格上基于口令的三方认证密钥交换协议

于金霞，廉欢欢，汤永利，史梦瑶，赵宗渠
（河南理工大学计算机科学与技术学院，河南 焦作 454000）

摘 要：三方口令认证密钥交换协议允许用户通过一个服务器在不安全的信道中建立一个受保护的会话密钥，而现有的格上 PAKE 协议绝大多数都是针对两方设计的，无法适用于大规模的通信系统。基于此，提出一种新的格上三方 PAKE 协议，该协议主要以可拆分公钥加密体制及其相应的近似平滑投射散列函数为基础进行构造，并通过在协议中引入消息认证机制的方式来防止消息重放攻击。与同类协议相比，所提协议减少了通信轮数，提高了效率和协议应用的安全性。

关键词：三方密钥交换；口令认证；LWE 问题；可证安全性
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018237

Password-based three-party authenticated key exchange protocol from lattices

YU Jinxia, LIAN Huanhuan, TANG Yongli, SHI Mengyao, ZHAO Zongqu
College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China

Abstract: Password-based three-party authenticated key exchange protocol allow clients to establish a protected session key through a server over insecure channels. Most of the existing PAKE protocols on lattices were designed for the two parties, which could not be applied to large-scale communication systems, so a novel three-party PAKE protocol from lattices was proposed. The PAKE protocol was constructed by using a splittable public-key encryption scheme and an associated approximate smooth projective Hash function, and message authentication mechanism was introduced in the protocol to resist replay attacks. Compared with the similar protocols, the new protocol reduces the number of communication round and improves the efficiency and the security of protocol applications.

Key words: three-party key exchange, password authentication, LWE problem, provable security

1 引言

在基于口令的认证密钥交换（PAKE, password-based authenticated key exchange）协议中，用户之间通过共享一个普通的低熵口令来认证通信方身份并进行密钥交换，最后建立共享的会话密钥。口令具有简单易记、操作方便的特点，基于口令的方案可以消除对公钥基础设施和安全硬件的依赖，且提高了系统的使用便利性。因此，基于口令的认证密钥交换协议是目前应用最为广泛的一种密钥交换协议[1-7]。

两方 PAKE（2PAKE, two-party PAKE）协议需

收稿日期：2018–02–05；**修回日期**：2018–06–09
通信作者：赵宗渠，zhaozong_qu@hpu.edu.cn
基金项目：国家密码管理局“十三五”国家密码发展基金资助项目（No.MMJJ20170122）；河南省科技厅基金资助项目（No.142300410147）；河南省教育厅基金资助项目（No.16A520013）；河南理工大学博士基金资助项目（No.B2014-044, No.B2016-39）；河南理工大学自然科学基金资助项目（No.T2018-1）
Foundation Items: The “13th Five-Year” National Crypto Development Foundation (No.MMJJ20170122), The Project of Science and Technology Department of Henan Province (No.142300410147), The Project of Education Department of Henan Province (No.16A520013), The Doctoral Fund of Henan Polytechnic University (No.B2014-044, No.B2016-39), The Natural Science Foundation of Henan Polytechnic University (No.T2018-1)

要每两个参与者共享一个口令建立会话密钥，但是这种方案在大量的用户通信中对口令存储比较复杂，需要消耗较高的管理成本。而三方 PAKE（3PAKE, three-party PAKE）协议使每个用户只需和服务器共享一个口令来进行认证，解决了 2PAKE 的局限性。

第一个真正意义上的 PAKE 协议最早由 Bellovin 等[1]提出，其安全性的分析采用启发式方法。2001 年，Katz，Ostrovsky 和 Yung[2]利用 CCA2（adaptive chosen-ciphertext attack）安全的加密体制及相应的平滑投射散列（SPH, smooth projection hash）函数进行密钥交换，提出第一个标准模型下的高效 PAKE 协议，简称 KOY 协议。2012 年，Zhao 等[3]基于 CDH 假设给出了一种可证明安全的 3PAKE 协议，协议利用陷门测试技术在 3eCK 模型下给出安全性证明。2015 年，Farash 等[4]提出了改进的 PAKE 协议，克服协议不能抵抗离线字典攻击的不足，且提供了会话密钥的前向保密性。随后，密码学者基于不同密码学组件设计了不同效率和安全性的 PAKE 协议[5-6]。

上述协议的安全性证明绝大多数都是依赖于大整数分解和离散对数问题的困难性，这些困难问题已经可以用量子算法在多项式时间内解决。而基于格困难问题的公钥密码体制在量子计算下还不存在多项式时间高效求解算法，并且格上的运算是矩阵–向量上的乘法，具备并行计算、效率高的特点。因此，设计一个基于格困难问题的口令认证密钥交换协议变得尤为重要。

在基于格理论的密码体制中，对 PAKE 的研究比较缺乏，直到 2009 年 Katz 等[7]才构造出了首个基于格的 CCA 安全的加密体制及其相应的近似平滑投射散列（ASPH, approximate smooth projection hash）函数，将这些组件与 KOY 协议[2]以及 Gennaro-Lindell 协议[8]相结合，提出第一个基于格的 2PAKE 协议。2011 年，Ding 等[9]将 Katz 等[8]提出的加密体制和近似平滑投射函数应用于 Groce-Katz 框架[10]，提出了一种基于格困难问题假设且效率较高的协议，并且在标准模型下给出此协议安全性证明。2013 年，叶茂等[11]利用 Katz 等[8]提出的公钥加密体制以及 ASPH 函数组件，基于 LWE 问题设计了第一个基于格的 3PAKE 协议，提高了安全性并满足大规模通信系统的应用需求，但仍存在通信效率较低的缺陷。2014 年，Peiker[12]提出一种基于环上带误差学习（RLWE, ring learning with error）的简单低带宽调和函数，利用这种技术构造密钥封装机制，实现了密钥交换。2015 年，Zhang 等[13]基于 RLWE 困难问题提出 2PAKE 协议，并给出安全性证明，但不适用于大规模的通信系统。2016 年，赵秀凤等[14]利用格困难问题提出一种密钥交换协议，但该协议需要密钥生成中心生成长期私钥和临时私钥，成本花销大。2017 年，Xu 等[15]利用 DH 思想，基于环上 LWE（learning with error）问题提出了可证明安全的 3PAKE 协议，但该协议存在效率低等局限。

2017 年，Zhang 等[16]将拆分的公钥加密体制应用于 Katz 等[7]的 3 次通信的框架中，提出了基于格困难问题且仅需两轮通信、效率较高的 PAKE 协议，但该方案是两方的口令密钥交换协议。由于三方 PAKE 协议建立最终的会话密钥需要融合所有用户的信息，那么需要添加函数对用户端信息进行计算，因此文献[16]提出的 2PAKE 协议无法直接应用于三方协议中。另外，三方协议在引入可信服务器后，用户端与服务器进行通信时会存在消息重放的可能性。

为解决上述协议存在的问题，本文提出一种新的基于 LWE 问题的三方 PAKE 协议。主要贡献有以下两个方面：1) 在文献[16]的基础上，添加伪随机函数来融合所有用户端的信息，并且在协议中引入消息认证机制，通过添加会话序列号的方式达到抵抗消息重放的目的，使本文所提三方协议更具有可行性；2) 利用拆分的公钥加密体制及相应的 ASPH 函数这两个组件构造协议，从而提高了通信效率。本文所提协议解决了 2PAKE 的局限，避免了消息重放攻击的弱点，具备抗量子攻击的特点，有较少的通信轮数和更高的通信效率。

2 背景知识

2.1 格的相关知识

定义 1 给定 m 个线性无关的向量 $\boldsymbol{B}=(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_m)\in\mathbb{R}^{m\times m}$，格 $\boldsymbol{\Lambda}\subset\mathbb{R}^m$ 定义为所有这些向量的整系数线性组合，即 $\boldsymbol{\Lambda}=\mathcal{L}(\boldsymbol{B})=\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i : x_i\in\mathbb{Z}\}$。

定义 2 q 元格。对于整数 q，满足 $q\mathbb{Z}^m\subseteq\mathbb{Z}^m$。对 $q,m,n\in\mathbb{Z}$，给定矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，定义：$\boldsymbol{\Lambda}_q(\boldsymbol{A})=\{\boldsymbol{y}\in\mathbb{Z}^m : \boldsymbol{y}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}(\mathrm{mod}\,q)\}$；$\boldsymbol{\Lambda}_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{y}\in$

$\mathbb{Z}^m : \boldsymbol{A}\boldsymbol{y} = \boldsymbol{0}(\mathrm{mod}\, q)\}$。

定义 3　对于任意 $s>0$，以向量 $\boldsymbol{c}\in\mathbb{R}^m$ 为中心，$\boldsymbol{x}\in\boldsymbol{\Lambda}$，参数为 s，在格 $\boldsymbol{\Lambda}\subseteq\mathbb{Z}^m$ 上的高斯分布函数定义为 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\frac{\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2})$。

