基于遍历矩阵的公钥加密方案

裴士辉[1,2],赵永哲[1],赵宏伟[1]
(1.吉林大学计算机科学与技术学院,吉林长春 130012; 2.浙江工业大学软件学院,浙江杭州 310032)

摘 要: 目前的公钥加密方案受到来自量子计算的威胁,研究在量子计算下安全的公开加密算法具有重要的意义.本文提出了遍历矩阵的概念,并给出了遍历矩阵的性质.同时提出了基于有限域上遍历矩阵的双侧幂乘问题(TEME:Two-side Ergodic Matrices Exponentiation),并证明了求解 TEME 问题是 NP 完全的.据此,本文提出了一个新的公钥加密方案,并在标准模型下,证明了该方案基于 TEME 问题的安全性,即该方案具有适应性选择密文攻击下的不可区分性.

关键词: 公钥密码; 遍历矩阵; NP 完全; 可证明安全性
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2010) 08-1908-06

Public Key Encryption Scheme Based on the Ergodic Matrices

PEI Shi-hui[1,2], ZHAO Yong-zhe[1], ZHAO Hong-wei[1]
(1. *School of Computer Science and Technology, Jilin University, Changchun, Jilin* 130012, *China*;
2. *School of Software, Zhejiang University of Technology, Hangzhou, Zhejiang* 310032, *China*)

Abstract: The current public key encryption schemes are vulnerable under the threat from quantum computing, it is necessary to research secure public key encryption algorithm under quantum computing. The concept of ergodic matrices and its property are given, and a new difficult problem named Two-side Ergodic Matrices Exponentiation (TEME) is proposed, which is proved at least NP-complete. Accordingly, we present a new public key encryption scheme based on ergodic matrices, and proved it is secure based on the TEME problem in the standard model, that is, the INDistinguishability against adaptively Chosen Ciphertext Attack (IND-CCA).

Key words: public key cryptography; ergodic matrix; NP-Complete; proved security

1 引言

自从 1976 年 Diffie 和 Hellman 提出了公钥密码的概念以来[1],出现了很多的公钥密码算法,所有的这些算法的安全性都依赖于相应的数学难题.主要的数学难题可以分为三类[2,3]:(1)整数分解问题(IFP);(2)离散对数问题(DLP);(3)椭圆曲线离散对数问题(ECDLP).

目前对上述问题的攻击算法,对于 IFP 和 DLP 问题的攻击是亚指数时间的攻击算法,而对于 ECDLP 的攻击算法是指数时间的.目前还不足以对上述算法构成真正的威胁.

但是,上述算法都受到量子计算机的威胁.Shor 给出了利用量子计算机进行因式分解的算法[4],该算法的时间复杂度为多项式时间.如果量子计算机能够达到控制 4000 个量子位的能力时,那么使用 Shor 算法可以快速地破解 IFP.基于离散对数问题的公钥密码体制同样受到 Shor 量子离散对数算法[4]的威胁,该算法的时间复杂度为多项式时间.另外,基于椭圆曲线的密码体制也受到量子算法的攻击,Proos 和 Zalka 提出了一个解决 F_p 上 ECDLP 的量子算法[5],该算法解决 ECDLP 需要 $7\log_2 p + 4\log_2\log_2 p$ qubits.另外,如果基于文中没有被证明的假设上述数字减少为 $5\log_2 p + 8(\log_2 p)^{1/2} + \log_2 p\log_2 p$.此外,如果使用 Draper 提出的量子加法[6],上述结果还会减少 n qubits.

首台量子计算机在 1998 年建成,只有 2 qubits.在 2000 年 shor 算法在 5 qubit 的计算机上实现了.2001 年建成了 7 qubit 的量子计算机.在该台计算机上,使用 Shor 算法可以分解数字 15[7].在 2005 年包含 8 qubits 的量子寄存器建成了[8].建成大的量子计算机看起来是困难的,也许是不可能的.但是,在研究密码体制的时候,假设大的量子计算机将会建成是有意义的.

2 公钥加密方案及其安全性定义

令消息空间 $Message = \{0,1\}^*$,密文空间 $Ciphertext = \{0,1\}^*$.随机串空间 $Coins$ 为 $\{0,1\}^\infty$(无穷字符串集合),公钥空间 $PK \subseteq \{0,1\}^*$,私钥空间 $SK \subseteq \{0,1\}^*$.

公钥加密方案是由三个算法组成 $\mathrm{ASYM} = (\mathcal{E}, \mathcal{D}, \mathcal{K})$.算法 $\mathcal{K}$ 是密钥生成算法,输入随机数 $r \in Coins$,输出密钥对 $(pk, sk) \in PK \times SK$;算法 $\mathcal{E}$ 是加密算法,输入

收稿日期:2009-09-27;修回日期:2009-12-17
基金项目:国家教育部博士点基金(No.20050183032)

公钥 $pk \in PK$,明文 $x \in Message$,随机数 $r \in Coins$(可选),输出密文 $y = \varepsilon(pk, x, r)$;算法 $\mathcal{D}$ 是解密算法,输入私钥 $sk \in SK$,密文 $y \in Ciphertext$,输出明文 $\mathcal{D}(sk, y) \cup \{BAD\}$.其中 BAD 表示密文是无效的,即它不是对任何明文的加密结果.

公钥加密方案要求,对于算法 $\mathcal{K}$ 可能输出的任意的(pk, sk),对于任意的 $x \in Message$ 和 $r \in Coins$,满足 $\mathcal{D}(sk, \varepsilon(pk, x, r)) = x$.

