基于RLWE问题的后量子口令认证密钥交换协议

李子臣[1],谢 婷[2,3],张卷美[2]
(1. 北京印刷学院,北京 102600; 2. 北京电子科技学院,北京 100070;
3. 西安电子科技大学通信工程学院,陕西西安 710071)

摘 要: 基于口令的认证密钥交换协议在现代通信网络中有很强的实用性.量子技术的迅速发展使得传统公钥密码体制的安全性面临严峻的形势,基于格理论构造密码系统已成为当前后量子密码研究的热点.本文基于格理论环上误差学习(RLWE)问题,使用Peikert式误差协调机制构造了一个C/S模式下的口令认证密钥交换协议(PAKE),设置了合理的参数保证双方以显著概率得到相同的会话密钥,并使用Java在Eclipse平台上进行了此协议的模拟实现.协议在C/S模式的PAKE安全模型下可证明安全,可抵御量子攻击,与现有的基于格理论设计的PAKE协议相比,通信量较低并且在安全度上有较强的优势,是一种简洁高效的后量子口令认证密钥交换协议.

关键词: 认证密钥交换; 环上误差学习问题; 格; 后量子
中图分类号: TP3 **文献标识码:** A **文章编号:** 0372-2112 (2021)02-0260-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20190101

Post Quantum Password-Based Authentication Key Exchange Protocol Based on Ring Learning with Errors Problem

LI Zi-chen[1], XIE Ting[2,3], ZHANG Juan-mei[2]
(1. *Beijing Institute of Graphic Communication, Beijing* 102600, *China*;
2. *Beijing Electronic Science & Technology Institute, Beijing* 100070, *China*;
3. *School of Telecommunications Engineering, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: Password-based authentication key exchange protocol is highly practical in modern communication networks. The rapid development of quantum technology has made the security of traditional public key cryptosystem face a severe situation. The construction of cryptosystem based on lattice theory has become a hot topic in the research of post-quantum cryptography. The scheme is based on the lattice theory error learning (RLWE) problem, and uses the Peikert error reconciliation mechanism to construct a password authentication key exchange (PAKE) protocol in C/S mode. Reasonable parameters are set to ensure that both parties get the same session key with significant probability, and by using Java to implement PAKE protocol on the Eclipse platform. The security of the protocol is proved under the standard BPR model and can withstand quantum attacks. Compared with the existing PAKE protocol based on lattice theory, the proposed protocol has lower communication and better security. It is a simple and efficient post-quantum password authentication key exchange protocol.

Key words: authenticated key exchange protocol; ring learning with errors; lattice; post quantum

1 引言

随着信息技术和网络技术的飞速发展,信息安全的研究具有重要的理论价值和广泛的实际应用价值.密钥交换协议[1]是信息安全所属的一项重要的研究内容,指两个或多个参与者通过利用其长期私钥和开放网络中所交换的临时消息产生一个共享会话密钥,随后此共享秘密会话密钥被用于安全通信.1976年,Diffie和Hellman首次提出密钥交换[2]的概念,但这一协议无法抵御中间人的攻击,而认证密钥交换(Authenticated

收稿日期:2019-01-16;修回日期:2020-07-17;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61370188);北京市自然科学基金委员会与北京市教育委员会联合资助项目(No.KZ201710015010)

Key Exchange,AKE)协议不仅使通信双方通过协商得到共享会话密钥,且可为双方提供有效认证.

口令认证密钥交换协议(Password Authenticated Key Exchange,PAKE)是 AKE 协议研究领域的一项重要分支,PAKE 协议使得通信参与者只需用一个低熵口令就可在不安全的信道上生成高熵会话密钥,避免了一般的 AKE 协议对于公钥基础设施存在前提的需求. 当今信息网络领域,许多计算机的访问控制大多是使用记忆性的口令认证机制. 根据用户的口令,一方面可以让服务器验证其登录用户身份,另一方面可以在服务器和用户之间建立安全的会话密钥. 这些协议的优点是不需要大量的密钥管理,基于口令的 AKE 协议用户只需记住口令便可实现对服务器安全的访问,在实施过程中具有相对简单,易于管理的优点. 大量的 PAKE 协议已经进入标准化和实用化. PAKE 应用实例包括 PAK 和 PPK [3],Juggling 口令认证密钥交换(J-PAKE)[4]. 在 RFC 使用的 Internet 密钥交换(IKE)协议 6617[5]中的安全预共享密钥(PSK)认证,TLS 协议中的使用的基于椭圆曲线的 J-PAKE 密码套件. 另外,应用实例还有,RFC 2945 中安全远程密码协议(SRP)[6]和加密密钥交换协议(EKE)[7],简单的密码指数密钥交换(SPEKE)[8]等,OpenSSL 也支持 J-PAKE,Firefox Sync 服务器采用 J-PAKE 进行身份验证和密钥交换.

当今量子计算技术的飞速发展,使得基于传统数论困难问题假设的公钥密码学面临安全性能威胁,目前,后量子密码主要包括基于哈希函数的密码算法、基于编码的密码算法、多变量公钥密码算法以及基于格的密码算法等. 2015 年 8 月,美国国家安全局(NSA)宣布将当前联邦政府使用的“密码算法 B 套件”将升级为抗量子密码系统. 2016 年 4 月,美国国家标准局(NIST)在全球范围内展开后量子密码算法的征集工作. 近年来,欧洲国家的“后量子密码”(PQCrypto)和“安全密码”(SAFEcrypto)项目和日本的 CREST 密码数学项目都取得了显著成果. 目前政府、工业界以及相关标准化组织对于实用化的后量子密码系统的需求迫切. 2018 年 4 月 11 – 13 日,美国国家标准与技术研究院(NIST)召开了首届后量子时代公钥密码标准化的国际会议.

