理想格上支持隐私保护的属性基加密方案

闫玺玺[1]，刘媛[1]，李子臣[2]，汤永利[1]，叶青[1]
（1. 河南理工大学计算机科学与技术学院，河南 焦作 454003；
2. 北京印刷学院信息工程学院，北京 102600）

摘 要：理想格上的加密方案具有密钥尺寸小、加密效率高的优势，利用理想格环上带误差学习（R-LWE, ring learning with error）问题，构造一种可以保护用户属性隐私的属性基加密方案，支持灵活的访问策略，提供用户隐私保护，并且提高方案效率，缩短密钥尺寸。该方案通过采用半策略隐藏方式，保护用户的隐私，从而避免用户的敏感属性值泄露给其他任何第三方。另外，将扩展的 Shamir 门限秘密共享技术应用于构造方案的访问结构，从而实现用户属性的“与”“或”“门限”这 3 种操作，具有更高的灵活性。经安全性分析证明，该方案在标准模型下满足自适应选择明文攻击安全。通过与其他方案的对比，该方案系统公钥、系统私钥、用户私钥长度以及密文长度都有所优化，在实际应用中更加有效。

关键词：属性基加密；理想格；隐私保护；环上带误差学习；访问树
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018048

Privacy-preserving attribute-based encryption scheme on ideal lattices

YAN Xixi[1], LIU Yuan[1], LI Zichen[2], TANG Yongli[1], YE Qing[1]
1.School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China
2. School of Information Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China

Abstract: Based on the small key size and high encryption efficiency on ideal lattices, a privacy-preserving attribute-based encryption scheme on ideal lattices was proposed, which could support flexible access policies and privacy protection for the users. In the scheme, a semi-hidden policy was introduced to protect the users' privacy. Thus, the sensitive values of user's attributes are hidden to prevent from revealing to any third parties. In addition, the extended Shamir secret-sharing schemes was used to construct the access tree structure which can support "and" "or" and "threshold" operations of attributes with a high flexibility. Besides, the scheme was proved to be secure against chosen plaintext attack under the standard mode. Compared to the existing related schemes, the scheme can yield significant performance benefits, especially the size of system public/secret keys, users' secret key and ciphertext. It is more effective in the large scale distributed environment.

Key words: attribute based encryption, ideal lattices, privacy-preserving, R-LWE, access tree

收稿日期：2017-06-06；**修回日期**：2017-12-13
通信作者：汤永利，yltang@hpu.edu.cn
基金项目：国家自然科学基金资助项目（No.61300216）；国家密码管理局“十三五”国家密码发展基金资助项目（No.MMJJ20170122）；河南省教育厅科研基金资助项目（No.16A520013）；河南理工大学博士基金资助项目（No.B2014-044）
Foundation Items: The National Natural Science Foundation of China (No.61300216), The "13th Five-Year" National Crypto Development Foundation(No.MMJJ20170122), The Scientific Research Project of Henan Province (No.16A520013)，Research Fund for the Doctoral Program of Henan Polytechnic University (No.B2014-044)

1　引言

随着互联网的高速发展及云计算的广泛应用，人们喜欢将个人数据外包给云端，但是这些外包给云端的数据中往往包含用户的一些敏感信息，为了防止用户隐私的泄露，经常需要对敏感的隐私信息进行加密处理。属性基加密[1]（ABE, attribute based encryption）机制用一系列的属性来表示用户的身份信息，利用对用户的密钥或密文设置的访问策略或属性集合的匹配程度，来判断解密者的解密能力，可以实现用户外包数据的一对多共享和细粒度访问控制，灵活性和实用性更高。自从 ABE 提出以来，基于各种困难假设和应用环境的 ABE 方案不断被提出，但大多 ABE 方案是以双线性映射为基础的，并不能很好地抵抗量子攻击。而基于格的密码系统具有较高的加密效率、密钥尺寸小、抗量子攻击等特点，成为后量子时代学者们的研究热点。

Ajtai 等[2]利用格理论构造出第一个公钥加密方案，该方案指出解决公钥密码系统中的平均困难问题，与解决公钥密码系统中的最坏困难问题是等价的，但该系统的效率极低。Regev[3]提出格上的带误差学习（LWE, learning with error）问题，本文指出利用 LWE 问题可以构造如基于身份的加密方案和 ABE 方案等公钥加密方案，且构造的公钥加密方案可以在最坏困难问题下抵抗量子攻击。Agrawal 等[4]利用格上 LWE 问题，分别针对大/小身份集合构造出 2 种不同的模糊身份加密方案，并最后证明方案的安全性可规约为 LWE 问题。Boyen[5]利用 LWE 问题构造基于属性的功能加密方案，该方案是一种密钥策略的 ABE 方案，但是方案的访问策略是利用线性秘密共享技术构造的，导致方案中用户的密钥尺寸过大。Liu 等[6]提出一种格上支持“门限”的属性分层加密方案，该方案基于 LWE 问题，并在标准模型下证明满足选择明文攻击（CPA, chosen-plaintext attack）安全。Zhao 等[7]提出格上基于属性的电路加密方案，该方案属于密钥策略 ABE，支持“与”操作并在选择模型下证明满足 LWE 假设。Wang[8]提出标准模型下基于格的密文策略的 ABE 方案，该方案在文献[4]的基础上构造 2 种属性基加密方法，并支持“与”操作。

