doi:10.11959/j.issn.1000-436x.2017068

# 支持高效撤销的多机构属性加密方案

张凯[1]，马建峰[2]，李辉[2]，张俊伟[2]，张涛[3]
（1. 西安电子科技大学通信工程学院，陕西 西安 710071；
2. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；3. 西安电子科技大学计算机学院，陕西 西安 710071）

**摘 要**：多机构属性加密方案非常适用于云存储环境下的数据访问控制。然而，高效的用户撤销仍是其中一个具有挑战的问题，这妨碍了多机构属性加密的实际应用。针对此问题，在素数阶群中提出一种支持高效撤销的多机构密文策略属性加密方案，并在随机预言模型下证明了方案是静态性安全和支持撤销的。分析结果表明所提方案极大地降低了用户的计算开销。此外，所提方案支持大属性域和所有单调访问结构，因此，在实际应用中更加灵活。
**关键词**：属性加密；多机构；撤销；大属性域
**中图分类号**：TP309 **文献标识码**：A

# Multi-authority attribute-based encryption with efficient revocation

ZHANG Kai[1], MA Jian-feng[2], LI Hui[2], ZHANG Jun-wei[2], ZHANG Tao[3]
(1. School of Telecommunications Engineering, Xidian University, Xi'an 710071, China;
2. School of Cyber Engineering, Xidian University, Xi'an 710071, China;
3. School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

**Abstract:** Multi-authority attribute-based encryption was very suitable for data access control in a cloud storage environment. However, efficient user revocation in multi-authority attribute-based encryption remains a challenging problem that prevents it from practical applications. A multi-authority ciphertext-policy attribute-based encryption scheme with efficient revocation was proposed in prime order bilinear groups, and was further proved statically secure and revocable in the random oracle model. Extensive efficiency analysis results indicate that the proposed scheme significantly reduce the computation cost for the users. In addition, the proposed scheme supports large universe and any monotone access structures, which makes it more flexible for practical applications.
**Key words:** attribute-based encryption, multi-authority, revocation, large universe

## 1 引言

作为一种特殊的公钥加密方案，属性加密方案(ABE，attribute-based encryption)[1,2]不仅能够保护数据的安全性，还能够实现细粒度的访问控制。在ABE中，数据拥有者能够加密数据给满足指定访问策略的多个用户，这种特性使其可广泛应用于云存储服务中。例如，在医疗系统中有大量的敏感信息存储在云服务器上，而患者需要相关医生查看自己的医疗信息以给出诊断结果，但又不希望其他人获取自己的隐私信息；这时，患有骨病的患者能够利用ABE加密自己的医疗信息并上传到云服务器上，同时，在加密过程中指定只有A医院骨科的所有主任医师和副主任医师能够访问自己的数据，其他用户便不能访问患者的医疗数据。

ABE可分为密钥策略ABE (KP-ABE，key-policy ABE)[2]和密文策略ABE (CP-ABE，ciphertext-policy ABE)[3]2种类型。在CP-ABE中，用户的私钥与自己的属性对应，密文与数据拥有者指定的访问策略对应，只有那些属性满足访问策略的用户能够成功

**收稿日期**：2016-10-19；**修回日期**：2017-01-23
**基金项目**：国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA016007）；国家自然科学基金资助项目（No.U1405255, No.61472310, No.61602365）
**Foundation Items:** The National High Technology Research and Development Program (863 Program) (No.2015AA016007), The National Natural Science Foundation of China (No.U1405255, No.61472310, No.61602365)

解密。在 KP-ABE 中，这种关系恰好相反，即私钥对应策略，密文对应属性。在早期的 ABE 系统[1~3]中，由一个中心权威机构负责管理所有属性和用户私钥。然而，在许多实际应用场景中，系统的所有属性并不能由一个机构来管理。比如，在一个密文数据库系统中，患者想要加密数据给同时具有“博士”和“医生”属性的用户，其中，“博士”属性由学校管理，而“医生”属性由医院管理，因此，只有一个权威机构的 ABE 显然不适用于这种场景。针对此问题，Chase[4]提出了多机构 ABE（MA-ABE，multi-authority ABE）系统，其中，不同的属性集由不同的权威机构进行管理。

与传统公钥加密一样，MA-ABE 系统中也会有用户的加入与退出。因此，如何实现对系统中用户有效撤销的同时，又不影响其他用户的解密能力是 MA-ABE 中的一个重要问题。针对此问题，已有一些可撤销的 MA-ABE 方案[5~7]被相继提出。然而，现有方案[5~7]中用户解密过程需要的双线性对和指数运算是和访问策略的复杂性线性相关的，从而导致用户的解密效率过低，影响系统的用户体验。

针对上述问题，本文提出了一个支持高效撤销的多机构 CP-ABE 方案，并证明了方案是静态性安全（statically secure）和可撤销的。本文方案利用云服务器来协助撤销，用户为自己产生私钥，权威机构为云服务器产生私钥。只有当云服务器利用自己的私钥对原始密文进行部分解密后，用户才能够解密密文。当要撤销用户时，云服务器只要将该用户对应的云服务器私钥删除即可。方案的特点总结如下。

1) 多机构：系统中每个属性权威机构（AA）管理自己领域内的属性集和私钥，不需要中心权威机构（CA），更符合实际应用场景。

2) 可撤销：不管被撤销的用户属性是否满足访问策略，都不能解密任何密文。

3) 高效：用户的解密开销仅是素数阶群（prime order group）中的一个指数运算，与属性个数和访问策略的复杂性无关。

4) 大属性域（large universe）：系统中的属性非常灵活，任何一个字符串都能够作为新属性加入系统，公钥长度也与系统的属性个数无关。

5) 丰富的访问策略：系统支持任意单调访问结构，从而能够实现细粒度的访问控制。

## 2 相关工作

自从 ABE [1]的概念被提出后，许多 CP-ABE 方案[3,8,9]被提出以实现细粒度访问控制。Bethencourt 等[3]构造了第一个支持任意单调访问结构的 CP-ABE 方案。随后，Waters[8]在标准模型下构造了一个高效的 CP-ABE 方案。文献[9]提出了支持大属性域的 CP-ABE 方案。在文献[9]中，属性域并不需要在系统建立时确定，公钥的长度也不随属性个数的增加而增加。为了更加符合实际需求，Chase[4]构造了第一个 MA-ABE 方案。Rouselakis 和 Waters[10]提出了一个支持大属性域的 MA-ABE 方案，但方案并不支持用户撤销。文献[11]提出了支持外包解密的 MA-ABE 方案，能够减少用户的解密开销。然而，文献[11]的方案，用户解密开销所需的指数运算个数仍然和访问策略复杂性有关，而本文方案中的用户解密开销只需一个指数运算。此外，本文方案中用户私钥由用户自己产生，不存在密钥托管问题。

