

一种混合多变量公钥签名方案

李晓莉¹, 乔帅庭², 刘 佳³

(1. 河南工业大学信息科学与工程学院, 郑州 450001;

2. 信息工程大学数字工程与先进计算国家重点实验室, 郑州 450001; 3. 防空兵指挥学院, 郑州 450052)

摘 要: 多变量公钥密码体制能抵抗量子计算机的攻击, 是后量子时代一种安全的密码体制备选方案。考虑到 Square 体制可有效抵抗线性化攻击, 不能抵抗差分攻击, 三角型密码系统能抵抗差分攻击, 但受到线性化方程攻击和最小秩攻击的情况, 结合 Square 体制和三角型密码系统, 采用新的混合签名结构框架重构中心映射, 提出一种混合多变量公钥签名方案。分析结果表明, 混合签名方案克服了 Square 体制和三角型密码系统的缺陷, 能够抵抗线性攻击(包含一般线性化方程攻击和高阶线性化方程攻击)、差分攻击、最小秩攻击和代数攻击, 具备较高的安全性。

关键词: 多变量公钥密码; 混合多变量签名方案; 线性攻击; 差分攻击; 最小秩攻击; 代数攻击

中文引用格式: 李晓莉, 乔帅庭, 刘 佳. 一种混合多变量公钥签名方案[J]. 计算机工程, 2015, 41(1): 121-125.

英文引用格式: Li Xiaoli, Qiao Shuaiting, Liu Jia. A Hybrid Multivariate Public Key Signature Scheme[J]. Computer Engineering, 2015, 41(1): 121-125.

A Hybrid Multivariate Public Key Signature Scheme

LI Xiaoli¹, QIAO Shuaiting², LIU Jia³

(1. College of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001, China;

2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China; 3. Air Defense Forces Command Academy, Zhengzhou 450052, China)

[Abstract] Multivariate public key cryptosystem mechanism can resist attacks from the quantum computer, so it is believed to be an alternative secure cryptosystem in the post-quantum age. Considering that the Square scheme can resist linearization attack, but it can not be resistant against differential attack, and tame transformation method can resist differential attack, but it cannot be resistant against linearization attack and the minrank attack, by combining the Square scheme and tame transformation method, and using a new framework, a new central mapping is redesigned, and a hybrid multivariate public key signature scheme is proposed. Analysis results show that the hybrid signature cryptosystem has good efficiency and overcomes the drawbacks of the Square scheme and tame transformation method. Meanwhile, it can also resist linearization attack (including ordinary linearization attack and High Order Linearization Equation (HOLE) Attack), differential attack, the minrank attack and algebraic attack.

[Key words] multivariate public key cryptography; hybrid multivariate signature scheme; linearization attack; differential attack; minrank attack; algebraic attack

DOI: 10.3969/j.issn.1000-3428.2015.01.022

1 概述

量子计算机的快速发展对信息安全体系造成极大的影响。Shor 算法的提出使得目前广泛使用的基于大数分解和离散对数的公钥签名算法受到严重威胁^[1-2]。为此, 具有抗量子计算性质的公钥密码受到

了广泛关注^[3]。多变量公钥密码体制就是在这种背景下发展而来。其安全性基于有限域上多元二次非线性方程组和多项式同构问题的难解性^[4-6]。

1999 年, Moh 提出了 TTM (Tame Transformation Method) 密码系统, 该密码系统的中心映射为“三角型”映射^[7], 具有很高的效率, 但受到线性攻击和最小秩攻

基金项目: 国家自然科学基金资助项目(61300123)。

作者简介: 李晓莉(1976-), 女, 讲师、博士, 主研方向: 信息安全; 乔帅庭, 硕士研究生; 刘 佳, 讲师、博士。

收稿日期: 2014-01-14 **修回日期:** 2014-03-26 **E-mail:** lixiaoli201311@163.com

击^[8-9]。2009年, Crystal Clough 提出了一种新的高效的加密方案 Square, 该方案能有效地抵抗线性攻击等^[10], 同年, Olivier Billet 等通过差分攻击手段寻找 Square 方案的不变子空间, 从而恢复出 Square 方案的密钥^[11]。当前的多变量公钥密码算法大部分受到不同程度的攻击, 如何构造出一种安全的多变量公钥加密和签名体制是一个值得研究的热点和难点。

