计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190900154

三次 MI 多变量公钥密码体制的安全性分析

张 栖 聂旭云
电子科技大学信息与软件工程学院 成都 610054
网络与数据安全四川省重点实验室 成都 610054
(1106845293@qq.com)

摘 要 三次 MI 多变量公钥签名体制是经典的多变量密码体制 MI 体制的改进。通过增加中心映射的次数,将公钥多项式从二次提升到三次来抵抗针对 MI 体制的线性化方程攻击。文中声称其体制的中心映射虽然满足二次化方程,但对其安全性没有影响。然而经过实验分析,对于以其中心映射构造的公钥加密体制,在找到所有的二次化方程后,结合 Grobner 基方法即可快速恢复合法密文相应的明文。同时,分析表明其方案实例抵抗最小秩攻击的时间复杂度并没有达到作者声称的 $O(2^{222})$,仅仅只有 $O(2^{129})$。

关键词:多变量公钥密码体制;二次化方程;秩攻击;MI
中图法分类号 TP309.7

Cryptanalysis of Cubic MI Multivariate Public Key Signature Cryptosystem

ZHANG Qi and NIE Xu-yun
University of Electronic Science and Technology of China, Sichuan Key Laboratory of Network and Data Security, Chengdu 610054, China
Sichuan Key Laboratory of Network and Data Security, Chengdu 610054, China

Abstract Cubic MI multivariate public key cryptosystem is an improvement of the classical multivariate public key cryptosystem MI. By increasing the degree of central mapping, the degree of public polynomial is promoted from quadratic to cubic to resist the Linearized Equation attack against MI system. The authors claim that the central mapping of the system satisfies the quadratic equation but has no effect on its security. However, through experimental analysis, for the public key cryptography constructed by its central mapping, after finding all the quadratic equations, the corresponding plaintext of the valid ciphertext can be recovered quickly by combining with the Grobner basis method. Simultaneously, it is also found that the complexity of the scheme instance to resist the minimum rank attack does not reach $O(2^{222})$, but only $O(2^{129})$.

Keywords Multivariate public key cryptosystem, Quadratization equation, Rank attack, MI

1 引言

多变量公钥密码(Multivariate Public Key Cryptosystem, MPKC)是抗量子攻击候选公钥密码候选方案之一。它的安全性主要基于求解有限域上随机产生的多变量多项式方程组的困难问题和多项式同态问题。

自 1988 年 Matsumoto 等[1]提出一个具有里程碑意义的 MI(Matsumoto-Imai)多变量公钥密码体制后,多变量公钥密码的设计与安全性分析吸引了较多密码研究者的关注。1995 年,Patarin 指出 MI 体制满足一阶线性化方程,并针对漏洞,提出了 HFE(Hide Field Equations)[2]体制。1998 年 Patarin 等在 MI 体制基础上使用减方法进行改进,即 C^{*-}[3]体制。SFLASH 就是在 C^{*-} 中确定具体参数后的方案,该方案在 2003 年被 NESSIE 选入 3 种推荐公钥签名方案之一。2007 年,Dubois 等在文献[4]中提出了差分攻击,并且用这种攻击成功破解了 SFLASH。2008 年,Ding 等使用投射方法[5]对 SFLASH 方案进行改进,并证明该方法破坏了公钥中存在的差分对称性,从而能够抵抗差分攻击。2016 年,Qiao 等提出一种扩展多变量公钥密码体制(Novel Extend Multivariate Public Key Cryptosystem, EMC)[6],并将其应用于 MI 体制来抵抗线性化方程攻击。2018 年,Lu 等[7]指出这种增强体制满足二次化方程,在找到所有二次化方程后,可恢复合法密文所对应的明文。

最小秩攻击是分析多变量公钥密码体制安全性的常用工具。这一类攻击最早是由 Kipnis 等[8]提出用于分析 HFE 加密体制的安全性。2013 年,Bettale 等[9]改进了 Kipnis 等的攻击方法,破解了 multi-HFE。2018 年,Baena 等[10]提出一种针对三次多变量公钥密码体制的最小秩攻击方法,将最小秩问题由二维扩展到了三维。

2012 年,Yuan 等提出了一种基于 MI 体制的改进方案[11]。通过增加中心映射的次数,将公钥多项式从二次提升到三次,从而可以避免原始 MI 体制中存在的线性化方程。

