基于 RLWE 的密文策略属性代理重加密

张恩[1,2]，裴瑶瑶[1,2]，杜蛟[3]

（1. 河南师范大学计算机与信息工程学院，河南 新乡 453007；
2. “智慧商务与物联网技术”河南省工程实验室，河南 新乡 453007；
3. 河南师范大学数学与信息科学学院，河南 新乡 453007）

摘 要：针对现有基于 LWE 的代理重加密方案存在无法实现细粒度访问及效率低的问题，结合线性秘密共享方案、RLWE 和属性加密，提出一种密文策略属性代理重加密方案。该方案可以缩短密钥尺寸、减小密文空间、提高加解密效率，同时利用线性秘密共享矩阵作为访问矩阵，满足授权人细粒度委托控制的需求，抵抗代理服务器和被授权人之间的合谋。安全分析表明，在基于 RLWE 假设的标准模型下，所提方案是安全的。

关键词：代理重加密；RLWE；属性加密；线性秘密共享方案；细粒度访问

中图分类号：TP309.2

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018239

RLWE-based ciphertext-policy attribute proxy re-encryption

ZHANG En[1,2], PEI Yaoyao[1,2], DU Jiao[3]

1. College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China
2. Engineering Lab of Intelligence Bussiness & Internet of Things of Henan Province, Xinxiang 453007, China
3. College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China

Abstract: To solve LWE-based proxy re-encryption schemes cannot achieve fine-grained access and low efficiency problem, a ciphertext-policy attribute-based proxy re-encryption scheme was proposed. The scheme based on linear secret sharing scheme, RLWE and attribute encryption could shorten the key size, reduce the ciphertext space and improve the efficiency of encryption and decryption. At the same time, the linear secret sharing matrix was used as an access matrix to meet the requirements of authorized person fine-grained commissioning control and to resist the collusion between the agent and the authorized person. In addition, the proposed scheme is shown to be secure under the ring learning with errors assumption in the standard model.

Key words: proxy re-encryption, RLWE, attribute encryption, linear secret sharing scheme, fine-grained access

1 引言

云计算作为一种新兴的服务模式，采用负载均衡、分布式计算等技术，能够方便地为远程用户提供计算和存储功能，从而节省本地开销、提高资源利用率。云计算的出现改变了人们共享数据、信息和知识的方式。借助于云平台的超大存储空间和快速计算能力，人们可以通过网络实时快捷地存储、查询和共享数据。但是当用户向云平台上传数据时，这些数据处于用户不可控范围。如何实现数据的安全共享已成为当前重要的安全问题，而代理重加密为该问题提供了一种有效的解决方法。

在 1998 年的欧洲密码学年会上，Blaze 等[1]首次提出代理重加密的概念。典型的代理重加密方案

收稿日期：2018−01−11；**修回日期**：2018−05−19

通信作者：张恩，zhangenzdrj@163.com

基金项目：国家自然科学基金资助项目（No.U1604156, No.61772176, No.61602158）；河南省科技攻关计划基金资助项目（No.172102210045）

Foundation Items: The National Natural Science Foundation of China (No.U1604156, No.61772176, No.61602158), The Science and Technology Research Project of Henan Province (No.172102210045)

涉及三方：代理授权人（Alice）、被授权人（Bob）和代理服务器。在代理重加密的过程中，代理授权人（Alice）生成一个代理重加密键，并将其发送给代理服务器。代理服务器可以把代理授权人（Alice）公钥加密的密文转换成被授权人（Bob）公钥对同一明文加密的密文。被授权人（Bob）可以用自己的私钥来恢复加密的消息，而不需要知道授权人的私钥信息。同时，代理服务器并未得到有关数据的明文信息，从而保证了数据的安全性。

一般来说，根据密文转换方向，可将代理重加密分为单向代理重加密和双向代理重加密。单向代理重加密仅能实现 A 到 B 的密文转换，而双向代理重加密不仅能实现 A 到 B 的密文转换，还可以实现 B 到 A 的密文转换。Blaze 等[1]首先构造了一种双向代理重加密方案，但该方案在抵抗合谋攻击方面存在一定的问题。Ivan 等[2]提出单向代理重加密方案的通用方法，但无法保证其安全性。Ateniese 等[3]首次基于双线性对设计出一种单向代理重加密方案并给出安全模型。但是，以上方案都无法抵抗选择明文攻击。Canetti 等[4]和 Libert 等[5]分别构建了 CCA 安全的双向代理重加密和单向代理重加密方案。

随着身份加密和属性加密的出现，人们将代理重加密分别与身份加密和属性加密相结合，对代理重加密进行了扩展。2005 年，Sahai 等[6]提出模糊的基于身份加密的机制（FIBE），但该机制仅能支持门限访问控制策略。为了实现灵活的访问控制，Goyal 等[7]在 2006 年首次提出密钥策略属性加密（KP-ABE）方案，Bethencourt 等[8]提出了密文策略属性加密（CP-ABE）方案。Jin 等[9]对 CP-ABE 方案进行改进，提出一种安全的隐藏明文策略的属性加密方案，有效地避免访问策略中敏感信息的泄露。2007 年，Green 等[10]将代理重加密与身份加密相结合，首次提出了基于身份的代理重加密（ID-PRE）概念。Liang 等[11]对 ID-PRE 方案进行改进，率先设计出基于属性的代理重加密（AB-PRE）方案。Weng 等[12]首次提出了条件代理重加密的概念。Luo 等[13]提出了一种单向非交互的基于密文策略属性代理重加密方案。Seo 等[14]构造出一种高效的基于属性的代理重加密（AB-PRE）方案。Wungpornpaiboon 等[15]基于密文策略的属性加密，提出一种支持个人电子医疗记录代理的两层代理重加密方案，其内层的策略由数据拥有者控制，外层的策略由代理者控制。Liang 等[16]对文献[11]进行了改进，使基于属性的代理重加密（AB-PRE）方案满足选择明文攻击安全。Xu 等[17]提出了一种基于 CP-ABE 的多授权的属性代理重加密方案，解决 CP-ABE 方案中密钥分发和撤销用户访问权限时存在的安全问题。