本文利用分支思想, 在 Square 体制和三角型密码系统基础上, 重构了中心映射, 设计了混合签名方案, 从线性攻击、差分攻击、最小秩攻击等对混合签名方案进行安全性分析。

2 背景知识

2.1 多变量公钥密码体制的一般结构

多变量公钥密码的陷门构造如下所示:

$$\begin{aligned} X = (x_1, x_2, \dots, x_n) &\xrightarrow{S} X' = \\ (x'_1, x'_2, \dots, x'_n) &\xrightarrow{Q} Y' = \\ (y'_1, y'_2, \dots, y'_m) &\xrightarrow{T} Y = \\ (y_1, y_2, \dots, y_m) & \end{aligned}$$

从而得到公钥:

$$P = T \circ Q \circ S = (p_1(x_1, x_2, \dots, x_n), \dots, (p_l(x_1, x_2, \dots, x_n))$$

其中, $S: X \rightarrow X' = M_i C + C_i$ 和 $T: Y' \rightarrow Y = M^T Y' + C_T$ 分别为 F_q^n 和 F_q^m 上随机选取的可逆仿射变换, 它们共同“隐藏”了中心映射 Q 的结构, 是私钥的重要组成部分。

公钥方程组每个 $p_k(x_1, x_2, \dots, x_n)$ 为一个关于 $x = (x_1, x_2, \dots, x_n)$ 的非线性二次方程:

$$y_k = p_k(x_1, \dots, x_n) = \sum_i P_{ik} x_i + \sum_{i > j} Q_{ik} x_i^2 + \sum_{i > j} P_{ijk} x_i x_j,$$

所有的系数和变量都在域 $k = F_q$ 中, q 为域 k 的阶。

解决此类问题相当于解决了有限域上的多元二次方程组求解问题, 即 MQ (Multivariate Quadratic) 问题^[12-13]。

2.2 Square 方案及其攻击

2.2.1 Square 方案

2009年, Crystal Clough 提出了一种新的高效的加密方案 Square, 该方案能有效地抵抗线性攻击等^[10]。

记 k 为一有限域, $k = F_q, q \equiv 3 \pmod{4}$ 。 K 为 k 的 $n+l$ 次扩域, $K \cong k[y]/[g(y)] = F_{q^{n+l}}$, l 满足 $n+l$ 为奇数。定义 k 同构 $\varphi: K \rightarrow k^{n+l}, \varphi(a_0 + a_1 x + \dots + a_{n+l-1} x^{n+l-1}) = (a_0, a_1, \dots, a_{n+l-1})$, $L_1: k^n \rightarrow k^{n+l}$ 为一个单射仿射变换, 中心映射 $F: K \rightarrow K, F(X) = X^2$, $L_2: k^{n+l} \rightarrow k^{n+l}$ 为一个可

逆仿射变换。Square 加密体制如图 1 所示。

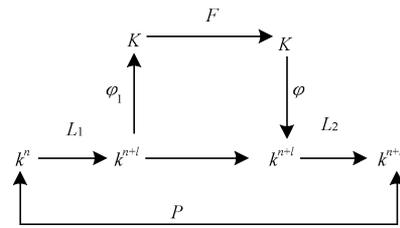


图 1 Square 加密体制

Square 体制的公钥为:

$$P = L_2 \circ \varphi \circ F \circ \varphi^{-1} \circ L_1$$

记 Square 体制的密文为 $(c_1, c_2, \dots, c_{n+l}) = P(m_1, m_2, \dots, m_n) \in k^{n+l}$, 解密如下所示:

(1) 计算 $Y = \varphi^{-1} \circ L_2^{-1}(c_1, c_2, \dots, c_{n+l})$;

(2) 解方程 $X^2 = Y$, 因 $q = 3 \pmod{4}$, 且 $n+l$ 为奇数, 则 $|K| \equiv 3 \pmod{4}$, 于是可得 $X = \pm Y^{\frac{q^{n+l}+1}{4}}$;

