一种新的基于椭圆曲线码的子域子码的 McEliece 密码系统

赵鸿伯[1] 钱路雁[1] 金玲飞[1,2]

[1](复旦大学计算机科学技术学院 上海 201203)

[2](东南大学移动通信国家重点实验室 江苏 南京 210096)

摘 要 1994 年,Shor 提出了具有多项式时间复杂度的针对整数分解问题和离散对数问题的量子算法。这意味着目前被广泛使用的 RSA 密码及其他基于离散对数问题的密码在可实用量子计算机出现的背景下是不安全的。可抗量子计算机攻击的后量子密码系统成为学界研究的热点问题。基于编码理论的密码系统是后量子密码系统的一个选择。在初始 McEliece 密码系统的基础上,设计一种新的基于椭圆曲线码的子域子码的 McEliece 密码系统。使用针对 McEliece 密码系统的通用攻击和针对基于代数几何码的 McEliece 密码系统的攻击对设计的密码系统进行安全分析。结果表明,该密码系统具有与初始 McEliece 密码系统相同的安全性能。

关键词 后量子密码 基于编码的密码系统 椭圆曲线码 McEliece 密码系统

中图分类号 TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.04.050

A NEW MCELIECE CRYPTOSYSTEM BASED ON SUBFIELD SUBCODE OF ELLIPTIC CURVE CODE

Zhao Hongbo[1] Qian Luyan[1] Jin Lingfei[1,2]

[1](*School of Computer Science, Fudan University, Shanghai 201203, China*)

[2](*National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, Jiangsu, China*)

Abstract In 1994, P. Shor introduced a quantum algorithm with polynomial time complexity to solve integer factorization problem and discrete logarithm problem. It means that the widely used RSA cryptography and other cryptosystems based on discrete logarithm problem are insecure in the emergence of practical quantum computers. Postquantum cryptosystem, which can resist quantum computer attacks, has become a hot research topic. Code-based cryptosystem is a choice of the post-quantum cryptosystem. On the basis of the initial McEliece cryptosystem, we designed a new McEliece cryptosystem based on subfield subcode of elliptic curve code. Secure performance of the proposed cryptosystem was evaluated by general attacks against McEliece cryptosystem and attacks against cryptosystem based on algebraic geometry(AG) codes. It is shown that the proposed cryptosystem has the same secure performance as the original McEliece cryptosystem.

Keywords Post quantum cryptography Code-based cryptosystem Elliptic curve code McEliece cryptosystem

0 引 言

1994 年,Shor 提出了能够在多项式时间复杂度内解决整数分解问题和离散对数问题的量子算法[1],这意味着在可实用的量子计算机出现的背景下,现今被广泛使用的 RSA 公钥密码系统及椭圆曲线公钥密码系统将不再安全。因此,密码学界开始研究能够抵抗量子计算机攻击的后量子密码系统,基于编码理论的密码系统便是后量子密码系统中的一类。

第一个基于编码理论的密码系统是由 McEliece 在 1978 年提出的基于二元 Goppa 码的 McEliece 公钥密码系统[2]。这一密码系统与现今使用的公钥密码系统相比拥有更快的加解密速度。到目前为止,尚没有

收稿日期:2018-10-10。东南大学移动通信国家重点实验室开放研究基金资助课题(2017D07)。**赵鸿伯**,硕士生,主研领域:密码学。**钱路雁**,硕士生。**金玲飞**,副教授。

有效的针对基于 Goppa 码的密码系统的攻击方法。

在后续的研究中,学者们尝试使用其他的纠错码来构造新的 McEliece 密码系统。2005 年,Gaborit 提出使用 QC-BCH 码来构造新的 McEliece 密码系统[3]。2007 年,Baldi 等[4]提出了基于 QC-LDPC 码的 McEliece 密码方案。2009 年,Berger 等[5]介绍了使用 QC-alternant 码构造的 McEliece 密码方案。2013 年,Misoczki 等[6]构造了基于 QC-MDPC 码的 McEliece 密码系统。2018 年,NIST 举行的后量子密码学标准竞赛上,多个基于编码理论的密码系统进入第一轮竞争,Aragon 等[7]提出了基于 QC-MDPC 码的 BIKE 密码系统,Melchor 等[8]学者提出的基于 QC 码的 HQC 密码系统等。