但是，由于基于 LWE 的密码方案中固有的二次乘法开销，导致系统的效率较低，因此，Lyubashevsky 等[9]提出环上带误差学习（R-LWE, ring learning with error）问题，相较于 LWE 密码体制，具有密钥尺寸小、加密效率高的优势。Zhu 等[10]首次利用理想格上 R-LWE 问题，构造 ABE 方案，该方案的加解密算法设计简单、加解密效率高、密钥尺寸短。随后，Tan 等[11]提出格上基于 R-LWE 问题的密文策略属性基加密方案，采用线性秘密共享技术实现访问策略的控制，并引入密钥随机化技术来抵抗共谋攻击。吴立强等[12]提出理想格上的高效模糊身份加密方案，方案基于理想格上的 R-LWE 问题，并利用用户身份信息的属性集合与加密属性集合足够“相近”时才能解密的思想，构造加密方案，方案可在标准模型下证明其满足选择身份和选择明文攻击安全。孙泽栋等[13]利用 R-LWE 的提出的密钥策略 ABE 方案，可以支持任意长度的属性集合，并满足半适应性安全，另外，方案的最后设计一个编译器，可以将 ABE 方案转化为全同态加密方案。杨海斌[14]利用理想格上的 R-LWE 问题提出一种新的身份分层加密方案，改进理想格上的陷门函数，并利用改进的陷门函数为用户产生私钥，方案的安全性可规约为判定 R-LWE 问题。闫玺玺等[15]提出一种理想格上的多机构属性基加密隐私保护方案，支持多个属性机构管理不同的属性集，并证明其满足自适应选择明文攻击安全。

从上述分析可以看出，格上的 ABE 方案并不成熟，大多方案仅支持“与”操作或“门限”操作，操作方式单一、灵活性不高。另外，大多方案很少考虑用户属性的泄露而导致用户敏感隐私的泄露。例如，在个人健康病例系统中，病人将自己的病例信息保存在云服务器，设置的访问策略如图 1 所示，但在这些属性中，身份证号和科室等都是病人较为敏感的信息，其内容涉及病人隐私，需要提供保护服务。因此，本文在理想格上首次提出一种支持隐私保护的属性基加密方案，主要思想包括 3 点。1) 利用理想格上的 R-LWE 问题构造 ABE 方案，缩短密钥尺寸，提高加密效率。2) 扩展的 Shamir 门限秘密共享技术的灵活运用，可以实现属性的“与”“或”“门限”操作，提高系统的灵活性。3) 采用半策略隐藏方式，将属性分为属性名和属性值 2 个部分，通过对属性名进行加密，将用户的具体属性值隐藏进密文，从而有效保护用户的属性隐私，具体访问策略如图 2 所示。

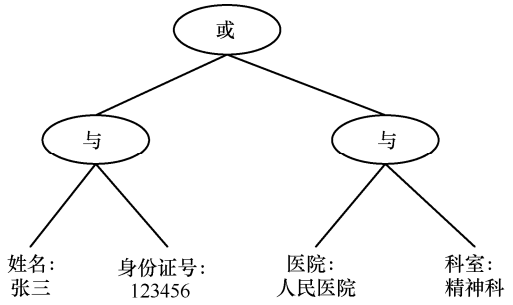

图 1 普通访问策略

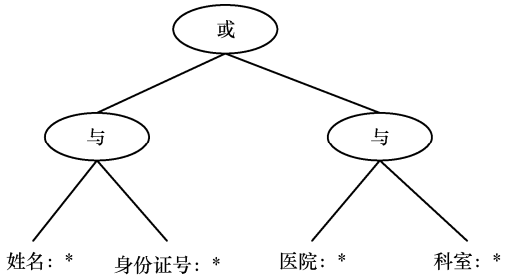

图 2 本文采用的半隐藏访问策略

2 相关知识

2.1 格的相关定义

定义 1 格是由 R^m 中 n 个线性无关的向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 的所有整数线性组合构成的集合，则格 $\Lambda=L(\boldsymbol{B})=\left\{\sum_{i=1}^{n}x_i\boldsymbol{b}_i:x_i\in Z,i=1,\cdots,n\right\}$，其中，$\boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$ 是格基，m 是维数，n 是秩，且满足 $m\geqslant n$，当 $m=n$ 时，则为满秩的格。

定义 2 q-元格。如果格中的每个元素都是整数，则该格为整数格。令 q 是素数，$\boldsymbol{A}\in Z_q^{n\times m}$，$\boldsymbol{u}\in Z_q^n$，定义 q-元格如下

$$\Lambda_q(\boldsymbol{A})=\{\boldsymbol{y}\in Z^m \text{ s.t. } \exists \boldsymbol{s}\in Z_q^n\ \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}=\boldsymbol{y}(\bmod q)\}$$

$$\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{y}\in Z^m \text{ s.t. } \boldsymbol{A}\cdot\boldsymbol{y}=0(\bmod q)\}$$

$$\Lambda_q^{u}(\boldsymbol{A})=\{\boldsymbol{y}\in Z^m \text{ s.t. } \boldsymbol{A}\cdot\boldsymbol{y}=\boldsymbol{u}(\bmod q)\}$$

定义 3 对于以向量 $\boldsymbol{c}$ 为中心、σ 为参数的格 Λ 上的离散高斯分布，定义如下 $D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\dfrac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}=\dfrac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\sum_{\boldsymbol{x}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}$，其中，$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\dfrac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{\sigma^2}\right)$。

