格上基于 OBDD 访问结构的抗密钥滥用属性加密方案

韩益亮[1,2]，郭凯阳[1,2]，吴日铭[1,2]，刘凯[1,2]
（1. 武警工程大学密码工程学院，陕西 西安 710086；
2. 武警部队密码与信息安全保密重点实验室，陕西 西安 710086）

摘 要：为了解决属性加密中的密钥安全问题，基于环上误差学习（RLWE）和有序二元决策图（OBDD）访问结构提出了一种抗密钥滥用的密文策略属性加密方案。首先，构造了 2 个不同的机构来共同生成用户的私钥，降低了机构泄露密钥的风险；其次，在每个私钥中嵌入了用户的特定信息，实现了密钥的可追踪性，并通过维护白名单避免了非法用户和恶意用户的访问。另外，所提方案采用有序二元决策图的访问结构，在支持属性与、或、门限操作的基础上增加了属性的正负值。分析表明，所提方案满足抗合谋攻击和选择明文攻击下的不可区分性安全，降低了存储和计算开销，和其他方案相比更具有实用性。

关键词：属性加密；抗密钥委托滥用；可追踪性；访问结构
中图分类号：TP309
文献标志码：A
DOI: 10.11959/j.issn.1000–436x.2023019

Attribute-based encryption scheme against key abuse based on OBDD access structure from lattice

HAN Yiliang[1,2], GUO Kaiyang[1,2], WU Riming[1,2], LIU Kai[1,2]
1. College of Cryptographic Engineering, Engineering University of PAP, Xi’an 710086, China
2. Key Laboratory of PAP for Cryptology and Information Security, Xi’an 710086, China

Abstract: In order to solve the key security problem in attribute-based encryption, a ciphertext policy attribute-based encryption scheme against key abuse was proposed based on the ring learning with error over ring and the access structure of ordered binary decision diagram. Firstly, two different institutions were constructed to jointly generate the user’s secret key, which reduced the risk of key disclosure by institutions. Secondly, the user’s specific information was embedded in each secret key to realize the traceability of the key, and the access of illegal users and malicious users were avoided by maintaining the white list. In addition, the access structure of ordered binary decision diagram was adopted by the proposed scheme, and the positive and negative values of attributes on the basis of supporting attribute AND, OR and Threshold operation were increased. Analysis shows that the proposed scheme meets the distinguishable security of anti-collusion attack and chosen-plaintext attack, reduces the storage and computing overhead, and it is more practical than other schemes.

Keywords: attribute-based encryption, key-delegation abuse resistance, traceability, access structure

0 引言

随着网络技术的进一步发展，空间中的数据量逐年递增，产生的数据交互需求越来越多，密码学和信息安全技术被广泛应用于各个领域。如何在保证数据安全性的同时最大限度地发挥信息的价值成为当今网络时代向前发展所必须攻克的难关之一。属性加密[1]作为一种新型密码体制改变了传统

收稿日期：2022–07–22；**修回日期：**2022–10–20
基金项目：国家自然科学基金资助项目（No.61572521）；陕西省自然科学基础研究计划基金资助项目（No.2021-JM252）
Foundation Items: The National Natural Science Foundation of China (No.61572521), Basic Research Program of Natural Science in Shaanxi Province (No.2021-JM252)

公钥密码“一对一”的加密模式，在保证数据安全性的同时可以提供灵活的访问控制，在数据的安全共享方面有着先天的优势，自 2005 年提出后，就受到了国内外学者的广泛关注。

在 Sahai 和 Waters 方案[1]的基础上，Goyal 等[2]构造了首个密钥策略的属性加密方案，即将策略嵌入密钥之中，通过密文中的属性信息是否与策略相匹配来决定是否解密成功，这与 Bethencourt 等[3]提出的密文策略属性加密（CP-ABE, cipher-text-policy attribute-based encryption）方案在结构上正好相反，上述 2 种结构也成为日后研究属性加密技术的 2 个重要分支。随着研究的深入，想要更加成熟地应用属性加密技术还面临一些亟待解决的问题，主要包括两类，一类是效率问题，即从访问结构、困难问题、方案设计等方面来提高属性加密技术的性能，使其在面对多用户、多任务量及其他高强度需求时能够有更好的表现；另一类是安全性问题，即解决属性撤销、密钥滥用、隐私泄露、合谋攻击等带来的风险挑战，使方案功能更加完善可靠。

为了解决这些问题，国内外学者进行了大量的研究。在访问结构方面，最初被应用在密文策略属性加密方案中的是“与”门结构，这种结构相对简单，但只能支持属性之间的“与”操作，灵活性不够。因此，Waters[4]采用线性秘密分享方案（LSSS, linear secret sharing scheme）访问结构构造了强数值假设下支持属性与、或和门限操作的 CP-ABE 机制。Ibraimi 等[5]在 2009 年提出的方案采用一般访问树结构，同样实现了支持属性的与、或、门限操作，之后大部分的属性加密方案都采用这 3 种访问结构来构造。2017 年，Li 等[6]将有序二元决策图（OBDD, ordered binary decision diagram）引入 CP-ABE，相较于 LSSS 和访问树，这种结构在与、或、门限操作的基础上还可以提供属性的正负值操作，使访问策略的表达能力更加丰富。之后，孙京宇等[7]在此结构上提出了基于椭圆曲线且支持撤销的 ABE 方案；汪倩倩等[8]提出了可追踪且支持撤销的 CP-ABE 方案，基于决策双线性 Diffie-Hellman（DBDH, decisional bilinear Diffie-Hellman）假设并在标准模型下证明了安全性。在防止密钥滥用方面，Hinek 等[9]最先关注了该问题并提出了解决方案，但是需要通过第三方来协助用户解密，不够实用；Li 等[10]通过在密钥中嵌入特定标记来实现密钥的可追踪性；Liu 等[11-13]针对密钥泄露问题进行了深入研究，提出的方案包括黑盒和白盒追踪，且性能良好。关于密钥委托问题，赵志远等[14]提出了一种支持密钥托管且同时支持属性撤销的 CP-ABE 方案，还将复杂计算进行外包，提高了系统的效率；闫玺玺等[15]提出的方案在解决密钥委托的同时也支持密钥追踪，并通过短签名技术保护了追踪参数。

目前，后量子密码体制的研究已经成为热点和趋势，而在属性加密方面，相较基于双线性映射构造的方案，格基属性加密方案在避免了复杂的双线性配对的基础上还能抗量子计算攻击。Agrawal 等[16]在格基身份加密方案的基础上讨论了格基属性加密方案的可能性；Boyen[17]提出了第一个格基 ABE 方案并将安全性归约到误差学习问题上；Wang 等[18]在 Agrawal 等[16]方案的基础上提出了基于与门的格上 CP-ABE 方案，但不具有实用性；Soo 等[19]构造了一个环上误差学习（RLWE, ring learning with error）问题上的 CP-ABE 方案，在提升策略丰富性的同时，使方案的结构更加简洁；于金霞等[20-21]基于访问树结构设计了一个理想格上的 CP-ABE 方案，然后依靠服务器外包构造了一个可以即时撤销属性的方案；闫玺玺等[22]关注了格基属性加密中的隐私保护问题，通过半策略隐藏的方式保护了用户隐私并在标准模型下证明了安全性；郭凯阳等[23]在属性撤销的基础上关注了属性分层的问题，构造了一个格上可撤销的分层属性加密方案；王想等[24]基于以太坊构造了格上可搜索的 ABE 方案，并将安全性归约于误差学习问题，实现了关键字的细粒度搜索。由于格基属性加密方案的研究历史较短，还有许多问题需要深入研究，本文重点关注了访问结构的优化和抗密钥滥用的问题，主要工作如下。

1) 构造了基于 OBDD 访问结构的方案，丰富了格基属性加密访问策略的形式，除了支持与、或及门限操作外，还支持属性的正负值，同时降低了系统的计算和存储开销，提升了方案的整体性能。

2) 将用户信息嵌入私钥中，实现了对恶意用户的追踪；通过维护白名单，可以实现用户的撤销以及过滤非法用户的功能；通过 2 个不同的机构独立生成用户的部分私钥，降低了授权机构泄露密钥的风险，一定程度上解决了密钥委托的问题。

3) 对所提方案进行了安全性分析，结果表明，所提方案在抗量子攻击的基础上满足抗合谋攻击

和选择明文攻击安全。通过性能对比和仿真实验对所提方案进行了分析，结果表明，所提方案相较其他方案在功能和性能上具有一定优势。

1　预备知识

1.1　格

定义 1[23]　设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 是 n 维空间上的 m 个线性无关向量，s_i 为系数，若该组向量线性组合构成的集合满足

$$\Lambda=\Lambda(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m)=\left\{\sum_{i=1}^{m}s_i\boldsymbol{b}_i,s_i\in Z\right\}$$

