一种新的基于 STS 陷门的中心映射*

王 晟,陈 勤*,张 旻
(杭州电子科技大学 计算机科学与技术系,浙江 杭州 310018)

摘要:针对现有的基于三角阶梯体制陷门的中心映射不适合构造高次多变元公钥密码系统的问题,提出了一种新的基于三角阶梯体制陷门的中心映射,详尽地给出了该映射的构造与生成过程及其快速求解算法,并对算法效率进行了分析。分析结果表明该映射不仅能有效控制密钥长度,还可快速将中间密文还原成明文,具有较好的性能,可用于构造高次的多变元公钥密码系统。

关键词:多变元公钥密码体制;三角阶梯体制;中心映射
中图分类号:TP309 **文献标识码**:A **文章编号**:1001-4551(2010)06-0112-04

A new central map based on trapdoor of step-wise triangular systems

WANG Sheng, CHEN Qin, ZHANG Min
(Department of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: Aiming at the problem that current central map based on the trapdoor of step-wise triangular systems is not fit to construct high power multivariate public key cryptosystems, a new central map based on the trapdoor of step-wise triangular systems was proposed. And its construction, generation process and the algorithm of fast decryption were described in detail. The analysis results of the algorithm show that the central map can control the length of key and recover the plaintext from the intermediate ciphertext quickly, which enables its application in constructing a high power of multivariate public key cryptosystems.

Key words: multivariate public-key cryptosystems; step-wise triangular system; central map

0 引 言

多变元公钥密码体制被认为是能抵御未来量子计算机攻击的几种公钥密码体制之一,其安全性基于有限域上求解多变元多项式方程组为一个 NP-C 问题[1]。该公钥体制具有较高的加、解密运算速度,且易于硬件实现,适用于计算能力和存储空间有限的小型通信设备,比如射频识别设备、无线传感器和掌上电脑等。多变元公钥密码体制通常都是基于某类陷门体制的,三角阶梯体制(Step-wise Triangular Systems, STS)是其中一种基本陷门体制,其最初思想源于 Shamir 的(Birational Permutation)方案[2],基于这类体制的方案有 TPM[3]、RSE(2)PKC[4]、RSSE(2)PKC[5]等。多数方案都是基于二次非线性方程组的,虽然具有很高的效率,却难以抵御某些结构攻击[6]和代数攻击[7]。提高非线性方程组的代数次数,一定程度上可以增强密码系统的安全性。因此,设计一种“在非线性方程组代数次数上有所增加,同时又具有较高性能”的多变元公钥密码系统是有必要的。中心映射是多变元公钥密码最重要的组成部分,其构造优劣直接影响密码系统的性能,因此,如何构造高次多变元

收稿日期:2009-10-30
基金项目:现代通信国家重点实验室基金资助项目(9140C110206070C11)
作者简介:王 晟(1985-),男,浙江杭州人,主要从事网络和信息安全方面的研究. E-mail: wangsheng281@163.com
通信联系人:陈 勤,男,教授,硕士生导师. E-mail: chenqin@hdu.edu.cn

公钥密码系统中的中心映射至关重要。中心映射既要能加快求解速度,又需要能有效地控制密钥长度。

本研究提出了一种新的基于 STS 陷门的可逆中心映射,可用于构造一种高次的基于布尔代数方程组的新型公钥密码系统。

1　中心映射的构造与生成

本研究提出的中心映射是由一个大型的可逆布尔矩阵以及一组高次的非线性布尔函数两部分组成的。布尔矩阵容易求逆适合构造可逆的仿射映射,而非线性布尔函数可提高公钥密码系统的代数次数。此外,这两部分都可进行压缩存储和生成。因此,用这两部分来构造中心映射,密钥长度也可得到有效控制。

设 F 是一个给定的域,对于给定的自然数 m、n,$M_{m\times n}(F)$ 为域 F 上 $m\times n$ 阶矩阵的集合,$GL_n(F)$ 为域 F 上 $n\times n$ 阶可逆矩阵的集合。

中心映射 P' 是由一个大型可逆布尔矩阵 $\boldsymbol{B}$,以及 $12n$ 个 8 变元的非线性布尔函数 $f_j(x_1,x_2,\cdots,x_{8n}),j\in(1,12n)$ 构成的。