基金项目:国家自然基金重点国际(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)
This work was supported by Major International (Regional) Joint Research Project of China National Science Foundation (61520106007) and International Scientific and Technological Innovation Cooperation Project in Sichuan Province (20GJHZ0273).
通信作者:聂旭云(xynie@uestc.edu.cn)

Yuan 等声称该体制的中心映射虽然满足二次化方程，但对其安全性没有影响。然而经过实验分析，对于以其中心映射构造的公钥加密体制，在找到所有的二次化方程后，结合 Grobner 基方法即可快速恢复合法密文相应的明文。同时，我们对该方案进行了最小秩分析，实验结果证明，该体制的中心映射到小域上对应矩阵的秩为 108。因此，该方案抵抗最小秩攻击的复杂度仅为 $O(2^{129})$，远远小于文献[11]中声称 $O(2^{222})$。

本文第 1 节给出了多变量公钥密码的一般形式，以及经典攻击的相关预备知识；第 2 节给出了三次 MI 公钥签名方案的简要描述；第 3 节给出了详细的安全性分析以及具体的实验步骤和实验结果；最后总结全文。

2　预备知识

2.1　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，$F:k^n\to k^m$ 称为中心映射。$x=(x_1,\cdots,x_n)$ 为明文变量，$y=(y_1,\cdots,y_m)$ 为密文变量。令：

$$P:x\in\mathbb{K}^n\xrightarrow{T}u=M_1x+c_1\xrightarrow{F}$$

$$v=F(u)\xrightarrow{U}y=M_2v+c_2\in\mathbb{K}^m$$

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，通常为一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 $\phi:K\to k^n$。其中，K 为 k 的 n 次扩域，F 为 K 上的单变量多项式。公钥的形式如下：

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

2.2　二次化方程

二次化方程最早是由曹巍巍等[12]提出来分析改进的 MFE 加密体制。

定义 1(二次化方程)　令 $y_i=P_i(x_i,\cdots,x_n)$ 是多变量公钥密码体制的公钥函数，其中 $y_1,\cdots,y_m$ 和 $x_1,\cdots,x_n$ 分别是密文变量和明文变量。给定公钥，若明文和密文满足如下等式：

$$\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=1}^{m}a_{ijk}x_ix_jy_k+\sum_{i=1}^{n}\sum_{j=i}^{n}b_{ij}x_ix_j+$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m}c_{ij}x_iy_j+\sum_{i=1}^{n}d_ix_i+\sum_{i=1}^{m}e_iy_i+f=0$$

给定密文变量的值，该方程就变成只含明文变量的二次多项式方程，则称该密码体制满足二次化方程。按照密文变量的次数，我们把二次化方程称为一阶二次化方程和高阶二次化方程。如果可以找到足够多的二次化方程，代入要破解的合法密文，攻击者就可以得到明文变量的二次多项式方程组。将所有得到的二次多项式方程与公钥方程组成新的方程组，再用 Groebner 基方法进行求解，就可以得到合法密文对应的明文。对于如何确定明文变量和密文变量是否存在二次化方程，我们根据以下两个性质来判断。

性质 1　令 $k=GF(q)$ 是一个 q 元域，$K=GF(q^n)$ 为 k 的 n 次扩域，设函数 $\pi:K\to k^n$ 是域 K 到 k^n 的 k-线性同构。映射 $Y=F(X)$ 是定义在域 K 上的函数，且满足：

$$\pi(Y)=(y_1,\cdots,y_n),\pi(X)=(x_1,\cdots,x_n)$$

如果 X 和 Y 满足二次化方程，则 x_i 和 $y_i(1\leqslant i\leqslant n)$ 也满足同阶的二次化方程。

性质 2　给定一个多变量公钥体制，如果其中心映射 $Y=F(X)$ 满足二次化方程，则其明文和密文也满足同阶的二次化方程。$(u_1,\cdots,u_m)$ 和 $(v_1,\cdots,v_n)$ 满足如下方程：

$$\sum_{1\leqslant i\leqslant j\leqslant n}a_{ij}v_iv_jg_{ij}(u_1,\cdots,u_m)+h(u_1,\cdots,u_m)+c=0$$

2.3　最小秩攻击

定义 2(最小秩问题)　给定正整数 m,n,r,k 及 k 个矩阵 $M_0,\cdots,M_k\in M_{m\times n}(k)$，确定是否存在一组系数 $\lambda_1,\cdots,\lambda_k\in k$，使得矩阵的线性组合 $\sum_{i=1}^{k}\lambda_iM_i-M_0$ 的秩小于或等于 r。

