

(1) Compute $\overline{\mathbf{y}}^T = (\overline{y}_1, \overline{y}_2, \cdots, \overline{y}_m) = \mathcal{L}_2^{-1}(\mathbf{y}) = (\mathbf{L}_2^{-1}\mathbf{y})^T$, and set

$$\mathbf{E}_1 = \begin{pmatrix} \overline{y}_1 & \overline{y}_2 & \cdots & \overline{y}_s \\ \overline{y}_{s+1} & \overline{y}_{s+2} & \cdots & \overline{y}_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{(s-1)s+1} & \overline{y}_{(s-1)s+2} & \cdots & \overline{y}_{s^2} \end{pmatrix} \in \mathbb{F}^{s\times s},$$

$$\mathbf{E}_2 = \begin{pmatrix} \overline{y}_{s^2+1} & \overline{y}_{s^2+2} & \cdots & \overline{y}_{s^2+s} \\ \overline{y}_{s^2+s+1} & \overline{y}_{s^2+s+2} & \cdots & \overline{y}_{s^2+2s} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{s^2+(s-1)s+1} & \overline{y}_{s^2+(s-1)s+2} & \cdots & \overline{y}_{2s^2} \end{pmatrix} \in \mathbb{F}^{s\times s}.$$

(2) By $\mathbf{E}_1 = \mathbf{AB}$ and $\mathbf{E}_2 = \mathbf{AC}$, we consider the following cases:

– If $\mathbf{E}_1$ is invertible, then $\mathbf{B}\mathbf{E}_1^{-1}\mathbf{E}_2 = \mathbf{C}$. We get n linear equations with n unknowns $\overline{x}_1, \cdots, \overline{x}_n$.

– If $\mathbf{E}_2$ is invertible, but $\mathbf{E}_1$ is not invertible, then $\mathbf{C}\mathbf{E}_2^{-1}\mathbf{E}_1 = \mathbf{B}$. We also obtain n linear equations with n unknowns $\overline{x}_1, \cdots, \overline{x}_n$.

– If $\mathbf{E}_1, \mathbf{E}_2$ are not invertible, but $\mathbf{A}$ is invertible, then $\mathbf{A}^{-1}\mathbf{E}_1 = \mathbf{B}$ and $\mathbf{A}^{-1}\mathbf{E}_2 = \mathbf{C}$. We consider the elements of $\mathbf{A}^{-1}$ as the new variables, and end up with $m = 2n$ linear equations in m unknowns. Then, we can eliminate the new variables to derive n linear equations in the $\overline{x}_1, \cdots, \overline{x}_n$.

– Otherwise, the decryption fails.

(3)Given the above solution $\overline{x}^T = (\overline{d}_1, \overline{d}_2, \cdots, \overline{d}_n)$, compute the plaintext

$$(d_1, d_2, \cdots, d_n) = \mathcal{L}_1^{-1}(\overline{x}_1, \cdots, \overline{x}_n).$$

5.2 Cryptanalysis

Except with the definition of $\mathbf{A}$, the cubic ABC scheme is same as ABC. So, we can also generate an equivalent private key for the cubic ABC applying the above similar method.

Since the elements $a_{i,j}, i, j \in [s]$ of $\mathbf{A}$ are random quadratic polynomials in $\{\overline{x}_1, \cdots, \overline{x}_n\}$, we can write $\mathbf{A} = \mathbf{A}^{(2)} + \mathbf{A}^{(1)} + \mathbf{A}^{(0)} = (a_{i,j}^{(2)}) + (a_{i,j}^{(1)}) + (a_{i,j}^{(0)})$, where the element $a_{i,j}^{(2)}$ of $\mathbf{A}^{(2)}$ is a quadratic polynomial, the element $a_{i,j}^{(1)}$ of $\mathbf{A}^{(1)}$ is a linear polynomial, and the element $a_{i,j}^{(0)}$ of $\mathbf{A}^{(0)}$ is a constant polynomial.

That is, $\mathbf{AB} = \mathbf{A}^{(2)}\mathbf{B} + \mathbf{A}^{(1)}\mathbf{B} + \mathbf{A}^{(0)}\mathbf{B}$, $\mathbf{AC} = \mathbf{A}^{(2)}\mathbf{C} + \mathbf{A}^{(1)}\mathbf{C} + \mathbf{A}^{(0)}\mathbf{C}$.

