基于遍历矩阵的公钥加密方案的安全性分析

古春生[1,2],景征骏[1,3],于志敏[1],吴访升[1]
(1.江苏理工学院计算机工程学院,江苏常州 213001;2.中国科学技术大学计算机科学与技术学院,安徽合肥 230027;
3.南京邮电大学计算机学院,江苏南京 210003)

摘 要: 针对裴士辉等构造的基于遍历矩阵的公钥加密方案,本文使用遍历矩阵性质和线性化方法,证明破解该公钥加密方案不比求解多项式有限域上离散对数问题更难,从而证明了他们关于该公钥加密方案的安全归约证明是不正确的.

关键词: 公钥密码学; 遍历矩阵; 离散对数问题; 安全性分析
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2014)10-2081-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.10.033

Security on Public Key Encryption Scheme Based on Ergodic Matrices

GU Chun-sheng[1,2], JING Zheng-jun[1,3], YU Zhi-min[1], WU Fang-sheng[1]
(1. *School of Computer Engineering, Jiangsu University of Technology, Changzhou, Jiangsu* 213001, *China*;
2. *School of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui* 230027, *China*;
3. *School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*)

Abstract: For the public key encryption scheme based on the ergodic matrices constructed by Pei et al., this paper proves that breaking this scheme is not harder than solving polynomial discrete logarithm problem on finite field applying the properties of ergodic matrices and linearization method. Thus, we show that their proof of security is not correct for this public key encryption scheme.

Key words: public key cryptography; ergodic matrix; discrete logarithm problem; security analysis

1 引言

基于因式分解、离散对数、椭圆曲线对数等困难问题构造的密码原语效率高[1~3],但在量子计算机上这些基于数论上的困难问题的密码原语都已经被破解[4~6].如何设计抗量子的密码方案一直是密码研究热点之一.近年来,部分密码研究学者从基于遍历矩阵上困难问题角度研究构造抗量子密码原语的可能性[7~11].但这些基于遍历矩阵的密码原语实际安全性需要深入研究分析.

文献[7]系统研究了有限域上遍历矩阵的性质,文献[8~11]分别构造了基于遍历矩阵的动态加密器、公钥加密、密钥传递协议、单向函数等密码原语.2010 年,文献[12]构造了基于有限域上遍历矩阵的双侧幂乘问题(TEME, Two-side Ergodic Matrices Exponentiation)的公钥加密方案,并证明该公钥方案安全性等价于 NP 完全问题.通过分析可以发现,文献[12]中定理 8 的安全归约证明不正确,即它仅将 TEME 归约到二等分多变量二次方程组的求解问题(BMQ, Bisection Multivariate Quadratic equation problem),并未将 NP 完全的 BMQ 问题归约到 TEME 问题.本文主要分析证明文献[12]中的有限域上 TEME 问题的求解难度可以归约到求解多项式有限域上离散对数问题,从而证明了文献[12]中基于 TEME 问题的公钥加密方案的破解难度不可能比求多项式离散对数问题更难.尽管目前人们还不知道有限域上离散对数问题的具体计算复杂性,但该问题存在次指数时间算法.根据文献[13]中的指数积分算法(算法 3.68),计算在有限域 $F_{2^n}^*$ 上离散对数算法的期望运行时间为 $L_{2^n}[1/3,c]$,这里 $L_p[\alpha,c]=O(\exp((c+o(1))(\ln p)^{\alpha}(\ln\ln q)^{1-\alpha})$, $c<1.587$. 对于 $p=q^n$,$(q>2)$, Lovorn[14] 分析了指数积分算法的期望运行时间为 $L_{q^n}[1/2,\sqrt{2}]$.

收稿日期:2011-10-13;修回日期:2014-04-19;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61142007);江苏理工学院科研基金(No.KYY12027);江苏省高校自然科学研究(No.13KJB520005);江苏省普通高校研究生科研创新计划(No.CXZZ13_0493);教育部人文社会科学研究项目(No.14YJAZH023);江苏省“青蓝工程”项目

因此,文献[12]中的公钥加密方案存在次指数时间破解算法.同时,根据文献[4,5]中离散对数的多项式时间量子算法,易知文献[12]中公钥加密方案并不能抗量子计算机的攻击.