基于格的密码体制一般具有线性渐进计算复杂度、可抵御量子攻击的优势,同时具有较好的扩展性,可设计加解密体制、数字签名、密钥交换协议、全同态密码等,被认为是后量子密码算法中最有力的竞争者. 格密码在应用实践方面,美国微软公司于 2016 年 4 月发布了格密码库;2016 年 7 月,美国谷歌公司后量子项目试验中,在其浏览器进行了基于格理论设计的密钥交换协议部署测试. 在后量子时代,设计简洁高效、安全的基于格的 PAKE 协议具有非常重要的理论意义和应用价值.

现阶段基于格理论的密码学已经受到了广泛关注,构造了一系列优秀的加解密方案,数字签名方案以及密钥交换协议,但对于基于格的 PAKE 协议的研究却比较缺乏. 2009 年,Katz 等[9]首次提出了将格理论相关困难问题用于 PAKE 协议的设计,构造了基于格的 CCA 的加密体制和近似平滑投射 Hash 函数,并使用这些组件对 KOY 协议[10]、Gennaro-Lindell[11]协议进行有效的改进,从而得到了第一个基于格理论的 PAKE 协议. 在 2010 年,胡学先[12]等提出了一个具有双向认证,计算效率更高的基于格理论的 PAKE 协议;在 2011 年,DingYi 等[13]将 Katz 等提出的加密体制与近似平滑投射 Hash 函数应用于 Groce-Katz 框架[14],设计出一个基于格理论的 PAKE 协议;在 2017 年 RSA 会议上,文献[15]使用经典的 PAK 和 PPK 的构造形式[15],提出了两个基于 RLWE 问题的口令认证密钥交换协议;同年,在文献[16]中,对文献[15]提出的两个协议进行实现和效率测试,并将其中的 PPK 协议集成到 TLS 协议之中,组成了一个后量子 TLS 协议套件;在 2018 年,Gao 等[17]基于误差协调机制设计了一种远程口令认证密钥交换协议.

本文提出了一个 C/S 模式下的基于格理论 RLWE 问题的口令认证密钥交换协议,客户端只需记忆与服务器共享的口令,服务器端存储通过 NTRU 算法产生的公私钥对. 协议使用 Peikert 提出的误差协调技术,通信双方通过共享口令实现相互认证并通过设置合理的参数保证双方以显著概率得到相同的会话密钥,使用 Java 在 Eclipse 平台上进行了 PAKE 协议的模拟实现. 本文设计的 PAKE 协议的安全性可归约为格理论的 RLWE 问题,并在 PAKE 协议模型下可证明安全,可抵御量子攻击,是一种计算简洁高效的后量子 PAKE 协议.

2　基础知识

2.1　环上带误差学习问题

定义 1[18](环上带误差的学习问题 RLWE)　定义 $\mathbb{Z}$ 上的多项式环,记作 $\mathbb{Z}[x]$;环 $R=\mathbb{Z}[x]/x^n+1$,对于任意正整数 $q\in\mathbb{Z}$,记多项式环 $R_q=\mathbb{Z}_q[x]/x^n+1$. 对于 R 和 R_q 上的任意多项式 y,则 y 的系数向量属于 $\mathbb{Z}^n$ 和 $\mathbb{Z}_q^n$. 对于 $s\in R_q$,A_{s,χ_β} 表示 $(a,as+e)\in R_q\times R_q$ 分布,其中 $a\leftarrow R_q$ 表示 a 随机均匀选自于 R_q,$e\leftarrow\chi_\beta$ 独立于 a,则 RLWE 假设是对于选自于 χ_β 的样本 s,A_{s,χ_β} 与 $R_q\times R_q$ 上的均匀分布是计算不可区分的.

定义 2[19](判定型 RLWE 问题 R-DLWE)　定义判定型 RLWE 为 R-DLWE$_{q,\chi}$,表示以不可忽略的概率优势去区分独立选自于 A_{s,χ_β} 的样本和随机均匀选自于 $R_q\times R_q$ 上的样本.

2.2 格上高斯分布

定义 3(高斯函数及高斯分布) 已知参数 $s>0$,$\boldsymbol{c}\in\mathbb{R}^n$,在 $\mathbb{R}^n$ 的高斯函数定义为 $\forall \boldsymbol{x}\in\mathbb{R}^n$,$\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}\right)$.

$\int_{\boldsymbol{x}\in\mathbb{R}^n}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})\mathrm{d}\boldsymbol{x}=s^n$ 为与高斯函数 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$ 相关的总测度. 由此可得,以参数向量 $\boldsymbol{c}$ 为中心,$s>0$ 的连续高斯分布为 $\forall \boldsymbol{x}\in\mathbb{R}^n$,$D_{s,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{s^n}$.

定义 4(格上的离散高斯分布) 已知格 Λ,参数为任意向量 $\boldsymbol{c}$ 和实数 $s>0$,定义格 Λ 的离散高斯分布为 $\forall \boldsymbol{x}\in\Lambda, D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\frac{D_{s,\boldsymbol{c}}(\boldsymbol{x})}{D_{s,\boldsymbol{c}}(\Lambda)}=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)}$.

其中,$D_{s,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}D_{s,\boldsymbol{c}}(\boldsymbol{x})$,$\rho_{s,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$.

当参数 $s>0$ 足够大时,格 Λ 上的离散高斯分布 $D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})$ 和连续高斯分布 $D_{s,\boldsymbol{c}}(\boldsymbol{x})$ 在很多方面十分接近,已知向量服从分布 $D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})$,其平均值非常接近中心向量 $\boldsymbol{c}$,并且该向量与中心向量的距离的平方的期望接近 $s^2n/2\pi$,对于服从分布的 $D_{s,\boldsymbol{c}}(\boldsymbol{x})$ 来说,平均值和期望值分别为 $\boldsymbol{c}$ 和 $s^2n/2\pi$.

