密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2014,1(5):465–480

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

密文长度恒定且属性直接可撤销的基于属性的加密*

张应辉[1,2], 郑 东[1], 李 进[3], 李 晖[4]

1. 西安邮电大学 无线网络安全技术国家工程实验室, 西安 710121
2. 中国科学院信息工程研究所 信息安全国家重点实验室, 北京 100093
3. 广州大学 计算机科学与教育软件学院, 广州 510006
4. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室, 西安 710071

通讯作者: 张应辉, E-mail: yhzhaang@163.com

摘 要: 密文策略的基于属性的加密(Ciphertext-Policy Attribute-Based Encryption: CP-ABE)特别适合于云计算环境下的访问控制系统. 在大部分已有的 CP-ABE 方案中, 密文长度会随着访问策略的复杂性的增加而线性增大, 且属性撤销问题没有得到解决. 属性撤销机制是 CP-ABE 在实际应用中的一个基本要求, 与间接的属性撤销机制相比, 直接的属性撤销机制效率更高, 不存在由密钥更新所带来的性能瓶颈. 在已有的大部分支持属性撤销的 CP-ABE 方案中, 每次撤销事件的发生都要求对所有的密文进行更新. 提出了密文长度恒定且属性直接可撤销的 CP-ABE 方案. 在随机预言机模型中, 基于判定性 m-BDHE 假设, 证明了新方案的安全性, 这里 m 表示系统中用户总数的一个上界. 在新方案中, 通过引入适用于多属性值环境的撤销辅助判断函数, 判断当属性撤销事件发生时, 是否需要对一个密文进行更新. 所提出的方案支持具有多个属性值和通配符的 AND 策略. 性能分析和比较表明新方案适用于实际应用, 特别是用户属性变化频繁且带宽资源受限的场景.

关键词: 云计算; 恒定的密文长度; 直接的属性撤销; 基于属性的加密
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000044

中文引用格式: 张应辉, 郑东, 李进, 李晖. 密文长度恒定且属性直接可撤销的基于属性的加密[J]. 密码学报, 2014, 1(5): 465–480.
英文引用格式: Zhang Y H, Zheng D, Li J, Li H. Attribute directly-revocable attribute-based encryption with constant ciphertext length[J]. Journal of Cryptologic Research, 2014, 1(5): 465–480.

Attribute Directly-revocable Attribute-based Encryption with Constant Ciphertext Length

ZHANG Ying-Hui[1, 2], ZHENG Dong[1], LI Jin[3], LI Hui[4]

1. National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

* 基金项目: 国家自然科学基金项目(61402366, 61272457, 61272037, 61472472, 61472091); 陕西省自然科学基础研究计划重点项目(2013JZ020); 工信部重大专项(2013ZX03002004)
收稿日期: 2014-08-01 定稿日期: 2014-08-13

2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
3. School of Computer Science, Guangzhou University, Guangzhou 510006, China
4. State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, China
Corresponding author: ZHANG Ying-Hui, E-mail: yhzhaang@163.com

Abstract: Ciphertext-policy attribute-based encryption (CP-ABE) is very suitable for realizing access control systems in cloud computing. In most of existing CP-ABE schemes, the ciphertext length linearly increases with the complexity of access policies and the attribute revocation issue remains to be an unsolved problem. Attribute revocation mechanisms are indispensable for practical adoption of CP-ABE. Compared with indirect attribute revocation, direct revocation enjoys better efficiency because it removes the performance bottleneck due to secret key update. In most of existing attribute revocable CP-ABE schemes, all the ciphertexts have to be updated whenever a revocation event occurs. In this paper, we propose an attribute direct-revocable CP-ABE scheme with constant ciphertext length. The proposed scheme is proven to be secure in the random oracle model under the decision m-BDHE assumption, where m is an upper bound of the number of users in the system. In the proposed scheme, an auxiliary revocation judgment function is introduced to check whether a ciphertext should be updated or not when revocation events occur. The proposed scheme can support AND-gate access policies with multiple attribute values and wildcards. Performance analysis and comparisons indicate that the proposed CP-ABE scheme is extremely suitable for real-world applications, especially for the scenarios where users' attributes change frequently and bandwidth issues are major concerns.

Key words: cloud computing; constant ciphertext length; direct attribute revocation; attribute-based encryption

1 引言

作为一种一对多的公钥密码学原语, 基于属性的加密(attribute-based encryption, ABE)[1]可用于实现云计算环境下的细粒度数据共享系统. ABE 主要分为两类, 即密钥策略的 ABE(key-policy ABE, KP-ABE)和密文策略的 ABE(ciphertext-policy ABE, CP-ABE)[2]. 在 KP-ABE 中, 访问策略被嵌入在私钥中, 而密文则与属性关联. 在 CP-ABE 中, 则是私钥与属性关联, 每一个密文对应一个访问策略. 由于把访问策略的制定权放在了数据拥有者手中, 与 KP-ABE 相比, CP-ABE 更加适用于云计算环境.

在基于 ABE 的数据共享系统中, 属性撤销机制至关重要. 事实上, 不同的用户往往具有部分相同的属性, 而这些用户的属性又会经常变化, 一个用户的某个属性被撤销可能会影响到其他用户的这一属性. 属性撤销机制可以保证用户的属性撤销不会相互影响. 比如, Alice 和 Bob 都是大学 Univ. A 的学生, 同时也都加入了该校的足球协会, 因此"Univ. A 的学生"和"Univ. A 的足球协会会员"是 Alice 和 Bob 所共有的属性. 如果 Alice 退出了 Univ. A 的足球协会, 则属性权威中心将会撤销 Alice 的属性"Univ. A 的足球协会会员", 同时不会对 Bob 的这一属性产生影响.

在已有的 ABE 方案中, 属性撤销机制分为间接的属性撤销机制和直接的属性撤销机制. 在间接属性撤销机制中, 一旦有撤销事件发生, 属性权威中心就对其他所有用户的属性私钥和系统公开参数进行相应的更新. 同时, 云存储服务器还要对所有的密文进行更新. 在直接的属性撤销机制中, 任何撤销事件的发生只影响被撤销用户, 而不会对其他用户产生影响, 即其他用户不需要到属性权威中心那里进行属性私钥的更新. 可见, 直接的属性撤销机制比间接的属性撤销机制更加实用.

此外, 密文长度对于 ABE 方案的实际应用也有着很大的影响. 在已有的大部分 CP-ABE 方案中, 密文长度会随着访问策略复杂性的增大而线性增加, 从而导致在数据共享应用中巨大的通信代价. 特别地, 在已有的支持属性撤销机制的 CP-ABE 方案中, 密文长度还会随着撤销事件的次数线性增大. 因此, 如果要在实际云平台上部署 CP-ABE, 非常有必要降低其密文长度并提供直接的属性撤销机制.

据作者所知, Zhang 等人[3]提出的支持 AND 策略的 CP-ABE 方案具有恒定大小的密文, 并且支持直接的属性撤销机制. 然而, 方案[3]的 AND 策略仅仅支持属性的正负取值和通配符, 记该 AND 策略为 $\mathrm{AND}^{*}_{+,-}$. 我们将构造一个更为有效的支持 AND 策略的属性可直接撤销的 CP-ABE 方案, 其访问策略支持属性的多个取值和通配符, 记为 AND^{*}_{m}, 并且具有恒定大小的密文. 值得注意的是, AND^{*}_{m} 比 $\mathrm{AND}^{*}_{+,-}$ 具有更加丰富的表达能力, 换句话说, 在同等表达能力的意义下, 支持 AND^{*}_{m} 的 CP-ABE 方案比基于 $\mathrm{AND}^{*}_{+,-}$ 的方案效率更高. 为了说明这一点, 我们考虑如下实例.

假设一个数据共享系统的属性域一共有 n 个属性, 其属性集记为 $U=\{\omega_1,\omega_2,\cdots,\omega_n\}$. 每一个属性具有多个取值, 第 i 个属性 ω_i 具有 n_i 个取值, 相应的取值集合记为 $S_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$. 在表 1 中, 我们考虑 AND^{*}_{m} 策略 $\mathrm{CP1}=v_{1,4}\wedge v_{2,3}\wedge *\wedge v_{4,1}$. 其中, IS 表示信息安全, CS 表示计算机科学, CE 表示通信工程. 另外, $n=4,n_1=4,n_2=3,n_3=3,n_4=2$.

