doi:10.11835/j.issn.1000-582X.2017.07.006

密文明文长度比可变的多变量公钥加密方案

向　宏[a,b],李思遥[b],蔡　斌[a,b]
(重庆大学 a.信息物理社会可信服务计算教育部重点实验室;b.软件学院,重庆 400044)

摘　要:多变量公钥密码体系是一种能保证后量子通信安全的重要方法。现今,能投入到实际应用、高效且安全的多变量公钥签名方案有很多,加密方案却很少。2013 年后量子密码会议上,Tao 等人提出了简单矩阵加密方案。该方案在保证安全性的前提下,具有较高的效率,但该方案的密文明文长度比固定为 2。针对这一情况,对简单矩阵加密方案进行改进,提出 Cubic AB 加密方案。在该方案中,矩阵 **A** 的各元素由随机二次多项式构成;并选用一个扁长的矩阵来取代原方案中的 **B**、**C** 矩阵。使得该方案在能抵抗秩攻击的同时,密文明文长度比能灵活改变。并且随着安全性的提高,密文明文长度会相应减小,解密过程也随之加快。

关键词:公钥密码体系;量子计算;多变量公钥密码体系;加密方案
中图分类号:TP309　　**文献标志码**:A　　**文章编号**:1000-582X(2017)07-037-06

Multivariate public key cryptography scheme with changeable ratio of ciphertext length to plaintext length

XIANG Hong[a,b], *LI Siyao*[b], *CAI Bin*[a,b]
(a. Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education;
b. School of Software Engineering, Chongqing University, Chongqing 400044, P.R.China)

Abstract: Multivariate public key cryptosystem is an important method to guarantee the security of communication after quantum computer appears. There are lots of practical multivariate signature schemes, but only a few multivariate encryption schemes show up. The simple matrix encryption scheme proposed by Tao, et al. is an efficient and secure multivariate encryption scheme in PQCrypto2013. However, the ratio of length of cipher text to plain text is always 2. Cubic AB encryption scheme is a way to fix it. It uses a very wide matrix to replace square matrixes (***B*** and ***C***), and the elements of matrix ***A*** are random quadratic polynomials. With this method, the ratio of length of cipher text to plain text could be changed easily. Besides, rank attack cannot be used to attack this scheme. At the same time, the length of cipher text and plain text will be shorter, which could make the process of decryption faster.

Keywords: public key cryptography;quantum computer;multivariate public-key cryptosystem;encryption scheme

密码技术是保证现代通信安全的重要工具。目前,实际应用中广泛使用的密码方案主要有:RSA、DSA 以及 ECC。这些密码方案的理论基础几乎都是数论难题,如:大整数的因子分解问题、离散对数问题等。随

收稿日期:2017-02-10
基金项目:国家自然科学基金资助项目(61472054)和中央高校基本科研业务费资助项目(106112014CDJZR095501)。Supported by the National Natural Science Foundation of China(61472054);Funda mental Research Funds for the centralUniversities (106112014CDJZR095501).
作者简介:向宏(1964-),重庆大学教授,博士生导师,主要从事信息安全方向研究,(Tel)13594361541;(E-mail)xianghong@cqu.edu.cn。

着量子计算机的实现，这些方案将变得不再安全。在量子计算机上利用 Shor 算法[1]，可以在多项式时间内完成大整数分解和离散对数求解。因此，设计能够抵抗量子计算攻击的公钥密码方案，来取代这些传统的密码方案，显得尤为重要。

多变量公钥密码方案是一种业界公认的能抵抗量子计算攻击的备选方案，具有执行速度快，且仅需要模块化的计算资源的特性。可以将其应用到低功耗的设备中，如 RFID、IC 卡[2]、传感网络等[3-5]。现在已经有许多能应用于实际应用的多变量公钥签名方案[6-10]。但是，高效且安全的多变量公钥加密方案却很少。