上述的部分密码方案被证明存在弱点。2010 年,Otmani 等[9]提出了针对 Gaborit 和 Baldi 提出的基于 QC-BCH 码和 QC-LDPC 码的 McEliece 密码系统的攻击方法。同一年,Faugère 等[10]提出了针对 Berger 等人设计的基于 QC-alternant 码的 McEliece 密码方案的攻击方法。2016 年,Guo 等[11]提出了针对 Misoczki 等人构造的基于 QC-MDPC 码的 McEliece 密码方案的攻击方法。

除了上述方案外,1996 年,Janwa 和 Moreno 提出代数几何码及其子码可以作为构造 McEliece 密码系统的一种选择[12]。虽然基于代数几何码及其子码的 McEliece 密码系统已经被证明不安全[13]。但目前尚没有针对基于代数几何码的子域子码的 McEliece 密码系统的有效的攻击方法,代数几何码的子域子码仍然可以作为构造 McEliece 公钥密码方案的一个选择。

本文的主要贡献在于构造了一个新的基于椭圆曲线码的子域子码的 McEliece 公钥密码系统。

1 预备知识

1.1 线性码基础知识

用$\mathbb{F}_q$表示存在 q 个元素的有限域。用$\mathbb{F}_q^n$表示在有限域$\mathbb{F}_q$上长度为 n 的线性空间。一个$\mathbb{F}_q$上的码长为 n,维数为 k 的线性码 C 是$\mathbb{F}_q^n$的一个子空间,这样的线性码被称为一个$[n,k]$线性码。对于任意两个码字 $x,y\in C$,它们之间的汉明距离是两个码字间不相同的对应位的数量和,记作 $d(x,y)$。对于任意一个码字 x,他的汉明重量是它与 0 向量的汉明距离,记为 $wt(x)=d(x,0)$。线性码 C 的最小码距 d 等于 C 中汉明重量最小的非零码字的汉明重量。我们称码长为 n,维度为 k,码距为 d 的线性码为一个$[n,k,d]$线性码。若一个 $k\times n$ 的矩阵 $\boldsymbol{G}$ 的所有行构成了 C 的一个基底,则称这个矩阵 $\boldsymbol{G}$ 为线性码 C 的一个生成矩阵。若一个矩阵 $\boldsymbol{H}$ 的所有行能够张成 $\boldsymbol{G}$ 的零空间,我们称矩阵 $\boldsymbol{H}$ 为线性码 C 的一个校验矩阵。

1.2 代数几何码

Goppa 于 1977 年发现了编码理论与代数几何之间的理论联系,并在 1981 年提出了代数几何码的构造方法[14]。

用 $\mathcal{X}$ 表示一条在有限域$\mathbb{F}_q$上的代数曲线。我们将线性组合 $D=\sum a_i\cdot x, a_i\in\mathbb{F}_q$, $x\in\mathcal{X}$称为 $\mathcal{X}$ 的一个除子。将集合$\{x\in\mathcal{X}\mid a_i\neq 0\}$称为除子 D 的支持,记作 $sup(D)$。令 $\mathcal{P}=\{\mathcal{P}_1,\mathcal{P}_2,\cdots,\mathcal{P}_n\}$表示 $\mathcal{X}$ 上的所有有理点的集合,由此可得到 $\mathcal{X}$ 上的一个除子 $D_{\mathcal{P}}=\sum_{i=1}^{n}\mathcal{P}_i$。令 E 代表 $\mathcal{X}$ 上的一个满足 $sup(D_{\mathcal{P}})\cap sup(E)=\varnothing$的除子,且 $L(E)$是一个与 E 相关的 Riemann-Roch 空间[15],则我们能够定义这样的一个赋值映射:

$$L(E)\rightarrow\mathbb{F}_q^n: f\mapsto(f(\mathcal{P}_1),\cdots,f(\mathcal{P}_2),\cdots,f(\mathcal{P}_n)) \quad (1)$$

这个赋值映射的像就是一个从曲线 $\mathcal{X}$ 上构造的代数几何码,记为 $C_L(\mathcal{X},\mathcal{P},E)$。$C_L(\mathcal{X},\mathcal{P},\mathcal{E})$的码长 n 等于有理点的个数,即 $n=|\mathcal{P}|$。$C_L(\mathcal{X},\mathcal{P},E)$维数 k 等于 $L(E)$的维数,即 $k=dim(L(E))$。$C_L(\mathcal{X},\mathcal{P},E)$的码距 d 由曲线 $\mathcal{X}$ 的亏格 g 决定,满足条件 $n-k-g+1\leqslant d\leqslant n-k+1$[16]。