则称 Λ 为格，同时称 n 为 Λ 的维数，m 为 Λ 的秩，$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 为 Λ 的一组基。

定义 2　如果存在一个多项式环 $R=\dfrac{Z[x]}{<f(x)>}$ 和一个理想 $I\subseteq R$，且格 $\Lambda\in Z^n$ 与 I 相关，则称其为理想格。

更严格的定义如下。若多项式环 $R=\dfrac{Z[x]}{<f(x)>}$ 满足以下 3 个性质，则称环 $R=\dfrac{Z[x]}{<f(x)>}$ 的理想为 $f(x)$-理想格，也可简写为 I。

1) $f(x)$ 的次数最高项系数为 1。

2) 多项式环 R 在 Z 上是不可约的。

3) 对于环上任意 2 个多项式 $g(x)$ 和 $h(x)$，都存在以下关系

$$\|g(x)h(x)\bmod f(x)\|<\mathrm{poly}(n)\|g(n)\|\|f(x)\|$$

其中，$\mathrm{poly}(n)$ 表示 n 的多项式函数。

定义 3　对于格 Λ 上以向量 $\boldsymbol{c}$ 为中心、σ 为分布标准差的 n 维离散高斯分布 $\rho_{\sigma,c}$，有

$$D_{\Lambda,\sigma,c}(x)=\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\Lambda)}=\frac{\rho_{\sigma,c}(x)}{\sum_{x\in\Lambda}\rho_{\sigma,c}(x)}$$

其中，$\rho_{\sigma,c}(x)=\exp\left(-\pi\dfrac{\|x-c\|^2}{\sigma^2}\right)$。

定义 4　判定性（Decisional）-RLWE 问题[23]。给定安全参数 λ，令 d,q 为基于安全参数上的整数，定义 $R_q=\dfrac{Z_q[x]}{f(x)}$ 为模 $f(x)$ 和 q 的整数多项式环，其中 $f(x)=x^d+1$。给定基于 λ 的离散分布 $\chi\subset R_q$，$e\leftarrow R_q$ 为 χ 上的随机噪声，对于均匀分布的密钥 $s\in R_q$，针对指定的挑战模型 O，通过输出结果来判定其是含有噪声的伪随机采样机 O_s，还是真正的随机采样机 O_s'。

O_s 输出伪随机样本 $(\omega,v)=(\omega,\omega s+e)\in R_q\times R_q$；$O_s'$ 输出真正的随机采样样本 $(\omega,v)\in R_q\times R_q$。

给定 $s\in R_q$ 时，攻击者可对 O 重复询问，其成功的优势定义为

$$\mathrm{adv}^{\mathcal{A}}=\left|\Pr[\mathcal{A}^{O_s}=1]-\Pr[\mathcal{A}^{O_s'}=1]\right|$$

其中，Pr[·]表示概率，若以上优势可忽略，那么认为其破解 Decisional-RLWE 问题是困难的。

1.2　OBDD 访问结构

二元决策图中有 2 种节点，终端节点和非终端（决策）节点，2 种节点都会被标记 0 或 1，终端节点没有子节点。对于非终端节点，其标记为 0 时的子节点为低节点，标记为 1 时的子节点为高节点，OBDD 是指所有变量顺序固定的一种特殊二元决策图[23]。

当访问策略中存在 m 个属性元素，假设其布尔函数表达为 $f(x_1,x_2,\cdots,x_m)$，由香农展开定理可得

$$f(x_1,x_2,\cdots,x_m)=x_if_{|x_i=1}+x_i'f_{|x_i=0},1\leqslant i\leqslant m$$

其中，$f_{|x_i=1}$ 和 $f_{|x_i=0}$ 是布尔函数 f 的协因子。香农展开是一个递归过程，需要预先指定变量的顺序。OBDD 中的每个非终端节点可以由四元组 $<i,\mathrm{id},\mathrm{low},\mathrm{high}>$ 表示，其中，i 表示属性编号，id 表示节点的唯一序列号，low 表示指向低子节点，high 表示指向高子节点。则可得 OBDD 访问结构的表达式为 $\{\mathrm{Node}_{\mathrm{id}}^{i}\mid \mathrm{id}\in\mathrm{Id},i\in\mathrm{IA}\}$，其中，Id 表示决策节点的序号集，IA 表示访问结构中的属性集合。访问策略转换成 OBDD 访问结构的具体算法如算法 1 所示，其中，Construct-OBDD(f,i)表示访问结构。

算法 1　访问策略转换成 OBDD 访问结构

输入　布尔函数 f、属性集 IA

输出　OBDD 访问结构

1) $i\leftarrow 0$

2) return OBDD = Construct-OBDD(f,i)

3) function Construct-OBDD(f,i)

4)　id $\leftarrow 1$

5)　if $i>n-1$ then

6)　　if $f==1$ then

7)　　id $\leftarrow 1$

8)　　else

9) id ← 0
10) end if
11) else
12) high ← Construct-OBDD($f_{x_i=1}, i+1$)
13) low ← Construct-OBDD($f_{x_i=0}, i+1$)
14) id ← id + 1
15) return $\text{Node}_{\text{id}}^{i}$
16) end if
17) end function

判断属性集是否满足访问策略的过程如下。对于含有属性 i 的非终端节点，若 $i \in D$，则沿 high 转向高子节点；否则，沿 low 转向低子节点。迭代以上步骤直到终端节点，若终端节点是 1，则属性集 D 符合 OBDD 访问结构；若终端节点是 0，则不符合。具体有效路径搜索算法如算法 2 所示。

算法 2 搜索 OBDD 有效路径
输入 OBDD 访问结构、用户属性集 D
输出 有效路径 P_j \失败 $\perp$

1) Cur-Node ← 2
2) function Get-Path(OBDD, D, Cur-Node)
3) if $i \in D \wedge \underline{i} = i$ then
4) if Cur-Node.high == 0 then
5) return fail
6) else if Cur-Node.high == 1 then
7) return Cur-Node
8) else
9) Cur-Node = Cur-Node.high
10) path.next = Get-Path(OBDD, D, Cur-Node)
11) end if
12) else
13) if Cur-Node.low == 0 then
14) return fail
15) else if Cur-Node.low == 1 then
16) return Cur-Node
17) else
18) Cur-Node = Cur-Node.low
19) path.next = Get-Path(OBDD, D, Cur-Node)
20) end if
21) end if
22) end function

在布尔函数转换的过程中，当给定变量序后通常采取以下 2 个简化规则来删除 OBDD 中的冗余节点。

1) S-删除规则。当节点 u 存在 u.low = u.high 时，删除 u，并将 u 的父节点直接连到 u.low 所对应的节点处。

2) 合并规则。对于节点 u 和 v，当存在 u.low = v.low 和 u.high = v.high 时，删除其中任一节点，并将其父节点连至剩下的节点处。

例如，访问策略的布尔表达式为 $f\{a_1, a_2, a_3\} = a_1 \wedge (a_2' \vee a_3)$，其中，$a_j$ 表示属性正值，a_j' 表示属性负值，对应的 OBDD 访问结构如图 1 所示。图 1 中，实线表示子节点为高，虚线表示子节点为低，则从根节点到终端节点为 1 的所有有效路径都是满足访问策略的属性集。

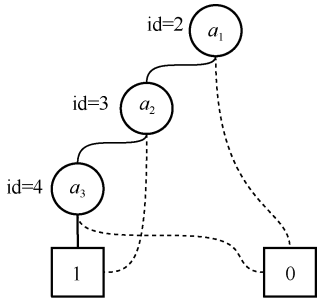


图 1 OBDD 访问结构

2 方案设计与安全模型

为了提升对大型文件的处理效率，本文方案采用对称加密将数据进行加密，并将其上传到数据服务器保存，这样需要属性加密的明文一般只包括文件的对称密钥。在密钥安全方面，方案设立了身份中心和属性中心 2 个独立的机构来分管用户的个人信息和生成密钥。其中，身份中心只能获取用户的 ID 信息，无法获取属性集信息；而属性中心只能获取该用户的属性集信息，无法获取 ID 信息。这样保证了任何一个机构都不能掌握用户完整的私钥，增加了机构泄露用户密钥的难度，通过在私钥中嵌入特定信息，当发生密钥泄露时，可以通过密钥追踪到相应的用户并采取撤销等措施降低损失。本文方案还在用户访问数据服务器前增加了白名单匹配，不在名单上的用户包括未成功注册的用户及被撤销的用户等，通过维护这样的白名单可以减少不必要的信息传输并防止非法用户进行数据访问。

2.1　形式化描述

系统模型如图 2 所示，主要包括以下 6 个主体。

可信机构（CA, certificate authority）。CA 为完全可信的主体，严格执行规范要求，生成系统的公共参数和主密钥并负责对泄露密钥的追踪。

身份中心（IC, identity center）。IC 为用户生成唯一的标记 ID，生成身份私钥及属性中心需要的参数，维护访问白名单，假设该实体是诚实但好奇的，会按照要求执行各种操作，但会尝试解密密文，且无法与用户或属性中心进行合谋。

