计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20200452
57(10): 2086-2103, 2020

基于模格的密钥封装方案的比较分析与优化

王 洋[1,3] 沈诗羽[2] 赵运磊[2] 王明强[1,3]
[1](山东大学数学学院 济南 250100)
[2](复旦大学计算机科学技术学院 上海 200433)
[3](密码技术与信息安全教育部重点实验室(山东大学) 济南 250100)
(wyang1114@email.sdu.edu.cn)

Comparisons and Optimizations of Key Encapsulation Mechanisms Based on Module Lattices

Wang Yang[1,3], Shen Shiyu[2], Zhao Yunlei[2], and Wang Mingqiang[1,3]
[1](*School of Mathematics*, *Shandong University*, *Jinan* 250100)
[2](*School of Computer Science*, *Fudan University*, *Shanghai* 200433)
[3](*Key Laboratory of Cryptologic and Information Security*(*Shandong University*), *Ministry of Education*, *Jinan* 250100)

Abstract Till now, there are two kinds of constructions of highly efficient key encapsulation mechanisms based on module LWE/LWR problems without using complicate error correcting codes: one is direct constructions based on (symmetric or asymmetric) module LWE/LWR problems such as Kyber, Aigis and Saber; the other is constructions based on key consensus mechanisms and module LWE/LWR problems such as AKCN-MLWE and AKCN-MLWR. In order to save bandwidth, the constructed key encapsulation mechanisms may usually compress the communications under tolerable security and efficiency. To the best of our knowledge, the existing literatures all focus on the security analysis of corresponding schemes under concrete parameters, and there are no literatures which focus on the analysis of similarities and differences about the above two kinds of constructions with the same (or different) compress functions, let alone the relationships between parameters and error rates. In this paper, we compare the above two kinds of constructions systematically. It is proved that constructions of AKCN-MLWE are better than constructions of Kyber when using the same compress functions and parameter settings from both theoretical analysis and practical tests. Meanwhile, similar analysis shows that the constructions of Saber are essentially the same as the constructions of AKCN-MLWR. Corresponding to the security strength of parameters recommended as Kyber-1024, we also analyze three kinds of methods about how to encapsulate 512 bits. Based on our theoretical analysis and a large number of experimental tests, we present new optimization suggestions and parameter recommendations for AKCN-MLWE and AKCN-MLWR. New optimized schemes corresponding to Aigis and Kyber (named AKCN-Aigis and AKCN-Kyber), and new recommended parameters are also proposed.

收稿日期:2020-06-12;**修回日期**:2020-07-30
基金项目:国家自然科学基金项目(61672019,61832012,61877011,61472084);国家重点研发计划项目(2017YFB0802000);国家密码发展基金(MMJJ20180210);山东省重点研发项目(2017CXG0701,2018CXGC0701)
This work was supported by the National Natural Science Foundation of China (61672019, 61832012, 61877011, 61472084), the National Key Research and Development Program of China (2017YFB0802000), the National Cryptography Development Fund (MMJJ20180210), and the Shandong Provincial Key Research and Development Program of China (2017CXG0701, 2018CXGC0701).
通信作者:赵运磊(ylzhao@fudan.edu.cn)

Key words　post-quantum cryptograph; module LWE/LWR problems; key encapsulation mechanisms; key consensus; error rates analysis

摘　要　到目前为止,不使用复杂纠错码的基于模 LWE/LWR 问题设计的高效密钥封装方案主要有 2 类:1)如 Kyber,Aigis 和 Saber 直接基于(对称或非对称)模 LWE/LWR 问题设计;2)如 AKCN-MLWE 和 AKCN-MLWR 基于密钥共识机制结合模 LWE/LWR 问题设计.一般来说,在满足一定安全性和实现效率的基础上,实际应用中构造的密钥封装方案会通过压缩一些通信比特来达到节省通信带宽的目的.据作者所知,现存文献的关注点一般集中在详细分析对应某具体参数条件下密码体制的安全性,还没有文献系统地分析上述 2 类构造方式的异同以及采用相同(或不同)压缩函数情况下不同参数选择与错误率的关系.从理论上系统地比较了直接基于 LWE/LWR 构造的密钥封装方案和基于密钥共识机制结合模 LWE/LWR 问题设计的密钥封装方案的异同,并从理论分析和实际测试 2 方面证明了当采用相同的压缩函数和相同的参数设置时,AKCN-MLWE 采用的构造方式要优于 Kyber 采用的构造方式,而 Saber 采用的构造方式本质上与 AKCN-MLWR 是相同的.针对 Kyber-1024 这一组参数对应的安全强度,还详细分析了 3 种封装 512 b 密钥长度的方法.根据理论分析和大量的实验测试,给出了 AKCN-MLWE 和 AKCN-MLWR 的新的优化建议和参数推荐,也给出了对于 Aigis 和 Kyber 的优化方案(对应的命名为 AKCN-Aigis 和 AKCN-Kyber)和新的参数推荐.

关键词　后量子密码;模 LWE/LWR 问题;密钥封装方案;密钥共识;错误率分析

中图法分类号　TP309

自从 1976 年 Diffie 和 Hellman[1] 提出利用单向陷门函数构造公钥密码算法以来,基于不同困难问题设计的各种各样的公钥密码体制相继被提出,并在密码学中有着极其广泛的应用.目前广泛使用的基于数论假设困难问题(如因子分解和离散对数问题)设计的公钥密码体制可以被 Shor 算法[2] 在量子多项式时间内攻破.随着 20 多年来量子计算机技术的快速发展以及抗量子密码技术的研究,后量子密码算法的标准化工作也逐渐被提上日程.2016 年美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)正式发起了对公钥加密(public key encryption, PKE)、密钥封装(key encapsulation mechanism, KEM)和数字签名这3 类基本公钥密码算法相关的抗量子密码算法标准的征集工作.第 1 轮 69 个候选算法中有 26 个算法入选到第 2 轮评估[3],这其中有 12 个候选算法(如 NewHope,FrodoKEM,CRYSTALS-KYBER,SABER,LAC 等)是基于格中困难问题设计的.CRYSTALS-KYBER 和 SABER 更是入选为 NIST 最近公布的第 3 轮竞选算法[4].2019 年我国举行了后量子密码算法竞赛[5-6],获奖的算法也大多是基于格中的困难问题设计的,其中密钥封装算法包括:Aigis,LAC,AKCN-MLWE,Scloud,Tale 等.

设计 PKE 和 KEM 时最常用的格中困难问题是(环,模)LWE/LWR 问题[7-10].非正式地讲,标准形式(normal form)判定版本的(多项式)模 LWE 问题[11] 是:给定模 $R_q^{m\times l}$ 中均匀选择的矩阵 $\boldsymbol{A}$,以及某些向量 $\boldsymbol{b}$,判断 $\boldsymbol{b}$ 是 R_q^l 中的均匀分布还是 $\boldsymbol{b}=\boldsymbol{As}+\boldsymbol{e} \bmod qR$,其中 $\boldsymbol{s}$ 和 $\boldsymbol{e}$ 服从 R^l 上的某分布 μ.而模 LWR 问题为给定模 $R_q^{m\times l}$ 中均匀选择的矩阵 $\boldsymbol{A}$,以及某些向量 $\boldsymbol{b}$,判断 $\boldsymbol{b}$ 是 R_q^l 中的均匀分布还是 $\boldsymbol{b}=\left\lfloor \frac{p}{q}\boldsymbol{As} \right\rceil$,其中 $\boldsymbol{s}$ 服从 R^l 上的某分布 μ.本文中我们采用系数嵌入来进行讨论.可以证明,对于适当的环 R 和分布 μ,上述问题的困难性可以归约到一类格中 worst-case 的基本困难问题(如 SIVP_γ)上.模 LWE 问题的 $\boldsymbol{s}$ 和 $\boldsymbol{e}$ 服从 R^l 上的相同分布 μ.为了进一步平衡安全性、实现效率以及通信带宽,文献[12-13]提出了非对称的 LWE 问题,即 $\boldsymbol{s}$ 和 $\boldsymbol{e}$ 服从 R^l 上的不同分布(更确切地说,是服从不同参数的某一类分布).目前,不使用复杂纠错码、接近于实用化的基于模 LWE/LWR 问题设计的高效 KEM 方案主要有 2 类:1)直接基于模 LWE/LWR 问题设计(如 Kyber[14],Saber[15] 和 Aigis[12]);2)基于文献[16-17]提出的密钥共识机制结合模 LWE/LWR 问题设计(如 KCL[18],AKCN-MLWE,AKCN-MLWR 和 AKCN-Hybrid).上述 2 类 KEM 方案的构造方式均为先构造 IND-CPA 安全的 PKE 加密方案,然后

采用 Fujisaki-Okamoto(FO)[19-21]转换来构造满足 IND-CCA 安全的密钥封装方案.

共识机制是文献[16-17]提出的一种新的密码原语,由(*Con*,*Rec*)2 个算法组成.非正式地讲,当输入均匀随机时,对称密钥共识机制的 *Con* 算法会输出某些相互独立的提示信号和随机的共识值.当 *Con* 和 *Rec* 算法的输入比较接近时,在提示信号的帮助下,*Rec* 算法可以恢复出 *Con* 算法输出的共识值.非对称密钥共识机制则可以人为地决定共识值(即上述 *Con* 算法的共识值作为输入,输出的提示信号与输入的共识值彼此相互独立).文献[16-17]给出了一般性共识机制参数应满足的条件关系式,并设计了无条件安全的参数接近最优的非对称和对称的密钥共识机制.基于这些密钥共识机制,文献[16-17]依赖不同的困难问题设计了多种密钥封装方案,AKCN-MLWE/MLWR 和 AKCN-Hybrid 就是基于非对称密钥共识机制和模 LWE/LWR 问题设计的一种密钥封装机制.

到目前为止,还没有文献系统地分析直接基于模 LWE/LWR 问题构造的密钥封装方案和基于密钥共识机制结合模 LWE/LWR 问题设计的密钥封装方案的异同,特别是采用相同(或不同)压缩函数情况下不同参数选择与错误率的关系.事实上,当安全强度较低(如 Kyber-512)时,没有必要设置参数使得错误率比安全强度小很多.同时为了兼顾安全性,在设置参数时也不能使错误率比安全强度大太多以保证不会由于解密错误的存在而降低方案抵抗量子敌手的能力.在安全强度与错误率相近的情况下,如何确定参数以达到尽量节省通信带宽的目的也有着很大的应用价值.

本文的主要贡献有 3 个方面:

1) 从理论上系统地比较了直接基于模 LWE/LWR 问题构造的密钥封装方案和基于密钥共识机制结合模 LWE/LWR 问题设计的密钥封装方案的异同,并对其具体错误率进行了较为精确的分析.本文从理论分析和实际测试 2 方面证明了当采用相同的压缩函数和相同的参数设置时,AKCN-MLWE 采用的构造方式要优于 Kyber 采用的构造方式;同时,Saber 采用的构造方式与 AKCN-MLWR 的构造方式没有本质的区别.

2) 由于 Grove 量子搜索算法的存在,为了实现大约 256 b 的量子安全强度,需考虑会话密钥长度约为 512 b 的 KEM 方案的设计.此外,目前的 TLS1.3 标准也强制要求提供 512 b 会话密钥的握手协商机制[22].因此,提供 512 b 的会话密钥也是现实的需求.对应 Kyber-1024 和 Fire-Saber 级别的参数,本文详细对比分析了 3 种可能的封装 512 b 密钥长度的方法.