1989 年,Justesen 等学者提出了构造基于有限域上的光滑不可约仿射曲线的代数几何码的简易方法[17]。根据单项式基底 $F(x)$和曲线的一个有理点集 $\mathcal{P}$,可以构造出曲线上的代数几何码的生成矩阵:

$$\begin{bmatrix} f_1(\mathcal{P}_1) & f_1(\mathcal{P}_2) & \cdots & f_1(\mathcal{P}_n) \\ f_2(\mathcal{P}_1) & f_2(\mathcal{P}_2) & \cdots & f_2(\mathcal{P}_n) \\ \vdots & \vdots & & \vdots \\ f_k(\mathcal{P}_1) & f_k(\mathcal{P}_2) & \cdots & f_k(\mathcal{P}_n) \end{bmatrix} \quad (2)$$

1.3 McEliece 密码系统

初始的 McEliece 密码系统是基于 Goppa 码构建的。该密码系统由密钥生成、加密算法和解密算法三个部分构成。

1.3.1 密钥生成

1) 在有限域 F_{2^m}上随机选取一个度数为 t 的不可约多项式。根据这一多项式构造一个参数$[n,k,d]$ Goppa 码的生成矩阵 $\boldsymbol{G}$,其中 $n=2^m$,$d=2t+1$。

2) 随机选择一个 $k\times k$ 的可逆矩阵 $\boldsymbol{S}$ 和一个 $n\times n$ 的置换矩阵 $\boldsymbol{P}$。

3) 计算公钥 $G_{\text{pub}}=\boldsymbol{SGP}$。

4) 将集合$(\boldsymbol{S},\phi,\boldsymbol{P})$作为私钥保存,其中 ϕ 代表二

元 Goppa 码的快速译码算法。

1.3.2 加密算法

令 m 代表一个长度为 k 的消息向量。加密算法的执行过程如下:

1) 随机生成一个长度为 n 的错误向量 $\boldsymbol{e}$,满足 $wt(\boldsymbol{e}) \leqslant t$。

2) 计算密文 $c = m\boldsymbol{G}_{\text{pub}} + \boldsymbol{e}$。

1.3.3 解密算法

对于获得的密文 c,解密算法的执行过程如下:

1) 消除置换矩阵的影响:计算 $x = c\boldsymbol{P}^{-1} = m\boldsymbol{S}\boldsymbol{G} + \boldsymbol{e}\boldsymbol{P}^{-1}$。

2) 使用译码算法 ϕ 清除错误向量:$u = \phi(x)$。

3) 计算消息向量:$m = uS^{-1}$。

2 基于椭圆曲线码的子域子码的 McEliece 公钥密码系统

2.1 基本思路

与其他代数几何码的子域子码相比,椭圆曲线码的子域子码拥有更长的码距。同时,2.4 节中介绍了针对椭圆曲线码的子域子码的快速译码算法。这使得椭圆曲线码的子域子码成为构造 McEliece 公钥密码系统的一个选择。

本节将介绍基于椭圆曲线码的子域子码的 McEliece 公钥密码系统。与初始的 McEliece 公钥密码系统类似,基于椭圆曲线码的子域子码的 McEliece 公钥密码系统也由密钥生成、加密算法和解密算法三个部分组成。

2.2 密钥生成

密钥生成的过程分为三个步骤:1) 需要构造 $\mathbb{F}_{2^m}$ 上的一个椭圆曲线码;2) 根据构造的椭圆曲线码来构造其在 $\mathbb{F}_2$ 上的子域子码;3) 根据获得的椭圆曲线码的子域子码构造 McEliece 公钥密码系统。

2.2.1 构造椭圆曲线码

1) 在有限域 $\mathbb{F}_q$,$q = 2^m$ 上随机选择一条椭圆曲线 $\mathcal{X}(x,y): y^2 + y = x^3 + ax + b$。椭圆曲线上的有理点的数量范围为 $[q - 2\sqrt{q} + 1, q + 2\sqrt{q} + 1]$[18]。