定义 4　令 $\rho_{s,\boldsymbol{c}}(\boldsymbol{\Lambda})=\sum_{\boldsymbol{x}\in\boldsymbol{\Lambda}}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$，对于任意 $s>0$，以向量 $\boldsymbol{c}\in\mathbb{R}^m$ 为中心，参数为 s 的格 $\boldsymbol{\Lambda}$ 上的离散高斯分布定义为 $D_{\boldsymbol{\Lambda},s,\boldsymbol{c}}(\boldsymbol{y})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{y})}{\rho_{s,\boldsymbol{c}}(\boldsymbol{\Lambda})}$，其中，$\boldsymbol{y}\in\boldsymbol{\Lambda}$。（若没有明确说明，$\boldsymbol{c}$ 默认为 0）

定义 5[17]　LWE 问题。对于任意正整数 $n,q\in\mathbb{Z}$，实数 $\alpha>0$，向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$，定义分布 $A_{\boldsymbol{s},\alpha}=\{(\boldsymbol{a},\boldsymbol{a}^t\boldsymbol{s}+e \mod q):\boldsymbol{a}\leftarrow{}_r\mathbb{Z}_q^n,\ e\leftarrow{}_r D_{\mathbb{Z},\alpha q}\}$。对于给定的任意 m 个独自取自 $A_{\boldsymbol{s},\alpha}$ 的采样 $(\boldsymbol{a}_1,b_1),\cdots,(\boldsymbol{a}_m,b_m)$，可以用矩阵形式表示为 $(\boldsymbol{A},\boldsymbol{b})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m$，其中，$\boldsymbol{A}=(\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m)$，$\boldsymbol{b}=(b_1,\cdots,\ b_m)^t$。如果对于任意 $\boldsymbol{s}\leftarrow{}_r\mathbb{Z}_q^n$，利用给定的多项式样品，不存在多项式概率时间算法能以不可忽略的概率恢复 $\boldsymbol{s}$，则 $\mathrm{LWE}_{n,q,\alpha}$ 问题是困难的。判定性 LWE 问题是区分任意多个 $A_{\boldsymbol{s},\alpha}$ 的独立样本和一致均匀分布的样本。对于给定的参数，判定性 LWE 问题的困难性可以规约到格上多项式因子内的量子近似最短线性无关向量问题（SIVP, shortest independent vector problem）的最坏情况。

2.2　安全模型

本节是在 Bellare 等[18]所提出模型（简称为 BPR 模型）基础上给出的本文协议的安全性分析模型。该协议依赖于一个假设：在协议执行之前，可信第三方制定公共参考串（CRS, common reference string）和其他公共参数。

协议参与方：每个协议参与方要么是用户 $U\in\mathcal{U}$，要么是可信服务器 $S\in\mathcal{S}$，其中，$\mathcal{U}$ 表示协议用户的集合。

长期密钥及实例：在基于认证密钥的协议中，长期密钥就是口令，可信服务器拥有口令列表 $pw_S=<pw_U>_{U\in\mathcal{U}}$，用户 $U\in\mathcal{U}$，拥有口令 pw_U，为简单起见，每个口令都是从一些字典集合 $\mathcal{D}$ 中独立均匀地选择出来的。每个用户可以与不同的意定通信方多次执行该协议，允许用户 $U\in\mathcal{U}$ 拥有无限数量的实例来执行该协议。其中，$\prod_U^i$ 表示用户 U 中的第 i 个实例，$\prod_S^j$ 表示服务器 S 中的第 j 个实例。每个实例只能使用一次且它与接下来被初始化为 $\perp$ 或 0 的变量有关。

sid_U^i、pid_U^i 和 sk_U^i 分别表示实例 $\prod_U^i$ 会话标识、意定通信方标识和其会话密钥。会话标识包括由实例 $\prod_U^i$ 发送和接收消息的有序连接，通信方标识指定实例所信任的用户。acc_U^i 和 $term_U^i$ 是布尔变量，分别表示实例 $\prod_U^i$ 已接受或拒绝。

敌手 $\mathcal{A}$ 是一个可以控制用户间所有通信信道的时间概率多项式算法。敌手 $\mathcal{A}$ 可以截获所有明文信息，读取它们并修改成想要的信息，也可以注入自己的信息；敌手 $\mathcal{A}$ 可以得到实例的会话密钥，也可以模仿会话密钥可能泄露的信息。敌手 $\mathcal{A}$ 和实例之间通过下述几种谕示询问来实现交互，这些谕示询问将敌手 $\mathcal{A}$ 的能力模型化，并生成谕示询问模型。

$\mathrm{send}(U,i,msg)$：敌手发送消息 msg 给用户实例 $\prod_U^i$。在接收到消息 msg 后，实例 $\prod_U^i$ 根据协议规范运行，并适当更新它的状态。谕示询问的输出是实例 $\prod_U^i$ 对收到的消息 msg 的响应输出。

$\mathrm{send}(S,j,msg)$：攻击者发送消息 msg 给服务器实例 $\prod_S^j$，且谕示询问的输出是实例 $\prod_S^j$ 收到消息 msg 之后的响应输出。

$\mathrm{execute}(U_1,i_1,U_2,i_2,S,j)$：如果用户实例 $\prod_{U_1}^{i_1}$、$\prod_{U_2}^{i_2}$ 与可信服务器实例 $\prod_S^j$ 没有被激活，这个谕示询问模型激活用户实例 $\prod_{U_1}^{i_1}$、$\prod_{U_2}^{i_2}$ 和服务器实例 $\prod_S^j$ 运行协议，且将执行的记录返回给攻击者。

$\mathrm{reveal}(U,i)$：这个谕示询问模型将生成的有效会话密钥 sk_U^i 返回给攻击者。

$\mathrm{test}(A,i)$：选择一个随机比特 $b\in{}_r\{0,1\}$，如果 $b=0$，则将均匀选择的随机值返回给敌手 $\mathcal{A}$；如果 $b=1$，将实例 $\prod_U^i$ 的会话密钥 sk_U^i 给敌手 $\mathcal{A}$。敌手 $\mathcal{A}$ 只能访问一次。

匹配会话：若 $sid_{U_1}^{i_1}=sid_{U_2}^{i_2}\neq\perp$，$pid_{U_1}^{i_1}=U_2$，$pid_{U_2}^{i_2}=U_1$，则称实例 $\prod_{U_1}^{i_1}$ 和 $\prod_{U_2}^{i_2}$ 互为匹配会话。

正确性：如果实例 $\prod_{U_1}^{i_1}$ 和 $\prod_{U_2}^{i_2}$ 互为匹配会话，$sk_{U_1}^{i_1}=sk_{U_2}^{i_2}\neq\perp$ 且双方都已经接受，即 $acc_{U_1}^{i_1}=acc_{U_2}^{i_2}=1$，则称 PAKE 协议是正确的。

定义 6　新鲜性。若满足以下条件，则称实例 $\prod_U^i$ 是新鲜的。

敌手 $\mathcal{A}$ 没有做出 $\mathrm{reveal}(U_1,i_1)$ 询问给实例 $\prod_{U_1}^{i_1}$。

敌手 $\mathcal{A}$ 没有做出 $\mathrm{reveal}(U_2,i_2)$ 询问给实例 $\prod_{U_2}^{i_2}$，

这里实例 $\prod_{U_1}^{i_1}$ 和实例 $\prod_{U_2}^{i_2}$ 互为匹配会话。

在谕示询问模型中，攻击者可以做出任意顺序多项式次以上查询，只要在某个时刻 $acc_U^i=1$ 进行的 test(A,i) 询问使实例 $\prod_U^i$ 是新鲜的。游戏继续直到攻击者输出一个对 b 的猜测 b'，如果 $b'=b$，则称攻击者赢得游戏。定义敌手 $\mathcal{A}$ 攻击 PAKE 协议 $\prod$ 的优势为 $\mathrm{adv}_{\Pi,\mathcal{A}}=\left|2\Pr[b'=b]-1\right|$。

定义 7 安全性。设口令字典空间为 $\mathcal{D}$，攻击次数 $Q(k)$ 表示攻击者以在线方式测试口令次数的边界值，其中，k 是与安全参数无关的常量。若对任意概率多项式时间的敌手 $\mathcal{A}$ 至多可进行 $Q(k)$ 次在线攻击，且满足 $\mathrm{adv}_{\Pi,\mathrm{A}}(k)\leqslant\dfrac{Q(k)}{|\mathcal{D}|}+\mathrm{negl}(k)$，则称 PAKE 协议 $\prod$ 是安全的。

2.3 基于格的公钥加密体制

一个带标签的 CCA 安全的公钥密码体制 $PK\varepsilon=(\mathrm{KeyGen},\mathrm{Enc},\mathrm{Dec})$，这个公钥加密体制的困难问题是基于 LWE 假设的，它的明文空间为 P。如果存在下述一对有效的可计算的函数(f,g)，则这个公钥密码体制是可拆分的。

