基于理想格的高效密文策略属性基加密方案

赵 建* 高海英 胡 斌
(解放军信息工程大学 郑州 450001)

摘 要：已有的基于格的密文策略属性基(CP-ABE)方案只能通过矩阵运算方法进行加解密，加解密效率不高，而效率较高的基于理想格的密钥策略属性基(KP-ABE)方案又存在对各类实际应用场景适应性较差的问题。为解决上述问题，该文利用理想格上的算法生成主密钥和密钥，同时在多项式环上进行运算，极大地提高了加解密效率；通过在原属性集合中添加虚拟属性，方案成功结合访问结构生成密文，同时授权用户可以构建出满足解密条件的子集，从而实现方案的正确解密；还利用单个陷门矩阵生成密钥，有效降低了公共参数和主密钥的数量。最终该文构建了一个基于理想格的支持门限访问结构的高效 CP-ABE 方案，并证明方案在环上容错学习(R-LWE)假设下是选择性安全的。与现有支持门限访问结构的方案的对比分析表明，该文方案公共参数数量更少、效率更高，且对实际应用场景有更好的适应性。

关键词：属性基加密方案；密文策略；理想格；环上容错学习
中图分类号： TP309.7 **文献标识码**： A **文章编号**： 1009-5896(2018)07-1652-09
DOI: 10.11999/JEIT170863

An Efficient Ciphertext-policy Attribute-based Encryption on Ideal Lattices

ZHAO Jian GAO Haiying HU Bin
(*The PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: The existing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) schemes from lattices are inefficient while they are performed in matrix operation, and these Key-Policy Attribute-Based Encryption (KP-ABE) schemes from ideal lattices with higher efficiency are inadaptable to most practical application scenarios. To solve these problems, the new scheme generates master keys and secret keys by the algorithms based on ideal lattices and the whole scheme is computed over a polynomial ring, thus its efficiency of encryption and decryption can be greatly improved. The ciphertexts associated with access structure are successfully generated by adding some virtual attributes to the original attribute set. Meanwhile, the authorized user can build a subset based on these virtual attributes for decrypting the scheme correctly. And the secret keys are generated by a single trapdoor matrix, which reduces the number of public parameters and master keys effectively. Finally, an efficient CP-ABE scheme for flexible threshold access structures on ideal lattices is proposed, and its security is reduced to decisional Learning With Errors over Ring (R-LWE) assumption against chosen plaintext attack in the selective security model. Comparative analysis of similar schemes shows that the new scheme has less public parameters and higher efficiency, and gets better adaptability to the practical application scenarios.

Key words: Attribute-Based Encryption (ABE); Ciphertext-policy; Ideal lattices; Learning With Errors over Ring (R-LWE)

1 引言

基于属性的加密体制(Attribute-Based Encryption, ABE)是由 Sahai 等人[1]在 2005 年提出的概念。在一个 ABE 方案中，用户的身份用一组描述性的属性来表示，同时置入一个灵活的访问结构，可以实现对加密数据的细粒度访问控制。

根据加密策略类型的不同，现有的属性基加密方案可以分为两种基本类型[2]：密钥策略方案(Key-Policy Attribute-Based Encryption, KP-ABE)和密文策略方案(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)。KP-ABE 中，密文与属性

收稿日期：2017-09-16；改回日期：2018-03-14；网络出版：2018-04-10
*通信作者：赵建 back_zj@126.com
基金项目：国家自然科学基金(61702548, 61601515)，河南省基础与前沿技术课题(162300410192)
Foundation Items: The National Natural Science Foundation of China (61702548, 61601515), The Fundamental and Frontier Technology Research of Henan Province (162300410192)

关联，密钥与访问结构关联；CP-ABE 中，密文与访问结构相关联，密钥与属性相关联。但在两类方案中，都是当属性集合满足访问结构时，解密者才能正确解密。KP-ABE 方案比较适合对特定的静态数据进行访问控制的情况，在增加新用户或增加用户访问权限方面有优势[3]。而 CP-ABE 方案更适用于实现对任意数据的动态访问控制，由加密者控制消息的解密权限，更接近于现实生活中的实际应用[4]。

早期 ABE 体制主要基于双线性映射上的困难问题，但由于这些困难问题不能抵抗量子攻击，所以这类方案在后量子时代的发展比较受限。Ajtai[5]于 1996 年给出了构造一类随机格的方法，随后开始不断出现基于格的基于身份的加密体制(Identity-Based Encryption, IBE)[6,7]及基于格的 ABE 加密体制。此外，近年来格也广泛应用于各类同态加密方案中[8]。基于格的密码体制优势十分明显，由于其运算具有线性特性，所以体制具有更快的执行效率，且格密码体制可以抵抗量子攻击。

2010 年，Lyubashevsky 等人[9]首次提出环上容错学习(Learning With Errors over Ring, R-LWE)的概念，并将 R-LWE 问题的困难性规约到理想格上的近似最短向量问题。基于理想格构造的密码方案优势明显，该密码体制具有较短的密文和密钥。2013 年，Lyubashevsky 等人[10]给出了 R-LWE 上一系列实用化算法和分析工具，极大地推动了基于 R-LWE 密码体制的实用化发展。2015 年，吴立强等人[11]提出了一个基于理想格的高效 FIBE 方案，该方案可看作是一个 KP-ABE 方案，方案支持门限访问结构。虽然该方案具有公钥长度短、密文扩展率低的优势，但其公共参数数量较大。

在现有的格基 ABE 方案中，绝大多数是 KP-ABE 方案，CP-ABE 方案相对较少。与格基 ABE 方案的情况不同，基于双线性映射的 ABE 方案有大量的密文策略方案[12–15]，且支持的访问结构也非常灵活。早在 2012 年，Zhang 等人[16]提出了支持门限访问结构的基于格的 CP-ABE 方案，之后格基 CP-ABE 方案支持的访问结构并没有太大发展，而且该方案加解密过程均采用矩阵运算，方案加解密效率有待提升。

针对上述情况，本文提出了一个支持门限访问结构的基于理想格的 CP-ABE 方案。新方案可实现多比特明文消息的同时加密，且加解密过程都在多项式环上进行，通过快速傅里叶变换(Fast Fourier Transform, FFT)大幅度提高加解密速度，实现效率高。与同类基于理想格的 KP-ABE 方案相比，新方案公共参数数量降低了大约 $1/3$，主密钥数量降低了 $|\mathcal{R}|$ 倍，且新方案支持密文策略结构，对实际应用场景有更广泛的适应性。新方案在加密等长明文消息时，产生的密钥数量与文献[16](密文策略方案的最佳水平)相同，比文献[11](密钥策略方案)扩大约 1 倍。

本文的组织结构如下：第 2 节中介绍基于理想格的属性基加密方案的基础知识；第 3 节给出新构建的支持门限访问结构的基于理想格的 CP-ABE 方案；第 4 节分析新方案的正确性；第 5 节证明新方案的安全性；第 6 节给出方案对比分析，并总结全文。

2　基础知识

2.1 符号与基本定义

本节主要介绍文中用到的一些符号的意义及格相关的基本定义，我们以列表的形式介绍文中涉及的符号定义。具体如表 1 所示。

乘法运算：文中用到了环多项式向量 $\hat{\boldsymbol{x}}=(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_m)^{\mathrm{T}}\in R^m$ 的两种乘法运算，具体定义如式(1)：

$$\hat{\boldsymbol{x}}\boldsymbol{y}=(\boldsymbol{x}_1\boldsymbol{y},\boldsymbol{x}_2\boldsymbol{y},\cdots,\boldsymbol{x}_m\boldsymbol{y})^{\mathrm{T}}\in R^m,\ \hat{\boldsymbol{x}}\in R^m,\ \boldsymbol{y}\in R,$$
$$\hat{\boldsymbol{x}}\otimes\hat{\boldsymbol{y}}=\sum_{i=1}^{m}\boldsymbol{x}_i\boldsymbol{y}_i\in R,\ \hat{\boldsymbol{x}}\in R^m,\ \hat{\boldsymbol{y}}\in R^m \tag{1}$$

