·安全技术· 文章编号：1000-3428(2018)04-0212-06 文献标志码：A 中图分类号：TP309

基于理想格的用户匿名口令认证密钥协商协议

王彩芬，陈 丽，张玉磊

（西北师范大学 计算机科学与工程学院，兰州 730070）

摘 要：基于标准格的密钥协商协议具有较长的密钥长度和较高的密文扩张率，且格的表示方式需要较大的空间，而理想格具有密钥长度短和运行效率高等优点。因此，结合环上误差学习问题，提出基于理想格的用户匿名口令认证密钥协商协议。使用低熵的口令，通过服务器实现相互认证和共享会话密钥，以避免在身份认证过程中用户长期密钥的存储安全受到威胁。分析结果表明，与传统的 2PAKE 和 3PAKE 协议相比，该协议具有较高的效率和较短的密钥长度，能够抵抗量子攻击，适用于大规模网络通信。

关键词：理想格；可证明安全；口令认证；密钥协商；环上误差学习问题

中文引用格式：王彩芬，陈 丽，张玉磊. 基于理想格的用户匿名口令认证密钥协商协议[J]. 计算机工程，2018，44(4)：212-217.

英文引用格式：WANG Caifen，CHEN Li，ZHANG Yulei. Password Authenticated Key Agreement Protocol with User Anonymity Based on Ideal Lattice[J]. Computer Engineering，2018，44(4)：212-217.

Password Authenticated Key Agreement Protocol with User Anonymity Based on Ideal Lattice

WANG Caifen，CHEN Li，ZHANG Yulei

（College of Computer Science and Engineering，Northwest Normal University，Lanzhou 730070，China）

【Abstract】The key agreement protocol based on standard lattice has longer key and higher ciphertext expansion rate，and the way of lattice representation needs larger space，while the ideal lattice has shorter key length and higher running efficiency. Therefore，combined with Ring Learning with Error(RLWE) problem，an anonymous password authentication key agreement protocol based on the ideal lattice is proposed. Users use low entropy passwords to authenticate and share session keys through servers，so as to avoid users' long-term key security being threatened in the process of identity authentication. The analysis results show that，compared with the traditional 2PAKE and 3PAKE protocols，the proposed protocol has higher efficiency and shorter key length，which can resist quantum attacks and is suitable for large-scale network communication.

【Key words】ideal lattice；provably secure；password authentication；key agreement；Ring Learning with Error(RLWE) problem

DOI：10.3969/j.issn.1000-3428.2018.04.034

0 概述

随着量子计算机的发展，传统的困难问题在量子计算下存在多项式求解算法，其安全性受到越来越多的挑战，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，基于标准格的密码方案具有较长的密钥和较高的密文扩张率，且格的表示方式需要较大的空间，而理想格的表示方式简单，对内具有乘法封闭性、对外具有乘法吸收性，其可以克服标准格的相关缺点。因此，理想格在密码方案中被广泛使用，如公钥加密[1-3]、数字签名[4-6]、密钥协商协议[7-9]等。

认证密钥交换(Authenticated Key Exchange，AKE)允许通信方在不安全的信道中相互认证并协商出共享密钥，两方口令认证密钥交换(Two-party Password Authenticated Key Exchange，2PAKE)[10]协议中每 2 个用户共享一个低熵口令，导致该协商协议不适用于用户间的通信。为解决 2PAKE 的局限性，密码学者提出三方口令认证密钥交换(Three-party Password Authenticated Key Exchange，3PAKE)

基金项目：国家自然科学基金(61662069，61562077，61662071)；西北师范大学青年教师科研能力提升计划项目(NWNU-LKQN-14-7)。
作者简介：王彩芬(1963—)，女，教授、博士，主研方向为网络与信息安全；陈 丽(通信作者)，硕士研究生；张玉磊，副教授、博士。
收稿日期：2017-05-22 **修回日期：**2017-06-23 **E-mail：**2015211281@nwnu.edu.cn

