基于 RLWE 支持身份隐私保护的双向认证密钥协商协议

杨亚涛[1,2]，韩新光[1,2]，黄洁润[2]，赵阳[2]

（1. 西安电子科技大学通信工程学院，陕西 西安 710071；2. 北京电子科技学院电子与通信工程系，北京 100070）

摘 要：为了解决执行认证密钥交换协议时通信双方身份隐私保护问题，提出了一种基于 C 类承诺机制的抗量子攻击的双向认证密钥协商协议。该协议通过 C 类承诺函数隐藏通信双方的真实身份信息，并基于 RLWE 困难问题，在保障身份匿名的前提下，通过 2 轮的消息交互不仅完成了双向身份认证，而且保证了传输消息的完整性，并协商出共享会话密钥。经过分析，在协议执行效率上，完成匿名的双向认证与密钥协商只需 2 轮的消息传输，与 Ding 等的协议对比，公钥长度缩短近 50%；在安全性上，所提协议能够抵抗伪造、重放、密钥复制和中间人攻击。所提协议在 eCK 模型下满足可证明安全性，同时所提协议基于格上的 RLWE 困难问题，可抵抗量子计算攻击。

关键词：隐私保护；承诺机制；格；双向认证；环上误差学习问题

中图分类号：TN918.4

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019218

Bidirectional authentication key agreement protocol supporting identity's privacy preservation based on RLWE

YANG Yatao[1,2], HAN Xinguang[1,2], HUANG Jierun[2], ZHAO Yang[2]

1. School of Telecommunication Engineering, Xidian University, Xi'an 710071, China

2. Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: In order to solve the problem of identity privacy preservation between two participants involved when implementing authenticated key agreement protocol, a bidirectional authenticated key agreement protocol against quantum attack based on C commitment scheme was proposed. Through the design of C commitment function, the real identity information of two participants involved was hidden. Based on RLWE difficult problem, under the premise to ensure identity anonymity, this protocol not only completed two-way identity authentication, but also ensured the integrity of the transmitted message, furthermore, the shared session key was negotiated. After been analyzed, in terms of protocol's execution efficiency, only two rounds of message transmission were needed to complete anonymous two-way authentication and key agreement in the proposed scheme. Compared with Ding's protocol, the length of public key was reduced by nearly 50%. With regard to security, the protocol could resist forgery, replay, key-copy, and man-in-the-middle attacks. It is proved that the proposed protocol satisfies the provable security under the eCK model. At the same time, the protocol is based on the RLWE problem of lattices, and can resist quantum computing attacks.

Key words: privacy preservation, commitment mechanism, lattice, bidirectional authentication, ring learning with error

收稿日期：2019–01–28；**修回日期**：2019–07–27

通信作者：韩新光，1098902457@qq.com

基金项目：“十三五”国家密码发展基金资助项目（No.MMJJ20170110）

Foundation Item: State Cryptography Development Fund of Thirteen Five-Year (No.MMJJ20170110)

1　引言

密钥交换协议（key exchange protocol）[1]能够使通信双方或者多方在复杂信道上安全通信。1976 年，Diffie 和 Hellman 设计了经典的 Diffie-Hellman 密钥交换协议[2]，密钥协商需要两轮消息传输，此协议无法抵抗敌手发起的中间人攻击和重放攻击等，同时也不能提供相互认证的功能。