2) 随机选择 $\mathcal{X}$ 上的 n 个有理点 $\mathcal{P}(\alpha,\beta)$ 构成有理点集 $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2, \cdots, \mathcal{P}_n\}$。

3) 定义一个二元单项式基底 $F(x,y) = \{x^i y^j \mid i,j \geqslant 0, j \leqslant 1, 2i + 3j \leqslant n - t - 1\}$,其中 $t = \left\lfloor \dfrac{d-3}{2} \right\rfloor$ 是错误向量的最大汉明重量。

4) 将 $F(x,y)$ 按照 $V(f_1) \leqslant V(f_2) \leqslant \cdots \leqslant V(f_{n-t-1})$ 顺序排列,其中 $V(f) = 2i + 3j$。

5) 使用 $F(x,y)$ 的前 k 个单项式 $F_k(x,y)$ 和有理点集 $\mathcal{P}$ 构造椭圆曲线码的生成矩阵 $\boldsymbol{G}_e$。构造的椭圆曲线码的参数为 $[n,k,d]$,其中 $d = n - k$。

2.2.2 构造椭圆曲线码的子域子码

1) 根据 $\boldsymbol{G}_e$ 计算椭圆曲线码的校验矩阵 $\boldsymbol{H}_e$。

2) 将 $\boldsymbol{H}_e$ 中的所有元素转变为 F_2^m 上的向量,构造新矩阵 $\boldsymbol{H}_2$。

3) 椭圆曲线码的子域子码的生成矩阵 $\boldsymbol{G}$ 是 $\boldsymbol{H}_2$ 的零空间的一个基底。构造的子域子码的参数为 $[N,K,D]$,其中 $N = n, K \geqslant mk - (m-1)n, D \geqslant d$。

2.2.3 生成密钥

1) 随机挑选一个 F_2 上的 $k \times k$ 可逆矩阵 $\boldsymbol{S}$,一个 $n \times n$ 转置矩阵 $\boldsymbol{P}$。

2) 计算公钥 $\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\boldsymbol{G}\boldsymbol{P}$。

3) 将有理点集 $\mathcal{P}$,可逆矩阵 $\boldsymbol{S}$ 和转置矩阵 $\boldsymbol{P}$ 作为私钥保存。

2.3 加密算法

对一个消息向量 m 的加密过程如下:

1) 随机生成一个长度为 n 的错误向量 $\boldsymbol{e}$ 且 $wt(\boldsymbol{e}) \leqslant t$。

2) 生成密文 $r = m\boldsymbol{G}_{\text{pub}} + \boldsymbol{e}$。

2.4 解密算法

2.4.1 椭圆曲线码的子域子码的快速译码算法

本节介绍针对椭圆曲线码的子域子码的快速译码算法。对于一个参数为 $[n,k,d]$ 的椭圆曲线码的子域子码,本节介绍的译码算法最多能够纠正 $t = \left\lfloor \dfrac{d-3}{2} \right\rfloor$ 个错误位。不妨将这一译码算法记为 $\boldsymbol{\Phi}$,算法过程如下:

1) 构造两个多项式 $A(x,y)$、$B(x,y)$:

$$A(x,y) = a_1 f_1 + a_2 f_2 + \cdots + a_{n-t-1} f_{n-t-1} \tag{3}$$

$$B(x,y) = b_1 f_1 + b_2 f_2 + \cdots + b_{n-t-k-1} f_{n-t-k-1} \tag{4}$$

其中,$a_i, b_i \in \mathbb{F}_q, f_i \in F(x,y)$。

2) 构造方程组 $A(\mathcal{P}_i) + B(\mathcal{P}_i) f(\mathcal{P}_i) = 0$,找到 A、B 的一个非零解:

$$\begin{cases} A(\mathcal{P}_1) + B(\mathcal{P}_1) r_1 = 0 \\ A(\mathcal{P}_2) + B(\mathcal{P}_2) r_2 = 0 \\ \vdots \\ A(\mathcal{P}_n) + B(\mathcal{P}_n) r_n = 0 \end{cases} \tag{5}$$

