# 支持直接撤销的固长密文策略属性基加密方案

朱国斌[1,2*]，谢 鑫[1,2]，张 星[1,2]，赵 洋[1,2]，熊 虎[1,2]

(1. 电子科技大学信息与软件工程学院 成都 610054；2. 网络与数据安全四川省重点实验室 成都 610054)

【摘要】该文提出一种支持直接撤销功能且具有固定长度的密文策略属性基加密方案，首先给出了该属性基加密方案的形式化定义和安全模型，然后对方案具体的实现进行了阐述，最后给出了该方案在标准模型下的安全性证明。该方案在密文长度和解密开销固定的同时，允许用户在加密过程中将撤销列表嵌入到密文中以实现直接撤销，保证了仅当用户所拥有的属性满足密文访问结构且用户身份没有出现在撤销列表的前提下，才可以使用自己的私钥解密执行解密。对比分析结果表明，该方案较同类方案具有更高的计算效率且支持更灵活的访问结构。

**关 键 词** 属性基加密； 访问结构； 密文策略； 直接撤销

**中图分类号** TP309 **文献标志码** A doi:10.12178/1001-0548.2020341

# Direct Revocable Ciphertext Policy Attribute-Based Encryption Scheme with Constant-Size Ciphertext

ZHU Guo-bin[1,2*], XIE Xin[1,2], ZHANG Xing[1,2], ZHAO Yang[1,2], and XIONG Hu[1,2]

(1. School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 610054;
2. Network and Data Security Key Laboratory of Sichuan Province Chengdu 610054)

**Abstract** By considering the dynamic user access privilege and the potential leakage of secret key, a direct revocable ciphertext policy attribute-based encryption (usually shorten as CP-ABE) scheme with constant-size ciphertext is proposed in this paper. Different from the indirect revocable CP-ABE, the proposed approach allows the data owner to assign the revoked users during the encryption without interacting the attribute authority periodically. The definition and security model of the direct revocable attribute-based encryption scheme are given and a concrete scheme is also constructed correspondingly. The security proof of the scheme is given under the standard model. The results of comparative analysis show that the scheme achieves higher computational efficiency and supports more flexible access structure than the state-of-the-art.

**Key words** attribute-based encryption; access structure; ciphertext policy; direct revocation

随着以云存储为代表的大规模分布式存储技术的成熟与推广，具有隐私保护与访问控制功能的密码机制有了重要的应用价值[1-2]。在基于身份加密算法的基础上，文献 [3] 提出了属性基加密 (attribute-based encryption, ABE) 方案。通过引入属性的概念，采用属性集替代用户身份，以实现对数据的细粒度访问。在属性基加密中，用户拥有的属性与加解密过程关联，只有当用户属性满足预定的访问结构时，用户才能够正确执行解密过程。属性基加密采用一对多的模式，将访问控制与数据加密相结合，通过用户属性的与、或、非和门限操作的组合，可以实现灵活的细粒度访问控制策略管理[4-5]。依据访问控制策略实现的方式，属性基加密算法可以被分为为两种类型：密文策略属性基加密 (ciphertext-policy ABE, CP-ABE)[6] 和密钥策略属性基加密 (key-policy ABE, KP-ABE)[7]。KP-ABE 将密文与解密策略关联，CP-ABE 则将用户私钥与解密策略关联。

早期的研究工作中，多数 ABE 方案主要关注对访问策略的表达与实现能力，未对用户属性撤销问题进行关注[8-11]。在实际应用中，不同用户通常拥有部分相同的属性，属性到期、属性变更、密钥泄露、用户动态加入与退出等情况往往会引发属性撤销的问题。具体地，实用的属性基加密应该在用户访问权限出现变化时，能够通过权限更新使得用

收稿日期：2020－09－21；修回日期：2020－10－15
基金项目：国家自然科学基金 (61602096)；四川省国际科技创新合作/港澳台科技创新合作项目 (2020YFH0062)
作者简介：朱国斌 (1981－)，男，博士，副研究员，主要从事网络安全、移动互联网安全、密码学方面的研究. E-mail：zhugb@uestc.edu.cn

户属性变化后不满足访问结构的用户无法使用旧密钥解密密文，同时不影响其他访问权限未发生变化的用户。因此，构建支持高效属性撤销的 ABE 方案成为亟需解决的关键问题[12]。

