改进的Medium-Field多变量公钥加密方案

王志伟[1]，郑世慧[1]，杨义先[1]，张智辉[2]

(1. 北京邮电大学网络与交换技术国家重点实验室 北京 海淀区 100876; 2. 索尼中国研究院 北京 海淀区 100080)

【摘要】提出了一种改进的MFE多变量公钥加密方案。能够抵御高阶线性化方程攻击。给出了该改进方案在秩攻击和XL&Gröbner基算法攻击下的计算复杂度。通过分析可知，只要参数选择恰当，该改进方案也能够抵御秩攻击和XL&Gröbner基算法攻击。因此，该改进方案是一种安全的多变量公钥加密方案。

关 键 词 有限域; 高阶线性化方程; MFE; 多变量公钥密码
中图分类号 TP309 文献标识码 A

Improved Medium-Field Multivariate Public Key Encryption Scheme

WANG Zhi-wei[1]，ZHENG Shi-hui[1]，YANG Yi-xian[1]，ZHANG Zhi-hui[2]

(1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications Haidian Beijing 100876; 2. SONY China Research Laboratory Haidian Beijing 100080)

Abstract In this paper, we design an improved MFE multivariate public key encryption scheme, which can resist the HOLE attack. There are other two attacks on MPKCs, the Rank attack and XL the &Gröbner basis attack. We provide the computational complexity under the Rank attack and XL&Gröbner basis attack. Through analysis, if we choose proper values of parameters, this improved scheme can resist both the Rand attack and the XL&Gröbner basis attack. Thus, this improved scheme is a secure multivariate public key encryption scheme.

Key words finite field; high order linearization equation; MFE; multivariate public key cryptosystem

近年来，公钥密码体制得到了迅猛的发展，涌现了RSA等一批基于因子分解和离散对数问题的公钥密码体制。文献[1]提出了一种攻击方法，利用量子计算机在多项式时间内解决因子分解和离散对数问题。这给密码学研究人员提出了一个新问题，如何构造新的公钥密码体制，使其能抵御未来基于量子计算机的攻击方法。多变量公钥密码体制是研究方向之一，它利用有限域上的多变量方程集合，通常是二次多变量方程集合，作为密码体制的公钥。它的设计基于一个NP-C问题，即求解一个在有限域上的非线性多变量方程组是困难的。

文献[2]提出了一种Medium-Field型的多变量公钥加密方案。与其他的多变量公钥密码加密方案相比，MFE加密方案的优点如下：(1) MFE方案从“小域”到“大域”的扩张次数非常少，使公钥长度和计算复杂度大大降低。这也是Medium Field的由来。(2) MFE方案的中心映射采用类似Tame映射的形式，使密钥的生成更高效。

文献[3]利用高阶线性化方程攻破了该方案，并提出了高阶线性化方程攻击(HOLE)的概念。

本文分析了文献[2-3]的方案，提出了一种能抗击高阶线性化方程攻击的新MFE方案，并进行了安全性分析。

1 MFE公钥加密方案[2]

设 K 是一个“小域”，L 是其 r 次扩域。定义一个K线性同构为 $\pi: L \to K^r$，取 L 在 K 上的一组基为 $(\theta_1, \theta_2, \cdots, \theta_r)$，$\pi$ 定义为 $\pi(a_1\theta_1 + a_2\theta_2 \cdots + a_r\theta_r) = (a_1, a_2, \cdots, a_r)$，$a_1, a_2, \cdots, a_r \in K$，$\pi_1: L^{12} \to K^{12r}$ 和 $\pi_2: L^{15} \to K^{15r}$。

MFE方案的私钥由两个可逆的仿射变换 ϕ_1 和 ϕ_3 组成，分别定义在 K^{12r} 和 K^{15r} 上。$\phi_2: L^{12} \to L^{15}$ 是一个中心映射，作为MFE的主要部分。公钥由15r 个多变量方程组成，这些多变量方程由 $\phi_3 \circ \pi_2 \circ \phi_2 \circ \pi_1^{-1} \circ \phi_1$ 构造而得。中心映射 $\phi_2(X_1, X_2, \cdots, X_{12}) = (Y_1, Y_2, \cdots, Y_{15})$，$Y_i$ 可表示为：

收稿时间：2007 – 08 – 20
基金项目：国家自然科学基金(90604022)；国家重点基础研究发展规划项目(2007CB310704)
作者简介：王志伟(1977 –)，男，博士生，主要从事信息安全与密码学方面的研究.