协议[11-12],并将其应用于大规模网络下的通信。文献[10]基于误差学习问题(Learing With Error, LWE),提出基于格的2PAKE协议,该方案存在密钥较长和效率较低等问题,无法应用在大规模的通信系统中。文献[7]针对一般格上密钥长度过大的问题提出基于理想格的环上误差学习(Ring Learning With Error,RLWE)问题,并证明其分布是伪随机的。文献[8]提出基于理想格的近似平滑投射 Hash 函数(ASPH)。文献[13]基于格的口令认证密钥交换协议,在相关加密算法的研究中提出基于理想格的2PAKE协议,该协议消息传输量较大,且不满足用户的匿名性。文献[10]提出基于理想格的认证密钥交换方案,其协议不使用任何加密原语,该方案的安全性基于 RLWE 困难问题,不适用于大规模网络中的通信。文献[11]基于 ASPH 提出基于格的3PAKE协议,该协议不满足用户的匿名性。文献[12]提出一种新型基于 RLWE 问题的认证密钥交换方案,该方案基于 RLWE 问题提出两方密钥协商协议。文献[14]提出基于验证元的3PAKE协议,该协议通信量较多,效率较低。

针对上述协议的局限性,本文提出基于理想格的用户匿名3PAKE协议,在文献[15]安全模型的基础上构建3PAKE协议的安全模型,并在标准模型下证明该协议的安全性。

1　相关定义

定义 1　理想格

令 $n=2^k(k\in\mathbb{Z})$,$f(x)=x^n+1\in Z[x]$,多项式环 $R=Z[x]/<f(x)>$ 中元素为 $<g(x)>=\{h(x)\in Z[x]\mid g(x)=h(x)\bmod f(x),\deg(g)<n\}$。$g(x)$的系数对应于 Z^n 中的一个向量,令 I 是环 $Z[x]/<f(x)>$的一个理想,则理想 I 按上述对应关系对应于 Z^n 中的一个子格,称对应于理想 $I\in Z[x]/<f(x)>$的 Z^n 中的一个子格为 f-理想格。

定义 2　离散高斯分布[16]

令 $\rho_r(X)=\exp(-\pi\|X\|^2/r^2)$,对于理想格 L,记 $\rho_r(L)=\sum_{X\in L}\rho_r(X)$。理想格 L 上的离散高斯分布 $D_{L,r}$定义为:对于任意 $X\in L$,若随机变量 ξ 满足 $P(\xi=X)=\frac{\rho_r(X)}{\rho_r(L)}$,则随机变量 ξ 服从离散高斯分布 $D_{L,r}$。

定义 3　RLWE 问题

设 $n=2^k\geqslant 1$,$k\in\mathbb{Z}$,环 $R=\mathrm{Z}[x]/(x^n+1)$。对任意正整数 q,类似的定义环 $R_q=\mathrm{Z}_q[x]/(x^n+1)$,对任意环 R 或 R_q 中的多项式 $y(x)$,用 Z^n 或 Z_q^n 中的系数向量来确定 y,多项式的范数定义为其系数向量的范数。

根据 RLWE 问题,有以下相关引理:

引理 1　对于 $\forall s,t\in\mathbb{R}$,有 $\|s\cdot t\|\leqslant\sqrt{n}\cdot\|s\|\cdot\|t\|$ 和 $\|s\cdot t\|_\infty\leqslant n\cdot\|s\|_\infty\cdot\|t\|_\infty$。

引理 2　对于任意实数 $\alpha=\omega(\sqrt{\lg n})$,有 $P_{x\leftarrow x_\alpha}[\|x\|>\alpha\sqrt{n}]\leqslant 2^{-n+1}$。

定义 4　*Cha* 和 Mod_2 函数[9]

奇数 $q>2$,定义 $Z_q=\left\{-\frac{q-1}{2},-\frac{q-3}{2},\cdots,\frac{q-1}{2}\right\}$,集合 $E=\{-\lfloor q/4\rfloor,-\lfloor(q-4)/4\rfloor,\cdots,\lfloor q/4\rceil\}$,*Cha* 是 E 的互补特征函数,如果输入 E 和 1,返回 $Cha(v)=0$,对于 $\forall v\in\mathbb{Z}_q$,$v+Cha(v)\cdot\frac{q-1}{2}\bmod q\in E$。辅助模块化函数 $Mod_2:\mathbb{Z}_q\times\{0,1\}\to\{0,1\}$,$Mod_2(v,b)=\left(v+b\cdot\frac{q-1}{2}\right)\bmod q\bmod 2$。

根据 *Cha* 和 Mod_2 函数定义,有以下引理:

引理 3　q 是一个基数,$v\in\mathbb{Z}_q$,$e\in\mathbb{Z}_q$,且 $|e|<q/8$,$\omega=v+2e$,此时,有 $Mod_2(v,Cha(v))=Mod_2(\omega,Cha(v))$。

定义 5　3PAKE 协议的安全模型

在文献[15]安全模型的基础上构建3PAKE协议的安全模型。协议中使用的符号及说明如表1所示。

表 1　基于理想格的 3PAKE 协议符号说明

符号	说明
B、C	用户名
TID_B、TID_C	用户 B、C 的临时身份
S	远程服务器
k	安全参数
pw_B、pw_C	用户 B、C 的口令
H_1、H_2、H_3	散列函数
β、ω	$\beta\in\{0,1\}$、$\omega\in\{0,1\}^n$
a、s	a、$s\in\mathbb{R}_q$
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
$\|$	连接运算符
A	概率多项式时间敌手
sk	由 B、C 生成的会话密钥

从以下方面描述安全模型的定义:

安全游戏:定义挑战者 XH 和概率多项式时间敌手 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 Y 分为2个非空集合:客户 X 和服务器 Σ,假设非空字典 D 的长度为 L。在开始游戏前,非空字典 D 随机均匀分配给每个客户 $C\in X$ 一个口令 pw_C,并给敌手 A 分配口令。$\forall S\in\Sigma$,有 $pw_S=(f(pw_C))_C$,f 是被 P 指定的有效、可计算的单向函数。XH 生成 P 的公共

参数,并发送给 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 $U \in Y$ 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并发起和运行协议。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 是实例相信其正在通信的用户身份,SK 是实例 $\prod_u^i$ 最终的计算目标,SID 是唯一标识协议运行并确保使用 SK 会话的字符串。

敌手 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(Y,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 A。假设 A 能看到 $\prod_u^i$ 接受或终止的询问结果。

Execute(X,i,S,j)询问:P 执行完成 $\prod_c^i$ 和 $\prod_s^i$ 后,把执行记录传递给敌手 A。

Reveal(Y,i)询问:返回 $\prod_u^i$ 所拥有的 sk_u^i 给 A。

Test(Y,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 发送给 A;若 $b=0$,将等长的随机值发送给 A。在游戏中,此询问只进行一次。

Corrupt(Y)询问:如果 $U \in Y$,返回 $(f(pw_C))_C$;否则,返回 pw_U 给 A。

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

匹配会话:如果满足以下条件,1)$\prod_v^i$ 和 $\prod_u^i$ 其中一个实例来自客户集 X,另一个实例来自服务器 Σ;2)实例 $\prod_v^i$ 和 $\prod_u^i$ 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 等于 SID,则称 $\prod_v^i$ 和 $\prod_u^i$ 互为匹配会话。

安全性定义:在游戏中,A 可以执行多项式次 Execute、Send 和 Test 询问,游戏结束时 A 输出 b',若 $b'=b$,则 A 成功攻破协议。设 n 是安全参数,D_n 是口令空间,A 攻击协议的优势定义为:$Adv_{D_n,G_x}(A) = 2P[Succ_P^{ake}(A)] - 1$。

2 基于理想格的密钥协商协议

针对文献[9-13]中存在的一些安全性问题,本文提出了基于理想格的用户匿名 3PAKE 协议。

2.1 协议内容

2.1.1 初始化阶段

如图 1 所示,当用户 B 和 C 进行安全通信时,用户分别输入临时身份 TID_B、TID_C,两者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。其中,协议基于 RLWE 困难问题,$R_q = Z_q/(x^n+1)$,$\sigma = Mod_2(k_S,\omega) = Mod_2(k_B,\omega) = Mod_2(k_C,\omega)$。

