doi:10.11959/j.issn.1000-436x.2015128

遍历矩阵密码体制的安全性

黄华伟[1]，彭长文[2]，瞿云云[1]，李春华[3]

（1. 贵州师范大学 数学与计算机科学学院, 贵州 贵阳 550001；
2. 贵州师范学院 数学与计算机科学学院, 贵州 贵阳 550018；3. 华东交通大学 理学院， 江西 南昌 330013）

摘 要：分析了基于有限域遍历矩阵的公钥密码体制的安全性。根据公钥，采取逆矩阵消去方法得到伪造私钥的线性方程组。从而证明了计算性 TEME 问题是多项式时间可解的，利用伪造私钥即可破解 PZZ1 密码体制的密文。在一些情况下，SEME 问题在多项式时间内可归约为离散对数问题，若密钥参数选取不当，PZZ2 密码体制是基于离散对数问题的，并不基于 NP 困难问题。

关键词：遍历矩阵；公钥密码；计算复杂度；有限域；算法

中图分类号：TN918 **文献标识码**：A

Security of the cryptosystems based on ergodic matrices

HUANG Hua-wei[1], PENG Chang-wen[2], QU Yun-yun[1], LI Chun-hua[3]

(1. School of Mathematics and Computer Science, Guizhou Normal University, Guiyang 550001, China;
2. School of Mathematics and Computer Sciences, Guizhou Normal College, Guiyang 550018, China;
3. School of Science, East China Jiaotong University, Nanchang 330013, China)

Abstract: The security of the public-key cryptosystems based on ergodicmatrices over finite field was analysed. According to the public key,a system of linear equations for the forged secret key bits is obtained by inverse matrix elimination method. It is proved that the computational TEME problem is solvablein polynomial time and the ciphertext of the PZZ1 cryptosystem can be decrypted by the forged secret key. In some case the SEME problem can be reduced to discrete logarithm problem in polynomial time. If the key parameters are chosen improperly, then PZZ2 cryptosystem is based on discrete logarithm problem instead of NP hard problem.

Key words: ergodic matrix; public-key cryptography; computational complexity; finite field; algorithm

1 引言

量子计算机的发展对目前广泛使用的公钥密码体制构成了潜在威胁。具有抗量子分析的密码体制受到了广泛关注。多变量密码是后量子密码学的一个重要研究方向。多变量密码体制的安全性基于有限域上多变元二次方程组的难解性，如 MQ 问题和 BMQ 问题都已被证明是 NP 完全的[1]。

有限域上的矩阵在密码学中有广泛应用，如 2004 年 Mukesh[2]提出基于有限域矩阵公钥加密体制，其安全性基于解有限域多变量同余方程组的困难性；2005 年 Stickel[3]设计了基于有限域矩阵的秘钥交换协议；2008 年 Shpilrain[4]对其进行了密码分析，指出该方案不能抵抗线性代数攻击。

近年来，Pei 和 Zhao 等[5~13]在研究多变量密码体制时提出了遍历矩阵（ergodic matrix）的概念。研究结果表明，有限域上的遍历矩阵在乘法下的周期最大，有限域上遍历矩阵的双侧幂乘问题一般是 NP 完全问题（它一般可归约为 BMQ 问题）。

如果有限域 F_p 上的 n 阶矩阵 $\boldsymbol{Q}$ 的周期为

收稿日期：2014-06-01；**修回日期**：2015-05-23

基金项目：国家自然科学基金资助项目(61462016,11261018)；贵州省科学技术基金资助项目([2014]2125, 2142)；贵州师范大学博士基金资助项目([2014]11904-0514021)

Foundation Items: The National Natural Science Foundation of China (61462016,11261018); The Science and Technology Foundation of Guizhou Province ([2014]2125, 2142); The Doctorial Foundation of Guizhou Normal University ([2014]11904-0514021)

p^n-1，那么矩阵 $\boldsymbol{Q}$ 称为遍历矩阵。已知遍历矩阵 $\boldsymbol{Q}_1$、$\boldsymbol{Q}_2$，非零矩阵 $\boldsymbol{M}$ 和 $\boldsymbol{P}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y$，求 x 和 y 的问题即为 TEME 问题。当 x=y，此时 TEME 问题称为 SEME 问题。在文献[9]中，Pei 等提出了第一个基于 TEME 问题的公钥密码体制（称为 PZZ1 密码体制）。文献[11]中 Pei 等又提出了基于 SEME 问题的随机预言机模型下 CCA 安全公钥密码体制（称为 PZZ2 密码体制）。

本文采用文献[4]的方法研究文献[9]和文献[11]提出的密码体制的安全性，详细分析了计算性 TEME 问题和 SEME 问题的计算复杂度，证明了如下结论。

1) 计算性 TEME 问题在多项式时间内可解，因此 PZZ1 密码体制被完全攻破。

2) 如果将矩阵 $\boldsymbol{P},\boldsymbol{Q}_1\boldsymbol{P},\cdots,\boldsymbol{Q}_1^{n-1}\boldsymbol{P},\boldsymbol{M},\boldsymbol{M}\boldsymbol{Q}_2,\cdots,\boldsymbol{M}\boldsymbol{Q}_2^{n-1}$ 都按行看做 $2n$ 个 n^2 维向量，若它们的秩等于 $2n-1$，则 SEME 问题在多项式时间内可归约为离散对数问题，因此若 PZZ2 密码体制的秘钥参数选取不当，其安全性将不是基于 NP 困难问题，实际上仍是基于离散对数问题。