表 1 符号定义

符号	意义	符号	意义
粗体小写 $\boldsymbol{a}$	列向量 $\boldsymbol{a}$	$\mathbb{Z}[x]$	整数系数多项式集合
粗体大写 $\boldsymbol{A}$	矩阵 $\boldsymbol{A}$	$\mathbb{R}[x]$	实数系数多项式集合
$\boldsymbol{A}^{\mathrm{T}}$	矩阵 $\boldsymbol{A}$ 的转置	$R=\mathbb{Z}[x]/\langle f(x)\rangle$	模 $f(x)$ 的多项式环
花体字母 $\mathcal{R}$	(属性)集合 $\mathcal{R}$	$R_q=\mathbb{Z}_q[x]/\langle f(x)\rangle$	模 $f(x)$ 且系数在 $\mathbb{Z}_q$ 上的多项式环
$\mathbb{Z}$	整数域	R^m	m 长的环多项式向量集合
$\mathbb{Z}_q$	模 q 的剩余类环	$\hat{\boldsymbol{x}}=(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_m)^{\mathrm{T}}$	m 长的环多项式向量
$\mathbb{Z}^{n\times m}$	$n\times m$ 整数矩阵集合	$i\in[l]$	$1\le i\le l$, i 是整数
$\mathbb{R}$	实数域	$\lfloor q/2\rfloor$	对 $q/2$ 下取整

整数格[17]：设 q 为素数，$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\boldsymbol{u}\in\mathbb{Z}_q^n$，如式(2)定义整数格：

$$\left.\begin{aligned}\Lambda_q(\boldsymbol{A})&=\left\{\boldsymbol{e}\in\mathbb{Z}^m\ \text{ s.t. }\exists\boldsymbol{s}\in\mathbb{Z}_q^n,\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}=\boldsymbol{e}(\bmod q)\right\}\\ \Lambda_q^{\perp}(\boldsymbol{A})&=\left\{\boldsymbol{e}\in\mathbb{Z}^m\ \text{ s.t. }\boldsymbol{A}\boldsymbol{e}=\boldsymbol{0}(\bmod q)\right\}\\ \Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})&=\left\{\boldsymbol{e}\in\mathbb{Z}^m\ \text{ s.t. }\boldsymbol{A}\boldsymbol{e}=\boldsymbol{u}(\bmod q)\right\}\end{aligned}\right\}\tag{2}$$

离散高斯分布[17]：现有正整数 m，格 $\Lambda\in\mathbb{R}^m$。任取向量 $\boldsymbol{c}\in\mathbb{R}^m$ 和正数 $\sigma\in\mathbb{R}$，定义 $\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/\sigma^2\right)$ 为 $\mathbb{R}^m$ 上的高斯型函数，其中心为 $\boldsymbol{c}$，参数为 σ；定义 $\rho_{\sigma,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})$ 为格 Λ 上 $\rho_{\sigma,\boldsymbol{c}}$ 的离散积分；$D_{\Lambda,\sigma,\boldsymbol{c}}$（$\boldsymbol{c}=\boldsymbol{0}$ 时也记作 $D_{\Lambda,\sigma}$）为格 Λ 上中心为 $\boldsymbol{c}$，参数为 σ 的高斯分布，其中，

$$\forall\boldsymbol{y}\in\Lambda,\ D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{y})=\frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{y})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}\tag{3}$$

2.2 R-LWE 假定[11]

设 $f(x)=x^n+1\in\mathbb{Z}[x]$，$p\in\mathbb{Z}$，$n=2^p$，素数 $q\geq 2$，已知一个特定的离散噪声分布为 $\mathcal{X}=D_{\mathbb{Z}_{-q},\delta}$（定义 $\mathcal{X}_{\max}$ 是分布中所有向量 Euclidean 范数的上确界，即在分布中任取一个向量 $\boldsymbol{x}$，都有 $\|\boldsymbol{x}\|\leq\mathcal{X}_{\max}$）。现有一个未确定的挑战预言机 $\mathcal{O}$，这个预言机的可能输出形如 $(\boldsymbol{w},\boldsymbol{v})=(\boldsymbol{w},\boldsymbol{w}\boldsymbol{s}+\boldsymbol{x})\in R_q\times R_q$ 的伪随机取样，其中，$\boldsymbol{w}\in R_q$ 是均匀分布的环多项式向量，$\boldsymbol{s}$ 是在 R_q 中选定的随机环多项式向量，$\boldsymbol{x}$ 是取自分布 $\mathcal{X}$ 的噪声向量，此时记预言机为 $\mathcal{O}_{\boldsymbol{s}}$。这个预言机也可能输出形如 $(\boldsymbol{w},\boldsymbol{v})$ 的取自均匀分布 $R_q\times R_q$ 的完全随机取样，此时记预言机为 $\mathcal{O}_{\$}$。

判定性 R-LWE 问题就是指算法根据多项式时间大小数目的取样，判定预言机为 $\mathcal{O}_{\boldsymbol{s}}$ 或 $\mathcal{O}_{\$}$。一个敌手 $\mathcal{A}$ 能够判定 R-LWE 问题的优势为

$$\mathrm{Adv}(\mathcal{A})=\left|\Pr\left[\mathcal{A}^{\mathcal{O}_{\boldsymbol{s}}}=1\right]-\Pr\left[\mathcal{A}^{\mathcal{O}_{\$}}=1\right]\right|\tag{4}$$

如果 $\mathrm{Adv}(\mathcal{A})$ 的大小是不可忽略的，就可以称敌手 $\mathcal{A}$ 能够解决判定性 R-LWE 问题。

2.3 形式化定义和安全模型[16]

定义 1 支持 $(\mathcal{W},t)$ 门限访问结构的 CP-ABE 方案一般由 Setup, KeyGen, Enc 和 Dec 4 个算法组成，下面分别介绍这 4 个算法：

$\mathrm{Setup}\left(1^{\lambda},r,d\right)\rightarrow(\mathrm{pk},\mathrm{msk})$：算法以安全参数 λ，系统中所有属性个数 r 和虚拟属性的个数 d 为输入；算法输出公钥 pk 和主密钥 msk。

$\mathrm{KeyGen}(\mathrm{pk},\mathrm{msk},\mathcal{S})\rightarrow\mathrm{sk}$：算法以公钥 pk、主密钥 msk 和用户的属性集合 $\mathcal{S}$ 为输入；算法输出密钥 sk。

$\mathrm{Enc}(\mathrm{pk},(\mathcal{W},t),\boldsymbol{m})\rightarrow\mathrm{ct}$：算法以公钥 pk，访问结构 $(\mathcal{W},t)$ 和消息 $\boldsymbol{m}$ 为输入；算法输出密文消息 ct。

$\mathrm{Dec}(\mathrm{sk},\mathrm{ct})\rightarrow\boldsymbol{m}$：算法以密钥 sk 和密文 ct 为输入；如果 $\mathcal{S}$ 满足 $(\mathcal{W},t)$，算法输出消息 $\boldsymbol{m}$，否则算法输出空集 $\perp$。

定义 2 一个 CP-ABE 方案，如果对于多项式时间的敌手 $\mathcal{A}$ 在如下游戏中的优势是可忽略的，那么这个方案在选择安全模型中可以称作是选择明文攻击下的语义不可区分(IND-sCPA)安全的：

目标：敌手 $\mathcal{A}$ 声明目标访问结构 $\left(\mathcal{W}^*,t^*\right)$。

初始设置：挑战者 $\mathcal{B}$ 根据目标访问结构及原方案的 Setup 算法，生成公共参数 pk 及私钥 msk，并公开 pk，保留 msk。

查询 1：敌手 $\mathcal{A}$ 可以向挑战者 $\mathcal{B}$ 提出多项式次数的密钥查询，但提交查询的属性集合 $\mathcal{S}$ 不能满足挑战的访问结构 $\left(\mathcal{W}^*,t^*\right)$。挑战者 $\mathcal{B}$ 将生成与属性集合 $\mathcal{S}$ 对应的密钥，并将密钥返回给敌手 $\mathcal{A}$。