定义 4 循环格是指循环移位格上的每个点中的分量，形成新的点还是该格上的点。即对于循环格 $\Lambda\in Z^n$，存在 $\forall(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n)\in\Lambda$，有 $(\boldsymbol{a}_2,\boldsymbol{a}_3,\cdots,\boldsymbol{a}_n,\boldsymbol{a}_1)\in\Lambda$。对循环格上的向量 $\boldsymbol{a}=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n)$ 嵌入多项式系数，得到 $f(x)=\boldsymbol{a}_1+\boldsymbol{a}_2x+\cdots+\boldsymbol{a}_nx^{n-1}$，则循环格对应多项式商环 $\dfrac{Z[x]}{<x^n-1>}$。

定义 5 理想格对应环 $\dfrac{Z[x]}{<f(x)>}$，且其中 $f(x)$ 不可规约。

2.2 困难问题

定义 6 判定性环上误差学习问题（decisional R-LWE$_{d,q,\chi}$）。给定安全参数 λ，令 d、q 为基于 λ 的整数，定义 $R=\dfrac{Z[x]}{f(x)}$ 为模 $f(x)$的整数多项式环，$R_q=\dfrac{Z_q[x]}{f(x)}$ 表示模 $f(x)$和 q 的整数多项式环，其中，$f(x)=x^n+1$。给定基于安全参数 λ 的分布 $\chi\subset R_q$，R-LWE$_{d,q,\chi}$ 问题中有一个指定的挑战模型 $\mathcal{O}$，对于 $s\in R_q$，判定该挑战模型是带噪声的伪随机采样机 $\mathcal{O}_s$ 还是真正的随机采样机 $\mathcal{O}_s'$。$\mathcal{O}_s$ 和 $\mathcal{O}_s'$有以下特征。

$\mathcal{O}_s$：输出伪随机样本，即$(w,v)=(w,ws+e)\in R_q\times R_q$，且样本中含有噪声，其中，$w$ 为环多项式，e 是系数取自离散分布 χ 的噪声，$s\in R_q$ 是一均匀分布的密钥。

$\mathcal{O}_s'$：输出真正的随机采样样品$(w,v)\in R_q\times R_q$。R-LWE$_{d,q,\chi}$ 问题允许敌手 $\mathcal{A}$ 对挑战模型 $\mathcal{O}$ 重复询问，敌手 $\mathcal{A}$ 判定 R-LWE$_{d,q,\chi}$ 问题，如果对于任意 $s\in R_q$，其优势 $Adv[\mathcal{A}]=\left|\Pr\left[\mathcal{A}^{\mathcal{O}_s}=1\right]-\Pr\left[\mathcal{A}^{\mathcal{O}_s'}=1\right]\right|$ 是可忽略的。

2.3 扩展的 Shamir(t,n)门限秘密共享

首先定义拉格朗日系数 $L_{i,S}$，对于 $i\in Z_q$ 和集合 S，有 $L_{i,S}(x)=\prod_{j\in S,j\neq i}\dfrac{x-j}{i-j}$。

扩展的 Shamir 秘密共享方案描述如下。1) 令 $P=\{P_1,P_2,\cdots,P_n\}$ 为参与者集合，t 为门限，$s\in R_q$ 为要分享的秘密。2) 分享者选择 $t-1$ 阶的多项式 $f(x)=s+\sum_{j=1}^{t-1}a_jx^j$，其中，$a_j\in R_q$ 且 $a_j\neq 0$。3) 分享者选择 n 个不同的元素 $x_i\in Z_q^*$，分别为参与者 P_i 计算 $s_i=f(x_i)\in R_q$，并将 (x_i,s_i) 发送给参与者 P_i。4) 任意 t 个用户可以使用拉格朗日插值法重构 s，

已知 $\{(x_i, s_i)\}_{i=1}^{t}$，则 $f(x)=\sum_{i=1}^{t} s_i \prod_{j=1, j\neq i}^{t} \frac{x-x_j}{x_i-x_j}$，令 $X=\{x_i\}_{i=1}^{t}$，所以分享的秘密 $s=f(0)=\sum_{i=1}^{t} s_i \prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i-x_j}=\sum_{i\in X} s_i L_{i,X}(0) \in R_q$。

3　算法定义和安全模型

3.1　算法定义

本文方案包括 4 个算法，即系统初始化算法、密钥生成算法、加密算法和解密算法，具体如下。

1) 系统初始化 Setup(1^{λ})$\rightarrow$(PP, MSK)。该算法由系统执行，以系统的安全参数1^{λ}和系统的属性集合为输入，以系统公共参数 PP 和系统主私钥 MSK 为输出。

2) 密钥生成 KeyGen(PP, MSK, A_{u})$\rightarrow SK_{\mathrm{u}}$。算法由系统中的用户和系统交互执行，以系统公共参数 PP、系统主私钥 MSK 和用户属性集 A_{u} 为输入，以用户私钥 SK_{u} 为输出。

3) 加密 Encrypt(PP, m, (τ, Z))$\rightarrow C$。算法由用户执行，以系统公共参数 PP、明文 m 和访问结构树 (τ, Z) 为输入，以密文 C 为输出。