在 2013 年的后量子密码会议上，Tao 等人提出了一种新的多变量公钥加密方案：简单矩阵加密方案(simple matrix scheme)[11]。该方案具有较高的效率，同时还能抵抗所有已知的针对多变量公钥密码方案的攻击算法。随后，Ding 与 Petzoldt 对该方案的安全性做了进一步加强，提出 3 次简单矩阵加密方案(cubic simple matrix scheme)[12]。之后，Tao 与 Xiang[13]、Petzoldt 与 Ding[14]对该方案的解密失败概率进行改进。除此之外，针对简单矩阵原始方案中密文明文长度比固定为 2 的情况，Petzoldt 提出了一种改进方案：ABCD 加密方案[14]，使得密文明文长度比不再固定为 2。但是，ABCD 方案的密文明文长度比值，可选范围很小，只有 2 个值。

针对 ABCD 加密方案提出进行改进，设计 Cubic AB 加密方案。利用 Cubic AB 加密方案，可增大密文明文长度比值可取范围。除此之外，Cubic AB 加密方案借鉴三次简单矩阵加密方案的思想，使用随机二次多项式构造公钥来提高安全性。使得 Cubic AB 加密方案除了能抵抗求解随机二次方程组的代数攻击，还能抵抗秩攻击。

1 简单矩阵加密方案

介绍多变量公钥密码体系的主要思想和简单矩阵加密方案。

1.1 多变量公钥密码体系

多变量公钥密码体系的核心部分在于构建了一组二次多项式

$$\begin{aligned} p^{(1)}(x_1,\dots,x_n)&=\sum_{i=1}^{n}\sum_{j=1}^{n}p_{ij}^{(1)}\cdot x_ix_j+\sum_{i=1}^{n}p_i^{(1)}\cdot x_i,\\ p^{(2)}(x_1,\dots,x_n)&=\sum_{i=1}^{n}\sum_{j=1}^{n}p_{ij}^{(2)}\cdot x_ix_j+\sum_{i=1}^{n}p_i^{(2)}\cdot x_i,\\ p^{(m)}(x_1,\dots,x_n)&=\sum_{i=1}^{n}\sum_{j=1}^{n}p_{ij}^{(m)}\cdot x_ix_j+\sum_{i=1}^{n}p_i^{(m)}\cdot x_i, \end{aligned}\tag{1}$$

该类密码方案的安全性依赖于 MQ(multivariate quadratic)问题。即：在公式(1)中的个 m 二次多项式 $p^{(1)}(x),\cdots,p^{(m)}(x)$ 中，找出一个 n 维向量 $\boldsymbol{X}(x_1,x_2,\cdots,x_n)$，使得 $p^{(1)}(x)=\cdots=p^{(m)}(x)=0$。而 MQ 问题的困难性已经被证明：当 $m\approx n$ 时，即便在有限域 GF(2)上，MQ 问题也是一个 NP 难题[15]。

通过 MQ 问题构建公钥密码方案，需要：1)找到一个很容易进行逆运算的二次映射 $\boldsymbol{F}:F^n\to F^n$。通常这个映射 $\boldsymbol{F}$ 也被称为中心映射。2)对外提供公钥时，中心映射需要被隐藏起来。因此将中心映射，与另外 2 个可逆线性仿射 $S:F^m\to F^m$ 和 $T:F^n\to F^n$ 复合。容易看出，通过这种方式构建的公钥密码系统，其安全性不仅只依赖 MQ 问题，还依赖于 EIP(extended isomorphism of polynomials)问题。3)最终对外提供的公钥为：$P=S\circ F\circ T:F^n\to F^m$。而私钥则包括：中心映射 $\boldsymbol{F}$，以及 2 个线性仿射 $\boldsymbol{S}$、$\boldsymbol{T}$。

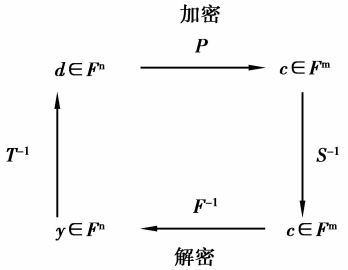

图 1 多变量加密方案标准加密解密流程

Fig.1 Encrgption and decryotion process of multivariate

多变量公钥加密方案的标准加密、解密过程如图 1 所示。

加密：对明文 $\boldsymbol{d}\in F^n$ 进行加密，只需要简单地用公钥，计算 $c=P(\boldsymbol{d})$，便得到密文 $c\in f^m$。