属性中心（AC, attribute center）。AC 为用户生成属性私钥并负责发送和更新版本号，和身份中心相同假设该实体是诚实但好奇的，且无法与用户或身份中心进行合谋。

数据服务器（DS, data server）。DS 存储数据并对需要访问的用户进行白名单检索，假设该实体是诚实但好奇的。

数据拥有者（DO, data owner）。DO 将对称加密的数据上传到数据服务器，并将对称密钥通过自己制定的策略生成密文上传到数据服务器上。

数据用户（DU, data user）。DU 可以访问需要的数据。

本文方案包括以下算法。

1) 初始化算法

$\text{Setup}(\lambda,U)\rightarrow \text{PP,MSK}$。由 CA 执行，确定安全参数 λ，输入包含所有属性的集合 U，输出公共参数 PP 和主密钥 MSK。

2) 加密算法

$\text{Encrypt}(\text{PP},M,A,\beta)\rightarrow \text{CT}$。由 DO 执行，输入 PP、明文数据 M 和访问策略 A 及版本号 β，输出密文 CT。

3) 身份私钥生成算法

$\text{IKeyGen}(\text{MSK},\text{ID})\rightarrow K_\alpha,K_\beta,t,\sigma$。由 IC 执行，输入 MSK 和用户的 ID，为用户输出身份私钥 K_α 和 K_β，之后向可信机构传递安全追踪参数 σ，以及向属性中心发送计算参数 t。将所有合法用户的身份私钥 K_β 汇总成系统白名单后再同步到数据服务器。

4) 属性私钥生成算法

$\text{AKeyGen}(\text{PP},\text{MSK},D,t,\beta)\rightarrow K_z$。由 AC 执行，输入 PP、MSK、用户的属性集 D、参数 t、版本号 β，输出属性私钥 K_z，其中版本号表示只有相同版本的密文和密钥才能实现解密的功能。版本号只能由属性中心设定且不会随意更改，并会随密钥一同发送给合法用户，为了便于表示，令 $\text{sk}=(K_\alpha,K_\beta,K_z)$。

5) 解密算法

$\text{Decrypt}(\text{PP},\text{CT},\text{sk})\rightarrow M$。由 DU 执行，输入公共参数 PP、密文 CT、用户的密钥 sk，解密成功输出 M，否则输出 $\perp$。

6) 追踪算法

$\text{Trace}(\text{MSK},\text{sk})\rightarrow \text{ID}$。由 CA 执行，输入主密钥 MSK、用户的密钥 sk，追踪成功则输出 ID，失败则输出 $\perp$。

本文方案流程如图 3 所示。为了便于展示，图 3 中设定密钥生成算法是在用户加密数据之前，但实际上这是 2 个不同用户的操作，理论上数据用户申请密钥和数据用户加密数据这 2 个过程不区分时间

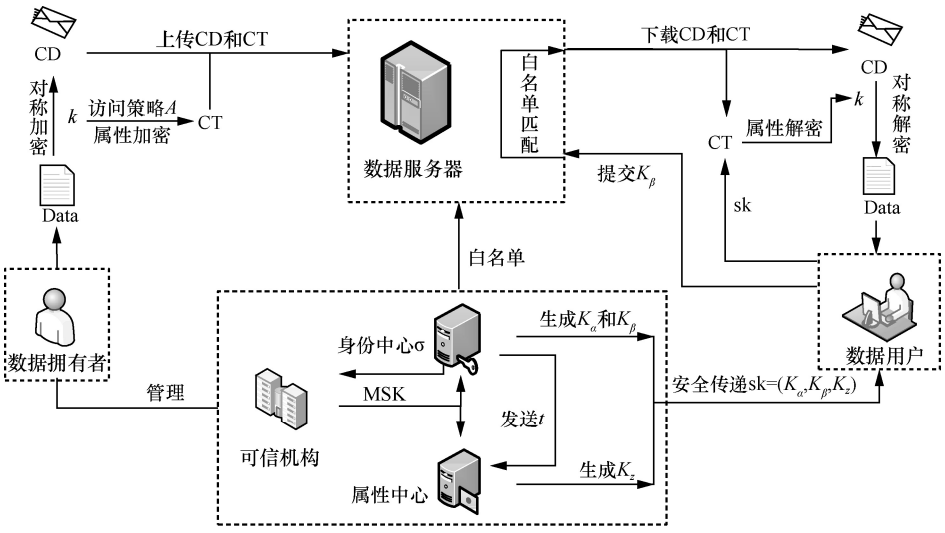


图 2　系统模型

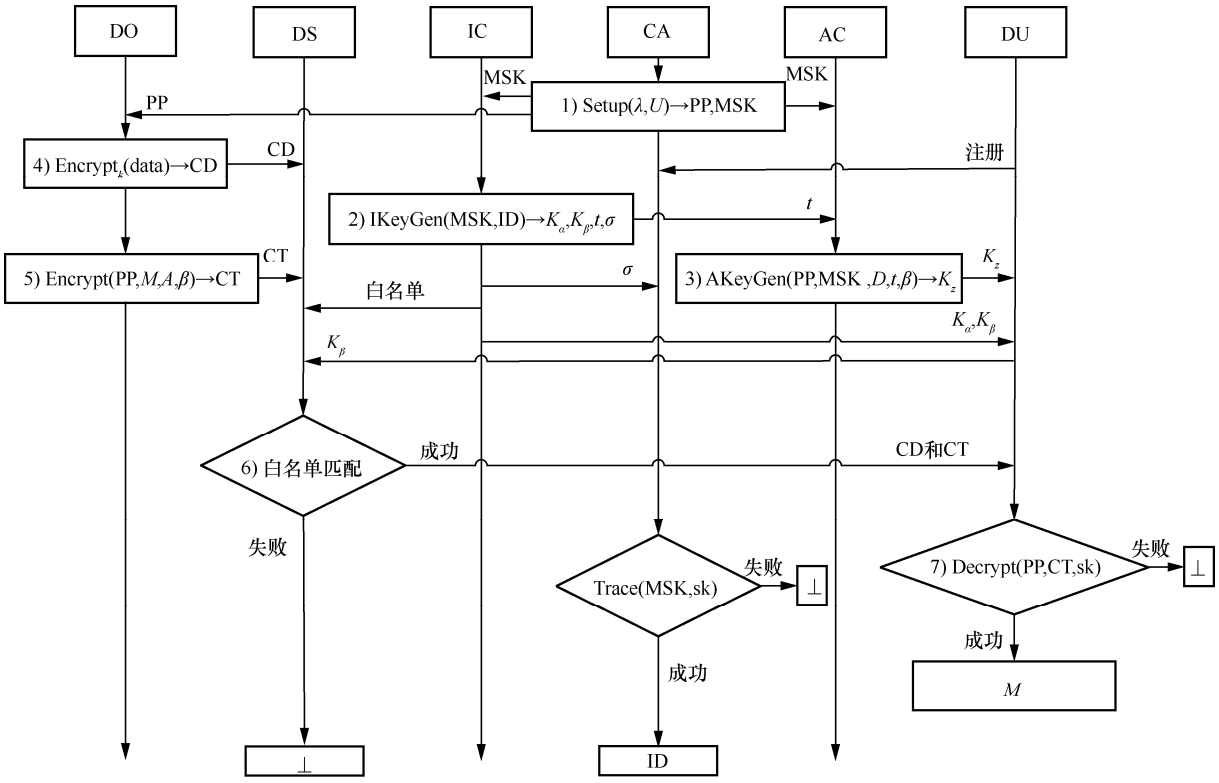


图 3 本文方案流程

先后顺序。为了保证表述的完整性，将追踪算法也在图 3 中进行展示，但需要注意的是该算法同样与其他算法不存在时间先后顺序。

2.2 安全模型

2.2.1 属性加密机制的安全模型

此类攻击者通常为不诚实的用户，通过描述攻击者 $\mathcal{A}_1$ 和模拟器 $\mathcal{B}$ 的交互游戏来定义属性加密机制的安全模型，该游戏为选择策略和选择明文攻击下的不可区分性游戏，具体过程如下。

初始化 $\mathcal{A}_1$ 选择一个要挑战的访问策略 A^*，并发送给 $\mathcal{B}$。

系统设置 $\mathcal{B}$ 运行算法为 $\mathcal{A}_1$ 生成 PP 和 MSK，并将 PP 发送给 $\mathcal{A}_1$。

阶段 1 $\mathcal{A}_1$ 发送私钥查询请求，$\mathcal{B}$ 收到 $\mathcal{A}$ 的请求后为其生成私钥并发送给 $\mathcal{A}_1$，注意查询的私钥其属性集并不满足 A^*。

