基于格的用户匿名三方口令认证密钥协商协议

王彩芬，陈丽
（西北师范大学计算机科学与工程学院，甘肃 兰州 730070）

摘 要：随着量子理论的快速发展，离散对数问题和大整数分解问题在量子计算下存在多项式求解算法，其安全性受到严重威胁，因此，提出 2 个基于环上带误差学习问题的用户匿名三方口令认证密钥协商方案，包括基于格的隐式认证密钥协商方案和基于格的显式认证密钥协商方案，并证明了其安全性。其中，隐式认证密钥协商协议通信量少、认证速度快，显式认证密钥协商协议安全性更高，同时实现用户和服务器的双向认证、可抗不可测在线字典攻击。与其他口令认证密钥协商协议相比，所提协议有更高的效率和更短的密钥长度，能够抵抗量子攻击，因此，该协议既高效又安全，适用于大规模网络下的通信。

关键词：格密码；可证明安全；口令认证；密钥交换；环上带误差
中图分类号：TP309.7
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018021

Three-party password authenticated key agreement protocol with user anonymity based on lattice

WANG Caifen, CHEN Li
College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China

Abstract: With the rapid development of quantum theory and the existence of polynomial algorithm in quantum computation based on discrete logarithm problem and large integer decomposition problem, the security of the algorithm was seriously threatened. Therefore, two authentication key agreement protocols were proposed rely on ring-learning-with-error (RLWE) assumption including lattice-based implicit authentication key agreement scheme and lattice-based explicit authentication key agreement scheme and proved its security. The implicit authentication key agreement protocol is less to communicate and faster to authentication, the explicit authentication key agreement protocol is more to secure. At the same time, bidirectional authentication of users and servers can resist unpredictable online dictionary attacks. The new protocol has higher efficiency and shorter key length than other password authentication key agreement protocols. It can resist quantum attacks. Therefore, the protocol is efficient, secure, and suitable for large-scale network communication.

Key words: lattice-based cryptology, provably secure, password authentication, key exchange, ring-learning-with-error

1 引言

随着大数据时代的到来以及量子计算机的快速发展，人们对数据的安全有了更高的要求，格密码依靠其独特的困难问题和归约结果成为密码学研究的热点，基于离散对数问题和大整数分解问题在量子计算下存在多项式求解算法，其安全性受到严重威胁，因此，格理论被应用于抗量子攻击的密

收稿日期：2017-09-18；**修回日期**：2018-01-17
基金项目：国家自然科学基金资助项目（No.61662069, No.61562077, No.61662071）；西北师范大学青年教师科研能力提升计划基金资助项目（No.NWNU-LKQN-14-7）
Foundation Items: The National Natural Science Foundation of China (No.61662069, No.61562077, No.61662071), The Foundation for Excellent Young Teachers by Northwest Normal University (No.NWNU-LKQN-14-7)

码体制中。

认证密钥交换（AKE, authenticated key exchange）允许通信双方相互认证并协商出共享密钥，两方口令认证密钥协商[1]（2PAKE, two-party password authenticated key exchange）协议要求用户和服务器共享相同的口令，实现单个用户和服务器的相互认证，不适用于用户和用户之间的通信，为解决其局限性，密码学研究者提出三方口令认证密钥交换[2,3]（3PAKE, three-party password authenticated key exchange）协议，使每个用户和服务器共享一个低熵的口令，实现用户间的相互认证和密钥协商，适用于大规模网络下的通信。认证密钥交换通常分为显式认证和隐式认证，显式认证是指协议结束后，用户 A 确信与之通信的就是意定的参与方 B；隐式认证是指协议结束后，用户 A 相信只有意定的参与方 B 才能计算出相同的会话密钥。显式认证协议中除了隐式认证之外，还包含一个显式密钥确认过程，使参加协议的用户可以确保其特别指定的用户确实已经拥有与其相同的会话密钥。

2005 年，文献[2]基于判定性 Diffie-Hellman 假设（DDH, decisional Diffie-Hellman assumption）提出 3PAKE 协议。2006 年，文献[3]提出可证明安全性的 3PAKE 协议，随后，有不同效率和安全性的 3PAKE[4,5]协议相继被提出，但是这些已有的 3PAKE 的安全性都依赖于离散对数问题和大整数分解问题等一系列传统的困难问题，不能抵抗量子攻击。2009 年，文献[6]首次提出了基于格的 2PAKE 协议，其方案基于误差学习（LWE, learning with error）问题，但存在密钥长度过长和效率低等问题。2011 年，文献[7]基于平滑投射散列函数（SPH, smooth projective hashing）提出了一个更高效的 2PAKE 协议。2012 年，文献[8]基于 LWE 问题提出可证明安全的两方密钥交换方案。2013 年，文献[9]使用密钥封装机制提出基于 RLWE 的密钥交换协议，但该协议被文献[10]指出难以抵抗外部攻击者实施的假冒攻击。由于 2PAKE 协议的局限性，文献[11]基于近似平滑投射散列函数（ASPH, approximate smooth projective hashing）提出格的 3PAKE 协议。2015 年，文献[12]基于 RLWE 困难问题提出可证明安全的 2PAKE 协议。同年，文献[13]基于 LWE 困难问题提出认证密钥交换方案，但该协议存在模数大、效率低等局限；文献[14]提出一种新型的基于环上带误差学习问题的认证密钥交换方案，但该方案是两方认证密钥协商协议。2016 年，文献[15]提出基于 LWE 的 2PAKE 协议。同年，文献[16]提出基于验证元的三方口令认证密钥交换协议，但通信量较多、效率较低。2017 年，文献[17]提出了基于口令的两方密钥协商协议的形式化模型，并证明其安全性。本文在其基础上，设计了一个基于格的 RLWE 困难问题的 3PAKE 协议的安全模型，并证明了协议的安全性。

为解决上述协议的局限性，提出 2 个基于格的用户匿名三方口令认证密钥协商协议，包括基于格的三方隐式认证密钥协商协议和基于格的三方显式认证密钥协商协议，其中，隐式认证密钥协商协议通信量少，显式认证密钥协商协议除了满足隐式认证的所有条件之外，还需要满足密钥确认，即协议参与方可以确定协议的其他参与方获得了特定的会话密钥，同时实现用户和服务器的双向认证、可抗不可测在线字典攻击。所提方案避免了 2PAKE 的局限性，有更高的效率和更短的密钥长度，能够抵抗量子攻击，适用于服务器和用户间的三方通信，并证明了其安全性。因此，该协议既高效又安全，适用于大规模网络下的通信。

2 预备知识

定义 1 离散高斯分布。令 $\rho_r(X)=\exp\left(-\pi\frac{\|X\|^2}{r^2}\right)$，对于格 L，记 $\rho_r(L)=\sum_{X\in L}\rho_r(X)$。格 L 上的离散高斯分布 $D_{L,r}$ 定义为对任意 $X\in L$，若随机变量 ξ 满足 $P_r(\xi=X)=\frac{\rho_r(X)}{\rho_r(L)}$，则称随机变量 ξ 服从离散高斯分布 $D_{L,r}$。

设环 $R=\frac{Z[x]}{f(x)}$，其中，$f(x)=x^n+1$，$n=2^k$，$k\in Z$。对于模数 q，记 $R_q=\frac{R}{qR}$，且 R_q 中的任何一个元素均可表示成一个次数为 $n-1$ 的多项式。

