

密文长度可变的 Simple Matrix 加密方案

王众, 韩益亮

(武警工程大学密码工程学院, 陕西 西安 710086)

摘要: 多变量公钥密码是抗量子密码的可靠候选之一, 其中的 Simple Matrix 方案是利用 3 个矩阵间的运算来构造的。提出了 Simple Matrix 方案的改进版本, 通过使用具有随机二次多项式的可改变形式的扁平矩阵进行构造, 使秩攻击对新的方案不可行, 且代数攻击对新方案的攻击至少和求解一组随机二次方程一样困难。新的方案将密文与明文的比例改进为大于等于两倍, 打破了固定不变的密文与明文比例, 使其拥有一个灵活的明密文比, 以适应不同的需求。

关键词: 多变量公钥密码; Simple Matrix 方案; 明密文比; 安全性分析

中图分类号: TN918.4

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018032

Simple Matrix encryption scheme with variable ciphertext length

WANG Zhong, HAN Yiliang

Engineering University of PAP, College of Cryptographic Engineering, Xi'an 710086, China

Abstract: Multivariable public key cryptography is one of the reliable candidates for anti-quantum cryptography. The Simple Matrix scheme is constructed using the operations between three matrices. An improved version of the Simple Matrix scheme was proposed. It is constructed by using two flat matrices with random quadratic polynomials, so that the rank attacks is infeasible for the new scheme, and the algebraic attacks breaks the system is at least as hard as solving a set of random quadratic equations. The new scheme will improve the proportion of ciphertext and plaintext to 2 times or more, break the fixed proportion of ciphertext and plaintext, so that it has a flexible proportion to adapt to different needs.

Key words: multivariable public key cryptography, Simple Matrix scheme, the proportion of plaintext and ciphertext, security analysis

1 引言

公钥密码在当今的计算机安全领域扮演着十分重要的角色。传统的公钥加密方案主要基于经典数论的相关知识, 比较典型的有 RSA、ECC (elliptic curves cryptography)、DSA (digital signature algorithm)、属性基的公钥密码等^[1]。1994 年,

Shor^[2]提出了一种在量子计算机上运行的多项式时间算法 (Shor 算法), 使分解大整数和求解 Abel 群上的离散对数问题在多项式时间内不再困难, 其时间复杂度大概为 $O(\log^3 N)$ (N 表示比特数为 N 的数), 这给基于经典数论问题的传统公钥密码学带来了威胁。而且随着计算机硬件技术的快速发展, 计算机的计算能力大幅提升, 在继传统计

收稿日期: 2018-03-10; 修回日期: 2018-04-01

通信作者: 韩益亮, hanyil@163.com

基金项目: 国家自然科学基金资助项目 (No.61572521)

Foundation Item: The National Natural Science Foundation of China (No.61572521)

算机出现并普及后, 又出现了以量子位为计算单位的计算机——量子计算机。在不久的将来, 大型的量子计算机出现后, 大部分传统的公钥密码将很容易被攻破。

目前, 主要的抗量子密码有: 基于编码的密码体制、基于格的密码体制 (LWE, learning with errors)、基于 Hash 函数的密码体制以及基于多变量的密码体制^[3]。为什么这些密码体制能够有效地抵抗量子计算机的攻击? 因为它们都是在 NP 难问题的基础上构建起来的, 而量子计算机相比于普通计算机在求解这一类问题上并没有显著的优势。抗量子密码中的基于多变量的密码体制, 相比于传统的公钥密码, 不仅能够有效地抵抗量子计算攻击, 而且在运行的效率方面有更多的优势, 并消耗更少的资源^[4]。尽管存在许多实用的多变量签名方案, 但有效和安全的多变量加密方案的数量还是有限的^[5]。

在 PQCrypto 2013 会议上, Cheng 等^[6]提出了一种新的多变量公钥加密方案 Simple Matrix (简称为 ABC 密码方案), 它可以抵抗大部分针对多变量公钥密码方案的攻击, 但是它的解密错误率却不可忽视。2014 年, Ding 等提出了对 Simple Matrix 方案的改进, 即 Cubic Simple Matrix 密码方案^[7], 使原来组成公钥的二次多变量多项式变为三次多变量多项式。这一改进, 可以有效地抵抗秩攻击^[8], 并且使代数攻击^[8]的困难性与解决随机二次多项式系统的困难性相近。Simple Matrix 方案与 Cubic Simple Matrix 方案都将密文与明文的比例控制在两倍关系, 使其应用起来不够灵活, 不能满足多种需求。本文提出了一种新的基于 Simple Matrix 的密码方案, 在保证安全性、可靠性的同时, 改变明文与密文之间的两倍固定关系, 提供了一种灵活可变的明文密文比例。