4) 解密 Decrypt(PP, SK_{u}, C)$\rightarrow m$。算法由用户执行，以系统公共参数 PP、用户私钥 SK_{u} 和密文 C 为输入，以明文 m 为输出。

3.2　安全模型

方案通过执行选择属性和选择明文攻击下的不可区分性（IND-sAtt-CPA, indistinguishability against selective attribute and chosen-plaintext attack）游戏进行安全性证明，游戏共有 2 个参与者，即模拟器 $\mathcal{B}$ 和一个敌手 $\mathcal{A}$，模拟器 $\mathcal{B}$ 通过模拟系统的运行步骤，回答敌手 $\mathcal{A}$ 的询问，具体游戏如下。

Setup　敌手 $\mathcal{A}$ 把它要挑战的访问结构树 (τ^*, Z^*) 发送给模拟器 $\mathcal{B}$；模拟器 $\mathcal{B}$ 负责为敌手 $\mathcal{A}$ 生成系统公共参数 PP 和系统主私钥 MSK，并将其生成的 PP 发送给敌手 $\mathcal{A}$。

Phase 1　敌手 $\mathcal{A}$ 为其不属于访问树 τ^* 的属性集合 S 发出私钥请求。模拟器根据敌手 $\mathcal{A}$ 提交的属性集合为其生成私钥 $SK_{\mathcal{A}}$，并将 $SK_{\mathcal{A}}$ 发送给敌手 $\mathcal{A}$。

Challenge　敌手 $\mathcal{A}$ 随机选择明文比特 $m^* \in \{0,1\}$ 发送给模拟器 $\mathcal{B}$，模拟器 $\mathcal{B}$ 随机选择 $b \in \{0,1\}$，如果 b=0，则模拟器 $\mathcal{B}$ 利用敌手在 Setup 中提交的访问结构树 (τ^*, Z^*) 加密明文比特 m^*，并将生成的挑战密文发送给敌手 $\mathcal{A}$；如果 b=1，则模拟器 $\mathcal{B}$ 将随机生成的发送给敌手 $\mathcal{A}$。

Phase 2　重复 Phase 1。

Guess　敌手 $\mathcal{A}$ 输出对 b 的猜想 b'。

定义本文方案 IND-sAtt-CPA 是安全的，如果对于任意多项式时间的敌手 $\mathcal{A}$，其攻击上述游戏的优势 $\varepsilon=\left|\Pr[b'=b]-\frac{1}{2}\right|$ 是可忽略的。

4　方案构造

本文方案的每个属性由 2 个部分构成：属性名和属性值，假设系统具有 n 个不同的属性名，即 $N=(a_1, a_2, \cdots, a_n)$，其中，$a_i$ 代表属性名。定义每个属性名下有 n_i 个不同的属性值，即每个属性名集合 $A_i=(a_{i,1}, a_{i,2}, \cdots, a_{i,n_i})$，其中，$a_{i,n_i}$ 代表属性名 a_i 下可选择的具体属性值。用户的属性集合为 $A_{\mathrm{u}}=(a_1:a_{1,t_1}, a_2:a_{2,t_2}, \cdots, a_n:a_{n,t_n})$，其中，$a_{i,t_i} \in A_i$，且用户的每个属性名下仅能选择设置一个属性值。本文访问结构用 (τ, Z) 表示，其中，τ 为访问结构树，访问树的叶子节点与加密的访问策略中属性名相对应，$Z=(z_{1,t_1}, \cdots, z_{n,t_n})$ 为加密者指定的属性值，且加密时将 Z 隐藏进密文中，一个解密用户的属性集合满足 (τ, Z)，当且仅当 $a_{i,t_i}=z_{i,t_i}$ 时，可以解密得到明文。

1) 系统初始化

输入安全参数 λ，输出公共参数 PP 和主私钥 MSK。系统随机选择一个大素数 $q=1 \bmod (2\lambda)$ 和一个正整数 p（通常情况下，p=2 或 3），满足 $p \ll q$ 且 $\gcd(p,q)=1$；令 $f(x)=x^n+1 \in Z[x]$，$R_q=\frac{Z_q[x]}{f(x)}$ 表示模 $f(x)$ 和 q 的整数多项式环，$\chi \subset R_q$ 为误差分布；系统随机选择 $a \in R_q$ 和 $sk \in R_q$，选择均匀随机误差项 $e \in \chi$，令 $pk=a \cdot sk+pe \in R_q$；对系统中每个属性名 a_i，随机选择 $(sk_i, sk_i^{-1}) \in R_q$ 和误差项 $e_i \in \chi$，计算 $pk_i=a \cdot sk_i^{-1}+pe_i \in R_q$。则 $PP=\{p, a, pk, (pk_i)_{\forall a_i}\}$，$MSK=\{sk, (sk_i, sk_i^{-1})_{\forall a_i}\}$

2) 密钥生成

该算法由用户与系统进行交互，输入用户的属性集 A_{u}、系统公共参数 PP 和系统主私钥 MSK，输出用户的私钥 SK_{u}。系统首先随机选择 $e' \in \chi$，计算 $D=sk+pe' \in R_q$，然后检查用户的属性值 a_{i,t_i} 是属

于哪个属性名 a_i 下的属性值，最后选择均匀随机误差项 $e_{i,t_i}' \in \chi$，计算 $D_{i,t_i}=sk_i a_{i,t_i}+pe_{i,t_i}' \in R_q$。则用户私钥 $SK_u=\left\{D,\left(D_{i,t_i}\right)_{(1\leqslant i\leqslant n)}\right\}$。