定义 2 RLWE 问题。设 $n=2^k\geqslant 1$，$k\in Z$，$q\geqslant 2$，χ 是 R_q 上的错误概率分布，对于 $s\in R_q$，RLWE 分布 $A_{s,\chi}$ 的一个抽样以下述方式产生：随机均匀选取 $a\in R_q$，从错误概率分布 χ 中抽取错误分量 $e\leftarrow\chi$，输出 $(a,as+e \bmod q)\in R_q\times R_q$。根据 RLWE 问题有以下相关引理。

引理 1 对于 $\forall s,t\in R$，有 $\|st\|\leqslant\sqrt{n}\,\|s\|\|t\|$ 和

$\| st \|_\infty \leqslant n \| s \|_\infty \| t \|_\infty$。

引理 2　对于任何实数 $\alpha = \omega(\sqrt{\lg n})$，有 $Pr_x \leftarrow \chi_\alpha[\| x \| > \alpha\sqrt{n}] \leqslant 2^{-n+1}$。

定义 3　*Cha* 和 Mod_2 函数[12]。奇数 $q > 2$，定义 $Z_q = \left\{-\frac{q-1}{2}, \cdots, \frac{q-1}{2}\right\}$，集合 $E := \{-\left\lfloor \frac{q}{4} \right\rfloor, \ldots, \left\lfloor \frac{q}{4} \right\rceil\}$，*Cha* 是 E 的互补特征函数，$Cha(v) = \begin{cases} 0, v \in E \\ 1, \text{其他} \end{cases}$，对于 $\forall v \in Z_q$，有 $v + Cha(v) \cdot \frac{q-1}{2} \bmod q \in E$。

辅助模块化函数 Mod_2。输入 $v \in z_q$ 和 $Cha(v) \in \{0,1\}$，输出 $Mod_2(v, Cha(v)) \in \{0,1\}$，$Mod_2 : Z_q \times \{0,1\} \to \{0,1\}$。令 $b = Cha(v)$，有 $Mod_2(v,b) = (v + b\frac{q-1}{2}) \bmod q \bmod 2$。

引理 3　q 是一个奇数，$v \in Z_q$，$e \in Z_q$，且 $|e| < \frac{q}{8}$，$\omega = v + 2e$，此时，有 $Mod_2(v, Cha(v)) = (v + Cha(v)\frac{q-1}{2}) \bmod q \bmod 2 = (\omega + Cha(v)\frac{q-1}{2}) \bmod q \bmod 2 = Mod_2(\omega, Cha(v))$。

定义 4　3PAKE 协议的安全模型。

安全游戏。定义挑战者$\mathcal{CH}$和概率多项式时间敌手$\mathcal{A}$的安全参数 k，挑战者代表诚实用户运行协议 P。

用户和口令。假设一个固定的用户集合$\mathcal{U}$分为 2 个非空集合：客户集合$\mathcal{C}$和服务器集合$\mathcal{S}$，假设长度为 L 的非空字典 D，在游戏开始前，非空字典 D 随机均匀分配每个客户 $C \in \mathcal{C}$的口令 pw_C，并给敌手$\mathcal{A}$分配口令。$\forall S \in \mathcal{S}$，有 $pw_S := (f(pw_C))_C$，f 是被 P 指定有效的、可计算的单向函数。$\mathcal{CH}$生成 P 的公共参数，并发送给$\mathcal{A}$，模型假设敌手知道恶意客户口令集合，游戏开始。

用户实例。在游戏期间，任何用户 $U \in \mathcal{U}$与用户实例 $\prod_U^i$ 关联，其中，i 为正整数，每个实例称为一个会话，敌手可以用下列询问来启用实例，发起和运行协议。当拥有匹配身份（PID） pid_U^i、会话身份（SID） sid_U^i 和一个会话密钥（SK） sk_U^i 时，实例 $\prod_U^i$ 可能接受。PID 是实例相信正在通信的用户身份；SK 是实例 $\prod_U^i$ 最终计算目标；SID 是唯一标识协议运行并确保使用 SK 会话的字符串。

敌手$\mathcal{A}$和协议用户间的交互通过下列询问实现，敌手能对任意实例 $\prod_U^i$ 进行以下询问。

Send($\mathcal{U}, i, M$)询问。消息 M 被发送给实例 $\prod_U^i$，实例按协议 P 的要求计算，并更新其状态，将结果输出给敌手$\mathcal{A}$。假设$\mathcal{A}$能看到询问结果 $\prod_U^i$ 接受或终止。

Execute($\mathcal{C}, i, \mathcal{S}, j$)询问。$P$ 执行完成 $\prod_C^i$ 和 $\prod_S^j$ 后，把执行记录传递给敌手$\mathcal{A}$。

Reveal($\mathcal{U}, i$)询问。返回 $\prod_U^i$ 所拥有的 sk_U^i 给$\mathcal{A}$。

Test($\mathcal{U}, i$)询问。为使此询问有效，实例 $\prod_U^i$ 必须是新鲜的。随机选择 b，若 $b = 1$，将真实的 sk_i^U 给$\mathcal{A}$；若 $b = 0$，将等长的随机值给$\mathcal{A}$。在游戏中，此询问只进行一次。

Corrupt($\mathcal{U}$)询问。如果 $U \in \mathcal{U}$，返回 $(f(pw_C))_C$，否则，返回 pw_U 给$\mathcal{A}$。

结束游戏。最后，$\mathcal{A}$输出 b' 作为 b 的猜测。如果 $b' = b$，则攻击者攻击成功。

实例的新鲜性。如果敌手$\mathcal{A}$通过安全模型询问，不能获得实例 $\prod_U^i$ 的会话密钥，则实例是新鲜的。即如果没有发生以下任一事件：1) Reveal($\mathcal{U}, i$)被询问；2) Reveal($\mathcal{V}, j$) 被询问或实例 $\prod_V^j$ 和 $\prod_U^i$ 是匹配会话；3)对测试询问和Send($\mathcal{U}, i, M$) 询问出现的 M 进行 Corrupt($\mathcal{V}$) 询问。则说明实例 $\prod_U^i$ 是新鲜的。

匹配会话。如果 1)一个实例来自客户集合$\mathcal{C}$，另一个实例来自服务器集合$\mathcal{S}$；2)实例 $\prod_U^i$ 和 $\prod_V^j$ 都已经接受；3) $pid_U^i = V$，$pid_V^j = U$；4) $sid_U^i = sid_V^j =: sid$ 并且值非空；5)没有其他实例接受 $sid = SID$，则称 $\prod_U^i$ 和 $\prod_V^j$ 互为匹配会话，

安全性定义。在游戏中，$\mathcal{A}$可以次执行 Execute、Send、Test 询问，游戏结束时$\mathcal{A}$输出 b'，若 $b' = b$，则$\mathcal{A}$成功攻破协议。设 n 是安全参数，D_n 是口令空间，$\mathcal{A}$攻击协议的优势定义为 $Adv_{D_n, G_x}(\mathcal{A}) = 2Pr[Succ_P^{ake}(\mathcal{A})] - 1$，其中，$Pr[Succ_P^{ake}(\mathcal{A})]$ 是敌手攻击协议 P 成功的概率。