2 多变量公钥密码系统以及 Simple Matrix 方案

多变量公钥密码系统一般是建立在复杂庞大的代数结构上的^[9], 设 $K = GF(q)$ 为一有限域, 则其公钥为一组有限域 K 上的多变量多项式方程组构成的映射 $F: F^n \rightarrow K^m$, 其具体方程组如下所示。

$$\begin{cases} y_1 = f_1(x_1, \dots, x_n) \\ y_2 = f_2(x_1, \dots, x_n) \\ \vdots \\ y_m = f_m(x_1, \dots, x_n) \end{cases} \quad (1)$$

公钥 P 可以看作是 3 个映射的合成, 即 $P = S \circ F \circ T$ 。其中, S 和 T 为域 K 上随机选取的可逆仿射变换, 它们的作用是将中心映射 F 的结构隐藏起来, 而中心映射同样是由一组 n 个变量 m 个方程的多变量多项式方程组构成。私钥为三元组 (S, F, T) ; 公钥为 $P(x_1, x_2, \dots, x_n) = (f_1, f_2, \dots, f_m)$ 。

加密过程: 将明文 $x_1, x_2, \dots, x_n$ 加密, 可得到密文 $y_1, y_2, \dots, y_m$, 对应每一个 y_i , 有

$$y_i = f_i(x_1, x_2, \dots, x_n) \quad (2)$$

解密过程: 解密过程是加密过程的逆, 通过私钥信息可以很容易得到 P^{-1} , 则

$$(x_1, x_2, \dots, x_n) = P^{-1}(y_1, y_2, \dots, y_m) \quad (3)$$

2.1 双极系统

目前, 多变量密码方案可分为双极模式 (bipolar)、混合模式 (mixed)、多项式同构模式 (IP, isomorphisms of polynomials) 以及多元二次模式 (MQ, multivariate quadratic)^[10]。其中, 大部分的多变量公钥密码是基于双极系统来构造的, 混合模式的较少^[11], 而另外 2 种则更少。

双极系统的公钥包括 2 部分: 一是系统所在有限域 K 以及它的域结构; 二是公钥映射 P 的 m 个多项式。私钥则为随机选取的可逆线性仿射变换 L_1 和 L_2 , 以及中心映射 F ^[12]。

设有限域 $K = GF(q)$, 在一个双极多变量密码系统当中, 公钥为 $K^n \rightarrow K^m$ 的映射 F 为

$$F(x_1, x_2, \dots, x_n) = (f_1, f_2, \dots, f_m)$$

其中, f_1 为 $F(x_1, x_2, \dots, x_n)$ 中的 n 元多项式。

其中心映射为 $\bar{F}$, 构造过程如下。

1) $\bar{F}(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n) = (\bar{f}_1, \bar{f}_2, \dots, \bar{f}_m)$, 其中 $\bar{f}_i \in K[\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n]$ 。

2) 对于映射 $\bar{F}(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n) = (\bar{y}_1, \bar{y}_2, \dots, \bar{y}_m)$ 的计算可以很容易解决, 相应地也可以快速地找到 $(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_m)$ 对应的唯一像 $(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$, 即 $\bar{P}^{-1}(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_m)$ 。

加密过程: 已知需要加密的消息为

$X = (x_1, x_2, \dots, x_n)$, 将 X 作为明文代入公钥多项式, 计算得到密文 $Y = F(X) = (y_1, y_2, \dots, y_m)$ 。

解密过程: 密文消息为 $Y = (y_1, y_2, \dots, y_m)$, 对其解密即为求解方程

$$Y = F(X) \quad (4)$$

首先求解 $L_1^{-1}(Y) = \bar{Y}$, 然后计算 $\bar{X} = \bar{F}^{-1}(\bar{Y})$, 再计算明文 $X = L_2^{-1}(\bar{X})$ 。