2001 年，Li 等[3]提出适用于多服务环境的身份验证协议，这个解决方案导致通信成本和计算成本太高，不能适用于实际情况。2012 年，Liu 等[4]提出了一个基于离散对数问题的多服务器认证协议。2004 年，Tsaur 等[5]提出了一种基于 RSA 算法和大整数问题的多服务器协议。同年，Juang[6]提出另一种使用对称加密来验证身份的多服务器身份验证协议。然而，Chang 等[7]表明 Juang 的协议易受离线字典攻击，因此提出了一个克服 Juang 的协议安全漏洞的方案。2009 年，Regev 等[8]提出了带错误的学习（LWE, learning with error）问题，说明了格上的最短向量问题等。2009 年，Liao 等[9]提出了一种多服务器场景下的认证协议。2010 年，Wu 等[10]提出了基于用户认证的密钥交换协议，该协议可以抵抗重放和密钥复制等攻击，并保证部分前向安全。Yoon 等[11]引入了另一个基于客户端/服务器的用户认证密钥交换协议来提高性能。2010 年，Lyubashevsky 等[12]引入环上带误差学习（RLWE, ring learning with error）问题，困难性基于理想格上的最短向量问题（SVP, shortest vector problem）。2011 年，He 等[13]提出了椭圆曲线上的用户认证和密钥交换协议，该协议提供了远程相互认证与密钥协商，并可抵御各种已知的攻击。然而，Islam 等[14]证明了 He 等[13]的协议易受已知密钥会话临时攻击、冒充攻击，无法保证用户的匿名性。2010 年，Hao 等[15]提出了一个基于客户/服务器模型的 PAKE（password authenticated key exchange）协议，该协议的安全性基于离散对数的困难性，这很容易受到量子计算机的攻击。2015 年，Zhang 等[16]提出了一种新的基于格理论的认证与密钥交换方案。但是，他们需要参与者公钥/私钥对来完成身份认证。文献[17]提出了一隐私保护的会话密钥协商方法。文献[18]提出了一种身份隐藏且非延展安全的认证密钥协商方法。2016 年，文献[19]提出了基于 LWE 的 2PAKE 协议。文献[20]提出了关于验证元的三方口令认证密钥交换协议，但是存在效率低、占用资源多等缺点。2016 年，Tseng 等[21]提出了用户身份验证和基于身份的密码系统的密钥协商协议，该协议能够抵抗移动多服务器中的随机数泄露攻击。2018 年，Wu 等[22]提出了一种新的基于混沌映射的多服务器环境用户匿名认证密钥协商方案，不能抵抗量子计算机的攻击。同年，Sharma 等[23]提出了一种无配对的认证密钥协商协议，计算成本低，特别是对于低功率设备，但是存在长期密钥泄露和短暂密钥泄露的风险。2017 年，Jheng 等[24]提出了一种基于格理论的客户端/服务器端模型的口令认证密钥协商协议，该协议通过共享口令完成相互认证密钥协商，但该协议用户的身份信息不具有匿名性且不能抵抗中间人攻击。

本文设计了一种基于 RLWE 支持身份隐私保护的认证密钥协商协议。该协议通过 C 类承诺机制的设计，将通信双方不愿暴露的真实身份信息隐藏为承诺值的形式，承诺值消息具有完整性，不可篡改。协议基于 RLWE 困难问题，在保障身份匿名的前提下，通过 2 轮的消息交互不仅完成了双向身份认证，而且保证传输消息的完整性，并协商出共享会话密钥。通过分析，在协议执行效率上，完成匿名的双向认证与密钥协商只需经过 2 轮的消息传输，公钥长度较短。在安全性上，所提协议能够抵抗伪造攻击、重放攻击、密钥复制攻击和中间人攻击。在 eCK 模型下满足可证明安全性，可以抵抗量子计算攻击。

2　基础知识

2.1　格

简单地说，格（lattice）是实数空间中线性无关向量的整系数组合的集合。可以形式化地描述为给定 n 个 m 维的线性无关的向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n \in R^{m\times n}$，由它们作为基形成的格是由下列向量组成的集合，如式(1)所示。

$$\ell(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)=\left\{\sum_{i=1}^{n} x_i\boldsymbol{b}_i \mid x_i \in Z\right\} \tag{1}$$

其中，$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 为格的一组基，记为

$\boldsymbol{B}=[\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n]\in R^{m\times n}$。

2.2 RLWE 问题

定义 1 搜索性 RLWE 问题。令 $R=\dfrac{Z_q[x]}{x^n+1}, n=2^k, k\geqslant 1, q=1\bmod 2n, a\in R$, a 均匀随机选取，$\boldsymbol{e}\in R$ 是服从正态分布 ψ_α 的差错向量，若已知 $b\in R$，且 $b=as+\boldsymbol{e}$，则由 a、b 求解 s 的问题就是搜索性 RLWE 问题。

定义 2 判定性 RLWE 问题。令 $R=\dfrac{Z_q[x]}{x^n+1}, n=2^k, k\geqslant 1, q=1\bmod 2n, s\in R$, s 均匀随机选取，$\boldsymbol{e}\in R$ 是服从正态分布 ψ_α 的差错向量，计算 $b=as+\boldsymbol{e}$，且 $b\in R$。记 $A_{s,\psi}$ 为 (a,b) 的分布，则如何区分 $A_{s,\psi}$ 与 $R\times R$ 上的均匀分布问题就是判定性 RLWE 问题。假设判定性 RLWE 问题是困难的，则 $A_{s,\psi}$ 伪随机。

2.3 eCK 模型

定义 3 假设会话 $\Pi_{i,j}^s$ 是新鲜的，则满足以下条件。

1) 敌手 E 未对通信方 i,j 进行 Ephemeral_Secret Reveal()和 Static_Key Reveal()查询。

2) 敌手 E 未对会话 $\Pi_{i,j}^s$ 进行 Session_Key Reveal()查询。

这里假设敌手 E 能够任意伪造、重放和删除通信信息，是一个概率多项式时间的图灵机，且可完成以下功能。

1) Establish_Party(i)。敌手 E 可在 CA 上注册参与者 i 的公钥。

2) Ephemeral_Secret Reveal(i)。敌手 E 获得 i 的临时私钥。

3) Session_Key Reveal ($\Pi_{i,j}^s$)。敌手 E 获得会话 $\Pi_{i,j}^s$ 计算得出的会话密钥。

4) Send ($\Pi_{i,j}^s, m$)。敌手 E 向会话 $\Pi_{i,j}^s$ 发送消息 m，会话 $\Pi_{i,j}^s$ 遵循规范应答消息 m。