# 1　相关工作

文献 [13] 首次提出用户属性撤销的概念。文献 [14] 采用基于身份的组播加密技术和线性秘密共享技术，提出了属性撤销的两种实现方式：间接撤销与直接撤销。间接撤销是指由可信的授权机构定期更新未撤销用户的密钥，被撤销的用户因不会收到更新而使得密钥失效。间接撤销的优势在于不需要维护撤销列表，其缺点是需要授权中心进行在线密钥更新，密钥更新的开销与用户数量线性相关，因此容易形成系统瓶颈。直接撤销由发送方在信息加密阶段将撤销用户的列表信息加入密文，从而实现对指定用户的撤销。直接撤销方案[15-17] 中大部分使用了广播加密技术，开销较大。为减轻授权机构的工作量，文献 [18] 采用版本号标记密钥密文，同时引入代理服务器，将代理重加密技术与 CP-ABE 相结合，降低了授权机构的工作量，实现了较小开销的属性撤销。文献 [19] 构造了一个基于中国剩余定理的可撤销 CP-ABE 方案，在实现直接撤销的同时可保持固定的密文和密钥长度。上述所有支持撤销的属性基加密方案仍然存在着属性撤销开销较大的问题，具有进一步优化的空间。

本文结合中国剩余定理和多值通配与门访问策略，提出了一个支持直接撤销功能的 CP-ABE 方案，该方案同时还具有密文长度和解密开销固定的特点。在给出形式化定义和安全模型后，采用双线性映射给出了方案的具体构造。形式化的安全证明和实验分析都表明本文方案是高效而安全的。

# 2　理论知识

## 2.1　中国剩余定理

设集合$\{m_1,m_2,\cdots,m_k\}(k\geqslant 2)$是$k$个正整数，且这 $k$ 个数互素，令$L=m_1*m_2*\cdots*m_k$。

那么存在以下同余方程组：

$$\begin{cases} X\equiv x_1 \bmod m_1 \\ X\equiv x_2 \bmod m_2 \\ \quad\vdots \\ X\equiv x_k \bmod m_k \end{cases}$$

以上方程组的解是唯一的：

$$X=\sum_{i=1}^{k}(x_iL_iN_i) \bmod L \tag{1}$$

式中，$L_i=\dfrac{L}{m_i}N_i=L_i^{-1} \bmod m_i$，式 (1) 为中国剩余定理。

## 2.2　多值通配与门

依据访问策略的不同，使用较多的是正负通配与门和多值通配与门，其中多值通配与门在相同访问策略下具有更好的灵活性，故本文选用了多值通配与门来表示访问控制结构。现假设有访问策略如表 1 所示。

**表 1　访问策略示例**

| 属性名称 | 所属学校 | 用户身份 | 用户性别 |
|---|---|---|---|
| | 大学A | 教师 | 女 |
| 属性取值 | 大学B | 辅导员 | 男 |
| | 大学C | | |
| 访问策略 | 大学C | * | 女 |

使用正负通配与门访问结构表达上述策略为：

$$\mathrm{AP}=w_1^-\wedge w_2^-\wedge w_3^+\wedge w_4^*\wedge w_5^*\wedge w_6^-\wedge w_7^+$$

式中，$w^+$表示访问策略中包含该属性；$w^-$表示不包含该属性；$w^*$表示与属性无关。该访问策略的多值通配与门访问结构为：

$$\mathrm{AP}=w_{1,3}\wedge *\wedge w_{3,2}$$

式中，分项为对应属性的取值；通配符*表示属性对解密过程无影响。由此可见，多值通配与门访问结构对访问策略的描述更为简明。现对多值通配与门结构定义如下。

**定义 1**　多值通配与门。给定一个属性列表 $L$ 和一个访问策略 $W$，$L|=W$表示 $L$ 与 $W$ 匹配，$L|\neq W$表示不匹配。给定一个属性列表$L=[L_1,L_2,\cdots,L_n]$和访问策略$W=[W_1,W_2,\cdots,W_n]=\wedge_{i\in I_W}$，对于$1\leqslant i\leqslant n$，若$L_i=W_i$或$W_i=*$，则称$L|=W$，否则$L|\neq W$。

其中，$I_W=\{i|1\leqslant i\leqslant n,W_i\neq *\}$为一个属性索引集。在计算过程只考虑$W$ 中出现的非通配符属性，选取对应下标的属性值进行计算 ($I_L$也选取对应的下标进行计算)，$W$中没有出现的属性其取值被表示为通配符*，对应的用户属性与解密能力无关。

## 2.3　困难性问题假设

**定义 2**　判定性 DBDH(decisional bilinear diffie-hellman) 假设。设有循环群$G,G_T$，群的阶均为大素数$p$，$g$为群$G$的生成元，存在双线性映射$e:G\times G\to G_T$，对于$\forall a,b,c\in Z_p^*$，给定五元组$(g,g^a,g^b,g^c,g^{abc})$，选取$z\in_R Z_p^*$，若不存在有效算法$C$在多项式

时间内以不可忽略的优势判断$e(g,g)^{abc}=e(g,g)^{z}$，则假设成立。

# 3 基于直接撤销的固长密文 CP-ABE 方案

## 3.1 方案模型

本方案中共有 5 个参与者：数据访问者、数据拥有者、数据存储服务器、外包解密服务器、权威中心。具体说明如下：

1) 权威中心 (trusted center, TC)：一个可信的第三方，其可以初始化系统的主公钥和主私钥，为用户生成和分发属性私钥。在用户撤销时，TC 执行撤销算法更新密文，使被撤销用户失去密文的解密权限。

