密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2017, 4(5): 485–497
©《密码学报》编辑部版权所有.
E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

后量子密码专栏

基于格的后量子密钥交换研究*

刘亚敏[1,2], 李祥学[3,5], 刘晗林[4]

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 100093
2. 保密通信重点实验室, 四川成都 810 信箱, 成都 610041
3. 华东师范大学 计算机科学技术系, 上海 200062
4. 上海交通大学 计算机科学与工程系, 上海 200240
5. 卫士通摩石实验室, 北京 100070

通讯作者: 李祥学, E-mail: xxli@cs.ecnu.edu.cn

摘 要: 理论上量子算法可高效破解基于整数分解类和离散对数类等经典数论假设的密码体制; 近年来量子计算机的研制进展迅速, 使经典公钥密码面临现实威胁. 因此, 设计后量子密码系统是当前密码学研究以及标准制定中的重要课题. 其中以后量子密钥交换协议的需求最为迫切, 因此成为近年来的热点研究方向. 本文主要关注基于格上的计算困难问题, LWE, 环 LWE 和模 LWE 设计的后量子密钥交换协议, 尤其是最基础的无认证密钥交换协议, 包括 BCNS15, NewHope/NewHope-Simple, Frodo, Kyber.KE 等. 本文将介绍这些协议中的关键技术, 参数选取, 以及通信量, 计算效率和安全性等指标.

关键词: 后量子密码; 密钥交换; LWE; 环 LWE; 模 LWE

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000200

中文引用格式: 刘亚敏, 李祥学, 刘晗林. 基于格的后量子密钥交换研究[J]. 密码学报, 2017, 4(5): 485–497.

英文引用格式: LIU Y M, LI X X, LIU H L. Post-quantum key exchange from lattice[J]. Journal of Cryptologic Research, 2017, 4(5): 485–497.

Post-quantum Key Exchange from Lattice

LIU Ya-Min[1,2], LI Xiang-Xue[3,5], LIU Han-Lin[4]

1. SKLOIS, Institute of Information Engineering, CAS, Beijing 100093, China
2. Science and Technology on Communication Security Laboratory, Mail Box 810, Chengdu 610041,China
3. Department of Computer Science and Technology, East China Normal University, Shanghai 200062, China
4. Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
5. Westone Cryptologic Research Center, Beijing 100070, China

Corresponding author: LI Xiang-Xue, E-mail: xxli@cs.ecnu.edu.cn

Abstract: Cryptosystems based on classical number-theoretical assumptions, such as integer factoring and discrete logarithm, can be broken by quantum algorithms efficiently in theory, while the rapid development of quantum computers is becoming threats of classical cryptosystems in practice.

* 基金项目: 保密通信重点实验室项目资助 (9140C110206150C11049); 国家自然科学基金项目 (61502480,61472249, 61572192, 61571191); 陕西省国际科技合作与交流计划 (2016KW-038)
收稿日期: 2017-08-15 定稿日期: 2017-10-10

Thus, the design of post-quantum cryptosystems is an important (or even urgent) research direction of cryptography, wherein the most urgent is the need for post-quantum key exchange protocols, which is a hot topic in recent years. In this paper we mainly focus on the post-quantum protocols from computational hard problems on lattices, such as LWE, ring-LWE, and module-LWE, especially the most-basic unauthenticated key exchange protocols, such as BCNS15, NewHope/NewHope-simple, Frodo, and Kyber.KE. We will introduce the key techniques, the choice of parameters, communication costs, computation efficiency and security of these protocols.

Key words: Post-quantum cryptography; key exchange; LWE; ring-LWE; module-LWE

1 后量子密钥交换研究背景

1.1 密钥交换协议基本概念

密钥交换协议 (key exchange protocols) 旨在让两方或者多方在不安全的信道上协商出共同的会话密钥; 该密钥将在之后的对称密码中使用, 从而建立安全的通信信道. 其中两方协议的情况最为普遍. 1976 年 Diffie 和 Hellman 提出了著名的 Diffie-Hellman 密钥交换协议 [1], 该协议通过两轮消息发送, 完成会话密钥的协商. 但是 Diffie-Hellman 式基础密钥交换只能提供被动安全, 不能抵抗中间人攻击和重放攻击等; 同时也不能提供相互认证的功能, 任何人都可以冒充协议参与方进行破坏.

具有更强安全性的是认证密钥交换 (authenticated key exchange, AKE) 协议, 它使通信双方能够认证彼此的身份, 并在信道上存在主动敌手 (能够实施删除、重放、注入、篡改等多种攻击) 的情形下仍然安全地协商出共同的会话密钥. AKE 协议包括两大类: 一类假设通信双方都各自拥有高熵的私钥, 我们通常所说的 AKE 协议即是这一类; 另一类假设双方拥有弱的共享口令, 即基于口令的密钥交换 [2](password-based authenticated key exchange, PAKE). 无认证的 Diffie-Hellman 式密钥交换协议也可与签名结合实现认证性, 这种方式具有模块化和灵活的优点, 因此成为研究的重点. 这三类密钥交换协议在现实的互联网安全协议 (如 SSL/TLS [3]) 中都发挥着重要的作用.

1.2 后量子公钥密码

目前使用的密钥交换协议及公钥加密, 签名等公钥密码算法主要是基于经典的困难问题构造的, 例如大整数分解或计算有限域/椭圆曲线群上的离散对数问题. 这些问题的已知最好的经典求解算法需要指数/亚指数 (至少超多项式) 时间复杂度; 然而研究表明, 理论上这些数论困难问题在量子计算模型下存在多项式时间的量子算法 [4–8]. 近年来量子计算机的研制进展迅速 [9,10], 使得经典公钥密码的安全性开始面临现实威胁.

这促使研究人员设计能够抵抗量子计算机攻击的密码——称为 “后量子” 或 “量子安全” 或 “抗量子” 密码. 2015 年 8 月, 美国国家安全局 (NSA) 发布了关于政府使用的 B 套密码算法的通知, 指出这套算法会在不久的将来向抗量子算法迁移 [11]. 同年, 美国国家标准技术研究所 (NIST) 开启了后量子密码项目以评估并标准化一个或多个抗量子攻击的公钥密码系统 [12], 包括公钥加密, 签名, 和密钥交换等三类最基础的公钥密码原语. 其中以密钥交换协议的需求最为迫切，因为密钥交换要求前向安全性, 需要考虑密钥的泄露对此前已传输信息的威胁 (对比签名, 只需保证在使用的当时不能伪造). 尤其, 攻击者可保存目前的通信内容, 并在未来使用量子计算机破解. 因此, 尽快设计和部署后量子密钥交换协议成为研究的热点.

目前, 用于构建后量子密码系统的常见数学技巧包括: 杂凑函数 (hash functions), 纠错码 (error correcting codes), 格 (lattices), 多变量方程 (multivariate equations), 以及超奇异椭圆曲线同源 (supersingular elliptic curve isogenies) 问题等. 其中, 基于杂凑的密码和多变量密码在构造签名方案时较有优势; 基于编码的密码更合适构造加密方案; 格密码是最通用的一类, 几乎所有经典密码概念都可以在格密码中实现; 超奇异同源密码是较新的一类, 目前其中较受关注的有密钥交换和签名方案的构造, 但是同源密码的计算效率很低, 还达不到实用性的要求. 因此, 本文主要讨论基于格的密钥交换协议研究.

2 LWE, 环 LWE, 及模 LWE

1996 年, Ajtai [13] 首先基于格上的计算困难问题, 小整数解 (Short Integer Solution, SIS) 问题, 构造了抗碰撞杂凑函数. 在 Ajtai 和 Dwork [14] 后续的工作中给出了基于其他格问题的公钥密码方案. 同时, Hoffstein, Pipher 和 Silverman [15] 给出了基于多项式环的 NTRU 公钥加密方案, 其安全性也与格上的困难问题密切关联.