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1 \\ Y_2 = X_2 + X_9X_{12} + X_{10}X_{11} + Q_2 \\ Y_3 = X_3 + X_1X_4 + X_2X_3 + Q_3 \\ Y_4 = X_1X_5 + X_2X_7 \qquad Y_5 = X_1X_6 + X_2X_8 \\ Y_6 = X_3X_5 + X_4X_7 \qquad Y_7 = X_3X_6 + X_4X_8 \\ Y_8 = X_1X_9 + X_2X_{11} \qquad Y_9 = X_1X_{10} + X_2X_{12} \\ Y_{10} = X_3X_9 + X_4X_{11} \qquad Y_{11} = X_3X_{10} + X_4X_{12} \\ Y_{12} = X_5X_9 + X_7X_{11} \qquad Y_{13} = X_5X_{10} + X_7X_{12} \\ Y_{14} = X_6X_9 + X_8X_{11} \qquad Y_{15} = X_6X_{10} + X_8X_{12} \end{cases} \tag{1}$$

式中　Q_1、Q_2、Q_3 构成一个3元组(Q_1,Q_2,Q_3)，是从 K^{3r} 到自身的三角形映射。

MFE方案的加密过程是对公钥多变量方程组赋值的过程，解密过程则是依次计算 $\phi_1^{-1}\circ\pi_1\circ\phi_2^{-1}\circ\pi_2^{-1}\circ\phi_3^{-1}$。关键在于如何计算 ϕ_2 的逆，可以利用 ϕ_2 的三角形结构来解决，方法如下：$X_1,X_2,\cdots,X_{12}$，Y_4，$Y_5,\cdots,Y_{15}$ 是六个 2×2 的矩阵，即：

$$\boldsymbol{M}_1=\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \qquad \boldsymbol{M}_2=\begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}$$

$$\boldsymbol{M}_3=\begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix} \quad \boldsymbol{Z}_3=\boldsymbol{M}_1\boldsymbol{M}_2=\begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}$$

$$\boldsymbol{Z}_2=\boldsymbol{M}_1\boldsymbol{M}_3=\begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix}$$

$$\boldsymbol{Z}_1=\boldsymbol{M}_2^{\mathrm{T}}\boldsymbol{M}_3=\begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix} \tag{2}$$

则有：

$$\begin{cases} \det(\boldsymbol{M}_1)\cdot\det(\boldsymbol{M}_2)=\det(\boldsymbol{Z}_3) \\ \det(\boldsymbol{M}_1)\cdot\det(\boldsymbol{M}_3)=\det(\boldsymbol{Z}_2) \\ \det(\boldsymbol{M}_2)\cdot\det(\boldsymbol{M}_3)=\det(\boldsymbol{Z}_1) \end{cases}$$

当$\boldsymbol{M}_1$、$\boldsymbol{M}_2$、$\boldsymbol{M}_3$都可逆时，可以从中求得 $\det(\boldsymbol{M}_1)$, $\det(\boldsymbol{M}_2)$ 和 $\det(\boldsymbol{M}_3)$。若 $\det(\boldsymbol{M}_1)=(\det(\boldsymbol{Z}_2)\cdot\det(\boldsymbol{Z}_3)/\det(\boldsymbol{Z}_1)^{1/2})$；则有：

$$\begin{cases} Y_1 = X_1 + \det(M_2) + Q_1 \\ Y_2 = X_2 + \det(M_3) + Q_2 \\ Y_3 = X_3 + \det(M_1) + Q_3 \end{cases}$$