由于 ABE 系统中存在用户的加入和退出，所以支持撤销的 ABE 受到广泛关注。文献[12~16]中的方案虽然支持 ABE 撤销，但并不支持多机构应用场景。Yang 等[5]提出了一个支持撤销的 MA-ABE 方案，该方案能够支持任意单调访问结构，但是并不支持大属性域。Huang 等[6]提出了支持大属性域的可撤销 MA-ABE 方案，但方案中除了多个 AA 外，还需要一个 CA，CA 的主密钥长度是和 AA 个数线性相关的。最近，Cui 等[7]在合数阶群（composite prime order group）下构造了一个支持撤销的 MA-ABE 方案。然而，上述方案[5~7]中用户的解密开销都是和访问策略复杂性线性相关的。与文献[5~7]相比，本文提出的方案中用户的解密开销只需一个指数运算，而且在支持大属性域的同时不需要 CA。

## 3 预备知识

### 3.1 访问结构

**定义 1** 访问结构(access structure)[17]。假设 $\{P_1,P_2,\cdots,P_n\}$ 是由 $n$ 个属性组成的集合。一个访问结构 $\mathbb{A}$ 是指由 $\{P_1,P_2,\cdots,P_n\}$ 的非空子集组成的集合，即 $\mathbb{A}\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\setminus\{\varnothing\}$。若集合 $D\in\mathbb{A}$，则称 $D$ 为授权集合；否则，称 $D$ 为非授权集合。访问结构 $\mathbb{A}$

称为是单调的，当且仅当对任意集合 $B$ 和 $C$，若 $B\in\mathbb{A}$，$B\subseteq C$，则 $C\in\mathbb{A}$。

### 3.2 线性秘密共享

**定义 2** 线性秘密共享(LSSS, linear secret sharing scheme)[17]。设 $p$ 是一个素数，当满足如下条件时，称属性集合 $P$ 上的秘密共享方案 $\Pi$ 在 $\boldsymbol{Z}_p$ 上是线性的。

1) 每个属性关于秘密 $s\in\boldsymbol{Z}_p$ 的分享值构成 $\boldsymbol{Z}_p$ 上的一个向量。

2) 对于每一个 $P$ 上的访问结构 $\mathbb{A}$，存在一个矩阵 $\boldsymbol{A}\in Z_p^{l\times n}$ 和函数 $\rho:[l]\to P$。$\rho$ 将矩阵 $\boldsymbol{A}$ 的行号 $i\in[l]$ 映射到属性 $\rho(i)$。令 $\vec{\boldsymbol{v}}=(s,y_2,\cdots,y_n)^{\mathrm{T}}$，$y_2,\cdots,y_n\in\boldsymbol{Z}_p$ 是随机元素。则 $s$ 关于 $\Pi$ 的 $l$ 个分享份额构成的向量 $\boldsymbol{\lambda}=\boldsymbol{A}\vec{\boldsymbol{v}}\in Z_p^{l\times 1}$。秘密分享份额 $\lambda_i=(\boldsymbol{A}\vec{\boldsymbol{v}})_i$ 分配给属性 $\rho(i)$。

上述秘密共享方案 $\Pi$ 满足线性重构性质：假定 $S$ 是 $\mathbb{A}$ 中的一个授权集合，$I=\{i:\rho(i)\in S\}\subseteq\{1,2,\cdots,l\}$，则存在多项式时间算法计算出满足等式 $\sum_{i\in I}c_i\lambda_i=(s,0,\cdots,0)$ 的常数 $\{c_i\in\boldsymbol{Z}_p\}$。这里称 $(\boldsymbol{A},\rho)$ 为 $\mathbb{A}$ 的访问策略。

### 3.3 双线性群和困难问题假设

设 $p$ 为素数，$G$ 和 $G_T$ 是 2 个 $p$ 阶循环乘法群，$g$ 是 $G$ 的生成元。当满足下列条件时，映射 $e:G\times G\to G_T$ 称为双线性对。

1) 双线性：$\forall u,v\in G,e(u^a,v^b)=e(u,v)^{ab}$。

2) 非退化性：$e(g,g)\neq 1$。

当双线性对 $e:G\times G\to G_T$ 和群运算是能够有效计算的，群 $G$ 称为是素数阶双线性群（prime order bilinear group）。

**定义 3** $q$-DBPBDHE2 假设[10]。群 $G$ 中的 $q$-DBPBDHE2 问题叙述如下：随机选取 $a,s,b_1,b_2,\cdots,b_q\in Z_p^*$，已知

$$D=(p,g,G,e,g^s,\{g^{a^i}\}_{i\in[2q],i\neq q+1},\{g^{b_ja^i}\}_{(i,j)\in[2q,q],i\neq q+1},$$

$$\{g^{\frac{s}{b_i}}\}_{i\in[q]},\{g^{\frac{sa^ib_j}{b_{j'}}}\}_{(i,j,j')\in[q+1,q,q],j\neq j'})$$

区分 $e(g,g)^{sa^{q+1}}$ 和 $G_T$ 中的随机元素 $R$。

当 $\left|\Pr\left[\mathcal{A}\left(D,e(g,g)^{sa^{q+1}}\right)=0\right]-\Pr\left[\mathcal{A}(D,R)=0\right]\right|\geqslant\varepsilon$，则称算法 $\mathcal{A}$ 解决 $q$-DBPBDHE2 问题的优势是 $\varepsilon$。

若任何多项式时间算法解决 $q$-DBPBDHE2 问题的优势都是可忽略的，则称 $q$-DBPBDHE2 假设在群 $G$ 中成立。

## 4 可撤销的多机构 CP-ABE 的定义和安全模型

本文的多机构 CP-ABE 系统中包含的主体有：属性权威机构（attribute authority）、数据拥有者（data owner）、云服务器（cloud sever）、用户（user）。像大多数的云服务器协助撤销 ABE 方案[14,15]一样，这里的云服务器是半可信的，即云服务器按正确步骤执行算法，不能与已被撤销的用户进行合谋。在解密过程中，云服务器帮助合法的用户对密文进行部分解密，用户进行最终解密得到明文。在撤销某个用户时，云服务器将该用户对应的云服务器密钥删除。