定义 5(亚高斯分布) 对于任意 $t\in\mathbb{R},\delta>0$,若随机变量 $X\in\mathbb{R}$ 的期望生成函数满足 $E[\exp(2\pi X)]\leqslant\exp(\delta)\cdot\exp(\pi r^2t^2)$,则称随机变量 X 服从参数 $r>0$ 的 δ-亚高斯分布. 对于 $\|X\|\leqslant B$,且 $E(X)=0$ 的随机变量 X 服从参数为 $B\sqrt{\pi}$ 的 0-亚高斯分布. 同理,对于所有的单位向量 μ,随机变量 $<\mu,Y>\in R$ 服从参数 $r>0$ 的 δ-亚高斯分布,则称随机实数向量 Y 服从参数 r 的 δ-亚高斯分布.

引理 1 已知 X_1 和 X_2 是相互独立的随机变量,如果 X_1 服从参数为 r_1 的 δ-亚高斯分布,X_2 服从参数为 r_2 的 δ-亚高斯分布,那么 X_1+X_2 服从参数为 $\sqrt{r_1^2+r_2^2}$ 的 $(\delta_1+\delta_2)$-亚高斯分布.

2.3 Peikert 误差协调机制

令 $\lfloor x\rceil=\lfloor x+\frac{1}{2}\rfloor\in Z$ 为近似取整函数,定义 $\lfloor x\rceil_p:=\lfloor x\cdot\frac{p}{q}\rceil$,$I_0:=\{0,1,\cdots,\lfloor\frac{q}{4}\rceil-1\}$,$I_1:=\left\{-\lfloor\frac{q}{4}\rfloor,\cdots,-1\right\}$;定义交叉近似函数 $\langle\cdot\rangle_2:Z_q\to Z_2$,具体地,$\langle v\rangle_2:=\lfloor\frac{q}{4}\cdot v\rfloor \bmod 2$;定义模近似函数 $\lfloor v\rceil_2=\begin{cases}0, & \text{当 } v\in I_0\cup I_1;\\ 1, & \text{其他.}\end{cases}$

引理 2[21] 对于偶数 q,如果 $v\in Z_q$ 是均匀随机的,那么给定 $\langle v\rangle_2$ 时,$\lfloor v\rceil_2$ 在 Z_q 上也是均匀随机的. 令 $E=\left[-\frac{q}{4},\frac{q}{4}\right)$,则协调函数 $rec:Z_q\times Z_2\to Z_2$ 定义为 $rec(w,b)=\begin{cases}0, & w\in I_1+E(\bmod q)\\ 1, & \text{其它}\end{cases}$.

引理 3[21] 对于偶数 q,如果 $w=v+e \bmod q$,且 $v\in Z_q$,$e\in E$ 那么 $rec(w,\langle v\rangle_2)=\lfloor v\rceil_2$.

当 q 为奇数时,为了避免派生不均匀性,引入了随机化函数. 令 $dbl:Z_q\to Z_{2q}$,$dbl(x)=2x-\bar{e}$,其中 $\bar{e}$ 为随机项,$\bar{e}$ 为 0 的概率为 $\frac{1}{2}$,$\bar{e}$ 为 1 和 -1 的概率为 $\frac{1}{2}$,从而保证 $\bar{e}$ 在模 2 运算后是均匀的.

引理 4[21] 对于奇数 q,如果 $v\in Z_q$ 是均匀随机的,令 $\bar{v}=dbl(v)\in Z_{2q}$,那么在给定 $\langle dbl(v)\rangle_2$ 的情况下,$\lfloor\bar{v}\rceil_2$ 在 Z_{2q} 上是均匀随机的. 令 $E=\left[-\frac{q}{4},\frac{q}{4}\right)$,则协调函数 $rec:Z_{2q}\times Z_2\to Z_2$ 定义为

$$rec(w,b)=\begin{cases}0, & w\in I_1+E(\bmod q)\\ 1, & \text{其它}\end{cases}.$$

引理 5[21] 对于奇数 q,令 $v=w+e\in Z_q$,$w,e\in Z_q$,且 $2e+\bar{e}\in E \bmod q$,那么 $rec(2w,\langle\bar{v}\rangle)=\lfloor\bar{v}\rceil_2$.

3 基于 RLWE 问题的 PAKE 协议设计

已知 $n=2^m$,$m\in Z$,q 是一个大于 8 的素数,满足 $q \bmod 2n=1$,R_q 是一个多项式环,且满足 $R_q=\mathbb{Z}_q[x]/x^n+1$,$\chi$ 是离散高斯分布,γ 是 χ 的标准差,pw 是长度为 32 字节客户端和服务器端的共享口令,g 是一个公共参数,(publickey,prikey)是服务器端的公私钥对,ID_c,ID_s 是客户端和服务器的长度为 64 字节的身份信息,T_{cur} 是当前时间,TS 是时间戳,其长度为 4 个字节.

下面对协议的步骤进行具体描述,过程如图 1 所示.

(1)客户端从离散高斯分布 χ 中随机选取得到秘密向量 $\boldsymbol{f}_c$,$\boldsymbol{a}$,选取随机数 $Nonce$,然后计算 $\boldsymbol{X}=\boldsymbol{ga}+\boldsymbol{f}_c$,使用 NTRU 算法[20]产生的公私钥对之中的公钥 pk_s,加密计算得到 $Auth_c=\boldsymbol{E}_{pk_s}[\mathrm{H}(\boldsymbol{X}|ID_c|pw|Nonce|\mathrm{TS}_1),Nonce]$,将 $(\boldsymbol{X},ID_c,Auth_c,\mathrm{TS}_1)$ 发送至服务器.

(2)服务器收到 $(\boldsymbol{X},ID_c,Auth_c,\mathrm{TS}_1)$ 后,服务器计算 T_{cur} 与 TS_1 的差,即如果当前时间 T_{cur} 与 TS_1 客户端请求时间戳 TS_1 间隔超过时间限制 ΔT,服务器会拒绝客户端的请求. 若未超过时间限制,服务器使用私钥 sk_s 解密得到 $Nonce$,验证哈希值. 通过验证后,服务器从离散高斯分布 χ 中随机选取得到秘密向量 $\boldsymbol{f}_s$,$\boldsymbol{b}$,然后计算 $\boldsymbol{Y}=\boldsymbol{gb}+\boldsymbol{f}_s$.