表 1 AND^{*}_{m} 策略

Table 1 AND^{*}_{m} policy

属性	ω_1	ω_2	ω_3	ω_4
描述	Institution	Department	Duty	Gender
取值	Univ. A	IS	Administrator	Male
	Univ. B	CS	Teacher	Female
	Univ. C	CE	Student	
	Univ. D			
CP1	Univ. D	CE	*	Male

显然, 为了实现与 CP1 相同的表达能力, 基于 $\mathrm{AND}^{*}_{+,-}$ 的 CP-ABE 方案必须采用访问策略 CP2. 如表 2 所示, $\mathrm{CP2}=\omega_1^{-}\wedge\omega_2^{-}\wedge\omega_3^{-}\wedge\omega_4^{+}\wedge\omega_5^{-}\wedge\omega_6^{-}\wedge\omega_7^{+}\wedge\omega_8^{*}\wedge\omega_9^{*}\wedge\omega_{10}^{*}\wedge\omega_{11}^{+}\wedge\omega_{12}^{-}$. 因此, 与 AND^{*}_{m} 相比, $\mathrm{AND}^{*}_{+,-}$ 将导致系统属性的总数非常大, 从而导致用户端更高的存储代价, 降低了系统的效率.

表 2 $\mathrm{AND}^{*}_{+,-}$ 策略

Table 2 $\mathrm{AND}^{*}_{+,-}$ policy

属性	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6	ω_7	ω_8	ω_9	ω_{10}	ω_{11}	ω_{12}
描述	Univ. A	Univ. B	Univ. C	Univ. D	IS	CS	CE	Administrator	Teacher	Student	Male	Female
取值	ω_1^{+}	ω_2^{+}	ω_3^{+}	ω_4^{+}	ω_5^{+}	ω_6^{+}	ω_7^{+}	ω_8^{+}	ω_9^{+}	ω_{10}^{+}	ω_{11}^{+}	ω_{12}^{+}
	ω_1^{-}	ω_2^{-}	ω_3^{-}	ω_4^{-}	ω_5^{-}	ω_6^{-}	ω_7^{-}	ω_8^{-}	ω_9^{-}	ω_{10}^{-}	ω_{11}^{-}	ω_{12}^{-}
CP2	ω_1^{-}	ω_2^{-}	ω_3^{-}	ω_4^{+}	ω_5^{-}	ω_6^{-}	ω_7^{+}	*	*	*	ω_{11}^{+}	ω_{12}^{-}

可见, 构造支持 AND^{*}_{m} 策略的 CP-ABE 方案, 提供直接的属性撤销机制并保证密文长度恒定, 是非常具有意义的研究.

1.1 本文的贡献

构造了一个支持 AND^{*}_{m} 策略且密文大小恒定的 CP-ABE 方案, 该方案提供了直接的属性撤销机制. 在

随机预言机模型中, 基于判定性 m-BDHE (bilinear Diffie-Hellman exponent)假设证明了方案的安全性, 其中 m 表示系统中用户总数的一个上界. 具体地讲, 在多属性值的环境下, 引入了一个撤销辅助判断函数, 以判断哪些密文受到了属性撤销事件的影响, 然后采用广播加密技术只更新受到影响的密文. 性能分析和比较表明, 新方案非常有效的实现了直接的属性撤销机制, 特别适用于用户属性变化频繁且带宽资源受限的实际应用场景.

1.2 相关研究工作

Sahai 和 Waters[1]首次提出了 ABE 的概念, 并构造了模糊的基于身份的加密, 这是一种门限策略的 ABE 方案. Goyal 等人[2]进一步扩展了这一概念, 把 ABE 分为 KP-ABE 和 CP-ABE. 本文主要关注 CP-ABE. Bethencourt 等人[4]首次构造了一个支持树结构的 CP-ABE 方案. 然而, 该方案的安全性是在一般群模型中给出的. 为了克服这一缺点, Cheung 和 Newport[5]提出了一个新的支持 $\mathrm{AND}^{*}_{+,-}$ 策略的 CP-ABE 方案, 并在标准模型下证明了该方案的安全性. 近年来, 关于 ABE 还有大量的研究, 例如多中心 ABE[6–8]、可追踪的 ABE[9,10]、匿名 ABE[11–14]以及外包 ABE[15–17]等.

然而, 已有 CP-ABE 方案大多数存在效率缺陷, 其密文长度都非常大, 会随着访问策略复杂性的增长线性增大. 考虑到带宽资源受限的实际应用场景, 有不少学者研究了密文长度恒定的 ABE 方案. Emura 等人[18]提出了第一个密文长度恒定的 CP-ABE 方案. 然而该方案的访问策略仅支持属性的正负取值, 不支持通配符, 记为 $\mathrm{AND}_{+,-}$. 一个用户可以解密当且仅当他的属性列表与访问策略完全一致, 因此该方案已经失去了基于属性的加密中一对多的意义. 类似地, 支持 AND_{m} 策略的 CP-ABE 方案[19,20]和支持 AND_{+} 策略的 CP-ABE 方案[21]也存在同样的问题. 这里, AND_{m} 表示属性具有多个取值但不支持通配符的 AND 策略, AND_{+} 表示属性仅仅取一个正值且不支持通配符的 AND 策略. Chen 等人[22]提出了一个 CP-ABE 方案, 其密文长度都是恒定的, 并支持 $\mathrm{AND}^{*}_{+,-}$ 策略, 类似的方案还有文献[23]. Herranz 等人[24]构造了支持 (l,n) 门限策略且密文大小恒定的 CP-ABE 方案, Ge 等人[25]提出了一个新的 (l,n) 门限策略且密文大小恒定的 CP-ABE 方案, Attrapadung 等人[26]提出了一个密文长度恒定的内积加密方案.

尽管上述 CP-ABE 方案拥有恒定大小的密文, 但是这些方案却不支持属性撤销机制. 在已有的方案中, 属性撤销机制包括间接的属性撤销机制[4,27–29]和直接的属性撤销机制[30–33]. 通过给每个属性设置一个有效期限, 方案[4,27]实现了间接的属性撤销机制, 然而这些方案不能实现即时的属性撤销. Yu 等人[28]提出的 CP-ABE 方案不再依赖于有效期实现属性撤销, 而是借助于一个半可信的代理服务器实现了即时的间接属性撤销, 即属性权威中心对没有被撤销事件牵涉的用户进行私钥更新, 代理服务器对所有的密文进行代理重加密. 通过让代理服务器使用属性群组密钥对所有密文进行代理重加密, Hur 等人[29]也提出了一个即时的间接属性撤销机制. 通过向合法用户分发一个对称密钥, Cheng 等人[30]实现了间接的用户撤销. 在文献[30]中, 文件被分成许多小片段, 然后存储在云平台上, 当撤销事件发生时, 数据拥有者对部分片段进行重加密. 然而, 由于属性私钥的更新, 间接属性撤销机制存在性能瓶颈. 为了克服这一缺陷, Attrapadung 等人基于广播加密技术提出了直接撤销机制[34], 然而仅仅支持用户级撤销, 无法实现细粒度的属性撤销. 此外, 该方案要求数据拥有者自己能够对数据的访问进行控制, 因此不适用于云计算环境. 广播加密的概念由 Fiat 等人[35]提出, Boneh 等人[31]构造了一个密文和私钥长度更小的广播加密方案. Wang 等人[32]在 KP-ABE 中实现了直接的属性撤销机制. 在合数阶双线性群中, 王等人[33]实现了属性可直接撤销的 CP-ABE 方案. 然而, 在上述直接可撤销的方案中, 密文长度会随着撤销事件的次数或者访问策略中属性的个数线性增长. 目前, Zhang 等人[3]提出的 CP-ABE 方案支持直接的用户/属性撤销, 并且具有恒定大小的密文, 然而该方案仅支持 $\mathrm{AND}^{*}_{+,-}$ 策略. 可见, 支持 AND^{*}_{m}, 策略且密文大小恒定的直接可撤销的 CP-ABE 方案值得进一步研究.

2 预备知识

2.1 符号说明

表 3 对本文所用到的一些符号的含义进行了解释.