然而，上述代理重加密方案均是基于经典密码学困难问题构造的，这些加密方案随着量子计算机的应用已变得不再安全。近年来，密码学者致力于设计安全、高效且能够有效抵御量子攻击的密码体系。格密码的出现为研究者提供了新的方法。2005 年，Regev 等[18]提出了一个新的格上困难问题——带误差的学习（LWE），并且证明它与格中最坏情况下的 SVP 问题是一样困难的。到目前为止，尚没有多项式时间量子算法能够破解格困难问题，而因子分解和离散对数问题可以通过 Shor 算法[19]在多项式时间内求解。Ajtai 等[20]发现，即使在最坏情况下，基于格困难问题的格密码系统也是非常安全的。

研究者根据格上的 LWE 问题设计出基于身份的加密方案[21-22]、基于属性的加密方案[23]以及基于密钥策略属性加密方案[24]。Kirshanova[25]和 Fan 等[26]分别基于 LWE 问题，提出了格上的代理重加密方案。Singh 等[27]将格上身份加密和代理重加密相结合，提出了一种基于身份的代理重加密方案。Kim 等[28]基于最坏情况下的格困难问题，提出了一种基于格上的抗合谋单向代理重加密方案，并且证明了该方案在随机预言模型下是安全的。Jiang 等[29]提出了格上基于多用户的单向代理重加密方案。张恩等[30]将声誉系统和基于 LWE 的对称代理重加密相结合，提出一个基于声誉系统的服务器辅助的隐私集合交集协议。Li 等[31]基于 LWEE（learning with errors in the exponent）概念提出了一种单比特单跳单向的代理重加密方案，解决基于 LWE 构造的代理重加密方案存在的噪声扩散问题。然而，基于格上 LWE 问题构造的代理重加密方案存在密钥尺寸过长、密文空间较大、效率较低的问题。2010 年，Lyubashevsky 等[32]对 LWE 问题进行改进，提出了 RLWE 问题，减小了密钥的尺寸。随后，Tan 等[33]在 2015 年提出基于 RLWE 密文策略属性加密体制。孙泽栋等[34]在 2016 年提出一种基于 RLWE 密钥策略属性加密体制。郑永辉等[35]设计一种环上基于属性的全同态加密体制的方案。张恩等[36]在 RLWE

困难问题的基础上，提出了抗隐蔽敌手的云外包秘密共享方案。Polyakov 等[37]基于 RLWE 的密钥交换，对 NTRU-RLWE 同态加密方案和 BV 同态加密方案进行改进，分别提出了 NTRU-ABD-PRE 方案和 BV-PRE 方案，但是这两种方案都无法实现细粒度的代理控制。目前尚没有基于 RLWE 的属性代理重加密方案。

为了解决现有基于 LWE 的代理重加密方案存在的加解密效率较低、无法实现细粒度访问的问题，本文在 Tan 方案[33]的基础上，提出一种基于 RLWE 的密文策略属性代理重加密方案，能够减小密钥尺寸、提高加解密效率、实现细粒度访问、抵抗代理者和授权者之间的合谋，达到抵御量子攻击的目的。本文所提方案具有以下特点。1) 细粒度访问控制。方案利用属性集合构造的访问结构来控制被授权人，被授权人可以为一个人、一个组织或多个组织，实现灵活的代理重加密。当且仅当被授权人的属性集合符合授权人设置的访问结构时，被授权人才能解密出密文。2) 高效性。和基于 LWE 的代理重加密方案相比，本文所提方案能够缩短密钥的尺寸、减小密文空间、节省内存资源、实现高效加解密运算。3) 防合谋。本文所提方案利用线性秘密共享方案来构造代理重加密键，使代理服务器通过代理重加密键无法获得授权者和被授权者的私钥信息，同时也能抵抗代理服务器与被授权者之间的合谋。4) 抗量子攻击。本文所提方案是基于格上的判定性 RLWE 问题构造的，借助于格的多维特点和格上的困难问题，使其在多项式量子算法内无法被攻破，提高了安全性，实现了抵御量子攻击的目的。

2　基础知识

2.1　格

定义 1　整数格。令 n 个线性无关的向量组成的整数格基为 $\boldsymbol{B}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)\in\mathbb{Z}^{m\times n}$，其中 $\mathbb{Z}$ 为整数集，m 和 n 为整数。整数格是指一组整数向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 线性组合构成的向量集合，即 $L(\boldsymbol{B})=\{\boldsymbol{Bc}:\boldsymbol{c}\in\mathbb{Z}^n\}$。若 $L(\boldsymbol{B})=L(\boldsymbol{B}')$，则必存在幺模矩阵 $\boldsymbol{U}$，满足 $\boldsymbol{B}=\boldsymbol{B}'\boldsymbol{U}$。

定义 2　格上的高斯分布。对于任意的 s>0 和格维数 $m\geqslant 1$，高斯函数 $\rho_s:R^m\to(0,1]$ 可定义为：

$$\rho_s(x)=\exp\left(-\Pi\frac{\|\boldsymbol{X}\|^2}{s^2}\right),\quad \boldsymbol{x}\in R^m。$$

对于任意格陪集 $\Lambda_y^{\perp}(A)$ 上以 0 为中心的离散高斯分布，有 x 处的概率为 $\rho_s(\boldsymbol{x})$，其他地方的概率为 0。

定义 3　最短向量问题（SVP, shortest vector problem）。给定一个整数格基 $\boldsymbol{B}\in\mathbb{Z}^{m\times n}$，找到一个非 0 的向量 $\boldsymbol{Bx}(\boldsymbol{x}\in\mathbb{Z}^n\setminus\{0\})$，对于任意的 $\boldsymbol{y}\in\mathbb{Z}^n\setminus\{0\}$，满足 $\|\boldsymbol{Bx}\|\leqslant\|\boldsymbol{By}\|$。

定义 4　最近向量问题（CVP, closest vector problem）。给定一个整数格基 $\boldsymbol{B}\in\mathbb{Z}^{m\times n}$ 和目标向量 $\boldsymbol{t}$（$\boldsymbol{t}$ 不一定是格上的点），找到一个非 0 向量 $\boldsymbol{Bx}(\boldsymbol{x}\in\mathbb{Z}^n\setminus\{t\})$，对于任意的 $\boldsymbol{y}\in\mathbb{Z}^n\setminus\{0\}$，满足 $\|\boldsymbol{Bx}-\boldsymbol{t}\|\leqslant\|\boldsymbol{By}-\boldsymbol{t}\|$。