### 4.1 定义

在本文的方案中，一个权威机构能够管理多个属性，但一个属性只能由某个特定的权威机构来管理。$U$ 代表属性空间，$U_\theta$ 代表权威机构空间，一个公开的函数 $T:U\to U_\theta$ 将属性 $i\in U$ 映射到管理 $i$ 的权威机构 $\theta\in U_\theta$。一个可撤销的多机构 CP-ABE（R-MA-CP-ABE, revocable multi-authority CP-ABE）方案包括以下算法。

$GlobalSetup(\lambda)\to GP$：输入安全参数 $\lambda$，输出系统的公开参数 $GP$。

$AuthoritySetup(GP,\theta)\to\{PK_\theta,SK_\theta\}$：每个权威机构 $\theta$ 利用公开参数 $GP$ 为自己产生公/私钥对 $\{PK_\theta,SK_\theta\}$。

$UserKeyGen(GP,id)\to\{UPK_{id},USK_{id}\}$：每个用户 $id$ 为自己产生公/私钥对 $\{UPK_{id},USK_{id}\}$。

$CSKeyGen(GP,\{SK_\theta\},id,UPK_{id},S)\to CSK_{id,S}$：输入 $GP$、$\{SK_\theta\}$、$UPK_{id}$、用户的身份 $id$ 和用户属性 $S$，输出针对用户 $id$ 的云服务器私钥 $CSK_{id,S}$，该算法由权威机构执行，并将私钥 $CSK_{id,S}$ 秘密发送给云服务器，最后将数组 $\{id,CSK_{id,S}\}$ 加入到云服务器密钥列表 $KT$ 中。

$Encrypt(GP,\{PK_\theta\},M,(\boldsymbol{A},\rho))\to CT$：输入 $GP$、$\{PK_\theta\}$、消息 $M$ 和访问策略 $(\boldsymbol{A},\rho)$，输出密文 $CT$，该算法由数据拥有者执行，并将密文 $CT$ 上传到云服务器。

$CSDecrypt(GP,CSK_{id,S},UPK_{id},CT)\to CT_{id}$：输入 $GP$，对应于属性集 $S$ 的云服务器私钥 $CSK_{id,S}$，

公钥 $UPK_{id}$ 和对应于访问策略 $(\boldsymbol{A},\rho)$ 的密文 $CT$ 。如果属性集 $S$ 满足访问策略 $(\boldsymbol{A},\rho)$，则输出部分解密密文 $CT_{id}$ 。否则输出 $\perp$ 表示解密失败。该算法由云服务器执行，并将 $CT_{id}$ 发送给用户 $id$ 。

$UserDecrypt\left(USK_{id},CT_{id}\right)\rightarrow M$ : 输入 $USK_{id}$ 和 $CT_{id}$，输出消息 $M$ 。

$Revoke\left(id,KT\right)\rightarrow KT\setminus\left\{id,CSK_{id,S}\right\}$ : 输入被撤销用户的身份 $id$ 和 $KT$，输出更新后的密钥列表 $KT=KT\setminus\left\{id,CSK_{id,S}\right\}$ 。

### 4.2 静态性安全模型

本节给出的 R-MA-CP-ABE 静态性安全模型主要是针对多个合法用户的合谋攻击，因此要求敌手不仅能够进行多次用户私钥询问，而且还能够对系统中其他合法用户的部分解密密文进行询问。模型允许敌手进行云服务器私钥询问，这样敌手显然可以利用云服务器私钥解密密文得到合法用户的部分解密密文。此外，假定敌手能够腐化一部分权威机构，从而自己生成这些权威机构的公钥。需要指出的是，在静态性安全模型[10]中，敌手的所有询问都需要在挑战之前完成。敌手和挑战者之间的游戏描述如下所示。

系统建立。挑战者执行 $GlobalSetup(\lambda)\rightarrow GP$，并将公开参数 $GP$ 发送给敌手。

询问阶段。敌手首先选择一部分腐化的权威机构 $C_\theta\subseteq U_\theta$，并自己生成这些权威的公钥。然后向挑战者做如下询问。

1) 选择未被腐化的权威机构 $N_\theta\subseteq U_\theta$，并询问这些权威的公钥。

2) 选取一部分合法用户 $\{id_i\}_{i=1}^m$，并询问对应的用户公/私钥对。

3) 选取 $\{S_i,id_i\}_{i=1}^n$，并询问对应的云服务器私钥。其中，$S_i\subseteq U$ 为用户 $id_i$ 拥有的属性集，$id_i(1\leqslant i\leqslant n)$ 互不相同，且 $T(S_j)\bigcap C_\theta=\varnothing$，即这里询问的任何属性都不能由腐化的权威机构 $C_\theta$ 来管理。注意 $n$ 的取值可以比 $m$ 大，即敌手不仅能够询问对应用户 $\{id_i\}_{i=1}^m$ 的云服务器私钥，也能够询问其他用户的云服务器私钥。

4) 选择 2 个长度相等的消息 $M_0$、$M_1$ 和一个访问策略 $(\boldsymbol{A},\rho)$，并询问挑战密文。这里，要求对每个询问过私钥的用户 $id_i(1\leqslant i\leqslant m)$，属性集 $S_{C_\theta}\bigcup S_i$ 不能满足访问策略 $(\boldsymbol{A},\rho)$。这里 $S_{C_\theta}$ 表示由所有腐化的权威机构 $C_\theta$ 管理的属性。