挑战 $\mathcal{A}_1$ 随机选择长度相同的明文信息 $M_0, M_1 \in \{0,1\}^n$ 发送给 $\mathcal{B}$。$\mathcal{B}$ 通过抛一枚均匀硬币来决定 $b \in \{0,1\}$，计算出挑战密文 c' 后发送给 $\mathcal{A}_1$。

阶段 2 重复阶段 1。

猜测 $\mathcal{A}_1$ 对 $\mathcal{B}$ 提交关于 b 的猜想 b'。

若 $b'=b$ 且查询的私钥其属性集始终不满足 A^*，则攻击者赢得此游戏，攻击者在该游戏中的优势定义为 $\left|\Pr[b'=b]-\frac{1}{2}\right|$。

定义 5 若任意攻击者在多项式时间内赢得上述游戏的优势是可忽略的，则本文方案满足选择策略和选择明文攻击下的密文不可区分性安全。

2.2.2 可追踪性模型

此类攻击者通常为恶意用户或第三方敌手，通过伪造新的密钥或改变密钥中的身份信息企图实现抗密钥追踪。通过描述攻击者和模拟器之间的交互游戏来定义方案的可追踪模型，具体过程如下。

初始化 模拟器运行算法生成公共参数并发送给攻击者 $\mathcal{A}_2$。

密钥查询 攻击者向模拟器询问不同身份的用户私钥。

密钥伪造 攻击者输出一个用户私钥 sk^*。

若运行追踪算法 $\mathrm{Trace}(\mathrm{MSK},\mathrm{sk}^*)\neq\perp$ 且 $\mathrm{Trace}(\mathrm{MSK},\mathrm{sk}^*)\to \mathrm{ID}^*$，$\mathrm{ID}^*\notin\{\mathrm{ID}_i\}$，其中 $\{\mathrm{ID}_i\}$ 表示系统中合法用户的 ID 集合，则认为攻击者赢得此游戏。攻击者在该游戏中的优势定义为 $\Pr[\mathrm{Trace}(\mathrm{MSK},\mathrm{sk}^*)\notin\perp\cup\{\mathrm{ID}_i\}]$。

定义 6　若任意攻击者在多项式时间内赢得上述游戏的优势是可忽略的，则本文方案满足可追踪性安全。

3　具体构造

$\text{Setup}(\lambda,U)\to \text{PP},\text{MSK}$。确定安全参数 λ 以及包含所有属性的集合 U，选择一个大素数 $q=1\bmod(2\lambda)$ 和一个较小的正整数 p，满足 $p\ll q$ 且 $\gcd(p,q)=1$。令 $R_q=\dfrac{Z_q[x]}{\langle f(x)\rangle}$ 表示模 $f(x)=x^n+1$ 和 q 的多项式环，$\chi=\chi(\lambda)$ 表示 R_q 上的误差分布，均匀随机选择 $(\text{SK}_0,\text{SK}_0^{-1})\leftarrow R_q$、$a\leftarrow R_q$ 以及噪声 $e_0\leftarrow\chi$，计算 $\text{PK}_0=a\text{SK}_0+pe_0\in R_q$。对于在 U 中的每一个正值属性，随机选择 $k_i\leftarrow R_q$；对于在 U 中的每一个负值属性，随机选择 $k_i'\leftarrow R_q$，方便起见令 $\overline{k_i}$ 表示这 2 种情况。输出公共参数 $\text{PP}=\left\{a,\text{PK}_0,\overline{k_i}\mid i\in U\right\}$ 和主密钥 $\text{MSK}=\left\{\text{SK}_0,\text{SK}_0^{-1}\right\}$。

$\text{Encrypt}(\text{PP},M,A,\beta)\to\text{CT}$。输入 PP、明文消息 M、访问策略 A 及版本号 β，将访问策略根据算法 1 转换成 OBDD 访问结构，$\text{OBDD}=\{\text{Node}_{\text{id}}^{i}\mid \text{id}\in\text{Id},i\in\text{IA}\}$，IA 是访问策略中包括的属性集合，Id 是所有非终端节点的编号，设访问结构从根节点到终端节点的有效路径有 V 个，满足访问结构的有效路径可表示为 $\{P_j,j\in[0,V-1]\}$。随机均匀选择噪声 e'，$e_j'\leftarrow\chi$，计算 $Z_j=\sum_{i\in I_j}\overline{k_i}$，其中 IA_j 是每个路径上包括的属性集合。输出密文 $\text{CT}=(\text{OBDD},C_0,C_{P_j})$，其中 $C_0=ra+pe'\in R_q$，$C_{P_j}=ra\beta Z_j+r\text{PK}_0+M+pe_j'\in R_q$，$j\in[0,V-1]$。

$\text{IKeyGen}(\text{MSK},\text{ID})\to K_\alpha,K_\beta,t,\sigma$。输入主密钥 MSK、用户 ID，随机选择 $\sigma\leftarrow R_q$ 和一对互逆元素 $(t,t^{-1})\leftarrow R_q$ 以及噪声 $e''\leftarrow\chi$。计算身份私钥

$$K_\alpha=\text{SK}_0t^{-1}+pe''\in R_q$$

$$K_\beta=\text{SK}_0(\text{ID}+K_\alpha+\sigma)\in R_q$$

并将 σ 作为安全追踪参数传递给可信机构，将 t 作为计算参数安全传递给属性中心。

$\text{AKeyGen}(\text{PP},\text{MSK},D,t,\beta)\to K_z$。输入公共参数 PP、主密钥 MSK、用户的属性集合 D 及参数 t，随机选择 $e_a\leftarrow\chi$，对于系统中每个属性，若 $i\in D$，则对应的属性私钥值为 k_i；若 $i\notin D\wedge i\in U$，则对应的属性私钥值为 k_i'，令 $Z_k=\sum_{i\in D}\overline{k_i}$，计算

$$K_z=t\beta Z_k\text{SK}_0^{-1}+t+pe_a\in R_q$$

则通过以上 2 个算法，用户最终得到的密钥为 $\text{sk}=(K_\alpha,K_\beta,K_z)$。

$\text{Decrypt}(\text{PP},\text{CT},\text{sk})\to M$。输入公共参数 PP、密文 CT 及用户的密钥 sk，通过 OBDD 路径搜索算法来确认用户是否满足访问策略，若满足，有 $\sum_{i\in D}\overline{k_i}=\sum_{i\in I_j}\overline{k_i}$，即 $Z_k=Z_j$，则有 $M'=C_{P_j}-C_0K_\alpha K_z$，$M=M'\bmod p$。输出 M。

$\text{Trace}(\text{MSK},\text{sk})\to\text{ID}$。输入主密钥 MSK 和用户私钥 sk，计算

$$\text{ID}=\text{SK}_0^{-1}K_\beta-K_\alpha-\sigma$$

得到这个密钥所嵌入的特定用户信息。

4　方案分析

4.1　正确性分析

首先，通过追踪算法的计算过程来验证方案追踪密钥的正确性。根据算法可知，可信机构拥有 $\text{MSK}=\left\{\text{SK}_0,\text{SK}_0^{-1}\right\}$ 和身份中心传递的安全追踪参数 σ。则根据追踪算法有

$$\text{ID}=\text{SK}_0^{-1}K_\beta-K_\alpha-\sigma$$

计算过程为

$$\begin{aligned}&\text{SK}_0^{-1}K_\beta-K_\alpha-\sigma=\\&\text{SK}_0^{-1}\text{SK}_0(\text{ID}+K_\alpha+\sigma)-K_\alpha-\sigma=\\&\text{ID}+K_\alpha+\sigma-K_\alpha-\sigma=\text{ID}\end{aligned}$$