P' 中的大型可逆布尔矩阵 $\boldsymbol{B}$,本研究采用文献[8]中的生成算法进行生成,生成后的大型可逆布尔矩阵 $\boldsymbol{B}\in M_{8n\times 12n}(F)$ 的形式如下:

$$\boldsymbol{B}_{8n\times 12n}=(b_{\mathrm{km}})_{8n\times 12n}=\begin{bmatrix} B_{11} & & & & \\ B_{21} & B_{22} & & & \\ B_{31} & B_{32} & B_{33} & & \\ & & \vdots & & \\ B_{n-2,1} & B_{n-2,2} & \cdots & B_{n-2,n-2} & \\ B_{n-1,1} & B_{n-1,2} & \cdots & B_{n-1,n-2} & B_{n-1,n-1} \\ B_{n,1} & B_{n,2} & \cdots & B_{n,n-2} & B_{n,n-1} \end{bmatrix} \tag{1}$$

式中 $\boldsymbol{B}_{i,j}\in M_{8\times 12}(F)(1\leqslant i\leqslant n,1\leqslant j\leqslant n,i\geqslant j,b_{\mathrm{km}}\in F)$。

$\boldsymbol{B}$ 可以表示为:

$$\boldsymbol{B}=[\boldsymbol{B}_1\quad\boldsymbol{B}_2]$$

其中 $\boldsymbol{B}_1\in GL_{8n\times 8n}(F)$ 为一个可逆仿射映射,$\boldsymbol{B}_2\in M_{8n\times 4n}(F)$。

$\boldsymbol{B}$ 的对角线上的每一个子块为:

$\boldsymbol{B}_{i,i}\in M_{8\times 12}(F)(1\leqslant i\leqslant n)$,$\boldsymbol{B}_{i,i}$ 可以表示为:

$$\boldsymbol{B}_{i,i}=[\boldsymbol{B}'_{i,1}\boldsymbol{B}'_{i,2}]$$

式中　$\boldsymbol{B}'_{i,1}\in GL_{8\times 8}(F)$,$\boldsymbol{B}'_{i,2}\in M_{8\times 4}(F)$。$P'=(y_1,\cdots,y_{8n})$ 是 $8n$ 个多项式构成的一个非线性布尔代数方程组(式中　$y_i=\sum b_{ij}f_j(x_1,x_2,\cdots,x_{8n});i\in(1,8n)$)。具体表示如下:

$$l_1=\begin{cases} b_{1,1}f_1+\cdots+b_{1,12}f_{12}=y_1 \\ \vdots \\ b_{8,1}f_1+\cdots+b_{8,12}f_{12}=y_8 \end{cases}$$

$$l_2=\begin{cases} b_{9,1}f_1+\cdots+b_{9,12}f_{12}+ \\ \vdots \\ b_{16,1}f_1+\cdots+b_{16,12}f_{12}+ \end{cases}$$

$$b_{9,13}f_{13}+\cdots+b_{9,24}f_{24}=y_9$$

$$\vdots \tag{2}$$

$$b_{16,13}f_{13}+\cdots+b_{16,24}f_{24}=y_{16}$$

$$l_n=\begin{cases} b_{8n-7}f_1+\cdots+b_{8n-7,12}f_{12}+\cdots+ \\ \vdots \\ b_{8n}f_1+\cdots+b_{8n,12}f_{12}+\cdots+ \end{cases}$$

$$b_{8n-7,12n-11}f_{12n-11}+\cdots+b_{8n-7,12n}f_{12n}=y_{8n-7}$$

$$\vdots$$

$$b_{8n,12n-11}f_{12n-11}+\cdots+b_{8n,12n}f_{12n}=y_{8n}$$

可知 P' 和多变元公钥密码体制下的基于 STS 陷门的中心映射的结构是相似的。P' 是下三角阶梯结构的方程组,共 n 层,每层上有 8 个方程。设 r 为层数($1\leqslant r\leqslant n$),则 l_r 为式(2)中第 r 层上的方程组。

设 $X_1=(x_1,x_2,\cdots,x_8)$ 为第 1 层上出现的变元,$X_r=(x_{8r-7},x_{8r-6},\cdots,x_{8r})$ 为第 r 层上的新增加的变元,

设 $Y_r=(y_{8r-7},y_{8r-6},\cdots,y_{8r})$ 和 $Y'_r=(y'_{8r-7},y'_{8r-6},\cdots,y'_{8r})$ 为第 r 层上的多项式组。则 $12n$ 个非线性布尔函数 $f_j(1\leqslant j\leqslant 12n)$ 可表示为 $f_{12(r-1)+j}(X_r)(1\leqslant j\leqslant 12,1\leqslant r\leqslant n)$。