挑战者应答。挑战者随机选择 $b\in\{0,1\}$，并返回应答。

1) 权威机构 $N_\theta\subseteq U_\theta$ 的公钥 $\{PK_\theta\}_{\theta\in N_\theta}$ 。

2) 用户 $\{id_i\}_{i=1}^m$ 的公/私钥对 $\{UPK_{id_i},USK_{id_i}\}_{i=1}^m$。

3) $\{S_i,id_i\}_{i=1}^n$ 对应的云服务器私钥 $\{CSK_{S_i,id_i}\}_{i=1}^n$。

4) 挑战密文 $CT^*\leftarrow Encrypt(GP,\{PK_\theta\},M_b,(\boldsymbol{A},\rho))$。

猜测。敌手输出猜测结果 $b'\in\{0,1\}$。

敌手赢得该游戏的优势定义为 $\left|\Pr\left[b=b'\right]-\frac{1}{2}\right|$。

**定义 4** 如果没有多项式时间敌手能够以不可忽略的优势赢得该游戏，则称 R-MA-CP-ABE 方案是静态性安全的。

需要指出的是，在上述游戏中，如果只允许云服务器私钥询问，则转变为只针对云服务器的攻击。而本节的模型允许 2 种私钥询问，所以是包含了多个合法用户合谋攻击和云服务器攻击 2 种情形的。

### 4.3 可撤销性安全模型

本节的可撤销性安全模型主要是针对多个撤销用户（不管其属性是否满足访问策略）的合谋攻击，所以敌手能够询问多个撤销用户的私钥。注意本文假定撤销用户不能与云服务器和权威机构合谋，所以敌手不能询问与撤销用户对应的云服务器私钥，也不能生成权威机构的公钥。同时，为了保证敌手能够获得未被撤销用户的部分解密密文，模型允许敌手访问与未被撤销用户对应的云服务器私钥。敌手和挑战者之间的游戏描述如下。

系统建立。与 4.2 节相同。

询问阶段。敌手向挑战者作如下询问。

1) 选择权威机构 $N_\theta\subseteq U_\theta$，并询问这些权威的公钥。

2) 选取一部分撤销用户 $\{id_i\}_{i=1}^m$，并询问对应的用户公/私钥对。

3) 选取一部分合法用户 $\{id_i\}_{i=m}^n$，并询问对应于 $\{S_i,id_i\}_{i=m}^n$ 的云服务器私钥。其中，$id_i(1\leqslant i\leqslant n)$ 互不相同。

4) 选择 2 个长度相等的消息 $M_0$、$M_1$ 和一个访问策略 $(\boldsymbol{A},\rho)$，并询问挑战密文。

挑战者应答。与 4.2 节相同。

猜测。与 4.2 节相同。

敌手赢得该游戏的优势定义为 $\left|\Pr[b=b']-\frac{1}{2}\right|$。

**定义 5**　如果没有多项式时间敌手能够以不可忽略的优势赢得该游戏，则称 R-MA-CP-ABE 方案是支持用户撤销的。

## 5　可撤销的多机构 CP-ABE 方案

本节将构造一个支持用户撤销的多机构 CP-ABE 方案，并在随机预言模型（random oracle model）下证明该方案是静态性安全和可撤销的。最后，给出了本文方案和相关方案的性能对比。

### 5.1　方案构造

本文中的访问策略是 $(\boldsymbol{A},\rho)$，其中，$\boldsymbol{A}$ 是一个 $l\times n$ 矩阵，$\rho:[l]\to \boldsymbol{Z}_p$ 将矩阵的行号 $x$ 映射到属性 $\rho(x)$。由于 $T:U\to U_\theta$ 将属性 $i\in U$ 映射到管理 $i$ 的权威机构 $\theta\in U_\theta$，所以函数 $\delta(\cdot)=T(\rho(\cdot))$ 将矩阵的行映射到一个权威机构。具体的 R-MA-CP-ABE 方案构造如下。

*GlobalSetup*$(\lambda)$：选择一个阶为素数 $p$ 的双线性群 $G$。$g$ 是 $G$ 的生成元，$e:G\times G\to G_T$ 是 $G$ 上的双线性对。然后选择 2 个散列函数 $H:Z_p^*\to G$，$F:U\to G$，输出公开参数 $GP=\{p,G,g,H,F,U,U_\theta,T\}$。

*AuthoritySetup*$(GP)$：每个权威机构 $\theta\in U_\theta$ 选取 2 个随机元 $\alpha_\theta,y_\theta\in Z_p^*$，公开自己的公钥 $PK_\theta=\{e(g,g)^{\alpha_\theta},g^{y_\theta}\}$，秘密保存私钥 $SK_\theta=\{\alpha_\theta,y_\theta\}$。

*UserKeyGen*$(GP,id)$：用户 $id$ 随机选择 $x_{id}\in Z_p^*$，计算自己的公钥 $UPK_{id}=\{g^{x_{id}},H(id)^{x_{id}}\}$，并将 $USK_{id}=\left(\frac{1}{x_{id}}\right)$ 作为用户私钥秘密保存。

*CSKeyGen*$\left(GP,\{SK_\theta\},id,UPK_{id},S\right)$：输入 $GP$、权威机构私钥 $\{SK_\theta\}$、用户的身份 $id$、公钥 $UPK_{id}$ 和用户属性 $S$。对所有 $i\in S$，如果 $T(i)=\theta$，则权威机构 $\theta$ 选择随机元素 $t_i\in \boldsymbol{Z}_p$，并计算 $K_{i,id}=g^{x_{id}\alpha_\theta}\cdot H(id)^{x_{id}y_\theta}F(i)^{t_i}$，$K_{i,id}{}'=g^{t_i}$。最后输出针对用户 $id$ 的云服务器私钥 $CSK_{id,S}=\left\{K_{i,id},K_{i,id}{}'\right\}_{i\in S}$，云服务器将数组 $\left\{id,CSK_{id,S}\right\}$ 加入到云服务器密钥列表 $KT$ 中。

*Encrypt*$(GP,\{PK_\theta\},M,(\boldsymbol{A},\rho))$：输入 $GP$、公钥 $\{PK_\theta\}$、消息 $M$ 和访问策略 $(\boldsymbol{A},\rho)$。首先随机选择 $s,y_2,\cdots,y_n,z_2,\cdots,z_n\in \boldsymbol{Z}_p$，令向量 $\vec{\boldsymbol{v}}=(s,y_2,\cdots,y_n)^{\mathrm{T}}$，$\vec{\boldsymbol{\omega}}=(0,z_2,\cdots,z_n)^{\mathrm{T}}$。对所有的 $x\in[l]$，计算 $\lambda_x=(\boldsymbol{A}\vec{\boldsymbol{v}})_x$，$\omega_x=(\boldsymbol{A}\vec{\boldsymbol{\omega}})_x$。随机选择 $r_x\in \boldsymbol{Z}_p$，计算密文

$$
\begin{aligned}
C_0&=Me(g,g)^s,\\
C_{1,x}&=e(g,g)^{\lambda_x}e(g,g)^{\alpha_{\delta(x)}r_x},\\
C_{2,x}&=g^{-r_x},\\
C_{3,x}&=g^{y_{\delta(x)}r_x}g^{\omega_x},\\
C_{4,x}&=F(\rho(x))^{r_x}
\end{aligned}
$$