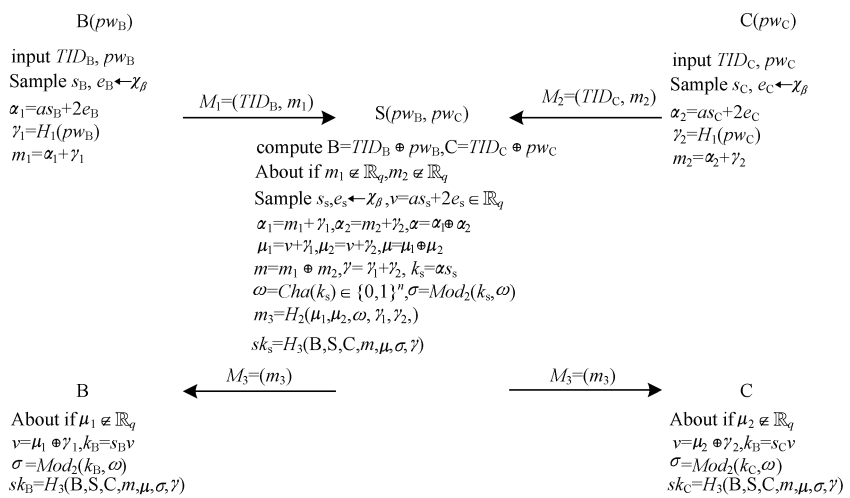

图 1 基于理想格的 3PAKE 协议示意图

当用户加入系统时,需要向服务器 S 注册。以用户 B 为例,该注册过程具体如下:

1)B→S:(B,Hpw_B)

用户 B 随机选取身份 B 和口令 pw_B,并任意选取随机数 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→B:(TID_B,$H(\cdot)$)

当 S 收到用户 B 的注册请求消息(B,Hpw_B)后,计算 $TID_B = B \oplus Hpw_B$,并将 TID_B、$H(\cdot)$发送给用户 B。

2.1.2　相互认证与密钥协商阶段

用户的相互认证与密钥协商具体过程如下:

1)B→S:$M_1 = \langle TID_B, m_1 \rangle$

用户 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 将 M_1 发送给 S。

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

用户 C 输入 TID_C,pw_C,随机选取 $s_C, e_C \leftarrow \chi_\beta$ 计算 $\alpha_2 = as_C + 2e_C$,$\gamma_2 = H_1(pw_C)$,$m_2 = \alpha_2 + \gamma_3$,C 将 M_2 发送给 S。

3)S→B,C:$M_3 = \langle m_3 \rangle$

收到 M_1、M_2 后,S 验证用户 B 和 C 的身份,并计算 $B = TID_B \oplus pw_B$,$C = TID_C \oplus pw_C$,验证用户 B 和 C 的身份成功后,如果 $m_1 \notin \mathbb{R}_q$,$m_2 \notin \mathbb{R}_q$,S 随机选取 $s_S, e_S \leftarrow \chi_\beta$ 计算 $v = as_S + 2e_S \in \mathbb{R}_q$,$\alpha_1 = m_1 + \gamma_1$,$\alpha_2 = m_2 + \gamma_2$,$\alpha = \alpha_1 \oplus \alpha_2$,$\mu_1 = v + \gamma_1$,$\mu_2 = v + \gamma_2$,$3\mu = \mu_1 \oplus \mu_2$,$m = m_1 \oplus m_2$,$\gamma = \gamma_1 \oplus \gamma_2$,$k_S = \alpha s_S$,$\omega = Cha(k_S) \in \{0,1\}^n$,$\sigma = Mod_2(k_S, \omega)$,$m_3 = H_2(\mu_1, \mu_2, \omega, \gamma_1, \gamma_2)$,$sk_S = H_3(B,C,S,m,\mu,\sigma,\gamma_1')$。将 M_3 发送给 B 和 C。

4)$sk_B = H_3(B,S,C,m,\mu,\sigma,\gamma)$

B 收到 M_3 后,验证 $\mu_1 \notin \mathbb{R}_q$,并计算 $v = \mu_1 \oplus \gamma_2$,$k_B = s_B v$,$\sigma = Mod_2(k_B, \omega)$ $sk_B = H_3(B,S,C,m,\mu,\sigma,\gamma)$,如果 $sk_B = sk_S$,此时 B 和 C 拥有共同的会话密钥。

5)$sk_C = H_3(B,S,C,m,\mu,\sigma,\gamma)$

C 收到 M_3 后,验证 $\mu_2 \notin \mathbb{R}_q$,并计算 $v = \mu_2 - \gamma_2$,$k_C = s_C v$,$\sigma = Mod_2(k_C, \omega)$ 和 $sk_C = H_3(B,S,C,m,\mu,\sigma,\gamma)$,如果 $sk_C = sk_S$,此时 B 和 C 拥有共同的会话密钥。

2.2　方案的正确性

q 是一个大素数,若 $q > 16\beta^2 n^{3/2}$,诚实用户运行方案,用户获得的会话密钥不匹配的概率可忽略。由引理 3 得,如果 k_C 和 k_S 非常接近,即 $|k_C - k_S| < q/4$,则每一方有相同的 σ 值。