Now, we can rewrite the public key as follows:

$$\begin{aligned}\overline{\mathcal{F}} &= \overline{\mathcal{F}}^{(3)} + \overline{\mathcal{F}}^{(2)} + \overline{\mathcal{F}}^{(1)} \\ &= \mathcal{L}_2 \circ (\mathcal{F}^{(3)} + \mathcal{F}^{(2)} + \mathcal{F}^{(1)}) \circ \mathcal{L}_1 \\ &= \mathcal{L}_2 \circ \mathcal{F}^{(3)} \circ \mathcal{L}_1 + \mathcal{L}_2 \circ \mathcal{F}^{(2)} \circ \mathcal{L}_1 + \mathcal{L}_2 \circ \mathcal{F}^{(1)} \circ \mathcal{L}_1\end{aligned}$$

where $\mathcal{F}^{(3)}$ (resp. $\mathcal{F}^{(2)}, \mathcal{F}^{(1)}$) is cubic (resp. quadratic, one) central map.

Similarly, we can also obtain $\mathcal{L}_2^{-1} \circ \overline{\mathcal{F}} = \mathcal{F}^{(3)} \circ \mathcal{L}_1 + \mathcal{F}^{(2)} \circ \mathcal{L}_1 + \mathcal{F}^{(1)} \circ \mathcal{L}_1$. Thus, we can find an equivalent secret key by using the same method of attacking ABC.

Theorem 3. Given the public key pk of the cubic ABC, there exists a polynomial time algorithm which finds an equivalent secret key.

Proof. By $\mathcal{L}_2^{-1} \circ \overline{\mathcal{F}} = \mathcal{F} \circ \mathcal{L}_1$, we have

$$(\mathcal{L}_2^{-1} \circ \overline{\mathcal{F}})(x_1, \cdots, x_n) = (\mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T)^T$$

where $y_j = \overline{f}_j(x_1, \cdots, x_n), j \in [m]$.

$$\begin{aligned}(\mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n) &= (\mathcal{F}^{(3)} \circ \mathcal{L}_1 + \mathcal{F}^{(2)} \circ \mathcal{L}_1 + \mathcal{F}^{(1)} \circ \mathcal{L}_1)(x_1, \cdots, x_n) \\ &= \widetilde{\mathcal{F}}^{(3)}(x_1, \cdots, x_n) + \widetilde{\mathcal{F}}^{(2)}(x_1, \cdots, x_n) + \widetilde{\mathcal{F}}^{(1)}(x_1, \cdots, x_n)\end{aligned}$$

Since $\mathbf{E}_1 = \mathbf{AB}$, $\mathbf{E}_2 = \mathbf{AC}$ and $\mathbf{E}_1, \mathbf{E}_2, \mathbf{A}, \mathbf{B}, \mathbf{C}$ are defined in the variables $\{\overline{x}_1, \cdots, \overline{x}_n\}$, we obtain a system in the variables $x_1, \cdots, x_n$ by replacing $\overline{\mathbf{x}}$ with $\mathbf{L}_1\mathbf{x}$:

$$\begin{cases}\mathbf{E}_1 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{B}} = \widetilde{\mathbf{A}}^{(2)}\widetilde{\mathbf{B}} + \widetilde{\mathbf{A}}^{(1)}\widetilde{\mathbf{B}} + \widetilde{\mathbf{A}}^{(0)}\widetilde{\mathbf{B}} \\ \mathbf{E}_2 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{C}} = \widetilde{\mathbf{A}}^{(2)}\widetilde{\mathbf{C}} + \widetilde{\mathbf{A}}^{(1)}\widetilde{\mathbf{C}} + \widetilde{\mathbf{A}}^{(0)}\widetilde{\mathbf{C}}\end{cases} \tag{5}$$