输出密文 $CT=(C_0,\{C_{1,x},C_{2,x},C_{3,x},C_{4,x}\}_{x\in[l]})$。

*CSDecrypt*$\left(CSK_{id,S},GP,UPK_{id},CT\right)$：输入 $GP$，用户 $id$ 的公钥 $UPK_{id}$，密文 $CT=(C_0,\{C_{1,x},C_{2,x},C_{3,x},C_{4,x}\}_{x\in[l]})$ 和云服务器私钥 $CSK_{id,S}=\{K_{i,id},K_{i,id}{}'\}_{i\in S}$。如果 $S$ 不满足访问策略 $(\boldsymbol{A},\rho)$，输出 $\perp$。否则，令 $I=\{x:\rho(x)\in S\}\subseteq\{1,2,\cdots,l\}$，并计算 $\{c_x\in \boldsymbol{Z}_p\}$ 满足 $\sum_{x\in I}c_xA_x=(1,0,\cdots,0)$。计算 $C_{1,id}=\prod_{x\in I}(C_{1,x})^{c_x}$，$C_{2,id}=\prod_{x\in I}\{e(K_{\rho(x),id},C_{2,x})e(H(id)^{x_{id}},C_{3,x})e(K_{\rho(x),id}{}',C_{4,x})\}^{c_x}$。最后云服务器将部分解密的密文 $CT_{id}=\left(C_0,C_{1,id},C_{2,id}\right)$ 发送给用户 $id$。

*UserDecrypt*$\left(USK_{id},CT_{id}\right)$：输入 $CT_{id}=(C_0,C_{1,id},C_{2,id})$ 和私钥 $USK_{id}=\{x_{id}\}$。计算 $C_{1,id}C_{2,id}^{\left(\frac{1}{x_{id}}\right)}=e(g,g)^s$，最后恢复 $M=\dfrac{C_0}{e(g,g)^s}$。

*Revoke*$\left(id,KT\right)$：输入用户身份 $id$ 和密钥列表 $KT$。查找并删除列表 $KT$ 中的数组 $\left\{id,CSK_{id,S}\right\}$，即更新 $KT=KT\setminus\left\{id,CSK_{id,S}\right\}$。

正确性。若属性集 $S$ 满足策略 $(\boldsymbol{A},\rho)$，令 $I=\{x:\rho(x)\in S\}$，则常数 $\{c_x\in \boldsymbol{Z}_p\}$ 满足 $\sum_{x\in I}\lambda_xc_x=s$ 和 $\sum_{x\in I}\omega_xc_x=0$。又因为 $\theta=T(\rho(x))=\delta(x)$，所以有

$$
\begin{aligned}
&C_{1,id}C_{2,id}^{\left(\frac{1}{x_{id}}\right)}\\
=&\prod_{x\in I}(C_{1,x})^{c_x}\prod_{x\in I}\{e(K_{\rho(x),id},C_{2,x})\cdot\\
&e(H(id)^{x_{id}},C_{3,x})e(K_{\rho(x),id}{}',C_{4,x})\}^{\frac{c_x}{x_{id}}}\\
=&\prod_{x\in I}\{e(g,g)^{\lambda_x}e(g,g)^{\alpha_{\delta(x)}r_x}e(g^{\alpha_{\delta(x)}}\cdot\\
&H(id)^{y_{\delta(x)}}F(\rho(x))^{\frac{t_{\rho(x)}}{x_{id}}},g^{-r_x})(H(id),
\end{aligned}
$$

$$
\begin{aligned}
&g^{y_{\delta(x)}r_x}g^{\omega_x})e(g^{\frac{t_{\rho(x)}}{x_{id}}},F(\rho(x))^{r_x})\}^{c_x}\\
&=\prod_{x\in I}(e(g,g)^{\lambda_x}e(H(id),g)^{\omega_x})^{c_x}\\
&=e(g,g)^{\sum_{x\in I}\lambda_x c_x}e(H(id),g)^{\sum_{x\in I}\omega_x c_x}\\
&=e(g,g)^{s}
\end{aligned}
$$

### 5.2 静态性安全证明

为了证明方案的安全性，需要证明下述引理。

**引理 1** 假定 Rouselakis-Waters(RW)方案[10]是静态性安全的，则本文提出的 R-MA-CP-ABE 方案也是静态性安全的。

**证明** 假设存在有一个多项式时间敌手 $\mathcal{A}$ 能以优势 $\varepsilon$ 攻破 R-MA-CP-ABE 方案，则将能构造一个模拟者 $\mathcal{B}$ 以优势 $\varepsilon$ 攻破 RW 方案。设 $\mathcal{C}$ 是 RW 方案中与 $\mathcal{B}$ 交互的挑战者。

系统建立。挑战者 $\mathcal{C}$ 将 RW 方案中的公开参数 $GP=\{p,G,g,H,F,U,U_\theta,T\}$ 发送给模拟者 $\mathcal{B}$。$\mathcal{B}$ 将 $GP$ 作为 R-MA-CP-ABE 方案的公开参数，并发送给敌手 $\mathcal{A}$。

询问阶段。敌手 $\mathcal{A}$ 首先选择一部分腐化的权威机构 $C_\theta\subseteq U_\theta$，生成并发送这些权威的公钥 $\{PK_\theta\}_{\theta\in C_\theta}$ 给模拟者 $\mathcal{B}$。然后针对 R-MA-CP-ABE 方案向 $\mathcal{B}$ 做如下询问。

1) 选择未被腐化的权威机构 $N_\theta\subseteq U_\theta$，并询问这些权威的公钥。

2) 选取一部分合法用户 $\{id_i\}_{i=1}^m$，并询问对应的用户公钥和私钥。

3) 选取 $\{S_i,id_i\}_{i=1}^n$，并询问对应的云服务器私钥。其中，$S_i\subseteq U$ 为用户 $id_i$ 拥有的属性集，$id_i(1\leqslant i\leqslant n)$ 互不相同，且 $T(S_j)\cap C_\theta=\varnothing$。这里，$n$ 取值比 $m$ 大，即敌手不仅能够询问对应于用户 $\{id_i\}_{i=1}^m$ 的云服务器私钥，也能够询问其他用户对应的云服务器私钥。