挑战：敌手 $\mathcal{A}$ 提供等长的消息 $\boldsymbol{m}_0,\boldsymbol{m}_1$，再由挑战者 $\mathcal{B}$ 随机选取 $\varphi\in\{0,1\}$，并将消息 $\boldsymbol{m}_{\varphi}$ 加密成挑战密文 ct^*。最后挑战者 $\mathcal{B}$ 将挑战密文返回给敌手 $\mathcal{A}$。

查询 2：与查询 1 阶段相同。

猜测：敌手 $\mathcal{A}$ 给出关于 φ 的猜测 φ'。

如果 $\varphi'=\varphi$，就可以称敌手 $\mathcal{A}$ 赢得了游戏。此时，敌手 $\mathcal{A}$ 在游戏中的优势定义为 $\left|\Pr[\varphi'=\varphi]-1/2\right|$。

2.4 重要算法

算法 1[18] $\mathrm{I}\text{-}\mathrm{TrapGen}(1,n,m,q)\rightarrow\left(\hat{\boldsymbol{g}},\boldsymbol{T}_{\hat{\boldsymbol{g}}}\right)$。

算法输入整数 n,m，素数 q 和次数为 n 的多项式 f；算法输出一个统计上接近均匀分布的多项式向量 $\hat{\boldsymbol{g}}=(\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_m)^{\mathrm{T}}\in R_q^m$ 和对应陷门 $\boldsymbol{T}_{\hat{\boldsymbol{g}}}\in\mathbb{Z}_q^{mn\times mn}$ 且 $\left\|\boldsymbol{T}_{\hat{\boldsymbol{g}}}\right\|\leq\widetilde{O}(\sqrt{n})$，满足

$$\begin{bmatrix}\mathrm{rot}_f\left(\boldsymbol{g}_1\right)\\ \mathrm{rot}_f\left(\boldsymbol{g}_2\right)\\ \vdots\\ \mathrm{rot}_f\left(\boldsymbol{g}_m\right)\end{bmatrix}^{\mathrm{T}}\cdot\boldsymbol{T}_{\hat{\boldsymbol{g}}}=\boldsymbol{0},$$

$$\mathrm{rot}_f\left(\boldsymbol{g}_i\right)=\begin{bmatrix}\boldsymbol{g}_i\\ \boldsymbol{g}_i x\bmod f\\ \vdots\\ \boldsymbol{g}_i x^{n-1}\bmod f\end{bmatrix},\ i\in[m]\tag{5}$$

算法 2[11] $\mathrm{I}\text{-}\mathrm{SampleLeft}\left(\hat{\boldsymbol{g}},\boldsymbol{T}_{\hat{\boldsymbol{g}}},\boldsymbol{u},\hat{\boldsymbol{a}},\hat{\boldsymbol{b}},\sigma\right)$。

算法输入 $\hat{\boldsymbol{g}}\in R_q^m$ 和对应陷门 $\boldsymbol{T}_{\hat{\boldsymbol{g}}}\in\mathbb{Z}_q^{mn\times mn}$，$\boldsymbol{u}\in$

R_q，任意的 $\hat{\boldsymbol{a}}, \hat{\boldsymbol{b}} \in R_q^m$，参数 $\sigma \geq \left\|\boldsymbol{T}_{\hat{\boldsymbol{g}}}\right\| \omega\left(\sqrt{\log_2 m}\right)$；算法输出一个满足分布 $D_{\mathbb{Z}^{2m\times n},\sigma}$ 的随机取样 $\hat{\boldsymbol{k}}$，并满足 $\hat{\boldsymbol{k}} \otimes \hat{\boldsymbol{e}} = \boldsymbol{u}$，其中，

$$\hat{\boldsymbol{e}}_i = \begin{bmatrix} \hat{\boldsymbol{g}} \\ \hat{\boldsymbol{a}} + \hat{\boldsymbol{b}} \end{bmatrix} \tag{6}$$

需要注意的是，算法在文献[11]中多了一个输入 $\mathrm{id} \in \{0,1\}^n$，但由算法的构造过程易知，移除这个输入并不影响算法的正确性。

算法 3[11]　$\text{I-SampleRight}\left(\hat{\boldsymbol{g}}, \boldsymbol{u}, \hat{\boldsymbol{a}}, \hat{\boldsymbol{b}}, \boldsymbol{T}_{\hat{\boldsymbol{b}}}, \sigma\right)$。

算法输入 $\hat{\boldsymbol{g}} \in R_q^m, \boldsymbol{u} \in R_q, \hat{\boldsymbol{a}} = \left(\hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_m\right) \in R_q^m$，其中 $\hat{\boldsymbol{r}}_1, \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{r}}_m \in R^m$ 是随机产生 m 个环多项式向量，$\hat{\boldsymbol{b}} \in R_q^m$ 及其对应陷门 $\boldsymbol{T}_{\hat{\boldsymbol{b}}} \in \mathbb{Z}_q^{mn\times mn}$，参数 $\sigma \geq \left\|\boldsymbol{T}_{\hat{\boldsymbol{b}}}\right\| \sqrt{m}\, \omega(\log_2 m)$；算法输出一个满足分布 $D_{\mathbb{Z}^{2m\times n},\sigma}$ 的随机取样 $\hat{\boldsymbol{k}}$，并满足 $\hat{\boldsymbol{k}} \otimes \hat{\boldsymbol{e}} = \boldsymbol{u}$，其中，

$$\hat{\boldsymbol{e}} = \begin{bmatrix} \hat{\boldsymbol{g}} \\ \hat{\boldsymbol{a}} + \hat{\boldsymbol{b}} \end{bmatrix} = \begin{bmatrix} \hat{\boldsymbol{g}} \\ \left(\hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_1, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_2, \cdots, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_m\right) + \hat{\boldsymbol{b}} \end{bmatrix} \tag{7}$$

与算法 2 情况相同，算法 3 也移除了原算法中的输入 $\mathrm{id} \in \{0,1\}^n$，且不影响算法的正确性。

3　方案描述

本节给出支持门限访问结构的基于理想格的 CP-ABE 方案。假设方案中总共有 r 个属性，安全参数为 λ。系统定义由 d 个虚拟属性组成的集合 $\mathcal{D}=\{r+1, r+2, \cdots, r+d\}$。

$\text{Setup}\left(1^\lambda, r, d\right) \to (\text{pk}, \text{msk})$：算法定义 $f(x) = x^n + 1$，输入正整数 $n = n(\lambda)$，$m = m(\lambda)$，素数 $q = q(\lambda)$，虚拟属性个数 $d \leq r$ 和属性集合 $\mathcal{R} = \{1, 2, \cdots, r\}$。

(1)算法首先定义 $\mathcal{R}' = \mathcal{R} \cup \mathcal{D}$。

(2)生成 $\left(\hat{\boldsymbol{g}}, \boldsymbol{T}_{\hat{\boldsymbol{g}}}\right) \leftarrow \text{I-TrapGen}(1, n, m, q)$。

(3)对于 $i \in \mathcal{R}'$，随机选取系数均匀分布的环多项式向量 $\hat{\boldsymbol{a}}_i \in R_q^m$。并随机选择均匀分布的向量 $\boldsymbol{u} = \left(u_1, u_2, \cdots, u_n\right)^{\mathrm{T}} \in R_q$ 及环多项式向量 $\hat{\boldsymbol{b}} \in R_q^m$。

(4)最后输出公钥 $\text{pk} = \left(\hat{\boldsymbol{g}}, \{\hat{\boldsymbol{a}}_i\}_{i\in\mathcal{R}'}, \hat{\boldsymbol{b}}, \boldsymbol{u}, q, f\right)$，主密钥 $\text{msk} = \left(\boldsymbol{T}_{\hat{\boldsymbol{g}}}\right)$。

$\text{KeyGen}(\text{pk}, \text{msk}, \mathcal{S}) \to \text{sk}$：算法输入公钥 pk、主密钥 msk 和用户的属性集合 $\mathcal{S}$，定义 $\mathcal{S}' = \mathcal{S} \cup \mathcal{D}$。