2.2 混合系统

混合型多变量公钥密码系统的公钥也是利用在有限域下的映射, 使用 $K^{n+m} \rightarrow K^l$ 的映射, 记为 H 。

$$H(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) = (h_1, \dots, h_l)$$

其中, $h_i \in K[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$ 。要构造一个这样的加密方案就需要找到相应的中心映射 $\bar{H}: K^{n+m} \rightarrow K^l$ 。

中心映射要满足对于任意给定的 $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$, 方程组 $\bar{H}(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n, \bar{y}_1, \bar{y}_2, \dots, \bar{y}_m) = (0, \dots, 0)$ 都很容易求解, 并且在多数情况下, 是一个关于变量 $\bar{y}_1, \bar{y}_2, \dots, \bar{y}_m$ 的线性方程组, 使输入明文可以很快得到密文。若是给定另外 m 个变量 $\bar{y}_1, \bar{y}_2, \dots, \bar{y}_m$, 则会得到一个关于变量 $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$ 的二次方程组 $\bar{H}(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n, \bar{y}_1, \bar{y}_2, \dots, \bar{y}_m) = (0, \dots, 0)$, 该随机的二次方程组, 是具有特殊结构的方程组, 能很容易对其进行求解, 即得到明文。找到符合要求的中心映射后, H 可以表示为如下的形式。

$$H = L_3 \circ \bar{H} \circ (L_2 \times L_1) \quad (5)$$

其中, $L_1: K^m \rightarrow K^m$ 和 $L_2: K^n \rightarrow K^n$ 的定义与双极系统中所定义的可逆线性映射相同, L_3 则是一个 K^l 到 K^l 的可逆线性映射。

混合系统的公钥包括: 1) 系统所在有限域 K 以及其域结构; 2) 构成公钥映射 H 的多项式方程。

混合多变量公钥密码系统的构造思想与双极系统类似, 都是利用仿射变换对中心映射进行隐藏, 不同的是混合系统是利用 3 个仿射变换 L_1 、 L_2 和 L_3 来隐藏方程 $H(X, Y) = (0, \dots, 0)$ 。目前, 基于混合系统的多变量公钥密码方案比较少, 其中较为著名的是 Patarin 提出的 Dragon 加密体制^[10]。

2.3 Simple Matrix 方案

Simple Matrix 算法是 Cheng 等于 2013 年提出, 它的算法结构比较特别, 是由 3 个矩阵构成,

主要的参数有 n 、 m 、 s 。其中, n 代表明文长度, m 代表密文长度, 二者之间的关系满足 $m=2n$, 即为密文长度为明文的两倍, 明文用变量 $X = (x_1, x_2, \dots, x_n)$, $s \in N$, 且 $s^2=n$ 。

然后, 定义 3 个小矩阵 A 、 B 、 C 维度均为 $s \times s$, 如下所示。

$$A = \begin{bmatrix} x_1 & \cdots & x_s \\ \vdots & \ddots & \vdots \\ x_{(s-1)s+1} & \cdots & x_n \end{bmatrix}$$

$$B = \begin{bmatrix} b_1 & \cdots & b_s \\ \vdots & \ddots & \vdots \\ b_{(s-1)s+1} & \cdots & b_n \end{bmatrix}$$

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

其中, A 的 n 个元素为变量 $X = (x_1, x_2, \dots, x_n)$ 本身; 矩阵 B 与 C 中的各元素均为变量 X 所组成的随机线性组合。

再定义 2 个维度为 $s \times s$ 的矩阵 E_1 、 E_2 。其中 $E_1 = AB$, $E_2 = AC$, 由前面对于矩阵 A 、 B 、 C 的描述可知, E_1 、 E_2 中的元素均为关于变量 $X = (x_1, x_2, \dots, x_n)$ 的二次多项式。 E_1 、 E_2 二者共有 m 个二次多项式, 这 m 个二次多项式, 组合为 Simple Matrix 算法的中心映射 $F: K^n \rightarrow K^m$ 。

接下来, 与双极模式的构造方法类似, 有 2 个可逆线性映射 $S: K^m \rightarrow K^m$, $T: K^n \rightarrow K^n$, 将它们与中心映射 F 相复合, 得到公钥 $P = S \circ F \circ T: K^n \rightarrow K^m$ 。私钥则包含 2 个矩阵 B 、 C 与可逆线性映射 S 、 T 。