这是一个 NP-困难问题。在 r 较小时，问题可解。

多变量二次多项式的齐二次项的系数可用一个对称矩阵来表示。对于多变量公钥密码体制来说，中心映射对应的矩阵可以表示成公钥对应矩阵的线性组合。如果中心映射对应矩阵的秩较低，那么通过求解最小秩问题可恢复体制的私钥。Kipnis 等首先利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 $P=U\circ\phi\circ F\circ\phi^{-}\circ T$，$P$ 是已知的公钥，U,T 和 F 是未知的私钥。文献[8]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：

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

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

$$\sum_{k=0}^{n-1}u_kP^{*k}=P'=T^*FT^{*t}$$

如果矩阵 $\boldsymbol{f}$ 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。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。

大部分多变量公钥密码体制都可以用最小秩攻击来分析，如 TTM[12]、HFE 及其变体等。为了抵抗最小秩攻击，必须提高体制中心映射对应矩阵的秩或者增大体制的参数以提高最小秩攻击的复杂度。

2.4　MI 加密方案

MI 体制的中心映射选取的是 q 元有限域的 n 次扩域上的单变量映射 $F(X)=X^{q^\theta+1}$，其中 $1\leqslant\theta\leqslant n$，满足 $\gcd(q^\theta+1,q^n-1)=1$。令 $\phi:K\to k^n$ 是一个线性同构，利用该同构映射及它的逆，可以将大域 K 上的中心映射 F 变为小域 k 上的映射 $f=\phi\circ F\circ\phi^{-}$ 和多变量公钥密码系统一般形式一样，它的公钥 $P=U\circ f\circ T=U\circ\phi\circ F\circ\phi^{-}\circ T$，私钥为仿射变换 U,T 和 F。对明文变量加密是通过计算 $P(x)=y$ 来完成的，解密是通过分别对这 3 个映射 F,U,T 的求逆完成的。

3　三次 MI 多变量公钥签名体制简介

令 k 为特征值为 2 的有限域，K 是 k 扩张次数为 n 的扩域。$\phi:K\to k^n$ 是标准 k-线性同构，ϕ^{-1} 为它的逆。三次 MI 签名体制的中心映射为 $F:Y=X^{q^\theta+3}$，其中 $n=2\theta+1$，满足 $t(2^\theta+3)\equiv1\bmod(2^n-1)$。

三次 MI 多变量公钥签名体制的公钥 $P:k^{n-s}\to k^{n-r}$，定义为：

$$(y_1,\cdots,y_{n-r})=P(x_1,\cdots,x_{n-s})$$
$$=T^-\circ\phi\circ F\circ\varphi^-\circ U^-(x_1,\cdots,x_n)$$

其中，$T^-:k^n\to k^{n-r}$ 定义为仿射变换 $T:k^n\to k^n$ 在最后 r 个坐标的投射，$U^-:k^{n-s}-k^n$ 定义为仿射变换 $U:k^n\to k^n$ 在最后 s 个坐标的约束。该多变量公钥密码体制的公钥为加密函数 P，私钥为仿射变换 U 和 T。考虑到签名验证效率及安全性，文献[11]给出的建议参数为 $q=2$，$n=111$，$\theta=55$，$r=33$，$s=3$。注意，当 $r=0$，$s=0$ 时，该体制为加密方案。

4 三次 MI 多变量公钥密码体制的二次化方程分析

三次 MI 体制的中心映射通过提高变量次数来避免 MI 体制中存在线性化方程。Yuan 等发现该体制的中心映射满足二次化方程，形式如下：

$$\begin{aligned}&Y=X^{q^\theta+3}\\&\Rightarrow YX^{-2}=X^{q^\theta+1}\\&\Rightarrow(YX^{-2})^{q^\theta-1}=X^{q^{2\theta}-1}\\&\Rightarrow Y^{q^\theta}X^{2-q^\theta+1}=X^{q^{2\theta}}Y\\&\Rightarrow Y^{q^\theta}X^2=X^{q^{2\theta}+q^{\theta+1}}Y\end{aligned}$$

文献[11]中声称该方程对其中心映射构造的密码体制的安全性没有影响。然而经过实验分析，对于该中心映射构造的公钥加密体制，给定公钥，在找到所有二次化方程后，结合 Grobner 基方法即可快速恢复合法密文相应的明文。