3) 加密

该算法由加密者执行，输入系统的公钥、明文 $m\in\{0,1\}^n$ 和加密者设置的访问结构 (τ,Z)，输出密文 C。其中，τ 为访问结构树，$Z=\left(z_{1,t_i},\cdots,z_{n,t_n}\right)$ 为访问结构中的属性值。

①利用扩展的 Shamir 门限秘密共享技术构造访问树，将叶子节点与加密者设置的属性名 a_i 相对应，其中，$a_i\in\tau$，且令 l 为访问树中叶子节点的属性名索引。秘密共享如下。随机选取环元素 $s\in R_q$，设置访问树根节点为 s，并标记该节点已分配，其孩子节点标记为未分配，对所有未分配的非叶子节点做以下操作。若操作符为 $\vee$，且其孩子节点未分配，则为其孩子节点赋值为环元素 s，并标记已分配；若操作符为 $\wedge$，且其孩子节点未分配，则随机选择环元素 $s_l\in R_q\ (j=1,2,\cdots,n-1)$，其中，$n$ 为其孩子节点个数，第 n 个孩子节点赋值为环元素 $s_n=s-\sum_{l=1}^{n-1}s_l$，并标记已分配；若操作符为 of，且其孩子节点未分配，则随机选取 $t-1$ 阶的多项式 $f(x)=s+\sum_{j=1}^{t-1}a_j x^j$，利用 Shamir$(t,n)$ 门限秘密共享技术对 $s\in R_q$ 进行分割，其中，t 为门限值，n 为孩子节点数，则其孩子节点 l 赋值为环元素 $s_l=f(l)$，并标记为已分配。

②访问结构中的属性值 $Z=\left(z_{1,t_i},\cdots,z_{n,t_n}\right)$ 隐藏进密文中。随机选择 $r\in R_q$ 和误差项 $e",e_{i,l}"\in\chi$，计算 $C_0=pk\cdot r\cdot s+m+pe"\in R_q$，$C_{i,l}=pk_i\cdot r\cdot s_l\cdot z_{i,t_i}^{-1}+pe_{i,l}"\in R_q$。

则密文 $C=\left\{C_0,\left(C_{i,l}\right)_{\forall a_i\in\tau}\right\}$。

4) 解密

该算法输入密文 C、用户密钥 SK_u 及用户属性值 a_{i,t_i}，输出明文 m。解密时，系统首先检查用户的属性名是否满足访问树，然后利用用户的属性值进行解密。即计算 $m'=C_0-D\sum_{a_{i,l}\in I_A}L_l C_{i,l}D_{i,t_i}$，其中，$L_l$ 为拉格朗日系数，I_A 为解密属性集。则 $m=m'\bmod p$。

5 方案分析

5.1 正确性

$$
\begin{aligned}
m'&=C_0-D\sum_{a_{i,l}\in I_A}L_l C_{i,l}D_{i,t_i}\\
&=C_0-D\sum_{a_{i,l}\in I_A}L_l\left(pk_i\cdot r\cdot s_l\cdot z_{i,t_i}^{-1}+pe_{i,l}"\right)D_{i,t_i}\\
&=C_0-D\left(pk_i\cdot r\cdot s\cdot z_{i,t_i}^{-1}D_{i,t_i}\right)-pD\sum_{a_{i,l}\in I_A}\left(L_l e_{i,l}"D_{i,t_i}\right)\\
&=C_0-D\left[\left(a\cdot sk_i^{-1}+pe_i\right)\cdot r\cdot s\cdot z_{i,t_i}^{-1}D_{i,t_i}\right]-\\
&\quad pD\sum_{a_{i,l}\in I_A}\left(L_l e_{i,l}"D_{i,t_i}\right)\\
&=C_0-D\left(a\cdot sk_i^{-1}\cdot r\cdot s\cdot z_{i,t_i}^{-1}D_{i,t_i}+pe_i\cdot r\cdot s\cdot z_{i,t_i}^{-1}D_{i,t_i}\right)-\\
&\quad pD\sum_{a_{i,l}\in I_A}\left(L_l e_{i,l}"D_{i,t_i}\right)\\
&=C_0-D\left[a\cdot sk_i^{-1}\cdot r\cdot s\cdot z_{i,t_i}^{-1}\left(sk_i\cdot a_{i,t_i}+pe_{i,t_i}'\right)\right]-\\
&\quad pDrsz_{i,t_i}^{-1}D_{i,t_i}e_i-pD\sum_{a_{i,l}\in I_A}\left(L_l e_{i,l}"D_{i,t_i}\right)\\
&=C_0-arsD-parsDe_{i,t_i}'sk_i^{-1}z_{i,t_i}^{-1}-pDrsz_{i,t_i}^{-1}D_{i,t_i}e_i-\\
&\quad pD\sum_{a_{i,l}\in I_A}\left(L_l e_{i,l}"D_{i,t_i}\right)\\
&=pk\cdot r\cdot s+m+pe"-ars\left(sk+pe'\right)-parsDe_{i,t_i}'sk_i^{-1}z_{i,t_i}^{-1}-\\
&\quad pDrsz_{i,t_i}^{-1}D_{i,t_i}e_i-pD\sum_{a_{i,l}\in I_A}\left(L_l e_{i,l}"D_{i,t_i}\right)\\
&=\left(a\cdot sk+pe\right)\cdot r\cdot s+m+pe"-ars\left(sk+pe'\right)-\\
&\quad parsDe_{i,t_i}'sk_i^{-1}z_{i,t_i}^{-1}-pDrsz_{i,t_i}^{-1}D_{i,t_i}e_i-\\
&\quad pD\sum_{a_{i,l}\in I_A}\left(L_l e_{i,l}"D_{i,t_i}\right)\\
&=m+prse+p\left(e"-e'\right)-parsDe_{i,t_i}'sk_i^{-1}z_{i,t_i}^{-1}-\\
&\quad pDrsz_{i,t_i}^{-1}D_{i,t_i}e_i-pD\sum_{a_{i,l}\in I_A}\left(L_l e_{i,l}"D_{i,t_i}\right)
\end{aligned}
$$

