基于格的类DH密钥交换协议设计与挑战

王 克[1,2],韩 将[3,4],谢惠琴[1],江浩东[5],陈 隆[4],张振峰[4]
(1. 北京电子科技学院密码科学与技术系,北京 100070;2. 贵州大学公共大数据国家重点实验室,贵州贵阳 550025;
3. 中国科学院大学,北京 100190;4. 中国科学院软件研究所可信计算与信息保障实验室,北京 100190;
5. 河南省网络密码技术重点实验室,河南郑州 450001)

摘 要: 迪菲-赫尔曼(Diffie-Hellman,DH)密钥交换协议,作为一种被广泛采用的密码学协议,在多种加密应用场景中发挥着关键作用. 然而,鉴于量子计算技术的快速发展,DH协议面临量子攻击的重大威胁,迫切需要开发具备抗量子安全性的替代方案. 其中,基于格的密钥交换协议是构建抗量子密钥交换协议的主要方法之一. 本文首先系统梳理了基于格的类DH密钥交换协议的设计,然后指出了该类协议与传统DH协议的两大显著差异:其一,协议严格禁止密钥重用,以避免由此引发的两种潜在密钥恢复攻击,这一限制显著影响了协议的灵活性与效率;其二,协议通常需要额外的交互,这不仅增加了通信复杂度和延迟,还导致其在实际应用环境中的效率下降. 这些差异使得基于格的类DH密钥交换协议在直接替代传统DH协议时难以继承全部优势. 为减轻抗量子迁移的成本,并实现与现有系统的无缝对接,探索设计支持密钥重用的非交互式类DH密钥交换协议,已成为当前密码学领域的一个重要研究方向. 此类协议旨在保留DH协议的高效性与易用性,同时增强对量子攻击的抵抗力. 最后,通过对此类协议优势与挑战进行深入剖析,本文明确了未来研究的方向,旨在进一步优化协议设计,提升性能,推动抗量子迁移技术的发展.

关键词: 格密码;密钥交换;密钥重用;非交互性;抗量子密码
基金项目: 中央高校基本科研业务费资金(No.3282023002);公共大数据国家重点实验室开放基金(No.PBD2024-0513);北京市自然科学基金(No.4234084);国家重点研发计划(No.2021YFB3100100)
中图分类号: TN918;TP309 **文献标识码:** A **文章编号:** 0372-2112(2025)05-1677-15
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250033

Design and Challenges of Lattice-Based DH Like Key Exchange Protocols

WANG Ke[1,2], HAN Jiang[3,4], XIE Hui-qin[1], JIANG Hao-dong[5], CHEN Long[4], ZHANG Zhen-feng[4]
(1. *Department of Cryptography Science and Technology*, *Beijing Electronic Science and Technology Institute*, *Beijing* 100070, *China*;
2. *State Key Laboratory of Public Big Data*, *Guizhou University*, *Guiyang*, *Guizhou* 550025, *China*;
3. *University of Chinese Academy of Sciences*, *Beijing* 100190, *China*;
4. *Trusted Computing and Information Security Laboratory*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*;
5. *Henan Key Laboratory of Network Cryptography Technology*, *Zhengzhou*, *Henan* 450001, *China*)

Abstract: The Diffie-Hellman (DH) key exchange protocol, as a widely adopted cryptographic protocol, plays a key role in various encryption application scenarios. However, given the rapid development of quantum computing technology, The DH protocol faces significant threats from quantum attacks and there is an urgent need to develop alternative solutions with post-quantum security. Among them, lattice-based key exchange protocols are one of the main methods for building post-quantum key exchange protocols. This paper first systematically reviews the design of lattice-based DH-like key exchange protocols, and then points out two major distinctions between this type of protocol and the DH protocol: firstly, the protocol strictly prohibits key reuse to avoid two potential key recovery attacks that may arise from it, which significantly affects the flexibility and efficiency of the protocol; Secondly, protocols often require additional interactions, which not only increase communication complexity and latency, but also lead to a decrease in efficiency in practical application environments. These differences make it difficult for lattice based class DH key exchange protocols to inherit all the advantages when directly replacing traditional DH protocols. To reduce the cost of post-quantum migration and achieve seamless inte-

收稿日期:2025-01-08;修回日期:2025-04-20;责任编辑:覃怀银

gration with existing systems, exploring the design of non-interactive class DH key exchange protocols that support key reuse has become an important research direction in the current field of cryptography. Such protocols aim to preserve the efficiency and usability of DH protocols while enhancing resistance to quantum attacks. Finally, through a thorough analysis of the advantages and challenges of such key exchange protocols, future research directions have been clarified. Aimed at further optimizing protocol design and improving performance, promote the development of post-quantum transfer technology.

Key words: lattice-based cryptography; key exchange; key reuse; non interactive; post-quantum cryptography

Foundation Item(s): Basic Research Funds for Central Universities (No.3282023002); Open Fund of State Key Laboratory of Public Big Data (No.PBD2024-0513); Beijing Natural Science Foundation (No.4234084); National Key Research and Development Program (No.2021YFB3100100)

1 引言

密钥交换协议是实践中最常用的加密原语之一，允许双方在不安全的网络上安全地生成共享密钥，提供安全的通信通道. 第一个著名的密钥交换协议是迪菲-赫尔曼(Diffie-Hellman，DH)密钥交换协议[1]，随后各种基于DH密钥交换协议的应用相继被提出，例如安全套接字层/传输层安全协议(Secure Sockets Layer/Transport Layer Security，SSL/TLS)[2]、互联网协议安全(Internet Protocol Security，IPSec)、安全外壳协议(Secure SHell，SSH)、Signal协议[3,4]或Noise协议框架[5]，其中SSL/TLS是实际应用中部署最为广泛的密码协议.

随着量子计算技术[6]的迅猛发展，量子安全威胁日益凸显，抗量子迁移策略已成为亟须关注的研究领域. 在此背景下，SSL/TLS的抗量子迁移被置于首要位置，其紧迫性不言而喻，是当前抗量子安全迁移策略中的重中之重. 作为SSL/TLS的核心机制，DH密钥交换协议的安全性基于离散对数困难问题，而这一问题在理论上可以被量子计算机攻破，因此，寻找DH协议的抗量子替代方案显得尤为重要. 特别地，美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)对抗量子密钥交换协议给予了高度关注，并将其视为优先研究和发展的对象[7]. 为了降低抗量子迁移的成本，实现无缝替换，设计一种类DH的抗量子密钥交换协议，成为当前密码学领域的一项关键挑战.

格是一种重要的数学结构，广泛用于设计抗量子安全的密码原语，基于格的密码学是抗量子密码学的重要组成部分. 特别地，在NIST进行标准化的抗量子密码算法中，3/4的算法是基于格的[8~10]. 在基于格的密码学中，容错学习(Learn With Error，LWE)问题占据着重要的地位. LWE问题由文献[11]于2009年提出，经过广泛而深入的研究，尚未发现可以在多项式时间内解决该问题的量子算法，因此，该问题普遍被认为可以抵抗量子攻击. 然而，基于LWE的密码方案存在密钥和密文尺寸大的问题. 为此，文献[12]于2010年引入了环上容错学习(Ring LWE，RLWE)问题. RLWE问题利用环的代数结构提高密码方案的效率，并且具有与LWE问题相似的困难性，被用于设计各种密码方案，是传统数论假设下的密码方案在未来量子计算时代的有力替代.

为了构建类DH的抗量子密钥交换协议，文献[13]借鉴了DH密钥交换协议的设计理念，提出了一种从基于RLWE的近似密钥交换中获得精确共享密钥的技术方案. 该技术方案的核心在于应用模糊提取器的思想[14~16]，从噪声数据中提取精确的共享值. 该过程被称为协调机制.

然而，基于格的类DH密钥交换协议未能继承DH协议的两个重要特征：支持密钥重用和非交互性. 如果基于格的类DH协议重用密钥，可能会带来密钥恢复的风险. 此外，为了从近似共享值协商出精确密钥，协议需要进行额外的交互，进而增加协议的复杂性和执行成本，还可能引入新的安全漏洞. 因此，对于依赖DH协议支持密钥重用和非交互性的应用而言，直接采用基于格的类DH协议替代DH协议，将不可避免地引发一系列技术和安全层面的问题.

为了探索格上支持密钥重用的非交互式密钥交换(Non-Interactive Key Exchange，NIKE)协议，学术界已经开展了一系列的研究. 本文通过系统梳理这些工作，并进行深入分析，旨在为探索格的NIKE协议指明研究方向.

2 预备知识

本节主要介绍所需的基本概念，包括格及格上的困难问题、DH密钥交换协议. 首先给出必要的符号说明，矩阵和向量分别用加粗的大写和小写字母表示，如矩阵$\boldsymbol{V}$和向量$\boldsymbol{v}$；$\mathbb{R}$和$\mathbb{Z}$分别表示实数集合和整数集合，$\mathbb{Z}_q$表示商环$\mathbb{Z}/q\mathbb{Z}$，其中$q\in\mathbb{N}$为正整数；R表示商环$R=\mathbb{Z}[x]/(f(x))$，R_q表示商环$R_q=\mathbb{Z}_q[x]/\big(f(x)\big)$，其中$f(x)$是不可约多项式.

2.1 基本概念

定义1 格是一种数学结构，定义为一组$\mathbb{R}^n$中线性无关向量$\boldsymbol{V}=\{\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_k\}$的整系数线性组合

$$\mathcal{L}=\mathcal{L}(\boldsymbol{V}):=\boldsymbol{V}\cdot\mathbb{Z}^k=\left\{\sum_{i=1}^{k}z_i\boldsymbol{v}_i:\ z_i\in\mathbb{Z}\right\}.$$

其中,向量$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_k$为格基;$k$为格的秩;$n$为格的维数.