定义 5　LWE 分布。令 $\mathbb{Z}$ 为整数集，q 为正整数，随机选择一个向量 $\boldsymbol{s}\in Z_q^n$ 作为私钥，$e\in R$ 服从某一正态分布 $\chi=\chi(k)$，同时随机均匀地选取 $\boldsymbol{a}\in Z_q^n$，计算出 b 的值 $b=<\boldsymbol{a},\boldsymbol{s}>+e$，且 $b\in Z_q$。此时 LWE 的分布 $A_{s,\chi}$ 为 $(\boldsymbol{a},b)\in Z_q^n\times Z_q$。

定义 6　RLWE 分布。随机选择 $\boldsymbol{s}\in R_q$ 作为私钥，$e\in R$ 服从环上某一正态分布 $\chi=\chi(k)$，同时随机均匀地选取 $a\in R_q$，计算出 b 的值 $b=<a,s>+e$，且 $b\in R_q$。此时 RLWE 的分布 $A_{s,\chi}$ 为 $(a,b)\in Z_q\times Z_q$。

定义 7　判定性 RLWE 问题。令安全参数为 K，$f(x)=x^d+1$，其中，$d=d(K)$ 是 2 的幂次。令 $R=\dfrac{Z_q[x]}{x^d+1}$，$q=1\bmod 2d$，$e\in R$ 服从于某一正态分布 $\chi=\chi(k)$，随机均匀地选取 $s\in R_q$ 和 $a\in R_q$，计算出 b 的值 $b=as+e$，且 $b\in R_q$。则 RLWE 上的分布 $A_{s,\chi}$ 为 $(a,b=as+e)$。如何区分 $A_{s,\chi}$ 与 R_q^2 上的均匀分布问题（a、b 都随机均匀地取自 R_q）就是判定性 RLWE 问题。

判定性 RLWE 问题的实例：询问一个未指定的预言机 O，该预言机可能是一个伪随机的采样器 O_P，即随机均匀地选取 $s\leftarrow R_q$、$a_i\leftarrow R_q$ 和 $e_i\leftarrow\chi$，并计算 $b_i=a_is+e_i$，最终得到 $(a_i,b_i)\in R_q^2$；也可能是真正随机的预言机 O_R，即 (a_i,b_i) 随机均匀取自 R_q^2。判定性 RLWE 问题允许一个敌手重复询问预言机 O。预言机利用采样器 O_P 和预言机 O_R 随机地返回若干个实例（a,b）给敌手，如果敌手能够准确分辨该实例来自 O_P 或 O_R 的优势 $|\Pr\left[A^{O_P}=1\right]-\Pr\left[A^{O_S}=1\right]|$ 是不可忽略的，则存在一个多项式时间敌手可以解决判定性 RLWE 问题。

2.2 访问结构和线性秘密共享

定义 8 单调的访问结构。定义一个大小为$|U|$的属性域$U=\{u_1,u_2,\cdots,u_{|U|}\}$。访问结构 A 是集合 U 上的一个非空集合，即 $A\subseteq U$。A 是一个单调的访问结构，在 A 中的集合为授权集合，不在 A 中的集合为非授权集合，且对于 $\forall B,C: B\in A$， $B\subseteq C$，有 $C\in A$。

定义 9 线性秘密共享方案（LSSS, linear secret sharing schemes）。基于一组属性集合 U 上的线性秘密共享方案 Π 具有以下特性。

1) 每一个属性关于秘密 s 的子份额形成一个向量。

2) 对于线性秘密共享方案 Π，存在一个 n 行 θ 列的矩阵 $\boldsymbol{F}\in R_q^{n\times\theta}$，$\boldsymbol{F}$ 的每一行对应一个属性，且行标签为 $p(i)\in\cup,\forall i\in[n]$。给定一个列向量 $\boldsymbol{v}=(s,r_2,\cdots,r_q)$，其中，$s\in R_q$ 是共享的秘密，$r_2,\cdots,r_q\leftarrow R_q$ 为随机选取的数。$\boldsymbol{Fv}$ 是方案 Π 中共享子份额对应的向量，且共享子份额为 $\delta_i=(\boldsymbol{Fv})_i$，即属性 $p(i)$的内积值为 $\boldsymbol{F}_i\boldsymbol{v}$。

线性秘密共享方案（LSSS）具有线性重构的性质。假设 Π 代表的线性秘密共享方案的访问结构为 A。令 $A^*\in A$ 是授权的集合，对于该集合的每一个属性，有 $I=\{i: p(i)\in A\}$，则存在一个常数 $\{w_i\in R_q\}_{i\in I}$ 和有效的共享子份额 δ_i，使 $\sum_{i\in I}\delta_i w_i=\boldsymbol{s}$。而对于非授权的集合则不存在这样的常数。

2.3 CP-ABPRE$_{\text{RLWE}}$ 方案的系统定义及安全模型

一个基于 RLWE 的密文策略属性代理重加密（CP-ABPRE$_{\text{RLWE}}$）方案由下述 6 个多项式算法构成。

1) Setup（K）：输入安全参数 K，通过安全参数构造一个多项式环 R，定义一个属性域 U，输出主公钥 PK 和主私钥 MSK。

2) Encrypt(PK，M，A')：输入主公钥 PK、1 bit 的信息 $M\in\{0,1\}$ 和访问结构 A'。根据线性秘密共享方案 Π，构造 LSSS 的访问结构 $(\boldsymbol{F}',p')$，并获得每个属性对应的子份额，输出加密密文 $CT'=(C,C_i)$。

3) Rekey(PK, A)：输入一个新的访问结构 A，构造 A 的 LSSS 访问结构$(\boldsymbol{F},p)$，并获得每个属性对应的子份额，结合访问结构 $(\boldsymbol{F}',p')$ 中每个属性集合对应的子份额，输出转换键 Rk。

4) ReEncrypt(CT' , Rk)：输入密文 CT' 和转换键 Rk，输出重加密的密文 CT=(C, C_j)。

5) KeyGen(MSK, A^*)：输入主私钥 MSK 和被授权人的属性集合 $\boldsymbol{A}^*$，输出被授权人私钥 SK。

6) Decrypt(PK, CT, SK)：输入密文 CT，系统的主公钥 PK，被授权人的私钥 SK。若被授权人属性满足访问结构 A，则输出 M^*，否则输出一个错误的符号 $\perp$。