所以有 $m=m'\bmod p$。

5.2 安全性证明

定理 1 如果存在一个任意多项式时间的敌手 $\mathcal{A}$ 以优势 ε 攻击选择属性和选择明文攻击下的不可区分性游戏，则存在模拟器 $\mathcal{B}$ 以优势 $\frac{\varepsilon}{2}$ 判定 R-LWE 问题。

证明 R-LWE 问题实例中，对于主私钥 $sk\in R_q$，模拟器 $\mathcal{B}$ 通过与敌手 $\mathcal{A}$ 进行 IND-sAtt-CPA 游戏，从而区别采样预言机 $\mathcal{O}$ 是真正的随机预言机 $\mathcal{O}_s'$ 还是带噪声的伪随机预言机 $\mathcal{O}_s$，游戏运行如下。

Setup

1) 模拟器 $\mathcal{B}$ 请求一个有 R-LWE 问题提供的采样预言机 $\mathcal{O}$ 并获得 $m+1$ 个 LWE 采样样品 $(\omega_k,v_k)\in R_q\times R_q$，其中，$k\in\{0,1,\cdots,m\}$。

2) 敌手 $\mathcal{A}$ 提交要挑战的访问结构树 (τ^*, Z^*)，其中，$Z^*=(z^*_{1,t_1},\cdots,z^*_{n,t_n})$ 为敌手指定的属性值。

3) 模拟器 $\mathcal{B}$ 运行系统初始化算法生成系统公共参数 *PP* 和主私钥 *MSK*，定义 $pk=p\omega_0\in R_q$；模拟器 $\mathcal{B}$ 对系统中每个属性名 a_i，随机选择 $(sk_i, sk_i^{-1})\in R_q$，若敌手的属性名 $a_i\in\tau^*$，计算 $pk_i=a\cdot sk_i^{-1}+pe_i\in R_q$，若敌手的属性名 $a_i\notin\tau^*$，定义 $pk_i=p\omega_i\in R_q$，然后模拟器 $\mathcal{B}$ 将公共参数 $PP=\{a, pk, (pk_i)_{\forall a_i}\}$ 发送给敌手 $\mathcal{A}$。

Phase 1

1) 敌手 $\mathcal{A}$ 为其属性集合 $S=(a_i:a_{i,t_i})$ 询问私钥，定义 *S* 不属于访问树，其中，$a_{i,t_i}\in A_i$。

2) 模拟器 $\mathcal{B}$ 首先计算 $D=sk+pe'\in R_q$；对于敌手提交的属性集合，模拟器 $\mathcal{B}$ 检查该属性集合，并运行密钥生成算法，对于集合中的每个属性值 a_{i,t_i}，计算 $D_{i,t_i}=sk_i\cdot a_{i,t_i}+pe_{i,t_i}'\in R_q$。模拟器 $\mathcal{B}$ 将敌手 $\mathcal{A}$ 的私钥 $SK_{\mathcal{A}}=\left\{D,\left(D_{i,t_i}\right)_{(1\leqslant i\leqslant n)}\right\}$ 发送给敌手。

Challenge

1) 敌手 $\mathcal{A}$ 随机选择明文比特串 $m^*\in\{0,1\}^n$ 发送给模拟器 $\mathcal{B}$。

2) 模拟器 $\mathcal{B}$ 随机选取环元素 $s^*\in R_q$，设置访问树根节点为 s^*，并标记该节点已分配，其孩子节点标记为未分配，对所有未分配的非叶子节点做以下操作：若操作符为 $\vee$，且其孩子节点未分配，则为其孩子节点赋值为环元素 s^*，并标记已分配；若操作符为 $\wedge$，且其孩子节点未分配，则随机选择环元素 $s_l^*\in R_q\,(l=1,2,\cdots,n-1)$，其中，*n* 为其孩子节点个数，第 *n* 个孩子节点赋值为环元素 $s_n^*=s-\sum_{l=1}^{n-1}s_l^*$，并标记已分配；若操作符为 *of*，且其孩子节点未分配，则随机选取 $t-1$ 阶的多项式，利用扩展的 Shamir(t,n) 门限秘密共享技术对 $s^*\in R_q$ 进行分割，其中，*t* 为门限值，*n* 为孩子节点数，则其孩子节点 *l* 赋值为环元素 $s_l^*\in R_q$，并标记为已分配。令 $v_0=\omega_0 s^*+e$，$v_i=\omega_i s_l^*+e_i$，模拟器 $\mathcal{B}$ 令 $v_0, v_1,\cdots, v_m$ 作为 R-LWE 实例的输入，计算 $C_0^*=pv_0+m^*\in R_q$，$C_{i,l}^*=pv_i\in R_q$。