Furthermore, given $\overline{\mathbf{y}}^T = (\overline{y}_1, \overline{y}_2, \cdots, \overline{y}_m) = \mathcal{L}_2^{-1}(\mathbf{y})$, we have

$$\mathbf{E}_1 = \begin{pmatrix} \overline{y}_1 & \overline{y}_2 & \cdots & \overline{y}_s \\ \overline{y}_{s+1} & \overline{y}_{s+2} & \cdots & \overline{y}_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{(s-1)s+1} & \overline{y}_{(s-1)s+2} & \cdots & \overline{y}_{s^2} \end{pmatrix} \in \mathbb{F}^{s\times s},$$

$$\mathbf{E}_2 = \begin{pmatrix} \overline{y}_{s^2+1} & \overline{y}_{s^2+2} & \cdots & \overline{y}_{s^2+s} \\ \overline{y}_{s^2+s+1} & \overline{y}_{s^2+s+2} & \cdots & \overline{y}_{s^2+2s} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{s^2+(s-1)s+1} & \overline{y}_{s^2+(s-1)s+2} & \cdots & \overline{y}_{2s^2} \end{pmatrix} \in \mathbb{F}^{s\times s}.$$

Replacing $\overline{\mathbf{y}}$ with $\mathbf{L}_2^{-1}(y_1, \cdots, y_m)^T$, we get a system in the variables $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$:

$$\begin{cases} \widetilde{\mathbf{E}}_1 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{B}} = \widetilde{\mathbf{A}}^{(2)}\widetilde{\mathbf{B}} + \widetilde{\mathbf{A}}^{(1)}\widetilde{\mathbf{B}} + \widetilde{\mathbf{A}}^{(0)}\widetilde{\mathbf{B}} \\ \widetilde{\mathbf{E}}_2 = \widetilde{\mathbf{A}} \cdot \widetilde{\mathbf{C}} = \widetilde{\mathbf{A}}^{(2)}\widetilde{\mathbf{C}} + \widetilde{\mathbf{A}}^{(1)}\widetilde{\mathbf{C}} + \widetilde{\mathbf{A}}^{(0)}\widetilde{\mathbf{C}} \end{cases} \tag{6}$$

Since $\widetilde{\mathbf{A}}^{(0)}$ is a constant matrix, we let $\widetilde{\mathbf{A}}^{(0)} = \widetilde{a}_{i,j}^0, i, j \in [s]$. In the following, we give several Claims about the elements of $\widetilde{\mathbf{A}}^{(2)}, \widetilde{\mathbf{A}}^{(1)}, \widetilde{\mathbf{B}}, \widetilde{\mathbf{C}}$ in the equation (6).

Claim 13. The elements $\widetilde{a}_{i,j}^{(2)}$ in $\widetilde{\mathbf{A}}^{(2)}$ can be represented quadratic combination of the set $\{x_1, \cdots, x_n\}$.

Proof. Since $a_{i,j}^{(2)}$ of $\mathbf{A}^{(2)}$ is a random quadratic polynomial in $\{\overline{x}_1, \overline{x}_2, \cdots, \overline{x}_n\}$. Assume $a_{i,j}^{(2)} = \sum_{t=1}^{n}\sum_{r=1}^{n} a_{i,j,t,r}^{(2)}\overline{x}_t\overline{x}_r, i, j \in [s]$.

By $\overline{\mathbf{x}} = \mathbf{L}_1\mathbf{x}$, we have $\overline{x}_t = \sum_{k=1}^{n} u_{t,k}x_k, t \in [n]$.

For $a_{i,j}^{(2)}$, replacing $\overline{x}_t$ with $\sum_{k=1}^{n} u_{t,k}x_k$, we obtain

$$\begin{aligned} \widetilde{a}_{i,j}^{(2)} &= \sum_{t=1}^{n}\sum_{r=1}^{n} a_{i,j,t,r}^{(2)}\overline{x}_t\overline{x}_r \\ &= \sum_{t=1}^{n}\sum_{r=1}^{n} a_{i,j,t,r}^{(2)}\sum_{\alpha=1}^{n} u_{t,\alpha}x_\alpha \sum_{\beta=1}^{n} u_{r,\beta}x_\beta \\ &= \sum_{\alpha=1}^{n}\sum_{\beta=1}^{n} \widetilde{a}_{i,j,\alpha,\beta}^{(2)}x_\alpha x_\beta, \end{aligned}$$

where $\widetilde{a}_{i,j,\alpha,\beta}^{(2)} = \sum_{t=1}^{n}\sum_{r=1}^{n} a_{i,j,t,r}^{(2)}u_{t,\alpha}u_{r,\beta}$

The result follows.