定理1　格. 令$f(x)$为一个n次不可约多项式,$R=\mathbb{Z}[x]/f(x)$为一个多项式环,I为环R的理想,则I中所有元素的系数构成$\mathbb{Z}^n$的一个子格,称对应于理想I的一个子格为f-理想格.

定义2　LWE. $\mathbb{Z}_q^n\times\mathbb{Z}_q$上的LWE分布$D_{c,\chi}$是指,对于一个向量$\boldsymbol{c}\in\mathbb{Z}_q^n$,均匀随机选择$\boldsymbol{t}\in\mathbb{Z}_q^n$,根据分布$\chi$选择$e$,输出$\left(\boldsymbol{t},\ u=\langle\boldsymbol{c},\boldsymbol{t}\rangle+e \bmod q\right)$. 判定性LWE问题是区分$\mathbb{Z}_q^n\times\mathbb{Z}_q$上的LWE分布$D_{c,\chi}$和一个均匀分布.

定义3　RLWE. $R_q\times R_q$上的RLWE分布$D_{\alpha,\zeta}$是指对于一个环元素$\alpha\in R_q$,均匀随机选$\beta\in R_q$,根据分布ζ选择ε,输出$(\beta,\ \gamma=\alpha\cdot\beta+\varepsilon \bmod q)$. 判定性RLWE问题是区分$R_q\times R_q$上的RLWE分布$D_{\alpha,\zeta}$和一个均匀分布.

2.2　密钥交换协议

密钥交换协议是一种消息驱动协议,通信双方中的一方在收到消息后被激活,执行内部计算,生成并发送消息,然后等待下一次激活. 协议完成后,生成的秘密密钥被称为会话密钥. 具体来说,参与方P_i的输入形式为$(P_i,\ P_j,s,\text{role})$,其中$P_j$为另一方的身份,$s$为会话ID,role代表协议的发起方或响应方. 如果参与双方P_i和P_j的输入分别为$(P_i,\ P_j,s,$发起方$)$和$(P_j,\ P_i,s,$响应方$)$,那么这两个会话被称为匹配会话. 协议被激活后,匹配会话的参与双方P_i和P_j交换消息(发起方先发送),并最终生成本地输出,包括双方的名称、会话标识符和计算的会话密钥值.

密钥交换协议的基本安全性是被动安全性,满足以下两条性质:(1)如果诚实的双方完成匹配会话,则它们输出相同的会话密钥;(2)任何不修改消息的攻击者正确区分会话密钥真实值和随机值的优势是可忽略的. 在被动安全的密钥交换协议中,设计主要关注防止被动攻击(如窃听),而不主动验证通信双方的身份. 因此,攻击者可以在通信过程中冒充任意一方,协议无法抵御主动攻击(如中间人攻击). 由于缺乏身份认证机制,被动安全的协议也被称为"无认证的密钥交换协议".

2.3　DH密钥交换协议

在公共网络上,双方通信需要确保安全,防止攻击者读取传输的信息,发生未经授权的访问或信息的意外泄露. 安全传输意味着使用加密密钥对信息进行加密,然后将其从一方发送到另一方. 为了实现两方之间安全地密钥传递,DH密钥交换协议被提出. 协议双方共享公共参数g和q,通过交换公钥信息来导出会话密钥,该密钥随后用于对后续的消息进行对称加密. DH密钥交换协议如图1所示,协议的两个参与方分别为Alice和Bob. Alice和Bob各自拥有私钥和公钥:$(\mathrm{SK_A},\ \mathrm{PK_A})$和$(\mathrm{SK_B},\ \mathrm{PK_B})$,双方在交换彼此的公钥后,分别基于自身的私钥和对方的公钥计算出相同的共享密钥K. 协议的正确性基于指数运算的可交换性,安全性则基于离散对数困难问题.

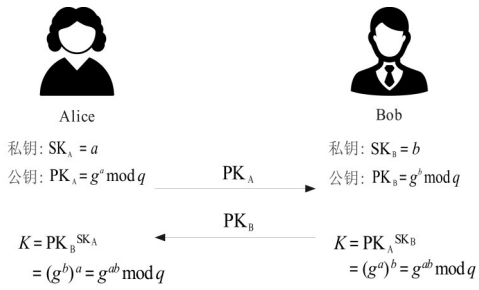

图1　DH密钥交换协议

DH密钥交换协议在网络安全通信和数据保护领域有着广泛的应用,例如,SSL/TLS协议采用DH密钥交换协议使客户端和服务器之间可以在不安全的网络中安全地交换对称加密算法所需的密钥;无线通信协议使用该协议进行基站和移动设备之间的密钥交换;虚拟专用网络(Virtual Private Network,VPN)协议和分布式系统使用该协议进行节点之间的密钥协商.

3　基于格的类DH密钥交换协议设计

DH密钥交换协议基于离散对数困难问题,无法抵抗量子计算机的攻击. 为了开发能够抵御量子攻击的密钥交换协议,文献[13]基于RLWE困难问题提出第一个基于格的抗量子密钥交换协议. 该协议借鉴了DH密钥交换协议的设计理念,其框架如图2所示. 在这一框架中,协议双方各自生成公钥和私钥,并交换彼此的公钥. 在得到对方的公钥后,参与方使用自身的私钥和对方的公钥,通过特定函数$F_{\mathrm{A}}(F_{\mathrm{B}})$计算出近似相等的预共享密钥$K_{\mathrm{A}}\approx K_{\mathrm{B}}$,为了确保双方协商出一致的会话密钥,Bob需要使用辅助函数Hint计算关于K_{B}的提示值(信号)w,并将其发送给Alice. 随后,双方根据各自

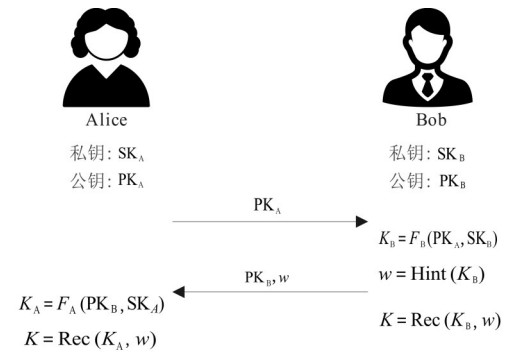

图2　基于格的类DH密钥交换协议设计框架

的预共享密钥和提示值,通过调和函数Rec计算出相同的会话密钥K. 这种机制被称为协调机制.

协调机制是实现基于格的类DH密钥交换协议的重要途径. 根据从近似共享值协商出精确共享值的方式,协调机制主要分为两大类:文献[13]提出的协调机制和文献[17]提出的协调机制,分别记为Ding协调机制和Peikert协调机制. 这两种协调机制是格上类DH密钥交换协议的基础.

3.1 Ding协调机制

在基于Ding协调机制的密钥交换协议[13]中,协议双方的近似共享值在最低有效位上一致. 协议响应方Bob发送提示值,有助于恢复最终生成的会话密钥的最低有效位,以便双方(以非常高的概率)就近似共享值中的相同值达成一致. 特别地,在Ding协调机制中,加性噪声项e、e'和e''乘以2,这样(除了模环绕),近似共享值K_A和K_B在最低有效位上一致. Bob发送的提示信息旨在(以非常高的概率)解决Alice的值K_A和Bob的值K_B具有不同模环绕(即相差一个模数q)的问题. 对于K_B的每个系数,Bob发送一个比特的信息,说明系数是否在区间$[-q/4, q/4]$中. 对于此区间内的系数,Alice和Bob的值有相同的模环绕,因此他们只需要提取最低有效位. 对于不在此区间内的系数,Alice和Bob需要在提取最低有效位之前添加$q/2$.

鉴于专利权保护机制的约束,Ding协调机制在推广与普及的进程中面临一定的局限性,导致其当前的应用范畴主要聚焦于Ding系列相关密钥协商协议中,向其他工作的拓展与应用较少.

3.2 Peikert协调机制

与Ding协调机制中使用最低有效位不同,Peikert协调机制利用近似共享值的最高有效位得到最终共享密钥. 特别地,Peikert协调机制将近似相等的预共享密钥值分为四个区间,其中两个区间具有相同的信号比特,如果它们不是相邻区间,则具有不同的信号比特. 即使攻击者可以得到密钥的信号信息,也无法确定密钥所在的区间. 在具体实施中,协议通过定义舍入函数、交叉舍入函数和协调函数,并集成运用这些函数以计算最终的共享密钥.

与Ding协调机制相比,Peikert协调机制受到众多密钥交换协议的青睐,并被广泛采用. 特别地,文献[18]将Peikert协调机制应用到密钥交换协议中,并进一步集成到TLS协议中进行了试验. 为了评估协议的性能,文献[19]对文献[18]中的协议与文献[13]中的协议进行了比较分析,结果表明,文献[13]中的协议具有较低的计算成本,且比文献[18]中的协议快11倍. 随后,文献[20]推广Peikert协调机制,基于LWE问题提出密钥交换协议Frodo,协议在多个比特达成一致,但要求误差值保持在较小的范围内. 为了获得更大的容错能力,文献[21]提出了密钥交换协议NewHope. 协议扩展了Peikert协调机制,通过引入多比特信号值替代之前的单比特信号值,并从四个系数中提取一个比特. NewHope协议在综合性能方面表现出色,谷歌在其Chrome网络浏览器的测试版本中使用该协议保护浏览器的安全性[22].

Ding协调机制和Peikert协调机制的最初版本会产生有偏差的密钥,需要借助“随机加倍”技术避免这种情况. 为此,文献[23]在Peikert协调机制的基础上引入了SafeBits的概念,进而提出了更有效的协调机制,并基于此设计了协议HILA5. 由于SafeBits技术可以产生无偏秘密,协议无需借助随机加倍函数来消除密钥的偏差. 与NewHope协议相比,HILA5协议在保持高效的同时,传输的消息长度更短,协商失败率更低.