2 预备知识

在本文中 p 为素数，$q=p^n$，F_p、F_q 都为有限域，$\boldsymbol{M}_n(F_p)$ 表示 F_p 上 $n\times n$ 矩阵的集合，$\boldsymbol{I}_n$ 和 $\boldsymbol{0}_n$ 分别表示有限域 F_p 上的 n 阶单位矩阵和零矩阵（有时简记为 $\boldsymbol{I}$ 和 $\boldsymbol{0}$）。

令 F_q 为有限域，$a\in F_q$。如果 a 的阶为 $q-1$(即 $q-1$ 是最小的正整数使 $a^{q-1}=1$)，则 a 称为本原元。$F_p[x]$ 中满足 $m(a)=0$ 的次数最小的多项式称为 a 在 F_p 上的极小多项式。令 $f\in F_p[x]$ 为 n 次多项式。如果 f 是 F_{p^n} 的一个本原元的极小多项式，则称 f 为有限域 F_p 的本原多项式。

定义 1[11] 令 $\boldsymbol{Q}\in\boldsymbol{M}_n(F_p)$。若 $\boldsymbol{Q}$ 的周期为 p^n-1（即 p^n-1 是使 $\boldsymbol{Q}^k=\boldsymbol{I}_n$ 成立的最小正整数 k），则称 $\boldsymbol{Q}$ 为 F_p 上的遍历矩阵(ergodic matrices)。

定义 2[11] 令 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 为 F_p 上的 n 阶遍历矩阵，$\boldsymbol{M}$ 为非零矩阵，$\boldsymbol{P}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y$。已知 $\boldsymbol{Q}_1$、$\boldsymbol{Q}_2$、$\boldsymbol{M}$、$\boldsymbol{P}$ 求解 x 和 y 的问题称为 TEME(two side ergodic matrices exponentiation)问题。

定义 3 令 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 为 F_p 上的 n 阶遍历矩阵，$\boldsymbol{M}$ 为非零矩阵，$\boldsymbol{P}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^x$。已知 $\boldsymbol{Q}_1$、$\boldsymbol{Q}_2$、$\boldsymbol{M}$、$\boldsymbol{P}$ 求解 x 的问题称为 SEME(symmetric ergodic matrices exponentiation)问题。

引理 1[6,13] 令 $\boldsymbol{Q}$ 为 F_p 上的 n 阶遍历矩阵。则

$$F_{p^n}\cong F_p[\boldsymbol{Q}]=\{\boldsymbol{M}\mid\boldsymbol{M}=a_0\boldsymbol{I}+a_1\boldsymbol{Q}+a_2\boldsymbol{Q}^2+\cdots+a_{n-1}\boldsymbol{Q}^{n-1},a_0,a_1,\cdots,a_{n-1}\in F_p\}$$

引理 2[13] 令 $\boldsymbol{Q}$ 为 F_p 上的 n 阶遍历矩阵，则 $\boldsymbol{Q}$ 的特征多项式是 F_p 上的 n 阶本原多项式。反之，F_p 上的 n 阶本原多项式的友矩阵是 F_p 上的 n 阶遍历矩阵。

引理 3[14] n 次首一多项式 $f(x)\in F_p[x]$ 为 F_p 上的本原多项式，当且仅当 $(-1)^n f(0)$ 为 F_p 的本原元且使 x^r 模 $f(x)$ 同余于 F_p 的某个元的最小正整数 $r=\dfrac{(p^n-1)}{p-1}$。当 $f(x)$ 为 F_p 上的本原多项式时，$x^r\equiv(-1)^n f(0)(\mathrm{mod}\, f(x))$。

定理 1 令 $\boldsymbol{Q}$ 为 F_p 上的 n 阶遍历矩阵且 $f(x)$ 为 $\boldsymbol{Q}$ 的特征多项式，则 $s=(-1)^n f(0)$ 为 F_p 的本原元且 $\boldsymbol{Q}^r=s\boldsymbol{I}_n$，其中，$r=\dfrac{(p^n-1)}{p-1}$。

证明 由引理 2 可知，$f(x)$ 为 F_p 上的 n 次本原多项式，再由引理 3 可知，$s=(-1)^n f(0)$ 是 F_p 的本原元且 $x^r\equiv s(\mathrm{mod}\, f(x))$。因此存在 $g(x)\in F_p[x]$ 使 $x^r-s=g(x)f(x)$。从而 $\boldsymbol{Q}^r-s\boldsymbol{I}_n=g(\boldsymbol{Q})f(\boldsymbol{Q})=0_n$，故 $\boldsymbol{Q}^r=s\boldsymbol{I}_n$。

3 PZZ1 密码体制的密码分析

在文献[9]中，Pei 等提出类似 Elgamal 密码体制的方案（简称 PZZ1 密码体制）。下面先对其进行描述，然后分析它的安全性。

3.1 PZZ1 密码体制的描述

公开参数。$\boldsymbol{Q}_1,\boldsymbol{Q}_2\in\boldsymbol{M}_n(F_p)$ 为遍历矩阵，$\boldsymbol{M}\in\boldsymbol{M}_n(\boldsymbol{F}_p)$ 为非零矩阵。

私钥：$x,y\in\{1,2,\cdots,p^n-1\}$

公钥：$\boldsymbol{P}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y$

1) 加密

设明文 $X\in\boldsymbol{M}_n(F_p)$，选取随机数 $r,r'\in\{1,2,\cdots,p^n-1\}$，计算

$$C_1=\boldsymbol{Q}_1^r\boldsymbol{M}\boldsymbol{Q}_2^{r'},\qquad C_2=\boldsymbol{Q}_1^r\boldsymbol{P}\boldsymbol{Q}_2^{r'}+X$$

