基于编码的后量子公钥密码研究进展

王丽萍 [1,2], 戚艳红 [2]

[1] 中国科学院信息工程研究所信息安全国家重点实验室, 北京 中国 100093
[2] 中国科学院大学网络空间安全学院, 北京 中国 100049

摘要 基于编码的公钥密码由于能抵抗量子攻击和美国 NIST 后量子公钥密码算法的征集而受到越来越多的关注。本文主要围绕最近的基于编码的 NIST 抗量子攻击公钥密码征集算法, 梳理基于编码的公钥方案具有的特点, 即三种加密方式, 三种重要的参与码类, 三种安全性基于的困难问题, 为对这方面有兴趣的科研人员提供一篇综述性论文。

关键词 后量子公钥密码; 基于编码的公钥密码; NIST 后量子候选方案
中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2019.03.03

Recent progress of code-based post-quantum public key cryptography

WANG Liping[1,2], QI Yanhong[2]

[1]State key laboratory of information security, Institute of Information Engineering , Chinese Academy of Sciences, Beijing 100093, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Code-based public key cryptography has received more and more attention due to its resistance to quantum attacks and call for post-quantum public key cryptography by NIST. In this paper, we focus on the NIST submissions based on hardness of syndrome decoding problem, and study the characteristics of these code-based schemes, i.e., three encryption methods, three important involving code classes, and three difficult problems. We provide a survey paper for those who are interested in this areas.

Key words post-quantum public key cryptography; Code-based public cryptography;NIST post-quantum candidates

1 背景

近些年来许多国家都投巨资用于量子计算机的研制, 量子计算机提高了密码分析的攻击能力, 由于 shor 算法可以在多项式时间内解决大整数分解和椭圆曲线上的离散对数问题[1], 因此一旦实用的量子计算机研制成功, 大部分实际在用的以大整数分解为基础的 RSA 或椭圆曲线加密的机密文件、国家机密等将不再安全。

实用量子计算机逼近的脚步迫使密码学家们需要提早做好准备, 着手研究能够抵抗量子攻击的密码体制。目前普遍认同基于格理论、基于编码理论和基于多变量等的密码体制能抵抗量子攻击, 并称它们为后量子密码, 因而公钥密码已经进入了后量子密码时代。

欧盟对后量子密码的研究非常重视, 召集了欧洲在该方向著名的科学家们成立后量子密码项目, 并且已经给出了一些后量子密码候选方案[2]。

鉴于量子计算机的快速发展, 2016 年秋美国国家标准与技术研究院(National Institute of Standards and Technology, 简称 NIST)发布了征集新的抗量子计算机攻击的加密算法、密钥交换算法和数字签名算法的时间表[3]。到 2017 年 11 月 30 日 NIST 征集截止, 共收到 82 个候选算法, 经过筛选共 69 个进入第一轮评估, 其中基于格的方案有 29 个, 基于编码的方案有 20 个, 基于多变量的方案有 10 个, 2 个基于 hash, 基于其他困难问题的有 8 个。目前进入第二轮评估的 17 个方案中有 7 个是基于编码的, 详见 NIST 网站[4]。

基于编码的后量子密码的综述已有很多[5-7], 本

通讯作者: 王丽萍, 博士, 研究员, Email: wangliping@iie.ac.cn
本课题得到国家自然基金(No. G1872355)资助和国家密码发展基金(No. MMJJ20170124)资助。
收稿日期: 2018-11-13; 修改日期: 2019-02-25; 定稿日期: 2019-02-28

文主要围绕最近的NIST后量子密码征集项目中的基于编码的算法提案, 梳理出基于编码的公钥方案具有的特点, 即三种加密方式, 三种重要的参与码类, 三种基于的困难问题, 为对这方面有兴趣的科研人员提供一篇综述性介绍。

2 预备知识

为叙述方便, 我们简要介绍一下本文会涉及的关于线性纠错码的一些概念和结果。

首先, 令$\mathbb{F}$为有限域, $\mathbb{F}$上码长为n、维数为k的$[n,k]$-线性码C是指$\mathbb{F}^n$的一个k维向量子空间, 因此它可以由一个$k\times n$的矩阵生成, 该矩阵称为C的生成矩阵。码C的对偶码是C的正交补空间, 对偶码的生成矩阵称为码C的校验矩阵。形如$(I_k \mid X)$的生成矩阵称为标准型或系统型, 形如$(Y \mid I_{n-k})$的校验矩阵称为标准型或系统型校验矩阵。如果$G=(I_k|X)$是一个$[n,k]$线性码C的一个标准型生成矩阵, 则C的校验矩阵为$\boldsymbol{H}=(-X^T|I_{n-k})$。

线性码中一个重要的概念是码重量和码距离, 一般常用的是汉明重量(Hamming weight), 即码字中的非零分量的个数, 记为$w_H(.)$, 两个向量的汉明距离是指它们差的汉明重量。然而近年来很多基于编码的密码体制使用了秩距离码(rank codes)。秩距离(rank distance)是在有限域$\mathbb{F}_{q^m}$上讨论, 设$\beta_1,\cdots,\beta_m$为其在$\mathbb{F}_q$上的一组基向量, $u=(u_1,u_2,...,u_n)\in\mathbb{F}_{q^m}^n$,每个$u_i$可以由基表示为$u_i=\sum_{j=1}^m x_{ji}\beta_j$, 则矩阵$\boldsymbol{U}=(x_{ji})_{1\leqslant j\leqslant m,1\leqslant i\leqslant n}$的秩称为$u$的秩重量, 注记为$w_R(.)$。$\forall u,v\in\mathbb{F}_{q^m}^n$, u和v的秩距离$d(u,v)=w_R(u-v)$。下面我们统一在有限域$\mathbb{F}$上介绍, 具体来说, 汉明距离时令$\mathbb{F}=\mathbb{F}_q$,秩距离时令$\mathbb{F}=\mathbb{F}_{q^m}$, q是素数幂, 距离如不专门说明, 可以是汉明距离, 也可以是秩距离。