3) 计算译码多项式 $d(x,y) = \dfrac{A(x,y)}{B(x,y)}$。

4) 纠错后的码字为 $\{d(\mathcal{P}_1), d(\mathcal{P}_2), \cdots, d(P\mathcal{P}_n)\}$。

2.4.2 快速译码算法证明

本节将证明椭圆曲线码的子域子码的快速译码算法的正确性。

1）证明多项式 $A(x,y)$、$B(x,y)$ 的存在性：将 a_i、b_j 看作是未知数，则式(5)是一个包含 n 个齐次线性方程的齐次方程组。其中未知数的个数为 $2(n-t-1)-k<n$，由此可知 a_i、b_j 存在非零解，即 $A(x,y)$、$B(x,y)$ 存在。

2）证明纠错后的码字等于 $\{d(\mathcal{P}_1),d(\mathcal{P}_2),\cdots,d(\mathcal{P}_n)\}$。不妨设收到的码字 mG_{pub} 等于 $(f(\mathcal{P}_1),f(\mathcal{P}_2),\cdots,f(\mathcal{P}_n))$，其中 $V(f)\leqslant k$。由 1）知，至少有 $n-t$ 个有理点 $\mathcal{P}_i$ 使得 $A(\mathcal{P}_i)+B(\mathcal{P}_i)f(\mathcal{P}_i)=0$。又由 $V(A+Bf)<n-t$ 知 $A+Bf=0$，即 $d(x,y)=f$。因此，$d(\mathcal{P}_i)=f(\mathcal{P}_i)=mG_{\text{pub}}$。

2.4.3 解密算法

根据上文介绍的椭圆曲线码的子域子码的快速译码算法，对收到的密文 $r=m\boldsymbol{SGP}+\boldsymbol{e}=\{r_1,r_2,\cdots,r_n\}$，解密算法过程如下：

1）消除置换矩阵 $\boldsymbol{P}$ 的影响：$r'=rP^{-1}=m\boldsymbol{SG}+\boldsymbol{e}'$。

2）清除错误位：$m'=\boldsymbol{\Phi}(r')=m\boldsymbol{S}$。

3）恢复消息向量：$m=m'\boldsymbol{S}^{-1}$。

3 安全性能分析

目前，针对 McEliece 密码系统主要存在两类攻击方法。第一类攻击尝试从密文中恢复明文信息的信息恢复攻击，信息集译码攻击算法是这一类攻击算法的代表，3.2 节中讨论了信息集译码攻击算法对提出的密码方案的安全性的影响。第二类是根据选取的编码的性质，试图从公钥中恢复私钥的密钥恢复攻击。目前，尚没有直接针对基于椭圆曲线码的子域子码的 McEliece 密码系统的密钥恢复攻击方法。由于椭圆曲线码是构建在亏格为 1 的代数曲线上的代数几何码，因此 3.4 节中讨论了针对基于代数几何码的 McEliece 密码系统的密钥恢复攻击对提出的密码系统的影响。最终证明，在现有的攻击方法下，本文中提出的密码系统是安全的。

3.1 穷搜攻击

穷搜攻击的基本思路是根据公钥矩阵的信息，通过遍历搜索所有可能的 $k\times k$ 可逆矩阵，$n\times n$ 置换矩阵以及使用的有理点集的方法，恢复出私钥 $(S,P,\mathcal{P})$。在 $\mathbb{F}_2$ 上，$k\times k$ 可逆矩阵的个数为 $|S|=\prod_{i=0}^{k-1}(2^k-2^i)=2^{k(k+1)-1}$，$n\times n$ 置换矩阵的个数为 $|P|=n!\approx n^n e^{-n}\sqrt{2\pi n}$。在 $\mathbb{F}_q$ 上，不同构的椭圆曲线的个数约为 $|\mathcal{X}|\approx 2q$[19]。椭圆曲线上的有理点的数量区间为 $[q-2\sqrt{q}+1,q+2\sqrt{q}+1]$。椭圆曲线上基数为 n 的有理点集 $|\mathcal{P}|$ 的数量区间为 $\left[\binom{q-2\sqrt{q}+1}{n},\binom{q+2\sqrt{q}+1}{n}\right]$。

基于上述分析，攻击者成功实施穷搜攻击的可能性为 $1/|S||P||\mathcal{P}||\mathcal{X}|$。当 n、k 取较大值时，设计的密码系统能够有效抵御穷搜攻击。

