lattice-based two-party AKA with reusable keys for the IoT

摘要:两方认证密钥交换允许安全通信的两方生成共享的会话密钥并提供身份认证，广泛应用于物联网场景中。随着量子计算机的快速发展，经典密码算法容易受到威胁，从而给物联网通信带来显著风险。近年来许多基于格的两方认证密钥交换方案被提出，以抵御量子攻击，然而绝大部分协议在密钥被重复使用时容易受到信号泄露攻击，并且效率不高。为了解决这些问题，本文提出了一种物联网场景下密钥可重用的高效格下两方认证密钥交换协议。

关键词：格密码，认证密钥交换，可重用密钥

1 引言

随着物联网（IoT）的快速发展，预计到 2025 年将有 750 亿个物联网设备投入使用。这种快速增长需要标准化协议和适当的架构来支持物联网设备的安全通信。物联网设备通常资源受限，计算能力和内存有限，因此需要高效的加密算法来确保其安全性。传统的加密算法，如基于大素数分解和离散对数问题的公钥加密系统，虽然在当前环境下安全，但随着量子计算机的发展，这些算法将面临严重威胁。1999 年，Shor 提出了能够在多项式时间内破解 RSA 的量子算法，而 RSA 的安全性依赖于大数分解的困难性。同样，Grover 的量子算法也能在多项式时间内搜索非结构化数据库。尽管对称密码学对量子计算机的抵抗能力较强，但量子计算机的出现将极大地影响非对称或公钥密码学的安全性。

密钥交换（Key Exchange, KE）是一种加密原语，允许通信双方在不泄露密钥信息的情况下生成共享密钥。Diffie 和 Hellman 在 1976 年提出了首个密钥交换协议，标志着现代密码学的诞生。然而，标准的 KE 协议容易受到中间人攻击，攻击者可以篡改通信内容，使双方误以为他们在安全通信。为了解决这一问题，认证密钥交换（Authenticated Key Exchange, AKE）应运而生，它通过身份验证机制防止中间人攻击，广泛应用于 SSL 和 TLS 等协议中。AKE 的认证可以是显式的（如使用签名方案）或隐式的（无需额外原语）。

传统的 AKE 协议基于 Diffie-Hellman 协议，其安全性依赖于离散对数假设。然而，随着量子计算机的出现，这些协议将变得不安全。因此，后量子密码学成为研究热点。第一个基于错误环学习（RLWE）的后量子密钥交换协议由 Ding 等人提出，该协议通过引入噪声和误差协调机制实现了密钥交换，但其在密钥重用时会面临信号泄露攻击，导致密钥信息泄露。因此，设计一种适用于物联网场景的高效、密钥可重用的格基两方认证密钥交换协议变得非常重要。

1.1 相关工作

认证密钥交换 (AKE) 允许双方相互认证并建立一个秘密的会话密钥，以建立一个安全的通道，这在文献中得到了很好的研究。随着量子计算机时代的到来，设计后量子安全的 AKE 方案成为一项紧迫的任务。

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。

构建类似原始 Diffie－Hellman 协议[3]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[21]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[21]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[22]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 [23]将 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[24]将类 Peikert 式

的格上被动安全的协议[22]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。Alkim 等[28]深入分析了 Bos 等[24]的协议方案及其实施，提出被称为 NewHope 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[29]。通过借鉴 Ding 等的基于 LWE 问题的协议设计思想[21]，Bos 等[30]又在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[22]，可被视为 BCNS 协议[24]的无环优化版本，而基本 LWE 难题较难题更为稳健，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[28]相比，该方案所需的计算时间和通信量要多得多。

物联网的兴起，设备数量日益增加，安全问题越来越重要，基于因式分解或离散对数等经典问题的密码学方案，Shor 算法可以解决上述两个问题。
量子攻击的威胁，基于格的密码学，信号泄露攻击，可重用密钥在物联网安全通信的重要性，主要目的是为了让通信双方的公私密钥对可以多次使用且不会泄露一点有关密钥的信息

众所周知，基于 rlwe 的 KE 协议对于密钥重用并不健壮，因为信号函数会泄漏有关密钥的信息。我们修改了以前基于 RLWE 的 KE 方案的设计，以允许在 ROM 中重复使用密钥。我们的构建使用了一种称为巴氏灭菌的新技术，该技术强制另一方发送的所谓 RLWE 样本确实与统一样本无法区分，因此确保在整个 KE 过程中没有信息泄漏。在此基础上，我们构建了一个新的 AKE 方案。该方案提供了隐式认证(即，它不需要使用任何其他认证机制，如签名方案)，并且在 Bellare-Rogaway 模型中被证明是安全的，并且在 ROM 中具有弱的完全前向保密。它在几个方面改进了先前基于格的 AKE 方案的设计。我们的构建只需要从一个离散高斯分布中采样，并且避免了拒绝采样和噪声泛洪技术，这与之前的建议不同(Zhang 等人，EUROCRYPT 2015)。因此，在计算和通信复杂性方面，该方案比以前的结构要高效得多。由于假设 RLWE 问题的硬度，我们的结构是可证明的安全的，因此它们被认为对量子对手具有鲁棒性，因此适合后量子应用。

1.2 协议的想法

令(epkj;eskj)作为 Pi 方静态和临时公钥和秘钥对。Pj 类似。象征性地，Pi 方计算的密钥 ki 可以被视为(sski;epkj) (Pi 的静态秘钥与 Pj 的临时公钥)，(eski;spkj) (Pi 的临时秘钥与 Pj 的静态公钥)，(eski;epkj) (Pi 的临时秘钥与 Pj 的临时公钥)。类似地，Pj 计算(sskj;Epki)、(eskj;spki)和(eskj;epki)。更精确地说，设 spki = pi = asi + 2ei 和 epk = xi = ari + 2fi (resp.)。spkj = pj = asj + 2ej 和 epk = yj = arj + 2fj)分别为 Pi 的静态公钥和临时公钥。Pj)。由 Pi 计算的密钥 ki 等于 (pj + $\bar{}$yj)(si+ ri + c) - pj si，这是双方静态密钥和临时密钥之间所有可能组合的总和，减去静态密钥之间交换的密钥结果。与之前的构建一样，我们对 yj 进行了巴氏灭菌，以避免任何信息泄漏。同样，由 Pj 计算的键 kj 等于(pi + $\bar{}$xi)(sj + rj + d)−pisj。当然，ki 和 kj 只是近似相等，因此使用函数 Sig 和 Mod2 来商定共享值。