5) Static_Key Reveal(i)。敌手 E 获得 i 的长期私钥。

6) Test ($\Pi_{i,j}^s$)。敌手 E 只可完成一次此查询，在一次新鲜会话 $\Pi_{i,j}^s$ 中，随机投掷硬币 $b\in\{0,1\}$，若 b=0，返回真正的协商密钥，若 b=1，返回会话密钥空间中的任意随机数。最终敌手 E 输出比特数 b'，如果 $b'=b$，则敌手 E 获胜。

2.4 C 类承诺机制

G 是阶为 q 的群，q 是素数，N 是群 G 的生成元[25]。承诺时期，承诺者承诺被隐藏信息 $a\in\{0,1,2,\cdots,q-1\}$，计算 $\mathrm{com}()=N^a$，将 com() 函数值发送给接收者。打开承诺，承诺者发送 a 给接收者，接收者证实等式 $\mathrm{com}()=N^a$。

3 协议设计

3.1 协议参数选取

假设 n 是 2 的整数次幂，pw 是 Alice 和 Bob 的共享口令，G 是阶为 q 的群，q 是素数，N 是群 G 的生成元。素数 q 满足 $q>8$ 且 $q\bmod 2n=1$，R_q 是模数为 q 的多项式环，且 $R_q=\dfrac{Z_q[X]}{(X_n+1)}$，$X$ 是在 R_q 上的高斯离散分布，g 是双方共享的公共参数，(pk,sk) 是 Bob 的公钥/私钥对，$\mathrm{ID_A}$和$\mathrm{ID_B}$ 是 Alice 和 Bob 的身份信息，协议中的 com 函数为 $\mathrm{com}()=N^{H(\mathrm{ID})}$。协议中涉及的散列函数 H 使用 SHA256 算法，输出 256 bit 的消息摘要。

3.2 协议执行流程

协议的执行流程如图 1 所示，具体如下。

1) Alice 随机选择 $y_1\in(1,2,\cdots,q)$，计算 $u_1=y_1+H(\mathrm{ID_A})$，Alice 的身份信息 $\mathrm{ID_A}$ 经过 com() 函数处理得到承诺值 M_A。Alice 选取参数 $f_\mathrm{A}, \alpha, \mathrm{Nonce}\leftarrow\chi$，利用 f_A,α 生成认证参数 $X=g\alpha+2f_\mathrm{A}$，随后利用 Bob 的公钥 pk 加密得到 Alice 的身份认证信息 $\mathrm{Auth_A}$，之后将 $H(\mathrm{ID_A})\,|\,X\,|\,\mathrm{Auth_A}\,|\,u_1$ 发送给 Bob。

2) Bob 接收到 $H(\mathrm{ID_A})\,|\,X\,|\,\mathrm{Auth_A}\,|\,u_1$ 后进行以下操作。

① Bob 接收到数据 $u_1\,|\,H(\mathrm{ID_A})$，首先验证消息 $y_1\,|\,u_1\,|\,M_\mathrm{A}$ 的完整性。Bob 计算 $y_1=u_1-H(\mathrm{ID_A})$，$d_\mathrm{A}=N^{y_1}$，$M_\mathrm{A}=\mathrm{com}(\mathrm{ID_A})$。验证 $N^{u_1}=d_\mathrm{A}M_\mathrm{A}$ 是否成立，如果等式成立，证明消息传送过程中，参数未被更改，消息具有完整性；反之，则消息验证失败，Bob 拒绝通信。

② Bob 收到 $\mathrm{Auth_A}$ 后，利用自己的私钥 sk 解密得到散列值 $H_\mathrm{A}=H(X\,|\,M_\mathrm{A}\,|\,\mathrm{pw}\,|\,\mathrm{Nonce})$ 和随机参数 Nonce。Bob 利用参数 $X\,|\,M_\mathrm{A}\,|\,\mathrm{pw}\,|\,\mathrm{Nonce}$，首先计算 $H_\mathrm{B}=H(X\,|\,M_\mathrm{A}\,|\,\mathrm{pw}\,|\,\mathrm{Nonce})$，若 $H_\mathrm{B}=H_\mathrm{A}$，则 Alice 的身份认证通过；反之失败，Bob 拒绝通信。若身份认证成功，Bob 随后选取参数 $f_\mathrm{B}, \beta, r_\mathrm{B}\leftarrow\chi$

