基于理想格的通用可组合两方口令认证密钥交换协议

舒 琴 王圣宝* 路凡义 韩立东 谭 肖
(杭州师范大学信息科学与工程学院 杭州 311121)

摘 要：大部分现有基于格的两方口令认证密钥交换协议(2PAKE)都是在基于不可区分的公共参考串模型或Bellare-Pointcheval-Rogaway(BBR)模型下被证明安全的。该文提出一个基于环上带误差学习问题的两方口令认证密钥交换协议，并在通用可组合框架下证明其安全性。与同类协议相比，新协议具有更高的安全性和更高的效率。

关键词：两方密钥交换协议；口令认证；环上带误差学习问题；通用可组合模型
中图分类号：TN918; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2021)06-1756-08
DOI: 10.11999/JEIT191029

Universally Composable Two-Party Password-Based Authenticated Key Exchange from Ideal Lattices

SHU Qin WANG Shengbao LU Fanyi HAN Lidong TAN Xiao
(*School of Information Science and Engineering*, *Hangzhou Normal University*, *Hangzhou* 311121, *China*)

Abstract: Most of the existing two-party password-based Authenticated Key Exchange (2PAKE) protocols from lattices are proven secure using the indistinguishable common reference string model or the Bellare-Pointcheval-Rogaway model. This paper proposes a two-party password-based authenticated key exchange protocol based on the Ring Learning With Errors (RLWE) problem and proves its security under the Universally Composable (UC) framework. Compared with similar protocols, the new protocol achieves a higher level of security and efficiency.

Key words: Two-Party Authenticated Key Exchange protocol (2PAKE); Password authentication; Ring Learning With Errors (RLWE); Universally Composable (UC) model

1 引言

两方口令认证密钥交换协议(Two-Party password-based Authenticated Key Exchange, 2PAKE)能够使得协议参与者使用低熵、易于记忆的口令(password)协商生成一个高熵的会话密钥。

目前，大多传统基于数论的底层困难问题都存在量子解决算法[1,2]。因此，随着量子计算机的发展，基于这些难题构造的密码协议或方案正面临所谓的量子威胁。同时，应对量子威胁的所谓“后量子密码”研究方兴未艾。其中，基于格(lattice)上难题(简称格基)的2PAKE协议的研究成为热点之一。2009年，Katz等人[3]构造了首个格基2PAKE协议。该协议的安全性在基于不可区分的公共参考串(Common Reference String，CRS)模型[4]下得到证明。随后，Ding等人[5]和Zhang等人[6]各自构造出新的格基2PAKE协议，同样在CRS模型下证明了安全性。此后，又有多个格基2PAKE协议陆续被提出[7–9]，它们使用的安全模型皆为BPR模型[10]。

CRS模型与BPR模型没有考虑到协议的可组合性以及口令的相关性。相较而言，通用可组合(Universally Composable，UC)模型[11]则很好地解决了这些问题。2017年，Gao等人[12]基于SRP协议[13]，提出了一个格基扩展版本协议，称为RLWE-SRP。另外，RLWE-SRP采用了由Ding等人[14]所提出的误差调和机制。但是，该机制效率较低，使得协议双方提取出的共同比特只是具有高熵，而并非均匀分布，需要一个随机提取器来获得均匀的值。相比而言，Peikert[15]于2014年提出的改进误差

收稿日期：2019-12-24；改回日期：2021-03-09；网络出版：2021-03-12
*通信作者： 王圣宝 shengbaowang@hznu.edu.cn
基金项目：国家重点研发计划项目(2017YFB0802000)，国家自然科学基金青年项目(61702152, 61702153)，浙江省教育厅科研项目(Y202044830)
Foundation Items: The National Key R&D Program of China (2017YFB0802000), The Youth Program of National Natural Science Foundation of China (61702152, 61702153), The Scientific Research Fund of Zhejiang Provincial Education Department (Y202044830)

调和机制能够使协议双方所提取的共同比特满足均匀分布。

采用Peikert式误差调和机制，本文提出一个更高效的具有通用可组合性的格基2PAKE协议，称为RLWE-CAPAKE，并在UC框架下证明其安全性。新协议的设计思想来源于Abdalla等人[16]于2008年提出的CAPAKE协议。新协议既保持了CAPAKE协议的优势，又能抵抗量子攻击。

2　预备知识

2.1　理想格

格是线性空间R_n上n个线性无关向量$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n$组成的点的集合，表示为$\boldsymbol{L}=\{a_1\cdot\boldsymbol{v_1}+a_2\cdot\boldsymbol{v}_2+\cdots+a_n\cdot\boldsymbol{v_n}|a_i$为整数$\}$，其中$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v_n}$称为格基。理想格[17]则是具有特殊环结构的格。理想$\mathcal{I}$是环$R=\mathbb{Z}[x]/f(x)$的一个商环，其中$f(x)$为首一整数多项式。n阶整数群Z^n上$\mathcal{I}$的集合便是理想格。相较于格，理想格可以使用一个向量表示一个n维格，大大降低了空间复杂度；理想格的特殊代数结构可以进行快速运算，大大降低了时间复杂度。最近，张洋等人[18]提出的理想格上格基的快速三角化算法有助于进一步降低运算的时间复杂度。

2.2　环上带误差学习问题

2010年，Lyubashevsky等人[17]提出了基于理想格的环上带误差学习(Ring Learning With Errors, RLWE)问题，并指出求解RLWE问题的难度可以量子规约到求解近似最短向量问题。被密码学界普遍认为能够抵抗量子攻击。

定义1　(RLWE分布)：设R为$\mathbb{Z}$上阶数为n的多项式环，$R_q=R/qR$为以正整数q为模的商环，χ_γ为R上以γ为标准差，0为分布中心，r为半径的高斯离散分布。设固定向量$\boldsymbol{s}$为秘密值，在$R_q\times R_q$上的RLWE分布A_{s,χ_γ}通过均匀随机地选择向量$\boldsymbol{a}\in R_q$, $\boldsymbol{e}\in\chi_\gamma$进行采样，并得到采样结果$(\boldsymbol{a},\boldsymbol{b}=\boldsymbol{s}\cdot\boldsymbol{a}+\boldsymbol{e}(\mathrm{mod}q))$。

