一种基于 RLWE 的三方口令认证密钥交换协议

王梓梁[1,2], 顾小卓[1,2], 任培欣[1,2]

[1] 中国科学院信息工程研究所 信息安全国家重点实验室 北京 中国 100093
[2] 中国科学院大学 网络空间安全学院 北京 中国 100049

摘要 随着量子理论研究的突破性进展, 传统公钥密码体制将在多项式时间内被破解, 设计后量子密码算法更加紧迫。格密码方案可以有效抵抗量子计算机攻击, 具有可移植性强、易于实现等优点, 已成为当前研究的热点。提出了一种基于格上 Ring Learning with Errors(RLWE)问题的三方口令认证密钥交换(Three-party Password Authenticated Key Exchange, 3PAKE)协议, 使用 $\tilde{D}_4$ 格解码方法构造错误协调机制, 通过口令提供三方身份认证, 最终在客户端之间生成会话密钥。在 Bellare Pointcheval Rogaway(BPR)模型中, 证明了协议满足相互认证安全、弱完美前向安全、会话密钥安全, 且能抵抗口令猜测字典攻击。与其他 3PAKE 协议相比, 设计的隐式认证结构显著减少了哈希计算次数, 采用的误差协调机制允许更大的容错距离, 在平衡维度、模数、标准差、错误率并选择合适的参数之后, 将协议错误率降低至 2^{-61}, 模数缩小至 12289, 进一步减少了计算量与通信量。在 C++上结合 NFL(NTT-based Fast Lattice)加速算法对协议进行了实现, 实验结果表明, 协议实现了高达 17 倍的加速, 具有 255 比特量子安全性。

关键词 RLWE; 后量子密码学; 三方口令认证密钥交换
中图法分类号 TP309.2 DOI 号 10.19363/J.cnki.cn10-1380/tn.2026.03.20

A RLWE-based Three-party Password Authenticated Key Exchange Scheme

WANG Ziliang[1,2], GU Xiaozhuo[1,2], REN Peixin[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract With breakthroughs in quantum theory research, public key cryptosystems based on classical mathematical problems can be cracked by Shor and Grover algorithms with large quantum computers in polynomial time. It becomes very urgent to design cryptographic algorithms that can resist quantum attacks. Many post-quantum algorithms have been studied on the lattice, because the lattice cryptography has some excellent properties such as strong portability and easy-to-implement characteristics, and it has become a current research hotspot. With the purpose of meeting the security and computational efficiency requirements for key exchange in user-user scenarios, this paper proposes a Three-party Password Authenticated Key Exchange (3PAKE) protocol based on the Ring Learning with Errors (RLWE) problem, which introduces the $\tilde{D}_4$ lattice as reconciliation mechanism, provides identity authentication between the server and two clients through pre-stored passwords, and enables the participants to establish a common secret session key in an insecure channel. In the Bellare Pointcheval Rogaway (BPR) model, it is proved that the protocol has mutual authentication security, weak perfect forward secrecy, session key security and resilience to password guessing attacks. Compared with other RLWE-based authenticated key exchange protocols, the implicit authenticatied scheme significantly reduces the number of hash calculations, and the error reconciliation mechanism allows higher error tolerance and smaller modulus, which leads to a significant reduction in message size and an increase in efficiency and security. Specifically, after balancing the dimensions, modulus, variance, error rate and selecting appropriate parameters, the error rate is reduced to 2^{-61} and the modulus is reduced to 12289, which further decreases the amount of calculation and communication complexity. The protocol is implemented in C++ with NFL (NTT-based Fast Lattice) acceleration algorithm, which accelerates the polynomial multiplication and significantly improves the efficiency of the entire protocol. The results in practice show the protocol achieves at most 17x speedup and provides 255-bit quantum security.

Key words ring learning with errors; post-quantum cryptography; three-party password authenticated key exchange

通讯作者: 顾小卓, 博士, 高级工程师, Email: guxiaozhuo@iie.ac.cn。
本课题得到北京市科学技术委员会项目(No. Z191100007119004)支持。
收稿日期: 2021-02-26; 修改日期: 2021-04-25; 定稿日期: 2023-08-30

1 引言

密钥交换(Key Exchange, KE)是一种基本的密码原语, 允许两个或多个实体在不安全的信道中交换数据建立共享密钥。1976 年, 为保证公开网络中密钥协商的安全性, Diffie 和 Hellman 提出了一种基于离散对数问题的密钥交换机制[1]。由于 Diffie-Hellman(DH)算法及在其基础上提出的密钥交换协议[1-3]不支持身份认证, 无法抵抗中间人攻击和重放攻击, 学者提出了认证密钥交换协议的概念(Authenticated Key Exchange, AKE)。认证密钥交换协议可以在抵抗假冒、篡改、否认等主动攻击的情况下, 确保会话中的参与者能与另一个诚实的参与者共享会话密钥。在实践中, 为实现认证, 通常利用公私钥对、共享对称密钥或者口令等来构建协议。与其他认证方式对比, 口令认证密钥交换协议(Password Authenticated Key Exchange, PAKE)既不需要公钥基础设施, 也不需要用户存储对称密钥, 通信双方只需共享一个简单、低熵、易于记忆的口令, 就可快速建立共享密钥, 具有数据量小、速度快等优点, 可广泛应用于物联网设备等通信场景中。

1992 年, Bellovin 和 Merritt 提出了第一个可避免离线字典攻击的两方口令认证密钥协商协议(Two-party Password Authenticated Key Exchange, 2PAKE)[4]。Jablon 通过改进 Diffie-Hellman 加密密钥交换算法, 构造了一种新的简化指数加密密钥交换方法(Simple Cryptographic Exponential Key Exchange, SPEKE)[5]。Halevi 和 Krawczyk 给出了一种提供双向认证、防止服务器泄露的用户匿名安全模型[6]。随后, Boyko 等提出了显式口令认证密钥交换(Password Authenticated Key exchange, PAK)协议、隐式口令认证密钥交换(Password Protected Key exchange, PPK)协议和新 PAK-X 协议[7], 并针对被动和主动敌手的情形, 分别给出了形式化安全性证明。PAK 协议是一种包含密钥确认过程的协议, 在协议完成之后协议参与者可以确认指定用户已生成相同的会话密钥。PPK 协议是一种更高效的密钥交换协议, 参与者不对生成的密钥进行确认, 但是可以保证除了拥有口令的诚实参与者以外其他用户不能生成会话密钥。在 PPK 中, 如果某个不诚实用户提供了错误的口令, 密钥协商仍然会继续进行, 但最终不会生成相同的会话密钥, 不诚实用户无法根据会话密钥进行后续的对称加密通信。

但是, 随着量子计算的发展, 传统公钥密码体系迎来了许多挑战。例如, Shor 算法[8]可以用量子计算机解决多项式时间内的整数分解问题和离散对数问题。Grover 算法[9]可以攻破分组密码, 比如 DES(Data Encryption Standard)和 AES(Advanced Encryption Standard)。这促使学者开始研究能够抵抗量子计算机攻击的密码协议。相对基于编码、多变量、散列值以及同源密码构造的后量子协议, 基于格的密码算法在灵活性、安全性和计算量等方面有着卓越的优势, 是近年来的研究热点。格上密码算法一般都是基于带误差学习(Learning With Errors, LWE[10])问题及其衍生的困难问题, 如 RLWE[11](Ring Learning With Errors)、MLWE[12](Module Learning With Errors)等。其中, 基于 RLWE 构造的算法安全性较高、计算速度快、通信开销低, 具有很高的研究价值和广阔的应用前景。

格上密钥协商方案通过引入随机小错误值来保证协议的后量子安全性, 但误差的存在也让通信双方计算出的密钥存在偏差, 因此需要设计相应的误差协调机制恢复出相同的密钥。Ding 等人首先构造了一种模糊提取器[13], 使通信双方能够在有噪声的情况下恢复出相同的会话密钥。基于 RLWE 问题, Peikert 设计了新的协调机制[14], 使用随机加倍函数, 引入交叉舍入函数和模舍入函数, 构造了一个两方密钥交换方案。在 2016 年的 Usenix 安全会议上, Alkim 等人提出了 Newhope 密钥交换方案[15]。Newhope 首次结合数论变换(Number Theoretic Transform, NTT)算法来实现格密钥交换, 加速了耗时最多的多项式计算过程, 极大地提高了整个协议的计算效率。为了满足更高的安全性需求, 张江等人提出了基于丁式误差协调机制的隐式认证密钥交换方案[16], 并基于 Bellare-Rogaway(BR)模型证明了方案的安全性。在 2017 年 RSA 会议上, Ding 等人[17]提出了基于 RLWE 问题的两方 PAK、PPK 协议。随后, Gao 等人[18]将 Ding 的 PAK 方案[17]在 C++中进行了高效实现, 并将 PPK 集成到 TLS 协议中。为了更高效地运行协议[17], Yang 等人[19]使用 AVX2 指令集对 PAK 的实现进行了优化。

然而, 以上认证密钥交换协议大都只针对双方通信的情形, 而在实际场景中, 随着业务的多样化, 参与方通常需要与第三方进行通信。当通信实体数量增加时, 整个网络需要存储的口令数量也会呈爆发式增长。具体来说, 如果网络中有 n 个用户参与通信, 每两个用户协商并共享一个会话密钥, 则整个通信网络中共需要预存储 $n(n-1)/2$ 个口令。在这种情况下, 2PAKE 协议将不再适用。为了解决上述问题, 密码学者提出了三方口令认证密钥交换(Three-party

Password Authenticated Key Exchange, 3PAKE)的概念。在 3PAKE 中, 通过引入可信服务器, 每个用户只需与服务器共享口令, 与其他用户通信时通过服务器进行身份认证, 进而生成会话密钥, 不用预存储其他用户的信息, 降低了口令存储、管理和更新的成本。

2000 年, Joux[20]基于椭圆曲线数学问题首次提出了三方密钥交换协议。由于没有身份认证, 该协议容易受到中间人攻击。Steiner 等人[21]基于口令认证, 提出了第一个 3PAKE 协议。Ding 和 Horster[22]指出, 安全的 3PAKE 方案不仅要抵抗在线字典攻击, 还需要抵抗离线口令猜测攻击。随后, Wu 等人提出了一种增强的 3PAKE 协议[23], 并进行了形式化安全性证明。目前, 基于传统数学难题的 3PAKE 方案的研究已经取得了许多进展[21-23]。但是, 基于格的三方认证密钥协商研究成果相对较少。2012 年, Ding 构造了一种基于理想格的密钥交换协议[13], 并将其扩展到多个参与者的情况。但是, 为了抵抗量子攻击并保证协议的正确性, 协议在参数选择上使用了大模数, 导致计算效率低, 同时由于未进行认证, 协议仍存在受到中间人攻击的风险。2018 年, Yu 等人[24]基于公钥加密系统和近似平滑投影哈希函数构造构建了一个 LWE-3PAKE 协议, 通过引入一种消息认证机制来避免重放攻击。最近, Xu 等人[25]和 Liu 等人[26]进一步对 3PAKE 协议进行了研究, 分别提出了理想格上满足相互认证、弱完美前向安全的显式 RLWE-3PAKE 协议。

总的来说, 目前几乎所有基于经典数学难题的 3PAKE 协议都不能抵抗量子攻击, 而基于格构造的密钥协商的研究成果较少, 且都存在模数大、通信复杂度高、运行效率低等问题, 不能达到实际应用中所要求的 128-bit 后量子安全度, 不适用于真实网络通信场景。

为了满足三方场景在安全性、计算效率上对密钥协商的需求, 本文提出了一种基于 RLWE 问题的隐式 3PAKE 协议。具体贡献如下:

1) 提出了一种隐式三方口令认证密钥协商的方法。相对于其他常用的需要多次进行哈希运算的显式三方认证方法, 隐式方案简化了认证结构, 减少了多项式哈希的次数以及传输消息的大小。实验结果表明, 隐式 3PAKE 方案在客户端-服务器-客户端场景中, 具有通信量小、运行效率高等优点。

2) 在 C++中对协议进行了高效实现。通过优化系统参数, 采用高效的误差协调机制 $\tilde{D}_4$, 结合 NFLlib 库以加速多项式乘法, 提高了整个协议的计算效率。与文献[17,26]的密钥交换协议相比, 我们的实现速度分别提高了 9~17 倍。

3) 在 Bellare Pointcheval Rogaway(BPR)安全模型中证明了协议的安全性。通过将敌手攻击本协议的优势归约至解决 DRLWE 问题的困难性, 证明协议可以提供相互认证和前向保密性。根据文献[15]中的分析算法, 方案实现了 255 位的量子安全, 可以抵抗原始攻击和双重攻击。

2 预备知识

2.1 RLWE 问题

Lyubashevsky 等人[11]在 2010 年首次提出了理想格上 RLWE 的概念, 使用多项式取代大矩阵参数, 解决了格密码系统密文尺寸过大的问题。以下给出 RLWE 问题困难性的定义。

定义 1. 搜索型 RLWE 问题. 设参数 n、q 为正整数, 定义多项式环 $R_q=\mathbb{Z}_q[x]/(X^n+1)$。$\chi$ 为环 R_q 上的分布, 令秘密 $s\leftarrow\chi$, 公共参数 $a\in R_q$, 随机选取错误值 $e\leftarrow\chi$, 令 $b=as+e\in R_q$。给定 (a, b), 求解秘密值 s。

定义 2. 判定型 RLWE 问题(Decision Ring Learning With Errors, DRLWE). 设参数 n、q 为正整数, 定义多项式环 $R_q=\mathbb{Z}_q[x]/(X^n+1)$。$\chi$ 为环 R_q 上的分布, 令秘密 $s\leftarrow\chi$, 随机选取错误值 $e\leftarrow\chi$。给定随机 $a\in R_q$, 判断 b 为满足 $b=as+e$ 的 RLWE 实例还是 R_q 上的随机值。

2.2 误差协调机制

基于理想格上 RLWE 问题构造密钥交换方案的一个关键难点就在于 RLWE 问题中带有错误值。一方面, 随机错误值是保证后量子安全的重要组成部分, 错误值的存在使得 RLWE 问题难以求解。另一方面, 错误值的存在使通信双方仅能得到近似的值, 无法直接作为会话密钥使用。因此, 需要使用相应的误差协调机制对错误值带来的误差进行处理。

2.2.1 $\tilde{D}_4$ 格解码

2012 年, Ding 等人构造了一种巧妙的丁式误差同步机制[13], 通信双方可根据信号值和协调函数, 从两个近似值中提取出相同的比特。为解决提取出的共同比特的分布仅具有高熵但不随机均匀的问题, Peikert 引入随机提取器, 给出了一种新型误差协调

机制[14]。随后, 许多学者基于 Peikert 误差协调机制提出了各种变形, 其中, 基于 $\tilde{D}_4$ 格解码的误差协调机制[15]更为高效实用。

对于两个在一定误差范围内的近似数值, 基于 $\tilde{D}_4$ 格解码的误差协调机制可以将其恢复成相同的值。相对文献[13-14]中的误差协调机制而言, $\tilde{D}_4$ 格解码方法是从四个 $\mathbb{Z}_q$ 元素中提取出一个比特, 因此容错范围更大, 在相同维度下具有模数更小、通信复杂度更低的优点。在环 R_q 上, 多项式环元素可由向量表示。为了更清晰地描述错误协调算法中多项式环元素与系数之间的转换关系, 本节单独使用粗体代表环元素, 使用正常体代表系数。四维格 $\tilde{D}_4$ 的格基 $\boldsymbol{B}$ 定义如下:

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

在四维格中, 与编码解码相关的两个关键格点为 $\boldsymbol{0}=(0,0,0,0)^t$, $\boldsymbol{g}=\left(\frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2}\right)^t$。定义误差协调机制中的 $\mathrm{CVP}_{\tilde{D}_4}$ 和 Decode 算法分别如算法 1、算法 2 所示。

算法 1. $\mathrm{CVP}_{\tilde{D}_4}(\boldsymbol{x}\in\mathbb{R}^4)$ 算法生成协调信息过程.

输入: 向量 $\boldsymbol{x}\in\mathbb{R}^4$

输出: 协调信息 $\boldsymbol{\omega}\in\{0,\ 1,\ 2,\ 3\}^4$

1. $\boldsymbol{v}_0\leftarrow[\boldsymbol{x}]$
2. $\boldsymbol{v}_1\leftarrow[\boldsymbol{x}-\boldsymbol{g}]$
3. $k\leftarrow(\|\boldsymbol{x}-\boldsymbol{v}_0\|_1<1)?0:1$
4. $(v_0,\ v_1,\ v_2,\ v_3)^t\leftarrow\boldsymbol{v}_k$
5. 返回 $(v_0,\ v_1,\ v_2,\ k)^t+v_3\cdot(-1,\ -1,\ -1,\ 2)^t$

算法 2. Decode 算法生成协调值过程.

输入: 向量 $\boldsymbol{x}\in\mathbb{R}^4/\mathbb{Z}^4$

输出: 协调值 $k\in\{0,\ 1\}$

1. $\boldsymbol{v}\leftarrow\boldsymbol{x}-[\boldsymbol{x}]$
2. 如果 $\|\boldsymbol{v}\|_1\le 1$, 返回 0; 否则返回 1

设 q 为模数, v、w 为满足 $\|\boldsymbol{v}-\boldsymbol{w}\|_1<3q/4-2$ 的近似向量 $\boldsymbol{v}\in\mathbb{Z}_q^4$、$\boldsymbol{w}\in\mathbb{Z}_q^4$, 基于 $\tilde{D}_4$ 格解码方法的误差协调机制包括两个函数:

1) 协调函数 $\mathrm{HelpRec}(\boldsymbol{v})$: 输入近似值 $\boldsymbol{v}\in\mathbb{Z}_q^4$, 选择随机均匀比特 $b\in\{0,1\}$, 输出协调向量 $\boldsymbol{\omega}=\mathrm{HelpRec}(\boldsymbol{v})=\mathrm{CVP}_{\tilde{D}_4}(\frac{4}{q}(\boldsymbol{v}+b\boldsymbol{g}))\ \mathrm{mod}\ 4$;

2) 恢复函数 $\mathrm{Rec}(\boldsymbol{w},\boldsymbol{\omega})$: 输入近似值 $\boldsymbol{w}\in\mathbb{Z}_q^4$, 协调向量 $\boldsymbol{\omega}\in\{0,\ 1,\ 2,\ 3\}^4$, 输出协调值 $k=\mathrm{Rec}(\boldsymbol{w},\boldsymbol{\omega})=\mathrm{Decode}(\frac{1}{q}\boldsymbol{w}-\frac{1}{4}\boldsymbol{B}\boldsymbol{\omega})\in\{0,\ 1\}$。

定义格点 p 的 Voronoi 胞为格空间中距离 p 比其他任意格点都近的点的集合。假设 Alice 和 Bob 分别拥有近似向量 $\boldsymbol{v},\ \boldsymbol{w}\in\mathbb{Z}_q^4$。Alice 首先随机掷币 $b\in\{0,\ 1\}$, 这是为了使最终的输出随机均匀, 称为 Voronoi 胞的边界模糊。然后, Alice 根据协调函数 HelpRec, 计算输入向量 $\boldsymbol{v}$ 在基 $\boldsymbol{B}$ 下的坐标, 并使用 $\mathrm{CVP}_{\tilde{D}_4}$ 算法得到协调向量 $\boldsymbol{\omega}$, 这指示了该坐标与它所在的 Voronoi 胞中心的距离。然后, Alice 将 $\boldsymbol{\omega}$ 发送给 Bob。根据恢复函数 Rec 和协调向量 $\boldsymbol{\omega}$, Alice 和 Bob 分别使用解码算法 Decode, 判断 $\boldsymbol{v}$ 和 $\boldsymbol{w}$ 在基 $\boldsymbol{B}$ 下的位置。如果该位置处于以格点 $\boldsymbol{0}=(0,0,0,0)^t$ 为中心的 Voronoi 胞, 则解码为 0; 如果处于以格点 $\boldsymbol{g}=(\frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2})^t$ 为中心的 Voronoi 胞, 则解码为 1。若 $\boldsymbol{v}$ 和 $\boldsymbol{w}$ 在基 $\boldsymbol{B}$ 下的坐标都处同一个 Voronoi 胞, 则 Alice 和 Bob 可直接解码得到相同的比特。如果不在同一个 Voronoi 胞中, 则双方根据协调向量 $\boldsymbol{\omega}$, 分别向 Alice 所在的 Voronoi 胞中心移动一段距离。只要 $\boldsymbol{v}$ 和 $\boldsymbol{w}$ 足够接近, 二者就可以移动到同一个 Voronoi 胞内, 从而解码得到相同的值。

由于 Voronoi 胞的形状和大小全等, 且协调信息仅指示输入向量 $\boldsymbol{v}$ 与 Voronoi 胞中心的距离, 但是并未泄露它所在的位置, 加上引入了边界模糊等技术, 因此最终解码得到的协调值仍具有不确定性。即当向量 $\boldsymbol{v}\in\mathbb{Z}_q^4$ 均匀随机时, 给定协调向量 $\boldsymbol{\omega}$, 解码输出的 k 仍是均匀随机的, 这被称为误差协调机制的安全性。

引理 1[15]. 正确性. 令模数 q 为奇素数, 向量 $\boldsymbol{v},\ \boldsymbol{w}\in\mathbb{Z}_q^4$, 选取均匀随机比特 $b\in\{0,\ 1\}$, 协调信息 $\boldsymbol{\omega}=\mathrm{HelpRec}(\boldsymbol{v})$, 在每个维度用 r 比特表示。如果两个向量近似, 且二者差距满足 $\|\boldsymbol{v}-\boldsymbol{w}\|_1\le(1-1/2^r)\cdot q-2$, 则可得到 $\mathrm{Rec}(\boldsymbol{v},\ \boldsymbol{\omega})=\mathrm{Rec}(\boldsymbol{w},\ \boldsymbol{\omega})$。

上述引理在 R_q 上依然成立。对于多项式环上的元素 $\boldsymbol{v}=(v_0, v_1,..., v_{n-1})$，可计算出协调信息 $\boldsymbol{\omega}=(\boldsymbol{\omega}_0,..., \boldsymbol{\omega}_{n/4-1})=(\text{HelpRec}(v_0, v_1, v_2, v_3),..., \text{HelpRec}(v_{n-4}, v_{n-3}, v_{n-2}, v_{n-1}))$。其协调值为 $\boldsymbol{k}=\text{Rec}(\boldsymbol{v}, \boldsymbol{\omega})=(\text{Rec}(v_0, v_1, v_2, v_3), ..., \text{Rec}(v_{n-4}, v_{n-3}, v_{n-2}, v_{n-1}))$。

2.2.2 Newhope 协议

2016 年, Alkim 等人在 Peikert 式误差协调机制的基础上, 根据基于 $\tilde{D}_4$ 格解码机制构造了未认证的 NewHope 密钥交换协议[15]。由于 Peikert 式误差协调机制需要每一个 $\mathbb{Z}_q$ 元素都提取出一个协调值, 而 $\tilde{D}_4$ 格解码机制是根据四个 $\mathbb{Z}_q$ 元素提取出一个协调值, 因此后者容错范围更大。与基于 Peikert 式误差协调的 BCNS15 协议[27]相比, 在错误率相同的情况下, NewHope 协议可使用更小的模数, 从而降低了协议通信量。当二者维度都设置为 $n=1024$ 时, NewHope 协议可达到 BCNS15 协议的两倍安全性, 同时通信量减半, 是一种更高效的密钥交换协议。图 1 为 NewHope 协议的交互过程。