线性码C的最小距离d是指最小的非零码字的重量。如果x是码字c通过噪声信道接收到的一个字, 即$x=c+e$, 则$s=Hx^T=He^T$就称作x的校验子。

对正整数n, 令$\mathbb{F}^n$为$\mathbb{F}$上的n维向量空间, 因此$\mathbb{F}^n$中的元素可以看成是一个行向量, 或者是$R=\mathbb{F}[X]/(X^n-1)$中的一个多项式。一个素数n称作本原的, 如果$X^n-1/(X-1)$是R内的一个不可约多项式。对于$\mathbb{F}^n$中的向量$\boldsymbol{u}=(u_0,\cdots,u_{n-1})$, $\boldsymbol{v}=(v_0,\cdots,v_{n-1})$, 我们可以定义类似于在$R$中的乘积运算, 即$\boldsymbol{uv}=\boldsymbol{w}=(w_0,\cdots,w_{n-1})\in\mathbb{F}^n$且

$$w_k=\sum_{i+j=k \bmod n} u_i v_j, k=0,1,\cdots,n-1 \tag{1}$$

下面介绍循环矩阵:

令$\boldsymbol{v}=(v_0,\cdots,v_{n-1})\in\mathbb{F}^n$, 由$v$导出的循环矩阵定义如下:

$$rot(v)=\begin{pmatrix} v_0 & v_{n-1} & \cdots & v_1 \\ v_1 & v_0 & \cdots & v_2 \\ \vdots & \vdots & \ddots & \vdots \\ v_{n-1} & v_{n-2} & \cdots & v_0 \end{pmatrix}\in\mathbb{F}^{n\times n} \tag{2}$$

因此, 很容易看到任意的两个元素$u,v\in\mathbb{F}^n$的乘积$u\cdot v$可以通过$rot(.)$表示为通常的向量-矩阵乘积,即

$$\begin{aligned} u\cdot v &= u\times rot(v)^T=(rot(u)\times v^T)^T \\ &= v\times rot(u)^T=v\cdot u \end{aligned} \tag{3}$$

令$s|n$, $[s\cdot\frac{n}{s},k]$线性分块码$C\subseteq\mathbb{F}^n$称作指标数为s的拟循环码, 如果对于任意的码字$c=(c_1,\cdots,c_s)\subseteq C$, 对每个分块$c_1,\cdots,c_s$同时做循环移位仍然是一个码字。

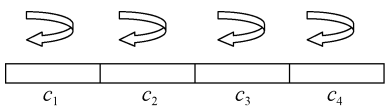

图 1 拟循环码的移位表示示例

Figure 1 Example of quasi-cyclic code shift

3 三种加密方式

基于编码的公钥方案加密方式有很多种, 本节我们总结出常用的三种类型的加密方式, 即McEliece型、Niederreiter型和ElGamal型。

3.1 McEliece型加密方案

第一个基于编码的密码体制是1978年McEliece提出的加密方案[8], 称作McEliece方案, 该方案也是最古老的公钥密码体制之一, 在合适的参数选取下, 至今仍然是安全的。下面我们就介绍一下这个方案。

McEliece方案:

密钥生成:

能纠t个错的$[n, k]$线性码ς的生成矩阵$\boldsymbol{G}$。

私钥 sk: ($\boldsymbol{S}$, $\boldsymbol{G}$, $\boldsymbol{P}$), 其中$\boldsymbol{S}$是一个混淆可逆矩阵和$\boldsymbol{P}$是一个置换矩阵。

公钥 pk: $G'=\boldsymbol{S}\cdot\boldsymbol{G}\cdot\boldsymbol{P}$

加密:

给定明文 m, 一个重量 $w(e)\leqslant t$ 的噪声向量 $\boldsymbol{e}$, 密文通过如下过程获得:

$$c \leftarrow mG' + e$$

解密:

令 $\boldsymbol{\Phi}_G$ 是能纠 t 个错误的译码算法, 则明文可通过如下过程解密得到:

$$m \leftarrow \Phi_G(cP^{-1})S^{-1}$$

McEliece 方案最大的不足之处就是公钥规模太大, 现在大家都采用如下的方案:

McEliece 方案的现代版:

密钥生成:

给定一个能纠 t 个错的$[n, k]$线性码ς的生成矩阵 $\boldsymbol{G}$。

私钥 sk: $\boldsymbol{G}$

公钥 pk: $\boldsymbol{G}' = (IQ)$ 为 G 的标准型

加密:

给定要加密的明文 $\mathbf{m}$,一个重量 $w(e)\leqslant t$ 的噪声向量 $\boldsymbol{e}$, 密文通过如下过程获得:

$$c = \leftarrow mG' + \boldsymbol{e}$$

解密:

令 $\boldsymbol{\Phi}_G$ 是能纠 t 个错误的译码算法, 则明文可通过如下过程解密得到:

$$m \leftarrow \Phi_G(c)$$

注: 1. 能选到一个标准的生成矩阵的码的概率是 29%, 因此密钥生成所需的时间比平均值慢 3.4 倍[4]。

2. 对于二元码, 公钥规模由 kn 比特变为 $k(n–k)$。

3. 对有限制的码类的攻击意味着 29%的概率可以攻击无限制的码类, 而他们的安全性最多只差 2 个比特。

4. 上述密码方案并没有对码类的选取有要求, 然而, 除了原方案中使用的 Goppa 码至今仍然是安全的, 替换的广义 Reed-Solomon 码、Gabidulin 码、Reed-Muller 码和卷积码等都几乎被彻底破解了[9-12]。

3.2 Niederreiter 型加密方案

Niederreiter 在 1986 年提出了利用广义 Reed-Solomon 码的校验矩阵加密的公钥体制[13], 然而, Sidelnikov 和 Shestakov 证明了这个方案是不安全的[9]。这两个体制的区别在于前者加密使用的是生成矩阵, 而后者使用的是校验矩阵, 因而如果后者也换成 Goppa 码则是对偶等价的[14]。

Niederreiter 型加密方案

密钥生成:

给定一个能纠 t 个错的$[n, k]$线性码ς的校验矩阵 $\boldsymbol{H}$。私钥 sk:$(\boldsymbol{S}, \boldsymbol{H}, \boldsymbol{P})$, 其中 $\boldsymbol{S}$ 是混淆可逆矩阵, $\boldsymbol{P}$ 是一个置换矩阵。

公钥 pk: $H' = \boldsymbol{S} \cdot \boldsymbol{H} \cdot \boldsymbol{P}$

加密:

重量 $wt(e)\leqslant t$ 的噪声向量 $\boldsymbol{e}$,被用来表示明文信息 m,密文 s 通过如下过程获得:

$$s \leftarrow H'e^T$$

解密:

令 $\boldsymbol{\Phi}_H$ 是能纠 t 个错误的译码算法, 则明文可通过如下过程解密得到:

$$e \leftarrow P^{-1}\boldsymbol{\Phi}_H(S^{-1}s)$$

同样, 我们给出 Niederreiter 型方案的现代版如下:

密钥生成:

给定一个能纠 t 个错的$[n, k]$线性码ς的校验矩阵 $\boldsymbol{H}$。

私钥 sk: $\boldsymbol{H}$

公钥 pk: $\boldsymbol{H}' = [Q \mid I_{n-k}] \leftarrow\!\!\!- \boldsymbol{H}$

加密:

重量 $w(e)\leqslant t$ 的噪音向量$\boldsymbol{e}$,被用来表示明文信息 m,密文 $\boldsymbol{s}$ 通过如下过程获得:

$$s \leftarrow H'e^T$$

解密:

令 $\boldsymbol{\Phi}_H$ 是能纠 t 个错误的译码算法, 则明文可通过如下过程解密得到:

$$e \leftarrow \boldsymbol{\Phi}_H(s)$$

3.3 ElGamal 型的加密方案

最近, 受格的思想启发, 一些基于编码的公钥方案的构造类似于基于 LWE(Learning With Errors),

Ring-LWE (Ring-Learning With Errors), LPN(Learning Parity with Noise)等的公钥方案, 该构造方法与以前的不同, 上面的方法都是直接隐藏码的结构, 而这个构造方法是一个与以往方法不同的突破, 为基于编码的密码研究给出了一个新思路。例如, NIST 候选算法中 HQC, RQC, Ouroboros-R 等方案就是基于上述加密方式构造的[4], 这三种加密方案的公钥规模都能达到 1000 字节以下, 可以和基于格的一些高效算法竞争。

具体来说, HQC、RQC 和 Ouroboros-R 等加密方案是类似于 ElGamal 型加密方式, 不同之处在于前者使用汉明距离后两者是秩距离。考虑在多项式剩余类环 $\mathbb{F}[X]/(X^n-1)$ 上, 公钥为 $(h,s=hx+y)$, 其中 h 为随机选取, x 和 y 是随机选取的低重量的多项式, 密文为(c_1,c_2), 其中 $c_1=hr_2+r_1$, $c_2=sr_2+e+mG$, r_1, r_2 和 e 为随机选取的低重量的多项式,m 是明文, G 是可以快速译码的某个码的生成矩阵。Ouroboros-R 在 c_2 中去掉 mG, 直接重建 e, r_1, r_2 生成的子空间。

第三类采用 ElGamal 型的加密形式, 我们以 NIST 候选方案 RQC 或 HQC 为例。其中 $\xleftarrow{\$}$ 表示随机选取。

ElGamal 型加密方案

密钥生成

随机取样 $h\xleftarrow{\$}R=\mathbb{F}[X]/(X^n-1)$, 能纠错的码 C 的生成矩阵 $\boldsymbol{G}$。

私钥 sk: $(x,y)\xleftarrow{\$}R^2$ 且 $w(x)=w(y)=w$.

公钥 pk: $(h,s=y+h\cdot x)$.

加密:

生成噪声向量 $e\xleftarrow{\$}R$、$(r_1,r_2)\xleftarrow{\$}R^2$ 使得 $w(e)=w(r_1)=w(r_2)=w_e$。密文(c_1, c_2)如下:

$$c_1=r_1+h\cdot r_2,\ \ c_2=mG+s\cdot r_2+e.$$

解密:

令 $\boldsymbol{\Phi}_G$ 是能纠 t 个错误的译码算法, 解密如下:

$$m\leftarrow\boldsymbol{\Phi}_G(c_2-c_1\cdot x)=\boldsymbol{\Phi}_G(m\boldsymbol{G}+yr_2-r_1x+e)$$

本节最后, 我们将20个基于编码的NIST方案根据加密方式的不同进行了如下的分类:

1.McEliece 型:

NTS-KEM, RLCE-KEM, DAGS, QC-MDPC KEM, LEDAkem, LEDApkc, McNie, Edon-K(已撤回), pqsigRM(已攻破), RaCoss(已攻破)

2.Niederreiter 型:

Classic McEliece, BIG QUAKE, BIKE-II, LAKE, LOCKER, RankSign(已攻破)

3.ElGamal 型:

HQC, Lepton, RQC, BIKE-I, BIKE-III, Ouroboros-R

4 三种常用码类

在基于编码的 McEliece 型和 Niederreiter 型公钥密码方案中, 公钥规模较小又安全的主要是三类码: Goppa 码、QC-MDPC 码和 QC-LRPC 码。

4.1 Goppa 码

Goppa 码是由 V. D. Goppa 提出的[15,16], 我们主要介绍一下用于 McEliece 方案的二元 Goppa 码。

令 m 和 t 为正整数, 令 $g(X)=\sum_{i=0}^{t}g_iX^i\in\mathbb{F}_{2^m}[X]$ 是次数为 t 的多项式, 称为 Goppa 多项式, 且 $L=(a_1,\cdots,a_n)\in\mathbb{F}_{2^m}^n$ 是 n 个不同元素的