从上式可以解出 X_1,X_2,X_3；从 $X_1X_4+X_2X_3=\det(\boldsymbol{M}_1)$ 可以求得 X_4；从式(2)中的方程可以依次求出 $X_5,X_6,\cdots,X_{12}$。

2　攻击方法

文献[3]利用高阶线性化方程(二阶)有效地攻击了MFE方案。

$\boldsymbol{M}^*$ 是一个二阶矩阵的伴随阵。从式(2)可得 $\boldsymbol{Z}_3=\boldsymbol{M}_1\boldsymbol{M}_2$，$\boldsymbol{Z}_2=\boldsymbol{M}_1\boldsymbol{M}_3$；又由 $\boldsymbol{M}_3\boldsymbol{M}_3^*\boldsymbol{M}_1^*\boldsymbol{M}_1\boldsymbol{M}_2=\boldsymbol{M}_3(\boldsymbol{M}_1\boldsymbol{M}_3)^*(\boldsymbol{M}_1\boldsymbol{M}_2)=\boldsymbol{M}_3\boldsymbol{Z}_2^*\boldsymbol{Z}_3$ 和 $\boldsymbol{M}_3\boldsymbol{M}_3^*\boldsymbol{M}_1^*\boldsymbol{M}_1\boldsymbol{M}_2=(\boldsymbol{M}_3\boldsymbol{M}_3)^*(\boldsymbol{M}_1\boldsymbol{M}_1^*)\boldsymbol{M}_2=\det(\boldsymbol{M}_3)\det(\boldsymbol{M}_1)\boldsymbol{M}_2=\det(\boldsymbol{Z}_2)\boldsymbol{M}_2$ 可得一个矩阵方程为 $\boldsymbol{M}_3\boldsymbol{Z}_2^*\boldsymbol{Z}_3=\det(\boldsymbol{Z}_2)\boldsymbol{M}_2$。从对应的矩阵元素可得：

$$\sum a'X_iY_jY_k=0 \tag{3}$$

如果将所有对应值代入式(3)中的 Y_i，就可以得到域 L 上四个关于 X_i 的线性方程，即可获得域 K 上的 $4r$ 个方程，这些方程对于明文分量是线性的。

在唯密文攻击中，将密文分量代入方程组中，得到 $8r$ 个关于明文分量的线性方程组。文献[3]将变量个数变得足够小，以此使用 Gröbner 基方法来求解该方程组。

文献[3]还提出了高阶线性化方程的概念，即方程中的明文分量是线性的，而密文分量是高次的，密文分量的次数即为高阶线性化方程的阶数。它是针对多变量密码体制的一种通用攻击，只要能从多变量密码体制的中心映射中构造出高阶线性化方程，则该体制就有可能被攻破。

3　改进的MFE公钥加密方案

本文对MFE方案进行了设计，K、L、π 如上述定义，$l=|L|$，$\pi_1:L^8\to K^{8r}$ 和 $\pi_2:L^{10}\to K^{10r}$。新方案的私钥仍由两个可逆的仿射变换 ϕ_1 和 ϕ_3 组成，分别定义在 K^{8r} 上和 K^{10r} 上。$\phi_2(X_1,X_2,\cdots,X_8)=(Y_1,Y_2,\cdots,Y_{10})$ 是中心映射，需要重新设计。Y_i 为：

$$\begin{cases} Y_1 = X_1 + X_5X_8 + X_6X_7 + Q_1 \\ Y_2 = X_2 + X_1X_4 + X_2X_3 + Q_2 \\ Y_3 = X_1X_5 + X_2X_7 \qquad Y_4 = X_1X_6 + X_2X_8 \\ Y_5 = X_3X_5 + X_4X_7 \qquad Y_6 = X_3X_6 + X_4X_8 \\ Y_7 = X_1X_5 + X_3X_7 \qquad Y_8 = X_2X_5 + X_4X_7 \\ Y_9 = X_1X_6 + X_3X_8 \qquad Y_{10} = X_2X_6 + X_4X_8 \end{cases} \tag{4}$$