(3)服务器从离散高斯分布 χ 中随机选取得到秘密向量 $\boldsymbol{r}_s$,计算 $\boldsymbol{K}_s=\boldsymbol{Xb}+\boldsymbol{r}_s$,通过计算随机化函数 $dbl(\boldsymbol{K}_s)$,得到 $\overline{\boldsymbol{K}_s}$,计算模函数 $\langle\overline{\boldsymbol{K}_s}\rangle_{2q,2}$,得到 $\boldsymbol{W}_s$. 通过计算可得 $Auth_s=\mathrm{H}(\boldsymbol{Y}|ID_S|pw|\boldsymbol{W}_s|Nonce+1|TS_2)$,最后计算得到共享会话

密钥 $\boldsymbol{SK}_s = \mathrm{H}(ID_c \mid ID_S \mid \boldsymbol{X} \mid \boldsymbol{Y} \mid \boldsymbol{W}_s \mid Nonce \mid \boldsymbol{V}_s)$,其中,$\boldsymbol{V}_s = \lfloor \boldsymbol{W} \rceil_{2q,2}$,服务器将$(\boldsymbol{Y}, ID_c, \boldsymbol{W}_s, Auth_s, TS_2)$发送至客户端.

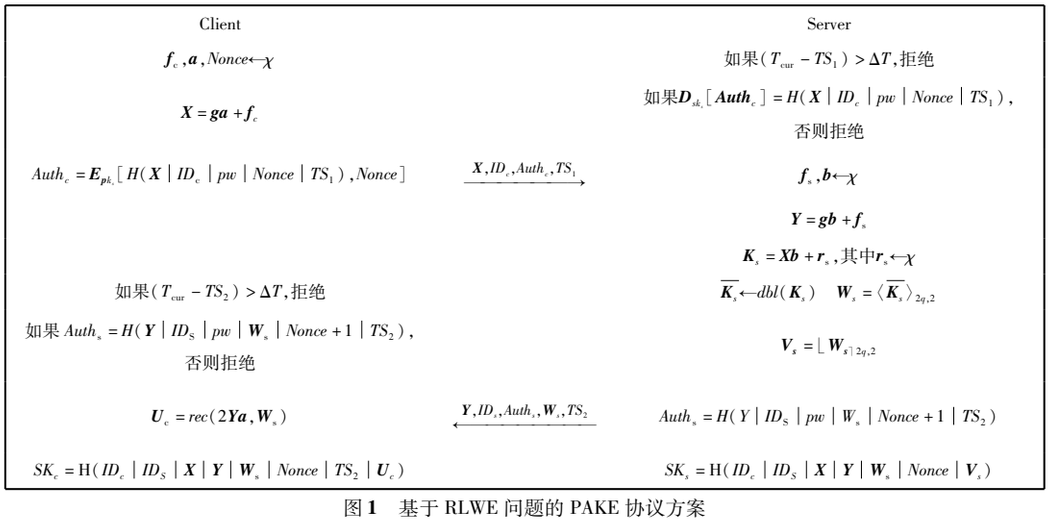

图 **1**　基于 RLWE 问题的 PAKE 协议方案

(4)客户端收到 $Auth_s$ 后,将计算 T_{cur} 与 TS_2 的差,如果当前时间 T_{cur} 与服务器端请求时间戳 TS_2 间隔超过时间限制 ΔT 时,客户端会拒绝服务器端的请求. 若未超过时间限制,验证 $Auth_s$ 与哈希值 $\mathrm{H}(\boldsymbol{Y} \mid ID_S \mid pw \mid \boldsymbol{W}_s \mid Nonce + 1 \mid TS_2)$,若验证通过,客户端从离散高斯分布 χ 中随机选取得到秘密向量 $\boldsymbol{r}_c$,计算 $\boldsymbol{U}_c = rec(2\boldsymbol{Ya}, \boldsymbol{W}_s)$,最终计算会话密钥 $\boldsymbol{SK}_c = \mathrm{H}(ID_c \mid ID_S \mid \boldsymbol{X} \mid \boldsymbol{Y} \mid \boldsymbol{W}_s \mid Nonce \mid \boldsymbol{U}_s)$.

通信双方在进行下一次会话密钥交换协议之前,客户端需要更新共享口令,使用上次建立的会话密钥进行加密,即 $\mathrm{UpdateMsg} = E_{pk_c}(pw' \mid pw \mid \mathrm{H}(pw' \mid pw))$,将此信息发送至服务器;当服务器接受到客户端的指令后,服务器使用共享会话密钥解密新的口令并记录存储,双方完成口令更新之后并消除之前的会话密钥信息. PAKE 协议口令更新如图 2 所示.

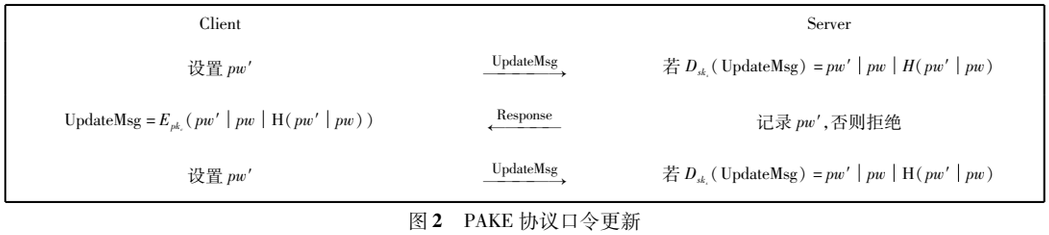

图 **2**　PAKE 协议口令更新

4　参数设置与正确性分析

根据本文设计方案,由 $\boldsymbol{K}_s = \boldsymbol{Xb} + \boldsymbol{r}_s$,将 $\boldsymbol{K}_s = \boldsymbol{Xb} + \boldsymbol{r}_s$ 代入可得 $\boldsymbol{K}_s = (\boldsymbol{ga} + \boldsymbol{f}_c)\boldsymbol{b} + \boldsymbol{r}_s = \boldsymbol{gab} + \boldsymbol{f}_c\boldsymbol{b} + \boldsymbol{r}_s$. 将 $\boldsymbol{Y} = \boldsymbol{gb} + \boldsymbol{f}_s$ 代入 $2\boldsymbol{Ya}$,可得 $2\boldsymbol{Ya} = 2\boldsymbol{gab} + 2\boldsymbol{f}_s\boldsymbol{a}$.