定义2　(判定RLWE问题)：给定多项式个独立样本$(\boldsymbol{a_i},\boldsymbol{b_i})\in R_q\times R_q$，任意PPT算法$A$能够区分样本取自RLWE分布$A_{s,\chi_\gamma}$还是均匀随机地取自$R_q\times R_q$的优势可忽略。

2.3　Peikert式误差调和机制

RLWE问题固有的误差问题会导致通信双方无法得到完全相同的会话密钥。为解决这一问题，Ding等人[14]在2012年首次提出误差调和机制(称为Ding式误差调和机制)。2014年，Peikert[15]指出Ding式误差调和机制中协议双方提取出的共同比特只是具有高熵，而并非均匀分布，需要一个随机提取器来获得均匀的值，这会带来较大的效率损失。他提出一个改进的误差调和机制(Peikert式误差调和机制)，该机制中协议双方提取的共同比特均匀分布。Peikert式误差调和机制具体描述如下：

对于偶数模数$q\geq2$，定义$\mathbb{Z}_q=\left\{-\frac{q}{2},\cdots,0,\cdots,\frac{q}{2}-1\right\}$及3个区间：$I_0:=\left\{0,1,\cdots,\left\lfloor\frac{q}{4}\right\rceil-1\right\}$, $I_1:=\left\{-\left\lfloor\frac{q}{4}\right\rceil,\cdots,-1\right\}(\mathrm{mod}q)$，$E:=\left[-\frac{q}{8},\frac{q}{8}\right)\cap\mathbb{Z}$，其中$\left\lfloor\frac{q}{4}\right\rceil$和$\left\lfloor\frac{q}{4}\right\rfloor$为$\mathbb{Z}_q$上的两个陪集，$\left\lfloor\frac{q}{4}\right\rceil=\left\lfloor\frac{q}{4}+\frac{1}{2}\right\rfloor\in\mathbb{Z}$。对于$\boldsymbol{v}\in\mathbb{Z}_q$, $\boldsymbol{w}=\boldsymbol{v}+\boldsymbol{e}(\mathrm{mod}q)$，定义3个函数：

定义3　(交叉取整函数)$\langle\cdot\rangle_{q,2}:\mathbb{Z}_q\to\mathbb{Z}_2$　如$b=\langle\boldsymbol{v}\rangle_{q,2}:=\left\lfloor\frac{4}{q}\cdot\boldsymbol{v}\right\rceil(\mathrm{mod}2)$；

定义4　(模取整函数)$\lfloor\cdot\rceil_{q,2}:\mathbb{Z}_q\to\mathbb{Z}_2$　如$\lfloor\boldsymbol{v}\rceil_{q,2}:=\left\lfloor\frac{2}{q}\cdot\boldsymbol{v}\right\rceil$；

定义5　(调和函数)$\mathrm{rec}(\boldsymbol{w},b):\mathbb{Z}_q\times\mathbb{Z}_2\to\mathbb{Z}_2$　如$\mathrm{rec}(\boldsymbol{w},b):=\begin{cases}0,\boldsymbol{w}\in I_b+E(\mathrm{mod}q)\\1,\boldsymbol{w}\notin I_b+E(\mathrm{mod}q)\end{cases}$。其中，$\mathrm{rec}(\boldsymbol{w},\langle\boldsymbol{v}\rangle_{q,2})=\lfloor\boldsymbol{v}\rceil_{q,2}$。

对于奇数模数q，可定义随机翻倍函数$\mathrm{dbl}(\cdot):\mathbb{Z}_q\to\mathbb{Z}_{2q}$，如$\bar{\boldsymbol{v}}=\mathrm{dbl}(\boldsymbol{v})=2\boldsymbol{v}-\bar{\boldsymbol{e}}$，其中$\bar{\boldsymbol{e}}\in\mathbb{Z}$。$\bar{\boldsymbol{e}}$模2后均匀随机且与$v$独立，$2\boldsymbol{w}=\bar{\boldsymbol{v}}+(2\boldsymbol{e}+\bar{\boldsymbol{e}})(\mathrm{mod}2q)\in\mathbb{Z}_{2q}$。

2.4　安全模型

本文设计的协议的安全性在Canetti等人[11]提出的UC框架下，结合Canetti-Rabin[19]提出的具有联合状态的UC(Joint state UC，JUC)定理，使用UC混合模型证明。

定义6　(混合模型下的安全实现) 给定混合模型下的n方协议π以及理想功能$\mathcal{F}$，如果对于任意概率多项式时间(Probabilistic Polynomial Time, PPT)混合敌手$\mathcal{H}$都存在PPT理想攻击者$\mathcal{S}$，使得对于任意环境$\mathcal{Z}$，在和混合敌手$\mathcal{H}$及协议π交互后输出1的概率分布与在和理想攻击者$\mathcal{S}$及理想功能$\mathcal{F}$交互后输出1的概率分布是多项式不可区分的，则称协议π在混合模型下UC安全地实现了理想功能$\mathcal{F}$。

3　基于理想格的两方PAKE协议

3.1　协议描述

相较于Abdalla等人[16]提出的CAPAKE协议，本文提出的新协议具有如下两个优势：(1)基于RLWE难题、采用文献[15]改进的误差调和机制，被密码学界普遍认为可以抵抗量子攻击；(2)新协议中，服务器不直接存储用户的口令，而只存储服务器ID及用户口令的哈希值$\mathrm{HPW}=H_0(S||\mathrm{PW})$。实际应用中，“单口令多用途”现象比较普遍，即用

户往往针对许多不同的应用服务器使用相同的口令。该改进避免了当服务器沦陷后，敌手可直接获得用户口令，从而可向其他服务器冒充为用户的风险。

3.1.1 初始化阶段

用户加入系统时，需向服务器注册。用户U将其口令PW及服务器ID即S输入哈希函数$\mathrm{H}_0(\cdot)$计算得到HPW，同时从商群R_q中均匀随机选择公共参数$\boldsymbol{a}$，将用户ID即U, HPW及$\boldsymbol{a}$通过安全信道发送给服务器S。S收到U的注册信息后将$\langle U,\mathrm{HPW},\boldsymbol{a}\rangle$添加到存储在数据库中的列表$\mathcal{L}$上，本文设定外部敌手无法获得服务器内部信息。