4) 选择 2 个长度相等的消息 $M_0$、$M_1$ 和一个访问策略 $(\boldsymbol{A},\rho)$，并询问挑战密文。这里，要求对每个询问过私钥的用户 $id_i(1\leqslant i\leqslant m)$，属性集 $S_{C_\theta}\cup S_i$ 不能满足访问策略 $(\boldsymbol{A},\rho)$。这里，$S_{C_\theta}$ 表示由所有腐化权威机构 $C_\theta$ 管理的属性。

挑战者应答。模拟者 $\mathcal{B}$ 将公钥 $\{PK_\theta\}_{\theta\in C_\theta}$ 发送给挑战者 $\mathcal{C}$，并询问 RW 方案中 $N_\theta\subseteq U_\theta$ 对应的公钥，$\{S_i,id_i\}_{i=1}^m$ 对应的私钥和挑战密文。$\mathcal{C}$ 返回给 $\mathcal{B}$ 相应的公钥 $\{PK_\theta\}_{\theta\in N_\theta}$、私钥 $\{SK_{S_i,id_i}=(g^{\alpha_\theta}H(id_i)^{y_\theta}\cdot F(j)^t,g^t)_{j\in S_i}\}_{i=1}^m$ 和挑战密文 $CT^*$。$\mathcal{B}$ 首先计算 R-MA-CP-ABE 方案中的用户私钥：对 $1\leqslant i\leqslant m$，随机选取 $x_{id_i}\in Z_p^*$，计算用户公钥 $UPK_{id_i}=\{g^{x_{id_i}},H(id_i)^{x_{id_i}}\}$ 和私钥 $USK_{id_i}=\left\{\frac{1}{x_{id_i}}\right\}$。然后计算 $\{S_i,id_i\}_{i=1}^n$ 对应的云服务器私钥，如下所示。

1) 对 $1\leqslant i\leqslant m$，$j\in S_i$，计算 $K_{j,id_i}=(g^{\alpha_\theta}H(id_i)^{y_\theta}F(j)^t)^{x_{id_i}}=g^{\alpha_\theta x_{id_i}}H(id_i)^{y_\theta x_{id_i}}F(j)^{tx_{id_i}}$，$K_{j,id_i}'=(F(j)^t)^{x_{id_i}}=F(j)^{tx_{id_i}}$。令 $CSK_{id_i,S_i}=\{K_{j,id_i},K_{j,id_i}'\}_{j\in S_i}$。

2) 对 $m\leqslant i\leqslant n$，$j\in S_i$，随机选取 $g_j\in G$ 和 $t_j\in Z_p^*$，计算 $K_{j,id_i}=g_jF(j)^{t_j}g_j$，$K_{j,id_i}'=F(j)^{t_j}$。令 $CSK_{id_i,S_i}=\left\{K_{j,id_i},K_{j,id_i}'\right\}_{j\in S_i}$。注意 $g^{\alpha_\theta}H(id_i)^{y_\theta}$ 是群 $G$ 中的元素，而 $G$ 是循环群，所以存在未知的 $x_{id_i}\in Z_p^*$ 使 $g_j=(g^{\alpha_\theta}H(id_i)^{y_\theta})^{x_{id_i}}=g^{\alpha_\theta x_{id_i}}H(id_i)^{y_\theta x_{id_i}}$，因此，$K_{j,id_i}=g_jF(j)^{t_j}=g^{\alpha_\theta x_{id_i}}H(id_i)^{y_\theta x_{id_i}}F(j)^{t_j}$ 和 $K_{j,id_i}'=F(j)^{t_j}$ 是分布合理的云服务器私钥。

$\mathcal{B}$ 将上述权威机构公钥 $\{PK_\theta\}_{\theta\in N_\theta}$、用户公钥和私钥 $\{UPK_{id_i},USK_{id_i}\}_{i=1}^m$、云服务器私钥 $\{CSK_{S_i,id_i}\}_{i=m}^n$ 和挑战密文 $CT^*$ 发送给敌手 $\mathcal{A}$。

猜测。敌手 $\mathcal{A}$ 输出猜测结果 $b'\in\{0,1\}$。$\mathcal{B}$ 同样输出 $b'$。

上述分布对于敌手 $\mathcal{A}$ 来说是和真实情况不可区分的，因此，若 $\mathcal{A}$ 能以优势 $\varepsilon$ 攻破 R-MA-CP-ABE 方案，则 $\mathcal{B}$ 也能以优势 $\varepsilon$ 攻破 RW 方案。

文献[10]已证明下述引理。

**引理 2**[10] 假定 $q$-DPBDHE2 假设成立，则 RW 方案[10]在随机预言模型下是静态性安全的。

**定理 1** 假定 $q$-DPBDHE2 假设成立，则本文的 R-MA-CP-ABE 方案在随机预言模型下是静态性安全的。

**证明** 由引理 1 和引理 2 能够直接得证。

### 5.3 可撤销性安全证明

本节证明的思路与引理 1 类似，首先证明下述引理。

**引理 3** 假定 Rouselakis-Waters(RW)方案[10]是静态性安全的，则本文的 R-MA-CP-ABE 方案是支

持用户撤销的。

**证明**　假设对于本文的 R-MA-CP-ABE 方案，存在一个多项式时间敌手 $\mathcal{A}$ 能够以优势 $\varepsilon$ 赢得 3.3 节中的可撤销游戏，则将能构造出一个模拟者 $\mathcal{B}$ 以优势 $\varepsilon$ 攻破 RW 方案。设 $\mathcal{C}$ 是 RW 方案中与 $\mathcal{B}$ 交互的挑战者。

系统建立。挑战者 $\mathcal{C}$ 将 RW 方案中的公开参数 $GP=\{p,G,g,H,F,U,U_\theta,T\}$ 发送给模拟者 $\mathcal{B}$。$\mathcal{B}$ 将 $GP$ 作为 R-MA-CP-ABE 方案的公开参数发送给敌手 $\mathcal{A}$。