本文安全归约证明思想在直觉上是非常简单的,即首先给出 TEME 中子问题 2 的多项式时间求解算法,然后归约子问题 1 到多项式有限域上的离散对数问题.具体步骤是:(1)计算遍历矩阵 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 的特征多项式 $f_1(\lambda),f_2(\lambda)$;(2)计算求解矩阵 $\boldsymbol{Q}_1^x$ 和 $\boldsymbol{Q}_2^y$;(3)根据遍历矩阵 $\boldsymbol{Q}_i$ 的集$\{\boldsymbol{Q}_i^k\mid k\in Z\}$与模为 $f_i(\lambda)$的有限域上多项式 $g_i(\lambda)$一一对应关系,即如果 $g_i(\boldsymbol{Q}_i)=\boldsymbol{Q}_i^k$,则 $g_i(\lambda)=\lambda^k \bmod f_i(\lambda)$,故可有效求解矩阵 $\boldsymbol{Q}_1^x$ 和 $\boldsymbol{Q}_2^y$ 所对应的多项式.因此,破解基于遍历矩阵的公钥加密方案就归约到求解多项式有限域上离散对数问题.

2 基于遍历矩阵的公钥加密方案

设集合$[n]=\{1,2,\cdots,n\}$.设 F_q 为有限域,$F_q[\lambda]$为 F_q 上多项式集,$F_q^{n\times n}$ 为 F_q 上所有 $n\times n$ 矩阵集.设 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 为满秩遍历矩阵,满足 $\boldsymbol{Q}_1^{q^n-1},\boldsymbol{Q}_2^{q^n-1}$ 是单位矩阵 $\boldsymbol{I}_{n\times n}$,且$<\boldsymbol{Q}_1>=\{\boldsymbol{Q}_1^k\mid k\in Z\}$,$<\boldsymbol{Q}_2>=\{\boldsymbol{Q}_2^k\mid k\in Z\}$.

定义 1(BMQ-问题) 在 F_q 上方程组 E 共有 m 个方程和 $2n$ 个变量,每个方程形式如下:

$$\sum_{i=1}^{n}\sum_{j=1}^{n}a_{i,j}^{(k)}x_iy_j=b^{(k)},a_{i,j}^{(k)},b^{(k)}\in F_q,k\in[m]$$

试求方程组 E 的一个解$(x_1,\cdots,x_n,y_1,\cdots,y_n)\in F_q^{2n}$.

定义 2(TEME-问题) 设 $\boldsymbol{Q}_1,\boldsymbol{Q}_2\in F_q^{n\times n}$ 为遍历矩阵,$\boldsymbol{M}\in F_q^{n\times n}\setminus\{\boldsymbol{0}\}$,$s,t\in[q^n-1]$.已知$(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t)$,求指数 s,t.

子问题 1 设 $\boldsymbol{Q}\in F_q^{n\times n}$ 为遍历矩阵,给定$(\boldsymbol{Q},\boldsymbol{Q}^w)$,求指数 $w\in[q^n-1]$.

子问题 2 设 $\boldsymbol{Q}_1,\boldsymbol{Q}_2\in F_q^{n\times n}$ 为遍历矩阵,$\boldsymbol{M}\in F_q^{n\times n}\setminus\{0\}$,$s,t\in[q^n-1]$.给定$(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t)$,求矩阵 $\boldsymbol{Q}_1^s,\boldsymbol{Q}_2^t$.

基于遍历矩阵的公钥加密方案[12]如下:

密钥产生(KeyGen) (1)选择遍历矩阵 $\boldsymbol{Q}_1,\boldsymbol{Q}_2\in F_q^{n\times n}$,矩阵 $\boldsymbol{M}\in F_q^{n\times n}\setminus\{\boldsymbol{0}\}$和 $v\in[q^n-1]$;(2)输出私钥为 $sk=(v)$,公钥为 $pk=(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{M}_1=\boldsymbol{Q}_1^v\boldsymbol{M}\boldsymbol{Q}_2^v)$.

加密算法(Enc) 给定 pk 和明文 x.

(1)随机选择 $u\in[q^n-1]$,计算 $\boldsymbol{Z}=\boldsymbol{Q}_1^{uv}\boldsymbol{M}\boldsymbol{Q}_2^{uv}$,$\boldsymbol{U}=\boldsymbol{Q}_1^u\boldsymbol{M}\boldsymbol{Q}_2^u$,hash = $H(Z)$,macKey = hash[1..mLen],encKey = hash[mLen + 1..mLen + eLen], encM = Enc(encKey,x),tag = Tag(macKey,encM).

