可撤销和可追踪的密钥策略属性基加密方案

齐芳，李艳梅，汤哲
（中南大学信息科学与工程学院，湖南 长沙 410083）

摘 要：针对基于密钥策略属性基加密（KP-ABE, key-policy attribute-based encryption）方案不能兼顾属性撤销和用户身份追踪的问题，提出一种支持可撤销和可追踪的 KP-ABE 方案。首先，该方案能够在不更新系统公钥和用户私钥的情况下实现对用户属性的撤销，更新代价比较小，同时可以根据解密密钥追踪到用户身份，从而有效地防止匿名用户的密钥泄露问题。其次，该方案基于线性访问结构（LSSS, linear secret sharing scheme），与树形访问结构相比，执行效率更高。最后，该方案基于判定性 q-BDHE 假设，给出了在标准模式下的安全性证明。通过与已有的 KP-ABE 方案进行对比分析得出，该方案的公钥长度更短、加解密的计算开销更低，且在实现属性可撤销的基础上实现了用户身份的可追踪功能，具有较为明显的优势。

关键词：基于密钥策略属性基加密；可撤销；可追踪；线性访问结构
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2018231

Revocable and traceable key-policy attribute-based encryption scheme

QI Fang, LI Yanmei, TANG Zhe
School of Information Science and Engineering, Central South University, Changsha 410083, China

Abstract: The existing key-policy attribute-based encryption (KP-ABE) scheme can not balance the problem of attribute revocation and user identity tracking. Hence, a KP-ABE scheme which supported revocable and traceable was proposed. The scheme could revoke the user attributes without updating the system public key and user private key with a less update cost. Meanwhile, it could trace the user identity based on decryption key which could effectively prevent anonymous user key leakage problem. The proposed scheme was based on linear secret sharing scheme (LSSS), which was more efficient than tree-based access structure. Based on the deterministic q-BDHE hypothesis, the proposed scheme gave security proof until standard mode. Finally, compared with the existing KP-ABE scheme, the scheme has a shorter public key length, lower computational overhead and realizes the traceability function of user identity based on the revocable attribute, which has obvious advantages.

Key words: KP-ABE, revocable, traceable, linear secret sharing scheme

1 引言

2007 年，Bethencourt 等[1]第一次提出了属性基加密（ABE, attribute-based encryption）机制的概念，该机制将用户私钥、密文分别和一组属性相关联，用户私钥只有满足密文访问策略时才可对密文进行解密，因此，可以实现细粒度的访问控制。现有的 ABE 机制根据解密策略的关联方式可以大致分

收稿日期：2018–01–11；**修回日期**：2018–05–19
通信作者：李艳梅，liyanmei_@csu.edu.cn
基金项目：国家自然科学基金重点项目（No.61632009）；长沙市科技计划基金资助项目（No.kq1701089）；国家重点研发计划基金资助项目（No.2018YFD0700500）
Foundation Items: The National Natural Science Foundation of China (No.61632009), The Science and Technology Project of Changsha (No.kq1701089), The National Key Research and Development Program of China (No.2018YFD0700500)

为两种，一种是基于密钥的属性基加密机制[2-4]（KP-ABE, key-policy attribute-based encryption），该机制中用户私钥与访问策略相关；另一种是基于密文的属性基加密机制[5-6]（CP-ABE, ciphertext- policy attribute-based encryption），该机制将密文与访问策略绑定。上述两种方案都实现了基于属性的细粒度访问策略。Waters 等[7]和 Goyal 等[8]的属性加密方案都是基于树形访问结构的，由文献[8]可知，树形访问结构下的密文长度会随访问树节点的增加呈指数级增长，执行效率比较低。而线性访问结构中密文和加密时间的长度是随着访问结构的增大呈线性增长的，且文献[9]中证明树型访问结构与线性访问结构是可以相互转换的，因此，本文的访问结构是基于 LSSS 的。