目前普遍作为标准的公钥加密方案的安全性定义是在选择密文攻击下的不可区分性(IND-CCA: Indistinguishability under chosen-ciphertext attack).这个概念由一个分为发现和猜测两阶段的实验过程给出.

定义 1　令 ASYM = $(\varepsilon, \mathcal{D}, \mathcal{K})$为公钥加密方案,令 A 为攻击者,考虑如下实验过程[9]:

Experiment $\mathrm{EXP}^{\text{ind-cca-fg}}_{\text{ASYM},A}$

$(pk, sk) \leftarrow \mathcal{K}$

$(x_0, x_1, s) \leftarrow A^{\mathcal{D}sk}(\text{find}, pk)$

$b \xleftarrow{R} \{0,1\}$

$y \leftarrow \varepsilon_{pk}(x_b)$

$\tilde{b} \leftarrow A^{\mathcal{D}sk}(\text{guess}, pk, y, s)$

If $\tilde{b} = b$

　then return 1

else

　return 0

定义攻击者 A 在选择密文的发现猜测过程中不可区分性的优势(ind-cca-advantage)为:

$$\mathrm{Adv}^{\text{ind-cca-fg}}_{\text{ASYM},A} = 2 \cdot \Pr[\mathrm{Exp}^{\text{ind-cca-fg}}_{\text{ASYM},A} = 1] - 1$$

对于任意的 t, c,定义公钥密码 ASYM 的 ind-cca-advantage 为:

$$\mathrm{Adv}^{\text{ind-cca-fg}}_{\text{ASYM}}(t, c) = \max_{A}\{\mathrm{Adv}^{\text{ind-cca-fg}}_{\text{ASYM},A}\}$$

其中的最大值是所有这样的攻击者的优势最大值:具有时间复杂度 t,其查询的信息长度之和最多为 c 位.

3　遍历矩阵及其性质

令 F_q 表示 q 元有限域,令 $M^{F_q}_{n\times n}$表示 F_q 上 $n \times n$ 矩阵的集合,令 F_q^n 表示 F_q 上 n 维列向量的集合.

定义 2　设矩阵 $\boldsymbol{m} \in M^{F_q}_{n\times n}$,如果对 $\forall\, \boldsymbol{v} \in F_q^n \setminus \{\boldsymbol{0}\}$,$\{\boldsymbol{mv}, \boldsymbol{m}^2\boldsymbol{v}, \boldsymbol{m}^3\boldsymbol{v}, \cdots, \boldsymbol{m}^{q^n-1}\boldsymbol{v}\}$恰好取遍 $F_q^n \setminus \{\boldsymbol{0}\}$,则称 $\boldsymbol{m}$ 为 F_q 上的"遍历矩阵"[10,11].

定义 3　设 $F_q[t]$为 F_q 关于符号"t"的多项式的集合.即有:

$$F_q[t] = \{p(t) \mid p(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_2 t^2 + a_1 t^1 + a_0 t^0 \ (a_i \in F_q, n = 0,1,2,\cdots)\}.$$

定义 4　设 $\boldsymbol{m} \in M^{F_q}_{n\times n}$,记 $\boldsymbol{m}$ 在矩阵乘法下的生成集为:

$$\langle \boldsymbol{m} \rangle = \{\boldsymbol{m}^k \mid k = 1,2,3,\cdots\}.$$

由 Cayley-Hamilton 定理,和有限域理论可以得到如下关于遍历矩阵的性质[10,11]:

定理 1　如果 $\boldsymbol{m} \in M^{F_q}_{n\times n}$为遍历矩阵,则 $\boldsymbol{m}$ 在矩阵乘法下的周期为$(q^n - 1)$.

引理 1　对 $\forall\, \boldsymbol{A} \in M^{F_q}_{n\times n}, k \in \{0,1,2,\cdots\}$;存在 $c_0, c_1, \cdots, c_{n-1} \in F_q$,使:

$$\boldsymbol{A}^k = c_0\boldsymbol{I} + c_1\boldsymbol{A} + c_2\boldsymbol{A}^2 + \cdots + c_{n-1}\boldsymbol{A}^{n-1}.$$

引理 2　对 $\forall\, \boldsymbol{m} \in M^{F_q}_{n\times n}$, $F_q[\boldsymbol{m}] = \{p(\boldsymbol{m}) \mid \deg(p) < n\}$.

引理 3　对 $\forall\, \boldsymbol{m} \in M^{F_q}_{n\times n}$, $|F_q[\boldsymbol{m}]| \leqslant q^n$.

引理 4　如果 $\boldsymbol{m} \in M^{F_q}_{n\times n}$非奇异,则 $\boldsymbol{m}$ 在 F_q 中矩阵乘法下的周期$\leqslant (q^n - 1)$.

引理 5　如果 $\boldsymbol{m} \in M^{F_q}_{n\times n}$在 F_q 中矩阵乘法下的周期 $= (q^n - 1)$,则有:

$$F_q[\boldsymbol{m}] = \langle \boldsymbol{m} \rangle \cup \{\boldsymbol{0}\} = \{\boldsymbol{0}, \boldsymbol{m}, \boldsymbol{m}^2, \cdots, \boldsymbol{m}^{q^n-1} = \boldsymbol{I}\}.$$

定理 2　$\boldsymbol{m} \in M^{F_q}_{n\times n}$为遍历矩阵当且仅当 $\boldsymbol{m}$ 在 F_q 中矩阵乘法下的周期 $= (q^n - 1)$.

定理 3　如果 $\boldsymbol{m} \in M^{F_q}_{n\times n}$为遍历矩阵,则 $F_q[\boldsymbol{m}]$在矩阵加法和乘法下恰好做成一个 q^n 元有限域.