3.3 比较分析与应用拓展

基于协调机制的密钥交换协议是帮助通信双方建立共享密钥的重要实现方式,除此之外,还可以通过公钥加密的方式实现共享密钥的建立,这种方式也称为密钥传输协议. 基于公钥加密的密钥传输协议直接来源于基于LWE/RLWE的加密方案[12,24]. 密钥交换协议与密钥传输协议的不同之处仅在于(通信双方Alice和Bob为了达成一致的共享密钥)Bob发送的额外信息. 在密钥交换协议中,Bob发送的是信号值;在密钥传输协议中,Bob发送的是密文. 与基于公钥加密的密钥传输协议相比,基于协调机制的密钥交换协议可以提供更高的带宽利用率.

事实上,协调机制不仅局限于密钥交换协议,还可以被广泛地用于构造多样化协议,其中典型代表为认证密钥协商协议[25]. 认证密钥协商协议在继承传统密钥协商协议功能性的基础上,进一步集成了身份验证机制,确保了通信双方在密钥协商过程中的身份真实性与可靠性,这一特性使得其在互联网环境中的应用尤为广泛与重要. 当前,针对协调机制的深入研究与实践探索正持续深入,旨在不断拓展其应用领域并优化其性能表现,为更多元化的信息安全需求提供坚实支撑[26].

4 密钥重用攻击

密钥重用是指在多个会话中重复使用同一个密钥,避免了每次会话都生成新密钥的复杂过程,被视为一种提高协议运行效率的手段. 尽管密钥重用在实际中很常见[27],但这并不意味着它是安全的. 重复使用密钥可能会增加数据泄露、未授权访问和其他安全风险的可能性. 特别地,文献[28]展示了互联网密钥交换(Internet Key Exchange,IKE)协议重用密钥对可以使攻击者绕过身份验证,入侵受害者主机或网络.

2015年,文献[29]指出,基于协调机制的RLWE密钥交换协议在密钥重用环境下存在密钥泄露的风险.随后,针对密钥交换协议的密钥重用攻击,学术界开展了一系列的研究工作.这些研究依据攻击者恢复不同协议参与方的密钥,可分为两大类别:一是信号泄露攻击,攻击者通过观察协议响应方的信号值(提示值),恢复协议响应方重用的密钥;二是密钥不匹配攻击,攻击者观察协议发起方计算的密钥与目标密钥是否匹配,进而成功恢复其密钥.

4.1　信号泄露攻击

信号泄露攻击最初聚焦于DING12密钥交换协议[13],旨在深入剖析该协议在替代传统DH密钥交换协议后所可能遭遇的潜在安全脆弱性.此后,该攻击策略被泛化并应用于Ding系列相关协议的分析中.随着研究的深入与技术的迭代,攻击手段持续优化与增强,不仅提升了攻击效率,还显著拓宽了攻击范围,逐步将目标扩展至基于Peikert协调机制的密钥交换协议体系,特别是其标志性成员——NewHope协议,以及一系列认证密钥交换协议,从而揭示了更广泛的协议在面对此类攻击时可能存在的安全挑战.

2017年,文献[30]证明RLWE密钥交换中使用的信号函数可以泄露信息以恢复重用公钥对应的私钥,并称这种攻击为信号泄露攻击.如图3所示,攻击者Eve扮演协议的发起方,在与诚实的响应方Bob建立会话的过程中,Eve巧妙地构造自己的公钥PK_E.按照图2中协议的流程,Bob得到Eve的公钥PK_E后,首先计算预共享密钥K_B,然后计算K_B的信号值w.Alice收到Bob的信号值w后,通过分析w成功恢复出文献[13]协议中Bob重用的私钥SK_B.然后,文献[31]通过引入更为精准的查询目标定位机制,显著减少攻击所需的查询次数,提高攻击的效率.接着,文献[32]应用稀疏信号收集策略,进一步减少信号泄露攻击所需的样本数量,不仅提高了对DING12密钥交换协议[13]的攻击效率,还攻破文献[33]提出的DBS密钥交换协议的密钥重用安全性.随后,文献[34]通过将信号泄露攻击问题转换为编码问题,并将其应用到密钥交换协议[13,33]中,显著减少恢复重用密钥所需的询问次数.鉴于文献[34]的方法存在大量的冗余操作,文献[35]最近改进了文献[34]的方法,提出一种将信号泄露攻击与深度优先搜索相结合的有效方法,进一步减少恢复重用密钥所需的询问次数.

在文献[31]的工作中,他们除了对基于Ding协调机制的协议进行分析外,还将攻击扩展到基于Peikert协调机制的密钥交换协议中,成功恢复出协议响应方重用的密钥.受到文献[30]工作的启发,文献[36]提出对NewHope协议[21]的信号泄露攻击.与Ding协调机制和Peikert协调机制相比,NewHope协议的协调机制更复杂,其信号函数基于一个特殊的格而构建,信号不会像DING12密钥交换协议那样有规律地变化.特别地,他们对NewHope协议的信号函数进行了详细的分析,并根据信号的特殊性质,巧妙构造发送的消息,恢复出协议响应方重用的密钥.

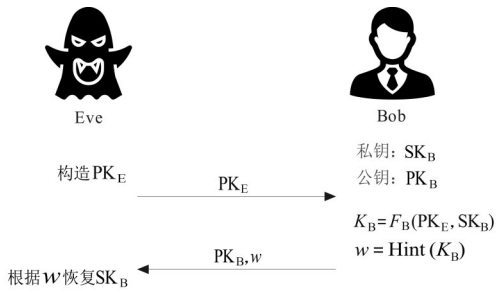

图3　信号泄露攻击

认证密钥协商协议同样存在临时密钥重用的情形,进而为攻击者提供了实施密钥重用攻击的可能性.2021年,文献[37]提出对Islam认证密钥协商协议[38]的信号泄露攻击,攻击者通过信号函数的输出恢复诚实方的密钥.最近,文献[39]指出,基于LWE的认证密钥交换协议[40]的一个安全弱点,使其容易受到信号泄露攻击.他们不仅设计并实施了一种具体的攻击策略,以验证该安全弱点的实际影响,还提出了相应的防御机制,旨在增强协议对信号泄露攻击的抵抗能力.匿名口令认证密钥交换协议是一种特殊的认证密钥交换协议[41~45],旨在允许用户以匿名的方式与服务器建立会话密钥用于后续通信,同时通过共享的低熵口令实现服务器对用户的访问权限认证.协议的关键在于保护用户的匿名性,即确保在认证和密钥交换过程中,用户的真实身份不会被泄露给服务器或第三方攻击者.2022年,文献[46]提出对基于格的匿名口令认证密钥交换协议LBA-PAKE[47]的信号泄露攻击,指出当协议重用主密钥时,协议中的信号值会泄露密钥的信息.同年,文献[34]用757次询问完全恢复出协议LBA-PAKE[47]的密钥.此外,他们还对文献[48]提出的双因素认证方案进行分析,并利用一次查询揭示了方案中秘密的部分信息.

4.2　密钥不匹配攻击

密钥不匹配攻击可追溯至Fluhrer攻击,旨在分析RLWE密钥交换协议在密钥重用情境下的安全性.此后,此类攻击策略被进一步拓展并应用于Ding系列密钥协商协议中,揭示了其潜在的安全漏洞.鉴于密钥封装机制可以作为密钥交换协议的有效实现方式,加之NIST推动的抗量子密码标准化进程,针对密钥封装机制的密钥不匹配攻击研究已成为学术界和工业界共同关注的焦点.为应对这一挑战,一系列旨在优化与增强

密钥不匹配攻击的改进策略与技术创新相继被提出，显著提升方案的安全保障能力.

2016 年，文献[49]提出针对 RLWE 密钥交换协议的重用密钥攻击. 与信号泄露攻击不同，Fluhrer 攻击关注的是协议的发起方. 如图 4 所示，攻击者 Eve 扮演协议响应方，在与诚实的发起方 Alice 进行交互的过程中，按照图 2 中的协议流程，Eve 计算预共享密钥 K_E 及其信号值 w，并发送特殊构造的消息，包括公钥 PK_E 和信号值 w. Eve 通过判断 Alice 计算的密钥 K 是否与自己计算的密钥 K' 相同（Eve 使用密钥 K 加密消息发送给 Bob，根据 Bob 的反应判断 K' 是否与 K 相同），从而获得 SK_A 的信息，进而恢复 Alice 重用的密钥 SK_A. 这种密钥重用攻击被称为密钥不匹配攻击，该名字精准地捕捉到了攻击使用的关键策略——判断双方计算的共享密钥是否匹配. 为了降低实施该攻击所需的样本数量，文献[32]提出了稀疏信号采集策略，不仅大幅度提升了攻击效率，为实现高效的攻击提供支持，还为后续的技术革新与深化研究奠定了坚实的基础.

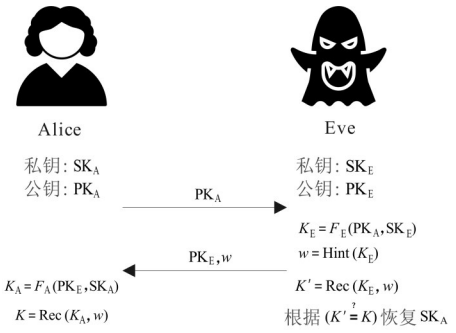

图 4 密钥不匹配攻击

受到文献[49]工作的启发，文献[31]于 2018 年提出了一种针对 DING12 密钥交换协议[13]的密钥重用攻击，其中攻击者通过判断最终计算的共享密钥是否一致，恢复协议发起方重用的密钥. 随后，文献[50]指出两个基于 Ding 协调机制的密钥交换协议也会遭受密钥不匹配攻击. 一个是可重用密钥的 RLWE 密钥交换协议，该协议是 NIST 抗量子密码标准化活动第一轮候选方案 Ding Key Exchange[51]的重要组成部分. 另一个是实用的随机 RLWE 密钥交换协议[52]，该协议在 DING12 密钥交换协议[13]的基础上，加入了额外的扰动项. 协议共有两种设计模式，一种是常规模式，另一种是密钥重用模式. 在常规模式中，每次实例化协议时都会生成新的密钥，而密钥重用模式支持双方重用公钥/私钥. 由于公钥/私钥的复用，在密钥重用模式下计算和通信成本较低. 在文献[50]提出的密钥不匹配攻击中，攻击者选择一个具有特殊结构的 RLWE 样本作为自己的公钥，并精心构造信号值，然后将两者一起发送给重用密钥的诚实发起方. 通过判断发起方计算的共享密钥与自己计算的密钥是否一致，攻击者能够恢复发起方重用的密钥.