定义 10 CP-ABPRE$_{\text{RLWE}}$ 的安全模型。一个基于 RLWE 的密文策略属性代理重加密方案的安全模型可以通过以下游戏来描述。

初始化：模拟器利用算法 Setup(K)获得主公钥 PK 和主私钥 MSK，并将主公钥 PK 发送给敌手 $\mathcal{A}$。令集合 NA 中的属性为敌手 $\mathcal{A}$ 未进行私钥查询的属性，集合 HA 中的属性为敌手 $\mathcal{A}$ 已进行私钥查询的属性。敌手宣布挑战的访问结构为 $\boldsymbol{A}_1$，并将其告知模拟器 $\mathcal{B}$。

阶段 1 敌手 $\mathcal{A}$ 进行如下查询。

1) 私钥查询。敌手 $\mathcal{A}$ 向模拟器 $\mathcal{B}$ 发送一系列属性集合 A^* 进行私钥查询，且已查询属性所构成的集合不满足访问结构 A_1。模拟器 $\mathcal{B}$ 运行密钥生成算法，构造属性集 A^* 的私钥 SK，并将其返回给敌手 $\mathcal{A}$。

2) 重加密键的查询。敌手对属性集合 A_a 和 A_b 进行重加密键的询问。模拟器 $\mathcal{B}$ 将构造的重加密键返回给敌手 $\mathcal{A}$。

3) 重加密的查询。敌手 $\mathcal{A}$ 对属性集合 A_a 和 A_b 进行重加密操作的询问。模拟器 $\mathcal{B}$ 运行重加密键生成算法，获得重加密键。随后运行重加密算法，得到密文 C_b，并将生成的密文 C_b 返回给敌手 $\mathcal{A}$。

挑战 敌手 $\mathcal{A}$ 向模拟器发送 1 bit 的信息 $M\in\{0,1\}$。模拟器 $\mathcal{B}$ 抛出一枚二进制硬币 r，并根据访问结构 A_1' 和 A_1 产生一个挑战密文。模拟器 $\mathcal{B}$ 将密文发送给敌手 $\mathcal{A}$ 作为挑战密文。

阶段 2 敌手 $\mathcal{A}$ 重复阶段 1 的操作，进行多次查询，且已查询私钥的属性所构成的集合仍不满足访问结构 A_1。

猜测 敌手 $\mathcal{A}$ 输出一个关于密文 r 的猜想 r'，若 r= r'，则敌手 $\mathcal{A}$ 获胜。

在上述游戏过程中，敌手 $\mathcal{A}$ 的优势可以定义为：$Adv_{\xi,A}(\lambda)=|\Pr[r=r']-\frac{1}{2}|$。

在此安全游戏中，若任何多项式时间敌手 $\mathcal{A}$ 的优势是可忽略的，则基于 RLWE 的密文策略属性代理重加密方案在基于 RLWE 假设的标准模型下是安全的。

3　方案描述

本文基于线性秘密共享方案和 RLWE，将代理重加密和属性加密相结合，提出了一种基于 RLWE 的密文策略属性代理重加密方案。具体方案如下。

1) Setup(K)：令安全参数为 K，选择一对正整数 q 和 p，且 $q=1 \bmod 2K$，$\gcd(p,q)=1$。令 $f(x)=x^d+1$，且 $d=d(K)$ 是 2 的幂次，则 $R=\dfrac{Z_q[x]}{f(x)}$ 是一个整数多项式环。令 $\chi=\chi(k)$ 服从某一正态分布，随机地选择 $\beta \leftarrow R_q$、$t \leftarrow R_q$ 和一个很小的错误值 $e \leftarrow \chi$，其中，β 为私钥，计算得到公钥 $\alpha=t\beta+pe \in R_q$。给定一个属性域 $U=\{u_1,u_2,\cdots,u_{|U|}\}$，对于 U 中的元素，随机地选择 $(\beta_i,\beta_i^{-1}) \leftarrow R_q$ 和很小的噪声 $e_i \leftarrow \chi$，并计算出 $\alpha_i=\beta_i+pe_i \in R_q$。最后，输出系统主公钥 $PK=\{t,\alpha,\alpha_i\}$ 和主私钥 $MSK=\{\beta,\beta_i,\beta_i^{-1}\}$。

2) Encrypt(PK,M, A')：在加密算法中，输入 1 bit 的信息 $M \in \{0,1\}$、主公钥 PK 和属性域 $U_a=\{u_1',u_2',\cdots,u_n'\}$ 所构成的访问结构 A'。根据线性秘密共享方案，构造 A' 所对应 LSSS 的访问结构 $(\boldsymbol{F}',p')$，其中，$\boldsymbol{F}' \in R_q^{n\times\theta}$ 为矩阵。矩阵的每一行映射 U_a 中唯一的一个属性，且行标签为 $p(i) \in U_a$，$\forall i \in [n]$。然后，构造一个向量 $\boldsymbol{v}'=(s,r_2',\cdots,r_\theta')$，其中，$s \in R_q$ 为共享的秘密，$r_2',\cdots,r_\theta' \leftarrow R_q$ 是随机选取的。通过属性域 U_a 和 LSSS 构造共享子份额对应的向量 $\boldsymbol{F}_v'$，计算属性域中每一个属性所对应的共享子份额 $\delta_i=F_i \times v' \in R_q$，$F_i$ 对应的是 $\boldsymbol{F}'$ 的第 i 行。最后，选择噪声 $e',e_i' \leftarrow \chi$ 和随机数 $r \leftarrow R_q$。输出加密的密文 CT'=(C,C_i) 为

$$C=\alpha rs+pM+pe' \in R_q$$
$$C_i=t\alpha_i r\delta_{i'}+pe_i' \in R_q$$

3) Rekey(PK, A): 令被授权人的属性域为 U_b=$\{u_1,u_2,\cdots,u_n\}$，该属性域对应的访问结构为 A。利用线性秘密共享方案 Π，构造 A 对应 LSSS 的访问结构 $(\boldsymbol{F},p)$，其中，$\boldsymbol{F} \in R_q^{n\times\theta}$ 为矩阵。矩阵的每一行映射 U_b 中唯一的一个属性，行标签为 $p(j) \in U_b$，$\forall j \in [n]$。然后，选择一个向量 $\boldsymbol{v}=(s,r_2,\cdots,r_q)$，其中，$s \in R_q$ 仍为共享的秘密，$r_2,\cdots,r_q \leftarrow R_q$ 是随机选取的数。通过属性域 U_b 和 LSSS 构造共享子份额对应的向量 $\boldsymbol{F}_v$。对于属性域中的每一个属性，计算该属性所对应的子份额 $\delta_j=\boldsymbol{F}_j \times v \in R_q$（$\boldsymbol{F}_j$ 对应矩阵 $\boldsymbol{F}$ 的第 j 行）。输入访问结构 $(\boldsymbol{F}',p')$ 和 $(\boldsymbol{F},p)$ 中每一个属性所对应的子份额和公钥，输出转换键 $Rk=(\alpha_i\delta_i)^{-1}\alpha_j\delta_j$。