1.3 贡献与技术

在这项工作中，我们提出了允许密钥重用的 AKE 的后量子解决方案。我们的方案的安全性基于 RLWE 假设[46]，密码学中一个公认的假设，从最坏情况格问题中得到平均情况的减少。基于此假设的方案通常提供后量子安全性，并且比基于离散对数的方案渐近地更有效。

1.3.1 使用可重用密钥进行密钥交换

首先，我们注意到如果 Pi 的消息是 RLWE 样本，那么由 Pj 计算的值 kj 与一致选择的值是不可区分的，因此，kj 的信号也与一致选择的值不可区分。因此，我们只需要强迫每一方在协议中诚实地行事。因此我们使用一种技术，称之为巴氏灭菌法，来迫使参与 KE 计划的各方诚实行事。该技术先前在[26]中在零知识证明的背景下被引入。该技术的思想如下:在从 Pi 接收 xi 后，Pj 方对 xi 进行巴氏消毒，即进行计算：

xi = xi + aH(xi) + 2fj

其中 H 是一个随机预言器，其输出从 x α 中采样，fj 从 x α 中采样。如果 xi 确实是 RLWE 样本，那么巴氏灭菌¯xi 也是 RLWE 样本，Pi 知道其中的秘密。然而，当 xi 不是 RLWE 样本时，对于 Pi 来说，¯xi 看起来是伪随机的。因此，kj 的信号也是伪随机的，Pi 无法从中提取 Pj 的秘钥信息。我们的结论是，方 Pi 不遵守协议没有任何好处。

为了保证 Pi 方也可以在多次执行协议时重用其密钥，我们对 Pj 发送的 yj 进行了巴氏消毒。协议的方案如图 1 所示。

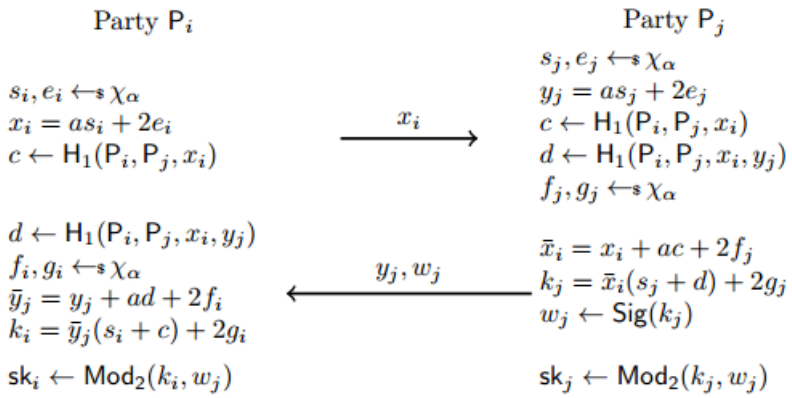


图 1 具有可重用键的 Ding’s Ke: x α 为 Rq 上的离散高斯分布，标准差为 α， H1:是一个哈希函数，其输出从 x α 中采样，Sig 和 Mod2 分别是信号和提取函数，如[28]所定义。

在 Diffie-Hellman KE[22]中，假设双方交换的消息都在 G 组中，我们通过让双方验证是否所有交换的值都在 G 组中来避免可能的攻击，这可以在多项式时间内完成。然而，在基于 RLWE 的 KE 中，由于交换消息是 RLWE 样本，因此不可能直接检查它们是否经过诚实计算。巴氏灭菌技术可以被看作是检查交换的信息是否在 G 中的类比，在 Diffie-Hellman KE 中，因为该技术也强制相关各方的良好行为。

1.3.2 新的认证密钥交换方案

我们的主要贡献是基于 RLWE 假设设计了一个新的 AKE 方案。我们构建的核心是上面描述的基于 rlwe 的 KE。该方案如图 2 所示。

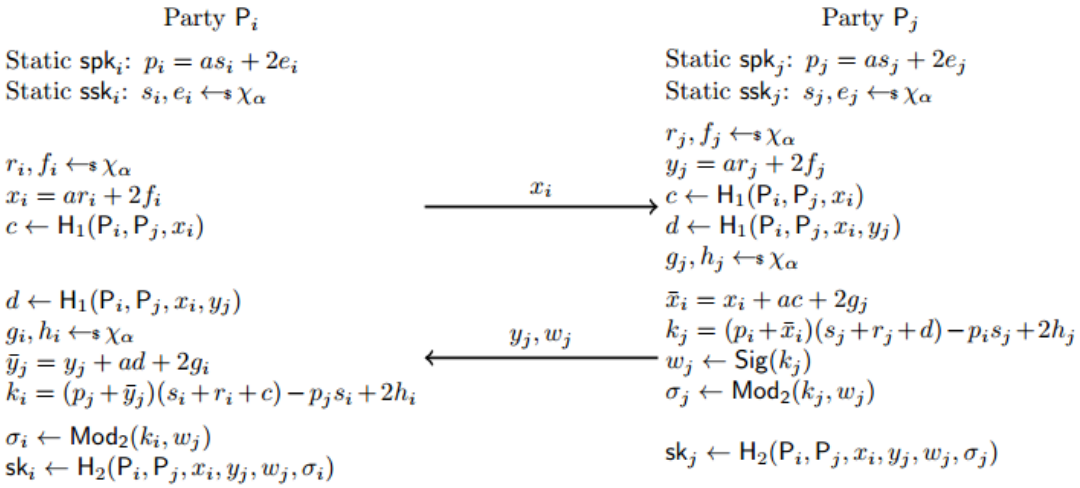


图 2:新的 AKE 方案:是 Rq 上的离散高斯分布，标准差为 α， H1:是一个哈希函数，其输出从 x α 中采样; H2 为 κ 位密钥派生函数，Sig 和 Mod2 分别为信号和提取函数，定义见[28]。

1.4 组织结构

第 2 节包括理解我们研究中使用的数学思想的基本定义。第 3 节包含新的密钥交换机制。第 4 节详细提供了我们协议的正式安全证明，第 5 节将性能与相关的现有密钥交换协议进行了比较。第 6 节讨论了论点和发现。最后，第 7 节对本文进行了总结。