(1)对于 $j \in [n]$，随机选择 d 次多项式 $p_j(x) \in \mathbb{Z}_q[x]$ 满足 $p_j(0) = u_j$，其中 u_j 为向量 $\boldsymbol{u}$ 的分量。并对于 $i \in \mathcal{S}'$，令 $\overline{\boldsymbol{u}}_i = \left(p_1(i), p_2(i), \cdots, p_n(i)\right)^{\mathrm{T}}$。需要注意的是，对于任意的子集 $\mathcal{J} \subseteq \mathcal{S}'$ ($|\mathcal{J}| = d+1$)，有 $\boldsymbol{u} = \sum_{j\in\mathcal{J}} L_j \overline{\boldsymbol{u}}_j$，其中拉格朗日系数为

$$L_j = \frac{\prod_{i\in\mathcal{J}, i\neq j} -i}{\prod_{i\in\mathcal{J}, i\neq j} (j-i)} \tag{8}$$

(2)对于 $i \in \mathcal{S}'$，令

$$\hat{\boldsymbol{e}}_i = \begin{bmatrix} \hat{\boldsymbol{g}} \\ \hat{\boldsymbol{a}}_i + \hat{\boldsymbol{b}} \end{bmatrix} \tag{9}$$

再计算 $\hat{\boldsymbol{k}}_i \leftarrow \text{I-SampleLeft}\left(\hat{\boldsymbol{g}}, \boldsymbol{T}_{\hat{\boldsymbol{g}}}, \overline{\boldsymbol{u}}_i, \hat{\boldsymbol{a}}_i, \hat{\boldsymbol{b}}, \sigma\right)$，满足 $\hat{\boldsymbol{k}}_i \otimes \hat{\boldsymbol{e}}_i = \overline{\boldsymbol{u}}_i$。

(3)最后输出密钥 $\text{sk} = \left(\left\{\hat{\boldsymbol{k}}_i \in Z_q^{2m}\right\}_{i\in\mathcal{S}'}\right)$。

$\text{Enc}(\text{pk}, (\mathcal{W}, t), \boldsymbol{m}) \to \text{ct}$：算法输入公钥 pk、系数为 $\{0,1\}$ 的环多项式形式的明文消息 $\boldsymbol{m} \in R$ 和门限访问结构 $(\mathcal{W}, t)$。定义 $\mathcal{W}' = \mathcal{W} \cup \{r+1, r+2, \cdots, r+d+1-t\}$。

(1)随机选取 $\boldsymbol{s} \in R_q$；随机选择系数服从分布 $D_{\mathbb{Z}^{m\times n},\delta}$ 的环多项式向量 $\hat{\boldsymbol{x}}_1 \in R^m$。

(2)对于 $i \in \mathcal{W}'$，选择 m 个环多项式向量 $\hat{\boldsymbol{r}}_{i,1}, \hat{\boldsymbol{r}}_{i,2}, \cdots, \hat{\boldsymbol{r}}_{i,m} \in R^m$，其系数取自 $\{-1,1\}$，定义 $\hat{\boldsymbol{x}}_{i,2} = \left(\hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,1}, \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,2}, \cdots, \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,m}\right)^{\mathrm{T}} \in R^m$。再由式(9)，计算

$$\hat{\boldsymbol{c}}_i = \hat{\boldsymbol{e}}_i \boldsymbol{s} + Y \begin{pmatrix} \hat{\boldsymbol{x}}_1 \\ \hat{\boldsymbol{x}}_{i,2} \end{pmatrix} \in R_q^{2m}，\text{其中 } Y = (r!)^2 \tag{10}$$

(3)选择噪声 $\boldsymbol{x}_0 \in R$，计算 $\boldsymbol{c}_0 = \boldsymbol{u}\boldsymbol{s} + Y\boldsymbol{x}_0 + \boldsymbol{m}\lfloor q/2 \rfloor \in R_q$。

(4)最后输出密文 $\text{ct} = \left(\boldsymbol{c}_0, \{\hat{\boldsymbol{c}}_i\}_{i\in\mathcal{W}'}\right)$。

$\text{Dec}(\text{sk}, \text{ct}) \to \boldsymbol{m}$：算法输入密文 ct 和密钥 sk。如果 $|\mathcal{S} \cap \mathcal{W}| < t$，算法输出 $\perp$。否则，算法将如下解密：

已知 $|\mathcal{S} \cap \mathcal{W}| \geq t$，就有 $|\mathcal{S}' \cap \mathcal{W}'| \geq d+1$。任取一子集 $\mathcal{J} \subseteq \mathcal{S}' \cap \mathcal{W}'$ 且满足 $|\mathcal{J}| = d+1$。计算

$$\boldsymbol{m}' = \boldsymbol{c}_0 - \sum_{j\in\mathcal{J}} \left(L_j \left(\hat{\boldsymbol{k}}_j \otimes \hat{\boldsymbol{c}}_j\right)\right) \bmod q \tag{11}$$

$\forall i \in \{0, 1, \cdots, n-1\}$，如果 $\left|m_i' - \lfloor q/2 \rfloor\right| \leq \lfloor q/4 \rfloor$，令 $m_i = 1$，否则 $m_i = 0$，其中 m_i 和 m_i' 分别为环多项式 $\boldsymbol{m}$ 和 $\boldsymbol{m}'$ 中 x^i 的系数。

4　方案正确性分析

本节主要分析方案的正确性，即证明如果用户的属性集合 $\mathcal{S}$ 满足访问结构 $(\mathcal{W}, t)$，那么解密者可以以很大概率正确解密出明文消息。解密算法首先计算

$$\begin{aligned}\boldsymbol{m}' &= \boldsymbol{c}_0 - \sum_{j\in\mathcal{J}}\left(L_j\left(\hat{\boldsymbol{k}}_j \otimes \hat{\boldsymbol{c}}_j\right)\right) \bmod q \\ &= \boldsymbol{u}\boldsymbol{s} + Y\boldsymbol{x}_0 + \boldsymbol{m}\lfloor q/2\rfloor \\ &\quad - \sum_{j\in\mathcal{J}}\left(L_j\left(\hat{\boldsymbol{k}}_j \otimes \left(\hat{\boldsymbol{e}}_j\boldsymbol{s} + Y\begin{pmatrix}\hat{\boldsymbol{x}}_1\\ \hat{\boldsymbol{x}}_{j,2}\end{pmatrix}\right)\right)\right) \bmod q \\ &= \boldsymbol{m}\lfloor q/2\rfloor + \boldsymbol{u}\boldsymbol{s} - \sum_{j\in\mathcal{J}}\left(L_j\left(\hat{\boldsymbol{k}}_j \otimes \hat{\boldsymbol{e}}_j\boldsymbol{s}\right)\right) \\ &\quad + Y\left(\sum_{j\in\mathcal{J}}\left(L_j\hat{\boldsymbol{k}}_j \otimes \begin{pmatrix}\hat{\boldsymbol{x}}_1\\ \hat{\boldsymbol{x}}_{j,2}\end{pmatrix}\right) + \boldsymbol{x}_0\right) \bmod q \end{aligned} \tag{12}$$

根据密钥生成算法，可得 $\sum_{j\in\mathcal{J}}\left(L_j\left(\hat{\boldsymbol{k}}_j \otimes \hat{\boldsymbol{e}}_j\right)\right) = \boldsymbol{u}$，将其代入式(12)得到：

$$\boldsymbol{m}' = \boldsymbol{m}\lfloor q/2\rfloor + Y\left(\sum_{j\in\mathcal{J}}\left(L_j\hat{\boldsymbol{k}}_j \otimes \begin{pmatrix}\hat{\boldsymbol{x}}_1\\ \hat{\boldsymbol{x}}_{j,2}\end{pmatrix}\right) + \boldsymbol{x}_0\right) \bmod q \tag{13}$$

据式(13)所示，只要保证 $Y\left(\sum_{j\in\mathcal{J}}\left(L_j\hat{\boldsymbol{k}}_j \otimes \begin{pmatrix}\hat{\boldsymbol{x}}_1\\ \hat{\boldsymbol{x}}_{j,2}\end{pmatrix}\right) + \boldsymbol{x}_0\right)$ 中任意系数不超过 $\lfloor q/4\rfloor$，解密者就可以正确解密。方案在下面的分析中需要用到如下的定理和引理。