3.1.2 相互认证及密钥交换阶段

用户和服务器每次会话会自动生成一个会话ID，会话ID为ssid的用户和服务器相互认证及密钥交换的过程如下，其中具体的计算如图1所示：

(1) $U\to S:\mathrm{M1}=\{U,X\}$：$U$输入$S,\mathrm{PW}$，再次计算HPW，均匀随机地从商群$R_q$中选择其私钥$s_x$、从高斯离散分布$\chi_\gamma$中选取误差$\boldsymbol{e}_{\boldsymbol{x}},\boldsymbol{e}_{\boldsymbol{x}}^{'}$，计算其公钥$\boldsymbol{X}=\boldsymbol{a}\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{x}}\in R_q$，最后将$U$和$\boldsymbol{X}$发送给$S$。

(2) $S\to U:\mathrm{M2}=\{S,Y^*\}$：收到M1后，$S$首先检测$\boldsymbol{X}$是否在商群$R_q$内，若不在，则退出该次会话；若在，则均匀随机地从$R_q$中选择其私钥$s_y$、从$\chi_\gamma$中选取误差$\boldsymbol{e}_{\boldsymbol{y}},\boldsymbol{e}_{\boldsymbol{y}}^{'}$，计算其公钥$\boldsymbol{Y}=\boldsymbol{a}\cdot\boldsymbol{s}_{\boldsymbol{y}}+\boldsymbol{e}_{\boldsymbol{y}}\in R_q$。随后利用$\boldsymbol{X}$生成带误差的中间秘密值$\boldsymbol{v}=\boldsymbol{X}\cdot\boldsymbol{s}_{\boldsymbol{y}}+\boldsymbol{e}_{\boldsymbol{y}}^{'}\in R_q$，对$\boldsymbol{v}$使用随机翻倍函数$\mathrm{dbl}(\cdot)$得到$\bar{\boldsymbol{v}}$，对$\bar{\boldsymbol{v}}$使用交叉取整函数$\langle\cdot\rangle_{2q,2}$得到$\sigma$，对$\bar{\boldsymbol{v}}$使用模取整函数$[\cdot]_{q,2}$得到不带误差的中间秘密值$K_s$。$S$使用对称密钥(ssid||HPW)加密$\boldsymbol{Y}$以及$\sigma$得到$Y^*$，最后将$S$和$Y^*$发送给$U$。

(3) $S\to U:\mathrm{M3}=\{\mathrm{Auth}\}$：收到M2后，$U$首先用(ssid||HPW)解密$Y^*$得到$Y||\sigma$，再利用$\boldsymbol{Y}$生成带误差的中间秘密值$\boldsymbol{w}=\boldsymbol{Y}\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{x}}^{'}\in R_q$，随后结合$\sigma$对$\boldsymbol{w}$使用调和函数$\mathrm{rec}(2\boldsymbol{w},\sigma)$得到不带误差的中间秘密值$K_u$。之后，$U$使用哈希函数$\mathrm{H}_1(\cdot)$、$\mathrm{H}_2(\cdot)$分别计算认证因子$\mathrm{Auth}=\mathrm{H}_1(\mathrm{ssid}\parallel U\parallel S\parallel\boldsymbol{X}\parallel\boldsymbol{Y}\parallel K_u)$、会话密钥$\mathrm{SK}_u=\mathrm{H}_2(\mathrm{ssid}\parallel U\parallel S\parallel\boldsymbol{X}\parallel\boldsymbol{Y}\parallel K_u)$，最后将Auth发送给$S$。

(4) $\mathrm{SK}_s=\mathrm{H}_2(\mathrm{ssid}\parallel U\parallel S\parallel\boldsymbol{X}\parallel\boldsymbol{Y}\parallel K_s)=\mathrm{SK}_u$：收到Auth后，$S$使用$\mathrm{H}_1(\cdot)$计算得到$\mathrm{Auth}^*=\mathrm{H}_1(\mathrm{ssid}\parallel U\parallel S\parallel\boldsymbol{X}\parallel\boldsymbol{Y}\parallel K_s)$并与Auth比较。若相等，$S$计算会话密钥$\mathrm{SK}_s=\mathrm{H}_2(\mathrm{ssid}\parallel U\parallel S\parallel\boldsymbol{X}\parallel\boldsymbol{Y}\parallel K_s)$；否则，$S$发出错误信息。

3.2 方案的正确性

若U和S诚实地运行协议，他们将以显著的概率得到$\mathrm{SK}_s=\mathrm{SK}_u$。协议中：

$$\begin{aligned}\boldsymbol{v}&=\boldsymbol{X}\cdot\boldsymbol{s}_{\boldsymbol{y}}+\boldsymbol{e}_{\boldsymbol{y}}^{'}=(\boldsymbol{a}\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{x}})\cdot\boldsymbol{s}_{\boldsymbol{y}}+\boldsymbol{e}_{\boldsymbol{y}}^{'}\\&=\boldsymbol{a}\cdot\boldsymbol{s}_{\boldsymbol{x}}\cdot\boldsymbol{s}_{\boldsymbol{y}}+\boldsymbol{e}_{\boldsymbol{x}}\cdot\boldsymbol{s}_{\boldsymbol{y}}+\boldsymbol{e}_{\boldsymbol{y}}^{'},\end{aligned}$$

$$\begin{aligned}\boldsymbol{w}&=\boldsymbol{Y}\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{x}}^{'}=(\boldsymbol{a}\cdot\boldsymbol{s}_{\boldsymbol{y}}+\boldsymbol{e}_{\boldsymbol{y}})\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{x}}^{'}\\&=\boldsymbol{a}\cdot\boldsymbol{s}_{\boldsymbol{y}}\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{y}}\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{x}}^{'}\\&=\boldsymbol{v}+\boldsymbol{e}_{\boldsymbol{y}}\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{x}}^{'}-\boldsymbol{e}_{\boldsymbol{x}}\cdot\boldsymbol{s}_{\boldsymbol{y}}-\boldsymbol{e}_{\boldsymbol{y}}^{'}\end{aligned}$$

