



立方多变量公钥密码体制的最小秩分析

张 栖^{1,2*}, 聂旭云^{1,2}

(1. 电子科技大学 信息与软件工程学院, 成都 610054; 2. 网络与数据安全四川省重点实验室(电子科技大学), 成都 610054)

(* 通信作者电子邮箱 1106845293@qq.com)

摘 要:立方加密体制是经典的多变量公钥密码体制 Square 的改进方案, 其中心映射由平方映射改为了立方映射, 由此将公钥多项式从二次提升到三次来抵抗针对二次多变量公钥密码体制的最小秩攻击。针对这种体制, 提出一种结合差分的最小秩攻击, 旨在恢复它的私钥。首先, 分析体制的中心映射差分, 并根据差分后的结构来确定它的秩; 然后, 求解公钥差分, 并提取二次项的系数矩阵; 接着, 由系数矩阵以及确定的秩构造一个最小秩问题; 最后, 结合扩展的 Kipnis-Shamir 方法对问题进行求解。实验结果表明, 利用最小秩攻击可以恢复立方加密体制的私钥。

关键词:多变量公钥密码体制; Square; 最小秩攻击; 最小秩问题; Kipnis-Shamir 攻击

中图分类号:TP 309.7 **文献标志码:**A

MinRank analysis of cubic multivariate public key cryptosystem

ZHANG Qi^{1,2*}, NIE Xuyun^{1,2}

(1. School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan 610054, China;

2. Sichuan Key Laboratory of Network and Data Security (University of Electronic Science and Technology of China),

Chengdu Sichuan 610054, China)

Abstract: The cubic cryptosystem is the improvement of the classical multivariable cryptosystem Square. By increasing the degree of central mapping from square mapping to cubic mapping, the public key polynomial was promoted from quadratic to cubic in order to resist the MinRank attack against the quadratic multivariable public key cryptosystem. Aiming at this system, a MinRank attack combining with difference was proposed to recover its private key. Firstly, the central mapping difference of the system was analyzed, and its rank was determined according to the structure after difference. Then, the difference of the public key was solved and the coefficient matrices of the quadratic term were extracted. After that, a MinRank problem was constructed by the coefficient matrix and the determined rank. Finally, the extended Kipnis-Shamir method was combined to solve the problem. The experimental results show that the private key of cubic cryptosystem can be recovered by using MinRank attack.

Key words: multivariable public key cryptosystem; Square; MinRank attack; MinRank problem; Kipnis-Shamir attack

0 引言

自 1988 年 Matsumoto 和 Imai 首次提出具有里程碑意义的 MI(Matsumoto Imai)多变量公钥密码体制(Multivariate Public Key Cryptosystem, MPKC)^[1]以来,该密码学原语的设计与安全性分析逐渐成为密码学界与信息安全界的一个研究热点。

多变量公钥密码体制的安全性基于求解有限域上随机产生的多变量二次多项式方程组(Multivariate Quadratic, MQ)的问题,它是一个 NP-困难问题。MQ 问题也可扩展为求解有限域上随机产生的多变量三次多项式方程组(Multivariate Cubic, MC)的问题。多变量公钥密码体制一般由两个仿射变换和一个中心映射复合而成,其中复合函数的表达式为公钥,两个仿射变换为私钥。多变量公钥密码体制的构造关键在于它的中心映射的构造,而针对多变量公钥密码的安全性分析也集中在分析其中心映射。关于多变量公钥密码体制的更多

详细描述可参考文献[2]。

最小秩问题(MinRank Problem, MR Problem)指的是给定正整数 m, n, r, j 及 j 个矩阵 $M_0, M_1, \dots, M_{j-1} \in M_{m \times n}(K)$, 确定是否存在一组系数 $\lambda_1, \lambda_2, \dots, \lambda_{j-1} \in K$, 使得

$$\text{Rank} \left(\sum_{i=1}^{j-1} \lambda_i M_i - M_0 \right) \leq r$$

这是一个 NP-困难问题。

每一个多变量二次多项式中的齐二次项可用一个对称矩阵来表示。公钥多项式对应的矩阵能够表示成为中心映射多项式对应的矩阵的线性组合。一旦中心矩阵多项式对应的矩阵的秩较小,就可以采用最小秩攻击(MinRank Attack, MR Attack)来尝试恢复私钥。事实上,最小秩攻击,就是利用在公钥多项式对应的矩阵的线性组合中寻找具有最小秩矩阵来还原其私钥-线性仿射变换 U 。

收稿日期:2019-12-03; **修回日期:**2020-03-25; **录用日期:**2020-04-02。 **基金项目:**国家自然科学基金重点国际(地区)合作研究项目(61520106007); 四川省国际科技创新合作/港澳台科技创新合作项目(20GJHZ0273)。