根据 ID 可以追踪到持有该密钥的用户。

接下来，通过解密部分来验证方案的正确性，下面根据算法内容对该部分进行分析，当合法用户的属性集满足数据拥有者设定的访问策略时，根据 OBDD 访问结构特性，必然存在 $\sum_{i\in D}\overline{k_i}=\sum_{i\in I_j}\overline{k_i}$，使 $Z_k=Z_j$，用户根据自己密钥中的 K_α 和 K_z 可计算 $M'=C_{P_j}-C_0K_\alpha K_z$，具体计算过程如下。

$$M' = C_{P_j} - C_0 K_\alpha K_z =$$
$$C_{P_j} - (ra + pe')(\mathrm{SK}_0 t^{-1} + pe'')(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a) =$$
$$C_{P_j} - (ra + pe')(\beta Z_k + \mathrm{SK}_0 + p(e_a \mathrm{SK}_0 t^{-1} +$$
$$e''(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a))) =$$
$$C_{P_j} - (ra\beta Z_k + ra\mathrm{SK}_0 +$$
$$pe'((Z_k + \mathrm{SK}_0 + p(e_a \mathrm{SK}_0 t^{-1} +$$
$$e''(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a))) +$$
$$pra(e_a \mathrm{SK}_0 t^{-1} + e''(t\mathrm{SK}_0^{-1} Z_k + t + pe_a))) =$$
$$(ra\beta Z_j + r\mathrm{PK}_0 + M + pe_j') -$$
$$(ra\beta Z_k + ra\mathrm{SK}_0 + pe'((Z_k + \mathrm{SK}_0 +$$
$$p(e_a \mathrm{SK}_0 t^{-1} + e''(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a))) +$$
$$pra(e_a \mathrm{SK}_0 t^{-1} + e''(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a))) =$$
$$(ra\beta Z_j + ra\mathrm{SK}_0 + pre_0 + M + pe_j') -$$
$$(ra\beta Z_k + raSK_0 + pe'((Z_k + SK_0 +$$
$$p(e_a \mathrm{SK}_0 t^{-1} + e''(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a))) +$$
$$pra(e_a \mathrm{SK}_0 t^{-1} + e''(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a))) =$$
$$M + pre_0 + pe_j' - pe'((Z_k + \mathrm{SK}_0 +$$
$$p(e_a \mathrm{SK}_0 t^{-1} + e''(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a))) +$$
$$pra(e_a \mathrm{SK}_0 t^{-1} + e''(t\beta \mathrm{SK}_0^{-1} Z_k + t + pe_a)))$$

进一步可得到 $M = M' \bmod p$。

4.2 安全性分析

本节主要围绕方案中属性加密机制的安全性、可追踪性、抗合谋攻击以及抗密钥委托滥用 4 个方面进行分析。

4.2.1 属性加密机制的安全性

定理 1[23] 如果任意多项式时间内存在一个攻击者 $\mathcal{A}_1$ 以 ε 的优势赢得 2.2.1 节中定义的选择策略和选择明文攻击下的不可区分性游戏，则存在一个模拟器 $\mathcal{B}$ 可以以 $\frac{\varepsilon}{2}$ 的优势判定 RLWE 问题。

证明 $\mathcal{B}$ 询问挑战预言机 O $(t+1)$ 次，返回 $(\omega_k, \upsilon_k) \in R_q \times R_q$，其中 $k \in \{0,1,2,\cdots,t\}$，游戏按照以下步骤运行。

初始化 给定系统中所有属性集合 U，$\mathcal{A}_1$ 提交要挑战的访问结构 A^*。

系统设置 $\mathcal{B}$ 运行系统初始化 Setup(λ, U) 算法，构造公共参数 PP。随机选择 $a \leftarrow R_q$，定义 $\mathrm{PK}_0 = p\omega_0 \in R_q$，模拟器 $\mathcal{B}$ 对于在 U 中的每一个正值属性，随机选择 $k_i \leftarrow R_q$；对于在 U 中的每一个负值属性，随机选择 $k_i' \leftarrow R_q$，接下来，$\mathcal{B}$ 返回 $\mathrm{PP} = \left\{a, \mathrm{PK}_0, \overline{k_i} \mid i \in U\right\}$ 给 $\mathcal{A}_1$。

阶段 1 查询密钥。$\mathcal{A}_1$ 进行私钥查询，由于其属性集不满足 A^*，即 $\mathcal{A}_1$ 无法计算出有效的 OBDD 路径。$\mathcal{B}$ 通过 IKeyGen 和 AKeyGen 算法返回 $\mathrm{sk} = (K_\alpha, K_\beta, K_z)$ 给攻击者，其中

$$K_\alpha = \mathrm{SK}_0 t^{-1} + pe'' \in R_q$$
$$K_\beta = \mathrm{SK}_0(\mathrm{ID} + K_\alpha) \in R_q$$
$$K_z = t\beta Z_k \mathrm{SK}_0^{-1} + t + pe_a \in R_q$$

挑战阶段 $\mathcal{A}_1$ 随机发送挑战消息 $M_0, M_1 \in \{0,1\}$ 给 $\mathcal{B}$，$\mathcal{B}$ 随机选择 $b \in (0,1)$ 然后对 M_b 进行加密，根据 A^* 得到 $\mathrm{OBDD} = \{\mathrm{Node}_{\mathrm{id}}^i \mid \mathrm{id} \in \mathrm{Id}, i \in \mathrm{IA}\}$，计算出所有的 $Z_j = \sum_{i \in I_j} \overline{k_i}$，随机均匀选择噪声 e'，$e_j' \leftarrow \chi$，输出密文 $\mathrm{CT} = (C_0, C_{P_j})$ 发送给攻击者 $\mathcal{A}_1$，其中

$$C_0 = ra + pe' \in R_q$$
$$C_{P_j} = ra\beta Z_j + rPK_0 + M + pe_j' \in R_q, \quad j \in [0, V-1]$$

阶段 2 重复阶段 1。

猜测阶段 $\mathcal{B}$ 收到 $\mathcal{A}_1$ 的猜测值 b'，并以此作为对 Decisional-RLWE 问题的回答。若 $b' = b$，输出 $O' = O_s$，那么 $\mathcal{A}_1$ 优势为 ε，则有

$$|\Pr[b' = b \mid O = O_s]| = \frac{1}{2} + \varepsilon$$
$$|\Pr[O' = O \mid O = O_s]| = \frac{1}{2} + \varepsilon$$

若 $b' \neq b$，输出 $O' = O_s'$，此时有

$$|\Pr[b' \neq b \mid O = O_s']| = \frac{1}{2}$$
$$|\Pr[O' = O \mid O = O_s']| = \frac{1}{2}$$

综上，$\mathcal{B}$ 成功判定 RLWE 问题的优势为

$$\frac{1}{2}\left|\Pr[O' = O \mid O = O_s]\right| + \frac{1}{2}\left|\Pr[O' = O \mid O = O_s']\right| - \frac{1}{2} =$$
$$\frac{1}{2}\left(\frac{1}{2} + \varepsilon\right) + \frac{1}{2}\left(\frac{1}{2}\right) - \frac{1}{2} = \frac{\varepsilon}{2}$$

证毕。

4.2.2 可追踪性

定理 2 如果任意多项式时间内攻击者 $\mathcal{A}_2$ 可以赢得 2.2.2 节中定义的可追踪模型的优势为 ε，则

存在一个模拟器$\mathcal{B}$可以以$\frac{\varepsilon}{2}$的优势判定 RLWE 问题。

证明　$\mathcal{B}$询问挑战预言机O $(t+1)$次，返回$(\omega_k,\upsilon_k)\in R_q\times R_q$，其中$k\in\{0,1,2,\cdots,t\}$，游戏按照以下步骤运行。

初始化　$\mathcal{B}$确定安全参数λ，输入包含所有属性的集合U，选择一个大素数$q=1\bmod(2\lambda)$和一个较小的正整数p，满足$p\ll q$且$\gcd(p,q)=1$。令$R_q=\frac{Z_q[x]}{\langle f(x)\rangle}$表示模$f(x)=x^n+1$和$q$的多项式环，$\chi=\chi(\lambda)$表示$R_q$上的误差分布，均匀随机选择$(\mathrm{SK}_0,\mathrm{SK}_0^{-1})\leftarrow R_q$，$a\leftarrow R_q$以及噪声$e_0\leftarrow\chi$，计算$\mathrm{PK}_0=a\mathrm{SK}_0+pe_0\in R_q$。对于在$U$中的每一个正值属性，随机选择$k_i\leftarrow R_q$；对于在$U$中的每一个负值属性，随机选择$k_i'\leftarrow R_q$，输出公共参数$\mathrm{PP}=\left\{a,\mathrm{PK}_0,\overline{k_i}\mid i\in U\right\}$发送给攻击者$\mathcal{A}_5$。

密钥查询　攻击者$\mathcal{A}_2$向模拟器询问不同身份的用户私钥，假设被询问的用户为ID_i，随机选择$\sigma\leftarrow R_q$和一对互逆元素$(t,t^{-1})\leftarrow R_q$以及噪声$e''\leftarrow\chi$。计算身份私钥

$$K_\alpha=\mathrm{SK}_0t^{-1}+pe''\in R_q$$

$$K_\beta=\mathrm{SK}_0(\mathrm{ID}+K_\alpha+\sigma)\in R_q$$

然后，属性中心随机选择$e_a\leftarrow\chi$，对于系统中每个属性，若$i\in D$，则对应的属性私钥值为k_i；若$i\notin D\wedge i\in U$，则对应的属性私钥值为k_i'，令$Z_k=\sum_{i\in D}\overline{k_i}$，计算

$$K_z=t\beta Z_k\mathrm{SK}_0^{-1}+t+pe_a\in R_q$$

则模拟器返回给攻击者的密钥为$\mathrm{sk}=(K_\alpha,K_\beta,K_z)$。

密钥伪造　攻击者$\mathcal{A}_2$输出一个用户私钥$\mathrm{sk}^*=(K_\alpha^*,K_\beta^*,K_z^*)$给模拟器。若攻击者没有赢得游戏，则输出$O'=O_s'$，此时有

$$|\Pr[\mathcal{A}_2\overline{\mathrm{win}}\mid O=O_s']|=\frac{1}{2}$$

$$|\Pr[O'=O\mid O=O_s']|=\frac{1}{2}$$

若攻击者赢得游戏，则输出$O'=O_s$，由于$\mathcal{A}_2$优势为ε，则

$$|\Pr[\mathcal{A}_2\mathrm{win}\mid O=O_s]|=\frac{1}{2}+\varepsilon$$

$$|\Pr[O'=O\mid O=O_s]|=\frac{1}{2}+\varepsilon$$

综上，$\mathcal{B}$成功判定 RLWE 问题的优势为

$$\frac{1}{2}\left|\Pr[O'=O\mid O=O_s]\right|+\frac{1}{2}\left|\Pr[O'=O\mid O=O_s']\right|-\frac{1}{2}=\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\left(\frac{1}{2}\right)-\frac{1}{2}=\frac{\varepsilon}{2}$$