3.2 信息集译码攻击

1962 年，Prange 针对一般线性码的译码问题提出了信息集译码算法[20]。

定义 1 令 G 代表一个 $[n,k]$ 线性码 C 的生成矩阵，I 代表 $\{1,2,\cdots,n\}$ 的一个基数为 k 的子集。选择 G 中以 I 为索引的列构成一个 $k\times k$ 矩阵 G_I。若 G_I 可逆，则称 I 为 G 的一个信息集。

下面是信息集译码算法的一个简单例子。

令 I 代表 $\mathbb{F}_q$ 上的一个线性码 C 的生成矩阵 G 的一个信息集，y 代表 $\mathbb{F}_q^n$ 上的一个向量，c 代表 C 的一个码字，且 $d(y,c)=w$，$w\neq 0$。令 y_I 和 c_I 代表按 I 索引的 y 和 c 的子集。若 $y_I=c_I$，则可以计算码字 $c=y_I G_I^{-1}G$。

P. J. Lee 和 E. F. Brickell 两位学者率先将信息集译码算法用于 McEliece 公钥密码系统的安全分析[21]。在此基础上，许多名学者对信息集译码攻击算法进行了改进[22-25]。当使用的线性码的码率 $\frac{k}{n}$ 接近 $\frac{1}{2}$ 时，能够使用码长 n 来估算算法的最坏时间复杂度[24]。表 1 中列出了不同的信息集译码攻击算法的最坏时间复杂度。从表 1 的结果可知，通过选取合适的线性码，提出的密码方案能够有效地抵御信息集译码攻击。

表 1 信息集译码攻击算法的时间复杂度

算法	LM[25]	MO[24]	BJMM[23]	Stern[22]	Prange[20]
时间复杂度	$O(2^{0.0465n})$	$O(2^{0.0473n})$	$O(2^{0.0494n})$	$O(2^{0.0557n})$	$O(2^{0.0576n})$

3.3 消息重传攻击

1997 年，Berson 和 Thomas 证明 McEliece 公钥密码系统在消息重传场景下是不安全的[26]。

令 m 代表一个明文向量。假设存在两个由 m 生成的密文 $c_1=mG_{\text{pub}}+e_1$ 和 $c_2=mG_{\text{pub}}+e_2$ 其中 $e_1\neq e_2$。由 McEliece 密钥方案的初始定义可知 $c_1-c_2=e_1-e_2$。根据这一关系，攻击者可以快速的找到一个信息集 I 使得 $c_I=m_I$，从而恢复出明文 m。

和初始的 McEliece 密钥方案相同，基于椭圆曲线码的子域子码的 McEliece 密钥方案在消息重传场景下也是不安全的。

为了使 McEliece 密码系统达到 CCA-2 安全级别。有学者提出了可用于基于编码理论的密码系统的具有 CCA-2 安全级别的加密方案[27-28]。

3.4　针对基于代数几何码的 McEliece 公钥系统的密钥恢复攻击

目前,尚没有针对基于代数几何码的子域子码的 McEliece 密码系统的攻击方法。由于选择的编码是代数几何码的一类子码,本节将分析针对基于代数几何码的 McEliece 密钥系统的攻击方法对提出的密钥系统的安全性能的影响。

3.4.1　Faure 的攻击算法

2007 年,Faure 和 Minder 提出了针对基于椭圆曲线码的 McEliece 密钥系统的攻击算法[29]。这一算法的基本思路是,根据椭圆曲线上所有有理点构成的阿贝尔群,攻击者能够找到一条与选择的曲线同构的椭圆曲线,并最终根据两条曲线间的映射来恢复所选用的椭圆曲线。

为了从公开信息中构造所选用的椭圆曲线的所有有理点构成的阿贝尔群,攻击者需要找到所选用的椭圆曲线码的一个具有最小汉明重量的码字。

定义 2　对于一个$[n,k,d]$椭圆曲线码,其码字的最小汉明重量等于它的码距 $d=n-k$。

椭圆曲线码的子域子码的码距大于等于其原码的码距。在实际构造中,当椭圆曲线码所在的有限域大于$\mathbb{F}_{2^6}$时,总能构造出码距大于原码码距的子域子码。比如,参数为[64,54,10]的椭圆曲线码的子域子码的参数为[64,10,16],参数为[128,113,15]的椭圆曲线码的子域子码的参数为[128,23,36]。