询问阶段。敌手 $\mathcal{A}$ 向 $\mathcal{B}$ 做如下询问。

1) 选择权威机构集合 $N_\theta \subseteq U_\theta$，并询问这些权威的公钥。

2) 选取一部分撤销用户 $\{id_i\}_{i=1}^m$，并询问对应的用户公/私钥对。

3) 选取一部分合法用户 $\{id_i\}_{i=m}^n$，并询问对应于 $\{S_i,id_i\}_{i=m}^n$ 的云服务器私钥。其中，$S_i \subseteq U$ 为用户 $id_i$ 拥有的属性集，$id_i(1\leqslant i\leqslant n)$ 互不相同。

4) 选择 2 个长度相等的消息 $M_0$、$M_1$ 和一个访问策略 $(\boldsymbol{A},\rho)$，并询问挑战密文。

挑战者应答。模拟者 $\mathcal{B}$ 询问 RW 方案中与 $N_\theta \subseteq U_\theta$ 对应的公钥和挑战密文。$\mathcal{C}$ 返回给 $\mathcal{B}$ 对应的公钥 $\{PK_\theta\}_{\theta\in N_\theta}$ 和挑战密文 $CT^*$。然后 $\mathcal{B}$ 执行如下操作。

1) 生成用户私钥：对 $1\leqslant i\leqslant m$，随机选取 $x_{id_i}\in Z_p^*$，计算用户公钥 $UPK_{id_i}=\{g^{x_{id_i}},H(id_i)^{x_{id_i}}\}$ 和私钥 $USK_{id_i}=\left\{\dfrac{1}{x_{id_i}}\right\}$。

2) 生成云服务器私钥：对 $m\leqslant i\leqslant n$，对 $j\in S_i$，随机选取 $g_j\in G$ 和 $t_j\in Z_p^*$，计算 $K_{j,id_i}=g_jF(j)^{t_j}g_j$，$K_{j,id_i}'=F(j)^{t_j}$。令 $CSK_{id_i,S_i}=\{K_{j,id_i},K_{j,id_i}'\}_{j\in S_i}$。注意 $g^{\alpha_\theta}H(id_i)^{y_\theta}$ 是群 $G$ 中的元素，而 $G$ 是循环群，所以存在未知的元素 $x_{id_i}\in Z_p^*$，使 $g_j=(g^{\alpha_\theta}H(id_i)^{y_\theta})^{x_{id_i}}=g^{\alpha_\theta x_{id_i}}H(id_i)^{y_\theta x_{id_i}}$，因此 $K_{j,id_i}=g_jF(j)^{t_j}=g^{\alpha_\theta x_{id_i}}H(id_i)^{y_\theta x_{id_i}}F(j)^{t_j}$ 和 $K_{j,id_i}'=F(j)^{t_j}$ 是分布合理的云服务器私钥。

$\mathcal{B}$ 将上述权威机构公钥 $\{PK_\theta\}_{\theta\in N_\theta}$、用户公/私钥对 $\{UPK_{id_i},USK_{id_i}\}_{i=1}^m$、云服务器私钥 $\{CSK_{S_i,id_i}\}_{i=m}^n$ 和挑战密文 $CT^*$ 发送给敌手 $\mathcal{A}$。

猜测。敌手 $\mathcal{A}$ 输出猜测结果 $b'\in\{0,1\}$。$\mathcal{B}$ 同样输出 $b'$。

**定理 2**　假定 $q$-DPBDHE2 假设成立，则本文的 R-MA-CP-ABE 方案在随机预言模型下是支持用户撤销的。

**证明**　由引理 2 和引理 3 能够直接得证。

### 5.4　性能对比

本节主要给出本文方案与相关方案[5~7]在特性（包括大属性域，无 CA）、存储开销和计算开销方面的对比分析。表 1 给出了具体的对比结果，其中，CA 表示中心权威机构，$|U|$ 代表系统中属性的个数，$|U_\theta|$ 代表系统中权威机构的个数，$|S|$ 代表用户属性的个数，$l$ 代表访问策略中矩阵的行数，$|I|$（$|I|\leqslant l$）代表其中用于解密的行数。由于一个权威机构能够管理多个属性，所以 $|U_\theta|\leqslant|U|$。$P$ 和 $E$ 代表群中的双线性对运算和指数运算。相比群中的双线性对运算和指数运算，乘法运算开销很小，所以表 1 忽略了计算开销中的乘法运算。

#### 5.4.1　特性对比

表 1 中的所有方案都是支持撤销的多权威机构 ABE。在文献[5~7]中，系统所使用的属性需要在系统建立时确定，而且公钥的长度是和 $|U|$ 线性相关的，所以系统中属性个数最多只有多项式大小，只能支持小属性域（small universe）。这会影响方案的

**表 1**　本文方案与相关方案的性能对比

| 方案 | 特性 | | 存储开销 | | | 计算开销 | | |
|---|---|---|---|---|---|---|---|---|
| | 大属性域 | 无 CA | 公钥 | 用户私钥 | 密文 | 素数阶群 | 加密 | 用户解密 |
| 文献[5]方案 | 否 | 否 | $2\|U\|+3$ | $\|S\|+2$ | $4l+3$ | 是 | $(5l+3)E$ | $2\|I\|P+\|I\|E$ |
| 文献[6]方案 | 是 | 否 | 4 | $2\|S\|+2$ | $2l+2$ | 是 | $(2l+2)E$ | $(2\|I\|+2)P+\|I\|E$ |
| 文献[7]方案 | 否 | 是 | $2\|U\|$ | $\|S\|$ | $3l+1$ | 否 | $(5l+1)E$ | $2\|I\|P+\|I\|E$ |
| 本文方案 | 是 | 是 | $2\|U_\theta\|$ | 1 | $4l+1$ | 是 | $(6l+1)E$ | $E$ |

系统可扩展性。比如，一个系统中加入了大量新属性，如果属性的总数超过了系统的初始设置，则需要对系统进行修改甚至重建。此外，文献[5,6]的系统中都存在一个拥有主密钥的 CA。文献[5]中的 CA 不仅需要在系统建立时与每个 AA 交互，而且要给所有用户产生部分私钥。文献[6]中的 CA 需要对系统中所有用户和 AA 进行认证交互。这会导致 CA 的计算和通信开销过大，进而成为整个系统的瓶颈。