3) 根据理论分析和大量实验测试,给出了 AKCN-MLWE、AKCN-MLWR 和 AKCN-Hybrid 的新的优化建议和参数推荐.同时也给出了对于 Aigis 和 Kyber 的优化方案(对应命名为 AKCN-Aigis 和 AKCN-Kyber)和新的参数推荐.

1 相关工作

Kyber 和 Aigis 采用的 IND-CPA 安全的 PKE 方案主要遵循文献[23]的设计框架(事实上目前很多基于 LWE 问题的 PKE 方案都是遵循这一框架设计的),而后采用 FO 转换来设计满足特定安全性要求的密钥封装方案.文献[12]观察到了由于压缩技术的使用,模 LWE 问题的秘密 $\boldsymbol{s}$ 和误差扰动 $\boldsymbol{e}$ 对 PKE 方案最后的解密错误率的影响不对等,系统化地提出了非对称模 LWE 问题和模 SIS 问题,并从实际攻击的角度详细测试了不同参数条件下底层困难问题对应的安全强度.这使得 Aigis 可以更好地平衡安全性、实现效率、错误率和通信带宽的关系.Saber 是直接基于模 LWR 问题设计的,采用的设计思路也是先设计 IND-CPA 安全的 PKE 方案,随后采用 FO 转换来设计密钥封装方案.AKCN-MLWE 和 AKCN-MLWR 的设计采用了文献[16-17]提出的非对称的密钥共识机制.本质上讲,Kyber 和 Aigis 采用的传统 LWE 形式的 PKE 方案以及 Saber 采用的模 LWR 形式的 PKE 方案均可以改写成非对称的密钥共识机制的形式(只不过采用的非对称的密钥共识算法与 AKCN-MLWE/MLWR 的不同),反之亦然.同时,我们注意到,结合原始 AKCN-MLWE 和 Aigis 的设计,我们可以更加优化参数的选择.需要说明的是,文献[23]及其变体密码体制均是针对加密单比特设计的.文献[16-17]中首先给出了更一般的加密形式并详细分析了相关参数所必须遵循的不等式界.

2 预备知识

本节定义一些符号并简单回顾 Kyber,Saber,Aigis 和 AKCN 采用的 IND-CPA 安全的加密体制的构造.

2.1　基本定义及符号说明

本文使用多项式环的系数嵌入并考虑分圆多项式环 $R:=\mathbb{Z}[X]/(X^n+1)$,这里 $n=2^k$ 为 2 的方幂.对于实数 $x\in\mathbb{R}$,我们使用符号 $\lfloor x\rceil$ 来表示对 x 的向下取整并定义四舍五入 $\lfloor x\rceil=\left\lfloor x+\frac{1}{2}\right\rfloor$.当 $\boldsymbol{x}$ 为向量(本文默认使用列向量)、矩阵或者多项式时,$\lfloor \boldsymbol{x}\rceil$ 表示对 $\boldsymbol{x}$ 的每个分量或系数进行四舍五入操作.对于向量 $\boldsymbol{v}$ 或矩阵 $\boldsymbol{A}$,我们使用符号 $\boldsymbol{v}^{\mathrm{T}}$ 或 $\boldsymbol{A}^{\mathrm{T}}$ 来表示其转置.对于某个有限集合 S,符号 $U(S)$ 表示集合 S 上的随机均匀分布.我们用符号 $x\hookleftarrow\mu$ 来表示按照概率分布 μ 来取样得到 x.同样,当 $\boldsymbol{x}$ 为向量、矩阵或者多项式时,$\boldsymbol{x}\hookleftarrow\mu$ 表示 $\boldsymbol{x}$ 的每个分量或系数均独立地服从分布 μ.对于某正整数 q,定义集合 $\mathbb{Z}_q=\mathbb{Z}/q\mathbb{Z}=\{0,1,\cdots,q-1\}$,我们也使用符号 $x'=x \bmod q$ 来表示 x 的落在集合 $\mathbb{Z}_q$ 中的代表元 x',并用符号 $x'=x \bmod^{\pm} q$ 来表示 x 的落在集合 $\left[-\frac{q}{2},\frac{q}{2}\right)\cap\mathbb{Z}$ 中的代表元 x'.对于 $x\in\mathbb{Z}_q$,我们定义 $\|x\|_\infty=|x \bmod^{\pm} q|$.而对于多项式环 R 中的元素 $f=f_0+f_1X+\cdots+f_{n-1}X^{n-1}$,我们定义 $\|f\|_\infty=\max\limits_{0\leqslant i\leqslant n-1}\|f_i\|_\infty$.此定义可以平凡地推广到 R^d 中,即对于 $\boldsymbol{f}=(f_1,f_2,\cdots,f_d)\in R^d$,定义 $\|\boldsymbol{f}\|_\infty=\max\limits_{1\leqslant i\leqslant d}\|f_i\|_\infty$.对于向量 $\boldsymbol{x}$,我们使用符号 $\|\boldsymbol{x}\|_\infty^{\pm}\in S$ 来表示 $\boldsymbol{x} \bmod^{\pm} q$ 的每一个系数均落在集合 S 中.

在实际应用中,我们一般考虑秘密和误差服从中心二项分布的模 LWE/LWR 问题.对于正整数 η,我们定义中心二项分布 S_η 为:取样 $\{(a_i,b_i)\}_{i=1}^{\eta}\hookleftarrow U((\{0,1\}^2)^\eta)$,输出 $\sum\limits_{i=1}^{\eta}(a_i-b_i)$.环 R 上定义的判定版本模 LWE 问题为区分多项式数目的均匀样本 $U(R_q^l\times R_q)$ 与样本 $(\boldsymbol{a}_i,b_i)$,其中 $\boldsymbol{a}_i\hookleftarrow U(R_q^l)$,$b_i=\boldsymbol{a}_i^{\mathrm{T}}\boldsymbol{s}+e_i$,$\boldsymbol{s}\hookleftarrow S_\eta^l$,$e_i\hookleftarrow S_\eta$.判定版本的模 LWE 假设是说,没有概率多项式时间的量子敌手可以以不可忽略的优势解决判定版本的模 LWE 问题.而环 R 上定义的模 LWR 问题为区分多项式数目的均匀样本 $U(R_q^l\times R_q)$ 与样本 $(\boldsymbol{a}_i,b_i)$,其中 $\boldsymbol{a}_i\hookleftarrow U(R_q^l)$,$b_i=\left\lfloor\frac{p}{q}\boldsymbol{a}_i^{\mathrm{T}}\boldsymbol{s}\right\rceil$,$\boldsymbol{s}\hookleftarrow S_\eta^l$.对应地,模 LWR 假设是说,没有概率多项式时间的量子敌手可以以不可忽略的优势解决模 LWR 问题.

2.2　格密码体制常用的压缩函数

为了节省通信带宽,在实际应用中设计的密码体制一般会采用一些压缩技术.目前,在不使用额外纠错码的情况下,格密码体制最常用的压缩函数[12,14,24]为:

$$\begin{cases}Compress_{q,d}(x)=\left\lfloor\frac{2^d}{q}x\right\rceil \bmod 2^d,\ x\in\mathbb{Z}_q,\\ Decompress_{q,d}(y)=\left\lfloor\frac{q}{2^d}y\right\rceil \bmod q,\ y\in\mathbb{Z}_{2^d}.\end{cases}$$

这里我们直接使用 2^d 是为了充分利用存储空间.容易验证,对于 $x\in\mathbb{Z}_q$,我们有:

$$\|x-Decompress_{q,d}(Compress_{q,d}(x))\|_\infty\leqslant\left\lfloor\frac{q}{2^{d+1}}\right\rceil.$$

为了讨论方便,我们称上述压缩函数为换模压缩函数.

在满足一定错误率要求的情况下,为了提高运算效率,文献[16-17]中也考虑了直接砍去低位比特的压缩函数:

$$\begin{cases}Compress_q^t(x)=\left\lfloor\frac{x}{2^t}\right\rceil \bmod 2^{\lceil\mathrm{lb}q\rceil-t},\ x\in\mathbb{Z}_q,\\ Decompress_q^t(y)=2^t y \bmod q,\ y\in\mathbb{Z}_{2^{\lceil\mathrm{lb}q\rceil-t}}.\end{cases}$$

此时,对于 $x\in\mathbb{Z}_q$,我们容易计算得:

$$\|x-Decompress_q^t(Compress_q^t(x))\|_\infty\in[-2^{t-1},2^{t-1})\cap\mathbb{Z}.$$

我们称此种压缩函数为砍比特压缩函数.当压缩相同比特数,即 $d=\lceil\mathrm{lb}q\rceil-t$ 时,我们有 $\left\lfloor\frac{q}{2^{d+1}}\right\rceil\leqslant 2^{t-1}$.

2.3　密钥共识机制

文献[16-17]中第 1 次提出一种称之为密钥共识的密码原语,利用此密码原语可以基于不同的困难问题设计密钥封装和公钥加密体制.AKCN-MLWE,AKCN-MLWR 和 AKCN-Hybrid 就是采用非对称的密钥共识算法基于模 LWE 问题、模 LWR 问题和模 LWE/LWR 混合问题设计的 IND-CPA 安全的公钥加密方案,进而通过现有的通用构造来设计 IND-CCA 安全的密钥封装协议.

定义 1. 非对称密钥共识算法[16-17] $AKC=(params,Con,Rec)$ 的定义为:

1) $params=(q,m,g,d,aux)$.表示系统参数,其中 q,m,g,d 均为正整数且满足关系式 $2\leqslant m$,$g\leqslant q$ 和 $1\leqslant d\leqslant\left\lfloor\frac{q}{2}\right\rfloor$.$aux$ 表示由 (q,m,g,d) 确定的辅助信息,其值可能为空.

2) $V\leftarrow Con(\Sigma_2,K_2,params)$.在输入为 $\Sigma_2\in\mathbb{Z}_q$,$K_2\in\mathbb{Z}_m$ 和 $params$ 的条件下,概率多项式时间算法 Con 输出公开提示信息 $V\in\mathbb{Z}_g$.

3) $K_1 \leftarrow Rec(\Sigma_1, V, params)$.在输入为 $\Sigma_1 \in \mathbb{Z}_q$,$V$ 和 $params$ 的条件下,确定多项式时间算法 Rec 输出 $K_1 \in \mathbb{Z}_m$.

我们称一个非对称密钥共识算法满足正确性,如果对于任意满足条件 $\|\Sigma_2 - \Sigma_1\|_\infty \leqslant d$ 的整数 Σ_1,$\Sigma_2 \in \mathbb{Z}$,均有 $K_1 = K_2$ 成立.我们称一个非对称密钥共识算法满足安全性,如果对于任意的在 $\mathbb{Z}_q$ 中均匀分布的 Σ_2,V 和 K_2 的分布都是相互独立的;同时对于任意的 $\widetilde{V} \in \mathbb{Z}_g$ 和 $\widetilde{K}_2, \widetilde{K}'_2 \in \mathbb{Z}_m$,都有:

$$Pr[V = \widetilde{V} \mid K_2 = \widetilde{K}_2] = Pr[V = \widetilde{V} \mid K_2 = \widetilde{K}'_2]$$

成立,这里概率取自 $\Sigma_2 \leftarrow U(\mathbb{Z}_q)$ 和 Con 中使用的随机性.在后续的讨论中,为了方便会省略掉 $params$.文献[16-17]证明了满足正确性和安全性的非对称密钥共识算法的参数 $params$ 应满足的条件.

定理 1[16-17]. 令 AKC 为任意一个参数为 $params = (q, m, g, d, aux)$ 的非对称密钥共识算法,如果 AKC 满足正确性和安全性,则 $2md \leqslant q\left(1 - \frac{m}{g}\right)$.