集合, 且 $g(a_i)\neq 0, i=1,2,\cdots,n.$

对于任意的向量 $c=(c_0,\cdots,c_{n-1})\in\mathbb{F}_2^n$, Goppa 码定义如下:

$$\varsigma(g(X),L)=\left\{(C_0,\cdots,C_{n-1})\in\mathbb{F}_2^n\middle|\right.$$

$$\left.S_c(X)=\sum_{i=1}^{n}\frac{c_{i-1}}{X-a_i}=0\bmod g(X)\right\}.$$

命题 4.1([15])对于 Goppa 码 $\varsigma(g(X),L)$, 则它的校验矩阵为

$$\boldsymbol{H}=\begin{pmatrix} g(a_1)^{-1} & \cdots & g(a_n)^{-1} \\ a_1g(a_1)^{-1} & \cdots & a_ng(a_n)^{-1} \\ \vdots & \cdots & \vdots \\ a_1^{t-1}g(a_1)^{-1} & \cdots & a_n^{t-1}g(a_n)^{-1} \end{pmatrix}$$

$$=\begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ \vdots & \cdots & \vdots \\ a_0^{t-1} & \cdots & a_n^{t-1} \end{pmatrix}\begin{pmatrix} g(a_1) & 0 & \cdots & 0 \\ 0 & g(a_2)^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g(a_n)^{-1} \end{pmatrix}$$

命题 4.2([15])对于二元 Goppa 码 $\varsigma(g(X),L)$ 且 $deg(g(X))=t$,则 Goppa 码是二元线性码, 参数为[n,k,d], 其中 $k \geqslant n-mt$ 且 $d \geqslant t+1$。特别地, 如果 $g(x)$是不可约多项式, 则 $d \geqslant 2t+1$。

关于 Goppa 码的译码算法, 最常用的就是 Berlekamp-Massey 算法[17-19], 特别地, 对于二元 Goppa 码, 文献[20]中为二元不可约 Goppa 码描述了一个能纠 t 个错误的更高效的译码算法, 该算法的计算复杂度为

$$O(n \cdot t \cdot m^2)$$

二元运算, 当 $mt \geqslant (n-k)$, 具体的算法读者可以参考文献, 在此就不赘述了。

在 NIST 基于编码的候选算法中, Classic McEliece 和 NTS-KEM 都使用了二元 Goppa 码的 Niederreiter 型加密方案, 其优点在于基于 Goppa 码的方案经历了将近 40 年的考验, 其安全性令人信服, 加解密速度快, 能抵抗量子计算机的攻击, 但缺点是公钥规模大, Classic McEliece 中 128 比特安全的公钥选取的长度是 1047319 字节。与 RSA 的参数相比, 密钥长度为 1024 比特的 RSA 的安全性与密钥长度为 69k 比特的 McEliece 体制的安全性相当。

为了减少公钥规模, 人们常常使用拟循环 Goppa(Quasi-Cyclic Goppa)码, 例如, NIST 候选方案 BIG-QUAKE。下面我们具体给出如何选取 Goppa 码的参数使之成为拟循环 Goppa 码。

1. 令 l 是一个能整除 2^m-1 的素数, 且 ς_l 是本原 l 阶单位根。

2. 令 n, t 是能被 l 整除的正整数, 且令 $r=\frac{t}{l}$。

3. 将 L 分成每块长为 l 的 n/l 块, $(a_{il}, a_{il+1}, \cdots, a_{il+l-1})$, 使得对任意的 $j \in \{1,2,\cdots,l-1\}$, $a_{il+j}=\varsigma_l^j a_{il}$。

4. Goppa 多项式 $g(X)$ 满足 $g(X)=h(X^l)$, 其中 $h(X) \in \mathbb{F}_{2^m}[X]$, 次数为 $\frac{t}{l}$ 且 $h(X^l)$ 是不可约多项式。

我们得到的 Goppa 码 $\varsigma(L,g(X))$ 是一个拟循环 Goppa 码, 且它的校验矩阵为

$$\boldsymbol{H}=(I|\boldsymbol{M}) \tag{4}$$

其中 $\boldsymbol{M}$ 是一个指标数为 l 的拟循环矩阵。

4.2 QC-MDPC 码

第二类基于编码的公钥方案中常用的是 QC-MDPC 码。所谓[n,k,w]-LDPC 或 MDPC(low- density or moderate-density parity-check)码是指码长为 n, 码的维数为 k, 校验矩阵的行汉明重量均为 w 的线性码。LDPC 码和 MDPC 码的区别仅在于行重量 w 的大小, LDPC 码行重量很小, 一般都小于 10, 译码算法非常快, 而 MDPC 码的行重量数量级为 $O(\sqrt{n\log n})$, 但仍然存在高效的译码算法。

为了克服公钥长度过长这一缺点, 类似于基于格的密码中使用循环格和理想格代替一般格的想法, 近几年流行的方法就是利用具有简洁的校验矩阵或生成矩阵的交错码或 Goppa 码的子类, 例如有些码类具有拟循环(Quasi-Cyclic,简写为 QC)[21]和拟双值(Quasi-Dyadic,简写为 QD)结构的生成矩阵的码类[22]。由于存储这样的生成矩阵或校验矩阵只需要存储一行就可以, 因此提高了存储效率。

基于 QC-LDPC 码的 McEliece 密码体制由于行重量太稀疏很容易被攻破[23,24], 因而基于 QC-MDPC 码的密码体制在文献[25]中提出, 目前只有在[26]论文给出了一个的攻击分析, 因此安全性也很高, 又由于其存储规模小, 译码效率高而受到青睐, 例如 NIST 基于编码的候选算法中 LEDAkem、LEDApkc、QC-MDPC KEM、BIKE 等都使用了 QC-MDPC 码的 McEliece 型或 Niederreiter 型或 ElGamal 型加密体制。

因此我们主要看一下密钥生成部分就可以了。

我们考虑形如下面的二元校验矩阵

$$H=(H_1 H_2 \cdots H_l)$$

其中 $r=n-k$, $n=rl$, r 是素数, 且 $\boldsymbol{H}_i$ 是 $r \times r$ 循环矩阵。构造这样的校验矩阵只需要产生一行就可以了, 即随机选取长度为 n 的汉明重量约 $O(\sqrt{n\log n})$ 的二元向量 h, 再将它分成 l 个长为 r 的子串, 即

$$h=\left[(h_0,h_1,\cdots,h_{r-1}),(h_r,\cdots,h_{2r-1}),\cdots,h_{r(l-1)},\cdots,h_{rl-1}\right]$$