(3) 计算 (由于 L_1 是仿射的, 只有一个 X 是 $L_1 \circ \varphi^{-1}$ 的象)。

2.2.2 Square 方案的攻击

2009年, 文献 [11] 通过差分攻击手段寻找 Square 方案的不变子空间, 从而恢复出 Square 方案的密钥^[11]。

将 Square 方案的公钥分解为:

$$P(X) = L_2(L_1(X)^2) + L_2(s \cdot L_1(X)) + t$$

其中, $s = \frac{1}{2}\sigma; t = \tau + L_2(\sigma^2)$; σ, τ 为 $E = F_q^{n+l}$ 中的秘密常量。

记:

$$P_2(X) = L_1(L_2(X)^2), P_1(X) = L_1(s \cdot L_2(X)), P_0(X) = t$$

$DP(X, Y) = L_2(2 \cdot L_1(X) \cdot L_1(Y))$, 考虑差分 $DP_y: X \rightarrow DP(X, y)$ 。由于 $L_1: k^n \rightarrow k^{n+l}$ 满秩, 则它的象的维数为 n 。任意选取线性独立的向量 y_1, y_2, \dots, y_n , 使得 $DP_{y_1}, DP_{y_2}, \dots, DP_{y_n}$ 能够表示 $\{DP_z\}_{z \in E}$ 的整个空间。记 $\Delta = \{P_1\} \cup \{DP_{y_i}\}_{i=1,2,\dots,n}$, 每个元素都可表示为 $L_2 \circ \nu_\alpha \circ L_1, \nu_\alpha$ 表示 E 中的元素乘以 α , 因而 $\Delta = \{L_2 \circ \nu_{\lambda_i} \circ L_1\}_{i=1,2,\dots,n}$, n 个值 $\lambda_1, \lambda_2, \dots, \lambda_n$ 未知, 但线性独立。

通常的方法是找到公钥方程 $D_1 = L_2 \circ \nu_{\lambda_1} \circ L_1 \in \Delta$ 和 $D_1 = L_2 \circ \nu_{\lambda_2} \circ L_1 \in \Delta$ 之间的线性映射 L , 使得:

$$L \circ D_1 = D_2 \tag{1}$$

显然, $L_0 = L_2 \circ \nu_{\lambda_2 \lambda_1^{-1}} \circ L_2^{-1}$ 是式 (1) 的特解, 式 (1) 的解并不局限于乘法, 且 L_1 不是双射, 需要更多的限制条件, 因此, 寻找满足下列条件的线性映射 L :

$$\forall i \in \{1, 2, \dots, m\}, L \circ (L_2 \circ \nu_{\lambda_i} \circ L_1) \in [L_2 \circ \nu_{\lambda_{m+1}} \circ L_1, \dots, L_2 \circ \nu_{\lambda_n} \circ L_1] \tag{2}$$

即若存在 λ 使得:

$$\forall i \in \{1, 2, \dots, m\}, \lambda \circ \lambda_i \in [\lambda_m, \dots, \lambda_n] \quad (3)$$

则 $L_2 \circ \nu_\lambda \circ L_2^{-1}$ 一定是式(2)的解。

恢复出线性映射 $L = L_2 \circ \nu_\lambda \circ L_2^{-1}$ 后, 密钥都可以计算出来。当签名时, 乘法 λ 可由 L 的特征多项式得到。 L_2 的等价表示 T_0 可由 $\tilde{L}_2 \circ L = \nu_\lambda \circ \tilde{L}_2$, 令 a 为随机选取的元素, 密钥的其他元素可通过下式求出:

$$S(a) = \sqrt{T_0^{-1}(P_2(a))}$$

$$s_0 = \frac{1}{S(a)} \cdot T_0^{-1}(P_1(a))$$

$$S_0 = \frac{1}{s_0} \cdot T_0^{-1} \cdot P_1$$

2.3 三角型方案及其攻击

2.3.1 三角型方案

文献[7]提出 TTM(Tame Transformation Method) 密码系统^[7], 该密码系统的中心映射为三角型映射 $G: F_q^m \rightarrow F_q^n$:

$$G(x_1, x_2, \dots, x_n) = \begin{pmatrix} x_1 + g_1(x_2, \dots, x_n) \\ x_2 + g_2(x_3, \dots, x_n) \\ \vdots \\ x_{n-1} + g_{n-1}(x_n) \\ x_n \end{pmatrix}$$