由 $k_C = s_C v = s_C(as_S + 2e_S) = as_C s_S + 2e_S s_C$,$k_S = as_S = (as_C + 2e_C)s_S = (as_B + 2e_B)s_S = as_C s_S + 2e_C s_S = as_B s_S + 2e_B s_C$,$k_B = s_B v = s_B(as_S + 2e_S) = as_B s_S + 2e_S s_B$,得到 $|k_C - k_S| = 2[e_S s_C - e_C s_S]$,$|k_B - k_S| = 2[e_S s_B - e_B s_S]$。由引理 2 得,每一个 e_S、s_C、e_C、s_S、e_B、s_B 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出 $\| k_C - k_S \| \leqslant 4\beta^2 n^{3/2} < q/4$,$\| k_B - k_S \| \leqslant 4\beta^2 n^{3/2} < q/4$。因此,$Mod_2(k_C, Cha(k_S)) = Mod_2(k_S, Cha(k_S)) = Mod_2(k_B, Cha(k_S))$。综上所述,诚实用户执行方案时,双方拥有相同的会话密钥。

3　安全性证明

认证协议能否得到广泛应用,不仅要其设计合理,还要具备正确性和安全性,本文给出基于理想格的用户匿名 3PAKE 协议的安全性证明。

定理 1　设 n 是安全参数,D_n 是口令空间,若 RLWE 问题是困难的,则方案在标准模型下是安全的。因此,存在可忽略函数 $negl(n)$,对运行时间为 t 的敌手 A,执行 Execute、Send、Test 询问的次数最多为 q_e、q_s、q_t,有 $Adv_{D_n,G_x}(A) \leqslant q_s / |D_n| + negl(n)$ 成立。

证明:设诚实的用户集是 E 和 F,H 是攻击者,证明利用游戏 G_x 来估计 H 的优势,记 $Adv(H, G_x)$ 表示 H 赢得游戏 G_x 的优势,其中 $x = 0 \sim 11$,$x \in \mathbb{Z}$。分析相邻游戏中 H 的优势差异,界定 H 在游戏中的最终优势,可知 H 在游戏 G_0 中的优势。在游戏 G_x 中,由于协议关于客户对称,因此对实例 F 进行类似于实例 E 的处理。

游戏 G_0 是 H 和真实协议的交互,H 向模拟器 S 询问,并收到回答。

游戏 G_1 和 G_0 基本相同,下述情况除外:模拟者选择不属于字典集 D_n 的口令 pw_E',对于 E,模拟者计算 $\gamma_1 = H_1(pw_E')$,其他计算保持不变。

S 为 H 模拟游戏的随机口令,进行 Execute 询问,S 用明文挑战对(pw_E,pw_E'),将得到的密文替换 Execute 询问中的 γ_1。S 检查 H 输出的比特 b'。若 $b' = b$,则 S 输出 1;否则,S 输出 0。因此,可知 S 的区分优势为式(1)成立。

$$|Adv(H,G_1) - Adv(H,G_0)| \leqslant negl(n) \qquad (1)$$

游戏 G_2 和 G_1 基本相同,下述情况除外:S 选取 $s_E', e_E' \in \chi_\beta$,计算 $\alpha_1' = as_E' + 2e_E'$,$m_1' = \alpha_1' + \gamma_1'$,并发送($TID_E'$,$m_1'$)给 H。

由于在计算时 α_1'的分布和一致分布不可区分,因此 H 猜测出 $m_1 = \alpha_1 + \gamma_1$ 的概率可忽略。由于 $TID_E = E \oplus pw_E$,若 H 假冒 TID_E' 发送给 S,S 计算