基于格的公钥加密体制具体如下。

令 $n_1,n_2\in\mathbb{Z}$，q 为素数，$n=n_1+n_2+1$，$m=O(n\log q)\in\mathbb{Z}$，$\alpha,\beta\in\mathbb{R}$。

① 密钥生成算法 $(pk,sk)\leftarrow\mathrm{KeyGen}(1^k)$：输入安全参数 k，计算 $(\boldsymbol{A}_0,\boldsymbol{R}_0)\leftarrow\mathrm{TrapGen}(1^n,1^m,q)$、$(\boldsymbol{A}_1,\boldsymbol{R}_1)\leftarrow\mathrm{TrapGen}(1^n,1^m,q)$ 和 $crs\leftarrow\mathrm{CRSGen}(1^k)$，输出公私钥对 $(pk,sk)=((\boldsymbol{A}_0,\boldsymbol{A}_1,crs),\boldsymbol{R}_0)$。

② 加密算法 $c\leftarrow\mathrm{Enc}(pk,label,pw)$：输入公钥 $pk=(\boldsymbol{A}_0,\boldsymbol{A}_1,crs)$、明文 $pw\in P$、$label\in\{0,1\}^*$，随机选取 $\boldsymbol{s}_0,\boldsymbol{s}_1\leftarrow_r\mathbb{Z}_q^{n_1}$，$\boldsymbol{e}_0,\boldsymbol{e}_1\leftarrow_r D_{\mathbb{Z}^m,\alpha q}$，输出密文 $c=(u,v)$、$u=f(pk,pw,r)$、$v=g(pk,label,pw,r)$。

③ 解密算法 Dec：将私钥 $sk=\boldsymbol{R}_0$、$label$ 和密文 $c=(u,v)$ 作为输入，输出相应的明文 pw 或⊥，记为 $pw\leftarrow\mathrm{Dec}(sk,label,(u,v))$。

基于格的公钥加密体制的正确性：对于所有的公私钥对(pk,sk)，密文 $c=(u,v)$ 的第一部分 u 在任何 v' 和 $label'\in\{0,1\}^*$ 的意义上修正明文 pw，在安全参数 k 和 sk、r 的随机选择中，$\mathrm{Dec}(sk,label',(u,v'))\notin\{\perp,pw\}$ 的概率是可以忽略的。

将基于格的公钥密码体制 CCA 游戏的挑战阶段进行修改：敌手 $\mathcal{A}$ 首先提交两个等长明文 $pw_0,pw_1\in P$，挑战者 $\mathcal{C}$ 随机选择一个比特 $b^*\leftarrow_r\{0,1\}$、随机数 $r^*\leftarrow_r\{0,1\}^*$，计算 $u^*=f(pk,pw_{b^*},r^*)$，将其返回给敌手 $\mathcal{A}$。敌手 $\mathcal{A}$ 接收到 u^* 之后输出 $label\in\{0,1\}^*$，最后，挑战者 $\mathcal{C}$ 计算 $v^*=g(pk,label,pw_{b^*},r^*)$，将计算出的密文 $c^*=(u^*,v^*)$ 发送给敌手 $\mathcal{A}$。

定义敌手的优势为 $\mathrm{adv}_{PK\varepsilon,\mathcal{A}}^{\text{ind-cca}}(1^\kappa)\overset{\text{def}}{=}\left|\Pr[b=b^*]-\dfrac{1}{2}\right|$，如果对于任意概率多项式时间的敌手 $\mathcal{A}$ 的优势 $\mathrm{adv}_{PK\varepsilon,\mathcal{A}}^{\text{ind-cca}}(1^k)$ 在安全参数 k 上是可忽略的，那么就称基于格的公钥密码体制是 CCA 安全的。

在上述描述中，“可拆分”性质除了体现在函数上，还体现在基于格的公钥密码体制的安全性上。修改后的 CCA 游戏，对手可以看见密文 c^* 的第一部分 u^*，然后自适应地确定 label，构成完整的挑战密文 $c^*=(u^*,v^*)$。其中，密文的一部分被看作对明文计算的函数，另一部分是有关用户身份的函数，这种性质已被用到身份基加密中[19]。通过这种通用转换（如 Canetti 等[20]提出的从 IBE（identity-based encryption）到 PKE（public-key encryption）的转换技术（简称为 CHK 技术））的应用，可以得到一个可拆分的 PKE，基于格的公钥密码体制中函数 g 输出一个标签，用来验证整个密文的有效性。最后，这里强调可拆分 PKE 的概念主要是为了达到两轮通信的目的。

2.4 近似平滑投射散列函数

平滑投射散列函数是由 Cramer 等[21]为实现 CCA 安全的公钥加密体制首次提出来的，后来在 PAKE 协议方面的一些研究[7,22]延伸了这个概念。本文采用文献[16]构造的基于格的 PAKE 协议的 ASPH 函数，此构造[16]根据文献[7]进行了修改。

假设 $PK\mathcal{E}=(\mathrm{KeyGen},\mathrm{Enc},\mathrm{Dec})$ 是一个由函数构成的在格上语义安全的公钥加密体制。假设给定一个有效密文 c，可以很容易将 $c=(u,v)$ 解析为(f,g)的输出。用密钥生成算法生成密钥对 $(pk,sk)\leftarrow\mathrm{KeyGen}(1^\kappa)$，$C_{pk}$ 表示相应于公钥 pk 的有效密文空间，$\mathcal{P}$ 是明文空间。定义

$$X=\{(label,c,pw)\mid(label,c)\in C_{pk};pw\in\mathcal{P}\}$$

$$L=\{(label,c,pw)\in X\mid label\in\{0,1\}^*;\ c=\mathrm{Enc}(pk,label,pw)\}$$

$$\overline{L}=\{(label,c,pw)\in X\mid label\in\{0,1\}^*;\ pw=\mathrm{Dec}(sk,label,c)\}$$

一个相应于公钥 pk 的公钥加密体制对应的 ϵ-approximate SPH 函数 $(K,\ell,\{H_{hk}:X\to\{0,1\}^{\ell}\}_{hk\in K}$, $\mathrm{HP},\mathrm{Proj}:K\to HP)$ 表示为：1) Hash 函数簇 $H=\{H_{hk}\}_{hk\in K}$，其中，定义域为 X，值域为 $\{0,1\}^{\ell}$，K 为 Hash 密文空间；2) 一个从 K 到 HP 上的密钥投射函数 Proj，其中，HP 为投射密钥空间。

1) 存在高效的算法：采样一个散列密钥 $hk\leftarrow_r K$，hk 是元组，其中每个元素服从离散高斯分布；对于 $hk\in K$，$x=(label,(u,v),pw)\in X$，计算 $H_{hk}(x)=H_{hk}(u,pw)$；计算投射密钥 $hp=\mathrm{Proj}(hk)$，其中 $hk\in K$。

2) 对任意 $hk\leftarrow_r K$、$x=(label,(u,v),pw)\in L$、随机数 r，得到 $u=f(pk,pw,r)$ 和 $v=g(pk,label,pw,r)$ 存在一个有效的算法计算 $\mathrm{Hash}(hp,x,r)=\mathrm{Hash}(hp,(u,pw),r)$。

正确性：对 $x=(label,(u,v),pw)\in L$ 以及投射密钥 $hp=\mathrm{Proj}(hk)$，满足 $\Pr[\mathrm{Ham}(H_{hk}(u,pw),\ \mathrm{Hash}(hp,(u,pw),r))\geqslant\epsilon\cdot]=\mathrm{negl}(k)$。

平滑性：对任意的函数 h：$HP\to X\backslash\bar{L}$、$hk\leftarrow_r K$、$hp=\mathrm{Proj}(hk)$、$x=h(hp)$、$\rho\leftarrow_r\{0,1\}^{\ell}$，两个分布 $(hp,H_{hk}(x))$ 和 (hp,ρ) 统计距离在安全参数 κ 上是可忽略的。

本文 ASPH 函数满足上述两个性质，其中，ASPH 函数概念与 Katz 等[7]的 ASPH 概念相比有 3 处修改：1) 投射函数只依赖于散列密钥；2) $H_{hk}(x)=H_{hk}(u,pw)$ 的值由散列密钥 hk、密文 $c=(u,v)$ 的第一部分 u 和明文 pw 来决定；3)对于 $x=h(hp)\notin\bar{L}$ 的适应性选择，光滑性成立。这里第一项修改使本文协议达到两轮通信，后两项为证明本文协议的安全性做准备。