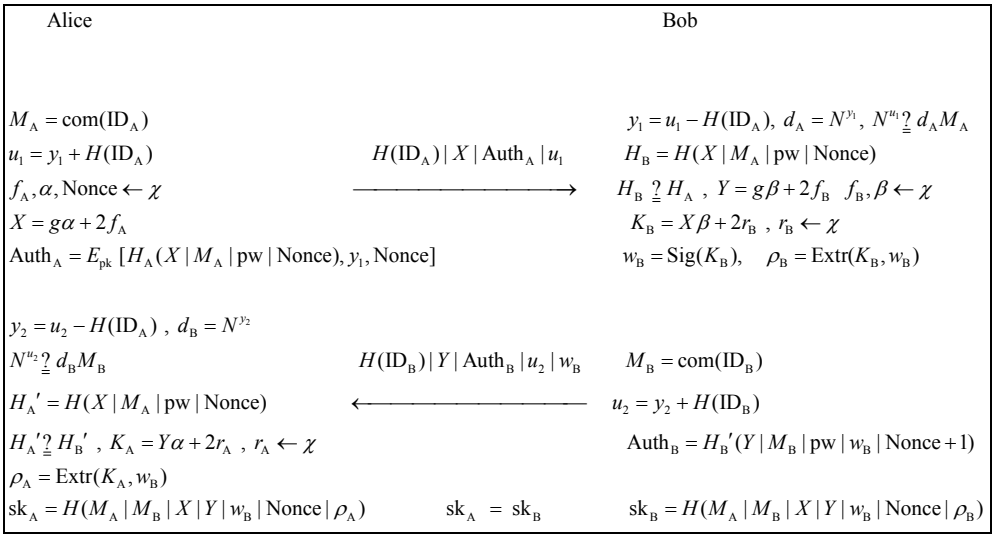


图 1　协议流程

得到认证参数 $Y = g\beta + 2f_B$，$K_B = X\beta + 2r_B$。利用 Sig 和 Extr 函数得到 $w_B = \mathrm{Sig}(K_B)$，$\rho_B = \mathrm{Extr}(K_B, w_B)$。

③Bob 将身份信息 ID_B 经 com() 函数处理得到承诺值 M_B，随机选择 $y_2 \in (1,2,\cdots,q)$，计算 $u_2 = y_2 + H(\mathrm{ID}_s)$ 和 Bob 的身份认证信息 $\mathrm{Auth}_B = H_B'(Y \mid M_B \mid \mathrm{pw} \mid w_B \mid \mathrm{Nonce}+1)$，随后将 $H(\mathrm{ID}_B) \mid Y \mid \mathrm{Auth}_A \mid u_2 \mid w_B$ 发送给 Alice。

最终 Bob 获得共享会话密钥 $\mathrm{sk}_B = H(M_A \mid M_B \mid X \mid Y \mid w_B \mid \mathrm{Nonce} \mid \rho_B)$。

3) Alice 接收到 $H(\mathrm{ID}_B) \mid Y \mid \mathrm{Auth}_A \mid u_2 \mid w_B$ 后进行以下操作。

① Alice 接收到 Bob 传来的数据 $u_2 \mid H(\mathrm{ID}_B)$，首先验证消息 $y_2 \mid u_2 \mid M_B$ 的完整性。Alice 计算 $y_2 = u_2 + H(\mathrm{ID}_B)$，$d_B = N^{y_2}$，$M_B = \mathrm{com}(\mathrm{ID}_B)$，并验证 $N^{u_2} = d_B M_B$ 是否成立。若等式成立，证明消息传递途中参数 $y_2 \mid u_2 \mid M_B$ 没有被更改，消息具有完整性。反之，消息验证失败，Alice 拒绝通信。

② Alice 利用参数 $Y \mid M_B \mid w_B$，将 $\mathrm{Nonce}+1$ 计算 $H_A' = H(Y \mid M_B \mid \mathrm{pw} \mid w_B \mid \mathrm{Nonce}+1)$。若等式 $H_A' = H_B'$ 成立，Bob 的身份认证成功。反之失败，Alice 拒绝通信。若身份认证成功，Alice 随机选取参数 $r_A \leftarrow \chi$，计算 $K_A = Y\alpha + 2r_A$，利用 Extr 函数得到参数 $\rho_A = \mathrm{Extr}(K_A, w_B)$，则 Bob 的共享会话密钥 $\mathrm{sk}_A = H(M_A \mid M_B \mid X \mid Y \mid w_B \mid \mathrm{Nonce} \mid \rho_A)$。共享会话密钥 $sk_A = sk_B$，完成密钥协商。