2.4 AKCN-MLWE/MLWR 加密算法

文献[16-17]基于非对称的密钥共识算法设计了 IND-CPA 安全的公钥加密体制 AKCN-MLWE 和 AKCN-MLWR.具体构造分别如图 1 和图 2 所示(图 2 为参数为 2 的方幂情况下的简化版本).其中 $AKC = (Con, Rec)$ 可以是任意满足正确性和安全性的非对称密钥共识算法,Gen 为某特定的输出伪随机的扩展函数.

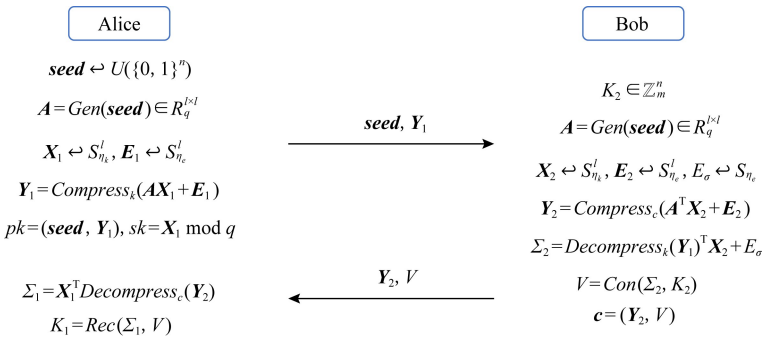

Fig. 1 IND-CPA secure encryption schemes used by AKCN-MLWE

图 1 AKCN-MLWE 采用的 IND-CPA 安全的加密体制的构造

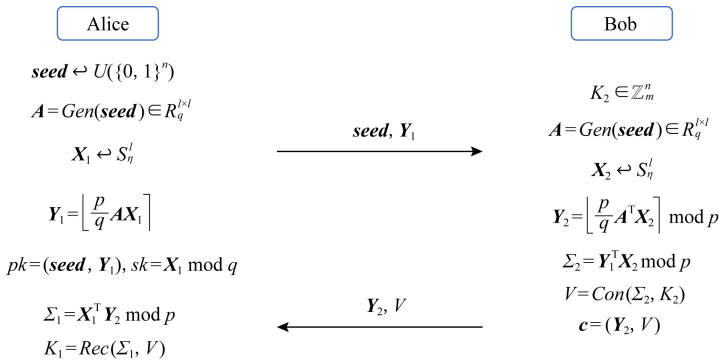

Fig. 2 IND-CPA secure encryption schemes used by AKCN-MLWR

图 2 AKCN-MLWR 采用的 IND-CPA 安全的加密体制的构造

AKCN-MLWE/MLWR 采用的共识算法为:

$$\begin{cases} Con(\Sigma_2, K_2) := V = \\ \quad \left\lfloor \frac{g}{q}\left(\Sigma_2 + \left\lfloor \frac{q}{m}K_2 \right\rceil\right)\right\rceil \bmod g, \\ Rec(\Sigma_1, V) := K_1 = \\ \quad \left\lfloor m\left(\frac{V}{g} - \frac{\Sigma_1}{q}\right)\right\rceil \bmod m. \end{cases} \tag{1}$$

二者的区别在于,AKCN-MLWE 选择的计算模数 q 为满足 NTT 算法条件的素数.而 AKCN-MLWR 选择的参数均为 2 的方幂且算法式(1)中对应的参数 q 为图 2 中对应的参数 p.文献[16-17]证明了 AKCN-MLWE 参数对应的共识算法满足正确性的参数要求为 $(2d+1)m < q\left(1 - \frac{m}{g}\right)$,而 AKCN-

MLWR 参数对应的共识算法满足正确性的参数要求为 $2dm<q\left(1-\frac{m}{g}\right)$.特别地,结合定理 1 可以看出,AKCN-MLWE/MLWR 采用的非对称密钥共识算法参数所满足的界均已经接近最优.

2.5　LWE/LWR 加密算法

Kyber,Aigis 和 Saber 等使用模 LWE/LWR 问题设计了 IND-CPA 安全的公钥加密体制.具体构造分别如图 3 和图 4 所示.为了方便与 AKCN-MLWE/MLWR 作对比,本文将加密算法改写为交互的形式,把第 2 个密文 V 直接写成显示的压缩和解压缩形式.为充分利用存储空间,一般将 g 的值设置为某些比较小的 2 的方幂.Kyber 采用对称形式判定版本的模 LWE 假设,即设置 $\eta_k=\eta_e$ 且对公钥 $\boldsymbol{Y}_1$ 和第 1 个密文 $\boldsymbol{Y}_2$ 采用相同的压缩函数.Aigis 采用的是非对称的模 LWE 假设,推荐设置的 η_k 和 η_e 一般不相等,且对公钥 $\boldsymbol{Y}_1$ 以及第 1 个密文 $\boldsymbol{Y}_2$ 压缩的比特数目也不相同.

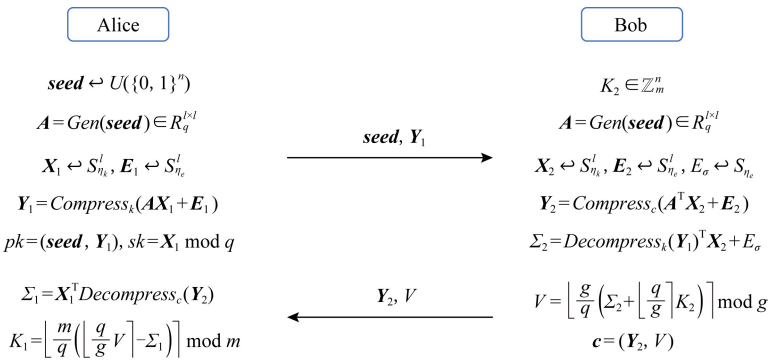

Fig. 3　IND-CPA secure encryption schemes based on LWE

图 3　LWE 形式的 IND-CPA 安全的加密体制的构造

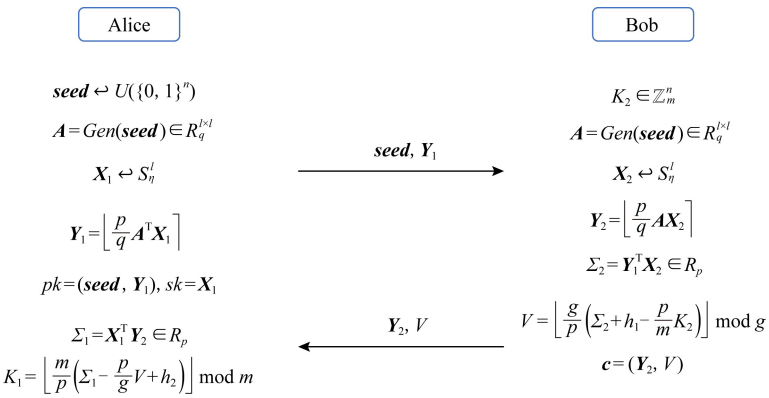

Fig. 4　IND-CPA secure encryption schemes used by Saber

图 4　Saber 采用的 IND-CPA 安全的加密体制的构造

图 3 中所示的是 Kyber 在 NIST 后量子密码算法征集中提交的第 1 轮算法设计,采用的是 2 轮压缩的构造方式,即对 $\boldsymbol{Y}_1$ 和 $(\boldsymbol{Y}_2,V)$ 同时进行压缩.在 NIST 第 2 轮中,为了保证可证明安全,Kyber 推荐的构造改为单次压缩,即取消了对公钥 $\boldsymbol{Y}_1$ 的压缩.值得注意的是,图 3 中使用的明文嵌入方式为 $\left\lfloor\frac{q}{m}\right\rceil K_2$.我们称这种明文嵌入方式为明文外嵌入.与之对应的,明文内嵌入的方式为 $\left\lfloor\frac{q}{m}K_2\right\rceil$.当 $m=2$ 时,容易验证这 2 种嵌入方式等价.

Saber 选择的参数与 AKCN-MLWR 一样均为 2 的方幂.注意到对于这种参数选择,对任意的 $x\in\mathbb{Z}_q$,我们有:

$$\left\lfloor\frac{p}{q}x\right\rceil=\left\lfloor\frac{p}{q}\left(x+\frac{q}{2p}\right)\right\rfloor.$$

若假设 $q=2^{\varepsilon_q}$,$p=2^{\varepsilon_p}$,$g=2^{\varepsilon_g}$ 和 $m=2^{\varepsilon_m}$ 满足条件 $\varepsilon_m\leqslant\varepsilon_g<\varepsilon_p<\varepsilon_q$(这里 g 相当于 Saber Round 2 提案里的参数 T,与 Saber Round 1 提案中的参数 t 的关系为 $g=T=2t$),那么可以将 Saber Round 2

提案中采用的 IND-CPA 安全的加密体制改写为如图 4 的形式.其中,h_1 为系数取 $2^{\varepsilon_q-\varepsilon_p-1}=\frac{q}{2p}$ 的常值多项式,h_2 为系数取 $2^{\varepsilon_p-\varepsilon_m-1}-2^{\varepsilon_p-\varepsilon_g-1}+2^{\varepsilon_q-\varepsilon_p-1}$ 的常值多项式.

需要特别说明的是,基于非对称密钥共识机制的 AKCN-MLWE/MLWR 的算法描述是对于一般性 m 的.而在 Kyber 和 Saber 方案的实际描述是针对特定 $m=2$ 这种情况.实际上,针对多比特 $m>2$ 的密钥共识机制和密钥封装机制最早在文献[16-17]中被明确提出,并详细给出了参数 (q,m,g,d) 之间必须遵循的不等式界.

3 共识机制形式下加密体制对比分析

本节我们把基于 LWE/LWR 问题的加密体制以及文献[16-17]中提出的利用共识机制设计的加密体制进行格式上的统一,并在理论上分析二者的差异.

3.1 LWE 加密体制转换为共识机制加密体制

根据 2.5 节,我们很容易将 LWE/LWR 形式的 IND-CPA 安全的加密体制转换为 2.4 节中共识机制形式的加密体制.对应地,图 3 中 LWE 形式的加密体制所采用的非对称的密钥共识算法 (Con,Rec) 为

$$\begin{cases} Con(\Sigma_2,K_2):=V=\\ \quad\left\lfloor\frac{g}{q}\left(\Sigma_2+\left\lfloor\frac{q}{m}K_2\right\rceil\right)\right\rceil \bmod g,\\ Rec(\Sigma_1,V):=K_1=\\ \quad\left\lfloor\frac{m}{q}\left(\left\lfloor\frac{q}{g}V\right\rceil-\Sigma_1\right)\right\rceil \bmod m, \end{cases} \tag{2}$$

这里我们采用明文内嵌入.当 $g\mid q$ 时,LWE 形式的加密算法转换的非对称密钥共识算法与 AKCN-MLWE 采用的完全一致.但是对于一般的 g 和 q,二者并不相同.使用类似文献[16-17]中的证明方法,我们可以得到如下引理.

引理 1. 记 $params=(q,m,g,d)$,则对于图 3 中 LWE 形式加密算法转换的非对称密钥共识算法 (Con,Rec),当参数满足条件 $(2d+2)m<q\left(1-\frac{m}{g}\right)$ 时,共识算法满足正确性要求.

证明. 根据定义,存在 $\theta\in\mathbb{Z}$ 和 $\varepsilon_1,\varepsilon_2\in\left(-\frac{1}{2},\frac{1}{2}\right]$,使得 $V=\frac{g}{q}\left(\Sigma_2+\frac{q}{m}K_2+\varepsilon_1\right)+\varepsilon_2+\theta g$.