定理 4　如果 $\boldsymbol{m} \in M^{F_q}_{n\times n}$为遍历矩阵,则 $< \boldsymbol{m} >$ 中恰有 $\phi(q^n - 1)$个遍历矩阵.称它们彼此"等价"(即等价的遍历矩阵都有共同的生成集,$\phi(x)$为 Euler 函数).

定理 5　如果 $\boldsymbol{m} \in M^{F_q}_{n\times n}$为遍历矩阵,则对 $\forall\, \boldsymbol{r} \in (F_q^n)^{\mathrm{T}} \setminus \{\boldsymbol{0}^{\mathrm{T}}\}$, $\{\boldsymbol{rm}, \boldsymbol{rm}^2, \cdots, \boldsymbol{rm}^{q^n-1}\}$恰好取遍 $(F_q^n)^{\mathrm{T}} \setminus \{\boldsymbol{0}^{\mathrm{T}}\}$.

引理 6　设 $\boldsymbol{m} \in M^{F_q}_{n\times n}$为遍历矩阵,则 $\boldsymbol{m}, \cdots, \boldsymbol{m}^{q^n-1}$的第 i 列恰好取遍 $F_q^n \setminus \{\boldsymbol{0}\}$($i \in \{1, \cdots, n\}$).

引理 7　设 $\boldsymbol{m} \in M^{F_q}_{n\times n}$为遍历矩阵,则 $\boldsymbol{m}, \cdots, \boldsymbol{m}^{q^n-1}$的第 i 行恰好取遍$(F_q^n)^{\mathrm{T}} \setminus \{\boldsymbol{0}^{\mathrm{T}}\}$ ($i \in \{1, \cdots, n\}$).

4　基于遍历矩阵的困难问题及其安全性

4.1　BMQ-问题及安全性分析

首先引入有限域上的"BMQ-问题",即有限域上的"二等分多变量二次方程组的求解问题(Bisectional Multivariate Quadratic equations problem)".其定义如下:

定义 5　BMQ-问题:F_q 上的方程组 E 共有 m 个方程和 $2n$ 个变量,每个方程都具有如下的形式:

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^{(k)} x_i y_j = b^{(k)} \quad (a_{ij}^{(k)}, b^{(k)} \in F_q, k = 1,2,\cdots,m)$$

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

不难看出,有限域上的 BMQ-问题是有限域上 MQ-问题(Multivariate Quadratic problem)的一个特例;不同之

处在于 BMQ-问题中的变量被分成了数量相同的两组，并且每个方程中只含有二次式，而任意一个二次式又都由这两组变量中各取其一的乘积构成.因此在 BMQ-方程组中，$2n$ 个变量恰好构成 n^2 个不同的二次式；与之不同，在 MQ-方程组中，$2n$ 个变量则能构成 $n(2n+1)=2n^2+n$ 个不同的二次式.有限域上的 MQ-问题已经被证明是 NP-完全问题.下面我们要证明有限域上的 BMQ-问题也是 NP-完全的.

定理 6 有限域 F_q 上的 BMQ-问题是 NP-完全的.

证明 已知图的 3-着色问题是 NP-完全的，如果该问题可归约为 F_q 上的 BMQ-问题，则后者也必是 NP-完全的.首先证明图的 3-着色问题可归约为 F_2 上的 BMQ-问题，构思如下：

(1)图的每个顶点 v_i 都对应 F_2 中的一对变量(x_i,y_i).

(2)顶点 v_i 的着色与其所对应变量(x_i,y_i)取值之间的对应关系为：

v_i 着颜色-1 当且仅当$(x_i,y_i)=(0,1)$

v_i 着颜色-2 当且仅当$(x_i,y_i)=(1,0)$

v_i 着颜色-3 当且仅当$(x_i,y_i)=(1,1)$

(3)对于图的每个孤立顶点 v_t，添加方程 $x_ty_t=1$ 到方程组 E 中.

(4)如果图的顶点 v_i 和 v_j 相邻，则添加方程 $x_iy_j+x_jy_i=1$ 到方程组 E 中.

由此可得 F_2 上的 BMQ-方程组 E.由第 3 步的方程 $x_ty_t=1$，可知其有唯一解$(x_t,y_t)=(1,1)$，这意味着对图的每个孤立顶点 v_t 着颜色-3；而由第 4 步的方程 $x_iy_j+x_jy_i=1$，有：

$$(x_i,y_i)\neq(0,0)\wedge(x_j,y_j)\neq(0,0)\wedge(x_i,y_i)\neq(x_j,y_j)$$

即如果图的顶点 v_i 和 v_j 相邻，则 v_i 和 v_j 每个只能用三种颜色之一着色，且 v_i 和 v_j 不同色.所以图的 3-着色问题可归约为求解 F_2 上的方程组 E；因此 F_2 上的 BMQ-问题是 NP-完全的.

用类似的方法可以证明图的 3-着色问题也可归约为 $F_q(q>2)$上的 BMQ-问题.因此 F_q 上的 BMQ-问题亦是 NP-完全的. 证毕.

4.2 TEME 问题

由于有限域上的遍历矩阵在乘法下的周期最大，并且以遍历矩阵的所有幂左乘一个非零列向量或右乘一个非零行向量的结果充分发散；所以可利用遍历矩阵的这些特性来构造密码系统所需要的困难问题.为此我们给出如下基于有限域上遍历矩阵的双侧幂乘问题(TEME: Two-side Ergodic Matrices Exponentiation)，其定义如下：

TEME 问题：$\boldsymbol{Q}_1,\boldsymbol{Q}_2\in M_{n\times n}^{F_q}$为遍历矩阵，$\boldsymbol{M}\in M_{n\times n}^{F_q}\setminus\{\boldsymbol{0}\}$，$x,y\in\{1,2,\cdots,q^n-1\}$；已知$(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y)$，求 x,y.