设 $F_r=[F_{r,1},F_{r,2}]$ 为第 r 层新增加的布尔函数,其中 $F_{r,1}=(f_{12(r-1)+1}(X_r),\cdots,f_{12(r-1)+8}(X_r))$,$F_{r,2}=(f_{12(r-1)+9}(X_r),\cdots,f_{12(r-1)+12}(X_r))$。

由于密码系统中明文与密文是一一对应的关系,中心映射的求解也必须是惟一的。本研究在 P' 的每一层上构造了一个双射的结构,即第 r 层中的变元 X_r 和多项式组 Y_r 之间是双射关系,对于任何给定的 Y_r,都只对应惟一解 X_r,这样明文和密文就具有一对一的关系。

此外,为了加快中心映射的求解速度,即已知 Y_r 要能快速求出 X_r,这需要通过构造一组特殊的非线性布尔函数 F_r 使得它与 Y_r 以及 X_r 满足某种关系,使得

P' 的求解变得高效。

$$\begin{cases} b_{1,1}f_1 + b_{1,2}f_2 + \cdots + b_{1,8}f_8 = y'_1 \\ \vdots \\ b_{8,1}f_1 + b_{8,2}f_2 + \cdots + b_{8,8}f_8 = y'_8 \end{cases} \tag{3}$$

$$\begin{cases} b_{1,9}f_9 + b_{1,10}f_{10} + \cdots + b_{1,12}f_{12} \\ \vdots \\ b_{8,9}f_9 + b_{8,10}f_{10} + \cdots + b_{8,12}f_{12} \\ = (y_1 - y'_1)(\mathrm{mod}2) \\ \vdots \\ = (y_8 - y'_8)(\mathrm{mod}2) \end{cases} \tag{4}$$

首先对于方程组 l_1，若 $\boldsymbol{B}'_{1,2} \times F_{1,2}$ 为一组常数，即式(4)中对于任意的 X_1，$(Y_r - Y'_r)\bmod 2$ 为一组常数，那么能够将 l_1 变成式(3)的形式。因 $\boldsymbol{B}'_{1,1}$ 可逆，可知 Y_1 和 $F_{1,1}$ 之间满足双射关系。而由 $F_{1,1}$ 又要得到惟一的 X_1，这等价于寻找一组具有惟一解的 8 变元平衡布尔函数使得 $F_{1,1}$ 和 X_1 也满足双射关系。

由 X_1 可计算出 F_1 的值，再代入方程组 l_2 可转化成如下形式：

$$\begin{cases} b_{9,13}f_{13} + b_{9,14}f_{14} + \cdots + b_{9,24}f_{24} = y_9'' \\ \vdots \\ b_{16,13}f_{13} + b_{16,14}f_{14} + \cdots + b_{16,24}f_{24} = y_{16}'' \end{cases} \tag{5}$$

其中

$$\begin{cases} y_9'' = (y_9 + b_{9,1}f_1 + \cdots + b_{9,12}f_{12})(\mathrm{mod}\ 2) \\ \vdots \\ y_{16}'' = (y_{16} + b_{16,1}f_1 + \cdots + b_{16,12}f_{12})(\mathrm{mod}\ 2) \end{cases}$$

可知式(5)和方程组 l_1 形式相同，若对于任意的 X_2，$\boldsymbol{B}'_{2,2} \times F_{2,2}$ 都为一组常数，因 $\boldsymbol{B}'_{2,1}$ 可逆，可知 Y_2 和 $F_{2,1}$ 之间也满足双射关系。那么只需生成一组具有惟一解的 8 变元平衡布尔函数 $F_{2,1}$，就能够由 Y_2 求出惟一解 X_2。

将 P' 每层上计算得到 F_{r-1} 的值($2 \leqslant r \leqslant n$)代入到方程组 l_r 都可转化成式 l_1 的形式。因此，要使得 P' 每层上的 Y_r 都能求得惟一解 X_r，只需生成一组具有惟一解的 8 变元平衡布尔函数使得 $F_{r,1}$ 和 X_r 满足双射关系，同时满足对于任意的 X_r，$\boldsymbol{B}'_{r,2} \times F_{r,2}$ 恒为一组常数。