目前，针对各种形式的 ABE 方案关于属性撤销方面的研究比较少，已有的撤销方案根据撤销执行方，可以分为直接撤销和间接撤销两类，Imai 等[10]指出间接撤销是指只有未被撤销的用户，即非撤销用户才可以对密钥进行更新。Pirretti 等[11]提出将有效期与一个属性相关联的撤销方案，但该方案存在诸多问题，如密钥存储和更新的工作量较大、授权中心可扩展性较差及无法实现属性到期前的撤销。Bethencourt 等[12]提出的方案是在用户属性和密文中都添加时间信息，但是授权中心的工作量会随着用户数量的增多急剧增大，且不能实现用户属性的动态及时撤销。Boldyreva 等[13]提出了利用二叉树进行撤销的方案，但该方案仍不支持及时撤销。直接撤销是信息发送方将用户的属性撤销列表直接嵌入密文中，从而完成属性密钥的撤销，该思路是由 OSW07[13]首次提出的，被撤销的用户失去了所有的解密属性，但在该方案中仅支持用户身份的撤销，无法实现用户部分属性撤销的问题。文献[10]中定义了两种撤销模型：一种是间接撤销模型，在这种模型下，用户的属性或身份，通过更新用户私钥来实现撤销，加密消息时，发送者不关心撤销列表；另一种是直接撤销模型，该模型中，用户的属性或者身份在撤销的时候会加入撤销列表中，将撤销列表加入密文中，而不影响用户私钥的生成。文献[14]提出了一个支持身份吊销的 KP-ABE 方案，但是该方案要求用户加密的属性集的大小必须是属性集大小的一半。文献[15]提出了一种直接撤销模式下具有细粒度属性撤销机制的加密方案，该方案中撤销的是单个属性下的某些用户，而不影响该用户下的其他属性，用户的部分属性被撤销后如果余下的属性集仍可以满足访问结构，则该用户还可以解密信息。文献[16]在现有的研究基础上，指出在不影响其他用户私钥的前提下，实现用户属性撤销是未来的研究方向。目前，基于直接撤销模式下的属性基加密机制因其撤销代价较小等优势，成为属性基加密机制的研究热点[17-19]，文献[17]提出一种可直接撤销的 CP-ABE 方案，针对 KP-ABE,文献[20]提出一种支持用户撤销的 KP-ABE 方案，但是该方案中仅支持用户撤销，还不能实现细粒度的撤销模式，因而 Wang 等[21]提出支持细粒度撤销机制的 KP-ABE 方案。文献[22]提出一种基于代理的 KP-ABE 撤销方案，该方案不需要更新用户密钥和已经加密的旧密文，但是需要第三方代理机构随时在线且完全可信。

密钥滥用问题一直是属性基加密机制的研究热点，因为用户是通过属性集来进行身份标识，所以可能会使不同用户有相同的属性集，无法唯一确定用户身份，因此，如果合法用户将自己的私钥给其他恶意用户分发出去，就会打乱事先定义的访问策略，而且还不能对该用户追责，因而引发密钥滥用的问题。文献[23-24]中引入了用户身份信息，可以实现对恶意用户身份追踪，但文献[23]中的撤销机制仅针对恶意用户。

上述研究内容均不能同时有效解决用户属性细粒度撤销和追踪用户身份的问题，因此，本文在现有的研究基础上，通过在密文中嵌入用户属性撤销列表，同时将用户身份标识和密钥相结合，从而可以实现用户部分属性撤销的细粒度访问控制，而且可以通过密钥追踪到用户身份，有效地防止了用户密钥泄露的问题，具有一定的实际应用价值。

2 基础知识

2.1 合数阶群上的双线性映射

定义 1 双线性映射。令 G,G_N 是 P 阶循环群，其中 P 为素数。令 g 为 G 群的生成元，定义映射 $e:G\times G=G_N$，若 e 满足如下 3 个性质，则称 e 为从 G 到 G_N 的双线性映射。

1) 双向性：$\forall a,b\in Z_p^*$，满足 $e(g^a,g^b)=e(g,g)^{ab}$。

2) 非退化性：$\exists g\in G$，使 $e(g,g)\neq 1$。

3) 可计算性：$\forall P,Q\in G,e(P,Q)$是可计算的。

2.2 访问结构

定义 2 访问结构。设$P=\{P_1,P_2,\cdots,P_n\}$是n个参与者的集合，集族$T\in 2^P\setminus\{\varnothing\}$，若访问结构$T$是单调的，则有$\forall B,C$，若$B\in T$且$B\in C$，则有$C\in T$，则称$T$中的集合为授权集，而不在$T$中的集合为非授权基集。