无法从子域子码中获得原码的一个具有最小汉明重量的码字使得 Faure 的攻击算法对提出的密码方案无效。

3.4.2　Couvreur 的攻击算法

2017 年,Couvreur 等人提出了针对基于代数几何码及其子码的 McEliece 系统的攻击算法。但 Couvreur 等在论文中阐明,这一攻击算法并不适用于基于代数几何码的子域子码的 McEliece 密码系统[13]。

3.5　公钥体积及推荐参数

与最初的 McEliece 密码方案相同。提出的基于椭圆曲线码的子域子码的 McEliece 密码系统的公钥是一个大小为 $n\times k$ 比特的矩阵。合适的具有 CCA-2 安全级别的加密方案能够在保持安全性能的同时,将密钥方案的公钥转变为一个大小为$(n-k)\times k$ 比特的标准形式矩阵[30]。

推荐使用$\mathbb{F}_{2^{12}}$上参数为[2 048,1 328,60]的椭圆曲线码的子域子码来构建安全级别为 80 比特的 McEliece 密码系统。在不采用具有 CCA-2 安全级别的加密方案的情况下,推荐方案的公钥体积为 2 719 744 比特。在采用具有 CCA-2 安全级别的加密方案的情况下,推荐方案的公钥体积为 956 160 比特。

4　结　语

本文的主要贡献在于构造了一个新的基于椭圆曲线码的子域子码的 McEliece 公钥密码系统。并使用针对 McEliece 公钥密码系统的攻击算法及针对基于代数几何码的 McEliece 密码系统的攻击算法对提出系统的安全性能进行分析。分析证明,在现有的攻击下,本文提出的基于椭圆曲线码的子域子码的公钥密码系统是安全的。

未来该方案可作为基于编码理论的密码系统的一个备选方案,在数字签名、零知识证明等方面展开进一步的研究。

参　考　文　献

[1] Shor P W. Polynominal time algorithms for discrete logarithms and factoring on a quantum computer[C]//Proceedings of the First International Symposium on Algorithmic Number Theory. London: Springer-Verlag, 1994.

[2] Mceliece R J. A Public-Key Cryptosystem Based on Algebraic Coding Theory[J]. Deep Space Network Progress Report, 1978, 44:114-116.

[3] Gaborit P. Shorter keys for code-based cryptography[C]//Proceedings of Workshop on Codes and Cryptography, WCC 2005, 2005:81-90.

[4] Baldi M, Chiaraluce F, Garello R, et al. Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem [C]//IEEE International Conference on Communications. IEEE, 2007.

[5] Berger T P, Cayrel P L, Gaborit P, et al. Reducing Key Length of the McEliece Cryptosystem [C]//International Conference on Progress in Cryptology-africacrypt. DBLP,2009.

[6] Misoczki R, Tillich J P, Sendrier N, et al. MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes[C]//IEEE International Symposium on Information Theory. IEEE, 2013.

[7] Aragon N, Barreto P S L M, Bettaieb S, et al. BIKE:bite flipping key encapsulation[OL]. http://bikesuite.org/files/BIKE.pdf.

[8] Melchor C A, Deneuville J C, Aragon N, et al. Hamming quasi-cyclic(HQC)[OL]. https://pqc-hqc.org/doc/hqc-specification_2017-11-30.pdf