生成一组具有惟一解的 8 变元平衡布尔函数，可用布尔置换的方式来实现。此外，若全部保存这 $12n$ 个非线性布尔函数，则密钥长度会很大。因此，需要对密钥长度进行压缩，用置换来控制密钥长度。首先生成 $F_{1,1}$ 的真值表，然后由一置换矩阵 $\boldsymbol{C}_{8\times n-1}$ 对 $F_{1,1}$ 的真值表进行置换，生成 $F_{r,1}$ 的真值表($2 \leqslant r \leqslant n$)。而 $\boldsymbol{B}_{r,2} \times F_{r,2}$ 恒为一组常数，则 $F_{r,2}$ 的真值表可由 $\boldsymbol{B}'_{r,2}$ 计算得到($1 \leqslant r \leqslant n$)。

根据给定的矩阵 $\boldsymbol{B}'_{r,2}$ 及 $\boldsymbol{C}_{8\times n-1}$，生成8变元平衡布尔函数 $F_r(1 \leqslant r \leqslant n)$ 的算法如下：

输入　矩阵 $\boldsymbol{B}'_{r,2}$ 及 $C_{8\times n-1}(1 \leqslant r \leqslant n)$；

输出　$F_r(1 \leqslant r \leqslant n)$；

Step 1 for $i \leftarrow 0$ to 255

对 i 进行置换并转化成二进制字符串，放入数组 $F[8][256]$ 中第 i 列；

Step 2 for $i \leftarrow 0$ to 7

从 F 中取出第 i 行，每一行表示一个8变元平衡布尔函数 $f_{i+1}(X_1)$

if(f_{i+1} 的代数次数 < 3)　转 Step 1；

Step 3　for $i \leftarrow 0$ to $n-1$

if($i > 0$) 计算 $f_{12i+j} = f_j(x_1 \oplus c_{1i}, x_2 \oplus c_{2i}, \cdots, x_8 \oplus c_{8i})(1 \leqslant j \leqslant 8)$；

设向量 $\boldsymbol{\alpha}_k = (b_{k,1}, \cdots, b_{k,4})$ 为 $\boldsymbol{B}'_{i+1,2}$ 中任意行向量($1 \leqslant k \leqslant 8$)，计算对于所有的 $\boldsymbol{\alpha}_k$ 都满足方程 $\boldsymbol{\alpha}_k \times [x_1, x_2, x_3, x_4]^{\mathrm{T}}$ 恒为0或1的所有可能的解，按真值从小到大重复排列，按 $f_{12i+j}(1 \leqslant j \leqslant 8)$ 的置换顺序进行置换。

用上述算法生成这 $12n$ 个非线性布尔函数，并用文献[8]中算法生成一个大型可逆布尔矩阵，也就生成了中心映射。因此，该映射的生成是容易的。此外，该映射不仅能有效控制密钥长度，而且将中间密文还原成明文的速度也是非常快的。以下先给出该映射的快速求解算法，然后对其密钥存储量以及求解效率进行分析。

2　中心映射求解算法

设 $Z = (z_1, \cdots, z_{8n})$ 表示密文，$Y = (y_1, \cdots, y_{8n})$ 表示 P' 中 $8n$ 个多项式的值，$X = (x_1, \cdots, x_{8n})$ 表示明文。解密时，Z 经过若干可逆线性变换后变成中间密文 Y，由 Y 求 X 就是中心映射的求解。

由于解密时是将非线性布尔函数 $f_j(1 \leqslant j \leqslant 12n)$ 视为变量，则 P' 是线性方程组，利用 P' 的特殊结构求解明文 $X = (x_1, \cdots, x_{8n})$ 是非常快速的。

解密时由中间密文 Y 和布尔矩阵 $\boldsymbol{B}$ 以及 F_r 的真值表($1 \leqslant r \leqslant n$)求解明文 X 的算法如下：

输入　Y 和 $\boldsymbol{B}$ 以及 F_r 的真值表；

输出　X；

Step 1 $r \leftarrow 1$;

Step 2 计算 $Y'_r = \boldsymbol{B}'_{r,2} \times F_{r,2}$;

Step 3 计算 $Y_r = (Y_r + Y'_r) \bmod 2$;

Step 4 计算 $F_{r,1} = \boldsymbol{B}'^{-1}_{r,1} \times Y_r$;

Step 5 根据 $F_{r,1}$ 计算 X_r 并输出,由 X_r 计算 $F_{r,2}$;