3　基于格的密钥协商协议

针对之前协议存在的安全性问题，提出了基于格的三方口令认证密钥协商协议，减少了公钥长度，降低了计算复杂度和消息传输量，提高了协议

的运行速度，实现了用户的匿名性。其中，隐式密钥协商协议通信量较少，显式认证密钥协商协议更安全。协议中使用的符号如表 1 所示。

表 1　　本文方案使用的符号说明

符号	说明
B、C	客户 B 和 C
TID_B、TID_C	客户 B 和 C 的临时身份
S	远程服务器
pw_B、pw_C	客户 B 和 C 的口令
h、H_1、H_2、H_3、H_4	散列函数
β、ω	$\beta \in \{0,1\}, \omega \in \{0,1\}^n$
a、s	$a, s \in R_q$
R_q	多项式环
χ_β	环上的高斯分布
Cha、Mod_2	函数
$\oplus$	异或运算符
$\mathcal{A}$	概率多项式时间敌手
$\mathcal{CH}$	挑战者
sk_{BC}	由客户 B 和 C 生成的会话密钥

3.1　基于格的三方隐式认证密钥协商方案

基于格的三方隐式认证密钥协商方案（以下简称方案 1）如图 1 所示。

3.1.1　初始化阶段

当客户 B 和 C 进行安全通信时，用户分别输入临时身份 TID_B、TID_C 在服务器的协助下进行相互认证，并协商一个共享的会话密钥，协议基于 RLWE 困难问题，其中，$R_q = \frac{Z_q}{x^n} + 1$ 是一个环，χ_β 是 R_q 上的高斯分布，Cha 和 Mod_2 是 2 个函数，$\sigma = Mod_2(k_S, \omega) = Mod_2(k_B, \omega) = Mod_2(k_C, \omega)$。当客户加入系统时，需要向服务器 S 注册。注册过程以客户 B 为例说明，具体如下。

1) $B \to S$:(B, Hpw_B)

客户 B 自由选择身份标识 B 和口令 pw_B，并随机选择一个随机数 a。B 计算 $Hpw_B = h(pw_B \| a)$，并将注册请求(B, Hpw_B)发送给服务器 S。

2) $S \to B$:$(TID_B, H(\cdot))$

当服务器 S 收到客户 B 的注册请求消息(B, Hpw_B)后，计算 $TID_B = B \oplus Hpw_B$，并将 TID_B、

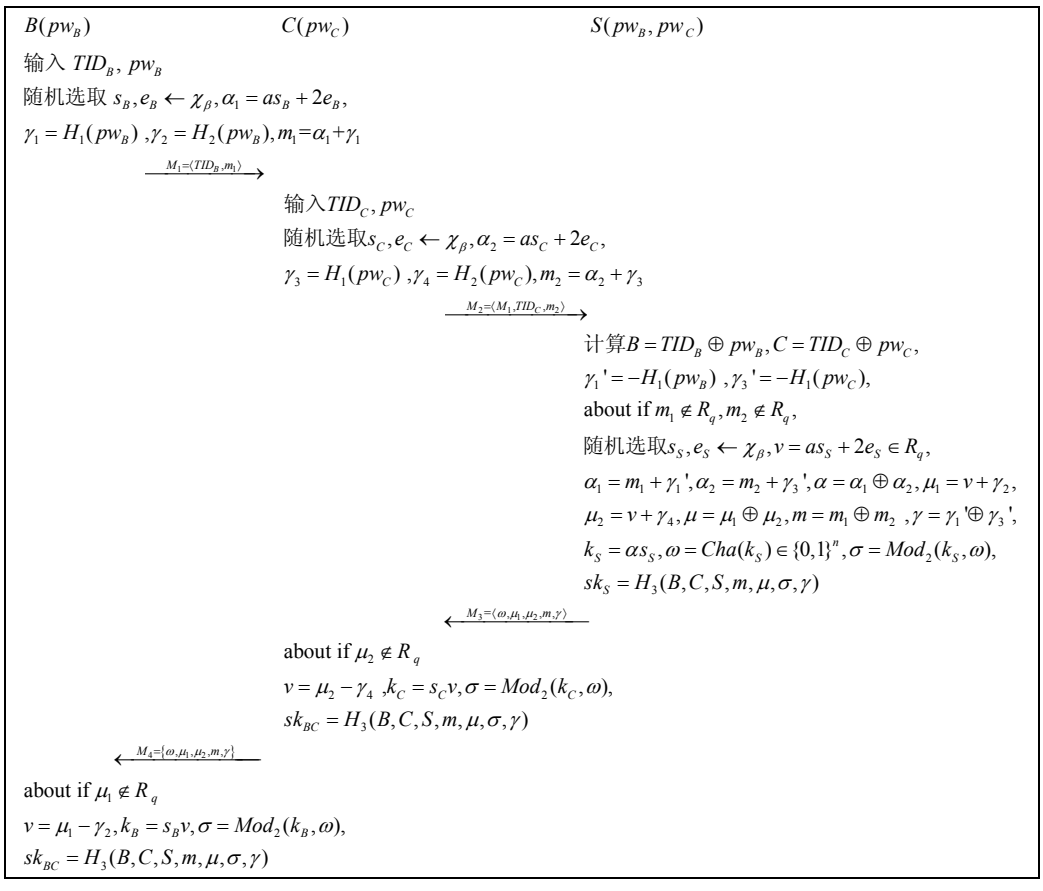

图 1　基于格的三方隐式认证密钥协商方案

$H(\cdot)$ 发送给客户 B。

3.1.2　隐式认证与密钥协商阶段

1) $B \to C: M_1 = \langle TID_B, m_1 \rangle$

客户 B 输入 TID_B、pw_B，随机选取 $s_B, e_B \leftarrow \chi_\beta$，计算 $\alpha_1 = as_B + 2e_B$，$\gamma_1 = H_1(pw_B)$，$\gamma_2 = H_2(pw_B)$ 和 $m_1=\alpha_1+\gamma_1$，B 发送 M_1 给 C。

2) $C \to S: M_2 = \langle M_1, TID_C, m_2 \rangle$

收到 M_1 后，客户 C 输入 TID_C、pw_C，随机选取 $s_C, e_C \leftarrow \chi_\beta$，计算 $\alpha_2 = as_C + 2e_C$，$\gamma_3 = H_1(pw_C)$，$\gamma_4 = H_2(pw_C)$ 和 $m_2=\alpha_2+\gamma_3$，C 发送 M_2 给 S。

3) $S \to C: M_3 = \langle \omega, \mu_1, \mu_2, m, \gamma \rangle$

收到 M_2 后，S 进行验证客户 B 和 C 的身份，计算 $B = TID_B \oplus pw_B$，$C = TID_C \oplus pw_C$，验证客户 B 和 C 的身份成功后，计算 $\gamma_1' = -H_1(pw_B)$ 和 $\gamma_3' = -H_1(pw_C)$，如果 $m_1 \notin R_q$，$m_2 \notin R_q$，S 随机选取 $s_S, e_S \leftarrow \chi_\beta$，计算 $v = as_S + 2e_S \in R_q$，$\alpha_1 = m_1 + \gamma_1'$，$\alpha_2 = m_2 + \gamma_3'$，$\alpha = \alpha_1 \oplus \alpha_2$，$\mu_1 = v + \gamma_2$，$\mu_2 = v + \gamma_4$，$\mu = \mu_1 \oplus \mu_2$，$m = m_1 \oplus m_2$，$\gamma = \gamma_1' \oplus \gamma_3'$，$k_S = \alpha s_S$，$\omega = Cha(k_S) \in \{0,1\}^n$，$\sigma = Mod_2(k_S, \omega)$ 和 $sk_S = H_3(B, C, S, m, \mu, \sigma, \gamma)$，$S$ 发送 M_3 给 C。