NIST 抗量子密码算法标准化的提交要求和评估准则指出，IND-CPA（INDistinguishability under Chosen Plaintext Attack）安全的密钥封装机制可以被用作被动安全的密钥交换协议. 因此，针对密钥封装机制的密钥不匹配攻击，涌现出了一系列的研究工作[53~55]. 2022 年，文献[56]结合格攻击技术，进一步降低密钥不匹配攻击所需的询问数. 具体而言，使用密钥不匹配攻击恢复部分密钥信息后，直接影响了密钥分布的统计特性，具体表现为对密钥的均值与协方差参数的显著扰动. 这种扰动降低了密钥空间的随机性与复杂性，从而为格攻击提供更为有利的条件，使得格攻击的实施变得更加简单和高效. 随后，文献[57]改进了密钥不匹配攻击，使得攻击者每次询问可以同时揭示多个系数的信息，从而显著降低了攻击所需的询问次数，进一步逼近攻击复杂度的下界. 与此同时，文献[58]也对密钥不匹配攻击进行了改进，与文献[57]采用的技术不同，文献[58]通过并行技术，在一次询问中同时恢复多个系数的信息. 最近，文献[59]结合并行技术和格攻击技术，对 NIST 抗量子密码标准算法 Kyber 实施了密钥不匹配攻击. 攻击结果显示，密钥的重复使用会显著削弱 Kyber 的安全性. 因此，在实际应用中，应避免 Kyber 重用密钥，以确保系统的安全防护水平不受此类攻击模式的影响.

与信号泄露攻击类似，认证密钥交换协议同样会遭受密钥不匹配攻击的威胁. 2024 年，文献[60]对文献[61]提出的认证密钥交换协议进行了密钥不匹配攻击，并在此基础上提出了相应的改进策略，以增强协议的安全性. 随后，文献[62]进一步对文献[61]改进后的认证密钥交换协议进行了深入的密钥不匹配攻击测试，并基于测试结果提出了改进建议，旨在进一步巩固协议抵抗此类攻击的能力. 这一系列研究不仅揭示了认证密钥交换协议在应对密钥不匹配攻击方面的挑战，还为后续设计更加安全高效的协议提供了参考和启示.

4.3 对比分析

在信号泄露攻击中，攻击者巧妙构造发送的信息，与诚实的协议响应者发起多次会话，并分析响应方输出的信号值，从而获取响应方重用的密钥. 此类攻击的核心在于响应方在协议流程中引入了一轮额外的交互，传递了一个信号值，以帮助和协议发起方达成最终一致的密钥. 如果不存在该额外轮，即未发送该信号值，则协议将能够有效抵御信号泄露攻击，展现出更高的安全性.

相比之下，密钥不匹配攻击则聚焦于协议双方在

会话过程中协商生成的密钥是否保持一致性,与信号泄露攻击在攻击手段上存在显著差异. 此类攻击不依赖于信号泄露,而是通过分析或操纵密钥协商过程,试图破坏或利用密钥不匹配的状态来达到攻击目的. 因此,即便协议响应方不额外实施一轮传送信号值,也无法有效规避密钥不匹配攻击的风险.

5　支持密钥重用的密钥交换协议的设计

支持密钥重用的密钥交换协议被称为静态密钥交换协议. DH密钥交换协议是一种典型的静态密钥交换协议,在Internet标准中被普遍采用以提高性能. 例如,在TLS 1.2中,DH密钥交换协议提供静态密钥模式(密钥重用),避免每次会话都重新计算密钥. 在TLS 1.3[2]中,PSK(Pre-Shared Key)模式和0-RTT(0 Round Trip Time)模式要求客户端和服务器保持一个长期的公钥. 此外,密钥重用现象亦常见于不同的密码套件及其迭代版本之间,如TLS与IKE. 这主要归因于在实际应用中,为所有"密码套件族"及其不同版本维持独立的密钥对不仅具有极高的挑战性,而且往往不受支持.

基于格的密钥交换协议作为DH密钥交换协议在量子计算时代的有力替代方案,在密钥重用环境下并不安全. 因此,这些密钥交换协议不能直接替代DH静态密钥交换协议. 为了探索支持密钥重用的密钥交换协议,一系列研究成果已相继涌现. 这些研究遵循了四条核心技术路径以达成其目标:一是构建多实例密钥交换协议框架,通过生成多个密钥实例,随后实施这些实例的随机化组合策略,从而支持密钥的重用;二是引入pasteurization技术,通过对重用的密钥进行特定的转换,提升密钥在重复使用过程中的随机性;三是添加随机性扰动,以保护重用密钥的安全;四是提出并论证全新的概念性设计方案,从根本上革新密钥重用的安全实现机制,通过理论创新与实践验证,实现密钥安全重用的目标. 上述四条路径共同构成了当前该领域研究的主要内容.

5.1　多实例密钥交换协议

密钥重用攻击的关键在于不诚实的协议参与者使用刻意构造的公钥,使得密钥协商协议中诚实的另一方重用的密钥被恢复. 为此,文献[63]提出一种通用的转换方法,可以对这些密钥协商协议进行转换,从而有效抵御密钥重用攻击. 如图5所示,在密钥协商过程中,协议双方先各自生成n个不同的密钥对(包含公钥和私钥),并交换彼此的n个公钥. 在得到对方的n个公钥后,参与方通过密钥协商函数KAF(Key Agreement Function)计算n^2个不同的共享密钥K^m,$m\in[1, n^2]$,这些共享密钥通过以所有可能的组合执行密钥协商(如图5协议流程)而获得. 最后,对这些共享密钥进行哈希运算H,得到最终的共享密钥K. 在这种方案下,任何使用恶意构造的公钥的行为都会导致共享密钥计算失败,从而有效应对密钥重用攻击. 此外,协议协商失败的数量随k呈指数增长,这使得攻击者无法提前预测可能的失败后果. 因此,攻击者无法谎报其最终共享密钥值,从而无法修复由密钥重用攻击所引发的安全漏洞与风险.

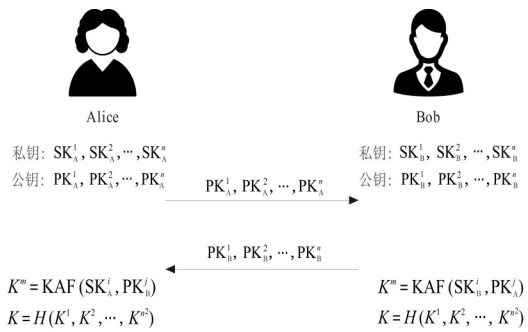

图5　多实例密钥交换

他们将这种转换应用到多种抗量子密钥协商方案,并分析攻击者的成功概率,以确定128位安全级别所需的参数大小. 虽然该转换导致密钥尺寸较原有方案扩大了k倍,计算时间也随之增长至k^2倍,然而,其为探索设计静态抗量子密钥交换协议提供了一条潜在的、有前景的路径.

5.2　Pasteurization技术

为了设计支持密钥重用的密钥交换协议,文献[51]在NIST抗量子密码标准化活动第一轮候选方案Ding Key Exchange中提出一个可重用密钥的RLWE密钥交换协议,其中协议支持响应者重用密钥. 具体来说,协议采用一种被称为"pasteurization"的技术,保证协议的发起方发送的RLWE样本与随机均匀的样本无法区分,确保在整个密钥交换过程中响应方的密钥信息没有被泄露. 如图6所示,参与双方先各自生成公钥和私钥,并交换彼此的公钥. 参与方在得到对方的RLWE样本(公钥信息)后,基于图2的协议流程,先对其进行变换(记为T),得到"新的公钥"(由于变换T相当于重新进行一次RLWE计算,因此新的公钥和随机均匀样本无法区分). 然后,通过密钥导出函数KDF(输入自身私钥和对方新的公钥)得到最终的共享密钥K. 随后,文献[50]对这个协议进行了深入的剖析,并基于分析结果提出相应的优化策略,成功实现了协议发起方密钥的重用,从而进一步增强了协议的灵活性与效率.

接着,文献[33]基于可重用密钥的RLWE密钥交换协议[51]提出了一个支持密钥重用的密钥交换协议,其中协议双方均使用"pasteurization"技术保证其发送

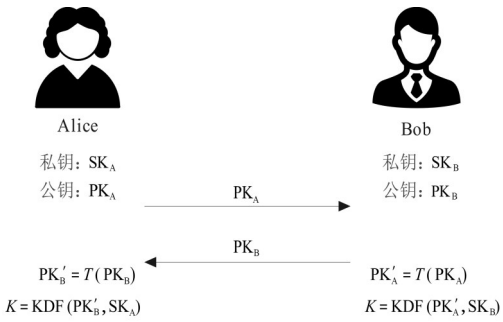

图6 pasteurization技术

的RLWE样本与随机均匀的样本无法区分. 然而,该协议后来被证明无法抵抗信号泄露攻击,在密钥重用环境下并不安全. 尽管如此,其中的巧妙思想和技术被一系列协议[64,65]所采纳. 文献[66]提出了一种抗量子的认证密钥交换协议. 协议的安全性基于Bi-GISIS(Bilateral Generalization Inhomogeneous Short Integer Solution)问题的困难性假设,并采用双边pasteurization技术,为协议提供了密钥可重用的特性. 随后,文献[67]基于Bi-GISIS困难问题提出了一种密钥交换协议,其中为了获得可重复使用的密钥,他们对双边pasteurization技术进行了改进. 协议可用于保护抗量子物联网的安全,其中密钥可重用的特性有效减少了物联网设备中使用密钥交换协议生成密钥的时间消耗,提升了系统的运行效率.