2) 数据拥有者 (data owner, DO)：将盲化处理后的明文发送给 TC，并接收 TC 加入撤销参数的返回结果，然后使用 TC 生成的公钥对明文加密后发送给数据存储服务器。

3) 数据访问者 (data visitor, DV)：从 TC 中获取自身属性集关联的私钥，在属性集满足解密所需的访问策略时，DV 能使用私钥解密密文获得正确的明文。

4) 数据存储服务器 (data storage server, DSS)：提供密文的存储服务。

5) 外包解密服务器 (outsourcing decryption server, ODS)：主要协助 DV 完成解密工作。方案中假定 ODS 是不可信的，其计算产生的结果为中间密文，DV 需在本地执行少量计算获得明文。

本方案的工作流程可描述为：1) TC 初始化系统，DO 从 TC 处获取公钥，依据访问结构和撤销参数，对明文进行加密处理，然后将密文发送给 DSS 存储；2) 在数据访问过程中，DV 首先从 DSS 上下载密文，并将转换密钥和密文一起发送给 ODS 进行预解密操作，并接收从 ODS 发回的预解密结果；3) DV 在预解密结果上执行本地解密过程，最后获取解密后的明文；4) 当需要进行用户撤销时，TC 执行撤销过程，对 DSS 中涉及用户撤销的密文进行更新，完成对用户透明的撤销过程。

## 3.2 算法定义

1) 初始化$\text{Setup}(1^{\lambda})\rightarrow(\text{PK},\text{MSK})$：权威中心初始化运行得到系统使用的公钥 PK 和主私钥 MSK，生成撤销参数表$T$与撤销参数$t$。

2) 密钥生成 KeyGen(PK, MSK, $L$)→(SK)：权威中心根据用户的属性列表 $L$，使用公钥 PK、主私钥 MSK 以及撤销参数表 $T$ 为用户构造相应的密钥 SK。

3) 加密 Encrypt(PK, $M$, $W$, ck, $t$)→(CT, $E(M)$)：使用随机选择的对称密钥 ck 加密明文 $M$ 并生成密文 $E(M)$，并对 ck 进行明文盲化得到 ck′。TC 对 ck′执行撤销算法得到 ck″。在对 ck′去盲生成 ck*后，使用访问策略 $W$ 生成密文 CT。

4) 预解密$\text{Pre}-\text{Decrypt}(\text{CT},\text{PK},\text{SK})\rightarrow(\text{CT}')$：DV 生成转换密钥 TK 后，连同密文 CT 一并发送给 ODS。若$L=W$，那么 ODS 将使用 TK 对密文进行预解密，输出 CT′。

5) 解密$\text{Decrypt}(\text{CT}',t,E(M))\rightarrow(M)$：当转换密文中的参数满足$T_0=C_0$时，DV 根据预解密结果 CT′与撤销参数 $t$ 计算 ck，进而解密 $E(M)$ 得到明文 $M$。

6) 属性撤销 Revocation：对于需要撤销权限的 $\text{User}_i$，TC 根据用户 ID 查找撤销系数表 $T$ 中对应的参数 $f_j$，计算新的撤销参数，对密文进行更新后，从 $T$ 中删除 $(\text{User}_i,f_j)$。

## 3.3 方案实现

本方案实现包括 6 个算法：初始化、密钥生成、加密、预解密、解密、属性撤销。

设$G$和$G_t$是阶为大素数$p$乘法循环群，$g$是$G$的生成元，映射$e:G\times G\rightarrow G_t$为一个双线性映射。假设系统的属性域一共有$n$个属性，其属性集记为$U=\{u_1,u_2,\cdots,u_n\}$，设第$i$个属性$u_i$具有$n_i$个取值，取值集合记为$V_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$。$H:\{0,1\}^{*}\rightarrow G_t$是一个抗碰撞的哈希函数。

1) 初始化$\text{Setup}(1^{\lambda})\rightarrow(\text{PK},\text{MSK})$

TC 运行 Setup 算法初始化系统，先选取$u,v,d\in G,x_{i,j},y_{i,j}\in_R Z_p^{*}(i\in[1,n],j\in[1,n_i])$，假定系统有 $m$ 个用户，针对每个用户 $\text{User}_l$，选择参数$f_l\in_R Z_p^{*}$，键值对$\{\text{User}_l,f_l\}(l\in m)$构成撤销参数表 $T$，生成撤销算法所需的撤销参数$t\in_R Z_p^{*}$，并将 $T$ 和 $t$ 存储在 TC。然后生成系统使用的公钥和主私钥，计算：

$$\text{X}_{i,j}=g^{-x_{i,j}},Y_{i,j}=e(g,g)^{y_{i,j}}\quad(1\leqslant i\leqslant n,1\leqslant j\leqslant n_i)$$