输出密文为 $C=(C_1,C_2)$

2) 解密

收到密文 $C=(C_1,C_2)$，计算 $C_2-\boldsymbol{Q}_1^xC_1\boldsymbol{Q}_2^y$ 并输出。

3.2　破解 PZZ1 密码体制

为分析 PZZ1 密码体制的安全性，先引入计算性 TEME 问题。

定义 4　（计算性 TEME 问题(CTEME)）设 $\boldsymbol{Q}_1,\boldsymbol{Q}_2\in\boldsymbol{M}_n(F_q)$ 为遍历矩阵，非零矩阵 $\boldsymbol{M}\in\boldsymbol{M}_n(F_q)$，$x,y\in\{1,2,\cdots,p^n-1\}$，$\boldsymbol{P}_1=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y$，$\boldsymbol{P}_2=\boldsymbol{Q}_1^{x'}\boldsymbol{M}\boldsymbol{Q}_2^{y'}$。已知 $\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{P}_1,\boldsymbol{P}_2$，求 $\boldsymbol{Q}_1^{x+x'}\boldsymbol{M}\boldsymbol{Q}_2^{y+y'}$。

定理 2　解决 CTEME 问题的有效算法能用来对 PZZ1 密文解密。

证明　假设存在有效算法 M1 能够解决 CTEME 问题。如果 PZZ 密文为 (C_1,C_2)，那么就输入 $\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y=\boldsymbol{P}$ 和 $\boldsymbol{Q}_1^{x'}\boldsymbol{M}\boldsymbol{Q}_2^{y'}=C_1$。于是 M1 输出 $\boldsymbol{Q}_1^{x+x'}\boldsymbol{M}\boldsymbol{Q}_2^{y+y'}$。由于 $X=C_2-\boldsymbol{Q}_1^xC_1\boldsymbol{Q}_2^y=C_2-\boldsymbol{Q}_1^{x+x'}\boldsymbol{M}\boldsymbol{Q}_2^{y+y'}$，可得到明文 X。

定理 3　CTEME 问题在多项式时间内可解。因此 PZZ1 密码体制可以在无需提供私钥时破解密文。

证明　令 $\boldsymbol{Q}_1,\boldsymbol{Q}_2\in\boldsymbol{M}_n(F_p)$ 为遍历矩阵，$\boldsymbol{M}\in\boldsymbol{M}_n(F_p)$ 为非零矩阵。设 $\boldsymbol{P}_1=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y$，$\boldsymbol{P}_2=\boldsymbol{Q}_1^{x'}\boldsymbol{M}\boldsymbol{Q}_2^{y'}$，其中，$x,y,x',y'\in\{1,2,\cdots,p^n-1\}$。

注意到解 CTEME 问题不需要解出 x,y,x',y'，只需伪造一对矩阵 $(\boldsymbol{Q}_1^{\tilde{x}},\boldsymbol{Q}_2^{\tilde{y}})$ 使 $\boldsymbol{P}_1=\boldsymbol{Q}_1^{\tilde{x}}\boldsymbol{M}\boldsymbol{Q}_2^{\tilde{y}}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y$。

由引理 1 可知，存在不全为 0 的 $x_i,y_i\in F_p(i=0,1,\cdots,n-1)$ 使

$$\boldsymbol{Q}_1^{-x}=x_0\boldsymbol{I}+x_1\boldsymbol{Q}_1+\cdots+x_{n-1}\boldsymbol{Q}_1^{n-1}$$
$$\boldsymbol{Q}_2^{y}=y_0\boldsymbol{I}+y_1\boldsymbol{Q}_2+\cdots+y_{n-1}\boldsymbol{Q}_2^{n-1}$$

因为 $\boldsymbol{Q}_1^{-x}\boldsymbol{P}_1=\boldsymbol{M}\boldsymbol{Q}_2^y$，所以

$$\begin{aligned}&x_0\boldsymbol{P}_1+x_1\boldsymbol{Q}_1\boldsymbol{P}_1+\cdots+x_{n-1}\boldsymbol{Q}_1^{n-1}\boldsymbol{P}_1\\&=y_0\boldsymbol{M}+y_1\boldsymbol{M}\boldsymbol{Q}_2+\cdots+y_{n-1}\boldsymbol{M}\boldsymbol{Q}_2^{n-1}\end{aligned}\tag{1}$$

由式 (1) 知，如果将矩阵 $\boldsymbol{P}_1$，$\boldsymbol{Q}_1\boldsymbol{P}_1$，…，$\boldsymbol{Q}_1^{n-1}\boldsymbol{P}_1,-\boldsymbol{M}$，$-\boldsymbol{M}\boldsymbol{Q}_2,\cdots,-\boldsymbol{M}\boldsymbol{Q}_2^{n-1}$ 都按行看做 $2n$ 个 n^2 维向量，则它们的秩小于 $2n$。不妨设它们的秩为 $2n-1$（其他情况可类似证明。）

将式(1)整理后，可得线性方程组的系数矩阵为 $(\boldsymbol{P}_1,\boldsymbol{Q}_1\boldsymbol{P}_1,\cdots,\boldsymbol{Q}_1^{n-1}\boldsymbol{P}_1,-\boldsymbol{M},-\boldsymbol{M}\boldsymbol{Q}_2,\cdots,-\boldsymbol{M}\boldsymbol{Q}_2^{n-1})$，其中，$\boldsymbol{P}_1,\boldsymbol{Q}_1\boldsymbol{P}_1,\cdots,\boldsymbol{Q}_1^{n-1}\boldsymbol{P}_1,-\boldsymbol{M}$，$-\boldsymbol{M}\boldsymbol{Q}_2,\cdots,-\boldsymbol{M}\boldsymbol{Q}_2^{n-1}$ 都按行写成 n^2 维列向量。既然矩阵的行秩等于列秩，通过高斯消元法，可得到一个具有 $2n$ 个未知数 $x_i,y_i(i=0,1,n-1)$，$2n-1$ 个方程的线性方程组。解出它的一个特解

$$(x_0,x_1,\cdots,x_{n-1})=(a_0,a_1,\cdots,a_{n-1})$$
$$(y_0,y_1,\cdots,y_{n-1})=(b_0,b_1,\cdots,b_{n-1})$$