令$\boldsymbol{e}^*=\boldsymbol{e}_{\boldsymbol{y}}\cdot\boldsymbol{s}_{\boldsymbol{x}}+\boldsymbol{e}_{\boldsymbol{x}}^{'}-\boldsymbol{e}_{\boldsymbol{x}}\cdot\boldsymbol{s}_{\boldsymbol{y}}-\boldsymbol{e}_{\boldsymbol{y}}^{'}\in R_q$，则$\boldsymbol{w}=\boldsymbol{v}+\boldsymbol{e}^*$，令$\bar{\boldsymbol{v}}=2\boldsymbol{v}-\bar{\boldsymbol{e}}=2(\boldsymbol{w}-\boldsymbol{e}^*)-\bar{\boldsymbol{e}}=2\boldsymbol{w}-(2\boldsymbol{e}^*+\bar{\boldsymbol{e}})\in\mathbb{Z}_{2q}$。由文献[15]的等式(2.1)、事实2.1、事实2.4可知，$2\boldsymbol{e}^*+\bar{\boldsymbol{e}}$的解码基的所有系数不在区间$[-q/4,q/4)$内的概率可忽略。根据文献[15]的声明3.2：对于偶数q，存在$\boldsymbol{v}\in\mathbb{Z}_q$, $\boldsymbol{e}\in E$满足$\boldsymbol{w}=\boldsymbol{v}+\boldsymbol{e}$，则$\mathrm{rec}(\boldsymbol{w},\langle\boldsymbol{v}\rangle_{q,2})=\lfloor\boldsymbol{v}\rceil_{q,2}$。因此，$U$和$S$诚实地运行协议，得到$\mathrm{SK}_s\neq\mathrm{SK}_u$的概率可忽略。

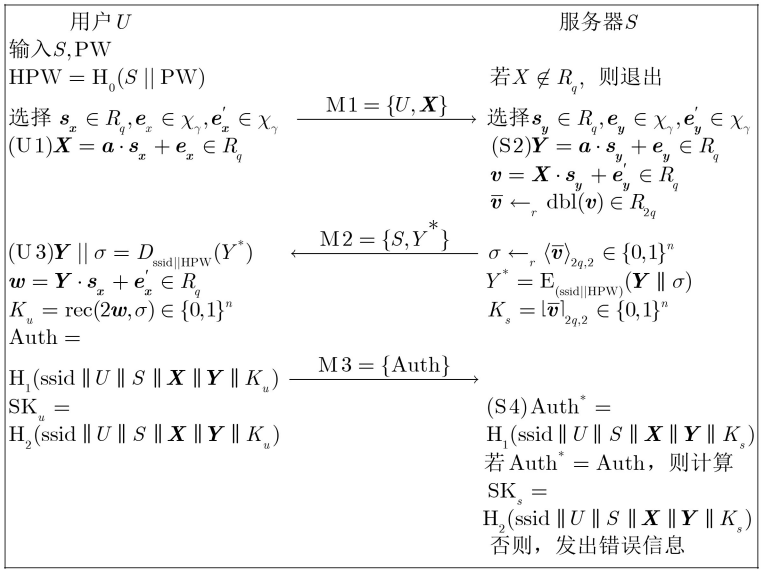

图 1 RLWE-CAPAKE的相互认证及密钥交换过程

4　安全性证明

定理1：在考虑适应性敌手的条件下，本文协议在$(\mathcal{F}_{\mathrm{RO}}, \mathcal{F}_{\mathrm{IC}})$混合模型中能够UC安全地实现理想功能$\mathcal{F}_{\mathrm{pwKE}}^{\mathrm{CA}}$的多会话扩展$\hat{\mathcal{F}}_{\mathrm{pwKE}}^{\mathrm{CA}}$。

根据定义6可知，证明定理1即可证明协议RLWE-CAPAKE在混合模型下UC安全地实现了理想功能$\hat{\mathcal{F}}_{\mathrm{pwKE}}^{\mathrm{CA}}$，即具有UC安全性。本节定义了一个序列游戏来证明定理1，这个序列游戏中理想攻击者逐步为挑战者模拟出协议中参与者的所有交互和输出。如果模拟出的信息和真实协议不可区分，那么就将真实环境下的协议安全问题规约到了理想模型中的协议安全问题。证明中使用了3个理想功能：Hofheinz等人[20]提出的随机预言功能$\mathcal{F}_{\mathrm{RO}}$, Liskov等人[21]提出的理想密码功能$\mathcal{F}_{\mathrm{IC}}$以及基于口令的认证密钥交换理想功能$\mathcal{F}_{\mathrm{pwKE}}^{\mathrm{CA}}$[16]。为了节省篇幅，上述3个理想功能的具体描述省略。

表1给出了利用这些游戏证明不可区分性的简要过程，$\mathcal{A}$为与协议RLWE-CAPAKE实体交互的敌手，$\mathcal{S}$为与理想功能$\hat{\mathcal{F}}_{\mathrm{pwKE}}^{\mathrm{CA}}$交互的理想攻击者。$\mathcal{S}$利用一个模拟的挑战者$\mathcal{A}$去攻击协议RLWE-CAPKE，试图获得攻击理想功能$\hat{\mathcal{F}}_{\mathrm{pwKE}}^{\mathrm{CA}}$的优势。$\mathcal{S}$为$\mathcal{A}$模拟出一系列预言机，$\mathcal{S}$把$\mathcal{Z}$的输入传递给$\mathcal{A}$，把$\mathcal{A}$的输出作为$\mathcal{S}$的输出使$\mathcal{Z}$可以读取。设$\mathcal{H}$为$(\mathcal{F}_{\mathrm{RO}}, \mathcal{F}_{\mathrm{IC}})$混合模型下敌手，与RLWE-CAPAKE实体交互时即为$\mathcal{A}$，与理想功能$\hat{\mathcal{F}}_{\mathrm{pwKE}}^{\mathrm{CA}}$交互时即为$\mathcal{S}$。这个序列游戏中游戏G2是考虑$\mathcal{A}$未执行查询，直接猜测出$K_u$意外获胜的情况。游戏G3和G5分别考虑了在第S4步之前未被攻陷和客户端已经被攻陷这两种情况。混合模型下，攻击者$\mathcal{H}$和协议的用户实例通过下述查询进行交互：