ϕ_2 除了 Q_1 和 Q_2 以外都是固定的，Q_1 和 Q_2 可以随机选择系数。Q_1 和 Q_2 构成一个二元组，是一个从 K^{2r} 到自身的三角形映射，定义类似于文献[2]。

定义 2×2 矩阵上的运算符“ $\tilde{}$ ”为 $\boldsymbol{M}^{\tilde{x}}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\tilde{x}}=\begin{pmatrix} a^x & b^x \\ c^x & d^x \end{pmatrix}$，在域 L 上，$\det(\boldsymbol{M}^{\tilde{l}})=(\det\boldsymbol{M})^l$。

将 $X_1,X_2,\cdots,X_8$，$Y_3,Y_4,\cdots,Y_{10}$ 写成4个2×2的矩阵为：

$$\boldsymbol{M}_1=\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix} \qquad \boldsymbol{M}_2=\begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}$$

$$\boldsymbol{Z}_1=\boldsymbol{M}_1^{\tilde{l}}\boldsymbol{M}_2=\begin{pmatrix} Y_3 & Y_4 \\ Y_5 & Y_6 \end{pmatrix} \qquad \boldsymbol{Z}_2=\boldsymbol{M}_2^{\mathrm{T}}\boldsymbol{M}_1=\begin{pmatrix} Y_7 & Y_8 \\ Y_9 & Y_{10} \end{pmatrix} \tag{5}$$

由于在域 L 上 $X_i^l = X_i$，所以 ϕ_2 可由式(4)求出。加密过程也是对公钥多变量多项式赋值的过程；解密过程相对复杂，仍是依次计算 $\phi_1^{-1} \circ \pi_1 \circ \phi_2^{-1} \circ \pi_2^{-1} \circ \phi_3^{-1}$，关键在于求 ϕ_2^{-1}，则有：

$$\begin{cases} [\det(\boldsymbol{M}_1)]^l \cdot \det(\boldsymbol{M}_2) = \det(\boldsymbol{Z}_1) \\ \det(\boldsymbol{M}_2) \cdot \det(\boldsymbol{M}_1) = \det(\boldsymbol{Z}_2) \end{cases} \tag{6}$$

由式(6)可以推出：

$$\det(\boldsymbol{M}_1) = \sqrt[l-1]{\left[\frac{\det(\boldsymbol{Z}_1)}{\det(\boldsymbol{Z}_2)}\right]} \tag{7}$$

$$\det(\boldsymbol{M}_2) = \frac{\det(\boldsymbol{Z}_2)}{\det(\boldsymbol{M}_1)} \tag{8}$$

通过解 K^{2r} 上的三角形映射 $Y_1 = X_1 + \det(\boldsymbol{M}_2) + Q_1$，$Y_2 = X_2 + \det(\boldsymbol{M}_1) + Q_2$，可以求出 X_1、X_2。求解 $X_3, X_4, \cdots, X_8$ 的方法如下：先计算 $A = (\det \boldsymbol{M}_2)^{-1}$，则有：

$$\begin{cases} X_3 = (Y_7 X_6 + Y_9 X_5) A \\ X_4 = (Y_8 X_6 + Y_{10} X_5) A \\ X_2 = (Y_3 X_6 + Y_4 X_5) A \\ \det(\boldsymbol{M}_1) = X_1 X_4 + X_2 X_3 \end{cases} \tag{9}$$

由式(9)可以解出 X_3、X_4、X_5、X_6；从 $Y_7 = X_1 X_5 + X_3 X_7$ 可解出 X_7；从 $Y_9 = X_1 X_6 + X_3 X_8$ 可解出 X_8。