(2)输出密文 $y=\boldsymbol{U}\parallel$ encM $\parallel$ tag.

解密算法(Dec) 给定 sk 和密文 $y=\boldsymbol{U}\parallel$ encM $\parallel$ tag.

(1)由 $\boldsymbol{U}$ 计算得 $\boldsymbol{Z}=\boldsymbol{Q}_1^{wv}\boldsymbol{M}\boldsymbol{Q}_2^{wv}$,hash = $H(Z)$,macKey = hash[1..mLen], encKey = hash[mLen + 1..mLen + eLen].

(2)使用验证算法 V,如果 V(macKey,encM,tag) = 0,返回 BAD,否则解密输出明文 x = Dec(encKey,encM).

在上面公钥加密方案中的矩阵指数乘法,散列函数,对称加解密算法等密码原语与本文研究无关,故不进行重复定义,具体参见文献[12].

3 公钥加密方案安全性分析

3.1 子问题 2 的多项式时间算法

本小节在证明子问题 2 存在多项式时间算法之前,先给出遍历矩阵的特征多项式一个性质.

引理 1 如果遍历矩阵 $\boldsymbol{Q}$ 满足条件$|<\boldsymbol{Q}>|=q^n-1$,则 $\boldsymbol{Q}$ 的特征多项式$f(\lambda)$为 $F_q[\lambda]$上次数为 n 的不可约多项式.

证明 如果 $f(\lambda)=g(\lambda)h(\lambda)$为可约多项式,则 $\deg(g(\lambda))<n$,$\deg(h(\lambda))<n$.由于 $f(\lambda)=|\lambda\boldsymbol{I}-\boldsymbol{Q}|$,故 $f(\boldsymbol{Q})=g(\boldsymbol{Q})h(\boldsymbol{Q})=\boldsymbol{0}$.因此 $g(\boldsymbol{Q})=\boldsymbol{0}$或 $h(\boldsymbol{Q})=\boldsymbol{0}$.假定 $h(\boldsymbol{Q})=\boldsymbol{0}$,则遍历矩阵集 $<\boldsymbol{Q}>$中元素与多项式有限域 $F_q[\lambda]/<h(\lambda)>$中元素一一对应,即$|<\boldsymbol{Q}>|=|F_q[\lambda]/<h(\lambda)>|<q^n-1$,与引理中条件$|<\boldsymbol{Q}>|=q^n-1$矛盾. 证毕

由引理 1,可以得到 F_q 上 $F_q[\lambda]$模 $f(\lambda)$产生的多项式有限域与遍历矩阵同构.

定理 1 给定遍历矩阵 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$,如果矩阵 $\boldsymbol{M},\boldsymbol{M}_1$ 满足关系 $\boldsymbol{M}_1=\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t$,则存在求解矩阵 $s(\boldsymbol{Q}_1),t(\boldsymbol{Q}_2)$的多项式时间算法,满足关系 $\boldsymbol{M}_1=s(\boldsymbol{Q}_1)\times\boldsymbol{M}\times t(\boldsymbol{Q}_2)$.

证明 设 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 的特征多项式分别为 $f_1(\lambda)$,$f_2(\lambda)$.

步骤 1 由引理 1 知 $f_1(\lambda),f_2(\lambda)$为次数 n 的不可约多项式.因为 $f_1(\boldsymbol{Q}_1)=\boldsymbol{0},f_2(\boldsymbol{Q}_2)=\boldsymbol{0}$,故一定存在$(x_1,\cdots,x_n),(y_1,\cdots,y_n)$满足关系

$$\boldsymbol{Q}_1^s=\sum_{i=1}^{n}x_i\boldsymbol{Q}_1^{i-1} \tag{1}$$

$$\boldsymbol{Q}_2^t=\sum_{i=1}^{n}y_i\boldsymbol{Q}_2^{i-1} \tag{2}$$

将关系式(1)(2)代入矩阵等式 $\boldsymbol{M}_1=\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t$,并对它进行整理,可以获得 n^2 个关于$(x_1,\cdots,x_n),(y_1,\cdots,y_n)$的二次方程组.使用线性化方法,将 $z_{ij}=x_iy_j,i,j\in[n]$作为一个变量,则得到一个包含 n^2 个未知变量的线性方程组.设 $\boldsymbol{A}\boldsymbol{z}=\boldsymbol{b}$ 为线性化方法产生的方程组.因为该线性方程组存在可行解,故矩阵 $\boldsymbol{A}$ 的秩与增广矩