2005 年, Regev [16] 提出了带错误的学习问题 (learning with errors problem, LWE), 证明了 LWE 与格上困难问题 (如近似最短向量问题 Gap-SVP) 相关, 并给出了基于 LWE 的公钥密码方案. 与之前出现的格上困难问题比较, LWE 在构建密码系统时更方便, 因而有大量 LWE 困难性及其在密码学中应用的研究 [17]. 本节将简单回顾几类 LWE 问题, 以帮助理解后文.

2.1 符号

令 χ 表示分布, $a \xleftarrow{\$} \chi$ 表示根据分布 χ 随机选取 a. 用 U 表示均匀分布. 向量用小写粗体表示, 比如 $\mathbf{a}$; 矩阵用大写粗体表示, 比如 $\mathbf{A}$. 向量 $\mathbf{a}$ 的转置记为 $\mathbf{a}^t$, 矩阵 $\mathbf{A}$ 的转置记为 $\mathbf{A}^t$. 两个向量 $\mathbf{a}$, $\mathbf{b}$ 的内积表示为 $\langle \mathbf{a}, \mathbf{b} \rangle$. 选取长度为 n 的向量且向量中的每一个元素都从分布 χ 中独立随机选取, 表示为 $\mathbf{a} \xleftarrow{\$} \chi^n$. 如果 A 是一个概率型算法, 则用 $y \xleftarrow{\$} \mathsf{A}(x)$ 表示在输入为随机的 x 值时运行算法 A 并将结果赋给变量 y, $y \xleftarrow{\$} \mathsf{A}^O(x)$ 表示算法 A 运行时能访问预言 O.

2.2 带错误的学习问题 (LWE)

搜索型 LWE 问题 (search LWE problem) 类似于求解有噪声的线性方程组: 给定矩阵 $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ 和向量 $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, 求解 $\mathbf{s} \in \mathbb{Z}^n$.

定义 1 (搜索型 LWE 问题) 令 n, m, q 为正整数, χ_s 和 χ_e 为 $\mathbb{Z}$ 上的分布. 令秘密 $\mathbf{s} \xleftarrow{\$} \chi_s^n$. 对 $i = 1, \cdots, m$, 令 $\mathbf{a}_i \xleftarrow{\$} U(\mathbb{Z}_q^n)$, 选取错误项 $e_i \xleftarrow{\$} \chi_e$, 并令 $b_i \leftarrow \langle \mathbf{a}, \mathbf{s} \rangle + e_i \bmod q$. 参数为 $(n, m, q, \chi_s, \chi_e)$ 的搜索型 LWE 问题定义为: 给定 $(\mathbf{a}_i, b_i)_{i=1}^m$, 计算秘密 $\mathbf{s}$.

在实际构造密码方案时, 使用得更多的是判定型的 LWE 问题 (decision LWE problem), 即对于合适的分布 χ_s 和 χ_e, LWE 样本 $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$ 看起来是在 $\mathbb{Z}_q$ 中均匀随机分布的.

定义 2 (判定型 LWE 问题) 令 n, q 为正整数, χ_s 和 χ_e 是 $\mathbb{Z}$ 上的分布. 令秘密 $\mathbf{s} \xleftarrow{\$} \chi_s^n$. 定义如下两个预言:

- $O_{\chi_e, \mathbf{s}}$: 选取 $\mathbf{a} \xleftarrow{\$} U(\mathbb{Z}_q^n)$, $e \xleftarrow{\$} \chi_e$, 返回 $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q)$;
- U: 选取 $\mathbf{a} \xleftarrow{\$} U(\mathbb{Z}_q^n)$, $u \xleftarrow{\$} U(\mathbb{Z}_q)$, 返回 $(\mathbf{a}, u)$.

参数为 (n, q, χ_s, χ_e) 的判定型 LWE 问题即区分 $O_{\chi_e, \mathbf{s}}$ 和 U.

当选择合适的参数 n, m, q, χ_s, χ_e 时, 搜索型 LWE 问题的难解性与格上困难问题相关. Regev [16] 使用量子归约 (quantum reduction) 技术将 LWE 问题的平均情形 (average-case) 困难性和随机格上 GapSVP_γ 和 SIVP_γ 问题的最坏情形 (worst-case) 困难性联系起来, 其中参数 γ 的选取与 LWE 问题的参数相关. 在选取合适的参数时, 判定型 LWE 问题和搜索型 LWE 问题是多项式等价的 [18].

通常 LWE 问题中的错误分布 χ_e 是宽度为 αq 的离散高斯分布 (discrete Gaussian distribution), 其中 $\alpha < 1$ 称为错误率. 在早期研究中, LWE 的秘密 $\mathbf{s}$ 服从均匀分布 ($\chi_s^n = U(\mathbb{Z}_q^n)$). Applebaum 等 [19] 给出了 LWE 的短秘密变体 (short secrets) 形式, 也就是 $\chi_s = \chi_e$, 并证明这种变体和使用均匀秘密分布的 LWE 问题的困难性相当. 在基于格的后量子密钥交换协议中, 我们使用的是 LWE 的这种短秘密变体.

2.3 环 LWE(learning with errors over rings)

基于 LWE 问题构造的密码系统, 由于参数中包含大矩阵 (例如 LWE 的公开参数 $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$), 因此其密钥, 密文尺寸通常很大, 这成为格密码实用化的一大技术障碍. 2010 年, 受 NTRU 等的启发, Lyubashevsky, Peikert 和 Regev [20,21] 提出了环 LWE, 从而解决了这一技术难题.

定义整系数多项式环 $R = \mathbb{Z}[x]/(x^n + 1)$, 其中 n 形如 2^k, k 为正整数. 令 q 为整数, 并定义环 $R_q = \mathbb{Z}_q[x]/(x^n + 1)$. 换而言之, R_q 包含了所有次数至多为 $n - 1$ 的多项式, 且其系数均在 $\mathbb{Z}_q$ 中. 搜索和判定型的环 LWE 问题与相关的 LWE 问题类似, 只是向量变成了环元素.

定义 3 (搜索型环 LWE 问题) 令 n, q 为正整数, χ_s 和 χ_e 为 R_q 上的分布. 令秘密 $s \xleftarrow{\$} \chi_s$, $a \xleftarrow{\$} U(R_q)$, 选取错误 $e \xleftarrow{\$} \chi_e$, 并令 $b \leftarrow as + e$. 参数为 (n, q, χ_s, χ_e) 的搜索型 Ring-LWE 问题定义为: 给定 (a, b), 求解秘密 s.

同样地, 判定型环 LWE 问题指对于合适的分布 χ_s 和 χ_e, 环 LWE 样本 $(a, as + e)$ 看起来是在 R_q 中均匀随机分布的.

定义 4 (判定型环 LWE 问题) 令 n, q 为正整数, χ_s 和 χ_e 为 R_q 上的分布. 令秘密 $s \xleftarrow{\$} \chi_s$. 定义如下两个预言:

- $O_{\chi_e,s}$: 选取 $a \xleftarrow{\$} U(R_q)$, $e \xleftarrow{\$} \chi_e$, 返回 $(a, as + e)$;
- U: 选取 $a \xleftarrow{\$} U(R_q)$, $u \xleftarrow{\$} U(R_q)$, 返回 (a, u).

参数为 (n, q, χ_s, χ_e) 的判定型环 LWE 问题即区分 $O_{\chi_e,s}$ 和 U.

对于合适的参数, 环 LWE 问题的困难性可以归约为理想格 (ideal lattice) 上的 SVP_γ 问题的困难性 (对比 LWE 问题, 其困难性基于一般格上的困难问题). LWE 问题中的短秘密变体, 搜索和判定型问题的等价性等结论, 也适用于环 LWE 的情形.