令

$$\boldsymbol{Q}_1^{-\tilde{x}}=a_0\boldsymbol{I}+a_1\boldsymbol{Q}_1+\cdots+a_{n-1}\boldsymbol{Q}_1^{n-1}$$
$$\boldsymbol{Q}_2^{\tilde{y}}=b_0\boldsymbol{I}+b_1\boldsymbol{Q}_2+\cdots+b_{n-1}\boldsymbol{Q}_2^{n-1}$$

显然，$\boldsymbol{Q}_1^{-\tilde{x}}\boldsymbol{P}_1=\boldsymbol{M}\boldsymbol{Q}_2^{\tilde{y}}$，因此 $\boldsymbol{P}_1=\boldsymbol{Q}_1^{\tilde{x}}\boldsymbol{M}\boldsymbol{Q}_2^{\tilde{y}}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y$。计算 $\boldsymbol{Q}_1^{\tilde{x}}=(\boldsymbol{Q}_1^{-\tilde{x}})^{-1}$。既然

$$\begin{aligned}\boldsymbol{Q}_1^{x+x'}\boldsymbol{M}\boldsymbol{Q}_2^{y+y'}&=\boldsymbol{Q}_1^{x'}(\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y)\boldsymbol{Q}_2^{y'}\\&=\boldsymbol{Q}_1^{x'}(\boldsymbol{Q}_1^{\tilde{x}}\boldsymbol{M}\boldsymbol{Q}_2^{\tilde{y}})\boldsymbol{Q}_2^{y'}\\&=\boldsymbol{Q}_1^{\tilde{x}}(\boldsymbol{Q}_1^{x'}\boldsymbol{M}\boldsymbol{Q}_2^{y'})\boldsymbol{Q}_2^{\tilde{y}}\\&=\boldsymbol{Q}_1^{\tilde{x}}\boldsymbol{P}_2\boldsymbol{Q}_2^{\tilde{y}}\end{aligned}$$

可解出 $\boldsymbol{Q}_1^{x+x'}\boldsymbol{M}\boldsymbol{Q}_2^{y+y'}$。这就证明了 CTEME 问题在多项式时间内可解。由定理 2 可知，PZZ1 密码体制可以在无需提供私钥时破解密文。

例 1　令 p=7, n=2, $\boldsymbol{Q}_1=\begin{pmatrix}0&1\\4&6\end{pmatrix}$, $\boldsymbol{Q}_2=\begin{pmatrix}0&1\\2&2\end{pmatrix}$, $\boldsymbol{M}=\begin{pmatrix}0&1\\2&3\end{pmatrix}$。易验证 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 是 F_7 上的遍历矩阵。取 $x=3$，$y=10$，$x'=9$，$y'=20$。则

$$\boldsymbol{P}_1=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y=\begin{pmatrix}5&3\\2&2\end{pmatrix},\quad \boldsymbol{P}_2=\boldsymbol{Q}_1^{x'}\boldsymbol{M}\boldsymbol{Q}_2^{y'}=\begin{pmatrix}5&1\\5&4\end{pmatrix}$$

给定 $(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{P}_1,\boldsymbol{P}_2)$，利用定理 3 的方法计算 $\boldsymbol{Q}_1^{x+x'}\boldsymbol{M}\boldsymbol{Q}_2^{y+y'}$。

解　设 $\boldsymbol{Q}_1^{-x}=x_0\boldsymbol{I}+x_1\boldsymbol{Q}_1,\boldsymbol{Q}_2^y=y_0\boldsymbol{I}+y_1\boldsymbol{Q}_2$。由

$$\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y=\begin{pmatrix}5&3\\2&2\end{pmatrix}$$

可得到如下的线性方程组

$$\begin{cases}5x_0+2x_1+5y_1=0\\3x_0+2x_1+6y_0+5y_1=0\\2x_0+4x_1+5y_0+y_1=0\\2x_0+3x_1+4y_0+6y_1=0\end{cases}$$

解出一组特解为 $(x_0,x_1,y_0,y_1)=(3,4,1,1)$。

计算

$$\boldsymbol{Q}_1^{-\tilde{x}}=x_0\boldsymbol{I}+x_1\boldsymbol{Q}_1=\begin{pmatrix}3&4\\2&6\end{pmatrix}$$

$$\boldsymbol{Q}_1^{\tilde{x}}=\begin{pmatrix}3&4\\2&6\end{pmatrix}^{-1}=\begin{pmatrix}2&1\\4&1\end{pmatrix}$$

$$\boldsymbol{Q}_2^{\tilde{y}}=y_0\boldsymbol{I}+y_1\boldsymbol{Q}_2=\begin{pmatrix}1&1\\2&3\end{pmatrix}$$

最后计算 $\boldsymbol{Q}_1^x\boldsymbol{P}_2\boldsymbol{Q}_2^y=\begin{pmatrix}2&1\\4&1\end{pmatrix}\begin{pmatrix}5&1\\5&4\end{pmatrix}\begin{pmatrix}1&1\\2&3\end{pmatrix}=\begin{pmatrix}6&5\\6&0\end{pmatrix}$。（可以验证结果恰好等于 $\boldsymbol{Q}_1^{x+x'}\boldsymbol{M}\boldsymbol{Q}_2^{y+y'}$。）