公钥即为：$\text{PK}=(g,u,v,d,\{X_{i,j},Y_{i,j}\}_{1\leqslant i\leqslant n,1\leqslant j\leqslant n_i})$

主私钥为：$\text{MSK}=(\{x_{i,j},y_{i,j}\}_{1\leqslant i\leqslant n,1\leqslant j\leqslant n_i})$

2) 密钥生成$\text{KeyGen}(\text{PK},\text{MSK},L)\rightarrow(\text{SK})$

具有属性列表$L=[L_1,L_2,\cdots,L_n]$的用户向权威中心申请私钥，设$L_i=v_{i,j}$，权威中心选择一个随机数$r\in_R Z_p^{*}$，计算：

$$K_i=g^{y_{i,j}}rx_{i,j}\qquad 1\leqslant i\leqslant n$$

$$K = g^r$$

然后依据初始化过程为用户生成的撤销参数，通过 $\text{User}_l$ 从表 $T$ 中获得$\{\text{User}_l, f_l\}(l \in m)$，并得到用户私钥：

$$\text{SK} = (L, f_l, K, \{K_i\}_{1 \leqslant i \leqslant n})$$

3) 加密$\text{Encrypt}(\text{PK}, M, W, \text{ck}, t) \to (\text{CT}, E(M))$

随机选择对称密钥 ck，并使用该密钥加密明文 $M$ 生成密文 $E(M)$。

设访问策略$W = \wedge_{I_W} W_i$, $W_i = v_{i,j}$，选择随机数$s \in_R Z_p^*$计算：

$$X_W = \prod_{i \in I_W} X_{i,j},\ Y_W = \prod_{i \in I_W} Y_{i,j}$$

先选择参数$z' \in_R Z_p^*$，对对称密钥 ck 进行第一次明文盲化：

$$\text{ck}' = \text{ck} \oplus H(z')$$

然后将盲化后的明文 ck′发送至 TC，TC 从初始化阶段生成的撤销参数表 $T$ 中取出所有用户的$f_l(l \in m)$和参数 $t$ 进行计算：

$$L = \prod_{l=1}^{m} f_l,\ L_l = \frac{L}{f_l}$$

$$N_l = L_l^{-1} \bmod f_l,\ [X]_l = t - f_l$$

$$[X] = \sum_{l=1}^{m} ([X]_l L_l N_l)$$

$$\text{ck}'' = \text{ck}' \oplus H(t)$$

TC 完成撤销算法处理后，将 ck″返回给 DO，DO 使用参数 $z'$完成去盲计算：

$$\text{ck}^* = \text{ck}'' \oplus H(z')$$

DO 使用 $\text{ck}^*$和与门访问策略 $W$ 作为后续加密算法的输入，加密对称密钥：

$$C_0 = \text{ck}^* Y_W^S,\ C_1 = g_s,\ C_2 = X_W^S$$

完成后的密文为：

$$\text{CT} = (W, C_0, C_1, C_2)$$

4) 预解密$\text{Pre} - \text{Decrypt}(\text{CT}, \text{PK}, \text{SK}) \to (\text{CT}')$

DV 向 DDS 获取密文 CT，并生成用于外包计算的转换密钥。选择$z \in_R Z_p^*$，计算：

$$K' = K^{\frac{1}{Z}},\ K_i' = K_i^{\frac{1}{Z}}\ (1 \leqslant i \leqslant n)$$

转换密钥为：

$$\text{TK} = (L, K', \{K_i'\}_{1 \leqslant i \leqslant n})$$

DV 将 (CT,TK) 发送至 ODS 进行解密运算，如果$L = W$则 ODS 进行如下计算：

$$T' = e\left(C_1, \prod_{i=I_l} K_i'\right) e(C_2, K') =$$

$$e(g^s, g^{\frac{1}{Z}\sum_{i \in I_L}(y_{i,j} + r x_{i,j})}) e(g^{-s\sum_{i \in I_W} x_{i,j}}, g^{\frac{r}{Z}}) = e(g,g)^{\frac{s\sum_{i \in I_L} y_{i,j}}{Z}}$$

即可输出预解密结果：

$$\text{CT}' = (T_0 = C_0, T')$$

ODS 将结果返回给解密用户。

5) 解密$\text{Decrypt}(\text{CT}', t, E(M)) \to (M)$

DV 检查转换密文中的参数是否满足$T_0 = C_0$，若等式不成立，中止解密。如成立则执行解密：

$$\text{ck}^* = \frac{C0}{(T')^Z} = \frac{\text{ck}^* e(g,g)^{s\sum_{i \in I_W} y_{i,j}}}{e(g,g)^{s\sum_{i \in I_L} y_{i,j}}} = \text{ck}^*$$