2.4 模 LWE(module learning with errors)

环 LWE 中的代数结构, 大大提高了基于其构造的密码系统效率, 但是也引起了对其安全性的隐忧 [22]. 2015 年, Langlois 和 Stele 研究了模 LWE(module-LWE) 问题 [23]. 作为一种代数结构, 模 (module) 是环和向量空间的一般化; 同时, 模格 (module lattice) 是对理想格和一般格的推广. 因此, 模 LWE 是 LWE 和环 LWE 的推广. 通过选取合适的参数, 基于模 LWE 构造的密码系统能够在效率和安全性之间很好地平衡.

定义 5 (搜索型模 LWE 问题) 令 n, m, d, q 为正整数, χ_s, χ_e 是 R_q 上的分布. 令秘密 $\mathbf{s} \xleftarrow{\$} \chi_s^d$, $\mathbf{a}_i \xleftarrow{\$} U(R_q^d)$, 选取错误 $e_i \xleftarrow{\$} \chi_e$, 并令 $b_i \leftarrow \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \in R_q$. 参数为 $(n, m, q, d, \chi_s, \chi_e)$ 的搜索型模 LWE 问题定义为: 给定 $(\mathbf{a}_i, b_i)_{i=1}^m$, 求解秘密 $\mathbf{s}$.

定义 6 (判定型模 LWE 问题) 令 n, d, q 为正整数, χ_s 和 χ_e 为 R_q 上的分布. 令秘密 $\mathbf{s} \xleftarrow{\$} \chi_s^d$. 定义如下两个预言:

- $O_{\chi_e,\mathbf{s}}$: 选取 $\mathbf{a} \xleftarrow{\$} U(R_q^d)$, $e \xleftarrow{\$} \chi_e$, 返回 $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$;
- U: 选取 $\mathbf{a} \xleftarrow{\$} U(R_q^d)$, $u \xleftarrow{\$} U(R_q)$, 返回 $(\mathbf{a}, u)$.

参数为 $(n, d, q, \chi_s, \chi_e)$ 的判定型模 LWE 问题即区分 $O_{\chi_e,\mathbf{s}}$ 和 U.

参数 d 和环 R_q 的选取可以使模 LWE 的安全性和效率灵活折衷. 当 $d = 1$, 环 $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ 时, 问题成为环 LWE; 当将环 R_q 设置为 $\mathbb{Z}_q$ 时, 问题成为 LWE. 当使用模 LWE 构造密码系统时, 增加环维度 n, 降低 d, 可以提高方案的效率; 同时 d 越小, 也意味着更多的代数结构, 从而可能影响对安全性的信心.

3 基于格的密钥交换

基于 (环/模)LWE 问题设计密钥交换的一个关键难题就在于这些问题中带有错误. 一方面, 错误对它们的后量子困难性有重要作用, 没有错误, 这些问题可以轻易求解; 另一方面, 基于这些问题构造密钥交换时, 错误的存在使协议的双方只能得到近似相等的值, 例如 Bob 通过计算得到 $v \in \mathbb{Z}_q$, 而 Alice 通过计算只能得到 $w = v + e \in \mathbb{Z}_q$. 因此对错误的处理成为格上密钥交换设计的技术挑战. 这个挑战可以使用两种方法来解决, 一种是使用错误协调机制 (error reconciliation mechanism), 其中的关键便是各种错误协调方法, 其思想类似于模糊提取器 (fuzzy extractor) [24]; 另一种是直接加密会话密钥, 其中的关键是密文压缩方法.

3.1 基于错误协调的构造

2012 年, 丁津泰等人 [25] 提出了一个巧妙的错误协调机制 (丁式错误协调), 使得交互的双方, Alice 和 Bob, 可以在两轮消息发送中得到共同的会话密钥, 又不影响会话密钥的伪随机性. 基于此思想, 丁等人首次在格上使用 (环)LWE 构造了 Diffie-Hellman 式密钥交换. 丁氏错误协调在张江 [26] 等人基于环 LWE 构造的 HMQV 式 AKE 协议, 以及丁等人 [2,27] 基于环 LWE 构造的 PAKE 协议中均有应用.

2014 年, Peikert [28] 提出一种变形的错误协调机制 (Peikert 式错误协调), 并被 Bos 等人 [29] 应用到实用化的 BCNS15 密钥交换协议中. 2015 年, Alkim 等人 [30] 将 Peikert 式错误协调扩展为 $\tilde{D}_4$ 格解码 (lattice $\tilde{D}_4$ decoding), 并构造了基于环 LWE 的 NewHope 协议. 2016 年, Bos 等人 [31] 提出 Peikert 式错误协调的多比特变形, 并构造了基于 LWE 的 Frodo 协议. 随后, 金正中和赵运磊等人 [32] 提出了密钥共识 (key consensus) 的概念, 其中对文献 [30,31] 中的错误协调机制都做出了优化.

注意到丁将基于错误协调机制构造 Diffie-Hellman 式密钥交换/传输协议的方法申请了专利 [33], 其权利要求中也包含了错误协调机制的各种相似变形. 因此 Peikert 的错误协调机制与其变形, 及它们在此类方案构造中的应用, 均被丁的专利涵盖.

以下我们将介绍几种错误协调机制, 以及基于其构造的 BCNS15, NewHope 和 Frodo 协议.

丁式错误协调. 丁式错误协调的主要思想就是对于奇数 q, 在 (环)LWE 的计算中使用偶数错误 (例如计算 $b = \langle \mathbf{a}, \mathbf{s} \rangle + 2\hat{e} \bmod q$), 使双方 (Alice 和 Bob) 最终得到的近似相等的值 $w, v \in \mathbb{Z}_q$ 有 $w = v + 2e \bmod q$ 的关系. 当没有发生回绕 (wrap-around) 时, 即计算时不需要模 q, 则 x, v 的最低比特是相同的, 双方可以将 w, v 的最低比特提取出来, 从而得到相同的值. 当发生回绕时, 即计算时需要执行模 q, w, v 的最低比特可能会不同. 这时 Bob 可以发送一个关于 v 的信号比特 (signal bit)σ 给 Alice. 只要 $|w - v|$ 足够小, 依据信号比特 σ, 使用合适的协调函数, 就可以提取出相同的比特. 只要 $v \in \mathbb{Z}_q$ 是均匀随机的, 即使给定 σ, 所提取出的比特也是具有高最小熵的. 这一方法可以扩展到双方拥有多个 $\mathbb{Z}_q$ 中元素的情形 (例如, Alice 和 Bob 均拥有一个 R_q 中的元素), 从每个元素中产生一个信号比特, 并提取出一个协调比特.

对于奇数 $q > 2$, 定义 $\mathbb{Z}_q = \{-\frac{q-1}{2}, \cdots, \frac{q-1}{2}\}$, 并将 $\mathbb{Z}_q$ 区间的中间一半定义为 $E = \{-\lfloor \frac{q}{4} \rfloor, \cdots, \lfloor \frac{q}{4} \rfloor\}$. 则信号函数 Cha 定义为:

$$\mathsf{Cha}(v) = \begin{cases} 0, & v \in E \\ 1, & \text{else} \end{cases}$$

显然, 对于任意 $v \in \mathbb{Z}_q$, $v + \mathsf{Cha}(v) \cdot \frac{q-1}{2} \bmod q$ 可以变换到 E 中.

定义模函数 (modular function)$\mathsf{Mod}_2 : \mathbb{Z}_q \times \{0,1\} \to \{0,1\}$ 为:

$$\mathsf{Mod}_2(v, \sigma) = (v + \sigma \cdot \frac{q-1}{2}) \bmod q \bmod 2$$

假设 Alice 和 Bob 分别拥有 w, v. 在 Bob 发送其信号比特 $\sigma = \mathsf{Cha}(v)$ 后, 双方均对 v 和 $w = v + 2e$ 应用模函数 Mod_2. 只要 $|e| < \frac{q}{8}$ 就可以得到相同的比特, 这一性质称为错误协调机制的**正确性**; 当 $v \in \mathbb{Z}_q$ 均匀随机时, 给定信号比特 $\sigma = \mathsf{Cha}(v)$, 模函数的输出仍然具有高熵, 这一性质称为错误协调机制的**安全性**.