[9] Otmani A, Tillich J P, Léonard Dallot. Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes[J]. Mathematics in Computer Science, 2010, 3(2):129 - 140.
[10] Faugère J C, Otmani A, Perret L, et al. Algebraic Cryptanalysis of McEliece Variants with Compact Keys[C]//Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2010: 279 - 298.
[11] Guo Q, Johansson T, Stankovski P. A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors[C]// International Conference on the Theory and Application of Cryptology and Information Security—ASIACRYPT 2016. Springer Berlin Heidelberg, 2016: 789 - 815.
[12] Janwa H, Moreno O. McEliece Public Key Cryptosystems Using Algebraic-Geometric Codes [C]//IEEE International Symposium on Information Theory. IEEE, 1996.
[13] Couvreur A, Marquez-Corbella I, Pellikaan R. Cryptanalysis of mceliece cryptosystem based on algebraic geometry codes and their subcodes[J]. IEEE Transactions on Information Theory, 2017, 63(8):5404 - 5418.
[14] Goppa V D. Codes on algebraic curves[J]. Soviet Mathematics Doklady, 1981, 24:170 - 172.
[15] Fulton W. Algebraic curves—an introduction to algebraic geometry(reprint vrom 1969)[M]. Boston: Addison-Wesley, 1989.
[16] Alzubi J, Alzubi O, Chen T. Forward error correction based on algebraic-geometric theory[M]. Berlin: Springer, 2014.
[17] Justesen J, Larsen K J, Jensen H E, et al. Construction and decoding of a class of algebraic geometry codes[J]. IEEE Transactions on Information Theory, 1989, 35(4):811 - 821.
[18] Silverman J H. The arithmetic of elliptic curves[M]. Berlin: Springer, 2009.
[19] Schoof R. Nonsingular plane cubic curves over finite fields [J]. Journal of Combinatorial Theory, Series A, 1987, 46 (2):183 - 211.
[20] Prange E. The use of information sets in decoding cyclic codes[J]. IRE Transactions on Information Theory, 1962, 8 (5):5 - 9.
[21] Lee P J, Brickell E F. An observation on the security of mceliece's public-key cryptosystem[C]//Advances in Cryptology — EUROCRYPT' 88: Workshop on the Theory and Application of Cryptographic Techniques. 1988: 275 - 280.
[22] Stern J. A method for finding codewords of small weight[C]// International Colloquium on Coding Theory and Applications. Springer, Berlin, Heidelberg, 1988.
[23] Becker A, Joux A, May A, et al. Decoding Random Binary Linear Codes in $2^{n/20}$: How 1 + 1 = 0 Improves Information Set Decoding[C]//International Conference on Theory & Applications of Cryptographic Techniques. Springer-Verlag, 2012.
[24] May A, Ozerov I. On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes[M]//Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015.
[25] Both L, May A. Decoding Linear Codes with High Error Rate and Its Impact for LPN Security[C]//International Conference on Post-quantum Cryptography. Springer, Cham, 2018.
[26] Berson T A. Failure of the mceliece public-key cryptosystem under message-resend and related-message attack[C]//Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 1997: 213 - 220.
[27] Kobara K, Imai H. Semantically secure mceliece public-key cryptosystems-conversions for mceliece PKC[C]//Public Key Cryptography. 2001.
[28] Kiltz E, Mohassel P, O'Neill A. Adaptive trapdoor functions and chosen-ciphertext security[C]//Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2010: 673 - 692.
[29] Faure C, Minder L. Cryptanalysis of the mceliece cryptosystem over hyperelliptic codes[C]//Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, 2008:99 - 107.
[30] Bernstein D J, Lange T, Peters C. Attacking and Defending the McEliece Cryptosystem[C]//International Workshop on Post-quantum Cryptography. Springer-Verlag, 2008.

(上接第 301 页)

[6] 孙韩林, 刘建华. 公众网络统一身份认证服务及标准研究[J]. 电信科学, 2017, 29(2):84 - 88.
[7] 邓红, 杨茹, 王亚东. 基于云计算平台的鉴权分析[J]. 信息技术, 2014, 38(7):180 - 182.
[8] Owen S. Zxing[M]. Zebra Crossing, 2013.
[9] Pedregosa F, Varoquaux G, Gramfort A, et al. Scikit-learn: Machine learning in Python[J]. Journal of machine learning research, 2011, 12(10): 2825 - 2830.
[10] M'Raihi D, Machani S, Pei M, et al. Totp: Time-based one-time password algorithm[R]. RFC 6238, 2011.
[11] McCallum A, Nigam K. A comparison of event models for naive bayes text classification[C]. AAAI-98 workshop on learning for text categorization. 1998, 752: 41 - 48.
[12] 邓小鹏, 邢春晓, 蔡莲红. Web 应用测试技术进展[J]. 计算机研究与发展, 2007, 44(8):1273 - 1283.
[13] 宋巍, 张春柳, 邬斌亮. Web 系统性能测试研究与实践[J]. 计算机应用与软件, 2015, 32(3): 4 - 6.
[14] Memon P, Hafiz T, Bhatti S, et al. Comparative Study of Testing Tools Blazemeter and Apache Jmeter[J]. Sukkur IBA Journal of Computing and Mathematical Sciences, 2018, 2(1):70 - 76.