DV 使用 TC 返回的中国剩余定理的 $[X]$ 参数和自身私钥 SK 中的$f_l$ 计算明文：

$$[X]_l = [X] \bmod f_l,\ t = [X]_l + f_l$$

$$\text{ck} = \text{ck}^* \oplus H(t)$$

最后用对称密钥 ck 对 $E(M)$ 解密得到明文 $M$。

6) 属性撤销 Revocation

假定因故需要撤销 $\text{User}_i$ 的数据访问权限，TC 先根据用户 ID 在撤销参数表 $T$ 中查找用户对应的参数 $f_j$，生成新的撤销参数$t^* \in_R Z_p^*$后计算：

$$R = H(t) \oplus H(t^*)$$

$$L' = \prod_{l=1}^{m} f_l,\ L_l' = \frac{L'}{f_l}$$

$$N_l = L_l'^{-1} \bmod f_l,\ [X']_l = t^* - f_l \quad l \neq j$$

$$[X'] = \sum_{l=1}^{m} ([X']_l L_l' N_l')$$

相关新参数确定后，TC 计算：

$$\overline{C_0} = C_0 \oplus R$$

使用$\overline{C_0}$替换原密文中的对应部分，使用$[X']$替换 DSS 中存储的中国剩余定理参数，更新后的密文结果为：

$$\text{CT}' = (W, \overline{C_0}, C_1, C_2)$$

完成替换后，TC 将该 $\text{User}_i$ 的键值对$(\text{User}_j, f_j)$从撤销参数表 $T$ 中删除，此时系统中不再包含 $\text{User}_i$ 的任何信息，当 $\text{User}_i$ 进行解密时就无法解密$[X']$得到新的撤销参数 $t^*$，因此无法完成解密得到明文。

# 4 方案分析

## 4.1 安全性分析

在属性基加密方案的安全分析中，通常做法是将敌手对方案的攻击归约到具体困难问题的求解，由于这些困难问题利用现有知识无法在多项式时间内找到其对应的解，因此其对应算法是安全的。

本节将证明方案在 DBDH 假设下是选择明文攻击下的不可区分性 (indistinguishability under chosen-plaintext attack, IND-CPA) 安全的，IND-CPA 游戏模式如图 1 所示。不可区分选择明文安全模型中包含两个参与方，分别是敌手和挑战者。敌手通过对挑战者发起询问，可以得到任意明文所对应的密文信息。根据已知的明文与密文的对应关系，敌手将尝试对加密系统进行破解。在之后的挑战阶段，敌手会向挑战者发送两条等长的明文，挑战者将随机选择一条明文进行加密，并将加密后的密文发送给敌手，敌手根据该密文猜测其对应明文，如果敌手能够以不可忽略的优势猜出对应明文，则称敌手在该过程中取得胜利。

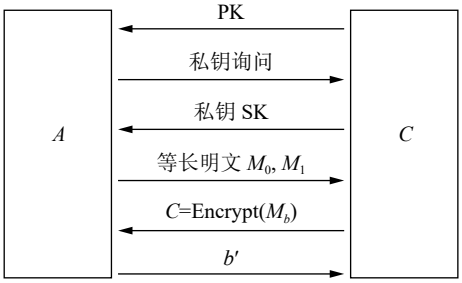


图 1 IND-CPA 游戏

**定理 1** 假定存在一个敌手 $A$ 以不可忽略的优势$\varepsilon$赢得 IND-CPA 游戏，那么就存在一个挑战者 $C$ 在解决 DBDH 问题时可以获得$\varepsilon/2$的优势。

证明：设挑战者 $C$ 选取阶为 $p$ 的乘法循环群 $G$ 和 $G_t$，$g$ 为群 $G$ 的生成元，$e$ 为双线性映射，H 为哈希函数，随机选择$a,b,c\in_R Z_p^*$。$C$ 执行掷币过程$\delta$，若$\delta=0$，则令$z=abc$，若$\delta=1$，则令$z\in_R Z_p^*$。$C$ 得到一个五元组：

$$(g,A,B,C,Z)=(g,g_a,g_b,g_c,e(g,g)^Z)$$

1) 启动 Initialization

敌手 $A$ 生成一个挑战策略：

$W^*=\wedge_{i\in I_{W^*}}W_i$，其中$I_{W^*}=\{i_1,i_2,\cdots,i_m\}(m<n)$

表示访问 $W^*$中不为通配符属性的下标集。$A$ 将 $W^*$发送给 $C$。

2) 初始化 Setup：$C$ 运行方案中 Setup 算法计算 PK 和 MSK。对于每个$i\in U, j\in U_i(U=\{U_1,U_2,\cdots,U_n\})$为所有属性的集合，选择一个随机数$\partial_{i,j}\in_R Z_p^*$与之对应，计算：

$$X_{i,j}=g^{-\partial_{i,j}}$$

$$Y_{i,j}=e(B,X_{i,j}^{-1})=e(g,g)^{b\partial_{i,j}}(1\leqslant i\leqslant n,1\leqslant j\leqslant n_i)$$