其中, 子向量 $(h_{ir},\cdots,h_{(i+1)r-1})$ 是 $\boldsymbol{H}_i$ 的第一行。

由于它的标准型是 $(H_l^{-1}H_l,\cdots,H_l^{-1}H_{l-1},I_r)$, 因此我们可以得到它的生成矩阵 $\boldsymbol{G}=(I_k Q)$, 其中

$$Q=\begin{pmatrix}(H_l^{-1}H_1)^T\\ \vdots \\ (H_l^{-1}H_{l-1})^T\end{pmatrix}$$

这样我们就把 H 作为私钥, G 作为公钥。

4.3 QC-LRPC 码

20 个基于编码的 NIST 候选方案中就有 6 个使用了秩距离码。秩距离是 1951 年华罗庚先生引入的[27], 最有影响的基于秩距离码的密码体制是由 Gabidulin, Paramonov 和 Tretjakov 在 1991 年提出的[28], 简称为 GPT。该密码体制用 Gabidulin 码来替换 McEliece 体

制中的 Goppa 码[29], Gabidulin 码中的码字可以看成一个矩阵, 因此码字的重量用该矩阵的秩衡量, 而不用常用的汉明重量表示。然而 GPT 算法被 Overbeck 攻破了[30], 主要原因就是 Gabidulin 码是类似于汉明距离下的 Reed -Solomon 码, 因而 Gabidulin 码的代数结构太强。

类似于 LDPC 或 MDPC 码, 可以定义 LRPC 码。令 $H=(h_{ij})_{1\leqslant i\leqslant n-k,1\leqslant j\leqslant n}\in\mathbb{F}_{q^m}^{(n-k)\times n}$ 是一个满秩矩阵, 使得它的所有矩阵元素产生一个小维数为 d 的 $\mathbb{F}_q$ 子空间。如果 d 比较小, 则称 C 是具有低秩重量 d 的 LRPC(低秩校验)码。

另外, 对于 LRPC 码, 同样有高效的恢复噪声支撑的算法。最近在基于编码的 NIST 候选方案 Ouroboros-R 中, 作者们同时利用了在文献[31]中给出的 LRPC 码的一般译码算法和在文献[32]中的改进算法, 给出了一个更高效的译码算法。详见上述参考文献。

由于秩距离码在参数选取上有优势, 在 NIST 候选算法中 LAKE、LOCKER、McNie 都使用了 QC-LRPC 码的 McEliece 型或 Niederreiter 型加密体制。

总体来说, 我们将 20 个基于编码的 NIST 方案根据其使用的码类进行了一个分类如下:

- Goppa 码: BIG-QUAKE, Classic McEliece, NTS-KEM
- QC-LRPC 码: LAKE, LOCKER, McNie, RQC, Ouroboros-R, RankSign(已攻破)
- QC-MDPC 码: BIKE, HQC, LEDAkem, LEDApkc, QC-MDPC KEM
- Dyadic Generalized Srivastava 码:DAGS
- 广义 Reed-Solomon 码: RLCE-KEM
- Reed-Muller 码:pqsigRM
- 随机线性码: Lepton, RaCoss

5 三种困难问题

基于编码的公钥方案的安全性也是要归约到某种困难问题, 我们列出了主要的三类困难问题, 校验子译码(SD)困难问题、拟循环码的校验子译码(QCSD)困难问题和拟循环秩码的校验子译码(RQCSD)困难问题。

5.1 SD 困难问题

首先我们给出什么是校验子译码(SD)困难问题。

校验子译码问题(Syndrome Decoding Problem): H 是有限域 $\mathbb{F}$ 上的随机线性码 C 的 $(n-k)\times n$ 的校验矩阵, $s\in\mathbb{F}^{n-k}$, 找一个重量小于 d 的字 $x\in\mathbb{F}^n$ 使得 $Hx^T=s$。

在汉明距离下, 上述问题在 1978 年就已经被证明是 *NP*-难问题[33], 最近, 在文献[34]中证明可以通过概率约化将秩距离下的校验子译码问题归约到汉明距离下, 因而同样可证明是 *NP*-难问题, 因此很多基于编码的公钥密码体制的安全性都声称主要基于随机线性码的校验子译码问题。

经典的 McEliece 体制中安全性是假定混淆过的公钥可以看成是随机线性码的生成矩阵, 因此我们也把这类的方案看成基于 SD 困难问题, 例如 NIST 候选方案的 Classic McEliece。

5.2 QCSD 困难问题

拟循环校验子译码问题(Quasi-Cyclic Syndrome Decoding (QCSD)Problem): H 是有限域 $\mathbb{F}$ 上的拟循环码 C 的 $(n-k)\times n$ 的拟循环校验矩阵, $s\in\mathbb{F}^{n-k}$,找一个汉明重量小于 d 的字 $x\in\mathbb{F}^n$ 使得 $Hx^T=s$。

校验子译码问题已经被证明是 *NP*-困难问题, 然而拟循环校验子译码问题的困难性还没有得到证明, 但目前也没有因为其结构的特殊性提出有效的攻击算法。但是由于降低了公钥规模, 因此很多基于编码的 NIST 候选算法都是基于这个问题的困难假设。

5.3 RQCSD 困难问题

拟循环校验子译码问题(Rank Quasi-Cyclic Syndrome Decoding (RQCSD) Problem): H 是有限域 $\mathbb{F}_{q^m}$ 上的拟循环码 C 的 $(n-k)\times n$ 的拟循环校验矩阵, $s\in\mathbb{F}_{q^m}^{n-k}$, 找一个秩重量小于 d 的字 $x\in\mathbb{F}_{q^m}^n$ 使得 $Hx^T=s$。

这个问题类似于上一个问题, 不同之处就是使用的是秩距离, 而不是汉明距离。

最后, 我们将 20 个基于编码的 NIST 方案根据基于的不同困难问题给出一个分类:

1. 基于 SD 问题:

Classic McEliece, NTS-KEM, RLCE-KEM, DAGS, Lepton, Edon-K(已撤回), pqsigRM(已攻破), RaCoss(已攻破)

