计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200400138

# 基于格的抗量子认证密钥协商协议研究综述

倪 亮[1] 王念平[2] 谷威力[1] 张 茜[1] 刘伎昭[1] 单芳芳[1]
1 中原工学院计算机学院 郑州 450007
2 中国人民解放军战略支援部队信息工程大学 郑州 450001

**摘 要** 最近在量子计算研究领域所取得的进展对当前网络安全协议中大多数的安全性依赖传统数论难题的方案构成了严重的潜在安全威胁,作为基础性网络安全协议的认证密钥协商协议首当其冲。由此,抗量子认证密钥协商协议成为了近来的一个研究热点。其中,基于格的后量子密码(Post-Quantum Cryptography)方案由于安全性强、计算效率高,于近年得到了广泛重视且现在正快速发展,有望被列入未来的抗量子密码算法标准。文中重点关注基于格的后量子认证密钥协商协议研究。首先,对抗量子认证密钥协商协议的研究背景进行介绍,并对当前基于格的后量子密码方案安全性设计所基于的主要计算性困难问题进行描述;接着,对现有典型基于格的后量子认证密钥协商协议进行概述,并以两方协议为主要研究对象,对相关方案的基本构造模式和若干当前典型相关协议的性能进行讨论、分析和比较;最后,对当前研究中存在的问题进行总结,并对相关研究的未来发展进行展望。

**关键词**:抗量子安全协议;后量子密码;基于格的密码;认证密钥协商;可证明安全
**中图法分类号** TP309

## Research on Lattice-based Quantum-resistant Authenticated Key Agreement Protocols:A Survey

NI Liang[1],WANG Nian-ping[2],GU Wei-li[1],ZHANG Qian[1],LIU Ji-zhao[1] and SHAN Fang-fang[1]
1 School of Computer Science,Zhongyuan University of Technology,Zhengzhou 450007,China
2 The PLA Strategic Support Force Information Engineering University,Zhengzhou 450001,China

**Abstract** Recent advances in quantum computing have posed a serious potential security threat to the majority of current network security protocols,whose security relies on classical number-theoretic hard problems. As the basic network security protocols,authenticated key agreement protocols bear the brunt. Therefore,quantum-resistant authenticated key agreement protocols have become a recent hot research topic. Thereinto,lattice-based post-quantum cryptographic schemes,with strong security and high computational efficiency,have gained extensive attention in recent years,and are developing rapidly,which are expected to be included in the future standards of quantum-resistant cryptographic algorithms. In this paper,research on lattice-based post-quantum authenticated key agreement protocols is focused on. Firstly,the research background of quantum-resistant authenticated key agreement protocols is introduced,and the main computational hard problems that the security designs of current lattice-based post-quantum cryptographic schemes depend on are also described. Then,an overview of the existing typical lattice-based post-quantum authenticated key agreement protocols is given,and by taking the two-party protocols as the main research object,the basic construction modes of related schemes and performance of several current typical related protocols are discussed,analyzed and compared. Lastly,the existing problems in the current research are summarized,and the future development of related research is also forecasted.

**Keywords** Quantum-resistant security protocol,Post-quantum cryptography,Lattice-based cryptography,Authenticated key agreement,Provable security

到稿日期:2020-04-29 返修日期:2020-07-08 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:河南省科技攻关计划项目(182102210130,192102210286);国家留学基金(201908410281);河南省高等学校重点科研项目(18A520052);国家自然科学基金(61672031)
This work was supported by the Science and Technology Research Program of Henan Province of China (182102210130,192102210286),State Scholarship Fund of China (201908410281),University Key Research Program of Henan Province of China (18A520052) and National Natural Science Foundation of China (61672031).
通信作者:倪亮(niliang402@zut.edu.cn)

## 1 引言

当前，人类正处于信息科学与技术飞速发展的时代，信息网络的广泛应用已成为社会进步和发展的重要标志之一。近年来，移动互联网技术、物联网和云计算等新型网络应用形式的出现，极大拓展了网络应用范围，也对安全性提出了更高要求，如何保证传输安全成为其中的核心问题。传输安全指的是建立在通信实体身份认证基础上的传输消息机密性、完整性和不可否认性等安全保护。密码技术是信息安全的核心技术，是网络空间安全的基石。基于密码理论和技术构建的方案为目前各类网络应用提供全方位的安全保证机制，特别地，主要依赖公钥密码技术构建的安全协议已成为网络空间安全的重要保障。

密钥协商协议是一类极其重要的基础性安全协议。在开放的网络环境中，借助密钥协商协议，两个或多个参与者通过利用其长期私钥和网络中所交换的临时消息能够产生一个共享的会话密钥。此共享的会话密钥随后可被用于保密通信或消息认证。认证密钥协商协议不仅允许参与者计算出会话密钥，而且能确保协议涉及参与者的认证性。由于实际应用中需要保证密钥协商的认证性和会话密钥的机密性，认证密钥协商协议成为核心的研究对象，这是保证后续通信安全的一种重要机制：利用所建立的会话密钥，参与者们可以在开放的网络中建立安全信道，从而保证传输消息的安全性。由此，构造安全的密钥协商协议对于设计安全可靠的网络通信系统起着基础性的重要作用，同时安全的密钥协商协议也是构建复杂的高层安全协议或安全系统的基础。

如何构建安全且高效的认证密钥协商协议一直是相关学术领域乃至信息技术行业领域研究和关注的一个热点。1976年，Diffie等[1]首次引入公钥密码思想，并基于经典数论难题——离散对数问题提出了著名的DH(Diffie-Hellman)协议，这是第一个真正意义上的密钥协商协议。但原始DH协议由于缺乏认证能力，容易遭受中间人攻击。为弥补这一漏洞，学者们开始对认证密钥协商协议展开研究。随后出现了大量改进的基于DH协议模块的认证密钥协商协议方案，且基于大整数分解问题等其他经典数论难题的一些认证密钥协商协议也陆续被提出。

当前，网络信息系统中广泛部署的许多至关重要的安全协议(包括TLS和IKE等因特网实用密钥协商类协议)，主要是利用RSA公钥体制、传统椭圆曲线公钥体制ECC和Diffie-Hellman密钥协商体制来实现的。这些传统公钥密码体系的安全性往往建立在一些经典数论难题的基础上，如大整数分解问题和在不同群上的离散对数问题。1994年，Shor[2]展示了量子计算机可在多项式时间内高效解决大整数分解和离散对数问题。由此，一旦有足够规模的量子计算机诞生，将使许多现代通信方式处于危险之中。近年来，量子计算技术发展突飞猛进，量子计算机研制进展迅速[3-5]，这使得对于上述经典计算机来说足够“困难”的问题必将在可预期的将来被轻易破解。尽管真正全功能型量子计算机何时才能出现目前尚没有准确预期，但研究者们普遍认为若当前不采取实质性预防措施，网络安全体系的崩溃很可能就是不远将来的确定性事件。而真正威胁当前密码的是专用量子计算机，因为一旦专用，制造工程的难度就会大幅降低；此外，网络安全领域研究者还应考虑“现在拦截，将来破解”的威胁模式[6]。因此，虽然大规模实用型通用量子计算机的出现可能还需数十年，但这种能力本身已具有了现实性威胁。这使得研究量子计算环境下安全的密码系统成为网络安全领域中一个迫切需要解决的基础性问题。在目前大量应用的密码算法中，已知的量子计算威胁对公钥密码的影响更显著，因为对称密码系统还可通过采取使密钥长度加倍等升级措施来应对量子威胁[7]；而公钥密码系统必须采取全新的方法来重建，由此也就成为了抗量子密码技术发展的重点领域。

后量子密码又称抗量子密码(Quantum-Resistant Cryptography)，其可在经典计算机上运行，被认为能够抵抗量子计算机攻击的密码体制[7]。与量子密码不同，此类密码技术开发采取传统方式，即基于特定数学领域困难问题研究开发算法，其应用不依赖于任何量子理论现象，但其计算安全性据信可抵御当前已知的任何形式的量子攻击。更为重要的是，它们还可与当前网络系统实现较高程度的兼容，从而减小当前密码系统向抗量子密码系统迁移时可能面临的阻力，具有较强的实践性、实用性和可操作性。

虽然对于量子计算机能否实现或何时实现这个问题还存在一些争议，但各国政府及研究机构已发起了设计在经典和量子计算模型下都安全的各类公钥密码算法的重大研究计划，从而达到以此逐步替代现有密码算法以确保信息安全的目的。当前，许多发达国家已着力加强后量子密码的研究，并设立了各类重大研究支持计划，如日本的CryptoMathCREST项目、欧洲的SAFEcrypto项目和PQCrypto项目等。美国国家安全局于2015年8月公开宣布计划将联邦政府各部门目前使用的ECC/RSA算法体系向后量子算法进行迁移以应对量子计算的威胁；美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)也于2016年2月正式面向全球公开了后量子密码标准化的路线图，并在同年秋正式公布征集后量子密码系统提案的计划，其最终正式的后量子密码算法标准拟于2021－2023年出台。

