doi:10.11959/j.issn.1000-436x.2016091

支持直接撤销的密文策略属性基加密方案

闫玺玺，孟慧
（河南理工大学计算机科学与技术学院，河南 焦作 454003）

摘 要：提出一种支持直接撤销的属性基加密方案，首先给出支持直接撤销的属性基加密定义和安全模型，其次给出具体的支持撤销的密文策略——属性基加密方案并对安全性进行证明，最后，与其他方案对比显示，该方案在密文和密钥长度方面都有所减少。该方案可以实现对用户进行即时撤销，当且仅当用户所拥有的属性满足密文的访问结构且不在用户撤销列表内时，才能使用自己的私钥解密出明文。
关键词：属性基加密；属性撤销；直接撤销；访问控制
中图分类号：TP309 **文献标识码：**A

Ciphertext policy attribute-based encryption scheme supporting direct revocation

YAN Xi-xi, MENG Hui
(School of Computer Science and Technology, Henan Poly nic University, Jiaozuo 454003, China)

Abstract: In order to support fine-grained attribute revocation in direct revocation mode an attribute-based encryption scheme with efficient revocation was proposed. The model of ABE supporting attribute revocation was given, and a concrete scheme was constructed which was proven its security under the standard model. Compared to the existing related schemes, the size of ciphertext and private/secret key was reduced. In additional, the new scheme achieved fine-grained and immediate attribute revocation which is more suitable for the practical applications.
Key words: attribute-based encryption, attribute revocation, direct revocation, access control

1 引言

属性基加密（ABE, attribute based encryption）[1]最早由 Sahai 等于 2005 年提出，它的出现解决了传统公钥密码体制的缺陷，一方面，数据拥有者仅需根据属性加密消息，只有符合密文属性要求的用户才能解密消息，降低了数据加密开销并保护了用户隐私；另一方面，通过属性的与、或、非和门限操作实现属性灵活的细粒度访问控制策略。ABE 机制的高效性、动态性、加密策略的灵活性以及细粒度访问控制使它在分布式文件管理、第三方数据管理、组密钥管理、隐私保护、付费电视系统等领域具有良好的应用前景[2,3]。属性基加密引入了与用户属性相关联的访问控制结构，只有当用户的属性符合访问控制策略时才能解密。实际应用中，经常会出现用户的加入或离开，用户权限发生变化，以及强制性的删除泄密用户等现象，不可避免地需要考虑密钥和属性的撤销问题。

2 相关工作

在已有的属性撤销方案中，根据撤销执行者的不同，当前 ABE 撤销机制的研究工作主要分为直接撤销和间接撤销 2 类。间接撤销由授权机构执行，授权机构周期性地更新未撤销用户的密钥，只有未

收稿日期：2015-08-06；修回日期：2015-11-09
基金项目：国家自然科学基金资助项目（No.61300216）；河南省科技攻关基金资助项目（No.132102210123, No.152102410048）；河南省教育厅科研项目（No12A520021, No.16A520013）；河南理工大学博士基金资助项目（No.B2013-043）
Foundation Items: The National Natural Science Foundation of China (No.61300216), Project of Science and Technology Department of Henan Province (No.132102210123, No.152102410048), Foundation of Henan Educational Committee (No.12A520021, No.16A520013), Doctoral Program of Henan Polytechnic University (No.B2013-043)