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

图 1 基于 RLWE 的 NewHope 协议

Figure 1 The RLWE-based NewHope protocol

在 NewHope 密钥交换协议中, 对于服务器, 计算得到的环元素值为 $\boldsymbol{v}'=\boldsymbol{us}=\boldsymbol{ass}'+\boldsymbol{e}'\boldsymbol{s}$。对于客户端, 计算得到的环元素值为 $\boldsymbol{v}=\boldsymbol{bs}'+\boldsymbol{e}''=\boldsymbol{ass}'+\boldsymbol{es}'+\boldsymbol{e}''$。$\boldsymbol{v}$ 与 $\boldsymbol{v}'$ 均近似于 $\boldsymbol{ass}'$，但存在偏差 $\boldsymbol{v}-\boldsymbol{v}'=\boldsymbol{es}'+\boldsymbol{e}''-\boldsymbol{e}'\boldsymbol{s}$, 无法直接作为共享密钥使用。因此, 协议需要引入 $\tilde{D}_4$ 误差协调机制对偏差进行处理, 使通信双方得到一致的会话密钥。如文献[15]所述, 在 $\tilde{D}_4$ 误差协调机制中, 已知协调信息 $\boldsymbol{r}$ 的情况下, 并不会泄露 $\boldsymbol{v}$ 的任何信息。此外, NewHope 协议使用 2 比特离散化, 即离散比特数 $r=2$。由引理 1 可知, 在服务器发送了协调信息 $\boldsymbol{r}$ 之后, 双方均对 $\boldsymbol{v}$ 和 $\boldsymbol{w}$ 执行协调函数 Rec，只要满足 $\|\boldsymbol{v}-\boldsymbol{w}\|_1 \le \frac{3}{4}q-2$，双方就可以得到相同的协调值, 哈希处理之后得到一致的共享密钥。

2.3 中心二项分布和采样

本节描述了中心二项式分布的定义, 该分布用于生成协议中的秘密值和小错误值。

定义 3. 中心二项分布. 令 ψ_k 为参数 k 的中心二项式分布, 期望值为 0, 标准差 $\beta=\sqrt{k/2}$。采样时, 随机选择 $b_i, b_i' \in \{0, 1\}$，计算采样值 $\sum_{i=0}^{k} b_i - b_i'$，采样结果为 $[-k, k]$ 的整数。

如文献[15]定理 4.1 所述, 参数为 k 的中心二项分布, 在性质和安全性上与标准差为 $\sqrt{k/2}$ 的离散高斯分布相似, 且能防止计时攻击。与文献[11,13-14, 16-17]采用的离散高斯分布相比, 中心二项分布不需要引入大的表格和高精度计算, 采样方式也更简单, 采样效率更高。因此, 论文使用能更高效地在硬件、软件上实现的中心二项分布进行随机数采样。

2.4 安全模型

1995 年, Bellare 和 Rogaway 提出了三方场景下的口令认证密钥交换协议的可证明安全模型(BPR 模型[28])。他们给出了该模型下的敌手攻击能力、安全性、匹配性和新鲜性定义。本文将 BPR 模型引入了基于 RLWE 和 PWE 问题构造的密码方案。模型详细介绍如下。

1) 参与者: 3PAKE 协议的参与者由客户端和可信服务器组成。每一次会话均包括两个客户端和一个服务器。每个参与者都可以发起一个或多个实例。参与者 U 的第 i 个实例定义为 Π_U^i。

2) 长期密钥: 每个诚实的客户端 U 都拥有一个长期的秘密口令 pw_U。对于诚实客户端 U，可信服务器存储其对应的口令哈希值 $<-H_1(\text{pw}_U), H_2(\text{pw}_U)>$。

3 敌手攻击能力: 设敌手 $\mathcal{A}$ 为可控制参与者通信信道的概率多项式时间(Probabilistic Polynomial Time, PPT)算法。敌手 $\mathcal{A}$ 与参与者之间通过 Oracle 查询进行交互。攻击者可以执行以下查询。

① Send(Π_U^i, m): 该询问用于描述主动攻击。敌手 $\mathcal{A}$ 向参与者 U 的实例 Π_U^i 发送消息 m, 接收到 m 后, 实例 Π_U^i 向敌手返回对应的响应消息。

② Excute(Π_A^i, Π_B^j, Π_S^k): 该询问用于描述被动攻击。敌手 $\mathcal{A}$ 通过该询问获得参与者之间交换的真实消息。

③ Reveal(Π_U^i): 该询问描述了会话密钥泄露攻击。如果 Π_U^i 的会话密钥SK 已生成, 则该查询有效且向敌手 $\mathcal{A}$ 返回SK 。

④ Corrupt(U): 此查询用于描述主动攻击。敌手 $\mathcal{A}$ 通过该查询可获得被攻陷的参与者 U 的口令 pw_U, 但无法获得协议运行过程中 U 的任何内部状态。

⑤ Hash(m): 敌手 $\mathcal{A}$ 可对随机预言机 Ω_h 进行询问, 从而获得任意哈希值。预言机检查 m 是否已被询问过。如果已被询问, Ω_h 将返回给敌手 Hash 表中的上一次询问的结果。否则, Ω_h 向敌手返回一个随机数 c, 并将 (m, c) 存储在哈希表中。

⑥ Test(Π_U^i): 此查询用于描述实例 Π_U^i 的会话密钥的语义安全性。如果会话密钥还未生成, 则返回 $\perp$。否则, 根据随机数 b 给出返回结果。如果 $b=0$, 则返回实例 Π_U^i 的真实会话密钥SK 。如果 $b=1$, 则向敌手 $\mathcal{A}$ 返回与其会话密钥长度相同的随机字符串 $\{0, 1\}^{\lambda}$, 其中 λ 为会话密钥的长度。仅当 Π_U^i 是新鲜的, 才能执行Test(Π_U^i) 询问。

在协议中, 伙伴关系和新鲜性的定义如下:

定义 4. 伙伴关系. 用户实例 Π_A^i 和 Π_B^j 被认为是伙伴, 如果满足以下条件:

1) Π_A^i 和 Π_B^j 相互交换了所需数量的消息;

2) Π_A^i 和 Π_B^j 建立的会话密钥相同;

3) 除了 Π_A^i 和 Π_B^j, 没有其他会话预言机拥有其会话密钥。

定义 5. 新鲜性. Π_U^i 被认为是新鲜的, 如果满足以下条件:

1) Π_U^i 已经接受;

2) Π_U^i 没有被进行Corrupt 询问;

3) Π_U^i 与其匹配会话没有被进行Reveal 询问。

定义 6. AKE 安全. 设 b 为 Test(Π_U^i) 查询选择的随机比特, b^* 为概率多项式时间(PPT)的敌手 $\mathcal{A}$ 选择的随机值。协议被认为是AKE 安全的, 如果 Π_U^i 是新鲜的, 且敌手赢得 Test(Π_U^i) 查询, 成功区分会话密钥与随机数的优势 $\mathrm{Adv}_P^{\mathrm{AKE}}(\mathcal{A})=|2\Pr[b^*=b]-1|$ 是可忽略的。

由于本节及之后的论文部分只涉及多项式, 未涉及系数及二者转换关系, 为简化公式, 环元素统一由正常细体表示。

定义 7. 误差配对(Pairing With Erros, PWE)问题. 令 ψ_k 是参数为 k 的离散高斯分布, 对于任意 $(a, s)\in R_q^2$, 令 $\tau(a, s)=\mathrm{Rec}(as, \mathrm{HelpRec}(as))$。对于概率多项式时间内的敌手 $\mathcal{A}$, 其输入为 (a_1, a_2, b, ω), 输出为 $\{0, 1\}^{n/4}$。其中 $(a_1, a_2, b)\in R_q^3$, $s\in R_q$ 是随机选择的, b 在 $a_1 s$ 上加入了小错误值, $\omega=\mathrm{HelpRec}(a_2 s)\in\{0, 1, 2, 3\}^n$。敌手 $\mathcal{A}$ 需要从输出中获得正确 $\tau(a_2, s)$。敌手攻击成功的优势为:

$$\mathrm{Adv}_{R_q}^{\mathrm{PWE}}(\mathcal{A})=\Pr[a_1\leftarrow R_q; a_2\leftarrow R_q;\ s, e\leftarrow\psi_k^n; b\leftarrow a_1 s+e;\ \omega\leftarrow\mathrm{HelpRec}(a_2 s):\ \tau(a_2, s)=A(a_1, a_2, b, \omega)]$$

。令 $\mathrm{Adv}_{R_q}^{\mathrm{PWE}}(t, N)=\max_{\mathcal{A}}\{\mathrm{Adv}_{R_q}^{\mathrm{PWE}}(\mathcal{A})\}$, 其中, t 是最大时间复杂度, 输出最多包含 N 个 $\{0, 1\}^{n/4}$ 元素。根据 PWE 假设, 概率多项式时间内的敌手攻击成功的优势 $\mathrm{Adv}_{R_q}^{\mathrm{PWE}}(t, N)$ 是可忽略的。

定义 8. 判定型误差配对(Decision Pairing with Errors, DPWE) 问题. 给定 $(a_1, a_2, b, \omega, \sigma)\in R_q\times R_q\times R_q\times\{0, 1, 2, 3\}^n\times\{0, 1\}^{n/4}$, 对于 $K\in R_q$, $\omega\leftarrow\mathrm{HelpRec}(K)$, $\sigma=\mathrm{Rec}(K, \omega)$。设 s, e_1, e_2 由 ψ_k^n 分布采样生成, 则 DPWE 问题是判断 (K, b) 满足 $K=a_2 s+e_1$, $b=a_1 s+e_2$, 还是 $R_q\times R_q$ 上的均匀随机值。

定义 9. RLWE-DH(Ring Learning With Errors-Diffie Hellman)问题. 令 R_q 和 ψ_k 的定义如上。给定环元素 (a_1, a_2, b, K), 其中 (a_1, a_2) 在 R_q^2 上是均匀随机的。对于 $g_y, s_y, e_y\leftarrow\psi_k^n$, RLWE-DH 问题是判断 (K, b) 满足 $K=a_2 s_y+g_y$, $b=a_1 s_y+e_y$, 还是

$R_q \times R_q$ 上的均匀随机值。

定理 1. (文献[17], 定理 1). 令 R_q 和 ψ_k 的定义如上。如果解决 DRLWE 问题是困难的, 那么解决 RLWE-DH 问题也是困难的。

证明. 设解决 DRLWE 问题是困难的。假设存在算法 $\mathbb{D}$, 当输入 (a_1, a_2, b, K), $\mathbb{D}$ 能以不可忽略的概率解决 RLWE-DH 问题。对于 $g_y, s_y, e_y \leftarrow \psi_k^n$, $\mathbb{D}$ 可以判断 (K, b) 是满足 $K=a_2 s_y + g_y$ 且 $b = a_1 s_y + e_y$ 的值, 还是 $R_q \times R_q$ 上的均匀随机值。

给定两个共享相同的 $s \leftarrow \psi_k^n$ 的 DRLWE 挑战示例 (a_1, b_1)、(a_2, b_2), 使用算法 $\mathbb{D}$ 可构造出能解决如下 RLWE 问题的区分器 $\mathbb{D}'$:

1) 令 $(a_1, a_2, b, K) = (a_1, a_2, b_1, b_2)$;