阵($\boldsymbol{A}\mid\boldsymbol{b}$)的秩相等.使用高斯消元法,一定可以将增广矩阵($\boldsymbol{A}\mid\boldsymbol{b}$)变换成如下形式:

$$\left[\begin{array}{cccccc|c} 1 & 0 & 0 & 0 & \cdots & 0 & b_1 \\ 0 & \ddots & 0 & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & 0 & \cdots & 0 & b_i \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{array}\right] \tag{3}$$

如果式(3)中变换后的增广矩阵的第 j 行系数部分全为 0,则第 j 行的 b_j 必为 0.否则方程组无解,与至少存在一个可行解矛盾.

步骤 2　如果 $\boldsymbol{A}(i,i)=1,\boldsymbol{A}(k,i)=0,\forall k\neq i$,那么第 i 行对应的变量取值为 b_i.如果某行为全 0,则该行所对应的变量取值为 0.

步骤 3　如果某一变量 $z_{ij}=x_iy_j=b_{i+n\times j}$,且 $b_{i+n\times j}\neq 0$,则取 $y_j=1,x_i=b_{i+n\times j}$.这里 $y_j=1$ 是任意的,可取值为 F_q 中的任意非零值.但是,当某个变量 y_j 的值被确定后,则与其相关的其他非零变量的值也就被相应确定.对于$\{x_1,\cdots,x_n,y_1,\cdots,y_n\}$中所有其他未取值变量都取值为 0.因此能够获得 $q-1$ 个满足关系 $\boldsymbol{M}_1=\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t$ 的解.

步骤 4　设$(x_1,\cdots,x_n),(y_1,\cdots,y_n)$为步骤 3 计算输出的式(1)(2)的一个可行解,计算矩阵 $s(\boldsymbol{Q}_1)=\sum_{i=1}^{n}x_i\boldsymbol{Q}_1^{i-1},t(\boldsymbol{Q}_2)=\sum_{i=1}^{n}y_i\boldsymbol{Q}_2^{i-1}$.注意这里求解的矩阵 $s(\boldsymbol{Q}_1),t(\boldsymbol{Q}_2)$并不一定等于 $\boldsymbol{Q}_1^s,\boldsymbol{Q}_2^t$,但一定满足关系 $\boldsymbol{M}_1=\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t$.

算法时间分析:

设 F_q 上一次四则运算需要时间为 β,($\beta=O(\log^2 q)$).

步骤 1　计算式(1)(2)需要时间为 $\Theta(n^4\beta)$.①因矩阵幂运算是式(1)计算中最耗时运算,它需要时间至多为 $n\times\Theta(n^3)=\Theta(n^4\beta)$,故式(1)计算共需时间为 $\Theta(n^4\beta)$.②计算式(2)也需要时间 $\Theta(n^4\beta)$.

计算矩阵 $\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t$ 的时间至多为 $\Theta(n^5\log n\beta)$.①计算矩阵积 $\boldsymbol{Q}_1^s\boldsymbol{M}$ 中每个元素需要时间 $\Theta(n^2\beta)$,矩阵积 $\boldsymbol{Q}_1^s\boldsymbol{M}$ 中共有 n^2 个元素,故需要时间 $\Theta(n^4\beta)$.②由于两个矩阵每个元素都是含有 n 个未知元的一次多项式,计算 $\boldsymbol{Q}_1^s\boldsymbol{M}$ 与 $\boldsymbol{Q}_2^t$ 矩阵积中一个元素需要时间 $\Theta(n^3\log n\beta)$.同样,矩阵积$(\boldsymbol{Q}_1^s\boldsymbol{M})\boldsymbol{Q}_2^t$有 n^2 个元素,因此计算矩阵 $\boldsymbol{Q}_1^s\boldsymbol{M}$ 与 $\boldsymbol{Q}_2^t$ 的乘积需要时间 $n^2\times\Theta(n^3\log n\beta)=\Theta(n^5\log n\beta)$.

计算标准形(3)需要时间 $\Theta(n^6\beta)$.①将矩阵关系式 $\boldsymbol{M}_1=\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t$ 转化为含 n^2 个未知元的方程组需要时间 $n^2\times\Theta(n^2)=\Theta(n^4\beta)$.②使用高期消元法将增广矩阵($\boldsymbol{A}\mid\boldsymbol{b}$)变换为标准形(3)需要时间$(1/3)n^6\beta=\Theta(n^6\beta)$.