撤销的用户才能更新密钥，通过新密钥解密新密文，而撤销用户将无法收到更新而导致密钥无效。文献[3]最早提出 ABE 属性撤销方法，通过给每个属性设置一个有效期，授权机构周期性地释放属性的最新版本，通过撤销用户某个属性的最新版本来实现对用户属性的撤销。文献[4]用属性的终止日期取代有效期，来限制密钥的使用时间。这 2 种方案都不能满足实际应用需求，密钥更新过程中，授权机构密钥更新的工作量与用户数据线性相关，另外，都不支持属性的即时撤销。文献[5]采用二叉树提出可撤销的 KP-ABE 机制，支持用户撤销，并不支持属性的即时撤销。为了实现属性的即时撤销，Ibraimi 等[6]提出引入第三方扮演仲裁者，将用户密钥分别由仲裁者和用户持有，实现 CP-ABE 撤销方案。Yu 等[7]引入半可信的代理服务器，基于代理重加密技术实现可撤销的 KP-ABE 方案。这 2 种方案实现了属性的即时撤销，减轻了授权机构的工作量，但要求第三方必须保持在线。文献[8]将数据文件分成许多小片段进行存储，当撤销事件发生时，数据拥有者对部分片段进行重加密，实现间接的用户撤销。Hur 等[9]基于二叉树，通过向合法用户分发一个对称密钥，提出一个支持完全细粒度属性撤销的 CP-ABE 方案，该方案支持属性的即时撤销，但是密钥维护代价高，且无法抵抗合谋攻击。Xie 等[10]对 Hur 的方案进行了优化，缩小了密文和密钥的尺寸，并减轻了密钥更新阶段的计算量，但是这 2 种方案都是基于一般的群假设安全问题。

间接撤销虽然可以实现属性的即时撤销，但由于授权机构需要与未撤销用户一直进行在线交互，进行密钥的更新工作，不适用于离线操作，也不能很好地抵抗合谋攻击。直接撤销由发送方执行，发送方在信息加密阶段直接加入撤销用户的列表信息，从而实现属性密钥的撤销。文献[11]首次提出基于密文策略属性基加密（CP-ABE, cipher-text-policy ABE）的直接撤销思想，把用户标识作为一种属性，利用“非”的用户标识与密文进行关联，当用户被撤销时，他的用户标识就成为“非”，将无法解密，从而实现撤销用户或者系统属性，但是该方案增加了密文和用户密钥长度。文献[12]结合广播加密思想，实现基于密钥策略属性基加密和密文策略属性基加密的属性直接撤销，该方案降低了撤销开销，撤销的用户不会影响其余未撤销用户的权限。直接撤销方法将唯一确定用户身份的属性信息作为用户标识，仅支持整个用户的撤销，无法解决用户部分属性撤销的问题，并且用户密钥和密文长度有所增加。文献[13]针对属性的细粒度撤销，基于合数阶双线性群实现了属性直接撤销的 CP-ABE 方案，该方案公钥参数与用户数量线性相关，容易造成公钥参数过长。文献[14]基于线性秘密分享方案（LSSS, linear secret sharing scheme）将属性撤销列表嵌入到密文中，实现支持属性直接撤销的 CP-ABE 方案的一般构造，并证明其满足自适应安全。

已有的直接撤销 ABE 方案[12~14]大多数都是基于合数阶双线性群和 LSSS 技术，通过在密文中嵌入用户撤销列表实现属性撤销，但是线性秘密分享中分享矩阵如何表达访问控制策略并没有进行详细的描述。对于一般的单调访问结构，文献[15]给出了构造相应 LSSS 的算法。文献[16]提出一种有效的算法生成 LSSS 中的分享矩阵，实现将门限访问树结构转换为 LSSS 矩阵访问结构。在标准假设下，LSSS 矩阵和访问树结构都支持属性的与、或、门限操作，但是 LSSS 秘密分享矩阵构造相对复杂。而访问树通常利用拉格朗日多项式插值来实现，构造复杂度相对较低，因此基于访问树的 ABE 方案在应用中更为实用。

本文将基于访问树结构和 Shamir 门限秘密分享技术，借鉴 Lewko 等[17]在可撤销的广播加密中所用到的“two equation”技术，结合 Ibraimi 等[18]提出的 ABE 方案，给出一个支持直接撤销的 CP-ABE 方案，并给出其相应的安全性证明。

3　算法定义和安全模型

3.1　算法定义

一个安全的支持直接撤销的 CP-ABE 方案由系统初始化 $Setup(k)$、密钥生成 $KeyGen(ID, w, mk, pk)$、加密算法 $Encrypt(m,t, pk, R)$、解密算法 $Decrypt(c, sk_{w,ID}, pk)$ 4 部分构成。

1) $Setup(k)$：输入安全参数 k，输出主密钥 mk 和主公钥 pk。

2) $KeyGen(ID,w, mk, pk)$：输入主密钥 mk，主公钥 pk，属性集合 w，用户标识 ID，输出用户 ID 关于属性集合 w 的私钥 $sk_{w,ID}$。