5.3 添加随机性扰动

2018年,文献[52]提出了一个实用的随机RLWE的密钥交换协议,协议有两种设计模式,一种是常规模式,另一种是密钥复用模式. 在密钥重用模式下,协议的响应方增加了更多的随机性,保护自己重用的密钥. 文献[50]同样对这个协议进行了深入的剖析,并基于分析结果提出相应的优化策略. 如图7所示,协议参与双方Alice和Bob先各自生成公钥和私钥,并交换彼此的公钥. 参与方在得到对方的公钥后,基于图2的协议流程,分别选择随机性δ_A和δ_B,并在使用密钥导出函数KDF(Key Derivation Function)计算最终的共享密钥K时,加入相应的随机性. 随机性的引入使得攻击者无法

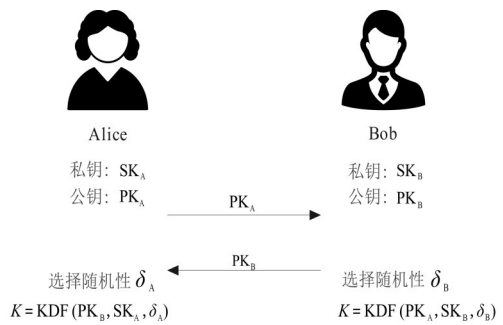

图7 添加随机性扰动

通过判断共享密钥是否一致来获取对方的私钥信息. 这些策略有效实现了协议参与方密钥的重用,显著提升了协议的灵活性与执行效率,为协议性能的优化与实际应用场景的拓展奠定了坚实基础.

最近,文献[68]基于先前的工作[50,52],设计并实现了一个高效的RLWE密钥交换协议. 协议采用了创新的架构设计,通过在协议双方计算近似共享密钥时添加随机性扰动,保证了随机密钥交换,旨在有效抵抗信号泄露攻击和密钥不匹配攻击,进而支持协议双方的密钥重用. 与先前的工作[50,52]相比,此设计在确保安全性的前提下,显著减少了计算开销,从而极大地优化了系统的整体运行效率与性能表现.

5.4 分裂密钥封装机制

为了提高对支持密钥重用的密钥交换协议的认识,文献[69]引入了分裂密钥封装机制(Split Key Encapsulation Mechanism, Split KEM)的概念,将基于DH协议的所需密钥可重用性转换为对基于KEM的消息流的研究. 如图8所示,在分裂密钥封装机制中,解封装方Alice生成解封装密钥对(D,d),封装方Bob生成封装密钥对(E,e). 在使用sEncaps封装密钥K时,不仅接收解封装方的公钥D作为输入,还接收封装方可能是静态的密钥e作为输入. 同样,在使用sDecaps解封装密文c时,不仅接收解封装方的密钥d作为输入,还接收封装方可能是静态的公钥E作为输入. 分裂KEM实现了更细粒度的密钥封装机制,其中封装过程分为密钥生成和后续的共享密钥计算步骤. 事实上,提交给NIST抗量子密码学标准化过程的许多KEM提案的被动安全(IND-CPA)版本,特别是基于格的提案,都可以看作是分裂KEM格式:封装过程可以分为密钥生成和共享密钥计算部分.

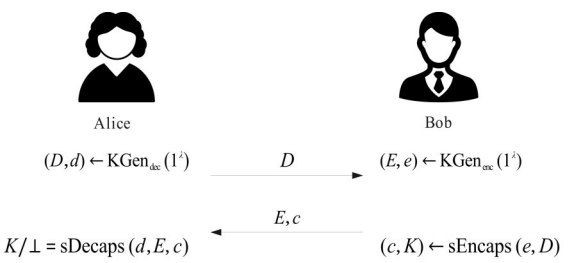

图8 分裂密钥封装机制

在给出分裂KEM的定义及其安全性后,文献[69]尝试基于抗量子困难假设对其进行安全地实例化. 尽管他们实例化的分裂密钥封装机制只实现了单边密钥重用,然而,这一机制的创新性应用为探索与构建静态密钥交换协议框架开辟了一条具有潜力的新途径.

除了基于格构建静态密钥交换协议外,基于同源的构造也是实现静态密钥交换协议的重要途径[70~72].

基于同源的密钥交换协议依赖于椭圆曲线之间同源的困难性,为密钥交换提供了一种新的、独特的视角和解决方案,进一步丰富了静态密钥交换协议的设计和实现手段.

5.5 对比与分析

为了深入理解上述四种支持密钥重用的技术,我们在图2协议(下称基础协议)的基础上,应用四种技术,并将得到的协议与基础协议在通信开销、安全性等方面进行对比,详见表1. 在通信开销方面,多实例密钥交换由于要交换彼此的n个公钥,因此通信开销是基础协议的n倍;而基于其他三种技术的协议,通信开销与基础协议相同. 在安全性方面,这四种技术均未改变原有协议的安全性,因此基于这些技术的协议都是被动安全的. 在计算复杂度方面,多实例密钥交换需要进行n^2次密钥协商,因此计算复杂度是基础协议的n^2倍;pasteurization技术需要重新计算一个新的公钥,计算复杂度较高;添加随机性扰动增加了抽样和相关计算步骤,计算复杂度高于基础协议;分裂密钥封装机制引入了更多的变量和计算,因此计算复杂度也高于基础协议. 在支持密钥重用方面,这四种技术均支持密钥重用. 在交互性方面,基于这四种技术的协议均未改变基础协议的交互性.

表1　基于四种支持密钥重用技术的协议的对比

协议(技术)	通信开销	安全性	计算复杂度	支持密钥重用	交互性
多实例密钥交换	n倍	被动安全	非常高(n^2倍)	支持	交互
pasteurization技术	相同	被动安全	较高	支持	交互
添加随机性扰动	相同	被动安全	高	支持	交互
分裂密钥封装机制	相同	被动安全	高	支持	交互

6 NIKE协议的设计

非交互密钥交换协议是一种特殊的密钥交换协议,其特点在于通信双方可以在没有直接信息交互的情况下生成一个共享密钥. 这种特性使得非交互密钥交换协议具有较低的通信复杂性,特别适用于资源受限的无线移动通信环境. 非交互密钥交换协议的设计通常基于复杂的数学难题或密码学原理,以确保密钥的安全性和不可预测性. 如图9所示,在NIKE协议中,参与双方先各自生成公钥和私钥,并交换彼此的公钥. 在获得对方的公钥后,Alice可以通过密钥导出函数KDF(输入Alice的私钥SK_A和Bob的公钥PK_B)计算共享密钥K;Bob也可以通过密钥导出函数KDF(输入Bob的密钥SK_B和Alice的公钥PK_A)计算相同的共享密钥K,整个过程无需额外交互. DH密钥交换协议是一个典型的NIKE方案.

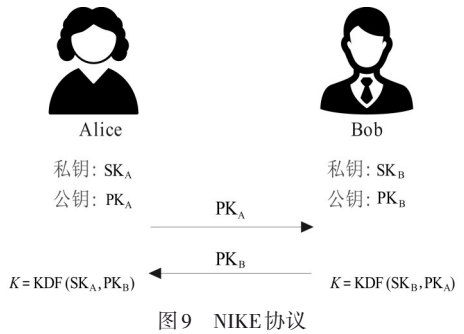

图9　NIKE协议

6.1 非交互性和抗量子迁移

在量子计算威胁日益显著的背景下,基于格的密钥交换协议[13,17,18,20,21]凭借其高效性,被视为是DH密钥交换协议在未来量子计算时代的潜在强有力替代. 然而,这些基于格的协议本质上偏离了DH协议的非交互性核心特征,其执行过程中引入了额外的交互,与DH密钥交换协议有着本质的不同. 具体而言,与DH协议非交互性相比,基于格的密钥交换协议因缺乏此特征而引入不必要的效率损耗,表现为额外的通信轮次和计算负担. DH协议无需多次往返通信即可达成密钥共享,而基于格的密钥交换协议则需要更多的交互步骤,这在实际应用中可能会导致效率降低.

对于许多已经内置交互的应用程序,基于格的密钥交换协议是DH协议的完美替代. 然而,在许多场景中,NIKE协议的非交互式特性至关重要. 特别地,在抗量子密钥交换协议的迁移中,对于一些使用DH协议的应用,如果非交互性未得到利用,那么向抗量子密钥交换的迁移相对简单,例如TLS协议. 然而,如果应用了DH协议的非交互性,抗量子密钥交换的迁移则会变得复杂. 这在一系列安全通信协议中表现得尤为明显,例如OPTLS、WireGuard、Noise协议框架、Signal安全消息协议和X3DH协议. 这些协议的一个显著技术特征是,它们共同依赖于静态DH密钥进行身份验证.

6.2 协议设计的探索与达成

在致力于开发基于格的NIKE的研究进程中,文献[73]于2017年率先勾勒出了一个开创性的设想,旨在构建一种被动安全的NIKE机制. 在此基础上,文献[74]深化了对该领域的探索,不仅贡献了一个具体的实现蓝图,还初步探讨了相关参数配置的设定. 然而,该实现方案在理论层面未能正式考虑被动安全性,同时忽视了主动安全性的评估,这构成了其显著的理论局限性. 此外,实践

验证表明,所选取的参数配置策略存在潜在风险,可能诱发密钥协商过程中密钥不一致的现象,从而对协议的整体有效性和可靠性构成不利影响.