2 基本原理

在本节中，我们将介绍基于格的密码学以及认证密钥交换协议的基本技术原理。

2.1 基于格的密码学

格是 n 维平面上点的集合，在数学上的描述如下：

设 $\mathbb{R}^k$ 为 k 维欧几里得空间。$\mathbb{R}^k$中的一个格就是下面这个集合：

$$L(a_1, a_2, \dots, a_m) = \sum_{i=1}^{m} x_i a_i : x_i \in \mathbb{Z} \qquad (1)$$

即在 $\mathbb{R}^k$ (k≥m) 中 m 个线性无关向量 a_1,a_2,…,a_m 的线性组合，m 和 k 分别代表格的秩和维数。如果 m=k，则称该格为满秩格。向量 a_1,a_2,…,a_m 的序列称为格基，可以用矩阵形式表示为 $B = [a_1, a_2, \dots, a_m] \in \mathbb{R}^{k \times m}$，其中基向量即为矩阵的每一列，使用该矩阵符号，(1) 式可以表示为：

$$L(B) = Bx : x \in \mathbb{Z}^m \qquad (2)$$

其中 Bx 是通常的矩阵向量乘法。

格上的困难问题，如 SVP (Short Vector Problem)、CVP(Closest Vector Problem)、LWE(Learning with errors Problem)、RLWE(Ring learning with errors Problem)等等对设计密码原语很有用，而 LWE 和 RLWE 是广泛用于设计密码原语比如密钥交换的困难问题，因为已经得到了很好的研究[16,17]，它们的定义如下：

LWE 问题：固定 n≥1，模数 q≥2 和 $\mathbb{Z}_q$ 上的错误概率分布 ψ。$\mathbb{Z}_q^n \times \mathbb{Z}_q$ 上 $A_{s,\psi}$ 为随机选择向量 $a \in \mathbb{Z}_q^n$，秘钥为 $s \in \mathbb{Z}_q^n$，根据 ψ 选择误差 $e \in \mathbb{Z}_q$ 得到的概率分布。然后，输出为 $(a, \langle a, s \rangle + e)$，其中加法在 $\mathbb{Z}_q$ 即模 q 中进行。如果存在一种算法利用模 q 和误差分布 ψ 来解决 LWE 问题，即对于任意 $s \in \mathbb{Z}_q^n$，给定任意数量的来自 $A_{s,\psi}$ 的相互独立的样本，它将在多项式时间内以高概率输出密钥 s。

RLWE 分布：对于安全参数 λ，设 $f(x) = x^n + 1$，其中 n = n(λ)是 2 的幂。设 q≥2 为素数，$R = \mathbb{Z}[x]/\langle f(x) \rangle$，$R_q = R/qR$，ψ 为 R_q 上具有较小标准差的离散高斯分布。通

过取样本 $(a_i, b_i) \in R_q \times R_q$ 可以产生一个分布 $A_{s,\psi}$，其中 a_i 均匀地从 R_q 中抽样，$b_i = a_i s + e$，其中 s 均匀地从 R_q 中抽取，误差 e 从 ψ 中抽样即 e←Sample(ψ)。

RLWE 假设：该假设表明，对于从分布 ψ 中抽取的固定样本，即$s \leftarrow Sample(\psi)$，给定多项式个数的样本，分布 $A_{s,\psi}$ 与 $R_q \times R_q$ 上的均匀分布在计算上不可区分。

2.2 调和机制

调和机制的思想是构建 Diffie – Hellman 式的密钥交换协议，双方在不需要加解密的情况下自然生成相同的共享密钥。与基于加密的密钥交换协议相比，这些类型的密钥交换协议提供了更好的带宽需求。

为了更好理解调和机制，我们可以考虑以下基于 RLWE 的密钥交换协议，其中双方尝试建立公共会话密钥。设 a 为已知元素，$a \in R_q$，且 χ_β 为 R_q 上的离散高斯分布，标准差为 β 。考虑如下的密钥交换协议操作：

首先，Alice 将其秘密和误差项采样为 $s_a, e_a \leftarrow \chi_\beta$，并将其公钥 p_a 发送给 Bob，其中 $p_a = a.s_a + e_a$。

然后，Bob 将其秘密和误差项采样为$s_b, e_b \leftarrow \chi_\beta$，并计算 σ_b 为 $\sigma_b = p_a.s_b = (a.s_a + e_a).s_b = a.s_a.s_b + e_a.s_b$。最后，Bob 计算 p_b 为 $p_b = a.s_b + e_b$并将其发送给 Alice。

Alice 接收到 p_b 后，计算 σ_a 为 $\sigma_a = p_b.s_a = (a.s_b + e_b).s_a = a.s_a.s_b + e_b.s_a$。

从以上步骤可以看出，σ_a 与 σ_b 非常接近，但它们并不相等。所以，要使σ_a 等于 σ_b 还需要额外的条件，这便是调和机制需要发挥作用的地方。因此，调和机制的主要功能是消除 σ_a 和 σ_b 值之间的微小差异，使密钥交换的双方拥有相同的共享密钥或会话密钥。在上面的场景中，Bob 需要发送关于 σ_b 的额外信息，以便 Alice 可以得到相同的 σ_a 值。这个附加信息是提示值，它是下面描述的提示函数的输出。

调和机制一般由两个函数组成：

信号函数 S()：该函数以 x 作为输入，其中 $x \in R_q$，输出信号值为 w = S(x)，其中 $w \in \{0,1\}^*$。

调和函数 Rec()：调和函数以 σ_a 和 σ_b 以及信号值 w 作为输入，输出调和值 $Rec(\sigma_a, w) = Rec(\sigma_b, w)$。

当然，调和机制的正常运行还需要满足两个条件。即：

正确性——如果 σ_a 和 σ_b 的计算值之差小于某个阈值，则 σ_a 等于 σ_b。数学上可以表示为 $||\sigma_a - \sigma_b|| <$ 阈值，则 $\sigma_a = \sigma_b$。这个阈值取决于所采用的调和机制。

安全性——对于任何元素 σ，$\sigma \leftarrow R_q$，调和函数 $Rec(\sigma, w)$ 均匀分布在$\{0,1\}^*$上(其中 w 是信号函数 w = S(σ)的输出)。