然后将生成的 PK 返回给 $A$。

3) 阶段 1：$A$ 选择一个属性集合$L=\{L_1,L_2,\cdots,L_n\},L\subseteq U,L_i=v_{i,j}$，且 $L$ 不满足 $W^*$，$A$ 将 $L$ 发送给挑战者 $C$ 查询私钥。$C$ 选择$\delta\in_R Z_p^*$，计算：

$$K_i=g^{(b+\delta)\partial_{i,j}},K=g^{\delta},\mathrm{ver}=1$$

$C$ 将 SK 返回给 $A$。

4) 挑战：$A$ 向 $C$ 提交两个等长的消息 $M_0$ 和 $M_1$，$C$ 选择$b\in_R\{0,1\}$，计算：

$$C_0=M_bY_{W^*}^C,C_1=g^c,C_2=X_{W^*}^C$$

设：

$$\sum_{i\in I_{W^*}}\partial_i=a+\eta$$

则有：

$$C_0=M_be(g,g)^{C\cdot\sum\limits_{i\in I_{W^*}}b\partial_i}=$$
$$M_be(g,g)^{cb(a+\eta)}=M_bZ(g,g)^{cb\eta}$$

完成计算后 $C$ 返回 CT 给 $A$。

5) 阶段 2：重复阶段 1 的操作。

6) 猜测 $G$：$A$ 输出猜测$b'\in\{0,1\}$，如果$b'=b$，$C$ 会猜测$\delta'=0$，即$Z=e(g,g)^{abc}$，这意味着$(g,A,B,C,Z)$是一个有效的 DBDH 组；否则$b'=b$，$C$ 对应猜测$\delta'=1,Z=e(g,g)^Z$，此时 $z$ 是随机数，表示$(g,A,B,C,Z)$是一个随机的五元组。故敌手优势计算如下：

当$\delta'=0,Z=e(g,g)^{abc}$时，$A$ 获得有效密文，优势为：

$$\Pr[b'=b|Z=e(g,g)^{abc}]=\frac{1}{2}+\varepsilon$$

当$\delta'=1,Z=e(g,g)^Z$时，优势为：

$$\Pr[b'=b|Z=R]=\frac{1}{2}$$

故挑战者 $C$ 赢得本游戏的优势为：

$$\mathrm{Adv}=\frac{1}{2}\Pr[b'=b|Z=$$
$$e(g,g)^{abc}]+\frac{1}{2}\Pr[b'=b|Z=R]-\frac{1}{2}=\frac{\varepsilon}{2}$$

至此，将本方案安全性问题规约为 DBDH 的复杂问题。

## 4.2 性能分析

本节对方案的性能进行分析，如表 2 所示。

**表 2　性能对比**

| 方案 | 密文长度 | 密钥长度 | 解密开销 |
|---|---|---|---|
| 文献[18] | $(n+1)\|G\|+\|G_t\|)$ | $(2n+1)\|G\|+\|Z_p\|$ | $(n+1)T_e$ |
| 文献[19] | $4\|G\|+2\|Z_p\|$ | $2\|G\|+2\|Z_p\|$ | $4T_{G_t}$ |
| 文献[20] | $(4n+3)\|G\|+2\|G_t\|$ | $(n+2)\|G\|$ | $2T_{G_t}$ |
| 文献[21] | $4\|G\|+\|G_t\|$ | $(n+1)\|G\|+\|Z_p\|$ | $\geqslant(n+1)T_e$ |
| 文献[22] | $2\|G\|+\|G_t\|$ | $2\|G\|$ | $2T_e$ |
| 文献[23] | $(2n+1)\|G\|+\|G_t\|$ | $(n+2)\|G\|$ | $2nT_e+nT_{G_t}$ |
| 文献[24] | $(n+1)\|G\|+\|G_t\|$ | $(n+2)\|G\|$ | $(n+2)T_e+nT_G$ |
| [25] | $(n+1)(\|G\|+\|G_t\|)$ | $(2n+2)\|G\|$ | $(2n+2)T_e+nT_G$ |
| 本文 | $2\|G\|+\|G_t\|$ | $(n+1)\|G\|+\|Z_p\|$ | $2T_{G_t}$ |

本文的性能分析主要选取的指标为：1) 密文长度，该指标主要反映 DSS 上存储加密文件的开销；2) 用户私钥的大小，该指标主要反映 DV 本地存储密钥的开销；3) 解密开销：该指标主要反映 DV 解密密文的计算开销[26]。在考虑解密开销时，仅考虑 DV 本地计算的开销，忽略方案中外包计算的开销。群 $G$ 和 $G_t$ 中单个成员的比特长度用$|G|$和$|G_t|$表示，$n$ 为属性域中的属性个数。在解密开销中，主要考虑双线性运算和指数运算这两类开销最大的计算次数。$T_{Gt}$ 为在群 $G_t$ 上完成指数运算的时间，$T_e$ 为完成双线性映射运算的时间。