2) 当输入 (a_1, a_2, b, K) 时, 运行 $\mathbb{D}$, 可以得到:

- $b_2 = a_2 \cdot s + e_2$, $b_1 = a_1 \cdot s + e_1$, 其中, e_1, e_2 根据分布 ψ_k^n 生成;
- 或者 b_2 和 b_1 是 R_q 上的均匀随机值。

由于 $\mathbb{D}$ 能以不可忽略的概率解决 RLWE-DH 问题, 则区分器 $\mathbb{D}'$ 也能以不可忽略的概率解决 DRLWE 问题, 这与 DRLWE 问题的困难性假设相悖。因此定理 1 的证。

定理 2. (文献[17], 定理 2). 令 R_q 和 ψ_k 的定义如上。如果解决 RLWE-DH 问题是困难的, 那么解决 DPWE 问题也是困难的。

证明. 设解决 RLWE-DH 问题是困难的。假设存在算法 $\mathbb{D}$, 当输入 $(a_1, a_2, b, \omega, \sigma)$, 对于 $K \in R_q$, $\omega \leftarrow \mathrm{HelpRec}(K)$, $\sigma = \mathrm{Rec}(K, \omega)$, $\mathbb{D}$ 能以不可忽略的优势区分 (K, b) 是满足 $K = a_2 s + e_1$ 和 $b = a_1 s + e_2$ 的值, 还是 $R_q \times R_q$ 上的均匀随机值。

构造区分器 $\mathbb{D}'$,当输入 (a_1, a_2, b, K), 可以使用算法 $\mathbb{D}$ 根据以下方式解决 RLWE-DH 问题:

1) 计算 $\omega \leftarrow \mathrm{HelpRec}(K)$, $\sigma = \mathrm{Rec}(K, \omega)$;

2) 输入 $(a_1, a_2, b, \omega, \sigma)$, 运行算法 $\mathbb{D}$ 以解决 DPWE 问题:

- 如果 $\mathbb{D}$ 输出 1, 那么 $K = a_2 s + e_1$, $b = a_1 s + e_2$, 其中 $s, e_1, e_2 \leftarrow \psi_k^n$。
- 否则, (K, b) 为 $R_q \times R_q$ 上的均匀随机值。

如果 $\mathbb{D}$ 能以不可忽略的优势解决 DPWE 问题, 则 $\mathbb{D}'$ 也能以不可忽略的优势解决 RLWE-DH 问题。这与以上 RLWE-DH 问题的困难性假设相悖。因此定理 2 得证。

根据定理 1 和定理 2, DPWE 问题可以被归约到解决 DRLWE 问题的困难性。即如果解决 DRLWE 问题是困难的, 那么解决 DPWE 问题是困难的, 从而解决 PWE 问题也是困难的。更详细的内容可参考文献[17]。

2.5 安全属性

设计一个 3PAKE 协议至少需要满足以下基本安全属性:

1) 相互认证安全。在通信过程中, 协议的三个参与者之间都要相互验证对方的身份, 完成两两之间的双向认证。

2) 前向保密性。如果所有参与者的长期密钥都丢失了, 也不影响之前建立的会话密钥的安全性, 则称该协议可提供完美前向安全。但是 HQMV[29]指出, 如果敌手可以主动选择临时密钥, 则没有认证密钥交换协议可以满足前向安全性。因此 HQMV 定义了弱完美前向保密性, 即在敌手只进行窃听、没有主动选择临时密钥的情况下, 如果会话完成之后参与方的长期密钥丢失不会影响之前建立的会话密钥的安全性, 则称协议满足弱完美前向保密性。

3) 已知会话密钥安全。即使敌手获得了之前某个会话的会话密钥, 也不能推出其他会话的共享密钥, 则满足已知会话密钥安全。

4) 抗口令字典攻击。为了保证口令的安全性, 协议需要保证任意攻击者发动离线字典攻击成功的优势可忽略, 发动在线字典攻击的概率为 $O(1/|D|)+\mu(n)$, 其中 $|D|$ 为口令字典的大小, $\mu(n)$ 为可忽略函数。

3 基于 RLWE 的三方口令认证密钥交换协议

本节提出一个格上三方口令认证密钥交换协议 RLWE-3PAKE。协议参与方包括两个客户端和一个服务器组成。客户端持有自己的口令, 服务器存储其口令哈希值。协议发起之后, 客户端和服务器分别生成随机秘密值和错误值, 结合口令哈希值, 共同隐藏在密钥中进行传输与响应。最后, 两个客户端通过 $\tilde{D}_4$ 格解码误差协调机制计算出与通信方一致的会话密钥。

3.1 应用场景

与经典的系统模型相似, 本文提出的基于口令认证的 3PAKE 协议由三个参与者组成, 分别为服务

器 Server、客户端 Alice 和客户端 Bob。其应用场景如图 2 所示。

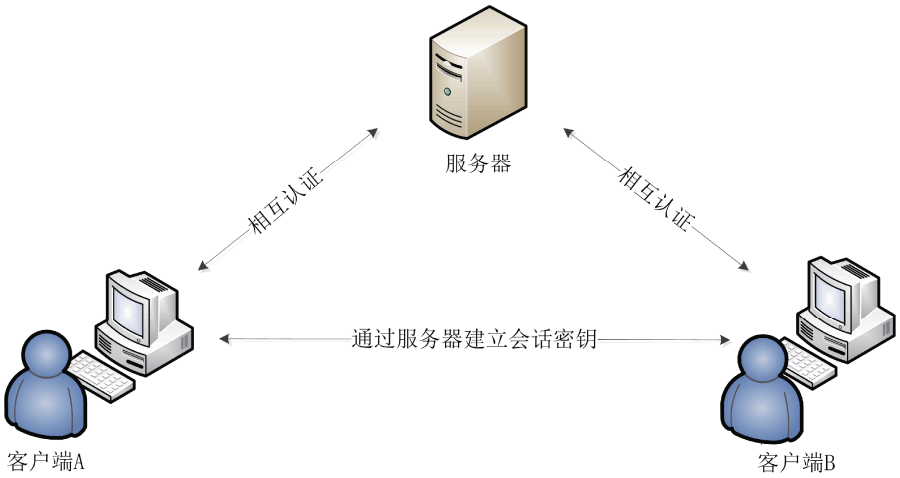

图 2 3PAKE 应用场景

Figure 2 The application scenario of the 3PAKE protocol

- 客户端 Alice 与 Server 共享口令 pw_A，客户端 Bob 与 Server 共享口令 pw_B。各客户端分别使用秘密口令与 Server 进行相互认证，在 Server 的协助下建立共享会话密钥。
- 服务器可信且存储所有客户端的口令哈希值，负责认证客户端、在客户端之间传递消息。

3.2 协议描述

令 A, B, S 分别为客户端 Alice、客户端 Bob、服务器 Server 的缩写。各参与方身份信息为 ID_i，其中 $i \in \{A, B, S\}$。定义多项式环 $R_q = Z_q[x]/(x^n+1)$，其中 q 为素模数，n 为多项式维度。注意，环 R_q 上的元素为多项式，其系数可由 n 维向量表示。令 H_1，H_2，H_3，H_4 为哈希函数，分别定义为：$H_l: \{0,1\}^* \to R_q$，$l \in \{1,2,3\}$，$H_4: \{0,1\}^* \to \{0,1\}^\lambda$，其中 λ 为会话密钥 SK 的长度。客户端 i 持有口令 pw_i，$i \in \{A, B\}$。服务器 S 持有两对口令验证值 $\langle \gamma'_{A_1}, \gamma_{A_2} \rangle = \langle -H_1(\mathrm{pw}_A), H_2(\mathrm{pw}_A) \rangle$ 和 $\langle \gamma'_{B_1}, \gamma_{B_2} \rangle = \langle -H_1(\mathrm{pw}_B), H_2(\mathrm{pw}_B) \rangle$。令 ψ_k 为中心为 0、标准差为 $\sqrt{k/2}$ 的中心二项分布，设 R_q 上的 $e_i \leftarrow \psi_k^n$ 为根据 ψ_k^n 分布采样生成的随机小错误值，即 e_i 的每个系数均取自中心二项分布 ψ_k。同样的，s_i 为中心二项分布 ψ_k^n 随机采样得到的小秘密值。图 3 描述了 RLWE-3PAKE 协议的流程:

1) 协议发起。客户端 A 向服务器 S 发送 $\langle \mathrm{ID}_A, \mathrm{ID}_B \rangle$ 以发起会话。

2) 第一次响应。服务器 S 随机生成 seed，根据 seed 和伪随机函数生成公共参数 $a \in R_q$，然后从中心二项分布上随机采样生成一些秘密值和错误值 $s_1, s_2, e_1, e_2, e_{SA}, e_{SB} \leftarrow \psi_k^n$，计算秘密值 $p_{S_1} = as_1 + e_1$，秘密值 $p_{S_2} = as_2 + e_2$，$m_{S_1} = p_{S_1} + \gamma'_{A_1}$，$m_{S_2} = p_{S_2} + \gamma'_{B_1}$。然后，$S$ 将 $\langle m_{S_1}, m_{S_2} \rangle$ 发送给客户端 A 和客户端 B。

3) 第二次响应。两个客户端可以分别同时进行响应。客户端 A 随机采样生成 $s_A, e_A \leftarrow \psi_k^n$，计算两个口令哈希值 $\gamma_{A_1} = H_1(\mathrm{pw}_A)$，$\gamma_{A_2} = H_2(\mathrm{pw}_A)$。在接收到来自 S 的消息 $\langle m_{S_1}, m_{S_2} \rangle$ 后，客户端 A 进行检查，如果 $m_{S_1}, m_{S_2} \notin R_q$，则中止协议。否则，继续计算并提取来自服务器的秘密值 $p_{S_1} = m_{S_1} + \gamma_{A_1}$，且生成秘密值 $p_A = as_A + e_A$，继续计算 $k_{AS} = p_{S_1} \cdot s_A$，信号值 $\omega_{AS} = \mathrm{HelpRec}(k_{AS})$，协调值 $\sigma_{AS} = \mathrm{Rec}(k_{AS}, \omega_{AS})$，$x_{AS} = p_A + p_{S_1} + \gamma_{A_2}$。并向服务器发送消息 $\langle x_{AS}, \omega_{AS} \rangle$。同时，客户端 B 随机采样生成 s_B，$e_B \leftarrow \psi_k^n$，计算两个口令哈希值 $\gamma_{B_1} = H_1(\mathrm{pw}_B)$，$\gamma_{B_2} = H_2(\mathrm{pw}_B)$。检查接收到的消息 $\langle m_{S_1}, m_{S_2} \rangle$ 是否满足 $m_{S_1}, m_{S_2} \in R_q$，如果不满足则终止协议。否则，B 从消息中提取出服务器的秘密密钥 $p_{S_2} = as_2 + e_2$，同时生成 B 的秘密值 $p_B = as_B + e_B$，并计算 $k_{BS} =$

$p_{S_2}\cdot s_B$，信号值 $\omega_{BS}=\mathrm{HelpRec}(k_{BS})$，协调值 $\sigma_{BS}=\mathrm{Rec}(k_{BS},\omega_{BS})$，$x_{BS}=p_{S_2}+p_B+\gamma_{B_2}$，并将 $\langle x_{BS},\omega_{BS}\rangle$ 发送给服务器 S。