4) $C \to B: M_4 = \langle \omega, \mu_1, \mu_2, m, \gamma \rangle$

收到 M_3 后，C 进行验证 $\mu_2 \notin R_q$ 后，计算 $v = \mu_2 - \gamma_4$，$k_C = s_C v$，$\sigma = Mod_2(k_C, \omega)$ 和 $sk_{BC} = H_3(B, C, S, m, \mu, \sigma, \gamma)$。

5) $sk_{BC} = H_3(B, C, S, m, \mu, \sigma, \gamma)$

收到 M_4 后，B 进行验证 $\mu_1 \notin R_q$ 后，计算 $v = \mu_1 - \gamma_2$，$k_B = s_B v$，$\sigma = Mod_2(k_B, \omega)$ 和 $sk_{BC} = H_3(B, C, S, m, \mu, \sigma, \gamma)$，此时 B 和 C 拥有共同的会话密钥。

3.2　基于格的三方显式认证密钥协商方案

由于基于格的三方隐式认证密钥协商方案通信量少、认证速度快，但不能保证用户得到了相应的会话密钥，因此，提出基于格的三方显式认证密钥协商方案（以下简称方案 2），如图 2 所示。

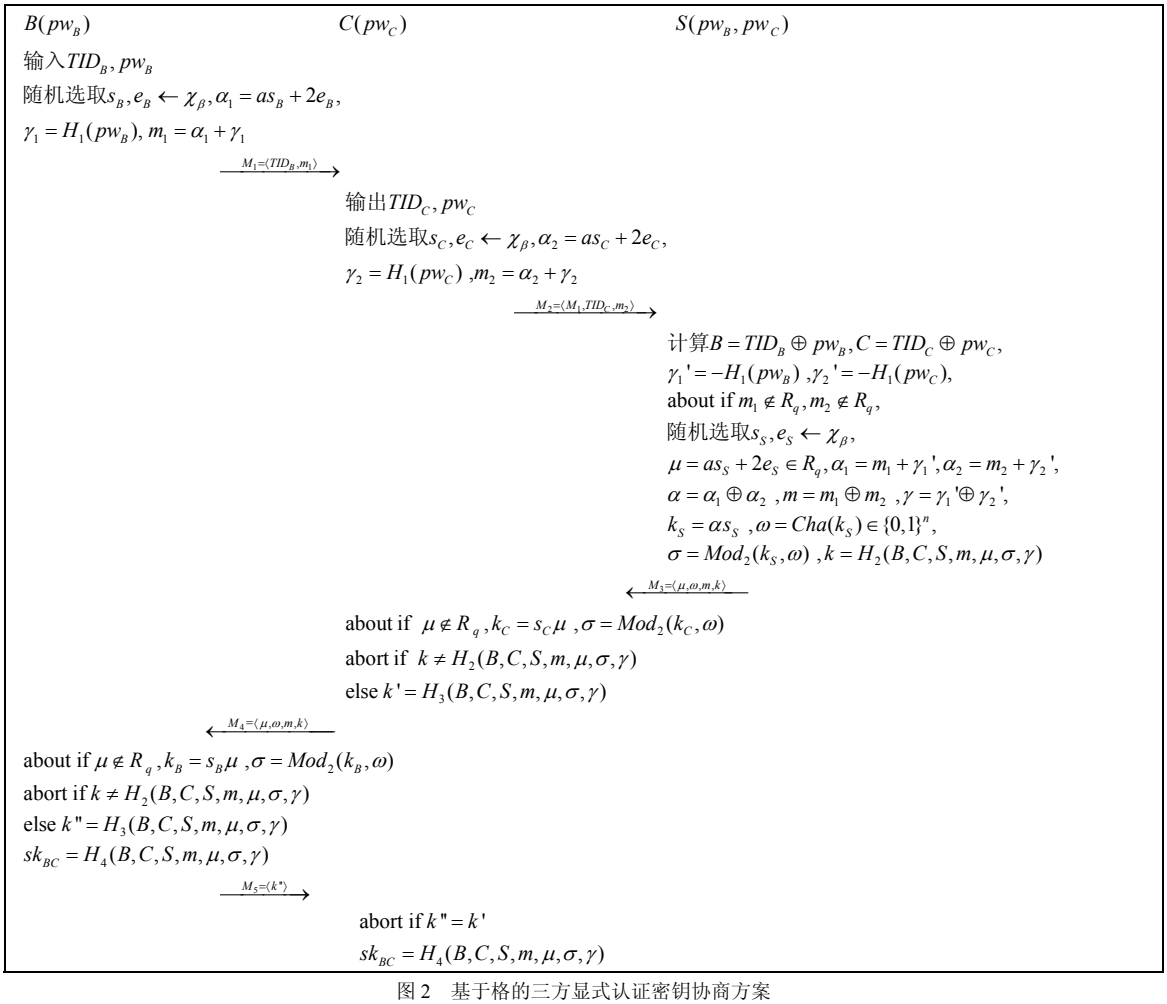

图 2　基于格的三方显式认证密钥协商方案

3.2.1 *初始化阶段*

基于格的显式认证密钥协商协议的初始化阶段和基于格的隐式认证密钥协商协议的初始化阶段相同，见 3.1.1 节。

3.2.2 显式认证与密钥协商阶段

1)$B \to C: M_1 = \langle TID_B, m_1 \rangle$

客户 B 输入 TID_B、PW_B，随机选取 $s_B, e_B \leftarrow \chi_\beta$，计算 $\alpha_1 = as_B + 2e_B$，$\gamma_1 = H_1(pw_B)$，$m_1 = \alpha_1 + \gamma_1$，$B$ 发送 M_1 给 C。

2)$C \to S: M_2 = \langle M_1, TID_C, m_2 \rangle$

收到 M_1 后，客户 C 输入 TID_C、PW_C，随机选取 $s_C, e_C \leftarrow \chi_\beta$，计算 $\alpha_2 = as_C + 2e_C$，$\gamma_2 = H_1(pw_C)$ 和 $m_2 = \alpha_2 + \gamma_2$，$C$ 发送 M_2 给 S。

3) $S \to C: M_3 = \langle \mu, \omega, m, k \rangle$

收到 M_2 后，S 进行验证客户 B 和 C 的身份，S 计算 $B = TID_B \oplus pw_B$，$C = TID_C \oplus pw_C$，验证客户 B 和 C 的身份成功后，计算 $\gamma_1' = -H_1(pw_B)$ 和 $\gamma_2' = -H_1(pw_C)$，如果 $m_1 \notin R_q$，$m_2 \notin R_q$，S 随机选取 $s_S, e_S \leftarrow \chi_\beta$，计算 $\mu = as_S + 2e_S \in R_q$，$\alpha_1 = m_1 + \gamma_1'$，$\alpha_2 = m_2 + \gamma_2'$，$\alpha = \alpha_1 \oplus \alpha_2$，$m = m_1 \oplus m_2$，$\gamma = \gamma_1' \oplus \gamma_2'$，$k_S = \alpha s_S$，$\omega = Cha(k_S) \in \{0,1\}^n$，$\sigma = Mod_2(k_S, \omega)$，$k = H_2(B, C, S, m, \mu, \sigma, \gamma)$，$S$ 发送 M_3 给 C。