3　基于格的三方 PAKE 协议

3.1　协议描述

本节基于文献[16]提出的可拆分公钥密码体制，利用 ASPH 函数簇这个组件设计一种格上的基于口令的三方认证密钥交换协议。协议中的符号说明如表 1 所示。

$PK\mathcal{E}=(\mathrm{KeyGen},\mathrm{Enc},\mathrm{Dec})$ 是一个关于函数(f,g)可拆分的公钥密码体制。相应的 ε – ASPH 函数簇由下列函数组成，其中，$\epsilon\in(0,\frac{1}{2})$ 是一个较小的实数：1) Hash 函数簇 $H=\{H_{hk}\}_{hk\in K}$，其中，定义域为 X，值域为 $\{0,1\}^{\ell}$，K 为 Hash 密钥空间。2) 密钥投射函数 $\mathrm{Proj}:K\to HP$，其中，HP 为投射密钥空间。κ 是安全参数，ℓ 是一个与 n 相关的整数 $\mathrm{ECC}:\{0,1\}^{\kappa}\to\{0,1\}^{\ell}$，表示纠错码的编码算法，可以纠错 2ϵ 部分；$\mathrm{ECC}^{-1}:\{0,1\}^{\ell}\to\{0,1\}^{\kappa}$ 是译码算法。$F=\{F_{\delta}:\delta\in\{0,1\}^{\ell_{\delta}}\}_{\delta\in\mathbb{N}}$ 表示伪随机函数簇。公共参数为 pk，作为公钥加密体制的公钥，由可信第三方用算法 $\mathrm{KeyGen}(1^{\kappa})$ 生成。在系统中没有用户需要知道 pk 对应的私钥。系统中引用会话序列号 $ssid$，会话序列号呈递增形式，且在成功完成一次会话之后，服务器记录每一个用户的本次会话序列号，可以验证发送的消息是否是重放的。图 1 概述了本文的 PAKE 协议。

表 1　基于格的三方协议 PAKE 协议中的符号说明

符号	说明
r_{A_1},r_{A_2}	用户 A 和 B 的随机值
hk	Hash 密钥
K	Hash 密钥空间
hp	投射密钥
$label$	标签
f,g	函数
δ_{SA},δ_{SB}	伪随机函数密钥
F	伪随机函数
ECC, ECC^{-1}	编码算法，译码算法
sk_{AB},sk_{BA}	由用户 A 和 B 生成的会话密钥

用户 A 和服务器 S 共享口令 $pw_A\in\mathcal{D}\subset P$，用户 B 和服务器 S 共享口令 $pw_B\in\mathcal{D}\subset P$，其中，$\mathcal{D}$ 是系统中有效口令的集合。

用户 A/B 选择随机值 $r_{A1}\leftarrow_r\{0,1\}^*$、散列密钥 $hk_{A1}\leftarrow_r K$（$r_{B1}\leftarrow_r\{0,1\}^*$、$hk_{B1}\leftarrow_r K$），用户 A 和 B 分别计算 $hp_{A1}=\mathrm{Proj}(hk_{A1})$、$hp_{B1}=\mathrm{Proj}(hk_{B1})$。发送方 $\prod_{U_1}^{i_1}$ 激活协议后会有一个会话序列号 $ssid_{U_1}$。用户 A 令 $label_{A1}:=A\|B\|S\|hp_{A1}\|ssid_A$，计算 $(u_{A1},v_{A1})=\mathrm{Enc}(pk,label_{\mathrm{A1}},pw_A,r_{A1})$，其中，$u_{A1}=f(pk,pw,r_{A1})$，$v_{A1}=g(pk,label_{A1},pw_A,r_{A1})$。用户 B 做出类似计算。用户 A 和 B 分别向服务器发送消息 $<A,B,S,hp_{A1},c_{A1}=(u_{A1},v_{A1}),ssid_A>$ 和 $<B,A,S,hp_{B1},c_{B1}=(u_{B1},v_{B1}),ssid_B>$。

服务器 S 收到用户 A 发送的消息，查看会话序列号 $ssid_A$ 是否大于服务器中保存的前次会话序列号，如果不大于该值则终止会话；否则，由已知的

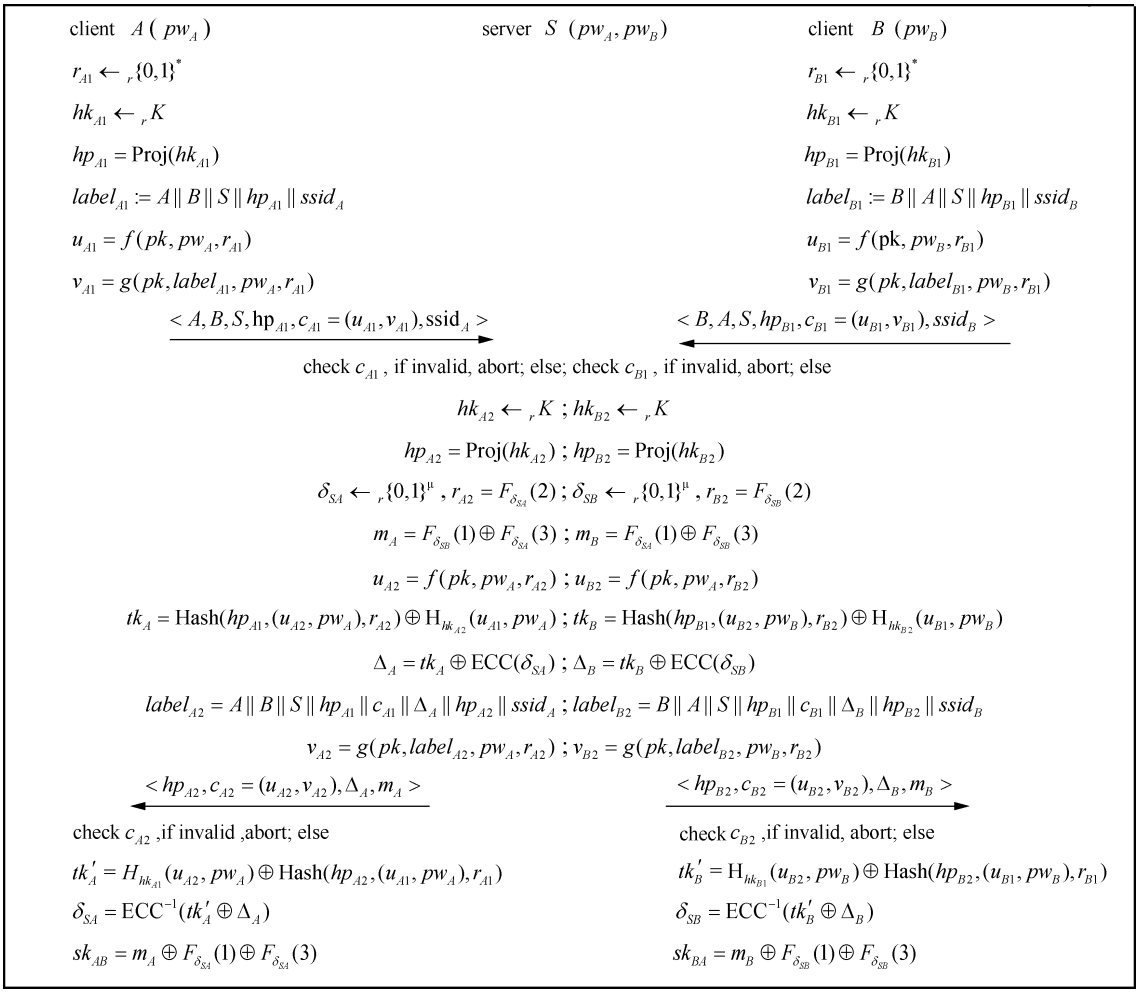

图 1　基于格的三方 PAKE 协议

pw_A 和 $ssid_A$ 、 $label_{A1} := A \| B \| S \| hp_{A1} \| ssid_A$ 验证 c_{A1} 是否是有效的密文。若检验 c_{A1} 无效，则拒绝并终止；反之，随机选择 $hk_{A2} \leftarrow_r K$ 、 δ_{SA} 、 δ_{SB} ，计算 $hp_{A2} = \text{Proj}(hk_{A2})$ 、 $r_{A2} = F_{\delta_{SA}}(2)$ 、 $m_A = F_{\delta_{SB}}(1) \oplus F_{\delta_{SA}}(3)$ 、 $u_{A2} = f(pk, pw_A, r_{A2})$ ，然后计算 $tk_A = \text{Hash}(hp_{A1}, (u_{A2}, pw_A), r_{A2}) \oplus \text{H}_{\text{hk}_{A2}}(u_{A1}, pw_A)$ 。用纠错码的编码算法 ECC 计算 $\Delta_A = tk_A \oplus \text{ECC}(\delta_{SA})$ 。令 $label_{A2} = A \| B \| S \| hp_{A1} \| c_{A1} \| \Delta_A \| hp_{A2} \| ssid_A$ ，计算 $v_{A2} = g(pk, label_{A2}, pw_A, r_{A2})$ 。最后向用户 A 发送消息 $< hp_{A2}, c_{A2} = (u_{A2}, v_{A2}), \Delta_A, m_A >$ ，并更新前次会话序列号为 $ssid_A$ 。服务器收到用户 B 的消息后也做出类似响应。本轮消息对密文有效性的验证既可以检验口令的正确性，也可以察觉攻击者的重放攻击。