由 $\overline{\boldsymbol{K}}_s = dbl(\boldsymbol{K}_s) = 2\boldsymbol{K}_s - \bar{\boldsymbol{e}}$,将 $\boldsymbol{K}_s = \boldsymbol{gab} + \boldsymbol{f}_c\boldsymbol{b} + \boldsymbol{r}_s$ 代入随机化函数 $dbl(\boldsymbol{K}_s)$,可得 $\overline{\boldsymbol{K}}_s = 2(\boldsymbol{gab} + \boldsymbol{f}_c\boldsymbol{b} + \boldsymbol{r}_s) - \bar{\boldsymbol{e}}$. 代入可得结果为 $2\boldsymbol{Ya} - \overline{\boldsymbol{K}}_s = 2\boldsymbol{gab} + 2\boldsymbol{f}_s\boldsymbol{a} - [2(\boldsymbol{gab} + \boldsymbol{f}_c\boldsymbol{b} + \boldsymbol{r}_s) - \bar{\boldsymbol{e}}]$,进一步简化得 $2(\boldsymbol{f}_s\boldsymbol{a} - \boldsymbol{f}_c\boldsymbol{b} - \boldsymbol{r}_s) + \bar{\boldsymbol{e}}$. 此时令 $\boldsymbol{e} = \boldsymbol{f}_s\boldsymbol{a} - \boldsymbol{f}_c\boldsymbol{b} - \boldsymbol{r}_s$,则可以得到 $2\boldsymbol{Ya} - \overline{\boldsymbol{K}}_s = 2\boldsymbol{e} + \bar{\boldsymbol{e}}$.

根据随机化函数定义,$\bar{\boldsymbol{e}}$ 的解码基系数服从 0 - 亚高斯分布,亚高斯分布参数为 $\sqrt{2\pi}$.

由于 $\boldsymbol{f}_s, \boldsymbol{a}, \boldsymbol{f}_c, \boldsymbol{b}, \boldsymbol{r}_s$ 为相互独立的随机变量,根据引理 1,$2\boldsymbol{e} + \bar{\boldsymbol{e}}$ 解码基所有系数都服从 3δ 亚高斯分布,亚高斯分布系数为 $2\sqrt{r'^2(2l^2 + n) + \pi/2}$,其中,$r'^2 = r^2 + 2\pi \mathrm{rad}(m)/m$,则 $2\boldsymbol{e} + \bar{\boldsymbol{e}}$ 以显著概率满足 $|2\boldsymbol{e} + \bar{\boldsymbol{e}}| \in [-2q/8, 2q/8]$. 从离散高斯分布 χ 随机选取得到 s_i,$\| g \cdot s_i \| \leqslant \hat{m} \cdot (r+1) \cdot \sqrt{n}$ 的概率为 $1 - 2^{-n}$,基于格理论 RLWE 问题的 PAKE 协议可以显著概率计算出相同的会话密钥 $\boldsymbol{SK}_C = \boldsymbol{SK}_S$.

由 $r'^2 \leqslant r^2 + 2\pi$,$w = \sqrt{In(2n/\varepsilon)/\pi}$,可得 $q \geqslant 8\sqrt{(r^2 + 2\pi)(2\hat{m}^2(r+1)^2 + 1)n} \cdot w = O(\hat{m} \cdot r^2\sqrt{n}) \cdot w$.

选取 $q = O(r^2 \cdot n^{2/3} \cdot \log n)$,$\hat{m} = O(n)$,此时 $\varepsilon = 2^{-128}$,令 $l = 2$,$r = \xi q$,$\xi = \alpha(3n/\log(3n))^{1/4}$,其中 $r = (3n/\log(3n))^{1/4} \cdot w(\sqrt{\log n})$,满足 $\alpha q \geqslant w\sqrt{\log n}$,则 $q = O(r^2 \cdot n^{2/3} \cdot \log n) = \tilde{O}(n^2)$,上述参数设置可以保证量子归约算法将理想格上的 $\tilde{O}(\sqrt{n}/\alpha)$ - 近似 SVP 问题归约为 RLWE 问题,且近似因子是 $\tilde{O}(\sqrt{n}/\alpha) = \tilde{O}(\sqrt{n} \cdot q) = \tilde{O}(n^{2.5})$.

在本协议方案中,设置参数 $n = 2^{10}$,$q = 1073479681$,α 为 $8/\sqrt{2\pi}$的离散高斯分布. 在 LWE 性能测试平台上对

此协议测试,结果如图 3 所示.

图3 LWE性能测试平台协议测试结果

5 安全性证明

下面使用文献[23]提出的 C/S 模式下的 PAKE 安全模型对协议方案进行安全性证明. 在口令认证协议中,协议中的每个参与者包括攻击者都被模拟为一组概率多项式时间随机谕言机. 一般定义两个参与者分别是客户端 C 和服务器 S. 服务器拥有系统公私钥,而客户端可以随机选择一个口令.

假定存在攻击者 A,C^i 和 S^i 表示进行第 i 次会话的客户端和服务器,将攻击者的能力抽象为对 Execute,Send ,Reveal,Corrupt,Test 随机谕言机的若干查询,这些查询可以是无序和自适应的. 查询的定义如下.

Execute(C^i,S^i):这种查询模拟了攻击者的被动攻击. 客户端和服务器执行第 i 次通信会话,攻击者通过查询搭档随机谕言机执行过程中的所有交互信息.

Send(U^i,M):这种查询模拟了攻击者对参与者的主动攻击,攻击者可以向参与者 U 发送消息,参与者 U 代表客户端 C 或服务器 S,同时发送消息后可以获得从参与者 U 返回的消息.