解密：对密文 $c\in f^m$ 进行解密，需要进行 3 次计算，即：$\boldsymbol{x}=\boldsymbol{S}^{-1}(c)$，$\boldsymbol{y}=\boldsymbol{F}^{-1}(x)$ 和 $\boldsymbol{d}=\boldsymbol{T}^{-1}(y)$。由此，得

到密文 c 对应的明文 $\boldsymbol{d}\in f^n$。

对于多变量公钥加密方案，通常有 $m>n$，因此通过解密过程得到的明文是唯一的。

1.2　简单矩阵加密方案

由 Tao 提出的简单矩阵加密方案的结构如下：

密钥生成：有参数 $s\in N$，且存在关系 $s^2=n$，$2n=m$。并定义 3 个维度为 $s\times s$ 的矩阵 $\boldsymbol{A}$，$\boldsymbol{B}$ 与 $\boldsymbol{C}$。形如

$$\boldsymbol{A}=\begin{pmatrix} x_1 & \cdots & x_s \\ \vdots & \ddots & \vdots \\ x_{(s-1)\cdot s+1} & \cdots & x_n \end{pmatrix},\boldsymbol{B}=\begin{pmatrix} b_1 & \cdots & b_s \\ \vdots & \ddots & \vdots \\ b_{(s-1)\cdot s+1} & \cdots & b_n \end{pmatrix},$$

$$\boldsymbol{C}=\begin{pmatrix} c_1 & \cdots & c_s \\ \vdots & \ddots & \vdots \\ c_{(s-1)\cdot s+1} & \cdots & c_n \end{pmatrix},$$

其中，矩阵 $\boldsymbol{B}$、$\boldsymbol{C}$ 的各元素是变量 $x_1,x_2,\cdots,x_n$ 的随机线性组合。

由矩阵 $\boldsymbol{A}$，$\boldsymbol{B}$ 与 $\boldsymbol{C}$ 计算出矩阵 $\boldsymbol{E}_1=\boldsymbol{A}\cdot\boldsymbol{B}$、$\boldsymbol{E}_2=\boldsymbol{A}\cdot\boldsymbol{C}$。容易看出，矩阵 $\boldsymbol{E}_1$、$\boldsymbol{E}_2$ 的维度也为 $s\times s$。其元素便是关于变量 $x_1,x_2,\cdots,x_n$ 的二次多项式。由这 m（即：$2\cdot s^2$）个二次多项式构成了中心映射 $\boldsymbol{F}:F^n\to F^m$。

然后，随机构造 2 个可逆线性仿射 $\boldsymbol{S}:F^m\to F^m$ 和 $\boldsymbol{T}:F^n\to F^n$，与中心映射 F 复合，得到公钥 $P=\boldsymbol{S}\circ F\circ\boldsymbol{T}:F^n\to F^m$。而私钥则包含 $\boldsymbol{S}$，$\boldsymbol{T}$ 与 $\boldsymbol{F}$。

加密：与标准过程一样，只需要对明文 $d\in F^n$，进行一次 $c=P(d)$ 运算即可。

解密：要对密文 $c\in F^m$ 进行解密，要经过 3 个步骤进行：

1）计算 $\boldsymbol{x}=\boldsymbol{S}^{-1}(c)$，得到一个 m 维向量 $\boldsymbol{x}\in F^m$。由简单矩阵加密方案的构造过程得知，将向量 $\boldsymbol{x}$ 转换为矩阵形式，便可得到矩阵 $\boldsymbol{E}_1$ 和 $\boldsymbol{E}_2$，形如

$$\boldsymbol{E}_1=\begin{pmatrix} x_1 & \cdots & x_s \\ \vdots & \ddots & \vdots \\ x_{(s-1)\cdot s+1} & \cdots & x_n \end{pmatrix},$$

$$\boldsymbol{E}_2=\begin{pmatrix} x_{n+1} & \cdots & x_{n+s} \\ \vdots & \ddots & \vdots \\ x_{n+(s-1)\cdot s+1} & \cdots & x_m \end{pmatrix}。$$