本文方案利用一个散列函数 $F$ 将属性映射到群 $G$ 中，任何一个字符串都可以作为新属性加入到系统中，所以不用在系统建立时确定要使用的属性个数。当加入新的属性时，系统的公开参数不会增加，所以也不会出现系统重建问题。另一方面，本文中每个 AA 利用散列函数 $F$ 将用户身份映射到群 $H$ 中来实现抗合谋攻击，从而实现完全的 AA 分权。每个 AA 和用户都可以独立产生私钥，不需要任何 CA。因此，本文所提方案更加符合实际应用需求。

#### 5.4.2 存储开销对比

表 1 中所有方案的密文都是对应于访问策略的，所以密文长度都是与访问策略中的参数 $l$ 线性相关的。因此，云服务器端的存储开销差别不大。在现实情况中，云服务器的存储和计算能力也是远强于个人用户的，所以本文主要考虑用户的各项开销。

文献[5,7]中每个 AA 的公钥长度和他管理的属性个数线性相关，所以系统的整体公钥长度是和 $|U|$ 线性相关的。文献[6]中的公钥长度虽然为常数，但其中 CA 的私钥长度却是与 $|U_\theta|$ 线性相关的。此外，文献[5~7]方案中的用户私钥是 AA 根据用户属性直接生成的，所以用户私钥长度是与 $|S|$ 线性相关的。因此，当属性个数过多时，用户的存储开销会比较大。

本文方案中一个 AA 可以管理多个属性，且 AA 的公钥长度和他管理的属性个数无关，所以整个系统的公钥长度只与 $|U_\theta|$ 线性相关，而与 $|U|$ 无关。又因 $|U_\theta| \leqslant |U|$，所以本文系统的公钥存储开销是要小于文献[5,7]的，但大于文献[6]。本文私钥生成过程分为 2 步：首先由用户为自己产生一组公私钥对，然后 AA 再利用用户公钥和属性来为云服务器端产生私钥。所以云服务器的私钥是和用户的属性个数有关的，而用户私钥长度仅为 1，远远小于其他方案[5~7]的用户私钥。因此，本文方案的用户存储开销小于文献[5~7]中的方案。

#### 5.4.3 计算开销对比

本文方案和文献[5~7]中的方案都是根据访问策略来加密数据的，所以加密过程中的指数运算个数都是和 $l$ 线性相关的。因此，用户的加密开销差别也不大。在文献[5~7]中，用户是直接对云服务器上原始密文解密的，所以解密过程中需要的指数运算和双线性对运算个数都是与访问矩阵中的参数 $|I|$ 线性相关的。

在本文方案中，云服务器首先将原始密文转化为一个易于解密的简单密文，用户再对简单密文进行解密，所以用户的解密开销只有一个指数运算。而一个指数运算在普通移动设备上的运行时间是小于 100 ms 的，这是能够被用户所接受的[18]。所以本文方案适用于使用移动设备进行数据解密的用户。需要注意的是，群中的双线性对运算比指数运算慢约 4 倍，而且合数阶群中的双线性对运算和指数运算要比素数阶群中的相同运算慢 1~2 个数量级[10]。因此，本文方案的用户解密开销远小于文献[5~7]中的方案。

## 6 结束语

针对多机构 ABE 方案中的撤销问题，本文提出了一种支持高效撤销的多机构 CP-ABE 方案，并且证明了方案是静态性安全和支持撤销的。相比于已有方案，本文方案的用户解密过程只需要一个指数运算，降低了用户的解密开销。此外，本文方案不仅没有 CA，而且支持大属性域，更加符合实际应用需求。

## 参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// EUROCRYPT. Aarhus, Denmark, 2005: 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. Alexandria, VA, USA, 2006: 89-98.

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

[4] CHASE M. Multi-authority attribute based encryption[C]//TCC. Amsterdam, The Netherlands, 2007: 515-534.

[5] YANG K, JIA X. Expressive, efficient and revocable data access control for multi-authority cloud storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(7): 1735-1744.

[6] HUANG X, TAO Q, QIN B, et al. Multi-authority attribute based encryption scheme with revocation[C]//The 24th International Conference on Computer Communication and Networks. IEEE, 2015: 1-5.

[7] CUI H, DENG R H. Revocable and decentralized attribute-based encryption[J]. The Computer Journal, 2016: bxw007.

[8] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//PKC. Taormina, Italy, 2011: 53-70.

[9] LEWKO A, WATERS B. Unbounded HIBE and attribute-based encryption[C]//EUROCRYPT. Springer Berlin Heidelberg, 2011: 547-567.

[10] ROUSELAKIS Y, WATERS B. Efficient statically-secure large-universe multi-authority attribute-based encryption[C]//Financial Cryptography and Data Security. Berlin: Springer, 2015: 315-332.

[11] ZHANG K, MA J, LIU J, et al. Adaptively secure multi-authority attribute-based encryption with verifiable outsourced decryption[J]. Science China Information Sciences, 2016, 59(9): 99105.

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

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

[14] YANG Y, DING X, LU H, et al. Achieving revocable fine-grained cryptographic access control over cloud data[C]//Information Security. Springer International Publishing, 2015: 293-308.

[15] YANG Y, LIU J K, LIANG K, et al. Extended proxy-assisted approach: achieving revocable fine-grained encryption of cloud data[C]//European Symposium on Research in Computer Security. Springer International Publishing, 2015: 146-166.

[16] 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.

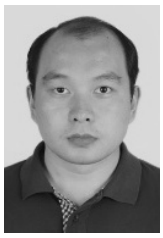
[17] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Technical-Israel Institute of Technology, Faculty of Computer Science, 1996.

[18] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]//The 20th USENIX Security Symposium. San Francisco, 2011: 523-538.

**作者简介：**

**张凯**（1987-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为密码学、信息安全等。

**马建峰**（1963-），男，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为计算机系统安全、移动与无线安全、系统可生存性和可信计算。



**李辉**（1983-），男，湖北武汉人，博士，西安电子科技大学副教授，主要研究方向为数据挖据、安全的数据查询和检索等。

**张俊伟**（1982-），男，陕西西安人，博士，西安电子科技大学副教授，主要研究方向为密码学、信息安全等。

**张涛**（1986-），男，陕西西安人，博士，西安电子科技大学讲师，主要研究方向为可信计算、社交网络等。