基于 MI 和 TPM 混合的多变量数字签名方案

鲁晓彬,鲍皖苏,李发达,田 礼
(解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 本文基于 MI 和 TPM 两类多变量公钥密码的公钥,利用"减"方法将其混合,提出了多变量数字签名方案的中心映射构造新方法,给出了基于 MI 和 TPM 混合的多变量数字签名方案,该方案能够有效抵抗高阶线性化方程攻击、秩攻击、XL&Gröbner 基攻击、差分攻击等现有典型攻击,并且与 Rainbow、Sflash^{v2} 等典型多变量数字签名方案相比,在签名长度、密钥存储规模等方面具有优势.

关键词: 多变量公钥密码; 数字签名; MI; TPM
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2012)10-2021-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.10.020

A MPKC Signature Scheme Based on Mixing of MI and TPM

LU Xiao-bin, BAO Wan-su*, LI Fa-da, TIAN Li
(*Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou* 450004, *China*)

Abstract: We use the method of minus to mix the public key of MI and TPM so that we propose a MPKC signature scheme based on MI and TPM. It is proved that the new scheme can resist high order linear equation attack, rank attacks, XL&Gröbner basis attack, differential attack. It enhances security apparently and has some advantage on the length of signature, signature generation and the size of private key.

Key words: multi-variable public key cryptography; digital signatures; MI; TPM

1 引言

1995 年,Shor 提出了量子计算下多项式时间解决大整数分解问题和离散对数问题子计算算法[1],对 RSA、ECC 等公钥密码带来了严重威胁.抗量子计算的公钥密码算法研究引起了国内外学者的广泛关注[2,3].多变量公钥密码体制(MPKC)被许多密码学专家认为是 RSA、ECC 公钥密码体制的一个可能的替代[4].

多变量公钥密码体制依赖的安全性基础是有限域上随机的多变量二次方程组的求解问题(MQ 问题)的困难性,该问题已经被证明是 NPC 问题.目前,多变量公钥密码设计的一般思路是:选取有限域 F_q(通常选取特征为 2 的域),在 F_q 中使用 n 进 m 出的多变量二次函数 $y = F(x)$,该函数称为中心映射,具有特殊结构使得其容易求逆.为隐藏中心映射的特殊结构,随机选取上的可逆仿射映射 S 和上的可逆仿射映射 T.多变量数字签名方案的私钥为(T, F, S),公钥为私钥 T, F, S 复合所得的多项式函数 $P = T \circ F \circ S$,即

$$\begin{cases} y_1' = p_1(x_1', \cdots, x_n') \\ \vdots \\ y_m' = p_m(x_1', \cdots, x_n') \end{cases}$$

若 M 为待签名的文档,Hash(x)为公开的安全 Hash 函数,y' = Hash(M)为文档的杂凑函数值,则签名过程如下:

(1)计算出 $y = T^{-1}(y')$;(2)计算 $x = F^{-1}(y)$;(3)计算 $x' = S^{-1}(x)$.

x'即为文档 M 的签名值.

签名验证时,将签名值 x'代入公钥函数($p_1(x_1', \cdots, x_n'), \cdots, p_m(x_1', \cdots, x_n')$)计算,如果结果等于文档的杂凑函数值 y',则认为签名有效,否则签名无效.

根据基本陷门函数的不同,多变量公钥密码的基本方案主要有 4 类:MI、HFE、UOV、TTM.但是,由于这些基本方案中心映射的代数结构未能被仿射变换有效隐藏,它们先后被证实是不安全的.比如 Patarin 基于线性化攻击方法[5]攻破了 MI 体制, Wolf 等人基于最小秩攻击方法攻破了 STS 体制[6]等.

收稿日期:2011-12-13;修回日期:2012-03-29

近年来,为提高多变量公钥密码的安全性,人们相继提出了很多针对基本方案的改进方法,如 Shamir 的“-”方法,根据该方法设计的 MIA-和 HFE-可以有效地抵抗 Gröbner 基攻击和线性化攻击;如基于 MI 体制的内部扰动和“+”方法得到的 PMI+.此外,还有增加醋变量的“v”方法,利用子域的“/”方法,分枝结构“⊥”方法,内部扰动“i”方法,以及基于扩展的方法[7]等等.但是,对一些方案的中心映射而言,有些改进方法并未能实质性地改变其原有结构,因而这些改进方案并不可行.例如,使用“-”方法对 MI 进行改进得到 SFlash 签名方案,该方案曾被入选 NESSIE 项目的智能卡标准(IST-1999-12324),被 Dubois 等人利用差分攻击攻破.因此,设计安全的多变量数字签名方案根本上还需要寻求新的中心映射设计方法.