4) 第三次响应。在服务器 S 接收到来自 A 和 B 的消息 $\langle x_{AS},x_{BS},\omega_{AS},\omega_{BS}\rangle$ 后，如果接收到的 x_{AS}，$x_{BS}\notin R_q$，则 S 中止协议。否则，S 提取出 A 的秘密密钥 $p_A=x_{AS}-p_{S_1}-\gamma_{A_2}$，$B$ 的秘密密钥 $p_B=x_{BS}-p_{S_2}-\gamma_{B_2}$，并计算 $k_{SA}=p_A\cdot s_1$，$k_{SB}=p_B\cdot s_2$，$\sigma_{SA}=\mathrm{Rec}(k_{SA},\omega_{SA})$，$\sigma_{SB}=\mathrm{Rec}(k_{SB},\omega_{SB})$，生成 $y_{SA}=p_B+H_3(\sigma_{SA})$，$y_{SB}=p_A+H_3(\sigma_{SB})$。然后，$S$ 将 $\langle y_{SA},y_{SB},x_{BS}\rangle$ 发送给 A，将 $\langle y_{SA},y_{SB},x_{AS}\rangle$ 发送给 B。

5) 第四次响应。收到来自服务器 S 的消息 $\langle y_{SA},y_{SB},x_{AS}\rangle$ 后，B 首先对消息进行检查，如果 $y_{SA},y_{SB},x_{AS}\notin R_q$，则 B 中止协议。否则，B 提取出 A 的秘密密钥 $p_A=y_{SB}-H_3(\sigma_{BS})$，从而计算 $k_B=p_A\cdot s_B$，得到用于协调的信号值 $\omega=\mathrm{HelpRec}(k_B)$，协调值 $k=\mathrm{Rec}(k_B,\omega)$，生成最终的会话密钥 $\mathrm{SK}_B=H_3(\mathrm{ID}_A,\mathrm{ID}_B,\mathrm{ID}_S,x_{AS},x_{BS},y_{SA},y_{SB},\omega,k)$，并将信号值 ω 发送给 A。

6) 协议完成。收到来自 S 和 B 的消息 $\langle y_{SA},y_{SB},x_{BS},\omega\rangle$ 后，A 提取出 B 的秘密密钥 $p_B=y_{SA}-H_3(\sigma_{AS})$，从而计算 $k_A=p_B\cdot s_A$，根据信号值 ω 和恢复函数 Rec 计算出协调值 $k=\mathrm{Rec}(k_A,\omega)$，获得会话密钥 $\mathrm{SK}_A=H_3(\mathrm{ID}_A,\mathrm{ID}_B,\mathrm{ID}_S,x_{AS},x_{AS},x_{BS},y_{SA},y_{SB},\omega,k)$。

公共参数: 与文献[13-14,16-17]不同，RLWE-3PAKE 方案并不直接在 R_q 上随机选取公共参数 a。服务器 S 先随机选择定义为 $\mathrm{seed}\leftarrow\{0,1,\ldots,255\}^{32}$ 的种子。根据种子和 SHAKE−128 函数，每个客户端各自将 seed 扩展生成相同的固定公共环元素 $a\in R_q$。这种方式可以避免不诚实的参与方选择特定构造的 a，防止敌手通过陷门攻击和 all-for-the-price- of-one 攻击猜测出协议参与方的秘密值。

误差分布: 在协议[17]中，错误值是根据离散高斯分布生成的。进行离散高斯分布采样需要大表格和高精度计算，会导致效率明显降低。文献[15]指出，使用中心二项分布替代相应参数的离散高斯分布不会显著降低其安全性，可提高协议运行效率，并有效防止计时攻击等问题。因此本文选择中心二项分布对秘密值、错误值进行采样。

Client A		Server S		Client B
Input B, pw_A	$\xrightarrow{ID_A,ID_B}$	$\mathrm{seed}\leftarrow\{0,1,\ldots,255\}^{32}$ $a\leftarrow\mathrm{Parse}(\mathrm{SHAKE}-128(\mathrm{seed}))$ $\langle\gamma'_{A_1},\gamma_{A_2}\rangle=\langle-H_1(pw_A),H_2(pw_A)\rangle$ $\langle\gamma'_{B_1},\gamma_{B_2}\rangle=\langle-H_1(pw_B),H_2(pw_B)\rangle$		Input A, pw_B
Sample $s_A,e_A\leftarrow\psi_k^n$ $\gamma_{A_1}=H_1(pw_A)$ $\gamma_{A_2}=H_2(pw_A)$		Sample $s_1,s_2,e_1,e_2,e_{SA},e_{SB}\leftarrow\psi_k^n$ $p_{S_1}=as_1+e_1$ $p_{S_2}=as_2+e_2$ $m_{S_1}=p_{S_1}+\gamma'_{A_1}$		Sample $s_B,e_B\leftarrow\psi_k^n$ $\gamma_{B_1}=H_1(pw_B)$ $\gamma_{B_2}=H_2(pw_B)$
Abort if $m_{S_1},m_{S_2}\notin R_q$ $p_{S_1}=m_{S_1}+\gamma_{A_1}$ $p_A=as_A+e_A$ $k_{AS}=p_{S_1}\cdot s_A$ $\omega_{AS}=\mathrm{HelpRec}(k_{AS})$ $\sigma_{AS}=\mathrm{Rec}(k_{AS},\omega_{AS})$ $x_{AS}=p_A+p_{S_1}+\gamma_{A_2}$	$\xleftarrow{m_{S_1},m_{S_2}}$ $\xrightarrow{x_{AS},\omega_{AS}}$	$m_{S_2}=p_{S_2}+\gamma'_{B_1}$ Abort if $x_{AS},x_{BS}\notin R_q$ $p_A=x_{AS}-\gamma_{A_2}-p_{S_1}$ $p_B=x_{BS}-\gamma_{B_2}-p_{S_2}$ $k_{SA}=p_A\cdot s_1$ $k_{SB}=p_B\cdot s_2$ $\sigma_{SA}=\mathrm{Rec}(k_{SA},\omega_{AS})$ $\sigma_{SB}=\mathrm{Rec}(k_{SB},\omega_{BS})$ $y_{SA}=p_B+H_3(\sigma_{SA})$ $y_{SB}=p_A+H_3(\sigma_{SB})$	$\xrightarrow{m_{S_1},m_{S_2}}$ $\xleftarrow{x_{BS},\omega_{BS}}$	Abort if $m_{S_1},m_{S_2}\notin R_q$ $p_{S_2}=m_{S_2}+\gamma_{B_1}$ $p_B=as_B+e_B$ $k_{BS}=p_{S_2}\cdot s_B$ $\omega_{BS}=\mathrm{HelpRec}(k_{BS})$ $\sigma_{BS}=\mathrm{Rec}(k_{BS},\omega_{BS})$ $x_{BS}=p_B+p_{S_2}+\gamma_{B_2}$
Abort if $y_{SA},y_{SB},x_{BS}\notin R_q$ $p_B=y_{SA}-H_3(\sigma_{AS})$ $k_A=p_B\cdot s_A$ $k=\mathrm{Rec}(k_A,\omega)$ $\mathrm{SK}_A=H_4(\mathrm{ID}_A,\mathrm{ID}_B,\mathrm{ID}_S,x_{AS},x_{BS},y_{SA},y_{SB},\omega,k)$	$\xleftarrow{y_{SA},y_{SB},x_{BS}}$ $\xleftarrow{\omega}$		$\xrightarrow{y_{SA},y_{SB},x_{AS}}$	Abort if $y_{SA},y_{SB},x_{AS}\notin R_q$ $p_A=y_{SB}-H_3(\sigma_{BS})$ $k_B=p_A\cdot s_B$ $\omega=\mathrm{HelpRec}(k_B)$ $k=\mathrm{Rec}(k_B,\omega)$ $\mathrm{SK}_B=H_4(\mathrm{ID}_A,\mathrm{ID}_B,\mathrm{ID}_S,x_{AS},x_{BS},y_{SA},y_{SB},\omega,k)$

图 3　基于 RLWE 的三方口令认证密钥交换协议

Figure 3　The RLWE-based three-party password authenticated key exchange

误差协调机制: 本文采用 Newhope 方案中的误差协调机制, 使用 $\tilde{D}_4$ 格解码方法进行错误协调, 相比于丁式误差协调、Peikert 式误差协调, 该方法容错率更高, 可显著缩小模数、降低通信量。根据引理 1, 当近似密钥满足 $\| k_v - k_w \|_1 \le (1-1/2^r)\cdot q - 2$, 则可计算出一致的协调值 σ。信号值 ω 与协调值 σ 是相互独立的。即使攻击者获得了 ω, 也无法分辨 σ 与均匀随机数。因此保证了错误协调机制的安全性和最终生成会话密钥的随机均匀性。

参数选择: 由于安全度与维度、错误值、模数有关, 如果用于生成误差的中心二项分布参数不变, 降低模数也可以显著提高量子安全度。因此, 在进行参数选择时, 需要平衡维度、模数、标准差、错误率, 尽可能在保证正确性的情况下提高量子安全度。考虑到前向保密性和实现效率, 本文选择维度 $n=1024$、标准差 $\beta=\sqrt{16/2}$。由于 NTT 算法可加速多项式计算, 因此本文选择了可用于 NTT 实现、满足 $q \equiv 1 \bmod 2n$ 的最小素模数 $q=12289$。模数越小, 密钥尺寸越小, 计算效率和通信复杂度越低。

相互认证: 客户端 i 持有口令 pw_i, 其中 $i \in \{A, B\}$。在 RLWE-3PAKE 协议中, 口令的明文仅为各参与者自己分别持有, 口令验证值仅为可信服务器秘密持有。假设敌手伪造客户端 B 的身份与诚实参与者进行交互。由于不知正确口令 pw_B 的敌手无法计算出正确的 p_{S_2} 和 k_{SA}, 因此不能与服务器生成一致的 $\sigma_{BS}=\sigma_{SB}$, 也不能与客户端计算出相同的协调值 $k=k'$。因此, 只有通过身份认证的用户可以生成正确的会话密钥。

3.3 正确性分析

根据 2.2 节定义的误差协调机制, 如果两个近似密钥的偏差满足误差容错距离范围, 则可以根据信号值, 从“小误差”中将近似密钥恢复成相同的会话密钥。

定理 3. 设三个参与者 A、B、S 诚实地执行协议以建立会话密钥。令 n 为多项式维度, q 为模数, $\beta=\sqrt{k/2}$ 为中心二项分布 ψ_k 的标准差。如果能同时满足 $\| k_{AS} - k_{SA} \|_1 \le 3q/4-2$, $\| k_{BS} - k_{SB} \|_1 \le 3q/4-2$ 和 $\| k_A - k_B \|_1 \le 3q/4-2$, 则 A、B 能以压倒性概率恢复出相同的会话密钥, 即得到 $\mathrm{Rec}(k_A, \omega) = \mathrm{Rec}(k_B, \omega)$。

证明. 为证明 3PAKE 协议正确性, 只需证明 $\mathrm{Rec}(k_A, \mathrm{HelpRec}(k_B)) = \mathrm{Rec}(k_B, \mathrm{HelpRec}(k_B))$ 即可。根据协议, 可得

$$\begin{aligned} k_{AS} - k_{SA} &= p_{S_1}\cdot s_A - p_A \cdot s_1 \\ &= s_A e_1 - s_1 e_A \\ k_{BS} - k_{SB} &= p_{S_2}\cdot s_B - p_B \cdot s_2 \\ &= s_B e_2 - s_2 e_B \\ k_A - k_B &= p_B \cdot s_A - p_A \cdot s_B \\ &= s_A e_B - s_B e_A \end{aligned}$$