带入 K_1 的表达式计算可得:

$$K_1=\left\lfloor\frac{m}{q}\left(\left\lfloor\Sigma_2+\frac{q}{m}K_2+\varepsilon_1+\frac{q}{g}\varepsilon_2\right\rceil-\Sigma_1\right)\right\rceil \bmod m.$$

所以,存在 $\varepsilon_3\in\left(-\frac{1}{2},\frac{1}{2}\right]$ 使得:

$$K_1=\left\lfloor K_2+\frac{m}{q}(\Sigma_2-\Sigma_1)+\frac{m}{q}(\varepsilon_1+\varepsilon_3)+\frac{m}{g}\varepsilon_2\right\rceil \bmod m.$$

根据假设,存在 $\theta'\in\mathbb{Z}$ 和 $\delta\in[-d,d]$ 使得 $\Sigma_2=\Sigma_1+\theta' q+\delta$.所以,我们可以推出:

$$K_1=\left\lfloor K_2+\frac{m}{q}\delta+\frac{m}{q}(\varepsilon_1+\varepsilon_3)+\frac{m}{g}\varepsilon_2\right\rceil \bmod m.$$

要满足正确性,则只需满足关系式:

$$\left|\frac{m}{q}\delta+\frac{m}{q}(\varepsilon_1+\varepsilon_3)+\frac{m}{g}\varepsilon_2\right|\leqslant\frac{md}{q}+\frac{m}{q}+\frac{m}{2g}<\frac{1}{2}$$

即可.整理即得,$(2d+2)m<q\left(1-\frac{m}{g}\right)$. 证毕.

当统一成共识形式的加密体制时,可以看出 AKCN-MLWE 采用的共识算法要比 Kyber 等采用的 LWE 加密形式转换而来的共识算法要好一些.但是二者非常的接近.注意到图 1 中基于共识算法设计的加密体制的误差的取值均为整数,所以尽管从数学上看,AKCN-MLWE 采用的非对称密钥共识机制要优于 Kyber 等采用的 LWE 加密形式转换而来的非对称密钥共识机制,但是对于某些参数来说,根据参数满足的关系式计算而来的 d 的上界的差别可能在 1 以内.这就使得这 2 种形式最后计算的错误率可能相同.

3.2 LWR 加密体制转换为共识机制加密体制

下面我们来分析基于 MLWR 问题的 Saber 加密体制采用的共识算法.我们令 $\Sigma_1'=\Sigma_1+h_1$,$\Sigma_2'=\Sigma_2+h_1$,则由图 4 的构造以及常值多项式 h_1 和 h_2 的取值易知,Saber 采用的共识算法为

$$\begin{cases} Con(\Sigma_2',K_2):=V=\\ \quad\left\lfloor\frac{g}{p}\left(\Sigma_2'-\frac{p}{m}K_2\right)\right\rfloor \bmod g,\\ Rec(\Sigma_1',V):=K_1=\\ \quad\left\lfloor\frac{m}{p}\left(\Sigma_1'-\frac{p}{g}V-\frac{p}{2g}\right)\right\rfloor \bmod m. \end{cases} \tag{3}$$

由于现在参数都是 2 的幂,我们可以使用更简单的方法推出引理 2.

引理 2. 记 $params=(p,m,g,d)$,其中 $p=2^{\varepsilon_p}$,$g=2^{\varepsilon_g}$ 和 $m=2^{\varepsilon_m}$ 满足条件 $\varepsilon_m\leqslant\varepsilon_g<\varepsilon_p$,则对

于图 4 中 Saber 采用的加密算法转换的非对称密钥共识算法(Con,Rec),当参数满足条件 $2dm\leqslant p\left(1-\frac{m}{g}\right)$时,共识算法满足正确性要求.

证明. 根据定义和参数选择,我们有:

$$2^{\varepsilon_p-\varepsilon_g}V=\Sigma'_2-2^{\varepsilon_p-\varepsilon_m}K_2-\varepsilon_V,$$

其中,$\varepsilon_V\in[0,2^{\varepsilon_p-\varepsilon_g}-1]\cap\mathbb{Z}$.所以,我们可以推出:

$$\left\lfloor\frac{m}{p}\left(\Sigma'_1-\frac{p}{g}V-\frac{p}{2g}\right)\right\rceil=\left\lfloor K_2+\frac{m}{p}\left(\Sigma'_1-\Sigma'_2+\varepsilon_V-\frac{p}{2g}\right)\right\rceil,$$

其中,$\varepsilon_V-\frac{p}{2g}\in\left[-\frac{p}{2g},\frac{p}{2g}-1\right]\cap\mathbb{Z}$.当:

$$-\frac{p}{2m}\leqslant\left\|\Sigma'_1-\Sigma'_2+\varepsilon_V-\frac{p}{2g}\right\|_\infty^{\pm}<\frac{p}{2m}$$

时,$K_1=K_2$ 成立.因为,$\Sigma'_1-\Sigma'_2=\Sigma_1-\Sigma_2$.所以,当 $\Sigma_1-\Sigma_2$ 的系数均落在区间

$$\left[-\frac{p}{2m}+\frac{p}{2g},\frac{p}{2m}-\frac{p}{2g}\right]\cap\mathbb{Z}\tag{4}$$

时,有 $K_1=K_2$.这等价于

$$2md\leqslant p\left(1-\frac{m}{g}\right).$$

证毕.

需要指出的是,文献[16-17]在推导 AKCN-MLWR 对应参数条件下共识机制式(1)所满足的界时采用了一些近似(采用的推导方法与一般参数的推导方法类似).当使用类似引理 2 的证明方法来推导共识机制式(1)所满足的正确性条件时,可以得到当 $\Sigma_1-\Sigma_2$ 的系数均落在区间

$$\left[-\frac{p}{2m}+\frac{p}{2g}+1,\frac{p}{2m}-\frac{p}{2g}+1\right]\cap\mathbb{Z}$$

时,$K_1=K_2$ 成立.对比式(4)可知,当统一成共识机制形式的加密体制时,AKCN-MLWR 与 Saber 采用的共识机制参数所满足的正确性条件相差很小.

同样需要指出的是,采用共识机制形式估计的错误率(即错误率采用 $\|\Sigma_1-\Sigma_2\|_\infty>d$ 的概率)会比密码体制的实际错误率偏高.这是因为当 $\|\Sigma_1-\Sigma_2\|_\infty\leqslant d$ 时,由共识机制的正确性可以保证一定有 $K_1=K_2$ 成立.但是由于推导共识机制参数应满足的不等式时采用了放缩(如引理 1 中的 ε_1,ε_2 和 ε_3 以及引理 2 中的 $\varepsilon_V-\frac{p}{2g}$),这就使得即使 $\|\Sigma_1-\Sigma_2\|_\infty>d$,仍有一定的概率使得 $K_1=K_2$ 成立.所以对于一个具体的密码体制,我们将在下面第 4 节探讨其错误率更精确的计算方式.

4　基于 MLWE 的 KEM 错误率比较分析

本节系统比较分析基于 MLWE 的密钥封装机制在不同压缩函数和加解密方式下的错误率差异.3.2 节提到 AKCN-MLWE/MLWR 如果直接利用 AKCN 的正确性条件分析得到错误率会比其实际的错误率略高,为了更精确地分析 AKCN-MLWE/MLWR 的具体错误率,我们将其转换为传统 LWE/LWR 加密体制的形式然后进行错误率分析.事实上,这就是将 AKCN 采用的非对称密钥共识算法(Con,Rec)简单展开的过程.

对比图 1 和图 3 容易看出,AKCN-MLWE 与 Kyber 等加密体制的差别仅体现在解密算法上.即 AKCN-MLWE 非对称密钥共识机制转换的 LWE 形式加密体制的解密算法是先计算 $\Sigma_1=\boldsymbol{X}_1^{\mathrm{T}}Decompress_c(\boldsymbol{Y}_2)$,随后再计算解密明文 $K_1=\left\lfloor\frac{m}{g}V-\frac{m}{q}\Sigma_1\right\rceil\bmod m$.注意到:

$$\frac{m}{g}V-\frac{m}{q}\Sigma_1=\frac{m}{q}\left(\frac{q}{g}V-\Sigma_1\right),$$

所以与 Kyber 以及 Aigis 等使用的传统的 LWE 形式的加密体制相比,AKCN-MLWE 非对称密钥共识机制转换的 LWE 形式加密体制的解密算法相当于未对第 2 个密文 V 完全解封装,节省了 1 步四舍五入运算.特别地,实际测试表明,多加 1 步四舍五入运算不仅增加了计算量,也相当于增加了额外的误差,从而会造成错误率偏高.

我们记 $\boldsymbol{Y}'_1=\boldsymbol{A}\boldsymbol{X}_1+\boldsymbol{E}_1$,$\boldsymbol{Y}'_2=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_2+\boldsymbol{E}_2$,$Z=\Sigma_2+\left\lfloor\frac{q}{m}\right\rceil K_2$ 并记:

$$\boldsymbol{\varepsilon}_1=\boldsymbol{Y}'_1-Decompress_k(Compress_k(\boldsymbol{Y}'_1)),$$
$$\boldsymbol{\varepsilon}_2=\boldsymbol{Y}'_2-Decompress_c(Compress_c(\boldsymbol{Y}'_2)),$$
$$\varepsilon_v=Z-\left\lfloor\frac{q}{g}\left\lfloor\frac{g}{q}Z\right\rceil\right\rceil,$$

则图 3 所示 LWE 形式加密体制的解密计算中,有:

$$\left\lfloor\frac{q}{g}V\right\rceil-\Sigma_1=\left\lfloor\frac{q}{m}\right\rceil K_2+Err,$$

其中,

$$Err=(\boldsymbol{E}_1-\boldsymbol{\varepsilon}_1)^{\mathrm{T}}\boldsymbol{X}_2-\boldsymbol{X}_1{}^{\mathrm{T}}(\boldsymbol{E}_2-\boldsymbol{\varepsilon}_2)+E_\sigma-\varepsilon_v\tag{5}$$

为误差.所以,我们令 $\varepsilon'=\frac{q}{m}-\left\lfloor\frac{q}{m}\right\rceil$,则当:

$$-\frac{1}{2}\leqslant\left\|\frac{m}{q}(Err-\varepsilon' K_2)\right\|_\infty^{\pm}<\frac{1}{2}$$

时,解密算法可以正确解密.等价地,对任意的 $K_2\in\mathbb{Z}_m^n$,正确解密的条件为

$$\begin{cases}-\dfrac{q}{2m}+\varepsilon'(m-1)\leqslant\|Err\|_\infty^{\pm}<\dfrac{q}{2m},\ \varepsilon'\geqslant 0,\\ -\dfrac{q}{2m}\leqslant\|Err\|_\infty^{\pm}<\dfrac{q}{2m}+\varepsilon'(m-1),\ \varepsilon'<0.\end{cases}\tag{6}$$

在判定版本的模 LWE 问题的假设下,我们可以认为 $\boldsymbol{Y}_1'$,$\boldsymbol{Y}_2'$ 和 Z 的系数独立地服从 $\mathbb{Z}_q$ 上的均匀分布.至此,我们可以使用程序来计算某一组具体参数对应的解密错误率.