3) $Encrypt(m,t, pk, R)$：算法以系统公钥 pk，消息 m，访问树 t 以及用户撤销列表 R 为输入，输出密文 c。

4) $Decrypt\left(c, sk_{w,ID}, pk\right)$:算法输入用户的私钥 $sk_{w,ID}$，密文 c，系统公钥 pk，当用户 ID 所拥有的与访问结构 t 相关的未被撤销的属性集合满足访问树，输出消息明文 m。

3.2 安全模型

下面将给出支持撤销的 CP-ABE 方案在选择明文攻击下的安全模型。

攻击者A和挑战者B之间具体攻击游戏如下。

准备阶段：攻击者A选择访问树 t^*，指定用户撤销列表 R^* 发送给挑战者B。

系统设置：挑战者B运行 $Setup\left(k\right)$ 算法生成主密钥 mk 和主公钥 pk，将公钥 pk 发送给攻击者A，自己保存主密钥 mk。

阶段 1：攻击者A选择询问用户 ID 关于属性集 w' 的私钥，要求 $w' = \{a_j \mid a_j \in w \cap t^*, ID \notin R^*\}$ 不能满足访问结构 t^*，即攻击者所询问的私钥不能直接成功解密最终的询问密文。挑战者B运行 $KeyGen\left(ID, w, mk, pk\right)$ 得到用户 ID 关于属性集合 w 的私钥 $sk_{w,ID}$，将 $sk_{w,ID}$ 返回给攻击者A。

挑战：攻击者A向挑战者B发送 2 个等长信息 m_0 和 m_1，挑战者B执行公平的掷硬币游戏选取 $b \in \{0,1\}$，运行 $Encrypt\left(m, t, pk, R\right)$ 算法，将得到的挑战密文 c' 返回给攻击者A。

阶段 2：同阶段 1，攻击者可以继续向挑战者进行询问。

猜测：攻击者猜测 $b' \in \{0,1\}$。如果 $b' = b$，则说明攻击者成功。攻击者进行游戏获得成功的优势为 $Adv_{\text{CP-ABE}}^{\text{IND-CPA}}(A) = \left|\Pr\left[b' = b\right] - \frac{1}{2}\right|$，其中，概率取决于随机参数的概率分布和算法的内部随机掷币。

如果没有概率多项式时间攻击者能够以不可忽略的优势赢得游戏，则称支持撤销的 CP-ABE 方案是选择明文安全的。

4 具体方案构造

4.1 方案构造

1) 系统初始化 $Setup(k)$

令属性集合 $I = \{1, 2, \ldots, m\}$，用户集合 $U = \{1, 2, \ldots, n\}$，输入安全参数 k，执行以下过程。

①选取一个双线性群 G_0，其阶为 p，生成元为 g，并且选取双线性映射 $e: G_0 \times G_0 \to G_1$。

②随机生成 $a, t_1, t_2, \ldots, t_m \in Z_p^*$，计算 $T_i = g^{t_i}$ $(1 \le i \le m)$，$y = e(g,g)^a$。

③随机生成 $b \in Z_p^*$，计算 $B = g^b$，$B' = g^{b^2}$。

公布公钥 $pk = (e, g, y, B, B', T_i)(1 \le i \le m)$，主密钥 $mk = (a, b, t_i)(1 \le i \le m)$。

2) 密钥生成 $KeyGen(ID, w, mk, pk)$

输入用户 $ID \in U$、属性集 $w \subseteq I$ 和系统主密钥 mk 和公钥 pk，输出用户的私钥 $sk_{w,ID}$。

① 随机为每个用户选取 $r, t \in Z_p^*$，计算 $D^{(1)} = g^{b^2 t} g^{a+r}$。

②对每个属性 $i \in w$，计算 $D_i^{(2)} = g^{r t_i^{-1}}$。

③对每个用户计算 $D^{(3)} = \left(g^{bID}\right)^t$，$D^{(4)} = g^t$。

因此，用户的私钥为 $sk_{w,ID} = (D^{(1)}, \{D_i^{(2)}\}_{i \in w}, D^{(3)}, D^{(4)})$。

3) 数据加密 $Encrypt\left(m, t, pk, R\right)$

基于属性域指定一个访问树 t，令 $R = U \setminus S$，S 为未撤销用户列表，用户撤销列表 $R = \{ID_1, ID_2, \ldots, ID_r\}$，对消息 m 进行加密。