其中, $g_i \in F_q[x_1, x_2, \dots, x_n]$ 是任意的二次多项式。

易知 G 是一个一一映射, 而且容易求逆: 给定 $G(x_1, x_2, \dots, x_n) = (y_1', y_2', \dots, y_n')$, 可以依次求出 $(x_1', x_2', \dots, x_n')$:

$$\begin{cases} x_n' = y_n' \\ x_{n-1}' = y_{n-1}' - g_{n-1}(y_n') \\ \vdots \\ x_2' = y_2' - g_2(y_3', \dots, y_n') \\ x_1' = y_1' - g_1(y_2', \dots, y_n') \end{cases}$$

2.3.2 对三角型方案的攻击

针对 TTM 三角型密码系统的攻击主要有 2 种: 线性化方程攻击和最小秩攻击。

线性化方程攻击是指 TTM 密码系统存在如下的线性化方程:

$$\sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i y_j + \sum_{i=1}^n b_i x_i + \sum_{i=1}^n c_i y_i + d = 0$$

其中, a_{ij}, b_i, c_i, d 为方程式的 $(n+1)^2$ 个系数。

在给出 $O((n+1)^2)$ 个明密文对 $(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$ 时, 可以求解上述方程组的系数。一旦所有的系数均被求解得到, 在给定密文 $y = (y_1, \dots, y_n)$ 的情况下, 就可得到关于明文 $x = (x_1, x_2, \dots, x_n)$ 的 n 个线性方程组。

最小秩攻击是指把 TTM 密码系统的分析问题转化成求解最小秩的问题。首先把 TTM 系统的公

钥多项式转化成二次型, 然后得到该二次型下的一组 $n \times n$ 矩阵 (M_1, M_2, \dots, M_m) 。希望找到一组向量 $(\lambda_1, \lambda_2, \dots, \lambda_m) \in F_q^m$, 使得 $Rank(\sum_{i=1}^m \lambda_i M_i) \leq d$, 其中, $Rank(\cdot)$ 表示矩阵的秩。在 TTM 系统中 d 比较小, 最小秩问题在多项式时间内可以求解, 也就是说最小秩攻击可以打败 TTM 密码系统。

3 签名方案

当前的多变量公钥密码体制中, 大部分处于不同程度地攻击, 构造一种安全性好的多变量公钥加密和签名方案仍是一个值得研究的开放课题。Square 加密体制能够抵抗线性攻击和最小秩攻击, 但是受到差分攻击的影响; 三角型密码系统能够抵抗差分攻击, 但不能抵抗线性攻击和最小秩攻击。