4 安全性分析

目前，针对多变量密码体制的攻击主要有线性化方程攻击(包括高阶)、秩攻击和 XL&Gröbner 基攻击三种。

4.1 线性化方程攻击

文献[4]提出线性化方程攻击，用于攻击 C^* 体制。文献[3]将线性化方程攻击推广到高阶线性化方程攻击，即线性化方程中允许密文变量出现高阶，但明文变量必须是线性的。

判断一个多变量密码体制是否存在线性化方程，即是判断其中心映射中是否存在线性化方程。由于本文所述的中心映射结构比较复杂，所以采取的判断方法是随机选取足够多的明文和密文对；将其代入待定系数的线性化方程中，得到一组关于系数的线性方程组。对于一阶线性方程和二阶线性化方程，所得的关于系数的线性方程组不能得到非零解，所以改进方案能抵御一阶线性方程攻击和二阶线性化方程攻击。对于更高阶的线性化方程，本文不再测试，因为此时即使存在线性化方程，其攻击复杂度已超过了 2^{80}。

4.2 秩攻击

文献[5]提出秩攻击，用于攻击HFE[6]。文献[7]用它来攻击TPM方案。文献[8]总结了秩攻击方法，分为低秩攻击和高秩攻击：(1) 低秩攻击，其计算复杂度为 $q^{uv}(m^2(nu/2 - m/6) + mn^2u)$。其中，$q$ 为 K 的大小；u 为中心映射各方程在基本域上线性组合的最小阶；m 为方程个数；n 为变量个数；$v = \lceil m/n \rceil$。在本文的改进方案中，可选 $q = 2^8$、$u = 2r$、$v = 2$，所以当 $r \geq 3$ 时，低秩攻击的计算复杂度超过 2^{90}。(2) 高秩攻击，其计算复杂度为 $q^w(wn^2 + n^3/6)$，w 为任意变量在中心映射各方程中出现的最小次数。在本文的改进方案中，$w = 4r$，所以当 $r \geq 3$ 时，高秩攻击的计算复杂度超过 2^{90}。

4.3 XL & Gröbner 基攻击

XL 算法是一种求解多变量多项式方程组的方法[9]，其复杂度为 $\left(n^{\sqrt{n}}/\sqrt{n}!\right)^{\omega}$ (使用普通高斯消元法时 $\omega = 3$，使用改进算法时 $\omega = 2.376\ 6$)[5]。对于本文的改进方案，当 $r \geq 4$、$n \geq 40$，XL 算法的复杂度应超过 2^{80}。

Gröbner 基算法是一类求解多变量方程组的方法，其中最快的是F5、F4算法。F5算法[10]的复杂度为 $2^{0.873n}$。对于本文的改进方案，$r \geq 10$、$n \geq 100$，F5算法的复杂度应超过 2^{80}。综上所述，本文的改进方案能抵御线性化方程攻击(包括高阶)，并且只要将系数 r、q 选取适当，也能够抵御秩攻击和 XL&Gröbner 基攻击，是一种安全的加密方案。

5 结 论

本文提出了一个改进的MFE多变量公钥加密方案。通过分析得出本文的方案是安全的，它不仅能抵抗高阶线性化方程攻击，而且能抵御另外两种现有的针对多变量密码体制的攻击。今后将进一步研究提高这个方案效率的方法。

参 考 文 献

[1] SHOR P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Rev, 1999, 41(2): 303-332.

[2] WANG Lih-chung, YANG Bo-yin, HU Yuh-hua, et al. A medium-field multivariate public key encryption scheme [C]//CT-RSA 2006. Heidelberg: Springer, 2006, LNCS 3806: 132-149.

[3] DING Jin-tai, HU Lei, NIE Xu-yun, et al. High oder linearization equation(hole) attack on multivariate public key cryptosystems[C]//PKC 2007. Heidelberg: Springer, 2007, LNCS 4450: 233-248.