4) $C \to B: M_4 = \langle \mu, \omega, m, k \rangle$

收到 M_3 后，C 进行验证 $\mu \notin R_q$ 后，计算 $k_C = s_C \mu$，$\sigma = Mod_2(k_C, \omega)$，如果 $k \neq H_2(B, C, S, m, \mu, \sigma, \gamma)$，则 $k' = H_3(B, C, S, m, \mu, \sigma, \gamma)$，$C$ 发送 M_4 给 B。

5) $B \to C: M_5 = \langle k'' \rangle$

收到 M_4 后，B 进行验证，$\mu \notin R_q$ 后，计算 $k_B = s_B \mu$，$\sigma = Mod_2(k_B, \omega)$，如果 $k \neq H_2(B, C, S, m, \mu, \sigma, \gamma)$，则 $k'' = H_3(B, C, S, m, \mu, \sigma, \gamma)$，$B$ 发送 M_5 给 C。

6) $sk_{BC} = H_4(C, B, S, m, \mu, \sigma, \gamma)$

收到 M_5 后，C 进行验证，如果 $k'' = k'$，此时 B 和 C 拥有共同的会话密钥 $sk_{BC} = H_4(C, B, S, m, \mu, \sigma, \gamma)$。

3.3 方案的正确性

2 个方案的正确性证明相同，下面是诚实用户执行方案 2 时双方拥有相同的会话密钥的正确性证明。

q 是一个大素数，如 $q > 16\beta^2 n^{\frac{3}{2}}$，在协议诚实执行之后，2 个用户获得的会话密钥不匹配的概率是可忽略的。由引理 3 得，如果 k_C 和 k_S 非常接近，即 $|k_C - k_S| < \frac{q}{4}$，则每一方有相同的 σ 值。$k_C = s_C \mu = s_C(as_S + 2e_S) = as_C s_S + 2e_S s_C$，$k_S = as_S = (as_C + 2e_C)s_S = as_C s_S + 2e_C s_S$，得到 $|k_C - k_S| = 2[e_S s_C - e_C s_S]$。由引理 2 得，每一个 e_S、s_C、e_C、s_S 小于 $\beta\sqrt{n}$ 的概率是不可忽略的，由引理 1 和三角不等式的性质可得 $\|k_C - k_S\| \leqslant 4\beta^2 n^{\frac{3}{2}} < \frac{q}{4}$，因此，$Mod_2(k_C, Cha(k_S)) = Mod_2(k_S, Cha(k_S))$。同理可得，$Mod_2(k_B, Cha(k_S)) = Mod_2(k_S, Cha(k_S))$。综上所述，诚实用户执行方案 2 时，双方拥有相同的会话密钥。

4 安全性证明

认证协议能否得到广泛应用，不仅要设计合理，还要验证协议的正确性和安全性，在文献[17]的安全模型基础上，给出基于格的三方隐式认证密钥协商协议的安全性证明。格理论是设计后量子安全公钥密码体制的一种重要基础理论，存在多种基于格的困难问题在量子计算下不存在多项式时间高效求解算法，因此，本文方案基于格上 RLWE 困难问题设计的密码协议可以抵抗量子攻击。由于基于格的三方显式认证密钥协商协议和基于格的三方隐式认证密钥协商协议证明方法相同，因此，只列出基于格的三方隐式认证密钥协商协议的证明过程。证明思路如下：定义协议 $P_i (i = 1, \cdots, 7)$，其中，$P_0 = P$，敌手攻击协议 P_{i-1} 的优势是可忽略的。敌手攻击协议 P_i 的优势大于敌手攻击协议 P_{i-1} 的优势，即协议 $P_0, P_1, \cdots, P_7$ 的安全性逐渐降低，最后，证明敌手攻击协议 P_7 成功的概率不大于 $\frac{n_{se}}{L}$，即协议 P_7 是安全的，因此，协议 P 是安全的。

定理 1 设敌手的运行时间为 t，其中，n_{se}、n_{ex}、n_{re}、n_{co} 分别表示询问类型 Send、Execute、Reveal、Corrupt，n_{ro} 表示询问随机预言机，$t' = O(t + (n_{ro} + n_{se} + n_{ex})t_{exp})$，敌手攻击协议 P 的优势定义为 $Adv_p^{ake}(\mathcal{A}) = \frac{n_{se}}{L} + O(Adv_{R_q}^{PWE}(t', n_{ro}^2) + \frac{(n_{se} + n_{ex}) + (n_{ro} + n_{se} + n_{ex})}{q^n})$。

协议 $P_0, P_1, \cdots, P_7$ 中，$P_0 = P$，有 $Adv_{p_0}^{ake}(\mathcal{A}) \leqslant Adv_{p_1}^{ake}(\mathcal{A}) + \varepsilon_1 \leqslant \cdots \leqslant Adv_{p_7}^{ake}(\mathcal{A}) + \varepsilon_7$ 成立，其中，$\varepsilon_1, \cdots, \varepsilon_7$ 是可忽略的值。

1) 假设 $n_{ro} \geqslant 1$ 且 $n_{se} + n_{ex} \geqslant 1$。

2) 假设随机预言机对任何新询问都使用新的输出进行响应，重复询问之前的消息时，输出相同。

3) 假设 $H_1(pw)$ 询问输出 $(as_h + 2e_h) \in R_q$，$H_2(pw)$ 询问输出 $(as_{h'} + 2e_{h'}) \in R_q$，已知 $(s_h + e_h)$ 和 $(s_{h'} + e_{h'})$。

4) 如果敌手 $\mathcal{A}$ 进行 $H_l(\cdot)$ 询问，其中，$l \in \{1,2\}$，相应的 $H_l'(\cdot)$ 询问自动进行，其中，$l' \in \{1,2\} \setminus \{l\}$。虽然所有的询问都由敌手 $\mathcal{A}$ 发出，但是 $\mathcal{A}$ 仅能看到 $H_l(\cdot)$ 的输出。

各协议介绍如下。

协议 P_0：原始协议 P。

协议 P_1：如果诚实用户随机选择协议使用过的 m 或 μ 值，则协议停止，敌手失败。

协议 P_2：协议在 Send 和 Execute 询问时不使用随机预言询问，敌手 $\mathcal{A}$ 的随机预言询问后返回与 Send 和 Execute 询问的结果响应一致。

协议 P_3：如果 $H_3(\langle C, B, S, m, \mu, \sigma, \gamma' \rangle)$ 询问被执行，则不检查 Execute 询问的一致性。因此，协议以随机输出进行响应而不是为了保持与 Execute 查询的一致性而进行反馈。