2. 基于 QCSD 问题:

BIG QUAKE, BIKE, QC-MDPC KEM, LEDAkem, LEDApkc, HQC

3. 基于 RQCSD 问题:

LAKE, LOCKER, McNie, RQC, Ouroboros-R, RankSign(已攻破)

6 常用攻击方法

公钥密码的研究一方面是密码方案的构造, 另外一个重要研究方向是对密码方案的密码分析。对基于纠错码的密码体制分析主要分为译码攻击(decoding attack)和结构攻击(structural attack)。首先说明什么是这两种攻击。基于纠错码的密码一般是将一个有高效译码算法的码 C 做线性变换得到一个混乱的码 C', 使得该码与随机码不可区分。

如果能通过 C'得到 C, 这就是结构攻击, 或者也叫密钥恢复攻击, 如果不能, 密码分析人员就面临需要译随机码 C', 这就是译码攻击, 是一种通用攻击。

结构攻击近些年来主要突出的是 Faugère 的工作[35,36], 他的工作主要是利用代数攻击, 构造出代数方程组, 利用 Gröbner 基等工具来解代数方程从而恢复密钥。

由于 C'随机性越来越好, 因而很难通过结构攻击来恢复密钥。而密码体制最通用的译码攻击就是直接求随机线性码的译码问题, 因此译码攻击的主要问题在于提高对随机线性码的译码算法复杂度。另一方面, 随机线性码的译码问题不仅是复杂度理论中的一个基本问题, 也是基于编码的公钥密码、LWE 和 LPN 等的核心问题, 因而译码算法复杂度在密码系统参数的选取上有着重要的地位。解决一般二元线性码的译码问题的经典算法最早是 1962 年 Prange 提出的信息集合译码算法[37], 之后出现了大量的算法都是对这个算法的改进[38-42], 特别是近些年来, Alexander May 等对这个算法做出大改进, 在错误个数小于一半码距的条件下, 在2011年亚密会、2012 年欧密会、2015 年欧密会上将随机线性码的译码算法复杂度由 $O(2^{0.054n})$ 到 $O(2^{0.049n})$ 直至提高到 $O(2^{0.0473n})$[43-45],其中 n 是码长。

最近, 文献[46]给出了在噪音重量 w 与码长 n 为亚线性关系时, 即 $w=o(n)$, 上述几乎各类信息集合译码算法的统一的渐近复杂度有如下结论:

定理 6.1 令码的维数 k 和重量 w 为码长 n 的函数, 且 $\lim_{n\to\infty} k/n=R$, $0<R<1$, $\lim_{n\to\infty} w/n=0$, 则通用的信息集合译码算法的计算复杂度为 $2^{cw(1+o(1))}$, $c=\log_2\frac{1}{1-R}$。

类似地,对秩重量同样有信息集合译码算法,目前最好的秩重量的信息集合译码的结论如下[47]:

对于 $\mathbb{F}_{q^m}$ 上的[n,k]秩码, 目前最好的错误重量为 w 的译码的组合攻击算法计算复杂度为:

$$O((nm)^3 q^{w\left\lceil\frac{m(k+l)}{n}\right\rceil-m})$$

最近, 人们开始越来越重视量子复杂度, 利用 Grover 量子搜索, 得到了汉明重量下的量子信息集合译码算法[48,49]。

另外一个近几年密码分析的比较突出的是侧信道攻击。侧信道攻击是在密码方案在实际设备上实现时会发生信息泄露而发起的攻击, 在基于编码的密码分析中侧信道攻击包括时间攻击(timing attack)、能量攻击(power attack)、差分攻击(differential attack)等。最早的侧信道攻击是发表在 CRYPTO 2008 会议上的对 McEliece 密码体制的侧信道攻击。之后文献[50-53]研究主要关注分析 McEliece 密码体制的时间攻击, 论文文献[54]对 McEliece 密码的软件实现中实施了能量攻击, 最近还有对该体制做差分攻击[55]。

7 数字签名

数字签名是密码理论中的一个重要部分, 很多的签名方案如 DSA、椭圆曲线 DSA 已在实际中应用, 它们的安全性主要依赖于离散对数, 同样不能抵抗量子攻击, 因此设计新的能抵抗量子攻击的签名体制也是一个亟须解决的问题。然而由于 McEliece 加密体制不是可逆的, 因此不能直接用于做签名或认证, 这也是基于编码的签名体制很少的原因。第一个基于编码的数字签名方案是由我国王新梅教授在 1990 年提出的[56], 两年后该方案被 Harn 和 Wang 攻击并修改[57], 但最终于 1992 年被彻底攻破[58], 直到 2001 年由 Courtois、Finiasz 和 Sendrier 才提出了第一个安全性基于编码的签名体制[59], 简称为 CFS。CFS 签名有较高的安全性, 但是其有很大的缺陷, 即签名效率低, 主要原因是对于能纠 t 个错误的话, 签名时间需要 $t!$, 显然随着 t 的增加, 签名时间将会呈指数迅速增长, 而较小的 t 又会带来安全性低的风险, 因此在一定程度上阻碍了 CFS 算法的应用。

基于编码的 NIST 候选算法中有三个签名算法 Ranksign、RaCoss、pqsigRM, 很遗憾的是, 均有有效的攻击算法将其破解。

面对国际上如火如荼的基于编码的后量子密码研究, 我国也非常重视, 已有一些不错的研究[60-62], 然而基于编码的后量子密码研究在国际上还没有很大的国际影响力, 需要更多的科研工作者投入到这方面的研究。

参考文献

[1] P. W. Shor. “Algorithms for quantum computation: Discrete logarithms and factoring.” *In 35th Annual Symposium on Foundations of Computer Science*, pp.124-134, 1994.

[2] EU Post-crypto project. “Initial recommendations of long-term secure post-quantum systems,” 2015.

[3] Dustin Moody. “Post quantum cryptography: NIST's plan for the future,” 2016.