$TID'_{\mathrm{E}}\oplus pw_{\mathrm{E}}$ 以验证 E 的身份,若验证通过,协议继续执行;否则,协议停止。若 RLWE 是困难问题,则式(2)成立。

$$|Adv(\mathrm{H},G_2)-Adv(\mathrm{H},G_1)|\leqslant negl(n) \tag{2}$$

游戏 G_3 和 G_2 基本相同,G_3 在游戏 G_2 的基础上,不再利用哈希函数计算 γ 的值,改为利用直接选取的随机数。因为 γ_1 已经被替换成 pw'_{E}的密文,所以(γ_1,pw'_{E})对哈希函数而言是一个非法输入,其输出统计接近于均匀分布,因此,每个替换造成的统计差距可忽略,即 H 最多执行 Execute 询问 q_e 次,游戏 G_3 和 G_2 的优势差可忽略,则式(3)成立。

$$|Adv(\mathrm{H},G_3)-Adv(\mathrm{H},G_2)|\leqslant negl(n) \tag{3}$$

游戏 G_4 和 G_3 基本相同,下述情况除外:S 选取 $s'_{\mathrm{S}},e'_{\mathrm{S}}\in\chi_\beta$,计算 $E=TID'_{\mathrm{E}}\oplus pw'_{\mathrm{E}}$,$\mathrm{F}=TID'_{\mathrm{F}}\oplus pw'_{\mathrm{F}}$验证 E 和 F 的身份后,计算 $v'=as'_{\mathrm{S}}+2e'_{\mathrm{S}}$,$k'_{\mathrm{S}}=\alpha s'_{\mathrm{S}}$,$\omega'=cha(k'_{\mathrm{S}})$,$\sigma'=Mod_2(k'_{\mathrm{S}},\omega')$,根据协议规范计算 m'_3、sk'_{S}并发送(m'_3,sk'_{S})给 H。设(μ'_1,v'_1)和(μ'_2,v'_2)是 2 个RLWE 的挑战组,构造求解 RLWE 问题的区分器 D,D 设置 $k'_{\mathrm{S}}=\mu'_1$,$a=\mu'_2$,$\omega'=v_1$,计算 $\omega'=cha(k'_{\mathrm{S}})$,设置 $\sigma'=v_2$,依据协议规范计算 m'_3,sk'_{E}。若 RLWE 是困难问题,则式(4)成立。

$$|Adv(\mathrm{H},G_4)-Adv(\mathrm{H},G_3)|\leqslant negl(n) \tag{4}$$

游戏 G_5 和 G_4 基本相同,下述情况除外:S 选取 s'_{E}计算 $k_{\mathrm{E}}=s'_{\mathrm{E}}v$,$\sigma'=Mod_2(k'_{\mathrm{E}},\omega')$,设置 sk_{E} 为共享密钥,ω 给定的条件下,$Mod_2(k'_{\mathrm{E}},\omega)$的输出分布统计接近均匀分布。在游戏 G_4 中会话状态完全随机化,则敌手通过 Test 询问不能获取任何优势。若 RLWE 是困难问题,则式(5)成立。

$$|Adv(\mathrm{H},G_5)-Adv(\mathrm{H},G_4)|\leqslant negl(n) \tag{5}$$

记 Send(E,i,F,i_2,S,j)询问为客户实例和服务器实例开始执行协议的即时消息,记 Send(S,j,$TID_{\mathrm{E}}\parallel m_1$)为向服务器实例$\prod_{\mathrm{S}}^{j}$发送第一轮消息,记 Send(E,$i$,$m_3\parallel sk_{\mathrm{S}}$)为向服务器实例$\prod_{\mathrm{E}}^{i}$发送第一轮消息。设一个客户实例$\prod_{\mathrm{E}}^{i}$收到形如$\langle m_3\parallel sk_{\mathrm{S}}\rangle$的消息是匹配生成的。

游戏 G_6 和 G_5 基本相同,下述情况除外:如果客户 E 收到 Send(E,i,$m_3\parallel sk_{\mathrm{S}}$)询问,检查$\langle m_3\parallel sk_{\mathrm{S}}\rangle$是否由匹配生成,如果不是,对 m_3 进行解密,求解 γ_1,如果 $pw_{\mathrm{E1}}=pw_{\mathrm{E}}$,则 H 攻击成功,但游戏 G_6 不减少 H 成功的概率。