① 选择随机数 $s \in Z_p^*$，计算 $C^{(1)} = my^s = me(g,g)^{as}$，$c^{(2)} = g^s$。

②设置访问树 t 根节点的值为待共享的值 s，将根节点置为已分配，其所有的孩子节点标记为未分配，对每个未分配的非叶子节点执行以下递归算法。

若标识符号为 of（门限操作），且它的孩子节点标记为未分配，采用 (t,n) Shamir 门限秘密共享机制将 s 赋值给孩子节点。n 是所有孩子节点的个数，t 是重构秘密所需的孩子节点个数，这里 $n \ne t$，每个孩子节点被赋予 $s_i = f(i)$，标记这些节点为已分配。

若标识符号为 $\wedge$（与操作），且它的孩子节点标记为未分配，采用 (t,n) Shamir 门限秘密共享机制将 s 赋值给孩子节点。这里 $t = n$，对每个孩子节点分配 $s_i = f(i)$，标记这些节点为已分配。

若标识符号为 $\vee$（或操作），且它的孩子节点标记为未分配，同样采用 Shamir 门限秘密共享机制将 s 赋值给孩子节点，这里 $t = 1$，即设置其孩子节点为 s，并标记节点为已分配。

其中，多项式 $y = f(x) = \sum_{i=0}^{t-1} a_i x^i$ 由 t 个点 $(x_i, y_i) = (i, s_i)$ 唯一确定。$l_i(0)$ 是拉格朗日系数，

$$f(0)=f(x)\big|_{x=0}=\sum_{i=0}^{t-1}f(i)l_i(x)\Big|_{x=0}=\sum_{i=0}^{t-1}s_i l_i(x)\Big|_{x=0}$$
$$=\sum_{i=0}^{t-1}s_i l_i(0)=s。$$

③对每个叶子节点 $a_{j,i}\in t$ （i 表示访问树中叶子节点所对应的索引值），计算 $C_{j,i}^{(3)}=T_j^{s_i}$。

④随机选择 $v_1,v_2,\mathrm{L},v_r\in Z_p^*$，且 $v_1+v_2+\mathrm{L}+v_r=s$，计算 $C_j^{(4)}=g^{bv_j}$，$C_j^{(5)}=(g^{b^2ID_j})^{v_j}$。

密文为 $c=\left(C^{(1)},C^{(2)},\left\{C_{j,i}^{(3)}\right\}_{a_{j,i}\in t},\left\{C_j^{(4)}\right\}_{j\in[1,r]},\left\{C_j^{(5)}\right\}_{j\in[1,r]}\right)$。

4) 数据解密 $Decrypt\left(c,sk_{w,ID},pk\right)$

选择可以满足访问树的最小集合 $w'\subseteq w$，并且用户 $ID\in S$，则执行解密操作。

①对每个属性 $i\in w'$，且当 $ID\neq ID_j$ 时，计算

$$K=\frac{e\left(C^{(2)},D^{(1)}\right)}{\prod_{i\in w'}e\left(C_{j,i}^{(3)},D_i^{(2)}\right)^{l_i(0)}}\prod_{j=1}^{r}\left(\frac{e\left(C_j^{(5)},D^{(4)}\right)}{e\left(C_j^{(4)},D^{(3)}\right)}\right)^{\frac{1}{ID-ID_j}}。$$