2.3 线性秘密共享方案

定义 3 LSSS。访问结构$T=(\boldsymbol{A},\rho)$，其中，$\boldsymbol{A}$是$d\times l$的矩阵，ρ是矩阵$\boldsymbol{A}$中的每一行A_x到参与方$\rho(x)$的映射，LSSS 的实现过程：随机选取向量$\vec{\boldsymbol{v}}=(s,v_2,v_3,\cdots,v_n)$，其中，$s$为要分享的秘密值，令$\overrightarrow{\boldsymbol{A}_i}$为矩阵$\boldsymbol{A}$的第$i$行代表的向量，计算$\sigma_i=\overrightarrow{\boldsymbol{A}_i}\times\vec{\boldsymbol{v}}$作为参与方$\rho(x)$的秘密分享值。若$\{\omega_x\}_{x\in A}$为一组恢复系数，则有$\sum_{\rho(x)\in A}\omega_x A_x=(1,0,\cdots,0)$，从而可以恢复秘密分享值。

2.4 判定性 *q*-BDHE 假设

定义 4 判定性 q-BDHE 假设。令G,G_{N}是阶为p的循环群（p为素数），g为G的一个生成元，e为双线性映射$e:G\times G=G_{\mathrm{N}}$，随机选取$\alpha,s\in Z_p$，计算

$$Q=\left(g,g^s,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},g^{\alpha^{q+2}},\cdots,g^{\alpha^{2q}}\right)$$

若不存在一个算法可以在多项式时间内以不可忽略的优势区分$e(g,g)^{\alpha^{q+1}s}$与G_{N}中的随机元素，则称 q-BDHE 假设成立。

3 模型定义

3.1 系统结构

支持可撤销和可追踪的 KP-ABE 方案由以下 5 个多项式时间算法组成。

setup $(\alpha,\beta,y,H(x),ID)\rightarrow(PK,MK)$ 初始化算法：输入随机数$\alpha,\beta,y\in Z_p$，用户身份标识ID，散列函数为$H(x)$，$H(x)$可以将任意长比特串映射为Z_p上的元素。输出系统公钥PK和主密钥MK，其中，PK隐含了系统属性集合$U=\{1,2,\cdots,n\}$和用户身份标识集合$D=\{1,2,\cdots,m\}$。

encrypt $(M,\lambda,s,PK,R)\rightarrow C$ 加密算法：输入明文M，λ为加密时的属性集合，随机值$s\in Z_p$，系统公钥PK以及属性撤销列表$R\in U$，输出密文C，密文中包含了属性撤销列表和加密属性集。

key generation $(MK,PK,\boldsymbol{A},\rho,ID)\rightarrow SK$ 密钥生成算法：输入系统密钥和公钥，$\boldsymbol{A}$为$d\times l$阶矩阵，$\rho(i)$表示矩阵第i行对应的属性以及用户身份标识ID，输出用户私钥SK。

decryption $(C,SK,PK,S)\rightarrow M$ 解密算法：输入密文C、用户私钥SK以及系统公钥PK，$S=U-R$为属性集合。输出明文M。

trace 追踪算法：如果非法用户拥有有效的解密密钥，则可以通过本算法验证密钥泄露者的身份，从而追踪到用户身份。

3.2 安全模型

定义一个公钥加密方案以达到选择明文攻击下的不可区分性，即（IND-CPA, indistinguishability under chose-plaintext attack）攻击类型。通过挑战者 Λ 和敌手 Γ 间的交互性游戏来定义上述攻击。

初始化阶段：敌手 Γ 选择一个要挑战的访问结构λ^*，对于其中的属性i，指定该属性的用户撤销列表R^*。

建立阶段：挑战者 Λ 运行系统初始化算法和密钥生成算法，输入挑战者 Λ 选择的随机数、散列函数和身份标识，输出系统公钥PK和主密钥MK，将公钥发送给敌手 Γ，自己保留主密钥。

挑战阶段：敌手 Γ 选取两条等长消息M_0和M_1，挑战者 Λ 随机选择b，即b取随机值 0 或 1，加密消息M_b，生成密文C^*并返回给敌手 Γ。

猜测阶段：敌手 Γ 返回对密文C^*的猜测值b'，如果$b'=b$，则敌手 Γ 获胜。

定义敌手 Γ 的攻击优势为$Pr[b'=b]-\frac{1}{2}$。

定义 4 如果任意多项式时间内敌手 Γ 赢得游戏的优势是可以忽略的，则称方案是 IND-CPA 安全的。

4 具体方案

对于 LSSS 访问结构$T=(\boldsymbol{A},\rho)$，其中，$\boldsymbol{A}$为$d\times l$阶的矩阵，$\rho(i)$为矩阵中第i行对应的属性。消息在属性集λ下进行加密后，想要解密该密文，则需要属性集λ满足访问结构$T=(\boldsymbol{A},\rho)$，即访问结构中存在系数$a_i\in Z_p$满足$\sum_{\rho(i)\in\lambda}a_i\overrightarrow{\boldsymbol{A}_i}=\vec{\boldsymbol{1}}$。令$G_1,G_2$是阶为$p$的双线性群，其中，$p$为素数，$g$为生成元，