3) 模拟器 $\mathcal{B}$ 随机选择 $b\in\{0,1\}$，如果 *b*=0，则模拟器 $\mathcal{B}$ 将其计算得到的挑战密文 $C=\left\{C_0^*,\left(C_{i,l}^*\right)_{a_i\in\tau^*}\right\}$ 发送给敌手 $\mathcal{A}$；如果 *b*=1，则模拟器 $\mathcal{B}$ 随机选择挑战密文 $C_0^*, C_{i,l}^*\in R_q$，并将随机生成的挑战密文 $C=\left\{C_0^*,\left(C_{i,l}^*\right)_{a_i\in\tau^*}\right\}$ 发送给 $\mathcal{A}$。

Phase 2

模拟器 $\mathcal{B}$ 重复 Phase 1。

Guess

模拟器 $\mathcal{B}$ 通过输出敌手 $\mathcal{A}$ 对 *b* 的猜想 b'，如果 $b'=b$，则输出 $\mathcal{O}=\mathcal{O}_s$，此时，敌手的优势 $\Pr[b'=b\,|\,\mathcal{O}=\mathcal{O}_s]=\frac{1}{2}+\varepsilon$；如果 $b'\neq b$，则输出 $\mathcal{O}=\mathcal{O}_s'$，此时，敌手的优势 $\Pr\left[b'\neq b\,|\,\mathcal{O}=\mathcal{O}_s'\right]=\frac{1}{2}$。

因此，敌手 $\mathcal{A}$ 区分密文 $C=\left\{C_0^*,\left(C_{i,l}^*\right)_{a_i\in\tau^*}\right\}$ 和 $R_q\times R_q$ 上的均匀随机分布的优势 $Adv_{\mathcal{A}}=\frac{1}{2}\Pr[b'=b\,|\,\mathcal{O}=\mathcal{O}_s]+\frac{1}{2}\Pr[b'=b\,|\,\mathcal{O}=\mathcal{O}_s']-\frac{1}{2}=\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\left(\frac{1}{2}+\varepsilon\right)-\frac{1}{2}=\frac{1}{2}\varepsilon$，且其优势是可忽略的，则任何多项式时间内敌手赢得 IND-sAtt-CPA 游戏的优势是可忽略的。

5.3　隐私保护分析

传统的 ABE 方案大多通过保护用户唯一的 GID 来保护用户的隐私，而很少考虑到用户其他属性泄露导致的隐私泄露问题；本文将用户的属性分为属性名和属性值 2 个部分，令$(a_1,a_2,\cdots,a_n)$表示系统的 *n* 个不同的属性名，每个属性名下有 n_i 个不同的属性值，即每个属性名集合 $A_i=(a_{i,1},a_{i,2},\cdots,a_{i,n_i})$，其中，$a_{i,n_i}$ 代表属性名 a_i 下可选择的具体属性值，定义用户的每个属性名下仅能选择设置一个属性值。加密时，加密者将访问树的每个叶子节点与设置的属性名 a_i 相对应，而将其具体的属性值 a_{i,n_i} 隐藏进密文中，这样，即使攻击者得到加密者的密文数据，仍不能得到任何加密者的具体的属性值，从而保护加密者的所有属性隐私。

5.4　性能分析

本文从系统公钥大小、系统私钥大小、用户私钥大小、密文大小、明文长度、密文膨胀率、是否提供隐私保护和支持访问策略等几个方面对相关方案进行比较，具体结果如表 1 所示。其中，*q* 为素数，*n* 为正整数，$m\geqslant 5n\log q$，*q*、*n*、*m* 为引理 2 中格上的相关参数，*N* 为系统属性总数，A_u 为

用户属性个数，A_c 为加密属性个数。

从表 1 可以看出，本文支持对用户的所有属性隐私的保护，而其他方案并不提供隐私保护功能；本文方案采用访问树结构支持属性的“与”“或”“门限”这 3 种操作，而文献[8]仅支持“与”操作，文献[10,12]支持“门限”操作，方式单一，灵活性较低。

性能方面，本文方案比其他方案整体相对更优。本文的系统公钥大小远远小于文献[8,12]，只比文献[10]多一个 R_q 元素，即 $n\log q$ 。系统私钥方面，文献[8,12]构造复杂，存储代价较大，本文方案系统私钥比文献[10]减少一个 R_q 元素，即 $n\log q$ ，达到优化。用户私钥方面，文献[8,12]中用户私钥均是由级联矩阵通过格上的原像采样函数生成的，用户私钥大小与级联矩阵的列数和用户的属性个数相关，而本文和文献[10]的用户私钥大小是通过对环多项式计算得到的，远远小于文献[8,12]。密文大小方面，文献[8,10]的密文大小同样与级联矩阵列数和加密设置的密文属性个数相关，而本文方案与文献[10]的密文大小仅与用户加密的属性个数相关，密文尺寸远小于文献[8,12]。文献[8]一次仅能加密单比特明文，而本文和文献[10,12]一次可以加密 n bit 的明文，加密效率高。密文膨胀率方面，本文和文献[10]的密文膨胀率相同，远小于文献[8,12]。