表 3 符号说明
Table 3 Symbol description

符号	含义
AND_{+}	仅支持属性取正值的 AND 策略
$\mathrm{AND}_{+,-}$	仅支持属性取正值和负值的 AND 策略
$\mathrm{AND}^{*}_{+,-}$	支持通配符以及属性取正值和负值的 AND 策略
AND_{m}	仅支持属性取多个值的 AND 策略
AND^{*}_{m}	支持通配符以及属性取多个值的 AND 策略
$x\in_R X$	从集合 X 中随机选取了一个元素 x
I_k	k 是一个正整数, $I_k=\{1,2,\cdots,k\}$
N_{now}	到当前时刻 now 为止, 属性权威中心发布属性撤销信息的次数
$R^{(i)}$	当第 i 个属性撤销事件发生时, 属性权威中心所发布的属性撤销信息/列表
R	$R=\{R^{(i)}\}_{1\leqslant i\leqslant N_{\mathrm{now}}}$, 即到时刻 now 为止, 属性权威中心所发布的所有属性撤销信息
$\mathrm{PP}^{(i)}$	当第 i 个属性撤销事件发生时, 属性权威中心所发布的公开的撤销参数
PP	$\mathrm{PP}=\{\mathrm{PP}^{(i)}\}_{1\leqslant i\leqslant N_{\mathrm{now}}}$, 即到时刻 now 为止, 属性权威中心发布的所有公开的撤销参数

2.2 密码学基础

定义 1(双线性对) 设 G 是一个阶为大素数 p 的乘法循环群, g 是 G 的一个生成元, G_T 是也是一个 p 阶的乘法循环群, 1_T 是 G_T 的单位元. 如果映射 $\hat{e}$ 满足如下三个条件, 则称 $\hat{e}$ 为一个双线性对:

(1) 双线性性: 对任意的 $a,b\in Z_p^*$, $\hat{e}\left(g^a,g^b\right)=\hat{e}\left(g,g\right)^{ab}$;

(2) 非退化性: 存在 $g_1,g_2\in G$, 使得 $\hat{e}\left(g_1,g_2\right)\neq 1_T$;

(3) 可计算性: 对任意的 $g_1,g_2\in G$, 存在计算 $\hat{e}\left(g_1,g_2\right)$ 的有效算法.

定义 2(判定性 (t,ε,l)-BDHE 假设) 本文所提出的CP-ABE方案的安全性依赖于判定性 (t,ε,l)-BDHE 假设. 设 G 是一个阶为大素数 p 的乘法循环群, g 和 h 是 G 的两个独立的生成元. 选取 $\alpha\in Z_p^*$, 计算 $g_i=g^{(\alpha^i)}$, 令 $\vec{y}_{g,\alpha,l}=\left(g_1,g_2,\cdots,g_l,g_{l+2},\cdots,g_{2l}\right)\in G^{2l-1}$. 设 B 是一个试图解决判定性 (t,ε,l)-BDHE 问题且输出 $\mu\in\{0,1\}$ 的算法, 如果不等式(1)成立, 则称 B 的优势为 ε.

$$\left|\Pr\left[B\left(g,h,\vec{y}_{g,\alpha,l},\hat{e}\left(g_{l+1},h\right)\right)=1\right]-\Pr\left[B\left(g,h,\vec{y}_{g,\alpha,l},Z\right)=1\right]\right|\geqslant\varepsilon \tag{1}$$

其中, 概率取值基于 g 和 h 在 G 中的随机取值, $\alpha\in Z_p^*$ 的随机性, 以及 B 的随机比特. 如果没有算法能够在时间 t 内以至少 ε 的优势解决判定性 (t,ε,l)-BDHE 问题, 则称 (t,ε,l)-BDHE 假设在 G 中成立.

2.3 访问策略

访问策略就是 CP-ABE 中的密文策略. 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，$L\not\models W$ 表示二者不匹配. 在本文中，我们考虑了访问策略 AND_m^*. AND_m^* 是访问策略 $\mathrm{AND}_{+,-}^*$ 的推广，文献[12]也采用了 AND_m^* 给定属性列表 $L=[L_1,L_2,\cdots,L_n]$ 和访问策略 $W=[W_1,W_2,\cdots,W_n]=\wedge_{i\in I_W}W_i$，对于 $1\leqslant i\leqslant n$，如果 $L_i=W_i$ 或者 $W_i=*$，则称 $L\models W$，否则 $L\not\models W$. 其中，$I_W=\{i\,|\,1\leqslant i\leqslant n, W_i\neq *\}$ 是一个下标索引集，明确了出现在 W 中的非通配符的属性. 没有出现在 W 中的属性表示其取值为通配符 $*$，这时用户是否具有相应的属性不会影响其解密能力.

2.4 撤销辅助判断函数

撤销辅助判断函数 RevoIndex[3]只适用于属性的正负取值. 在属性具有多个取值的环境下，为了检测一个访问策略 W 是否受到属性撤销信息 $R^{(k)}$ 的影响，本文引入了一个辅助函数 mRevoIndex. 具体地讲，当第 k 个属性撤销事件发生时，基于 mRevoIndex 可以判断是否需要对与 W 对应的密文进行更新. 在描述 mRevoIndex 之前，先解释 mRevoIndex 所涉及到的几个符号:

(1) $U^{(k)}=\{\omega_i\,|\,i\in I_{U^{(k)}}\}\subseteq U$ 表示当第 k 个属性撤销事件发生时，属性权威中心所撤销的属性集，其中 $I_{U^{(k)}}$ 表示这些属性的索引.

(2) $R^{(k)}=\{R_\omega^{(k)}\,|\,\omega\in U^{(k)}\}$ 表示当第 k 个属性撤销事件发生时，属性权威中心发布的属性撤销信息/列表.

(3) $R_\omega^{(k)}=\{R_v^{(k)}\}_{v\in S_\omega}$ 表示与 $R^{(k)}$ 和属性 ω 对应的用户的索引集，即当第 k 个属性撤销事件发生时，所拥有的属性 ω 被撤销的用户的索引集，这里 S_ω 表示属性 ω 的取值集合.

(4) $R_v^{(k)}$ 表示 $R_\omega^{(k)}$ 中的属性 ω 取值为 v 的用户.

(5) $R_W^{(k)}$ 表示当第 k 个属性撤销事件发生时，与 W 对应的被牵涉到的用户的索引集.

撤销辅助判断函数 mRevoIndex 的具体描述如下:

撤销辅助判断函数 mRevoIndex

算法开始

(1) 输入 PK, W 和 $R^{(k)}$;

(2) 将 W 解析为 $W=\wedge_{i\in I_W}W_i$;

(3) 将 $R^{(k)}$ 解析为 $R^{(k)}=\{R_\omega^{(k)}\,|\,\omega\in U^{(k)}\}=\left\{\{R_v^{(k)}\}_{v\in S_\omega}\,|\,\omega\in U^{(k)}\right\}$;

(4) 令 $I_{R_W^{(k)}}=I_W\cap I_{U^{(k)}}$;

(5) 计算 $R_W^{(k)}=\cup_{i\in I_{R_W^{(k)}}}R_{W_i}^{(k)}=\cup_{i\in I_{R_W^{(k)}}}R_{v_{i,k_i}}^{(k)}$，其中 $W_i=v_{i,k_i}$;

(6) 输出 $R_W^{(k)}$.

算法结束

需要指出的是，如果 $R_W^{(k)}=\varnothing$，则 W 不受第 k 个属性撤销事件的影响，即不受 $R^{(k)}$ 的影响. 从而，当第 k 个属性撤销事件发生时，与 W 对应的密文不需要更新. 否则 $R_W^{(k)}=\varnothing$，则 W 受到第 k 个属性撤销事件的影响，即受到 $R^{(k)}$ 的影响. 从而，当第 k 个属性撤销事件发生时，与 W 对应的密文必须进行更新，使得

$R_W^{(k)}$ 所对应的用户不能再解密更新后的密文. 特别地, 设 $R=\left\{R^{(k)}\right\}_{1\leqslant k\leqslant N_{\text{now}}}$, 计算

$$R_W^{(k)}=\text{mRevolndex}\left(\text{PK},W,R^{(k)}\right)$$

令 $R_W=\bigcup_{1\leqslant k\leqslant N_{\text{now}}}R_W^{(k)}$. 如果 $R_W=\varnothing$, 则 W 不受 R 的影响. 否则 $R_W\neq\varnothing$, 则 W 受到了 R 的影响.

3 算法定义和安全模型

3.1 算法定义

类似于文献[3], 一个直接可撤销的 CP-ABE 方案由系统建立算法 Setup、密钥生成算法 KeyGen、加密算法 Encrypt、更新密钥生成算法 UKeyGen、密文更新算法 CTUpdate 和解密算法 Decrypt 构成, 具体描述如下:

Setup$\left(1^{\lambda}\right)\rightarrow\left(\text{PK},\text{MK}\right)$: 系统建立算法由属性权威中心运行. 算法以安全参数 λ 为输入, 输出系统公开参数 PK 和主私钥 MK. 属性权威中心把 PK 公开, 把 MK 秘密保存.

keyGen$\left(\text{PK},\text{MK},L\right)\rightarrow\text{SK}_L$: 密钥生成算法由属性权威中心运行. 算法以系统公开参数 PK, 主私钥 MK 和属性列表 L 为输入, 输出与 L 关联的属性私钥 SK_L.

Encrypt$\left(\text{PK},M,W,R\right)\rightarrow\text{CT}_W$ ①: 加密算法由加密者运行. 算法以系统公开参数 PK, 明文消息 M, 访问策略 W 和属性撤销信息 R 为输入, 输出与 W 对应的的密文 CT_W. 如果 W 不受 R 的影响, 则称 CT_W 为 Type-1 密文, 否则 W 受到 R 的影响, 则称 CT_W 为 Type-2 密文.