e 为 $G_1 \times G_1 \to G_2$ 的双线性映射。

$\text{setup}(\alpha,\beta,y,H(x),ID) \to (PK,MK)$：定义属性集合 $U=\{1,2,\cdots,n\}$，每个属性 $t \in U$。用户身份集合 $D=\{1,2,\cdots,m\}$，其中，用户的身份标识 $ID \in D$。随机选取 $\alpha,\beta,y \in Z_p$。选择散列函数 $H(x)$，该函数可以将任意长度的字符串映射为 Z_p 上的元素，生成系统公钥为

$$PK=\begin{cases} Y=e(g,g)^y \\ g_{ID}=g^{\beta H(ID)} \\ h=g^{\alpha}, g_t=g^{\alpha_t}, t \in U \end{cases} \tag{1}$$

生成系统主密钥为

$$MK=\{t,\alpha,\beta,y\}_{t \in U} \tag{2}$$

$\text{encrypt}(M,\lambda,s,PK,R) \to C$ 加密算法：输入明文 M、随机数 $s \in Z_p$、系统公钥 PK 以及属性撤销列表 R，且明文的加密是在属性集 λ 下进行的，然后输出密文为

$$C=\begin{cases} \lambda, c_0=g^s, c_0'=g^{\alpha s}, c_i=g^{t_i}, i \in \lambda \\ c'=MY^s, c''=e\left(g,\mathrm{g}_{n+1}\right)^s, R \end{cases} \tag{3}$$

$\text{key generation}(MK,PK,\boldsymbol{A},\rho,ID) \to SK$：密钥生成算法，将访问结构 T、系统公钥 PK、系统主密钥 MK 以及用户身份标识 ID 作为输入。访问结构 $T=(\boldsymbol{A},\rho)$，其中，$\boldsymbol{A}$ 为 $d \times l$ 阶的矩阵，$\rho(i)$ 为矩阵中第 i 行对应的属性。随机选取向量 $\vec{\boldsymbol{v}}=(s,v_2,v_3,\cdots,v_n)$ 满足 $\vec{\mathbf{1}} \times \vec{\boldsymbol{v}}=s$，即满足 $\sum_{i=1}^{l} v_i=y$，且将用户身份标识 ID 嵌入用户密钥中，得到解密密钥为

$$SK=\begin{cases} D=g^{\frac{y}{\alpha+\beta H(ID)}} \\ D_i=g^{\frac{\overrightarrow{\boldsymbol{A}_i} \times \vec{\boldsymbol{v}} \alpha \beta H(ID)}{t_{\rho(i)}}} \\ I_0=g^{y+\beta H(ID)} \\ I_1=g^{\beta H(ID)}, I_2=ID \end{cases} \tag{4}$$

$\text{decryption}(C,SK,PK,S) \to M$ 解密算法：输入密文 C、用户私钥 SK 以及系统公钥 PK，其中，$S=U-R$ 为用户未被撤销的属性集。解密计算过程如下。

$$\begin{aligned} F &= \left(\prod_{\rho(i) \in \lambda} e\left(D_i, C_0, C_{\rho(i)}\right)^{a_i}\right) c'' \\ &= \left(\prod_{\rho(i) \in \lambda} e\left(g^{\frac{\overrightarrow{\boldsymbol{A}_i} \times \vec{\boldsymbol{v}} \cdot \alpha \cdot \beta H(ID)}{t_{\rho(i)}}}, g^s g^{t_{\rho(i)}}\right)^{a_i}\right) e\left(g, g_{n+1}\right)^s \\ &= e(g,g)^{\sum_{\rho(i) \in \lambda} \overrightarrow{\boldsymbol{A}_i} \times \vec{\boldsymbol{v}} \alpha \beta H(ID) a_i s} e(g,g)^{\alpha s(n+1)} \\ &= e(g,g)^{y \alpha s \beta H(ID)} e(g,g)^{\alpha s(n+1)} \end{aligned} \tag{5}$$

