doi:10.11887/j.cn.202004020　　http://journal.nudt.edu.cn

基于编码的加密体制综述*

李　喆,韩益亮,李　鱼,朱率率,杨晓元
(武警工程大学 密码工程学院,陕西 西安　710086)

摘　要:量子算法的提出,使得传统的密码体制在量子计算下不再安全。基于编码的加密方案具有抗量子攻击特性,引起密码学界广泛关注。许多密码学者对基于编码的加密方案进行深入研究,在研究过程中,人们对其加密方案的优势和缺点逐渐有了深刻的认识。目前,基于编码的密码体制已成为后量子密码学最有前途的方案之一。综述了基于编码加密体制的发展现状,阐述了现有基于编码的加密体制和目前已知存在的攻击,并指明了未来具有潜力的发展方向。

关键词:编码;后量子密码;加密体制;密码分析
中图分类号:TN309.7　　**文献标志码**:A　　**文章编号**:1001-2486(2020)04-134-09

An overview of code-based encryption schemes

LI Zhe, *HAN Yiliang*, *LI Yu*, *ZHU Shuaishuai*, *YANG Xiaoyuan*
(College of Cryptographic Engineering, Engineering University of PAP, Xi'an 710086, China)

Abstract: The quantum algorithm which was put forward recently has led to great insecurity of cryptographic analysis of the coding under quantum computing. The future of the code-based cryptography with anti-quantum attack properties was questioned by many people. However, in the research process, people gradually had a deep understanding of the advantages and disadvantages of its encryption scheme. At present, the code-based cryptography has become one of the most promising post-quantum cryptography schemes. The code-based encryption schemes were summarized and the existing attacks of their original schemes were analyzed. Finally, the nature of the security problem of encoding-based encryption system is analyzed, and the future development direction is expounded.

Keywords: coding; post-quantum cryptography; encryption scheme; cryptanalysis

2019 年 10 月 26 日,第十三届全国人大常委会第十四次会议通过了《中华人民共和国密码法》,通过制度的形式把信息安全的重要性上升为国家意志。现在社会中的银行交易、无人驾驶、卫星通信、指挥控制等方面,密码学具有不可替代的作用。随着科学技术的飞速发展,量子计算机逐渐进入人们的视野,其强大的计算能力备受青睐,量子计算机强大的计算能力在诸多方面带来了极大的便利,但是其强大的计算能力也对经典计算机(图灵机)条件下基于数论的密码体制带来了严重的威胁。目前,大部分密码体制都依赖于经典计算机在多项式时间内无法有效解决的两个计算困难问题,即大整数分解和离散对数问题。Shor[1]提出了可以在多项式时间内破解大整数问题和离散对数问题的量子算法,这一算法使得经典的公钥密码方案极不安全,RSA[2]、离散椭圆曲线方案(Elliptic Curve Cryptography, ECC)[3]等密码体制的安全性受到挑战。因此,为了应对量子计算机带来的挑战,许多密码学者尝试构造可以抵御量子计算的新型密码体制,即抗量子计算密码体制(Post-Quantum Cryptography, PQC)。PQC 主要有五种[4]:基于编码的公钥密码体制、基于格的公钥密码体制、基于哈希树的公钥密码体制、基于多变量的公钥密码体制、超奇异椭圆曲线同源密码。

2015 年,美国和欧盟分别推动抗量子密码的标准化进程[5]。2018 年,美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)面向全球征集抗量子密码,举办第一轮 PQC 算法征集会议,基于编码的密码体制占有很大的比例[6]。2019 年,NIST 评选第二轮后量子密码算法,基于编码的密码方案依然具有很大的

* **收稿日期**:2019-12-16
基金项目:国家自然科学基金资助项目(61572521,U1636114);国家重点研发计划资助项目(2017YFB0802000)
作者简介:李喆(1994—),男,安徽宿州人,硕士研究生,E-mail:18091791659@163.com;
韩益亮(通信作者),男,教授,博士,博士生导师,E-mail:hanyil@163.com

比重[7]。在未来的研究过程中,基于编码的密码体制依然是研究的热点。

为了使我国后量子密码算法同步推进,国家密码局于 2018 年面向全国征求密码算法,目前,全国密码算法设计竞赛第一轮算法评选结果已经揭晓,第二轮算法评选正在进行中,预计于 2022 年左右开展抗量子密码算法标准化工作。

基于编码的密码体制最初是由 McEliece[8] 提出的,其一般性译码问题属于一般线性码的非确定性多项式完全问题。到目前为止,原始的方案依然具有安全性。该体制采用 Goppa 码,具有加解密速度快、计算复杂度低的优点。但现实中没有大量使用该体制的原因是,其密钥储存空间太大、码率低。Niederreiter[9] 提出了基于 GRS 码的 Niederreiter 密码体制,相较于 McEliece 体制,该体制密钥存储空间减少,但仍然不能投入到实际使用中。因此,许多学者为了减小密钥的尺寸,推动提高密码方案的实用化,改进 McEliece 体制,提出了用其他结构更加紧凑的编码代替 Goppa 码,例如准循环低密度奇偶校验码(Quasi-Cyclic Low-Density Parity Check, QC-LDPC)码[10]、Polar 码[11]、中密度奇偶校验码(Medium Density Parity Check, MDPC)码[12]、Gabidulin 码[13]、低秩奇偶校验(Low Rank Parity Check, LRPC)码[14],改进的密码方案减少了密钥长度,但容易受到攻击[15]。

后来,基于编码的方案进一步发展,一些学者对 McEliece 体制的结构进行变型。Wang[16] 在生成矩阵的每一列中都嵌入了随机列并构造了一种线性随机码的加密方案 RLCE。Kim 等[17] 通过将 McEliece 和 Niederreiter 相结合,利用秩度量的编码构造了 McNie 密码方案。刘相信等[18] 通过隐藏明文的汉明重量,将校验矩阵拆分构造了一种新型密码方案。Mostafa[19] 通过利用错误向量的汉明重量大于编码最小距离的性质,构造了一种不同的密码方案。

本文根据编码的性质,总结了基于汉明度量编码和基于秩度量的加密方案,归纳了目前发展的现状,展望了未来的发展方向。介绍了目前基于 McEliece 方案进行结构改变的新型密码方案,为将来研究抗量子密码方案提供了新的方向。综述了目前对基于编码的密码方案主流的攻击方法。

1　基于纠错码的密码体制

1.1　McEliece 加密体制

该密码体制包括密钥生成(公钥、私钥)、加密过程、解密过程三部分。

1)密钥生成过程如下:

①随机生成长度为 n,维度为 k 的 $k\times n$ 阶生成矩阵 $\boldsymbol{G}$,其中最小距离 $d\geqslant 2t+1$;

②生成 $k\times k$ 阶随机非奇异可逆矩阵 $\boldsymbol{S}$;

③生成 $n\times n$ 阶二元随机置换矩阵 $\boldsymbol{P}$。

$\boldsymbol{G}$ 左乘随机非奇异可逆矩阵 $\boldsymbol{S}$,右乘随机置换矩阵 $\boldsymbol{P}$,得到扰乱后的 $k\times n$ 阶矩阵 $\boldsymbol{G}^{\text{pub}}$,$\boldsymbol{G}^{\text{pub}}=\boldsymbol{SGP}$。其中,公钥为 $\boldsymbol{G}^{\text{pub}}$ 和 t;私钥为 $\boldsymbol{S}$、D_C、$\boldsymbol{P}$,D_C 是编码 C 的译码算法。

2)加密过程如下:

①随机选择错误向量 $\boldsymbol{e}\in F^n$,其中,F^n 为有限域上的 n 维线性向量空间,$wt(\boldsymbol{e})\leqslant t$;

②发送方利用接收方的公钥 $\boldsymbol{G}^{\text{pub}}$对发送的消息 m 进行加密,得到密文 $\boldsymbol{c}$。$\boldsymbol{c}=m\boldsymbol{G}^{\text{pub}}\oplus\boldsymbol{e}$,其中 $m\in F^k$。

3)解密过程如下:

①接收方收到密文 $\boldsymbol{c}$,利用自己的私钥对密文进行解密;

②$\boldsymbol{cP}^{-1}=(m\boldsymbol{S})\boldsymbol{G}\oplus\boldsymbol{eP}^{-1}$。

利用编码的译码算法进行译码,$m\boldsymbol{S}=D_C(\boldsymbol{cP}^{-1})$,$m_1=m\boldsymbol{S}$,$m=m_1\boldsymbol{S}^{-1}$。

目前,这一方案的研究目标和发展方向主要有以下三类:

1)采用 Goppa 码的原始方案,到目前为止都足够安全,下一步的关注点是,在保证安全性的基础上,分析目前存在的攻击类型,合理选用参数,对 Goppa 码进行变型,如交织 Goppa 码;

2)进一步分析原始方案存在的攻击,尤其是要关注侧信道攻击,在模拟仿真平台上实现密码方案,通过侧信道攻击检验方案的安全性;

3)分析 McEliece 密码体制延展性以及消息重放攻击,进一步研究方案保证其安全性。

1.2　Niederreiter 密码体制

Niederreiter 采用 McEliece 的对偶形式提出了 Niederreiter 体制,与 McEliece 公钥密码体制不同的是,Niederreiter 密码体制采用一致校验矩阵来构造加密算法。同样地,该密码体制包括密钥生成(公钥、私钥)、加密过程、解密过程三部分。

1)密钥生成过程如下:

①系统参数:$n,t\in\mathbb{N}$。

②生成 $\boldsymbol{M}$:$(n-k)\times(n-k)$ 阶可逆矩阵。

③生成 $\boldsymbol{H}$:纠正 t 个错误的编码 C 的 $(n-k)\times n$ 阶校验矩阵。

④生成 $\boldsymbol{P}$:$n\times n$ 阶随机置换矩阵。

⑤计算 $\boldsymbol{H}^{\text{pub}} = \boldsymbol{MHP}$。

2)加密过程如下:

计算 $s = \boldsymbol{H}^{\text{pub}}\boldsymbol{e}^{\text{T}}$,其中,$\boldsymbol{e} \in \{0,1\}^n$。

3)解密过程如下:

计算 $\boldsymbol{M}^{-1}s = \boldsymbol{HPe}^{\text{T}}$,利用伴随式译码算法恢复 $\boldsymbol{Pe}^{\text{T}}$,计算 $\boldsymbol{e}^{\text{T}} = \boldsymbol{P}^{-1}\boldsymbol{Pe}^{\text{T}}$。

McEliece 体制的公钥为 $k \times n$ bit,Niederreiter 公钥体制的公钥为 $(n-k) \times n$ bit,采用这种对偶变型的密码方案,可以有效减小密钥长度。在 McEliece 体制中,攻击者可以通过两个被加密消息之间的关系来确定错误位置。而 Niederreiter 公钥体制并不存在延展性,所以不会遭到密文的延展性攻击和消息重放攻击。

目前,这一方案的研究目标和发展方向主要有以下两类:

1)研究重点逐渐聚焦在采用 Niederreiter 密码体制进行签名方案的构造;

2)研究改进 Niederreiter 密码体制在硬件上面的实现,提高效率和实用性。

1.3 研究现状

目前关于 McEliece 密码体制的研究大概分为两类:

1)研究改进 McEliece 原始方案的结构分析其原始方案的底层编码,选择性能更优的码字来替代原始方案的 Goppa 码,达到减小密钥长度的目的,使其投入到实际运用中;

2)研究分析 McEliece 原始方案及其变型的安全性,分析其存在安全性问题的原因,进一步完善密码方案。

2 采用其他编码改进的 McEliece 体制

2.1 基于汉明度量编码的密码方案

2.1.1 基于 LDPC/MDPC 码的密码方案

采用 LDPC 码或 MDPC 码代替原来的 Goppa 码,LDPC 码或 MDPC 码具有有效的迭代译码算法,可以明显降低译码错误率,并且采用其循环结构可以有效减小公钥尺寸。MDPC 码奇偶校验矩阵的行列密度比 LDPC 码高。

Monico 等[20]提出用 LDPC 码代替原来的 Goppa 码。Baldi 等[10]提出基于 QC-LDPC 码的 McEliece 体制,该体制可以减小密钥大小,具有一定的安全性,采用比特迭代译码算法可以快速解码。但其对偶码存在低维数的漏洞,易被攻破。Baldi 等[21]提出改进的 QC-LDPC 变型,其中可逆矩阵和置换矩阵都采用稀疏矩阵,提高了安全性,可以抵抗结构化攻击。Shooshtari 等[22]指出,Baldi 改进后的方案容易受到信息集译码攻击(Information Set Decoding, ISD),原因是改进后的 QC-LDPC 方案中,会出现循环矩阵的循环块为偶数的情况。

Misoczki 等[23]提出基于 QC-MDPC 码的 McEliece 体制来抵御已知的对 LDPC 码的攻击,同时减小了密钥量。Guo 等[24]通过研究译码错误率与密钥距离谱之间的联系,对文献[23]提出的 QC-MDPC 方案进行了密钥恢复攻击。Fabšič 等[25]同样通过大量实验寻找置换矩阵 $\boldsymbol{Q}$ 与译码错误率之间的关联性,对密钥进行恢复攻击。