4) ReEncrypt(CT',Rk)：输入重加密前的密文 CT' 和转换键 Rk，输出重加密后的密文 $CT=(C,C_j)$，其中，C_j=$C_iRk=t\alpha_j r\delta_j+Rkpe_i'$。

5) KeyGen(MSK, A^*)：在密钥生成算法中，通过主私钥 MSK 和属性集合 A^*来产生私钥。选择一对随机数 b 和它的逆 $b^{-1}(b \in R_q, b^{-1} \in R_q)$以及错误值 e" 和 e_j''。输出被授权人属性所对应的私钥为

$$SK=\beta b^{-1}+pe'' \in R_q$$
$$SK_j=\beta_j^{-1}b+pe_j'' \in R_q, \forall_j \in A^*$$

6) Decrypt(PK，CT，SK)：给定公钥 PK、被授权人的私钥 SK 和密文 CT，恢复消息 M。如果被授权人的属性集 $A^* \in A$，则 $I \subset \{1,2,\cdots,n\}$ 被定义为 $I=\{j:p(j) \in A^*\}$。如果 $\{\delta_j\}$ 是有效的共享子份额，计算出一系列的常量 $\{w_j \in R_q\}_{j\in I}$，使 δ_j 和 w_j 满足 $\sum_{j\in I}\delta_j w_j=s$。最后，计算出 $M^*=pM=C-SK\sum_{j\in I}C_iRkw_jSK_j$，输出 M=M^*，否则，输出一个错误的符号 ⊥。

4　方案分析

4.1　正确性分析

通过上述方案描述可知，属性集合满足访问结构的被授权人可以成功解密出 M^*，不满足访问结构的被授权人则无法解密出 M^*。M^* 的计算过程如下

$$\begin{aligned}
M^* &= C-SK\textstyle\sum_{j\in I}C_i\cdot Rk\cdot w_j\cdot SK_j \\
&= C-SK\textstyle\sum_{j\in I}(t\cdot\alpha_j r\delta_j+Rk\cdot pe_i')w_jSK_j \\
&= C-SKs\textstyle\sum_{j\in I}(tr\alpha_jSK_j)-pSK\sum_{j\in I}e_i'\ Rkw_jSK_j \\
&= C-SKs\textstyle\sum_{j\in I}tr(\beta_j+pe_i)SK_j-pSK\sum_{j\in I}e_i'\ Rkw_jSK_j \\
&= C-SKtrsb-pSKtrs\textstyle\sum_{j\in I}(\beta_je_j''+e_i\beta_j^{-1}b+ \\
&\quad pe_ie_j'')-pSK\textstyle\sum_{j\in I}e_i'\ Rkw_jSK_j
\end{aligned}$$

$$= \alpha rs + pM + pe' - SKtrsb - pSKtrs \cdot \sum_{j\in I}(\beta_j e_j'' + e_i\beta_j^{-1}b + pe_i e_j'') - pSK\sum_{j\in I} e_i' Rkw_j SK_j$$
$$= (t\beta + pe)rs + pM + pe' - (\beta + pe''b)trs - pSK \sum_{j\in I} trs(\beta_j e_j'' + e_i\beta_j^{-1}b + pe_i e_j'') - e_i' Rkw_j SK_j$$
$$= pM + p(rse + e' - e''trsb) - pSK\sum_{j\in I} trs(\beta_j e_j'' + e_i\beta_j^{-1}b + pe_i e_j'') - e_i' Rkw_j SK_j$$

在上述方案中，由于 e、e'、e_i、e_i'、e''、e_j'' 是较小的错误值，方案可以通过选择适当的参数使 $p(rse+e'-e''trsb) - pSK\sum_{j\in I} trs(\beta_i e_j'' + e_i\beta_j^{-1}b + pe_i e_j'') - e_i' \cdot Rkw_j SK_j \bmod p = 0$。因此，当 $M^* \bmod p$ 接近 1 时，明文消息为 1；否则，明文消息为 0。

4.2 安全性分析

本节主要证明在基于 RLWE 假设的标准模型下，CP-ABPRE$_{\text{RLWE}}$ 方案是安全的。

定理 1 在基于 RLWE 假设的标准模型下，如果存在一个多项式时间算法的敌手 $\mathcal{A}$ 可以攻破 CP-ABPRE$_{\text{RLWE}}$ 方案，那么就可以构造一个模拟器 $\mathcal{B}$ 以不可忽略的优势攻破判定性 RLWE 问题。

证明 假设存在一个概率多项式时间（PPT, probabilistic polynomial time）算法的敌手 $\mathcal{A}$ 以优势 ε 在基于 RLWE 假设的标准模型中攻破 CP-ABPRE$_{\text{RLWE}}$ 方案，那么就存在一个 PPT 算法的模拟器 $\mathcal{B}$ 以 $\frac{\varepsilon}{2}$ 的优势攻破判定性 RLWE 问题。模拟器 $\mathcal{B}$ 的运行过程如下。

首先，挑战者根据定义 7 来设置判定性 RLWE 问题的实例。挑战者通过掷出一枚公平的二进制硬币 r 来代替询问一个未指定的预言机 O。当 r=0 时，询问的预言机是伪随机的采样器 O_P；否则，询问的预言机为真正的随机预言机 O_R。模拟器 $\mathcal{B}$ 利用敌手 $\mathcal{A}$ 来区分不同的预言机。

初始化 模拟器选择一个大小为|U|的属性域 U，并定义两个集合 NA 和 HA。集合 NA 中的属性是敌手 $\mathcal{A}$ 未进行私钥查询的属性，而集合 HA 中的属性是敌手 $\mathcal{A}$ 已进行私钥查询的属性。同时，敌手 $\mathcal{A}$ 宣布自己挑战的访问结构为 A_1，并将其告知模拟器 $\mathcal{B}$。