再计算

$$\begin{aligned} F' &= e\left(D, hI_1\right) e\left(\frac{I_0}{I_1}, c_0\right) \\ &= e\left(g^{\frac{y}{\alpha+\beta H(ID)}}, g^{\alpha} g^{\beta H(ID)}\right) e\left(g^y, g^s\right) \\ &= e(g,g)^y e(g,g)^{ys} \end{aligned} \tag{6}$$

最终计算得到

$$\begin{aligned} & c' \frac{F}{F'} \frac{e\left(\prod_{i \in S, i \neq ID} g_{n+1-i+ID}, c_0\right)}{e\left(g_{ID}, \left(h \prod_{i \in S} g_{n+1-i}\right)^s\right)} \\ &= Me(g,g)^{ys} e(g,g)^{\alpha s \beta H(ID)} \cdot \\ & e(g,g)^{\alpha s(n+1)} \frac{e(g,g_{n+1})^{-s}}{e\left(g_{ID}, h\right)^s} \\ &= M \end{aligned} \tag{7}$$

trace 追踪算法：因为密钥中嵌入了用户的身份标识，每个用户都满足

$$e\left(I_0, g\right) = e\left(I_1, g\right) e\left(g^y, g\right) \tag{8}$$

所以如果当非法用户拥有有效的密钥时，就可以根据 I_2 得到密钥泄露方的用户 ID。

5 安全性证明

定理 1 基于上述 3.2 节所定义的安全模型下，若 q-BDHE 假设成立，则第 4 节给出的方案是 IND-CPA 安全的。

证明 采用反证法，若存在一个概率多项式时间算法的敌手 Γ 能以 ε 的优势赢得安全性游戏，则可以构造一个概率多项式时间算法 B 能以不可忽略优势 $\frac{\varepsilon}{2}$ 解决判定性 q-BDHE 问题。

挑战者 Λ 首先选取两个阶为 p 的循环群 G_1 和

G_2，其中，p 为素数，令 $n=p$。并定义 e 为 G_1 到 G_2 的双线性映射，令 g 为 G_1 的生成元。从 Z_p 中随机选取 a,b,c,z，挑战者通过抛掷硬币的游戏随机选取 b，b 的取值为 0 或 1。当 $b=0$ 时，挑战者计算 $Z=e(g,g)^{abc}$；当 $b=1$ 时，$Z=e(g,g)^{z}$。

init：模拟算法运行敌手 Γ，敌手 Γ 的身份标识为 ID，同时敌手 Γ 给出一个挑战属性集合 λ 和属性撤销列表 R，集合中的属性 i 都属于 U。

setup：首先设置 $Y=e(g,g)^{ab}$，对于每个属性 i，若 $i\in\lambda$，则 $g_i=g^{r_i}$，其中，$r_i=\alpha_i$ 且 r_i 为随机值。若 $i\notin\lambda$，则 $g_i=g^{bt_i}$，其中，$bt_i=\alpha_i$ 且 t_i 为随机值。令 $S=U-R$，模拟算法 B 随机选取一个 b 值，计算 $h=g^b\left(\prod_{j\in S}g_{n+1-j}\right)^{-1}$，其中，$\forall j\in S$，$\lambda=b-\sum_{\forall j\in S}\alpha^{n+1-j}$。最后将公钥发送给敌手。

第一阶段：敌手 Γ 提交自己的身份标识，询问访问结构所对应的私钥，私钥的询问分两种情况，即 λ 满足访问结构，或 λ 不满足访问结构。若该询问不满足访问结构 $T=(\boldsymbol{A},\rho)$，其中，$\boldsymbol{A}$ 为 $d\times l$ 阶的矩阵，$\rho(i)$ 为矩阵中第 i 行对应的属性，则该访问结构中 $f_M(\lambda)=0$。模拟算法 B 在生成私钥时需要随机生成一个向量 $\vec{\boldsymbol{u}}=(u_1,u_2,\cdots,u_l)$，并满足 $\vec{\mathbf{1}}\times\vec{\boldsymbol{u}}=ab$。令矩阵 $\boldsymbol{A}^*$ 为 $\boldsymbol{A}$ 的子矩阵，因为 $\vec{\mathbf{1}}$ 对于 $\boldsymbol{A}^*$ 是独立的，所以存在一个向量 $\vec{\boldsymbol{w}}=(w_1,w_2,\cdots,w_l)$ 满足 $\boldsymbol{A}_\lambda\vec{\boldsymbol{w}}=\vec{\mathbf{0}}$，而 $\vec{\mathbf{1}}\vec{\boldsymbol{w}}=h$，令 $A_j=(m_{j1},m_{j2},\cdots,m_{jl})$，则可得到对应的私钥如下。