Moufek 等[26]提出一种新的思路,将两种奇偶校验码结合使用。该方案通过 QC-LDPC 码和 QC-MDPC 码的级联使用,可以减少密钥长度,采用伪随机生成矩阵具有一定的安全性。Dragoi 等[27]对文献[26]改进的方案进行安全性分析,发现文献[26]改进的方案存在极大的漏洞。

目前,这一方案的研究目标和发展方向主要有以下两类:

1)研究 QC-LDPC 码和 QC-MDPC 码的性质,进一步改进方案的译码算法,减小译码错误率,提高译码效率;

2)分析采用 QC-LDPC 码和 QC-MDPC 码密码方案的结构,研究低重量搜索攻击对其密码方案的影响,并对其安全性做进一步分析。

2.1.2 基于 Polar 码的密码方案

Polar 码是目前可以在理论上证明趋于 Shannon 限的编码。Arikan 提出 Polar 码[28],并深入研究 Polar 码的性质,后来众多学者进一步研究了 Polar 码的结构及性能。

首先,Polar 码比 Goppa 码等其他编码纠错能力更强;其次,极化码的连续消除译码算法比 Goppa 码的译码效率更高,降低了解密过程中的计算复杂度。通过研究极性码的性质,Mahdlavifar 等尝试把极化码应用到密码学中,并取得了一定的进展[29]。Hooshmand 等[30]利用极化码的性质构造对称密码体制。Hooshmand 等[31]为了避免主动攻击和被动攻击,通过分析有限长度极化码的性质,提出了基于物理层加密(Physical Layer Encryption, PLE)方案[32],在合法的通信双方建立安全可靠的保密通信。

Shrestha 等[33]将 Polar 码应用到编码密码中,提出了基于 Polar 码的 McEliece 密码方案。Hooshmand 等[34]在原有方案的基础上,优化了基于 Polar 码的 McEliece 密码方案,减少了密钥存

储空间。但是,Bardet 等[35]分析了文献[34]中提出的基于 Polar 码的 McEliece 密码方案的结构,提出了密钥恢复攻击的方法。这种攻击方法可以获得文献[33]方案解密密文所需要的任何信息。杨超等[36]利用 Polar 码译码算法的低复杂性构造 Niederreiter 公钥密码体制,并进行了仿真分析。Drăgoi 等[37]证明任何基于弱递减单项式码的密码方案都有可能受到密钥恢复攻击,基于 Polar 码的密码方案也不例外。

目前,这一方案的研究目标和发展方向主要有四类:

1)进一步研究 Polar 码,研究其极化现象的原因,提高中等长度码字的编码效率;

2)进一步研究其译码算法,分析连续消除算法,列表连续删除译码算法,加入循环冗余检验位的列表连续删除算法的性能,在提高译码正确率的同时提高译码效率;

3)把 Polar 码的极化性质应用到签名领域,把极化性质与签名有效结合,提高签名的效率;

4)通过把 Polar 码与其他性能好的码字相级联,克服了 Polar 码在中等长度时性能差的缺点,总体上使密码方案的效率与安全性达到最佳。

2.1.3　基于 RS 码/GRS 码的密码方案

该体制采用 RS 码或 GRS 码代替 McEliece 原始方案中的 Goppa 码。GRS 码存在有效译码算法,可以有效减少公钥长度。

基于 GRS 码的 Niederreiter 体制变型被 Silelnikov 等完全攻破,当公钥 $\boldsymbol{H}^{\text{pub}}$ 的列元素可以表示为支撑元素的多项式,利用各列元素的关系可求出支撑向量和常数向量[38]。Wieschebrink[39]提出用 GRS 码与随机码并列的级联码避免了文献[38]中提到的攻击。Couvreur 等[40]针对三种 GRS 变型,采用 GRS 码的平方码构造与随机码相区分的区分器,进而采用密钥恢复攻击,能够在多项式时间内攻破文献[39]所采用的级联码方案。

Márquez-Corbella 等[41]提出用两个 GRS 码构造"$u/u+v$"的变型。目前,这一方案的研究目标和发展方向主要有两类。

1)进一步研究文献[38]针对基于 GRS 码的密码体制提出的攻击方法,分析这种攻击是否会对 McEliece 体制原始方案的安全性造成影响;

2)进一步研究采用 GRS 码的 Niederreiter 体制,利用 Niederreiter 体制可以抵抗反应攻击和延展性攻击的优点,深究其本质,设计可以达到原始方案的新型密码体制。

2.2　基于秩度量编码

基于汉明度量的 McEliece 密码,使用 Goppa 码或 MDPC 码,其缺点是有相对较大的密钥。原始基于编码的密码方案是基于具有汉明度量的 Goppa 码,实际上可以考虑基于秩度量的编码。秩度量的特别之处在于译码问题的实际难度随着参数的增大而迅速增大。在同样安全级别下,基于秩度量的密码方案比基于汉明度量的密码方案更安全。与基于汉明度量的编码相比,秩度量中已知的具有高效译码算法的码族很少。可以用于 McEliece 方案的两大类秩度量编码,即 Gabidulin 码和 LRPC 码。基于 LRPC 码的密码方案,因其低代数结构,逐渐成为研究的热点。

Kshevetskiy 等对基于 Gabidulin 码的原始方案进一步优化参数,在保证安全性的同时进一步减少密钥尺寸[42]。Overbeck[43]针对基于秩度量编码的原始方案及其变型进行分析,提出一种有效的攻击方法。该攻击主要是对基于秩度量码的密码方案进行分析,发现 Gabidulin 码包含一个巨大的向量空间不变作用下的弗罗贝尼乌斯自同构。后来,许多学者试图用其他扰乱矩阵来避免存在的已知其他攻击,但是 Gabidulin 代码自身存在的问题仍没有消失[44]。换句话说,对编码进行扰乱的生成器的一些核心部分仍然存在向量空间不变的问题,这就增加了系统的弱点。