2）参考标准过程，需要求出 n 维向量 $\boldsymbol{y}\in F^n$，使得 $\boldsymbol{F}(y)=x$。而根据具体情况的不同，有 3 种不同的方式来求出向量 $\boldsymbol{y}$。

a.若矩阵 $\boldsymbol{E}_1$ 可逆，则由 $\boldsymbol{B}\cdot\boldsymbol{E}_1^{-1}\cdot\boldsymbol{E}_2=\boldsymbol{C}$ 得到 n 个关于 $y_1,y_2,\cdots,y_n$ 的线性方程。由此，便可求出向量 $\boldsymbol{y}$。

b.若矩阵 $\boldsymbol{E}_1$ 不可逆，但矩阵 $\boldsymbol{E}_2$ 可逆。类似的，有 $\boldsymbol{C}\cdot\boldsymbol{E}_2^{-1}\cdot\boldsymbol{E}_1=\boldsymbol{B}$。也可得到 n 个关于 $y_1,y_2,\cdots,y_n$ 的线性方程。由此，求出向量 $\boldsymbol{y}$。

c.若矩阵 $\boldsymbol{E}_1$、$\boldsymbol{E}_2$ 均不可逆，但矩阵 $\boldsymbol{A}$ 可逆。将矩阵 $\boldsymbol{A}^{-1}$ 的元素视为新的未知变量。同时，有 $\boldsymbol{A}^{-1}\boldsymbol{E}_1=\boldsymbol{B}$，$\boldsymbol{A}^{-1}\boldsymbol{E}_2=\boldsymbol{C}$。由此，可以得到 m 个关于 $y_1,y_2,\cdots,y_n$ 与 $\boldsymbol{A}^{-1}$ 的各元素的线性方程。

d.若矩阵 $\boldsymbol{E}_1$、$\boldsymbol{E}_2$ 和 $\boldsymbol{A}$ 均不可逆，则解密失败。

3）最后，通过线性仿射 $\boldsymbol{T}$，计算出明文 $\boldsymbol{d}=\boldsymbol{T}^{-1}(\boldsymbol{y})$。

解密失败的概率决定于矩阵 $\boldsymbol{A}$ 是否可逆，其概率又取决于有限域的元素个数 q。所以解密失败的概率大约为 $1/q$。

在进行第二步时，可能会求出多个满足条件的向量 $\boldsymbol{y}$。只需要将求得的结果代入中心映射，判断是否与原密文相同即可。

2　Cubic AB 加密方案

2.1　方案结构

在所有的简单矩阵加密方案及其变种方案中，其密文明文长度比都为 2。即使是 ABCD 加密方案，其密文明文长度比值，也只能是 1.5 和 1.33 其中之一，并不能更灵活地改变密文明文长度之比。笔者提出 Cubic

AB 加密方案，通过使用一个扁长的矩阵 $\boldsymbol{B}$ 来取代简单矩阵加密方案中的矩阵 $\boldsymbol{B}$ 和 $\boldsymbol{C}$。并用变量 $x_1,x_2,\cdots,x_n$ 的二次多项式来充当矩阵 $\boldsymbol{A}$ 的各元素，以此提高方案的安全性。其结构如下：

密钥生成：参数 $s,u\in N$，且 $s<u$。令 $m=s\cdot u$，$n=m-s^2=s\cdot(u-s)$。由此，定义一个维度为 $s\times s$ 的矩阵 $\boldsymbol{A}$，以及维度为 $s\times u$ 的矩阵 $\boldsymbol{B}$，形如

$$\boldsymbol{A}=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1s}\\a_{21}&a_{22}&\cdots&a_{2s}\\\vdots&\vdots&\ddots&\vdots\\a_{s1}&a_{s2}&\cdots&a_{ss}\end{pmatrix},$$

$$\boldsymbol{B}=\begin{pmatrix}b_{11}&b_{12}&\cdots&b_{1s}&\cdots&b_{1u}\\b_{21}&b_{22}&\cdots&b_{2s}&\cdots&b_{2u}\\\vdots&\vdots&&\vdots&&\vdots\\b_{s1}&b_{s2}&\cdots&b_{ss}&\cdots&b_{su}\end{pmatrix}。$$