所以步骤 1 需要时间至多为 $\Theta(n^6\beta)$.

步骤 2　通过式(3)求解变量 z_{ij}需要时间至多为 $\Theta(n^4\beta)$.

步骤 3　计算一个可行解需要时间至多为 $\Theta(n^2\beta)$.在求解 z_{ij}以后,共有 n^2 个方程 $x_i*y_j=z_{ij},i,j\in[n]$.根据 z_{ij}的值可依次确定 x_i,y_j 的值,故计算时间至多为 $\Theta(n^2\beta)$.

步骤 4　由步骤 1 知,计算矩阵 $s(\boldsymbol{Q}_1),t(\boldsymbol{Q}_2)$需要时间至多为 $\Theta(n^3\beta)$.

上述 4 个步骤时间进行求和可得总时间至多为 $\Theta(n^6\beta)$.

算法空间分析:

设保存 F_q 上一个元素需要存储空间为 α,($\alpha=O(\log q)$).

步骤 1　易于分析,计算式(1)(2)共需存储空间为 $\Theta(n^3\alpha)+\Theta(n^3\alpha)=\Theta(n^3\alpha)$.计算 $\boldsymbol{Q}_1^s\boldsymbol{M}\boldsymbol{Q}_2^t$ 需要存储空间为 $\Theta(n^4\alpha)$.计算标准形(3)需要存储空间为 $\Theta(n^4\alpha)$.所以步骤 1 所需存储空间至多为 $\Theta(n^4\alpha)$.

步骤 2　存放变量 z_{ij}需要存储空间为$\Theta(n^2\alpha)$.

步骤 3　存储 n^2 个方程 $z_{ij}=x_iy_j=b_{i+n\times j}$需要存储空间为 $\Theta(n^2\alpha)$.

步骤 4　矩阵 $s(\boldsymbol{Q}_1),t(\boldsymbol{Q}_2)$每个至多需要存储空间 $\Theta(n^2\alpha)$.所以 4 个步骤至多需要存储空间 $\Theta(n^4\alpha)$.

3.2　公钥加密方案安全性分析

本小节先归约子问题 1 的求解到多项式有限域上离散对数问题,然后分析证明方案安全性.

定理 2　给定$(\boldsymbol{Q},\boldsymbol{Q}^w)$,求解整数 w 问题多项式时间归约到求解多项式有限域上离散对数问题.

证明　设 $f(\lambda)$是 $\boldsymbol{Q}$ 的特征多项式.由引理 1 知 $f(\lambda)$为度为 n 的不可约多项式.因 $f(\boldsymbol{Q})=\boldsymbol{0}$,故一定存在唯一$(w_1,\cdots,w_n)$满足 $\boldsymbol{Q}^w=\sum_{i=1}^{n}w_i\boldsymbol{Q}^{i-1}$.给定$(\boldsymbol{Q},\boldsymbol{Q}^w)$,根据等式关系 $\boldsymbol{Q}^w=\sum_{i=1}^{n}w_i\boldsymbol{Q}^{i-1}$可以产生关于变量$(w_1,\cdots,w_n)$的线性方程组,并求解得到$(w_1,\cdots,w_n)$.设 $g(\lambda)=\sum_{i=1}^{n}w_i\lambda^i$,根据遍历矩阵 $\boldsymbol{Q}$ 的集$\{\boldsymbol{Q}^k\mid k\in Z\}$与模为 $f(\lambda)$的 F_q 上多项式一一对应关系,可知 $g(\lambda)\equiv\lambda^w\bmod f(\lambda)$.因此,求解整数 w 问题归约到求解在模为$f(\lambda)$的多项式有限域上的离散对数问题,即计算 $w=\log_\lambda g(\lambda)\bmod f(\lambda)$.

算法时间空间分析:根据定理 1 中步骤 1 的分析,计算 $\sum_{i=1}^{n}w_i\boldsymbol{Q}^{i-1}$共需时间为 $\Theta(n^4\beta)$,使用高斯消元法求解含 n 个变量线性方程组需要时间为$\Theta(n^3\beta)$.而

且,算法运行需要存储空间至多为 $\Theta(n^3\alpha)$.因此,该归约算法是多项式时间算法.