定理 1[19] 对于任意的实数 $s>0$，$T>0$ 和 $\boldsymbol{x}\in\mathbb{R}^n$，有

$$\Pr\left[\left\langle \boldsymbol{x}, D_{z^n,s}\right\rangle > Ts\|\boldsymbol{x}\|\right] \le 2\exp\left(-\pi T^2\right) \tag{14}$$

引理 1[17] 令 $Y=(r!)^2$，对于集合 $\mathcal{J}$，定义拉格朗日系数

$$L_i = \prod_{j\in\mathcal{J}, j\neq i}\frac{-j}{i-j} \tag{15}$$

那么，对于 $i\in\mathcal{J}$，YL_i 是整数且满足 $|YL_i| \le Y^2 \le (r!)^4$。

定理 2 对于任意 $\hat{\boldsymbol{x}}$，$\hat{\boldsymbol{r}}\in R^m$，且 $\hat{\boldsymbol{r}}$ 系数取自 $\{-1,1\}$，则 $\|\hat{\boldsymbol{x}}\otimes\hat{\boldsymbol{r}}\| \le nm\|\hat{\boldsymbol{x}}\|$。

证明 已知 $\hat{\boldsymbol{x}} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_m)^{\mathrm{T}}$，设 $\|\hat{\boldsymbol{x}}\| = \|\boldsymbol{x}_t\| = \max_{i\in[m]}\|\boldsymbol{x}_i\|$，对于 $i\in[m]$，$\boldsymbol{x}_i = \left(x_{i,0}, x_{i,1}, \cdots, x_{i,n-1}\right)$，$\boldsymbol{r}_i = \left(r_{i,0}, r_{i,1}, \cdots, r_{i,n-1}\right)$，计算

$$\|\hat{\boldsymbol{x}}\otimes\hat{\boldsymbol{r}}\| = \left\|\sum_{i=1}^{m}\boldsymbol{x}_i\cdot\boldsymbol{r}_i\right\| = \left\|\sum_{i=1}^{m}\left(x_{i,0}, x_{i,1}, \cdots, x_{i,n-1}\right)\begin{pmatrix}\boldsymbol{r}_i\\ \boldsymbol{r}_i x \bmod \boldsymbol{f}\\ \boldsymbol{r}_i x^2 \bmod \boldsymbol{f}\\ \vdots\\ \boldsymbol{r}_i x^{n-1} \bmod \boldsymbol{f}\end{pmatrix}\right\| = \left\|\sum_{i=1}^{m}\left(x_{i,0}, x_{i,1}, \cdots, x_{i,n-1}\right)\begin{pmatrix} r_{i,0} & r_{i,1} & \cdots & r_{i,n-1}\\ r_{i,n-1} & r_{i,0} & \cdots & r_{i,n-2}\\ \vdots & \vdots & \ddots & \vdots\\ r_{i,1} & r_{i,2} & \cdots & r_{i,0}\end{pmatrix}\right\|$$

$$\begin{aligned} &= \sqrt{\left(\sum_{i=1}^{m}\sum_{\substack{0\le j\le n-1\\ k=(0-j)\bmod n}} x_{i,j}r_{i,k}\right)^2 + \left(\sum_{i=1}^{m}\sum_{\substack{0\le j\le n-1\\ k=(1-j)\bmod n}} x_{i,j}r_{i,k}\right)^2 + \cdots + \left(\sum_{i=1}^{m}\sum_{\substack{0\le j\le n-1\\ k=(n-1-j)\bmod n}} x_{i,j}r_{i,k}\right)^2} \\ &\le \sqrt{\left(\sum_{i=1}^{m}\sum_{j=0}^{n-1}|x_{i,j}|\right)^2 + \left(\sum_{i=1}^{m}\sum_{j=0}^{n-1}|x_{i,j}|\right)^2 + \cdots + \left(\sum_{i=1}^{m}\sum_{j=0}^{n-1}|x_{i,j}|\right)^2} = \sqrt{n\left(\sum_{i=1}^{m}\sum_{j=0}^{n-1}|x_{i,j}|\right)^2} \le \sqrt{nm\sum_{i=1}^{m}\left(\left(\sum_{j=0}^{n-1}|x_{i,j}|\right)^2\right)} \\ &\le \sqrt{nm\sum_{i=1}^{m}\left(n\left(\sum_{j=0}^{n-1}\left(x_{i,j}\right)^2\right)\right)} \le \sqrt{nm\sum_{i=1}^{m}\left(n\left(\sum_{j=0}^{n-1}\left(x_{t,j}\right)^2\right)\right)} = nm\sqrt{\sum_{j=0}^{n-1}\left(x_{t,j}\right)^2} = nm\|\hat{\boldsymbol{x}}\| \end{aligned} \tag{16}$$

证毕

下面分析噪声多项式 $Y\left(\sum_{j\in\mathcal{J}}\left(L_j\hat{\boldsymbol{k}}_j \otimes \begin{pmatrix}\hat{\boldsymbol{x}}_1\\ \hat{\boldsymbol{x}}_{j,2}\end{pmatrix}\right) + \boldsymbol{x}_0\right)$ 的系数是如何得到的。已知 $\hat{\boldsymbol{k}}_j = \left(\boldsymbol{k}_{j,1}, \cdots, \boldsymbol{k}_{j,m}, \boldsymbol{k}_{j,m+1}, \cdots, \boldsymbol{k}_{j,2m}\right)^{\mathrm{T}}$，$(\hat{\boldsymbol{x}}_1, \hat{\boldsymbol{x}}_{j,2}) = \left(\boldsymbol{x}_1^1, \cdots, \boldsymbol{x}_m^1, \boldsymbol{x}_{j,1}^2, \cdots, \boldsymbol{x}_{j,m}^2\right)^{\mathrm{T}}$，由 $\otimes$ 乘法的定义可得：

$$\hat{\boldsymbol{k}}_j \otimes \begin{pmatrix}\hat{\boldsymbol{x}}_1\\ \hat{\boldsymbol{x}}_{j,2}\end{pmatrix} = \sum_{t=1}^{m}\boldsymbol{k}_{j,t}\cdot\boldsymbol{x}_t^1 + \sum_{t=1}^{m}\boldsymbol{k}_{j,t+m}\cdot\boldsymbol{x}_{j,t}^2 \tag{17}$$

因此，

$$\begin{aligned} &Y\left(\sum_{j\in\mathcal{J}}\left(L_j\hat{\boldsymbol{k}}_j \otimes \begin{pmatrix}\hat{\boldsymbol{x}}_1\\ \hat{\boldsymbol{x}}_{j,2}\end{pmatrix}\right) + \boldsymbol{x}_0\right) \\ &= Y\left(\sum_{j\in\mathcal{J}}\left(L_j\left(\sum_{t=1}^{m}\boldsymbol{k}_{j,t}\cdot\boldsymbol{x}_t^1 + \sum_{t=1}^{m}\boldsymbol{k}_{j,t+m}\cdot\boldsymbol{x}_{j,t}^2\right)\right) + \boldsymbol{x}_0\right) \end{aligned} \tag{18}$$

已知 $|\mathcal{J}| = d+1$，再根据算法 I-SampleLeft 的定义知 $\hat{\boldsymbol{k}}_j$ 满足分布 $D_{\mathbb{Z}^{2m\times n},\sigma}$。由式(18)可以看出，噪声多项式的每一项系数的求解等价于先求

$2mY(d+1)L_j \le 2mY^2(d+1)$ (引理 1)个服从分布 $D_{\mathbb{Z}^n,\sigma}$ 的 $\boldsymbol{k}$ 和 $\boldsymbol{x} \in R$ (易知满足 $\boldsymbol{x} \in \mathbb{R}^n$)的内积，再与 Y 个噪声 $\boldsymbol{x}_0$ 中对应的多项式系数 x_0 求和。

由此，根据定理 1，计算解密失败的概率为

$$\begin{aligned}&\Pr\left[2mY^2(d+1)\left|\langle \boldsymbol{k},\boldsymbol{x}\rangle\right| + Yx_0 \ge q/4\right]\\&= \Pr\left[\left|\langle \boldsymbol{k},\boldsymbol{x}\rangle\right| \ge (q/4 - Yx_0)/2mY^2(d+1)\right]\\&= \Pr\left[\left|\langle \boldsymbol{k},\boldsymbol{x}\rangle\right| \ge T\sigma\|\boldsymbol{x}\|\right] < 2\exp\left(-\pi T^2\right)\end{aligned} \tag{19}$$