证毕。

4.2.3　抗合谋攻击

定义此类攻击者为多个恶意用户，为便于描述，称其为攻击者 3。其拥有任意多个用户密钥并企图合谋来解密超出他们能力之外的密文。

针对攻击者 3，作为合法用户，其拥有属于自己的私钥，其中

$$K_\alpha=\mathrm{SK}_0t^{-1}+pe''\in R_q$$

$$K_\beta=\mathrm{SK}_0(\mathrm{ID}+K_\alpha+\sigma)\in R_q$$

$$K_z=t\beta Z_k\mathrm{SK}_0^{-1}+t+pe_a\in R_q$$

其中，K_α、K_β和K_z均是均匀分布在环上的元素，且在私钥生成过程中，由于$(t,t^{-1})\leftarrow R_q$和σ为随机均匀产生，因此即使拥有相同属性集的用户，其得到的私钥也是不同的，除非其能够解决 Decisional-RLWE 问题，否则恶意用户从不同的私钥中难以分析得到有效信息，也就无法伪造密钥来破解超出其自身属性范围的密文，因此本文方案满足抗合谋攻击安全。

4.2.4　抗密钥委托滥用

定义攻击者主要有两类，一类为恶意的身份中心，称为攻击者 4，此类攻击者拥有系统的主密钥，并尝试解密密文，但这类攻击者不能和用户或属性中心合谋；另一类为恶意的属性中心，称为攻击者 5，其与攻击者 4 类似拥有系统的主密钥，并尝试解密密文，但不能和用户或身份中心合谋。

针对攻击者 4，其掌握主私钥和用户的 ID，可以生成部分私钥，但由于其无法获取用户的属性集信息，因此无法伪造某用户的属性私钥K_z来诬陷该用户，通过公共参数攻击者 3，可以尝试构造一个新的属性集来伪造新的属性私钥，但由于版本号由属性中心设定，系统中可以获得版本号信息的是属性中心及合法用户，根据攻击者 4 的定义，其无法与

属性中心或其他用户进行合谋，因此无法获得正确的版本号，则其伪造的私钥将无法解密密文。

攻击者 5 与攻击者 4 类似，其掌握主私钥和用户的属性集信息，可以生成属性私钥 K_z，但其不掌握用户的 ID 信息，且用户专属的安全追踪参数只有身份中心和可信机构知道，根据定义，攻击者 5 无法伪造出 K_β，在不和身份中心或用户合谋的情况下，其将无法通过白名单检索及成功解密密文。综上，在身份中心和属性中心无法合谋的条件下，本文方案解决了机构委托的问题。

4.3 性能分析

本节将选取一些具有代表性的方案，从功能性和效率方面与本文方案进行分析对比。为了便于理解，将涉及的符号进行统一说明，如表 1 所示。

表 1 符号说明

符号	意义
N	系统属性数量
A_u	用户属性数量
A_c	策略中的属性数量
m_1、m_2	陷门参数
V	有效路径数量
l	系统中属性机构数量

4.3.1 功能性分析

本节选取了一些抗密钥滥用的属性加密方案，从访问结构、困难问题、可追踪性和抗密钥委托以及撤销机制和抗量子威胁几个方面进行分析，功能比较如表 2 所示。文献[8]方案实现了可追踪性和属性级的细粒度撤销，基于 OBDD 的结构支持属性正负值表达，但没有抗密钥委托的功能；文献[14]方案实现了在抗密钥委托的同时可以提供用户级和属性级粒度的撤销操作，但无法追踪密钥；文献[15]方案同时实现了追踪和抗密钥委托 2 个功能，并且通过短签名技术还可以防止追踪参数被伪造，但只支持与门结构，且没有提供撤销功能；本文方案实现了可追踪性、抗密钥委托和用户级的撤销外，可以抵抗量子攻击的威胁，采用和文献[8]相同的访问结构，在策略的表达上要优于文献[14-15]方案，但本文方案目前只是通过维护白名单实现了用户级的撤销，并不能实现更加细粒度的属性级撤销。

4.3.2 效率分析

本节选取了一些格基属性加密方案从存储性能、计算开销和通信开销等方面进行分析，假设方案中区分正负属性，并且设定系统中正负属性各为 N，则系统中总共包含的所有属性数量为 $2N$。

1) 存储性能

本节主要从系统公钥、主私钥、密钥及密文长度等几个方面对存储开销进行对比，结果如表 3 所示。方案 1 和方案 3 基于 LWE 问题进行构造，系统公钥、系统私钥、用户私钥和密文的长度远大于方案 2 和本文方案。与方案 2 相比，除了系统公钥长度相同外，本文方案的系统私钥和用户私钥长度均远小于方案 2。而且本文方案的系统私钥、用户私钥和密文的长度均不受属性数量的影响，其中系统私钥和用户私钥的存储开销是定值，当系统私钥

表 2 功能比较

对比方案	访问结构	困难问题	可追踪性	抗密钥委托	撤销机制	抗量子威胁
文献[8]方案	OBDD	DBDH	√	—	属性级	—
文献[14]方案	LSSS	q-BDHE	—	√	用户/属性级	—
文献[15]方案	与门	DBDH	√	√	—	—
本文方案	OBDD	RLWE	√	√	用户级	√

表 3 存储开销对比

方案	系统公钥长度	系统私钥长度	用户私钥长度	密文长度
方案 1[25]	$n(km_1+1)\log q$	$lm_1^2\log q$	$m_1A_u\log q$	$(m_1A_c+1)\log q$
方案 2[22]	$n(2N+2)\log q$	$n(4N+1)\log q$	$n(A_u+1)\log q$	$n(A_c+1)\log q$
方案 3[26]	$n(m_2+1)\log q$	$m_2^2\log q$	$2m_2A_u\log q$	$(2m_2A_c+1)\log q$
本文方案	$n(2N+2)\log q$	$2n\log q$	$3n\log q$	$n(V+1)\log q$

和用户私钥中包含的属性越多时，本文方案的存储开销优势越明显。同时本文方案的密文长度与 OBDD 访问结构中的有效路径数量 V 呈正相关，当 $V \leqslant A_c$ 时，本文方案的密文长度不会大于方案 2 的密文长度。综合以上情况来看，本文方案的整体存储性能要优于其他 3 个方案。

模拟访问策略的布尔表达式为 $f(a,b,c,d)=a+b'c+bd'+c'd$，可知系统中有 4 正 4 负共 8 个属性，则 $A_c=8$，又由 OBDD 访问结构可推算出 $V=5$，同时令 $q=257$，$n=128$，假设系统中属性数量 $N=30$，用户私钥中属性数量 $A_u=15$，再由文献[22,25-26]可知，陷门参数 $m_1=5n\log q$，$m_2=6n\log q$。通过以上数据可以模拟不同方案的存储开销，如图 4 所示。

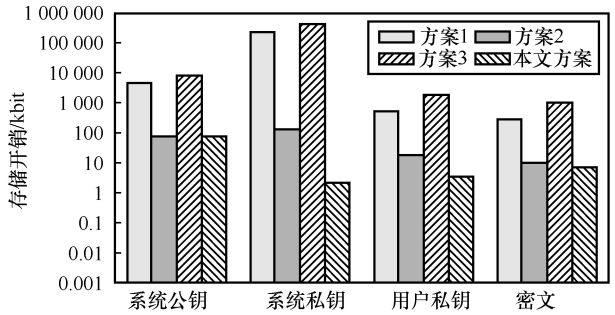


图 4　不同方案的存储开销

访问策略的不同决定了有效路径数量 V 的不同，模拟访问策略的布尔表达式为 $f(a,b,c,d)$，即只包含 4 正 4 负共 8 个属性，分析当访问策略类似于 $f(a,b,c,d)=a+b+c+d$ 时，有效路径数量有最大值 $V=24$；当访问策略类似于 $f(a,b,c,d)=abcd$ 时，有效路径数量有最小值 $V=1$。有效路径数量只与密文长度有关，在其他参数不变的情况下，不同有效路径数量下密文长度对比如图 5 所示。从图 5 中可以看出，当 $V=8$ 时，本文方案的密文长度与方案 2 相同，但即使有效路径取最大值时，密文长度与方案 2 仍处在同一量级，且远小于其他 2 个方案。