为节约通信量, 协议选取离散化比特数 $r=2$, 协调信息在每个维度只用 2 比特表示。根据引理 1, 当 $\| k_{AS} - k_{SA} \|_1 \le 3q/4-2$ 且 $\| k_{BS} - k_{SB} \|_1 \le 3q/4-2$ 时, 可得到协调值 $\sigma_{AS}=\sigma_{SA}$ 和 $\sigma_{BS}=\sigma_{SB}$。客户端 A 根据 σ_{AS} 获得正确的秘密密钥 p_B, 客户端 B 由 σ_{BS} 获得秘密密钥 p_A。如果满足 $\| k_A - k_B \|_1 \le 3q/4-2$, 则两客户端能恢复出相同的 k。文中选择 $q=12289$, $n=1024$, $k=16$, 根据文献[15]引理 D.4 所证, 可计算出该参数下密钥协商失败的概率小于 2^{-61}。

4 安全性分析

本节通过引入一系列协议 $P_0, ..., P_5$, 对方案的安全性进行了证明。论文将敌手攻击成功的优势归约至解决 DRLWE 数学难题的困难性和在线字典攻击的优势, 从而证明协议满足 AKE 安全。

4.1 安全性证明

定理 4. 令 P=RLWE-3PAKE 为图 1 所示协议。口令字典 D 的大小为 $|D|$。假设时间 t 内敌手 $\mathcal{A}$ 分别进行了 q_{se}、q_{ex}、q_{re}、q_{co}、q_{ro} 次 Send、Execute、Reveal、Corrupt 和随机预言机查询。令 $t' = O(t + (q_{\mathrm{se}} + q_{\mathrm{ex}} + q_{\mathrm{ro}})t_{\exp})$, 敌手攻击 RLWE-3PAKE 协议成功的优势为

$$\begin{aligned} \mathrm{Adv}_p^{\mathrm{ake}}(\mathcal{A}) \le O(1/|D|) + O(&\mathrm{Adv}_{R_q}^{\mathrm{DRLWE}}(t', q_{\mathrm{ro}}) \\ &+ \mathrm{Adv}_{R_q}^{\mathrm{PWE}}(t', q_{\mathrm{ro}}) + \frac{(q_{\mathrm{se}}+q_{\mathrm{ex}})(q_{\mathrm{ro}}+q_{\mathrm{se}}+q_{\mathrm{ex}})}{q^n}) \end{aligned}$$

证明. 为证明定理 4, 本文使用了一系列与 P 有关的协议 $P_0, ..., P_5$, 其中 $P=P_0$, P_5 考虑了在线字典猜测攻击。通过定义以下协议, 本节将证明:

$$\mathrm{Adv}_{P_0}^{\mathrm{ake}}(\mathcal{A}) \le \mathrm{Adv}_{P_1}^{\mathrm{ake}}(\mathcal{A}) + \varepsilon_1 \le ... \le \mathrm{Adv}_{P_5}^{\mathrm{ake}}(\mathcal{A}) + \varepsilon_5$$

其中 $\varepsilon_1, ..., \varepsilon_5$ 是可忽略的值。敌手 $\mathcal{A}$ 赢得游戏的优势可归约到在线字典攻击成功的优势。本文假设 q_{ro} 和 $q_{\mathrm{se}}+q_{\mathrm{ex}}$ 均大于等于 1, 随机预言机 $H_l(\cdot)$ 输出 R_q 上的随机值, 其中 $l \in \{1, 2, 3\}$。

协议 P_0. P_0 是协议 P 的原型。

协议 P_1. 与 P_0 不同, 协议 P_1 的 $H_l(\cdot)$ 查询不再输

出 R_q 上的随机值, 而是返回满足 $as+e\in R_q$ 的环元素, 其中 $s, e\leftarrow\psi_k^n$。P_1 分别通过维持哈希表 $\wedge_{H_l}$ 和 $\wedge_{H_4}$ 来模拟随机预言机查询 $H_l(\cdot), H_4(\cdot)$。

令 m 为哈希询问的输入, c 为其输出。在进行随机预言机查询 $H_l(m)$ 时, 如果哈希表 $\wedge_{H_l}$ 中已存有 (m, c) 的记录, 则模拟器直接返回 c 的值。否则, 模拟器从分布 ψ_k^n 上随机选取 s_h, e_h, 返回 R_q 上的均匀随机环元素 $c=as_h+e_h$, 并将 (m, c) 的值增加到哈希表 $\wedge_{H_l}$ 中。

在进行随机预言机查询 $H_4(m)$ 时, 如果哈希表 $\wedge_{H_4}$ 中已存有 (m, c) 的记录, 则模拟器直接返回 c 的值。否则, 模拟器随机选取 $c\in\{0, 1\}^\lambda$, 返回 c, 并将 (m, c) 的值增加到哈希表 $\wedge_{H_4}$ 中。

推论 1. 对于任意敌手 $\mathcal{A}$,

$$\mathrm{Adv}_{p_0}^{\mathrm{ake}}(\mathcal{A})\le\mathrm{Adv}_{p_1}^{\mathrm{ake}}(\mathcal{A})+\mathrm{Adv}_{R_q}^{\mathrm{DRLWE}}(t', q_{\mathrm{ro}})$$

证明. 在 DRLWE 假设下, 环元素 $c=as_h+e_h$ 与随机值 $c'\in R_q$ 是计算不可区分的。因此, 除非敌手能以不可忽略的概率解决 DRLWE 问题, 否则区分协议 P_1 与 P_0 的概率是可忽略的。

协议 P_2. P_2 与协议 P_1 的区别在于, 如果诚实参与者随机选择的 $\langle m_{S_1}, m_{S_2}, x_A, x_B, y_{SB}, y_{SA}\rangle$ 的值已被先前的查询揭露过并使用过, 则 P_2 中止。

推论 2. 对于任意敌手 $\mathcal{A}$,

$$\mathrm{Adv}_{P_1}^{\mathrm{ake}}(\mathcal{A})\le\mathrm{Adv}_{P_2}^{\mathrm{ake}}(\mathcal{A})+\frac{O((q_{\mathrm{se}}+q_{\mathrm{ex}})(q_{\mathrm{ro}}+q_{\mathrm{se}}+q_{\mathrm{ex}}))}{q^n}$$

证明. 令事件 E 表示当前 Send、Execute 或者随机预言机查询得到的 $\langle m_{S_1}, m_{S_2}, x_A, x_B, y_{SB}, y_{SA}\rangle$ 里一个或多个环元素的值, 已在先前的询问中被揭露过, 且这些值已作为输入被发送并使用过。设敌手最多分别进行 q_{se}、q_{ex}、q_{ro} 次 Send、Execute 和随机预言机查询。环 R_q 上的元素有 n 个系数, 每个系数可取 q 个不同值, 因此环元素最多有 q^n 种组合。当前询问中生成的 $\langle m_{S_1}, m_{S_2}, x_A, x_B, y_{SB}, y_{SA}\rangle$ 里的某个环元素的值与先前 Send、Execute 和随机预言机询问中已揭露过的值相同的概率为 $\frac{q_{\mathrm{se}}+q_{\mathrm{ex}}+q_{\mathrm{ro}}}{q^{\mathrm{n}}}$。如果事件 E 不发生, 也必须要有 $q_{\mathrm{se}}+q_{\mathrm{ex}}$ 个独特的值。因此, $\langle m_{S_1}, m_{S_2}, x_A, x_B, y_{SB}, y_{SA}\rangle$ 中的任意一个或多个元素的值不独特的概率为

$$\frac{O((q_{\mathrm{se}}+q_{\mathrm{ex}})(q_{\mathrm{ro}}+q_{\mathrm{se}}+q_{\mathrm{ex}}))}{q^n}$$

协议 P_3. 协议 P_3 与 P_2 的区别在于敌手 $\mathcal{A}$ 是否在 Corrupt 查询之前得到了会话密钥。

推论 3. 对于任意敌手 $\mathcal{A}$,

$$\mathrm{Adv}_{P_2}^{\mathrm{ake}}(\mathcal{A})\le\mathrm{Adv}_{P_3}^{\mathrm{ake}}(\mathcal{A})+2\mathrm{Adv}_{R_q}^{\mathrm{DRLWE}}(t', q_{ro})+2\mathrm{Adv}_{R_q}^{\mathrm{PWE}}(t', q_{ro})$$

证明. 令事件 E 为敌手在 Corrupt 查询之前就得到了会话密钥 SK=$H_3(\mathrm{ID}_A, \mathrm{ID}_B, \mathrm{ID}_S, x_A, x_B, y_{SA}, y_{SB}, \omega, k)$。可以通过敌手 $\mathcal{A}$, 构造用于解决 PWE 假设的区分器 $\mathbb{D}$, 模拟协议的运行。对于输入 (a, X, Y, ω), 设 $Y=as_y+e_y$, $\mathbb{D}$ 需要找到协调值 $\sigma=\tau(X, s_y)$。$\mathbb{D}$ 模拟运行协议 P_3, 与 P_2 相比有着以下区别:

1) 在 Execute(Π_A^i, Π_B^j, Π_S^k) 查询中, $\mathbb{D}$ 随机选择 $s_f, e_f, s_{ff}, e_{ff}\leftarrow\psi_k^n$, 设置 $y_{SB}=X+(as_f+e_f)$, $p_B=Y+(as_{ff}+e_{ff})$, 并选择 $\omega=\{0, 1, 2, 3\}^n$。

2) 当敌手 $\mathcal{A}$ 完成协议且成功完成 Test(Π_U^i) 测试时, 根据随机预言机 $H_3(\cdot)$ 查询中返回的值 $H_3(\sigma_{BS})=as_h+e_h\in R_q$, 区分器 $\mathbb{D}$ 可以计算:

$$\begin{aligned}k_B&=p_A(s_y+s_{ff})\\&=(y_{SB}-H_3(\sigma_{BS}))s_B\\&=(X+(as_f+e_f)-(as_h+e_h))(s_y+s_{ff})\\&=Xs_y+(a(s_f-s_h)+(e_f-e_h))s_y\\&\quad+(X+(as_f+e_f)-(as_h+e_h))s_{ff}\\&\approx Xs_y+Y(s_f-s_h)+(X+(as_f+e_f)-(as_h+e_h))s_{ff}\end{aligned}$$

因此, 可以得到 $Xs_y=k_B-Y(s_f-s_h)-(X+(as_f+e_f)-(as_h+e_h))s_{ff}$。且 $\sigma'=\mathrm{Rec}(k_B-Y(s_f-s_h)-(X+(as_f+e_f)-(as_h+e_h))s_{ff}, \omega)$。最后, 将 σ' 添加至可能为 $\tau(X, s_y)$ 的值列表中。

在协议 P_2 中, 模拟器使用真实的 $y_{SB}=as_{SB}+e_{SB}$。在协议 P_3 中, 模拟器使用随机生成的 $y_{SB}=X+(as_f+e_f)$ 代替真实的 $y_{SB}=as_{SB}+e_{SB}$。若要成功区分二者, 则需要解决 DRLWE 问题或者 PWE 问题。即如果敌手能以不可忽略的优势解决 DRLWE 问题, 或者事件 E 发生并且区分器 $\mathbb{D}$ 可以将正确的 σ' 添加至 $\tau(X, s_y)$ 的值列表, 则协议 P_3 与 P_2 是可区分的。但是, 由于敌手的运行时间 t' 是有限的, 查询次数也是有限的, 根据 PWE 假设和 DRLWE 问题的困难性,

可知区分协议 P_3 与 P_2 的优势可忽略。

协议 P_4. P_4 与 P_3 不同之处在于敌手 $\mathcal{A}$ 是否进行了离线字典攻击。

推论 4. 对于任意敌手 $\mathcal{A}$,

$$\mathrm{Adv}_{P_3}^{\mathrm{ake}}(\mathcal{A}) \le \mathrm{Adv}_{P_4}^{\mathrm{ake}}(\mathcal{A}) + 2\mathrm{Adv}_{R_q}^{\mathrm{DRLWE}}(t', q_{ro}) + 2\mathrm{Adv}_{R_q}^{\mathrm{PWE}}(t', q_{ro})$$