□

Similar to Claim 12, we can directly get the following results.

Claim 14. The elements $\widetilde{a}_{i,j}^{(1)}$ in $\widetilde{\mathbf{A}}^{(1)}$ can be represented linear combination of the set $\{x_1, \cdots, x_n\}$. Namely, $\widetilde{a}_{i,j}^{(1)} = \sum_{k=1}^{n} \widetilde{a}_{i,j,k}^{(1)}x_k$.

Claim 15. The elements $\widetilde{b}_{i,j}, \widetilde{c}_{i,j}$ in $\widetilde{\mathbf{B}}, \widetilde{\mathbf{C}}$ can be represented linear combination of the set $\{x_1, \cdots, x_n\}$. Namely, $\widetilde{b}_{i,j} = \sum_{k=1}^{n} \widetilde{b}_{i,j,k}x_k, \widetilde{c}_{i,j} = \sum_{k=1}^{n} \widetilde{c}_{i,j,k}x_k$.

The proof of Theorem 3 continue:
Now, we analyze the $(1,1)$ element of $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$ in the equation 6 as follows:

$$\begin{aligned}
(\widetilde{\mathbf{A}}\widetilde{\mathbf{B}})_{1,1} &= (\widetilde{\mathbf{A}}^{(2)}\widetilde{\mathbf{B}})_{1,1} + (\widetilde{\mathbf{A}}^{(1)}\widetilde{\mathbf{B}})_{1,1} + (\widetilde{\mathbf{A}}^{(0)}\widetilde{\mathbf{B}})_{1,1} \\
(\widetilde{\mathbf{A}}^{(2)}\widetilde{\mathbf{B}})_{1,1} &= \sum_{\theta=1}^{s} \widetilde{a}_{1,\theta}^{(2)}\widetilde{b}_{\theta,1} \\
&= \sum_{\theta=1}^{s} (\sum_{\alpha=1}^{n} \sum_{\beta=1}^{n} \widetilde{a}_{1,\theta,\alpha,\beta}^{(2)} x_\alpha x_\beta)(\sum_{k=1}^{n} \widetilde{b}_{\theta,1,k} x_k) \\
(\widetilde{\mathbf{A}}^{(1)}\widetilde{\mathbf{B}})_{1,1} &= \sum_{\theta=1}^{s} \widetilde{a}_{1,\theta}^{(1)}\widetilde{b}_{\theta,1} \\
&= \sum_{\theta=1}^{s} (\sum_{k=1}^{n} \widetilde{a}_{1,\theta,\alpha}^{(1)} x_\alpha)(\sum_{k=1}^{n} \widetilde{b}_{\theta,1,k} x_k) \\
(\widetilde{\mathbf{A}}^{(0)}\widetilde{\mathbf{B}})_{1,1} &= \sum_{\theta=1}^{s} \widetilde{a}_{1,\theta}^{(0)}\widetilde{b}_{\theta,1} \\
&= \sum_{\theta=1}^{s} \widetilde{a}_{1,\theta}^{(0)} \sum_{k=1}^{n} \widetilde{b}_{\theta,1,k} x_k
\end{aligned}$$

It is easy to verify there exist sn^3 different quadratic terms $\widetilde{a}_{1,\theta,\alpha,\beta}^{(2)}\widetilde{b}_{\theta,1,k}$ in $(\widetilde{\mathbf{A}}^{(2)}\widetilde{\mathbf{B}})_{1,1}$, sn^2 different quadratic terms $\widetilde{a}_{1,\theta,\alpha}^{(1)}\widetilde{b}_{\theta,1,k}$ in $(\widetilde{\mathbf{A}}^{(1)}\widetilde{\mathbf{B}})_{1,1}$, and sn different quadratic terms $\widetilde{a}_{1,\theta}^{(0)}\widetilde{b}_{\theta,1,k}$ in $(\widetilde{\mathbf{A}}^{(0)}\widetilde{\mathbf{B}})_{1,1}$. Namely, there are $s(n^3+n^2+n)$ different quadratic terms in $(\widetilde{\mathbf{A}}\widetilde{\mathbf{B}})_{1,1}$. So, there are $sn(n^3+n^2+n)$ different quadratic terms in $\widetilde{\mathbf{A}}\widetilde{\mathbf{B}}$.