综合分析，本文方案支持用户的所有属性隐私的保护，同时采用访问树结构支持属性的“与”“或”“门限”这 3 种操作，提高系统的灵活性与安全性。另外，方案在系统公私钥、用户密钥和密文大小方面都有所优化，加密效率高，密文膨胀率低，在实际应用中更加有效。

6 结束语

本文利用理想格上的 R-LWE 问题构造 ABE 方案，解决数据外包环境下外包数据中用户的属性隐私泄露问题，相比于标准格上 ABE 方案中只能加密单个比特明文数据，本文可加密 n bit 的明文，既提高系统的加密效率，又减小密钥长度和密文长度。同时，利用扩展的 Shamir 门限秘密共享机制设置访问策略，实现属性的“与”“或”“门限”这 3 种操作，增加系统的灵活性。另外，将用户的属性分成 2 个部分：属性名和属性值，加密时使用属性名进行加密，而将属性值隐藏，从而保护用户的具体属性值不被泄露给任何第三方。实际应用中用户将加密数据存储在云服务器中，有时会根据需要撤销某些属性，下一步将对格上用户属性的即时撤销方案进行研究。

表 1　　**相关方案对比**

方案	系统公钥大小	系统私钥大小	用户私钥大小	密文大小	明文长度	密文膨胀率	隐私保护	支持操作
文献[8]方案	$n(3m+N+1)\log q$	$mm\log q$	$2mA_u$	$(2mA_c+1)\log q$	1	$(2mA_c+1)\log q$	×	与
文献[10]方案	$n(N+1)\log q$	$n(2N+2)\log q$	$(nA_u)\log q$	$n(A_c+1)\log q$	n	$(A_c+1)\log q$	×	门限
文献[12]方案	$n(3mN+1)\log q$	$Nm^2n^2\log q$	$2mnA_u$	$n(2mA_c+1)\log q$	n	$(2mA_c+1)\log q$	×	门限
本文方案	$n(N+2)\log q$	$n(2N+1)\log q$	$(nA_u+n)\log q$	$n(A_c+1)\log q$	n	$(A_c+1)\log q$	√	与、或、门限

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology-EUROCRYPT. 2005: 457-473.

[2] AJTAI M, DWORK C. A public-key cryptosystem with worst-case/average-case equivalence[C]//ACM Symposium on Theory of Computing(STOC). 1997:284-293.

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

[4] AGRAWAL S, BOYEN X, VAIKUNTANATHAN V, et al. Functional encryption for threshold functions (or fuzzy IBE) from lattices[C]//International Conference on Practice and Theory in Public Key Cryptography. 2012:280-297.

[5] BOYEN X. Attribute-based functional encryption on lattices[C]//The 10th Theory of Cryptography Conference, Lecture Notes in Computer Science. 2013: 122-142.

[6] LIU X M, MA J F, XIONG J B, et al. Threshold attribute-based encryption with attribute hierarchy for lattices in the standard model[J]. IET Information Security, 2014, 8(4):217-223.

[7] ZHAO J, GAO H Y, ZHANG J Q. Attribute-based encryption for circuits on lattices[J]. Tsinghua Science and Technology, 2014, 45(5):463-469.

[8] WANG Y T. Lattice ciphertext policy attribute-based encryption in the standard model[J]. International Journal of Network Security, 2014, 16(6):444-451.

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

[10] ZHU W L , YU J P, ZHANG P, et al. Efficient attribute-based encryption

from R-LWE[J]. Chinese Journal of Electronics, 2014, 23(4): 778-782.

[11] 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.

[12] 吴立强, 杨晓元, 韩益亮. 基于理想格的高效模糊身份加密方案[J]. 计算机学报, 2015, 38(4):775-782.
WU L Q, YANG X Y, HAN Y L. An efficient FIBE scheme based on ideal lattices[J]. Chinese Journal of Computers, 2015, 38(4):775-782.

[13] 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(Z1): 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(Z1): 125-131.

[14] 杨海斌. 一种新的格上基于身份的分层加密方案[J]. 武汉大学学报（理学版）, 2016, 62(2):155-160.
YANG H B. A new hierarchical identity-based encryption scheme based on lattices[J]. Journal of Wuhan University (Nature Science Edition), 2016, 62(2):155-160.

[15] 闫玺玺, 刘媛, 李子臣, 等. 云环境下理想格上的多机构属性基加密隐私保护方案[J]. 信息网络安全, 2017(8): 19-25.
YAN X X, LIU Y, LI Z C, et al. A privacy-preserving multi-authority attribute encryption scheme on ideal lattices in the cloud environment[J]. Netinfo Security, 2017(8): 19-25.

[作者简介]

闫玺玺（1985-），女，河南灵宝人，博士，河南理工大学副教授、硕士生导师，主要研究方向为网络与信息安全、数字版权管理、数字内容安全和密码学。

刘媛（1989-），女，河南濮阳人，河南理工大学硕士生，主要研究方向为密码学、网络与信息安全。

李子臣（1965-），男，河南温县人，北京印刷学院教授、博士生导师，主要研究方向为信息安全、电子商务和密码学。

汤永利（1972-），男，河南焦作人，博士后，河南理工大学教授、硕士生导师，主要研究方向为密码学算法检测、网络与信息安全。

叶青（1981-），女，辽宁营口人，博士，河南理工大学讲师、硕士生导师，主要研究方向为密码学和数字签名。