$m_3=H_2(\mu_1,\mu_2,\omega,\gamma_1,\gamma_2)$,因为哈希函数的单向性,所以攻击者很难求解出真实的 $\gamma_1=H_1(pw_{\mathrm{E}})$,即使求出正确的 γ_1,也很难得到真实的口令 pw_{E}。因此,式(6)成立。

$$|Adv(\mathrm{H},G_6)|\leqslant|Adv(\mathrm{H},G_5)| \tag{6}$$

游戏 G_7 和 G_6 基本相同,下述情况除外:如果客户 E 收到 Send(E,i,$m_3\parallel sk_{\mathrm{S}}$)询问,且$\langle m_3\parallel sk_{\mathrm{S}}\rangle$由匹配生成,此时,客户和 S 使用共同的 γ_1,因为 γ_1 对 H 不可见,所以 H 成功攻击协议的概率不变。因此,式(7)成立。

$$|Adv(\mathrm{H},G_7)|=|Adv(\mathrm{H},G_6)| \tag{7}$$

游戏 G_8 和 G_7 基本相同,下述情况除外:修改 Send(E,i,F,i_2,S,j)询问,若客户被 Send(E,i,F,i_2,S,j)询问激活,则使用不属于字典集 D_n 的口令pw'_{E},求 $\gamma_1=H_1(pw'_{\mathrm{E}})$。因此,式(8)成立。

$$|Adv(\mathrm{H},G_8)-Adv(\mathrm{H},G_7)|\leqslant negl(n) \tag{8}$$

游戏 G_9 和 G_8 基本相同,下述情况除外:对 Send(S,j,$TID_{\mathrm{E}}\parallel m_1$)询问,如果$\langle TID_{\mathrm{E}}\parallel m_1\rangle$不是由$\prod_{\mathrm{E}}^{i}$生成,则解密 $\gamma_1=H_1(pw_{\mathrm{E}})$,若得到 $pw_{\mathrm{E1}}=pw_{\mathrm{E}}$,则攻击者成功并停止模拟。该修改不减少敌手 H 攻击协议成功的概率,则式(9)成立。

$$|Adv(\mathrm{H},G_9)|\leqslant|Adv(\mathrm{H},G_8)| \tag{9}$$

游戏 G_{10} 和 G_9 基本相同,下述情况除外:对 Send(E,j,$TID_{\mathrm{B}}\parallel m_1$)询问进行修改,如果$\langle TID_{\mathrm{E}}\parallel m_1\rangle$是由$\prod_{\mathrm{E}}^{i}$生成,或不是由客户 E 实例生成,但解密后可得到 $pw_{\mathrm{E1}}\neq pw_{\mathrm{E}}$,则将服务器端的 γ_1 替换成随机值。因为 γ_1 在游戏 G_8 中被替换成虚拟口令pw'_{E}的密文,$\gamma_1=H_1(pw'_{\mathrm{E}})$,所以($\gamma'_1$,$pw'_{\mathrm{E}}$)是一个非法输入,其输出分布接近于均匀分布,因此,其优势差是可忽略的,则式(10)成立。

$$|Adv(\mathrm{H},G_{10})-Adv(\mathrm{H},G_9)|\leqslant negl(n) \tag{10}$$

游戏 G_{11} 和 G_{10} 基本相同,下述情况除外:对 Send(S,j,$TID_{\mathrm{E}}\parallel m_1$)询问进行修改,将服务器端 m_3 替换成口令 pw'_{E}的密文,由式(1)可得式(11)成立。

$$|Adv(\mathrm{H},G_{11})-Adv(\mathrm{H},G_{10})|\leqslant negl(n) \tag{11}$$

若攻击者猜测口令失败,则只可通过猜测随机比特 b 攻击协议,如果用随机值代替会话密钥,则 H 成功的概率为 1/2。如游戏 G_6 和 G_9,H 每次通过猜测随机比特 b 获得正确口令的概率最多是 $1/|D_n|$,因此,H 最后成功攻破协议的优势最多为 $q_s/|D_n|$。综上式(1)~式(11),有 $Adv_{D_n,G_x}(\mathrm{H})\leqslant q_s/|D_n|+negl(n)$成立,敌手攻破协议的优势是可忽略的量,即定理 1 结论成立。

4 协议性能分析比较

从安全性和效率 2 个方面,对本文方案与文献[9-11,13-14]方案进行比较,结果如表 2 所示。从表 2 可以看出,在安全性方面,与传统的 3PAKE 协议