②计算 $m=\dfrac{C^{(1)}}{K}$。

正确性证明

$$e\left(C^{(2)},D^{(1)}\right)$$
$$=e\left(g^s,g^{b^2t}g^{a+r}\right)$$
$$=e\left(g,g\right)^{sb^2t}e\left(g,g\right)^{as}e\left(g,g\right)^{rs}\qquad(1)$$
$$\prod_{i\in w'}e\left(C_{j,i}^{(3)},D_i^{(2)}\right)^{l_i(0)}$$
$$=\prod_{i\in w'}e\left(T_j^{s_i},g^{rt_j^{-1}}\right)^{l_i(0)}$$
$$=\prod_{i\in w'}e\left(g^{t_j s_i},g^{rt_j^{-1}}\right)^{l_i(0)}$$
$$=e\left(g,g\right)^{\sum_{i=0}^{t-1}rs_i l_i(0)}$$
$$=e\left(g,g\right)^{rs}\qquad(2)$$

$$\prod_{j=1}^{r}\left(\frac{e\left(C_j^{(5)},D^{(4)}\right)}{e\left(C_j^{(4)},D^{(3)}\right)}\right)^{\frac{1}{ID-ID_j}}$$
$$=\prod_{j=1}^{r}\left(\frac{e\left(\left(g^{b^2ID_j}\right)^{v_j},g^t\right)}{e\left(g^{bv_j},\left(g^{b^2ID}\right)^t\right)}\right)^{\frac{1}{ID-ID_j}}$$
$$=\prod_{j=1}^{r}\left(e\left(g,g\right)^{b^2t\left(ID_j-ID\right)v_j}\right)^{\frac{1}{ID-ID_j}}$$
$$=e\left(g,g\right)^{-b^2t\sum_{j=1}^{r}v_j}$$
$$=e\left(g,g\right)^{-b^2ts}\qquad(3)$$
$$K=e\left(g,g\right)^{as}\qquad(4)$$
$$\frac{C^{(1)}}{K}=\frac{me\left(g,g\right)^{as}}{e\left(g,g\right)^{as}}=m\qquad(5)$$

4.2　安全性证明

本方案基于判定双线性 Diffie-Hellman 问题（DBDH, decisional bilinear Diffie-Hellman problem）。给定 $\left(g,g^a,g^b,g^c,Z\right)$，其中，$a,b,c,q\in Z_p^*$，$Z=e\left(g,g\right)^q$，计算 $e\left(g,g\right)^{abc}$，判断 $Z=e\left(g,g\right)^{abc}$ 是否成立。一个概率性多项式时间算法B能够以优势 e 求解 DBDH 问题，当且仅当满足

$$\Pr\left[B\left(g,g^a,g^b,g^c,e\left(g,g\right)^{abc}\right)=1\right]-$$
$$\Pr\left[B\left(g,g^a,g^b,g^c,e\left(g,g\right)^{q}\right)=1\right]\geq e$$

定理 1　假设 DBDH 成立，那么敌手就无法在多项式时间内选择访问树 t^* 下攻破支持撤销的 CP-ABE 方案，该方案是 IND-sAtt-CPA 安全的。

证明　如果存在一个攻击者A可以攻破本方案，则存在一个算法B可以攻破 DBDH 问题，即输入 $\left(g,g^{a_1},g^{a_2},g^s,Z_m=e\left(g,g\right)^q\right)$，算法B决定等式 $Z_m=e\left(g,g\right)^{a_1a_2s}$ 是否成立。

初始化：攻击者A选择访问树 t^* 和用户撤销列表 $R=\left\{ID_1,ID_2,\mathrm{L},ID_{r^*}\right\}$ 发送给挑战者B。

系统设置：挑战者B运行 $Setup\left(k\right)$ 算法。

①选择随机数 $x'\in Z_p^*$，设置 $e\left(g,g\right)^a=e\left(g,g\right)^{a_1a_2}e\left(g,g\right)^{x'}$，使 $a=a_1a_2+x'$，计算 $y=e\left(g,g\right)^a$。

②对每一个属性 $a_j\in\Omega\left(1\leq j\leq n\right)$，选择随机数 $s_j\in Z_p^*$，如果 $a_j\notin t^*$，设 $T_j=B^{s_j^{-1}}$，那么 $t_j=a_2s_j^{-1}$；如果 $a_j\in t^*$，设 $T_j=g^{s_j}$，那么 $t_j=s_j$。