(1)TestPwd查询：参与者完全被模拟时，验证某一方的口令是否为想要的那个口令；

(2)NewKey查询：参与者完全被模拟且口令未泄露时，验证两方是否拥有相同的口令；

(3)GoodPwd查询：参与者未完全被模拟时，验证某一方的口令是否为想要的那个口令；

(4)SamePwd查询：参与者未完全被模拟且口令未泄露时，验证两方是否拥有相同的口令。

具体证明过程如下：

游戏 G0：该游戏是环境$\mathcal{Z}$与现实世界的敌手$\mathcal{A}$及RLWE-CAPAKE协议的实例在随机预言模型以及理想密码模型下进行交互。

游戏 G1：理想攻击者$\mathcal{S}$模拟随机预言机和加解密预言机。

(1)在随机预言模型下，$\mathcal{S}$维持一个长度为q_H的列表$\Lambda_{\mathcal{H}}$，用于提供随机预言机$\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$的查询应答。对于一个Hash查询$H_n(q)(n=0$或1或2)，如果在$\Lambda_{\mathcal{H}}$中存在(n,q,r)记录，则返回r；否则，随机选取一个$r\in\{0,1\}^{l_{\mathcal{H}_n}}$，如果$\Lambda_{\mathcal{H}}$已经存在$(n,*,r)$记录则中止查询，否则在$\Lambda_{\mathcal{H}}$中添加$(n,q,r)$记录并返回$r$。

(2)在理想密码模型下，$\mathcal{S}$维持一个长度为$q_{\mathcal{E}}+q_{\mathcal{D}}$的列表$\Lambda_{\mathrm{ED}}=\{(\mathrm{ssid},X,\mathrm{HPW},Y||\sigma,\boldsymbol{s_a},\boldsymbol{e_a},\mathcal{E},Y^*)\}\cup\{(\mathrm{ssid},X,\mathrm{HPW},Y||\sigma,\boldsymbol{s_a},\boldsymbol{e_a},\mathcal{D},Y^*)\}$来提供具有如下属性的加解密预言机查询应答：(a) 对同一口令的同一问题的查询，回答一致；(b) 任一口令的模拟方案加解密是可置换的；(c) 不同口令对应的密文不同。其中$\boldsymbol{s_a},\boldsymbol{e_a}$用于在解密查询时构造$Y||\sigma$。对于一个加密查询$\mathcal{E}_{\mathrm{ssid}||\mathrm{HPW}}(Y||\sigma)$，如果$\Lambda_{\mathrm{ED}}$中存在$(\mathrm{ssid},X,\mathrm{HPW},Y||\sigma,*,*,*,Y^*)$记录则返回$Y^*$；否则，随机选取$Y^*\in G^*=G\{1\}$，如果$\Lambda_{\mathcal{ED}}$中存在$(*,*,*,*,*,*,*,Y^*)$记录则中止查询，否则在$\Lambda_{\mathrm{ED}}$中添加$(\mathrm{ssid},X,\mathrm{HPW},\perp,Y||\sigma,\perp,\perp,\mathcal{E},Y^*)$并返回$Y^*$，其中$\perp$代表此处无需用到该值。对于一个解密查询$\mathcal{D}_{\mathrm{ssid}||\mathrm{HPW}}(Y^*)$，如果在$\Lambda_{\mathrm{ED}}$中存在$(*,*,\mathrm{HPW},Y||\sigma,*,*,*,Y^*)$记录就返回$Y||\sigma$；否则，随机选择$s_s\in R_q$，$\boldsymbol{e_s}\in\chi_\gamma$，$\boldsymbol{e_s'}\in\chi_\gamma$，计算

表 1　UC框架不可区分性证明概览

游戏	模型	游戏					模拟器	挑战者
		U1	U2	U3	U4	哈希与加解密		
G0	现实	真实	真实	真实	真实	真实	协议	$\mathcal{A}$
G1	混合	真实	真实	真实	真实	模拟	$\mathcal{H}$	$\mathcal{A}$
G2	混合	真实	真实	真实	真实	模拟	$\mathcal{H}$	$\mathcal{A}$
G3	混合	真实	真实	真实	模拟	模拟	$\mathcal{H}$	$\mathcal{A}$
G4	混合	模拟	真实	模拟	真实	模拟	$\mathcal{H}$	$\mathcal{A}$
G5	混合	真实	真实	真实	模拟	模拟	$\mathcal{H}$	$\mathcal{A}$
G6	混合	真实	模拟	真实	模拟	模拟	$\mathcal{H}$	$\mathcal{A}$
G7	理想	模拟	模拟	模拟	模拟	模拟	$\mathcal{S}$	$\mathcal{A}$

$\boldsymbol{Y'}=a\cdot\boldsymbol{s_s}+\boldsymbol{e_s}\in R_q$ ， $\boldsymbol{v'}=X\cdot\boldsymbol{s_s}+\boldsymbol{e_s}^{'}\in R_q$ ，$\bar{\boldsymbol{v}}'\leftarrow_r\mathrm{dbl}(\boldsymbol{v'})\in R_{2q}$ 及$\sigma'\leftarrow_r\langle\bar{\boldsymbol{v}}'\rangle_{2q,2}\in\{0,1\}^n$ ，如果Λ_{ED}中存在$(*,*,*,Y||\sigma,*,*,*,*)$记录则中止查询，否则在$\Lambda_{\mathrm{ED}}$中添加$(\mathrm{ssid},X,\mathrm{HPW},Y'||\sigma',\boldsymbol{s_s},\boldsymbol{e_s},\mathcal{D},Y'^*)$并返回$Y||\sigma$。上面出现的两种终止查询情况是为了满足不同的口令对应不同的密文这一属性。证毕