UKeyGen$\left(\text{PK},\text{MK},R^{(k)}\right)\rightarrow\left(\text{PP}^{(k)},\text{UK}^{(k)}\right)$: 更新密钥生成算法由属性权威中心运行. 算法以系统公开参数 PK, 主私钥 MK 和第 k 个属性撤销事件所对应的属性撤销信息 $R^{(k)}$ 为输入, 输出与 $R^{(k)}$ 对应的公开参数 $\text{PP}^{(k)}$ 和更新密钥 $\text{UK}^{(k)}$. 属性权威中心将 $\text{PP}^{(k)}$ 公开, 把 $\text{UK}^{(k)}$ 通过安全信道发送云存储服务器.

CTUpdate$\left(\text{PK},\text{CT}_W,\text{UK}^{(k)},R^{(k)}\right)\rightarrow\text{CT}_W'$ ②: 当且仅当 W 受到 $R^{(k)}$ 的影响时, 云存储服务器执行密文更新算法. 算法以系统公开参数 PK, 与 W 对应的密文 CT_W, 更新密钥 $\text{UK}^{(k)}$ 和 $R^{(k)}$ 为输入, 输出与 CT_W 对应的更新后的密文 CT_W'. 如果 CT_W 为 Type-1 密文, 则称 CT_W' 为 Type-3 密文; 如果 CT_W 为 Type-2 密文, 则称 CT_W' 为 Type-4 密文; 如果 CT_W 为 Type-3 或 Type-4 密文, 则更新后的密文 CT_W' 的类型保持不变.

Decrypt$\left(\text{PK},\text{PP},\text{CT}_W,\text{SK}_L\right)\rightarrow M$ or $\perp$: 解密算法由解密者运行. 算法以系统公开参数 PK, 与 W 对应的消息 M 的密文 CT_W, 以及与属性列表 L 关联的属性私钥 SK_L 为输入, 如果 $L\vert=W$ 且 SK_L 没有被牵涉到与 CT_W 相关联的撤销事件中, 则输出明文消息 M, 否则输出错误符号 $\perp$.

由于解密者与云服务器需要对四种密文进行区分, 我们默认密文包含了 2 个比特的信息, 用于表明该密文的类型. 基于这 2 个比特的潜在信息, 解密者与云服务器能够区分密文的类型.

---

①如果一个用户被牵涉到与 R 相关的某个属性撤销事件中, 且 W 受到 R 的影响, 即使该用户的属性列表匹配 W, 也无法从 $\text{CT}_W=\textbf{Encrypt}\left(\text{PK},M,W,R\right)$ 解密出 M.

②如果一个用户被牵涉到与 $R^{(k)}$ 相关的撤销事件中, 且 W 受到 $R^{(k)}$ 的影响, 即使该用户能够解密 CT_W, 他也无法解密 $\text{CT}_W'=\textbf{CTUpdate}\left(\text{PK},\text{CT}_W,\text{UK}^{(k)},R^{(k)}\right)$. 一般来说, 加密策略可以由需要加密资源的属性或允许访问者的属性来决定.

3.2 安全模型

根据挑战密文的类型, 相应的敌手可以分为两类: Type-Ⅰ敌手 A_{I} 和 Type-Ⅱ敌手 A_{II}. A_{I} 的目标是攻破 Type-1 密文, 由于这类密文不涉及属性撤销事件, 因此 A_{I} 不能对满足挑战策略的属性列表进行密钥生成询问. 反之, A_{II} 的目标是攻破 Type-2、Type-3 和 Type-4 密文, 由于这类密文涉及属性撤销事件, 因此 A_{II} 可以对满足挑战策略的属性列表进行密钥生成询问. 类似于文献[5]中的方案, 本文的方案考虑了选择安全性, 即选择访问策略和明文攻击下的密文不可区分性(indistinguishability against selective ciphertext-policy and chosen-plaintext attacks, IND-sCP-CPA). 类似于文献[3], 形式化定义基于下面的 IND-sCP-CPA 游戏, 该游戏在敌手 $A_i\left(i=\mathrm{I},\mathrm{II}\right)$ 和挑战者 S 之间交互式进行.

Init: 敌手 $A_i\left(i=\mathrm{I},\mathrm{II}\right)$ 提交一个挑战策略 W^* 给挑战者 S. 此外, A_{II} 再提交属性撤销信息 $R^*=\left\{R^{*(1)},R^{*(2)},\cdots,R^{*(j)}\right\}$ 和属性撤销列表 $R^{*(k)}$, 其中 $k\geqslant j+1$.

Setup: S 选择一个足够大的安全参数 λ, 运行系统建立算法 Setup, 生成主私钥 MK 和相应的系统公开参数 PK. S 保存 MK, 把 PK 发送给 A_i.

Phase 1: 除了哈希询问以外, A_i 可以发起多项式次如下询问:

(1) **KeyGen Oracle** O_{KeyGen}: A_i 提交一个属性列表 L 给 S, S 根据敌手的类别进行如下回答:

对于 A_{I}, 如果 $L\left|\neq W^*\right.$, 则 S 生成一个属性私钥 SK_L 并发送给 A_i, 否则输出 $\perp$.

对于 A_{II}, S 直接生成一个属性私钥 SK_L 并发送给 A_{II}.

(2) **UKeyGen Oracle** O_{UKeyGen}: A_i 提交一个属性撤销列表 $R^{(k)}$, S 返回与 $R^{(k)}$ 对应的更新密钥 $\mathrm{UK}^{(k)}$.

(3) **CTUpdate oracle** O_{CTUpdate}: A_i 提交一个密文 CT_W 和属性撤销列表 $R^{(k)}$, S 返回与 CT_W 对应的更新后的密文 CT'_W.

Challenge: 一旦决定结束 Phase 1, A_i 就输出两个等长的消息 M_0 和 M_1. S 随机选取 $b\in\{0,1\}$, 并根据敌手的类别生成如下挑战密文:

(1) 对于 A_{I}, S 计算 $\mathrm{CT}_{W^*}=\mathrm{Encrypt}\left(\mathrm{PK},M_b,W^*,\varnothing\right)$, 显然 CT_{W^*} 是 Type-1 密文.

(2) 对于 A_{II}, 有如下三种情况需要考虑:

Case 1. W^* 受到 R^* 的影响. 在这种情况下, S 返回 $\mathrm{CT}_{W^*}=\mathrm{Encrypt}\left(\mathrm{PK},M_b,W^*,R^*\right)$, 因此挑战密文 CT_{W^*} 属于 Type-2.

Case 2. W^* 没有受到 R^* 的影响, 但是受到了 $R^{*(k)}$ 的影响. 在这种情况下, S 返回

$$\mathrm{CT}'_{W^*}=\mathrm{CTUpdate}\left(\mathrm{PK},\mathrm{CT}_{W^*},\mathrm{UK}^{(k)},R^{*(k)}\right)$$

其中 $\mathrm{CT}_{W^*}=\mathrm{Encrypt}\left(\mathrm{PK},M_b,W^*,R^*\right)$, 因此挑战密文 CT'_{W^*} 属于 Type-3.

Case 3. W^* 同时受到 R^* 与 $R^{*(k)}$ 的影响. 在这种情况下, 类似于 Case 2, S 计算 CT'_{W^*} 并返回给 A_{II}, 显然 CT'_{W^*} 属于 Type-4。

Phase 2: 同 **Phase 1**. 此外, A_i 可以对挑战密文进行密文更新询问.

Guess: A_i 输出一比特 $b'\in\{0,1\}$, 其赢得游戏当且仅当 $b'=b$. 定义 A_i 在 IND-sCP-CPA 游戏中的优势为

$$\mathrm{Adv}_{\text{CP-ABE}}^{\text{IND-sCP-CPA}}(A)=\left|\Pr[b'=b]-\frac{1}{2}\right|$$

定义 3(直接可撤销的 CP-ABE 的安全性) 如果没有概率多项式时间敌手能够以不可忽略的优势赢得 IND-sCP-CPA 游戏, 则称直接可撤销的 CP-ABE 方案是 IND-sCP-CPA 安全的.