当询问满足访问结构时

$$D_j=g^{b(\alpha\beta H(ID))\frac{\sum_{k=1}^{l}m_{ji}\lambda_j}{\lambda_{\rho(j)}}} \tag{9}$$

当询问不满足访问结构时

$$\begin{aligned}D_j&=g^{\alpha\beta H(ID)\frac{\sum_{x=1}^{l}m_{ji}}{h\beta_{\rho(j)}}}g^{\alpha\beta H(ID)\frac{\sum_{x=1}^{l}x_{ji}\left(h\lambda_j-\sum_{x=1}^{l}\lambda_x\right)}{h\beta_{\rho(j)}}}\\&=g^{(\alpha\beta H(ID))\left(\frac{\sum_{x=1}^{l}m_{ji}}{h\beta_{\rho(j)}}+\frac{\sum_{x=1}^{l}x_{ji}\left(h\lambda_j-\sum_{x=1}^{l}\lambda_x\right)}{h\beta_{\rho(j)}}\right)}\end{aligned} \tag{10}$$

Challenge：敌手 Γ 向模拟算法提交两条长度不可区分的消息 M_1 和 M_2，模拟器通过投掷硬币游戏随机选择 $b\notin\{0,1\}$，然后对消息 M_b 进行加密，计算密文为

$$C=\left(\lambda,c'=M_bZ,\left\{c_i=g^{ri}\right\}_{i\in\lambda}\right) \tag{11}$$

并将密文返回给敌手 Γ。

第二阶段：重复第一阶段的操作。

Guess：本阶段敌手输出对 τ 的猜测 τ'。

若 $\tau'=\tau$，模拟算法输出对 b 的猜测 $b'=0$。

若 $\tau'\neq\tau$，模拟算法输出对 b 的猜测 $b'=1$。

分析：当 $b=0$ 时，$Z=e(g,g)^{abc}$，可得属性集 λ 下的有效密文为

$$C=\left(\lambda,c'=M_bg^{abc},\left\{c_i=g^{r_i}\right\}_{i\in\lambda}\right) \tag{12}$$

这种情况下，敌手 Γ 挑战成功，可以得到对消息的加密结果。假设敌手的攻击优势为 $\varepsilon=Pr[\tau=\tau']-\frac{1}{2}$，此时模拟算法在游戏中的优势为

$$Pr[b=b'|b=0]=Pr[\tau'=\tau]=\varepsilon+\frac{1}{2} \tag{13}$$

当 $b=1$ 时，$Z=e(g,g)^{z}$，则可以得到

$$C'=\left(\lambda,c'=M_bg^{z},\left\{c_i=g^{br_i}\right\}_{i\in\lambda}\right) \tag{14}$$

对于敌手，变量 z 是未知的，因此，C' 对于敌手也是未知的，这种情况下模拟算法就失去了攻击优势。易见，此时模拟算法攻击成功的概率为

$$Pr[b=b'|b=1]=Pr[\tau'\neq\tau]=\frac{1}{2} \tag{15}$$

综上，模拟算法在 q-BDHE 游戏中获胜的概率为

$$\begin{aligned}&Pr[b=b']-\frac{1}{2}=Pr[b=b'|b=0]Pr[b=0]+\\&Pr[b=b'|b=1]Pr[b=1]-\frac{1}{2}\\&=\left(\varepsilon+\frac{1}{2}\right)\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}-\frac{1}{2}\\&=\frac{\varepsilon}{2}\end{aligned} \tag{16}$$

证明模拟算法 B 能以不可忽略的优势 $\frac{\varepsilon}{2}$ 解决判定性 q-BDHE 游戏。易见，这是不可能的，所以该假设不成立，从而证明本文所提方案是 IND-CPA 安全的。证毕。