3.1 方案描述

本文将 2 种方案结合起来, 构造一种混合的多变量公钥签名方案。混合签名方案的结构如图 2 所示。

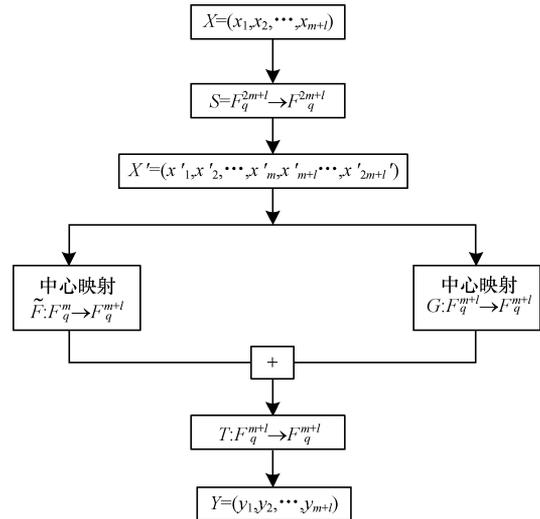


图 2 混合签名方案

其中, $S: F_q^{2m+1} \rightarrow F_q^{2m+1}$ 和 $T: F_q^{m+1} \rightarrow F_q^{m+1}$ 分别为可逆仿射变换, 中心映射 $\tilde{F}: F_q^m \rightarrow F_q^{m+1}$ 的构造思想类似于 Square 加密体制, $\tilde{F} = \varphi \circ F \circ \varphi^{-1} \circ L, L: k^m \rightarrow k^{m+1}$ 为单射仿射变换, φ 为 k 同构: $K \rightarrow k^{m+1}, \varphi(a_0 + a_1x + \dots + a_{m+1}x^{m+1}) = (a_0, a_1, \dots, a_{m+1}), F: K \rightarrow K, F(X) = X^2$; 中心映射 $G: F_q^{m+1} \rightarrow F_q^{m+1}$ 为三角型映射。

由混合签名方案的构造图可知, 公钥 $P: F_q^{2m+1} \rightarrow F_q^{m+1}$ 为:

$$P = T \circ (\tilde{F} + G) \circ S = T \circ (\varphi \circ F \circ \varphi^{-1} \circ L + G) \circ S$$

公钥包含以下内容:

- (1) 有限域 k 以及域上的加法和乘法运算;
- (2) 映射 $P = T \circ (\tilde{F} + G) \circ S$ 。

私钥包含以下内容:

(1) 可逆仿射变换 $S: F_q^{2m+l} \rightarrow F_q^{2m+l}$ 和 $T: F_q^{m+l} \rightarrow F_q^{m+l}$;

(2) 单射仿射变换 $L: F_q^m \rightarrow F_q^{m+l}$;

(3) 三角型映射 $G: F_q^{m+l} \rightarrow F_q^{m+l}$ 。

签名: 设 M 为待签名文件, 用公开的哈希函数 $Hash$ 计算 $(x_1, x_2, \dots, x_{2m+l}) = Hash(M)$ ($l \ll m$)。签名步骤如下:

(1) 计算 $X' = (x_1', x_2', \dots, x_{2m+l}') = S(x_1, x_2, \dots, x_{2m+l})$;

(2) 选取 $X' = (x_1', x_2', \dots, x_{2m+l}')$ 中的前 m 个分量, 即 $(x_1', x_2', \dots, x_m')$, 则其余的分量记为 $(x_{m+1}', \dots, x_{2m+l}')$, 经过中心映射, 计算 $Y_1' = (y_{11}', y_{12}', \dots, y_{1(m+l)}')$ $= \tilde{F}(x_1', x_2', \dots, x_m')$ 和 $Y_2' = (y_{21}', y_{22}', \dots, y_{2(m+l)}')$ $= G(x_{m+1}', \dots, x_{2m+l}')$, 得到 $Y' = (y_1', y_2', \dots, y_{m+l}') = Y_1' \oplus Y_2' = (y_{11}' + y_{21}', \dots, y_{1(m+l)}' + y_{2(m+l)}')$;

(3) 经过仿射变换 T , 得到 $Y = (y_1, y_2, \dots, y_{m+l}) = T(y_1', y_2', \dots, y_{m+l}')$ 即为签名值。

验证: 验证者收到消息 M 和签名 $(y_1, y_2, \dots, y_{m+l})$ 后, 验证如下:

(1) 计算 $Hash(M) = (x_1, x_2, \dots, x_{2m+l})$;

(2) 验证方程组 $P(x_1, x_2, \dots, x_{2m+l}) = (y_1, y_2, \dots, y_{m+l})$ 是否成立。若成立, 则签名有效, 否则, 签名无效。

3.2 方案效率分析

本文方案在中心映射的设计上采用分支思想, 在硬件实现上, 便于进行并行化操作。不妨设消息摘要的长度为 $2m+l$, 则在一般情况下 (没有采用分支时) 完成签名需要在多项式时间 $O((2m+l)^2)$ 内完成; 在本文的方案中, 完成签名至多在多项式时间 $O(m^2 + (m+l)^2)$, 约为 $O(2m^2)$, 即签名的时间复杂度为 $O(2m^2)$ 。因此, 方案具有很好的效率。由混合签名方案的结构可知, 签名长度为 $(m+l)q$ 。