2) 计算开销

本节主要对算法在加解密及密钥追踪过程中涉及的计算开销进行分析。由于加法运算开销较小，本文主要考虑乘法及模运算，其中，mul 表示乘法运算，mod 表示模运算，计算开销如表 4 所示。本文方案加密过程中的计算量主要与有效路径的个数相关，与方案 2 的计算量处于同一水平，且远小于方案 1 和方案 3；而在解密计算过程中，本文方案乘法的运算次数远少于其他 3 个方案。需要注意的是，虽然本文方案计算开销较小，但在加解密过程需要运行与 OBDD 相关的 2 个算法，在一定程度上增加了额外的开销。

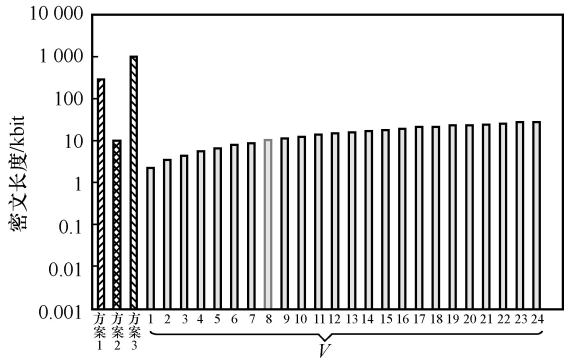


图 5　不同方案与本文方案不同有效路径数量下密文长度对比

表 4　　**计算开销**

方案	加密开销	解密开销
方案 1	$(m_1nA_c+m_1)$mul	$l(m_1+1)A_d$mul + mod
方案 2	$(3nA_c+2n)$mul	$(2nA_d+n)$mul + mod
方案 3	$(2m_2nA_c+n)$mul	$(2m_2+1)A_d$mul + mod
本文方案	$(4nV+n)$mul	$2n$mul + mod

不同方案的计算开销如图 6 所示。本文方案无论是加密还是解密操作，计算开销都远小于其他方案。解密操作与有效路径数量无关，不同有效路径数量下加密操作计算开销对比如图 7 所示。从图 7 可以看出，当 V 为 6 或 7 时，本文方案中加密操作的计算开销与方案 2 几乎相同，但即使 V 取最大值时，加密操作的计算开销与方案 2 仍处在同一量级，且远小于其他 2 个方案。

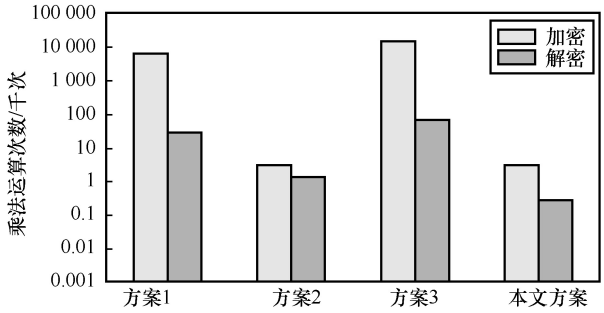


图 6　不同方案的计算开销

3) 通信开销

本节主要对方案的通信开销进行分析。整个通

信过程主要涉及用户密钥和密文的传输开销，由于方案 1 和方案 3 基于 LWE 问题进行构造，每次加密只有 1 bit，当加密相同明文数据时造成的开销较大，这里主要与方案 2 进行对比。

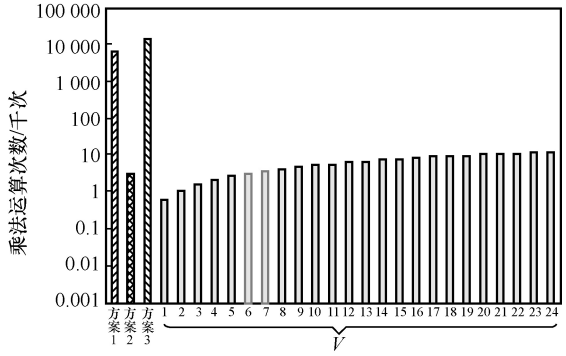


图 7　不同方案与本文方案不同有效路径数量下加密操作计算开销对比

用户密钥方面，本文方案的密钥尺寸不会随着属性数量的改变而改变，其他方案的密钥尺寸与属性数量成正比，当用户密钥中包含的属性数量较多时，本文方案的优势更加明显。当用户密钥中包含的属性数量变化时，密钥尺寸分析如图 8 所示。

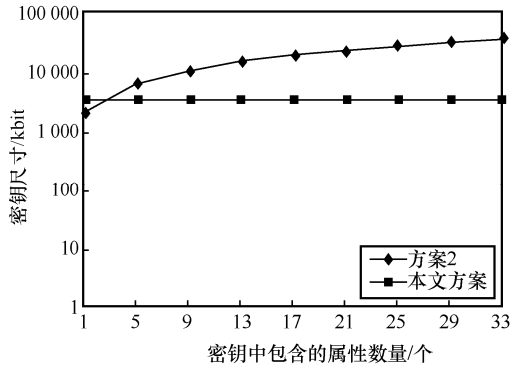


图 8　密钥尺寸分析

密文方面，由于本文方案使用 IPFS 存储原始加密数据，加密的明文只是存储地址和对称密钥，因此设置明文为 1 280 bit，当密文中的属性数量变化时，密文开销分析如图 9 所示。从图 9 可以看出，方案 2 的密文开销与属性数量成正比，本文方案的密文开销与属性数量没有直接关系，而与有效路径数量相关，即由具体的访问策略决定，将密文尺寸与属性数量的关系脱钩并不意味着一定有优势，也可能带来更大的开销，这并非 OBDD 访问结构的优点，只能作为一个特点。

通过 OBDD 访问结构的性质不难发现，当访问策略中“与”操作较多时，满足策略的路径数量较少，相应的开销就会减少。为了清晰展示这一关系，本文模拟有效路径数量为属性数量的随机倍数，可以发现对于有效路径数量较少的情况，密文开销远小于相同属性数量下方案 2 的开销，但同样由于访问策略的不同，也会存在开销远超过方案 2 的情况，但结合密钥和密文两部分来分析通信开销，本文方案存在一定的优势。

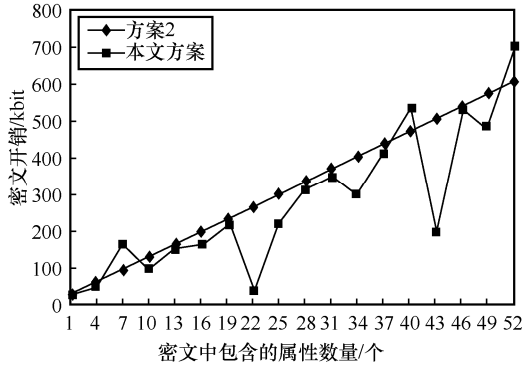


图 9　密文开销分析

4.3.3　实验分析

为了进一步分析方案的性能，本节进行了仿真实验。由于格上属性加密方案的相关仿真实验较少，难以与其他方案进行有效的对比分析，本文主要对算法的运行效率进行测试。实验环境为 AMD Ryzen 7-5800H 处理器 3.20 GHz，16.0 GB 内存，64 位 Windows11 操作系统。实验程序基于 C++语言编写，采用 Qt Creator 开发环境基于 NTL 库实现。

在本节实验中，设置参数 $q=8\,380\,417$，$p=3$，U 中包含 10 个属性，模拟设置数据拥有者的访问策略为

$$f\{a_1,a_2,a_3,a_4\}=(a_1\wedge a_2)\vee(a_3\wedge a_4)$$

数据用户的属性集为 $\{a_1,a_2\}$。实验测试了环多项式不同维度下各个算法的运行时间，为了确保实验结果的准确性，每种情况下分别进行 30 次的仿真模拟，再将得到的数据求均值，得到最终的结果，如图 10 所示。其中，密钥生成算法的运行时间是方案中 IKeyGen 和 AKeyGen 算法的运行时间之和，从实验数据整体分析，密钥生成、加密算法和解密算法消耗的时间相对较长，并且由于参数选择的随机性，这 3 个算法运行的最长时间和最短时间的跨度也较大，而初始化和追踪算法的运行时间相对较短，实验结果与算法的理论分析相符。