作者简介:张栖(1994—),男,四川巴中人,硕士研究生,主要研究方向:网络安全、多变量公钥密码学; 聂旭云(1975—),男,江西吉安人,副教授,博士,CCF 会员,主要研究方向:多变量公钥密码学、大数据安全、隐私保护。



这一类攻击最早是由 Kipnis 等^[3]提出用于分析隐藏域方程 (Hidden Field Equations, HFE) 加密体制的安全性。2013 年, Bettale 等^[4]改进了 Kipnis 等的攻击方法破解了 multi-HFE。Zhang 等^[5]利用秩攻击破解了 Yasuda 等提出的一个签名方案, 并提出了一种改进方案来抵挡秩攻击^[6]。秩攻击同样可用于分析不平衡油醋类 (Unbalanced Oil and Vinegar, UOV) 签名体制^[7]。在秩攻击的要求下, 该类体制一般要求醋变量的个数是油变量个数的两倍。Yasuda 等^[8]基于彩虹体制 (Rainbow) 提出了一种改进的数字签名方案, 但很快就被 Perlner 等^[9]用最小秩攻击所破解了, Ikematsu 等^[10]借鉴了该体制的思想, 提出一种基于 HFE 体制的加密方案来抵抗最小秩攻击。另外, 秩攻击还可以在其他密码学领域作为安全性分析方法, 如认证方案 (Authentication Scheme)^[11]。

Square 加密方案^[12]与 MI 体制和 HFE 体制一样, 是属于“小域-大域”方案, 即其公钥是有限域 K 上的多变量二次多项式, 而其中映射是 K 的扩域上的单变量平方运算。相对于 HFE 体制而言, Square 体制极大地缩减了加密和解密成本, 但同时该体制既存在差分对称性^[13], 也具有最小秩缺陷。立方加密方案^[14]是 Square 方案的改进。通过将中心映射改为扩域上的单变量立方运算, 使得公钥多项式的次数由二次提升到三次, 来抵抗针对具有低秩中心映射的二次多变量公钥密码体制的最小秩攻击。本文分析表明, 立方加密方案的中心映射经过差分过后, 具有和 Square 方案一样的低秩缺陷。因此, 立方加密方案的公钥差分后得到的系数矩阵, 也具有低秩线性组合。结合改进的 Kipnis-Shamir 方法^[4], 即可恢复该体制的私钥。

1 预备知识

1.1 多变量公钥密码体制的一般形式

令 $k = F_q$ 是一个 q 元域, n 和 m 是两个正整数。 U 和 T 分别是 k^n 和 k^m 上的两个随机选取的仿射变换, $F: k^n \rightarrow k^m$ 称为中心映射。 $\mathbf{x} = (x_1, x_2, \dots, x_n)$ 为明文变量, $\mathbf{y} = (y_1, y_2, \dots, y_m)$ 为密文变量。令

$$P: \mathbf{x} \in \mathbb{K}^n \xrightarrow{T} \mathbf{u} = \mathbf{M}_1 \mathbf{x} + \mathbf{c}_1 \xrightarrow{F} \mathbf{v} = F(\mathbf{u}) \xrightarrow{U} \mathbf{y} = \mathbf{M}_2 \mathbf{v} + \mathbf{c}_2 \in \mathbb{K}^m$$

函数 $P = U \circ F \circ T$ 的表达式为多变量公钥密码体制的公钥, 通常为多组多变量二次多项式。 U 和 T 为私钥。

注意, 若在大域上构造中心映射 F , 需引入 k -线性同构 $\phi: K \rightarrow k^n$ 。其中 K 为 k 的 n 次扩域, F 为 K 上的单变量多项式。公钥形式如下:

$$P = U \circ \phi \circ F \circ \phi^{-1} \circ T$$

1.2 最小秩攻击

最小秩攻击是一个 NP-困难问题。在 r 比较小的时候, 问题可解。

Kipnis 等^[3]首先使用最小秩攻击来分析 HFE 公钥密码体制, 其方法被称为 Kipnis-Shamir 方法。

观察 $P = U \circ \phi \circ F \circ \phi^{-1} \circ T$, P 是已知的公钥, U 、 T 和 F 是未知的私钥。在文献^[3]中, 作者提出可以通过 k -线性同构 ϕ 将公钥 P 提升到大域上得到 P^* , 方法如下:

$$\begin{aligned} P^* &= \phi \circ P \circ \phi^{-1} = \\ &= \phi \circ U \circ \phi^{-1} \circ F \circ \phi \circ T \circ \phi^{-1} = \\ &= (\phi \circ U \circ \phi^{-1}) \circ F \circ (\phi \circ T \circ \phi^{-1}) = \\ &= U^* \circ F \circ T^* \end{aligned} \quad (1)$$