4.1 二次化方程

根据三次 MI 加密体制中心映射满足的二次化方程，结合性质 1 和性质 2 可知，明密文变量也满足同阶的二次化方程组，形式如下：

$$\sum_{i=1}^{n}\sum_{j=1}^{i}\sum_{k=1}^{m}a_{ijk}x_ix_jy_k+\sum_{i=1}^{n}\sum_{j=1}^{m}b_{ij}x_iy_j+\sum_{i=1}^{n}\sum_{j=1}^{i}c_{ij}x_ix_j+\sum_{j=1}^{m}e_jy_j+f=0 \tag{1}$$

为了完成攻击，需要找到所有的二次化方程。找到一个二次化方程意味着找到它所有的系数。令所有的二次化方程的系数向量生成的线性空间为 V，它的维数记为 D。因此，找到所有的二次化方程等价于找到该空间的一组基。方程(1)中的系数个数为：

$$\Omega=\frac{n^2(n+1)}{2}+\frac{n(n+1)}{2}+n^2+1$$

利用公钥生成比 Ω 略多的明密文对，代入二次化方程，得到一组关于二次化方程系数的方程组。求解该方程组，得到解空间的一组基，也就得到了 D 个线性无关的二次化方程。将要破解的合法密文代入这组基方程中，即可得到关于明文的二次多项式方程。

上述过程与要破解的密文无关，给定公钥后可以进行预计算。

4.2 唯密文攻击

给定公钥 $y_i=P_i(x_1,\cdots,x_n)$，$1\leqslant i\leqslant m$ 和合法密文 $(y_1',\cdots,y_m')$，明文恢复攻击的目的是通过求解如下方程组来恢复明文：

$$y_i'=P_i(x_1,\cdots,x_n),1\leqslant i\leqslant m \tag{2}$$

由方程组(2)可知，变量个数固定，线性无关的方程个数越多，方程组就越容易求解。

在得到所有二次化方程后，将需要破解的密文代入到这些方程中，可得到一个关于明文变量的多变量二次方程组，即：

$$\sum_{i=1}^{n}\sum_{j=i}^{n}a_{i,j}^{(k)}x_i'x_j'+\sum_{i=1}^{n}b_i^{(k)},x_i'+c^{(k)}=0$$

将上述方程组合并到方程组(2)中得到一个新的方程组，用 Grobner 基方法求解新方程组。实验结果表明，对新的方程组求解所需要的时间比直接求解方程组(2)更短。这是因为变量个数固定，方程个数的增加可以降低 Grobner 基求解过程的正则次数 d_{reg}。其中，d_{reg} 是衡量 Grobner 基求解方法计算复杂度的关键参数。

4.3 实验步骤及结果

该实验是在普通 PC 机上使用 MAGMA 完成的。具体步骤如下：

步骤 1 计算二次化方程的系数个数：

$$\frac{n^2(n+1)}{2}+\frac{n(n+1)}{2}+n^2+1=\frac{n^3}{2}+2n^2+\frac{n}{2}+1$$

步骤 2 由给定的公钥生成比系数个数略多的明密对，如 $\frac{n^3}{2}+2n^2+\frac{n}{2}+10$(记为 N)组明密对。将这些明密对代入方程(1)，得到 N 个变量组成的线性化方程，求解该线性方程组的复杂度为 $O(N^3)$。

步骤 3 在求出这 D 个线性无关的二次化方程后，将需要求解的密文代入，通过高斯消元，得到 D 个关于明文变量的线性无关的二次多项式方程。

步骤 4 将这 D 个二次多项式方程与公钥多项式合并，得到 D' 个以明文变量为未知量的二次多项式方程组，最后使用 Grobner 基算法求解，可以快速恢复明文。

实验中，由于内存的限制，n 大小不超过 30。$q=2$ 时，选取不同的 n 和 θ 来进行实验，并对实验各个环节的时间进行了统计，如表 1 所列。

表 1 不同参数下二次化方程破解时间的比较

Table 1 Comparison of cracking time of quadratic equation under different parameters

q	n	θ	D	T1/s	T21/s	T31/s
2	15	7	303	3.69	0.26	0.03
2	19	9	472	13.38	0.93	0.04
2	23	11	687	74.75	6.53	0.05
2	27	13	916	192.41	19.51	0.06

