Cryptanalysis of Simple Matrix Scheme for Encryption

Chunsheng Gu

School of Computer Engineering, Jaingsu 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 equation attack, we propose a polynomial time algorithm, which directly recovers 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 original 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 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 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. MPKC is based on a system of multivariate polynomials over a finite field that is an NP-hard problem. However, this does not mean that a public key scheme based on multivariate polynomial is secure. Recently, Tao et al. [1] 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 [2] 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. Recently, Tao, Xiang, Petzoldt, and Ding [3] generalized the ABC scheme by using non-square matrices, instead of square matrices. To eliminate the decryption failures from ABC, Petzoldt, Ding, and Wang [4] described a new version of ABC, which uses tensor product of matrices. However, Hashimoto [5] showed the security of this variant is much weaker than that of the origin ABC scheme.

In order to analyze the security of ABC and its variants, Moody, Perlner, and Smith-Tone [7] 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 [3], 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 above attack algorithm needs exponential time. Thus, the attack based on subspace differential invariants [7] did not completely break the ABC and its variants.

Our main contribution is to prove that the ABC cryptosystem [1] and its variants [2, 3] 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 use with linearization techniques. Then using linearization equation technique, we present a polynomial time algorithm (i.e. $O(s^3 n^1 2 \log q)$ time) for ABC that solves an equivalent private 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 [1, 3], but only the cubic linearization equations. That is, we can use a new linearization method to find an equivalent private key from the public key. Furthermore, the variants of ABC in [2, 3] have the same algebraic structure as the original ABC scheme, consequently the above attack method can also generalize to these variants.

Organization. Section 2 describes the ABC cryptosystem. Section 3 analyzes the security of ABC. Section 4 describes the security of the variants of ABC. Section 5 draws conclusion.

2 ABC Cryptosystem

In this section, we briefly describe the ABC cryptosystem. For simplicity, we use the same notations in [1].

We 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 $m = 2n$. For a given integer s, let $\mathbb{F}^s$ denote the set of all s-tuples of elements of $\mathbb{F}$. We denote the plaintext by $(x_1, x_2, \cdots, x_n) \in \mathbb{F}^n$ and the ciphertext by $(y_1, y_2, \cdots, y_m) \in \mathbb{F}^m$. 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,

$$\mathcal{L}_1(x) = L_1 x, \mathcal{L}_2(y) = L_2 y,$$

where $L_1 \in \mathbb{F}^{n \times n}, L_2 \in \mathbb{F}^{m \times m}$, $x = (x_1, x_2, \cdots, x_n)^T$ and $y = (y_1, y_2, \cdots, y_m)^T$.

Key Generation:

(1) Given the set $\{x_1, \cdots, x_n\}$, set

$$A = \begin{pmatrix} x_1 & x_2 & \cdots & x_s \\ x_{s+1} & x_{s+2} & \cdots & x_{2s} \\ \vdots & \vdots & \cdots & \vdots \\ x_{(s-1)s+1} & x_{(s-1)s+2} & \cdots & x_{s^2} \end{pmatrix},$$

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

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

where $b_{i,j}, c_{i,j}, i, j \in [s]$ are randomly linear combinations of $\{x_1, \cdots, x_n\}$.

(2) Set $E_1 = A \cdot B$ and $E_2 = A \cdot C$.

(3) Define the central map $\mathcal{F}$ as follows:

$$\mathcal{F}(x_1, \cdots, x_n) = (f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n)),$$

where $f_{(i-1)s+j}$ is the (i, j) element in E_1, $f_{s^2+(i-1)s+j}$ is the (i, j) element in E_2.

(4) Choose two invertible linear maps $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$ and $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$. Let $L_1 \in \mathbb{F}^{n\times n}$ and $L_2 \in \mathbb{F}^{m\times m}$ are respectively linear transformation matrices corresponding to $\mathcal{L}_1, \mathcal{L}_2$.

(5) Define the maps $\overline{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1 = (\overline{f}_1(x_1, \cdots, x_n), \cdots, \overline{f}_m(x_1, \cdots, x_n))$.

(6) Output the public key $pk = \{\overline{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1\}$ and the private key $sk = \{L_1, L_2, B, C\}$.