公式两边同时复合 U^{*-1} , 可得到 $U^{*-1} \circ P^* = F \circ T^*$, 由这个方程, 最终可以得到“基本方程”, 如下:

$$u_j P^{*j} = P' = T^* F T^{*t} \quad (2)$$

其中: P^{*k} 表示矩阵 P^* 的每个元素经过 q^k 幂次提升, u_k ($k = 0, 1, \dots, n-1$) 表示矩阵 U 的第一列元素。如果矩阵 F 的秩 r 是有界的, 那么 P' 的秩也是有界的。当秩 r 足够小时, 恢复 u_k 就可以规约到求解最小秩问题。

如何求解最小秩问题, Kipnis 和 Shamir 提出了 Kipnis-Shamir 模型^[3]。对于一个秩为 r 的线性组合, 它一定存在 $n-r$ 维的左核, 可以根据已知的 k 个齐次公钥矩阵和确定的秩 r , 得到一个由 $r(n-r) + k$ 个变量 $n(n-r)$ 个方程组成的多项式系统。

注意, Kipnis-Shamir 方法需要使用 k -线性同构将公钥矩阵从小域提升到大域, 这导致后续最小秩问题求解的成本增加。 Bettale 等^[4]基于 Kipnis-Shamir 方法提出了一种改进方法, 不需要将公钥从小域提升到大域, 可以直接求解最小秩问题, 极大地提升了最小秩问题的求解速度。本文实验部分也是采用这种方法。

1.3 Square 加密方案

Square 加密方案^[12]是 Baena 等根据 HFE 方案的设计思想设计而成。令 k 为特征值为 q 的有限域, K 是 k 的 n 次扩域。 $\phi: K \rightarrow k^n$ 是标准 k -线性同构, ϕ^{-1} 为它的逆。 Square 体制的中心映射为: $F: Y = X^2$ 。为了保证该映射可逆, 需满足 $\gcd(2, q^n - 1) = 1$ 。

和多变量公钥密码体制的一般形式一样, 它的公钥 $P = U \circ f \circ T = U \circ \phi \circ F \circ \phi^{-1} \circ T$, 私钥为 U , T 和 F 。对明文变量加密是通过求解 $P(\mathbf{x}) = \mathbf{y}$ 完成, 解密是通过对三个映射 U 、 T 和 F 的求逆完成。

根据它的中心映射的形式, 可确定其对应系数矩阵的秩为 1。也就是说, 该体制的公钥在经过同构变换从小域映射到大域后, 所对应的系数矩阵存在一组秩为 1 的线性组合, 形式如下:

$$\text{Rank} \left(\sum_{j=0}^{n-1} u_j P^{*j} \right) = 1$$

使用 Kipnis-Shamir 模型, 求解即可得到 u_k 。完整的私钥恢复过程可参考文献^[3]。

1.4 立方加密方案

立方加密方案是根据 Square 加密方案改进而成, 该方案的中心映射为: $F: Y = X^3$ 。为了保证该映射可逆, 需满足 $\gcd(3, q^n - 1) = 1$, 这就要求 $q \equiv 2 \pmod{3}$ 且 q 为奇数。设 d 为满足 $3t \equiv 1 \pmod{(q^n - 1)}$ 的整数, 则 F^{-1} 为 $X = F^{-1}(Y) = Y^{d \pmod{(q^n - 1)}}$ 。

相较于 Square 加密方案, 该方案中心映射的次数由 2 增加到 3, 它的公钥矩阵也由二维矩阵扩展到三维矩阵。尽管最小秩问题可以由二维矩阵扩展到三维矩阵, 但如何确定一个三维矩阵的秩是非常困难的, 甚至很难知道一个三维矩阵可能的最大秩^[15]。



2 立方加密方案的最小秩分析

虽然立方加密方案可以抵抗针对二维矩阵的最小秩攻击,但经过分析,可发现该体制的中心映射差分过后具有和 Square 方案中心映射相似的性质,在 A 点的差分结果如下:

$$DF(X, A) = F(X + A) - F(X) - F(A) + F(0) = (X + A)^3 - X^3 - A^3 + 0 = 3AX^2 + 3A^2X$$

差分过后齐二次项对应矩阵和 Square 方案中心映射对应矩阵的秩相等,并且立方加密方案的公钥经过差分后,逆向推导的中心映射 F' 的性质和 $DF(X, A)$ 相似,关系如下:

$$DP(x, a) = U \circ \phi \circ F' \circ \phi^{-1} \circ T \quad (3)$$

其中 $a \in k^n$, F' 是秩为 1 的二次多项式, $DP(x, a)$ 表示公钥多项式 P_1, P_2, \dots, P_n 在 a 点的差分。对于这种低秩中心映射,可以使用最小秩攻击恢复其私钥。同时,为了降低计算成本,本文采用一种扩展的 Kipnis-Shamir 方法^[4]。这种方法通过将 k -线性同构 ϕ 及它的逆 ϕ^{-1} 表示成矩阵形式,不需引入另外的 ϕ ,可直接在小域上求解最小秩问题。