设置 模拟器 $\mathcal{B}$ 运行 Setup(K)多项式生成算法，构造出公钥 PK 如下。

令 $\alpha = t\beta + pe \in R_q$，对于属性 $i \in U$，如果属性 $i \in A_1$，则定义 $\alpha_i = ps_i \in R_q$；否则 $\alpha_i = \beta_i + pe_i \in R_q$。

最后，模拟器 $\mathcal{B}$ 把公钥 $PK = \{t, \alpha, \alpha_i\}$ 返回给敌手。

阶段 1 敌手 $\mathcal{A}$ 可以进行如下查询。

1) 私钥查询。敌手 $\mathcal{A}$ 向模拟器 $\mathcal{B}$ 发送一系列的属性集 A^* 进行私钥查询，且已查询的属性集合不满足访问结构 A_1。模拟器 $\mathcal{B}$ 运行密钥生成算法，构造属性集 A^* 的私钥 SK 为

$$SK_0 = \beta \cdot b^{-1} + pe'' \in R_q$$
$$SK_j = \beta_j^{-1} \cdot b + pe_j'' \in R_q, \forall_j \in A^*$$

2) 重加密键的查询。敌手对属性集合 A_a 和 A_b 进行重加密键的询问。首先，模拟器将集合 A_a 和线性秘密共享方案相结合，构造出 LSSS 的矩阵 $\boldsymbol{F}' \in R_q^{n\times\theta}$，且矩阵的每一行所对应属性的共享子份额为 δ_a。接着，模拟器将集合 A_b 与线性秘密共享方案相结合，构造出 LSSS 的矩阵 $\boldsymbol{F} \in R_q^{n\times\theta}$，且矩阵的每一行所对应属性的共享子份额为 δ_b。此时，重加密键为 $Rk = (\alpha_a\delta_a)^{-1}\alpha_b\delta_b$。模拟器 $\mathcal{B}$ 将生成的重加密键返回给敌手 $\mathcal{A}$。敌手可以进行多次查询。

3) 敌手 $\mathcal{A}$ 对属性集合 A_a 和 A_b 进行重加密操作的询问。模拟器 $\mathcal{B}$ 运行重加密键生成算法，获得重加密键。随后运行重加密算法，得到密文 C_b，并将生成的密文返回给敌手 $\mathcal{A}$。

挑战 敌手 $\mathcal{A}$ 接受挑战，并向模拟器 $\mathcal{B}$ 发送 1 bit 的信息 $M \in \{0,1\}$。模拟器 $\mathcal{B}$ 抛出一枚二进制硬币 r，并根据访问结构 A_1' 和 A_1 产生一个挑战密文。模拟器 $\mathcal{B}$ 将密文发送给敌手 $\mathcal{A}$ 作为其挑战密文。产生的挑战密文如下。

如果 r=0，则随机地选择 $m, m_j \leftarrow R_q$，此时 $C = pm \in R_q$，$C_j = pm_j \in R_q$。

如果 $r=1$，对于任意属性 $j \in A_1$，随机地选择 $n, n_i, Rk \leftarrow R_q$，此时 $C = pn + M \in R_q$，$C_j = pn_i Rk \in R_q$。

阶段 2 重复阶段 1 的操作，进行多次查询，且已查询私钥的属性集合仍不满足访问结构 A_1。

猜测 模拟器 $\mathcal{B}$ 从敌手 $\mathcal{A}$ 中得到一个关于 r 的猜测 r'，并输出 r' 作为挑战的结果。如果 $r' = r$，则输出 $O' = O_P$，否则 $O' = O_R$。

由上述安全游戏可知，敌手 $\mathcal{A}$ 在此游戏的优势 ε 为 $|\Pr[r' = r] - \frac{1}{2}|$。因此，RLWE 预言机 O 的优势分为以下两种情况。

1) 在伪随机的采样器中，敌手的优势为 ε，此时 $O=O_P$，$\Pr[r'=r \mid O=O_P]=\frac{1}{2}+\varepsilon$。则模拟器挑战困难问题的优势为 $\Pr[O'=O \mid O=O_P]=\frac{1}{2}+\varepsilon$。

2) 在真正随机的预言机中，敌手没有任何优势，此时 $O=O_R$，$\Pr[r'\neq r \mid O=O_R]=\frac{1}{2}$，则模拟器挑战困难问题的优势为 $\Pr[O'=O \mid O=O_R]=\frac{1}{2}$。

在此游戏中，模拟器 $\mathcal{B}$ 在判定性 RLWE 问题中的优势为

$$\begin{aligned}&\frac{1}{2}(\Pr[O'=O \mid O=O_P]+\Pr[O'=O \mid O=O_R])-\frac{1}{2}\\&=\frac{1}{2}\left(\frac{1}{2}+\varepsilon+\frac{1}{2}\right)-\frac{1}{2}\\&=\frac{\varepsilon}{2}\end{aligned}$$

4.3　性能比较

首先，将文献[1,9,11,27-28,37]方案和所提方案进行比较，如表 1 所示。同时，将文献[25-26,28-29]方案和所提方案产生的密钥尺寸进行对比，如表 2 所示。最后，对方案进行仿真，分别如图 1 和图 2 所示。

由 Shor 方案[19]可知，基于 DDH 或 DBDH 困难问题构造的算法可以通过 Shor 量子算法在多项式时间内求解，故传统的基于 DDH 或 DBDH 的代理重加密方案[1,9,11]不能有效抵抗量子攻击。由 Regev 方案[18]可知，给定任意的 m=poly(n)、模 $q\leqslant 2^{poly(n)}$ 以及参数为 $\alpha q\geqslant 2\sqrt{n}(0\leqslant\alpha\leqslant 1)$ 的离散高斯错误分布 χ，对于 $\gamma=\tilde{O}(n/\alpha)$，量子算法解决判定性 LWE 问题和量子算法解决 GapSVP_γ 和 SIVP_γ 问题是一样困难的。故基于格上 LWE 构造的方案[27-28]可以有效地抵抗量子攻击。由 Lyubashevsky 方案[32]可知，给定任意的 m=poly(n)、模 q 以及错误率 $\alpha<1$ 的错误分布 χ，对于 $\gamma=\mathrm{poly}(n)/\alpha$，量子算法解决判定性 RLWE 问题和量子算法解决 SVP_γ 问题是一样困难的。故基于格上 RLWE 构造的方案[37]可以有效地抵抗量子攻击。而本文基于格上 RLWE 构造的方案，在量子多项式