由于文献[12]中的公钥加密方案进行加密和解密时都需要计算双侧幂,这种双侧幂运算非常费时,通过分析易知每次加密或解密算法需要时间为 $\Theta(n^7\beta\log q)$.因此文献[12]中的公钥加密方案效率较低.为提高计算效率,一般 q 不会太大.不失一般性,在下面定理中设 $q=n^{O(1)}$.即使 $q=2^{O(n)}$,子问题 2 仍然存在多项式时间算法.

定理 3 假定 $q=n^{O(1)}$.破解文献[12]中的基于遍历矩阵的公钥加密方案难度多项式时间内归约到求解多项式有限域上离散对数问题.

证明 设 O 为求解多项式有限域上离散对数问题神谕机(Oracle machine).给定公钥 $pk=(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{M}_1=\boldsymbol{Q}_1^{v_1}\boldsymbol{M}\boldsymbol{Q}_2^{v_2})$,由定理 1 计算求解 $q-1$ 组解 $s_i(\boldsymbol{Q}_1)$, $t_i(\boldsymbol{Q}_2)$, $i\in[q-1]$.对每一组解 $s_i(\boldsymbol{Q}_1)$, $t_i(\boldsymbol{Q}_2)$,计算其对应的多项式分别为 $g_1(\lambda)$, $g_2(\lambda)$.由定理 2 分别归约到多项式有限域上离散对数 $\log_\lambda g_j(\lambda)\bmod f_j(\lambda)$,调用多项式有限域上离散对数神谕机 O 并比较结果是否相等.如它们相等,则该值就是私钥,否则继续计算.根据假设 $q=n^{O(1)}$,故在多项式次数内一定可以找到一组离散对数相等的值.因此,破解文献[12]中公钥加密方案难度多项式时间内归约到求解多项式有限域上离散对数问题.

4 公钥加密方案举例($n=3,q=5$)

设 $\boldsymbol{Q}_1=\begin{bmatrix}0&0&2\\1&0&1\\0&1&0\end{bmatrix}$, $\boldsymbol{Q}_2=\begin{bmatrix}0&0&2\\1&0&0\\0&1&1\end{bmatrix}$,

$\boldsymbol{M}=\begin{bmatrix}2&1&0\\3&4&2\\0&1&3\end{bmatrix}$, $\boldsymbol{M}_1=\boldsymbol{Q}_1^{55}\boldsymbol{M}\boldsymbol{Q}_2^{55}=\begin{bmatrix}3&0&3\\2&0&0\\1&4&1\end{bmatrix}$.

可以验证 $|<\boldsymbol{Q}_1>|=|<\boldsymbol{Q}_2>|=124=5^3-1$.易于计算 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 的特征多项式分别为 $f_1(\lambda)=|\lambda\boldsymbol{I}-\boldsymbol{Q}_1|=\lambda^3+4\lambda+3$, $f_2(\lambda)=|\lambda\boldsymbol{I}-\boldsymbol{Q}_2|=\lambda^3+4\lambda^2+3$.由引理 1 知 $f_1(\lambda)$, $f_2(\lambda)$为不可约多项式.计算含未知变量矩阵如下:

$$s(\boldsymbol{Q}_1)=\sum_{i=1}^{3}x_i\boldsymbol{Q}_1^{i-1}=\begin{bmatrix}x_1&2x_3&2x_2\\x_2&x_1+x_3&x_2+2x_3\\x_3&x_2&x_1+x_3\end{bmatrix},$$

$$t(\boldsymbol{Q}_2)=\sum_{i=1}^{3}y_i\boldsymbol{Q}_2^{i-1}=\begin{bmatrix}y_1&2y_3&2y_2+2y_3\\y_2&y_1&2y_3\\y_3&y_2+y_3&y_1+y_2+y_3\end{bmatrix}.$$

用矩阵 $s(\boldsymbol{Q}_1)$, $t(\boldsymbol{Q}_2)$替换矩阵等式 $\boldsymbol{M}_1=\boldsymbol{Q}_1^{s}\boldsymbol{M}\boldsymbol{Q}_2^{t}$ 中矩阵变量 $\boldsymbol{Q}_1^{s},\boldsymbol{Q}_2^{t}$,并整理得线性方程组如下:

$$\boldsymbol{A}=\begin{bmatrix}2&0&1&1&2&3&0&1&4\\3&2&3&4&2&1&2&3&3\\0&3&2&1&4&2&3&2&3\\1&2&3&0&1&4&4&1&1\\4&2&1&2&3&3&3&2&4\\1&4&2&3&2&3&3&3&2\\0&1&4&4&1&1&1&0&2\\2&3&3&3&2&4&1&1&1\\3&2&3&3&3&2&0&1&1\end{bmatrix}\begin{bmatrix}y_1x_1\\y_1x_2\\y_1x_3\\y_2x_1\\y_2x_2\\y_2x_3\\y_3x_1\\y_3x_2\\y_3x_3\end{bmatrix}=\begin{bmatrix}3\\2\\1\\0\\0\\4\\3\\0\\1\end{bmatrix}$$