本文基于 MI 和 TPM 两类多变量公钥密码的公钥,提出了多变量数字签名方案中心映射的设计新方法,该方法破坏了 MI 和 TPM 中心映射的特殊代数结构,从而使得签名方案中心映射的多项式系数分布更加随机,在此基础上给出了基于 MI 和 TPM 混合的多变量数字签名方案,以下简称 M-T 方案.研究表明,M-T 方案可以抵抗高阶线性化方程攻击、秩攻击、XL&Gröbner 基攻击、差分攻击等现有典型攻击方法.

2 符号说明

为叙述方便,对本文出现的概念和符号定义如下:

表 1 符号标记

$GF(q)$	表示二元域$\{0,1\}$的 t 次扩域,即 $q=2^t$
$a\cdot b$	代表空间向量中的内积运算
$a\cdot b$	代表元素在所在域中的乘法运算
$a\circ b$	代表两个映射的合成运算
X^t	代表列向量的转置,即为行向量

3 MI 体制和 TPM 体制

3.1 MI 体制

MI 体制是 1988 年由 Matsumoto 和 Imai 提出的.令 $k=GF(q)$,$g(x)\in k[x]$是任意 n 次不可约多项式.定义 $K=k[x]/g(x)$为 k 的 n 次扩域.选取 θ 使得 $0<\theta<n$ 并有

$$gcd(q^{\theta}+1,q^n-1)=1$$

θ 的选取是为了保证中心映射 $\tilde{F}$ 为可逆映射.

定义 K 上的中心映射 $\tilde{F}$ 如下

$$\tilde{F}(x)=x^{1+q^{\theta}}$$

其中,$x\in K$.

1995 年,Patarin 提出线性化攻击攻破了 MI 体制,该攻击方法的基本思想是在中心映射的表达式中通过变换或构造,找到足够多的满足以下有关明文变量和密文变量的恒等式

$$\sum_{i=1,j=1}^{n,m}a_{ij}x_iy_j+\sum_{i=1}^{n}b_ix_i+\sum_{j=1}^{m}c_jy_j+d=0$$

其中,x_i,y_j 分别代表明文变量和密文变量.

3.2 TPM 体制

Shamir 提出的 TPM(“Triangle Plus Minus”)方案是 TTM 的改进,其在原 TTM 的中心映射中减掉 r(r 远远小于 n)个初始方程,再加入 u 个随机多项式.令 $K=GF(q)$,定义映射 $\Psi:K^n\alpha K^{n+u-r}$,则中心映射$(y_1,\cdots,y_{n+u-r})=\Psi(x_1,\cdots,x_n)$定义如下

$$\begin{cases}y_1=x_1+g_1(x_{n-r+1},\cdots,x_n)\\ y_2=x_2+g_2(x_1;x_{n-r+1},\cdots,x_n)\\ y_3=x_3+g_3(x_1,x_2;x_{n-r+1},\cdots,x_n)\\ \vdots\\ y_{n-r}=x_{n-r}+g_{n-r}(x_1,\cdots,x_{n-r-1};x_{n-r+1},\cdots,x_n)\\ y_{n-r+1}=g_{n-r+1}(x_1,\cdots,x_n)\\ \vdots\\ y_{n-r+u}=g_{n-r+u}(x_1,\cdots,x_n)\end{cases}$$

其中,$g_i(1\leqslant i\leqslant n+u-r)$是 K 上随机选取的二次多项式.

2000 年,Louis Goubin 等人利用最小秩攻击方法攻破该方案.该方法的基本思想是将私钥 S,T 及 $g_i(i=1,\cdots,n+u-r)$的求取归结为最小秩问题,通过 Kernel Attack 方法得到私钥 S,T 的等效密钥及 g_i,$i=1,\cdots,n+u-r$ 的系数,从而攻破该方案.

4 基于 MI 与 TPM 混合的多变量数字签名方案

4.1 中心映射设计方法

以下给出 *M-T* 方案中心映射的设计方法.