当前，国际后量子密码研究主要集中在对基于Hash函数的公钥密码、基于编码的公钥密码、多变量公钥密码、基于格的公钥密码以及超奇异椭圆曲线同源密码等的研究。其中，基于Hash函数的公钥密码和多变量公钥密码在构造签名方案时较有优势；基于编码的公钥密码更适合构造加密方案；超奇异椭圆曲线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，但是其计算效率很低，还达不到实用性要求且对其安全性的研究也还处于初始阶段，其安全强度也需要经历更多的密码分析及时间考验[7-9]。

在所有被认为具有抵御量子威胁潜力的公钥密码体制中，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。已知存在多种格上难题在量子计算下还没有多项式时间高效求解算法，如其中的基础核心问题——最短向量问题(Shortest Vector Problem，SVP)及最近向量问题(Closest Vector Problem，CVP)等。因此，格密码算法可抵御量子攻击。格密码算法还具有两个突出优点：1)安全性高，因

为格上密码算法的安全性可以归约到格上难题最坏情形下的困难性；2）计算速度快，因为格上密码不需要大整数运算，仅涉及单精度整型向量的加法和乘法以及格上高斯抽样等。目前，NTRU 体系[10]以及带误差的学习（Learning With Errors，LWE）问题体系[11-13]是基于格密码系统发展实用前景最好的两种方案构建形式。近年来，基于格的密码体制得到了广泛重视且正在快速发展，格密码有望在未来成为后量子密码技术的标准。

本文重点聚焦格上后量子认证密钥协商协议的研究。本文首先介绍了文中主要涉及的格密码基本原理；然后对基于格的后量子认证密钥协商协议的研究现状进行了回顾和分析；最后，通过对当前相关研究中所存在的问题进行讨论，总结并展望格上后量子认证密钥协商协议的研究方向及其相关领域未来发展的趋势。

## 2　基本原理

本节将对相关基本概念和基本原理进行简单回顾[14]，重点对当前相关典型格密码方案安全性设计基于的主要格上现代计算性困难问题进行简要描述，以帮助理解后文。

### 2.1　符号表示

令 $\mathbb{Z}$ 代表整数集，$\mathbb{R}$ 代表实数集。对于一个实数 $r\in\mathbb{R}$，用 $\lfloor r\rfloor$ 代表不大于 $r$ 的最大整数，用 $\lfloor r\rceil=\lfloor r+1/2\rfloor$ 代表与 $r$ 最为接近的整数。对于任意正整数 $a$ 和 $b$，使用符号 $lcm(a,b)$ 来表示 $a$ 和 $b$ 的最小公倍数。对于任意整数 $i,j\in\mathbb{Z}$，若 $i<j$，则使用符号 $[i,j]$ 来表示整数的集合 $\{i,i+1,\cdots,j-1,j\}$。令 $\chi$ 代表分布，$e\leftarrow\chi$ 表示根据分布 $\chi$ 随机选取 $e$；若 $S$ 是一个集合，则 $x\leftarrow S$ 表示从集合 $S$ 中均匀随机选取一个元素 $x$。用粗体大写字母（如 $\boldsymbol{B}$）表示矩阵，并且将矩阵 $\boldsymbol{B}$ 的转置矩阵记为 $\boldsymbol{B}^t$；用粗体小写字母（如 $\boldsymbol{b}$）表示向量，并且将向量 $\boldsymbol{b}$ 的转置向量记为 $\boldsymbol{b}^t$。下文所有出现的向量都默认为列向量。设两个向量 $\boldsymbol{x},\boldsymbol{y}\in\mathbb{R}^n$，其中 $n$ 是一个正整数，且有 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$，$\boldsymbol{y}=(y_1,y_2,\cdots,y_n)$，则向量 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的内积用 $\boldsymbol{x}\cdot\boldsymbol{y}$ 或 $\langle\boldsymbol{x},\boldsymbol{y}\rangle$ 来表示：$\boldsymbol{x}\cdot\boldsymbol{y}=\langle\boldsymbol{x},\boldsymbol{y}\rangle=x_1y_1+x_2y_2+\cdots+x_ny_n$。

### 2.2　格上主要现代计算性难题

1996 年，Ajtai[15]首先利用基于格的计算难题——短整数解（Short Integer Solution，SIS）问题，构造了抗碰撞哈希函数。在后续工作中，Ajtai 等[16]又给出利用其他基于格的难题构造的公钥密码方案。同时，Hoffstein 等[10]给出了基于多项式环的 NTRU 公钥加密方案，其安全性也与基于格的难题密切相关。2005 年，Regev[11]提出带误差的学习难题，并证明了 LWE 难题与格上基本难题（如近似最短向量问题 GapSVP）是紧密相关的，还给出了基于 LWE 难题的公钥密码方案。此后又出现了一系列以 Regev 的工作[11]为基础的有关基本 LWE 难题的变体及由其所构造的密码方案[12-13,17-19]。与从前的格上基本难题相比，LWE 系列难题在构造密码方案时更为方便，因此有大量关于 LWE 系列问题的困难性及其在密码学中应用的研究[14]。

下文主要对 LWE 系列难题进行概述，目前大多数基于格的密码方案都是直接基于这类难题进行设计的。设参数 $n,m,q$ 为正整数，其中 $m$ 是次要的，因此有时甚至并不对其进行明确定义；$n$ 是须被考虑的主要“困难性”参数（如选取 $n\geqslant100$）。设 $\chi$ 为 $\mathbb{Z}$ 上的一个分布，称为误差分布。为了方便定义，先给出 *LWE* 分布的定义。对于一个称为秘密的向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$，LWE 分布 $A_{\boldsymbol{s},\chi}\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ 通过以下方式来取样，即：均匀随机选取 $\boldsymbol{a}\in\mathbb{Z}_q^n$，且选择 $e\leftarrow\chi$，然后输出 $(\boldsymbol{a},b=\langle\boldsymbol{s},\boldsymbol{a}\rangle+e \bmod q)$。

（1）搜索性 LWE 问题：对于一个均匀随机选择的秘密向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$，给定 $m$ 个取自 LWE 分布 $A_{\boldsymbol{s},\chi}$ 的独立抽样 $(\boldsymbol{a}_i,b_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$（$\boldsymbol{s}$ 对于所有抽样来说是固定的），求解秘密 $\boldsymbol{s}$。

（2）判定性 LWE 问题：给定 $m$ 个独立抽样 $(\boldsymbol{a}_i,b_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$，其中每个抽样或者选自 LWE 分布 $A_{\boldsymbol{s},\chi}$（对于来自 LWE 分布 $A_{\boldsymbol{s},\chi}$ 的所有抽样，其均匀随机选择的秘密向量 $\boldsymbol{s}\in R_q^k$ 是固定的）或者选自均匀分布 $U$，判定性 LWE 问题就是以不可忽略的优势来区分上述抽样的分布究竟属于哪种情况。

当选择合适的参数 $n,m,q,\chi$ 时，搜索性 LWE 问题难度与格上基本计算问题相关。Regev[11]使用量子规约技术将 LWE 问题的平均情况难度和随机格上 $\mathrm{GapSVP}_\gamma$ 和 $\mathrm{SIVP}_\gamma$ 问题的最坏情况的难度联系起来，其中参数 $\gamma$ 的选择与 LWE 问题的参数有关。当选择适当的参数时，搜索性 LWE 问题和判定性 LWE 问题是多项式等价的[20]。

通常，LWE 问题中的错误分布 $\chi$ 是宽度为 $\alpha q$ 的离散高斯分布，其中 $\alpha<1$ 称为错误率。在早期研究中，LWE 的秘密 $\boldsymbol{s}$ 服从均匀分布。然而，Applebaum 等[21]给出 LWE 的短秘密（Short Secrets）变体形式，即选取 $\boldsymbol{s}\leftarrow\chi^n$，并证明这种变体与使用均匀秘密分布的 LWE 问题的难度相当。在当前基于格后量子密钥协商协议中，经常使用的是 LWE 的这种短秘密变体形式。

关于 LWE 问题，还存在一个变体，称为带取整的学习（Learning With Rounding，LWR）问题[17]。本质上，LWR 问题是使误差成为确定性的关于 LWE 问题的“去随机化（Derandomized）”变体。类似于 LWE 问题的定义，我们首先给出 *LWR* 分布的定义。令 $\chi_s$ 为 $\mathbb{Z}_q^n$ 上的某个分布，选择 $\boldsymbol{s}\leftarrow\chi_s$。对于整数 $q\geqslant p\geqslant2$ 以及任意 $x\in\mathbb{Z}_q$，定义 $\lfloor x\rceil_p=\lfloor x\cdot(p/q)\rceil$。那么，对于正整数 $n$ 和 $q\geqslant p\geqslant2$，LWR 分布 $\boldsymbol{A}_{n,q,p}(\boldsymbol{s})\in\mathbb{Z}_q^n\times\mathbb{Z}_p$ 通过以下方式获得：从 $\mathbb{Z}_q^n$ 中均匀随机抽样 $a$，然后输出 $(a,\boldsymbol{s}\in R_q^k)\in\mathbb{Z}_q^n\times\mathbb{Z}_p$。下面对 LWR 问题进行简要描述。