与简单矩阵加密方案不同的是，矩阵 $\boldsymbol{A}$ 的各元素是变量 $x_1,x_2,\cdots,x_n$ 的随机二次多项式；而矩阵 $\boldsymbol{B}$ 的各元素依然是变量 $x_1,x_2,\cdots,x_n$ 的随机线性组合。

由矩阵 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 计算出矩阵 $\boldsymbol{E}=\boldsymbol{A}\cdot\boldsymbol{B}$。容易看出，矩阵 $\boldsymbol{E}$ 的维度也为 $s\times u$，其元素便是关于变量 $x_1,x_2,\cdots,x_n$ 的 3 次多项式。这 m（即：$s\cdot u$）个 3 次多项式便构成了中心映射 $\boldsymbol{F}:F^n\to F^m$。

然后，将中心映射与 2 个随机生成的可逆线性仿射 $S:F^m\to F^m$、$T:F^n\to F^n$，进行复合，得到公钥 $P=S\circ F\circ\boldsymbol{T}:F^n\to F^m$。私钥则包含 $\boldsymbol{S}$，$\boldsymbol{T}$ 与 $\boldsymbol{F}$。

加密：用公钥 P 对明文 $d\in F^n$ 进行 $c=P(d)$ 计算，即可得到密文 $c\in F^m$。

解密：对密文进行解密需要经过 3 个步骤：

1）计算 $\boldsymbol{x}=\boldsymbol{S}^{-1}(c)$，得到一个 m 维向量 $\boldsymbol{x}\in F^m$。并用向量 $\boldsymbol{x}$ 的分量作为矩阵 $\boldsymbol{E}$ 的元素，即

$$\boldsymbol{E}=\begin{pmatrix}x_1&x_2&\cdots&x_u\\x_{u+1}&x_{u+2}&\cdots&x_{2\cdot u}\\\vdots&\vdots&\ddots&\vdots\\x_{(s-1)\cdot u+1}&x_{(s-1)\cdot u+2}&\cdots&x_{s\cdot u}\end{pmatrix}。$$

2）需要对向量 $\boldsymbol{x}$ 进行中心映射 $\boldsymbol{F}$ 的逆运算，得到 n 维向量 $\boldsymbol{y}\in F^n$。与简单矩阵加密方案不同，此处只讨论 2 种情况：

a.若矩阵 $\boldsymbol{A}$ 可逆，将矩阵 $\boldsymbol{A}^{-1}$ 的各元素视为新的未知量。同时，需要对向量 $\boldsymbol{y}$ 进行求解。因此，一共有 s^2+n、即 m 个未知量。而矩阵 $\boldsymbol{A}$ 可逆，还存在关系 $\boldsymbol{A}^{-1}\cdot\boldsymbol{E}=\boldsymbol{B}$。由此，可得到 m 个关于 $y_1,y_2,\cdots,y_n$ 与 $\boldsymbol{A}^{-1}$ 各元素的线性方程。便可使用高斯消元法对方程组进行求解。

b.若矩阵 $\boldsymbol{A}$ 不可逆，则解密失败。

3）再由 $\boldsymbol{d}=\boldsymbol{T}^{-1}(y)$，计算出明文。

与简单矩阵加密方案类似，在解密过程执行第二步时，有可能求出多个满足条件的向量 $\boldsymbol{y}$。同样，也只需要将求出的向量 $\boldsymbol{y}$，代入中心映射 F，确保计算出的结果与向量 $\boldsymbol{x}$ 相同。