令 $K=GF(q)$为所用多变量数字签名方案采用的基本有限域,又令 $y_1=f_1(x_1)$为输入规模 n_1 输出规模 m_1,$y_2=f_2(x_2)$为输入规模 n_2 输出规模 m_2 的两个不同方案的公钥,(不妨假设 $m_1\geqslant m_2$),其中,$y_i=(y_{i1},\cdots,y_{im_i})$,$x_i=(x_{i1},\cdots,x_{in_i})$,$i=1,2$. $y_1=f_1(x_1)$与 $y_2=f_2(x_2)$都为 K 上的多变量二次多项式函数构成的向量.为避免中心映射结构的对称而导致缺陷,采用“-”的方法,舍掉 $y_1=f_1(x_1)$中最后 m_1-m_2 个方程,则此时 $y_1=f_1(x_1)$为输入规模 n_1 输出规模 m_2.

定义新的中心映射 $F(x_1,x_2,y_1,y_2)$如下:

$$y_1\cdot f_2(x_2)=y_2\cdot f_1(x_1)$$

4.2 M-T 多变量数字签名方案

对于 TPM,选取 $K=GF(q)$,为方便混合选取参数 $u\geqslant r$,对于明文变量$(x'_{11},x'_{12}\cdots,x'_{1n})$和密文变量$(y'_{11},y'_{12}\cdots,y'_{1n+u-r})$,公钥 $y_1=f_1(x_1)$可写为

$$\begin{cases} y_{11} = x_{11} + g_1(x_{1n-r+1}, \cdots, x_{1n}) \\ y_{12} = x_{12} + g_2(x_{11}; x_{1n-r+1}, \cdots, x_{1n}) \\ y_{13} = x_{13} + g_3(x_{11}, x_{12}; x_{1n-r+1}, \cdots, x_{1n}) \\ \vdots \\ y_{1n-r} = x_{1n-r} + g_{n-r}(x_{11}, \cdots, x_{1n-r-1}; x_{1n-r+1}, \cdots, x_{1n}) \\ y_{1n-r+1} = g_{n-r+1}(x_{11}, \cdots x_{1n}) \\ \vdots \\ y_{1n-r+u} = g_{n-r+u}(x_{11}, \cdots x_{1n}) \end{cases}$$

其中,y_{1j}, x_{1j}分别是密文变量$(y'_{11}, y'_{12} \cdots, y'_{1n-r+u})$和明文变量$(x'_{11}, x'_{12} \cdots, x'_{1n})$经过仿射变换 T_1^{-1}, S_1 得到,g_{1j}为系数在 K 上的二次多项式.

对于 MI,同样选取基域 $K = GF(q)$,对于中心映射

$$\tilde{F}(x) = x^{1+q^{\theta}}$$

通过仿射变换 T_2^{-1}, S_2 对明密文变量的作用,并将其转化为相应向量空间中的方程得到公钥 $y_2 = f_2(x_2)$.

定义　M-T 方案的中心映射 $F(x_1, x_2, y_1, y_2)$如下

$$y_1 \cdot f_2(x_2) = y_2 \cdot f_1(x_1)$$

然后分别随机选取 K^{2n}上的可逆仿射映射 $\tilde{S}$ 和 $\tilde{T}$,则 M-T 方案的公钥为中心映射 $F(x_1, x_2, y_1, y_2)$经过仿射映射 $\tilde{S}$ 和 $\tilde{T}$ 对明文和密文进行变换后的一组多项式方程组

$$F(\tilde{S}(x_1), \tilde{S}(x_2), \tilde{T}^{-1}(y_1), \tilde{T}^{-1}(y_2)) = 0$$

即

$$\tilde{T}^{-1}(y_1) \cdot f_2(\tilde{S}(x_2)) - \tilde{T}^{-1}(y_2) \cdot f_1(\tilde{S}(x_1)) = 0$$

其中,$\tilde{S}(x_1), \tilde{S}(x_2)$分别表示 $\tilde{S}(x)$的前半部分和后半部分,也即 $\tilde{S}(x)$分别作用在$(x_{11}, \cdots, x_{1n_1})$与$(x_{21}, \cdots, x_{2n_2})$上的仿射变换,$\tilde{T}^{-1}(y_1), \tilde{T}^{-1}(y_2)$类似.由此可以得到 M-T 公钥,它由 n 个关于 $4n$ 个变量的三次多项式方程构成,其具体形式如下

$$\sum \alpha_{ijk} x_i x_j y_k + \sum \beta_{ij} x_i y_j + \sum \gamma_i y_i + \sum \alpha'_{ij} x_i x_j + \sum \beta'_i x_i + \gamma' = 0$$

将这样的公钥方程记为 $p_i(x_1, \cdots, x_{2n}, y_1, \cdots, y_{2n}) = 0$,则 M-T 方案的公钥为 $P = (p_1, \cdots, p_n)$.