③选择随机数 $b_1,b_2,\mathrm{L},b_r\in Z_p^*$，令 $b_1+,b_2+\mathrm{L}+b_r=b$，计算 $g^b=\prod_{1\leq i\leq r^*}g^{b_i}$，$g^{b^2}=\prod_{1\leq i,j\leq r^*}\left(g^{b_ib_j}\right)$ 则公钥 $pk=(e,g,g^b,g^{b^2},\ g^{x'},y,T_j(1\leq j\leq n))$，$mk=\left(a,t_j,x',b\left(1\leq j\leq n\right)\right)$。

挑战者B将公钥 pk 发送给攻击者A，自己保存主密钥 mk。

阶段1：攻击者A选择属性集 $w=\{a_j \mid a_j \notin t^*\}$ 和 $ID_i \notin R$，向挑战者B发出属性私钥询问请求。

①挑战者B随机选择 $r',t' \in Z_p^*$，并满足 $t=-\frac{a}{b_i^2}+t'$，$r=r'a_2-a_1a_2$，因为 $a=a_1a_2+x'$，所以，$D^{(1)}=\left(\prod_{1\le j,k\le n,\ j,k\ne i} g^{-\frac{(a_1a_2+x')b_jb_k}{b_i^2}}\right)\left(\prod_{1\le j\le n}\left(g^{b_jb_k}\right)^{t'}\right)g^{x'+r'a_2}$。

②对每个属性 $a_j \in w$，因为 $r=r'a_2-a_1a_2$，$t_j=a_2s_j^{-1}$，计算 $D^{(2)}=g^{(r'a_2-a_1a_2)a_2^{-1}s_j}=g^{-a_1s_j}g^{r's_j}=\frac{g^{r's_j}}{A^{s_j}}$。

③计算 $D^{(3)}=\left(\prod_{1\le j\le n,\ j\ne i} g^{-\frac{(a_1a_2+x')b_jID_i}{b_i^2}}\right)\prod_{1\le j\le n}\left(g^{b_jID_i}\right)^{t'}$，$D^{(4)}=g^{-\frac{(a_1a_2+x')}{b_i^2}}g^{t'}$。

挑战者B将属性密钥 $sk_{w,ID}=(D^{(1)},\{D_i^{(2)}\}_{i\in w},D^{(3)},D^{(4)})$ 发送给攻击者A。

挑战：攻击者A向挑战者B发送2个等长信息 m_0 和 m_1，挑战者B执行公平的掷硬币游戏选取 $b\in\{0,1\}$，进行以下操作。

①随机选择 $s'\in Z_p^*$，计算 $C^{(1)}=M_be(g,g)^{(a_1a_2+x')(s+s')}=M_be(g,g)^{a_1a_2s}e\left(g^{x'},g^s\right)e(g,g)^{a_1a_2s'}e(g,g)^{s'}$，$C^{(2)}=g^{s+s'}$。

②设置访问树 t 根节点的值为待共享的值 $s+s'$，将根节点置为已分配，其所有的孩子节点标记为未分配，对每个未分配的非叶子节点执行以下递归算法。

若标识符号为 of（门限操作），且它的孩子节点标记为未分配，采用 (t,n) Shamir 门限秘密共享机制将 $s+s'$ 赋值给孩子节点。n 是所有孩子节点的个数，t 是重构秘密所需的孩子节点个数，这里 $n\ne t$，每个孩子节点被赋予 $h_i'=f(i)$，标记这些节点为已分配。

若标识符号为 $\wedge$（与操作），且它的孩子节点标记为未分配，采用 (t,n) Shamir 门限秘密共享机制将 $s+s'$ 赋值给孩子节点。这里 $t=n$，对每个孩子节点分配 $h_i'=f(i)$，标记这些节点为已分配。

若标识符号为 $\vee$（或操作），且它的孩子节点标记为未分配，同样采用 Shamir 门限秘密共享机制将 $s+s'$ 赋值给孩子节点，这里 $t=1$，即设置其孩子节点为 $s+s'$，并标记节点为已分配。