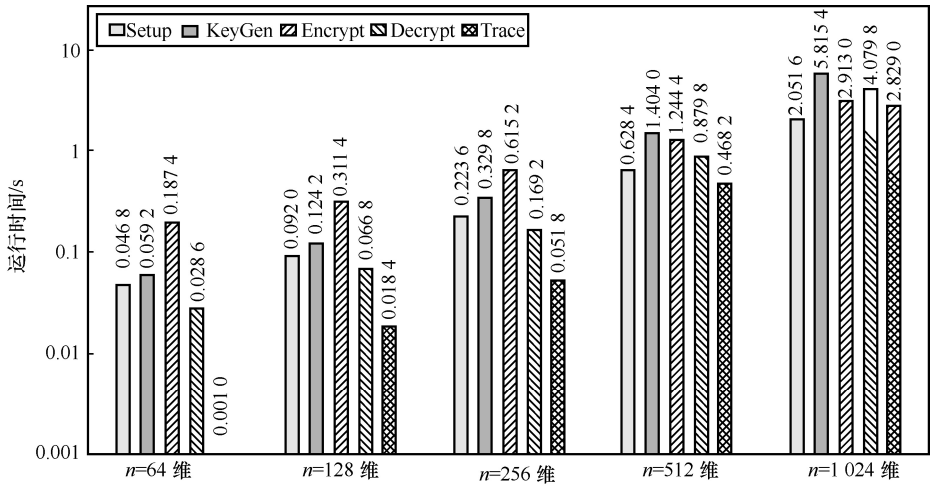


图 10 仿真实验结果

5 结束语

本文基于 OBDD 访问结构构造了一个格上的可抗密钥滥用的属性加密方案，除了可以追踪恶意用户的密钥外，还可以实现抗密钥委托的功能，同时由于 OBDD 访问结构的特点，不仅支持属性的与、或、门限操作，还能支持属性的正负值，而且在一定程度上降低了存储和计算开销。分析表明，本文方案在具有抗量子攻击的同时满足抗合谋攻击和选择策略及选择明文攻击下的不可区分性安全，与其他格基属性加密方案相比，在功能和性能上均有一定的优势，但是本文方案并没有考虑更细粒度的属性更新及撤销问题，这将是下一步研究的重点。

参考文献：

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

[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. New York: ACM Press, 2006: 89-98.

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

[4] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//Proceedings of International Workshop on Public Key Cryptography. Berlin: Springer, 2011: 53-70.

[5] IBRAIMI L, PETKOVIC M, NIKOVA S, et al. Mediated ciphertext-policy attribute-based encryption and its application[C]//Proceedings of International Workshop on Information Security Applications. Berlin: Springer, 2009: 309-323.

[6] LI L, GU T L, CHANG L, et al. A ciphertext-policy attribute-based encryption based on an ordered binary decision diagram[J]. IEEE Access, 2017, 5: 1137-1145.

[7] 孙京宇, 朱家玉, 田自强, 等. 基于椭圆曲线加密且支持撤销的属性基加密方案[J]. 计算机应用, 2022, 42(7): 2094-2103.
SUN J Y, ZHU J Y, TIAN Z Q, et al. Attribute based encryption scheme based on elliptic curve cryptography and supporting revocation[J]. Journal of Computer Applications, 2022, 42(7): 2094-2103.

[8] 汪倩倩, 欧毓毅. 可追踪且可撤销的基于 OBDD 访问结构的 CP-ABE 方案[J]. 计算机应用研究, 2021, 38(4): 1185-1189.
WANG Q Q, OU Y Y. Traceable and revocable CP-ABE scheme OBDD-based access structure[J]. Application Research of Computers, 2021, 38(4): 1185-1189.

[9] HINEK M J, JIANG S, SAFAVI-NAINI R, et al. Attribute based encryption with key cloning protection[R]. 2008.

[10] LI J, REN K, KIM K. A2BE: accountable attribute-based encryption for abuse free access control[R]. 2009.

[11] LIU Z, CAO Z F, WONG D S. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & communications Security. New York: ACM Press, 2013: 475-486.

[12] LIU Z, CAO Z F, WONG D S. Traceable CP-ABE: how to trace decryption devices found in the wild[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(1): 55-68.

[13] LIU Z, CAO Z F, WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 76-88.

[14] 赵志远, 朱智强, 王建华, 等. 云存储环境下无密钥托管可撤销属性基加密方案研究[J]. 电子与信息学报, 2018, 40(1): 1-10.
ZHAO Z Y, ZHU Z Q, WANG J H, et al. Revocable attribute-based encryption with escrow-free in cloud storage[J]. Journal of Electronics & Information Technology, 2018, 40(1): 1-10.

[15] 闫玺玺, 何旭, 刘涛, 等. 抗密钥委托滥用的可追踪属性基加密方

案[J]. 通信学报, 2020, 41(4): 150-161.
YAN X X, HE X, LIU T, et al. Traceable attribute-based encryption scheme with key-delegation abuse resistance[J]. Journal on Communications, 2020, 41(4): 150-161.

[16] AGRAWAL S, BOYEN X, VAIKUNTANATHAN V, et al. Functional encryption for threshold functions (or fuzzy IBE) from lattices[C]//Proceedings of International Workshop on Public Key Cryptography. Berlin: Springer, 2012: 280-297.

[17] BOYEN X. Attribute-based functional encryption on lattices[M]. Berlin: Springer, 2013.

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

[19] SOO F T, SAMSUDIN A. Lattice ciphertext-policy attribute-based encryption from ring-LWE[C]//Proceedings of International Symposium on Technology Management and Emerging Technologies (ISTMET). Piscataway: IEEE Press, 2015: 258-262.

[20] 于金霞, 杨超超, 杨丽伟, 等. 理想格上支持访问树的属性基加密方案[J]. 重庆邮电大学学报(自然科学版), 2019, 31(1): 113-119.
YU J X, YANG C C, YANG L W, et al. Attribute-based encryption scheme supporting tree access structure on ideal lattices[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2019, 31(1): 113-119.

[21] 于金霞, 杨超超, 张棋超, 等. 外包环境下格上可撤销的属性基加密方案[J]. 计算机科学与探索, 2020, 14(2): 244-251.
YU J X, YANG C C, ZHANG Q C, et al. Revocable ciphertext-policy attribute-based encryption in data outsourcing systems from lattices[J]. Journal of Frontiers of Computer Science and Technology, 2020, 14(2): 244-251.

[22] 闫玺玺, 刘媛, 李子臣, 等. 理想格上支持隐私保护的属性基加密方案[J]. 通信学报, 2018, 39(3): 128-135.
YAN X X, LIU Y, LI Z C, et al. Privacy-preserving attribute-based encryption scheme on ideal lattices[J]. Journal on Communications, 2018, 39(3): 128-135.

[23] 郭凯阳, 韩益亮, 吴日铭. 基于 RLWE 的可撤销分层属性加密方案[J]. 信息技术与网络安全, 2021, 40(8): 9-16.
GUO K Y, HAN Y L, WU R M. Revocable hierarchical attribute-based encryption scheme from RLWE[J]. Information Technology and Network Security, 2021, 40(8): 9-16.

[24] 王想, 陈燕俐. 基于以太坊的格上属性基可搜索加密方案[J]. 重庆邮电大学学报(自然科学版), 2021, 33(4): 675-682.
WANG X, CHEN Y L. Attribute-based searchable encryption scheme from lattices on Ethereum[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2021, 33(4): 675-682.

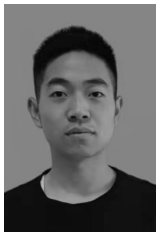
[25] 闫玺玺, 刘媛, 李子臣, 等. 利用 LWE 问题构造的多机构属性基加密方案[J]. 西安电子科技大学学报, 2018, 45(4): 129-136.
YAN X X, LIU Y, LI Z C, et al. Multi-authority attribute-based encryption scheme from LWE problem[J]. Journal of Xidian University, 2018, 45(4): 129-136.

[26] 唐慧, 汪学明. 基于格的多授权密文属性加密方案[J]. 计算机应用研究, 2022, 39(2): 563-566, 571.
TANG H, WANG X M. Multi-authority ciphertext-policy attributed-based encryption scheme from lattice[J]. Application Research of Computers, 2022, 39(2): 563-566, 571.

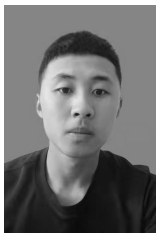
[作者简介]

韩益亮（1977– ），男，甘肃会宁人，博士，武警工程大学教授、博士生导师，主要研究方向为公钥密码学、网络安全等。

郭凯阳（1995– ），男，河北邯郸人，武警工程大学硕士生，主要研究方向为密码学。



吴日铭（1994– ），男，江西赣州人，武警工程大学硕士生，主要研究方向为信息安全。



刘凯（1997– ），男，河南南阳人，武警工程大学硕士生，主研究方向为信息安全。