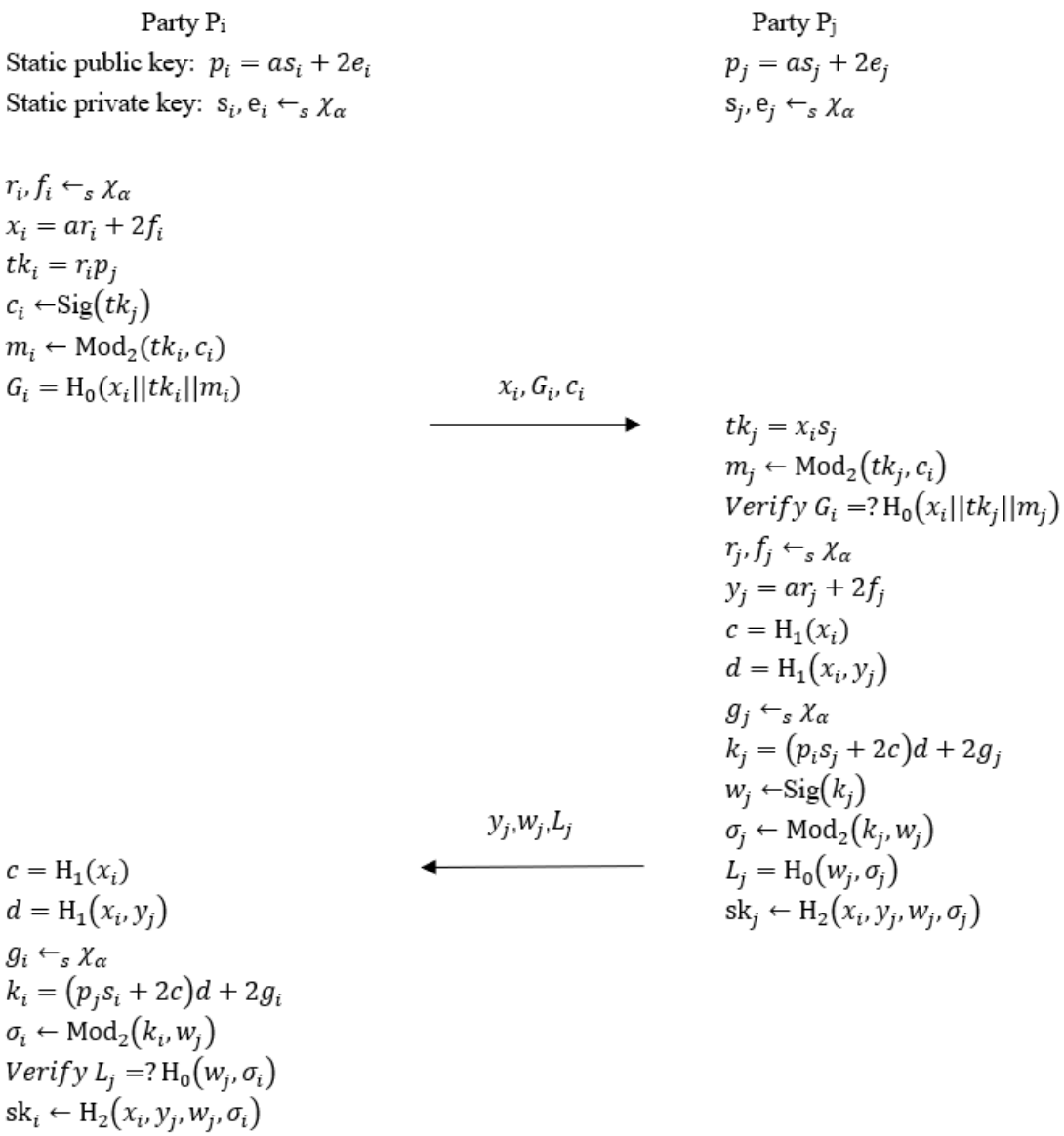
3 方案介绍

3.1 ROR 安全模型

我们描述了适用于两步 AKE 方案的 ROR 模型[11]，该模型也在[56]中使用。在这个模型中，攻击者完全控制了网络，这意味着它可以读取、修改、拦截和注入网络中的消息。它还允许显示已经建立的会话密钥，对现实世界中使用协议时可能出现的信息泄漏进行建模，以及显示用户的静态秘密密钥，以便捕获 PFS。我们简要介绍一下安全模型。

在这项工作中，AKE 方案Π的执行由两方执行，发起者 I 和响应者 r。设 N 为使用 AKE 协议的用户数量。每个用户都有一对静态公钥和密钥。与往常一样，我们假设用户的静态公钥由证书颁发机构(CA)或使用其他机制进行验证。

弱完美前向保密(wPFS)意味着攻击者无法恢复未经其干预而建立的会话密钥[41]。即使攻击者知道密钥交换中涉及的双方的静态秘密密钥，这也应该成立。限制对手在一个新会话上查询 Test oracle 是 wPFS 的概念。回想一下，wPFS 是两通道 KE 协议可以实现的最强类型的 PFS。



3.2 方案介绍

A. 准备阶段

服务器执行以下步骤来完成系统初始化。

1) 服务器选择安全参数 n，使其为 2 的幂，n 的值需要根据协议所适用的应用的灵敏度来合理选择。

2) 服务器选择一个奇素数 q，使得 $q \mod 2n = 1$，一个 R_q 上的离散高斯分布 χ_α，其标准差为 α，一个随机元素 $a \leftarrow_s R_q$。

3) 服务器选择两个单向哈希函数。其中 $\mathrm{H}_1: \{0,1\}^* \rightarrow \chi_\alpha$ 是一个输出从 χ_α 中采样的哈希函数，$\mathrm{H}_2: \{0,1\}^* \rightarrow \{0,1\}^\kappa$ 是一个密钥导出函数，上述两个函数都被建模为随机预言机。

4) 最后，服务器公开发布系统参数$\{n, q, \chi_\alpha, a, \mathrm{H}_1(), \mathrm{H}_2()\}$。

B. 密钥生成阶段

P_i 方生成其静态公钥为 $p_i = as_i + 2e_i$，其中 $s_i, e_i \leftarrow_s \chi_\alpha$，静态私钥为 s_i。类似地，对于 P_j 方来说，其静态公钥为 $p_j = as_j + 2e_j$，静态私钥为 s_j。

C. 密钥交换阶段

1) P_i 进行如下操作：

P_i 从 χ_α 中采样得到 r_i, f_i，即 $r_i, f_i \leftarrow_s \chi_\alpha$，并计算自身临时公钥 $x_i = ar_i + 2f_i \bmod q$，然后将计算得到的 x_i 发送给 P_j。

2) P_j 收到 x_i 后，进行如下操作：

P_j 从 χ_α 中采样得到 r_j, f_j，即 $r_j, f_j \leftarrow_s \chi_\alpha$，并计算自身临时公钥 $y_j = ar_j + 2f_j \bmod q$，然后计算得到 $c = \mathrm{H}_1(x_i)$ 以及 $d = \mathrm{H}_1(x_i, y_j)$。