4 支持 AND_m^* 策略的直接可撤销的 CP-ABE 方案

4.1 具体构造

Setup(1^λ): 设 G 和 G_T 是两个阶为大素数 p 的乘法循环群, g 是 G 的一个生成元, $\hat{e}:G\times G\to G_T$ 是一个双线性映射. 假设系统的属性域一共有 n 个属性, 其属性集记为 $U=\{\omega_1,\omega_2,\cdots,\omega_n\}$. 每一个属性具有多个取值, 第 i 个属性 ω_i 具有 n_i 个取值, 相应的取值集合记为 $S_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$. 定义两个无碰撞的哈希函数 $H_0:Z_p^*\times\{0,1\}^{\log_2 n}\times\{0,1\}^{\log_2 n_m}\to Z_p^*$ 和 $H_1:Z_p^*\to G$, 其中 $n_m=\max_{i=1}^n n_i$. 此外, 属性权威中心选取 $x,y\in_R Z_p^*$, 对于 $1\leqslant i\leqslant n$ 和 $1\leqslant k_i\leqslant n_i$, 计算 $X_{i,k_i}=g^{-H_0(x\|i\|k_i)}$ 和 $Y_{i,k_i}=\hat{e}(g,g)^{H_0(y\|i\|k_i)}$. 选取 $\alpha,\beta\in_R Z_p^*$, 计算 $v=g^\beta$ 和 $\left\{g_i=g^{(\alpha^i)}\right\}_{i\in I_{2m}\setminus m+1}$, 这里正整数 m 表示系统中用户数量的一个上界. 最后, 所生成的系统公开参数为 $\mathrm{PK}=\left\langle g,\{X_{i,k_i},Y_{i,k_i}\}_{1\leqslant i\leqslant n,1\leqslant k_i\leqslant n_i},\{g_i\}_{i\in I_{2m}\setminus m+1},v\right\rangle$, 主私钥为 $\mathrm{MK}=\langle x,y,\beta\rangle$.

KeyGen$(\mathrm{PK},\mathrm{MK},L)$: 具有属性列表 $L=[L_1,L_2,\cdots,L_n]$ 的用户向属性权威中心申请属性私钥. 属性权威中心选取 $\mathrm{sk}\in_R Z_p^*$, 对 $1\leqslant i\leqslant n$, 计算 $\overline{\sigma}_i=\sigma_{i,k_i}=g^{H_0(y\|i\|k_i)}H_1(\mathrm{sk})^{H_0(x\|i\|k_i)}$, 这里假设 $L_i=v_{i,k_i}$. 此外, 属性权威中心计算 $d=g_{\mathrm{sn}}^\beta$, 这里 sn 是一个序列号, 对应着加入系统的第 sn 个用户. 最终生成的属性私钥为 $\mathrm{SK}_L=\left\langle \mathrm{sn},\mathrm{sk},\{\overline{\sigma}_i\}_{1\leqslant i\leqslant n},d\right\rangle$.

Encrypt(PK,M,W,R): 假设属性权威中心已经发布了 N_{now} 个属性撤销列表 $R=\left\{R^{(i)}\right\}_{1\leqslant i\leqslant N_{\mathrm{now}}}$. 为了在访问策略 $W=\wedge_{i\in I_W}W_i$ 下加密消息 M, 这里设 $W_i=v_{i,k_i}$, 加密者计算 $\langle X_W,Y_W\rangle=\left\langle\prod_{i\in I_W}\overline{X}_i,\prod_{i\in I_W}\overline{Y}_i\right\rangle$, 其中 $\left\langle\overline{X}_i,\overline{Y}_i\right\rangle=\left\langle X_{i,k_i},Y_{i,k_i}\right\rangle$. 此外, 对于 $1\leqslant i\leqslant N_{\mathrm{now}}$, 加密者计算 $R_W^{(i)}=\mathrm{mRevolndex}\left(\mathrm{PK},W,R^{(i)}\right)$, 令 $R_W=\bigcup_{i=1}^{N_{\mathrm{now}}}R_W^{(i)}$, 则 R_W 表示 R 中与 W 对应的属性撤销信息. 接着, 加密者选取 $s\in_R Z_p^*$, 计算密文 CT_W 如下:

(1) 如果 $R_W=\varnothing$, 则 CT_W 为 Type-1 密文. 此时, R 中不存在影响 W 的撤销信息. 加密者计算 $C_0=MY_W^s$, $C_1=g^s$ 和 $C_2=X_W^s$ 输出密文 $\mathrm{CT}_W=\langle W,C_0,C_1,C_2\rangle$.

(2) 如果 $R_W\neq\varnothing$, 则 CT_W 为 Type-2 密文. 此时, W 受 R 的影响. 加密者计算 $K_R=\hat{e}(g_1,g_m)^s$ 和 $C_R=\left(v\cdot\prod_{i\in I_m-R_W}g_{m+1-i}\right)^s$, 令 $C_0=MY_W^sK_R$, $C_1=g^s$, $C_2=X_W^s$, 并输出 $\mathrm{CT}_W=\langle W,C_0,C_1,C_2,C_R\rangle$.

UKeyGen$\left(\mathrm{PK},\mathrm{MK},R^{(k)}\right)$: 属性权威中心选取 $\mathrm{uk}^{(k)}\in_R Z_p^*$, 计算 $\mathrm{UK}^{(k)}=\mathrm{uk}^{(k)}\beta$, $\mathrm{PP}^{(k)}=v^{\mathrm{uk}^{(k)}}=g^{\mathrm{UK}^{(k)}}$. 将 $\mathrm{PP}^{(k)}$ 公开, 把 $\mathrm{UK}^{(k)}$ 通过安全信道发送给云存储服务器.

CTUpdate$\left(\mathrm{PK},\mathrm{CT}_W,\mathrm{UK}^{(k)},R^{(k)}\right)$: 当第 k 次属性撤销事件发生时, 根据相应的属性撤销列表 $R^{(k)}$, 云存

储服务器对密文 CT_W 进行更新. 根据 CT_W 的类别, 考虑如下四种情况:

Case 1. 密文 $\mathrm{CT}_W=\langle W,C_0,C_1,C_2\rangle$ 由加密者生成, 属于Type-1密文. 在这种情况下, $k=1$. 对于 $1\leqslant i\leqslant k$, 计算 $R_W^{(i)}=\mathrm{mRevolndex}\left(\mathrm{PK},W,R^{(i)}\right)$. 令 $R_W^{(k)}=R_W^{(k)}-\bigcup_{i=1}^{k-1}R_W^{(i)}$, 其中 $R_W^{(0)}=\varnothing$. 如果 $R_W^{(k)}=\varnothing$, 则不需要更新.否则 $R_W^{(k)}\neq\varnothing$, 云存储服务器计算 $K=\hat{e}\left(g_1,g_m\right)^{\mathrm{UK}^{(k)}}$, 令 $C_0'=C_0\cdot K$, $C_{\hat{R}}=C_{R^{(k)}}$, 其中 $C_{R^{(k)}}=\left(v\cdot\prod_{i\in I_m-R_W^{(k)}}g_{m+1-i}\right)^{\mathrm{UK}^{(k)}}$. 最终得到更新之后的Type-3密文 $\mathrm{CT}_W'=\left\langle W,C_0',C_1,C_2,C_{\hat{R}}\right\rangle$.

Case 2. 密文 $\mathrm{CT}_W=\langle W,C_0,C_1,C_2,C_R\rangle$. 由加密者生成, 属于 Type-2 密文. 在这种情况下, 假设 $R=\left\{R^{(1)},R^{(2)},\cdots,R^{(j)}\right\}$, 则 $j\geqslant 1$, $k=j+1$. 类似于 Case 1, 云存储服务器生成 C_0' 和 $C_{\hat{R}}$. 最终得到更新之后的 Type-4 密文 $\mathrm{CT}_W'=\left\langle W,C_0',C_1,C_2,C_R,C_{\hat{R}}\right\rangle$.

Case 3. 密文 $\mathrm{CT}_W=\left\langle W,C_0,C_1,C_2,C_{\hat{R}}\right\rangle$. 由云存储服务器经过密文更新得到, 属于Type-3密文. 在这种情况下, $k\geqslant 2$. 对于 $1\leqslant i\leqslant k$, 计算 $R_W^{(i)}=\mathrm{mRevolndex}\left(\mathrm{PK},W,R^{(i)}\right)$, 令 $R_W^{(k)}=R_W^{(k)}-\bigcup_{i=1}^{k-1}R_W^{(i)}$. 如果 $R_W^{(k)}=\varnothing$, 则不需要更新. 否则 $R_W^{(k)}\neq\varnothing$, 云存储服务器计算 $K=\hat{e}\left(g_1,g_m\right)^{\mathrm{UK}^{(k)}}$, 令 $C_0'=C_0\cdot K$, $C_{\hat{R}}'=C_{\hat{R}}\cdot C_{R^{(k)}}$, 其中 $C_{R^{(k)}}=\left(v\cdot\prod_{i\in I_m-R_W^{(k)}}g_{m+1-j}\right)^{\mathrm{UK}^{(k)}}$. 最终得到更新之后的Type-3密文 $\mathrm{CT}_W'=\left\langle W,C_0',C_1,C_2,C_{\hat{R}}'\right\rangle$.