Simple Matrix 算法的加密过程如下。

对明文 $X = (x_1, x_2, \dots, x_n)$ 进行加密, 直接用公钥 P 对其运算得到密文 $Y = (y_1, y_2, \dots, y_m)$ 。

$$Y = (y_1, y_2, \dots, y_m) = P(x_1, x_2, \dots, x_n)$$

Simple Matrix 算法的解密过程如下。

对密文 $Y = (y_1, y_2, \dots, y_m)$ 进行解密, 可以分为以下 3 个步骤。

1) 利用可逆线性映射 S , 对密文进行运算得到 $Z = (z_1, z_2, \dots, z_m) = S^{-1}(y_1, y_2, \dots, y_m)$ 。

2) 由 Simple Matrix 的结构可知, 中心映射 F 的每一个多项式, 是矩阵 E_1 、 E_2 中的元素, 它们

都是由变量所组成的二次多项式。 E_1 、 E_2 中各元素的值为 $Z=(z_1, z_2, \dots, z_m)$ 。

$$E_1 = \begin{bmatrix} z_1 & \cdots & z_s \\ \vdots & \ddots & \vdots \\ z_{(s-1)s+1} & \cdots & z_n \end{bmatrix}$$

$$E_2 = \begin{bmatrix} z_{n+1} & \cdots & z_{n+s} \\ \vdots & \ddots & \vdots \\ z_{n+(s-1)s+1} & \cdots & z_m \end{bmatrix}$$

3) 对中心映射求原像, $F(W)=Z$, $W=(w_1, w_2, \dots, w_n)$ 根据不同情况有 3 种解法。

首先, 若矩阵 E_1 可逆, 则可根据 $BE_1^{-1}E_2=C$ 可以得到 n 个关于变量 W 的线性方程, 便可求出 W 。

其次, 若是矩阵 E_2 可逆, 则根据 $CE_1^{-1}E_2=B$ 也同样可以得到 n 个关于变量 W 的线性方程, 由此求出 W 。

最后, 若 E_1 、 E_2 均不可逆, 但是 A 可逆, 则将 A^{-1} 矩阵中的元素看作新的变量, 为 $(p_1, p_2, \dots, p_n)$ 。所以有 $A^{-1}E_1=B$, $A^{-1}E_2=C$, 因此就有了 m 个关于变量 $(w_1, w_2, \dots, w_n)$, $(p_1, p_2, \dots, p_n)$ 的线性方程, 便可以解出变量 W 。

若矩阵 A 、 E_1 、 E_2 均不可逆, 则无法解密。

4) 利用可逆线性映射 T 对 W 进行运算, 进而得到明文 X 。

$$X=(x_1, x_2, \dots, x_n)=T^{-1}(w_1, w_2, \dots, w_n)$$

在对中心映射 $F(W)=Z$ 求逆时, 可能会有多个解出现, 只需将这些解代入中心映射 F 求 Z 进行比较。从上述解密过程中可以看出, Simple Matrix 方案解密是否成功的关键在于矩阵 A 是否可逆。若是一个阶为 q 的有限域, 矩阵为方阵且在有限域上, 则该矩阵不可逆的概率为 $\frac{1}{q}$, 即有

$\frac{1}{q}$ 的可能性使解密失败。

3 Simple Matrix 方案改进版本

3.1 构造思想

从第 2 节的介绍中, 可以看出 Simple Matrix 算法中的密文与明文比例被固定为两倍的关系, 这会导致方案不够灵活, 不能满足多种需求。本节提出一种改进版本, 使密文与明文之间的比例

更加灵活, 并将其公钥由原来的二次多项式组成改为由三次多项式组成, 提供了更高的安全性。

首先, 有 3 个小矩阵 A 、 B 、 C 。其中, 矩阵 A 与 Simple Matrix 方案中的类似, 其维度同样为 $s \times s$, $s \in N$, 且 $s^2=n$ 。与 Simple Matrix 方案不同的是, 其元素的组成为变量 $X=(x_1, x_2, \dots, x_n)$ 的二次多项式而非变量本身。

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1s} \\ \vdots & \ddots & \vdots \\ a_{s1} & \cdots & a_{ss} \end{bmatrix}$$

$$a_{ij} = \sum_{r=1}^n \sum_{s=r}^n a_{rs} x_r x_s + \sum_{r=1}^n \beta_r^{(ij)} x_r + \varepsilon \quad (6)$$