为了抵御文献[43]提及的攻击,Loidreau[45]对维度等参数进行优化,提出一种基于新型秩度量的编码体制。Coggia 等[46]对文献[45]提出的密码方案进行安全性分析,指出当 $\lambda=2$ 时,攻击者有超过 50% 的可能性用区分器把公共代码和随机码区分开,利用这个区分器可以在多项式时间内实现密钥恢复攻击。Aragon 等[47]提出一种新的译码算法,该方法可以降低以往方案的译码错误概率。Aragon 等[48]利用 LRPC 码在选择明文攻击下的不可区分性(INDistinguishability-Chosen ciPhertext Attacks, IND-CPA)情况解密失败条件下,采用一种代数方法对解密失败发生的情况进行建模,然后根据攻击者可以利用 IND-CPA 方案中发送给解密 oracle 的错误这一事实,对比文献[24]中提出的对 QC-MDPC 码密钥恢复攻击,Aragon 等尝试把这种攻击应用到基于秩度量的密码方案。

与汉明度量相比,秩度量的优势比较明显,在一定的参数选择范围下,通过搜索低重量攻击的复杂度会明显提升。

目前,这一方案的研究目标和发展方向主要

有以下两类：

1）分析研究 LRPC 码的结构，改进译码算法以减小 LRPC 码的译码错误率；

2）寻找隐藏 Gabidulin 码结构的方法，使其能够抵抗文献[43]提及的攻击。

3 McEliece 加密方案结构的变型

3.1 McNie 方案

Kim 等[17]提出将 McEliece 方案和 Niederreiter 方案结合的 McNie 加密方案，该方案采用4－循环低秩奇偶校验码，能够抵抗目前已知的结构化攻击，减小了密钥的大小。Lau 等[49]针对 McNie 方案提出了一种密钥恢复攻击，能够恢复 McNie 方案所有参数下的密钥，进而提出了一种新的基于 Gabidulin 码的 McNie 方案，该新方案不存在译码失败率。Aragon 等[48]对 McNie 方案采用消息恢复攻击和改进的信息集译码攻击，使 McNie 方案的安全级别减半。Kim 等[50]在文献[49]改进的基础上，进一步提出了 McNie2-Gabidulin 方案，该方案具有 IND-CPA 安全性，密钥尺寸小于其他没有译码失败概率的密码方案。

1）密钥生成过程如下：

①对于给定的参数 n 和 r，产生下列矩阵：

$\boldsymbol{G}'$：域 F_{q^m} 上的信息数为 k、最小距离 $l>n-k$ 码 C 的 $k\times n$ 阶生成矩阵。

$\boldsymbol{S}$：$(n-k)\times(n-k)$ 阶可逆矩阵。

$\boldsymbol{H}$：一个能够纠正 r 个错误的码 C 的 $(n-k)\times n$ 阶校验矩阵。

$\boldsymbol{P}$：$n\times n$ 阶随机置换矩阵。

②计算矩阵 $\boldsymbol{F}=\boldsymbol{G}'\boldsymbol{P}^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{S}$。

公钥：$(\boldsymbol{G}',\boldsymbol{F})$。

私钥：$(\boldsymbol{S},\boldsymbol{H},\boldsymbol{P})$。

2）加密过程如下：秩度量为 r 的向量 $\boldsymbol{e}\in F_{q^m}^n$，计算

$$\boldsymbol{c}_1=m\boldsymbol{G}'+\boldsymbol{e} \tag{1}$$

$$\boldsymbol{c}_2=m\boldsymbol{F} \tag{2}$$

3）解密过程如下：

$$\boldsymbol{S}'=\boldsymbol{c}_1\boldsymbol{P}^{-1}\boldsymbol{H}^{\mathrm{T}}-\boldsymbol{c}_2\boldsymbol{S}^{-1}=\boldsymbol{e}\boldsymbol{P}^{-1}\boldsymbol{H}^{\mathrm{T}} \tag{3}$$

接收者利用译码算法

$$\varphi_{H(S')}=\boldsymbol{e}\boldsymbol{P}^{-1} \tag{4}$$

$$\boldsymbol{c}_1-\boldsymbol{e}=m\boldsymbol{G}' \tag{5}$$

得到 m。

把 McNie 体制和 McEliece 类比，则

$$\boldsymbol{G}'=\boldsymbol{SGPF}=\boldsymbol{G}'\boldsymbol{P}^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{S}=(\boldsymbol{SGP})\boldsymbol{P}^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{S} \tag{6}$$

因为 $\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{0}$，所以 $\boldsymbol{F}=\boldsymbol{0}$，推出 $\boldsymbol{c}_2=\boldsymbol{0}$，$\boldsymbol{c}_1=m\boldsymbol{G}'+\boldsymbol{e}$，这就是 McEliece 体制的原始方案。

目前，这一方案的研究目标和发展方向主要有以下两类：

1）分析研究 McNie 方案，找到 McNie 方案没有入围第二轮抗量子候选方案的原因；

2）寻找隐藏 Gabidulin 码结构的方法，使其能够抵抗文献[43]提及的攻击。

3.2 改进版 Niederreiter 密码方案

刘相信等[18]对错误向量 $\boldsymbol{e}$ 的重量进行了隐藏，提出的 Niederreiter 密码方案改进版可以抵抗 ISD 攻击。

1）密钥生成过程如下：

①选择二元 (n,k,t) Goppa 码，纠错能力为 t，校验矩阵为 $(n-k)\times n$，快速译码算法为 $\beta_{\boldsymbol{H}t}$。

②将 $\boldsymbol{H}$ 随机拆分成两个矩阵 $\boldsymbol{H}_1$、$\boldsymbol{H}_2$（$\boldsymbol{H}=\boldsymbol{H}_1+\boldsymbol{H}_2$），随机选取三个阶数为 $(n-k)\times(n-k)$ 可逆矩阵 $\boldsymbol{S}_1$、$\boldsymbol{S}_2$、$\boldsymbol{S}_3$，选取一个 $n\times n$ 阶的可逆置换矩阵 $\boldsymbol{P}$，分别计算 $\boldsymbol{H}'=\boldsymbol{S}_1\boldsymbol{H}_1\boldsymbol{P}$，$\boldsymbol{H}''=\boldsymbol{S}_2\boldsymbol{H}_2\boldsymbol{P}$，$\boldsymbol{H}'''=\boldsymbol{S}_3\boldsymbol{H}\boldsymbol{P}$。

③公钥：$(\boldsymbol{H}',\boldsymbol{H}'',\boldsymbol{H}''',t)$。

④私钥：$(\boldsymbol{S}_1,\boldsymbol{S}_2,\boldsymbol{S}_3,T,\beta_{\boldsymbol{H}t})$。