其中，$T = (q/4 - Yx_0)\big/2mY^2(d+1)\sigma\|\boldsymbol{x}\|$。

再讨论 T 中 $\|\boldsymbol{x}\|$ 的最大值。为了求 $\|\boldsymbol{x}\|$ 的最大值，需要分别求 $\|\hat{\boldsymbol{x}}_1\|$ 和 $\|\hat{\boldsymbol{x}}_{j,2}\|$ 的最大值。已知环多项式向量 $\hat{\boldsymbol{x}}_1 \in R^m$ 的系数服从分布 $D_{\mathbb{Z}^{m\times n},\delta}$，同时有 $\hat{\boldsymbol{x}}_{j,2} = \left(\hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{j,1}, \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{j,2}, \cdots, \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{j,m}\right)^{\mathrm{T}} \in R^m$，其中 $\hat{\boldsymbol{r}}_{j,1}, \hat{\boldsymbol{r}}_{j,2}, \cdots, \hat{\boldsymbol{r}}_{j,m} \in R^m$ 且系数取自 $\{-1,1\}$。根据定理 2 有 $\|\hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{j,1}\| \le nm\|\hat{\boldsymbol{x}}_1\|$，而噪声环多项式向量 $\|\hat{\boldsymbol{x}}_1\| \le \mathcal{X}_{\max}$，所以有 $||\hat{\boldsymbol{x}}_{j,2}|| \le nm\mathcal{X}_{\max}$，即 $||\boldsymbol{x}|| \le nm\mathcal{X}_{\max}$。

再根据噪声多项式系数 $x_0 \le \mathcal{X}_{\max}$，有

$$\begin{aligned}T &= \left(q/4 - Yx_0\right)\big/2Y^2(d+1)\,m\sigma\|\boldsymbol{x}\|\\&\ge \left(q/4 - Y\mathcal{X}_{\max}\right)\big/2Y^2(d+1)nm^2\,\sigma\mathcal{X}_{\max} \ge t\end{aligned} \tag{20}$$

方案可以在初始设置中定义 $q \ge 4\left(2Y^2(d+1)\cdot nm^2\sigma\mathcal{X}_{\max}t + Y\mathcal{X}_{\max}\right)$，其中 t 为一常数，不妨假设 $t \ge 15$。此时解密失败的概率 $2\exp\left(-\pi T^2\right)$ 是可以忽略不计的，所以方案将会以很大的概率正确解密。

5　方案安全性分析

本节证明新方案在 R-LWE 假设下是选择性安全的。

定理 3　假设判定性 R-LWE 问题是困难的，那么本文的 CP-ABE 方案是选择性 CPA 安全的。

证明　下面通过敌手 $\mathcal{A}$ 和挑战者 $\mathcal{B}$ 之间的交互游戏来证明方案的安全性。假设敌手 $\mathcal{A}$ 能够在选择安全模型下以选择明文攻击方式以不可忽略的优势攻破上述方案，那么挑战者 $\mathcal{B}$ 就能够以不可忽略的优势解决判定性 R-LWE 问题。

假设系统中所有属性组成的集合为 $\mathcal{R} = \{1,2,\cdots,r\}$，虚拟属性集合为 $\mathcal{D} = \{r+1, r+2, \cdots, r+d\}$，并定义 $\mathcal{R}' = \mathcal{R} \cup \mathcal{D}$。

挑战者 $\mathcal{B}$ 首先查询预言机 O，并得到如下的一个 R-LWE 预言机取样实例：

$$\begin{aligned}&\left[\left(\boldsymbol{w}_0, \boldsymbol{v}_0\right)\right] \in \left(R_q^n \times R_q\right),\\&\left[\left(\boldsymbol{w}_1^1, \boldsymbol{v}_1^1\right), \left(\boldsymbol{w}_1^2, \boldsymbol{v}_1^2\right), \cdots, \left(\boldsymbol{w}_1^m, \boldsymbol{v}_1^m\right)\right] \in \left(R_q^n \times R_q\right)^m\end{aligned} \tag{21}$$

目标：

敌手 $\mathcal{A}$ 给出访问结构 $\left(\mathcal{W}^*, t^*\right)$ 作为挑战目标，其中 $1 \le t^* \le \min\left\{\left|\mathcal{W}^*\right|, d\right\}$，并定义 $\mathcal{W}' = \mathcal{W}^* \cup \left\{r+1, r+2, \cdots, r+d+1-t^*\right\}$。

初始设置：

(1) 挑战者 $\mathcal{B}$ 生成 $\left(\hat{\boldsymbol{b}}, \boldsymbol{T}_{\hat{\boldsymbol{b}}}\right) \leftarrow$ I-TrapGen$(1,n,m,q)$。并根据 R-LWE 取样，令 $\hat{\boldsymbol{g}} = \left(\boldsymbol{w}_1^1, \boldsymbol{w}_1^2, \cdots, \boldsymbol{w}_1^m\right)^{\mathrm{T}}$，$\boldsymbol{u} = \boldsymbol{w}_0$。

(2)对于 $i \in \mathcal{W}'$，挑战者 $\mathcal{B}$ 随机产生 m 个环多项式向量 $\hat{\boldsymbol{r}}_{i,1}^*, \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \hat{\boldsymbol{r}}_{i,m}^* \in R^m$，并计算 $\hat{\boldsymbol{a}}_i = \left(\hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,1}^*, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,m}^*\right) - \hat{\boldsymbol{b}}$。对于 $i \in \mathcal{R}'/\mathcal{W}'$，挑战者 $\mathcal{B}$ 随机产生 m 个环多项式向量 $\hat{\boldsymbol{r}}_{i,1}^*, \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \hat{\boldsymbol{r}}_{i,m}^* \in R^m$，并计算 $\hat{\boldsymbol{a}}_i = \left(\hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,1}^*, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,m}^*\right)$。

(3)最后挑战者 $\mathcal{B}$ 给出公钥 $\mathrm{pk} = \left(\hat{\boldsymbol{g}}, \{\hat{\boldsymbol{a}}_i\}_{i\in\mathcal{R}'}, \hat{\boldsymbol{b}}, \boldsymbol{u}\right)$，并保留 $\boldsymbol{T}_{\hat{\boldsymbol{b}}}$，$\left\{\hat{\boldsymbol{r}}_{i,j}^*\right\}_{i\in\mathcal{R}', j\in[m]}$，$\left\{\boldsymbol{v}_1^j\right\}_{j\in[m]}$ 和 $\boldsymbol{v}_0$。

查询 1：

挑战者 $\mathcal{B}$ 对于敌手 $\mathcal{A}$ 查询的属性集合 $\mathcal{S}$，只要满足 $\left|\mathcal{S} \cap \mathcal{W}^*\right| \le t^* - 1$，即查询的属性集合 $\mathcal{S}$ 不满足挑战的访问结构 $\left(\mathcal{W}^*, t^*\right)$，挑战者 $\mathcal{B}$ 就将对应的私钥返还给敌手。

(1)首先定义 $\mathcal{S}' = \mathcal{S} \cup \{r+1, r+2, \cdots, r+d\}$，有 $|\mathcal{S}' \cap \mathcal{W}'| \le d$。然后在集合 $\mathcal{S}'$ 中选取子集 $\overline{\mathcal{S}}$，满足 $\mathcal{S}' \cap \mathcal{W}' \subseteq \overline{\mathcal{S}}$ 且 $\left|\overline{\mathcal{S}}\right| = d$。

(2)对于 $i \in \overline{\mathcal{S}}$，定义

$$\hat{\boldsymbol{e}}_i = \begin{bmatrix}\hat{\boldsymbol{g}}\\ \hat{\boldsymbol{a}}_i + \hat{\boldsymbol{b}}\end{bmatrix} \tag{22}$$