当图 3 的构造采用明文内嵌入的方式设计时,记 $\varepsilon''=\dfrac{q}{m}K_2-\left\lfloor\dfrac{q}{m}K_2\right\rceil$,则对任意的 $K_2\in\mathbb{Z}_m^n$,此时正确解密的条件为

$$-\frac{q}{2m}+\max_{K_2}\varepsilon''\leqslant\|Err\|_\infty<\frac{q}{2m}+\min_{K_2}\varepsilon''.\tag{7}$$

与式(6)相比,对于绝大部分参数(特别是 m 比较大时),明文内嵌入的方式带来的错误率会更小.但是当 m 比较小时,这 2 种嵌入方式对应的错误率大小需要视具体参数的选择而定.

对于 AKCN-MLWE 对应的情况,我们采用上述符号并记:

$$\varepsilon_v'=Z-\frac{q}{g}\left\lfloor\frac{g}{q}Z\right\rceil,$$

则计算可得:

$$Err=(\boldsymbol{E}_1-\boldsymbol{\varepsilon}_1)^{\mathrm{T}}\boldsymbol{X}_2-\boldsymbol{X}_1{}^{\mathrm{T}}(\boldsymbol{E}_2-\boldsymbol{\varepsilon}_2)+E_\sigma-\varepsilon_v'.$$

此时,采用明文外嵌入和明文内嵌入 2 种方式对应的错误率同样可以结合关系式(6)(7)通过程序计算给出.

采用 Kyber 提交的在 NIST 前 2 轮竞选中提交的推荐参数,我们测试的错误率结果如表 1 所示:

Table 1 Error Rates of Kyber Recommended Parameters

表 1 Kyber 推荐参数的错误率

Parameters	Kyber-512-1	Kyber-768-1	Kyber-1024-1	Kyber-512-2	Kyber-768-2	Kyber-1024-2
n	256	256	256	256	256	256
m	2	2	2	2	2	2
l	2	3	4	2	3	4
q	7 681	7 681	7 681	3 329	3 329	3 329
η	5	4	3	2	2	2
d	11	11	11	10	10	11
t	2	2	2	2	2	1
g	2^3	2^3	2^3	2^3	2^4	2^5
δ_1	$2^{-145.2}$	$2^{-142.7}$	$2^{-169.0}$	$2^{-178.6}$	$2^{-165.0}$	$2^{-174.9}$
δ_2	$2^{-139.7}$	$2^{-136.3}$	$2^{-160.2}$	$2^{-150.8}$	$2^{-138.7}$	$2^{-167.1}$
δ_3	$2^{-138.1}$	$2^{-135.7}$	$2^{-161.7}$	$2^{-171.1}$	$2^{-158.8}$	$2^{-169.8}$
δ_4	$2^{-148.1}$	$2^{-145.6}$	$2^{-171.9}$	$2^{-181.4}$	$2^{-168.8}$	$2^{-179.7}$
δ_5	$2^{-142.6}$	$2^{-139.3}$	$2^{-163.1}$	$2^{-153.7}$	$2^{-142.5}$	$2^{-171.9}$
δ_6	$2^{-138.1}$	$2^{-135.7}$	$2^{-161.7}$	$2^{-171.1}$	$2^{-158.8}$	$2^{-169.8}$

Kyber Round 1 采用的是对称形式的判定版本的模 LWE 假设且对公钥和第 1 个密文采用相同的压缩函数,所以表 1 中取 $\eta=\eta_k=\eta_e$,$d=d_k=d_c$,$t=t_k=t_c$,其中 d_k 表示公钥压缩后的比特长度,t_k 表示公钥压缩的比特数,d_c 表示第 1 个密文压缩后的比特长度.t_c 表示第 1 个密文压缩的比特数(所以,$d=\lceil\mathrm{lb}\,q\rceil-t$).表 1 中的 Kyber-512-1 表示对应的参数为 Kyber 在 NIST 第 1 轮的推荐参数 Kyber-512,其余类似符号表示的意思以此类推.Kyber Round 2 未对公钥压缩,所以相当于 $t_k=0$,$d_k=\lceil\mathrm{lb}\,q\rceil$.

不同情况的错误率我们使用 $\{\delta_i\}_{i=1}^6$ 来表示.其中,δ_1 为原始 LWE 形式加密体制采用换模压缩函数最后测得的错误率;δ_2 为原始 LWE 形式加密体制采用砍比特压缩函数最后测得的错误率;δ_3 为原始 LWE 形式加密体制转换为 3.1 节中的非对称密钥共识算法再采用图 1 所示共识形式加密最后测得的错误率,压缩函数使用的是换模压缩函数;δ_4 为

AKCN 使用的共识算法转换为传统 LWE 形式的加密体制并使用换模压缩函数最后测得的错误率;δ_5 为 AKCN 使用的共识算法转换为传统 LWE 形式的加密体制并使用砍比特压缩函数最后测得的错误率;δ_6 为使用 AKCN 的非对称密钥共识算法采用图 1 所示共识形式加密最后测得的错误率,压缩函数使用的是换模压缩函数.

针对表 1 的测试数据,我们给出 4 方面的讨论.

1) 当采用的加密方式相同时,使用换模压缩函数造成的错误率要低于使用砍比特压缩函数造成的错误率.由 2.2 节的分析,当 $d=\lceil \mathrm{lb}q \rceil - t$ 时,我们有 $\left\lfloor \frac{q}{2^{d+1}} \right\rceil \leqslant 2^{t-1}$.也就是说,使用换模压缩造成的误差的绝对值上界不超过使用砍比特压缩造成的误差的绝对值上界.事实上,对于素数 q,采用换模压缩造成的误差的概率分布在除去 2 个端点值 $\pm\left\lfloor \frac{q}{2^{d+1}} \right\rceil$ 之外的值上均匀分布,并且取值为端点值的概率比较小.而砍比特压缩造成的误差的概率分布几乎是 $[-2^{t-1}, 2^{t-1}) \cap \mathbb{Z}$ 上的均匀分布(取 0 的概率稍高).考虑到误差要累加较多次,并且最后计算错误率时基本上是计算 $\|Err\|_\infty$ 超过某临界值的概率,所以当采用的加密方式相同时,换模压缩函数引起的错误率会较低(但是,换模压缩的计算代价也同样高于简单的砍比特压缩).

2) 当选择同样的参数并且采用相同的压缩函数时,LWE 加密形式测得的误差会比共识形式测得的误差小.这是因为采用 3.1 节的共识机制式(2)并使用图 1 的加密形式来计算错误率时,相当于计算 $\|\Sigma_2-\Sigma_1\|_\infty \geqslant d$ 的概率,其中

$$\Sigma_2-\Sigma_1=(\boldsymbol{E}_1-\boldsymbol{\varepsilon}_1)^{\mathrm{T}}\boldsymbol{X}_2-\boldsymbol{X}_1{}^{\mathrm{T}}(\boldsymbol{E}_2-\boldsymbol{\varepsilon}_2)+E_\sigma. \tag{8}$$

对比误差表达式(5)可以看出二者仅仅相差一个 ε_v,即 $Err_{\mathrm{LWE}}=Err_{\mathrm{AKC}}-\varepsilon_v$.考虑 $m=2$ 的情况,在计算错误率时,LWE 加密形式的错误率约为 $Pr\left(\|Err_{\mathrm{LWE}}\|_\infty \geqslant \frac{q}{4}\right)$. 非对称密钥共识形式计算的错误率约为 $Pr\left(\|Err_{\mathrm{AKC}}\|_\infty \geqslant B \approx \frac{q}{4}\left(1-\frac{m}{g}\right)\right)$. 非对称密钥共识算法的正确性保证了 $\|Err_{\mathrm{AKC}}\|_\infty < B$ 时,一定可以正确解密.由于我们在推导共识机制参数应满足的关系式时使用了放缩,即相当于把 Err_{LWE} 的概率分成了 2 部分,先把 $|\varepsilon_v|$ 取了上界,再来估计余下部分超过 $Pr\left(\frac{q}{4}-|\varepsilon_v|\right)$. 但是,对于一组固定的参数,$\varepsilon_v$ 也是一个概率分布.也就是说,当 $\|Err_{\mathrm{AKC}}\|_\infty \geqslant B$ 时,基于非对称密钥共识算法设计的加密体制也有一定的概率正确解密.因此,采用共识形式测试得到的错误率会高一些.我们以 Kyber 在 NIST 第 1 轮给出的推荐参数 Kyber-768 为例进一步说明.针对这一组参数,LWE 加密形式的错误率约为 $Pr(\|Err_{\mathrm{LWE}}\|_\infty \geqslant 1\,920)$.非对称密钥共识形式计算的错误率约为 $Pr(\|Err_{\mathrm{AKC}}\|_\infty \geqslant 1\,440)$.而分布列 ε_v 的取值在 $[-480,480] \cap \mathbb{Z}$ 中.此时,采用共识形式来计算误差即相当于先取 $|\varepsilon_v|=480$,再来计算 Err_{LWE} 中余下的 Err_{AKC} 部分大于 $1\,920-480=1\,440$ 的概率.值得指出的是,这个差异仅仅是计算错误率的不同方式或放缩的力度造成的,与密码体制无关.本文的一个特别的贡献是给出了 AKCN-MLWE 的更为精确的错误率分析方法.

3) 对比 δ_3 和 δ_6,我们发现虽然 3.1 节的理论分析表明 AKCN 采用的非对称密钥共识机制要优于传统 LWE 加密形式转换而来的非对称密钥共识机制,但是二者计算的错误率相同.对于 Kyber 提交 NIST 的这 2 轮参数,错误率相同的原因如我们在 3.1 节末尾所述.对于这些参数,根据非对称密钥共识算法的参数应满足的关系式计算而来的 d 的上界的差别在 1 以内.我们仍以 Kyber NIST Round 1 给出的推荐参数 Kyber-768 为例进行说明.此时,$q=7\,681$,$g=8$,$m=2$.容易计算得,传统 LWE 加密形式转换而来的非对称密钥共识机制要求上界为 $d<1\,439.187\,5$;而 AKCN-MLWE 采用的非对称密钥共识机制要求的上界为 $d<1\,439.687\,5$.由于对应的误差取值为整数,所以这 2 种情况计算的错误率都是 $Pr(\|Err_{\mathrm{AKC}}\|_\infty \geqslant 1\,440)$.因而最后计算的错误率相同.

4) 对于固定的一组参数,当采用相同的压缩函数时,AKCN-MLWE 使用的非对称密钥共识算法转换而来的 LWE 加密形式的密码体制的错误率更低(如对比 δ_1 和 δ_4,或 δ_2 和 δ_5).这说明正如本节一开始指出的,对第 2 个密文 V 不进行完全解封装不仅能节省 1 步四舍五入运算,还可以降低错误率.这也从一个侧面表明了确实如 3.1 节分析,AKCN-MLWE 采用的非对称密钥共识机制更优(注意到我们并没有对 $\boldsymbol{Y}_1$ 和 $\boldsymbol{Y}_2$ 也进行类似的操作.这是因为我们需要利用 $\boldsymbol{Y}_1$ 和 $\boldsymbol{Y}_2$ 使用 NTT 算法来进行乘法运算.因此,需要将 $\boldsymbol{Y}_1$ 和 $\boldsymbol{Y}_2$ 解压缩为环 R^l 中的元素).