③对每个叶子节点 $a_{j,i}\in t^*$，计算 $C_{j,i}^{(3)}=g^{h_is_j}$。

④随机选择 $v_1',v_2',\cdots,v_r' \in Z_p^*$，且 $v_1'+v_2'+\cdots+v_r'=s'$，令 $v_i''=\frac{b_is}{b}+v_i'$，计算 $C_j^{(4)}=g^{bv_j''}=g^{sb_i}\left(\prod_{1\le j\le r'} g^{b_j}\right)^{v_j'}$，$C_j^{(5)}=\left(g^{b^2ID_j}\right)^{v_j'}=\left(\prod_{1\le j\le r^*} g^{sb_ib_jID_j}\right)\cdot\left(\prod_{1\le j\le r^*} g^{b_ib_jID_j}\right)^{v_j'}$。

挑战者B将密文 $c=\left(C^{(1)},C^{(2)},\{C_{j,i}^{(3)}\}_{a_{j,i}\in t},\{C_j^{(4)}\}_{j\in[1,r']},\{C_j^{(5)}\}_{j\in[1,r]}\right)$ 返回给攻击者A。

阶段2：同阶段1，攻击者A可以继续向挑战者B进行询问。

猜测：攻击者A输出猜测 $b'\in\{0,1\}$。

如果 $b'=b$，则挑战者输出1，表示DBDH成立，$Z=e(g,g)^{a_1a_2s}$。否则，输出0，表明 $Z=e(g,g)^{a_1a_2s}$。

当 $Z=e(g,g)^{a_1a_2s}$，攻击者获得的是有效的密文，攻击者的优势为 $\Pr\left[b'=b \mid Z=e(g,g)^{a_1a_2s}\right]=\frac{1}{2}+e$。

当 $Z=e(g,g)^q$ 时，攻击者获得的密文是随机的，并不能获得明文的任何信息，$\Pr\left[b'\ne b \mid Z=e(g,g)^q\right]=\frac{1}{2}$。

因此，$\Pr\left[B\left(g,g^{a_1},g^{a_2},g^s,e(g,g)^{a_1a_2s}\right)=1\right]-\Pr\left[B\left(g,g^{a_1},g^{a_2},g^s,e(g,g)^q\right)=1\right]\ge e$ 成立，即假定攻击者A能够以优势 e 求解DBDH。

综上分析，假设DBDH成立，如果没有敌手可以在多项式时间内选择访问树 t^* 下攻破支持撤销的CP-ABE方案，那么该方案是IND-sAtt-CPA安全的。

5 效率分析

下面与其他几个直接撤销ABE方案从密文长

表 1　　各种直接撤销机制对比

方案	密文长度	私钥长度	公钥长度	访问策略
文献[11]	$2t+1+O(r)$	$(2k+2)\log n$	$3\log n+O(n)$	与门
文献[12]BCP-ABE1	$t+2$	$k+2$	$m+l+3+2n-1$	LSSS
文献[12]BCP-ABE2	$t+1+2r$	$k+4$	$m+l+7$	LSSS
文献[13]	$2t+3r+1$	$2k+1$	$2l+2n+2$	LSSS
本文方案	$t+2r+2$	$k+3$	$l+5$	访问树

度、属性私钥大小、系统公钥大小、解密过程的计算量等方面进行比较，具体比较结果如表 1 所示，表中数据代表群 G 中元素的总数，群 G 中一个元素的比特长度为 L，l 表示属性域中的属性总个数，n 表示系统中用户的最大数目，r 表示用户撤销列表中用户个数，t 表示加密时访问策略中出现的属性的个数，k 表示用户所拥有的属性个数，m 表示用户所允许拥有属性的最大数目。

从表 1 对比结果可以看出，文献[11]仅仅支持与门访问策略，无法实现灵活的访问控制。文献[12]中 BCP-ABE1 方案 1 密文长度虽然比 BCP-ABE2 方案短小，但是公钥长度却远远比方案 2 长，并且与系统用户数量相关，无法提高系统的效率。文献[12,13]均采用 LSSS 表示访问策略，支持与、或、门限访问策略，但是文献[13]所提方案中密文长度、私钥长度和公钥长度均没有文献[12]所提方案简短。本文方案对公钥长度进行了优化，与文献[12]中 BCP-ABE2 相比，在密文长度增加群 G 中 1 个元素长度的代价下，公钥长度得到了大大的缩短，并且使公钥长度与系统用户数量、用户所拥有属性数量无关，使系统用户数量和用户拥有属性数量不受限制，提高系统的效率，系统范围越广，用户和用户拥有属性越多，本方案在存储空间和效率上的优势越明显。经过以上分析，可见本文方案与其他方案相比较达到了优化。