证明. 令事件 E 表示敌手成功进行了离线字典攻击, 则可利用敌手 $\mathcal{A}$ 构造用于解决 PWE 假设的区分器 $\mathbb{D}$, 模拟协议的执行。输入 (a, X, Y, ω), 设置 $Y = as_y + e_y$, $\mathbb{D}$ 模拟执行协议 P_4, 与 P_3 相比有着以下区别:

1) 在 $\mathrm{Execute}(\Pi_A^i, \Pi_B^j, \Pi_S^k)$ 查询中, $\mathbb{D}$ 设置 $m_{S_1} = X + (as_f + e_f)$, $p_A = Y + (as_{ff} + e_{ff})$, 其中 s_f, s_{ff}, e_f, $e_{ff} \leftarrow \psi_k^n$, 并选择 $\omega \in \{0, 1, 2, 3\}^n$。

2) 当敌手 $\mathcal{A}$ 完成协议, 并离线猜测了口令 pw_A 时, 随机预言机查询中返回 $\gamma_{A_1} = H_1(\mathrm{pw}_A) = as_h + e_h \in R_q$。则 $\mathbb{D}$ 可以计算:

$$\begin{aligned} k_{AS} &= p_{S_1} \cdot s_A \\ &= (m_{S_1} + \gamma_{A_1}) \cdot s_A \\ &= (X + as_f + e_f + as_h + e_h)(s_y + s_{ff}) \\ &= Xs_y + (a(s_f + s_h) + (e_f + e_h))s_y \\ &\quad + (X + as_f + e_f + as_h + e_h)s_{ff} \\ &\approx Xs_y + Y(s_f + s_h) + (X + as_f + e_f + \gamma_{A_1})s_{ff} \end{aligned}$$

因此, 可以得到 $Xs_y = k_{AS} - (Y(s_f + s_h) + (X + as_f + e_f + \gamma_{A_1})s_{ff})$, 且 $\sigma' = \mathrm{Rec}(k_{AS} - (Y(s_f + s_h) + (X + as_f + e_f + \gamma_{A_1})s_{ff}), \omega)$。最后, 将 σ' 添加到 $\tau(X, s_y)$ 的可能值列表。

在协议 P_3 中, 模拟器使用真实的 $m_{s_1} = as_{m_1} + e_{m_1}$。在协议 P_4 中, 模拟器使用随机构造的 $m_{S_1} = X + (as_f + e_f)$ 代替真实的 $m_{s_1} = as_{m_1} + e_{m_1}$。如果能解决 DRLWE 问题或者 PWE 问题, 则可成功区分二者。因此, 如果敌手能以不可忽略的优势解决 DRLWE 问题, 或事件 E 发生并且区分器 $\mathbb{D}$ 可以将正确的 σ' 添加至 $\tau(X, s_y)$ 的值列表, 则协议 P_4 与 P_3 可区分。由于敌手的运行时间 t' 和查询次数有限, 根据 DRLWE 和 PWE 问题的困难性, 可知区分协议 P_4 与 P_3 的优势是可忽略的。

协议 P_5. P_5 与 P_4 是相似的, 但是 P_5 中存在一个敌手 $\mathcal{A}$ 不能获得的内部口令预言机。预言机持有所有的口令并且接受来自敌手 $\mathcal{A}$ 的在线字典攻击。如果 $\mathcal{A}$ 猜到了正确的 $\mathrm{pw}' = \mathrm{pw}_U$, 其中 $U \in \{A, B\}$, 则模拟器返回 1, 否则返回 0。

推论 5. 对于任意敌手 $\mathcal{A}$,

$$\mathrm{Adv}_{P_4}^{\mathrm{ake}}(\mathcal{A}) = \mathrm{Adv}_{P_5}^{\mathrm{ake}}(\mathcal{A}) \le O(1/|D|)$$

证明. 显然, P_5 与 P_4 是完美不可区分的。在线字典攻击仅允许敌手猜测 q_{se} 次口令。令事件 E 为敌手成功在线猜测到了新鲜会话的口令。设口令字典的大小为 $|D|$, 则敌手得到正确口令的概率 $P(E) \le q_{\mathrm{se}}/|D|$。对于新鲜会话 Π_U^i, 如果事件 E 不发生, 由于敌手 $\mathcal{A}$ 无法获得 SK_U^i, 因此 $\mathcal{A}$ 进行 $\mathrm{Test}(\Pi_U^i)$ 测试并成功输出 $b^* = b$ 从而赢得游戏的概率为 $1/2$。可以计算出, $\Pr(\mathrm{Succ}_{P_5}^{\mathrm{ake}}(\mathcal{A})) \le \Pr(E) + \Pr(\mathrm{Succ}_{P_5}^{\mathrm{ake}}(\mathcal{A})|E) + \Pr(\mathrm{Succ}_{P_5}^{\mathrm{ake}}(\mathcal{A})|\neg E) \le \Pr(E) + \frac{1}{2}(1 - \Pr(E)) \le \frac{q_{\mathrm{se}}}{2|D|} + \frac{1}{2}$, 敌手攻击 P_5 成功的优势为 $\mathrm{Adv}_{P_5}^{\mathrm{ake}}(\mathcal{A}) = 2\Pr(\mathrm{Succ}_{P_5}^{\mathrm{ake}}(\mathcal{A})) - 1 = O(1/|D|)$。

根据推论 1-5, 定理 4 得证。根据 DRLWE 问题的困难性, 解决 PWE 和 DRLWE 的优势是可忽略的, 且 $O(1/|D|)$ 和 $\frac{O((q_{\mathrm{se}} + q_{\mathrm{ex}})(q_{\mathrm{ro}} + q_{\mathrm{se}} + q_{\mathrm{ex}}))}{q^n}$ 的值也是可忽略的, 因此 $\mathrm{Adv}_P^{\mathrm{ake}}(\mathcal{A}) \le \varepsilon$, 其中 ε 表示可忽略的值, 协议满足 AKE 安全。

4.2 安全属性

相互认证安全: 在 RLWE-3PAKE 协议中, 口令的明文由各参与者自己分别持有, 可信服务器仅持有口令验证值。假设敌手伪造客户端 B 的身份与各参与者进行交互。由于不知正确口令 pw_B 的敌手无法计算出正确的 p_{S_2} 和 p_A, 不能与服务器生成一致的 $\sigma_{BS} = \sigma_{SB}$, 也不能与客户端计算出相同的协调值 $k = k'$, 所以无法被其他参与方认证。因此, 我们的协议可以提供相互身份验证的安全性。

前向安全: 在 RLWE-3PAKE 协议中, 每次新的会话都会随机生成一些新的临时密钥。即使参与方相同、口令相同, 由于新秘密值和新错误值是随机的, 因此计算出来的新会话密钥也是随机的。即每次共享的会话密钥都独立于其他会话的会话密钥。由于本方案的前向安全性建立在敌手不知已完成密钥协商会话中临时秘密 s_i 的前提上, 因此协议可满足弱完美前向安全。

已知会话密钥安全: 各参与方使用临时密钥建立

会话密钥, 不同会话中随机生成的临时密钥不同, 各个会话的共享密钥都是相互独立的。即使敌手获得了先前的某个共享密钥, 其他的会话也仍然是安全的。

抵御口令猜测攻击: 如推论 5-6 所示, 离线和在线字典攻击的可能性可以忽略不计。对于离线对手, 由于未知 p_{S_1}、p_{S_2}、p_A、p_B, 即使进行了离线字典攻击, 除非可以解决 PWE、DRLWE 问题, 否则很难检查猜测结果的正确性。对于在线对手, 攻击次数被限制为 q_{se} 次, 远小于字典大小 $|D|$, 因此成功的可能性也可以忽略不计。因此, 我们的协议可以抵抗口令猜测攻击。

5 性能分析

本节介绍了论文的参数选择, 并分析了 RLWE-3PAKE 协议的安全度、通信复杂度和运行时间。

5.1 实验环境及参数选择

实验运行于处理器 Intel(R) Core(TM) i5-4590T @ 2.00GHz、内存 12GB、操作系统 Ubuntu 20.04.1 上。在基于 RLWE 问题的密码算法中, 多项式计算是最耗时的操作之一。NFLlib(NTT-based Fast Lattice Library[30])是一种对 NTT 运算进行优化的加速算法, 可提高多项式计算效率。通过 C++上 NFLlib 算法实现协议, 需要选择适合 NTT 运算的模数(要求 $q \equiv 1 \bmod 2n$)。同时, 为确保协议正确性和后量子安全性, 本方案选择多项式维度 $n=1024$、模数 $q=12289$、中心二项分布的参数 $k=16$。

5.2 各操作运行时间

本方案将协议中使用的各项操作分别运行 10000 次, 取平均值记录为实验结果。表 1 给出了方案算法具体操作的运行时间(单位: μs)。可以看出, 采用 NFLlib 算法对多项式运算进行优化后, 协议中运行时间最短的为 NTT 域上两个环元素的加减计算, 其次为多项式乘法和多项式乘加计算。最耗时的操作是公共环元素 a 的生成, 这是由于为了避免陷门攻击和 all-for-the-price-of-one 攻击, 需要先随机生成 32 字节的种子, 并使用伪随机数生成器根据种子计算哈希值, 从而得到公共参数, 其过程比较复杂, 因此运行时间最长。

表 1 协议各操作运行时间(单位: μs)

Table 1 Running time of each operation in the protocol (μs)

操作	T_{set}	T_{error}	T_{mul}	T_{muladd}	T_{add}	T_{sub}
时间	18.683	10.983	0.5	0.8	0.2	0.2
操作	$T_{helprec}$	T_{rec}	T_{rh}	T_{h}	T_{NTT}	T_{iNTT}
时间	5.189	4.373	15.896	3.704	13.3	14.2

注: T_{set} 为生成公共环元素 a 的运行时间, T_{error} 为在中心二项分布上进行随机错误值采样的运行时间, T_{mul} 为两个环元素相乘的运行时间, T_{muladd} 为两个环元素乘再相加的运行时间, T_{add} 为两个环元素相加的运行时间, T_{sub} 为两个环元素相减的运行时间, $T_{helprec}$ 为使用协调函数生成信号值和协调值的运行时间, T_{rec} 为恢复出协调值的运行时间, T_{h} 为生成会话密钥的哈希函数运行时间; T_{NTT} 为将环元素转换到 NTT 域元素的运行时间, T_{iNTT} 为将 NTT 域元素转换到环元素的运行时间, T_{rh} 为相关随机数生成运算的运行时间

5.3 实验结果分析与比较

在基于格上困难问题构造的口令认证密钥交换协议中, 本文选择最为典型的基于 RLWE 的两方 PAKE 协议[17]、三方 PAKE 协议[26]在参数、效率和性能上进行了对比。以上方案在表格中分别用 Ding[17]、Liu[26]表示。

5.3.1 参数比较

在参数选择方面, 基于 RLWE 问题的 Ding 等人的两方 APKE 协议[17]选取参数 $n=1024$、$q=2^{32}-1$、$\beta=8/\sqrt{2\pi}$, 采用离散高斯分布和丁式误差协调机制。基于 RLWE 问题的 Liu 等人的三方 PAKE 协议[26]设置参数为维度 $n=1024$、模数 $q=2^{32}-1$、标准差 $\beta=8$, 使用离散高斯分布和 Peikert 式误差协调方式。表 2 给出了本文与文献[17,26]在数学困难假设、通信方、参数选择等方面的对比。可以看到, 本方案的模数远小于 Ding[17]、Liu[26]的协议。