Step 6 将 F_r 代入并计算

$y_i = (y_i + \sum_{j=12(r-1)+1}^{j=12r} b_{i,j} f_j(X_r)) \bmod 2 (8r + 1 \leqslant i \leqslant 8n)$;

Step 7 $r \leftarrow r + 1$;

Step 8 若 $r \leqslant n$,转 Step 2;

Step 9 输出 $X = (X_1, \cdots, X_n)$。

3　性能分析

3.1　密钥存储量

中心映射 P' 的密钥长度包括大型布尔矩阵的密钥长度和 $12n$ 个非线性布尔函数的密钥长度。布尔矩阵由 n 个 8×8 的可逆矩阵以及一个 16 变元平衡布尔函数来生成[8],密钥存储量为 $n \times 8^2 + 5 \times 2^4$。$12n$ 个非线性布尔函数 $f_j(x_1, x_2, \cdots, x_{8n})$ 由 8 个 8 变元平衡布尔函数和一个置换矩阵生成,密钥存储量为 $8 \times 2^8 + 8 \times (n - 1)$。若 $n = 12$,P' 的密钥存储量为 373 Bytes。

3.2　算法复杂度

布尔函数的生成主要包括置换、解方程组、判断布尔函数的代数次数。置换的复杂度为 $O(n)$;解方程组的复杂度等价于矩阵相乘的复杂度 $O(n^3)$,step 3 中需要 $12 \times 8 \times 4 \times 2^4 = 6\,144$ 个乘法;判断一个代数次数为 $i(1 \leqslant i \leqslant n - 1)$ 的 n 变元平衡布尔函数最坏情况下复杂度为 $O(2^{n-1} \times \sum_{k=n-1}^{i} C_n^k)$。中心映射 P' 的求解主要包括布尔矩阵求逆和矩阵相乘运算。n 阶布尔矩阵求逆复杂度约为 $O(2n^3)$,step 2 需 384 个乘法,step 4 求 12 个可逆布尔矩阵约需 $12 \times 2 \times 8^3 = 12\,888$ 个异或操作,step 6 中相乘需 $8 \times 12 \times \sum_{r=11}^{1} r = 6\,336$ 个乘法。因此,解密运算约需 2^{14} 个基本运算。

通过对中心映射的密钥长度以及求解效率的分析,该映射具有较好的性能,可以用它来构造一种高次的基于布尔代数方程组的新型公钥密码系统。

4　结束语

本研究提出了一种新的基于 STS 陷门的中心映射,通过分析表明该映射不仅可以有效地控制密钥长度,还可快速将中间密文还原成明文,具有较好的性能。该映射主要用于构造一种高次的基于布尔代数方程组的新型公钥密码系统。中心映射只是多变元公钥密码中最重要的一个组成部分,构造完中心映射以后,还需对其进行线性变换,隐藏其内部结构,最终来生成公钥,这些相关工作还需作进一步研究。

参考文献(References):

[1] GARAY M R, JOHNSON D S. Computers and intractability: a guide to the theory of NP-Completeness[M]. San Francisco: W H Freeman, 1979.

[2] SHAMIR A. Efficient signature schemes based on birational permutations[M]. Berlin: Springer Berlin/Heidelberg, 1993.

[3] GOUBIN L, COURTOIS N T. Cryptanalysis of the TTM cryptosystem[M]. Berlin: Springer Berlin/Heidelberg, 2000.

[4] KASAHARA M, SAKAI R. A construction of public-key cryptosystem based on singular simultaneous equations[J]. **IEICE Transactions on Fundamental Electronics, Communications and Computer Science**, 2005, 80(1): 75 - 80.

[5] KASAHARA M, SAKAI R. A construction of public key cryptosystem for realizing ciphtertext of size 100 bit and digital signature scheme[J]. **IEICE Transactions on Fundamental Electronics, Communications and Computer Science**, 2004, 80(1): 102 - 109.

[6] WOLF C, BRAEKEN A, PRENEEL B, et al. Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC[M]. Berlin: Springer Berlin/Heidelberg, 2004.

[7] DING Jin-tai, HU Lei, NIE Xu-yun, et al. High order linearization equation(hole) attack on multivariate public key cryptosystems[M]. Berlin: Springer Berlin/Heidelberg, 2007.

[8] 陈　勤,黄小珠,张　旻. 多变量密码体制下大型布尔矩阵生成算法[J]. 计算机工程与应用, 2009, 45(19): 75 - 77.

[**编辑**:李　辉]