另外, 2 个矩阵 B 与 C 的维度分别为 $s \times u$, $s \times v$, $u \in N$, $v \in N$, 其中的元素与 Simple Matrix 中的 B 、 C 矩阵的元素相同均为变量 $X=(x_1, x_2, \dots, x_n)$ 的线性组合。

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

$$C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1s} & \cdots & c_{1v} \\ c_{21} & c_{22} & \cdots & c_{2s} & \cdots & c_{2v} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{s1} & c_{s2} & \cdots & c_{ss} & \cdots & c_{sv} \end{bmatrix}$$

$$b_{ij} = \sum_{r=1}^n a_r^{(ij)} x_r + \mu \quad (7)$$

$$c_{ij} = \sum_{m=1}^n a_m^{(ij)} x_m + \theta \quad (8)$$

然后, 计算 2 个矩阵 E_1 、 E_2 , 其中 $E_1=AB$, E_1 的维度为 $s \times u$, $E_2=AC$ 其维度为 $s \times v$ 。由前所述, 矩阵 E_1 、 E_2 中的元素均为三次多项式。

$$E_1 = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1s} & \cdots & e_{1u} \\ e_{21} & e_{22} & \cdots & e_{2s} & \cdots & e_{2u} \\ \vdots & \vdots & & \vdots & & \vdots \\ e_{s1} & e_{s2} & \cdots & e_{ss} & \cdots & e_{su} \end{bmatrix}$$

$$E_2 = \begin{bmatrix} \bar{e}_{11} & \bar{e}_{12} & \cdots & \bar{e}_{1s} & \cdots & \bar{e}_{1v} \\ \bar{e}_{21} & \bar{e}_{22} & \cdots & \bar{e}_{2s} & \cdots & \bar{e}_{2v} \\ \vdots & \vdots & & \vdots & & \vdots \\ \bar{e}_{s1} & \bar{e}_{s2} & \cdots & \bar{e}_{ss} & \cdots & \bar{e}_{sv} \end{bmatrix}$$

$$e_{ij} = \sum_{r=1}^n \sum_{s=r}^n \sum_{t=s}^n \alpha_{rst}^{(ij)} x_r x_s x_t + \sum_{r=1}^n \sum_{s=r}^n \beta_{rs}^{(ij)} x_r x_s + \sum_{r=1}^n \delta_r^{(ij)} x_r + \varepsilon \quad (9)$$

$$\bar{e}_{ij} = \sum_{a=1}^n \sum_{b=a}^n \sum_{c=b}^n \alpha_{abc}^{(ij)} x_a x_b x_c + \sum_{a=1}^n \sum_{b=a}^n \beta_{ab}^{(ij)} x_a x_b + \sum_{a=1}^n \delta_a^{(ij)} x_a + \varepsilon \quad (10)$$

E_1 、 E_2 中的元素共有 $m = su + sv$ ，这 m 个元素均为变量 $X = (x_1, x_2, \dots, x_n)$ 所组成的三次多项式，则其中心映射即为 $H: K^n \rightarrow K^m$ 。还需要2个可逆仿射变换 $T: K^n \rightarrow K^n$ ， $S: K^m \rightarrow K^m$ ，对中心映射进行隐藏。该方案的公钥即为 $P = S \circ H \circ T: K^n \rightarrow K^m$ ，私钥即为映射 S 、 T 以及矩阵 B 、 C 。

加密时，直接将明文代入公钥 P 中即可。在解密时，关键是矩阵 A 是否可逆，若矩阵 A 可逆，可将矩阵 A^{-1} 中的元素视为新的元素分别与矩阵 E_1 、 E_2 相乘，即得 $A^{-1}E_1 = B$ ， $A^{-1}E_2 = C$ ，则有 $2n(2s^2)$ 个变量， $m = su + sv$ 个线性方程， $m \geq 2n$ ，所以最终可以求解出明文变量 $X = (x_1, x_2, \dots, x_n)$ 。

3.2 加密解密过程

1) 加密过程：类似于 Simple Matrix 方案，将明文 $X = (x_1, x_2, \dots, x_n)$ 代入公钥 P 的公式中，即可得到密文 $Y = (y_1, y_2, \dots, y_n)$ 。