Peikert 式错误协调. 在丁等人最初提出的错误协调机制中, 双方提取出来的共同比特并不是均匀分布的, 只是具有高熵, 还需要一个随机提取器来得到均匀的值, 这也会带来效率损失. Peikert 提出的变形错误协调机制, 使双方可以直接得到均匀的共同比特 [28].

对于偶数模数 $q \geqslant 2$, 定义 $\mathbb{Z}_q = \{-\frac{q}{2}, \cdots, 0, \cdots, \frac{q}{2} - 1\}$. 此外, 定义三个区间:

$$I_0 = \{0, 1, \cdots, \lfloor \frac{q}{4} \rceil - 1\}, I_1 = \{-\lfloor \frac{q}{4} \rfloor, \cdots, -1\}, E = [-\frac{q}{8}, \frac{q}{8}) \cap \mathbb{Z}$$

对于 $x \in \mathbb{Z}_q$, 定义如下三个函数:

- 交叉取整函数 (Cross-rounding function)$\langle \cdot \rangle_{q,2} : \mathbb{Z}_q \to \mathbb{Z}_2$: $\langle x \rangle_{q,2} := \lfloor \frac{4}{q} \cdot x \rfloor \bmod 2$.
- 模取整函数 (Modular rounding function)$\lfloor \cdot \rceil_{q,2} : \mathbb{Z}_q \to \mathbb{Z}_2$: $\lfloor x \rceil_{q,2} := \lfloor \frac{2}{q} \cdot x \rceil$.

- 协调函数 $\mathsf{Rec}: \mathbb{Z}_q \times \mathbb{Z}_2 \to \mathbb{Z}_2$:

$$\mathsf{Rec}(w,\sigma) := \begin{cases} 0, & w \in I_\sigma + E \bmod q \\ 1, & \text{else} \end{cases}$$

假设 Alice 和 Bob 分别拥有 $w, v \in \mathbb{Z}_q$. Bob 的信号比特由交叉取整函数产生, 即 $\sigma = \langle x \rangle_{q,2}$; Bob 使用模取整函数从 v 中提取出一个比特; 而 Alice 使用协调函数, 根据信号比特 σ, 从 w 中提取一个比特.

Peikert 式错误协调与丁式错误协调本质上是对偶的, 丁式错误协调取 $\mathbb{Z}_q$ 元素的低位比特, 而 Peikert 式错误协调取 $\mathbb{Z}_q$ 元素的高位比特. 它们的容错范围也相同, 即 Peikert 式错误协调的正确性 $\lfloor v \rceil_{q,2} = \mathsf{Rec}(w,\sigma)$, 其前提也是 $|e| < \frac{q}{8}$. 区别在于 Peikert 式错误协调的基础形式使用偶数模数, 因此它的模取整函数将 $\mathbb{Z}_q$ 区间划分为大小相等的两半, 一半中的元素提取为比特 0, 另一半提取为 1, 因此其安全性为当 $v \in \mathbb{Z}_q$ 均匀随机时, 给定信号比特, 模取整函数的输出仍然在 $\{0,1\}$ 中均匀.

若 q 为奇数, 则可定义随机翻倍函数 (randomized doubling function)$\mathsf{dbl}(\cdot): \mathbb{Z}_q \to \mathbb{Z}_{2q}$ 为 $\mathsf{dbl}(x) := 2x - \bar{e}$, 其中 $\bar{e} = 0$ 的概率为 $\frac{1}{2}$, 且 $\bar{e} = \pm 1$ 的概率均为 $\frac{1}{4}$. 若 x 在 $\mathbb{Z}_q$ 中均匀随机, 则 $\mathsf{dbl}(x)$ 在 $\mathbb{Z}_{2q}$ 中也是均匀随机的. 现在为了从 $w \in \mathbb{Z}_q$ 中提取比特, 模取整函数, 交叉取整函数和协调函数都应用到 $2w \in \mathbb{Z}_{2q}$; 而区间 I_0, I_1, E 的范围也相应地改变.

Peikert 式错误协调的多比特变形. 对于偶数模数 $q \geqslant 2$, 定义 $\mathbb{Z}_q$ 为 $\{0, 1, \cdots, q-1\}$. 令 B 为从每个 $\mathbb{Z}_q$ 元素中提取的比特数, 且 $1 \leqslant B < (\log_2 q) - 1$. 则交叉取整函数, 模取整函数和协调函数定义如下:

- 交叉取整函数 $\langle \cdot \rangle_{q,2^B}: \mathbb{Z}_q \to \mathbb{Z}_2$: $\langle x \rangle_{q,2^B} := \lfloor \frac{2^{B+1}}{q} \cdot x \rceil \bmod 2$.
- 模取整函数 $\lfloor \cdot \rceil_{q,2^B}: \mathbb{Z}_q \to \mathbb{Z}_{2^B}$: $\lfloor x \rceil_{q,2^B} := \lfloor \frac{2^B}{q} \cdot x \rceil \bmod 2^B$.
- 协调函数 $\mathsf{Rec}: \mathbb{Z}_q \to \mathbb{Z}_{2^B}$: $\mathsf{Rec}(w,\sigma) = \lfloor v \rceil_{2^B}$, 其中 v 是离 w 最近且使得 $\langle v \rangle_{2^B} = \sigma$ 的元素.

基本的 Peikert 式错误协调正是 $B = 1$ 的情形. 在文献 [31] 中为了方便起见, 模数 q 为 2 的方幂. 使用随机翻倍技术, q 可以是任意模数. 这种多比特变形方法的安全性和正确性均为对一比特情形的推广; 并且所提取的比特数 B 越大, 协调函数的容错范围, $|v - w| < \frac{q}{2^{B+2}}$, 便越小.

$\tilde{D}_4$ 格解码. 与 Peikert 式错误协调的多比特变形相反, $\tilde{D}_4$ 格解码方法是从四个 $\mathbb{Z}_q$ 元素中提取出一个比特. 这样协调函数可以容忍更大的错误. 四维格 $\tilde{D}_4$ 的基 $\mathbf{B}$ 定义为

$$\mathbf{B} = (\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \mathbf{g}) = \begin{pmatrix} 1 & 0 & 0 & 1/2 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 1/2 \end{pmatrix}$$

$\tilde{D}_4$ 是平凡的四维整数格 D_4 的简单变形, 其中的 CVP 问题 (closest vector problem) 可高效求解, 因此其适用于编码和解码. 与 $\tilde{D}_4$ 格中的编码解码相关的两个格点是 $\mathbf{0} = (0,0,0,0)^t$ 与 $\mathbf{g} = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})^t$. 定义格点 $\mathbf{p}$ 的 Voronoi 胞 (Voronoi cell) 为格空间中离 $\mathbf{p}$ 比其它任意格点都近的点的集合. 对于一个四维向量 $\mathbf{y} \in [0,1)^4$, 若它在 $\mathbf{0}$ 的 Voronoi 胞中, 则解码为 0; 若它在 $\mathbf{g}$ 的 Voronoi 胞中, 则解码为 1.

假设 Alice 和 Bob 分别拥有距离接近的 $\mathbf{x}, \mathbf{x}' \in \mathbb{Z}_q^4$. 若 $\mathbf{x}, \mathbf{x}'$ 在同一个 Voronoi 胞中, 则它们自然地可以解码成同一个比特. 但它们也有可能在不同的 Voronoi 胞中. 因此, Bob 将发送一个协调向量, 来指示 $\mathbf{x}'$ 与它所在的 Voronoi 胞中心的距离. 随后双方均将这个距离向量加到各自的点上, 将 $\mathbf{x}, \mathbf{x}'$ 向 $\mathbf{x}'$ 所在的 Voronoi 胞的中心移动. 若 $\mathbf{x}, \mathbf{x}'$ 足够接近, 则它们将移动到同一个 Voronoi 胞, 从而解码成同一个比特. 为了节约通信量, 协调向量在每个维度只用 r 比特表示, 称为 r 比特离散化 (r-bit discretization).