（3）LWR 问题：简要地说，（判定性）LWR 问题描述的是，对于足够大的安全参数，没有多项式时间的敌手（算法）$\mathcal{A}$ 能够以不可忽略的概率区分 *LWR* 分布 $\boldsymbol{A}_{n,q,p}(\boldsymbol{s})\in\mathbb{Z}_q^n\times\mathbb{Z}_p$ 和均匀分布 $U=(a\leftarrow\mathbb{Z}_q^n,\lfloor u\rceil_p)$（其中，$u\leftarrow\mathbb{Z}_q$）。即使 $\mathcal{A}$ 能够访问多项式数量级的抽样，这个问题也是成立的。

Banerjee 等[17]提供了针对超多项式数量级 $q$ 的从 LWE 问题到 LWR 问题的一个有效规约。令 $b$ 代表秘密向量 $\boldsymbol{s}$ 中任意组件的界，Bogdanov 等[22]则展示出：当 $q\geqslant2mbp$（即 $m\leqslant q/2bp$）时，LWE 问题能够被规约为具有 $m$ 个独立随机抽样的（判定性）LWR 假设，而且，实际上从 LWE 到 LWR 的规约与秘密向量 $\boldsymbol{s}$ 的分布是独立的。

基于 LWE 问题构造的安全方案，由于参数中包含大矩阵，因此其密钥、密文等参数尺寸通常很大，这在一定程度上

对基于格的后量子密码系统的实用化起到了阻碍作用。在NTRU等方案的启发下，Lyubashevsky等[12-13]提出了环LWE问题。定义整系数多项式环：$R=\mathbb{Z}[x]/(x^n+1)$，其中$n$为$2^k$的形式，$k$为正整数。设$q$为正整数，并定义环$R_q=\mathbb{Z}_q[x]/(x^n+1)$。也就是说，$R_q$包含了所有次数最多为$n-1$的多项式，并且其系数都在$\mathbb{Z}_q$中。与基本的LWE问题类似，下面给出相关的搜索性和判定性环LWE(RLWE)问题。首先，定义RLWE分布的概念。设$\chi$为$R_q$上的分布，对于一个称为秘密的$s\in R_q$，RLWE分布$A_{s,\chi}\in R_q\times R_q$通过以下方式来取样：均匀随机选取$a\in R_q$，且选择$e\leftarrow\chi$，输出$(a,b=s\cdot a+e \bmod q)$。下面给出RLWE问题的描述。

(4)搜索性RLWE问题：对于一个均匀随机选择的秘密$s\in R_q$，给定取自RLWE分布$A_{s,\chi}$的抽样$(a,b=s\cdot a+e \bmod q)\in R_q\times R_q$，求解秘密$s$。

(5)判定性RLWE问题：给定$m$个独立的抽样$(\boldsymbol{a}_i,b_i)\in R_q\times R_q$，其中的每个抽样或者选自RLWE分布$A_{s,\chi}$(对于来自RLWE分布$A_{s,\chi}$的所有抽样，其均匀随机选择的秘密$s\in R_q$是固定的)或者选自均匀分布$U$，判定性*RLWE*问题就是以不可忽略的优势来区分上述抽样的分布究竟属于哪种情况。

当选择合适的参数时，RLWE问题的困难性可规约为理想格上的$\mathrm{SVP}_\gamma$问题的困难性(而LWE问题的困难性基于一般格上的困难问题)。LWE问题中的短秘密变体、搜索性和判定性问题的等价性等结论，也适用于RLWE的情况。

RLWE问题利用了理想环的代数结构，一方面提高了基于其设计的密码方案的效率，另一方面也带来了一定程度的安全性隐患[23-26]。Langlosis等对模格(Module Lattice)上的LWE(MLWE)问题[18]进行了研究。模(Module)作为一种代数结构，是环和向量空间的一般化；而模格是对理想格和一般格的推广。因而，MLWE问题是LWE问题和RLWE问题的推广。通过选择合适的参数，基于MLWE构造的密码系统可以在安全性和效率之间较好地达到平衡。下面给出MLWE问题的描述。

首先，给出关于MLWE分布的定义。设$n,m,q,k$为正整数，$\chi$为$R_q$上的分布。对于一个秘密$\boldsymbol{s}\in R_q^k$，MLWE分布$A_{s,\chi}\in R_q^k\times R_q$通过以下方式来取样：均匀随机选取$\boldsymbol{a}\in R_q^k$，且选择误差$e\leftarrow\chi$，输出$(\boldsymbol{a},b=\langle\boldsymbol{s},\boldsymbol{a}\rangle+e \bmod q)$。接下来，给出MLWE问题的描述。

(6)搜索性MLWE问题：对于一个均匀随机选择的秘密$\boldsymbol{s}\in R_q^k$，给定$m$个取自MLWE分布$A_{s,\chi}$的独立抽样$(\boldsymbol{a}_i,b_i)\in R_q^k\times R_q$($\boldsymbol{s}$对于所有抽样来说是固定的)，求解秘密$\boldsymbol{s}$。

(7)判定性MLWE问题：给定$m$个独立抽样$(\boldsymbol{a}_i,b_i)\in R_q^k\times R_q$，其中每个抽样或者选自MLWE分布$A_{s,\chi}$(对于来自MLWE分布$A_{s,\chi}$的所有抽样，其均匀随机选择的秘密向量$\boldsymbol{s}\in R_q^k$是固定的)或者选自均匀分布$U$，判定性*MLWE*问题就是以不可忽略的优势区分上述抽样分布究竟属于哪种情况。

参数$k$和环$R_q$的选择可以使MLWE的安全性和效率灵活折中。当$k=1$，环$R_q=\mathbb{Z}_q[x]/(x^n+1)$时，MLWE问题转化为RLWE问题；当将环$R_q$设置为$\mathbb{Z}_q$时，MLWE问题又转化为一般LWE问题。当使用MLWE构建密码方案时，增加环维度$n$，降低$k$，可以提高方案的效率；同时，$k$越小，意味着具有更多的代数结构，从而可能增加安全隐患。

另外，仿效MLWE问题，若将基本的LWR问题应用到模格之上，也可以得到相应模格上的LWR(MLWR)问题[19]。关于MLWR问题的具体细节本文不再赘述。

## 3 研究现状分析

如前文所述，由于格密码的自身优势，目前对于抗量子(后量子)认证密钥协商协议的研究很多都是集中在基于格的方案研究方面。格上困难问题具有抗量子攻击的特性，当前在构造相关方案时经常利用的典型后量子难题包括LWE系列问题等。然而，格系统中元素的乘法操作并不满足可交换性。如，基于LWE类问题设计密钥协商协议的一个关键难题就是这些问题中往往带有误差：一方面，误差对其后量子困难性有重要作用，没有误差，这些问题可轻易求解；另一方面，基于这些问题构造密钥协商协议时，误差的存在使协议各方只能得到近似相等的值。因此，基于格的认证密钥协商协议的设计不能完全照搬Diffie-Hellman类协议的构建模式，必须拓展新的思路来解决基于格的认证密钥协商问题。如对误差的处理就是对基于格的密钥建立方案设计的一个技术挑战，该挑战可使用两种方法来解决：1)使用误差协调机制(Error Reconciliation Mechanism)，其关键就是采用各种误差调和技术，其思想类似于模糊提取器(Fuzzy Extractor)[27]；2)直接对会话密钥进行加密等操作后传送(由此构造的方案在本质上应属于密钥传输协议)，其关键就是采用密文压缩技术。另外，基于格的密钥协商协议的设计有时也可能会借助SIS问题，必须设计合理的编解码机制以支持协议方案的高效实现。由于引入了噪声(即误差)，协议产生的会话密钥存在一定的错误概率，而且收发双方发送的协议消息结构难以构造成完全对称的形式，但可通过适当的参数设置将错误概率降低到可以忽略的程度。

总体来说，现有基于格的密钥协商协议的构建方式主要有两种：1)基于后量子难题直接进行协议构造，如基于(R)LWE难题，并通过引入噪声(误差)来设计密钥协商协议；2)基于密钥封装机制(Key Encapsulation Mechanism，KEM)[28]构造密钥协商协议。基于KEM的方式一般需要发送方对某些秘密比特进行编码，收发双方必须从协商出的秘密信息中通过特定的解码技术抽取共同的秘密比特。KEM可由相关的后量子公钥加密算法转换所得，利用KEM会使得秘密比特得以安全地传输，从而给安全密钥协商协议的构造带来极大的方便。然而，基于KEM的协议构造难以克服效率受限的弊端。由此，构建不依赖于KEM的高效密钥协商协议成为一个重要的科学问题。