用户 A 收到服务器的消息后，计算 $tk'_A = \text{H}_{hk_{A1}}(u_{A2}, pw_A) \oplus \text{Hash}(hp_{A2}, (u_{A1}, pw_A), r_{A1})$ 和伪随机函数密钥 δ_{SA} ，再用已知的 hp_{A2} 、 Δ_A 、 ssid_A 和计算的 r_{A2} 验证 c_{A2} ，若无效则拒绝；反之，计算会话密钥 $sk_{AB} = m_A \oplus F_{\delta_{SA}}(1) \oplus F_{\delta_{SA}}(3)$ 。用户 B 也做出类似响应计算出会话密钥 $sk_{BA} = m_B \oplus F_{\delta_{SB}}(1) \oplus F_{\delta_{SB}}(3)$ 。

基于格的三方 PAKE 协议的两轮消息认证中，第一轮用户向服务器发送的密文中包含带标签的密文，服务器通过检验密文的有效性实现服务器对用户的显示认证，在第二轮中实现了用户对服务器的显示认证，因此本文协议实现了用户与服务器的双向认证。

另外，服务器在接收用户 A 和 B 发送的消息之后，对本次会话序列号 $ssid_A / ssid_B$ 与前次保存的会话序列号进行比较，由于会话序列号 ssid 呈递增形式，因此检查若不大于之前的会话序列号，则消息是重放的，否则该消息不是重放的。因此本文协议实现了抵抗消息重放攻击的作用。

正确性：基于格的三方 PAKE 协议表明诚实用户以压倒性概率得到相同会话密钥。首先所有诚实

方生成的密文是有效的，然后根据 ASPH 的近似正确性可知 Hash $(hp,(u,pw),r)$ 和 $H_{hk}(u,pw)$ 的汉明距离大于 ϵ 的概率是可以忽略的，因此 tk_A (tk_B) 和 tk'_A (tk'_B) 的汉明距离至多为 2ϵ，且由 ECC 的定义可知其可以纠错 2ϵ 部分，用户 A/B 和服务器可以得到相同的 δ_{SA}/δ_{SB}，所以用户 A 和 B 可得到相同的会话密钥。

3.2　安全性证明

本节在 2.2 节所述的安全模型证明了协议的安全性。

定理 1　如果 $PK\mathcal{E}=(\mathrm{KeyGen},\mathrm{Enc},\mathrm{Dec})$ 是基于 LWE 困难问题假设的可拆分 CCA 安全公钥加密体制及与之相应的 ϵ - ASPH 函数簇：1)Hash 函数簇 $H=\{H_{hk}\}_{hk\in HK}$，其中，定义域为 X，值域为 $\{0,1\}^{\ell}$，HK 为 Hash 密钥空间；2) 密钥投射函数 $\mathrm{Proj}:HK\to HP$，其中，HP 为投射密钥空间。$\mathrm{ECC}:\{0,1\}^{\kappa}\to\{0,1\}^{\ell}$ 是纠错码的编码算法，可以纠错 2ϵ 部分，$F=\{F_{\delta}\}$ 是安全的伪随机函数簇，那么本文协议是一个安全的 PAKE 协议。

假设 $0\in P\backslash\mathcal{D}$，0 在系统中不是一个有效的口令。首先，由于格上公钥加密体制 $PK\mathcal{E}$ 的 CCA 安全性，敌手通过 execute 询问不能得到真正口令的任何有用信息。在 execute 询问的回答中如果对口令 pw 的加密被代替为对 0 的加密，对敌手而言在计算上是不可区分的。因为 $0\notin\mathcal{D}$，通过 ASPH 的光滑性，在 execute 询问中实例的会话密钥与均匀分布的会话密钥对敌手来说是不可区分的。其次，如果敌手只是简单地在诚实的实例之间传递信息，对于 execute 询问其验证是相同的。如果敌手修改了一些实例的消息输出（即 *label* 密文对），然后一方用 CCA 安全提供的解密谕示解密修改的密文，检验解密结果 pw' 是否与真正的口令 pw 相等。若 $pw'=pw$，称这种攻击是成功的（这种更改会增加攻击者的优势）。利用加密体制 $PK\mathcal{E}$ 的 CCA 安全性，pw 是从 $\mathcal{D}$ 中均匀随机选择出来的，$\Pr[pw'=pw]$ 至多为 $\dfrac{1}{|\mathcal{D}|}$。因此对于敌手而言，得到的相应的会话密钥与均匀分布的会话密钥是不可区分的。

证明　通过 G_0 到 G_{10} 一系列的游戏来证明定理 1。其中，G_0 是真实安全的游戏，G_{10} 是均匀选择会话密钥的随机游戏。这个安全是通过展示敌手的优势来建立的，从游戏 G_0 到 G_{10}，敌手的优势之差最多为 $\dfrac{Q(\kappa)}{|\mathcal{D}|}+\mathrm{negl}(\kappa)$。

$\mathrm{adv}_{\mathcal{A},i}(\kappa)$ 表示在游戏 G_i 中敌手的优势。协议关于用户是对称的，以下证明只取一个用户，除了特殊说明，对于用户 B 的实例处理类似于用户 A 的实例。

游戏 G_0：这个实验对应于安全模型中的真实攻击，所有发出的谕示询问的回答根据协议的规范都是诚实的回答。

游戏 G_1：这个实验与游戏 G_0 相似，只是在每次 execute 询问的回答中 tk'_A 的值直接用其相应的 hk_{A1}、hk_{A2} 来计算，例如，$tk'_A=\mathrm{H}_{\mathrm{hk}_{A1}}(u_{A2},pw_A)\oplus\mathrm{H}_{hk_{A2}}(u_{A1},pw_A)$。

引理 1　基于格 PAKE 协议的 ϵ - ASPH 函数簇为：1)Hash 函数簇 $H=\{H_{hk}\}_{hk\in HK}$，其中，定义域为 X，值域为 $\{0,1\}^{\ell}$，HK 为 Hash 密钥空间；2)密钥投射函数 $\mathrm{Proj}:HK\to HP$，其中，HP 为投射密钥空间。纠错码的编码算法 $\mathrm{ECC}:\{0,1\}^{\kappa}\to\{0,1\}^{\ell}$，存在 $\left|\mathrm{adv}_{\mathcal{A},1}(\kappa)-\mathrm{adv}_{\mathcal{A},0}(\kappa)\right|\leqslant\mathrm{negl}(\kappa)$。

证明　由于模拟器知道 hk_1 和 hk_2，由 ASPH 的近似正确性和 ECC 的正确性可知引理 1 成立。

游戏 G_2：将 execute 做修改，密文 c_{A1} 被代替为对 $0\notin\mathcal{D}$ 的加密。

引理 2　如果 $PK\mathcal{E}=(\mathrm{KeyGen},\mathrm{Enc},\mathrm{Dec})$ 是一个基于格的 CCA 安全的方案，那么 $|\mathrm{adv}_{\mathcal{A},2}(\kappa)-\mathrm{adv}_{\mathcal{A},1}(\kappa)|\leqslant\mathrm{negl}(\kappa)$。

证明　因为敌手 $\mathcal{A}$ 只能做出多项式次 execute 询问，通过标准混合论证只考虑一个 execute 询问就足够了。游戏 G_1 和 G_2 之间唯一的不同是将 $0\notin\mathcal{D}$ 的加密结果代替为对 pw_A 的加密。任何概率多项式时间下对手 $\mathcal{A}$ 都可以以不可忽略的优势区分这两个游戏，并且它可以直接转换成算法 $\mathcal{B}$，这个算法以相同的优势打破底层格上公钥加密体制的 CCA 安全性。

给出一个挑战公钥 pk，算法 $\mathcal{B}$ 将 pk 作为协议的 CRS（公共参数），在游戏 G_1 中与敌手 $\mathcal{A}$ 交互。当算法 $\mathcal{B}$ 需要回答敌手 $\mathcal{A}$ 的 execute 询问时，首先随机选择一个散列密钥 $hk_{A1}\leftarrow_r K$，计算投射密钥 $hp_{A1}=\mathrm{Proj}(hk_{A1})$。然后算法 $\mathcal{B}$ 提交两个明文 $(pw_A,0)$ 和 $\mathrm{label}_{A1}:=A\|B\|S\|\mathrm{hp}_{A1}\|ssid_A$ 给它的挑战者，得到一个挑战密文 c^*_{A1}。最后算法 $\mathcal{B}$ 用 c^*_{A1} 作