因此, $\tilde{D}_4$ 格解码方法中, 生成协调信息的函数 HelpRec 和协调函数 Rec 定义如下:

- $\mathsf{HelpRec}(\mathbf{x}; b) = \mathsf{CVP}_{\tilde{D}_4}(\frac{2^r}{q}(\mathbf{x} + b\mathbf{g})) \bmod 2^r$.
  对于输入四维向量 $\mathbf{x} \in \mathbb{Z}_q^4$, HelpRec 函数首先使用随机掷币 $b \in \{0,1\}$, 以 $\frac{1}{2}$ 的概率往 $\mathbf{x}$ 上加上向量 $\mathbf{g}$, 这是 Peikert 的随机翻倍技术的扩展, 在这里称为 Voronoi 胞的边界模糊 (edge blurring) 技术, 为了使最终协调函数的输出均匀. 随后, 输入被变换到 $[0, 2^r)^4$ 空间中, 使用 $\mathsf{CVP}_{\tilde{D}_4}$ 算法找到

距离其最近的格点在基 $\mathbf{B}$ 下的坐标, 并最终生成协调信息 $\mathbf{r} \in \{0, 1, \cdots, 2^r - 1\}^4$.

- $\mathsf{Rec}(\mathbf{x}, \mathbf{r}) = \mathsf{Decode}(\frac{1}{q}\mathbf{x} - \frac{1}{2^r}\mathbf{Br})$.
  对于输入四维向量 $\mathbf{x} \in \mathbb{Z}_q^4$ 和协调信息 $\mathbf{r} \in \{0, 1, \cdots, 2^r - 1\}^4$, $\mathbf{x}$ 首先被变换到 $[0, 1)^4$ 空间中, 按照协调信息移动距离 $\mathbf{Br}$, 并使用解码函数 Decode, 判断其在格点 $\mathbf{0}$ 还是格点 $\mathbf{g}$ 的 Voronoi 胞中, 从而解码为比特 0 或 1.

$\tilde{D}_4$ 格解码方法的安全性在于对于点 $\mathbf{x}$, 协调信息只泄露了它与其所在 Voronoi 胞中心的距离, 并未泄露其所在的 Voronoi 胞, 因此最终解码函数的输出仍然存在不确定性; 当 $\mathbf{x} \in \mathbb{Z}_q^4$ 均匀随机时, 由于 Voronoi 胞的形状全等, 以及边界模糊技术, 最终解码函数的输出在 $\{0, 1\}$ 中是均匀的.

$\tilde{D}_4$ 格解码方法的正确性在于当两个点 $\mathbf{x}, \mathbf{x}'$ 距离足够近时, 它们最终将移动到同一个 Voronoi 胞中, 从而解码为相同比特. 与以往的错误协调机制不同, 在这里容错距离是使用 1-范式来衡量的, 即 $\|\mathbf{x} - \mathbf{x}'\|_1 < (1 - \frac{1}{2^r}) \cdot q - 2$. 在文献 [30] 中取 $r = 2$, 容错距离可接近 $\frac{3}{4}q$. 显然, r 越大, 意味着发送的协调信息越完整, 容错距离也将越大.

3.2 BCNS15

Bos 等人基于环 LWE, 使用 Peikert 式错误协调机制构造了无认证的基础 KE 协议 [29], 并为其选择了具体的实现参数, 集成到 OpenSSL 中 [29], 如图1所示.

公共参数:		
判定型环 LWE 参数 q, n, χ		
$a \xleftarrow{\$} U(R_q)$		
Alice		Bob
$s, e \xleftarrow{\$} \chi$		$s', e' \xleftarrow{\$} \chi$
$b \leftarrow as + e \in R_q$	$\xrightarrow{b}$	$b' \leftarrow as' + e' \in R_q$
		$e'' \xleftarrow{\$} \chi$
		$v \leftarrow bs' + e'' \in R_q$
		$\bar{v} \xleftarrow{\$} \mathsf{dbl}(v) \in R_{2q}$
	$\xleftarrow{b', c}$	$c \leftarrow \langle \bar{v} \rangle_{2q,2} \in \{0, 1\}^n$
$k_A \leftarrow \mathsf{Rec}(2b's, c) \in \{0, 1\}^n$		$k_B = \lfloor \bar{v} \rceil_{2q,2} \in \{0, 1\}^n$

图 1 BCNS15: 基于环 LWE 的非认证 Diffie-Hellman 式密钥交换
Figure 1 BCNS15: Unauthenticated Diffie-Hellman-like key exchange from ring-LWE

在 BCNS15 协议中, Alice 和 Bob 交换环 LWE 样本 $b = as + e$ 和 $b' = as' + e'$. 随后双方可以计算近似的环元素

$$b's = sas' + se' \approx sas' + s'e = bs' \in R_q = \mathbb{Z}_q[x]/(x^n + 1).$$

使用 Peikert 式错误协调, 双方可以从各自的环元素中提取出 n 个均匀比特, 作为会话密钥.

安全性. 若判定型环 LWE 对于方案选定的参数是困难的, 则 BCNS15 密钥交换协议就是一个安全的非认证密钥交换协议. 这个结论与文献 [28, 34] 中一致. 在协议中, 判定型环 LWE 保证了 Bob 计算的值 $v = bs' + e''$ 在 R_q 中是均匀随机分布的, 因此错误协调机制的安全性保证了最终生成的会话密钥的均匀随机性.

参数. BCNS15 协议选择的初始化参数为 $n = 1024$, $q = 2^{32} - 1$. 错误分布 χ 是标准差为 $\frac{8}{\sqrt{2\pi}}$ 的离散高斯分布. 在该参数设置下, 最终生成共同会话密钥失败的概率远低于 2^{-128}. 在方案中, Alice 发送的信息为一个环元素, 共 $1024 \times 4B = 4096B$; Bob 发送的信息为一个环元素和 1024 比特的协调信息, 共 $4096B + 128B = 4224B$.

基于 Albrecht 等人 [35] 的困难性评估, 使用量子算法攻破这些参数定义的系统需要 $2^{163.8}$ 次操作和至少 $2^{94.4}$ 的内存消耗. 借助于 Grover 算法的量子计算机 (对应搜索复杂度需开平方), 这意味着有 81.9

比特的量子安全级别. 不过后续论文 [30,31] 中采用的评估方法显示, BCNS15 的后量子安全性并没有达到 80 比特.

3.3 NewHope

参数: $q = 12289 < 2^{14}$, $n = 1024$
错误分布: Ψ_{16}

Alice		Bob
$\text{seed} \xleftarrow{\$} \{0,1\}^{256}$		
$a \leftarrow \mathsf{Parse}(\mathsf{SHAKE}-128(\text{seed}))$		
$s, e \xleftarrow{\$} \Psi_{16}$		$s', e', e'' \xleftarrow{\$} \Psi_{16}$
$b \leftarrow as + e \in R_q$	$\xrightarrow{(b,\text{seed})}$	$a \leftarrow \mathsf{Parse}(\mathsf{SHAKE}-128(\text{seed}))$
		$u \leftarrow as' + e'$
		$v \leftarrow bs' + e'' \in R_q$
$v' \leftarrow us$	$\xleftarrow{(u,r)}$	$r \xleftarrow{\$} \mathsf{HelpRec}(v)$
$\nu \leftarrow \mathsf{Rec}(v', r)$		$\nu \leftarrow \mathsf{Rec}(v, r)$
$\mu \leftarrow \mathsf{SHA3}-256(\nu)$		$\mu \leftarrow \mathsf{SHA3}-256(\nu)$

图 2 基于环 LWE 的 NewHope 协议
Figure 2 The NewHope protocol from ring-LWE

2015 年, Alkim 等人 [30] 全面提升了 Bos 等人的 KE 协议, 提出了 NewHope 密钥交换协议[1]. 如图2所示. 与 BCNS15 相比, NewHope 做出的主要改进包括:

- 使用 $\tilde{D}_4$ 格解码方法替换 Peikert 式错误协调, 可容忍更大的错误, 从而降低了模数, 缩减了通信量. BCNS15 中通信双方最终可以生成 1024 比特的会话密钥, 但是实际上 256 比特就足够了, 因此, 使用 $\tilde{D}_4$ 格解码, 刚好可以生成 256 比特的会话密钥. 这样, 协议中使用的模数 $q = 12289$ 只有 14 比特, 大大小于 BCNS15 使用的 32 比特.
- 将离散高斯分布替换为中心二项分布 Ψ_{16}, 以提高算法计算效率, 并证明了分布的替换不影响方案的安全性.
- 去掉了协议的固定公共参数, 环元素 a; 取而代之的是在每次协议执行时使用一个种子重新选取协议双方的公共参数, 有效地规避了在公共参数中植入陷门的 all-for-the-price-of-one 攻击; 这个种子的发送只增加了 256 比特 $= 32B$ 的通信量.
- 用 NTT(number-theoretic transform) [36] 提高计算效率. 协议中的模数 $q = 12289 \equiv 1 \bmod 2n$, 也是依据 NTT 的需求而选取的.

与 BCNS15 协议相比, NewHope 达到了相同维数下的两倍安全性和一半通信量. Alice 发送一个环元素和一个种子, 共 $14 \times 128B + 32B = 1824B$. Bob 发送一个环元素, 以及协调信息; 在 NewHope 中, 设置 $r = 2$, 即使用 2 比特离散化, 这样, 为了协调出一个比特, 需要发送一字节协调信息, Bob 的信息发送量一共为 $14 \times 128B + 256B = 2048B$. 在文献 [30] 中, 主要使用 Primal 攻击和 Dual 攻击评估方案的后量子安全性, 而 NewHope 的后量子安全性远超 128 比特.

与目前使用中的经典椭圆曲线密钥交换 ECDH 方案相比, NewHope 的计算效率更高; 通信量虽然比 ECDH 大不少, 但也是现实可接受的. 因此, 美国的谷歌公司于 2016 年在其 Chrome 浏览器中测试了 NewHope 方案的部署 [37], 该测试的结论是 NewHope 的部署对于通信并没有带来障碍.

3.4 Frodo

由于 LWE 的安全性较之环 LWE 更为稳健, 在 2016 年, Bos 等人 [31] 又基于 LWE 问题构造了一个基础 KE 协议, 称为 Frodo[2]. Frodo 可以视为 BCNS15 的无环优化版本. 为了降低通信量, 在 Frodo 中

[1]其命名来源于星球大战电影第四部, Star Wars: Episode IV - A New Hope
[2]其命名来自魔戒中人物, 持戒人 Frodo

使用 Peikert 式错误协调的多比特变形. 在其推荐参数设置中, 从每个 $\mathbb{Z}_q$ 元素中可提取出 4 比特, 这样, 为了生成 256 比特的会话密钥, 只需保证双方都能生成 64 个 $\mathbb{Z}_q$ 元素, 从而可以降低通信量.

Frodo 保留了 NewHope 中每次随机生成公共参数 (矩阵 $\mathbf{A}$) 的做法, 以避免在矩阵 $\mathbf{A}$ 中植入陷门的攻击, 但是矩阵 $\mathbf{A}$ 的生成占协议运行时间的 40%, 成为一个计算瓶颈. 较之 NewHope, Frodo 的安全性显得更可靠, 因为其直接基于 LWE, 而不是环 LWE; 在效率方面, Frodo 所需的计算时间和通信量都更大, 约为 NewHope 的十数倍.

Alice		Bob
$\mathsf{seed}_{\mathbf{A}} \xleftarrow{\$} U(\{0,1\}^s)$		
$\mathbf{A} \leftarrow \mathsf{Gen}(\mathsf{seed}_{\mathbf{A}})$		
$\mathbf{S}, \mathbf{E} \xleftarrow{\$} \chi(\mathbb{Z}_q^{n\times\bar{n}})$		
$\mathbf{B} \leftarrow \mathbf{AS} + \mathbf{E}$	$\xrightarrow{(\mathsf{seed}_{\mathbf{A}}, \mathbf{B})}$ $\in \{0,1\}^s \times \mathbb{Z}_q^{n\times\bar{n}}$	$\mathbf{A} \leftarrow \mathsf{Gen}(\mathsf{seed}_{\mathbf{A}})$
		$\mathbf{S}', \mathbf{E}' \xleftarrow{\$} \chi(\mathbb{Z}_q^{\bar{m}\times n})$
		$\mathbf{B}' \leftarrow \mathbf{S}'\mathbf{A} + \mathbf{E}'$
		$\mathbf{E}'' \xleftarrow{\$} \chi(\mathbb{Z}_q^{\bar{m}\times\bar{n}})$
		$\mathbf{V} \leftarrow \mathbf{S}'\mathbf{B} + \mathbf{E}''$
	$\xleftarrow{\mathbf{B}', \mathbf{C}}$ $\in \mathbb{Z}_q^{\bar{m}\times n} \times \mathbb{Z}_q^{\bar{m}\times\bar{n}}$	$\mathbf{C} \leftarrow \langle \mathbf{V} \rangle_{q,2^B}$
$K \leftarrow \mathsf{Rec}(\mathbf{B}'\mathbf{S}, \mathbf{C})$		$K \leftarrow \lfloor \mathbf{V} \rceil_{q,2^B}$

图 3 基于 LWE 的 Frodo 协议

Figure 3 The Frodo protocol from LWE

3.5 基于加密的构造

在基于格的密钥交换协议设计中使用错误协调机制可以减少通信量, 但是增加了方案的复杂度. 而使用基于加密的构造, Bob 选择会话密钥, 将其加密后发送给 Alice, 这种方法更为简单, 但是传输会话密钥的密文较之传输协调比特增加了通信量. 为了降低通信量, 需要使用密文压缩技术, 即将密文元素从 $\mathbb{Z}_q$ 映射到 $\mathbb{Z}_p$ 上, 其中 $p < q$. 由于密文元素的低位比特主要是噪音信息, 丢掉这些信息, 对恢复其所加密的密钥影响不大.

目前使用基于加密的方式构造的密钥交换 (传输) 协议主要有基于环 LWE 的 NewHope-Simple 和基于模 LWE 的 Kyber.KE.

3.5.1 NewHope-Simple

2016 年, Alkim 等人 [38] 提出了 NewHope 协议的简化版本 NewHope-Simple, 并使用了密文压缩技术, 使得通信量较之 NewHope 只增加了 6.25%. 协议如图4所示. NewHope-Simple 协议中环 R_q, 模数 q, 错误分布等参数的选取与 NewHope 中均相同. 主要差别在于 Bob 选择 256 比特长的随机串 ν, 使用 $\mathsf{NHSEncode}$ 函数将其编码为环元素 k, 即, 每四个 $\mathbb{Z}_q$ 元素中编码 ν 的一个比特, 与 $\tilde{D}_4$ 格的编码方法有类似之处. 随后, 环元素 k 被加密为环元素 c; 使用 $\mathsf{NHSCompress}$ 函数, c 中的每个分量都从 $\mathbb{Z}_q$ 压缩到 $\mathbb{Z}_8$ 中, 仅占用三个比特. 这样, 压缩后的密文只有 $3 \times 128B = 384B$; 与 NewHope 中 256B 的协调信息相比, 只增加了 128B.