P_j 从 χ_α 中采样得到 $g_j \leftarrow_s \chi_\alpha$ 并计算 $k_j = (p_i s_j + 2c)d + 2g_j$。

P_j 计算 $w_j \leftarrow \mathrm{Sig}(k_j)$ 以及 $\sigma_j \leftarrow \mathrm{Mod}_2(k_j, w_j)$，最后得到共享密钥 $\mathrm{sk}_j \leftarrow \mathrm{H}_2(x_i, y_j, w_j, \sigma_j)$

P_j 将 (y_j, w_j) 发送给 P_i

3) P_i 收到 (y_j, w_j) 后，进行如下操作：

P_i 计算得到 $c = \mathrm{H}_1(x_i)$ 以及 $d = \mathrm{H}_1(x_i, y_j)$

P_i 从 χ_α 中采样得到 $g_i \leftarrow_s \chi_\alpha$ 并计算 $k_i = (p_j s_i + 2c)d + 2g_i$。

P_j 计算 $\sigma_i \leftarrow \mathrm{Mod}_2(k_i, w_j)$，最后得到共享密钥 $\mathrm{sk}_i \leftarrow \mathrm{H}_2(x_i, y_j, w_j, \sigma_i)$

由于 P_i 和 P_j 的静态公私钥对会保持不变，而它们的临时公私钥对在每次密钥交换阶段都会改变，如果 P_i 和 P_j 两方在密钥交换阶段有一方冒充了别的身份参与，后续双方通信阶段会出现问题，因此这也间接完成了双向认证。

下面的引理证明了方案的正确性，即双方 P_i 和 P_j 在执行协议后最终拥有相同的共享密钥。

正确性：为了证明该方案的正确性，只需证明 $\sigma_i = \sigma_j$。特别地，由于我们是通过 k_i、k_j 和 w_j 计算得到 σ_i 和 σ_j，而

$$k_i = (p_j s_i + 2c)d + 2g_i = as_i s_j d + 2e_j s_i d + 2cd + 2g_i$$
$$k_j = (p_i s_j + 2c)d + 2g_j = as_i s_j d + 2e_i s_j d + 2cd + 2g_j$$

因此，我们可以计算得到 $k_i - k_j = 2(e_j s_i d + g_i - e_i s_j d - g_j)$。从前面两个定理可以得到：

$$\|k_i - k_j\| < 2\left(2\alpha^3 n^{\frac{5}{2}} + 2\alpha\sqrt{n}\right)$$

由第三个定理，可以最终得到：

$$\left(2\alpha^3 n^{\frac{5}{2}} + 2\alpha\sqrt{n}\right) < \frac{q}{8}.$$

综上所述，我们得到了 $\sigma_i = \sigma_j$ 的正确性条件，只需 q 满足上式即可保证会话密钥 sk_i 和 sk_j 是相同的。

3.3 安全性分析

在本节中，我们通过使用流行的 ROR 模型[]来展示本协议的形式安全性。在我们的安全模型中，*Execute*、*Send* 和 *Test* 预言机查询和其他安全定义是根据 ROR 模型直接设置的。在本文中，我们额外定义了一个预言器查询来扩展攻击者的能力。

CorruptP (P^i)：模拟物联网设备 P^i 被对手操纵。该查询将存储在 P^i 中的信息泄露给对手 A。

通过遵循 ROR 模型，攻击者 A 能够多次进行 *Execute*、*Send* 和 *Test* 预言机查询，然后 A 需要猜测隐藏在 *Test* 预言机中的随机位 *b* 的值。位 *b* 是均匀随机的，它决定了 *Test* 查

询的输出是一个真实的会话密钥还是一个随机数。当 A 猜对随机位 b 时，就认为 A 赢了。S 是 A 获胜的情况。

定义 1（语义安全）：对手 A 在打破所提出的两方认证密钥交换协议的语义安全方面的优势可以定义如下：

$$\mathrm{Adv}_A = |2\Pr[S] - 1|$$

如果 Adv_A 的优势可以忽略不计，则我们提出的两方认证密钥交换可以被认为是安全的。

*理论 1：*假设在认证密钥交换会话期间，A 的优势在于利用概率多项式时间(PPT)方法寻找 sk_i 或者 sk_j。那么，在我们提出的协议中 A 在突破语义安全获取 P_i 和 P_j 之间会话密钥方面的优势可以写成：

$$\mathrm{Adv}_A \leq \frac{q_{H_2}^2}{|\mathcal{H}|} + \frac{(q_e+q_s)^2+2q_s}{|\mathcal{G}|} + 2\mathrm{Adv}_{\mathcal{A}}^{\mathrm{RLWE}}. \quad (8)$$

其中，q_{H_2}、q_e 和 q_s 分别为 H_2 查询、*Execute* 查询和 *Send* 查询的个数。$|\mathcal{H}|$ 和 $|\mathcal{G}|$ 分别表示 H_2 和分布 χ_α 的空间。符号 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{RLWE}}$表示 A 解决 RLWE 问题的优势。

*证明：*该证明与[]中的证明类似，由一系列游戏组成，表示为 Game_i，其中 i = 0,1,2,3,4。对于每个游戏 Game_i，我们将 $\mathrm{S_i}$ 表示为 A 正确猜测 *Test* 查询中涉及的隐藏位 b 的事件。

1) Game_0：该游戏模拟了在 ROR 模型下针对提出的两方认证密钥交换协议的真实攻击。在 Game_0 开始时，A 猜测的位 b 是随机选择的。所以，很明显：

$$\mathrm{Adv}_A = |2\Pr[\mathrm{S_0}] - 1| \quad (9)$$

2) Game_1：该游戏模拟对 P_i 和 P_j 之间的通道进行窃听攻击。对手 A 通过 *Execute* 查询获取协议中传输的消息，并使用这些信息执行 *Test* 查询，以确定 *Test* 查询的输出是一个真实的会话密钥还是一个随机数。根据所提出的协议，A 通过窃听只能得到参数$\{w_j\}$，但 A 不知道$\{s_j, g_i\}$，也不能生成$\{k_j, \sigma_j\}$来得到会话密钥 sk_j。因此，窃听攻击不会增加 A 在 Game_1 中的获胜概率。因此我们可以得到：

$$\Pr[\mathrm{S_0}] = \Pr[\mathrm{S_1}] \quad (10)$$

3) Game_2：该游戏模拟了主动攻击，这与 *Execute*、*Send* 和 hash 查询相关。对手 A 试图将修改后的信息发送给参与者，而参与者无法从$\{x_i, y_j\}$的碰撞中发现这些信息，碰撞概率由生日悖论得出。由于$\{x_i, y_j\}$的计算涉及秘密值$\{r_i, r_j\}$，误差项$\{f_i, f_j\}$，它们是从离散高斯分布 χ_α 中抽样得到。因此，我们可以得到：

$$|\Pr[\mathrm{S_1}] - \Pr[\mathrm{S_2}]| \leq \frac{q_{H_2}^2}{2|\mathcal{H}|} + \frac{(q_e+q_s)^2}{2|\mathcal{G}|}. \quad (11)$$