随机选取 $\hat{\boldsymbol{k}}_i \leftarrow D_{\mathbb{Z}^{2m\times n},\sigma}$，并计算 $\overline{\boldsymbol{u}}_i = \hat{\boldsymbol{k}}_i \otimes \hat{\boldsymbol{e}}_i$。由此，对于 $j \in [n]$，可以构造 d 次多项式 $p_j(x) \in \mathbb{Z}_q[x]$，这些多项式满足 $\boldsymbol{u} = \left(p_1(0), p_2(0), \cdots, p_n(0)\right)^{\mathrm{T}}$，$\overline{\boldsymbol{u}}_i = \left(p_1(i), p_2(i), \cdots, p_n(i)\right)^{\mathrm{T}}$。根据多项式阶数和集合 $\overline{\mathcal{S}}$ 的大小，易知如上的多项式很容易构造。

(3)对于 $i \in \mathcal{S}'/\overline{\mathcal{S}}$，由子集 $\overline{\mathcal{S}}$ 的选取知 $i \notin \mathcal{W}'$。定义

$$\hat{\boldsymbol{e}} = \begin{bmatrix}\hat{\boldsymbol{g}}\\ \hat{\boldsymbol{a}}_i + \hat{\boldsymbol{b}}\end{bmatrix} = \begin{bmatrix}\hat{\boldsymbol{g}}\\ \left(\hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,1}^*, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,m}^*\right) + \hat{\boldsymbol{b}}\end{bmatrix} \tag{23}$$

再利用 2 中构造的多项式 $p_j(x)$，定义 $\overline{\boldsymbol{u}}_i = \left(p_1(i), p_2(i), \cdots, p_n(i)\right)^{\mathrm{T}}$。调用 I-SampleRight 算法计算私钥：

$$\hat{\boldsymbol{k}}_i \leftarrow \text{I-SampleRight}\left(\hat{\boldsymbol{g}}, \overline{\boldsymbol{u}}_i, \hat{\boldsymbol{a}}_i, \hat{\boldsymbol{b}}, \boldsymbol{T}_{\hat{\boldsymbol{b}}}, \sigma\right) \tag{24}$$

满足 $\hat{\boldsymbol{k}}_i \otimes \hat{\boldsymbol{e}}_i = \overline{\boldsymbol{u}}_i$。由 I-SampleRight 的定义可知，挑战者 $\mathcal{B}$ 生成的私钥与原方案生成的私钥在统计上是不可区分的。

(4) 最后挑战者 $\mathcal{B}$ 返还给敌手 $\mathcal{A}$ 密钥 $\mathrm{sk} = \left(\left\{\hat{\boldsymbol{k}}_i\right\}_{i\in\mathcal{S}'}\right)$。

挑战：

敌手 $\mathcal{A}$ 向挑战者 $\mathcal{B}$ 提供两个等长的消息 $\{\boldsymbol{m}_0, \boldsymbol{m}_1\} \in R$。$\mathcal{B}$ 随机选择一个 $\boldsymbol{m}_\varphi\,(\varphi \in \{0,1\})$ 加密，令 $Y = (r!)^2$，其中 r 是指方案中属性的个数，并输出挑战密文：

$$\left.\begin{aligned} \boldsymbol{c}_0 &= Y\boldsymbol{v}_0 + \boldsymbol{m}_\varphi \lfloor q/2 \rfloor \\ \hat{\boldsymbol{c}}_i &= Y\begin{pmatrix} \left(\boldsymbol{v}_1^1, \boldsymbol{v}_1^2, \cdots, \boldsymbol{v}_1^m\right)^{\mathrm{T}} \\ \left(\boldsymbol{v}_1^1, \boldsymbol{v}_1^2, \cdots, \boldsymbol{v}_1^m\right)^{\mathrm{T}} \otimes \hat{\boldsymbol{r}}_{i,1}^*, \left(\boldsymbol{v}_1^1, \boldsymbol{v}_1^2, \cdots, \boldsymbol{v}_1^m\right)^{\mathrm{T}} \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \left(\boldsymbol{v}_1^1, \boldsymbol{v}_1^2, \cdots, \boldsymbol{v}_1^m\right)^{\mathrm{T}} \otimes \hat{\boldsymbol{r}}_{i,m}^* \end{pmatrix}_{i\in\mathcal{W}'} \end{aligned}\right\} \tag{25}$$

需要注意的是，本文在生成挑战密文时，R-LWE 取样中的随机向量为 $\boldsymbol{s}^*$，挑战密文中的随机向量为 $\boldsymbol{s} = Y\boldsymbol{s}^*$，所以对于 $i \in \mathcal{W}'$，有

$$\begin{aligned} \hat{\boldsymbol{c}}_i &= Y\begin{pmatrix} \left(\boldsymbol{v}_1^1, \boldsymbol{v}_1^2, \cdots, \boldsymbol{v}_1^m\right)^{\mathrm{T}} \\ \left(\boldsymbol{v}_1^1, \boldsymbol{v}_1^2, \cdots, \boldsymbol{v}_1^m\right)^{\mathrm{T}} \otimes \hat{\boldsymbol{r}}_{i,1}^*, \left(\boldsymbol{v}_1^1, \boldsymbol{v}_1^2, \cdots, \boldsymbol{v}_1^m\right)^{\mathrm{T}} \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \left(\boldsymbol{v}_1^1, \boldsymbol{v}_1^2, \cdots, \boldsymbol{v}_1^m\right)^{\mathrm{T}} \otimes \hat{\boldsymbol{r}}_{i,m}^* \end{pmatrix} \\ &= Y\begin{pmatrix} \left(\boldsymbol{w}_1^1, \boldsymbol{w}_1^2, \cdots, \boldsymbol{w}_1^m\right)^{\mathrm{T}} Y\boldsymbol{s}^* \\ \left(\boldsymbol{w}_1^1, \boldsymbol{w}_1^2, \cdots, \boldsymbol{w}_1^m\right)^{\mathrm{T}} Y\boldsymbol{s}^* \otimes \hat{\boldsymbol{r}}_{i,1}^*, \left(\boldsymbol{w}_1^1, \boldsymbol{w}_1^2, \cdots, \boldsymbol{w}_1^m\right)^{\mathrm{T}} Y\boldsymbol{s}^* \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \left(\boldsymbol{w}_1^1, \boldsymbol{w}_1^2, \cdots, \boldsymbol{w}_1^m\right)^{\mathrm{T}} Y\boldsymbol{s}^* \otimes \hat{\boldsymbol{r}}_{i,m}^* \end{pmatrix} \\ &\quad + \begin{pmatrix} \hat{\boldsymbol{x}}_1 \\ \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,1}^*, \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,m}^* \end{pmatrix} = Y\begin{pmatrix} \hat{\boldsymbol{g}} \\ \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,1}^*, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \hat{\boldsymbol{g}} \otimes \hat{\boldsymbol{r}}_{i,m}^* \end{pmatrix} \\ &\quad + \begin{pmatrix} \hat{\boldsymbol{x}}_1 \\ \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,1}^*, \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,2}^*, \cdots, \hat{\boldsymbol{x}}_1 \otimes \hat{\boldsymbol{r}}_{i,m}^* \end{pmatrix} = \begin{pmatrix} \hat{\boldsymbol{g}} \\ \hat{\boldsymbol{a}}_i + \hat{\boldsymbol{b}} \end{pmatrix}\boldsymbol{s} + \begin{pmatrix} \hat{\boldsymbol{x}}_1 \\ \hat{\boldsymbol{x}}_{i,2} \end{pmatrix} \end{aligned} \tag{26}$$

由 R-LWE 取样的性质可知，挑战密文对于敌手 $\mathcal{A}$ 来说与原方案正常生成的密文在统计上是不可区分的。

查询 2：与查询 1 阶段相同。

猜测：

挑战者 $\mathcal{B}$ 根据敌手 $\mathcal{A}$ 给出的 φ 的猜测结果 φ' 来判决 R-LWE 问题。如果 $\varphi' = \varphi$，挑战者 $\mathcal{B}$ 猜测 R-LWE 取样取自 $\mathcal{O}_s$；否则挑战者 $\mathcal{B}$ 猜测 R-LWE 取样取自 $\mathcal{O}_{\hat{s}}$。