2) 解密过程如下。

① 先对密文 Y 进行处理，利用可逆仿射变换 S 对信息 Y 进行逆运算，得到变量 W ， $W = (w_1, w_2, \dots, w_n) = S^{-1}Y = S^{-1}(y_1, y_2, \dots, y_n)$ 。

② 对中心映射 H 求逆， $Z = H^{-1}(W)$ ，关于变量 $Z = (z_1, z_2, \dots, z_n)$ 的二次多项式所组成的矩阵 A ，若矩阵 A 可逆，则将矩阵 A^{-1} 中的元素看作新的变量 $\bar{Z} = (\bar{z}_1, \bar{z}_2, \dots, \bar{z}_n)$ ，计算 $A^{-1}E_1 = B$ 。

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

$$= \begin{bmatrix} \bar{z}_{11} & \cdots & \bar{z}_{1s} \\ \vdots & \ddots & \vdots \\ \bar{z}_{s1} & \cdots & \bar{z}_{ss} \end{bmatrix} \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1s} & \cdots & w_{1u} \\ w_{21} & w_{22} & \cdots & w_{2s} & \cdots & w_{2u} \\ \vdots & \vdots & & \vdots & & \vdots \\ w_{s1} & w_{s2} & \cdots & w_{ss} & \cdots & w_{su} \end{bmatrix}$$

可以得到 su 个关于变量 $Z = (z_1, z_2, \dots, z_n)$ 和

$\bar{Z} = (\bar{z}_1, \bar{z}_2, \dots, \bar{z}_n)$ 的方程。同理，运用 $A^{-1}E_2 = C$ 可得 sv 个关于变量 $Z = (z_1, z_2, \dots, z_n)$ 和 $\bar{Z} = (\bar{z}_1, \bar{z}_2, \dots, \bar{z}_n)$ 的方程。通过联立以上 su 与 sv 个方程可以得到方程个数为 $m = su + sv$ ，变量个数为 $2n(2s^2)$ 的方程组，由于 $m \geq 2n$ ，可以解出变量 $Z = (z_1, z_2, \dots, z_n)$ 。

若矩阵 A 不可逆则解密失败。

③ 对变量 $Z = (z_1, z_2, \dots, z_n)$ 进行处理，运用仿射变换 T 对变量 Z 进行逆运算，即可得变量 $X = (x_1, x_2, \dots, x_n) = T^{-1}Z = T^{-1}(z_1, z_2, \dots, z_n)$ 。

由上述解密过程可以看出，改进版 Simple Matrix 方案解密失败的概率与原始 Simple Matrix 方案解密失败的概率相同，也就是说，若是一个阶为 q 的有限域，矩阵为方阵且在有限域上，则该矩阵不可逆的概率为 $\frac{1}{q}$ ，即有 $\frac{1}{q}$ 的可能性使解密失败。

4 安全性分析

4.1 秩攻击

秩攻击是对多变量公钥密码比较有效的一种攻击方法，它分为低秩攻击 (MinRank attack) [13] 与高秩攻击 (HighRank attack) [14]。

低秩攻击的目的是找到公钥中的一个线性组合，且它的秩为最小秩 r 。其定义为：对在有限域 K 上的 m 个维度为 $n \times n$ 的矩阵 $M_i (1 \leq i \leq m)$ ，找出一个非平凡的线性组合，即 $M = \mu_1 M_1 + \mu_2 M_2 + \cdots + \mu_m M_m$ ，且这个线性组合的秩不大于 r ($\text{rank}(M) \leq r$) [13]。最小秩问题也是一个 NP 问题，但是当 r 足够小的时候，其复杂度可以接受并能够求解。例如，在 HFE 方案中，一个低秩的多项式对应中心映射中的多项式。攻击者可以通过寻低秩的线性组合来恢复可逆仿射变换 T ，最终获得明文。

在高秩攻击中，攻击者则是找到关于中心多项式中出现次数最少的变量的线性组合。例如，Rainbow 方案 [15] 中最后一层中的油变量，就是出现次数最少的变量，通过对每一层重复这种攻击，攻击者可以恢复可逆仿射变换 S ，最终恢复明文。