Similarly, there are also $sn(n^3+n^2+n)$ different quadratic terms in $\widetilde{\mathbf{A}}\widetilde{\mathbf{C}}$.

Now, we can construct a system of linear equations with $2sn(n^3+n^2+n)+m^2$ unknown variables from the public key of the cubic ABC scheme by applying linearization methods, and solve an equivalent private key by using Algorithm 1 in Claim 8.

Furthermore, solving an equivalent private key takes time at most $(2sn(n^3+n^2+n)+m^2)^3 \log q = O(s^3n^{12}\log q)$.

This completes the proof of Theorem 3.

□

6 Conclusions

In this paper, using linearization method, we have proposed a polynomial time algorithm for ABC proposed by Tao et al. in [11], which directly solves an equivalent private key from the public key of ABC. Furthermore, our attack method can also be applied to the variants in [12, 13] since the variants proposed by Tao et al. and Ding et al. preserve the same algebraic structure as the ABC scheme [11]. Therefore, the ABC cryptosystem [11] and its variants [12, 13] are insecure.

References

1. P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal Computing 1997, 26(5), pp. 1484-1509.

2. R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 1978, 21(2), pp. 120-126.
3. T. Elgamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, CRYPTO 1984, LNCS 196, pp. 10-18.
4. V. S. Miller. Use of elliptic curves in cryptography. CRYPTO 1985, LNCS 218, pp. 417-426.
5. J A Buchmann, D Butin. Post-Quantum Cryptography: State of the Art. The New Codebreakers, LNCS 9100, 2016, pp.88-108.
6. M.R. Garey, D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company, New York (1979).
7. T. Matsumoto, H. Imai, Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption, EUROCRYPT 1988, LNCS 330, pp. 419-453.
8. J. Patarin, Cryptanalysis of the Matsumoto and Imai public Key Scheme of Eurocrypt'88, CRYPTO 1995, LNCS 963, pp. 248-261.
9. J. Patarin, Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP), EUROCRYPT 1996, LNCS 1070, pp. 38-48.
10. A. Kipnis, A. Shamir, Cryptanalysis of the HFE public key cryptosystem, CRYPTO 1999, LNCS 1666, pp. 19-30.
11. C. Tao, A. Diene, S. Tang, J. Ding, Simple matrix scheme for encryption, PQCrypto 2013, LNCS 7932 (2013), pp. 231-242.
12. C. Tao, H. Xiang, A. Petzoldt, J. Ding, Simple Matrix - a multivariate public key cryptosystem (MPKC) for encryption, Finite Fields and Their Applications 35 (2015), pp. 352-368.
13. J. Ding, A. Petzoldt, L.C. Wang, The cubic simple matrix encryption scheme, PQCrypto 2014, LNCS 8772 (2014), pp. 76-87.
14. A. Petzoldt, J. Ding, L.C. Wang, Eliminating decryption failures from the simple matrix encryption scheme, http://eprint.iacr.org/2016/010, 2016.
15. Y. Hashimoto, A note on tensor simple matrix encryption scheme, http://eprint.iacr.org/2016/065.
16. Z. Peng, S. Tang, J. Chen, C. Wu, and X. Zhang, Fast Implementation of Simple Matrix Encryption Scheme on Modern x64 CPU, ISPEC 2016, LNCS 10060, pp. 151-166, 2016.
17. D. Moody, R. Perlner, and D. Smith-Tone, An Asymptotically Optimal Structural Attack on the ABC Multivariate Encryption Scheme, PQCrypto 2014, LNCS 8772 (2014), pp. 180-196. http://eprint.iacr.org/2014/399
18. D. Moody, R. Perlner, and D. Smith-Tone, Improved Attacks for Characteristic-2 Parameters of the Cubic ABC Simple Matrix Encryption Scheme, http://eprint.iacr.org/2017/199
19. A. Kipnis, J. Patarin, L. Goubin, Unbalanced Oil and Vinegar schemes, EUROCRYPT 1999, LNCS 1592, pp. 206-222.