注：T1 为生成明密对时间；T2 为得到二次化方程的时间；T3 为 Grobner 求解的时间

5 MI 体制及其变体的最小秩攻击分析

Ding 等[13] 使用原始的 Kipnis-Shamir 方法在大域上对 MI 进行了安全性分析，并得出 MI 体制中心映射对应矩阵的秩为 2。

本节对该攻击方法进行了优化，并通过实验验证了在小域上进行最小秩攻击的计算复度要远比在大域上的低。

5.1 原始 MI 体制的最小秩攻击分析

观察 $P=U\circ\phi\circ F\circ\phi^{-1}\circ T$，通过同构变换把大域上的中心映射降到小域上，即：

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

公式两边同时复合 U^{-1}，得到 $U^{-1}\circ P=\boldsymbol{f}\circ T$，由这个方程最终可以得到一个“基本方程”，表达式如下：

$$\sum_{i=1}^{n}u_iP_i=\boldsymbol{f}'=T\boldsymbol{f}T^t$$

如果矩阵 $\boldsymbol{f}$ 的秩 r 是有界的，那么 $\boldsymbol{f}'$ 的秩 r 也是有界的。当 r 确定后，恢复 u_i 就可以规约到最小秩问题的求解。与原

始的 K-S 攻击方法不同，优化的攻击方法没有通过再引入同构变换将公钥从小域提升到大域，而是将中心映射从大域映射到了小域。

5.2　实验步骤及结果

该实验是在普通 PC 机上用 MAGMA 完成的。给定 q，n，θ，从而确定秩 r。完整攻击步骤如下。

步骤 1　提取公钥对应矩阵 $P_i \in k^{n\times n}$。如果公钥是非齐次的，那么需要取公钥对应矩阵的子矩阵。

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

$$\begin{pmatrix} 1 & x_{1,1} & \cdots & x_{1,r} \\ \vdots & \vdots & & \vdots \\ 1 & x_{n-r,1} & \cdots & x_{n-r,r} \end{pmatrix}$$

矩阵行向量是线性无关的。设 $\lambda_1,\cdots,\lambda_{n-1}$ 为待定系数，公钥矩阵线性组合 $M=\sum_{i=1}^{n-1}\lambda_i P_i - P_0$。

步骤 3　对于确定的秩 r，解最小秩问题 $Rank(M)\leqslant r$ 等价于求解方程组 $KM\times M=0$。

实验中选取了不同的 q，n，θ 来进行对比。结果显示，秩 r 的大小只与参数 n 和 θ 有关，具体结果如表 2 所列。

表 2　不同参数下最小秩攻击的复杂度

Table 2　Complexity of minimum rank attack under different parameters

q	n	θ	r	$Cpx1$	$Cpx2$
2	33	16	32	$O(2^{48})$	$O(2^{66})$
2	33	21	30	$O(2^{46})$	$O(2^{66})$
2	35	21	28	$O(2^{44})$	$O(2^{70})$
4	33	16	32	$O(2^{81})$	$O(2^{133})$
4	33	21	30	$O(2^{77})$	$O(2^{133})$
4	35	21	28	$O(2^{73})$	$O(2^{141})$

注：Cpx1 为优化算法的复杂度；Cpx2 为原始算法的复杂度

5.3　三次 MI 体制的最小秩攻击分析

若要解决三次最小秩问题，首先要知道如何表示三维矩阵的秩。

定义 3（三维矩阵的秩）[8]　给定一个三维矩阵 $A\in F^{n\times m\times l}$，$A$ 的秩就是 r 个秩为 1 的二维矩阵 $S_1,\cdots,S_r\in F^{m\times l}$，使得对于所有的二维矩阵 $A[i,\cdot,\cdot]$，都属于由 $S_1,\cdots,S_r$ 所张成的线性空间。

给出三维矩阵的秩的表示，通过对 Kipnis-Shamir 模型的扩展，得到一个新的由二维矩阵组成的方程系统。

定义 4（Kipnis-Shamir 扩展模型）　给定一组三维矩阵 $M_0,\cdots,M_k\in F^{n\times n\times n}$，它们的线性组合 $A=\sum_{i=1}^{k}\lambda_i M_i - M_0$ 的秩为 r，那么根据定义 3，我们可以得到如下方程：

$$\sum_{j=1}^{r} a_{ij}S_j = A[i,\cdot,\cdot], i=1,\cdots,n \tag{3}$$

因为矩阵 S_i 的秩为 1，所以可令 $S_i=v_i u_i^{\mathrm{T}}$，代入式(3)中，得到一个方程系统如下：

$$\sum_{j=1}^{r} a_{ij}v_j u_j^{\mathrm{T}} = A[i,\cdot,\cdot], i=1,\cdots,n \tag{4}$$