3.3　协议的正确性证明

假设 q 是大于 2 的素数，$Z_q = \left\{-\frac{q-1}{2}, \cdots, \frac{q}{2}\right\}$，$E = \left\{-\frac{q}{4}, \cdots, \frac{q}{4}\right\}$，信号函数 $\mathrm{Sig}(x)$ 可定义为

$$\mathrm{Sig}(x) = \begin{cases} 0, & x \in E \\ 1, & \text{其他} \end{cases} \tag{2}$$

证明　假设 q 是大于 8 的奇数，则 Extr 函数[26]定义为

$$\mathrm{Extr}(x, \delta) = \left(x + \delta \frac{q-1}{2} \bmod q\right) \bmod 2,\ \delta = \mathrm{Sig}(x)$$

给定 2 个数 $x, y \in Z_q$，$x - y = 2\varepsilon$，$|2\varepsilon| \leqslant \frac{q}{4} - 2$，则 Extr 函数可表示为

$$\mathrm{Extr}(x, \delta) = \left(x + \delta \frac{q-1}{2} \bmod q\right) \bmod 2 =$$
$$\left(y + \delta \frac{q-1}{2} \bmod q + 2\varepsilon\right) \bmod 2 =$$
$$\left(y + \delta \frac{q-1}{2} \bmod q\right) \bmod 2 + 2\varepsilon \bmod 2 =$$
$$\left(y + \delta \frac{q-1}{2} \bmod q\right) \bmod 2 = \mathrm{Extr}(y, \delta)$$

利用 Sig 函数和 Extr 函数可得，$k_A, k_B \in Z_q$，$k_A - k_B = 2\varepsilon$，且 $|2\varepsilon| \leqslant \frac{q}{4} - 2$。由此可得 $\rho_A = \mathrm{Extr}(k_A, w_B) = \mathrm{Extr}(k_B, w_B) = \rho_B$。从而 $\mathrm{sk}_A = \mathrm{sk}_B$。

证毕。

3.4 协议的安全性证明

定义 4 敌手 E 获胜的优势可定义为

$$\mathrm{Adv}\Pi(\mathrm{E})=\left|\Pr[b'=b]-\frac{1}{2}\right|$$

协议安全性条件介绍如下。

1) 敌手 E 可在匹配会话中获得相等的会话密钥。

2) 在随机多项式时间内，敌手 E 取得游戏胜利的概率忽略不计。

定理 1 在多项式时间内，若敌手 E 在游戏中以不可忽略的概率获胜，则存在模拟器 Q，能够以 $\mathrm{Adv}\Pi(\mathrm{Q})$ 优势在以上时间内解决最短向量困难问题。

证明 协议的安全性证明可归约到求解基于格上最短向量困难的问题上。假设敌手 E 攻击协议成功，则证明敌手可以解决格上的最短向量困难问题。由于协议中会话密钥与随机数的不可区分性，敌手 E 在协议运行多次的情形下，选择单次目标会话，从密钥空间中的随机数或真实的会话密钥之间随机获得一个，协议的安全性基于敌手 E 仅以可忽略的概率分辨真实的会话密钥和密钥空间中的随机值。

1) 密钥复制攻击

敌手 E 与通信双方创建一个与测试会话拥有一致会话密钥的会话，协议中会话密钥的产生所依赖的参数 $f_{\mathrm{A}},f_{\mathrm{B}},\alpha,\mathrm{Nonce},r_{\mathrm{B}},r_{\mathrm{A}}$ 随机选取，则证明在不同随机参数的输入情形下产生相同的会话密钥的概率可忽略。敌手 E 在 eCK 模型下不允许对同一通信参与者进行 Static_Key Reveal()和 Ephemeral_ Secret Reveal()的同步查询，因此真实会话与攻击会话中同时拥有相同的认证密钥和相同随机数的事件发生的概率可忽略，协议可抵抗密钥复制攻击。

2) 伪造攻击

敌手 E 计算得到 $\rho_{\mathrm{A}},\rho_{\mathrm{B}}$，借助随机预言机获得会话密钥 $\mathrm{sk}_{\mathrm{A}}=H(M_{\mathrm{A}}\|M_{\mathrm{B}}\|X\|Y\|w_{\mathrm{B}}\|\mathrm{Nonce}\|\rho_{\mathrm{A}})$。假设敌手 E 通过模拟器 Q 的随机选取获得的 n 次会话中包括 m 次匹配会话，则模拟器 Q 在通信双方 Alice 和 Bob 之间获得匹配会话的概率为 $p=\dfrac{C_m^2}{C_n^2}=\dfrac{m(m-1)}{n(n-1)}$。如果敌手 E 以概率 p 获得匹配会话，且敌手 E 成功地获得了会话密钥 sk_{A}，说明敌手 E 可计算 ρ_{A}, ρ_{B}，由于 ρ_{A} = SVP $(k_{\mathrm{A}},w_{\mathrm{A}})$，$\rho_{\mathrm{B}}$ = SVP $(k_{\mathrm{B}},w_{\mathrm{B}})$，说明模拟器 Q 能够攻克格上的最短向量问题。敌手 E 在 eCK 模型下不能对同一参与者完成 Static_Key Reveal()和 Ephemeral_ Secret Reveal()的同步查询，而且随机预言机随机选取相同输入的情况可忽略，敌手 E 和模拟器 Q 的关系为