Corrupt(C):攻击者可以从客户端获得先前的口令.

Corrupt(S):攻击者可以获得服务器的私钥,相当于从服务器获得先前的口令.

Reveal1(U^i):这个查询模拟随机谕言机的会话密钥泄漏,攻击者可从通信参与者任意一方获得获得会话密钥.

Test(U^i):这个查询描述协议的语义安全性. 用来定义攻击者的优势. 它只能运行一次,并且只能对一个“新鲜”的随机谕言机进行. 当攻击者进行 Test 查询时,协议随机选择一个比特 b,如果 $b=1$,则返回会话密钥 SK,否则,返回一个相同长度的随机数组.

攻击者根据返回值以及利用其他查询获得的信息,猜测 b 的值. 攻击者根据 Test 查询的返回值,猜测 b 的值,记为 b'. 若攻击者猜测出 b 的值,则称攻击者的攻击成功.

定义攻击者成功的概率为$\Pr_A^P[\mathrm{Succ}]=\Pr[b=b']$. 相应的,攻击者的成功的优势为:$\mathrm{Adv}_A^P(k)=2\ \Pr_A^P[\mathrm{Succ}]-1$.

如果攻击者成功的优势是可忽略的,那么称协议是安全的.

实验 P0 该实验模拟了标准模型下针对本文提出的 PAKE 协议的一次真实的攻击,攻击者可以使用任何随机谕言机对协议进行查询.

实验 P1 在此次实验中,随机谕言机产生的消息为 $\boldsymbol{msg}_c=(\mathrm{ID}_c,\boldsymbol{X},\mathrm{Auth}_c)$ 或者 $\boldsymbol{msg}_c=(\mathrm{ID}_s,\boldsymbol{Y},\boldsymbol{W}_s\ \mathrm{Auth}_s)$,并且哈希函数需要满足下列两个性质:

(1)消息 msg_c 或者 msg_s 不能重复,即当 $i\neq j$ 时,$msg_c^i\neq msg_c^j$、$msg_s^i\neq msg_s^j$.

(2)哈希函数可抵抗碰撞.

在实验 P0,无确切的性质但是仍然存在消息重复的情况,也会有哈希函数碰撞的情况发生. 在消息 msg 中包含参数从 $\boldsymbol{X}=\boldsymbol{ga}+2\boldsymbol{f}_c$、$\boldsymbol{Y}=\boldsymbol{gb}+2\boldsymbol{f}_s$,其中 $\boldsymbol{a}$、$\boldsymbol{b}$、$\boldsymbol{f}_c$、$\boldsymbol{f}_s$ 从 χ 中随机选择,因此消息重复的概率接近为 0,一般情况下哈希函数发生碰撞的概率为 0. 因此攻击者无法区分 P0 和 P1,实验优势差 $|\mathrm{Adv}_A^{P0}(k)-\mathrm{Adv}_A^{P1}(k)|$ 是可以忽略的.

实验 P2 在实验 2 中,攻击者 A 使用一个随机向量 $\boldsymbol{K}'_s$,代替通过 Execute(C,S)查询得到的参数 $\boldsymbol{K}_s=\boldsymbol{X}b+2r_s$,如果 $\boldsymbol{K}_s$ 是一个 RLWE 实例,那么攻击者包含的数据与实验 P1 相同;如果 $\boldsymbol{K}_s$ 是一个随机均匀向量,那么攻击者包含的数据与实验 P2 相同. 如果攻击者可以区分实验 P1 与 P2 的数据,那么意味着攻击者可以区分 RLWE 分布,因此可以得出实验 P1 与 P2 的攻击者优势差几乎为 0,即 $|\mathrm{Adv}_A^{P1}(k)-\mathrm{Adv}_A^{P2}(k)|$ 是可以忽略的. 因此,当 $\boldsymbol{K}'_s$ 是一个随机向量时,则 $\boldsymbol{V}'_s$ 也是随机均匀向量,会话密钥 $\boldsymbol{SK}'_s$ 从 $\boldsymbol{V}'_s$ 中产生,即 $\boldsymbol{SK}'_s$ 的产生与 $\boldsymbol{K}'_s$ 不相关.

定理 1 如果攻击者通过 Corrupt(U^i)可以得到之前会话口令 pw^{i-1},根据上述证明可知会话密钥的产生与口令是相互独立的,因此攻击者无法获得当前的会话密钥 Sk^i 和新的口令 pw^{i+1},因攻击者通过此 Corrupt(U^i)查询优势没有增加.

实验 P3 攻击者通过 Execute(C^i,S^i)查询得到会话密钥 $\boldsymbol{SK}_c=\boldsymbol{SK}_s$,其中 *Nonce* 值被随机值 *Nonce'* 所替代. 已知 $\boldsymbol{SK}'_s$ 由 $msg_c=(\mathrm{ID}_c、\boldsymbol{X}、\mathrm{E}_{pk_s}[\mathrm{H}(\boldsymbol{X}|ID_c|pw|Nonce'),Nonce'])$ 产生,如果攻击者可以通过 msg_c 区分 $\boldsymbol{SK}_s$ 和 $\boldsymbol{SK}'_s$,意味着敌手可以打破密码系统的安全性,因此可得实验 P2 和 P3 的优势差几乎为 0,即 $|\mathrm{Adv}_A^{P2}(k)-$

$\mathrm{Adv}_A^{P3}(k)$ | 是可以忽略的.

实验 P4　在本实验中,攻击者向随机谕言机发送 $Send_1(S,\mathrm{msg}_c)$ 与 $Send_2(S,\mathrm{msg}_s)$ 两种查询,如果攻击者发送的 msg_c 通过认证,即 msg_c 是有效的,说明攻击者拥有正确的口令;如果攻击者发送的 msg_s 通过认证,即 msg_s 是有效的. 上述两种情况均被认为是成功的攻击,否则,需要参照实验 P3 决定攻击者是否攻击成功,可以得出实验 P4 的优势大于 P3,即 $|\mathrm{Adv}_A^{P3}(k) \leqslant \mathrm{Adv}_A^{P4}(k)|$.