为了对求解 TEME 问题的困难性进行分析，首先给出下面两个问题：

问题 1 $\boldsymbol{Q}\in M_{n\times n}^{F_q}$为遍历矩阵，$x\in\{1,2,\cdots,q^n-1\}$；已知$(\boldsymbol{Q},\boldsymbol{Q}^x)$，求整数 x.

问题 2 $\boldsymbol{Q}_1,\boldsymbol{Q}_2\in M_{n\times n}^{F_q}$为遍历矩阵，$\boldsymbol{M}\in M_{n\times n}^{F_q}\setminus\{\boldsymbol{0}\}$，$x,y\in\{1,2,\cdots,q^n-1\}$；已知$(\boldsymbol{Q}_1,\boldsymbol{Q}_2,\boldsymbol{M},\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y)$；求矩阵 $\boldsymbol{Q}_1^x$ 和 $\boldsymbol{Q}_2^y$.

可以证明如下定理：

定理 7 问题 TEME 可解，当且仅当“问题 1”和“问题 2”均可解.

定理 8 求解“问题 2”等价于求解 F_q 上的 BMQ-问题.

证明 对于问题 2，由 Cayley-Hamilton 定理，可知 $n\times n$ 矩阵 $\boldsymbol{A}$ 的任意次幂均能用 $\boldsymbol{A}^0,\cdots,\boldsymbol{A}^{n-1}$线性表示.所以可令：

$$\boldsymbol{Q}_1^x=\sum_{i=0}^{n-1}x_i\boldsymbol{Q}_1^i,\ \boldsymbol{Q}_2^y=\sum_{j=0}^{n-1}y_j\boldsymbol{Q}_2^j,\qquad x_i,y_j\in F_q$$

则有：

$$\boldsymbol{B}=\boldsymbol{Q}_1^x\boldsymbol{M}\boldsymbol{Q}_2^y=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(x_iy_j)\boldsymbol{Q}_1^i\boldsymbol{M}\boldsymbol{Q}_2^j$$

$$=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(x_iy_j)\boldsymbol{A}_{ij},\qquad \boldsymbol{A}_{ij}=\boldsymbol{Q}_1^i\boldsymbol{M}\boldsymbol{Q}_2^j$$

将每个 $n\times n$ 矩阵 $\boldsymbol{A}_{ij}$和 $\boldsymbol{B}$ 都按行线性化为 n^2 维向量，则可得到 F_q 上的 BMQ-方程组 E.E 中共有 $2n$ 个变量$(x_0,\cdots,x_{n-1},y_0,\cdots,y_{n-1})$和 m 个方程.其中：

$$\begin{aligned}m&=Rank(F_q[\boldsymbol{Q}_1]\boldsymbol{M}\boldsymbol{F}_q[\boldsymbol{Q}_2])\\&=Rank(\{\boldsymbol{Q}_1^0,\cdots,\boldsymbol{Q}_1^{n-1}\}M\{\boldsymbol{Q}_2^0,\cdots,\boldsymbol{Q}_2^{n-1}\})\\&=Rank(\{\boldsymbol{A}_{ij}\})\end{aligned}$$

为 F_q 上 n^2 维向量组$\{\boldsymbol{A}_{00},\boldsymbol{A}_{01},\cdots,\boldsymbol{A}_{(n-1)(n-1)}\}$的秩.

由于 $\boldsymbol{Q}_1$ 和 $\boldsymbol{Q}_2$ 均为遍历矩阵，所以 $F_q[\boldsymbol{Q}_1]$和 $F_q[\boldsymbol{Q}_2]$在矩阵加法和乘法下均做成 q^n 元有限域，因此 $\boldsymbol{B}_1=[\boldsymbol{Q}_1^0,\boldsymbol{Q}_1^1,\cdots,\boldsymbol{Q}_1^{n-1}]$和 $\boldsymbol{B}_2=[\boldsymbol{Q}_2^0,\boldsymbol{Q}_2^1,\cdots,\boldsymbol{Q}_2^{n-1}]$分别做成 $F_q[\boldsymbol{Q}_1]$和 $F_q[\boldsymbol{Q}_2]$关于 F_q 的一组基.且 $\boldsymbol{Q}_1^x$ 和 $\boldsymbol{Q}_2^y$ 分别由$(x_0,\cdots,x_{n-1})$和$(y_0,\cdots,y_{n-1})$唯一地确定；所以求解问题 2 等价于求解方程组 E.即求解问题 2 等价于求解 F_q 上的 BMQ-问题. 证毕.

有限域上的 BMQ-问题已被证明是 NP-完全的.由定理 8，可知“问题 2”也是 NP-完全的.而求解问题 TEME 需要同时求解“问题 1”和“问题 2”.所以 TEME 问题至少是 NP-完全的.目前针对 NP-完全问题还没有多项式时间的解法，因而基于 TEME 问题构造相应的公钥加密算法可以有效地抵抗量子攻击.

4.3 基于问题 TEME 的单向函数

由 TEME 问题的困难性，可构造出如下单向函数

$f_m(x)$.