$$\mathrm{Adv}\Pi(\mathrm{Q})\geqslant\frac{m(m-1)}{n(n-1)}\mathrm{Adv}\Pi(\mathrm{E})$$

假设敌手 E 能够在多项式时间内，利用 n 次会话中的 m 次匹配会话，并且在游戏中以优势 $\mathrm{Adv}\Pi(\mathrm{Q})$ 获胜，证明模拟器 Q 可在多项式时间内以优势 $\mathrm{Adv}\Pi(\mathrm{Q})$ 攻克 SVP，并满足 $\mathrm{Adv}\Pi(\mathrm{Q})\geqslant\dfrac{m(m-1)}{n(n-1)}\mathrm{Adv}\Pi(\mathrm{E})$，则协议可抵抗伪造攻击得证。

3) 抵抗重放攻击

重放攻击即攻击者通过二次发送复制信息欺骗通信参与者的行为。协议中，Alice 每次随机选取参数 f_{A}, α, Nonce, r_{A}，计算 X, K_{A}, ρ_{A}；Bob 每次随机选取参数 f_{B}, β, r_{B}，计算 Y, w_{B}, ρ_{B}。使当前单次会话生成的认证函数值 $\mathrm{Auth}_{\mathrm{A}}$, $\mathrm{Auth}_{\mathrm{B}}$ 不同，导致最终产生的会话密钥 sk_{A}, sk_{B} 不可匹配，表明协议可抵抗消息的重放攻击。

4) 抵抗中间人攻击

中间人攻击可通过获取通信双方的通信信息，进行篡改和窃听的攻击行为。Bob 接收到数据 $u_1\|H(\mathrm{ID}_{\mathrm{A}})$，首先验证消息 $y_1\|u_1\|M_{\mathrm{A}}$ 的完整性。计算 $y_1=u_1-H(\mathrm{ID}_{\mathrm{A}})$，$d_{\mathrm{A}}=N^{y_1}$，$M_{\mathrm{A}}=\mathrm{com}(\mathrm{ID}_{\mathrm{A}})$。验证 $N^{u_1}=d_{\mathrm{A}}M_{\mathrm{A}}$ 是否成立，若成立，则证明通信过程中消息 $y_1\|u_1\|M_{\mathrm{A}}$ 完整没有被更改。同理，Alice 接收到 Bob 传来的数据 $u_2\|H(\mathrm{ID}_{\mathrm{B}})$，首先验证消息 $y_2\|u_2\|M_{\mathrm{B}}$ 的完整性。Alice 计算 $y_2=u_2-H(\mathrm{ID}_{\mathrm{B}})$，$d_{\mathrm{B}}=N^{y_2}$，$M_{\mathrm{B}}=\mathrm{com}(\mathrm{ID}_{\mathrm{B}})$，并验证 $N^{u_2}=d_{\mathrm{B}}M_{\mathrm{B}}$ 是否成立，若成立，则证明通信过程中消息完整，$y_2\|u_2\|M_{\mathrm{B}}$ 没有被更改。在这 2 次验证消息完整性的过程中，由于仅传输双方双份身份信息的摘要值 $H(\mathrm{ID}_{\mathrm{A}})\|H(\mathrm{ID}_{\mathrm{B}})$ 和经过处理的参数 $u_1\|u_2$，并不能获得参数 $y_1\|y_2$ 和 $M_{\mathrm{A}}\|M_{\mathrm{B}}$，则中间人无法对 $N^{u_1}=d_{\mathrm{A}}M_{\mathrm{A}}$ 和 $N^{u_2}=d_{\mathrm{B}}M_{\mathrm{B}}$ 中的任意一项进行篡改并最终使等式成立，故此协议可抵抗中间人攻击。