引理 1 游戏G0和游戏G1对于任意环境$\mathcal{Z}$都是计算不可区分的。

证明：根据哈希函数的抗碰撞性，对于$r\neq r'$，$\mathcal{A}$得到$H_n(r)=H_n(r')(n=0$或1或2)的概率是可忽略的。根据RLWE判定问题，$\mathcal{A}$成功区分Y'是取自RLWE分布A_{s,χ_γ}还是$R_q\times R_q$的概率可忽略。对于$Y\neq Y'$ ，$\sigma\neq\sigma'$ ，$Y^*\neq Y'^*$ ，$\mathcal{E}_{\mathrm{ssid}||\mathrm{HPW}}(Y'||\sigma')$ 和$\mathcal{E}_{\mathrm{ssid}||\mathrm{HPW}}(Y||\sigma)$得到相同的密文$Y^*$的概率及$\mathcal{D}_{\mathrm{ssid}||\mathrm{HPW}}(Y'^*)$和$\mathcal{D}_{\mathrm{ssid}||\mathrm{HPW}}(Y^*)$得到相同的$Y||\sigma$的概率也是可忽略的。因此$\mathcal{A}$无法在PPT内区分游戏G0和游戏G1。 证毕

游戏 G2：此游戏与游戏G1基本相同，不同之处在于如果现实世界敌手$\mathcal{A}$在未执行任何查询的情况下成功猜测出K_u，则理想攻击者S中止模拟随机预言机和加解密预言机。

引理 2 游戏 G1和游戏G2对于任意环境$\mathcal{Z}$都是计算不可区分的。

证明：现实世界敌手$\mathcal{A}$在未执行任何查询的情况下成功猜测出K_u发生的概率是可忽略的，故$\mathcal{A}$无法在PPT内区分游戏G1和游戏G2。 证毕

游戏 G3：假定$\mathcal{S}$有能力掌控协议前3轮的双方参与者，可知道两参与者的口令，而敌手可通过完全获得参与者的内部存储器来攻陷参与者。如果在第S4步之前没有发生攻陷，$\mathcal{S}$模拟两方参与者模拟协议的执行。如果在第S4步最开始，两方参与者仍然都没有被攻陷，且所有的消息都是预言机产生的，则$\mathcal{S}$执行SamePwd查询，验证两方口令是否相同。如果两方口令相同，$\mathcal{S}$在密钥空间中随机选择一个密钥K并发送给两方参与者；否则，$\mathcal{S}$在密钥空间中随机选择一个密钥单独发给客户端，服务器则只收到错误信息。如果在第S4步之前某一方参与者已经被攻陷，$\mathcal{S}$将不执行任何操作。

引理 3 游戏G2和游戏G3对于任意环境$\mathcal{Z}$都是计算不可区分的。

证明：当两方参与者的口令相同时，此游戏与游戏G2不可区分；当两方参与者的口令不同时，除了碰撞外，此游戏中协议的第S4步的一次执行与现实世界模型中协议的第S4步的一次执行不可区分。由哈希函数的抗碰撞性可知，发生碰撞的概率可忽略，故$\mathcal{A}$无法在PPT内区分游戏G2和游戏G3。 证毕

游戏 G4：$\mathcal{S}$在不获得客户端口令的情况下，从协议的最开始模拟未被攻陷的客户端：在第U1步，$\mathcal{S}$模拟客户端选择随机数$\boldsymbol{s_x}\in R_q,\boldsymbol{e_x}\in\chi_\gamma$并计算相应的$X$发送给服务器；在第U3步，若$\mathcal{S}$模拟的客户端仍然未被攻陷，则它不能发起对$Y^*$的解密查询。随后，如果客户端收到的消息都是预言机生成的，$\mathcal{S}$通过$\mathcal{H}'_1$查询获取$\mathrm{Auth}=H'_1(\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y^*)$，其中$\mathcal{H}'_1$为$\mathcal{S}$的私有随机预言机。如果客户端收到的信息不是预言机生成的，分两种情况进行操作：(1)若服务器被$\mathcal{A}$攻陷，则$\mathcal{S}$可以得到服务器的口令(此时的模拟器为$\mathcal{H}$，它同时具有$\mathcal{A}$和$\mathcal{S}$两种身份)，或者如果Y^*已在加密查询下被$\mathcal{A}$获取，$\mathcal{S}$可利用加解密查询列表$\Lambda_{\mathcal{ED}}$恢复出服务器使用的口令。随后，在接收Y^*时，$\mathcal{S}$进行GoodPwd查询，若口令正确，$\mathcal{S}$通过$\mathcal{H}_1$查询获取$\mathrm{Auth}=H_1(\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_u)$；否则，通过$\mathcal{H}'_1$查询获取$\mathrm{Auth}=H'_1(\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y^*)$。(2)如果$Y^*$未在加密查询下被$\mathcal{A}$获取过，$\mathcal{S}$模拟客户端通过$\mathcal{H}'_1$查询获取$\mathrm{Auth}=H'_1(\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y^*)$。但是若$\mathcal{A}$询问了以$\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_u$或$\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_s$为输入的$\mathcal{H}_0$或$\mathcal{H}_1$查询会使得游戏中止。

在第U3步，在$\mathcal{S}$模拟的客户端仍未被$\mathcal{A}$攻陷时，如果由$\mathcal{H}'_1$查询获取Auth且没有攻陷发生在任何一方，则$\mathcal{S}$通过$\mathcal{H}'_0$查询获取SK_u。如果由$\mathcal{H}_1$查询获取Auth，或由$\mathcal{H}'_1$查询获取Auth但之后发生了攻陷，则$\mathcal{S}$通过$\mathcal{H}_0$查询获取SK_u。如果在此步$\mathcal{S}$模拟的客户端被攻陷，$\mathcal{S}$可以得到内部状态$\boldsymbol{s_x}$, $\boldsymbol{e_x}$及HPW，从而可以计算出$Y||\sigma$，接下来，$\mathcal{S}$重新执行预言机获取$\mathrm{Auth}=H_1(\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_u)$和$\mathrm{SK}_u=H_2(\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_u)$。