注：定理 3 和例 1 表明，PZZ1 密码体制可以在无需提供私钥时破解密文。因此 PZZ1 密码体制可被完全攻破。

4 PZZ2 密码体制的安全性

在文献[11]中，Pei 等设计了类似于 DHIES 密码体制的基于遍历矩阵 SEME 问题的密码体制（简称 PZZ2 密码体制）。本文首先描述该方案的具体步骤，然后分析该方案的安全性核心 SEME 问题的困难性。

4.1 PZZ2 密码体制的描述

本节引用文献[11]。令 SYM=$(\overline{E},\overline{D})$ 表示密钥长度为 *elen* 的对称密码体制。令 MAC=(J,V) 表示密钥长度为 *mlen* 的消息认证码。令 $H:M_n(F_p)\to(0,1)^{mlen+elen}$ 为一将矩阵表示成二进制位串的散列函数。

令基于遍历矩阵的公钥密码体制为 PZZ2=(E,D,K)，其由密钥生成算法 K、加密算法 E 和解密算法 D 组成。

密钥生成算法 K 为

Algorithm K

Begin

$x\leftarrow\{1,\cdots,q^n-1\}$

$pk\leftarrow Q_1^xMQ_2^x$

$sk\leftarrow x$

return (pk,sk)

End

加密算法 E 为

Algorithm $E(pk=Q_1^xMQ_2^x,m)$

Begin

$u\leftarrow\{1,\cdots,q^n-1\}$

$\boldsymbol{Z}\leftarrow\boldsymbol{Q}_1^u pk\boldsymbol{Q}_2^u$

$\boldsymbol{U}\leftarrow\boldsymbol{Q}_1^u\boldsymbol{M}\boldsymbol{Q}_2^u$

$hash\leftarrow H(Z)$

$macKey\leftarrow hash^{[1,\cdots,mlen]}$

$encKey\leftarrow hash[mlen+1\cdots mlen+elen]$

$encM\leftarrow\overline{E}(encKey,m)$

$tag\leftarrow J(macKey,encM)$

$c\leftarrow U\|encM\|tag$

return (pk,sk)

End

解密算法 D 为

Algorithm $D(sk=x,c)$

Begin

$U\|encM\|tag\leftarrow c$

$\boldsymbol{Z}\leftarrow\boldsymbol{Q}_1^{sk}\boldsymbol{U}\boldsymbol{Q}_2^{sk}$

$hash\leftarrow H(Z)$

if $V(macKey,encM,tag)=0$

then return *BAD*

$m\leftarrow\overline{D}(encKey,encM)$

return m

End

4.2 SEME 问题与离散对数问题的关系

容易看到 PZZ2 密码体制中，由公钥求私钥实际上是 SEME 问题，它是 TEME 问题的特例。下面证明 SEME 问题在某些情况下并不是 NP 问题，其实质仍然是离散对数问题。

定理 4 令 $r=\dfrac{(p^n-1)}{p-1}$，$\boldsymbol{Q}_1^r=s_1\boldsymbol{I},\boldsymbol{Q}_2^r=s_2\boldsymbol{I}$，$\boldsymbol{P}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^x$。如果 $(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{P})$ 满足以下条件。

1) 将矩阵 $\boldsymbol{P},\boldsymbol{Q}_1\boldsymbol{P},\cdots,\boldsymbol{Q}_1^{n-1}\boldsymbol{P},-\boldsymbol{M},-\boldsymbol{M}\boldsymbol{Q}_2,\cdots,-\boldsymbol{M}\boldsymbol{Q}_2^{n-1}$ 都按行看做 $2n$ 个 n^2 维向量，它们的秩等于 $2n-1$。

2) 若 $(1+(\log_{s_1}s_2)^{-1}\bmod p,\ p-1)=1$，那么 SEME 问题在多项式时间内可归约为离散对数问题。

证明 令 $\boldsymbol{Q}_1,\boldsymbol{Q}_2\in\boldsymbol{M}_n(F_p)$ 为遍历矩阵，$\boldsymbol{M}\in\boldsymbol{M}_n(F_p)$ 为非零矩阵，$\boldsymbol{P}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^x$，其中，$x\in\{1,2,\cdots,p^n-1\}$，下面试图求解 x。

由引理 1 可知，存在不全为 0 的 $x_i,y_i\in F_p(i=0,1,n-1)$ 使

$$\boldsymbol{Q}_1^{-x}=x_0\boldsymbol{I}+x_1\boldsymbol{Q}_1+\cdots+x_{n-1}\boldsymbol{Q}_1^{n-1}$$

$$\boldsymbol{Q}_2^{x}=y_0\boldsymbol{I}+y_1\boldsymbol{Q}_2+\cdots+y_{n-1}\boldsymbol{Q}_2^{n-1}$$

由 $\boldsymbol{Q}_1^{-x}\boldsymbol{P}=\boldsymbol{M}\boldsymbol{Q}_2^x$，若 $\boldsymbol{P},\boldsymbol{Q}_1\boldsymbol{P},\cdots,\boldsymbol{Q}_1^{n-1}\boldsymbol{P},-\boldsymbol{M},-\boldsymbol{M}\boldsymbol{Q}_2,\cdots,-\boldsymbol{M}\boldsymbol{Q}_2^{n-1}$ 按行看作 $2n$ 个 n^2 维向量，则它们的秩小于 $2n$。根据定理 4 的条件 1)，它们的秩为 $2n-1$。类似于定理 3 的证明，利用高斯消元法可得一个具有 $2n$ 个未知数 $x_i,y_i(i=0,1,n-1)$，$2n-1$ 个方程的线性方程组。解出它的一个特解

$$(x_0,x_1,\cdots,x_{n-1})=(a_0,a_1,\cdots,a_{n-1})$$

$$(y_0,y_1,\cdots,y_{n-1})=(b_0,b_1,\cdots,b_{n-1})$$

令

$$a(\boldsymbol{Q}_1)=a_0\boldsymbol{I}+a_1\boldsymbol{Q}_1+\cdots+a_{n-1}\boldsymbol{Q}_1^{n-1}$$