定义 6　选定遍历矩阵 $\boldsymbol{Q}_1, \boldsymbol{Q}_2 \in M_{n\times n}^{F_q}$ 和 $\boldsymbol{M} \in M_{n\times n}^{F_q} \setminus \{\boldsymbol{0}\}$,并令:$\boldsymbol{A} = \{1,2,\cdots,q^n-1\}$, $\boldsymbol{B} = <\boldsymbol{Q}_1>\boldsymbol{M}<\boldsymbol{Q}_2>$,则对任意的 $m = \boldsymbol{Q}_1^a \boldsymbol{M} \boldsymbol{Q}_2^b \in \boldsymbol{B}$,由 TEME 可构造出单向函数 $f_m(x)$:

$$f_m: A \to \boldsymbol{B}, \quad f_m(x) = Power(x, \boldsymbol{m}) = \boldsymbol{Q}_1^{xa} \boldsymbol{M} \boldsymbol{Q}_2^{xb}$$

上面虽然给出了单向函数 $f_m(x)$的定义,但还有一个关键问题需要解决;这就是在仅知道($\boldsymbol{Q}_1, \boldsymbol{Q}_2, \boldsymbol{M}, x, \boldsymbol{m} \in <\boldsymbol{Q}_1>\boldsymbol{M}<\boldsymbol{Q}_2>$)而不知($a, b$)的情况下,如何计算双侧乘幂 $Power(x, \boldsymbol{m})$. 因为矩阵乘法不满足结合律,所以无法直接用乘幂的方法对 $Power(x, \boldsymbol{m})$求值. 为此定义 $\boldsymbol{B} = <\boldsymbol{Q}_1>\boldsymbol{M}<\boldsymbol{Q}_2>$ 中的二元运算$\otimes$,使:

$$\boldsymbol{m}_1 = \boldsymbol{Q}_1^a \boldsymbol{M} \boldsymbol{Q}_2^b, \boldsymbol{m}_2 = \boldsymbol{Q}_1^c \boldsymbol{M} \boldsymbol{Q}_2^d \in \boldsymbol{B}$$
$$\Rightarrow \boldsymbol{m}_1 \otimes \boldsymbol{m}_2 = \boldsymbol{Q}_1^{a+c} \boldsymbol{M} \boldsymbol{Q}_2^{b+d}$$

利用运算$\otimes$,通过快速指数运算可得 $\boldsymbol{B}$ 中 $Power(x, \boldsymbol{m})$的求值算法.

所以单向函数 $f_m(x)$实现的关键是,如何在 $\boldsymbol{Q}_1, \boldsymbol{Q}_2, \boldsymbol{M}, \boldsymbol{m}_1 = \boldsymbol{Q}_1^a \boldsymbol{M} \boldsymbol{Q}_2^b, \boldsymbol{m}_2 = \boldsymbol{Q}_1^c \boldsymbol{M} \boldsymbol{Q}_2^d \in \boldsymbol{B}$ 已知而 a, b, c, d 未知的情况下,快速计算 $\boldsymbol{m}_1 \otimes \boldsymbol{m}_2 = \boldsymbol{Q}_1^{a+c} \boldsymbol{M} \boldsymbol{Q}_2^{b+d}$ 的值. 令 $Rank(\boldsymbol{B}) = \boldsymbol{m}$,则可求出 n^2 维向量组 $\boldsymbol{B} = <\boldsymbol{Q}_1>\boldsymbol{M}<\boldsymbol{Q}_2>$ 的一个极大线性无关组:

$$V = \{\boldsymbol{Q}_1^{i_1} \boldsymbol{M} \boldsymbol{Q}_2^{j_1}, \boldsymbol{Q}_1^{i_2} \boldsymbol{M} \boldsymbol{Q}_2^{j_2}, \cdots, \boldsymbol{Q}_1^{i_m} \boldsymbol{M} \boldsymbol{Q}_2^{j_m}\},$$
$$i_k, j_k \in \{0,1,\cdots,n-1\}$$

由于 $\boldsymbol{B}$ 中的任何向量均可由 V 线性表示,因此可得求解 $\boldsymbol{m}_1 \otimes \boldsymbol{m}_2$ 的算法如下:

(1)通过解 F_q 中的线性方程组,求出 $\lambda_1, \lambda_2, \cdots, \lambda_m \in F_q$,使:

$$\boldsymbol{m}_1 = \sum_{k=1}^{m} \lambda_k (\boldsymbol{Q}_1^{i_k} \boldsymbol{M} \boldsymbol{Q}_2^{j_k})$$

(2)计算:

$$\boldsymbol{m}_1 \otimes \boldsymbol{m}_2 = \boldsymbol{Q}_1^c \boldsymbol{m}_1 \boldsymbol{Q}_2^d = \sum_{k=1}^{m} \lambda_k (\boldsymbol{Q}_1^c \boldsymbol{Q}_1^{i_k} \boldsymbol{M} \boldsymbol{Q}_2^{j_k} \boldsymbol{Q}_2^d)$$
$$= \sum_{k=1}^{m} \lambda_k (\boldsymbol{Q}_1^{i_k} \boldsymbol{m}_2 \boldsymbol{Q}_2^{j_k})$$

这样我们便完全实现了单向函数 $f_m(x)$.

5　基于遍历矩阵的公钥加密方案

5.1　加密组件

5.1.1　消息认证码

令消息空间 $Message = \{0,1\}^*$,密钥空间 $mKey = \{0,1\}^{mlen}$,值域空间 $Tag = \{0,1\}^{tlen}$.

消息认证码是由一对算法组成 MAC = (Γ, Ψ). 算法 Γ 是 MAC 生成算法,输入密钥 $k \in mKey$ 和消息 $x \in Message$;输出字符串 $\Gamma(k, x)$,其输出也称为标签(tag);算法 Ψ 是 MAC 验证算法,输入密钥 $k \in mKey$、消息 $x \in Message$ 和标签 $\tau \in Tag$;输出一个布尔值 $\Psi(k, x, \tau) \in (0,1)$,如果消息通过验证输出 1,如果消息未通过验证,输出 0.