与针对 MI 体制的攻击方法一样，我们使用同构变换把三次 MI 体制中心映射从大域降低到小域，最终可以得到一个“基本方程”，形式如下：

$$\sum_{i=1}^{n} u_i P_i = F' = TFT^t$$

如果这个线性组合的秩 r 是有界的，那么恢复 u_i 就可以规约到三次最小秩问题。

5.4　实验步骤及结果

该实验是在普通 PC 机上使用 MAGMA 完成的。在三次 MI 公钥方案中，作者选取的参数 $n=111$，$\theta=55$。完整的攻击步骤如下：

步骤 1　首先生成 $2(\theta+1)$ 个 n 维未知向量 $(v_1,\cdots,v_{\theta+1})$，$(u_1,\cdots,u_{\theta+1})$。按照脚标依次求两组向量的克罗内克积，得到一组秩为 1 的矩阵，表示为 $S_i=v_i u_i^{\mathrm{T}}$。

步骤 2　设 $(\lambda_i,\cdots,\lambda_{n-1})$ 为一组待定系数，对于给定的公钥矩阵 $M_0,\cdots,M_{n-1}\in F^{n\times n\times n}$，它们的线性组合表示为 $\boldsymbol{A}=\sum_{i=1}^{n-1}\lambda_i M_i - M_0$。

步骤 3　将三维矩阵 $\boldsymbol{A}$ 表示成 n 个二维矩阵 $\boldsymbol{A}[i,\cdot,\cdot]$，并和矩阵 $v_i u_i^{\mathrm{T}}$ 构造式(4)。该系统的方程个数为 $n^3=1\,367\,631$，变量个数为 $r\times 2n+r\times n+n-1=3rn+n-1$。

根据文献[11]，求解这个方程组的复杂度为：

$$O(q^{\lceil \frac{m}{n} \rceil r} m^3)$$

其中，$m=n=111$，$q=2$，$r=108$，复杂度为 $O(2^{129})$，远比文献[11]作者声称的复杂度 $O(2^{222})$ 低。

结束语　本文给出了三次 MI 体制的安全性分析，证明该体制的加密方案不能抵抗二次化方程的攻击。在找到所有二次化方程后，利用 Grobner 基可快速求解该方程。因此，在设计中心映射时需要避免二次化方程。同时还发现，该方案在小域上抵抗最小秩攻击的复杂度远比作者在大域上给出的复杂度低。需注意，本文中的攻击方法并不适合三次 MI 签名体制，将在后续工作中进一步进行分析。

参 考 文 献

[1] MATSUMOTO T, IMAI H. Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption [M]. Advances in Cryptology-EUROCRYPT'88, 1988: 419-453.

[2] PATARIN J. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms[C]// International Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1996: 33-48.

[3] PATARIN J, GOUBIN L, COURTOIS N. C−+* and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 1998: 35-50.

[4] DUBOIS V, FOUQUE P A, STERN J. Cryptanalysis of SFLASH with Slightly Modified Parameters[C]// Proceedings of the 26th annual international conference on Advances in Cryptology. Springer, 2007: 264-275.

[5] DING J, DUBOIS V, YANG B Y, et al. Could SFLASH be repaired? [C]// International Colloquium on Automata, Languages, and Programming. Springer-Verlag, 2009: 691-701.

[6] SHUAI T Q, HAN W B, LI Y F, et al. Construction of extended multivariate public key cryptosystems[J]. International Journal of Network Security, 2016, 18(1): 60-67.

[7] LU G, XUE L Y, NIE X Y, et al. Cryptanalysis of Novel Extended Multivariate Public Key Cryptosystem with Invertible Cycle[J]. International Journal of Network Security, 2018, 20(3): 509-514.

[8] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization[J]. Advances in Cryptology—CRYPTO'99, Lecture Notes in Computer Science, 1999, 1666: 19-30.

[9] BETTALE L, JEAN-CHARLES F, PERRET L. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic [J]. Designs, Codes and Cryptography, 2013, 69(1): 1-52.