2.1 改进的 Kipnis-Shamir 方法

命题 1^[4] 设 $(\theta_1, \theta_2, \dots, \theta_n) \in K^n$ 为域 K 基于域 k 上的一组基, $M_n \in K^{n \times n}$ 是一个由这组基经过 Frobenius 变换得到的矩阵,形式如下:

$$\begin{bmatrix} \theta_1 & \theta_1^q & \dots & \theta_1^{q^{n-1}} \\ \theta_2 & \theta_2^q & \dots & \theta_2^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ \theta_n & \theta_n^q & \dots & \theta_n^{q^{n-1}} \end{bmatrix}$$

k -线性同构 $\phi: K \rightarrow k^n$ 可以表示成如下形式:

$$V \rightarrow (V, V^q, \dots, V^{q^{n-1}}) \cdot M_n^{-1} \quad (4)$$

它的逆 ϕ^{-1} 可表示成:

$$(v_1, v_2, \dots, v_n) \rightarrow (v_1, v_2, \dots, v_n) \cdot M_n[1] \quad (5)$$

$(v_1, v_2, \dots, v_n) \cdot M_n[1]$ 表示该向量第一个元素。

命题 2^[4] 设矩阵 $A = [a_{i,j}] \in k^{n \times n}$, 矩阵 $B = [b_{i,j}] = A \cdot M_n \in K^{n \times n}$, 则矩阵 B 的各列存在如下关系:

$$b_{i,j} = b_{i,j-1}^q; 0 \leq i, j \leq n$$

在得到 M_n 后,即可使用矩阵乘积来表示复合映射 $DP(x, a) = U \circ \phi \circ F' \circ \phi^{-1} \circ T$ 。首先取多项式组 $DP(x, a)$ 的齐二次项系数矩阵,得到 G_1, G_2, \dots, G_n 。令 $h_1, h_2, \dots, h_n = \phi^{-1} \circ F' \circ \phi$ 表示基域多项式组,它们的系数矩阵为 H_1, H_2, \dots, H_n 。根据式(4)和(5),可以用矩阵 M_n 来表示这组系数矩阵,形式如下:

$$(H_1, H_2, \dots, H_n) = (M_n \cdot F^{*0} \cdot M_n^t, M_n \cdot F^{*1} \cdot M_n^t, \dots, M_n \cdot F^{*(n-1)} \cdot M_n^t) \cdot M_n^{-1} \quad (6)$$

其中: F^{*k} 表示中心映射 F' 的 q^k 次幂的系数矩阵,它的元素表示为 $f_{i-k,j-k}^{q^k}$ 。复合映射的矩阵表示过程如下:

$$DP(x, a) = U \circ \phi \circ F' \circ \phi^{-1} \circ T(x) \Rightarrow$$

$$(G_1(x), G_2(x), \dots, G_n(x)) = (h_1(xM_T), h_2(xM_T), \dots,$$

$$h_n(xM_T))M_U \Rightarrow (xG_1x^t, xG_2x^t, \dots, xG_nx^t) =$$

$$(xM_T \cdot H_1 \cdot M_T^t x^t, xM_T \cdot H_2 \cdot M_T^t x^t, \dots, xM_T \cdot H_n \cdot$$

$$M_T^t x^t)M_U \Rightarrow (G_1, G_2, \dots, G_n) = (M_T \cdot H_1 \cdot M_T^t, M_T \cdot$$

$$H_2 \cdot M_T^t, \dots, M_T \cdot H_n \cdot M_T^t) \cdot M_U$$

将式(6)代入,得:

$$(G_1, G_2, \dots, G_n) = (M_T \cdot M_n \cdot F^{*0} \cdot M_n^t \cdot M_T^t, M_T \cdot M_n \cdot F^{*1} \cdot M_n^t \cdot M_T^t, \dots, M_T \cdot M_n \cdot F^{*(n-1)} \cdot M_n^t \cdot M_T^t) \cdot M_U^{-1} \cdot M_n^{-1} \cdot M_U \Rightarrow (G_1, G_2, \dots, G_n) \cdot M_U^{-1} \cdot M_n = (M_T \cdot M_n \cdot F^{*0} \cdot M_n^t \cdot M_T^t, M_T \cdot M_n \cdot F^{*1} \cdot M_n^t \cdot M_T^t, \dots, M_T \cdot M_n \cdot F^{*(n-1)} \cdot M_n^t \cdot M_T^t) \quad (7)$$