为 execute 询问的回答，将敌手 $\mathcal{A}$ 的输出作为算法 $\mathcal{B}$ 的猜测。如果 c^*_{A1} 是 pw_A 的加密结果，算法 $\mathcal{B}$ 完全模拟敌手 $\mathcal{A}$ 在游戏 G_1 的攻击环境，否则算法 $\mathcal{B}$ 模拟敌手 $\mathcal{A}$ 在游戏 G_2 的攻击环境。因此如果敌手 $\mathcal{A}$ 能以不可忽略的优势区分 G_1 和 G_2，算法 $\mathcal{B}$ 能以相同的优势打破 CCA 安全性。

游戏 G_3：将 execute 询问做出修改，tk_A 的值直接用其相应的散列密钥 hk_{A1} 和 hk_{A2} 计算，例如，$tk_A = \mathrm{H}_{hk_{A1}}(u_2, pw) \oplus \mathrm{H}_{hk_{A2}}(u_1, pw)$，并将密文 c_{A2} 用 $0 \notin \mathcal{D}$ 的加密代替。

引理 3 公钥加密体制在 LWE 假设下是一个可拆分的 CCA 安全的方案，且根据 ASPH 的定义及纠错编码算法可以纠错 2ϵ 部分错误的性质，有 $\left|\mathrm{adv}_{\mathcal{A},3}(\kappa) - \mathrm{adv}_{\mathcal{A},2}(\kappa)\right| \leqslant \mathrm{negl}(\kappa)$。

证明 这个引理通过一系列类似游戏 G_0 到 G_2 来显示，此外，游戏利用 2.3 节中考虑的修改的 CCA 安全游戏，而不是标准的 CCA 安全游戏。

游戏 G_4：在 execute 询问中，强制用户计算的 tk'_A 和服务器计算的 tk_A 一致，其他计算保持不变。

引理 4 根据近似平滑散列函数的定义及性质，有 $\left|\mathrm{adv}_{\mathcal{A},4}(\kappa) - \mathrm{adv}_{\mathcal{A},3}(\kappa)\right| \leqslant \mathrm{negl}(\kappa)$。

证明 在每次 execute 询问中，两个密文 $c_{A1} = (u_{A1}, v_{A1})$ 和 $c_{A2} = (u_{A2}, v_{A2})$ 都是不属于字典集 $\mathcal{D}$ 的加密结果，且 $tk'_A = tk_A = \mathrm{H}_{hk_{A1}}(u_{A1}, pw) \oplus \mathrm{H}_{hk_2}(u_{A2}, pw)$，其值是统计接近于均匀分布。在 execute 询问中，屏蔽部分 $\Delta_A = tk_A \oplus \mathrm{ECC}(\delta_{SA})$ 向敌手 $\mathcal{A}$ 隐藏 $\delta_{SA} \in_r \{0,1\}^\mu$，由于 $\delta_{SA} \in_r \{0,1\}^\mu$ 是随机均匀的，在游戏 G_4 中修改部分只有可忽略的统计差距，攻击者至多只能进行多项式次 execute 询问，所以最终引起的优势差是可忽略的。

游戏 G_5：将 execute 询问中的伪随机函数做出修改，对每个随机选择的 δ_{SA}，把 $F_{\delta_{SA}}(i), i = 1,2,3$ 的值换成独立均匀选取的随机数。

引理 5 $\left|\mathrm{adv}_{\mathcal{A},5}(\kappa) - \mathrm{adv}_{\mathcal{A},4}(\kappa)\right| \leqslant \mathrm{negl}(\kappa)$

证明 在 execute 询问中，用户与服务器共享有相同的随机选取的 tk_A，故将会得到相同的 δ_{SA}，根据伪随机函数簇的定义可知引理 5 成立。

从游戏 G_1 到游戏 G_5，以用户 A 为例完成了对 execute 询问模拟方式的修改，敌手不能从这些询问中得到用户口令的任何信息。

接下来将开始考虑 send 询问。开始之前根据协议一部分被发出的消息将 send 询问分为 3 类，记 $\mathrm{send}_0(A, i_1, B, i_2, S, j)$ 为激活用户实例和服务器实例开始执行协议的消息；$\mathrm{send}_1(S, j, (A, B, S, hp_{A1}, c_{A1}, ssid_A))$ 为向服务器实例 $\prod_S^j$ 发送消息 $msg_1 = (A, B, S, hp_{A1}, c_{A1}, ssid_A)$；$\mathrm{send}_2(A, i_1, (hp_{A2}, c_{A2}, \Delta_A, m_A))$ 为向用户实例 $\prod_A^{i_1}$ 发送消息 $msg_2 = (hp_{A2}, c_{A2}, \Delta_A, m_A)$。如果服务器实例 $\prod_S^j$ 收到的消息 msg_1 是有效的，才能向敌手返回相应的消息 msg_2。另外，在密钥生成阶段生成公共参数 pk 的同时，模拟者 $\mathcal{C}$ 记录对应的私钥 sk。

游戏 G_6：对于 $\mathrm{send}_1(S, j, msg'_1 = (A', B', S', hp'_{A1}, c'_{A1}, ssid'_A))$ 询问，令 $label'_{A1} \coloneqq A' \| B \| S \| hp'_{A1} \| ssid'_A$，如果 c_{A1} 不是有效的密文，则模拟者拒绝该消息，其中，如果检验 $ssid'_A$ 不大于服务器保存前次会话序列号的值，则拒绝该消息。否则，模拟者 $\mathcal{C}$ 用 pk 相应的私钥 sk 解密 $pw'_A = \mathrm{Dec}_{sk}(c'_{A1})$，若 $pw'_A = pw_A$，则认为敌手 $\mathcal{A}$ 成功并结束游戏的模拟。

引理 6 由近似平滑投射函数的定义，有 $\mathrm{adv}_{\mathcal{A},5}(\kappa) \leqslant \mathrm{adv}_{\mathcal{A},6}(k) + \mathrm{negl}(k)$。

证明 考虑 c'_{A1} 是一个有效的密文，因为模拟者 $\mathcal{C}$ 在游戏 G_5 中知道 pk 相应的私钥 sk，所以可以解密 $(label'_{A1}, c'_{A1})$ 得到解密结果 pw'_A。很显然 $pw'_A = pw_A$ 这种修改可以增加敌手的优势。至于 $pw'_A \neq pw_A$ 这种情况，有 $(label'_{A1}, c'_{A1}, pw_A) \notin \overline{L}$。通过 ASPH 的光滑性，由实例 $\prod_S^j$ 输出的隐秘部分 $\Delta_A = tk_A \oplus \mathrm{ECC}(\delta_{SA})$ 统计上是向敌手隐藏 $\delta_{SA} \in_r \{0,1\}^\mu$，因此 $pw'_A \neq pw_A$ 这种修改只有可忽略的统计差距，可知引理 6 是成立的。

游戏 G_7：对于 $\mathrm{send}_2(A, i_1, msg'_2 = (hp'_{A2}, c'_{A2}, \Delta'_A, m'_A))$ 询问，令 $msg_1 = (A, B, S, hp_{A1}, c_{A1}, ssid_A)$ 是由之前的 $\mathrm{send}_0(A, i_1, B, i_2, S, j)$ 询问输出的消息。

如果 msg'_2 是之前 $\mathrm{send}_1(S, j, msg_1)$ 询问的输出，模拟者直接用相应的 hk_{A1} 和 hk_{A2} 来计算 tk'_A，强制用户实例与服务器实例拥有相同的 δ_{SA}。由于 δ_{SA} 对敌手是隐藏的，所以此修改不改变敌手的优势。

令 $label'_{A2} \coloneqq A \| B \| S \| hp_{A1} \| c_{A1} \| hp'_{A2} \| \Delta'_A \| ssid_A$，如果检验 c'_{A2} 不是有效的密文，模拟者 $\mathcal{C}$ 拒绝询问；否则，模拟者 $\mathcal{C}$ 用 pk 相应的私钥 sk 解密密文得到解密结果 pw'_A，若 $pw'_A = pw_A$，模拟者 $\mathcal{C}$ 认为敌手成功并停止模拟，此修改增加敌手的优势。

引理 7 根据近似平滑散列函数的定义及纠错

编码算法可以纠错 2ϵ 部分错误的性质，有 $\mathrm{adv}_{\mathcal{A},6}(\kappa) \leqslant \mathrm{adv}_{\mathcal{A},7}(k) + \mathrm{negl}(\kappa)$。

游戏 G_8：对 $\mathrm{send}_0(A,i_1,B,i_2,S,j)$ 询问进行修改，如果用户被 send_0 激活，则对 $0 \notin \mathcal{D}$ 加密得到密文 c_{A1}。

引理 8　如果 $PK\mathcal{E}$= (KeyGen, Enc, Dec) 是一个基于 LWE 困难假设的 CCA 安全的方案，那么 $\left|\mathrm{adv}_{\mathcal{A},8}(\kappa) - \mathrm{adv}_{\mathcal{A},7}(k)\right| \leqslant \mathrm{negl}(k)$。