协议 P_4：如果对客户端实例或服务器实例进行了正确的密码猜测（由 $H_3(\cdot)$ 询问，使用正确的输入来计算会话密钥），则协议停止，敌手成功。

协议 P_5：如果敌手对同一服务器实例进行 2 次口令猜测，协议停止，敌手失败。

协议 P_6：如果敌手对同一客户端实例进行 2 次口令猜测，协议停止，敌手失败。

协议 P_7：协议使用内部口令预言机，保存所有口令并接受询问，该询问测试给定口令是否为给定客户端或服务器的正确口令。内部口令预言机对敌手无效，预言机在初始化过程中生成所有的口令。若来自 P_4 的正确口令猜测被改变，使每当敌手进行口令询问时，向预言机提交查询以确定它是否正确。

引理 4　对任何敌手 $\mathcal{A}$，有 $Adv_{p_0}^{ake}(\mathcal{A}) \leqslant Adv_{p_1}^{ake}(\mathcal{A}) + \dfrac{O((n_{se} + n_{ex}) + (n_{ro} + n_{se} + n_{ex}))}{q^n}$。

证明　考虑最新生成的 m 或 μ 值，Send、Execute 或询问随机预言机的概率是 $\dfrac{(n_{ro} + n_{se} + n_{ex})}{q^n}$，如果事件 E 不发生，$n_{se} + n_{ex}$ 的值是唯一的。任何一个 m 或 μ 值不唯一的概率是 $\dfrac{O((n_{se} + n_{ex}) + (n_{ro} + n_{se} + n_{ex}))}{q^n}$。

引理 5　对任何敌手 $\mathcal{A}$，有 $Adv_{p_1}^{ake}(\mathcal{A}) = Adv_{p_2}^{ake}(\mathcal{A}) + \dfrac{O(n_{ro})}{q^n}$。

证明　P_1 和 P_2 在敌手进行 $H_3(\langle C, B, S, m, \mu, \sigma, \gamma_1' \rangle)$ 询问时才能区分，其中，$\gamma_1' = -H_1(pw_B)$，敌手不进行 $H_1(\cdot)$ 询问的概率是可忽略的。

引理 6　对任何敌手 $\mathcal{A}$ 的运行时间 t，有 $t' = O(t + (n_{ro} + n_{se} + n_{ex})t_{exp})$，即 $Adv_{p_2}^{ake}(\mathcal{A}) \leqslant Adv_{p_3}^{ake}(\mathcal{A}) + 2Adv_{R_q}^{PWE}(t', n_{ro})$。

证明　事件 E 不发生时，P_2 和 P_3 是不可区分的，$\mathcal{A}$ 运行协议 P_2 时，事件 E 发生的概率为 ε，所以有 $Pr[Succ_{p_2}^{ake}(\mathcal{A})] \leqslant Pr[Succ_{p_3}^{ake}(\mathcal{A})] + \varepsilon$，即 $Adv_{p_2}^{ake}(\mathcal{A}) \leqslant Adv_{p_3}^{ake}(\mathcal{A}) + 2\varepsilon$。

假设存在算法 D 可以解决判定性 RLWE 困难问题，模拟协议，已知 (a, X, Y, W)，模拟 P_2 中 $\mathcal{A}$ 的变化。

1) Execute($\mathcal{C}, i, \mathcal{S}, j$)询问，设置 $m = X + (as_f + 2e_f)$，其中，$s_f, e_f \leftarrow R_q$；$\mu = Y + (as_{ff} + 2e_{ff})$，其中，$s_{ff}, e_{ff} \leftarrow \chi_\beta$，且 $\omega \leftarrow \{0,1\}^n$。

2) $\mathcal{A}$ 完成后，对每一个 $H_l(\langle C, B, S, m, \mu, \sigma, \gamma' \rangle)$ 询问，其中，$l \in \{2,3,4\}$，在执行询问时生成 m 和 μ，H_l 询问返回 $-\gamma_1' = as_h + 2e_h \in R_q$，模拟计算 k_S，有

$$\begin{aligned} k_S &= \alpha(s_y + s_{ff}) = (X - (as_h + 2e_h))(s_y + s_{ff}) \\ &= Xs_y - (as_h + 2e_h)s_y + (X - (as_h + 2e_h))s_{ff} \\ &\approx Xs_y - Ys_h + (X - (as_h + 2e_h))s_{ff} \\ &= Xs_y - Ys_h + (X + \gamma_1')s_{ff} \end{aligned} \tag{2}$$

所以有 $Xs_y = k_S + Ys_h - (X + \gamma_1')s_{ff}$，因此，$\sigma' = Mod_2(k_S + Ys_h - (X + \gamma_1')s_{ff}, W)$。最后，将 σ' 的值添加到 $\tau(X, s)$ 的列表中。

在执行询问期间，模拟器设置 $m = X + (as_f + 2e_f)$ 代替 $m = as_m + 2e_m$，因为 X 是从 R_q 中随机选择的，所以是不可区分的。当模拟器设置 $\mu = Y + (as_{ff} + 2e_{ff})$ 代替 $\mu = as_S + 2e_S$ 时，由于判定性 RLWE 问题，所以是不可区分的。综上所述，这

种模拟与 P_2 不可区分，直到 E 发生或以不可忽略的优势解决判定性 RLWE 问题。t' 是算法 D 的运行时间，D 以 ε 的优势创建大小为 n_{ro} 的列表，$t'=O(t+(n_{\mathrm{ro}}+n_{\mathrm{se}}+n_{\mathrm{ex}})t_{\exp})$，则 $Adv_{R_q}^{ake}(D)\leqslant Adv_{R_q}^{PWE}(t',n_{\mathrm{ro}})$。

引理 7 对任何敌手 $\mathcal{A}$，有 $Adv_{p_3}^{ake}(\mathcal{A})\leqslant Adv_{p_4}^{ake}(\mathcal{A})$。

证明 显然成立，因为增加了敌手赢得游戏的机会。

引理 8 对任何敌手 $\mathcal{A}$ 的运行时间 t，有 $t'=O(t+(n_{\mathrm{ro}}+n_{\mathrm{se}}+n_{\mathrm{ex}})t_{\exp})$，即 $Adv_{p_4}^{ake}(\mathcal{A})\leqslant Adv_{p_5}^{ake}(\mathcal{A})+4Adv_{R_q}^{PWE}(t',(n_{\mathrm{ro}})^2)$。

证明 敌手 $\mathcal{A}$ 模拟运行协议 P_5，对同一服务器实例 2 次口令猜测发生的概率为 ε，构造算法 D，模拟协议，已知 (a,X,Y,W)，模拟 P_5 中 $\mathcal{A}$ 的变化。

1) $H_l(pw)$ 询问，输出 $Xs_h+(as_f+2e_f)$。

2)用消息 $\langle C,m\rangle$ 询问服务器实例 Π_S^j，其中，$m\in R_q$，设置 $\mu=Y+(as_{\mathit{ff}}+2e_{\mathit{ff}})$，其中，$s_{\mathit{ff}},e_{\mathit{ff}}\leftarrow\chi_\beta$。

3)不成对的客户端实例 Π_C^i 接收非法询问时终止，服务器实例 Π_S^j 接收协议最后的消息询问时终止。此时，$H_l(\cdot)$ 询问输出服从 $\{0,1\}^k$ 中的均匀分布。