Case 4. 密文 $\mathrm{CT}_W=\left\langle W,C_0,C_1,C_2,C_R,C_{\hat{R}}\right\rangle$. 由云存储服务器经过密文更新得到, 属于Type-4密文. 在这种情况下, 假设 $R=\left\{R^{(1)},R^{(2)},\cdots,R^{(j)}\right\}$, 则 $j\geqslant 1$, $k\geqslant j+2$. 类似于Case 3, 云存储服务器生成 C_0' 和 $C_{\hat{R}}'$. 最终得到更新之后的Type-4密文 $\mathrm{CT}_W'=\left\langle W,C_0',C_1,C_2,C_R,C_{\hat{R}}'\right\rangle$.

Decrypt$\left(\mathrm{PK},\mathrm{PP},\mathrm{CT}_W,\mathrm{SK}_L\right)$: 拥有属性私钥 $\mathrm{SK}_L=\left\langle \mathrm{sn},\mathrm{sk},\left\{\overline{\sigma}_i\right\}_{1\leqslant i\leqslant n},d\right\rangle$ 的解密者试图解密密文 CT_W. 解密者首先检测 L 和 W, 如果 $L\left|\neq W\right.$, 则返回 $\perp$. 否则, $L\left|=W\right.$, 根据 CT_W 的类别, 考虑如下四种情况:

Case 1. 密文 $\mathrm{CT}_W=\langle W,C_0,C_1,C_2\rangle$ 属于Type-1密文. 解密者计算 $\sigma_W=\prod_{i\in I_W}\overline{\sigma}_i$, 并恢复出消息

$$M=\frac{C_0}{\hat{e}\left(\sigma_W,C_1\right)\cdot\hat{e}\left(H_1\left(\mathrm{sk}\right),C_2\right)}.$$

Case 2. 密文 $\mathrm{CT}_W=\langle W,C_0,C_1,C_2,C_R\rangle$ 属于Type-2密文. 假设 $R=\left\{R^{(1)},R^{(2)},\cdots,R^{(j)}\right\}$, 则 $j\geqslant 1$. 对于 $1\leqslant i\leqslant j$, 解密者计算 $R_W^{(i)}=\mathrm{mRevolndex}\left(\mathrm{PK},W,R^{(i)}\right)$, 令 $R_W^{(k)}=\bigcup_{i=1}^{j}R_W^{(i)}$. 如果 $\mathrm{sn}\in R_W$, 返回 $\perp$. 否则 $\mathrm{sn}\notin R_W$, 解密者计算 $\sigma_W=\prod_{i\in I_W}\overline{\sigma}_i$ 和 $K_R=\dfrac{\hat{e}\left(g_{\mathrm{sn}},C_R\right)}{\hat{e}\left(d\cdot\prod_{i\in I_m-R_W}^{i\neq\mathrm{sn}}g_{m+1-i+\mathrm{sn}},C_1\right)}$, 并返回

$$M=\frac{C_0}{\hat{e}\left(\sigma_W,C_1\right)\cdot\hat{e}\left(H_1\left(\mathrm{sk}\right),C_2\right)\cdot K_R}.$$

Case 3. 密文 $\mathrm{CT}_W=\left\langle W,C_0,C_1,C_2,C_{\hat{R}}\right\rangle$ 属于Type-3密文. 假设 $R^{(N_{\mathrm{now}})}$ 是属性权威中心发布的最新的属性

撤销信息. 对于$1\leqslant i\leqslant N_{\text{now}}$, 解密者计算$R_W^{(i)}=\text{mRevolndex}\left(\text{PK},W,R^{(i)}\right)$, 令$R_W=\bigcup_{i=1}^{N_{\text{now}}}R_W^{(i)}$. 如果$\text{sn}\in R_W$, 返回$\perp$. 否则$\text{sn}\notin R_W$, 计算$\sigma_W=\prod_{i\in I_W}\bar{\sigma}_i$, 返回$M=\dfrac{C_0}{\hat{e}\left(\sigma_W,C_1\right)\cdot\hat{e}\left(H_1(\text{sk}),C_2\right)\cdot K_{\hat{R}}}$, 其中

$$K_{\hat{R}}=\frac{\hat{e}\left(g_{\text{sn}},C_{\hat{R}}\right)}{\prod_{k=1}^{N_{\text{now}}}\hat{e}\left(d\cdot\prod_{i\in I_m-R_W^{(k)}}^{i\neq\text{sn}}g_{m+1-i+\text{sn}},\text{PP}^{(k)}\right)}.$$

Case 4. 密文$\text{CT}_W=\left\langle W,C_0,C_1,C_2,C_R,C_{\hat{R}}\right\rangle$属于Type-4密文. 假设$R^{(N_{\text{now}})}$是属性权威中心发布的最新的属性撤销信息, $R=\left\{R^{(1)},R^{(2)},\cdots,R^{(j)}\right\}$, 则$j\geqslant 1$且$j+1\leqslant N_{\text{now}}$. 对于$1\leqslant i\leqslant N_{\text{now}}$, 解密者计算$R_W^{(i)}=\text{mRevolndex}\left(\text{PK},W,R^{(i)}\right)$, 令$R_W=\bigcup_{i=1}^{j}R_W^{(i)}$, $\hat{R}_W=\bigcup_{i=1}^{N_{\text{now}}}R_W^{(i)}$. 如果$\text{sn}\in\hat{R}_W$, 返回$\perp$. 否则$\text{sn}\notin\hat{R}_W$, 计算$\sigma_W=\prod_{i\in I_W}\bar{\sigma}_i$, 返回消息$M=\dfrac{C_0}{\hat{e}\left(\sigma_W,C_1\right)\cdot\hat{e}\left(H_1(\text{sk}),C_2\right)\cdot K_R\cdot K_{\hat{R}}}$, 其中

$$K_R=\frac{\hat{e}\left(g_{\text{sn}},C_R\right)}{\hat{e}\left(d\cdot\prod_{i\in I_m-\mathcal{R}_W}^{i\neq\text{sn}}g_{m+1-i+\text{sn}},C_1\right)},\ K_{\hat{R}}=\frac{\hat{e}\left(g_{\text{sn}},C_{\hat{R}}\right)}{\prod_{k=1}^{N_{\text{now}}}\hat{e}\left(d\cdot\prod_{i\in I_m-R_W^{(k)}}^{i\neq\text{sn}}g_{m+1-i+\text{sn}},\text{PP}^{(k)}\right)}.$$

4.2 安全性分析

定理 1 假设敌手$A\left(A_{\text{I}},A_{\text{II}}\right)$对随机预言机$H_1$最多进行$q_{H_1}$次询问, 最多进行$q_K$次密钥生成询问. 如果群$G$中判定性$(T,\varepsilon,m)$-BDHE假设成立, 则本文所提出的方案是$(T',\varepsilon,m)$安全的, 其中$T'=T+O\left(q_{H_1}+(m+n)q_K+N\right)T_1+O(N)T_2$, $N=\sum_{i=1}^{n}n_i$, m是系统中用户总数的一个上界, n是属性域的大小, T_1和T_2分别表示群G和G_T中模指数运算的时间复杂性.

证明: 假设存在一个敌手$A\left(A_{\text{I}},A_{\text{II}}\right)$, 在时间$T$内, 攻破本文方案的优势满足$\text{Adv}_{\text{CP-ABE}}^{\text{IND-sCP-CPA}}(A)\geqslant\varepsilon$. 我们可以建立一个模拟者$S$, 它能够以优势$\varepsilon$解决群$G$中的判定性$m$-BDHE问题. S以一个随机的判定性m-BDHE挑战$\left(g,h,\vec{y}_{g,a,m},Z\right)$为输入, 这里$\vec{y}_{g,a,m}=\left(g_1,g_2,\cdots,g_m,g_{m+2},\cdots g_{2m}\right)$, Z要么等于$\hat{e}\left(g_{m+1},h\right)$, 要么是$G_T$中的一个随机元素. S扮演着IND-sCP-CPA游戏中的挑战者, 并与A进行如下交互:

Init. $A\left(A_{\text{I}},A_{\text{II}}\right)$向$S$发送一个挑战策略$W^*=\bigcap_{i\in I_{W^*}}W_i$, 这里$I_{W^*}=\left\{i_1,i_2,\cdots,i_w\right\}(w\leqslant n)$表示$W^*$中所出现的属性的索引. 此外, A_{II}再提交属性撤销信息$R^*=\left\{R^{*(1)},R^{*(2)},\cdots,R^{*(j)}\right\}$和属性撤销列表$R^{*(k)}$, 其中$k\geqslant j+1$. 在游戏中, S回答A发起的随机预言询问. S维护两个表L_1和L_2, 用于存储随机预言询问的答案.