3.5.2 Kyber.KE

2017 年, Bos 等人 [39] 在称为 CRYSTALS(Cryptographic Suite for Algebraic Lattices) 的格密码算法套装中推出了 Kyber 系列算法[3], 其中包括具有抗选择密文攻击 (chosen ciphertext attacks) 安全性的密钥封装方案 Kyber, 以及从 Kyber 得到密钥交换协议 Kyber.KE. 为了达到安全性和效率的最优,

[3]其命名来自于星球大战中制造光剑的原材料, Kyber 水晶

参数: $q = 12289 < 2^{14}$, $n = 1024$
错误分布: Ψ_{16}

Alice		Bob
$\text{seed} \xleftarrow{\$} \{0,1\}^{256}$		
$a \leftarrow \mathsf{Parse}(\mathsf{SHAKE}-128(\text{seed}))$		
$s, e \xleftarrow{\$} \Psi_{16}$		$s', e', e'' \xleftarrow{\$} \Psi_{16}$
$b \leftarrow as + e \in R_q$	$\xrightarrow{(b,\text{seed})}$	$a \leftarrow \mathsf{Parse}(\mathsf{SHAKE}-128(\text{seed}))$
		$u \leftarrow as' + e'$
		$\nu \xleftarrow{\$} \{0,1\}^{256}$
		$\nu' \leftarrow \mathsf{SHA3}-256(\nu')$
		$k \leftarrow \mathsf{NHSEncode}(\nu') \in R_q$
		$c \leftarrow bs' + e'' + k \in R_q$
$c' \leftarrow \mathsf{NHSDecompress}(\bar{c})$	$\xleftarrow{(u,\bar{c})}$	$\bar{c} \xleftarrow{\$} \mathsf{NHSCompress}(\bar{c})$
$k' \leftarrow c' - us$		$\mu \leftarrow \mathsf{SHA3}-256(\nu')$
$\nu' \leftarrow \mathsf{NHSDecode}(k')$		
$\mu \leftarrow \mathsf{SHA3}-256(\nu')$		

图 4 基于环 LWE 的 NewHople-Simple 协议
Figure 4 The NewHope-Simple Protocol from ring-LWE

Kyber 系列算法在模格上基于模 LWE 问题设计, 这使得算法既具有基于环 LWE 的方案的高效率, 其安全性更为可靠.

密钥封装方案 Kyber 包括三个算法: (Kyber.KeyGen, Kyber.Encaps, Kyber.Decaps). 其中 Kyber.KeyGen 生成公私钥对 (pk,sk); Kyber.Encaps 生成密文 c 和封装密钥 K; Kyber.Decaps 从密文 c 中解密得到 K. 这些算法中对公钥 pk 和密文 c 均使用了压缩技术. Kyber.KE 的结构完全基于这三个算法, 十分简单; 其总通信量包括 Kyber 的公钥 pk 和密文 c. 如图5所示.

Alice		Bob
$(\text{pk},\text{sk}) \xleftarrow{\$} \mathsf{Kyber.KeyGen}()$		
	$\xrightarrow{\text{pk}}$	
	$\xleftarrow{c}$	$(c, K) \xleftarrow{\$} \mathsf{Kyber.Encaps}(\text{pk})$
$\text{key} := \mathsf{Kyber.Decaps}(sk, c)$		$\text{key} := K$

图 5 基于模 LWE 的 Kyber.KE 协议
Figure 5 The Kyber.KE Protocol from module-LWE

Kyber.KE 的效率取决于密钥封装方案 Kyber 的效率. 在 Kyber 的推荐参数中, 使用的环 $R_q = \mathbb{Z}[x]/(x^{256}+1)$, 模 LWE 参数 $d = 3$, 模数 q 为 7681, 为 13 比特. 和 NewHope 中一样, Kyber 中模数的选取依据也是为了 NTT 的使用. Kyber 中的秘密和错误分布也均使用中心二项分布 β_η, 其参数 $\eta = 4$. 在这样的参数设置下, Kyber 的后量子安全性有 161 比特. 使用压缩技术, 其公钥只有 1088B, 而其密文只有 1184B. 因此, Kyber.KE 的通信量已经少于 NewHope; 其计算效率也与 NewHope 相当.

3.6 几类密钥交换协议的性能对比

表1给出了一些非认证密钥交换/传输协议的性能对比, 包括经典的 RSA-3072, ECDH 协议, 基于格的 BCNS, NewHope, 基于 NTRU 加密的密钥传输, Frodo(推荐参数), NewHope-Simple, Kyber.KE, 以及基于同源的 SIDH [40,41]. 其中 Kyber.KE 的数据来自于文献 [39], 测试平台有所不同; 其它方案的数据来自于文献 [31]. 在表1中, Alice0 表示 Alice 构造她输出消息的过程, 而 Alice1 是她处理从 Bob 处接收

表 1 几类密钥交换/传输协议的性能对比

Table 1 Performance of several key exchange protocols

方案	计算时间 (毫秒)			通信量 (字节)		安全性	
	Alice0	Bob	Alice1	$A \to B$	$B \to A$	经典	后量子
RSA-3072	0	0.09	0.49	387/0	384	128	0
ECDH	0.366	0.698	0.331	32	32	128	0
BCNS	1.01	1.59	0.174	4096	4224	163	76
NewHope	0.11	0.16	0.03	1824	2048	229	206
NTRU EES743EP1	2.00	0.28	0.15	1027	1022	256	128
Frodo(推荐参数)	1.13	1.34	0.13	11377	11296	144	130
NewHope-simple	-	-	-	1824	2176	229	206
*Kyber.KE	0.077	0.1	0.11	1088	1184	-	161
SIDH	135	464	301	564	564	192	128

到消息后的处理过程, 并且由此得到共享密钥. $A \to B$ 表示 Alice 给 Bob 发送的信息, $B \to A$ 表示 Bob 给 Alice 发送的信息.

从表上可以看出, 在计算效率上, 基于格的后量子密钥交换协议普遍表现较好, 尤其是 NewHope 和 Kyber.KE, 甚至超越了经典的 RSA 和 ECDH. 在通信量方面, 后量子密钥交换普遍大于经典协议, 只有 SIDH 的通信量可以接近经典协议, 但是 SIDH 的计算时间过长. 总体上, NewHope 和 Kyber.KE 在后量子密钥交换协议中表现得性能均衡, 已经高度实用化.

3.7 从无认证密钥交换到 AKE

以上介绍的各类基于格的密钥交换协议都是无认证协议, 只提供被动安全性; 而实际应用中必须要考虑网络上的主动攻击者. Peikert [28] 指出了在基于格的密钥交换协议在抵御主动型敌手时所面临的挑战; Fluhrer [42] 详细给出了一种针对 Ring-LWE 协议重用临时密钥的显式攻击. 因此, NIST 的算法征集项目中指出, 对于密钥交换协议提案, 需要给出将其增强为 AKE 的方法.

一般地, 通过与签名方案的结合, 可以为无认证密钥交换协议提供认证性 [29]. 尤其, del Pino 等人 [43] 使用带消息恢复功能的签名与无认证密钥交换协议结合, 即实现了认证性, 又节约了通信量.

此外, Fujioka 等人 [44] 提出了一个将具有 CCA 安全性的密钥封装机制转换为 AKE 的框架, 这个框架也适用于基于格的构造; 尤其, CCA 安全的密钥封装机制可以由基本的抗选择明文攻击 (chosen-plaintext attacks, CPA) 安全的密钥封装机制, 使用 Fujisaki-Okamoto [45] 的变换得到. Kyber 中即采用了这一方法, 得到了具有认证性的密钥交换协议 Kyber.AKE [39].

4 展望

目前政府, 工业界, 标准化组织等对于实用化后量子密码系统的需求较为迫切, 预计接下来未来几年将是实用化后量子密码学快速发展时期; 在后量子密钥交换协议方向尤其如此. 基于格密码中 LWE, 环 LWE 和模 LWE 问题设计的方案, 其参数尺寸和通信量合理, 计算高效, 是后量子公钥加密和密钥交换的希望之一, 尤其是基于环 LWE 的 NewHope 方案和基于模 LWE 的 Kyber 算法套装. 期待这一领域继续发展, 出现更为优秀的方案.

References

[1] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6): 644–654.