相比,本文方案能够抵抗量子攻击,满足用户匿名性,用户和服务器的相互认证可抗不可测在线字典攻击,同时本文方案还具有较高的效率。文献[9]基于RLWE 困难问题的 2PAKE 协议需要 2 轮通信,因此,其 3PAKE 协议至少需要 4 轮通信,且不满足用户匿名性;文献[10]基于 LWE 困难问题的 2PAKE 协议需要 3 轮通信,因此,其 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,不能抵抗字典攻击,且不能满足用户匿名性;文献[11]基于 ASPH 的 3PAKE 协议需要 3 轮通信,通信量较多且不满足用户的匿名性;文献[13]基于 ASPH 的 2PAKE 协议需要 3 轮通信,因此,其 3PAKE 协议至少需要 6 轮通信,通信量大且不满足用户匿名性,不能在大规模通信系统中使用;文献[14]基于 ASPH 的 3PAKE 协议,需要 4 轮即 8 条消息传输量,效率较低且不满足用户匿名性。由于基于理想格的密钥协商协议较少,因此与其他方案相比,本文协议减少了公钥长度,降低了计算复杂度和消息传输量,提高了运行速度。

表 2　不同协议性能比较

比较项目	文献[9]协议	文献[10]协议	文献[11]协议	文献[13]协议	文献[14]协议	本文协议
类型	2-party	2-party	3-party	2-party	3-party	3-party
用户匿名性	否	否	否	否	否	是
相互认证	是	否	是	是	是	是
抵抗量子攻击	能	能	能	能	能	能
不可测字典攻击	是	否	是	是	是	是
困难假设	RLWE	LWE	ASPH	ASPH	ASPH	RLWE
采样数	$m=\Omega(n\lg q)$	$m=\Omega(n\lg q)$	$m=\Omega(n\lg q)$	$m=\Omega(\lg q)$	$m=\Omega(n\lg q)$	$m=\Omega(\lg q)$
公钥长度/bit	$m(2n+1)\lg q$	$m(2n+1)\lg q$	$3mn\lg q$	$3mn\lg q$	$m(2n+1)\lg q$	$2mn\lg q$
密文扩展率	$2mn/(n-1)$	m/n	$3mn/(n-1)$	$2mn/(n-1)$	$3mn/(n-1)$	m/n
运算方法	环运算	矩阵运算	环运算	环运算	环运算	环运算
计算复杂度	$O(2^{2n-2})$	$O(mn)$	$O(m\lg n)$	$O(m\lg n)$	$O(2^{2n+2})$	$O(m\lg n)$
消息传输量	2 轮	3 轮	3 轮	3 轮	4 轮	2 轮

5　结束语

基于标准格的密码方案存在运行效率较低等缺点,而理想格的表示方式简单,具有较少的密钥量、较短的密钥长度、较低的运行开销以及较高的运行效率等特点。因此,本文提出基于理想格的用户匿名 3PAKE 协议,实现用户和服务器的双向认证,并在标准模型下证明该协议的安全性。下一步将研究高效的基于理想格的多方密钥协议。

参考文献

[1] 杨晓元,吴立强,张敏情,等. 基于理想格的适应性选择密文安全公钥加密方案[EB/OL]. [2017-04-20]. http://www.docin.com/p-1273161598.html.

[2] 古春生. 近似理想格上的全同态加密方案[J]. 软件学报,2015,26(10):2696-2719.

[3] 魏理豪,艾解清,刘生寒. 理想格上高效的身份基加密方案[J]. 计算机工程,2016,42(7):134-138.

[4] 冯超逸,赵一鸣. 基于理想格的可证明安全数字签名方案[J]. 计算机工程,2017,43(5):103-107.

[5] 杨丹婷,许春根,徐　磊,等. 理想格上基于身份的签名方案[J]. 密码学报,2015,2(4):306-316.

[6] 孙意如,梁向前,商玉芳. 理想格上基于身份的环签名方案[J]. 计算机应用,2016,36(7):1861-1865.

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

[8] 叶　茂,胡学先,刘文芬. 基于理想格的近似平滑投射 Hash 函数[J]. 信息工程大学学报,2013,14(1):13-21.

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

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

[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.

[12] 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.

[13] 叶　茂. 基于格的口令认证密钥交换协议和相关加密算法研究[D]. 郑州:解放军信息工程大学,2013.

[14] 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.

[15] MACKENZIE P. The PAK suite: protocols for password-authenticated key exchange[EB/OL]. [2017-05-05]. https://www.researchgate.net/publication/2544702_The_PAK_suite_Protocols_for_Password-Authenticated_Key_Exchange.

[16] 詹海峰. 基于格的高斯抽样和密钥交换[D]. 西安:西安电子科技大学,2014.

编辑　吴云芳