6　结束语

针对已有的属性撤销方案的不足，本文提出了支持直接撤销的密文策略属性基加密模型，并给出了其安全性定义。以 Ibraimi 等[18]提出的 CP-ABE 方案为基础，构造出一个具体的支持直接撤销的 CP-ABE 方案并证明其满足选择明文攻击安全。本文方案与已有的方案进行对比，密文长度、用户私钥长度以及公钥长度都得到了减短，但是该方案的公钥参数与属性总数量线性相关。因此，实现一个公钥参数与用户数量、属性数量无关的且支持属性撤销的 CP-ABE 方案，是笔者下一步工作所要重点考虑的问题。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// Advances in Cryptology - EUROCRYPT 2005. Berlin, c2005: 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security. New York, c2006: 89-98.

[3] PIRRETTI M, TRAYNOR P, MCDANIEL P, et al Secure attribute-based systems[C]//The ACM Conf on Computer and Communications Security. New York, c2006: 99-111.

[4] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//The 2007 IEEE Symp on Security and Privacy. Washington, c2007: 322-334.

[5] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[C]//The ACM Conf on Computer and Communications Security. New York, c2008: 417-426.

[6] IBRAIMI L, PETKOVIC M, NIKOYA S, et al. Mediated ciphertext-policy attribute-based encryption and its application[C]//The 10th Int'l Workshop on Information Security Applications-WISA. Berlin, c2009: 310-322.

[7] YU S C, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]//The ASIAN ACM Conf on Computer and Communications Security (ASIACCS 2010). New York, c2010: 262- 270.

[8] CHENG Y, WANG Z Y, MA J, et al. Efficient revocation i ciphertext-policy attribute-based encryption based cryptographic cloud storage [J]. Journal of Zhejiang University-Science, 2013, 14(2): 85-97.

[9] HUR J, NOH D K. Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, l22(7): 1214-1221.

[10] XIE X X, MA H, LI J, et al. An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing [J]. Journal of Universal Computer Science, 2013, l19(16): 2349-2367.

[11] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[C]//The ACM Conf on Computer and Communications Security. New York, c2007: 195-203.

[12] ATTAPADUNG N, IMAI H. Conjunctive broadcast and attribute-based encryption[C]//The Pairing-Based Cryptography-Pairing 2009. Berlin, c2009: 248-265.

[13] **王鹏翮,冯登国,张立武.一种支持完全细粒度属性撤销的** CP-ABE **方案**[J].**软件学报**, 2012, 23(10): 2805-2816.
WANG P P, FENG D G, ZHANG L W. CP-ABE scheme supporting fully fine-grained attribute revocation[J]. Journal of Software, 2012, 23(10): 2805-2816.

[14] WU Q X. A generic construction of ciphertext-policy attribute-based encryption supporting attribute revocation[J]. China Communications,2014, l11(1): 93-100.

[15] LIU Z, CAO Z F. On efficiently transferring the linear secret-sharing schemes matrix in ciphertext-policy attribute-based encryption[J/OL]. http://eprint.iacr.org/2010/374.pdf, 2010.

[16] LIU Z, CAO Z F. Efficient generation of linear secret haring scheme matrices from threshold access trees[C]//Cryptology ePrint Archive: Listing.c2010.

[17] LEWKO A, SAHAI A, WATERS B. Revocation systems with very small private keys[C]//IEEE Symposium on Security and Privacy (SP). Oakland, USA, c2010:273-285.

[18] IBRAIMI L, TANG Q, HARTEL P, et al. Efficient and provable secure ciphertext-policy attribute-based encryption schemes[C]//The Information Security Practice and Experience. Berlin, c2009: 1-12.

作者简介：

闫玺玺（1985-），女，河南灵宝人，博士，河南理工大学讲师，主要研究方向为数字版权管理、数字内容安全、计算机网络安全。

孟慧（1981-），女，河南孟县人，博士，河南理工大学讲师，主要研究方向为数字签名、数字内容安全、计算机网络安全。