[4] NIST. “Post quantum crypto project.” http://csrc.nist.gov/groups/ST/post-quantum-crypto, 2017. Available at https://csrc.nist.gov/Projects/Post-Quantum-for-Cryptography/Post-Quantum-Cryptography-Standardization/call-for-Proposalls. List of First Round candidates available at https://csrc.nist.gov/projects/post-quantum- cryptography/round-1-submissions.

[5] R. Overbeck and N. Sendrier, “Code-based cryptography,” *Post-Quantum Cryptography*, pp.95-145, Springer Berlin Helberger, 2009.

[6] P.-L. Cayrel, SMEY Alaoui, G. Hoffmann, M. Meziani and R. Niebuhr, “Recent progress in code-based cryptography,” *Information Security and Assurance* (*ISA*), pp.21-32, 201.

[7] D. Engelbert, R. Overneck and A. Schmidt, “A summary of McEliece-type cryptosystems and their security,” *JMC*, 2007 1(2), pp.151-199.

[8] R.J. McEliece. “A public-key cryptosystem based on algebraic coding theory,” *Deep Space Network Progress*, vol. 44, pp.114-116, 1978.

[9] V. M. Sidelnikov and S. O. Shestakov. “On insecurity of cryptosystems based on generalized Reed-Solomon codes.” *Discrete Mathematics and Applications*, pp.439-444, 1992.

[10] G. Landais and J.-P. Tillich. “An effcient attack of a McEliece cryptosystem variant based on convolutional codes,” *PQCRYPT* 2013, pp.102-117.

[11] R. Overbeck. “Structural attacks for public key cryptosystems based on Gabidulin codes,” *Journal of Cryptology* 21, pp.280-301.

[12] V. M. Sidelnikov. “A public-key cryptosystem based on binary Reed-Muller codes,” *Discrete Mathematics and Applications*, pp.191-207, 1994.

[13] H. Niederreiter. “Knapsack-type cryptosystems and algebraic coding theory,” *Problems of Control and Information Theory*, 15(2), pp.159-166, 1986.

[14] Y. X. Li, R. H. Deng and X. M. Wang. “The equivalence of McEliece’s and Niederreiter's public-key cryptosystems,” *IEEE Trans. on Inform. Theory*, vol. 40, pp.271-273,1994.

[15] V. D. Goppa, “A new class of linear error-correcting codes,” *Probl. Peredach. Inform.* 6(3), pp.24-30, 1970.

[16] V. D. Goppa, “Rational representation of codes and (L, g) codes,” *Probl. Peredach. Inform.* 7(3), pp.41-49, 1971.

[17] Berlekamp, E.R., “Algebraic coding theory.” McGraw-Hill (1968).

[18] Massey, J. L., “Shift-register synthesis and BCH decoding.” *IEEE Trans. Inform. Theory* 15, pp.122-127 (1969).

[19] Nicholas J. Patterson, “The algebraic decoding of Goppa codes,” *IEEE Transactionson Information Theory* 21 (1975), pp.203-207.

[20] D. Engelbert, R. Overbeck and A. Schmidt, “Asummary of McEliece-type cryptosystems and their security,” *J. Math. Cryptol*. 1 (2007), no. 2, pp.151-199.

[21] T. Berger, P.-L. Cayrel, P. Gaborit and A. Otmani. “Reducing key length of the McEliece cryptosystem,” *AFRICACRYPT* 2009, LNCS, vol. 5580, pp. 77-97.

[22] R. Misoczki, and P. Barreto. “Compact McEliece keys from Goppa codes,” *SAC* 2009, pp.376-392.

[23] M. Baldi, F. Chilaraluce, R. Garello and F. Mininni. “Low-density parity-check codes in the McEliece cryptosystem,” *ICC* 2007, pp.24-28.

[24] M. Baldi and F. Chiaraluce. “Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes,” *ISIT* 2007, pp.2591-2595.

[25] R. Misoczki, J. P. Tillich, N. Sendrier and P. S. Barreto.“MDPC-McEliece: new McEliece variants from moderate density parity-check codes,” *IEEE International Symposium on Infromation Theory* 2013, pp.2069-2073.

[26] Q. Guo, T. Johanson and P. Stankovski. “A key recovery attack on MDPC with CCA security using decoding errors,” *ASIACRYP*’ 2016,pp. 789-815.

[27] H. Loo-Kengn. “A theorem on matrices over a field and its applications, *Chinese mathematical society*,” Vol. 1, No. 2, pp. 109-163, 1951.

[28] E. M. Gabidulin, A. V. Paramonov and Q. V. Tretjakov. “Ideals over a non-commutative ring and their applications to cryptography,” *EUROCRYPT*’91, pp.8-11,1991.

[29] E. M. Gabidulin. “Theory of codes with maximum rank distance, ”*Probl. Peredachi Inf.* (21), pp.3-16, 1985.

[30] R. Overbeck. “Structural attacks for public key cryptosystems based on Gabidulin codes,” *Journal of Cryptology* 21, pp. 280-301.

[31] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor. “Low rank parity check codes and their application to cryptography.” In Proceedings of the Workshop on *Coding and Cryptography WCC’2013*, Bergen, Norway, 2013.

[32] N. Aragon, P. Gaborit, A. Hautevile, and and J.-P. Tillich. “Improvement of generic attacks on therank syndrome decoding problem.” 2017. Pre-print.available at https://www.unilim.fr/pages-perso/philipe.gaborit/ newGRS.pdf.

[33] E. Berlekamp, R. McEliece and H. Van Tilborg. “On the inherent intractability of certain coding problems,” *IEEE on IT*, vol. 24, No. 3, pp.384-386, 1978.

[34] P. Gaborit and G. Zemor. “On the hardness of the decoding and the minimum distance problem for rank codes,” *IEEE Trans. Information Theory*, 62 (12), pp.7245-7252, 2016.

[35] J.-C. Faugère, A. Otmani, L. Perret and J.-P. Tillich. “Algebraic cryptanalysis of McEliece variants with compact keys,” *EUROCRYPT* 2010, LNCS 6110, pp.279-298, 2010.

[36] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc and J.-P. “Tillich. Structural cryptanalysis of McEliece schemes with compact keys,”*Designs,codes and Cryptography*, 2016,79(1): 87-112.