显然，$\boldsymbol{Q}_1^{-x}, a(\boldsymbol{Q}_1)$ 之商可以是一个常数。故存在 $k\in F_p^*$，使 $\boldsymbol{Q}_1^{-x}=ka(\boldsymbol{Q}_1)$，$\boldsymbol{Q}_2^{x}=kb(\boldsymbol{Q}_2)$。从而有

$$\begin{cases}\log_{\boldsymbol{Q}_1}(ka(\boldsymbol{Q}_1))\equiv(-x)\\ \log_{\boldsymbol{Q}_2}(kb(\boldsymbol{Q}_2))\equiv x\end{cases}\quad(\mathrm{mod}(p^n-1))\qquad(2)$$

(下文中未注明的情形≡都表示 $\mathrm{mod}(p^n-1)$ 相等。)

由式（2）可得

$$\log_{\boldsymbol{Q}_1}(k\boldsymbol{I})+\log_{\boldsymbol{Q}_2}(k\boldsymbol{I})\equiv-(\log_{\boldsymbol{Q}_1}(a(\boldsymbol{Q}_1))+\log_{\boldsymbol{Q}_2}(b(\boldsymbol{Q}_2)))\qquad(3)$$

既然 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 是 F_p 上的遍历矩阵，由定理 1 可知，存在 F_p 的 2 个本原元 s_1,s_2 使 $\boldsymbol{Q}_1^r=s_1\boldsymbol{I},\boldsymbol{Q}_2^r=s_2I$，其中，$r=\dfrac{(p^n-1)}{(p-1)}$。因此

$$\log_{\boldsymbol{Q}_1}(s_1\boldsymbol{I})\equiv\log_{\boldsymbol{Q}_2}(s_2\boldsymbol{I})\equiv r$$

设 $k=s_1^{z_1}=s_2^{z_2}$，即 $z_1=\log_{s_1}k, z_2=\log_{s_2}k$。从而

$$\begin{aligned}\log_{\boldsymbol{Q}_1}(kI)+\log_{\boldsymbol{Q}_2}(kI)&\equiv\log_{\boldsymbol{Q}_1}(s_1^{z_1}I)+\log_{\boldsymbol{Q}_2}(s_2^{z_2}I)\\&\equiv\log_{\boldsymbol{Q}_1}(s_1I)^{z_1}+\log_{\boldsymbol{Q}_2}(s_2I)^{z_2}\\&\equiv z_1\log_{\boldsymbol{Q}_1}(s_1I)+z_2\log_{\boldsymbol{Q}_2}(s_2I)\\&\equiv z_1r+z_2r\\&\equiv r(\log_{s_1}k+\log_{s_2}k)\\&\equiv r(\log_{s_1}k+\frac{\log_{s_1}k}{\log_{s_1}s_2})\\&\equiv r\log_{s_1}k(1+(\log_{s_1}s_2)^{-1})\end{aligned}$$

由式（3）可得

$$r\log_{s_1}k(1+(\log_{s_1}s_2)^{-1})\equiv-(\log_{\boldsymbol{Q}_1}(a(\boldsymbol{Q}_1))+\log_{\boldsymbol{Q}_2}(b(\boldsymbol{Q}_2)))\qquad(4)$$

将式（4）左右两边约去 r 可得

$$\log_{s_1}k(1+(\log_{s_1}s_2)^{-1})\equiv\frac{-(\log_{\boldsymbol{Q}_1}(a(\boldsymbol{Q}_1))+\log_{\boldsymbol{Q}_2}(b(\boldsymbol{Q}_2)))}{r}(\mathrm{mod}\,p-1)$$

由定理 4 的条件 2)易知，

$$\log_{s_1}k\equiv\frac{-(\log_{\boldsymbol{Q}_1}(a(\boldsymbol{Q}_1))+\log_{\boldsymbol{Q}_2}(b(\boldsymbol{Q}_2)))}{r}(1+(\log_{s_1}s_2)^{-1})^{-1}(\mathrm{mod}\,p-1)$$

求解出唯一的 k 只需计算 3 个离散对数 $\log_{s_1}s_2$，$\log_{\boldsymbol{Q}_1}(a(\boldsymbol{Q}_1))$ 和 $\log_{\boldsymbol{Q}_2}(b(\boldsymbol{Q}_2))$。再由式（2）可知，$x\equiv\log_{\boldsymbol{Q}_2}(kb(\boldsymbol{Q}_2))$，故再计算一个离散对数即得唯一解 x。其中，定理 4 的方法本质上是解模 (p^n-1) 同余的二元一次方程组式（2），其未知数为 k 和 x。

如果定理 4 的条件 1)不成立，则 $\boldsymbol{P},\boldsymbol{Q}_1\boldsymbol{P}$,…, $\boldsymbol{Q}_1^{n-1}\boldsymbol{P},\boldsymbol{M},\boldsymbol{MQ}_2$,…, $\boldsymbol{MQ}_2^{n-1}$ 的秩一定小于 2n−1。此时利用定理 4 的方法不能求出 x，因为得到类似于式(2)的同余方程组仍只有 2 个方程，而未知数超过 2 个。

如果定理 4 的条件 2)不成立，此时利用定理 3 的方法会求解出多个结果，到底哪个是真解仍无法判断，见例 2。

例 2　令 p=7, n=2, $\boldsymbol{Q}_1=\begin{pmatrix}0&1\\4&6\end{pmatrix}$, $\boldsymbol{Q}_2=\begin{pmatrix}0&1\\2&2\end{pmatrix}$, $\boldsymbol{M}=\begin{pmatrix}0&1\\2&3\end{pmatrix}$。取 $x=25$，则 $\boldsymbol{P}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^x=\begin{pmatrix}6&1\\2&0\end{pmatrix}$。