表 2　　**密钥尺寸对比**

方案	公钥的尺寸	私钥的尺寸
文献[25]	$O(n^2)$	$O(n^2)$
文献[26]	$O(n^2)$	$O(n^2)$
文献[28]	$O(n^2)$	$O(n^2)$
文献[29]	$O(n^2)$	$O(n^2)$
所提方案	$O(n)$	$O(n)$

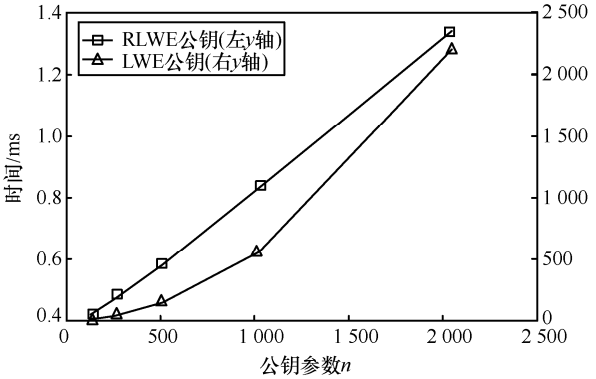

图 1　公钥产生的时间

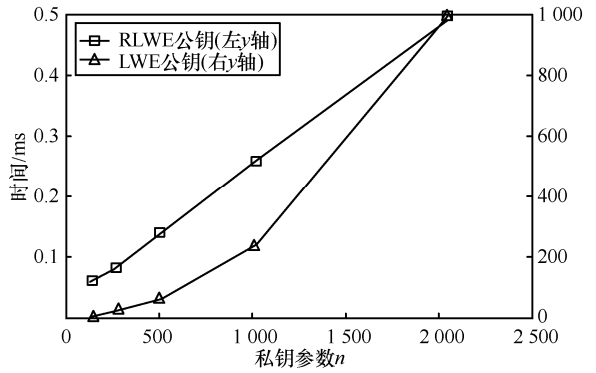

图 2　私钥产生的时间

表 1　　**方案比较**

方案	是否抵抗量子攻击	困难问题	支持的访问门限	密文转换方向	是否抗合谋
文献[1]	否	DDH	无	双向	否
文献[9]	否	DBDH	无	单向	是
文献[11]	否	DBDH	与	单向	是
文献[27]	是	LWE	无	双向	否
文献[28]	是	LWE	无	单向	是
文献[37]	是	RLWE	无	单向	是
所提方案	是	RLWE	与，或	单向	是

时间内无法求解，也可以有效地抵抗量子攻击。

文献[1,9,27-28,37]方案不支持门限访问策略，不能实现细粒度的访问控制；而对于文献[11]，虽能实现细粒度的访问控制，但该访问结构仅能支持与门限。为了更细粒度地控制被授权人，所提方案基于 RLWE 问题，将密文策略属性加密、线性秘密共享和代理重加密相结合，提出了一个支持与和或门限的代理重加密方案。同时，所提方案利用线性秘密共享方案来构造代理重加密键，代理服务器和被授权者合谋无法得到授权者的私钥信息，解决了代理服务器与被授权者之间的合谋问题。

基于传统密码学困难问题构造的代理重加密方案[1,9,11]在大素数或椭圆双曲线性环境下进行操作，计算复杂、效率低下。而基于 LWE 问题构造的代理重加密方案[25-26,28-29]在小整数范围内对矩阵进行操作，可以实现并行计算，但存在密钥尺寸较大的问题。所提方案基于 LWE 的变体 RLWE 这一特殊的代数结构进行构造。根据定义 5 和定义 6 可知，在 LWE 分布中随机均匀选取的 $\boldsymbol{a}$ 和 $\boldsymbol{s}$ 为向量，而在 RLWE 分布中随机均匀选取的 a 和 s 为常数。由于 a 和 s 选取形式的不同，使基于 RLWE 和基于 LWE 构造的公钥和私钥的尺寸不同。基于 LWE 构造的公钥和私钥为矩阵，且尺寸大小为 $O(n^2)$，而基于 RLWE 构造的公钥和私钥为向量，尺寸大小为 $O(n)$。和基于 LWE 构造的方案相比，所提方案基于 RLWE 构造，可以缩短公钥和私钥尺寸、减小密文的空间，从而降低加解密复杂度。表 2 为在相同参数条件下所提方案和文献[25-26,28-29]方案的密钥尺寸的比较。同时，本文在处理器为 Intel Core i7 @ 3.4 GHz 的 Lenovo Ghost win7 x64 上采用 python2.7 对方案进行仿真，在不同参数条件下（n=128, 256, 512, 1 024, 2 048），测试基于 RLWE 和基于 LWE 产生公钥和私钥的时间，结果如图 1 和图 2 所示。由图 1 和图 2 可知，基于 RLWE 产生公钥和私钥时间明显小于基于 LWE 产生公钥和私钥的时间。同时，随公钥参数和私钥参数的增加，基于 RLWE 产生的公钥和私钥的时间呈线性增长，而基于 LWE 产生的公钥和私钥时间呈指数增长。

5 结束语

随着云计算的高速发展，数据共享成为研究的热点，代理重加密受到广泛的关注。但基于 LWE 的代理重加密方案存在效率低、无法实现细粒度的访问等问题。本文结合 RLWE、线性秘密共享和属性加密，提出一种密文策略的属性代理重加密方案。该方案可以缩短密钥尺寸、减小密文空间、提高加解密效率。同时，本文将代理重加密和密文策略属性加密相结合，对被授权人（被授权人可以为一个人、一个组织或多个人）进行细粒度的访问控制，达到抵御量子攻击的目的。安全分析表明，在基于 RLWE 困难问题的标准模型下，所提方案是安全的。

参考文献：

[1] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]//Advances in Cryptology EUROCRYPT. 1998: 127-144.

[2] IVAN A A, DODIS Y. Proxy cryptography revisited[C]//Network and Distributed System Security Symposium. 2003.