4) Game_3：该游戏模拟了信号泄露攻击，其中对手 A 使用 *Send* 查询来获取信号以恢复静态私钥 s_j。由于 $k_j = p_i s_j d + 2cd + 2g_j$ 并且 d 在每次查询中都是新鲜的，因此攻击者试图预测 d 来选择合适的 x_i 从而从信号 w_j 中泄露有关 s_j 的信息，这是很难实现的，由于$d \in \chi_\alpha$，我们可以得到：

$$|\Pr[S_2] - \Pr[S_3]| \leq \frac{q_s}{|\mathcal{G}|}. \quad (12)$$

5) Game$_4$：该游戏构造了 *CorruptP* (P^i) 预言机。在这种情况下，对手 A 获得重用的静态密钥 s_j。现在，A 试图得到上一个会话生成的共享会话密钥来破坏完美的前向安全性。为了生成上一个会话产生的共享密钥 sk_j，A 仍然需要 g_j 来计算 σ_j，其难度与解决 RLWE 问题相同。因此，我们可以得到：

$$|\Pr[S_3] - \Pr[S_4]| \leq \mathrm{Adv}_{\mathcal{A}}^{\mathrm{RLWE}} \quad (13)$$

由于所有游戏都将被执行，因此对手 A 需要使用 *Test* 查询猜测 *b* 以赢得游戏，显然有 $\Pr[S_4] = 1/2$。

利用(9)，我们可以得到：

$$\frac{1}{2}\mathrm{Adv}_A = \left|\Pr[S_0] - \frac{1}{2}\right|. \quad (14)$$

利用(11)-(13)的三角不等式，可得：

$$|\Pr[S_1] - \Pr[S_4]| \leq \frac{q_{H_2}^2}{2|\mathcal{H}|} + \frac{(q_e+q_s)^2+2q_s}{2|\mathcal{G}|} + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{RLWE}} \quad (15)$$

更进一步，由(10)可得：

$$\left|\Pr[S_0] - \frac{1}{2}\right| \leq \frac{q_{H_2}^2}{2|\mathcal{H}|} + \frac{(q_e+q_s)^2+2q_s}{2|\mathcal{G}|} + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{RLWE}} \quad (16)$$

现在，通过式(14)和式(16)，我们可以得到所需的式(8)。

理论 2：所提的密钥交换协议可以抵抗 PPT 敌手的信号泄露攻击。

证明: 信号泄露攻击是 Ding 等人首次在[]中提出的，假设攻击者扮演 P_i 的角色创建公钥 $p_i = k$，如果 P_j 计算 $k_j = ks_j$ 并利用 f 得到 $w_j = f(ks_j)$，即 $w_j[i] = f(ks_j[i])$。根据信号函数的概念，当 k 从 0 增加到 $q-1$时，$w_j[i]$ 会从 0 翻转到 1 或从 1 翻转到 0，这种切换一共有 $2|s_j[i]|$ 次，因此攻击者可以计算 $w_j[i]$ 的翻转次数并通过将 k 从 0 到 $q-1$ 循环来得到 $s_j[i]$。

在本文所提方案中，$k_j = (p_i s_j + 2c)d + 2g_j$，其中 $c = \mathrm{H}_1(x_i)$，$d = \mathrm{H}_1(x_i, y_j)$，$x_i$ 和 y_j 分别为两方各自生成的临时公钥，很容易得知在每次会话中 c、d 和 g_j 都会发生变化，并且 $w_j = f\left((ks_j + 2c)d + 2g_j\right)$，随着 k 的增加，每当 $(ks_j + 2c)d + 2g_j$ 进入或者离开区间 $\left[-\frac{q}{4}, \frac{q}{4}\right]$ 时，$w_j[i]$ 值会翻转。在这种情况下，由于 $s_j[i]$ 是随机抽样出来的，攻击者无法从 $w_j[i]$ 值的翻转次数中得出任何可信的结论，换句话说，攻击者无法利用信号值泄漏来获取 $s_j[i]$。因此，本文方案可以抵抗信号泄漏攻击。

4 性能分析

本节介绍了所提议方案的性能评估，并比较了我们所提议的密钥交换设计与现有设计的性能成本。

SHA512 的实现已经在 python 中完成，而不考虑多线程处理或并行计算。在实现中使用了库 LatticeCrypto[41]、hashlib 和 Crypto。我们在 SageMath 中执行了格运算代码的实现。

安装 Windows 11 Pro 工作站操作系统(3.9 千兆赫兹 Intel（R) Xeon(R)W-2245 CPU，128 千兆字节随机存取存储器）的戴尔台式电脑作为服务器，安装 Windows 11 处理操作系

统(1.19 千兆赫兹 Intel（R) Core(TM) i3 处理器，4.00 千兆字节随机存取存储器）的联想台式电脑作为最终用户系统。我们为改进协议选择了与 LBA-PAKE [19] 类似的参数，但素数 q 除外。参数分别为：q = 1073479709，标准偏差 α = 3.192，n = 128、256 和 512。我们选择了与 [25] 中类似的较大 q 值，这是因为要在正确性和安全性之间和开销做出权衡，并注意到 [25] 中 q 的选择可能会以很小的概率导致密钥协议失败。我们使用 SHA3-256 作为哈希函数 H0 的实例化，而 H2 的实现方式与 H1 类似，只是从 Rq 中采样时使用了种子。为了证明我们协议的性能，我们在电脑和手机上分别重复了改进方案的每个基本计算操作 10 000 次，然后取平均值。符号 TH0、TH1、TH2、TSig 和 TMod2 分别表示 H0、H1、H2、Sig 和 Mod2 的平均运行时间。而 Tsamp 和 Tmul 分别表示从离散高斯分布 χα 中采样和 Rq 中两个多项式相乘的平均运行时间。其中多项式乘法和 H2() 是最耗时的操作。