给定 $(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{P})$，利用定理 4 的方法通过解离散对数计算 x。

解　设 $\boldsymbol{Q}_1^{-x}=x_0\boldsymbol{I}+x_1\boldsymbol{Q}_1,\boldsymbol{Q}_2^{x}=y_0\boldsymbol{I}+y_1\boldsymbol{Q}_2$。由

$$\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^x=\begin{pmatrix}6&1\\2&0\end{pmatrix}$$

得到如下的线性方程组

$$\begin{cases}6x_0+2x_1+5y_1=0\\x_0+6y_0+5y_1=0\\2x_0+x_1+5y_0+y_1=0\\4x_1+4y_0+6y_1=0\end{cases}$$

可以验证其系数矩阵的秩为 3，解出一组特解为 $(x_0,x_1,y_0,y_1)=(2,2,0,1)$。

计算

$$a(\boldsymbol{Q}_1)=x_0\boldsymbol{I}+x_1\boldsymbol{Q}_1=\begin{pmatrix}2&2\\1&0\end{pmatrix}$$

$$b(\boldsymbol{Q}_2)=y_0\boldsymbol{I}+y_1\boldsymbol{Q}_2=\begin{pmatrix}0&1\\2&2\end{pmatrix}$$

计算离散对数 $\log_{\boldsymbol{Q}_1}(a(\boldsymbol{Q}_1))=47$, $\log_{\boldsymbol{Q}_2}(b(\boldsymbol{Q}_2))=1$。

由 $\boldsymbol{Q}_1^r=3\boldsymbol{I}$, $\boldsymbol{Q}_2^r=5\boldsymbol{I}$ $\left(r=\dfrac{7^2-1}{7-1}=8\right)$，得 $s_1=3,s_2=5$。

根据式(4)，得到关于 k 的同余方程

$$8\log_3k(1+(\log_35)^{-1})\equiv-(47+1)\ (\mathrm{mod}\ 48)$$

左右两边约去 8，可得

$$\log_3k(1+(\log_35)^{-1})\equiv0\ (\mathrm{mod}\ 6)$$

求解离散对数 $\log_35=5(\mathrm{mod}\,7)$，代入可得

$$4\log_3k\equiv0\ (\mathrm{mod}\ 6)$$

从而 $\log_3k\equiv0\ (\mathrm{mod}\ 3)$，解得 k=1 或 6。最后计算离散对数 $\log_{\boldsymbol{Q}_2}(kb(\boldsymbol{Q}_2))$ 得 x=1 或 25（其中 x=25

是真解）。之所以有 2 个解，是因为(4, 6)=2，不满足定理 4 的条件 2)。

4.3 改进的密钥生成算法

从 4.2 节的分析可知，如果 PZZ2 密码体制的秘钥参数同时满足定理 4 的 2 个条件，那么它也不是基于 NP 困难问题，其实质仍是基于离散对数问题的密码体制。既然 PZZ2 方案使用矩阵作为公钥且加解密步骤中都有矩阵模指数运算，因而在这种情况下 PZZ2 密码体制与基于有限域乘法群上离散对数问题的密码体制相比并没有优势，反而效率较低。

要使 PZZ2 密码体制优于基于离散对数问题的公钥密码，其公钥和私钥不能同时满足定理 3 的 2 个条件，这时从公钥求私钥不能归约为离散对数问题。因此，如果使用 PZZ2 密码体制，就有必要改进其密钥生成算法，改进的密钥生成算法如下。

1) 生成奇素数 p，使其满足

$$\left(\left(\frac{p-3}{2}\right)^{-1}, p-1\right)=1$$

2) 调用本原多项式生成算法，生成有限域 F_p 上的 n 次首一本原多项式 $f(x)$，并计算 $s_1=(-1)^n f(0)$。将 $f(x)$的友矩阵作为第 1 个遍历矩阵 $\boldsymbol{Q}_1$。

3) 计算 $s_2=s_1^{\left(\frac{p-3}{2}\right)^{-1}}$，生成另一个 n 次首一本原多项式 $g(x)$满足 $s_2=(-1)^n g(0)$。将 $g(x)$的友矩阵作为第 2 个遍历矩阵 $\boldsymbol{Q}_2$。

4) 随机选取 $x\in\{1,2,\cdots,p^n-1\}$。

5) 随机选取非零矩阵 $\boldsymbol{M}\in\boldsymbol{M}_n(F_p)$。计算 $\boldsymbol{P}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^x$。计算 $\boldsymbol{Q}_1\boldsymbol{P}$,$\cdots$, $\boldsymbol{Q}_1^{n-1}\boldsymbol{P}$, $\boldsymbol{M}\boldsymbol{Q}_2$,$\cdots$, $\boldsymbol{M}\boldsymbol{Q}_2^{n-1}$。

6) 求 $n^2\times 2n$ 矩阵

$$(\boldsymbol{P}_1,\boldsymbol{Q}_1\boldsymbol{P}_1,\cdots,\boldsymbol{Q}_1^{n-1}\boldsymbol{P}_1,-\boldsymbol{M},-\boldsymbol{M}\boldsymbol{Q}_2,\cdots,-\boldsymbol{M}\boldsymbol{Q}_2^{n-1})$$

的秩 r（其中，$\boldsymbol{P}_1,\boldsymbol{Q}_1\boldsymbol{P}_1,\cdots,\boldsymbol{Q}_1^{n-1}\boldsymbol{P}_1,-\boldsymbol{M},-\boldsymbol{M}\boldsymbol{Q}_2,\cdots,-\boldsymbol{M}\boldsymbol{Q}_2^{n-1}$ 都按行写成 n^2 维列向量）。若 $r<2n-1$，输出 $(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{P})$ 作为公钥，输出 x 作为私钥；若 $r\geqslant 2n-1$，返回步骤 5)重新选择 $\boldsymbol{M}$。