2）加密过程如下：

将明文 m 编码成汉明重量 t 的向量 $\boldsymbol{e}$，并将 $\boldsymbol{e}$ 拆分为两个向量 $\boldsymbol{e}_1$、$\boldsymbol{e}_2$，且 $\boldsymbol{e}=\boldsymbol{e}_1+\boldsymbol{e}_2$，$wt(\boldsymbol{e}_1)=t_1$，$wt(\boldsymbol{e}_2)=t_2(t\neq t_1\neq t_2)$。计算

$$\begin{cases}\boldsymbol{c}_1=\boldsymbol{e}_1\boldsymbol{H}'^{\mathrm{T}}\\ \boldsymbol{c}_2=\boldsymbol{e}_1\boldsymbol{H}''^{\mathrm{T}}\\ \boldsymbol{c}_3=\boldsymbol{e}_2\boldsymbol{H}'''^{\mathrm{T}}\end{cases} \tag{7}$$

将 $(\boldsymbol{c}_1,\boldsymbol{c}_2,\boldsymbol{c}_3)$ 发送给接收方。

3）解密过程：收到 $(\boldsymbol{c}_1,\boldsymbol{c}_2,\boldsymbol{c}_3)$ 后，计算

$$\boldsymbol{c}_1(\boldsymbol{S}_1^{-1})^{\mathrm{T}}=\boldsymbol{e}_1\boldsymbol{H}'^{\mathrm{T}}(\boldsymbol{S}_1^{-1})^{\mathrm{T}}=\boldsymbol{e}_1\boldsymbol{P}^{\mathrm{T}}\boldsymbol{H}_1^{\mathrm{T}} \tag{8}$$

$$\boldsymbol{c}_2(\boldsymbol{S}_2^{-1})^{\mathrm{T}}=\boldsymbol{e}_1\boldsymbol{H}''^{\mathrm{T}}(\boldsymbol{S}_2^{-1})^{\mathrm{T}}=\boldsymbol{e}_1\boldsymbol{P}^{\mathrm{T}}\boldsymbol{H}_2^{\mathrm{T}} \tag{9}$$

$$\boldsymbol{c}_3(\boldsymbol{S}_3^{-1})^{\mathrm{T}}=\boldsymbol{e}_2\boldsymbol{H}'''^{\mathrm{T}}(\boldsymbol{S}_3^{-1})^{\mathrm{T}}=\boldsymbol{e}_2\boldsymbol{P}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}} \tag{10}$$

因为 $\boldsymbol{H}=\boldsymbol{H}_1+\boldsymbol{H}_2$，$\boldsymbol{e}=\boldsymbol{e}_1+\boldsymbol{e}_2$。所以

$$\boldsymbol{c}_1(\boldsymbol{S}_1^{-1})^{\mathrm{T}}+\boldsymbol{c}_2(\boldsymbol{S}_2^{-1})^{\mathrm{T}}+\boldsymbol{c}_3(\boldsymbol{S}_3^{-1})^{\mathrm{T}}=\boldsymbol{e}\boldsymbol{P}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}} \tag{11}$$

利用译码算法 $\beta_{\boldsymbol{H}t}$ 进行译码可得 $\boldsymbol{e}\boldsymbol{P}^{\mathrm{T}}$，再利用私钥 $\boldsymbol{P}$，即可得到密文 $\boldsymbol{e}=\boldsymbol{e}\boldsymbol{P}^{\mathrm{T}}(\boldsymbol{P}^{\mathrm{T}})^{-1}$。

目前，这一方案的研究目标和发展方向主要有两类：

1）研究本方案的安全性，隐藏后的错误向量是否可以保证密码方案的安全；

2）选择其他编码进一步减少密钥长度，例如 LRPC 码。

3.3　改进错误向量的密码方案

Mostafa[19] 在其博士论文中提出 Mostafa Esmaeili 方案,该方案在 McEliece 加密的基础上,改变了 McEliece 的结构,不再利用可逆矩阵和置换矩阵对生成的矩阵进行扰乱,主要利用汉明重量大于编码最小距离的错误向量,构造了新型的密码方案。该密码方案与 McEliece 方案构造过程类似,包括密钥生成(公钥、私钥)、加密过程、解密过程三部分。

1)密钥生成过程如下:

①$\boldsymbol{G}$:域 $\boldsymbol{F}$ 上的维度为 k、最小距离 $d \geqslant 2t+1$ 的码 C 的 $k \times n$ 阶生成矩阵。

②$\boldsymbol{H}$:域 $\boldsymbol{F}$ 上的 $(n-k) \times n$ 阶的校验矩阵。

③$\boldsymbol{S}$:$(n-k) \times (n-k)$ 随机非奇异可逆矩阵。

④公钥:$(\boldsymbol{G}, \boldsymbol{S}(\boldsymbol{H}^{-1})^{\mathrm{T}})$。

⑤私钥:$\boldsymbol{H}^{\mathrm{T}}\boldsymbol{S}^{-1}$。

2)加密过程如下:

发送者选择长度为 l_1 的消息 m,随机选择长度为 l_2 的随机比特串 r(其中 $l = l_1 + l_2$),将随机比特串 r 与明文 m 并联,得到 $[r|m]$。随机选择 $n-k$ 位的向量 $\boldsymbol{s}$,计算 $\boldsymbol{sS}(\boldsymbol{H}^{-1})^{\mathrm{T}}$,假如 $wt(\boldsymbol{sS}(\boldsymbol{H}^{-1})^{\mathrm{T}}) < d$,重新选择向量 $\boldsymbol{s}$。

发送者使用接收者的公钥对并联后的消息进行加密,得到

$$\boldsymbol{c} = [r|m]\boldsymbol{G} + \boldsymbol{sS}(\boldsymbol{H}^{-1})^{\mathrm{T}} \tag{12}$$

3)解密过程如下:

接收者收到密文 $\boldsymbol{c}$ 后,使用自己的私钥对密文进行解密。

$$\boldsymbol{cH}^{\mathrm{T}}\boldsymbol{S}^{-1} = ([r|m]\boldsymbol{G} + \boldsymbol{sS}(\boldsymbol{H}^{-1})^{\mathrm{T}})\boldsymbol{H}^{\mathrm{T}}\boldsymbol{S}^{-1} = \boldsymbol{s} \tag{13}$$

接收者通过自己的私钥对密文进行解密得到 $\boldsymbol{s}$,然后用向量 $\boldsymbol{s}$ 乘以公钥 $\boldsymbol{S}(\boldsymbol{H}^{-1})^{\mathrm{T}}$,得到 $\boldsymbol{sS}(\boldsymbol{H}^{-1})^{\mathrm{T}}$,然后计算

$$[r|m]\boldsymbol{G} = \boldsymbol{c} + \boldsymbol{sS}(\boldsymbol{H}^{-1})^{\mathrm{T}} \tag{14}$$