混合签名方案的公钥为 $P: F_q^{2m+l} \rightarrow F_q^{m+l}$, 即 $(m+l)$ 个 $(2m+l)$ 元二次多项式, 公钥长度为 $(m+l)[(C_{2m+l}^{2m+l} + 2m+l) + (2m+l+1)]q$, 约为 $(2m^3 + 4m^2)q$ 。

4 安全性分析

混合签名方案的公钥 $P: F_q^{2m+l} \rightarrow F_q^{m+l}$ 为:

$$P = T \circ (\tilde{F} + G) \circ S = T \circ (\varphi \circ F \circ \varphi^{-1} \circ L + G) \circ S$$

目前, 针对多变量数字签名方案的典型攻击方法主要有线性化方程攻击 (线性攻击)、差分攻击、秩攻击、代数攻击等, 当针对多变量数字签名方案的攻击算法计算复杂度均大于 $O(2^{80})$ 时, 称该方案的安全强度达到 $O(2^{80})$ 。下面以选取参数 $q = 2^{16}$, $m = 16$, $l = 4$ 为例对混合签名方案进行安全分析。

4.1 线性攻击

混合签名方案的公钥 P 也可表示为:

$$P = T \circ \varphi \circ F \circ \varphi^{-1} \circ L \circ S + T \circ G \circ S$$

其中, $T \circ \varphi \circ F \circ \varphi^{-1} \circ L \circ S$ 为 Square 密码体制; $T \circ G \circ S$ 为三角型密码系统。

对 $T \circ \varphi \circ F \circ \varphi^{-1} \circ L \circ S$ 而言, 中心映射 $F = X^2$ (即 MI 的中心映射 $Y = X^{\theta+1}$ 中 $\theta = 0$ 的情形)。而线性化方程攻击是利用 MI 类的中心映射的关系 $XY^{\theta} - X^{\theta}Y = 0$ 得到的 X 与 Y 的线性关系进行攻击的。在混合签名方案中, 取 $\theta = 0$, 不能得到系统 $T \circ \varphi \circ F \circ \varphi^{-1} \circ L \circ S$ 关于 X 与 Y 的线性关系, 从而得不到公钥 $P = T \circ (\tilde{F} + G) \circ S$ 中 X 与 Y 的线性关系, 所以, 混合签名方案可抵抗一般线性化方程攻击。

Ding 等人在 PKC 2007 提出了针对中间域多变量公钥加密体制 (MFE) 的高阶线性化方程攻击^[14]。考虑混合签名方案中含有三角型密码系统, 需要对混合签名方案进行抗 HOLE 攻击分析。

由混合签名方案的公钥为: $P = T \circ (\varphi \circ F \circ \varphi^{-1} \circ L + G) \circ S = T \circ (\tilde{F} + G) \circ S$ 。在签名过程中经过变换 S 后, 变量分为两部分 (x_1, x_2, \dots, x_m) 和 $(x_{m+1}, x_{m+2}, \dots, x_{2m+l})$, 中心映射为 $\tilde{F} + G: X' \rightarrow Y'$, 即:

$$\begin{cases} y_{11}' + y_{21}' = x_{m+1}' + g_{m+1}(x_{m+2}', \dots, x_{2m+l}') \\ y_{12}' + y_{22}' = x_{m+2}' + g_{m+2}(x_{m+3}', \dots, x_{2m+l}') \\ \dots \end{cases}$$

$$y_{1(m+l)}' + y_{2(m+l)}' = x_{2m+l}'$$

变形可得:

$$\begin{cases} y_{21}' = x_{m+1}' + g_{m+1}(x_{m+2}', \dots, x_{2m+l}') + y_{11}' \\ y_{22}' = x_{m+2}' + g_{m+2}(x_{m+3}', \dots, x_{2m+l}') + y_{12}' \\ \dots \end{cases}$$

$$y_{2(m+l)}' = x_{2m+l}' + y_{1(m+l)}'$$

不妨假设:

$$\begin{cases} y_{21}' = x_{m+1}' + g_{m+1}(x_{m+2}', \dots, x_{2m+l}') \\ y_{22}' = x_{m+2}' + g_{m+2}(x_{m+3}', \dots, x_{2m+l}') \\ \dots \end{cases}$$