证明　通过一个标准的混合论证，只考虑一个 $\mathrm{send}_0(A,i_1,B,i_2,S,j)$ 询问就够了。在这种情况下，游戏 G_8 与 G_7 之间仅有的不同是将不属于字典集 $\mathcal{D}$ 的口令加密结果代替真实口令 pw 的加密结果。任何概率多项式时间下敌手 $\mathcal{A}$ 都可以以不可忽略的优势区分这两个游戏，这个时间概率多项式敌手可以直接转换为算法 $\mathcal{B}$，这个算法可以打破公钥密码体制的 CCA 安全。

给出一个挑战公钥 pk，算法将 pk 作为协议的 CRS，为敌手 $\mathcal{A}$ 模拟在游戏 G_7 中的攻击环境。当算法 $\mathcal{B}$ 需要回答敌手的 send_0 回答时，首先随机选择散列密钥 $hk_{A1} \leftarrow_r K$，计算投射密钥 $hp_{A1} = \mathrm{Proj}(hk_{A1})$。然后算法 $\mathcal{B}$ 将两个密文 $(pw_A, 0)$ 和 $label_{A1} := A \| B \| S \| \cdot \| hp_{A1} \| ssid_A$ 提交给它的挑战者，得到一个挑战密文 c^*_{A1}。最后算法 $\mathcal{B}$ 将 $(A, B, S, hp_{A1}, c^*_{A1})$ 发送给敌手 $\mathcal{A}$。当算法 $\mathcal{B}$ 必须解密一些有效的 $label$ 密文对 $(label'_{A1}, c'_{A1}) \neq (label_{A1}, c^*_{A1})$，它提交 $(label'_{A1}, c'_{A1})$ 给自己的 CCA 安全挑战者。在某时刻，敌手 $\mathcal{A}$ 输出一个比特值 $b \in \{0,1\}$，算法 $\mathcal{B}$ 将输出的 b 作为自己的猜测。如果 c^*_{A1} 是对 pw_A 加密的密文，算法 $\mathcal{B}$ 为敌手 $\mathcal{A}$ 完全模拟游戏 G_7 的攻击环境。所以，如果敌手 $\mathcal{A}$ 可以以不可忽略的优势区分游戏 G_7 和 G_8，算法 $\mathcal{B}$ 可以具有相同的优势打破公钥加密体制的 CCA 安全。

游戏 G_9：$\mathrm{send}_1(S, j, msg'_1 = (A', B', S', hp'_{A1}, c'_{A1}))$ 询问被修改，如果 msg'_1 是之前 send_0 询问的输出，模拟者 $\mathcal{C}$ 用相应的散列密钥 (hk_{A1}, hk_{A2}) 计算 tk_A；否则，模拟者 $\mathcal{C}$ 执行方式完全类似于游戏 G_8。

引理 9　根据近似平滑投射散列函数的定义及纠错编码算法可以纠错 2ϵ 部分错误的性质，有 $\left|\mathrm{adv}_{\mathcal{A},9}(k) - \mathrm{adv}_{\mathcal{A},8}(k)\right| \leqslant \mathrm{negl}(k)$。

证明　如果 msg'_1 是之前 send_0 询问的输出，那么有：1) 模拟者 $\mathcal{C}$ 知道相应的散列密钥 (hk_{A1}, hk_{A2})；2) $c'_{A1} = (u'_{A1}, v'_{A1})$ 是对 $0 \notin \mathcal{D}$ 的加密。因此，由服务器实例输出的 $\Delta_A = tk_A \oplus \mathrm{ECC}(\delta_{SA})$ 向对手隐藏了 $\delta_{SA} \in_r \{0,1\}^\mu$，可以知道在游戏 G_9 中的修改描述了一个可忽略的统计差距。

游戏 G_{10}：对 $\mathrm{send}_1(S, j, msg'_1 = (A', B', S', hp'_{A1}, c'_{A1}))$ 进行修改，如果 msg'_1 是之前 send_0 询问的输出，模拟者 $\mathcal{C}$ 用对 $0 \notin \mathcal{D}$ 的加密密文代替密文 c_{A2}；否则，模拟者 $\mathcal{C}$ 执行方式完全类似于游戏 G_9。

引理 10　如果 $PK\mathcal{E}$= (KeyGen, Enc, Dec) 是一个基于 LWE 困难假设的可拆分 CCA 安全方案，那么有 $\left|\mathrm{adv}_{\mathcal{A},10}(k) - \mathrm{adv}_{\mathcal{A},9}(k)\right| \leqslant \mathrm{negl}(k)$。

证明　如同前面的一样，敌手 $\mathcal{A}$ 只考虑一个由实例 $\prod_A^{t_i}$ 发出的 $\mathrm{send}_1(S, j, msg'_1 = (A', B', S', hp'_{A1}, c'_{A1}))$ 询问就足够了。任何时间概率多项式敌手 $\mathcal{A}$ 以不可忽略的优势区分这两个游戏，这个时间概率多项式可以直接转换为算法，这个算法 $\mathcal{B}$ 以相同的优势打破基于格的公钥加密体制的 CCA 安全性。

给出一个挑战公钥 pk，算法 $\mathcal{B}$ 设置 pk 为协议的 CRS，并在游戏 G_9 中与敌手 $\mathcal{A}$ 交互。当算法 $\mathcal{B}$ 需要回答 send_1 询问时，首先选择一个散列密钥 $hk_{A2} \leftarrow_r K$、一个随机会话密钥 $\delta_{SA} \in_r \{0,1\}^\mu$，计算 $hp_{A2} = \mathrm{Proj}(hk_{A2})$。然后算法 $\mathcal{B}$ 提交密文 $(pw_A, 0)$ 给它的挑战者。算法 $\mathcal{B}$ 得到 u^*_{A2} 之后，计算 $tk_A = \mathrm{H}_{hk_{A1}}(u^*_{A2}, pw_A) \oplus \mathrm{H}_{hk_{A2}}(u'_{A1}, pw_A)$、$\Delta_A = tk_A \oplus \mathrm{ECC}(\delta_{SA})$，将 $label_{A2} := A \| B \| S \| hp'_{A1} \| c'_{A1} \| hp_{A2} \| \Delta_A \| ssid_A$ 提交给修改的 CCA 安全挑战者，得到挑战密文 $c^*_{A2} = (u^*_{A2}, v^*_{A2})$。最后算法 $\mathcal{B}$ 将 $(hp_A, c^*_{A2}, \Delta_A, m_A)$ 发送给敌手 $\mathcal{A}$。当算法 $\mathcal{B}$ 解密出有效的 $label$ 密文 $(label'_{A2}, c'_{A2}) \neq (label_{A2}, c^*_{A2})$，它将 $(label'_{A2}, c'_{A2})$ 提交给它的挑战者。在某时刻，敌手 $\mathcal{A}$ 输出一个比特值，算法 $\mathcal{B}$ 输出 b 作为它的猜测。如果 c^*_{A2} 是对 pw_A 的加密，模拟者为敌手 $\mathcal{A}$ 模拟游戏 G_9 的攻击环境，否则模拟游戏 G_{10} 的攻击环境。因此，如果敌手 $\mathcal{A}$ 可以以不可忽略的优势区分游戏 G_9 和 G_{10}，那么算法 $\mathcal{B}$ 可以以相同的优势打破格上的公钥加密体制 CCA 安全性。

目前已完成与用户 A 相关的 send 询问的修改，同样地，与用户 B 相关的 send 询问的修改类似于此方式。

这里令事件 $\mathcal{E}$ 为敌手 $\mathcal{A}$ 提交一个密文，密文可以被解密得到真正的口令 pw_A。如果事件 $\mathcal{E}$ 不会发

生，则敌手的优势在安全参数 κ 上是可忽略的。现在分析事件 $\mathcal{E}$ 发生的概率，在游戏 G_{10} 中，所有谕示询问输出的密文都是对 $0 \notin \mathcal{D}$ 的加密结果，敌手通过谕示询问不能得到真正口令的任何有用信息。由于敌手 $\mathcal{A}$ 至多有 $Q(\kappa)$ 次在线攻击，事件 $\mathcal{E}$ 发生的概率至多为 $\frac{Q(\kappa)}{|\mathcal{D}|}$，通过计算可知，$\mathrm{adv}_{\mathcal{A},10}(k) \leqslant \frac{Q(\kappa)}{|\mathcal{D}|} + \mathrm{negl}(\kappa)$。综合引理 1~引理 10 可知，$\mathrm{adv}_{\mathcal{A},0}(\kappa) \leqslant \frac{Q(\kappa)}{|\mathcal{D}|} + \mathrm{negl}(\kappa)$，那么定理 1 结论成立。