[3] ATENIESE G, FU K, GREEN M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information and System Security (TISSEC), 2006, 9(1): 1-30.

[4] CANETTI R, HOHENBERGER S. Chosen-ciphertext secure proxy re-encryption[C]//The 14th ACM Conference on Computer and Communications Security. 2007: 185-194.

[5] LIBERT B, VERGNAUD D. Unidirectional chosen-ciphertext secure proxy re-encryption[C]//International Workshop on Public Key Cryptography. 2008: 360-379.

[6] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 2005: 457-473.

[7] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security. 2006: 89-98.

[8] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE Symposium on Security and Privacy. 2007: 321-334.

[9] GREEN M, ATENIESE G. Identity-based proxy re-encryption[C]//Applied Cryptography and Network Security. 2007: 288-306.

[10] JIN C C, FENG X Y, SHEN Q N. Fully secure hidden ciphertext policy attribute-based encryption with short ciphertext size[C]//The 6th International Conference on Communication and Network Security. 2016: 91-98.

[11] LIANG X, CAO F Z, LIN H, et al. Attribute based proxy re-encryption with delegating capabilities[C]//The 4th International Symposium on Information, Computer, and Communications Security. 2009: 276-286.

[12] WENG J, DENG R H, DING X, et al. Conditional proxy re-encryption secure against chosen-ciphertext attack[C]//The 4th International Symposium on Information, Computer, and Communications Security. 2009: 322-332.

[13] LUO S, HU J, CHEN Z. Ciphertext policy attribute-based proxy re-encryption[C]//Information and Communications Security. 2010: 401-415.

[14] SEO H. J, KIM H. Attribute-based proxy re-encryption with a constant number of pairing operations[J]. Journal of Information and Communication Convergence Engineering, 2012, 10(1): 53-60.

[15] WUNGPORNPAIBOON G, VASUPONGAYYA S. Two-layer ciphertext-policy attribute-based proxy re-encryption for supporting PHR delegation[C]//Computer Science and Engineering Conference. 2016: 1-6.

[16] LIANG K, FANG L, SUSILO W, et al. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security[C]//The 5th International Conference on Intelligent Networking and Collaborative Systems. 2013: 552-559.

[17] XU X L, ZHOU J L, WANG X H, et al. Multi-authority proxy re-encryption based on CPABE for cloud storage systems[J]. Journal of Systems Engineering and Electronics, 2016, 27(1): 211-223.

[18] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//The 37th Annual ACM Symposium on Theory of Computing (STOC'05). 2005: 84-93.

[19] SHOR P W. Polynomial-time algorithms for prime factorizetion and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303-332.

[20] AJTAI M. Generating hard instances of lattice problems[C]//The 28th Annual ACM Symposium on Theory of Computing. 1996: 99-108.

[21] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions [C]//The 40th Annual ACM Symposium on Theory of Computing. 2008: 197-206.

[22] AGRAWAL S, BOYEN X, VAIKUNTANATHAN V, et al. Fuzzy identity based encryption from lattices[J]. IACR Cryptology ePrint Archive, 2011: 414.

[23] BOYEN X. Attribute-based functional encryption on lattices[J]. Lecture Notes in Computer Science: Theory of Cryptography, 2013, 7785: 122-142.

[24] DAN B, GENTRY C, GORBUNOV S, et al. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2014: 533-556.

[25] KIRSHANOVA E. Proxy re-encryption from lattices[C]//Public Key Cryptography. 2014: 77-94.

[26] FAN X, LIU F H. Various proxy re-encryption schemes from lattices[J]. IACR Cryptology ePrint Archive, 2016: 278.

[27] SINGH K, RANGAN C P, BANERJEE A K. Lattice based identity based proxy re-encryption scheme[J]. Journal of Internet Services and Infor- mation Security, 2013, 3(3/4): 38-51.

[28] KIM K S, JEONG I R. Collusion-resistant unidirectional proxy re-encryption scheme from lattices[J]. Journal of Communications and Networks, 2016, 18(1): 1-7.

[29] JIANG M M, HU Y P, WANG B C, et al. Lattice-based multiuse unidirectional proxy re-encryption[J]. Security and Communication Networks, 2015, 8(18): 3796-3803.

[30] ZHANG E, LI F, NIU B, et al. Server-aided private set intersection based on reputation[J]. Information Sciences, 2017, 387: 180-194.

[31] LI Z P, MA C G, WANG D, et al. Toward proxy re-encryption from learning with errors in the exponent[C]//Trustcom/BigDataSE/ICESS. 2017: 683-690.

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

[33] TAN S F, SAMSUDIN A. Lattice ciphertext-policy attribute-based encryption from ring-LWE[C]//International Symposium on Technology Management and Emerging Technologies. 2015: 258-262.

[34] 孙泽栋, 祝跃飞, 顾纯祥, 等. 基于 RLWE 的密钥策略属性加密体制[J]. 通信学报, 2016, 37(S1): 125-131.
SUN Z D, ZHU Y F, GU C X, et al. RLWE-based key-policy ABE scheme[J]. Journal on Communications, 2016, 37(S1): 125-131.

[35] 郑永辉, 康元基, 顾纯祥, 等. 环上基于属性的全同态加密体制设计[J]. 通信学报, 2017, 38(4): 55-63.
ZHENG Y H, KANG Y J, GU C X, et al. Attribute-based fully homomorphic encryption scheme over rings [J]. Journal on Communications, 2017, 38(4): 55-63.

[36] 张恩, 耿魁, 金伟, 等. 抗隐蔽敌手的云外包秘密共享方案[J]. 通信学报, 2017, 38(5): 57-65.
ZHANG E, GENG K, JIN W, et al. Cloud outsourcing secret sharing scheme against covert adversaries[J]. Journal on Communications, 2017, 38(5): 57-65.

[37] POLYAKOV Y, KURT R. Fast proxy re-encryption for publish/subscribe systems[J]. ACM Transactions on Privacy and Security, 2017, 20(4): 1-31.

[作者简介]

张恩（1974−），男，河南新乡人，博士，河南师范大学副教授、硕士生导师，主要研究方向为密码协议、隐私保护、云计算安全。

裴瑶瑶（1992−），男，河南南阳人，河南师范大学硕士生，主要研究方向为密码协议。

杜蛟（1978−），男，湖北英山人，博士，河南师范大学讲师，主要研究方向为密码学与应用数学。