利用译码算法对 $[r|m]\boldsymbol{G}$ 进行解密,得到 $[r|m]$,把长度为 l_2 的随机比特串 r 丢弃,最后得到明文 m。

目前,这一方案的研究目标和发展方向主要有三类:

1)研究编码的性质,寻找适合构造本方案的编码;

2)研究本密码方案是否可以抵御其他类型的攻击;

3)利用本方案中汉明重量大于编码最小距离的错误向量这种新的思想,尝试把这种新的思想应用于签名、密钥交换、密钥封装等密码学原语中。

4　安全性分析

对基于编码密码体制的攻击,主要有密钥恢复攻击[51]和信息集译码攻击[52]等。

1)密钥恢复攻击。原始 McEliece 体制采用的是 Goppa 码,具有一些随机码的特征。$\boldsymbol{G}^{\mathrm{pub}} = \boldsymbol{SGP}$,攻击者只有找到扰乱矩阵 $\boldsymbol{S}$、置换矩阵 $\boldsymbol{P}$,才有可能恢复出生成矩阵 $\boldsymbol{G}$,最后才能通过 Goppa 码的快速译码算法解码密文。假如攻击者找不到扰乱矩阵 $\boldsymbol{S}$、置换矩阵 $\boldsymbol{P}$,无法恢复出生成矩阵 $\boldsymbol{G}$,也就无法达到破译密文的目的。事实上,可逆矩阵 $\boldsymbol{S}$、置换矩阵 $\boldsymbol{P}$ 的码族非常大,通过找到可逆矩阵 $\boldsymbol{S}$、置换矩阵 $\boldsymbol{P}$ 这种方法来恢复生成矩阵 $\boldsymbol{G}$ 在理论上是不可行的。

2)信息集译码攻击。目前对 McEliece 体制最有效的方法是解方程组 $m = (m_1, m_2, \cdots m_k)$,方程 $c_{1\times n} = m_{1\times k}\boldsymbol{S}_{k\times k}\boldsymbol{G}_{k\times n} \cdot \boldsymbol{P}_{n\times n} \oplus \boldsymbol{e}$,假如 $\boldsymbol{e}$ 为零矢量,则可以通过复杂度 $O(k^3)$ 的快速译码算法,在已知 $\boldsymbol{c}$、$\boldsymbol{G}^{\mathrm{pub}}$ 的情况下,可求解 m。若假定 $\boldsymbol{e}$ 的 t 个非零元素在 n bit 中均匀分布,则随机在 $\boldsymbol{e}$ 中选择 k 个元素,恰好为零的概率是 C_{n-t}^{k}/C_{n}^{k},攻击者若随机在 $\boldsymbol{e}$ 中选择 k 个元素,并认为它们全为零,通过解线性方程组来破译密文,需要的工作因子 $W = K \times C_{n-t}^{k}/C_{n}^{k}$。当取 $n = 1024$ 时,Admas 等给出了使 W 最大时 t 的值,即 $t = 37$[53],此时 McEliece 体制有最高的安全性,$W \approx 2^{84.1}$。

3)区分器攻击。当区分器攻击密码方案时,区分器利用公钥矩阵不具有随机性,则将公钥矩阵和随机二进制矩阵进行区分。Faugère 等[54]发现采用的编码和密码方案的秩具有一定的相关性。当采用的 Goppa 码的码率接近于 1,攻击者构造了一个 Goppa 码区分器,很容易将随机码和 Goppa 码区分。区分器攻击的基本思想就是利用公共码和随机码的可区分性,区分密码方案所采用的代码是否为随机码,从而达到攻击的目的。

4)侧信道攻击。侧信道攻击通过检测密码方案实现过程中的一些物理现象,例如软件的运行时间或硬件的功耗来分析密码方案,以达到攻击的目的。Strenzke 等[55]提出对 McEliece 公钥体制的侧信道攻击,Strenzke 指出在解密过程中采用 Patterson 译码算法,时间功耗攻击是非常有效的,在密钥生成时能量攻击可以对校验矩阵的构造造成极大的破坏。如果编码的支撑向量已知,则在密钥生成过程中的奇偶校验矩阵构造中,

通过分析不可约 Goppa 多项式的求值所带来的功耗,可以得到不可约 Goppa 多项式。对 Patterson 译码算法的定时攻击使用了错误定位多项式的次数恰好等于接收到单词中的错误数量这一事实。因此,为了得到明文,可以尝试请求对伪密码文本进行解密。Shoufan 等[56]在文献[55]分析的基础上,对原始攻击做了进一步分析。Heyse 等[57]分析了解密过程中可逆矩阵和置换矩阵的功耗攻击。Molter 等[58]用所测量的功耗轨迹图峰值信息取代时序信息,对时序分析和错误注入相结合的攻击方法进行了研究。Chen 等[59]提出一种分析基于编码的差分攻击功率的新型方法,该攻击采用的方法是计算硬件实现上选定的基于 QC-MDPC 码单密文的特征值。Chen 等[60]采用与校验矩阵大小相同的 Boolean 的方法隐藏信息,进一步对密钥和特征值进行优化。Santini 等[61]研究了基于稀疏对偶校验码的密码方案,在采用循环校验码的情况下,通过新的侧信道攻击方法恢复出比目前已知的其他攻击更多的信息。

5)其他攻击。由于 McEliece 公钥密码体制存在延展性[62],攻击者可以通过观察两个密文之间的关联性来确定错误向量。另外一种反应攻击[63]则是对密文加以修改,合法接收方收到修改密文,攻击者观察其反应。消息在信道传递的过程中,攻击者非法截取密文,然后对截取的密文添加更多的错误位,如果接收方译码失败,表明修改的错误位在原来的错误向量 $\boldsymbol{e}$ 上。攻击者利用这种方法,最多重复 k 次就能恢复一个没有错误的信息。

5 展望

目前,基于编码的体制主要采用两类具有快速译码算法的码:秩度量码和汉明度量码。其存在的共同问题是密钥尺寸太大,为了减小密钥尺寸,推动基于编码加密体制的实用化进程,可以从以下几方面完善密码体制。

1)密码体制中编码理论方面还值得继续研究,例如研究码的结构特征,寻找新的性能更优、安全性更强的码,将编码理论中的码应用到密码学中;改进译码算法,降低译码复杂度,提高译码效率;研究如何构造随机性更强的公钥矩阵,使攻击者不能在公钥中得到生成矩阵或校验矩阵。

2)尝试在原有方案的基础上对结构进行改变,减少密钥长度,提高密码方案的实用化。

3)研究基于编码加密方案的软硬件实现,优化算法的能耗,提高实现效率,做好抗量子密码的实用化准备。

4)研究分析目前存在的攻击的共性,预测还可能存在的攻击,针对这些攻击,设计更加完善的密码方案。

6 结论

目前,后量子密码标准化进程正稳步推进,后量子密码方案已完成第二轮评选,我国也有序推进后量子算法标准化进程,基于编码的后量子密码方案已成为研究的热点。McEliece 密码方案是很早的基于编码的方案,具有抗量子计算的优点,在量子计算机大规模投入使用之前,亟待研究基于编码的密码方案。后量子密码评选方案中包括公钥加密、密钥封装、数字签名和密钥交换。本文综述了基于汉明度量编码和基于秩度量编码加密方案的发展历程及研究现状,介绍了基于 McEliece 方案进行结构改变的方案,分析了目前对基于编码加密方案主流的攻击类型。由于编码种类的多样性,本文仅对典型的编码进行了介绍,还有许多其他类型的编码没有进行详细概述。

参考文献(References)

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM Review, 1999, 41(2): 303 – 332.