而相应的私钥为$(T_1, F_1, S_1, T_2, F_2, S_2, \tilde{T}, \tilde{S})$.

签名生成:

令 Y 是消息 M 经 Hash 函数所得到的长度为 $2n$ 的杂凑值,则签名需要进行如下步骤:

(1)计算出$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \tilde{T}^{-1}(Y)$,其中 $y_1 = (y_{11}, y_{12}, \cdots, y_{1n})$, $y_2 = (y_{21}, y_{22}, \cdots, y_{2n})$分别表示 $\tilde{T}^{-1}(Y)$的前半部分和后半部分;

(2)对于 $y_1 = (y_{11}, y_{12}, \cdots, y_{1n})$,随机选取 F_q 中 $u - r$ 个值,得到 $\bar{y}_1 = (y_{11}, y_{12}, \cdots, y_{1n+u-r})$,利用私钥 T_1, F_1, S_1 进行求逆,相应结果记为 x_1,即 $x_1 = S_1^{-1} \circ F_1^{-1} \circ T_1^{-1}(\bar{y}_1)$;对于 y_2,利用私钥 T_2, F_2, S_2 求逆得到 x_2,其中 x_1, x_2 均为长度为 n 的向量;

(3)由 x_1, x_2 计算出 $S = \tilde{S}^{-1}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, S 即为消息 M 的一个有效签名.

签名验证:

给定消息 M 的杂凑函数值 $Y = (y_1, \cdots, y_{2n})$以及签名 $S = (s_1, \cdots, s_{2n})$,将其代入公钥 $P = (p_1, \cdots, p_n)$中,如果所有的多项式方程 $p_i(s_1, \cdots, s_{2n}, y_1, \cdots, y_{2n}) = 0$ 都成立,则认为 S 是 M 的有效签名,否则签名无效.

5　方案分析

5.1　正确性分析

给定签名 $S = (s'_1, \cdots, s'_{2n})$与消息 M 的杂凑函数值 $Y^t = (y'_1, \cdots, y'_{2n})$,由于 $\tilde{T}^{-1}(y_1) = (y'_1, \cdots, y'_n)$, $\tilde{T}^{-1}(y_2) = (y'_{n+1}, \cdots, y'_{2n})$,对于 $y_1 = (y_{11}, y_{12}, \cdots, y_{1n})$,随机选取 $GF(q)$中 $u - r$ 个值后得到 $\bar{y}_1 = (y_{11}, y_{12}, \cdots, y_{1n+u-r})$,有 $\bar{y}_1 = T_1 \circ F_1 \circ S_1(x_1)$,其中 $x_1 = \tilde{S}(s_1)$.选取该方程组前 n 个方程,则有 $\tilde{T}^{-1}(y_1) = f_1(\tilde{S}(s_1))$.同样,对于 y_2,有 $\tilde{T}^{-1}(y_2) = f_2(\tilde{S}(s_2))$,其中,所以有

$$\tilde{T}^{-1}(y_1) \cdot f_2(\tilde{S}(s_2)) = \tilde{T}^{-1}(y_2) \cdot f_1(\tilde{S}(s_1))$$

即

$$p_i(s_1, \cdots, s_{2n}, y_1, \cdots, y_{2n}) = 0 \quad (1 \leqslant i \leqslant n)$$

5.2　安全分析

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、秩攻击、差分攻击、Gröbner 基攻击等,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 $q = 2^8, n = 16$ 为例对 M-T 方案进行安全分析.

5.2.1　线性化攻击

首先,引用对 MI 体制攻击方法在其相应扩域中通过对其进行变换或构造寻求线性关系也不能实现,因为 M-T 方案中心映射转化到相应扩域中的形式如下所示:

$$\hat{Y}_1 \cdot [\hat{T}_2 \circ \hat{F}_2 \circ \hat{S}_2(\hat{X}_2)] = \hat{Y}_2 \cdot [\hat{T}_1 \circ \hat{F}_1 \circ \hat{S}_1(\hat{X}_1)]$$

其中,$\hat{Y}_i, \hat{X}_i (i = 1, 2)$表示向量 y_i, x_i 转化到域中的元素,$\hat{T}_i, \hat{F}_i, \hat{S}_i$ 表示 T_i, F_i, S_i 转化到域中的映射.可以看到,在扩域中,对映射 F_1 的变换必须使得映射 F_2 同时转化为线性,才能使整个中心映射可以利用线性化攻击,而 MI 的中心映射与 TPM 的中心映射结构不同,所以通过变换不能够得到线性关系.其次,在构建中心映射的过程中,使用了“-”方法,也会避免线性化方程的攻击.