文献 [18]、[19] 和 [22] 均实现了密文固长。文献 [18] 在实现了固长密文和密钥的同时降低了 DSS 和 DV 的存储开销，但其解密开销为本方案的两倍。本文方案的密文长度比文献 [16] 和文献 [19] 小，但略大于文献 [22]。文献 [22] 通过牺牲应用的灵活性，对存储开销和计算开销都进行了优化，但优化导致该方案在应用时要求所有满足或不满足访问结构的属性均对应才能解密，因此降低了实用性。

由于本方案实现了密文固长，且密文长度只有$2|G|+|G_t|$，与实现了撤销功能的文献 [18]、[19]、[25] 和实现了外包功能的文献 [20] 相比，本方案有更小的密文与密钥存储开销。

如表 3 所示，除了文献 [20] 和 [22] 以外，其他的文献都实现了撤销机制，而方案 [18] 实现了间接撤销。除了文献 [18] 和 [22]，其他在适应性安全模型下都是安全的。而本文所提方案是支持直接撤销的 CP-ABE，且方案安全性在适应性安全模型中被规约到 DBDH 假设上。

在解密开销方面，本方案实现了外包计算，将方案中复杂双线性计算的部分交由外包服务器完成，DV 在本地只需进行少量运算，开销仅为 $2T_{Gt}$，故 DV 的运算开销相比于文献 [18]、文献 [22]、文献 [24]、文献 [25] 和解密复杂度与撤销次数相关的文献 [21] 更小。

**表 3　各文献方案比较**

| 文献 | 撤销方式 | 安全模型 | 安全假设 |
|---|---|---|---|
| 文献[18] | 间接撤销 | 选择安全 | DBDH假设 |
| 文献[19] | 直接撤销 | 适应性安全 | aMSE-DDH假设 |
| 文献[20] | 无 | 适应性安全 | DL假设 |
| 文献[21] | 直接撤销 | 适应性安全 | m-BDHE假设 |
| 文献[22] | 无 | 适应性安全 | DBDH假设 |
| 文献[23] | 直接撤销 | 选择安全 | n-eDDH假设 |
| 文献[24] | 直接撤销 | 适应性安全 | d+4-MDDH假设 |
| 文献[25] | 直接撤销 | 适应性安全 | ($d$+3)-MDDH假设 |
| 本文 | 直接撤销 | 适应性安全 | DBDH假设 |

此外，在具有 Intel Core i5-8 400 CPU @ 2.8GHz 和 16 GB 内存的 Windows 10 PC 的实验环境下，使用 JPBC 库对性能分析中所涉及的方案通过实验模拟进一步进行分析和比较[27]。实验主要模拟了各方案的解密过程。由图 2 所示，随着属性域中属性个数的增加，文献 [18]、[21]、[22]、[24] 以及 [25] 的解密时间增加。本文所提方案、文献 [19]、[20] 以及 [22] 所提方案的解密所需时间基本保持不变，而又在这几个方案之中，本文所提出的方案具有最短的解密时间，因此具有较高的效率。

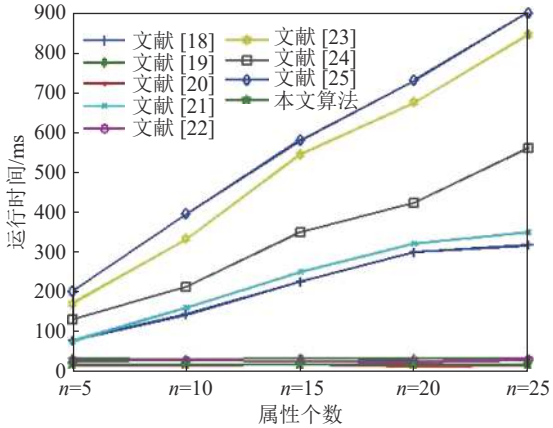


图 2　解密时间比较

## 5 结束语

本文提出了一种高效直接撤销且具有外包解密功能的属性基加密方案。该方案以中国剩余定理为基础实现了用户撤销功能，只需更新密文即可撤销用户权限，达到了可撤销存储的目的，确保了系统的前向安全性，不影响未撤销用户的私钥，满足高效、便捷的动态权限变更需求。同时，方案采用了相对更加灵活的多值通配与门构造基础方案，降低了访问策略的构造复杂度。本方案实现了密文固长，显著降低了存储开销。此外，为减少用户本地的解密开销，本方案将复杂运算安全地外包至第三方服务器，进一步降低了解密过程开销。在安全性上，本方案采用 IND-CPA 安全模型，将安全性规约至 DBDH 问题，完成了安全性证明。与同类方案的对比分析结果表明，本方案在灵活性和性能上有一定的优势，有良好的实用价值。

## 参 考 文 献


[1] XIONG H, WU Y, JIN J C, et al. Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIoT[J]. IEEE Internet of Things Journal, 2020, DOI: 10.1109/JIOT.2020.2999510.