从解密过程的第二步中，可以看到，由于需要为 $\boldsymbol{A}^{-1}$ 矩阵保留 s^2 个未知量，以保证方程组能够求解。因此，需要将明文的长度设计为：$n=m-s^2$。故，密文明文长度之比为

$$\alpha=\frac{m}{n}=\frac{s\cdot u}{s\cdot u-s^2}=1+\frac{s}{u-s}。\tag{2}$$

容易看出，比值通过参数 s、u 控制，使得取值范围大大增加，较于 ABCD 加密方案，粒度更细。

2.2 安全性分析

2.2.1 秩攻击

秩攻击是针对多变量密码方案的一种主要攻击方法。秩攻击主要分为 2 种：小秩攻击（minrank attack）、高秩攻击（highrank attack）。针对不同的多变量密码方案，利用小秩攻击和高秩攻击，攻击者可以还原出私钥中的可逆线性仿射 $\boldsymbol{T}$ 和 $\boldsymbol{S}$。

对于 Cubic AB 加密方案而言，其矩阵 $\boldsymbol{A}$ 的各元素是变量 $x_1,x_2,\cdots,x_n$ 的随机二次多项式。所以，秩都

接近 n，并且变量 $x_1,x_2,\cdots,x_n$ 在中心映射中出现的次数基本相同。因此，针对 Cubic AB 加密方案，并不能利用秩攻击来进行攻击。

2.2.2　直接攻击

直接攻击即，直接对公钥所构成的非线性方程组 $P(\boldsymbol{d})=c$ 进行求解，最终求得明文 $\boldsymbol{d}$。

对于 Cubic AB 加密方案而言，其矩阵 $\boldsymbol{A}$ 的元素是关于变量 $x_1,x_2,\cdots,x_n$ 的随机二次多项式；矩阵 $\boldsymbol{B}$ 的元素是关于变量 $x_1,x_2,\cdots,x_n$ 的随机线性组合。

即便简化方案，攻击者只需要对中心映射进行求解，即：$\boldsymbol{F}(\boldsymbol{x})=\boldsymbol{y}$。由于中心映射是通过 $\boldsymbol{A}\cdot\boldsymbol{B}=\boldsymbol{E}$ 而来。所以，即便攻击者还被告知了矩阵 $\boldsymbol{B}$ 的值，依然有 $\boldsymbol{A}=\boldsymbol{E}\cdot\boldsymbol{B}^{-1}$（矩阵 $\boldsymbol{B}$ 的广义逆矩阵）。此时，攻击者还是需要求解一个二次方程组。并且，这个方程组的系数是随机的（矩阵 $\boldsymbol{A}$ 的元素是变量 $x_1,x_2,\cdots,x_n$ 的随机二次多项式）。

因此，针对 Cubic AB 加密方案，使用直接攻击，其难度比求解一个随机二次方程组更大。

2.3　建议参数

如果选定 Cubic AB 加密方案在有限域 $GF(2^8)$ 上进行计算，则该方案解密失败概率的上限定可确定为：2^{-8}。相对于 3 次简单矩阵加密方案，Cubic AB 加密方案并没有使得安全性降低。相反，在固定密文长度时，增加明文长度（增加变量数目），还会提高方案的安全性。因此，参考 3 次简单矩阵加密方案的密文长度。由公式(2)可以看出密文明文长度之比，根据参数 s、u 的不同，可以变得很灵活。

在表 1 中列举了六组，在满足不同安全级别，选择不同的 s、u 参数，对应的明文、密文长度及其比值，以及生成的公钥、私钥大小。

表 1　Cubic AB 加密方案的参数选择

Table 1　Parameter settings of Cubic AB Scheme

安全级别	s,u	明文/bit	密文/bit	公钥/KB	私钥/KB	α
80	7,14	392	784	2 110	16.5	2
80	6,16	480	768	3 717	18.2	1.6
80	6,17	528	816	5 212	21.1	1.55
100	8,16	512	1 024	5 980	28.1	2
100	7,18	616	1 008	10 100	30.9	1.63
100	7,19	672	1 064	13 756	35.2	1.58