然而，在改进版的 Simple Matrix 方案中，矩阵 A 的元素是随机选择的多元二次多项式。因此，它们的秩接近于 n ，不能使用低秩攻击。并且所有变量出现在每个中心多项式中的次数大约相

同, 这就不能使用高秩攻击。因此, 可以得到结论, 秩攻击不适用于改进版的 Simple Matrix 方案。

4.2 代数攻击

XL 算法^[16]和 Gröbner 基算法是主要的解非线性方程的方法^[17], 也是攻击多变量公钥密码的一种有效方法。在多变量公钥密码系统中, 将密文变量代入公钥多项式方程组中, 即可得到一组关于明文变量的多项式方程组 $Y = F(X)$, 直接对该方程组求解而得到明文, 这就是代数攻击或称为直接攻击的主要思想。XL 算法的本质是计算 Gröbner 基, 可以看作是 F4 算法^[18]的一种冗余变体, 目前最为有效的求 Gröbner 基的方法是由 Faugere 提出的 F4 和 F5 算法, 利用 F5 算法, 可以破解针对 HFE 体制的挑战 1^[19]。F5 算法通过计算 Gröbner 基的方法破解多变量密码算法的计算复杂度约为 $2^{0.873n}$, 其中, n 为变量的数目^[20]。

在利用代数攻击检验改进版 Simple Matrix 方案时, 攻击者面对的是一个由 n 个变量所组成的 $m(m \geq 2n)$ 个多元三次多项式方程所组成的方程组。如前面所提及的, 该系统是通过将包含随机选择的多元二次多项式的矩阵 A 与包含多元线性组合的矩阵 B 和 C 相乘而获得的 (忽略可逆仿射变换 S 和 T)。那么对该三次方系统的求解至少与系数是随机选取的多元二次方系统的求解是一样的难度。

5 效率分析

5.1 明文密文比例分析

由第4节对于改进版本的 Simple Matrix 的叙述可知, 明文长度为 n , 且有 $s \in N, n = s^2$, 而密文长度为 m , m 满足 $m = su + sv$, u 代表矩阵 B 的列数, v 代表矩阵 C 的列数。若想求得明文, 则线性方程的个数应当大于等于变量的个数, 由第3节对于解密过程的叙述, 可知 $m \geq 2n$, 即 $su + sv \geq 2s^2$ 。由此, 可以说明矩阵 B 与 C 是相对灵活的矩阵, 只要保证它们各自行的个数等于 s , 而二者列的个数满足不等式 $su + sv \geq 2s^2$ 即可在矩阵 A 可逆的条件下顺利解密。

密文与明文的比例可表示为

$$\tau = \frac{m}{n} = \frac{su + sv}{s^2} = \frac{u + v}{s} \geq 2, (u + v \geq 2s) \quad (11)$$

由上述不等式可知, 在 $u + v \geq 2s$ 的条件下, 改进版 Simple Matrix 方案可以打破密文与明文的两倍固定限制, 又减少了明文与密文之间的一些联系, 提供了一种更为灵活安全的明密文比例, 以满足不同的加密需求。

5.2 攻击效率

下面通过实验比较直接攻击对原始版 Simple Matrix 方案以及改进版 Simple Matrix 方案的攻击效果, (m, n) 分别代表密文与明文规模, 为方便比较抵抗直接攻击的能力, 令改进版 Simple Matrix 的密文与明文比为两倍, 与原始方案保持一致, 2 种方案均在域 GF(256) 上进行。实验对比结果如表 1 所示。

表 1 直接攻击效果对比

密文与明文比	原始方案		改进版本	
	Time/s	Memory/MB	Time/s	memory/MB
(32,16)	—	—	0.83	5.17
(8,4)	—	—	2.76	9.87
(14,7)	0.02	3.37	15.37	18.21
(18,9)	0.67	6.25	—	—
(28,14)	3.47	7.94	—	—

通过实验对比可以发现改进版 Simple Matrix 方案比 Simple Matrix 方案的求解复杂度更大, 耗时更长, 安全性更高, 并且随着密文明文规模的扩大, 消耗的时间呈指数增长。