[10] BAENA J, CABARCAS D, ESCUDERO D E, et al. Rank Analysis of Cubic Multivariate Cryptosystems [C] // International Conference on Post-quantum Cryptography. Springer, Cham, 2018: 355-374.

[11] YUAN F, ZHAO S, OU H, et al. A New Public Key Signature Scheme Based on Multivariate Polynomials[M] // Web Information Systems and Mining. Springer Berlin Heidelberg, 2012: 239-245.

[12] CAO W W, NIE X Y. Cryptanalysis of Two Quartic Encryption Scheme and One Improved MFE Scheme [C] // International Conference on Post — quantum Cryptography. Springer Berlin Heidelberg, 2010: 41-60.

[13] DING J, SCHMIDT D. Multivariate public key cryptosystems [M] // Springer Science Business Media. LLC, 2006: 44-63.

ZHANG Qi, born in 1994, master degree candidate. His main research interests include network security, multivariate public key cryptograghy.

NIE Xu-yun, born in 1975, Ph.D, associate professor. His main research interests include multivariate public key cryptography, big data security and privacy protection.

(上接第 343 页)

算法。但实时的网络安全状态评估与态势感知可视化[13]仍具有较高的研究价值。

(3)目前该领域正处在增长阶段,但对于网络安全评估的态势没有明确的边界定义,对于理论体系要进一步深入研究。在应用方面如何将大量异构的网络安全数据以可视化的形式呈现,并使其具有准确的预测功能、自动化的防御机制、智能化的专家系统和便捷的交互操作,都是网络安全态势感知目前热门的研究方向[14]。诸多的应用需求与挑战,都需要该领域的研究人员在今后的工作中一一应对。

参 考 文 献

[1] CHEN Y, CHEN C M, LIU Z Y, et al. The methodology function of CiteSpace mapping knowledge domains [J]. Studies in Science of Science, 2015, 33(2): 242-253.

[2] CHEN C M. CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature [J]. Journal of the Association for Information Science & Technology, 2014, 57(3): 359-377.

[3] CHEN H, CHEN G, BLASCH E. Analysis and visualization of large complex attack graphs for networks security[C] // Defense & Security Symposium. International Society for Optics and Photonics, 2007.

[4] SALMON P M, STANTON N A, WALKER G H, et al. Is it really better to share? Distributed situation awareness and its implications for collaborative system design [J]. Theoretical Issues in Ergonomics Science, 2010, 11(1/2): 58-83.

[5] BASS T. Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness[J]. Communications of the ACM, 2000, 43(4): 99-105.

[6] SHIFFLET J. A Technique Independent Fusion Model For Network Intrusion Detection[J]. Proceedings of the Mid states Conference on Undergraduate Research in Computer Science and Mathematics, 2005, 3(1): 13-19.

[7] ENDSLEY M R. Situation awareness misconceptions and misunderstandings[J]. Journal of Cognitive Engineering & Decision Making, 2015, 9(1): 4-32.

[8] SHIRAVI H, SHIRAVI A, GHORBANI A A. A survey of visualization systems for network security [J]. Visualization and Computer Graphics, 2012, 18(8): 1313-1329.

[9] GONG J, ZANG X D, SU Q, et al. Survey of Network Security Situation Awareness [J]. Journal of Software, 2017, 28(4): 1010-1026.

[10] LIN H L, WANG Y Z, JIA Y T, et al. Network big data oriented knowledge fusion methods: A survey [J]. Chinese Journal of Computers, 2017, 40(1): 1-27.

[11] FRANKE U, BRYNIELSSON J. Cyber situational awareness—A systematic review of the literature [J]. Computers & Security, 2014, 46(1): 18-31.

[12] GUANG K, SHUO W, GUANGMING T. Research on Key Technologies of Network Security Situational Awareness for Attack Tracking Prediction[J]. Chinese Journal of Electronics, 2019, 28(1): 162-171.

[13] BEAVER J, STEED C, PATTON R, et al. Visualization techniques for computer network defense[J]. Proc. of the SPIE Int'l Society for Optical Engineering, 2011, 8019(18): 6-9.

[14] WANG H Q, LAI J B, ZHU L, et al. Survey of network situation awareness system[J]. Journal of Computer Science, 2006, 33(10): 5-10.

BAI Xue, born in 1993, postgraduate, is a member of China Computer Federation. Her main research interests include network security and data visualization.

Nurbol, born in 1981, Ph.D, professor, is a member of China Computer Federation. His main research interests include network security and data mining.