### 3.1 主要相关工作概述

构建类似原始Diffie-Hellman协议[1]这样高效的格上密钥协商协议依然是后量子密码方案设计领域的一个重要目标。在此方面，Ding等[29]利用基本LWE问题构造了首个安全性依赖于格上难题的密钥协商协议，该协议是被动安全的，

具有与原始 Diffie-Hellman 协议类似的对称结构，执行也较为高效，而且可扩展到基于 RLWE 问题的密钥协商协议，从而使得密钥更短且效率更高。Ding 等的协议[29]构建没有借助 KEM 机制，其核心思想是通过引入噪声，并借助所设计的一个巧妙的误差协调机制（Ding 式误差协调）实现了密钥协商，这为格上后量子密钥协商协议的后续研究带来了许多新的启示。

此后，Peikert[30]基于 RLWE 问题构造了一个被动安全的高效 KEM，并提出了一种变形的误差协调机制（Peikert 式误差协调），利用 SIGMA 范式[31]将该 KEM 体制与基于格的数字签名和 MAC 体制结合，从而得到后量子认证密钥协商协议。Bos 等[32]将类 Peikert 式的格上被动安全的协议[30]嵌入 TLS 协议中，借助数字签名构造出显示认证的协议（BCNS 方案），但若借助 RSA 签名和 DSA 签名这类传统认证机制并不能构造出一种完整的后量子认证密钥协商解决方案。Zhang 等[33]基于 Ding 等的密钥协商协议[29]，使用理想格构造出与 HMQV[34]在结构上类似的认证密钥协商协议，该协议具有弱完美前向保密性，且未使用 KEM 和数字签名等密码机制，效率较高。他们还使用弱的 BR 模型，在随机预言模型[35]下证明了所提方案的安全性是基于 RLWE 问题。Alkim 等[36]深入分析了 Bos 等的协议方案及其实施[32]，提出被称为 NewHope（新希望）的改良协议，他们通过设置新的参数，推荐更合适的误差分布以及引入更有效的误差调和机制等改进措施，使方案执行效率和安全性得以大幅度提升；之后，他们基于加密方式并借助密文压缩技术，又给出 NewHope 协议的一个简化变体 NewHope-Simple[37]。通过借鉴 Ding 等的基于 LWE 问题的协议设计思想[29]，Bos 等[38]又在一般格（标准格）上构造了基于基本 LWE 问题的后量子认证密钥协商协议——Frodo，该协议具有前向保密性，并采用有效可抽样噪音分布和有效而动态的公开参数生成等设计思路，吸取并扩展了 Peikert 式误差协调技术[30]，可被视为 BCNS 协议[32]的无环优化版本，而基本 LWE 难题较 RLWE 难题更为稳健，因此其安全性显得更为可靠，他们将所提方案嵌入 TLS 协议，展示了该方案在性能上甚至能与某些理想格上基于 RLWE 问题的相关方案媲美。然而，与 NewHope 协议[36]相比，Frodo 所需的计算时间和通信量要多得多。Jin 等[39-40]提出了密钥共识（Key Consensus）的概念，其中对现有的一些基于格的相关协议方案[36,38]中的误差协调机制进行了总结并做出了优化。Bos 等[41]在 CRYSTALS（Cryptographic Suite for Algebraic Lattices）的格密码套装中推出了 Kyber 系列算法，其中包括具有 CCA 安全的 KEM 方案 Kyber 和从 Kyber 得到的密钥交换（密钥传输）协议 Kyber.KE。Kyber 系列算法在模格（Module Lattice）上基于模 LWE（Module Learning With Errors，MLWE）问题[18]设计，在效率和安全性之间达到了较好的平衡。D'Anvers 等[19]给出密码原语包 Saber，其中包括 CCA 安全的 KEM 方案和由此得到的结构与 Diffie-Hellman 类协议相似的认证密钥协商方案，其安全性基于模 LWR（Module Learning With Rounding，MLWR）问题。与安全性基于 MLWE 问题的 Kyber 方案[41]相比，Saber 方案不需要噪声采样，节省了计算时间和熵的使用，进一步减小了通信带宽，更便于实施。

### 3.2　相关协议基本设计模式的分析和讨论

基于上述相关典型协议方案的设计结构，本文对当前基于格的抗量子认证密钥协商协议的基本构造机制进行了更深入的探讨，在此重点对两方协议的基本设计模式进行分析了和讨论。

从现有大多数格上抗量子（后量子）认证密钥协商协议的构建来看，首先被动安全的密钥协商协议是设计认证密钥协商协议的基础本原，设计高效合理的被动安全密钥协商协议是成功设计实用认证密钥协商协议的一个重要前提。被动安全的密钥协商协议构造需要实现以下两个主要目标。1）会话密钥的正确性：各协议参与方（合法用户）在协议运行结束后都能计算出相同的会话密钥。2）会话密钥的保密性：实施被动攻击的敌手（非法用户）无法计算出正确的会话密钥。由格密码体系的特点，通过参照和综合当前典型相关协议设计，本文先探讨格上被动安全的密钥协商协议的基本构造模式，为此，下文介绍两类密钥共识（Key Consensus，KC）方案的定义。KC 可作为格上密钥建立协议的基本构造模块，其概念来自 Jin 等的思想[39-40]。

在给出相关定义之前，首先引入一个与任意正整数 $q\geqslant 1$ 相关的新函数 $|\cdot|_q$，定义：$|\boldsymbol{x}|_q=\min\{x \bmod q, q-x \bmod q\}$。其中，$x\in\mathbb{Z}$ 可为任意整数，$|\boldsymbol{x}|_q$ 为整数且满足 $0\leqslant|\boldsymbol{x}|_q\leqslant q-1$。例如，$|\boldsymbol{x}|_q=\min\{-1 \bmod q,(q+1) \bmod q\}=\min\{q-1,1\}=1$。在下面的描述中，我们使用 $|d_1-d_2|_q$ 来度量两个元素 $d_1,d_2\in\mathbb{Z}_q$ 之间的距离。由此，下面给出对称密钥共识（Symmetric Key Consensus，SKC）和非对称密钥共识（Asymmetric Key Consensus，AKC）这两类 KC 方案的定义（其中，SKC 方案在概念上与文献[39-40]中定义的 KC 方案相对应）。

（1）对称密钥共识方案 SKC=（paras，Conci，Recon）是一个三元组，其各元素的定义如下：

1）$Paras=(q,m,g,d,aux)$ 代表系统参数，其中，$q,m,g,d$ 为正整数且满足 $2\leqslant m,g\leqslant q,0\leqslant d\leqslant\lfloor q/2\rfloor$，$aux$ 代表通常由 $(q,m,g,d)$ 所决定的某些辅助值且可被设置为“空”（用一个特殊符号“⊥”来标示）。

2）$(k_1,v)\leftarrow Conci(d_1,paras)$：对于输入 $(d_1\in\mathbb{Z}_q,paras)$，概率多项式时间调制算法 $Conci$ 输出 $(k_1,v)$。其中，$k_1\in\mathbb{Z}_m$ 是共享密钥；$v\in\mathbb{Z}_g$ 是一个在协议运行过程中公开发送给通信对方的提示信号，用来帮助协议双方达成关于会话密钥的共识。

3）$k_2\leftarrow Recon(d_2,v,paras)$：对于输入 $(d_2\in\mathbb{Z}_q,v,paras)$，确定性多项式时间调和算法 $Recon$ 输出 $k_2\in\mathbb{Z}_m$。

正确性：我们说一个对称密钥共识方案 SKC 是正确的，如果对于满足条件 $|d_1-d_2|_q\leqslant d$ 的任意 $d_1,d_2\in\mathbb{Z}_q$，若 $(k_1,v)\leftarrow Conci(d_1,paras)$ 且 $k_2\leftarrow Recon(d_2,v,paras)$，都有 $k_1=k_2$。

安全性：我们说一个对称密钥共识方案 SKC 是安全的，如果每当 $d_1\leftarrow\mathbb{Z}_q$ 且 $k_1$ 为 $Conci(d_1,paras)$ 的输出时，$k_1$ 和 $v$ 是独立的且 $k_1$ 在 $\mathbb{Z}_m$ 上是均匀分布的。概率取自 $d_1$ 的抽样和 $Conci$ 使用的随机抛币。