[4] PATARIN J. Cryptanalysis of Matsumoto and Imai public key scheme of eurocrypt'88[C]//CRYPTO. Heidelberg: Springer, 1995, LNCS 963: 248-261.

(下转第1159页)

5 总　结

自组网络的安全机制有自身的特点，其密钥分配和管理一直是研究的热点问题之一。本文在随机密钥预分配方案基础上，通过引入分簇方案，提出基于簇的自组网络密钥预分配方案，并进行了性能分析，其性能相比随机密钥预分配方案有一定提高。

参　考　文　献

[1] RAM R, JASON R. A brief overview of mobile Ad Hoc networks: challenges and directions [J]. IEEE Communications Magazine, 2002, 40(5): 20-22.

[2] CARMAN D W, KRUUS P S, MATT B J. Constraints and ap-proaches for distributed sensor security. [2007-07-08]. [J/OL]. http://www.cs.umbc.edu/courses/graduate.

[3] NEUMAN B C, TSO T K. An authentication service for computer networks IEEE Communications[J]. 1994, 32(9): 33-38.

[4] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. Washington: [s.n.], 2002: 4l-47.

[5] CHAN H, PERRIG A, SONG D. Random key edist rjbuti0n schem es for sensor networks[C]//The Proceedings of the IEEE Symposium on Security and Privacy, Berkeley. California: IEEE, 2003: 197-213.

[6] 刘志宏, 马建峰, 黄启萍. 基于区域的无线传感器网络密钥管理[J]. 计算机学报, 2006, 29(9): 1608-1616.

[7] 章　静, 许　力, 林志伟. 自组网中基于簇的混合密钥管理策略[J]. 计算机应用, 2006, 26(6): 1328-1330.

[8] CHEN Jiang-wei, LI Xu, YI Mu. A new group rekeying scheme based on t-packing designs for Ad Hoc networks [M/CD]. The Proceeding of INFOSCALE2007. ACM Press. 2007.

[9] SUNG J C, HEE Y Y. An efficient key pre-distribution scheme for secure distributed sensor networks[C]//EUC 2005 workshops, Lecture Notes in Computer Science.[S. l.]: Springer-Verlag, 2005, 3823: 1088-1097.

[10] LIN Zhi-wei, LI Xu, WANG Da-jin, et al. A coloring based backbone construction algorithm in wireless Ad hoc network[C]//Advances in Grid and Pervasive Computing. The Proceedings of GPC 2006, Lecture Notes in Computer Science. [S. l.]: Springer Press, 2006.

编　辑　税　红

(上接第1154页)

[5] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE public key cryptosystem by relinearization[C]//CRYPTO 1999. Heidelberg: Springer, 1999, LNCS 1666: 19-30.

[6] PATARIN J. Hidden field equations and isomorphisms of polynomials: two new families of asymmetric algorithms[C]//EUROCRYPT 1996. Heidelberg: Springer, 2007, LNCS 1070: 33-48.

[7] GOUBIN L, COURTOIS N. Cryptanalysis of the TTM cryptosystem[C]//ASIACRYPT 2000. Heidelberg: Springer, 2000, LNCS 1976: 44-57.

[8] YANG B, CHEN J. Building secure tame-like multivariate public key cryptosystems the new TTS[C]//ACISP 2005. Heidelberg: Springer, 2005, LNCS 3574: 518-531.

[9] COURTOIS N, KLIMOV A, PATARIN J, et al. Efficient algorithms for solving overdefined systems of multivariate polynomial equations[C]//EUROCRYPT 2000. Heidelberg: Springer, 2000, LNCS 1807: 392-407.

[10] YANG B-Y, CHEN J, COURTOIS N. On asymptotic security estimates in XL and Gröbner bases-related algebraic cryptanalysis[C]//ICICS-2004. Heidelberg: Springer, 2004, LNCS 3269: 401-413.

编　辑　黄　莘