使用高斯消元法,可得到线性方程组的解:

$$\begin{bmatrix}1&0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0\\0&0&0&0&0&1&0&0&0\\0&0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\end{bmatrix}\begin{bmatrix}y_1x_1\\y_1x_2\\y_1x_3\\y_2x_1\\y_2x_2\\y_2x_3\\y_3x_1\\y_3x_2\\y_3x_3\end{bmatrix}=\begin{bmatrix}2\\4\\2\\0\\0\\0\\2\\4\\2\end{bmatrix}\Rightarrow\begin{bmatrix}y_1x_1\\y_1x_2\\y_1x_3\\y_2x_1\\y_2x_2\\y_2x_3\\y_3x_1\\y_3x_2\\y_3x_3\end{bmatrix}=\begin{bmatrix}2\\4\\2\\0\\0\\0\\2\\4\\2\end{bmatrix}.$$

根据定理 1 中步骤 3,变量值取为 $x_1=1$, $x_2=2$, $x_3=1$, $y_1=2$, $y_2=0$, $y_3=1$.它们是满足关系 $\boldsymbol{M}_1=s(\boldsymbol{Q}_1)\boldsymbol{M}t(\boldsymbol{Q}_2)$的一个可行解.易于验证方程组存在下面 $q-1=4$ 个可行解都满足关系 $\boldsymbol{M}_1=s(\boldsymbol{Q}_1)\boldsymbol{M}t(\boldsymbol{Q}_2)$.

$$\begin{cases}x_1=1,y_1=2\\x_2=2,y_2=0,\\x_3=1,y_3=2\end{cases}\quad\begin{cases}x_1=2,y_1=1\\x_2=4,y_2=0,\\x_3=2,y_3=1\end{cases}$$

$$\begin{cases}x_1=3,y_1=4\\x_2=1,y_2=0,\\x_3=3,y_3=4\end{cases}\quad\begin{cases}x_1=4,y_1=3\\x_2=3,y_2=0.\\x_3=4,y_3=3\end{cases}$$

同时,也易于验证下面多项式有限域上的离散对数关系式:

$$\begin{cases}\lambda^{86}\equiv\lambda^2+2\lambda+1\bmod f_1(\lambda)\\\lambda^{24}\equiv2\lambda^2+0\lambda+2\bmod f_2(\lambda)\end{cases},$$

$$\begin{cases}\lambda^{117}\equiv2\lambda^2+4\lambda+2\bmod f_1(\lambda)\\\lambda^{117}\equiv1\lambda^2+0\lambda+1\bmod f_2(\lambda)\end{cases},$$

$$\begin{cases}\lambda^{55}\equiv3\lambda^2+1\lambda+3\bmod f_1(\lambda)\\\lambda^{55}\equiv4\lambda^2+0\lambda+4\bmod f_2(\lambda)\end{cases},$$

$$\begin{cases}\lambda^{24}\equiv4\lambda^2+3\lambda+4\bmod f_1(\lambda)\\\lambda^{86}\equiv3\lambda^2+0\lambda+3\bmod f_2(\lambda)\end{cases}.$$

同样,将上述关系式中 λ 用相应的遍历矩阵 $\boldsymbol{Q}_1,\boldsymbol{Q}_2$ 替换,则得到下面关系式:

$\boldsymbol{M}_1=\boldsymbol{Q}_1^{86}\boldsymbol{M}\boldsymbol{Q}_2^{24}$, $\boldsymbol{M}_1=\boldsymbol{Q}_1^{117}\boldsymbol{M}\boldsymbol{Q}_2^{117}$,

$$\boldsymbol{M}_1 = \boldsymbol{Q}_1^{55}\boldsymbol{M}\boldsymbol{Q}_2^{55}, \quad \boldsymbol{M}_1 = \boldsymbol{Q}_1^{24}\boldsymbol{M}\boldsymbol{Q}_2^{86}.$$

因此,破解文献[12]中基于遍历矩阵的公钥加密方案不会比求解多项式有限域上离散对数问题更难.