对于上述正确且安全的对称密钥共识方案 SKC，文献

[39-40]证明其参数$(m,d,q,g)$满足约束条件$2md \leqslant q(1-1/g)$，并给出了一个具体的实例算法如算法1所示。

**算法1** SKC实例算法

Paras=(q,m,g,d,aux),aux={q′= lcm(q,m),α =q′/q,β =q′/m}.
procedure Conci($d_1$,paras) // $d_1 \in [0, q-1]$
e←[−⌊(α−1)/2⌋,⌊α/2⌋];
$d_A = (\alpha d_1 + e) \bmod q'$;
$k_1 = \lfloor d_A/\beta \rfloor \in \mathbb{Z}_m$;
$v' = d_A \bmod \beta$;
$v' = \lfloor v'g/\beta \rfloor$; //$v \in \mathbb{Z}_g$
return($k_1$,v);
end procedure
procedure Recon($d_2$,v,paras) //$d_2 \in [0, q-1]$
$k_2 = \lfloor \alpha d_2/\beta - (v+1/2)/g \rceil \bmod m$;
return $k_2$;
end procedure

文献[39-40]证明了上述SKC实例在满足条件$(2d+1)m < q(1-1/g)$(其中$m \geqslant 2, g \geqslant 2$)时是正确的，而且也证明了该SKC实例是安全的。具体来说，就是当$d_1 \leftarrow \mathbb{Z}_q$时，$k_1$和$v$是独立的，且$k_1$在$\mathbb{Z}_m$上是均匀分布的，其中概率取自$d_1$的抽样和*Conci*使用的随机抛币，其证明的具体细节在此不再赘述。利用SKC方案，我们可以构造出一类原始的密钥建立协议，如图1所示。

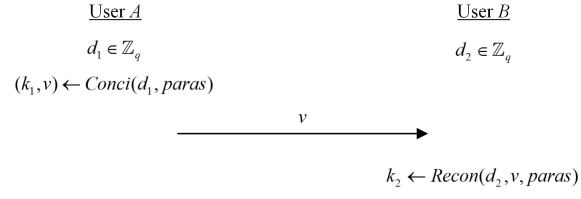


图1 基于SKC的原始密钥建立协议

Fig. 1 SKC-based primitive key establishment protocol

图1中，用户$A$和用户$B$为协议的执行方，$k_1, k_2 \in \mathbb{Z}_m$，$v \in \mathbb{Z}_g$，并且满足条件：$|d_1 - d_2|_q \leqslant d$。

(2)非对称密钥共识方案$AKC=(paras, Conci, Recon)$是一个三元组，其各元素的定义如下。

1)$Paras=(q,m,g,d,aux)$代表系统参数，其中，$q,m,g,d$为正整数且满足$2 \leqslant m, g \leqslant q, 1 \leqslant d \leqslant \lfloor q/2 \rfloor$，$aux$代表通常由$(q,m,g,d)$所决定的某些辅助值且可被设置为空。

2)$v \leftarrow Conci(d_1, k_1, paras)$：对于输入$(d_1 \in Z_q, k_1 \in Z_m, paras)$，概率多项式时间调制算法*Conci*输出公开提示信号$v \in Z_g$。

3)$k_2 \leftarrow Recon(d_2, v, paras)$：对于输入$(d_2, v, paras)$，确定性多项式时间算法*Recon*输出$k_2 \in \mathbb{Z}_m$。

正确性：我们说一个非对称密钥共识方案AKC是正确的，如果对于满足条件$|d_1 - d_2|_q \leqslant d$的任意$d_1, d_2 \in \mathbb{Z}_q$，且$v \leftarrow Conci(d_1, k_1, paras)$，$k_2 \leftarrow Recon(d_2, v, paras)$，都有$k_1 = k_2$。

安全性：我们说一个非对称密钥共识方案AKC是安全的，如果$d_1$在$\mathbb{Z}_q$上是均匀分布的且$v$为$Conci(d_1, k_1, paras)$的输出时，$v$与$k_1$之间是独立的。具体来说，对于任意$v' \in \mathbb{Z}_g$和任意$k_1', k_1'' \in \mathbb{Z}_m$，满足$\Pr[v == v' \mid k_1 = k_1'] = \Pr[v = v' \mid k_1 = k_1'']$，其中，概率取自$d_1 \leftarrow \mathbb{Z}_q$和*Conci*使用的随机抛币。

对于上述正确且安全的非对称密钥共识方案AKC，文献[39-40]证明其参数$(m,d,q,g)$满足约束条件$2md \leqslant q(1-m/g)$，并给出了一个具体的AKC实例算法，如算法2所示。

**算法2** AKC实例算法

Paras=(q,m,g,d,aux)，其中，aux=⊥.
procedure Conci($d_1$,$k_1$,paras) // $d_1 \in [0, q-1]$
$v = \lfloor g(d_1 + \lfloor k_1 q/m \rceil)/q \rceil \bmod g$;
return v;
end procedure
procedure Recon($d_2$,v,paras) //$d_2 \in [0, q-1]$
$k_2 = \lfloor m(v/g - d_2/q) \rceil \bmod m$;
return $k_2$;
end procedure

文献[39-40]也证明了上述AKC实例在满足条件$(2d+1)m < q(1-m/g)$时是正确的，而且还证明了该实例是安全的。具体来说，就是当$d_1 \leftarrow \mathbb{Z}_q$时，$v$是独立于$k_1$的，证明的具体细节在此不再赘述。利用AKC方案，我们也可以构造出另一类原始的密钥建立协议，如图2所示。

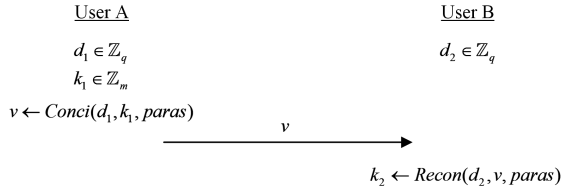


图2 基于AKC的原始密钥建立协议

Fig. 2 AKC-based primitive key establishment protocol

图2中，用户$A$和用户$B$为协议的执行方，$k_1, k_2 \in \mathbb{Z}_m$，$v \in \mathbb{Z}_g$，并且满足条件：$|d_1 - d_2|_q \leqslant d$。

从本质上来说，现有的主要格上后量子密钥建立协议的底层设计大多数类属于SKC和AKC这两种基本的构造模式(对于算法1和算法2来说，选择不同的具体参数可构造出不同的原始协议实例)，而基于SKC和AKC的密钥建立协议具有以下不同的性能和特性。1)基于SKC的方案相当于格密码系统中的Diffie-Hellman类密钥协商协议，而基于AKC的方案则相当于格密码系统中的El Gamal类密钥传输协议。2)对两方密钥建立协议来说，密钥传输意味着会话密钥的产生主要由单方所主导(一方产生会话密钥经加密封装传输给另一方)，这与密钥协商在产生会话密钥时双方角色对等、地位相同、共同决定会话密钥的生成是不同的。由此，在实践中对基于AKC的方案进行部署时，因执行者的实际操作问题(如响应者使用的随机数质量不好或像现实中实施某些TLS协议时在多个会话中重用密钥等)对会话密钥安全性所造成的损害可能比使用基于KC的方案进行部署时要大得多，而对实用性密码方案而言，对称性通常也是一个良好的性质。3)基于SKC的方案用途更广，能被直接改编成一个密钥传输协议或选择明文攻击(Chosen-Plaintext Attacks，CPA)安全的公钥加密方案，而且更适于通过SIGMA机制[31]与像IKE和TLS协议这样基于Diffie-Hellman模块的现有协议标准相结合。此外，对于上文建议的参数，SKC实际上比AKC更高

效。由上文的相关论述可见，在使用相同的参数$(q,m,g)$时（即在带宽相同的情况下），基于 SKC 的协议比基于 AKC 的方案具有更低的误差概率；而在使用相同的参数$(q,m,d)$时（即在误差概率相同的情况下），基于 SKC 的协议比基于 AKC 的方案具有更小的带宽。

基本的被动安全的密钥协商协议只能防备执行被动攻击的敌手，而在实际应用中必须要考虑网络上执行主动攻击的敌手。例如，NIST 的算法征集项目中要求，对于密钥协商协议提案，需要给出将其增强为认证密钥协商协议方案的方法。一般来说，签名方案的结合使用可使被动安全的密钥协商协议具备认证性[32]。例如，Del Pino 等[42]将带消息恢复功能的签名与被动安全的密钥协商协议结合，既实现了认证性，又减少了通信量，节约了通信成本；De Saint Guilhem 等[43]给出了一个简单而有效的通用变换方法，可将两步被动安全（非认证）的密钥协商协议转换成前向安全的认证密钥协商协议，该方法也可用来构建后量子认证密钥协商协议，且转换并不借助数字签名方案，仅需要利用自适应选择密文攻击下的不可区分性（Indistinguishability under Chosen Ciphertext Attack，IND-CCA）安全的公钥加密方案（如基于 RLWE 难题的相关方案）和消息认证码（Message Authentication Code，MAC）方案。