5 基于 MLWR 的 KEM 错误率比较分析

本节对 AKCN-MLWR 与 Saber 的错误率进行对比分析.此时,我们假设参数 $q=2^{\varepsilon_q}$,$p=2^{\varepsilon_p}$,$g=2^{\varepsilon_g}$ 和 $m=2^{\varepsilon_m}$ 满足条件 $\varepsilon_m\leqslant\varepsilon_g<\varepsilon_p<\varepsilon_q$.对比图 2 和图 4 可知,AKCN-LWR 采用共识机制转换的加密和解密分别对应为

$$V=\left\lfloor\frac{g}{p}\left(\Sigma_2+\frac{p}{m}K_2\right)\right\rceil,$$

$$K_1=\left\lfloor\frac{m}{p}\left(\frac{p}{g}V-\Sigma_1\right)\right\rceil.$$

我们有:

$$\frac{p}{g}V=\Sigma_2+\frac{p}{2g}+\frac{p}{m}K_2-\varepsilon_V,$$

其中,$\varepsilon_V\in[0,2^{\varepsilon_p-\varepsilon_g}-1]\cap\mathbb{Z}$.因而,我们可以推出:

$$\frac{m}{p}\left(\frac{p}{g}V-\Sigma_1\right)=K_2+\frac{m}{p}\left(\Sigma_2-\Sigma_1+\frac{p}{2g}-\varepsilon_V\right).$$

所以,正确解密条件为

$$-\frac{p}{2m}\leqslant\left\|\Sigma_2-\Sigma_1+\frac{p}{2g}-\varepsilon_V\right\|_\infty^{\pm}<\frac{p}{2m}.\tag{9}$$

我们采用文献[17]的符号,记 $\{x\}_p=x-\frac{q}{p}\times\left\lfloor\frac{p}{q}x\right\rceil$,则容易计算得:

$$\Sigma_2-\Sigma_1=\frac{p}{q}(\boldsymbol{X}_1^{\mathrm{T}}\{\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_2\}_p-\{\boldsymbol{A}\boldsymbol{X}_1\}_p^{\mathrm{T}}\boldsymbol{X}_2).$$

我们采用目前业界比较通用的假设[15,25-27],即当 $\boldsymbol{A}$ 均匀选择时,假设 $\{\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_2\}_p$ 或 $\{\boldsymbol{A}\boldsymbol{X}_1\}_p^{\mathrm{T}}$ 的系数为区间 $\left[-\frac{q}{2p},\frac{q}{2p}\right)\cap\mathbb{Z}$ 上的均匀分布.但是,由于 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_2$ 和 $\boldsymbol{A}\boldsymbol{X}_1$ 这 2 个量有一定的相关性,我们可以采用与文献[17]中的引理 1 和定理 7 类似的方法证明,对于某固定的 $a\in R_{\frac{q}{p}}$,在条件

$$\boldsymbol{X}_1^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_2=a\ \bmod\frac{q}{p}$$

成立的情况下,变量 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_2$ 和 $\boldsymbol{A}\boldsymbol{X}_1$ 相互独立.我们也近似地认为 ε_V 服从 $[0,2^{\varepsilon_p-\varepsilon_g}-1]\cap\mathbb{Z}$ 上的均匀分布.因而,$\frac{p}{2g}-\varepsilon_V$ 服从 $\left(-\frac{p}{2g},\frac{p}{2g}\right]\cap\mathbb{Z}$ 上的均匀分布.在不等式(9)两边同时乘以 $\frac{q}{p}$,并记 $\varepsilon_V'=\frac{q}{p}\times\left(\frac{p}{2g}-\varepsilon_V\right)$,则可以推出正确解密的条件为

$$-\frac{q}{2m}\leqslant\|\boldsymbol{X}_1^{\mathrm{T}}\{\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_2\}_p-\{\boldsymbol{A}\boldsymbol{X}_1\}_p^{\mathrm{T}}\boldsymbol{X}_2+\varepsilon_V'\|_\infty^{\pm}<\frac{q}{2m},$$

其中 ε_V' 服从分布 $\frac{q}{p}U\left(\mathbb{Z}\cap\left[-\frac{p}{2g},\frac{p}{2g}\right)\right)$.至此,我们可以通过程序测试 AKCN-MLWR 更精确的解密错误率.

采用完全类似的方法,我们也可以计算图 4 所示 Saber 加密体制的解密错误率.我们取 $\Sigma_1'=\Sigma_1+h_1$,$\Sigma_2'=\Sigma_2+h_1$,则计算可得 $\Sigma_1-2^{\varepsilon_p-\varepsilon_g}V+h_2=\frac{p}{m}K_2+\Sigma_1'-\Sigma_2'+\varepsilon_V-\frac{p}{2g}+\frac{p}{2m}$.所以,Saber 正确解密的条件为

$$-\frac{p}{2m}\leqslant\left\|\Sigma_1'-\Sigma_2'+\varepsilon_V-\frac{p}{2g}\right\|_\infty^{\pm}<\frac{p}{2m}.$$

注意到 $\Sigma_1'-\Sigma_2'=\Sigma_1-\Sigma_2$,我们也可以推出 Saber 正确解密的等价条件为

$$-\frac{q}{2m}\leqslant\|\{\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_1\}_p^{\mathrm{T}}\boldsymbol{X}_2-\boldsymbol{X}_1^{\mathrm{T}}\{\boldsymbol{A}\boldsymbol{X}_2\}_p-\varepsilon_V'\|_\infty^{\pm}<\frac{q}{2m}.$$

可以看出,Saber 与 AKCN-MLWR 的错误率计算的区别仅仅差在端点 $\pm\frac{q}{2m}$ 上.

由于实际应用中的误差分布一般取 $\pm\frac{q}{2m}$ 的概率相同,所以 Saber 与 AKCN-MLWR 没有本质上的差别.

6 基于模 LWE/LWR 混合模式的 KEM 错误率分析

我们称文献[17]中使用非对称密钥共识机制同时结合模 LWE 和模 LWR 问题来设计 CPA 安全的加密体制的方法为 AKCN-Hybrid,其具体构造如图 5 所示,其中的参数以及(Con,Rec)算法与第 5 节类似.

需要指出的是,在文献[17]的构造中,图 5 中的 $\Sigma_2=\left\lfloor\frac{p}{q}\boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{X}_2\right\rceil$.这样的设置对于密码体制的参数没有额外的限制,可以直接基于相应的 LWE 问题和 LWR 问题来证明对应方案的 IND-CPA 安全性,即文献[17]中的构造具有更广的普适性.而在本节的讨论中,为了充分利用存储空间,我们默认设置的参数满足条件 $m\mid g\mid p$,并且均为 2 的方幂.在这种特殊情况下,我们可以直接利用 Con 算法中的四舍五入来证明对应体制的安全性.NIST 第 1 轮的竞选

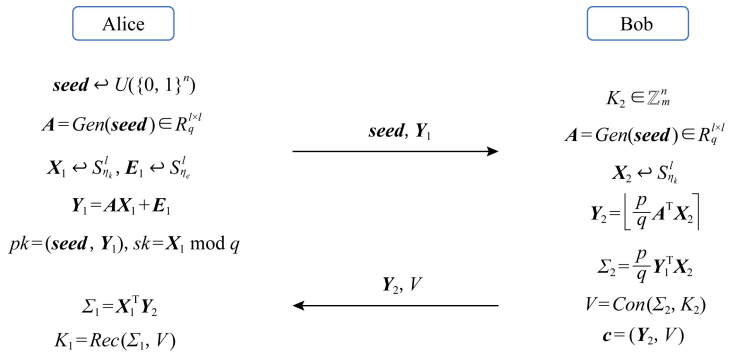

Fig. 5　IND-CPA secure encryption schemes based on Module LWE/LWR

图 5　同时基于模 LWE/LWR 问题设计的 IND-CPA 安全的加密体制的构造

算法 Lizard/RLizard(分别基于欧式格 LWE/LWR 问题和环 LWE/LWR 问题)的构造方式与此类简化的 AKCN-Hybrid 的构造类似.

此时,我们有:

$$V=\left\lfloor \frac{g}{q}\boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{X}_2 \right\rceil+\frac{g}{m}K_2 \bmod g.$$

记

$$\varepsilon'_v=\boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{X}_2-\frac{q}{g}\left\lfloor \frac{g}{q}\boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{X}_2 \right\rceil,$$

则有

$$m\left(\frac{V}{g}-\frac{\Sigma_1}{p}\right)=K_2+\frac{m}{q}(\boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{X}_2-\varepsilon'_v)-\frac{m}{p}\boldsymbol{X}_1^{\mathrm{T}}\boldsymbol{Y}_2=$$

$$K_2+\frac{m}{q}(\boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{X}_2-\varepsilon'_v-\frac{q}{p}\boldsymbol{X}_1^{\mathrm{T}}\boldsymbol{Y}_2).$$

所以,当

$$-\frac{q}{2m}\leqslant\boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{X}_2-\frac{q}{p}\boldsymbol{X}_1^{\mathrm{T}}\boldsymbol{Y}_2-\varepsilon'_v<\frac{q}{2m}$$

时,可以正确解密.我们采用前面各节的符号,容易计算得到:

$$\boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{X}_2-\frac{q}{p}\boldsymbol{X}_1^{\mathrm{T}}\boldsymbol{Y}_2=\boldsymbol{E}_1^{\mathrm{T}}\boldsymbol{X}_2+\boldsymbol{X}_1^{\mathrm{T}}\{\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}_2\}_p.$$

至此,我们可以利用类似第 5 节中 AKCN-MLWR 的假设或 RLizard[25] 的假设和处理方法使用程序来计算 AKCN-Hybrid 的错误率.

7　封装 512 b 的 EKM 方案对比分析

由于量子搜索算法(Grove 算法)的存在,理论上来讲 2λ 比特长的密钥最多只能提供 λ 比特的安全强度.从这个角度来看,为了实现大约 256 b 的量子安全强度,我们需考虑会话密钥长度约 512 b 的 KEM 方案的设计.这对应着 Kyber-1024 和 Fire-Saber 这 2 组参数.此外,目前的 TLS1.3 标准也强制要求提供 512 b 会话密钥的握手协商机制[22],因此提供 512 b 的会话密钥也是现实的需求.

根据前面的分析并为了简化讨论,在本文后续部分讨论错误率时,我们仅使用换模压缩函数和基于 AKCN 共识机制的加解密函数(这是由于我们在本节中需要明确地考虑加密多比特的情况)但采用将 AKCN 共识机制展开成 LWE 加密形式进行更为精确的错误率分析.LWR 形式对应的分析是类似的.首先,如 Aigis 观察到的,由于压缩函数的使用,LWE 误差 $\boldsymbol{E}_i$ 和秘密 $\boldsymbol{X}_i$ 对于最后解密误差 Err 的影响不对等.特别地,当固定 q, d_k, d_t 和 g 时,改变 η_k 对 Err 带来的影响要比改变 η_e 带来的影响大得多.此外,互换 d_k 和 d_t 的值对最后的解密误差几乎无影响.这是因为对于一般的参数,误差 $(\boldsymbol{E}_1-\boldsymbol{\varepsilon}_1)^{\mathrm{T}}\boldsymbol{X}_2-\boldsymbol{X}_1{}^{\mathrm{T}}(\boldsymbol{E}_2-\boldsymbol{\varepsilon}_2)$ 服从的分布与误差 $-(\boldsymbol{E}_1-\boldsymbol{\varepsilon}_1)^{\mathrm{T}}\boldsymbol{X}_2+\boldsymbol{X}_1{}^{\mathrm{T}}(\boldsymbol{E}_2-\boldsymbol{\varepsilon}_2)$ 服从的分布几乎相同.当公钥和第一个密文的压缩尺寸不同时,我们一般采取公钥压缩的比特数目较少(即公钥压缩后的规模大),第 1 个密文压缩的比特数目较多来与 Kyber NIST Round 2 的设计保持相近.