[2] KATZ J, VAIKUNTANATHAN V. Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices[C]. In: Advances in Cryptology—ASIACRYPT 2009. Springer Berlin Heidelberg, 2009: 636–652.

[3] DIERKS T, RESCORLA E. The Transport Layer Security (TLS) Protocol Version 1.2[S]. RFC 5246 (Proposed Standard), Aug. 2008.

[4] HALLGREN S. Fast quantum algorithms for computing the unit group and class group of a number field[C]. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing. ACM, 2005: 468–474.

[5] HALLGREN S. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem[J]. Journal of the ACM (JACM), 2007, 54(1): 4.

[6] SCHMIDT A, VOLLMER U. Polynomial time quantum algorithm for the computation of the unit group of a number field[C]. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing. ACM, 2005: 475–480.

[7] SHOR P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]. In: 35th Annual Symposium on Foundations of Computer Science, 1994. IEEE, 1994: 124–134.

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

[9] DEVORET M H, SCHOELKOPF R J. Superconducting circuits for quantum information: an outlook[J]. Science, 2013, 339(6124): 1169–1174.

[10] MOSCA M. Cybersecurity in an era with quantum computers: will we be ready?[J]. IACR Cryptology ePrint Archive, 2015, 2015: 1075.

[11] NSA Suite B cryptography: Cryptography today[OL]. https://www.nsa.gov/ia/programs/suiteb_cryptography/. 2015.

[12] NIST. Workshop on cybersecurity in a post-quantum world[OL]. http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm. 2015.

[13] AJTAI M. Generating hard instances of lattice problems[C]. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. ACM, 1996: 99–108.

[14] AJTAI M, DWORK C. A public-key cryptosystem with worst-case/average-case equivalence[C]. In: Proceedings of the 29th Annual ACM Symposium on Theory of Computing. ACM, 1997: 284–293.

[15] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: A ring-based public key cryptosystem[C]. In: International Algorithmic Number Theory Symposium. Springer Berlin Heidelberg, 1998: 267–288.

[16] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 34.

[17] PEIKERT C. A decade of lattice cryptography[J]. Foundations and Trends in Theoretical Computer Science, 2016, 10(4): 283–424.

[18] MICCIANCIO D, MOL P. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions[C]. In: Advances in Cryptology—CRYPTO 2011. Springer Berlin Heidelberg, 2011: 465–484.

[19] APPLEBAUM B, CASH D, PEIKERT C, et al. Fast cryptographic primitives and circular-secure encryption based on hard learning problems[C]. In: Advances in Cryptology—CRYPTO 2009. Springer Berlin Heidelberg, 2009: 595–618.

[20] LYUBASHEVSKY V, PEIKERT C, REGEV O. On Ideal Lattices and Learning with Errors over Rings[C]. In: Advances in Cryptology—EUROCRYPT 2010. Springer Berlin Heidelberg, 2010: 1–23.

[21] LYUBASHEVSKY V, PEIKERT C, REGEV O. A Toolkit for Ring-LWE Cryptography[C]. In:Advances in Cryptology—EUROCRYPT 2013. Springer Berlin Heidelberg, 2013: 35–54.

[22] PEIKERT C. How (not) to instantiate ring-LWE[C]. In: International Conference on Security and Cryptography for Networks. Springer International Publishing, 2016: 411–430.

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

[24] DODIS Y, REYZIN L, SMITH A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[C]. In: International conference on the theory and applications of cryptographic techniques. Springer Berlin Heidelberg, 2004: 523–540.

[25] DING J, XIE X, LIN X. A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem[J]. IACR Cryptology EPrint Archive, 2012, 2012: 688.

[26] ZHANG J, ZHANG Z, DING J, et al. Authenticated key exchange from ideal lattices[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 719–751.

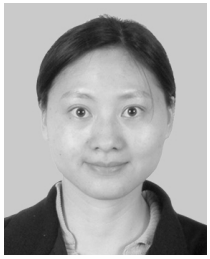
[27] DING J, ALSAYIGH S, LANCRENON J, et al. Provably secure password authenticated key exchange based on RLWE for the post-quantum world[C]. In: Cryptographers' Track at the RSA Conference. Springer, 2017: 183–204. .

[28] PEIKERT C. Lattice cryptography for the internet[C]. In: International Workshop on Post-Quantum Cryptography. Springer, 2014: 197–219.

[29] BOS J W, COSTELLO C, NAEHRIG M, et al. Post-quantum key exchange for the TLS protocol from the ring

learning with errors problem[C]. In: 2015 IEEE Symposium on Security and Privacy (SP). IEEE, 2015: 553–570.
[30] ALKIM E, DUCAS L, PÖPPELMANN T, et al. Post-quantum key exchange—A new hope[C]. In: USENIX Security Symposium, 2016: 327–343.
[31] BOS J, COSTELLO C, DUCAS L, et al. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE[C]. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 1006–1018.
[32] JIN Z, ZHAO Y. Optimal key consensus in presence of noise[J]. arXiv preprint arXiv:1611.06150, 2016.
[33] DING J. Cryptographic systems using pairing with errors: U.S. Patent 9,246,675[P]. 2016-1-26.
[34] LINDNER R, PEIKERT C. Better key sizes (and attacks) for LWE-based encryption[C]. In: Proceedings of the 11th International Conference on Topics in Cryptology: CT-RSA 2011. Springer-Verlag, 2011: 319–339.
[35] ALBRECHT M R, PLAYER R, SCOTT S. On the concrete hardness of learning with errors[J]. Journal of Mathematical Cryptology, 2015, 9(3): 169–203.
[36] LONGA P, NAEHRIG M. Speeding up the number theoretic transform for faster ideal lattice-based cryptography[C]. In: International Conference on Cryptology and Network Security. Springer International Publishing, 2016: 124–139.
[37] BRAITHWAITE M. Google Security Blog: Experimenting with post-quantum cryptography, July 2016[OL].
[38] ALKIM E, DUCAS L, PÖPPELMANN T, et al. NewHope without reconciliation[J]. IACR Cryptology ePrint Archive, 2016, 2016: 1157.
[39] BOS J, DUCAS L, KILTZ E, et al. CRYSTALS–Kyber: a CCA-secure module-lattice-based KEM[J]. IACR Cryptology ePrint Archive, 2017, 2017: 634.
[40] COSTELLO C, LONGA P, NAEHRIG M. Efficient algorithms for supersingular isogeny Diffie-Hellman[C]. In: Advances in Cryptology—CRYPTO 2016. Springer Berlin Heidelberg, 2016: 572–601.
[41] LUCA D F, DAVID J, JÉRÔME P. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies[J]. Mathematical Cryptology, 2014, 8(3): 209–247.
[42] FLUHRER S R. Cryptanalysis of ring-LWE based key exchange with key share reuse[J]. IACR Cryptology ePrint Archive, 2016, 2016: 85.
[43] DEL PINO R, LYUBASHEVSKY V, POINTCHEVAL D. The whole is less than the sum of its parts: Constructing more efficient lattice-based AKEs[C]. In: International Conference on Security and Cryptography for Networks. Springer International Publishing, 2016: 273–291.
[44] FUJIOKA A, SUZUKI K, XAGAWA K, et al. Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism[C]. In: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. ACM, 2013: 83–94.
[45] FUJISAKI E, OKAMOTO T. How to enhance the security of public-key encryption at minimum cost[C]. In: International Workshop on Public Key Cryptography. Springer Berlin Heidelberg, 1999: 53–68.

作者信息



刘亚敏 (1983–), 湖南邵阳人, 助理研究员. 主要研究领域为公钥密码算法的设计.
E-mail:
ymliu@is.ac.cn

李祥学 (1974–), 江苏连云港人, 博士, 研究员. 主要研究领域为安全技术.
E-mail:
xxli@cs.ecnu.edu.cn

刘晗林 (1993–), 湖南衡阳人, 硕士研究生. 主要研究领域为密码学.
E-mail:
hans1024@sjtu.edu.cn