2020年,文献[75]深入探讨了基于格设计NIKE协议的潜在可行性.具体而言,研究者们通过两个可有效计算的密钥协调函数来刻画NIKE,并充分考虑了三类密钥协调函数.通过严谨地分析,他们指出其中两类函数在构建NIKE时存在根本性局限,即这些函数无法充分满足NIKE协议的安全与效率要求.进一步地,他们指出第三类函数在构造NIKE时面临的核心技术难题:任何基于格的且具有多项式模噪声比的NIKE都不可避免地会面临协商出错的风险,这一挑战构成了当前研究领域的显著障碍.

事实上,所有已知的NIKE安全性规约均未能达到紧致性,实现紧致安全的NIKE方案面临的主要技术挑战在于自适应安全性.为了研究NIKE方案的安全性规约,文献[76]深入探索了选择性安全和完全自适应安全之间的安全概念和方案.具体来说,他们发现,通过扩大NIKE的公钥和私钥尺寸可以获得更紧致的安全性规约,虽然这种权衡存在固有限制,但是可以通过放宽对安全性的严格要求,规避该固有限制.特别地,他们基于LWE问题,首先构造了一个基于标签的NIKE,然后在此基础上计算NIKE最终的共享密钥.这一研究成果为基于格的NIKE协议设计提供了新的视角与思路.

经过一系列的尝试,2023年,文献[77]基于模格上容错学习(Module Learning With Errors,MLWE)问题,设计了一种创新的非交互式密钥交互协议——Swoosh.该研究深入分析Swoosh协议的安全性,并据此提出了详细的参数设置以优化其实现.随后,通过与同类型的方案对比,揭示了Swoosh协议在密钥尺寸缩减和运行效率提升方面的显著优势.特别地,他们首先构建了一个被动安全的NIKE方案,然后通过应用一个通用编辑器技术,进一步将该协议提升至主动安全级别,增强了协议的防御能力.事实上,他们的工作与文献[75]的研究结论是一致的,即当采用超多项式模噪声比的MLWE实例时,实现NIKE协议是可行的,文献[77]的确采用了符合此条件的参数设置.

6.3 协议的多用户安全性

为了拓展NIKE的应用场景,文献[78]探讨了基于LWE的NIKE方案的多用户安全性,即当同一公钥被用于与多个不同用户生成共享密钥时(如图10所示)协议的安全性.当所有用户都诚实地为NIKE方案生成密钥,且其正确性误差可以忽略不计时,该方案能够有效保障多用户环境下的安全性.然而,基于LWE的NIKE方案为了实现可忽略的误差,需要依赖于一个超多项式复杂的模型,进而影响了其整体效率表现.研究表明,当误差不可忽略时,单用户安全并不意味着多用户安全.尽管如此,当系统中用户数量被预先设定为固定值时,基于LWE的多项式模NIKE方案,在诚实用户群体内,依然能够实现多用户安全性的要求,这一结论得益于LWE问题固有的抗侧信道泄露特性.进一步地,研究探索了一个增强的多用户安全模型框架,该框架允许存在恶意实体参与公钥的生成过程,从而提升了安全威胁的复杂性.值得注意的是,以往基于LWE的NIKE方案在达到此类增强型安全目标时,往往依赖于量子随机预言机模型,而该研究的所有成果均在无需此类假设的标准模型下获得验证,展现了更高的实用价值和理论深度.

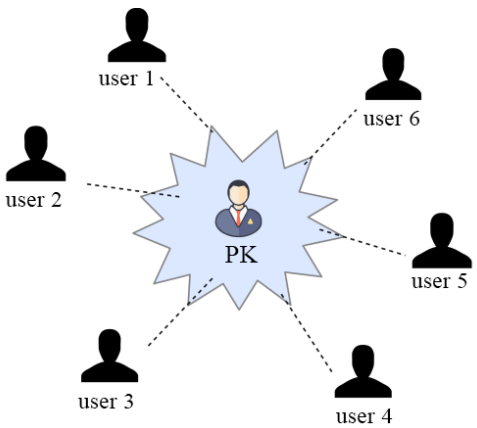

图10 多用户场景

6.4 非交互性和密钥重用安全性

事实上,协议的交互性和协议的密钥可重用性之间存在着一定的关联性.由密钥重用而引起的信号泄露攻击,本质上是协议交互模式带来的直接后果.具体而言,如果协议的响应方不发送额外的信号值给发起方,则攻击者就无法通过分析信号值来恢复响应方重用的密钥.换言之,如果协议设计为非交互式,则有望规避信号泄露攻击,从而提升协议的安全性.

为了进一步拓展NIKE方案的应用场景,研究人员开始聚焦于其多用户场景下的安全性评估与优化.在此场景中,同一公钥被用于与多个不同用户安全地生成共享密钥,这一设定与密钥重用安全性的需求高度契合,均要求在确保安全性的前提下,能够高效支持通信.因此,深入探究协议的多用户安全性和密钥重用安全性之间的内在联系,对于理解协议运作机制,提升协议安全能力及效率具有重要的意义.这一研究方向不仅有助于优化现有协议架构,还可能启发新的安全协议设计理念,从而推动量子安全通信领域的持续发展.

7 未来研究方向展望

通过对支持密钥重用的格上NIKE协议相关文献

的系统梳理与深入分析,本文提出了几点具有前瞻性的研究方向,以供进一步探索与拓展.

(1)在支持密钥重用的策略中,多实例密钥交换因成本较高而面临挑战;分裂密钥封装机制目前仍停留在理论层面,未得到充分实践;Pasteurization技术和随机性添加方法在应对信号泄露攻击时效果有限,难以有效保障响应方密钥的重用. 因此,未来的一个重要研究方向是探索切实可行的策略,以实现协议响应方密钥的安全重用. 具体而言,可以通过以下方法实现密钥的安全重用:①采用分层密钥派生机制,从主密钥派生出多个会话密钥,确保每次会话使用不同的密钥;②利用零知识证明技术验证密钥的合法性,防止信号泄露攻击;③使用基于身份的加密技术,将用户身份与密钥绑定,增强密钥重用的安全性;④引入同态加密技术或多方计算技术,保护密钥派生过程,确保密钥重用的安全性.

(2)支持密钥安全重用的关键在于有效防范密钥重用攻击,其中抵御信号泄露攻击尤为重要,这种攻击往往部分归因于协议所采用的协调机制. 如果能够证明信号泄露攻击是协调机制固有的脆弱性,这将指引我们调整研究方向,明确研究目标,进而探索基于格的类DH协议设计的新路径,突破传统协调机制的局限. 具体而言,可以通过以下方法分析方案的固有脆弱性:①将方案置于形式化的安全模型中,若攻击在模型中被证明有效,则说明这是方案的固有脆弱性;②通过归约证明,将方案的安全性建立在某个已知困难问题上,若攻击能够绕过这种归约,则说明方案存在固有脆弱性;③若攻击依赖于方案设计中的某些不切实际的假设,则可以证明这是固有脆弱性.

(3)Swoosh协议是一种重要的基于格的NIKE协议,通过采用较大的参数设置,确保协议能够成功协商出一致的会话密钥. 然而,这种做法也带来了较高的通信成本和计算复杂度,从而在一定程度上限制了其在实际场景中的广泛应用. 为了提升该协议的实用价值,进一步优化显得尤为迫切,特别是在确保协议正确性的同时,合理缩减参数规模,寻求安全性与效率之间的最佳平衡点,这将是未来研究的重要方向. 格密码方案的参数选择是一个复杂的过程,需要结合理论分析、实验验证和工具支持,综合考虑安全性、效率和实现细节,以选择最优参数. 目前已有一些工具和资源可辅助参数选择,例如:①LWE Estimator,用于评估基于LWE问题的方案安全性,提供多种攻击算法的估计,帮助用户选择合适的参数;②PQCrypto,专注于后量子密码学的资源集合,提供多种格密码相关工具和实现;③Lattice-Based Crypto library (LBC),开源的格密码库,提供多种格密码方案的实现和参数选择工具.

(4)当前NIKE协议的设计在技术路线上较为单一,主要体现在从近似相等的预共享密钥推导最终会话密钥的方法上. 特别地,Swoosh协议通过从近似相等的预共享密钥的最低位中提取一致的共享秘密. 因此,探索并开发多样化的设计路径与方法,是未来研究中亟待重视的重要方向. 值得注意的是,Swoosh协议通过引入零知识证明技术实现了非交互性. 因此,深入探索和优化零知识证明技术将成为设计NIKE协议的关键方向之一. 此外,近年来基于编码的NIKE协议已被提出并得到广泛研究. 由于编码问题与格问题在数学结构和困难性上存在密切关联,这类协议为设计基于格的NIKE协议提供了重要借鉴和启发. 通过借鉴编码问题的解决方案并结合格密码学的优势,有望设计出更高效且安全的NIKE协议.

(5)以往对协议的密钥可重用性和非交互性的研究,通常采用彼此独立的研究路径. 然而,事实上,密钥可重用性和非交互性之间存在密切的内在联系,例如信号泄露攻击与非交互性的关联,以及NIKE的多用户安全性与密钥重用之间的相互影响. 如果能够系统性地将这两个特性融合起来进行综合研究,可能会同时解决这两个问题,从而实现更高的研究效率. 具体而言:可以基于格密码的数学结构,设计一种同时支持密钥重用和非交互性的协议;鉴于信号泄露攻击通常与非交互性协议中的密钥重用有关,可以设计一种能够抵抗信号泄露攻击的非交互式协议,同时支持密钥重用;由于多用户安全性是NIKE协议的重要目标,而密钥重用可能增加多用户环境下的安全风险,可以设计一种同时支持多用户安全性和密钥重用的协议,实现两者的平衡.