其中，算法的步骤 1)~步骤 3)可保证密钥参数不满足定理 4 的条件 2)。$\left(\left(\frac{p-3}{2}\right)^{-1}, p-1\right)=1$ 使 s_2 一定是 F_p 的本原元。这时

$$1+(\log_{s_1} s_2)^{-1}=1+\left(\left(\frac{p-3}{2}\right)^{-1}\right)^{-1}=\frac{p-1}{2}$$

从而$(1+(\log_{s_1} s_2)^{-1}, p-1)=\frac{p-1}{2}\neq 1$。

算法的步骤 5)~步骤 6)可保证生成的密钥不满足定理 4 的条件 1)。

5 结束语

虽然 TEME 问题通常是 NP 困难的，但 PZZ1 密码体制是基于计算性 TEME 问题，PZZ2 密码体制是基于 SEME 问题。本文结果表明计算性 TEME 问题是多项式时间可解的，SEME 问题在一些情况下可多项式时间内归约为离散对数问题。

因此，由 PZZ1 密码体制的密文和公钥可以完全得到明文，该方案被完全破解。若 PZZ2 密码体制的秘钥参数选择不当，则它也不是基于 NP 困难问题，其实质仍是基于离散对数问题的密码体制。本文改进的密钥生成算法可避免这种情况，此时 PZZ2 密码体制很可能具有抗量子分析的特性。

参考文献：

[1] DING J T. Multi-Variate Public Key Cryptosystems[M]. Berlin: Springer-Verlag , 2006.

[2] MUKESH K S. Public key cryptography with matrices[A]. Proceedings of the IEEE Workshop on Information Assurance[C]. United States Military Academy, 2004. 146-152.

[3] STICKEL E. A new method for exchanging secret keys[A]. Proc of the Third International Conference on Information Technology and Applications (ICITA05) [C]. 2005. 426-430.

[4] SHPILRAIN V. Cryptanalysis of stickel's key exchange scheme[A]. Computer Science in Russia 2008, LNCS 5010 [C]. 2008. 283-288.

[5] ZHAO Y, WANG L, ZHANG W. Information-exchange using the ergodic matrices in GF(2) [A]. Proc ACNS 2004 [C]. Icisa Press, 2004. 388-397.

[6] 赵永哲, 黄声烈, 姜占华等. GF(2*k*)上的遍历矩阵及其特性分析[J]. 小型微型计算机系统, 2005, 26(12): 2135-2139.
ZHAO Y Z, HUANG S L, JIANG Z H, *et al*. Ergodic matrix over GF (2*k*) and its properties[J]. Mini-Micro Systems, 2005, 26(12): 2135-2139.

[7] 赵永哲，姜占华，黄声烈. 基于 F2 上遍历矩阵的 Shamir 三次传递协议的实现[J]. 小型微型计算机系统, 2006, 27(6):986-991.
ZHAO Y Z, JIANG Z H, HUANG S L. Implementation of Shamir's three pass protocol based on ergodic matrix over finite field[J]. Mini-

Micro Systems, 2006, 27(6):986-991.

[8] 赵永哲, 裴士辉, 王洪军等. 利用有限域上的遍历矩阵构造动态加密器[J]. 小型微型计算机系统, 2007, 28 (11): 2010-2014.
ZHAO Y Z, PEI S H, WANG H J, *et al*. Using the ergodic matrices over finite field to construct the dynamic encryptor[J]. Mini-Micro Systems, 2007, 28 (11):2010-2014.

[9] PEI S H, ZHAO Y Z, ZHAO H W. Construct public key encryption scheme using ergodic matrices over GF(2) [A]. TAMC 2007 [C]. Berlin, Springer-Verlag, 2007.181-188.

[10] PEI S H, ZHAO H W, ZHAO Y Z. Public key cryptography based on ergodic matrices over finite field[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6):1525-1528.

[11] 裴士辉, 赵永哲, 赵宏伟. 基于遍历矩阵的公钥加密方案[J]. 电子学报, 2010, 38(8) : 1908-1913.
PEI S H, ZHAO Y Z, ZHAO H W. Public key encryption scheme based on the ergodic matrices[J]. Chinese Journal of Electronics, 2010, 38(8):1908-1913.

[12] 赵永哲,赵博,裴士辉等. HFEM 公钥密码方案的设计与实现[J]. 通信学报,2011,32(6):24-31.
ZHAO Y Z, ZHAO B, PEI S H, *et al*. Design and implement on the HFEM public key scheme[J]. Journal on Communications, 2011,32(6): 24-31.

[13] 赵永哲,赵博,裴士辉. 有限域上遍历矩阵的特性研究[J]. 数学学报,2012,55(3):457-468.
ZHAO Y Z, ZHAO B, PEI S H. On the properties of the ergodic matrix over finite field[J]. ACTA Mathematica Sinica, 2012, 55(3): 457-468.

[14] LIDL R, NIEDERREITER H. Introduction to Finite Fields and Their Applications[M]. Cambridge: Cambridge University Press, 1986.

作者简介：

黄华伟（1978-），男，江西樟树人，贵州师范大学副教授，主要研究方向为密码学与信息安全。

彭长文（1980-），女，贵州大方人，贵州师范学院副教授，主要研究方向为差分方程及函数论。

瞿云云（1983-），男，贵州金沙人，贵州师范大学副教授，主要研究方向为密码学与信息安全。

李春华（1973-），男，江西宜丰人，华东交通大学副教授，主要研究方向为半群代数理论。