证毕。

4 性能分析

为了证明本文方案的优势，将其与其他经典方案进行性能对比分析，如表 1 所示。文献[27]是 LWE

表 1　　**协议性能对比分析**

协议	用户匿名性	双向认证	消息完整性验证	抵抗不可测字典攻击	困难假设	运算方法	公钥长度/bit	消息传输轮数/轮
文献[27]方案	否	否	—	否	LWE	矩阵运算	$(2n+1)\lg q$	3
文献[16]方案	否	是	—	是	RLWE	环运算	$(2n+1)\lg q$	2
文献[28]方案	否	是	—	是	RLWE	环运算	$2n\lg q$	2、3
文献[29]方案	否	是	—	是	ASPH	环运算	$(2n+1)\lg q$	4
文献[30]方案	是	是	—	是	RLWE	环运算	$2n\lg q$	3
文献[24]方案	否	是	否	是	RLWE	环运算	$n\lg q$	2
本文方案	是	是	是	是	RLWE	环运算	$n\lg q$	2

问题上的 2PAKE 协议，不满足客户和服务端的双向认证，易受不可测字典攻击，消息传输 3 轮。文献[16]是 RLWE 困难问题上的 2PAKE 协议，消息传输 2 轮，用户无法匿名。以上 2 种方案公钥长度均为$(2n+1)\lg q$。文献[28]设计了隐式和显式认证 2 类 2PAKE 协议，公钥长度为 $2n\lg q$，消息传输轮数分别为 2 轮和 3 轮，用户无法匿名。文献[29]困难假设基于 ASPH 困难问题，用户无法匿名，公钥长度为$(2n+1)\lg q$，且需要 4 轮通信，消息传输轮数最多。文献[30]提出了一种基于格的三方认证密钥协商协议，困难假设基于 RLWE 问题，用户具有匿名性，可抵抗不可测字典攻击，消息传输轮数为 3 轮，公钥长度为 $2n\lg q$。文献[24]提出了一种基于格理论的客户端/服务器端模型下口令认证密钥协商协议，用户不具有匿名性，消息传输需要 2 轮，公钥长度为 $n\lg q$，可抵抗不可测字典攻击，消息不具备完整性验证。本文方案公钥长度为 $n\lg q$，在实现用户匿名性的前提下与以上方案相比公钥长度最短，消息传输轮数少，仅需要 2 轮通信，且能抵抗中间人攻击、不可测字典攻击、密钥复制攻击、重放攻击、伪造和量子攻击。通过与 Ding 等[28]的协议对比，本文方案公钥长度缩短 50%，且消息传输轮数仅需要 2 轮，具有更好的安全性和通信性能。

5　结束语

认证密钥交换协议可以在不安全的信道上协商出共同的会话密钥。为了解决执行认证密钥交换协议时通信双方身份匿名问题，本文提出了一种基于 C 类承诺机制的抗量子攻击的双向认证密钥协商协议。该协议通过 C 类承诺机制的设计，将通信双方不愿暴露的真实身份信息隐藏为承诺值的形式。协议基于 RLWE 困难问题，在保障身份匿名的前提下，通过 2 轮的消息交互不仅完成了双向身份认证，而且保证传输消息的完整性，并协商出共享会话密钥。通过分析，在协议执行效率上，完成匿名的双向认证与密钥协商只需经过 2 轮的消息传输，公钥长度较短。本文协议满足可证明安全，可抵抗量子攻击。下一步研究计划将把本文协议进行软件快速实现。

参考文献：

[1] DODIS Y, MIRONOV I, STEPHENS-DAVIDOWITZ N. Message transmission with reverse firewalls-secure communication on corrupted machines[C]//Annual Cryptology Conference. Springer, 2016: 341-372.

[2] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[3] LI L H, LIN L C, HWANG M S. A remote password authentication scheme for multiserver architecture using neural networks[J]. IEEE Transactions on Neural Networks, 2001, 12(6): 1498-1504.

[4] LIU C, LIN C, HARN L, et al. Security analysis of remote password authentication schemes for multiserver architecture using neural networks[J]. Journal of Computational & Theoretical Nanoscience, 2012, 7(1): 680-683.

[5] TSAUR W J, WU C C, LEE W B. A smart card-based remote scheme for password authentication in multi-server Internet services[J]. Computer Standards & Interfaces, 2004, 27(1): 39-51.

[6] JUANG W S. Efficient multi-server password authenticated key agreement using smart cards[J]. IEEE Transactions on Consumer Electronics, 2004, 50(1): 251-255.

[7] CHANG C C, LEE J S. An efficient and secure multi-server password authentication scheme using smart cards[C]//International Conference on Cyberworlds. 2004: 417-422.

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

[9] LIAO Y P, WANG S S. A secure dynamic ID based remote user authentication scheme for multi-server environment[J]. Computer Standards & Interfaces, 2009, 31(1): 24-29.

[10] WU T Y, TSENG Y M. An efficient user authentication and key exchange protocol for mobile client-server environment[J]. Computer Networks, 2010, 54(9): 1520-1530.

[11] YOON E J, YOO K Y. A new efficient ID-based user authentication and key exchange protocol for mobile client-server environment[C]//IEEE International Conference on Wireless Information Technology & Systems. IEEE, 2010: 1-4.