8　结论

在抗量子迁移的背景下,作为DH密钥交换协议的潜在替代方案,基于格的类DH密钥交换协议设计备受关注. 遵循DH协议设计理念,基于格的类DH协议需要额外借助协调机制实现双方共享密钥的建立. 与DH协议相比,基于格的类DH协议展现出两大显著的区别:不支持重用密钥和非交互性. 一方面,基于格的类DH协议如果重用密钥会招致密钥重用攻击,另一方面,由于协调机制的引入,基于格的类DH协议本质上属于交互式协议范畴.

设计支持密钥重用的格上NIKE协议,有助于实现未来量子计算环境下对DH协议的无缝替代,减少向抗量子时代迁移过程中的成本负担. 本文全面而系统地梳理了设计过程中存在的问题及其面临的挑战,并展望了研究的未来发展趋势与潜在的研究方向,以期为该领域的进一步探索提供有价值的参考与启示,推动抗量子迁移技术的发展.

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] KUMARI N, MOHAPATRA A K. A comprehensive and critical analysis of TLS 1.3[J]. Journal of Information and Optimization Sciences, 2022, 43(4): 689-703.

[3] BIENSTOCK A, FAIROZE J, GARG S, et al. A more complete analysis of the signal double ratchet algorithm[M]//Advances in Cryptology-CRYPTO 2022. Cham: Springer Nature Switzerland, 2022: 784-813.

[4] MOUSAVI S J, CHAHARSOOGHI K, ALI MONTAZER G. Using blockchain to improve the security of the X3DH key exchange protocol[J]. International Journal of Information and Communication Technology Research, 2023, 15(3): 11-20.

[5] DOWLING B, RÖSLER P, SCHWENK J. Flexible authenticated and confidential channel establishment (fACCE): Analyzing the noise protocol framework[M]//Public-Key Cryptography-PKC 2020. Cham: Springer International Publishing, 2020: 341-373.

[6] 范桁. 量子计算纠错取得突破性进展[J]. 物理学报, 2023, 72(7): 7-9.
FAN H. Breakthrough of error correction in quantum computing[J]. Acta Physica Sinica, 2023, 72(7): 7-9. (in Chinese)

[7] MAVROEIDIS V, VISHI K, MATEUSZ D, et al. The impact of quantum computing on present cryptography[J]. International Journal of Advanced Computer Science and Applications, 2018, 9(3): 405-414.

[8] CHOI Y R, CHOI Y S, et al. Analysis of NIST PQC standardization process and round 4 selected/non-selected algorithms[J]. Jouranl of Information and Security, 2024, 24(2): 71-78.

[9] 燕云飞, 李斌, 魏源鑫, 等. Dilithium算法的FPGA高效扩展性优化[J]. 计算机科学, 2024, 51(S1): 838-846.
YAN Y F, LI B, WEI Y X, et al. Efficient scalability optimization of dilithium algorithm based on FPGA[J]. Computer Science, 2024, 51(S1): 838-846. (in Chinese)

[10] 吕顺森, 李斌, 翟嘉琪, 等. Crystal-Kyber算法的FPGA高效并行优化[J]. 电子学报, 2024, 52(5): 1679-1689.
LÜ S S, LI B, ZHAI J Q, et al. FPGA efficient parallel optimization of crystal-kyber[J]. Acta Electronica Sinica, 2024, 52(5): 1679-1689. (in Chinese)

[11] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2009, 56(6): 1-40.

[12] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[M]//Advances in Cryptology-EUROCRYPT 2010. Berlin: Springer Berlin Heidelberg, 2010: 1-23.

[13] DING J T, XIE X, LIN X D. A simple provably secure key exchange scheme based on the learning with errors problem[EB/OL]. (2014-07-29)[2025-01-07]. https://eprint.iacr.org/2012/688.

[14] 宋敏特, 侯凯, 茹占强, 等. 一种面向PUF的模糊提取器设计与实现[J]. 中国科学院大学学报(中英文), 2024, 41(1): 127-135.
SONG M T, HOU K, RU Z Q, et al. Design and implementation of fuzzy extractor for PUF[J]. Journal of University of Chinese Academy of Sciences, 2024, 41(1): 127-135. (in Chinese)

[15] CANETTI R, FULLER B, PANETH O, et al. Reusable fuzzy extractors for low-entropy distributions[J]. Journal of Cryptology, 2020, 34(1): 2.

[16] VAN HERREWEGE A, KATZENBEISSER S, MAES R, et al. Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-Enabled RFIDs[M]//Financial Cryptography and Data Security. Berlin: Springer Berlin Heidelberg, 2012: 374-389.

[17] PEIKERT C. Lattice cryptography for the Internet[M]// Post-Quantum Cryptography. Cham: Springer International Publishing, 2014: 197-219.

[18] 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]//2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2015: 553-570.

[19] GAO X W, DING J T, SARASWATHY R V, et al. Comparison analysis and efficient implementation of reconciliation-based RLWE key exchange protocol[J]. International Journal of High Performance Computing and Networking, 2019, 13(2): 141.

[20] 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. New York: ACM, 2016: 1006-1018.

[21] ALKIM E, DUCAS L, PÖPPELMANN T, et al. Post-quantum key exchange: A new hope[C]//Proceedings of the 25th USENIX Security Symposium (USENIX Security 16). Piscataway: IEEE, 2016: 327-343.

[22] PAQUIN C, STEBILA D, TAMVADA G. Benchmarking post-quantum cryptography in TLS[M]//Post-Quantum Cryptography. Cham: Springer International Publishing, 2020: 72-91.

[23] SAARINEN M O. HILA5: On reliability, reconciliation, and error correction for ring-LWE encryption[M]//Selected Areas in Cryptography-SAC 2017. Cham: Springer International Publishing, 2017: 192-212.

[24] YADAV S. An extensive study on lattice-based cryptography and its applications for RLWE-based problems[J]. Universal Research Reports, 2023, 10(3): 104-110.

[25] DHARMINDER D, REDDY C B, DAS A K, et al. Post-quantum lattice-based secure reconciliation enabled key agreement protocol for IoT[J]. IEEE Internet of Things Journal, 2023, 10(3): 2680-2692.

[26] JIA W J, XUE G H, WANG B C, et al. Module-LWE-based key exchange protocol using error reconciliation mechanism[J]. Security and Communication Networks, 2022, 2022(1): 8299232.

[27] MARIA NAVIN J R, SURESH P, PRADEEP K R. Implementation of OpenSSL API's for TLS 1.2 operation[J]. International Journal of Advanced Computer Research (IJACR), 2013, 3(12): 179-183.

[28] FELSCH D, GROTHE M, SCHWENK J, et al. The dangers of key reuse: Practical attacks on ipsec ike[C]//Proceedings of the 27th USENIX Security Symposium. Baltimore: USENIX Association, 2018: 567-583.

[29] KIRKWOOD D, LACKEY B C, MCVEY J, et al. Failure is not an Option: Standardization Issues for Post-Quantum Key Agreement[R]. Workshop on Cybersecurity in a Post-Quantum World. 2015: 21.

[30] DING J T, ALSAYIGH S, SARASWATHY R V, et al. Leakage of signal function with reused keys in RLWE key exchange[C]//2017 IEEE International Conference on Communications (ICC). Piscataway: IEEE, 2017: 1-6.

[31] DING J T, FLUHRER S, RV S. Complete attack on RLWE key exchange with reused keys, without signal leakage[M]//Information Security and Privacy. Cham: Springer International Publishing, 2018: 467-486.

[32] BINDEL N, STEBILA D, VEITCH S. Improved attacks against key reuse in learning with errors key exchange[M]//Progress in Cryptology - LATINCRYPT 2021. Cham: Springer International Publishing, 2021: 168-188.

[33] DING J T, BRANCO P, SCHMITT K. Key exchange and authenticated key exchange with reusable keys based on RLWE assumption[J]. IACR Cryptology ePrint Archive, 2019, 2019: 665.

[34] QIN Y, DING R Y, CHENG C, et al. Light the signal: Optimization of signal leakage attacks against LWE-Based key exchange[M]//Computer Security-ESORICS 2022. Cham: Springer International Publishing, 2022: 677-697.

[35] LI Z W, XU J, HU L. Signal leakage attack meets depth first search: An improved approach on DXL key exchange protocol[EB/OL]. (2023-11-06) [2025-01-07]. https://eprint.iacr.org/2023/1709.

[36] LIU C, ZHENG Z X, ZOU G N. Key reuse attack on newhope key exchange protocol[M]//Information Security and Cryptology - ICISC 2018. Cham: Springer International Publishing, 2019: 163-176.

[37] DABRA V, BALA A, KUMARI S. Flaw and amendment of a two-party authenticated key agreement protocol for post-quantum environments[J]. Journal of Information Security and Applications, 2021, 61: 102889.

[38] ISLAM S H. Provably secure two-party authenticated key agreement protocol for post-quantum environments[J]. Journal of Information Security and Applications, 2020, 52: 102468.

[39] PURSHARTHI K, MISHRA D. On the security of ring learning with error-based key exchange protocol against signal leakage attack[J]. Security and Privacy, 2023, 6(5): e310.

[40] DHARMINDER D. LWEDM: Learning with error based secure mobile digital rights management system[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(2): e4199.