$$y_{2(m+l)}' = x_{2m+l}'$$

类似于 MFE 加密方案^[15], 变量 $(x_{m+1}', x_{m+2}', \dots, x_{2m+l}')$ 与 $(y_{21}', y_{22}', \dots, y_{2(m+l)}')$ 存在高阶线性化方程, 但系统加入了 $(y_{11}', y_{12}', \dots, y_{1(m+l)}')$, 相当于在三角型系统中加入了外部干扰, 而加入外部干扰后就打破了高阶线性化方程攻击的可能^[16]。事实上, 在一般情况下, 在三角型系统中, 中心映射的输入变量与输出变量一般不会存在特殊的关系, 即不会存在高阶线性化方程关系, 所以混合签名方案能抵抗高阶线性化方程攻击。

综上所述, 混合签名方案可抵抗线性化攻击。

4.2 差分攻击

多变量公钥密码系统中, 差分攻击主要针对中心映射形如 $F: X \rightarrow X^{q^l+1}$ 的体制提出^[17]。

由于在系统中 $P_1 = T \circ \varphi \circ F \circ \varphi^{-1} \circ L \circ S$ 中 F 的特殊形式使得 $DP_1(X, Y) = T(2 \cdot S(X) \cdot S(Y))$, 从而可以寻找不变子空间来恢复密钥信息。

但混合签名方案中 $P = T \circ (\tilde{F} + G) \circ S$ 引入了中心映射 G , G 不是形如 $G: X \rightarrow X^{q^l+1}$ 的映射, 整体中心映射的结构发生变化, 且引入 G 后条件 $DP(X, Y) = T(2 \cdot S(X) \cdot S(Y))$ 也不能满足, 针对 Square 的攻击也不适应于新的混合签名方案, 所以, 利用差分手段对混合签名方案进行攻击不可行。

4.3 秩攻击

考虑到针对三角型密码系统的攻击主要是最小秩攻击, 这里的秩攻击特指最小秩攻击。最小秩攻击的复杂度为 $q^r (w^2 (nt/2 - w/6) + wn^2t) \sim O(q^r w^3)$, 其中, $t = \lfloor \frac{w}{n} \rfloor$; r 各方程的线性组合所能达到的最小秩; n 为方程组中变量的个数; w 为方程的个数^[18]。由给出的参数可知, 混合签名方案中 $q = 2^{16}$, $m = 20$, $n = 36$, 从而 $t = 1$ 。将中心映射转为可以利用的矩阵形式, 将公钥转为 20 个 36×36 的矩阵, r 为公钥矩阵的一组线性组合达到的最小秩。只要保证 $r \geq 5$, 最小秩攻击的复杂度就大于 $O(2^{80})$ 。

在三角型密码系统中, 通常 r 的取值很小, 比如 TTM 体制, $r = 2$, 所以三角形系统容易受到最小秩攻击^[7]。在混合签名方案中, 引入了 Square 方案, 从而使得 r 增大, 所以 20 个 36×36 的矩阵的线性组合的秩很容易满足 $r \geq 5$ 。

综上, 在参数选取合适的情况下, 混合签名方案可抵御最小秩攻击。

4.4 代数攻击

代数攻击是直接针对公钥方程组的, 常用的工具包括 Gröbner 基攻击和 XL 算法^[19-20]。

根据方程的个数 m 和变量的个数 n 之间的关系, 代数攻击分为 $m = n$, $m > n$ 和 $m < n$ 3 种情况进行。但在混合签名方案中, 方程的个数为 $m + l$, 变量的个数为 $2m + l > m + l$, 所以仅就 $m < n$ 的情形进行讨论。当 $m < n$ 时, 多元二次方程组为不定方程组^[11], 求解的复杂度约等于穷尽搜索的复杂度 $O(q^m)$ 。在本文方案中, 参数 $q = 2^{16}$, $m = 20$, 复杂度为 $O(2^{320})$, 所以, 混合签名方案能够抵抗代数攻击。

5 结束语

本文结合 Square 体制和三角型密码系统, 构造了新的中心映射, 提出一种混合的多变量公钥签名方案。由安全性分析可知, 该方案克服了 Square 体制和三角型密码系统的缺陷, 能够抵抗线性攻击、差分攻击、最小秩攻击和代数攻击。本文签名方案参数的选取以及是否存在对其新的攻击是下一步要研究的问题。

参考文献

[1] Shor P. Polynomial-time Algorithms for Prime Factorization

and Discrete Logarithms on a Quantum Computer[J]. Aiam Journal on Scientific Computing, 1999, 41(2):303-332.