此外，也有一些学者研究利用 KEM 或公钥加密方案来直接构造认证密钥协商协议的方法。Fujioka 等[44]给出利用选择明文攻击安全的公钥加密方案和选择密文攻击（Chosen-Ciphertext Attack，CCA）安全的公钥加密方案来构造可证明安全的通用认证密钥协商协议的方法；随后，他们[45]又对此构建方案进行了改进，提出直接利用单向 CCA 安全的 KEM 来构造在随机预言模型[35]下可证明安全认证密钥协商协议的方法。Fujioka 等提出的这两种协议通用构建方法[44-45]也可用于格方案的构造。其中，CCA 安全的公钥加密方案和 KEM 方案可分别由基本的 CPA 安全的公钥加密方案和 KEM 方案使用 Fujisaki-Okamoto 变换[28,46-47]得到，如 Kyber 方案就采用了文献[45]中的方法而得到具有认证性的密钥协商协议 Kyber. AKE[41]。Hövelmanns 等[48]给出直接由 CPA 安全的加密方案来构造通用认证密钥协商协议的框架，这可被视为对文献[45]中协议构造方法的一个改进。

### 3.3　若干相关典型方案性能对比和分析

表 1 列出了若干（两方）密钥建立协议的性能。其中，重点对现存的一些典型的格上后量子密钥建立协议（实例）进行了对比，具体比较项目包括由毫秒（ms）值度量的协议发起者（Initiator）和响应者（Responder）的（平均）计算时间、由比特（bits）值度量的公私钥规模和通信量（协议执行双方的通信总量）以及安全级别等。

表 1　若干密钥建立协议的性能

Table 1　Performance of several key establishment protocols

| Scheme | Running Time/ms | | Communication/bits | Size/bits | | (Claimed) Quantum Security | Problem | Lattice Type |
|---|---|---|---|---|---|---|---|---|
| | Initiator | Responder | | Public Key | Secret Key | | | |
| 2-ZZDSD-100 | 29.268 | 29.296 | 91136 | 45056 | 6537 | 100 | RLWE | Ideal Lattices |
| 2-ZZDSD-210 | 41.047 | 41.104 | 210944 | 104448 | 13914 | 210 | RLWE | Ideal Lattices |
| Peikert-106 | 1.165 | 2.133 | 27341 | 7168 | 2048 | 106 | RLWE，RSIS | Ideal Lattices |
| Peikert-192 | 4.143 | 4.467 | 44544 | 7168 | 3072 | 192 | RLWE，RSIS | Ideal Lattices |
| BCNS | 1.184 | 1.59 | 66560 | 32768 | 32768 | 76 | RLWE | Ideal Lattices |
| NewHope | 0.146 | 0.164 | 30976 | 14592 | 14336 | 206 | RLWE | Ideal Lattices |
| Frodo (recommended) | 1.26 | 1.34 | 181384 | 90368 | 10240 | 130 | LWE | Standard Lattices |
| Kyber. AKE (recommended) | 0.187 | 0.1 | 37120 | 8704 | 9984 | 161 | MLWE | Module Lattices |
| Saber. KE (recommended) | — | — | 16384 | 7936 | 18432 | 180 | MLWR | Module Lattices |
| ECDH-256 | 0.697 | 0.698 | 512 | 256 | 256 | × | ECDL | × |

表 1 中的这些协议（实例）的构建主要基于不同格上的 LWE 系列问题（或其变体），具体涉及标准格（Standard Lattices）上的 LWE 问题、基于理想格（Ideal Lattices）的环 LWE（RLWE）/环 SIS（RSIS）问题以及模格上的 LWE（MLWE）/LWR（MLWR）问题（关于这些计算性问题的定义和解释请参见前文相关描述）。表 1 中所列的格上密钥建立协议在设计结构上具有一定的代表性，其中包括 Zhang 等的方案（2-ZZDSD-100 和 2-ZZDSD-210）[33]、Peikert 的方案（Peikert-106 和 Peikert-192）[30] 以及 BCNS[32]、NewHope[36]、Frodo[38]、Kyber. AKE[41] 和 Saber. KE[19] 方案。这些格密码协议的作者在其相关文献中往往给出了多个可选（参数）的方案，表 1 列出的是其主要方案或使用推荐参数的方案（以“recommended”标记）。另外，表 1 还列出了一个传统的椭圆曲线 Diffie-Hellman 类协议 ECDH-256[38,49] 的性能，作为执行高效的经典密钥建立方案的代表来参与比较。ECDH-256 方案的设计基于椭圆曲线离散对数（Elliptic Curve Discrete Logarithm，ECDL）问题，该协议不属于格方案且不能提供抗量子攻击的安全性（在表 1 中以符号“×”来表示）。表 1 中，Zhang 等的方案和 Peikert 方案的数据来自文献[50]；BCNS，NewHope，Frodo 和 ECDH-256 方案的数据源来自对文献[38,49]中相关数据的收集和处理；Kyber. AKE 方案的数据来自文献[41]；Saber. KE 方案的数据来自文献[19]（相关文献中只提供了 Saber. KEM 执行的测试数据，没有提供 Saber. KE 执行的测试数据，由此以符号“-”来标记相关表项）。由于上述协议的设计基于不同的计算性难题且提供不同程度的后量子安全性，其实施又依托不同平台并采用不同程度优化，因此在各方案和其实施之间进行完全公平的比较是不可能的。然而，从表 1 可以清楚地看出：在计算效率上，基于格的后量子密钥建立协议表现较好，尤其近年提出的某些方案（如 NewHope 和 Kyber. AKE）甚至超越了具有较高性能的经典密码协议方案（ECDH-256），但在通信量和密钥规模方面，后量子密钥建立协议普遍远大于经典协议。另一方面，在表 1 中所列格密

码协议中，Saber. KE 的通信量是最小的，而根据文献[19]中对几类相关基于格的后量子 KEM 方案的比较得出，Saber. KEM 的总体性能比同样基于模格的 Kyber. KEM 略高，由此也可以推断：协议设计若采用基于 KEM 的通用构建方式（如文献[45]中的协议构造方法），Saber 方案可能会比 Kyber 方案更具优势。

总的来说，对密钥建立协议而言，基于格的后量子密码方案（如 NewHope 和 Kyber. AKE）的性能更加均衡，已经可以进行较高程度的实用化。然而，与相关经典协议相比，格密码协议在某些方面仍然存在一定的差距。除了通信量和密钥规模较大的问题，格协议方案的实施在某些方面还不够灵活。例如，对许多基于 LWE 系列问题的格上密钥建立协议来说，由于其自身的设计特点（如为了实现误差协调机制），在执行时需要协议双方依次顺序地发送消息和处理，无法像某些相关经典方案（如 Diffie-Hellman 类协议）那样做到协议双方消息同时发送和并行处理，这在一定程度上影响了协议的运行性能，同时也限制了其在某些特定场合下的应用和实施。

## 4 总结和展望

由前文论述可以看出，对于抗量子（后量子）密码技术的研究现已逐渐成为密码学和网络安全领域研究的热点和趋势。相应地，对于抗量子（后量子）认证密钥协商协议的研究也开始蓬勃展开。但从总体来看，目前国内外对此方面的研究尚处于初始阶段，许多理论和技术还有待成熟、完善或深入。对基于格的后量子认证密钥协商协议的研究来说，仍有不少问题需要解决，需要开展进一步的研究工作，主要工作内容和研究思路如下。

（1）在协议安全模型和相关的可证明安全研究方面仍有许多工作尚待完成。安全模型的好坏直接决定着依托其进行安全论证的协议的安全性，强安全模型的使用有助于设计出可提供强安全性保证的协议。目前，对后量子认证密钥协商协议的证明，主要使用较弱的安全模型（如 BR 模型、BJM 模型或传统的 CK 模型），但在较强的安全模型（如 eCK 类模型）下可证明安全的方案却很少。另外，当前安全模型的定义也并未完全考虑敌手在量子环境下的攻击能力。显然，量子攻击者的能力比传统攻击者的能力更强[51-54]，若将其局限于传统计算环境，是极不现实的。例如，对可证明安全的后量子密码方案来说，基于随机预言模型（Random Oracle Model，ROM）的方案通常比基于标准模型的方案的效率更高，然而，现存许多基于 ROM 的后量子密码方案仅在经典的随机预言模型（Classical Random Oracle Model，CROM）[35]下被证明是安全的，并没有提供在量子随机预言模型（Quantum Random Oracle Model，QROM）[51-54]下的安全性证明。因此，后量子时代的安全模型的定义值得深思。如何在安全模型中严格描述攻击者在量子环境中的攻击能力以及如何在这样的后量子安全模型下证明相关方案的安全性也是一个开放问题。