[41] 郭渊博, 尹安琪. 基于格的口令认证密钥交换协议综述[J]. 通信学报, 2022, 43(12): 172-187.
GUO Y B, YIN A Q. Research on password-authenticated key exchange protocol over lattices[J]. Journal on Communications, 2022, 43(12): 172-187. (in Chinese)

[42] 尹安琪, 汪定, 郭渊博, 等. 可证明安全的抗量子高效口令认证密钥交换协议[J]. 计算机学报, 2022, 45(11): 2321-2336.
YIN A Q, WANG D, GUO Y B, et al. Provably secure quantum resistance efficient password-authenticated key exchange protocol[J]. Chinese Journal of Computers, 2022, 45(11): 2321-2336. (in Chinese)

[43] 尹安琪, 曲彤洲, 郭渊博, 等. 格上基于密文标准语言的可证明安全两轮口令认证密钥交换协议[J]. 电子学报, 2022, 50(5): 1140-1149.
YIN A Q, QU T Z, GUO Y B, et al. Provably secure two-round PAKE based on ciphertext standard language over lattices[J]. Acta Electronica Sinica, 2022, 50(5): 1140-1149. (in Chinese)

[44] 尹安琪, 郭渊博, 汪定, 等. 可证明安全的抗量子两服务器口令认证密钥交换协议[J]. 通信学报, 2022, 43(3): 14-29.
YIN A Q, GUO Y B, WANG D, et al. Provably secure

quantum resistance two-server pass-word-authenticated key exchange protocol[J]. Journal on Communications, 2022, 43(3): 14-29. (in Chinese)

[45] 李子臣, 谢婷, 张卷美 . 基于RLWE问题的后量子口令认证密钥交换协议[J]. 电子学报, 2021, 49(2): 260-267.
LI Z C, XIE T, ZHANG J M. Post quantum password-based authentication key exchange protocol based on ring learning with errors problem[J]. Acta Electronica Sinica, 2021, 49(2): 260-267. (in Chinese)

[46] DING R Y, CHENG C, QIN Y. Further analysis and improvements of a lattice-based anonymous PAKE scheme[J]. IEEE Systems Journal, 2022, 16(3): 5035-5043.

[47] DABRA V, BALA A, KUMARI S. LBA-PAKE: Lattice-based anonymous password authenticated key exchange for mobile devices[J]. IEEE Systems Journal, 2021, 15(4): 5067-5077.

[48] WANG Q X, WANG D, CHENG C, et al. Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(1): 193-208.

[49] FLUHRER S R. Cryptanalysis of ring-LWE based key exchange with key share reuse[J]. IACR Cryptology EPrint Archive, 2016, 2016: 85.

[50] WANG K, JIANG H D. Analysis of two countermeasures against the signal leakage attack[M]//Progress in Cryptology-AFRICACRYPT 2019. Cham: Springer International Publishing, 2019: 370-388.

[51] MOODY D, ALAGIC G, ALPERIN-SHERIFF J M, et al. Status report on the first round of the nist post-quantum cryptography standardization process[R]. Technical report, National Institute of Standards and Technology, 2019.

[52] GAO X W, DING J T, LI L, et al. Practical randomized RLWE-based key exchange against signal leakage attack[J]. IEEE Transactions on Computers, 2018, 67(11): 1584-1593.

[53] 张晓涵, 程池, 余天润 . 对密钥不匹配攻击的进一步理论分析: 以NTRU-HRSS为例[J]. 电子学报, 2023, 51(4): 1081-1092.
ZHANG X H, CHENG C, YU T R. Further theoretical analysis of key mismatch attacks: A case study of NTRU-HRSS[J]. Acta Electronica Sinica, 2023, 51(4): 1081-1092. (in Chinese)

[54] TANAKA Y, UENO R, XAGAWA K, et al. Multiple-valued plaintext-checking side-channel attacks on post-quantum KEMs[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023: 473-503.

[55] QIN Y, CHENG C, ZHANG X H, et al. A systematic approach and analysis of key mismatch attacks on lattice-based NIST candidate KEMs[M]//Advances in Cryptology-ASIACRYPT 2021. Cham: Springer International Publishing, 2021: 92-121.

[56] MI R Q, JIANG H D, ZHANG Z F. Bit security analysis of lattice-based KEMs under plaintext-checking attacks[M]//Selected Areas in Cryptography-SAC 2023. Cham: Springer Nature Switzerland, 2024: 255-274.

[57] GUO Q, MÅRTENSSON E. Do not bound to a single position: Near-optimal multi-positional mismatch attacks against kyber and saber[M]//Post-Quantum Cryptography. Cham: Springer Nature Switzerland, 2023: 291-320.

[58] SHAO M Y, LIU Y J, ZHOU Y B. Pairwise and parallel: Enhancing the key mismatch attacks on kyber and beyond[C]//Proceedings of the 19th ACM Asia Conference on Computer and Communications Security. New York: ACM, 2024: 548-559.

[59] GUO Q, MÅRTENSSON E, et al. The perils of limited key reuse: Adaptive and parallel mismatch attacks with post-processing against kyber[J]. IACR Communications in Cryptology, 2024, 1: 3-72.

[60] YADAV S, DABRA V, MALIK P, et al. Flaw and amendment of Dharminder et al.'s authentication protocol for satellite communication[J]. Security and Privacy, 2024, 7(4): e383.

[61] DHARMINDER D, DADSENA P K, GUPTA P, et al. A post quantum secure construction of an authentication protocol for satellite communication[J]. International Journal of Satellite Communications and Networking, 2023, 41(1): 14-28.

[62] MISHRA D, PURSHARTHI K. Cryptanalysis with improvement on lattice-based authenticated key exchange protocol for mobile satellite communication networks[J]. Security and Privacy, 2024, 7(5): e407.

[63] AZARDERAKHSH R, JAO D, LEONARDI C. Post-quantum static-static key agreement using multiple protocol instances[M]//Selected Areas in Cryptography- SAC 2017. Cham: Springer International Publishing, 2017: 45-63.

[64] ISLAM S H, BASU S. PB-3PAKA: Password-based three-party authenticated key agreement protocol for mobile devices in post-quantum environments[J]. Journal of Information Security and Applications, 2021, 63: 103026.

[65] BASU S, SEYHAN K, ISLAM S H, et al. MLWR-2PAKA: A hybrid module learning with rounding-based authenticated key agreement protocol for two-party communication[J]. IEEE Systems Journal, 2023, 17(4): 6093-6103.

[66] AKLEYLEK S, SEYHAN K. A probably secure Bi-GI-

SIS based modified AKE scheme with reusable keys[J]. IEEE Access, 2020, 8: 26210-26222.

[67] SEYHAN K, NGUYEN T N, AKLEYLEK S, et al. Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security[J]. Journal of Information Security and Applications, 2021, 58: 102788.

[68] PURSHARTHI K, MISHRA D. A computationally efficient and randomized RLWE-based key exchange scheme[J]. Cluster Computing, 2024, 27(2): 1599-1610.

[69] BRENDEL J, FISCHLIN M, GÜNTHER F, et al. Towards post-quantum security for signal's X3DH handshake[M]//Selected Areas in Cryptography. Cham: Springer International Publishing, 2021: 404-430.

[70] DOBSON S, GALBRAITH S D. Post-quantum signal key agreement from SIDH[M]//Post-Quantum Cryptography. Cham: Springer International Publishing, 2022: 422-450.

[71] 刘一丹, 程庆丰. 同源密码方案综述[J]. 密码学报, 2023, 10(4): 667-684.
LIU Y D, CHENG Q F. A survey of isogeny-based cryptographic schemes[J]. Journal of Cryptologic Research, 2023, 10(4): 667-684. (in Chinese)

[72] CAMPOS F, CHÁVEZ-SAAB J, CHI-DOMÍNGUEZ J J, et al. Optimizations and practicality of high-security CSIDH[J]. IACR Communications in Cryptology, 2024, 1: 1-21.

[73] LYUBASHEVSKY V. Converting newhope/lwe key exchange to a diffe-hellman-like algorithm[J]. Crypto Stack Exchange, 2017, 1: 2.

[74] DE KOCK B. A Non-Interactive Key Exchange Based on Ring-Learning with Errors[D]. Eindhoven: Eindhoven University of Technology, 2018.

[75] GUO S Y, KAMATH P, ROSEN A, et al. Limits on the efficiency of (ring) LWE-based non-interactive key exchange[J]. Journal of Cryptology, 2021, 35(1): 1.

[76] HESSE J, HOFHEINZ D, KOHL L, et al. Towards tight adaptive security of non-interactive key exchange[M]// Theory of Cryptography. Cham: Springer International Publishing, 2021: 286-316.

[77] GAJLAND P, DE KOCK B, QUARESMA M, et al. SWOOSH: Efficient lattice-based non-interactive key exchange[C]//Proceedings of the 33rd USENIX Security Symposium (USENIX Security 24). Philadelphia: USENIX, 2024: 487-504.

[78] LANGREHR R. On the multi-user security of LWE-based NIKE[M]//Theory of Cryptography. Cham: Springer Nature Switzerland, 2023: 33-62.

作者简介

王　克　男,1992年出生于河南省南阳市. 现为北京电子科技学院密码科学与技术系讲师. 主要研究方向为基于格的公钥密码算法分析.
E-mail: wangke_unique@163.com

江浩东　男,1990年出生于河南省南阳市. 现为战略支援部队信息工程大学副教授. 主要研究方向为抗量子密码研究.
E-mail: hdjiang13@gmail.com

韩　将　男,1986年出生于山东省青岛市. 现为中国科学院软件研究所可信计算与信息保障实验室博士研究生. 主要研究方向为抗量子密码研究.
E-mail: kenglong@126.com

陈　隆　男,1988年出生于安徽省黄山市. 现为中国科学院软件研究所可信计算与信息保障实验室副研究员. 主要研究方向为抗量子密码研究.
E-mail: chenlong@iscas.ac.cn

谢惠琴　女,1992年出生于福建省宁德市. 现为北京电子科技学院密码科学与技术系副教授. 主要研究方向为量子密码与量子算法.
E-mail: xiehuiqindky@163.com

张振峰　男,1972年出生于河南省南阳市. 现为中国科学院软件研究所可信计算与信息保障实验室研究员. 主要研究方向为密码学与数据安全.
E-mail: zhenfeng@iscas.ac.cn