[2] Rivest R L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120 – 126.

[3] Koblitz N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48(177): 203 – 209.

[4] 王丽萍, 戚艳红. 基于编码的后量子公钥密码研究进展[J]. 信息安全学报, 2019, 4(2): 20 – 28.
WANG Liping, QI Yanhong. Recent progress of code-based post-quantum public key cryptography [J]. Journal of Cyber Security, 2019, 4(2): 20 – 28. (in Chinese)

[5] Chen L, Jordan S, Liu Y K, et al. Report on post-quantum cryptography [M]. Maryland: National Institute of Standards and Technology, 2016.

[6] Alagic G, Alperin-Sheriff J, Apon D, et al. Status report on the first round of the NIST post-quantum cryptography standardization process [M]. Maryland: National Institute of Standards and Technology, 2019.

[7] Roma C A, Tai C A, Hasan M A. Energy consumption of round 2 submissions for NIST PQC standards [R]. Maryland: National Institute of Standards and Technology, 2019.

[8] McEliece R J. A public-key cryptosystem based on algebraic coding theory [J]. DSN Progress Report, 1978, 42(44): 114 – 116.

[9] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory [J]. Problems of Control and Information Theory, 1986, 15(2): 159 – 166.

[10] Baldi M, Chiaraluce F, Garello R, et al. Quasi-cyclic low-density parity-check codes in the McEliece

cryptosystem[C]// Proceedings of IEEE International Conference on Communications, 2007: 951 – 956.

[11] Mafakheri B, Eghlidos T, Pilaram H. An efficient secure channel coding scheme based on Polar codes [J]. The ISC International Journal of Information Security, 2017, 9(2): 13 – 20.

[12] Tillich J P. The decoding failure probability of MDPC codes[C]// Proceedings of IEEE International Symposium on Information Theory (ISIT), 2018: 941 – 945.

[13] Gabidulin E, Rashwan H, Honary B. On improving security of GPT cryptosystems[C]//Proceedings of IEEE International Symposium Information Theory-ISIT, 2009: 1110 – 1114.

[14] Aragon N, Gaborit P, Hauteville A, et al. Low rank parity check codes: new decoding algorithms and applications to cryptography[R]. arXiv: 1904.00357vl, 2019: 1 – 45.

[15] Bucerzan D, Dragoi V, Kalachi H T. Evolution of the McEliece public key encryption scheme [J]. Springer International Publishing, 2017: 129 – 149.

[16] Wang Y G. Quantum resistant random linear code based public key encryption scheme RLCE[C]// Proceedings of IEEE International Symposium on Information Theory (ISIT), 2016: 2519 – 2523.

[17] Kim J L, Kim Y S, Galvez L, et al. McNie: a code-based public-key cryptosystem [J]. arXiv Preprint arXiv: 1812.05008, 2018.

[18] 刘相信, 杨晓元. Niederreiter 公钥密码方案的改进[J]. 计算机应用, 2018, 38(7): 1956 – 1959.
LIU Xiangxin, YANG Xiaoyuan. Improvement of Niederreiter public key cryptosystem[J]. Computer Application, 2018, 38(7): 1956 – 1959. (in Chinese)

[19] Mostafa E. Application of linear block codes in cryptography[D]. Iran: Isfahan University of Technology, 2019.

[20] Monico C, Rosenthal J, Shokrollahi A. Using low density parity check codes in the McEliece cryptosystem [C]// Proceedings of IEEE International Symposium on Information Theory, 2000: 2 – 15.

[21] Baldi M, Bodrato M, Chiaraluse F. A new analysis of the McEliece cryptosystem based on QC-LDPC codes [C]// Proceedings of 6th International Conference SCN, 2008, 5229: 246 – 262.

[22] Shooshtari M K, Ahmadian-Attari M, Johansson T, et al. Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes [J]. IET Information Security, 2016, 10 (4): 194 – 202.

[23] Misoczki R, Tillich J P, Sendrier N, et al. MDPC-McEliece: new McEliece variants from moderate density parity-check codes [C]// Proceedings of IEEE International Symposium on Information Theory, 2013: 2069 – 2073.

[24] Guo Q, Johansson T, Stankovski P. A key recovery attack on MDPC with CCA security using decoding errors [M]// Advances in Cryptology. Berlin: Springer, 2016: 789 – 815.

[25] Fabšič T, Hromada V, Stankovski P, et al. A reaction attack on the QC-LDPC McEliece cryptosystem [C]// Proceedings of International Workshop on Post-Quantum Cryptography, 2017: 51 – 68.

[26] Moufek H, Guenda K, Gulliver T A. A new variant of the McEliece cryptosystem based on QC-LDPC and QC-MDPC codes [J]. IEEE Communications Letters, 2017, 21(4): 714 – 717.

[27] Dragoi V, Kalachi H T. Cryptanalysis of a public key encryption scheme based on QC-LDPC and QC-MDPC codes[J]. IEEE Communications Letters, 2017, 22 (2): 264 – 267.

[28] Arikan E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels [J]. IEEE Transactions on Information Theory, 2009, 55(7): 3051 – 3073.

[29] Mahdavifar H, Vardy A. Achieving the secrecy capacity of wiretap channels using Polar codes [J]. IEEE Transactions on Information Theory, 2011, 57(10): 6428 – 6443.

[30] Hooshmand R, Aref M, Eghlidos T. Secret key cryptosystem based on non-systematic Polar codes [J]. Wireless Personal Communications, 2015, 84(2): 1345 – 1373.

[31] Hooshmand R, Aref M R. Efficient Polar code-based physical layer encryption scheme [J]. IEEE Wireless Communications Letters, 2017, 6(6): 710 – 713.