（2）在可提供良好安全性质的方案设计方面，相关的后量子安全协议研究依然是任重而道远。后量子认证密钥协商协议的研究起步较晚，目前的方案设计仍更多关注基础性（被动安全的）密钥协商协议的构造和一些基本的安全特性的实现（如弱的完美前向保密性）。由此，如何构建具有更多先进安全性质（如临时秘密泄露安全性、充分完美前向保密性和抗最大程度泄露攻击等）、可提供更强安全性保证的协议是一个开放问题。

（3）执行效率是后量子安全协议研究要关注的重要问题。执行效率通常从计算复杂性、通信效率和存储空间需求等几方面来衡量。用后量子安全协议替换传统安全协议面临的一个巨大挑战是：大多数后量子公钥密码方案比传统公钥密码方案具有更大的密钥规模。这可能会导致现行相关网络协议（如传输层安全协议 TLS、Internet 密钥交换协议 IKE 等）系统的改动。因此，如何进行网络协议系统中相关组件的替换需要仔细考量。正如前文所述，经过不断改进，最近提出的某些格上后量子密码协议方案在计算效率方面甚至可以与当前网络上部署的那些基于传统数论难题（如椭圆曲线离散对数问题）的相关密码方案相抗衡，然而在通信效率和存储空间需求等其他方面仍需要很大的改进。对格上后量子密钥建立协议而言，目前很多方案设计都是采用基于 KEM 或公钥加密方案的模块化通用构建方式（如文献[44-45]中的协议构造方法）。为进一步提高方案效率，有必要研究更为精简的协议构造模式，而在设计上应尽可能少地直接调用像 KEM、公钥加密、签名及 MAC 这样的密码方案，基于格上后量子难题直接进行协议构造可能是一个较好的选择。

除了上述问题，基于格的后量子认证密钥协商协议在实际部署时也有一些其他问题是需要考虑的。例如，现今许多经典的认证密钥协商协议本质上都是基于最初的 Diffie-Hellman（DH）模块[1]构建的，利用 DH 模块可以很自然地体现密钥协商过程中协议执行各方对于会话密钥产生的同等贡献性（Contributiveness）；同时，DH 密钥既可作为一次协议执行的临时密钥又可作为多次协议执行的（半）静态密钥，其密钥可重用性（Key-Reusability）使得该类经典协议的实际部署非常灵活和便利，但这些良好的特性是当前许多基于格的相关协议（特别是基于 KEM 构建的协议）所不具备的[55]。实际上，目前有不少典型的格密钥建立协议（如 NewHope 系列方案[36-37]）在密钥重用时是具有安全隐患的[25-26,55-57]。最近，Brendel 等[55]引入“分裂（Split）KEM”的概念并提出相关的形式化框架，以试图系统性地解决上述问题，然而他们却无法成功提出一个满足其定义要求的强安全的后量子“分裂（Split）KEM”的实例。由此，该工作更多体现的是理论和概念上的意义。这样，如何构建与当前经典 DH 类认证密钥协商协议相似并具有上述良好特性的格上后量子相关协议是一个值得深入探讨的问题。此外，认证密钥协商协议在当前各类网络和通信环境中有着广泛的应用，如何构建适用于一定应用环境的实用后量子协议方案也是一个现实问题。

目前，量子计算成为越来越被重视的一大科技领域，由于其拥有巨大的潜在价值，世界多国都在积极整合各方面的研究力量和资源来开展协同攻关，谷歌、微软和 IBM 等大型高科技公司也强势介入量子计算研究。相关技术和理论的飞速发展使量子时代已不再遥远。量子计算机的商业化前景也正

逐渐明朗，业界不少科技巨头已在相关技术和产业化方面进行了布局。例如，谷歌提出“量子优越性(Quantum Supremacy)”的目标，以在计算能力上实现其量子计算机产品对于当前经典超级计算机的巨大超越，并且其专家预言：量子计算领域即将迎来历史性里程碑，小型量子计算机会在5年内逐渐兴起。

现代公钥密码构成了当今网络空间的“信任链之锚”，而量子计算在解决大规模计算难题方面的巨大潜能将对现行网络信息系统中广为实施的公钥体系构成严重的实质性威胁，作为网络基础性安全协议的认证密钥协商类协议(如因特网TLS和IKE协议等)首当其冲，向抗量子安全体系的迁移已刻不容缓。鉴于低成本和易兼容的特点，后量子安全方案在其中扮演着极其重要的角色。在这种形势下，相关领域的研究已在国家之间引发“军备竞赛”。近年来，欧洲国家的“后量子密码”(PQCrypto)和“安全密码”(SAFEcrypto)项目以及日本的CREST密码数学项目都取得了显著成果，美国也在相关政府机构和企业界的推动下，在后量子密码的学术研究、标准制定和成果应用等领域占据领先地位[58]。美国的谷歌公司于2016年开始进行后量子密码技术的测试活动，其在实用性实验中选用了基于格的NewHope方案[36]来保护谷歌服务器和Chrome浏览器之间的真实流量，这是后量子认证密钥协商协议在现实世界中的首例部署应用，该测试的结论是后量子密码协议NewHope的部署并没有给通信带来障碍[9,58]。在知名信息技术企业对互联网行业的影响力的作用下，后量子密码技术的应用也势必得到了有力的推进。

**结束语**　大规模量子计算机足以破坏现有网络信息系统的安全基础。在当前量子计算技术飞速发展及其应用日渐深入的背景下，后量子密码系统及其实用化已成为在信息网络安全领域被学术界、工业界、标准化组织乃至政府所关注的焦点。利用格密码中LWE系列问题设计的方案，其参数尺寸和通信量合理，计算高效，是后量子密码方案实用化的希望之一。由此，基于格的后量子认证密钥协商协议研究也开始蓬勃展开，并相继出现了一些优秀的方案。但总体来看，该项研究尚处于初始阶段，还有不少问题需要解决，如相关方案性能仍有待提升，其应用也有待进一步的深入等。本文聚焦格上后量子认证密钥协商协议的研究，对相关领域的研究现状进行了阐述和分析，对目前基于格的后量子认证密钥协商协议研究中所出现的问题进行了讨论，并由此对其将来的工作方向进行了总结，对未来相关研究的发展趋势进行了展望，这可为相关领域的研究提供一定的参考。在基于格的后量子认证密钥协商协议研究方面，未来将在高级和新型安全方案(如基于身份和基于属性等相关安全协议)的设计和分析等方向开展工作，探讨构建较强模型下可证明安全且执行较为高效的方案；同时研究相关方案在某些新型网络分布式系统(如云计算、物联网等特定环境)中的应用。

## 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. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. SIAM J. Comput., 1997, 26(5): 1484-1509.

[3] DEVORET M H, SCHOELKOPF R J. Superconducting Circuits for Quantum Information: an Outlook [J]. Science, 2013, 339(6124): 1169-1174.

[4] KELLY J, BARENDS R, FOWLER A G, et al. State Preservation by Repetitive Error Detection in a Superconducting Quantum Circuit[J]. Nature, 2015, 519: 66-69.

[5] WAN Y. Summary of Hot Research Topics in Information Technology in 2017[J]. Science & Technology Review, 2018, 36(1): 91-97.

[6] CESARE C. Online Security Braces for Quantum Revolution [J]. Nature, 2015, 525(7568): 167-168.

[7] CHEN L, JORDAN S, LIU Y K, et al. Report on Post-Quantum Cryptography[M]. US Department of Commerce, National Institute of Standards and Technology, 2016.

[8] GALBRAITH S D, PETIT C, SHANI B, et al. On the Security of Supersingular Isogeny Cryptosystems[C]// Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2016). Berlin, Heidelberg: Springer, 2016: 63-91.

[9] 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.

[10] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: A Ring-Based Public Key Cryptosystem[C]// Proceedings of the Third International Symposium on Algorithmic Number Theory (ANTS 1998). Berlin, Heidelberg: Springer, 1998: 267-288.

[11] REGEV O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[J]. J. ACM, 2009, 56(6): 1-40.

[12] LYUBASHEVSKY V, PEIKERT C, REGEV O. On Ideal Lattices and Learning with Errors Over Rings[C]// Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2010). Berlin, Heidelberg: Springer, 2010: 1-23.

[13] LYUBASHEVSKY V, PEIKERT C, REGEV O. A Toolkit for Ring-LWE Cryptography[C]// Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2013). Berlin, Heidelberg: Springer, 2013: 35-54.

[14] PEIKERT C. A Decade of Lattice Cryptography[J]. Foundations and Trends in Theoretical Computer Science, 2016, 10(4): 283-424.

[15] AJTAI M. Generating Hard Instances of Lattice Problems[J]. Quaderni di Matematica, 2004, 13: 1-32.

[16] AJTAI M, DWORK C. A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence[C]// Proceedings of the 29th annual ACM symposium on Theory of computing (STOC 1997). New York: Association for Computing Machinery, 1997: 284-293.