4 性能分析

本节从安全性和效率两个方面，对本文协议和 Katz 等[11]提出的 PAKE 协议（简记 K-PAKE 协议）、Xu 等[15]提出的 PAKE 协议（简记 X-PAKE 协议）及 Zhang 等[16]提出的 PAKE 协议（简记 Z-PAKE 协议）进行比较，这些协议均基于格困难问题。4 种协议性能比较如表 2 所示，其中，$n = n_1 + n_2 + 1$。

在安全性方面，本文协议在方案中添加会话序列号，提供了更强的消息认证机制，由表 2 可以看出，与其他协议[11,15-16]相比，本文协议可以抵抗重放攻击，安全性能更高。

在效率方面，本文协议利用改进的基于格的 CCA 安全的公钥加密体制，减少了加密参数，降低了计算代价。由表 2 可以看出，与其他协议相比[11,15-16]，本文协议的服务器计算开销和用户计算开销都较低。此外，本文协议只需要两轮通信，通信开销主要由密文和投射密钥的大小来决定，而投射密钥只依赖于散列密钥，这使本文协议的通信效率提高。

K-PAKE 协议是基于 LWE 的 3PAKE 协议，需要 3 轮通信，通信代价主要取决于密文、投射密钥和消息认证码的大小，而密文大小要比本文协议大 $O(n)$ 个因素，投射密钥由密文和散列密钥决定，因此投射密钥大小比本文协议大。此外，K-PAKE 协议进行双向认证需要计算并传输消息认证码，而本文协议通过验证双方密文的有效性进行双向认证。根据分析和表 2 数据可得，K-PAKE 协议的通信开销比本文协议要大。

X-PAKE 协议提出基于格的 3PAKE 协议，通信轮数为 3 轮，消息传输量为 6 条，通信代价主要取决于多项式环和多个散列函数计算得出的值，由于协议需要传输的消息量较多，造成通信开销增大。根据分析和表 2 数据可得，X-PAKE 协议的通信开销比本文协议大。

Z-PAKE 协议是基于格的 2PAKE 协议，是针对两方设计的，不适用于大规模的通信系统，协议需要两轮通信，通信代价主要取决于密文和投射密钥的大小，本文协议和 Z-PAKE 协议相比，除了多一个用户同样的开销之外，并没有增加其他较大的开销。但是 Z-PAKE 协议按照传统的方式实现为 3PAKE 协议，至少需要 4 轮通信，即 8 条消息传输量，而本文三方协议只需 2 轮通信即 4 条传输量。根据分析和表 2 可得，本文协议的通信开销较低，还可以抵抗重放攻击。

以上分析结果表明，本文协议适用于大规模的通信系统，不仅具有抵抗重放攻击的安全性，还具有较低的通信和计算开销。因此，本文协议更具有可行性。

5 结束语

本文提出三方的口令认证密钥交换协议，协议中使用的密码机制是基于格上的 LWE 困难问题，在后量子时代具有重要意义。三方的 PAKE 协议是客户端–客户端–服务器的形式，大量用户只与服务器共享一个口令即可建立共享会话密钥，因此更符合用户端到端安全通信的需求。除此之外，本文协议可以有效抵抗攻击者重放之前的消息，提高了协议应用的安全性。在随机预言模型下，本文给出了严格的安全性证明。相比已有的同类协议，本文协

表 2 4 种协议性能比较

协议	类型	抵抗重放攻击	通信轮数	通信开销	服务器计算开销	用户计算开销
K-PAKE 协议	3-party	否	3	$2[(m+n+mn)\mathrm{lb}q+3n]$	$O(n\mathrm{lb}q)$	$O(n^2\mathrm{lb}q)$
X-PAKE 协议	3-party	否	3	$7n\mathrm{lb}q+9n+5$	$O(n\mathrm{lb}n\mathrm{lb}q)$	$O(n\mathrm{lb}n\mathrm{lb}q)$
Z-PAKE 协议	2-party	否	2	$(2m+2n_1)\mathrm{lb}q+n$	$O(n\mathrm{lb}n\mathrm{lb}q)$	$O(n\mathrm{lb}n\mathrm{lb}q)$
本文协议	3-party	是	2	$2[(2m+2n_1)\mathrm{lb}q+2n]$	$O(m\mathrm{lb}n)$	$O(m\mathrm{lb}n)$

议在通信效率和安全性上均有所提高。本文所设计的格上基于口令的认证密钥交换协议，口令以明文的形式存储在服务器上，一旦服务器信息泄露，攻击者获得口令后会伪装成合法用户与服务器通信，这将对用户和服务器的数据安全带来危害。因此，构造一个不让服务器直接存储明文口令的格上 3PAKE 协议是未来的研究方向。

参考文献：

[1] BELLOIN S M, MERRITT M. Encrypted key exchange: password-based protocols secure against dictionary attacks[C]//IEEE Symposium on Research in Security and Privacy. 1992: 72-84.

[2] KATZ J, OSTROVSKY R, YUNG M. Efficient password-authenticated key exchange using human-memorable passwords[M]. Advances in Cryptology-EUROCRYPT. 2001: 475-494.

[3] ZHAO J, GU D. Provably secure three-party password-based authenticated key exchange protocol[J]. Information Sciences, 2012, 184(1): 310-323.

[4] FARASH M S, ISLAM S H, OBAIDAT M S. A provably secure and efficient two-party password‐based explicit authenticated key exchange protocol resistance to password guessing attacks[J]. Concurrency & Computation Practice & Experience, 2015, 27(17): 4897-4913.

[5] ABLALLA M, BENHAMOUDA F, MACKENZIE P. Security of the J-PAKE password-authenticated key exchange protocol[C]//IEEE Symposium on Security and Privacy. 2015: 571-587.

[6] 魏福山, 马建峰, 李光松, 等. 标准模型下高效的三方口令认证密钥交换协议[J]. 软件学报, 2016, 27(9): 2389-2399.
WEI F S, MA J F, LI G S, et al. Efficient three-party password-based authenticated key exchange protocol in the standard model[J]. Journal of Software, 2016, 27(9): 2389-2399.

[7] KATZ J, VAIKUNTANATHAN V. Smooth projective hashing and password-based authenticated key exchange from lattices[M]. Advances in Cryptology-ASIACRYPT. 2009: 636-652.

[8] GENNARO R, LINDELL Y. A framework for password-based authenticated key exchange[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 2003: 524-543.

[9] DING Y, FAN L. Efficient password-based authenticated key exchange from lattices[C]//Seventh International Conference on Computational Intelligence and Security. 2012: 934-938.

[10] GROCE A, KATZ J. A new framework for efficient password-based authenticated key exchange[C]//Proceedings of the 17th ACM conference on Computer and communications security. 2010: 516-525.

[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] PEIKERT C. Lattice cryptography for the internet[M]. Post-Quantum Cryptography. 2014: 197-219.

[13] ZHANG J, ZHANG Z, DING J, et al. Authenticated key exchange from ideal lattices[M]. Advances in Cryptology - EUROCRYPT. 2015: 719-751.

[14] 赵秀凤, 高海英, 王爱兰. 基于 RLWE 的身份基认证密钥交换协议[J]. 计算机研究与发展, 2016, 53(11): 2482-2490.
ZHAO X F, GAO H Y, WANG A L. An identity-based authenticated key exchange protocol from RLWE[J]. Journal of Computer Research and Development, 2016, 53(11): 2482-2490.

[15] XU D Q, HE D B, CHOO K K R. Provably secure three-party password authenticated key exchange protocol based on ring learning with error[C]//IACR Cryptology ePrint Archive. 2017: 360.

[16] ZHANG J, YU Y. Two-round PAKE from approximate SPH and instantiations from lattices[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2017: 37-67.

[17] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//ACM Symposium on Theory of Computing. 2005: 84-93.

[18] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[M]. Advances in Cryptology-EUROCRYPT. 2000: 139-155.

[19] ABE M, CUI Y, IMAI H, et al. Efficient hybrid encryption from ID-based encryption[J]. Designs Codes & Cryptography, 2010, 54(3): 205-240.

[20] RAN C, HALEVI S, KATZ J. Chosen-ciphertext security from identity-based encryption[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 2004: 207-222.

[21] CRAMER R, SHOUP V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption[C]// International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology. 2002: 45-64.

[22] KATZ J, VAIKUNTANATHAN V. Round-optimal password-based authenticated key exchange[M]. Theory of Cryptography. 2011: 293-310.

[作者简介]

于金霞（1974–），女，河南博爱人，博士，河南理工大学教授，主要研究方向为人工智能、信息安全。

廉欢欢（1993–），女，河南沁阳人，河南理工大学硕士生，主要研究方向为信息安全、密码学。

汤永利（1972–），男，河南孟州人，博士，河南理工大学教授、硕士生导师，主要研究方向为信息安全、密码学。

史梦瑶（1998–），女，河南许昌人，河南理工大学硕士生，主要研究方向为信息安全、密码学。

赵宗渠（1974–），男，河南沁阳人，博士，河南理工大学讲师，主要研究方向为密码学、网络安全、恶意代码分析。