在第S4步，若服务器被攻陷，且$\mathcal{S}$进行GoodPwd查询后口令正确，$\mathcal{S}$重新执行预言机获取$\mathrm{Auth}=H_1(\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_s)$ 和$\mathrm{SK}_s=H_2(\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_s)$。当且仅当$\mathcal{A}$在攻陷之前询问了以$\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_u$或$\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_s$为输入的$\mathcal{H}_0$或$\mathcal{H}_1$查询，$\mathcal{A}$能够对游戏G4与游戏G3进行区分。

引理 4 游戏G3与游戏G4对于任意环境$\mathcal{Z}$都是计算不可区分的。

证明：$\mathcal{A}$未在加密查询下并且获取过Y^*的情况下知道相应的s_y和$\boldsymbol{e_y}$的概率可忽略，$\mathcal{A}$在第S4步攻陷服务器之前询问了以$\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_u$或$\mathrm{ssid}\,\|\,U\,\|\,S\,\|\,X\,\|\,Y\,\|\,K_s$为输入的$\mathcal{H}_0$或$\mathcal{H}_1$查询的概率也可忽略，故$\mathcal{A}$无法在PPT内区分游戏G3与游戏G4。 证毕

游戏 G5：在该游戏中，$\mathcal{S}$模拟在第S4步中没被攻陷的服务器。分如下两种情况：

(1)如果在第S4步之前没有攻陷发生，且所有的信息都是预言机产生的，则$\mathcal{S}$之后的操作与G3中的操作相同。

(2)如果在第S4步之前客户端已经被$\mathcal{A}$攻陷，或者某一信息不是预言机产生的(比如$\mathcal{A}$已经通过解密Y^*获得Y)，$\mathcal{S}$恢复出服务器已使用过的口令，并验证客户端发送的Auth是否正确。如果Auth正确，$\mathcal{S}$询问关于服务器的GoodPwd查询，若口令正确，服务器会获得和客户端同样的密钥，否则，会获得一条错误信息。如果Auth不正确，服务器会获得一条错误信息。

若服务器在第S4步被$\mathcal{A}$攻陷，$\mathcal{S}$恢复出服务器的口令，查询列表$\Lambda_{\mathcal{ED}}$找到该口令相应的信息发送给$\mathcal{A}$。当$\mathcal{A}$意外猜测到了Y时，$\mathcal{A}$可在客户端发送完Auth之后模仿客户端，此时游戏中止。

引理 5　游戏G4和游戏G5对于任意环境$\mathcal{Z}$都是计算不可区分的。

证明：$\mathcal{A}$意外猜测到Y的概率可忽略，故$\mathcal{A}$无法在PPT内区分游戏G4和游戏G5。　　证毕

游戏 G6：$\mathcal{S}$从协议开始模拟未被攻陷的服务器。在第S2步，$\mathcal{S}$随机选择一个未执行过加密查询的Y^*发送给客户端。如果在之后服务器被$\mathcal{A}$攻陷，$\mathcal{S}$利用列表$\Lambda_{\mathcal{ED}}$获得相应的$\boldsymbol{s_y}$, $\boldsymbol{e_y}$及$Y||\sigma$并发送给$\mathcal{A}$。如果一直到游戏的最后两参与者仍未被攻陷，与游戏G3不同，他们会得到一个共享的基于口令的会话密钥。参与者之一被攻陷的情况与游戏G4和游戏G5中的描述相同，且游戏的执行不依赖Y^*的值。

引理 6　游戏G5和游戏G6对于任意环境$\mathcal{Z}$都是计算不可区分的。

证明：游戏G3, G4和G5中可能中止情况发生的概率都是可忽略的，故$\mathcal{A}$无法在PPT内区分游戏G5和游戏G6。　　证毕

游戏 G7：$\mathcal{S}$从协议开始模拟未被攻陷的客户端和服务器，其中将游戏G6中使用的混合模型下的GoodPwd查询和SamePwd查询分别替换为理想模型下的TestPwd查询和NewKey查询，若游戏中止或终止都会告知$\mathcal{A}$。

引理 7　游戏G6和游戏G7对于任意环境$\mathcal{Z}$都是计算不可区分的。

证明：如果两方参与者拥有相同的ssid，相对的角色(客户端和服务器)并且有相同的(X, Y^*)对，则称两方参与者拥有匹配会话。如果客户端和服务器拥有匹配会话，则他们会得到相同的会话密钥：如果两方都未被攻陷，则他们的会话密钥与实验G3中相同；如果客户端未被攻陷，服务器被攻陷，他们的会话密钥与游戏G4中相同；如果客户端被攻陷，则他们的会话密钥与游戏G5相同。如果客户端和服务器未拥有匹配会话，他们的(X, Y^*)对或Auth必有不同，两方拥有相同的(X, Y^*)对的概率以q_ε^2/q为上界，这个概率可忽略，其中q_ε为向预言机加密查询的次数。故$\mathcal{A}$无法在PPT内区分游戏G6和游戏G7。　　证毕

由于游戏G7与理想功能$\hat{\mathcal{F}}_{\text{pwKE}}^{\text{CA}}$中的客户端和服务器拥有完全一致的行为，因此游戏G7与理想功能$\hat{\mathcal{F}}_{\text{pwKE}}^{\text{CA}}$对于任意环境$\mathcal{Z}$都是概率多项式不可区分的。进一步综合引理1至引理7可知，对于任意环境$\mathcal{Z}$，在和混合敌手$\mathcal{H}$及新提出协议的实例交互后输出1的概率分布与在和理想攻击者$\mathcal{S}$及理想功能$\hat{\mathcal{F}}_{\text{pwKE}}^{\text{CA}}$交互后输出1的概率分布是计算不可区分的。定理1证毕。

5　效率分析

本节从安全性和计算与通信效率两方面对本文所提出的新协议与Ding等人[7]提出的PAK理想格扩展协议(RLWE-PAK)及Gao等人[12]提出的SRP理想格扩展协议(RLWE-SRP)进行比较。Ding式REC代表Ding式误差调和机制，Peikert式REC代表Peikert式误差调和机制。

如表2所示，这3个协议均基于RLWE问题，且通信开销也基本相同。RLWE-PAK与本文新协议的环运算次数基本相同，但是它的安全性证明基于BPR模型。如前所述，该模型相对UC模型而言不够完善。进一步，相比RLWE-SRP协议，虽然两者都在UC框架下被证明安全性，但是，本文新协议具有更少的环运算次数，即具有更高的计算效率。因此，综合而言，新协议具有更高的安全性和更好的效率。