4) $\mathcal{A}$ 完成后，对每一个 $H_l(\langle C,B,S,m,\mu,\sigma,\gamma'\rangle)$ 和 $H_{l'}(\langle C,B,S,m,\mu,\hat{\sigma},\hat{\gamma}'\rangle)$ 询问，其中，$l,l'\in\{2,3,4\}$，$\sigma\in R_q$ 和 $\hat{\sigma}\in R_q$，SA_1 询问服务器实例 Π_S^j，输入 $\langle C,m\rangle$，输出 $\langle\mu,\mathrm{k},\omega'\rangle$，其中，$m\in R_q$。$H_l(pw)$ 询问返回 $-\gamma_1'=Xs_h+(as_f+2e_f)\in R_q$，$H_l(p\hat{w})$ 询问返回 $-\hat{\gamma}_1'=Xs_{\hat{h}}+(as_{\hat{f}}+2e_{\hat{f}})\in R_q$ 且 $s_h\neq s_{\hat{h}}$。模拟计算

$$\begin{aligned}k_S&=\alpha(s_y+s_{\mathit{ff}})=(m+\gamma_1')(s_y+s_{\mathit{ff}})\\ \hat{k}_S&=\alpha(s_y+s_{\mathit{ff}})=(m+\hat{\gamma}_1')(s_y+s_{\mathit{ff}})\\ \hat{k}_S-k_S&=(\hat{\gamma}_1'-\gamma_1')(s_y+s_{\mathit{ff}})\\ &=(\hat{\gamma}_1'-\gamma_1')s_y+(\hat{\gamma}_1'-\gamma_1')s_{\mathit{ff}}\end{aligned}\tag{3}$$

所以有 $Xs_y=(\hat{k}_S-k_S-Y(s_f-s_f)-(\hat{\gamma}_1'-\gamma_1')s_{\mathit{ff}})(s_h-s_{\hat{h}})^{-1}$，因此，将 $Mod_2[(\hat{k}_S-k_S-Y(s_f-s_{\hat{f}})-(\gamma_1'-\hat{\gamma}_1')s_{\mathit{ff}})(s_h-s_{\hat{h}})^{-1},W]$ 的值添加到 $\tau(X,s)$ 的列表中。此模拟与 P_5 是不可区分的，对同一服务器实例 2 次口令猜测发生的概率为 ε。假设 $\mathcal{A}$ 遵循时间和询问限制，模拟器可以阻止 $\mathcal{A}$ 超过这些界限。t' 是算法 D 的运行时间，D 以 ε 的优势创建大小为 $n_{\mathrm{ro}}{}^2$ 的列表，$t'=O(t+(n_{\mathrm{ro}}+n_{\mathrm{se}}+n_{\mathrm{ex}})t_{\exp})$，因此，$Adv_{R_q}^{PWE}(D)\leqslant Adv_{R_q}^{PWE}(t',n_{\mathrm{ro}}{}^2)$。

引理 9 对任何敌手 $\mathcal{A}$ 的运行时间 t，有 $t'=O(t+(n_{\mathrm{ro}}+n_{\mathrm{se}}+n_{\mathrm{ex}})t_{\exp})$，即 $Adv_{p_5}^{ake}(\mathcal{A})\leqslant Adv_{p_6}^{ake}(\mathcal{A})+4Adv_{R_q}^{PWE}(t',(n_{\mathrm{ro}})^2)$。

证明 与引理 4 的证明相同，R_q 的随机元素添加到 $H_2(\cdot)$ 询问的输出中，并将 X 添加到 R_q 的随机元素中。

引理 10 对任何敌手 $\mathcal{A}$ 的运行时间 t，有 $Adv_{p_6}^{ake}(\mathcal{A})=Adv_{p_7}^{ake}(\mathcal{A})$。敌手 $\mathcal{A}$ 运行协议 P_7 成功的概率为

$$\begin{aligned}&Pr(Succ_{p_7}^{ake}(\mathcal{A}))\leqslant Pr(correctpw)+\\ &Pr(Succ_{p_7}^{ake}(\mathcal{A})|\neg correctpw)Pr(\neg correctpw)\end{aligned}\tag{4}$$

证明 P_6 和 P_7 是完全不可区分的。

如果从长度为 L 的口令字典中统一选择口令，则 $Pr(correctpw)\leqslant\frac{n_{\mathrm{se}}}{L}$。因为在口令预言机最多 n_{se} 次询问后发生损坏询问。

因为 *correctpw* 事件不发生，则 $\mathcal{A}$ 成功的唯一方法是对新的实例 Π_U^i 进行一个 Test 询问，并猜测 Test 查询中使用的比特。敌手不依赖于 sk_U^i，则成功的概率为 $\frac{1}{2}$，即 $Pr(Succ_{p_7}^{ake}(\mathcal{A})|\neg correctpw)=\frac{1}{2}$。

根据 Reveal$(\mathcal{U},i)$ 询问的定义，没有新的实例 Π_U^i，也没有 $\Pi_j^{U'}$ 的 Reveal$(\mathcal{U}',j)$ 询问。执行协议 P_1 时，如果有超过一个客户端实例和一个服务器实例使用相同的 *sid*，则敌手失败。因此，Reveal 询问的输出独立于 sk_U^i。

执行协议 P_4 时，$H_3(\cdot)$ 询问返回独立的随机值。因此，在 sk_U^i 之后 $H_3(\cdot)$ 询问独立于 sk_U^i。所以，敌手不依赖于 sk_U^i，则成功的概率是 $\frac{1}{2}$。因为 $Pr(\neg correctpw)=1-Pr(correctpw)$，所以有

$$\begin{aligned}&Pr(Succ_{p_7}^{ake}(\mathcal{A}))\leqslant Pr(correctpw)+\\ &Pr(Succ_{p_7}^{ake}(\mathcal{A})|\neg correctpw)Pr(\neg correctpw)\\ &\leqslant Pr(correctpw)+Pr(Succ_{p_7}^{ake}(\mathcal{A})|\neg correctpw)\\ &(1-Pr(correctpw))\\ &\leqslant\frac{n_{\mathrm{se}}}{L}+\frac{1}{2}\left(1-\frac{n_{\mathrm{se}}}{L}\right)\\ &\leqslant\frac{1}{2}+\frac{n_{\mathrm{se}}}{2L}\end{aligned}\tag{5}$$

表 2　　**性能比较**

协议	文献[6]方案	文献[11]方案	文献[12]方案	文献[13]方案	文献[16]方案	本文方案 1	本文方案 2
类型	2-party	3-party	2-party	2-party	3-party	3-party	3-party
用户匿名性	否	否	否	否	否	是	是
相互认证	否	是	是	是	是	是	是
抵抗量子攻击	能	能	能	能	能	能	能
不可测字典攻击	否	是	是	是	是	是	是
困难假设	LWE	ASPH	RLWE	RLWE	ASPH	RLWE	RLWE
采样数	$m=\Omega(n\lg q)$	$m=\Omega(n\lg q)$	$m=\Omega(n\lg q)$	$m=\Omega(\lg q)$	$m=\Omega(n\lg q)$	$m=\Omega(\lg q)$	$m=\Omega(\lg q)$
公钥长度/bit	$m(2n+1)\lg q$	$3mn\lg q$	$m(2n+1)\lg q$	$2mn\lg q$	$m(2n+1)\lg q$	$2mn\lg q$	$2mn\lg q$
密文扩展率	$\frac{m}{n}$	$\frac{3mn}{n-1}$	$\frac{2mn}{n-1}$	$\frac{m}{n}$	$\frac{3mn}{n-1}$	$\frac{m}{n}$	$\frac{m}{n}$
运算方法	矩阵运算	环运算	环运算	环运算	环运算	环运算	环运算
计算复杂度	$O(mn)$	$O(m\lg n)$	$O(2^{2n-2})$	$O(m\lg n)$	$O(2^{2n+2})$	$O(m\lg n)$	$O(m\lg n)$
消息传输量/轮	3	3	2	2/3	4	2	3