为了达到封装 512 b 会话密钥且不低于 200 b 后量子安全的目的,基于 MLWE 问题,我们主要有 3 种实现方法:1)采用 Kyber NIST 第 2 轮 1024 参数进行 2 次封装,即 $n=256, l=4, m=2$ 封装 2 次;2)采用类似的参数,考虑 $m=4$ 封装 1 次;3)扩大环的扩张次数,即设置 $n=512, l=2, m=2$ 封装 1 次.

我们首先来比较前 2 种方法,使用方法 1 的设置来共享 512 b 会话密钥相当于要用同一个公钥来进行 2 次封装,此时错误率至多为原来 2 倍,总通信带宽为

$$n+nld_k+2(nld_c+n\ \mathrm{lb}\,g).$$

使用方法 2 的设置来共享 512 b 会话密钥只需封装 1 次,但是我们要考虑错误率.共识加密形式下参数应满足的关系式(如引理 1)为我们计算错误率提供了启发式的参考.在误差分布变化不大的情况下,当 m 增加 1 倍时,我们只需要把 q 和 g 均增加 1 倍即可保证错误率变化不大.理想情况下,采用方法 2 的设置的总通信带宽约为 $n+nl(d_k+1)+nl(d_c+1)+n(\mathrm{lb}\,g+1)$.所以,前 2 种方法的总通信带宽的差为

$$\Delta=nl(d_c-2)+n(\mathrm{lb}\,g-1).$$

由于实用中,d_c 和 g 均不会太小,所以方法 1 的总通信带宽一定比方法 2 大.在实用中我们一般选择 q 为满足 NTT 计算条件的素数,且当 q 增大 1 倍左右,g,d_k 和 d_c 增加 1 b 时,误差项中的 ε_v,$\boldsymbol{\varepsilon}_1$ 和 $\boldsymbol{\varepsilon}_2$ 均会发生变化,改变的大小与 q 有关,所以实际应用中不像理想情况分析的那样.但是我们仍可以按照上述分析来大致确定参数再通过具体程序测试来微调确定哪一组参数较优.

我们对比测试 NIST 第 2 轮的 Kyber-1024 这一组参数,结果如表 2 所示:

Table 2 Multi-bits Comparisons of Kyber Round 2

表 2 Kyber 第 2 轮参数多比特测试比较

Parameters	Kyber Round 2 $m=2$, Two Encs	Kyber Round 2 $m=4$, One Enc
n	256	256
m	2	4
l	4	4
q	3 329	7 681
η	2	2
d	11	11
t	1	2
g	2^5	2^7
$\lvert K\rvert$/B	32	32
$\lvert pk\rvert$/B	1 568	1 696
$\lvert ct\rvert$/B	3 136	1 632
B/B	4 704	3 328
sec	230	208
δ_4	$2^{-178.7}$	$2^{-182.9}$

表 2 的符号与表 1 一致,不同的是,$|K|$,$|pk|$,$|ct|$ 和 B 分别表示共享密钥长度、Alice 和 Bob 各自传输信息的带宽以及总通信带宽,单位为 B;sec 表示对应参数的密码体制的量子安全强度.

下面我们来比较方法 2 和 3.首先注意到计算解密错误率是先计算 Err 的一个系数满足相应条件的概率,再乘以 n 取一致界来给出 $\|Err\|_\infty$ 满足相应条件的概率.而当 q,g,d_k,d_t,η_k 和 η_e 固定时,方法 2 和 3 对应的 Err 的系数服从相同的分布.所以,当 m 取值相同时,方法 3 的错误率会比方法 2 的错误率大 1 倍.但是,共识加密形式下参数应满足的关系式告诉我们,当 m 增大 1 倍时,为保持最后计算的错误率相差不大,q 和 g 也要相应地增大 1 倍.此时,为了保证最后解密误差 Err 的变化不大,我们需要将 d_k 和 d_t 也增加 1 b 以保证在 η_k 和 η_e 不变的情况下 $\boldsymbol{\varepsilon}_1$ 和 $\boldsymbol{\varepsilon}_2$ 变化不大.此时,相当于增加了带宽.同时注意到,为保证安全性保持相近,增大 q 很可能也意味着要适当增大 η_k 和 η_e(即大约要保持 $\frac{\eta}{q}$ 相近.当然由于实际应用中 q 可能不是严格增大 1 倍,所以保持 η 不变也有可能使得安全强度变换不太大.具体情况视具体参数的选择而定).因此,虽然对于一些特定的参数选择,可能适当调整安全强度和错误率能够使得方法 2 采用的方式节省一定的带宽,但是对于绝大多数的参数设置而言,方法 2 采用的方式很难同时兼顾错误率、安全性和通信带宽.

综上所述,对于绝大多数的参数设置而言,方法 3 采用的设置可以更好地平衡错误率、安全强度与通信带宽.但对应的缺点是:在具体实现时需要修改一些算法,在算法兼容性和适配性上不如方法 2.

8 优化的 KEM 方案和参数推荐

根据本文针对基于模格的 KEM 方案系统性的比较分析,在本节中我们给出基于模格 KEM 的方案优化,并通过大量的测试给出新的参数推荐.

针对基于 MLWE 的 KEM 方案,在相同的参数选择下,本文的比较分析得出如下结论:同时采用基于 AKCN-MLWE 共识机制的加解密过程和换模压缩函数是更优的组合.首先,基于 AKCN-MLWE 共识机制的加解密过程更为简单高效,同时本文的具体错误率分析方法(即错误率不采用 AKCN-MLWE 原始共识机制的正确性条件进行粗略计算,而是进行更为精确的具体分析)也表明基于 AKCN-MLWE 共识机制的加解密算法具有更低的错误率.其次,虽然换模压缩函数相对于砍比特压缩函数要复杂,但是对应的会带来更低的错误率,同时也可以更好地与 Kyber 和 Aigis 进行兼容.

相对于原始的 AKCN-MLWE,本节优化的

AKCN-MLWE 方案仅更换了其压缩函数;相对于 Kyber 和 Aigis,本节优化的 AKCN-MLWE 可以视作仅对其解密算法做了优化(更简单且错误率更低),而密钥生成和加密算法仍然和原始的 Kyber 和 Aigis 方案保持一样.这样,优化后的 AKCN-MLWE 方案可以取得与 Kyber 和 Aigis 方案最大程度的兼容和适配.在后文的描述中,AKCN-MLWE 方案默认是这种优化的方案.另外,和 Kyber 的 NIST 第 2 轮提案一样,从保证可证明安全性的角度,我们也默认 AKCN-MLWE 不对公钥的 $\boldsymbol{Y}_1$ 进行压缩.但是 Aigis 采用的是类似 Kyber 在 NIST 第 1 轮中采用的 2 轮压缩的构造方式,所以表 5 中为保持一致,AKCN-Aigis 同样也采用 2 轮压缩的构造方式.

为了表述方便,后文我们记 AKCN-Kyber 为将 NIST 第 2 轮的 Kyber 加密方案的解密过程换成 AKCN-MLWE 共识形式转换的解密形式;同样地,AKCN-Aigis 表示将 Aigis 加密方案的解密过程换成 AKCN-MLWE 共识形式转换的解密形式.

AKCN-MLWE 与 AKCN-MLWR 的新参数推荐如表 3 和表 4 所示,采用的符号与表 1 和表 2 相同.对于 AKCN-MLWE-1024 这组参数,目标是封装 512 b 的密钥,我们分别给出了 2 种方式下的具体参数:AKCN-MLWE-1024-1 是 $n=256$ 和 $m=4$,从而具有更好的兼容和适配性;AKCN-MLWE-1024-2 采用 $n=512$ 和 $m=2$,具有更优良的带宽性能.

Table 3　New Parameters of AKCN-MLWE

表 3　AKCN-MLWE 新参数

Parameters	AKCN-MLWE-512	AKCN-MLWE-768	AKCN-MLWE-1024-1	AKCN-MLWE-1024-2
n	256	256	256	512
m	2	2	4	2
l	2	3	4	2
q	3 329	3 329	3 329	3 329
η	1	1	1	1
d	8	9	11	9
t	4	3	1	3
g	2^3	2^3	2^7	2^4
$\lvert K\rvert$/B	32	32	64	64
$\lvert pk\rvert$/B	800	1 184	1 568	1 600
$\lvert ct\rvert$/B	608	960	1 632	1 408
B/B	1 408	2 144	3 200	3 008
sec	91	149	210	210
δ_4	$2^{-76.9}$	$2^{-161.4}$	$2^{-168.5}$	$2^{-164.2}$

Table 4　New Parameters of AKCN-MLWR

表 4　AKCN-MLWR 新参数

Parameters	AKCN-MLWR-512	AKCN-MLWR-768	AKCN-MLWR-1024-1	AKCN-MLWR-1024-2
n	256	256	256	512
m	2	2	2	2
l	2	3	4	2
q	2^{12}	2^{12}	2^{12}	2^{12}
p	2^9	2^9	2^{10}	2^{10}
g	2^4	2^4	2^4	2^4
η	2	1	2	2
$\lvert K\rvert$/B	32	32	32	64
$\lvert pk\rvert$/B	608	896	1 312	1 344

Continued (Table 4)

Parameters	AKCN-MLWR-512	AKCN-MLWR-768	AKCN-MLWR-1024-1	AKCN-MLWR-1024-2
$\|ct\|$/B	704	992	1 408	1 536
B/B	1 312	1 888	2 720	2 880
sec	119	179	238	238
δ	$2^{-102.4}$	$2^{-138.3}$	$2^{-187.5}$	$2^{-186.5}$

在表 4～7 中,δ 表示错误率.由于我们想要使用相同的参数 q,当 $q=2^{12}$ 时很难像 AKCN-MLWE-1024-1 一样同时兼顾安全性与错误率,因此 AKCN-MLWR-1024-1 仍然是封装 256 b 的密钥.注意到,由 3.2 节和第 5 节的分析,AKCN-MLWR 的新参数也可以看作是对 Saber NIST Round 2 的 3 组参数的优化推荐.

我们给出的 AKCN-Aigis 的新参数推荐如表 5 所示.表 5 中采用的符号同样与表 1 和表 2 相同.为了便于比较,我们也将 Aigis 的参数列出来.其中,Aigis-512,Aigis-768 和 Aigis-1024 分别对应文献[12]中加密体制推荐参数 Params I,Params II 和 Params III.与 Aigis 推荐的参数相比,AKCN-AIGIS 采用了统一的 $q=7\,681$(Aigis-1024 采用的是 12 289)和统一的中心二项分布参数$(\eta_k,\eta_e)=(1,4)$,这更有利于算法的模块化部署实现和增强算法的适配性.

由于 Aigis-768 推荐参数很好地综合了安全性和错误率,所以我们推荐的 AKCN-Aigis-768 的参数与 Aigis-768 相同.不同之处在于,AKCN-Aigis 采用的解密算法相比于 Aigis 的更简单,同时在相同的参数下 AKCN-Aigis 的解密错误率也更低.值得指出的是,推荐参数 AKCN-Aigis-1024-2 可以与 Aigis-1024 在相近的安全强度下(208 对比 213),能够以更低的错误率($2^{-216.2}$ 对比 $2^{-211.8}$)和更小的通信带宽(2 816 B 对比 3 008 B,节省了 192 B,约 6.3% 的通信带宽)封装相同长度的密钥(512 b).