综上所述,M-T 方案能够克服 MI 体制结构缺陷,可以抵抗线性化攻击.

5.2.2 秩攻击

在 TPM 方案中,中心映射方程与公钥方程可以通过转化为矩阵形式建立联系,并由第一个中心映射方程的矩阵秩较小的特点将其转化为容易求解的最小秩问题.

但是 M-T 方案却可以抵抗秩攻击.中心映射将其转化为可以利用的矩阵形式,首先将公钥转化为 16 个 32×32 的矩阵,若随机选取公钥矩阵的一组线性组合,使得所得组合矩阵的秩达到最小,设最小秩为 $r'=16$,要得到这样一个线性组合,需要 $q^{\lceil m/n\rceil r'}$ 次尝试,整个算法的复杂性是 $O(2^{128})$.综上所述,M-T 方案能够克服 TPM 体制结构缺陷,可以抵抗秩攻击.

5.2.3 差分攻击

近年来,差分分析作为一种强有力的工具应用于多变量公钥密码分析.该方法能够成功的关键在于多变量二次公钥密码的差分是线性映射,分析它的核或者秩能够得到关于私钥的一些信息.针对 SFLASH 体制的差分攻击方法利用了其中心映射特殊结构 $F: x \mapsto x^{q^i+1}$,而在 M-T 方案中,并没有类似结构.并且变量 x, y 混合在一起,攻击者想要由公钥方程得到类似 $y=f(x)$ 的低次多变量表示是不可行的,因此,差分方法对于 M-T 方案是不可行的.

5.2.4 Gröbner 基攻击[8]

目前,最有效的 Gröbner 基方法是 $F4$、$F5$ 算法.$F5$ 算法被成功用于攻破了 HFE 体制的几个实例.该方法能够成功攻击 HFE 实例,关键在于能够区分由 HFE 所得的方程组与随机的多变量二次多项式方程系统.M-T 方案的公钥中变量数目远多于方程数目,若对多出的 16 个变量随机赋值,则问题可以转化利用 Gröbner 基解决 16 个变量数目为 16 的方程组,对于选取的参数,利用该方法求解的复杂性 $O(2^{3\times 16}\cdot 2^{8\times 16})$,即 $O(2^{176})$.因此 M-T 方案能够抵抗 Gröbner 基方法攻击.

5.2.5 复线性化、XL、FXL 攻击

复线性化方法、XL 方法和 FXL 方法用于求解超定方程组系统,即 $\varepsilon\cdot n^2(\varepsilon>0)$个方程、$n$ 个变量.Kipnis 和 Shamir 对 HFE 的攻击中,利用多变量二次多项式的矩阵表示,得到了 $O(n^2)$个关于 $O(n)$个变量的多项式方程,而复线性化方法、XL 方法和 FXL 方法正是用求解此类方程组.M-T 方案中,攻击者能得到 n 个关于 $2n$ 个变量的二次多项式方程,方程个数远小于变量数目,不适用于此类攻击方法.若对多出的 16 个变量随机赋值,则利用该方法求解的计算复杂度为 $O(2^{36}\cdot 2^{8\times 16})$,即 $O(2^{164})$.

综上所述,M-T 方案可以有效地避免 MI 与 TPM 单一结构带来的弱点,安全强度能够达到 $O(2^{80})$.

5.3 规模分析

公钥规模:公钥为是由 16 个如下形式的多项式方程组成

$$\sum \alpha_{ijk}\, x_i x_j y_k + \sum \beta_{ij}\, x_i y_j + \sum \gamma_i y_i + \sum \alpha'_{ij}\, x_i x_j + \sum \beta'_i x_i + \gamma' = 0$$

则公钥规模为

$$\left(\frac{n^2\cdot(n+1)}{2}+\frac{n\cdot(n+1)}{2}+n^2+2n+1\right)\cdot n = \frac{n^3+4n^2+5n+2}{2}\cdot n$$

对于所选参数,公钥大约需要 40KB 的存储空间.