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

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

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

(1) Compute $\overline{y} = (\overline{y}_1, \overline{y}_2, \cdots, \overline{y}_m) = \mathcal{L}_2^{-1}(y) = (L_2^{-1}y^T)^T$ and set

$$E_1 = \begin{pmatrix} \overline{y}_1 & \overline{y}_2 & \cdots & \overline{y}_s \\ \overline{y}_{s+1} & \overline{y}_{s+2} & \cdots & \overline{y}_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{(s-1)s+1} & \overline{y}_{(s-1)s+2} & \cdots & \overline{y}_{s^2} \end{pmatrix} \in \mathbb{F}^{s\times s},$$

$$E_2 = \begin{pmatrix} \overline{y}_{s^2+1} & \overline{y}_{s^2+2} & \cdots & \overline{y}_{s^2+s} \\ \overline{y}_{s^2+s+1} & \overline{y}_{s^2+s+2} & \cdots & \overline{y}_{s^2+2s} \\ \vdots & \vdots & \vdots & \vdots \\ \overline{y}_{s^2+(s-1)s+1} & \overline{y}_{s^2+(s-1)s+2} & \cdots & \overline{y}_{2s^2} \end{pmatrix} \in \mathbb{F}^{s\times s}.$$

(2) By $E_1 = AB$ and $E_2 = AC$, we consider the following cases:

– If E_1 is invertible, then $BE_1^{-1}E_2 = C$. We get n linear equations with n unknowns $x_1, \cdots, x_n$.

– If E_2 is invertible, but E_1 is not invertible, then $CE_2^{-1}E_1 = B$. We also obtain n linear equations with n unknowns $x_1, \cdots, x_n$.

– If E_1, E_2 are not invertible, but A is invertible, then $A^{-1}E_1 = B$ and $A^{-1}E_2 = C$. We consider the elements of 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 x_i.

– If A is a singular matrix and the rank of A is r, then we let

$$\begin{aligned} W &= \begin{pmatrix} W_{1,1} & W_{1,2} \\ W_{2,1} & W_{2,2} \end{pmatrix}, \\ A &= \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix}, \\ B &= \begin{pmatrix} B_{1,1} & B_{1,2} \\ B_{2,1} & B_{2,2} \end{pmatrix}, \\ C &= \begin{pmatrix} C_{1,1} & C_{1,2} \\ C_{2,1} & C_{2,2} \end{pmatrix}, \\ E_1 &= \begin{pmatrix} E1_{1,1} & E1_{1,2} \\ E1_{2,1} & E1_{2,2} \end{pmatrix}, \\ E_2 &= \begin{pmatrix} E2_{1,1} & E2_{1,2} \\ E2_{2,1} & E2_{2,2} \end{pmatrix}, \end{aligned}$$

where $W_{1,1}, A_{1,1}, B_{1,1}, C_{1,1}, E1_{1,1}, E2_{1,1}$ are $r \times r$ matrices. Therefore, we get $2sr$ linear equations in $sr + n$ unknowns

$$\begin{aligned} W_{1,1}E1_{1,1} + W_{1,2}E1_{2,1} &= B_{1,1}, \\ W_{1,1}E1_{1,2} + W_{1,2}E1_{2,2} &= B_{1,2}, \\ W_{1,1}E2_{1,1} + W_{1,2}E2_{2,1} &= C_{1,1}, \\ W_{1,1}E2_{1,2} + W_{1,2}E2_{2,2} &= C_{1,2}. \end{aligned}$$

Now, we eliminate sr elements in $W_{1,1}W_{1,2}$ to obtain sr linear equations with the variables $x_1, \cdots, x_n$. Using Gaussian elimination, we can write some variables (e.g. z) as linear combinations of other unknown variables (e.g. $n-z$) and substitute them into the central map equations. Then, we solve this new system of equations of degree two in $n - z$ unknowns using linearization technique. Consequently, we can find a solution $\overline{x}_1, \cdots, \overline{x}_n$. However, we maybe obtain more than one solution, but the probability of this case is very small.

(3) Compute the plaintext $(x_1, x_2, \cdots, x_n) = \mathcal{L}_1^{-1}(\overline{x}_1, \cdots, \overline{x}_n)$.

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,

$$\begin{aligned}
&(\mathcal{L}_2^{-1} \circ \overline{\mathcal{F}})(x_1, \cdots, x_n)\\
&= (L_2^{-1}(\overline{f}_1(x_1, \cdots, x_n), \cdots, \overline{f}_m(x_1, \cdots, x_n))^T)^T\\
&= (L_2^{-1}(y_1, \cdots, y_m)^T)^T
\end{aligned}$$