Setup. S需要生成系统公钥PK. S选取$j^*\in_R\{1,2,\cdots,w\}$和$x,x',y,y'\in_R Z_p^*$, 然后执行:

(1) 如果$i_j\in I_{W^*}-\left\{i_{j^*}\right\}$, 假设$W_{i_j}=v_{i_j,k_{i_j}}$, S计算

$$\left(X_{i_j,k_{i_j}},Y_{i_j,k_{i_j}}\right)=\left(g^{-H_0\left(x\|i_j\|k_{i_j}\right)}g_{m+1-i_j}^{-1},\hat{e}(g,g)^{H_0\left(y\|i_j\|k_{i_j}\right)}\right)$$

此外, 对于$k\neq k_{i_j}$, S计算$\left(X_{i_j,k},Y_{i_j,k}\right)=\left(g^{-H_0\left(x'\|i_j\|k\right)},\hat{e}(g,g)^{H_0\left(y'\|i_j\|k\right)}\right)$.

(2) 对于i_{j^*}, 假设$W_{i_{j^*}}=v_{i_{j^*},k_{i_{j^*}}}$, S计算

$$\left(X_{i_{j^*},k_{i_{j^*}}},Y_{i_{j^*},k_{i_{j^*}}}\right)=\left(g^{-H_0\left(x\|i_{j^*}\|k_{i_{j^*}}\right)}\prod_{t\in I_{W^*}-\left\{i_{j^*}\right\}}g_{m+1-t},\hat{e}(g,g)^{H_0\left(y\|i_{j^*}\|k_{i_{j^*}}\right)}\hat{e}(g,g)^{\alpha^{m+1}}\right)$$

此外，对于 $k\neq k_{i_{j^*}}$，S 计算 $\left(X_{i_{j^*},k},Y_{i_{j^*},k}\right)=\left(g^{-H_0\left(x'\|i_{j^*}\|k\right)},\hat{e}(g,g)^{H_0\left(y'\|i_{j^*}\|k\right)}\right)$.

(3) 如果 $i_j\notin I_{W^*}$，对于 $1\leqslant k_{i_j}\leqslant n_{i_j}$，$S$ 计算

$$\left(X_{i_j,k_{i_j}},Y_{i_j,k_{i_j}}\right)=\left(g^{-H_0\left(x\|i_j\|k_{i_j}\right)},\hat{e}(g,g)^{H_0\left(y\|i_j\|k_{i_j}\right)}\right)$$

此外，S 选取 $\beta\in_R Z_p^*$. 如果 $R_{W^*}\neq\varnothing$，令 $v=g^{\beta}\left(\prod_{j\in U^*}g_{m+1-j}\right)^{-1}$，其中 $U^*\subseteq R_{W^*}$ 表示 A_{II} 要挑战的那些被牵涉入撤销事件的用户的索引集. 否则 $R_{W^*}=\varnothing$，令 $v=g^{\beta}$. 最终，系统公开参数

$$\mathrm{PK}=\left\langle g,\left\{X_{i,k_i},Y_{i,k_i}\right\}_{1\leqslant i\leqslant n,1\leqslant k_i\leqslant n_i},\left\{g_i\right\}_{i\in I_{2m}\setminus m+1},v\right\rangle$$

S 发送 PK 给 $A\left(A_{\mathrm{I}},A_{\mathrm{II}}\right)$.

Phase 1. $A\left(A_{\mathrm{I}},A_{\mathrm{II}}\right)$ 发起如下询问:

(1) **Hash Oracle** $O_{H_0}(\cdot)$: 当 A 对“·”进行 H_0 询问，S 首先检查 L_0 中是否含有包含“·”的条目，如果有，就返回以前的取值. 否则，选取 $r\in_R Z_p^*$，把 $\langle\cdot,r\rangle$ 添加到 L_0 中，并返回 r.

(2) **Hash Oracle** $O_{H_1}(\mathrm{sk})$: 当 A 对 sk 进行 H_1 询问，S 首先检查 L_1 中是否含有包含“sk”的条目，如果有，就返回以前的取值. 否则，S 执行如下操作: 如果 sk 对应着密钥生成询问中的一个属性列表 L，S 在 L_1 中添加 $\left\langle\mathrm{sk},g_{i_j}g^z\right\rangle$，并返回 $g_{i_j}g^z$，这里 $z\in_R Z_p^*$，i_j 与 L 对应并满足 $L_{i_j}\notin W_{i_j}$. 否则，S 选取 $i_j\in_R\{1,2,\cdots,n\}$，$z\in_R Z_p^*$，在 L_1 中添加 $\left\langle\mathrm{sk},g_{i_j}g^z\right\rangle$，并返回 $g_{i_j}g^z$.

(3) **KeyGen Oracle** $O_{\mathrm{KeyGen}}(L)$: 假设 A 对 L 进行密钥生成询问，如果 $L\left|\neq W^*\right.$，一定存在 $i_j\in I_{W^*}$ 使得 $L_{i_j}\notin W_{i_j}$. 不失一般性，假设 $L_{i_j}=v_{i_j,\hat{k}_{i_j}}$，$W_{i_j}=v_{i_j,k_{i_j}}$. S 选取 $\mathrm{sk}\in_R Z_p^*$. 此外，S 计算 $\bar{\sigma}_{i_j}=\sigma_{i_j,\hat{k}_{i_j}}=g^{H_0\left(y'\|i_j\|\hat{k}_{i_j}\right)}\left(g_{i_j}g^z\right)^{H_0\left(x'\|i_j\|\hat{k}_{i_j}\right)}$. 对于 $t\neq i_j$，S 选取 $z\in_R Z_p^*$，计算:

Case 1. 如果 $t\in I_{W^*}-\left\{i_{j^*}\right\}$，假设 $L_t=v_{t,k_t}$，S 计算 $\bar{\sigma}_t=\sigma_{t,k_t}=g^{H_0(y\|t\|k_t)}\left(g_{i_j}\right)^{H_0(x\|t\|k_t)}g_{m+1-t+i_j}\left(\bar{X}_t\right)^{-z}$.

Case 2. 如果 $t=i_{j^*}$，假设 $L_{i_{j^*}}=v_{i_{j^*},k_{i_{j^*}}}$，$S$ 计算

$$\bar{\sigma}_{i_{j^*}}=\sigma_{i_{j^*},k_{i_{j^*}}}=g^{H_0\left(y\|i_{j^*}\|k_{i_{j^*}}\right)}\left(g_{i_j}\right)^{H_0\left(x\|i_{j^*}\|k_{i_{j^*}}\right)}\left(\prod_{k\in I_{W^*}-\left\{i_{j^*},i_j\right\}}g_{m+1-k+i_j}^{-1}\right)\left(\bar{X}_{i_{j^*}}\right)^{-z}.$$

Case 3. 如果 $t\notin I_{W^*}$，假设 $L_t=v_{t,k_t}$，S 计算 $\bar{\sigma}_t=\sigma_{t,k_t}=g^{H_0(y\|t\|k_t)}\left(g_{i_j}g^z\right)^{H_0(x\|t\|k_t)}$.

然后，如果 $R_{W^*}\neq\varnothing$，S 计算 $d=g_{\mathrm{sn}}^{\beta}\prod_{j\in U^*}g_{m+1-j+\mathrm{sn}}^{-1}$，显然 $d=\left(g^{\beta}\prod_{j\in U^*}g_{m+1-j}^{-1}\right)^{\left(\alpha^{\mathrm{sn}}\right)}=v^{\left(\alpha^{\mathrm{sn}}\right)}$. 如果 $R_{W^*}=\varnothing$，S 计算 $d=g_{\mathrm{sn}}^{\beta}=v^{\left(\alpha^{\mathrm{sn}}\right)}$. 另一方面，如果 $A=A_{\mathrm{II}}$ 且 $L\left|=W^*\right.$，S 选择 $i_j\in_R I_{W^*}$，并采用上述方

法生成私钥. 最终, S 返回 $\mathrm{SK}_L=\left\langle \mathrm{sn},\mathrm{sk},\{\bar{\sigma}_i\}_{1\leqslant i\leqslant n},d\right\rangle$.

(4) **UKeyGen Oracle** $O_{\mathrm{UKeyGen}}(L)$: A 提交一个属性撤销列表 $R^{(k)}$, S 选取 $\mathrm{uk}^{(k)}\in_R Z_p^*$, 计算 $\mathrm{UK}^{(k)}=\mathrm{uk}^{(k)}\beta$, $\mathrm{PP}^{(k)}=v^{\mathrm{uk}^{(k)}}=g^{\mathrm{UK}^{(k)}}$, 返回 $\mathrm{UK}^{(k)}$ 并公开 $\mathrm{PP}^{(k)}$.

(5) **CTUpate oracle** O_{CTUpdate}: A 提交一个密文 CT_W 和属性撤销列表 $R^{(k)}$. 基于密文更新算法的定义, S 利用 $\mathrm{UK}^{(k)}$ 生成与 $R^{(k)}$ 对应的 CT_W 的更新密文 CT'_W, 并返回 CT'_W 给 A.