[32] Jin H X, Liu R K, Zhang C Y. Low transmission overhead for Polar coding physical-layer encryption [J]. China Communications, 2019, 16(2): 246 – 256.

[33] Shrestha S R, Kim Y S. New McEliece cryptosystem based on Polar codes as a candidate for post-quantum cryptography[C]// Proceedings of 14th International Symposium on Communications and Information Technologies (ISCIT), 2014: 368 – 372.

[34] Hooshmand R, Shooshtari M K, Eghlidos T, et al. Reducing the key length of McEliece cryptosystem using Polar codes[C]//Proceedings of 11th International ISC Conference on Information Security and Cryptology, 2014: 104 – 108.

[35] Bardet M, Chaulet J, Dragoi V, et al. Cryptanalysis of the McEliece public key cryptosystem based on Polar codes[C]// Proceedings of Post-Quantum Cryptography, 2016: 118 – 143.

[36] 杨超, 肖东亮, 顾珍珍, 等. 基于 Polar 码的 Niederreiter 公钥密码体制[J]. 密码学报, 2018, 5(6): 623 – 630.
YANG Chao, XIAO Dongliang, GU Zhenzhen, et al. Niederreiter public key cryptosystem based on Polar codes [J]. Journal of Cryptologic Research, 2018, 5(6): 623 – 630. (in Chinese)

[37] Drăgoi V, Beiu V, Bucerzan D. Vulnerabilities of the McEliece variants based on Polar codes[C]//Proceedings of International Conference on Security for Information Technology and Communications, 2018: 376 – 390.

[38] Sidelnikov V M, Shestakov S O. On insecurity of cryptosystems based on generalized Reed-Solomon codes [J]. Discrete Mathematics and Applications, 1992, 2 (4): 439 – 444.

[39] Wieschebrink C. Two NP-complete problems in coding theory with an application in code based cryptography [C]// Proceedings of IEEE International Symposium on Information Theory, 2006: 1733 – 1737.

[40] Couvreur A, Gaborit P, Gauthier-Umaña V, et al. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes [J]. Designs, Codes and Cryptography, 2014, 73(2): 641 – 666.

[41] Márquez-Corbella I, Tillich J P. Using Reed-Solomon codes in the $(u|u+v)$ construction and an application to cryptography [C]//Proceedings of IEEE International Symposium on Information Theory (ISIT), 2016: 930 – 934.

[42] Kshevetskiy A, Gabidulin E. The new construction of rank codes [C]//Proceedings of International Symposium on

Information Theory, 2005: 2105 – 2108.

[43] Overbeck R. Structural attacks for public key cryptosystems based on Gabidulin codes [J]. Journal of Cryptology, 2008, 21(2): 280 – 301.

[44] Horlemann-Trautmann A L, Marshall K, Rosenthal J. Extension of Overbeck's attack for Gabidulin-based cryptosystems[J]. Designs, Codes and Cryptography, 2018, 86(2): 319 – 340.

[45] Loidreau P. A new rank metric codes based encryption scheme[C]// Proceedings of International Workshop on Post-Quantum Cryptography, 2017: 3 – 17.

[46] Coggia D, Couvreur A. On the security of a Loidreau's rank metric code based encryption scheme [J]. arXiv Preprint arXiv: 1903.02933, 2019.

[47] Aragon N, Gaborit P, Hauteville A, et al. Low rank parity check codes: new decoding algorithms and applications to cryptography [J]. IEEE Transactions on Information Theory, 2019, 65(12): 7697 – 7717.

[48] Aragon N, Gaborit P. A key recovery attack against LRPC using decryption failures [C]// Proceedings of Coding and Cryptography, International Workshop, 2019.

[49] Lau T S C, Tan C H. Key recovery attack on McNie based on low rank parity check codes and its reparation: 13th international workshop on security [M]// Advances in Information and Computer Security. Springer, Cham, 2018.

[50] Kim J L, Kim Y S, Galvez L, et al. A new code-based public-key cryptosystem [R]. arXiv: 1812.05008v2, 2019.

[51] Upadhyay L. Quantum cryptography: a survey [C]// Proceedings of International Conference on Innovations in Bio-Inspired Computing and Applications, 2019: 20 – 35.

[52] Welch Z. An analysis of potential standards for post-quantum cryptosystems [D]. Ottawa: Carleton University, 2019.

[53] Adams C M, Meijer H. Security-related comments regarding McEliece's public-key cryptosystem[J]. IEEE Transactions on Information Theory, 1987, 35(2): 454 – 455.

[54] Faugère J C, Gauthier-Umana V, Otmani A, et al. A distinguisher for high-rate McEliece cryptosystems [J]. IEEE Transactions on Information Theory, 2013, 59 (10): 6830 – 6844.

[55] Strenzke F, Tews E, Molter H G, et al. Side channels in the McEliece PKC[C]// Proceedings of International Workshop on Post-Quantum Cryptography, 2008: 216 – 229.

[56] Shoufan A, Strenzke F, Molter H G, et al. A timing attack against patterson algorithm in the McEliece PKC [C]// Proceedings of International Conference on Information Security and Cryptology, 2009: 161 – 175.

[57] Heyse S, Moradi A, Paar C. Practical power analysis attacks on software implementations of McEliece[C]// Proceedings of Post-quantum Cryptography, Third International Workshop, Darmstadt, 2010.

[58] Molter H G, Stöttinger M, Shoufan A, et al. A simple power analysis attack on a McEliece crypto processor [J]. Journal of Cryptographic Engineering, 2011, 1(1): 29 – 36.

[59] Chen C, Eisenbarth T, von Maurich I, et al. Differential power analysis of a McEliece cryptosystem[C]// Proceedings of International Conference on Applied Cryptography and Network Security, 2015: 538 – 556.

[60] Chen C, Eisenbarth T, von Maurich I, et al. Masking large keys in hardware: a masked implementation of McEliece[C]// Proceedings of International Conference on Selected Areas in Cryptography, 2016: 293 – 309.

[61] Santini P, Battaglioni M, Chiaraluce F, et al. Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes[J]. arXiv Preprint arXiv: 1904.12215, 2019.

[62] Cayrel P L, Gueye C T, Ndiaye O, et al. Critical attacks in code-based cryptography [J]. International Journal of Information and Coding Theory, 2015, 3(2): 158 – 176.

[63] Santini P, Baldi M, Chiaraluce F. Assessing and countering reaction attacks against post-quantum public-key cryptosystems based on QC-LDPC codes[C]// Proceedings of International Conference on Cryptology and Network Security, 2018: 323 – 343.