6 结束语

Simple Matrix 方案是多变量公钥密码中较新的密码体制, 巧妙运用了 3 个矩阵间的运算来构造中心映射。本文对原始的 Simple Matrix 方案进行改进, 将原来公钥映射中的二次多项式用三次多项式代替, 可以有效地对秩攻击等攻击方法做有效的防御, 提升了方案的安全性, 并打破原始 Simple Matrix 方案中密文与明文长度两倍的固定关系, 减少了明文与密文之间的一些联系, 使方案更加灵活可靠。但是该改进方案中, 密文长度大于等于两倍的明文长度, 还需要进一步改进, 使密文长度可以小于两倍的明文长度甚至小于一倍的明文长度。下一步工作是扩大明密文比例的取值范围, 并提供一个加解密效率更高的方案。

参考文献:

- [1] RIVEST R L, SHAMIR A, ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 21(2), 120-126: 1978.
- [2] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[C]//Quantum Entanglement and Quantum Information-Proceedings of CCAST. 1999: 303-332.
- [3] BERNSTEIN D J, BUCHMANN J, DAHMEN E. Post quantum cryptography[M]. Berlin Heidelberg: Springer, 2010.
- [4] BOGDANOV A, EISENBARTH T, RUPP A, et al. Time-area optimized publickey engines: MQ-cryptosystems as replacement for elliptic curves?[C]//Cryptographic Hardware and Embedded Systems—CHES 2008. 2008:45-61.
- [5] DING J, SCHMIDT D. Rainbow, a new multivariable polynomial signature scheme[C]//International Conference on Applied Cryptography and Network Security. 2005:164-175.
- [6] CHENG T, DIENE A, TANG S, et al. Simple matrix scheme for encryption[C]//International Workshop on Post-Quantum Cryptography. 2013:231-242.
- [7] DING J, PETZOLDT A, WANG L C. The cubic simple matrix encryption scheme[C]//Post-Quantum Cryptography. 2014:76-87.
- [8] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE public key cryptosystem[C]//Advances in Cryptology—CRYPTO'99. 1999: 19-30.
- [9] SAKUMOTO K, SHIRAI T, HIWATARI H. Public-key identification schemes based on multivariate quadratic polynomials[J]. Technical Report of Ieice Isec, 2011, 111:706-723.
- [10] PATARIN J. Asymmetric cryptography with a hidden monomial[C]//Advances in Cryptology—CRYPTO '96. 1996:45-60.
- [11] DING J, GOWER J E, SCHMIDT D S. Multivariate public key cryptosystems[M]. US : Springer US, 2006.
- [12] 丁斗博. 多变量公钥密码中 TTS 方案的分析与改进[D]. 西安: 西安电子科技大学, 2013.
DING D B. Analysis and improvement on the multivariate quadratic TTS scheme[D]. Xi'an: Xidian University, 2013.
- [13] GOUBIN L, COURTOIS N. Cryptanalysis of the TTM Cryptosystem[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2000: 44-57.
- [14] COPPERSMITH D, STERN J, VAUDENAY S. Attacks on the birational permutation signature schemes[C]//Advances in Cryptology—CRYPTO'93. 1993:435-443.
- [15] DING J, SCHMIDT D. Rainbow, a new multivariable polynomial signature scheme[C]//Applied Cryptography and Network Security. 2005:164-175.
- [16] COURTOIS N, KLIMOV A, PATARIN J, et al. Efficient algorithms for solving overdefined systems of multivariate polynomial equations[C]//Advances in Cryptology—EUROCRYPT 2000. 2000: 392-407.
- [17] FAUGERE J C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)[C]//The 2002 International Symposium on Symbolic and Algebraic Computation. 2002:75-83.
- [18] FAUGERE J C. A new efficient algorithm for computing Grobner bases (F4)[J]. Journal of Pure and Applied Algebra,1999,139: 61-88.
- [19] DING J, BUCHMANN J. Solving degree and degree of regularity for polynomial systems over a finite fields[C]//The First International Conference on Symbolic Computation and Cryptography (SCC 2008). 2008.
- [20] MOHAMED M S E, CABARCAS D, DING J, et al. MXL 3: an efficient algorithm for computing gröbner bases of zero-dimensional ideals[C]//International Conference on Information Security and Cryptology. 2009:87-100.

[作者简介]



王众 (1995-), 男, 山东泰安人, 武警工程大学硕士生, 主要研究方向为抗量子密码。

韩益亮 (1977-), 男, 甘肃会宁人, 武警工程大学教授、博士生导师, 主要研究方向为抗量子密码。