2.4　效率分析

比较 Cubic AB 加密方案和简单矩阵加密方案的解密过程，第一步与第三步仅仅是矩阵与向量之间相乘，运算量相差不多。在第二步中，对线性方程组进行求解，要执行的运算较多，性能消耗主要在此。线性方程的系数矩阵的维度为 $m\times n$ 时，通过高斯消元法对方程组进行求解，在有限域上进行乘法操作的次数为

$$\frac{n\cdot(n+1)\cdot(3m-n+1)}{6}+\frac{n(n-1)}{2}。$$

在同样的安全级别下，Cubic AB 方案的 m、n 参数取值都比简单矩阵方案的取值更小。容易得出，Cubic AB 方案在第二步执行的有限域乘法的次数更少。在表 2 中列举了在不同安全级别下，两种方案在解密过程第二步中执行有限域乘法操作的次数。

表 2　2 种方案的乘法操作次数

Table 2　Multiplications of the two cryptography schemes

方案	安全级别	m,n	次数	比值
SM	80	128,64	224 576	—
AB	80	98,49	101 626	0.453
SM	100	162,81	452 682	—
AB	100	128,64	224 576	0.496

说明：SM 为简单矩阵加密方案，AB 为 Cubic AB 加密方案

容易得出,Cubic AB加密方案的解密过程,比简单矩阵加密方案更快。

3 结 论

研究对ABCD加密方案的思想进行扩展,通过使用一个扁长的矩阵 $\boldsymbol{B}$ 来取代ABCD方案中的一组方阵,设计了Cubic AB多变量公钥加密方案,使得该方案的密文明文之比取值更灵活。同时,借鉴3次简单矩阵加密方案来提高新方案的安全性,相应的明文、密文可以更短,从而降低解密过程的计算量。

参考文献:

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. Siam Review,1997,41(2):1484-1509.

[2] Hwajeong S, Jihyun K, Jongseok C, et al. Small private key mqpks on an embedded microprocessorg[J]. Sensors,2014,14(3):5441-5458.

[3] Singaravelu P, Verma S. Feasibility of rainbow signature for broadcast authentication in sensor networks[C]// Vehicular Technology Conference (VTC Spring).[S.L.]:IEEE,2011:1-5.

[4] Singaravelu P, Verma S. Practicability of HFE scheme for wireless sensor network[C]// Transactions on Computational Science XVII. Berlin: IEEE,2013:116-132.

[5] Sundar D S, Narayan N. A novel voting scheme using quantum cryptography[C]// Open Systems (ICOS), 2014 IEEE Conference on.[S.L.]:IEEE,,2014:66-71.

[6] Ding J, Schmidt D. Rainbow, a new multivariable polynomial signature scheme[C]// Applied Cryptography and Network Security. Berlin: Springer,2005:164-175.

[7] Petzoldt A, Bulygin S, Buchmann J. Linear recurring sequences for the UOV key generation revisited[C]// Information Security and Cryptology-ICISC 2012. Berlin: Springer,2013:441-455.

[8] Porras J, Baena J, Ding J. ZHFE, a new multivariate public key encryption scheme[C]// Post-Quantum cryptography.[S.L.]: Springer International Publishing,2014:229-245.

[9] Petzoldt A, Bulygin S, Buchmann J. Fast verification for improved versions of the UOV and rainbow signature schemes[C]// Post-Quantum Cryptography. Berlin: Springer,2013:188-202.

[10] Petzoldt A, Thomae E, Bulygin S, et al. Small public keys and fast verification for multivariate quadratic public key systems[J]. Cryptographic Hardware & Embedded System,2011:475-490.

[11] Tao C, Diene A, Tang S, et al. Simple matrix scheme for encryption[C]// Post-Quantum Cryptography. Berlin: Springer, 2013:231-242.

[12] Ding J, Petzoldt A, Wang L C. The cubic simple matrix encryption scheme[C]// Post-Quantum Cryptography.[S.L.]: Springer International Publishing,2014:76-87.

[13] Tao C, Xiang H, Petzoldt A, et al. Simple matrix-a multivariate public key cryptosystem(MPKC) for encryption[J]. Finite Fields & Their Applications,2015,35:352-368.

[14] Petzoldt A. Eliminating Decryption Failures from the Simple Matrix Encryption Scheme. http://eprint.iacr.org/2016/010.pdf,2016.

(编辑 侯 湘)