消息认证码要求对于所有的 $k \in mKey$ 和 $x \in Message$,满足 $\Psi(k, x, \Gamma(k, x)) = 1$.

这里所谓的 MAC 的安全性是指:在选择消息攻击下强的不可伪造性(suf-cma:strong existential unforgeability under chosen message attack). 在定义中要考虑一个实验过程. 在实验过程中,首先选择随机密钥 $k \in mKey$,密钥对攻击者是保密的. 但攻击者 F 可以访问验证码生成预言机 $\Gamma_k(\cdot)$和验证预言机 $\Psi_k(\cdot)$. 最后如果攻击者可以输出有效的消息-标签对(x^*, τ^*),并且其中的 x^* 没有查询过预言机 $\Gamma_k(\cdot)$,则称攻击者可以伪造.

定义 7　令 MAC = (Γ, Ψ)为消息认证码方案,令 F 表示攻击者. 考虑如下实验过程[12]:

Experiment $\mathrm{EXP}_{\mathrm{MAC},F}^{\text{suf-cma}}$
　$k \xleftarrow{R} mKey$
　$(x^*, \tau^*) \leftarrow F^{\Gamma_k(\cdot), \Psi_k(\cdot,\cdot)}$
　if $\Psi_k(x^*, \tau^*) = 1$ 并且 x^* 没有查询过预言机 $\Gamma_k(\cdot)$
　　return 1
　else
　　return 0

定义 F 的在选择消息攻击下不可伪造的优势(suf-cma-advantage)为:

$$\mathrm{Adv}_{\mathrm{MAC},F}^{\text{suf-cma}} = \Pr[\mathrm{Exp}_{\mathrm{MAC},F}^{\text{suf-cma}} = 1]$$

对于任意的 t, q_t, μ_t, q_v,和 μ_v,定义消息认证码的 suf-cma-advantage 为:

$$\mathrm{Adv}_{\mathrm{MAC}}^{\text{suf-cma}}(t, q_t, \mu_t, q_v, \mu_v) = \max_F \{\mathrm{Adv}_{\mathrm{MAC},F}^{\text{suf-cma}}\}$$

其中的最大值是所有这样的攻击者的优势最大值:具有时间复杂度 t,对验证码生成预言机进行最多 q_t 次查询,其查询结果的长度之和最多为 μ_t 位;对验证预言机进行最多 q_v 次查询,其查询结果的长度之和最多为 μ_v 位.

5.1.2　对称加密

令 $Message = \{0,1\}^*$, $eKey = \{0,1\}^{elen}$, $Ciphertext = \{0,1\}^*$, $Coins = \{0,1\}^\infty$(无穷字符串集合).

对称加密方案是由一对算法组成 $SYM = (\bar{\mathcal{E}}, \bar{\mathcal{D}})$. 算法 $\bar{\mathcal{E}}$ 是加密算法,输入密钥 $k \in eKey$、明文 $x \in Message$ 和随机位串 $r \in Coins$,输出密文 $\bar{\mathcal{E}}(k, x, r)$;算法 $\bar{\mathcal{D}}$ 是解密算法,输入密钥 $k \in eKey$ 和密文 $y \in Ciphertext$,输出 $\bar{\mathcal{D}}(k, y) \in Message \cup \{BAD\}$,其中 BAD 表示密文是无效的,即它不是对任何明文的加密结果.

对称加密方案要求对于所有的 $x \in Message$, $k \in eKey$ 和 $r \in Coins$,满足:

$$\bar{\mathcal{D}}(k, \bar{\mathcal{E}}(k, x, r)) = x.$$

这里所谓的对称加密方案的安全性是指:对于分为发

现和猜测两阶段的选择明文攻击下的不可区分性(ind-cpa-fg: Indistinguishability under chosen-plaintext find-guess attack).为了定义对称加密方案的安全性,我们假设攻击者按照发现和猜测两个阶段的实验过程进行攻击.

定义 8 令 $SYM=(\bar{\mathcal{E}},\bar{\mathcal{D}})$为对称加密方案,令 A 为攻击者,考虑如下实验过程[13]:

Experiment $\mathrm{EXP}^{\text{ind-cpa-fg}}_{\mathrm{SYM},A}$

$k \xleftarrow{R} eKey$

$(x_0,x_1,s)\leftarrow A^{\bar{\mathcal{E}}(k,\cdot)}(\text{find})$

$b \xleftarrow{R} \{0,1\}$

$y \leftarrow \bar{\mathcal{E}}(k,x_b)$

$\tilde{b} \leftarrow A^{\bar{\mathcal{E}}(k,\cdot)}(\text{guess},y,s)$

if $\tilde{b}=b$

then return 1

else return 0

定义攻击者 A 在选择明文的发现猜测过程中不可区分性的优势(ind-cpa-advantage)为:

$$\mathrm{Adv}^{\text{ind-cpa-fg}}_{\mathrm{SYM},A}=2\cdot\Pr[\mathrm{Exp}^{\text{ind-cpa-fg}}_{\mathrm{SYM},A}=1]-1$$

对于任意的 t,q 和 μ,定义对称密码的 ind-cpa-advantage 为:

$$\mathrm{Adv}^{\text{ind-cpa-fg}}_{\mathrm{SYM}}(t,q,\mu)=\max_{A}\{\mathrm{Adv}^{\text{ind-cpa-fg}}_{\mathrm{SYM},A}\}$$

其中的最大值是所有这样的攻击者的优势最大值:具有时间复杂度 t,对加密预言机进行最多 q 次查询,其查询结果的长度之和最多为 μ 位.