设 $M_U^{-1} \cdot M_n = S = [s_{i,j}], M_T \cdot M_n = W = [w_{i,j}]$, 式(7)可化简为:

$$(G_1, G_2, \dots, G_n) \cdot S = (W \cdot F^{*0} \cdot W^t, W \cdot F^{*1} \cdot W^t, \dots, W \cdot F^{*(n-1)} \cdot W^t) \quad (8)$$

令 $(s_{0,0}, s_{1,0}, \dots, s_{n-1,0})$ 为矩阵 S 的第一列元素,则根据式(8),可得到“基本方程”,如下:

$$\sum_{i=0}^{n-1} s_{i,0} \cdot G_{i+1} = W \cdot F^{*0} \cdot W^t = W \cdot F' \cdot W^t \quad (9)$$

由前文分析可知,矩阵 F' 的秩 r 为 1,则恢复 $s_{i,0} (0 \leq i \leq n-1)$ 可以规约到最小秩问题的求解。

2.2 实验步骤及结果

完整的实验过程可在普通 PC 上用 MAGMA 实现,PC 的配置为: Inter Core i5-4300U CPU, 2.50 GHz, 8 GB 内存。给定 q, n , 秩 $r = 1$, 具体实验步骤如下:

步骤 1 对于给定公钥 P_1, P_2, \dots, P_n , 依次求解出差分,得到差分过后二次项所对应系数矩阵 G_1, G_2, \dots, G_n 。

步骤 2 生成一个 $(n-r) \times n$ 的矩阵 KM , 形式如下:

$$\begin{bmatrix} 1 & 0 & \dots & 0 & x_{1,1} & x_{1,2} & \dots & x_{1,r} \\ 0 & 1 & \dots & 0 & x_{2,1} & x_{2,2} & \dots & x_{2,r} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & x_{n-r,1} & x_{n-r,2} & \dots & x_{n-r,r} \end{bmatrix}$$

矩阵行向量是线性无关的。根据式(7),存在非零向量 $(s_{0,0}, s_{1,0}, \dots, s_{n-1,0})$, 使得 $KM \times \left(\sum_{i=0}^{n-1} s_{i,0} G_{i+1} \right) = 0$ 。求解得到 $(s_{0,0}, s_{1,0}, \dots, s_{n-1,0})$, 根据命题 2, 即可恢复完整的矩阵 S :

$$\begin{bmatrix} s_{0,0} & s_{0,0}^q & \dots & s_{0,0}^{q^{n-1}} \\ s_{1,0} & s_{1,0}^q & \dots & s_{1,0}^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ s_{n-1,0} & s_{n-1,0}^q & \dots & s_{n-1,0}^{q^{n-1}} \end{bmatrix}$$

然后由 $M_U \cdot M_n^{-1} = S \Rightarrow M_U = S \cdot M_n$ 恢复矩阵 U 。需注意, S 的恢复是由最小秩问题求解得到。根据文献[16], 该攻击的计算复杂度主要由最小秩问题求解决定, 为 $O(n^{2w}) (2 \leq w \leq 3)$ 。

步骤 3 在恢复 U 后, 令 $(w_{0,0}, w_{1,0}, \dots, w_{n-1,0})$ 为矩阵 W 的第一列元素, 矩阵 K 为 $\sum_{i=0}^{n-1} s_{i,0} \cdot G_{i+1}$ 的左核, 可得到如下方程组:

$$Frob_{(l-1) \bmod n}(K) \cdot (w_{0,0}, w_{1,0}, \dots, w_{n-1,0})^t = 0 \quad (10)$$

其中 $l = 1, 2, \dots, r$, $Frob_l(K)$ 表示 K 的每列元素经过 Frobenius 变换^[4]后得到的矩阵。求解出这个方程组后, 根据命题 2, 即可恢复 W :

$$\begin{bmatrix} w_{0,0} & w_{0,0}^q & \dots & w_{0,0}^{q^{n-1}} \\ w_{1,0} & w_{1,0}^q & \dots & w_{1,0}^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ w_{n-1,0} & w_{n-1,0}^q & \dots & w_{n-1,0}^{q^{n-1}} \end{bmatrix}$$

然后由 $M_T \cdot M_n = W \Rightarrow M_T = W \cdot M_n^{-1}$ 恢复矩阵 M_T 。



步骤 4 公钥已知,在成功恢复矩阵 M_U 和 M_T 后,根据 $P = U \circ \phi \circ F \circ \phi^{-1} \circ T$,逆向恢复中心映射 F 。