因此，有 $Pr(Succ_{p_7}^{ake}(\mathcal{A}))\leqslant\frac{n_{se}}{L}$。

综合引理 4~引理 10 的结论可知，定理 1 结论成立。因此，方案可证明是安全的。

5　协议性能比较

从安全性和效率出发，给出本文 2 个方案与文献[6,11~13,16]方案的比较，如表 2 所示。

在安全性方面，与传统的 3PAKE 协议相比，本文方案 1 和方案 2 能够抵抗量子攻击，同时实现了用户的匿名性以及用户和服务器的双向认证，可抵抗不可测在线字典攻击。文献[6]是基于 LWE 困难问题的 2PAKE 协议，需要 3 轮通信，所以 3PAKE 协议至少需要 6 轮通信，且不满足用户和服务器的相互认证，不能抵抗不可测字典攻击，不满足用户匿名性；文献[11]是基于 ASPH 的 3PAKE 协议，需要 3 轮通信，不满足用户的匿名性；文献[12]是基于 RLWE 困难问题的 2PAKE 协议需要 2 轮通信，所以 3PAKE 协议至少需要 4 轮通信，且不满足用户匿名性；文献[13]提出隐式认证和显式认证 2 个 2PAKE 方案，分别需要 2 轮和 3 轮通信，所以 3PAKE 协议至少需要 4 轮和 6 轮通信，效率较低且不满足用户匿名性；文献[16]提出基于 ASPH 的 3PAKE 协议，需要 4 轮即 8 条消息传输量，通信量多、效率较低且不满足用户匿名性。本文方案 1 和方案 2 是 3PAKE 协议，分别需要 2 轮和 3 轮通信，远高于文献[6,12,13,16]的通信效率。文献[11]与本文方案 2 的消息传输量相同，但效率低于本文方案 1。与现有方案相比，本文方案需要的采样数小，减少了公钥长度，降低了计算复杂度和消息传输量，提高了协议的运行速度，实现了用户的匿名性。因此，本文方案 1 和方案 2 具有更高的安全性和通信效率。

6　结束语

基于口令认证的密钥协商协议是用户仅选择一个简单的口令，通过服务器，在用户间建立一个共享的会话密钥。由于 2PAKE 协议不能实现大规模端到端的通信，且传统的困难问题不能抵抗量子攻击，因此，提出 2 个基于格的 3PAKE 协议，包括基于格的用户匿名三方隐式认证密钥协商方案和基于格的用户匿名三方显式认证密钥协商方案，并证明了协议的安全性。其中，隐式认证密钥协商协议通信量少、执行效率高，显式认证密钥协商协议安全性更高，同时实现用户和服务器的双向认证可抗不可测在线字典攻击。因此，所提协议既高效又安全。

参考文献：

[1] LAW L, MENEZES A, QU M, et al. An efficient protocol for authenticated key agreement[J]. Designs, Codes and Cryptography, 2003, 28(2): 119-134.

[2] ABADLLA M, FOUQUE P A, POINTCHEVAL D. Password-based authenticated key exchange in the three-party setting[C]//International Workshop on Public Key Cryptography. 2005: 65-84.

[3] RAIMANDO M D, GENNARO R. Provably secure threshold password-authenticated key exchange[J]. Journal of Computer and System Sciences, 2006, 72(6): 978-1001.

[4] ZHAO F, GONG P, LI S, et al. Cryptanalysis and improvement of a

three-party key agreement protocol using enhanced Chebyshev polynomials[J]. Nonlinear Dynamics, 2013, 74(1-2): 419-427.

[5] XIE Q, ZHAO J, YU X. Chaotic maps-based three-party password-authenticated key agreement scheme[J]. Nonlinear Dynamics, 2013, 74(4): 1021-1027.

[6] KATZ J, VAIKUNTANATHAN V. Smooth projective hashing and password-based authenticated key exchange from lattices[C]// International Conference on the Theory and Application of Cryptology and Information Security. 2009: 636-652.

[7] DING Y, FAN L. Efficient password-based authenticated key exchange from lattices[C]//2011 Seventh International Conference on Computational Intelligence and Security (CIS). 2011: 934-938.

[8] DING J, XIE X, LIN X. A simple provably secure key exchange scheme based on the learning with errors problem[J]. IACR Cryptology Eprint Archive, 2014: 688.

[9] FUJIOKA A, SUZUKI K, XAGAWA K, et al. Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism[C]//The 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. 2013: 83-94.

[10] 胡学先, 魏江宏, 叶茂. 对一个强安全的认证密钥交换协议的分析[J]. 电子与信息学报, 2013, 35(9): 2278-2282.
HU X X, WEI J H, YE M. Cryptanalysis of a strongly secure authenticated key exchange protocol[J]. Journal of Electronics & Information Technology, 2013, 35(9): 2278-2282.

[11] 叶茂, 胡学先, 刘文芬. 基于格的三方口令认证密钥交换协议[J]. 电子与信息学报, 2013, 35(6): 1376-1381.
YE M, HU X X, LIU W F. Password authenticated key exchange protocol in the three party setting based on lattices[J]. Journal of Electronics & Information Technology, 2013, 35(6): 1376-1381.

[12] ZHANG J, ZHANG Z, DING J, et al. Authenticated key exchange from ideal lattices[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2015: 719-751.

[13] DING J, ALASYIGH S, LANCRENON J, et al. Provably secure password authenticsated key exchange based on RLWE for the post-quantum world[C]//Cryptographers' Track at the RSA Conference. 2017: 183-204.

[14] 杨孝鹏, 马文平, 张成丽. 一种新型基于环上带误差学习问题的认证密钥交换方案[J]. 电子与信息学报, 2015, 37(8): 1984-1988.
YANG X P, MA W P, ZHANG C L. New authenticated key exchange scheme based on ring learning with errors problem[J]. Journal of Electronics & Information Technology, 2015, 37(8): 1984-1988.

[15] STEBILA D, MOSCA M. Post-quantum key exchange for the Internet and the open quantum safe project[R]. Cryptology Eprint Archive, Report 2016/1017, 2016.

[16] 杨晓燕, 侯孟波, 魏晓超. 基于验证元的三方口令认证密钥交换协议[J]. 计算机研究与发展, 2016, 53(10): 2230-2238.
YANG X Y, HOU M B, WEI X C. Verifier-based three-party password authenticated key exchange protocol[J]. Journal of Computer Research and Development, 2016, 53(10): 2230-2238.

[17] XU D, HE D, CHOO K R, et al. Provably secure three-party password authenticated key exchange protocol based on ring learning with error[J]. IACR Cryptology Eprint Archive, 2017: 360.

[作者简介]

王彩芬（1963-），女，河北安国人，博士，西北师范大学教授、博士生导师，主要研究方向为密码学、网络安全、信息安全。

陈丽（1991-）女，甘肃武威人，西北师范大学硕士生，主要研究方向为网络与信息安全、密钥协商协议。