[2] MEI Q, XIONG H, CHEN J H, et al. Efficient certificateless aggregate signature with conditional privacy-preserving in IoV[J]. IEEE Systems Journal, 2020, DOI: 10.1109/JSYST.2020.2966526.

[3] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Proceeding of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005). Berlin: Springer-Verlag, 2005: 457-473.

[4] XIONG H, BAO Y Y, NIE X Y, et al. Server-aided attribute-based signature supporting expressive access structures for industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2020, 16(2): 1013-1023.

[5] XIONG H, KANG Z Q, CHEN J H, et al. A novel multiserver authentication scheme using proxy resignature with scalability and strong user anonymity[J]. IEEE Systems Journal, 2020, DOI: 10.1109/JSYST.2020.2983198.

[6] GOYAL V, PANDEY O, AMIT S, et al. Attribute-based encryption for fine-grained access control of encryption data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006). New York: ACM, 2006: 89-98.

[7] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of 2007 IEEE Symp. on Security and Privacy. New York: IEEE, 2007: 321-334.

[8] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. New York: ACM, 2007: 195-203.

[9] CHASE M. Multi-authority attribute based encryption[C]//Proc of the 4th Theory of Cryptography Conference (TCC 2007). Berlin: Springer-Verlag, 2007: 515-534.

[10] GOYAL V, JAIN A, PANDEY O, et al. Bounded ciphertext policy attribute based encryption[C]//Proceedings of the 35th International Colloquium (ICALP 2008). Berlin: Springer-Verlag, 2008.579-591.

[11] WEI J H, LIU W F, HU X X. Forward-secure ciphertext-policy attribute-based encryption scheme[J]. Journal of Communications, 2014, 35(7): 38-45.

[12] 谢鑫. 高效可撤销存储的属性基加密方案研究[D]. 成都: 电子科技大学, 2020.
XIE Xin. A research of efficient revocable storage attribute-based encryption scheme[D]. Chengdu: University of Electronic Science and Technology of China, 2020.

[13] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[C]//Proceedings of the 15th ACM conference on Computer and Communications Security. [S. l. ]: ACM, 2008: 417-426.

[14] ATTRAPADUNG N, IMAI H. Attribute-based encryption supporting direct/indirect revocation modes[C]//IMA International Conference on Cryptography and Coding. Berlin, Heidelberg: Springer, 2009: 278-300.

[15] NAOR M, PINKAS B. Efficient trace and revoke schemes[C]//International Conference on Financial Cryptography. Berlin, Heidelberg: Springer, 2000: 1-20.

[16] BONEH D, GENTRY C, WATERS B. Collusion resistant broadcast encryption with short ciphertexts and private keys[C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 2005: 258-275.

[17] LEWKO A, SAHAI A, WATERS B. Revocation systems with very small private keys[C]//2010 IEEE Symposium on Security and Privacy. [S. l. ]: IEEE, 2010: 273-285.

[18] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. [S. l. ]: ACM, 2010: 261-270.

[19] ZHAO Y, REN M, JIANG S, et al. An efficient and revocable storage CP-ABE scheme in the cloud computing[J]. Computing, 2019, 101(8): 1041-1065.

[20] LAI J, DENG R H, GUAN C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343-1354.

[21] ZHANG Y H, ZHENG D, LI J, et al. Attribute directly-revocable attribute-based encryption with constant ciphertext length[J]. Journal of Cryptologic Research, 2014, 1(5): 465-480.

[22] EMURA K, MIYAJI A, NOMURA A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]//International Conference on

Information Security Practice and Experience. Berlin, Heidelberg: Springer, 2009: 13-23.

[23] SAHAI A, SEYALIOGLU H, WATERS B. Dynamic credentials and ciphertext delegation for attribute-based encryption[C]//Annual Cryptology Conference. Berlin, Heidelberg: Springer, 2012: 199-217.

[24] YU G, MA X, CAO Z, et al. Server-aided directly revocable ciphertext-policy attribute-based encryption with verifiable delegation[C]//International Conference on Information and Communications Security. Cham: Springer, 2017: 172-179.

[25] 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.

[26] XIONG H, ZHAO Y N, HOU Y Z, et al. Heterogeneous signcryption with equality test for IIoT environment[J]. IEEE Internet of Things Journal, 2020, DOI: 10.1109/JIOT.2020.3008955.

[27] XIONG H, MEI Q, ZHAO Y N, et al. Scalable and forward secure network attestation with privacy-preserving in cloud-assisted internet of things[J]. IEEE Sensors Journal, 2019, 19(18): 8317-8331.

编　辑　叶　芳