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

$$\begin{aligned}
&(\mathcal{F} \circ \mathcal{L}_1)(x_1, \cdots, x_n)\\
&= \mathcal{F}(\mathcal{L}_1(x_1, \cdots, x_n))\\
&= \mathcal{F}(L_1(x_1, \cdots, x_n)^T)\\
&= \mathcal{F}(\overline{x}_1, \cdots, \overline{x}_n)\\
&= (f_1(\overline{x}_1, \cdots, \overline{x}_n), \cdots, f_m(\overline{x}_1, \cdots, \overline{x}_n))
\end{aligned}$$

Again by $E_1 = A \cdot B$ and $E_2 = A \cdot C$ and the definition of the central map $\mathcal{F}$, we can get $\overline{E}_1 = \overline{A} \cdot \overline{B}$ and $\overline{E}_2 = \overline{A} \cdot \overline{C}$. That is, $\overline{E}_1, \overline{E}_2, \overline{A}, \overline{B}, \overline{C}$ are defined in the variables $\{\overline{x}_1, \cdots, \overline{x}_n\}$.

Claim 1. Suppose $L_2^{-1} = \begin{pmatrix} v_{1,1} & \cdots & v_{1,m} \\ \vdots & \vdots & \vdots \\ v_{m,1} & \cdots & v_{m,m} \end{pmatrix}$, then

$$\overline{y}^T = \mathcal{L}_2^{-1}(y_1, \cdots, y_m) = L_2^{-1}(y_1, \cdots, y_m)^T = (\sum_{j=1}^m v_{1,j}y_j, \cdots, \sum_{j=1}^m v_{m,j}y_j)^T.$$

Claim 2. Suppose $L_1 = \begin{pmatrix} u_{1,1} & \cdots & u_{1,n} \\ \vdots & \vdots & \vdots \\ u_{n,1} & \cdots & u_{n,n} \end{pmatrix}$, then

$$\overline{x}^T = \mathcal{L}_1(x_1, \cdots, x_n) = L_1(x_1, \cdots, x_n)^T = (\sum_{j=1}^n u_{1,j}x_j, \cdots, \sum_{j=1}^n u_{n,j}x_j)^T.$$

Since $b_{i,j}, c_{i,j}, i, j \in [s]$ are randomly linear combinations of $\{x_1, \cdots, x_n\}$, without loss of generality, we assume $b_{i,j} = \sum_{k=1}^n b_{i,j,k}x_k$ and $c_{i,j} = \sum_{k=1}^n c_{i,j,k}x_k$

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

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

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

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

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

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

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

Claim 4. Suppose $\overline{A}, \overline{B}, \overline{C}, \overline{E}_1, \overline{E}_2$ 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 $\overline{E}_1 = \overline{A} \cdot \overline{B}$ and $\overline{E}_2 = \overline{A} \cdot \overline{C}$, 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, we substitute $\overline{x}_1, \cdots, \overline{x}_n$ and $\overline{y}_1, \cdots, \overline{y}_m$ into the system of quadratic equations to get the result.

Claim 6. Given $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$ of the system of equations in Claim 5, then the system of equations becomes cubic equations in $3n^2 + m^2$ unknowns $\{b_{i,j,k}, c_{i,j,k}, i, j \in [s], k \in [n]\}$, $\{u_{i,j}, i, j \in [n]\}$, and $\{v_{i,j}, i, j \in [m]\}$.

Claim 7. Given $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$ of the system of equations in Claim 6, then the system of the above equations becomes a system of linear equations with $2sn^4 + m^2$ unknowns generated by using linearization 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 $\{v_{i,j}, i, j \in [m]\}$.

Proof. On the one hand, by $\overline{E}_1 = \overline{A} \cdot \overline{B}$ and $\overline{E}_2 = \overline{A} \cdot \overline{C}$ only the right side of the equations produces quadratic expressions on variable $\overline{x}_1, \cdots, \overline{x}_n$. Now, we count the number of terms in the $(1,1)$ element of $\overline{A} \cdot \overline{B}$ as follows:

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

It is not difficult to verify that there are $s \times n \times (n^2) = sn^3$ different terms in the $(1,1)$ element of $\overline{A} \cdot \overline{B}$. So, the total number of different terms in $\overline{A} \cdot \overline{B}$ are sn^4. Furthermore, from the perspective of unknown variables of B, C, L_1, any cubic term in these elements must be of the form $b_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$ or $c_{i,j,k}u_{i_1,j_1}u_{i_2,j_2}$. Consequently, there are at most $2 \times sn^4 = 2sn^4$ cubic terms. On the other hand, the left side of the equations have the linear terms with m^2 unknowns in L_2^{-1}. Consequently, the total number of unknowns generated by linearization method is $2sn^4 + m^2$.