- [2] Fu Xingqun, Bao Wandu, Zhou Chun. Speeding up Implementation for Shor's Factorization Quantum[J]. Chinese Science Bull, 2010, (4):322-327.
- [3] Bernstein D J, Buchmann J, Dahmen E. Post-quantum Cryptography[M]. Berlin, Germany: Springer, 2009.
- [4] Ding Jintai, Yang B Y. Multivariate Public Key Cryptography[M]. Berlin, Germany: Springer, 2009.
- [5] 孙昌毅, 李益发, 斯雪明. 基于多变量公钥密码体制的代理重签名方案[J]. 计算机工程, 2012, 38(17): 116-118.
- [6] 乔帅庭, 韩文报, 李益发, 等. 基于外部干扰的中间域公钥签名方案的优化[J]. 信息工程大学学报, 2013, 14(2):135-140.
- [7] Moh T. A Public Key System with Signature and Master Key Functions[J]. Communications in Algebra, 1999, 27(5):2207-2222.
- [8] Goubin L, Courtois N T. Cryptanalysis of the TTM Cryptosystem [C]//Proceedings of Asiacrypt' 00. Berlin, Germany: Springer, 2000:44-57.
- [9] Tsujii S, Gotaishi M, Tadaki K, et al. Proposal of a Signature Scheme Based on STS Trapdoor [EB/OL]. (2004-05-20). <http://www.eprint.iacr.org/2004/366>.
- [10] Clough C, Baena J, Ding J T, et al. Square, A New Multivariate Encryption Scheme [C]//Proceedings of CT-RSA' 09. Berlin, Germany: Springer, 2009:252-264.
- [11] Billet O, Macario-Rat G. Cryptanalysis of the Square Cryptosystems[C]//Proceedings of ASIACRYPT' 09. Berlin, Germany: Springer, 2009:451-468.
- [12] 孙昌毅, 李益发, 张文政, 等. 基于多变量密码体制的新型代理签名方案[J]. 四川大学学报: 自然科学版, 2013, 49(3):565-569.
- [13] 陶羽. 多变量数字签名的研究与设计[D]. 西安: 西安电子科技大学, 2012.
- [14] Ding J, Hu L, Nie X, et al. High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems [C]//Proceedings of PKC' 07. Berlin, Germany: Springer, 2007:233-248.
- [15] Wang L C, Yang B Y, Hu Y H, et al. A "Medium-field" Multivariate Public-key Encryption Scheme [C]//Proceedings of CT-RSA' 06. Berlin, Germany: Springer, 2006:132-149.
- [16] Tian L, Bao W S. A Medium Field Multivariate Public key Signature Scheme with External Perturbation [C]//Proceedings of Conference on Intelligent Information Technology and Security Informatics. [S. l.]: IEEE Perss, 2010:753-757.
- [17] Fouque P A, Granboulan L, Stern J. Differential Cryptanalysis for Multivariate Schemes [C]//Proceedings of EUROCRYPT' 05. Berlin, Germany: Springer, 2005: 341-353.
- [18] 鲁晓彬. 几类多变量数字签名方案研究[D]. 郑州: 解放军信息工程大学, 2012.
- [19] Albrecht M R, Cid C, Faugère J C, et al. On the Relation Between the MXL Family of Algorithms and Gröbner Basis Algorithms[J]. Journal of Symbolic Computation, 2012, 47(8):926-941.
- [20] Thomae E, Wolf C. Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited[C]//Proceedings of PKC' 12. [S. l.]: IEEE Press, 2012:156-171.

编辑 索书志