6　性能分析

本节将对本文所提方案进行性能分析，内容包括公钥 PK、系统主密钥 MK、密文 C、用户密钥 SK、属性是否可撤销和用户是否可追踪以及对相关文献进行计算开销等方面进行对比。其中，

m 表示的是系统用户数量，n 表示用户用以进行加密的属性集，G_1,G_2 是阶为 p 的双线性群。其中，p 为素数，G_e 为 $G_1\times G_1=G_2$ 的双线性映射操作，L 为 LSSS 访问结构矩阵中的行或访问树的叶子节点，λ 为用户进行解密的属性集，R 为属性撤销列表。

表 1 通过对如上几种方案从公钥长度、系统主密钥长度、密文长度以及用户解密密钥长度以及方案是否具有可撤销性和可追踪性等方面进行比较，得出本文所提方案中的公钥长度与用户密钥是最短的，文献[24]的系统主密钥最短，密文中加入了撤销列表，因此，实现了属性的可撤销，用户解密密钥中嵌入用户的身份信息，因此，实现了用户身份的精准追踪。表 2 是对相关文献在计算开销方面的对比，由表 2 可知，文献[20]的加解密开销比文献[22]低，文献[23]中由于涉及两个循环群的运算，所以加解密开销文献[22]要高，本文所提方案的加解密开销低于文献[24]，同时加密开销为所有方案最低，解密开销仅略高于文献[20]。

综上表述，本文所提方案的公钥和用户密钥长度最短，且加密开销最低，同时可以实现细粒度的属性撤销和用户追踪。从密钥长度计算开销以及实现功能方面来看，都有较明显的优势。

7 结束语

本文提出了一种基于 LSSS 访问策略的可撤销、可追踪的 KP-ABE 加密方案，可以实现用户部分属性撤销而不影响其他用户的解密密钥，同时可以通过用户密钥追踪到用户身份，可以有效解决用户密钥泄露的问题，且在标准模型下证明本文所提方案可以解决 q-BDHE 假设，从而证明本文所提方案是 IND-CPA 安全的。未来相关的研究方案有：在现有的研究基础上实现用户身份的撤销；针对单授权中心安全性隐患和性能瓶颈的问题，实现多授权中心的 KP-ABE 加密方案。

参考文献：

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

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

[3] ATTRAPADUNG N, LIBERT B, PANAFIEU E. Expressive key-policy attribute-based encryption with constant-size cipher-texts[C]//International Conference on Practice and Theory in Public Key Cryptography. 2011:90-108.

[4] ATTRAPADUNG N, IMAI H. Conjunctive broadcast and attribute-based encryp-tion[C]//Pairing-Based Cryptography-Pairing 2009. 2009: 248-265.

表 1 密文与密钥长度及功能性对比

方案	公钥长度	系统主密钥	密文长度	用户私钥长度	可撤销	可追踪
文献[12]	$m+n+4$	$3n+2m+2$	$n+\|R\|+2$	$2\|L\|$	×	×
文献[13]1th	$2(m+n+1)$	$2n+3$	$2\|\lambda\|+3$	$2\|L\|$	√	×
文献[13]2th	$2(m+n+1)$	3	$2\|\lambda\|+3$	$4\|L\|$	√	×
文献[22]	$m+n+3$	$n+7$	$\|\lambda\|+4$	$3\|L\|$	×	√
文献[24]	$4m+n=1$	2	$\|\lambda\|+5$	$3\|L\|+m+2$	√	×
本文	$m+n+1$	$n+3$	$\|\lambda\|+\|R\|+3$	$\|L\|+3m$	√	√

表 2 计算开销比较

方案	加密	解密
文献[20]	$(2n+1)G_1+G_e$	$(n+3)G_e$
文献[22]	$2G_1+(n+1)G_e+G_2$	$(4n+3)G_e+G_2$
文献[23]	$nG_1+(n+1)G_2+G_e$	$(n+1)G_e+nG_1+(n+1)G_2$
文献[24]	$(n^2+1)G_e+G_1$	$2(n+1)G_e+(2n+3)G_1$
本文	$2G_e+3G_1$	$(n+5)G_e+G_1$

[5] ROY S, CHUAH M. Secure data retrieval based on ciphertext policy attribute-based encryption CP-ABE system for the DTNs[R]. Lehigh CSETech. 2009.

[6] ATTRAPADUNG N, HERRANZ J, LIBERT B, et al. Attribute-based encryption schemes with constant size ciphertexts[J]. Theoretical Computer Science, 2012, 422(3): 15-38.