[37] E. Prange. “The use of information sets in decoding cyclic codes,” *IRE Transactions on Information Theory*, IT-8: S3-S9, 1962.

[38] P. J. Lee and E. F. Brickell. “An observation on the security of McEliece's public-key cryptosystem.” In Advances in Cryptology -

EUROCRYPT 1988, pp.275-280, 1988.

[39] J. S. Leon. “A probabilistic algorithm for computing minimum weights of large error correcting codes.” *IEEE Transactions on Information Theory*, 34(5), pp.1354 -1359, 1988.

[40] J. Stern. “A method for finding codewords of small weight. ”In Proceedings of the 3rd *International Colloquium on Coding Theory and Applications*, pp.106-113, London, UK, 1989. Springer-Verlag.

[41] D. J. Bernstein, T. Lange, and C. Peters. “Smaller decoding exponents: ball-collision decoding.” In *CRYPTO*, volume 6841 of Lecture Notes in Computer Science, pp. 743-760. Springer, 2011.

[42] M. Finiasz and N. Sendrier. “Security bounds for the design of code-based cryptosystems.” In M. Matsui, editor, *Asiacrypt* 2009, LNCS 5912, pp.88-105, 2009.

[43] A. May, A. Meurer and E. Thomae. “Decoding random linear codes in,” *Asiacrypt* 2011, LNCS 7073, Springer, pp.107-124, 2011.

[44] A. Becker,a A. Joux, A. May and A. Meurer. “Decoding random binary linear codes in : How1+1=0 Improves Information Set Decoding, ”*Eurocrypt* 2012, LNCS 7237, Springer, pp.520-536, 2012.

[45] A. May and I. Ozerov. “On computing nearest neighbors with applications to decoding of binary linear codes,” *Eurocrypt* 2015, Springer-Verlag, 2015.

[46] R. C. Torres and N. Sendrier, “Analysis of information set decoding for a sub-linear error weight,” *Post-Quantum Cryptography, PQCrypto* 2016, pp.144-161, 2016.

[47] P. Gaborit, O. Ruatta, and J. Schrek. “On the complexity of the rank syndrome decoding problem.” *IEEE Transactions on Information Theory*, 62(2): pp.1006-1019, 2016.

[48] Bernstein and D.J. “Grovervs McEliece.” In *Post-Quantum Cryptography* 2010 , N. Sendrier, Ed., vol. 6061 of Lecture Notes in Comput. Sci., Springer, pp.73-80, 2010.

[49] G. Kachigar and J.P. Tillich. “Quantum information set decoding algorithms,” International Workshop on *Post-quantum Cryptography* 2017, pp.69-89, 2017.

[50] F. Strenzke, “A Timing attack against the secret permutation in the McEliece PKC,” *PQCrypto* 2010, LNCS 6061, Springer,pp. 95-107, 2010.

[51] A. Shoufan, F. Strenzke, H. G. Molter, and M. Stottinger, “A timing attack against Patterson algorithm in the McEliece PKC,” *ICISC* 2009, LNCS 5984, Springer, pp.161-175, 2010.

[52] R. Avanzi, S. Hoerder, D. Page, and M. Tunstall, “Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems,” *Journal of Cryptographic Engineering* , 1(4), pp.271-281, 2011.

[53] F. Strenzke, “Timing Attacks against the syndrome inversion in code-based cryptosystems,” *PQCrypto* 2013, LNCS 7932, Springer, pp. 217-230, 2013.

[54] S. Heyse, A. Moradi, and C. Paar, “Practical power analysis attacks on software implementations of McEliece,” *PQCrypto* 2010, LNCS 6061, Springer, pp.108-125, 2010.

[55] C. Chen, T. Eisenbarth, I. von Maurich and R. Steinwandt, “Differential power analysis of a McEliece cryptosystem,” *Cryptology* ePrint Archive, Report 2014/534, 2014.

[56] X. Wang. “Digital signature scheme based on error-correcting codes,” *Electronics Letters* 26, pp.898–899, 1990.

[57] L. Harn and D.-C. Wang. “Cryptanalysis and modification of digital signature scheme based on error-correcting codes,” *Electronics Letters*, 28 (2), pp.157-159, 1992.

[58] M. Alabbadi and S. B. Wicker. “Security of Xinmei digital signature scheme,” *Electronic Letters*, 29 (9), pp.890-891, 1992.

[59] N. Courtois, M. Finiasz and N. Sendrier. “How to achieve a McEliece-based digital signature scheme,” In advances in Cryptology-*ASIACRYPT* 2001, pp.157-174, 2001.

[60] K. Chen. “A new identification algorithm in cryptography,” *Policy and Algorithms*, pp.244-249 (1985).

[61] Y. Li and C. Liang. “A digital signature scheme constructed with error-correcting codes,” *Chinese: Acta Electronica Sinica* 19, pp.102-104, 1991.

[62] Y.L.Han,J.J.Lan and X.Y.Yang.“The cipher scheme based on LRPC code and multiple variables,” *Journal of Cryptologic Research*, vol.3, no.1, pp.55-56, 2016.
(韩益亮, 蓝锦佳, 杨晓元. 基于 LRPC 码和多变量的签密方案, *密码学报*, 2016, 3(1), 56-66.)

[63] R.Fang and D.Zheng,“An improved digital signature algorithm based on coding,” *Journal of Xi’an University of Posts and Telecommunications*, vol.20, 2015.
(任方, 郑东: 一种基于编码的数字签名算法的改进, *西安邮电大学学报*,卷 20, 2015.)

王丽萍 于 2003 年在中国科学技术大学应用数学专业获得博士学位。现任中国科学院信息工程研究所, 信息安全国家重点实验室研究员。研究领域为密码和编码等。研究兴趣包括: 后量子公钥密码、代数译码算法、序列等。Email: wangliping@iie.ac.cn

戚艳红 于 2017 年在河北大学网络工程专业获得学士学位。现在中国科学院大学网络空间安全专业攻读硕士学位。研究领域为后量子公钥密码。研究兴趣包括: 数字签名。Email: qiyanhong@iie.ac.cn