5.1.3 Hash 函数

令 $H: M^{F}_{n\times n}\rightarrow(0,1)^{hLen}$ 为一将矩阵表示成二进制位串的 Hash 函数.

为了保证基于遍历矩阵的公钥加密方案具有选择密文攻击下的不可区分性,H 应满足基于遍历矩阵的 Oracle Diffie-Hellman 假设.

定义 9 令 A 表示攻击者,考虑如下两个实验过程[12]:

Experiment $\mathrm{EXP}^{\text{odh-real}}_{H,A}$

$v \xleftarrow{R} \{1,\cdots,q^n-1\}$; $V \leftarrow \boldsymbol{Q}_1^v\boldsymbol{M}\boldsymbol{Q}_2^v$

$u \xleftarrow{R} \{1,\cdots,q^n-1\}$; $U \leftarrow \boldsymbol{Q}_1^u\boldsymbol{M}\boldsymbol{Q}_2^u$

$W \leftarrow H(\boldsymbol{Q}_1^{uv}\boldsymbol{M}\boldsymbol{Q}_2^{uv})$

$\mathcal{H}_v(X)=H(f_X(v))$(预言机)

$b \leftarrow A^{\mathcal{H}_v(\cdot)}(\boldsymbol{U},\boldsymbol{V},W)$

return b

Experiment $\mathrm{EXP}^{\text{odh-rand}}_{H,A}$

$v \xleftarrow{R} \{1,\cdots,q^n-1\}$; $V \leftarrow \boldsymbol{Q}_1^v\boldsymbol{M}\boldsymbol{Q}_2^v$

$u \xleftarrow{R} \{1,\cdots,q^n-1\}$; $U \leftarrow \boldsymbol{Q}_1^u\boldsymbol{M}\boldsymbol{Q}_2^u$

$W \xleftarrow{R} \{0,1\}^{hlen}$

$\mathcal{H}_v(X)=H(f_X(v))$(预言机)

$b \leftarrow A^{\mathcal{H}_v(\cdot)}(\boldsymbol{U},\boldsymbol{V},W)$

return b

上述实验中,攻击者 A 返回的 b 的数值是这样确定的:如果 W 的指数是 $\boldsymbol{U}$、$\boldsymbol{V}$ 的指数的乘积 b 为 1,否则为 0.

定义攻击者 A 攻击基于遍历矩阵的 Oracle Diffie-Hellman 问题的优势为:

$$\mathrm{Adv}^{\text{odh}}_{H,A}=\Pr[\mathrm{EXP}^{\text{odh-real}}_{H,A}=1]-\Pr[\mathrm{EXP}^{\text{odh-rand}}_{H,A}=1]$$

假设上述优势是可以忽略的.

定义 9 中的攻击者 A 可以访问预言机 $\mathcal{H}_v(X)=H(f_X(v))$,但是不能向预言机查询值 $\boldsymbol{Q}_1^u\boldsymbol{M}\boldsymbol{Q}_2^u$.

5.2 基于遍历矩阵的公钥加密方案

令 SYM = $(\bar{\mathcal{E}},\bar{\mathcal{D}})$表示密钥长度为 *elen* 的对称加密方案.

令 MAC = $(\mathcal{T},\mathcal{V})$表示密钥长度为 *mlen* 的消息认证码.

令 $H: M^{F}_{n\times n}\rightarrow(0,1)^{mlen+elen}$ 为一将矩阵表示成二进制位串的 Hash 函数.

令基于遍历矩阵的公钥加密方案为 EMPES = $(\mathcal{E},\mathcal{D},\mathcal{K})$,其由密钥生成算法 $\mathcal{K}$、加密算法 $\mathcal{E}$ 和解密算法 $\mathcal{D}$ 组成.

密钥生成算法 $\mathcal{K}$ 为:

Algorithm $\mathcal{K}$

Begin

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

$\boldsymbol{pk} \leftarrow \boldsymbol{Q}_1^v\boldsymbol{M}\boldsymbol{Q}_2^v$

$sk \leftarrow v$

return $(\boldsymbol{pk},sk)$

End

加密算法 $\mathcal{E}$ 为[12]:

Algorithm $\mathcal{E}(\boldsymbol{pk}=\boldsymbol{Q}_1^v\boldsymbol{M}\boldsymbol{Q}_2^v,x)$

Begin

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

$\boldsymbol{Z} \leftarrow f_{pk}(u)=\boldsymbol{Q}_1^{uv}\boldsymbol{M}\boldsymbol{Q}_2^{uv}$

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

$hash \leftarrow H(\boldsymbol{Z})$

$macKey \leftarrow hash[1..mLen]$

$encKey \leftarrow hash[mLen+1..mLen+eLen]$

$encM \leftarrow \bar{\mathcal{E}}(encKey,x)$

$tag \leftarrow \mathcal{T}(macKey,encM)$

$y \leftarrow \boldsymbol{U}\|encM\|tag$

Retrun y

End

解密算法 $\mathcal{D}$ 为[12]:

Algorithm $\mathcal{D}$ $(sk=v,y)$

Begin

$\boldsymbol{U}\|encM\|tag \leftarrow y$

$\boldsymbol{Z} \leftarrow f_U(sk)=\boldsymbol{Q}_1^{uv}\boldsymbol{M}\boldsymbol{Q}_2^{uv}$