5.3.2 性能比较

表 3 给出了本文与文献[17,26]在效率和性能上的对比。与 Ding 等人提出的 2PAKE 协议[17]相比, 本文方案通过在多项式采样、多项式计算和误差协调的时间上进行优化, 达到了 9 倍的加速。一方面, 由于本文方案在进行误差协调时, 通过采用 $\tilde{D}_4$ 格解码方式, 增加了容错距离, 将模数从 32 比特缩小至 14 比特, 降低了误差协调时间。另一方面, 由于本文方案模数远小于方案[17], 通过选取合适的参数, 再结合 C++上的 NFLlib 库, 采用 NTT 算法提高了多项式计算的效率。此外, 本文采用更高效实用的中心二项

分布替代离散高斯分布, 降低了采样时间。结合以上优化方式, 整个协议的运行时间和性能都得到了提高。注意到本文通信量高于文献[17]的两方 RLWE-PPK 协议, 这是因为本文的方案涉及三方通信, 更适用于用户-服务器-用户的实际应用场景, 因此也需要更多的通信轮数。

与 Liu 等人构造的三方 PAKE 协议[26]相比, 本文方案也从多项式采样、多项式计算、误差协调方式、协议结构和通信量上进行了优化。同样地, 本文采用更高效的中心二项分布替代方案[26]中的离散高斯分布, 使用更快速的 NTT 算法——NFL 替代 FFT 算法对多项式计算进行加速。为使可允许的模数更小, 基于 $\tilde{D}_4$ 格解码的误差协调方式增加了容错范围, 从每 4 个比特中协调出 1 个比特。文献[15]引理 D.4 指出, 当选取参数 $n=1024$、$q=12289$、$k=16$ 时, 密钥协商失败的概率低于 2^{-61}。相对于协议[26]的 Peikert 式误差协调, $\tilde{D}_4$ 格解码的模数只需 14 比特, 远小于方案[26]使用的 32 比特, 因此提高了误差协调效率。综合以上优化方法, 整个协议的运行效率比[26]中的方案效率提高了 16 倍。

此外, 在认证密钥交换过程中, 涉及的参与方越多, 需要交互的信息也就越多。因此降低通信复杂度也是设计三方认证密钥交换协议的关键点之一。本文在协议结构上也进行了创新, 使用隐式口令认证方式进行三方密钥交换。与 Liu 等人的显式 3PAKE 协议[26]相比, 隐式口令认证方式简化了协议认证结构、减少了通信中的哈希次数和消息内容, 而且本方案采用较小的模数也会显著降低消息中的密钥大小, 因此通信量比[26]减少了 2 倍。

在量子环境下, 威胁最大的攻击方式为 primal 攻击和 dual 攻击。根据文献[15]的 core-sieving 模型, RLWE 问题的复杂度可作为 LWE 问题进行分析。给定 LWE 实例 $(\boldsymbol{M}, \boldsymbol{b}=\boldsymbol{Ms}+\boldsymbol{e})$, $\boldsymbol{M}\in\mathbb{Z}_q^{m\times n}$, primal 攻击定义了格 $\boldsymbol{\Lambda}=\{\boldsymbol{x}\in\mathbb{Z}^{m+n+1}: (\boldsymbol{M}\,|\,\boldsymbol{I}_m\,|\,-\boldsymbol{b})\boldsymbol{x}=\boldsymbol{0} \bmod q\}$, dual 攻击定义了格 $\boldsymbol{\Lambda}'=\{(\boldsymbol{x},\boldsymbol{y})\in\mathbb{Z}^m\times\mathbb{Z}^n: \boldsymbol{M}^t\boldsymbol{x}=\boldsymbol{y} \bmod q\}$。本文分别使用 BKZ 算法寻找 primal 格和 dual 格中的最短向量以解决 LWE 问题, 从而对两种攻击方法的复杂度进行度量。令 g 为 BKZ 算法所需的块维度, 则攻击的复杂度边界约为 $2^{0.265g}$, 安全度为 $0.265g$。在该模型下, 安全度主要与实例的维度、模数、误差分布有关。与文献[17,26]对比, 由于本文方案的维度相同, 误差分布标准差近似, 但模数远小于协议[17,26], 因此安全度更高。实验结果表明, 本协议具有 255 比特的后量子安全性, 可以抵抗这两种量子敌手, 并且完全满足实际应用中对后量子密码算法的安全性需求(后量子安全度 128 比特以上)。

表 2 方案参数比较

Table 2 Comparison of the parameters of the protocols

方案	困难假设	通信方	n	q	β	误差分布	误差协调方式
Ding[17]	RLWE(后量子)	两方	1024	2^{32}-1	$8/\sqrt{2\pi}$	离散高斯分布	丁式
Liu[26]	RLWE(后量子)	三方	1024	2^{32}-1	8	离散高斯分布	Peikert 式
本文	RLWE(后量子)	三方	1024	12289	$\sqrt{8}$	中心二项分布	$\tilde{D}_4$ 格解码式

(注: 多项式环为 $R_q=Z_q[x]/(X^n+1)$, n 为环 R_q 上多项式维度, q 为多项式系数模数, β 为误差分布的标准差)

表 3 方案性能比较(单位: ms)

Table 3 Comparison of the performance of the protocols (ms)

方案	A	B	S	总时间	通信量(byte)	BKZ 块维度	后量子安全度
Ding[17]	4.135	-	4.712	8.847	8328	296	78
Liu[26]	4.396	4.865	7.289	16.550	45824	335	88
本文	0.257	0.466	0.263	0.966	22288	962	255

6 结论

本文基于理想格提出了一种新的隐式三方口令认证密钥交换协议 RLWE-3PAKE, 以解决量子环境下客户端-服务器-客户端通信安全问题。RLWE-3PAKE 基于 RLWE 问题, 采用容错率更高的 $\tilde{D}_4$ 格解码构造错误协调机制, 通过口令提供服务器和客户端之间的身份认证, 最终在客户端之间生成会话密钥。在效率方面, 通过使用快速的误差协调机制 $\tilde{D}_4$, 结合高效的中心二项分布采样, 并采用加速多项式计算过程的 NTT-based Fast Lattice Library 库, 将整个协议的计算效率提高了 9~17 倍。

在安全性方面, 基于格上 RLWE 问题的困难性, 协议达到了 255 比特的后量子安全度。同时, 根据三方环境下的 BPR 模型, 证明协议能够抵抗口令猜测攻击, 并且具备相互认证安全和前向保密性。

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] Rivest R L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems[J]. *Communications of the ACM*, 1978, 21(2): 120-126.

[3] Koblitz N. Elliptic Curve Cryptosystems[J]. *Mathematics of Computation*, 1987, 48(177): 203-209.

[4] Bellovin S M, Merritt M. Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks[C]. *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, 2002: 72-84.

[5] Jablon D P. Strong Password-only Authenticated Key Exchange[J]. *ACM SIGCOMM Computer Communication Review*, 1996, 26(5): 5-26.

[6] Halevi S, Krawczyk H. Public-Key Cryptography and Password Protocols[J]. *ACM Transactions on Information and System Security*, 1999, 2(3): 230-268.

[7] Boyko V, MacKenzie P, Patel S. Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman[M]. Advances in Cryptology — EUROCRYPT 2000. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000: 156-171.

[8] Shor P W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring[C]. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 2002: 124-134.

[9] Grover L K. A Fast Quantum Mechanical Algorithm for Database Search[C]. *The twenty-eighth annual ACM symposium on Theory of Computing*, 1996: 212-219.

[10] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[C]. *The thirty-seventh annual ACM symposium on Theory of computing*, 2005: 84-93.

[11] Lyubashevsky V, Peikert C, Regev O. On Ideal Lattices and Learning with Errors over Rings[J]. *IACR Cryptol EPrint Arch*, 2010, 2012: 230.

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

[13] Ding J T. A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem[J]. *IACR Cryptology EPrint Archive*, 2012, 2012: 688.

[14] Peikert C. Lattice Cryptography for the Internet[M]. Post-Quantum Cryptography. Cham: Springer International Publishing, 2014: 197-219.

[15] Peikert C. Lattice Cryptography for the Internet[J]. *IACR Cryptology ePrint Archive*, 2014, 2014: 70.

[16] Zhang J, Zhang Z F, Ding J T, et al. Authenticated Key Exchange from Ideal Lattices[M]. Advances in Cryptology - EUROCRYPT 2015. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 719-751.

[17] Ding J T, Alsayigh S, Lancrenon J, et al. Provably Secure Password Authenticated Key Exchange Based on RLWE for the Post-Quantum World[M]. Topics in Cryptology - CT-RSA 2017. Cham: Springer International Publishing, 2017: 183-204.

[18] Gao X W, Ding J T, Li L, et al. Efficient Implementation of Password-Based Authenticated Key Exchange from RLWE and Post-Quantum TLS[J]. *Int J Netw Secur*, 2017, 20: 923-930.

[19] Yang Y S, Gu X Z, Wang B, et al. Efficient Password-Authenticated Key Exchange from RLWE Based on Asymmetric Key Consensus[M]. Information Security and Cryptology. Cham: Springer International Publishing, 2020: 31-49.

[20] Joux A. A one round Protocol for Tripartite Diffie-Hellman[J]. *Journal of Cryptology*, 2004, 17(4): 263-276.

[21] Steiner M, Tsudik G, Waidner M. Refinement and Extension of Encrypted Key Exchange[J]. *ACM SIGOPS Operating Systems Review*, 1995, 29(3): 22-30.

[22] Ding Y, Horster P. Undetectable On-Line Password Guessing Attacks[J]. *ACM SIGOPS Operating Systems Review*, 1995, 29(4): 77-86.

[23] Wu Shuhua. Cryptanalysis of a Communication-Efficient Three-Party Password Authenticated Key Exchange Protocol[J]. *Information Sciences*, 2012, 215: 83-96.

[24] Wu Shuhua, Pu Qiong, Wang Shengbao, et al. Cryptanalysis of a communication-efficient three-party password authenticated key exchange protocol[J]. *Information Sciences*, 2012, 215(6): 83-96.

[25] J Yu, H. Li, Y. Tang, et al. Password-based three-party authenticated key exchange protocol from lattices[J]. *Journal on Communications*, 2018, 39(11): 91-101.

[26] Liu C, Zheng Z X, Jia K T, et al. Provably Secure Three-Party Password-Based Authenticated Key Exchange from RLWE[M]. Information Security Practice and Experience. Cham: Springer International Publishing, 2019: 56-72.

[27] 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*, 2015: 553-570.

[28] 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]. *IEEE Symposium on Security and Privacy*, 2015: 553-570.

[29] Krawczyk H. HMQV: A High-Performance Secure Diffie-Hellman Protocol[M]. Advances in Cryptology - CRYPTO 2005. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 546-566.

[30] Aguilar-Melchor C, Barrier J, Guelton S, et al. NFLlib: NTT-Based Fast Lattice Library[M]. Topics in Cryptology - CT-RSA 2016. Cham: Springer International Publishing, 2016: 341-356.

王梓梁 于 2014 年在四川大学信息安全专业获得工学学士学位。现在中国科学院大学网络空间安全专业攻读工学硕士学位。研究领域为网络安全协议。研究兴趣包括: 后量子密码算法、可搜索加密等。Email: wangziliang@.iie.ac.cn

顾小卓 于 2008 年在解放军信息工程大学通信与信息系统专业获得博士学位。现任中国科学院信息工程研究所国家重点实验室高级工程师。研究领域为网络安全协议。研究兴趣包括: 安全协议设计、后量子安全等。Email: guxiaozhuo@iie.ac.cn

任培欣 于 2019 年在南京邮电大学网络工程专业获得学士学位。现在中国科学院信息工程研究所攻读硕士学位。研究领域为后量子密钥交换协议, 研究兴趣包括: 后量子安全、云计算安全。Email: renpeixin@iie.ac.cn