文献[14]中的推荐参数为 $n = 15, q = 59, r = 1$ 。根据文献[16],该攻击的计算复杂度主要由最小秩问题求解决定,为:

$$O(n^{2w}) \leq 2^{23}; 2 \leq w \leq 3$$

由于域的大小并不会影响理论分析的结果,因此,在实验中,令 $q = 5, n$ 的大小不超过 30。实验运行时间和复杂度估计如表 1 所示。从表 1 中可以看出,攻击的效率较高,符合理论分析的结果。

表 1 不同参数下最小秩攻击的代价和破解时间的比较

Tab. 1 Comparison of cost and cracking time of MinRank attack under different parameters

| q | n | 时间复杂度 | 恢复 S 时间/s | 恢复 W 时间/s |
|-----|-----|----------|-------------|-------------|
| 5 | 11 | 2^{21} | 0.016 | 0.001 |
| 5 | 17 | 2^{25} | 0.390 | 0.068 |
| 5 | 21 | 2^{27} | 0.406 | 0.047 |
| 5 | 27 | 2^{29} | 0.998 | 0.094 |

为了能够让该体制抵抗最小秩攻击,同时考虑到效率问题,本文建议使用减方法来提高该体制的安全性,减去的公钥多项式个数为 $s=2$ 。

2.3 实例

为了更清楚阐述攻击流程,在本节展示一个具体实例。同时为了简化计算流程,本实例采用可逆线性变换而不是仿射变换。令 $q = 5, n = 7$,线性变换 U 和 T 的系数矩阵 M_U, M_T 分别为:

$$M_U = \begin{pmatrix} 2 & 1 & 0 & 1 & 2 & 2 & 0 \\ 2 & 1 & 0 & 1 & 0 & 4 & 3 \\ 4 & 1 & 3 & 1 & 1 & 4 & 3 \\ 0 & 1 & 2 & 4 & 0 & 2 & 0 \\ 1 & 4 & 1 & 4 & 0 & 1 & 3 \\ 2 & 2 & 0 & 0 & 1 & 4 & 2 \\ 2 & 3 & 4 & 4 & 3 & 1 & 2 \end{pmatrix}$$

$$M_T = \begin{pmatrix} 0 & 0 & 4 & 4 & 4 & 1 & 3 \\ 0 & 3 & 0 & 0 & 1 & 0 & 3 \\ 2 & 3 & 1 & 0 & 4 & 1 & 0 \\ 2 & 4 & 1 & 4 & 2 & 4 & 0 \\ 3 & 3 & 0 & 2 & 2 & 2 & 2 \\ 3 & 4 & 1 & 4 & 2 & 3 & 3 \\ 3 & 1 & 1 & 1 & 4 & 4 & 0 \end{pmatrix}$$

公钥差分过后的系数矩阵为:

$$G_1 = \begin{pmatrix} 1 & 4 & 1 & 2 & 4 & 3 & 0 \\ 4 & 0 & 3 & 1 & 2 & 3 & 3 \\ 1 & 3 & 1 & 0 & 0 & 3 & 4 \\ 2 & 1 & 0 & 3 & 0 & 1 & 0 \\ 4 & 2 & 0 & 0 & 0 & 2 & 4 \\ 3 & 3 & 3 & 1 & 2 & 0 & 0 \\ 0 & 3 & 4 & 0 & 4 & 0 & 1 \end{pmatrix}$$

$$G_2 = \begin{pmatrix} 1 & 2 & 3 & 1 & 3 & 3 & 4 \\ 2 & 2 & 3 & 1 & 1 & 0 & 3 \\ 3 & 3 & 0 & 2 & 0 & 1 & 0 \\ 1 & 1 & 2 & 0 & 2 & 2 & 0 \\ 3 & 1 & 0 & 2 & 0 & 1 & 0 \\ 3 & 0 & 1 & 2 & 1 & 4 & 0 \\ 4 & 3 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 0 & 4 & 4 & 0 & 2 & 2 & 1 \\ 4 & 0 & 0 & 1 & 4 & 4 & 0 \\ 4 & 0 & 0 & 3 & 2 & 2 & 0 \\ 0 & 1 & 3 & 0 & 0 & 3 & 0 \\ 2 & 4 & 2 & 0 & 4 & 3 & 0 \\ 2 & 4 & 2 & 3 & 3 & 4 & 4 \\ 1 & 0 & 0 & 0 & 0 & 4 & 0 \end{pmatrix}$$