私钥规模:M-T 方案私钥$(T_1, S_1, T_2, S_2, \tilde{T}, \tilde{S}, g_i)$,则私钥规模为

$$n^2\cdot 4+(2n)^2\cdot 2+n\cdot\frac{n\cdot(n+1)}{2}$$

对于所选参数,私钥大约需要 5KB 的存储空间.

签名长度:M-T 方案的签名长度为 $8n$.对于所选参数,签名长度需要 128bit.

下表列出在安全强度均为 $O(2^{80})$时 M-T 方案与 Rainbow、Sflash^{v2}的规模比较[9]:

表 2 M-T 方案与 Rainbow、Sflash^{v2}的规模比较

方案名	参数	公钥长度	私钥长度	签名长度
新方案	$q=256, n=16$	40KB	5KB	128bit
Rainbow	$q=256, n=37, u=5$	16KB	10KB	296bit
Sflash^{v2}	$q=128, n=37, r=11$	18KB	5.6KB	259bit

注:q 为所在有限域元素个数,n 为公钥方程的个数,u 为 Rainbow 方案中醋变量个数,r 为 Sflash^{v2}方案中减掉的方程个数.

由上表可知,M-T 方案在私钥存储规模与签名长度上与 Rainbow 和 Sflash 签名体制相比具有优势,但公钥存储规模相对较大.

6 结论

本文利用 MI 体制与 TPM 体制的公钥的混合产生新的中心映射,给出了基于 MI 和 TPM 混合的多变量公钥签名方案,即 M-T 方案.理论研究表明,M-T 方案可以抵抗高阶线性化方程攻击、秩攻击、XL&Gröbner 基攻击、差分攻击等攻击方法,提高了原有方案的安全性.

参考文献

[1] P W Shor. Polynomial-Time Algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM Journal on Computing, 1997, 26(5): 1484 – 1509. (preliminary version in FOCS 1994)

[2] 付向群,鲍皖苏,周淳,钟普查.具有高概率的整数分解量子算法[J].电子学报,2011,39(1):35 – 39.

FU Xiang-qun, BAO Wan-su, ZHOU Chun, ZHONG Pu-cha. Quantum Algorithm for Prime Factorization with High Probability[J]. Acta Electronica Sinica, 2011, 39(1): 35 – 39. (in Chinese)

[3] Vivien Dubois, Nicolas Gama. The degree of regularity of HFE systems [A]. Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security[C]. Berlin, 2010, 6477, 557 – 576.

[4] Jintai Ding, Timothy J, Victoria Kruglov. Growth of the ideal generated by a quadratic boolean function[A]. PQCrypto 2010 [C]. Berlin, 2010, 6061, 13 – 27.

[5] Jacques Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88 [J]. Computer Science, 1995, 963: 248 – 261

[6] Christopher Wolf, An Braeken, Bart Preneel. Efficient cryptnalysis of RSE(2)PKC and RSSE(2)PKC[OL]. Cryptology ePrint Archive. http://eprint.iacr.org/, 2011.8.11.

[7] WANG HouZhen, ZHANG HuanGuo, WANG ZhangYi, etc. Extended multivariate public key cryptosystems with secure encryption function [J]. Science China, 2011, 54(6): 1161 – 1171.

[8] Mohamed, M, Cabarcas, D, Ding, J, et al. An Efficient Algorithm for Computing Grobner Bases of Zero-Dimensional Ideals [A]. Information security and cryptology ICISC 2009[C]. Berlin 2010, 5984: 87 – 100.

[9] Jintai Ding. Multivariate Public Key Cryptosystems [M]. Berlin: Springer-Verlag, 2006. 94 – 96

作者简介

鲁晓彬　男,1982 年出生于河南邓州,解放军信息工程大学电子技术学院,硕士生,研究方向为公钥密码.
E-mail: keven_896@163.com

鲍皖苏　男,1966 年出生于安徽天长,解放军信息工程大学电子技术学院,教授,博士生导师,主要研究方向为公钥密码、量子密码、密码管理.
E-mail: 2010thzz@sina.com

李发达　男,1989 年出生于山东济南,解放军信息工程大学电子技术学院,硕士生,研究方向为量子密码、公钥密码.
E-mail: keven_896@163.com

田　礼　男,1983 年出生于四川乐至,解放军信息工程大学电子技术学院,硕士生,研究方向为公钥密码.
E-mail: tianli091183@sohu.com