5 结论

本文主要研究分析了基于遍历矩阵的公钥加密方案的安全性.使用遍历矩阵性质和线性化方法,本文归约证明了破解文献[12]中的基于遍历矩阵的公钥加密方案问题到多项式有限域上离散对数问题,从而证明了文献[12]中对基于遍历矩阵的公钥加密方案的安全归约证明是不正确的.

参考文献

[1] 于佳,程相国,李发根,等.标准模型下可证明安全的入侵容忍公钥加密方案[J].软件学报,2013,24(2):266 – 278.
Yu J, Cheng XG, Li FG, et al. Provably secure intrusion-resilient public-key encryption scheme in the standard model[J]. Journal of Software, 2013, 24(2): 266 – 278. (in Chinese)

[2] 杜红珍,黄梅娟,温巧燕.高效的可证明安全的无证书聚合签名方案[J].电子学报,2013,41(1):72 – 76.
Du Hong-zhen, Huang Mei-juan, Wen Qiao-yan. Efficient and provably-secure certificateless aggregate signature scheme[J]. Acta Electronica Sinica, 2013, 41(1): 72 – 76. (in Chinese)

[3] 康立,唐小虎,范佳.基于认证的高效公钥加密算法[J].电子学报,2008,36(10):2055 – 2059.
Kang Li, Tang Xiao-hu, Fan Jia. Efficient certificate-based public-key encryption scheme[J]. Acta Electronica Sinica, 2008, 36(10): 2055 – 2059. (in Chinese)

[4] P W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(1): 1484 – 1509.

[5] J Proos, C Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves[J]. Quantum Information and Computation, 2003, 3(4): 317 – 344.

[6] 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, et al. Quantum algorithm for prime factorization with high probability[J]. Acta Electronica Sinica, 2011, 39(1): 35 – 39. (in Chinese)

[7] 赵永哲,赵搏,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 Yong-Zhe, Zhao Bo, Pei Shi-Hui. On the properties of the ergodic matrix over finite field[J]. Acta Mathematica Sinica, 2012, 55(3): 457 – 468. (in Chinese)

[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 yong-zhe, Pei shi-hui, Wang hong-jun, et al. Using the ergodic matrices over finite field to construct the dynamic encryptor[J]. Journal of Chinese Computer Systems, 2007, 28(11): 2010 – 2014. (in Chinese)

[9] Pei Shi-hui, Zhao Hong-wei, Zhao Yong-zhe. Public key cryptography based on ergodic matrices over finite field[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6): 1525 – 1528.

[10] 赵永哲,姜占华,黄声烈.基于 F_2 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 Yongzhe, Jiang Zhanhua, Huang Shenglie. Implementation of Shamir's three pass protocol based on ergodic matrix over finite field[J]. Journal of Chinese Computer Systems, 2006, 27(6): 986 – 991. (in Chinese)

[11] 孙永雄,赵永哲,杨永健,等.基于遍历矩阵的单向(陷门)函数的构造方案[J].吉林大学学报:信息科学版,2006,24(5):555 – 560.
Sun Yongxiong, Zhao Yongzhe, Yang Yongjian, et al. Scheme to construct one-way(trapdoor)functions based on ergodic matrices[J]. Journal of Jilin University: Information Science Edition, 2006, 24(5): 555 – 560. (in Chinese)

[12] 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 Shi-hui, Zhao Yong-zhe, Zhao Hong-wei. Public key encryption scheme based on the ergodic matrices[J]. Acta Electronica Sinica, 2010, 38(8): 1908 – 1913. (in Chinese)

[13] A J Menezes, S Vanstone, P C van Oorschot. Handbook of Applied Cryptography [M]. USA: CRC Press, 2001.

[14] R Lovorn. Rigorous subexponential algorithms for discrete logarithms over finite fields[D]. USA: University of Georgia, 1992.

作者简介

古春生　男,1971 年 3 月生,安徽芜湖人,2005 年获中国科学技术大学管理科学与工程学博士学位,现为江苏理工学院副教授,主要从事公钥密码学方面研究.
E-mail: guchunsheng@gmail.com

景征骏　男,1978 年 10 月生,江苏丹阳人,现为南京邮电大学博士研究生,主要从事数字签名方面研究.
E-mail: jzj.jstu@gmail.com