实验 P5　假设攻击者在实验 P4 中攻击成功,攻击者向预言机进行 $Send_1(S,\mathrm{msg}_c)$ 查询,得到 $msg_c=(\mathrm{ID}_c、\boldsymbol{X}、\mathrm{E}_{pk_s}[\mathrm{H}(\boldsymbol{X}|ID_c|pw|Nonce'),Nonce'])$,其中的口令 pw 被随机值 pw'所替代. 由于在协议中的 NTRU 密码系统和哈希函数是足够安全的密码设施,攻击者无法从 $\mathrm{Auth}_c=[\mathrm{H}(\boldsymbol{X}|ID_c|pw|Nonce'),Nonce']$ 中得到正确的口令 pw,因此可以得出实验 P4 和 P5 的优势差几乎为 0,即 $|\mathrm{Adv}_A^{P4}(k)-\mathrm{Adv}_A^{P5}(k)|$是可以忽略的.

实验 P6　攻击者向随机谕言机进行 $\mathrm{Execute}(C^i,S^i)$ 查询,得到认证消息 $\mathrm{Auth}_s=\mathrm{H}(\boldsymbol{Y}|ID_s|pw|\boldsymbol{W}_s|Nonce+1)$,其中的口令 pw 被随机值 pw''所替代. 由于在协议中的 NTRU 密码系统和哈希函数是足够安全的密码设施,攻击者无法从 $msg_c=(\mathrm{ID}_c、\boldsymbol{X}、\mathrm{E}_{pk_s}[\mathrm{H}(\boldsymbol{X}|ID_c|pw|Nonce'),Nonce'])$ 中得到正确的会话密钥 $\boldsymbol{SK}$,因此可以得出实验 P5 和 P6 的优势差几乎为 0,即 $|\mathrm{Adv}_A^{P5}(k)-\mathrm{Adv}_A^{P6}(k)|$是可以忽略的.

通过实验分析可以得出结论 $|\mathrm{Adv}_A^{P0\sim P5}(k) \leqslant \mathrm{Adv}_A^{P6}(k)|$,如果实验 P6 攻击者成功的优势是可忽略的,那么所有先前的实验的优势均是可以忽略的.

由以上分析可知,实验 P6 攻击成功的概率 $\mathrm{Pr}_A^6[\mathrm{Succ}]=\frac{1}{2}$,在协议中攻击者通过随机谕言机进行查询,获得成功的概率与随机猜测的概率相同. 因此可得 $\mathrm{Adv}_A^{P6}(k)=2\ \mathrm{Pr}_A^{P6}[\mathrm{Succ}]-1=0$.

综合以上分析,由于 $|\mathrm{Adv}_A^{P0\sim P5}(k) \leqslant \mathrm{Adv}_A^{P6}(k)|$,可得 $\mathrm{Adv}_A^{P}(k)=2\ \mathrm{Pr}_A^{P}[\mathrm{Succ}]-1=0$,即攻击者基于随机预言机进行查询,对协议进行攻击成功的优势几乎为 0. 本文构造的 PAKE 协议方案基于随机预言机在 C/S 模式下的 PAKE 安全模型下是可证明安全,此 PAKE 协议的安全性最终可归约为格上的 RLWE 问题的困难性.

6　效率对比

6.1　PAKE 协议实现

本文设计了一个 C/S 模式下的后量子 PAKE 协议,方案基于格理论 RLWE 困难问题,使用 Java 语言在 Eclipse Neon. 3 平台下进行了协议的实现,双方产生了相同的会话密钥结果如图 4 所示.

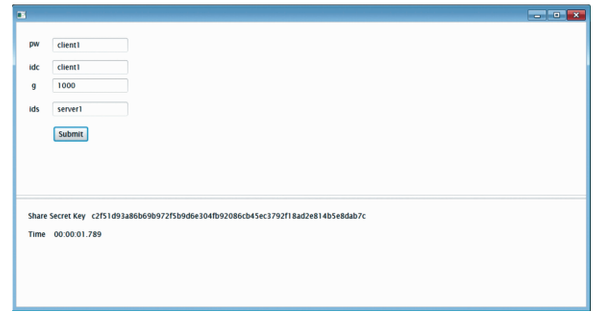

图4　PAKE协议通信双方共享会话密钥

6.2　相关方案对比

根据当前基于格上困难问题构造的 PAKE 协议的最新学术成果,与本文设计的基于格理论 RLWE 问题并使用 Peikert 式误差协调机制[21]构造的 PAKE 协议进行综合分析. 选取了 2017 年丁等提出的基于丁式误差协调机制[22]的 RLWE-PAK[15] 和 RLWE-PPK[15] 两个协议,另外选取了 2018 年高等人设计的基于丁式误差协调机制的 RLWE-SRP[16] 协议,与本文构造的 PAKE 协议在困难问题假设、误差协调技术、安全模型、安全度、和通信量几个方面进行对比. 四种方案参数维度 $n=1024$,模数 $q=1073479681$,均选取离散高斯分布且标准差 $\sigma=8/\sqrt{2\pi}\approx 3.192$. 表 1 是四种方案对比情况,本文方案在安全度上有一定的优势,并且通信量相对较低.