[17] BANERJEE A, PEIKERT C, ROSEN A. Pseudorandom Func-

tions and Lattices[C]// Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2012). Berlin, Heidelberg: Springer, 2012: 719-737.

[18] LANGLOIS A, STEHLÉ D. Worst-Case to Average-Case Reductions for Module Lattices[J]. Designs, Codes and Cryptography, 2015, 75(3): 565-599.

[19] D'ANVERSJ P, KARMAKAR A, SINHA ROY S, et al. Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM[C]// Proceedings of the 10th International Conference on Cryptology in Africa (AFRICACRYPT 2018). Cham: Springer, 2018: 282-305.

[20] MICCIANCIO D, MOL P. Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions [C]// Proceedings of the 31st Annual Cryptology Conference. Berlin, Heidelberg: Springer, 2011: 465-484.

[21] APPLEBAUM B, CASH D, PEIKERT C, et al. Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems[C]// Proceedings of the 29th Annual International Cryptology Conference (CRYPTO 2009). Berlin, Heidelberg: Springer, 2009: 595-618.

[22] BOGDANOV A, GUO S, MASNY D, et al. On the Hardness of Learning with Rounding over Small Modulus[C]// Proceedings of the 13th International Conference on Theory of Cryptography (TCC 2016). Berlin, Heidelberg: Springer, 2016: 209-224.

[23] PEIKERT C. How (Not) to Instantiate Ring-LWE[C]// Proceedings of the 10th International Conference on Security and Cryptography. Cham: Springer, 2016: 411-430.

[24] GONG B, ZHAO Y. Cryptanalysis of RLWE-Based One-Pass Authenticated Key Exchange[C]// Proceedings of the 8th International Workshop on Post-Quantum Cryptography. Cham: Springer, 2017: 163-183.

[25] DING J, FLUHRER S, RV S. Complete Attack on RLWE Key Exchange with Reused Keys, Without Signal Leakage[C]// Proceedings of the the 23rd Australasian Conference on Information Security and Privacy. Cham: Springer, 2018: 467-486.

[26] BAUER A, GILBERT H, RENAULT G, et al. Assessment of the Key-Reuse Resilience of NewHope[C]// Proceedings of the Cryptographers' Track at the RSA Conference 2019. Cham: Springer, 2019: 272-292.

[27] DODIS Y, REYZIN L, SMITH A. Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data [C]// Proceedings of the the 23rd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2004: 523-540.

[28] DENT A W. A Designer's Guide to KEMs[C]// Proceedings of the 9th IMA International Conference on Cryptography and Coding. Berlin, Heidelberg: Springer, 2003: 133-151.

[29] DING J, XIE X, LIN X. A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem[EB/OL]. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2012/688.pdf.

[30] PEIKERT C. Lattice Cryptography for the Internet[C]// Proceedings of the 6th International Workshop on Post-Quantum Cryptography. Cham: Springer, 2014: 197-219.

[31] KRAWCZYK H. SIGMA: The 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols [C]// Proceedings of the 23rd Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 2003: 400-425.

[32] 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]// Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP 2015). USA: IEEE Computer Society, 2015: 553-570.

[33] ZHANG J, ZHANG Z, DING J, et al. Authenticated Key Exchange from Ideal Lattices[C]// Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2015: 719-751.

[34] KRAWCZYK H. HMQV: A High-Performance Secure Diffie-Hellman Protocol[C]// Proceedings of the 25th Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 2005: 546-566.

[35] BELLARE M, ROGAWAY P. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols[C]// Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS 1993). New York: Association for Computing Machinery, 1993: 62-73.

[36] ALKIM E, DUCAS L, ELMANN T, et al. Post-Quantum Key Exchange — A New Hope[C]// Proceedings of the 25th USENIX Security Symposium. USA: USENIX Association, 2016: 327-343.

[37] ALKIM E, DUCAS L, ELMANN T, et al. NewHope without Reconciliation[EB/OL]. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2016/1157.pdf.

[38] BOS J, COSTELLO C, DUCAS L, et al. Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE [C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS 2016). New York, NY, USA: Association for Computing Machinery, 2016: 1006-1018.

[39] JIN Z, ZHAO Y. Optimal Key Consensus in Presence of Noise [EB/OL]. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2017/1058.pdf.

[40] JIN Z, ZHAO Y. Generic and Practical Key Establishment from Lattice[C]// Proceedings of the 17th International Conference on Applied Cryptography and Network Security. Cham: Springer, 2019: 302-322.

[41] BOS J, DUCAS L, KILTZ E, et al. CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM[C]// Proceedings of the 2018 IEEE European Symposium on Security and Privacy. London, UK: IEEE, 2018: 353-367.

[42] DEL PINO R, LYUBASHEVSKY V, POINTCHEVAL D. The Whole is Less Than the Sum of Its Parts: Constructing More Efficient Lattice-Based AKEs[C]// Proceedings of the 10th International Conference on Security and Cryptography. Cham:

Springer，2016：273-291.

[43] DE SAINT GUILHEM C，SMART N P，WARINSCHI B. Generic Forward-Secure Key Agreement Without Signatures[C]// Proceedings of the 20th International Conference on Information Security. Cham：Springer，2017：114-133.

[44] FUJIOKA A，SUZUKI K，XAGAWA K，et al. Strongly Secure Authenticated Key Exchange from Factoring，Codes，and Lattices[C]// Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography. Berlin，Heidelberg：Springer，2012：467-484.

[45] FUJIOKA A，SUZUKI K，XAGAWA K，et al. Practical and Post-Quantum Authenticated Key Exchange from One-Way Secure Key Encapsulation Mechanism[C]// Proceedings of the 8th ACM SIGSAC Symposium on Information，Computer and Communications Security. New York，NY，USA：Association for Computing Machinery，2013：83-94.

[46] FUJISAKI E，OKAMOTO T. How to Enhance the Security of Public-Key Encryption at Minimum Cost[C]// Proceedings of the Second International Workshop on Practice and Theory in Public Key Cryptography. Berlin，Heidelberg：Springer，1999：53-68.

[47] HOFHEINZ D，HVELMANNS K，KILTZ E. A Modular Analysis of the Fujisaki-Okamoto Transformation[C]// Proceedings ofthe 15th International Conference on Theory of Cryptography. Cham：Springer，2017：341-371.

[48] HVELMANNS K，KILTZ E，SCHÄGE S，et al. Generic Authenticated Key Exchange in the Quantum Random Oracle Model[C]// Proceedings of the 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography. Cham：Springer，2020：389-422.

[49] NEJATOLLAHI H，DUTT N，RAY S，et al. Post-Quantum Lattice-Based Cryptography Implementations：A Survey[J]. ACM Computing Surveys，2019，51(6)：129-169.

[50] BINDEL N，BUCHMANN J，RIE S. Comparing Apples with Apples：Performance Analysis of Lattice-Based Authenticated Key Exchange Protocols[J]. International Journal of Information Security，2018，17(6)：701-718.

[51] BONEH D，DAGDELEN Ö，FISCHLIN M，et al. Random Oracles in a Quantum World[C]// Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security. Berlin，Heidelberg：Springer，2011：41-69.

[52] SAITO T，XAGAWA K，YAMAKAWA T. Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model[C]// Proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham：Springer，2018：520-551.

[53] JIANG H，ZHANG Z，CHEN L，et al. IND-CCA-Secure Key Encapsulation Mechanism in the Quantum Random Oracle Model，Revisited[C]// Proceedings of the 38th Annual International Cryptology Conference. Cham：Springer，2018：96-125.

[54] KATSUMATA S，YAMADA S，YAMAKAWA T. Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model[C]// Proceedings of the 24th International Conference on the Theory and Applications of Cryptology and Information Security. Cham：Springer，2018：253-282.

[55] BRENDEL J，FISCHLIN M，GÜNTHER F，et al. Challenges in Proving Post-Quantum Key Exchanges Based on Key Encapsulation Mechanisms[EB/OL]. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2019/1356.pdf.

[56] QIN Y，CHENG C，DING J. A Complete and Optimized Key Mismatch Attack on NIST Candidate NewHope[C]// Proceedings of the 24th European Symposium on Research in Computer Security. Cham：Springer，2019：504-520.

[57] DING J，CHENG C，QIN Y. A Simple Key Reuse Attack on LWE and Ring LWE Encryption Schemes as Key Encapsulation Mechanisms (KEMs) [EB/OL]. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2019/271.pdf.

[58] WU H S. Analysis of Post-Quantum Cryptographic Development[EB/OL]. (2017-01-13). The Website of Knowfar Institute for Strategic and Defence Studies. http://www.knowfar.org.cn/html/zhanlue/201701/13/657.htm.

**NI Liang**，born in 1975，Ph.D，lecturer，is a member of China Computer Federation. His main research interests include network security and cryptography.