Table 5 New Parameters of AKCN-Aigis

表 5 AKCN-Aigis 新参数

Parameters	Aigis-512	Aigis-768	Aigis-1024	AKCN-Aigis-512	AKCN-Aigis-768	AKCN-Aigis-1024-1	AKCN-Aigis-1024-2
n	256	256	512	256	256	256	512
m	2	2	2	2	2	4	2
l	2	3	2	2	3	4	2
q	7 681	7 681	12 289	7 681	7 681	7 681	7 681
η_k	2	1	2	1	1	1	1
η_e	12	4	8	4	4	4	4
d_k	10	9	11	9	9	12	10
d_c	9	9	10	8	9	11	10
t_k	3	4	3	4	4	1	3
t_c	4	4	4	5	4	2	3
g	2^3	2^4	2^4	2^4	2^4	2^6	2^3
$\|K\|$/B	32	32	64	32	32	64	64
$\|pk\|$/B	672	896	1 472	608	896	1 568	1 344
$\|ct\|$/B	672	992	1 536	640	992	1 600	1 472
B/B	1 344	1 888	3 008	1 248	1 888	3 168	2 816
sec	100	147	213	90	147	208	208
δ	$2^{-81.9}$	$2^{-128.7}$	$2^{-211.8}$	$2^{-85.3}$	$2^{-132.7}$	$2^{-198.6}$	$2^{-216.2}$

我们在表 6 中给出 AKCN-Kyber 的新参数推荐.本节开头所述,AKCN-Kyber 算法仅优化了 Kyber 的解密算法,使得解密算法更高效且错误率更低.为了和 Kyber 兼容,AKCN-Kyber-512/768 采用了 Kyber-512/768 相同的参数,区别是错误率更低一些且解密算法更高效.AKCN-Kyber-1024 是封装

512 b 的共享密钥,而 Kyber-1024 封装的是 256 b 的密钥.

最后,我们在表 7 中给出 AKCN-Hybrid 的新参数对比与推荐.其中,*sec* 表示 AKCN-Hybrid 构造中依赖模 LWE 和模 LWR 问题设计的组件(长期私钥与临时私钥)对应的安全强度.

Table 6　New Parameters of AKCN-Kyber

表 6　AKCN-Kyber 新参数

Parameters	Kyber-512	Kyber-768	Kyber-1024	AKCN-Kyber-512	AKCN-Kyber-768	AKCN-Kyber-1024
n	256	256	256	256	256	512
m	2	2	2	2	2	2
l	2	3	4	2	3	2
q	3 329	3 329	3 329	3 329	3 329	3 329
η	2	2	2	2	2	2
d_k	12	12	12	12	12	12
d_c	10	10	11	10	10	11
t_k	0	0	0	0	0	0
t_c	2	2	1	2	2	1
g	2^3	2^4	2^5	2^3	2^4	2^5
$\|K\|$/B	32	32	32	32	32	64
$\|pk\|$/B	800	1 184	1 568	800	1 184	1 600
$\|ct\|$/B	736	1 088	1 568	736	1 088	1 728
B/B	1 536	2 272	3 136	1 536	2 272	3 328
sec	100	164	230	100	164	230
δ	$2^{-178.6}$	$2^{-165.0}$	$2^{-174.9}$	$2^{-181.4}$	$2^{-168.8}$	$2^{-178.7}$

Table 7　New Parameters of AKCN-Hybrid

表 7　AKCN-Hybrid 新参数

Parameters	AKCN-Hybrid-512-1	AKCN-Hybrid-512-2	AKCN-Hybrid-768-1	AKCN-Hybrid-768-2	AKCN-Hybrid-1024-1	AKCN-Hybrid-1024-2	AKCN-Hybrid-1024-3
n	256	256	256	256	256	256	512
m	2	2	2	2	2	4	2
l	2	2	3	3	4	4	2
q	3 329	3 329	3 329	3 329	3 329	3 329	3 329
η	1	2	1	2	2	1	1
p	2^8	2^9	2^9	2^9	2^{10}	2^{10}	2^9
g	2^3	2^2	2^3	2^6	4	2^7	2^4
$\|K\|$/B	32	32	32	32	32	64	64
$\|pk\|$/B	800	800	1 184	1 184	1 568	1 568	1 600
$\|ct\|$/B	608	672	960	1 088	1 440	1 504	1 408
B/B	1 408	1 472	2 144	2 272	3 008	3 072	3 008
sec	91/124	100/119	149/179	164/188	230/238	210/227	210/246
δ	$2^{-79.8}$	$2^{-121.5}$	$2^{-182.2}$	$2^{-139.3}$	$2^{-222.4}$	$2^{-165.9}$	$2^{-185.1}$

9 总 结

在本文中,我们从理论上系统地比较了直接基于模 LWE/LWR 问题构造的密钥封装方案和基于密钥共识机制结合模 LWE/LWR 问题设计的密钥封装方案的异同,并从理论分析和实际测试 2 方面证明了当采用相同的压缩函数和相同的参数设置时,AKCN-MLWE 采用的设计方式在节省运算的同时也能有效地降低解密误差.而 Saber 采用的构造方式本质上与 AKCN-MLWR 是相同的.针对 Kyber-1024 和 Fire-Saber 这 2 组参数对应的安全强度,我们对比分析了 3 种可能的封装 512 b 密钥长度的方法.根据分析,我们给出了 AKCN-MLWE, AKCN-MLWR 和 AKCN-Hybrid 的新的优化建议和参数推荐,也给出了对于 Aigis 和 Kyber 的优化方案(对应的命名为 AKCN-Aigis 和 AKCN-Kyber)及优化参数推荐.

参 考 文 献

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

[2] Shor P. Algorithms for quantum computation: Discrete logarithms and factoring [C] //Proc of the 35th Annual Symp on Foundations of Computer Science. Piscataway, NJ: IEEE, 1994: 124-134

[3] NIST. Post-Quantum Cryptography Round 2 Submissions [EB/OL]. (2019-01-30)[2020-06-11]. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

[4] NIST. Post-Quantum Cryptography Round 3 Submissions [EB/OL]. (2020-07-23)[2020-07-23]. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions

[5] Chinese Association for Cryptologic Research. Public key algorithms selected to the second round competition of national cryptographic algorithm competitions [EB/OL]. (2019-09-27)[2020-07-23]. http://sfjs.cacrnet.org.cn/site/term/list_77_1.html (in Chinese)
(中国密码学会. 全国密码算法设计竞赛进入第 2 轮公钥算法[EB/OL]. (2019-09-27)[2020-07-23]. http://sfjs.cacrnet.org.cn/site/term/list_77_1.html)

[6] Chinese Association for Cryptologic Research. Announcement of the selection results of the national cryptographic algorithm competitions [EB/OL]. (2020-01-02)[2020-06-11]. https://www.cacrnet.org.cn/site/content/854.html (in Chinese)
(中国密码学会. 关于全国密码算法设计竞赛算法评选结果的公示[EB/OL]. (2020-01-02)[2020-06-11]. https://www.cacrnet.org.cn/site/cont-ent/854.html)

[7] Regev O. On lattices, learning with errors, random linear codes, and cryptography [C] //Proc of the 37th Annual ACM Symp on Theory of Computing. New York: ACM, 2005: 84-93

[8] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings [G] //LNCS 6110: Advances in Cryptology-EUROCRYPT 2010. Berlin: Springer, 2010: 1-23

[9] Banerjee A, Peikert C, Rosen A. Pseudorandom functions and lattices [G] //LNCS 7237: Advances in Cryptology-EUROCRYPT 2012. Berlin: Springer, 2012: 719-737

[10] Langlois A, Stehle D. Worst-case to average-case reductions for module lattices [J]. Designs Codes and Cryptography, 2015, 75(3): 565-599

[11] Rosca M, Stehle D, Wallet A. On the ring-LWE and polynomial-LWE problems [G] //LNCS 10820: Advances in Cryptology-EUROCRYPT 2018. Berlin: Springer, 2018: 146-173

[12] Zhang Jiang, Yu Yu, Fan Shuqin, et al. Tweaking the asymmetry of asymmetric-key cryptography on lattices: Kems and signatures of smaller sizes [G] //LNCS 12111: Public-Key Cryptography-PKC 2020. Berlin: Springer, 2020: 37-65

[13] Zhang Jiang, Fan Shuqin. On the hardness of the asymmetric learning with errors problem [J]. Journal of Electronics and Information Technology, 2020, 42(2): 327-332 (in Chinese)
(张江, 范淑琴. 关于非对称含错学习问题的困难性研究[J]. 电子与信息学报, 2020, 42(3): 327-332)

[14] Bos J, Ducas E, Kiltz E, et al. Crystals-Kyber: A CCA-secure module-lattice-based KEM [C] //Proc of IEEE European Symp on Security and Privacy (EuroS&P 2018). Piscataway, NJ: IEEE, 2018: 353-367

[15] D'Anvers J, Karmakar A, Roy S. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM [G] //LNCS 10831: Progress in Cryptology-AFRICACRYPT 2018. Berlin: Springer, 2018, 282-305

[16] Jin Zhengzhong, Zhao Yunlei. Optimal key consensus in presence of noise [DB]. arXiv: 1611.06150, [2020-07-23]. https://arxiv.org/abs/1611.06150?context=math.IT

[17] Jin Zhengzhong, Zhao Yunlei. Generic and practical key establishment from lattice [G] //LNCS 11464: Applied Cryptography and Network Security. Berlin: Springer, 2019: 302-322

[18] Zhao Yunlei, Jin Zhengzhong, Gong Boru, et al. A modular and systematic approach to key establishment and public-key encryption based on LWE and its variants [EB/OL]. NIST PQC Round 1 Submission, 2017 [2020-06-11]. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

[19] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes [J]. Journal of Cryptology, 2013, 26(1): 80-101

[20] Hofheinz D, Hövelmanns K, Kiltz E. A modular analysis of the Fujisaki-Okamoto transformation [G] //LNCS 10677: Theory of Cryptography-TCC 2017. Berlin: Springer, 2017: 341-371

[21] Jiang Haodong, Zhang Zhenfeng, Chen Long, et al. IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited [G] //LNCS 10993: Advances in Cryptology-CRYPTO 2018. Berlin: Springer, 2018, 96-125

[22] Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, [EB/OL]. (2020-07-23) [2020-03-07]. https://datatracker.ietf.org/doc/rfc8446/

[23] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption [G] //LNCS 6558: Topics in Cryptology-CT-RSA 2011. Berlin: Springer, 2011: 319-339

[24] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages [G] //LNCS 6841: Advances in Cryptology-CRYPTO 2011. Berlin: Springer, 2011: 505-524

[25] Lee J, Kim D, Lee H, et al. Rlizard: Post-quantum key encapsulation mechanism for IoT devices [J]. IEEE Access, 2019, 7: 2080-2091

[26] Jung C, Lee J, Ju Y, et al. LizarMong: Excellent key encapsulation mechanism based on RLWE and RLWR [G] //LNCS 11975: Information Security and Cryptology-ICISC 2019. Berlin: Springer, 2019: 208-224

[27] Baan H, Bhattacharya S, Fluhrer S, et al. Round 5: Compact and fast post-quantum public-key encryption [G] //LNCS 11505: PQCrypto 2019: Post-Quantum Cryptography. Berlin: Springer, 2019: 83-102

Wang Yang, born in 1990. PhD, postdoctoral fellow at the School of Mathematics, Shandong University. His main research interests include lattice theory and post-quantum cryptography.

Shen Shiyu, born in 1997. Master candidate in the School of Computer Science, Fudan University. Her main research interests include lattice-based cryptography and cryptographic engineering.

Zhao Yunlei, born in 1974. PhD, distinguished professor at Fudan University. His main research interests include post-quantum cryptography, cryptographic protocols, and theory of computing.

Wang Mingqiang, born in 1971. PhD, professor, PhD supervisor at the School of Mathematics, Shandong University. His main research interests include lattice theory, quantum computation and post-quantum cryptography.