[12] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2010: 1-23.

[13] HE D B, CHEN J H, HU J. An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security[J]. Information Fusion, 2012, 13(3): 223-230.

[14] ISLAM S H, BISWAS G P. Comments on ID-based client authentication with key agreement protocol on ECC for mobile client-server environment[C]//International Conference on Advances in Computing and Communications. Springer, 2011: 628-635.

[15] HAO F, RYAN P. J-PAKE: authenticated key exchange without PKI[J]. Transactions on Computational Science, 2010, 6480: 192-206.

[16] 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 (EUROCRYPT 2015). Berlin Heidelberg: Springer, 2015: 719-751.

[17] 姚期智, 赵运磊. 一种高效且隐私保护的会话密钥协商方法: CN105162585A[P]. (2015–12–16)[2019−01−28].
YAO Q Z, ZHAO Y L. An efficient session key agreement method with privacy preservation: CN105162585A[P]. (2015–12–16)[2019−01−28].

[18] 赵运磊, 李俊全. 一种身份隐藏且非延展安全的认证密钥协商方法: CN105099671A[P]. (2015–11–25)[2019−01−28].
ZHAO Y L, LI J Q. An authentication key agreement method with hidden identify and non extended security: CN105099671A[P]. (2015–11–25)[2019−01−28].

[19] STEBILA D, MOSCA M. Post-quantum key exchange for the Internet and the open quantum safe project[C]//International Conference on Selected Areas in Cryptography. Berlin Heidelberg: Springer, 2016: 14-37.

[20] 李文敏, 温巧燕, 张华. 基于验证元的三方口令认证密钥交换协议[J]. 通信学报, 2008, 29(10):149-152.
LI W M, WEN Q Y, ZHANG H. Verifier-based password-authenticated key exchange protocol for three-party[J]. Journal on Communications, 2008, 29(10): 149-152.

[21] TSENG Y M, HUANG S S, YOU M L. Strongly secure ID-based authenticated key agreement protocol for mobile multiserver environments[J]. International Journal of Communication Systems, 2016, 30(11): 1-13.

[22] WU F, XU L L, LI X. A new chaotic map-based authentication and key agreement scheme with user anonymity for multi-server environment[C]//International Conference on Frontier Computing. Springer, 2018: 335-344.

[23] SHARMA G, SAHU R A, KUCHTA V, et al. Authenticated group key agreement protocol without pairing[C]//International Conference on Information and Communications Security. Springer, 2018: 606-618.

[24] JHENG Y S, TSO R, CHEN C M, et al. Password-based authenticated key exchange from lattices for client/server model[C]//International Conference on Ubiquitous Information Technologies and Applications. Springer, 2017: 315-319.

[25] 张宗洋. 承诺和零知识的非延展属性研究[D]. 上海: 上海交通大学, 2012.
ZHANG Z Y. Non-malleable commitments and non-malleable zero-knowledge[D]. Shanghai: Shanghai Jiao Tong University, 2012.

[26] MICCIANCIO D, REGEV O. Worst-case to average-case reductions based on Gaussian measures[C]// 45th Annual IEEE Symposium on Foundations of Computer Science. IEEE Computer Society, 2004: 372-381.

[27] KATZ J, VAIKUNTANATHAN V. Smooth projective hashing and password-based authenticated key exchange from lattices[C]//15th International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2009: 636-652.

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

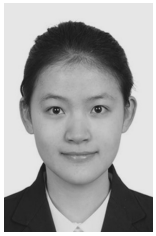
[29] 杨晓燕, 侯孟波, 魏晓超. 基于验证元的三方口令认证密钥交换协议[J]. 计算机研究与发展, 2016, 53(10):2230-2238.
YANG X Y, HOU M B, WEI X C. Verifier-based three-party password authenticated key exchange protocol[J]. Journal of Computer Research & Development, 2016, 53(10): 2230-2238.

[30] 王彩芬, 陈丽. 基于格的用户匿名三方口令认证密钥协商协议[J]. 通信学报, 2018, 39(2): 21-30.
WANG C F, CHEN L. Three-party password authenticated key agreement protocol with user anonymity based on lattice[J]. Journal on Communications, 2018, 39(2): 21-30.

[作者简介]

杨亚涛（1978– ），男，河南平顶山人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为密码学与信息安全。

韩新光（1994– ），男，陕西咸阳人，西安电子科技大学硕士生，主要研究方向为格理论与信息安全。



黄洁润（1995– ），女，江苏南通人，北京电子科技学院硕士生，主要研究方向为格密码与信息安全。

赵阳（1995– ），男，山东日照人，北京电子科技学院硕士生，主要研究方向为密码学与信息安全。