最后，我们对比了本方案与其他方案的计算成本，在我们的协议中，服务器选择三个高斯样本，在 Qp 中进行两次标量乘法，在 Qp 中进行两次分量乘法和加法，执行一次 H 哈希函数，计算一次特征函数。因此，我们协议的总计算成本为 1.747032 ms，

Operations	$n = 128$	$n = 256$	$n = 512$
T_{H0}	$35.3/125.7$	$66.2/229.7$	$134.4/439.2$
T_{H1}	$142.9/809.0$	$279.6/1541.9$	$575.7/3200.2$
T_{H2}	$216.3/901.6$	$412.6/1815.5$	$847.3/3522.6$
T_{samp}	$114.9/694.6$	$226.3/1338.5$	$462.1/2773.8$
T_{mul}	$178.0/302.1$	$627.3/922.7$	$2371/3495.4$
T_{Sig}	$115.6/605.0$	$226.4/1155.6$	$457.6/2428.2$
T_{Mod_2}	$106.9/509.1$	$220.0/972.3$	$440.0/1988.8$

表 1 服务器端/用户端基本操作的运行时间（单位：微秒）

Schemes	User	Server	Total run time
Wang et al. Improved KERK	$4t_g + 3t_{sm} + 3t_{amp} + 2t_h + 2t_{ad}$	$4t_g + 3t_{sm} + 3t_{amp} + 2t_h + 2t_{ad} + t_\zeta$	6.438424
Dabra et al. LBA-PAKE	$3t_g + 2t_{sm} + t_{ad} + 3t_{amp} + 2t_h + t_H$	$3t_g + 2t_{sm} + 3t_{amp} + 2t_h + t_{ad} + t_\zeta + t_H$	5.565888
Ding et al. AKE	$4t_g + 2t_{sm} + 5t_{ad} + 3t_{amp} + 2t_h + t_H$	$4t_g + 2t_{sm} + 5t_{ad} + 3t_{amp} + 2t_h + t_H + t_\zeta$	7.815244
PRKE	$t_g + 2t_{sm} + 2t_{amp} + t_H$	$2t_g + 2t_{sm} + 2t_{amp} + t_H + t_\zeta$	2.517426
Improved PRKE	$2t_g + 3t_{sm} + 2t_{amp} + t_{ad} + t_{mul} + t_H$	$2t_g + 3t_{sm} + 2t_{amp} + t_{ad} + t_{mul} + t_H + t_\zeta$	3.955532
Improved LBA-PAKE	$3t_g + 3t_{sm} + 3t_{amp} + 2t_h + t_H$	$3t_g + 3t_{sm} + 3t_{amp} + 2t_h + t_H + t_\zeta$	5.317888
Our Protocol	$2t_{\square} + 2t_{sm} + 2t_{amp} + t_H$	$2t_g + 2t_{sm} + 2t_{amp} + t_H + t_\zeta$	1.747032

表 2 以毫秒为单位的计算复杂度比较

5 讨论

LBA-PAKE [29], Improved KERK[18,27,30]是基于零知识认证密钥交换的概念构建的。该技术使用了除 RLWE 之外的其他安全原语，即以高斯分布输出的 H1 哈希函数。如果攻击

者成功地破坏了 H1 函数，这可能会对安全性造成威胁。因此，安全性最好依赖于 RLWE 假设下提供的不可区分样本。

此外，根据表 2，LBA-PAKE[29]比我们的方案多使用了两个高斯样本和两个多分量的乘法和加法。即使经过如此高的计算，[29]仍然容易受到信号泄漏攻击[30]的攻击。改进的 KERK[18]比我们的方案多使用了 4 个高斯样本，多使用了 2 个分量乘法和加法，多使用了 2 个标量乘法。[27]比我们的方案多使用了四个高斯样本和两个多分量的乘法和加法。[17]比我们的方案少使用一个高斯样本，但该方案被发现容易受到密钥不匹配攻击[18]。改进的 PRKE[18]比我们的方案多使用了两次标量乘法，在 Qp 中使用了两次额外的加法和两次额外的乘法。[30]比我们的方案多使用了两个高斯样本，多使用了两个分量乘法和加法，多使用了两个标量乘法。因此，通过分析表 2 所示的所有方案，我们可以看出所提出的方案具有最佳的效率。

受到这项工作的启发，为 TLS 协议、移动设备和互联网设计了各种密钥交换方案[12,13,33,42]。然而，[43]提出[12,33,42]容易受到信号泄漏攻击，[13]容易受到密钥不匹配攻击。因此，为了抵抗这些攻击，各种对策方案已经发布。表 2 中包含了这些内容。

6 结论

本文提出了一种密钥重用模式下的量子安全、计算效率高的密钥交换协议。该机制确保随机密钥交换，以解决信号泄漏和密钥不匹配攻击的安全性。通过详细的形式化安全证明，证明了该技术的安全性。并进行了对比研究和性能评估，表明计算效率有了显著提高。在未来，人们可以将这一思想扩展到为智能基础设施应用（如智能电网、智能城市和智能交通）设计经过身份验证的密钥交换机制，因为量子安全密钥交换方案将取代当前的密钥交换系统，以获得后量子安全的世界。

参考文献

1. Stallings, W.: Cryptography and Network Security, 4/E. Pearson Education India (2006)

2. Zhao, Z., Ma, S., Qin, P.: Password authentication key exchange based on key consensus for iot security. Clust. Comput. 26(1), 1–12 (2023)

3. Hellman, M.: New directions in cryptography. IEEE Trans. Inform. Theory 22(6), 644–654 (1976)

4. Jing, Z., Gu, C., Yu, Z., Shi, P., Gao, C.: Cryptanalysis of lattice-based key exchange on small integer solution problem and its improvement. Clust. Comput. 22(1), 1717–1727 (2019)

5. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science, IEEE, pp. 124–134 (1994)

6. Soni, L., Chandra, H., Gupta, D.S., Keval, R.: Quantum-resistant public-key encryption and signature schemes with smaller key sizes. Clust. Comput. 2, 1–13 (2022). https://doi.org/10.1007/s10586-022-03955-y

7. Tang, Y., Ba, Y., Li, L., Wang, X., Yan, X.: Lattice-based public-key encryption with conjunctive keyword search in multi-user setting for iiot. Clust. Comput. 25(4), 2305–2316 (2022)

8. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. J. ACM (JACM) 60(6), 1–35(2013)

9. Ding, J., Xie, X., Lin, X.: A simple provably secure key exchange scheme based on the learning with errors problem. Cryptology ePrint Archive (2012)

10. Harn, L., Mehta, M., Hsin, W.-J.: Integrating Diffie–Hellman key exchange into the digital signature algorithm (dsa). IEEE Commun. Lett. 8(3), 198–200 (2004)

11. Zhang, J., Zhang, Z., Ding, J., Snook, M., Dagdelen, O¨ .: Authenticated key exchange from ideal lattices, In: Annual international conference on the theory and applications of cryptographic techniques, Springer, pp. 719–751 (2015)

12. Bos, J.W., Costello, C., Naehrig, M., Stebila, D.: Post-quantum key exchange for the tls protocol from the ring learning with errors problem. In: IEEE symposium on security and privacy. IEEE 2015, 553–570 (2015)

13. Alkim, E., Ducas, L., Po¨ppelmann, T., Schwabe, P.: Post-quantum key exchange-a new hope. In: USENIX security symposium, Vol. 2016 (2016)

14. Bos, J., Costello, C., Ducas, L., Mironov, I., Naehrig, M., Nikolaenko, V., Raghunathan, A., Stebila, D.: Frodo: Take off the ring! practical, quantum-secure key exchange from lwe, In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 1006–1018 (2016)

15. Fluhrer, S.: Cryptanalysis of ring-lwe based key exchange with key share reuse, Cryptology ePrint Archive (2016)

16. Ding, J., Saraswathy, R., Alsayigh, S., Clough, C.: How to validate the secret of a ring learning with errors (rlwe) key, Cryptology ePrint Archive (2018)

17. Gao, X., Ding, J., Li, L., Liu, J.: Practical randomized rlwe-based key exchange against signal leakage attack. IEEE Trans. Comput. 67(11), 1584–1593 (2018)

18. Wang, K., Jiang, H.: Analysis of two countermeasures against the signal leakage attack, in: International Conference on Cryptology in Africa, Springer, pp. 370–388 (2019)

19. Regev, O.: The learning with errors problem. Invited Survey CCC 7(30), 11 (2010)

20. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. J. ACM (JACM) 60(6), 1 – 35 (2013)

21. Steinfeld, R., Sakzad, A., Zhao, R.K.: Titanium: proposal for a nist post-quantum public-key encryption and kem standard. NIST PQC Round 1, 4 – 12 (2017)

22. Ros¸ca, M., Sakzad, A., Stehle´, D., Steinfeld, R.: Middle-product learning with errors, In: Advances in Cryptology – CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20 – 24, 2017, Proceedings, Part III, Springer, pp. 283 – 297 (2017)

23. Hamburg, M.: Module-lwe key exchange and encryption: The three bears, Tech. rep., Technical report, National Institute of Standards and Technology, 2017 (2018)

24. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehle´, D.: Crystals-kyber: a cca-secure module-lattice-based kem. In: IEEE European symposium on security and privacy (EuroS &P). IEEE 2018, 353 – 367 (2018)

25. Langlois, A., Stehle´, D.: Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr. 75(3), 565 – 599 (2015)

26. Kirkwood, D., Lackey, B.C., McVey, J., Motley, M., Solinas, J.A., Tuller, D.; Failure is not an option: Standardization issues for post-quantum key agreement. In: Workshop on Cybersecurity in a Post-Quantum World, p. 21 (2015)

27. Ding, J., Branco, P., Schmitt, K.: Key exchange and authenticated key exchange with reusable keys based on rlwe assumption, Cryptology ePrint Archive (2019)

28. Feng, Q., He, D., Zeadally, S., Kumar, N., Liang, K.: Ideal lattice-based anonymous authentication protocol for mobile devices. IEEE Syst. J. 13(3), 2775 – 2785 (2018)

29. Dabra, V., Bala, A., Kumari, S.: Lba-pake: lattice-based anonymous password authenticated key exchange for mobile devices. IEEE Syst. J. 15(4), 5067 – 5077 (2020)

30. Ding, R., Cheng, C., Qin, Y.: Further analysis and improvements of a lattice-based anonymous pake scheme. IEEE Syst. J. 16(3), 5035 – 5043 (2022)

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

32. Pursharthi, K., Mishra, D.: On the security of ring learning with error-based key exchange protocol against signal leakage attack, Security and Privacy e310

33. Ding, J., Alsayigh, S., Lancrenon, J., Snook, S.R.V.M.: Provably secure password authenticated key exchange based on rlwe for the post-quantum world. In: Topics in Cryptology – CT-RSA 2017: The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14 – 17, 2017, Proceedings, Springer, 2017, pp. 183 – 204

34. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the fortieth annual ACM symposium on Theory of computing, 2008, pp. 197 – 206 (2008)

35. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. SIAM J. Comput. 37(1), 267 – 302 (2007)

36. Zhang, Y., Chen, J., Huang, B.: An improved authentication scheme for mobile satellite communication systems. Int. J. Satell. Commun. Netw. 33(2), 135 – 146 (2015)

37. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-lwe and security for key dependent messages. In: Advances in Cryptology – CRYPTO 2011: 31st Annual

Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31, Springer, pp. 505 – 524 (2011)

38. Abdalla, M., Fouque, P.-A., Pointcheval, D.: Password-based authenticated key exchange in the three-party setting. In: International workshop on public key cryptography, Springer, pp. 65 – 84 (2005)

39. Islam, S.H.: Provably secure two-party authenticated key agreement protocol for post-quantum environments. J. Inform. Secur. Appl. 52, 102468 (2020)

40. Ding, J., Alsayigh, S., Saraswathy, R., Fluhrer, S., Lin, X., Leakage of signal function with reused keys in rlwe key exchange. In: IEEE international conference on communications (ICC). IEEE 2017, 1 – 6 (2017)

41. Longa, P.: Post-quantum cryptography lwe (learning with errors) library, https://github.com/microsoft/LWE_Library.git (2017)

42. Peikert, C.: Lattice cryptography for the internet, in: PostQuantum Cryptography: 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings 6, Springer, pp. 197 – 219 (2014)

43. Dabra, V., Bala, A., Kumari, S.: Reconciliation based key exchange schemes using lattices: a review. Telecommun. Syst. 77, 413 – 434 (2021)