假设敌手 $\mathcal{A}$ 猜测正确的概率 $\Pr[\varphi' = \varphi] \geq 1/2 + \varepsilon$，那么挑战者 $\mathcal{B}$ 可以以

$$\begin{aligned} &\frac{1}{2}\Pr\left[\varphi' = \varphi \middle| \mathcal{O}_s\right] + \frac{1}{2}\Pr\left[\varphi' = \varphi \middle| \mathcal{O}_{\hat{s}}\right] \\ &\quad = \frac{1}{2} \times \left(\frac{1}{2} + \varepsilon\right) + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2} + \frac{\varepsilon}{2} \end{aligned} \tag{27}$$

的概率解决判定性 R-LWE 问题。 证毕

根据定理 3 和判定性 R-LWE 问题的安全性，可以证明新方案是安全的。

6 对比分析与总结

表 2 中 $|\mathcal{R}|$ 表示方案中所有属性的数量 ($|\mathcal{R}| >> 2$), $|\mathcal{S}|$ 表示用户属性集合大小 ($|\mathcal{S}| \leq |\mathcal{R}|$), d 表示虚拟属性的个数(一般可设置 $d = |\mathcal{R}|$), $|n \times m|$ 表示 $n \times m$ 维矩阵大小 ($m > n$), $|n|$ 表示 n 维向量大小。表 2 中的对比表明，与文献[11]相比，在同时加密 n 维长度的明文消息时，本文方案公共参数数量降低大约 1/3，主密钥数量降低 $|\mathcal{R}|$ 倍。由于现有的密文策略方案均使用虚拟属性，就会不可避免地带来密钥量的增长，新方案在加密等长明文消息时，产生的密钥数量与目前结果最好的文献[16]中的密文策略方案相同，比方案[11](密钥策略方案)扩大约一倍。虽然本文方案与文献[11]的两个方案同时支持 FFT 运算，但本文方案对实际应用场景有更广泛的适应性，同时比文献[16]加解密效率更高。

本文构建了一个基于理想格的支持门限访问结构的 CP-ABE 加密方案，新方案加解密效率高，公共参数和主密钥数量少，还适用于绝大多数实际应用环境。在现有的格基 ABE 方案中，CP-ABE 方案数量极少，本文设计的新方案对于后续设计支持更灵活访问结构的 CP-ABE 方案有一定意义。同时，构建更灵活的格基 CP-ABE 方案及利用理想格设计效率更高的 ABE 方案是我们下一步工作的主要方向。

表 2 本文与现有支持门限访问结构的 ABE 方案的对比

	本文方案	文献[11]	文献[16]
困难问题	R-LWE	R-LWE	LWE
访问策略	密文策略	密钥策略	密文策略
明文长度	n	n	1
公参量	$(\lvert\mathcal{R}\rvert+d+2)\times\lvert n\times m\rvert+\lvert n\rvert$	$(3\times\lvert\mathcal{R}\rvert)\times\lvert n\times m\rvert+\lvert n\rvert$	$(\lvert\mathcal{R}\rvert+d+2)\times\lvert n\times m\rvert+\lvert n\rvert$
主密钥量	$\lvert mn\times mn\rvert$	$\lvert\mathcal{R}\rvert\times\lvert mn\times mn\rvert$	$\lvert m\times m\rvert$
私钥量	$(d+\lvert\mathcal{S}\rvert)\times\lvert n\times 2m\rvert$	$\lvert\mathcal{R}\rvert\times\lvert n\times 2m\rvert$	$(d+\lvert\mathcal{S}\rvert)\times\lvert 2m\times 1\rvert$
运算方法	FFT 运算	FFT 运算	矩阵运算

参 考 文 献

[1] SAHAI A and WATERS B. Fuzzy identity-based encryption [C]. Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

[2] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine grained access control of encrypted data[C]. Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, USA, 2006: 89–98. doi: 10.1145/1180405.1180418.

[3] 赵建. 基于格的属性基加密方案研究[D]. [硕士论文], 解放军信息工程大学, 2015: 4–7.
ZHAO Jian. Research on attribute-based encryption from lattices[D]. [Master dissertation], The PLA Information Engineering University, 2015: 4–7.

[4] MALLUHI Q, SHIKFA A, and TRINH V. A ciphertext-policy attribute-based encryption scheme with optimized ciphertext size and fast decryption[C]. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates, 2017: 230–240. doi: 10.1145/3052973.3052987.

[5] AJTAI M. Generating hard instances of lattice problems (extend abstract)[C]. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadelphia, USA, 1996: 99–108. doi: 10.1145/237814.237838.

[6] GENTRY C, PEIKERT C, and VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]. Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, 2008: 197–206. doi: 10.1145/1374376.1374407.

[7] AGRAWAL S and BOYEN X. Identity-based encryption from lattices in the standard model[OL]. http://www.cs.stanford.edu/~xb/ab09/, 2009.

[8] ACAR A, AKSU H, ULUAGAC A S, *et al*. A survey on homomorphic encryption schemes: Theory and implementation[OL]. https://arxiv.org/pdf/1704.03578.pdf, 2017.

[9] LYUBASHEVSKY V, PEIKERT C, and REGEV O. On ideal lattices and learning with errors over rings [J]. *Journal of the ACM*, 2010, 60(6): 1–35. doi: 10.1145/2535925.

[10] LYUBASHEVSKY V, PEIKERT C, and REGEV O. A toolkit for ring-LWE cryptography[C]. Advances in Cryptology — The 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 2013: 35–54. doi: https://doi.org/10.1007/978-3-642-38348-9_3.

[11] 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. doi: 10.3724/SP.J.1016.2015.00775.
WU Liqiang, YANG Xiaoyuan, and HAN Yiliang. An efficient FIBE scheme based on ideal lattices[J]. *Chinese Journal of Computers*, 2015, 38(4): 775–782. doi: 10.3724/SP.J.1016. 2015.00775.

[12] SUN Lei, WANG Shuaili, LI Zuohui, *et al*. Large universe ciphertext-policy attribute-based encryption with efficient revocation[C]. Advances in Engineering Research — The 2nd International Conference on Electrical, Automation and Mechanical Engineering, Shanghai, China, 2017: 243–249. doi: 10.2991/eame-17.2017.58.

[13] NING Jianting, DONG Xiaolei, GAO Zhenfu, *et al*. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes[J]. *IEEE Transactions on Information Forensics & Security*, 2017, 10(6): 1274–1288. doi: 10.1109/TIFS.2015.2405905.

[14] HU Peng and GAO Haiying. Ciphertext-policy attribute-based encryption for general circuits from bilinear maps[J]. *Wuhan University Journal of Natural Sciences*, 2017, 22(2): 171–177. doi: 10.1007/s11859-017-1231-8.

[15] ODELU V, DAS A, RAO Y, *et al*. Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment[J]. *Computer Standards & Interfaces*, 2017, 54(1): 3–9. doi: 10.1016/j.csi.2016.05.002.

[16] ZHANG Jiang, ZHANG Zhenfeng, and GE Aijun. Ciphertext policy attribute-based encryption from lattices[C]. Proceedings of the 7th ACM Symposium on Information,

Computer and Communications Security, Seoul, Korea, 2012: 16–17. doi: 10.1145/2414456.2414464.

[17] AGRAWAL S, BOYEN X, VAIKUNTANATHAN V, *et al*. Fuzzy identity based encryption from lattices[C]. Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 2012: 280–297. doi: 10.1007/978-3-642-30057-8_17.

[18] STEHLÉ D, STEINFELD R, TANAKA K, *et al*. Efficient public key encryption based on ideal lattices[C]. Advances in Cryptology — The 15th Annual International Conference on the Theory and Application of Cryptology & Information Security, Tokyo, Japan, 2009: 617–635. doi: https://doi.org/10.1007/978-3-642-10366-7_36.

[19] MICCIANCIO D and REGEV O. Worst-case to average-case reductions based on Gaussian measures[J]. *SIAM Journal on Computing*, 2007, 37(1): 267–302. doi: 10.1137/ S0097539705447360.

赵 建：男，1989 年生，博士生，研究方向为公钥密码的设计与分析.

高海英：女，1976 年生，教授，博士生导师，研究方向为密码技术的设计与分析.

胡 斌：男，1971 年生，教授，博士生导师，研究方向为密码技术的设计与分析.