$hash \leftarrow H(\boldsymbol{Z})$

$macKey \leftarrow hash[1..mLen]$

$encKey \leftarrow hash[mLen+1..mLen+eLen]$
if $\nu(macKey, encM, tag)=0$
　then return *BAD*
$x \leftarrow \bar{\Omega}(encKey, encM)$
Retrun x
End

5.3 方案的安全性

根据文献[12]中的证明方法,可以证明如下定理:

定理 9　令 SYM 表示用到的对称加密方案,令 MAC 表示用到的消息认证方案,令 H 表示用到的 Hash 函数. 令 EMPES(Ergodic Matrices Public Key Encryption Scheme)表示基于遍历矩阵的公钥加密方案,对于任意的 t,q,μ 和 c,攻击者进行选择密文攻击的优势为:

$$\begin{aligned}\mathrm{Adv}_{\mathrm{EMPES}}^{\text{ind-cca-fg}}(t,q,\mu,c) \leqslant & \mathrm{Adv}_{\mathrm{SYM}}^{\text{ind-cpa-fg}}(t,0,0)\\ & + 2\cdot\mathrm{Adv}_{H}^{\mathrm{odh}}(t,q)\\ & + 2\cdot\mathrm{Adv}_{\mathrm{MAC}}^{\text{suf-cma}}(t,1,c,q,\mu)\end{aligned}$$

即如果对称加密方案 SYM 和消息认证方案 MAC 是安全的,函数 H 满足基于遍历矩阵的 Oracle Diffie-Hellman 假设,那么 EMPES 是安全的.

EMPES 方案由公钥推出私钥是一个 TEME 问题,该问题是 NP 完全的. 因此本方案的安全性优于其于整数分解问题、离散对数问题和椭圆曲线离散对数问题的公钥密码.

6 结束语

困难问题的构造是公钥密码的核心,直接关系到所构造的公钥密码的安全性. 本文提出了基于有限域上遍历矩阵的双侧幂乘问题(TEME)问题. 并证明了其求解难度至少是 NP-完全的. 所以基于 TEME 问题构造新的公钥密码体制,其安全强度要高于目前所广泛使用的公钥密码体制,这不但可以形成自主创新的公钥密码技术,还可防范公钥密码系统所面临的量子计算威胁. 以此为基础,本文提出了基于遍历矩阵的公钥加密方案,并在标准模型下证明了其安全性,即本方案具有在选择密文攻击下的不可区分性(IND-CCA).

参考文献:

[1] W Diffie, M E Hellman. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644 – 654.

[2] 郭兴阳. 基于攻击的数字签名安全性分析研究[D]. 湖南长沙:国防科学技术大学, 2006.4.

[3] 钱海峰. 若干数字签名方案的分析、设计与应用[D]. 上海:上海交通大学, 2006.6.

[4] P W Shor. Algorithms for quantum computation: discrete logarithms and factoring[J]. SIAM Journal on Computing, 1994, 26(5): 1484 – 1509.

[5] J Proos, C Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves[EB/OL]. http://arxiv.org/abs/quant-ph/0301141, 2003-1-25.

[6] T G Draper. Addition on a quantum computer[EB/OL]. http://arxiv.org/abs/quant-ph/ 0008033, 2000-9-7.

[7] L M K Vandersypen, M Steffen, G Breyta, C S Yannoni, M H Sherwood, I L Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance [J]. Nature, 2001, 414(6866): 883 – 887.

[8] H Hfner, W Hsel, C F Roos, J Benhelm, D Chek al kar, M Chwalla, T Kber, U D Rapol, M Riebe, P O Schmidt, C Becher, O Ghne, W Dr, R Blatt. Scalable multiparticle entanglement of trapped ions[J]. Nature, 2005, 438(7068): 643 – 646.

[9] S Micali, C Rackoff, B Sloan. The notion of security for probabilistic cryptosystems[J]. SIAM Journal on Computing, 1988, 17(2): 412 – 426.

[10] PEI Shihui, ZHAO Hongwei, ZHAO Yongzhe. Public key cryptography based on ergodic matrices over finite field[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6): 1525 – 1528.

[11] Pei Shi-hui, Zhao Yong-zhe, Zhao Hong-wei. Construct public key encryption scheme using ergodic matrices over GF(2)[A]. Proceedings of the 4th International Conference on Theory and Applications of Models of Computation, TAMC 2007[C]. Berlin: Springer-Verlag, 2007. 181 – 188.

[12] M Abdalla, M Bellare, P Rogaway. The oracle Diffie-Hellman assumptions and an analysis of DHIES[A]. Topics in Cryptology CT-RSA 2001[C]. Berlin: Springer-Verlag, 2001. 143 – 158.

[13] M Bellare, A Desai, E Jokipii, P. Rogaway. A concrete security treatment of symmetric encryption: analysis of the DES mode of operation[A]. Proceedings of the 38th Annual Symposium on Foundations of Computer Science[C]. Los Alamitos: IEEE Computer Society Press, 1997. 394 – 403.

作者简介:

裴士辉　男,1969 年生于吉林省吉林市. 博士,吉林大学计算机科学与技术学院讲师,目前在浙江工业大学软件学院从事博士后研究工作. 主要研究方向为应用密码学、无线传感器网络. E-mail: peish@jlu.edu.cn

赵永哲(通讯作者)　男,1961 年生于北京市. 吉林大学计算机科学与技术学院教授,主要研究方向为密码学,信息安全. E-mail: yongzhe@jlu.edu.cn

赵宏伟　男,1962 年生于沈阳市,吉林大学计算机科学与技术学院教授,博士生导师. 主要研究方向为计算机应用技术.