$$G_4 = \begin{pmatrix} 3 & 2 & 0 & 2 & 2 & 2 & 0 \\ 2 & 4 & 0 & 2 & 3 & 0 & 4 \\ 0 & 0 & 3 & 4 & 2 & 1 & 3 \\ 2 & 2 & 4 & 0 & 1 & 4 & 0 \\ 2 & 3 & 2 & 1 & 1 & 1 & 4 \\ 2 & 0 & 1 & 4 & 1 & 2 & 1 \\ 0 & 4 & 3 & 0 & 4 & 1 & 3 \end{pmatrix}$$

$$G_5 = \begin{pmatrix} 1 & 0 & 3 & 2 & 3 & 4 & 4 \\ 0 & 2 & 0 & 1 & 4 & 2 & 2 \\ 3 & 0 & 3 & 3 & 3 & 1 & 1 \\ 2 & 1 & 3 & 2 & 4 & 2 & 3 \\ 3 & 3 & 3 & 4 & 0 & 4 & 1 \\ 4 & 2 & 1 & 2 & 4 & 4 & 1 \\ 4 & 2 & 1 & 3 & 1 & 1 & 2 \end{pmatrix}$$

$$G_6 = \begin{pmatrix} 2 & 2 & 3 & 4 & 4 & 3 & 0 \\ 2 & 2 & 0 & 1 & 1 & 1 & 4 \\ 3 & 0 & 1 & 1 & 0 & 2 & 2 \\ 4 & 1 & 1 & 2 & 4 & 4 & 3 \\ 1 & 1 & 0 & 4 & 3 & 1 & 2 \\ 2 & 2 & 4 & 1 & 3 & 1 & 1 \\ 0 & 4 & 2 & 3 & 2 & 1 & 1 \end{pmatrix}$$

$$G_7 = \begin{pmatrix} 2 & 2 & 3 & 4 & 4 & 3 & 0 \\ 2 & 2 & 0 & 1 & 1 & 1 & 4 \\ 3 & 0 & 1 & 1 & 0 & 2 & 2 \\ 4 & 1 & 1 & 2 & 4 & 4 & 3 \\ 4 & 1 & 0 & 4 & 3 & 1 & 2 \\ 3 & 1 & 2 & 4 & 1 & 3 & 1 \\ 0 & 4 & 2 & 3 & 2 & 1 & 1 \end{pmatrix}$$

求解最小秩问题,恢复 $(s_{0,0}, s_{1,0}, \dots, s_{6,0})$:
 $(1, \alpha^{56258}, \alpha^{53040}, \alpha^{7689}, \alpha^{27122}, \alpha^{66498}, \alpha^{31713})$

由命题 2 可恢复矩阵 S , 根据 $M_U \cdot M_n^{-1} = S$ 恢复矩阵 M_U :

$$M_U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 4 & 4 & 3 & 1 & 3 \\ 3 & 3 & 3 & 0 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 & 3 & 1 & 0 \\ 4 & 1 & 4 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 4 & 3 & 3 & 1 \\ 0 & 1 & 2 & 0 & 3 & 3 & 3 \end{pmatrix}$$

恢复矩阵 M_U 后,由式(10)可求得 $(\omega_{0,0}, \omega_{1,0}, \dots, \omega_{6,0})$:
 $(1, \alpha^{49685}, \alpha^{31282}, \alpha^{16867}, \alpha^{65802}, \alpha^{30380}, \alpha^{26890})$

由命题 2 可恢复矩阵 W , 再根据 $M_T \cdot M_n = W$ 恢复 M_T :

$$M_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 4 & 0 & 2 & 4 & 3 & 4 \\ 1 & 4 & 4 & 4 & 4 & 0 & 1 \\ 0 & 2 & 2 & 4 & 4 & 2 & 4 \\ 2 & 1 & 3 & 3 & 0 & 1 & 1 \\ 1 & 1 & 4 & 3 & 1 & 4 & 4 \\ 3 & 3 & 2 & 3 & 1 & 2 & 1 \end{pmatrix}$$

恢复 M_U 和 M_T 后,由 $P = U \circ \phi \circ F \circ \phi^{-1} \circ T$ 即可恢复中心映射 F :

$$Y = \alpha^{65157} X^3 + \alpha^{26595} X^2 + \alpha^{7564} X + \alpha^{73773}$$



恢复得到的 U, T, F 即为一组等价密钥。

3 结语

本文结合差分方法和最小秩攻击方法,对立方多变量公钥加密体制进行了安全性分析,发现该体制中心映射经过差分后具有低秩缺陷,利用本文的攻击方法可成功地恢复体制的私钥。对立方多变量公钥加密体制使用减方法增强后可得到立方多变量公钥签名体制。减方法在减去一定个数的公钥多项式后,剩余的公钥多项式差分后所对应的系数矩阵不能构成差分后中心映射对应矩阵的线性组合,使得最小秩攻击无法对其产生作用。未来的工作中,将进一步分析该签名体制的安全性。