表 2　理想格上口令基2PAKE协议的性能比较

协议	通信开销	环运算次数	安全模型	难题假设	误差调和
RLWE-PAK	$2n\log_2 q+n$	4	BPR模型	RLWE	Ding式REC
RLWE-SRP	$2n\log_2 q+n$	5	UC模型	RLWE	Ding式REC
本文协议	$2n\log_2 q+n$	4	UC模型	RLWE	Peikert式REC

6 结束语

本文提出了一个基于RLWE问题的2PAKE协议，并在UC框架下详细证明了其安全性。新协议采用了更加高效的误差调和机制。通过与现有相关协议进行比较，结果表明了新协议具有更高的安全性和计算效率。

参 考 文 献

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. *SIAM Review*, 1999, 41(2): 303–332. doi: 10.1137/S0036144598347011.

[2] HALLGREN S. Fast quantum algorithms for computing the unit group and class group of a number field[C]. The Thirty-Seventh Annual ACM Symposium on Theory of Computing, Baltimore, USA, 2005: 468–474. doi: 10.1145/1060590.1060660.

[3] KATZ J and VAIKUNTANATHAN V. Smooth projective hashing and password-based authenticated key exchange from lattices[C]. The 15th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, Tokyo, Japan, 2009: 636–652. doi: 10.1007/978-3-642-10366-7_37.

[4] JIANG Shaoquan and GONG Guang. Password based key exchange with mutual authentication[C]. The 11th International Workshop on Selected Areas in Cryptography, Waterloo, Canada, 2004: 267–279. doi: 10.1007/978-3-540-30564-4_19.

[5] DING Yi and FAN Lei. Efficient password-based authenticated key exchange from lattices[C]. The 2011 Seventh International Conference on Computational Intelligence and Security, Sanya, China, 2011: 934–938. doi: 10.1109/CIS.2011.210.

[6] ZHANG Jiang and YU Yu. Two-round PAKE from approximate SPH and instantiations from lattices[C]. The 23rd International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 2017: 37–67. doi: 10.1007/978-3-319-70700-6_2.

[7] DING Jintai, ALSAYIGH S, LANCRENON J, *et al*. Provably secure password authenticated key exchange based on RLWE for the post-quantum world[C]. The Cryptographers' Track at the RSA Conference, San Francisco, USA, 2017: 183–204. doi: 10.1007/978-3-319-52153-4_11.

[8] LI Zengpeng and WANG Ding. Two-round PAKE protocol over lattices without NIZK[C]. The 14th International Conference on Information Security and Cryptology, Fuzhou, China, 2019: 138–159. doi: 10.1007/978-3-030-14234-6_8.

[9] KARBASI A H, ATANI R E, and ATANI S E. A new ring-based SPHF and PAKE protocol on ideal lattices[J]. *ISeCure*, 2019, 11(1): 1–11. doi: 10.22042/ISECURE.2018.109810.398.

[10] BELLARE M, POINTCHEVAL D, and ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]. International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, 2000: 139–155. doi: 10.1007/3-540-45539-6_11.

[11] CANETTI R, HALEVI S, KATZ J, *et al*. Universally composable password-based key exchange[C]. The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 404–421. doi: 10.1007/11426639_24.

[12] GAO Xinwei, DING Jintai, LIU Jiqiang, *et al*. Post-quantum secure remote password protocol from RLWE problem[C]. The 13th International Conference on Information Security and Cryptology, Xi'an, China, 2018: 99–116. doi: 10.1007/978-3-319-75160-3_8.

[13] WU T. The secure remote password protocol[C]. The 1998 Internet Society Network and Distributed System Security Symposium, San Diego, USA, 1998: 97–111.

[14] DING Jintai, XIE Xiang, and LIN Xiaodong. A simple provably secure key exchange scheme based on the learning with errors problem[R]. Cryptology ePrint Archive: Report 2012/688, 2012.

[15] PEIKERT C. Lattice cryptography for the internet[C]. The 6th International Workshop on Post-Quantum Cryptography, Waterloo, Canada, 2014: 197–219. doi: 10.1007/978-3-319-11659-4_12.

[16] ABDALLA M, CATALANO D, CHEVALIER C, *et al*. Efficient two-party password-based key exchange protocols in the UC framework[C]. The Cryptographers' Track at the RSA Conference, San Francisco, USA, 2008: 335–351. doi: 10.1007/978-3-540-79263-5_22.

[17] LYUBASHEVSKY V, PEIKERT C, and REGEV O. On ideal lattices and learning with errors over rings[C]. The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, French, 2010: 1–23. doi: 10.1007/978-3-642-13190-5_1.

[18] 张洋, 刘仁章, 林东岱. 理想格上格基的快速三角化算法研究[J]. 电子与信息学报, 2020, 42(1): 98–104. doi: 10.11999/JEIT190725.

ZHANG Yang, LIU Renzhang, and LIN Dongdai. Fast triangularization of ideal latttice basis[J]. *Journal of Electronics & Information Technology*, 2020, 42(1): 98–104. doi: 10.11999/JEIT190725.

[19] CANETTI R and RABIN T. Universal composition with

joint state[C]. The 23rd Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2003: 265–281. doi: 10.1007/978-3-540-45146-4_16.

[20] HOFHEINZ D and MÜLLER-QUADE J. Universally composable commitments using random oracles[C]. First Theory of Cryptography Conference on Theory of Cryptography, Cambridge, USA, 2004: 58–76. doi: 10.1007/978-3-540-24638-1_4.

[21] LISKOV M, RIVEST R L, and WAGNER D. Tweakable block ciphers[C]. The 22nd Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2002: 31–46. doi: 10.1007/3-540-45708-9_3.

舒　琴：女，1995年生，硕士，研究方向为基于格的认证协议.

王圣宝：男，1978年生，副教授，研究方向为认证及密钥建立与区块链安全.

韩立东：男，1982年生，讲师，研究方向为可搜索加密.

谭　肖：男，1985年生，讲师，研究方向为公钥密码学.

责任编辑：马秀强