Proof of theorem 1 continues. By Claim 7, we take a sequence of different plaintext/ciphertext pairs to consist of a system of $2sn^4 + m^2$ linear equations. Then we solve this system to find q solutions. Except 0, the remaining $q - 1$ solutions are feasible and equivalent.

Complexity of time. First, we can generate a system of linear equations with $2sn^4 + m^2$ unknown variables from the public key in time $O((2sn^4 + m^2)\log q) = O(sn^4 \log q)$. Then, using Gaussian elimination, we can solve this system of linear equations in time $O((sn^4 + m^2)^3 \log q) = O(s^3n^{12} \log q)$. Thus, our algorithm runs in polynomial time. □

4 Improvements and Cryptanalysis

To improve security and efficiency of ABC, Tao et al. and Ding et al. respectively proposed variants of ABC in [2, 3]. Since these improved schemes preserve the same algebraic structure as the origin ABC scheme [1], as a result, the attack method described above can also be applied to variants. Thus, the variants of ABC are also insecure. In the following, we only describe the variant in [3].

4.1 Improvement of ABC

We 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 the set $\{x_1, \cdots, x_n\}$, we take

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

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

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

where $a_{i,j}$ in A are randomly chosen from the set $\{x_1, \cdots, x_n\}$, and $b_{i,j}$ in B, $c_{i,j}$ in C are randomly linear combinations of $x_1, \cdots, x_n$.

(2) Set $E_1 = A \cdot B$ and $E_2 = A \cdot C$.

(3) Generate the central map $\mathcal{F}$, which consists of the $m = s \cdot (u + v)$ components of the matrices E_1 and E_2.

(4) Choose two invertible linear maps $\mathcal{L}_2 : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{L}_1 : \mathbb{F}^n \to \mathbb{F}^n$.

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

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

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

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

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

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

(2) Find a vector $x \in \mathbb{F}^n$ such that $\mathcal{F}(x) = \overline{y}$. Assume $\overline{A} = A(x)$.

– If the rank of $\overline{A}$ is r, then there exists an $r \times s$ matrix W such that $W \cdot \overline{A} = I$, where I is the $r \times r$ identity matrix. By $\overline{E}_1 = \overline{A} \cdot B$ and $\overline{E}_2 = \overline{A} \cdot C$, we get $W \cdot \overline{E}_1 = B$ and $W \cdot \overline{E}_2 = C$. We consider the elements of W as new

variables and generate $r(u+v)$ linear equations in $rs+n$ unknowns. Now, we can eliminate rs elements of W from these equations. Therefore, we obtain $r \cdot (u+v-s)$ linear equations in the variables $x_1, x_2, \cdots, x_n$.
Using Gaussian elimination, we can write some variables (e.g. z) as linear combinations of other unknown variables (e.g. $n-z$) and substitute them into the central map equations. Then, we solve this new system of equations of degree two in $n-z$ unknowns using linearization technique. Consequently, we can find a solution $\overline{x}_1, \cdots, \overline{x}_n$.

- In the case of $rank(\overline{A}) < r$, decryption remains an open problem.

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

4.2 Cryptanalysis

In the improved construction, the rectangular matrices A, B, C are used instead of the square matrix in the origin ABC. All other constructions remains the same as ABC. From the above cryptanalysis of ABC, our attack does not depend on the matrix shape. Therefore, our attack can directly generalize to the improvement of ABC.

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

Proof. The proof is completely similar to that of Theorem 1.

5 Conclusion

In this paper, using linearization equation method, we have proposed a polynomial time algorithm for ABC proposed by Tao et al. in [1], which directly recovers an equivalent private key from the public key of ABC. Furthermore, our attack method can also be applied to the variants in [2, 3] since the variants proposed by Tao et al. and Ding et al. preserve the same algebraic structure as the origin ABC scheme [1]. Therefore, the ABC cryptosystem [1] and its variants [2, 3] are insecure.

References

1. C. Tao, A. Diene, S. Tang, J. Ding, Simple matrix scheme for encryption, PQCrypto 2013, LNCS 7932 (2013), pp. 231-242.
2. J. Ding, A. Petzoldt, L.C. Wang, The cubic simple matrix encryption scheme, PQCrypto 2014, LNCS 8772 (2014), pp. 76-87.
3. 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.
4. A. Petzoldt, J. Ding, L.C. Wang, Eliminating decryption failures from the simple matrix encryption scheme, http://eprint.iacr.org/2016/010, 2016.
5. Y. Hashimoto, A note on tensor simple matrix encryption scheme, http://eprint.iacr.org/2016/065.

6. 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.
7. 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. 180C196. http://eprint.iacr.org/2014/399