参考文献 (References)

- [1] MATSUMOTO T, IMAI H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption [C]// Proceedings of the 1988 Workshop on the Theory and Application of Cryptographic Techniques, LNCS 330. Berlin: Springer, 1988: 419-453.
- [2] 胡磊, 聂旭云. 多变量公钥密码发展研究报告(2010—2014) [J]. 中国密码学会通讯, 2016(2): 15-22. (HU L, NIE X Y. Research report on the development of multivariable public key cryptography (2010-2014) [J]. Communication of Chinese Association for Cryptologic Research, 2016(2): 15-22.)
- [3] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE public key cryptosystem by relinearization [C]// Proceedings of the 19th Annual International Cryptology Conference, LNCS 1666. Berlin: Springer, 1999: 19-30.
- [4] BETTALE L, FAUGÈRE J C, PERRET L. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic [J]. Designs, Codes and Cryptography, 2013, 69(1): 1-52.
- [5] ZHANG W, TAN C H. Algebraic cryptanalysis of Yasuda, Takagi and Sakurai's signature scheme [C]// Proceedings of the 2014 International Conference on Information Security and Cryptology. Cham: Springer, 2014: 53-66.
- [6] ZHANG W, TAN C H. A secure variant of Yasuda, Takagi and Sakurai's signature scheme [C]// Proceedings of the 17th International Conference on Information Security and Cryptology, LNCS 8949. Cham: Springer, 2014: 53-66.
- [7] KIPNIS A, PATARIN J, GOUBIN L. Unbalanced oil and vinegar signature schemes [C]// Proceedings of the 1999 International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 1592. Berlin: Springer, 1999: 206-222.
- [8] YASUDA T, SAKURAI K. A multivariate encryption scheme with rainbow [C]// Proceedings of the 17th International Conference on Information and Communications Security, LNCS 9543. Cham: Springer, 2015: 236-251.
- [9] PERLNER R, PETZOLDT A, SMITH-TONE D. Total break of the SRP encryption scheme [C]// Proceedings of the 24th International Conference on Selected Areas in Cryptography, LNCS 10719. Cham: Springer, 2017: 355-373.
- [10] IKEMATSU Y, PERLNER R, SMITH-TONE D, et al. HFERP — a new multivariate encryption scheme [C]// Proceedings of the 9th International Conference on Information and Communications Security, LNCS 10786. Cham: Springer, 2018: 396-416.
- [11] FAUGÈRE J C, EL DIN M S, SPAENLEHAUER P J. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology [C]// Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation. New York: ACM, 2010: 257-264.
- [12] CLOUGH C, BAENA J, DING J, et al. Square, a new multivariate encryption scheme [C]// Proceedings of the 2009 Cryptographers' Track at the RSA Conference, LNCS 5473. Berlin: Springer, 2009: 252-264.
- [13] 鲁刚, 聂旭云, 秦志光, 等. 一种多变量公钥密码体制的安全性分析 [J]. 电子科技大学学报, 2018, 47(2): 242-246. (LU G, NIE X Y, QIN Z G, et al. Cryptanalysis of a multivariate public key cryptosystem [J]. Journal of University of Electronic Science and Technology of China, 2018, 47(2): 242-246.)
- [14] 鲁刚. 多变量公钥密码体制的设计与安全性分析研究 [D]. 成都: 电子科技大学, 2017: 107. (LU G. Research on design and cryptanalysis of multivariate public key cryptosystem [D]. Chengdu: University of Electronic Science and Technology of China, 2017: 107.)
- [15] HILLAR C J, LIM L H. Most tensor problems are NP-hard [J]. Journal of the ACM, 2013, 60(6): No. 45.
- [16] PETZOLDT A, CHEN M S, DING J, et al. HMFEP—an efficient multivariate signature scheme [C]// Proceedings of the 8th International Workshop on Post-Quantum Cryptography, LNCS 10346. Cham: Springer, 2017: 205-223.

This work is partially supported by the Major International (Regional) Joint Research Project of the National Natural Science Foundation of China (61520106007), the International Scientific and Technological Innovation Cooperation Project/ Scientific and Technological Innovation Cooperation Project with Hong Kong, Macao and Taiwan in Sichuan Province (20GJHZ0273).

ZHANG Qi, born in 1994, M. S. candidate. His research interests include network security, multivariate public key cryptography.

NIE Xuyun, born in 1975, Ph. D., associate professor. His research interests include multivariate public key cryptography, big data security, privacy protection.