表 1　基于格设计的口令认证密钥交换协议的性能比较

方案	困难假设	误差协调方式	安全模型	安全度(单位:bit)	通信量(单位:Byte)	
					$A\rightarrow B$	$B\rightarrow A$
RLWE-PAK[15]	$Ideal-SIVP_{\tilde{o}(4.5)}$	丁式	RO 模型	184	4192	4256
RLWE-PPK[15]	$Ideal-SIVP_{\tilde{o}(4.5)}$	丁式	RO 模型	184	4192	4224
RLWE-SRP[16]	$Ideal-SIVP_{\tilde{o}(4.5)}$	丁式	UC 模型	209	4150	4228
本方案	$Ideal-SIVP_{\tilde{o}(2.5)}$	Peikert 式	PAKE 模型[23]	225	3940	4068

7 结语

PAKE 协议不需要存在公钥基础设施等一般 AKE 协议所要求的前提假设,通信用户只需使用一个低熵口令就可以在不安全的信道生成高熵会话密钥,在现代通信网络中有很强的实用性. 量子计算机及相关技术的飞速发展,使得基于传统数论困难问题设计的现代公钥密码体制面临着严重的安全威胁. 为抵抗量子攻击,后量子密码的研究成为了当前信息安全研究的热点话题. 基于格的口令认证密钥交换协议使得通信用户只需用一个低熵口令就可在不安全的信道生成高熵会话密钥,避免了一般认证密钥交换协议要求存在公钥基础设施等前提假设,同时它还继承了基于格密码体制可抗量子攻击、一般具有线性渐进计算复杂度的优势.

本文基于格理论 RLWE 问题并使用 Peikert 式误差协调机制构造了一个 C/S 模式下的口令认证密钥交换协议,设置了合理的参数保证客户端和服务器双方以显著概率得到相同的会话密钥. 协议在文献[23]中的 PAKE 模型下可证明安全,可抵御量子攻击,与现有的基于格理论设计的 PAKE 协议相比,通信量较低并且在安全度上有一定的优势. 下一步考虑使用 LWE 困难问题,设计更加简单高效、更具实用价值的后量子安全的口令认证密钥协议.

参考文献

[1] Dodis Y, Mironov I, Stephens-Davidowitz N. Message transmission with reverse firewalls-secure communication on corrupted machines[A]. International Cryptology Conference [C]. Berlin, GER: Springer-Verlag, 2016. 341 –372.

[2] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644 –654.

[3] Victor B, Philip M, Sarvar P. Provably secure password-authenticated key exchange using diffie-hellman[A]. Theory and Application of Cryptographic Techniques[C]. Berlin, GER: Springer-Verlag, 2000. 156 –171.

[4] Hao F. J-PAKE: password-authenticated key exchange by juggling [EB/OL]. https://www. rfc-editor. org/info/rfc8236, 2017: 1 –15.

[5] Harkins D. Secure pre-shared key (PSK) authentication for the internet key exchange protocol (IKE)[J]. Educause Quarterly, 2012, 50(4): 725 –726.

[6] Wu T D. The secure remote password protocol[A]. Network and Distributed System Security Symposium[C]. Berlin, GER: Springer-Verlag, 1998. 97 –111.

[7] Steven M, Michael J. Cryptographic protocol for remote authentication[P]. USA: US5440635 A, 1995.

[8] David P. Cryptographic methods for remote authentication [P]. USA: US7010692B2, 2006.

[9] Katz J, Vaikuntanathan V. Smooth projective hashing and password-based authenticated key exchange from lattices [A]. International Conference on the theory and Application of Cryptology and Information Security[C]. Berlin, GER: Springer-Verlag, 2009. 636 –652.

[10] Katz J, Ostrovsky R, Yung M, et al. Efficient password-authenticated key exchange using human-memorable passwords[A]. Theory and Application of Cryptographic Techniques[C]. Berlin, GER: Springer-Verlag, 2001. 475 –494.

[11] Gennaro R, Lindell Y. A framework for password-based authenticated key exchange[A]. Theory and Application of Cryptographic Techniques[C]. Berlin, GER: Springer-Verlag, 2003. 524 –543.

[12] 胡学先. 标准模型下口令认证密钥交换协议的分析与设计[D]. 解放军信息工程大学, 2010.

[13] Ding Y, Fan L. Efficient password-based authenticated key exchange from lattices [A]. Computational Intelligence and Security [C]. New York, USA: IEEE, 2011. 934 –938.

[14] Groce A, Katz J. A new framework for efficient password-based authenticated key exchange[A]. ACM Conference on Computer and Communications Security [C]. New York, USA: ACM, 2010. 516 –525.

[15] Ding J, Alsayigh S, Lancrenon J, et al. Provably secure password authenticated key exchange based on RLWE for the post-quantum world[A]. The Cryptographers' track at the RSA Conference[C]. Berlin, GER: Springer-Verlag, 2017. 183 –204.

[16] Gao X, Ding J, Li L, et al. Efficient implementation of password-based authenticated key exchange from RLWE and post-quantum TLS[J]. IACR Cryptology ePrint Archive, 2017: 1192 –1199.

[17] Gao X, Ding J, Liu J, et al. Post-quantum secure remote password protocol from RLWE problem[A]. International Conference on Information Security and Cryptology [C]. Berlin, GER: Springer-Verlag, 2017. 99 –116.

[18] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[A]. International Cryptology Conference[C]. Berlin, GER: Springer-Verlag, 2010. 1 –23.

[19] Applebaum B, Cash D, Peikert C, et al. Fast cryptographic primitives and circular-secure encryption based on hard learning problems[A]. International Cryptology Conference[C]. Berlin, GER: Springer-Verlag, 2009. 595 –618.

[20] Hoffstein J, Pipher J, Silverman J H, et al. NTRU: A ring-

based public key cryptosystem[A]. Algorithmic Number Theory Symposium[C]. Berlin, GER: Springer-Verlag, 1998. 1423:267 – 288.

[21] Peikert C. Lattice cryptography for the Internet[A]. International Workshop on Post-Quantum Cryptography[C]. Berlin, GER: Springer-Verlag, 2014. 8772:197 – 219.

[22] Ding J, Universuty C. A simple provably secure key exchange scheme based on the learning with errors problem[J]. IACR Cryptology ePrint Archive, 2012:688 – 702.

[23] Xun Y, Tso R, Okamoto E. Identity-based password-authenticated key exchange for client/server model[A]. International Conference on Security and Cryptography[C]. Berlin, GER: Springer-Verlag, 2012. 45 – 54.

作者简介

李子臣(通信作者)　男,1965 年出生,河南焦作人. 北京印刷学院信息工程学院教授、博士生导师,主要研究方向为信息安全、数字水印、数字签名、密码学等.

E-mail:lizc2020@163.com