[7] SAHAI A, WATERS B. Fuzzy identity-based encryption[M]. Advances in Cryptology EURO-CRYPT. 2005: 457-473.

[8] GOYAL V, JAIN A, PANDEY O, et al. Bounded ciphertext policy attribute based encryption[M]. Automata, Languages and Programming. 2008: 579-591.

[9] BEIMEL A. Secure schemes for secret sharing and key distribution[J]. International Journal of Pure & Applied Mathematics, 1996.

[10] ATTRAPADUNG N, IMAI H. Attribute-based encryption supporting direct/indirect revoca-tion modes[C]//Ima International Conference on Cryptography and Coding. 2009: 278-300.

[11] PIRRETTI M, TRAYNOR P, MCDANIEL P, et al. Secure attribute-based systems[C]//ACM Conference on Computer and Communications Security. 2006: 799-837.

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

[13] BOLDYREVA A, GOYAL V, KUNMAR V. Identity-based encryption with efficient re-vocation modes[C]//The ACM Conference on Computer and Communications Security. 2008: 417-426.

[14] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[C]//CCS 07 ACM Conference on Computer & Commu-nications Security. 2007: 195-203.

[15] STADDON J, GOLLE P, RASMUSSEN P. A content-driven access control sys-tem[C]//Symposium on Identity and Trust on the Internet. 2008: 26-35.

[16] WANG P, FENG D, ZHANG L. Towards attribute revocation in key-policy attribute based encryption[C]//International Conference on Cryptology and Network Security. 2011: 272-291.

[17] 苏金树, 曹丹, 王小峰, 等. 属性基加密机制[J]. 软件学报, 2011, 22(6): 1299-1315.
SU J S, CAO D, WANG X F, et al. Attribute-based encryption schemes[J]. Journal of Software, 2011,22(6): 1299-1315

[18] 闫玺玺, 孟慧. 支持直接撤销的密文策略属性基加密方案[J]. 通信学报, 2016, 37(5): 44-50.
YAN X X, MENG H. Ciphertext policy attribute-based encryption scheme supporting direct revocation[J]. Journal on Communications, 2016, 37(5): 44-50.

[19] 胡海英, 商威. 一种可撤销的 KP-ABE 方案[J]. 计算机系统应用, 2013, 22(9): 123-128.
HU H Y, SHANG W. A revocable KP-ABE scheme[J]. Computer Systems and Application, 2013, 22(9): 123-128.

[20] SHI Y, ZHENG Q, LIU J, et al. Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation[J]. Information Sciences, 2015, 295: 221-231.

[21] 王鹏翩, 冯登国, 张立武. 一个基于访问树的支持用户撤销的 KP-ABE 方案[C]//中国计算机网络与信息安全学术会议. 2011.
WANG P P, FENG D G, ZHANG L W. A KP-ABE scheme supporting user revocation based on access tree[C]//China Computer Networks and Information Security Conference. 2011.

[22] 林娟, 薛庆水, 曹珍富. 基于代理的即时属性撤销 KP-ABE 方案[J]. 计算机工程, 2014, 40(10): 20-24.
LING J, XUE Q X, CAO Z F. Proxy-based immediate attribute revocation KP-ABE Scheme[J]. Computer Engineering, 2014, 40(10): 20-24.

[23] 马海英, 曾国荪. 可追踪并撤销叛徒的属性基加密方案[J]. 计算机学报, 2012, 35(9): 1845-1855.
MA H Y, ZENG G S. An attribute-based en-cryption scheme for traitor tracing and revo-cation together[J].Chinese Journal of Computers, 2012, 35(9): 1845-1855.

[24] 马海英, 曾国荪, 陈建平, 等. 适应性安全的可追踪叛徒的基于属性加密方案[J]. 通信学报, 2016, 37(1): 76-87.
MA H Y, ZENG G S, CHEN J P, et al. Adaptively secure attribute-based encryption for traitor tracing[J]. Journal on Communications, 2016, 37(1): 76-87.

[作者简介]

齐芳（1978–），女，湖南长沙人，博士，中南大学副教授、博士生导师，主要研究方向为网络信息安全、通信协议。

李艳梅（1990–），女，山西吕梁人，中南大学硕士生，主要研究方向为信息安全、现代密码学。

汤哲（1977–），男，湖南长沙人，博士，中南大学副教授、硕士生导师，主要研究方向为智能技术、机器人、工业控制、电池管理与应用。