Challenge. S 令 $x_{W^*}=\sum_{t\in I_{W^*}}H_0(x\,\|\,t\,\|\,k_t)=\sum_{j=1}^{w}H_0(x\,\|\,i_j\,\|\,k_{i_j})$, $y_{W^*}=\sum_{j=1}^{w}H_0(y\,\|\,i_j\,\|\,k_{i_j})$, 并定义 $\left\langle X_{W^*},Y_{W^*}\right\rangle$ 如下:

$$\begin{cases} X_{W^*}=\bar{X}_{i_{j^*}}\prod_{t\in I_{W^*}-\{i_{t^*}\}}\bar{X}_t=\left(g^{-H_0\left(x\|i_{j^*}\|k_{i_{j^*}}\right)}\prod_{t\in I_{W^*}-\{i_{t^*}\}}g_{m+1-t}\right)\cdot\prod_{t\in I_{W^*}-\{i_{t^*}\}}g^{-H_0(x\|t\|k_t)}g_{m+1-t}^{-1}=g^{-x_{W^*}} \\ Y_{W^*}=\bar{Y}_{i_{j^*}}\prod_{t\in I_{W^*}-\{i_{t^*}\}}\bar{Y}_t=\hat{e}(g,g)^{H_0\left(y\|i_{j^*}\|k_{i_{j^*}}\right)}\hat{e}(g,g)^{\alpha^{m+1}}\cdot\prod_{t\in I_{W^*}-\{i_{t^*}\}}\hat{e}(g,g)^{H_0(y\|t\|k_t)}=\hat{e}(g,g)^{\sum_{j=1}^{w}H_0\left(y\|i_j\|k_{i_j}\right)+\alpha^{m+1}} \end{cases}$$

A 向 S 提交两个等长的消息 M_0 和 M_1. S 选取 $b\in_R\{0,1\}$, 并计算 $C_0^*=M_bY_{W^*}^S=M_bZ\hat{e}(g,h)^{y_{W^*}}$, $C_1^*=h$ 和 $C_2^*=h^{-x_{W^*}}$. 然后, S 生成挑战密文如下:

(1) 对于 A_{I}, $R_{W^*}=\varnothing$, S 返回 $\mathrm{CT}_{W^*}=\left\langle W^*,C_0^*,C_1^*,C_2^*\right\rangle$, 此时 CT_{W^*} 是 Type-1 密文.

(2) 对于 A_{II}, $R_{W^*}\neq\varnothing$, 有三种情况需要考虑:

Case 1. W^* 受到了 R^* 的影响. 在这种情况下, S 计算 $K_{R^*}=Z$, $C_0^*=C_0^*K_{R^*}$, 令

$$C_{R^*}=h^{\beta}=\left(g^{\beta}\right)^s=\left(g^{\beta}\left(\prod_{j\in U^*}g_{m+1-j}\right)^{-1}\left(\prod_{j\in U^*}g_{m+1-j}\right)\right)^s=\left(v\cdot\prod_{j\in U^*}g_{m+1-j}\right)^s.$$

然后, 返回 $\mathrm{CT}_{W^*}=\left\langle W^*,C_0^*,C_1^*,C_2^*,C_{R^*}\right\rangle$, 则 CT_{W^*} 属于 Type-2 密文.

Case 2. W^* 不受 R^* 的影响, 但是受到了 $R^{*(k)}$ 的影响. 在这种情况下, S 令 $\mathrm{CT}'_{W^*}=\left\langle W^*,C_0^*,C_1^*,C_2^*\right\rangle$, 返回 $\mathrm{CT}_{W^*}=\mathrm{CTUpdate}\left(\mathrm{PK},\mathrm{CT}'_{W^*},\mathrm{UK}^{(k)},R^{*(k)}\right)$ 作为挑战密文, 显然 CT_{W^*} 是Type-3密文.

Case 3. W^* 既受到 R^* 的影响, 也受到 $R^{*(k)}$ 的影响. 在这种情况下, 类似于Case 2, S 计算 CT_{W^*} 作为挑战密文, 显然 CT_{W^*} 是Type-4密文.

值得注意的是, 只要 $Z=\hat{e}(g_{m+1},h)$, 则挑战密文 CT_{W^*} 就是 M_b 的一个有效密文. 如果Z是 G_T 中的一个随机元素, 则对于 A 而言, CT_{W^*} 与 b 独立.

Phase 2. 同Phase 1. 此外, A 可以对挑战密文 CT_{W^*} 进行密文更新询问.

Guess: A 输出对 b 的猜测 b'. 如果 $b=b'$, 则 S 输出1, 以表示它在判定性 m-BDHE 游戏中认为 $Z=\hat{e}(g_{m+1},h)$. 否则, 输出0, 以表明Z是 G_T 中的一个随机元素. 所以, 如果 $Z=\hat{e}(g_{m+1},h)$, 则 CT_{W^*} 是一个有效的密文, 从而

$$\Pr\left[S\left(g,h,\vec{y}_{g,\alpha,n},\hat{e}(g_{m+1},h)\right)=1\right]=\frac{1}{2}+\mathrm{Adv}_{\text{CP-ABE}}^{\text{IND-sCP-CPA}}(A)\geqslant\frac{1}{2}+\varepsilon.$$

如果 Z 是 G_T 中的一个随机元素, 则 M_b 对 A 完全隐藏, 因此 $\Pr\left[S\left(g,h,\vec{y}_{g,\alpha,m},Z\right)=1\right]=1/2$. 所以, 在求解判定性 m-BDHE 问题的过程中, S 的优势至少为 ε. 很容易得到其所需时间 T 满足

$$T' = T + O\left(q_{H_1} + (m+n)q_K + \sum_{i=1}^{n} n_i\right)T_1 + O\left(\sum_{i=1}^{n} n_i\right)T_2$$

5 性能分析

关于密文长度恒定的CP-ABE方案和支持属性撤销的CP-ABE方案已有不少研究. 我们对这些方案与新方案进行了性能比较. 如表 4 所示, 性能分析的指标包括密文长度$|\mathrm{CT}|$, 属性私钥的大小$|\mathrm{SK}|$, 系统公开参数的大小$|\mathrm{PK}|$, 解密过程的计算量, 属性撤销机制, 是否适用于云计算环境, 以及访问策略的灵活性. 其中, L_0和L_1分别表示群G和G_T中一个元素的比特长度, L_k表示用户的属性私钥对应的属性集的比特大小, L_{kek}表示密钥加密密钥的比特长度[29], k表示用户所拥有的属性个数, m表示系统中用户的最大数目, n表示属性域中的属性总个数, r表示撤销事件的数目, t表示访问策略中出现的属性的个数, N表示系统中属性取值的总数. 此外, $k_{\max}$和$t_{\max}$分别表示k和t所能取的最大值[31], 符号"/"表示不关注此项, Tree表示树结构的访问策略, LSSS表示基于线性秘密分享(linear secret sharing scheme)的矩阵结构的访问策略.

表 4 CP-ABE 方案的性能比较
Table 4 Performance comparison of CP-ABE schemes

方案	参数大小 (bit)			解密代价	属性撤销机制		云计算	访问策略
	$\|\mathrm{CT}\|$	$\|\mathrm{SK}\|$	$\|\mathrm{PK}\|$	(pairing)	间接	直接		
[23]	$2L_0+L_1$	$(2n+1)L_0$	$(2n+1)L_0$	2k+1	×	×	√	$\mathrm{AND}^*_{+,-}$
[18,19]	$2L_0+L_1$	$2L_0$	$(N+2)L_0+L_1$	2	×	×	√	AND_m
[20]	$2L_0+L_1$	$2L_0$	$(N+2)L_0+L_1$	2	×	×	√	AND_m
[22]	$2L_0+L_1$	$(n+1)L_0$	nL_0+nL_1	2	×	×	√	$\mathrm{AND}^*_{+,-}$
[4]	$2(t+1)L_0+L_1$	$(2k+1)L_0+L_{\mathrm{kek}}$	L_0+L_1	2k+1	√	×	√	Tree
[28]	$(n+1)L_0+L_1$	$(2n+1)L_0+L_k$	$(3n+1)L_0+L_1$	n+1	√	×	√	$\mathrm{AND}^*_{+,-}$
[29]	$2(t+1)L_0+L_1$	$(2k+1)L_0+(\log m)L_{\mathrm{kek}}$	L_0+L_1	2k+1	√	×	√	Tree
[31] 1	$(t+2)L_0+L_1$	$(k+2)L_0$	$(k_{\max}+t_{\max}+2m+1)L_0$	2t+m+1	/	×	×	LSSS
[31] 2	$(t+2r+1)L_0+L_1$	$(k+4)L_0$	$(k_{\max}+t_{\max}+7)L_0+L_1$	2t+2r+1	/	×	×	LSSS
[35]	$(6t+1)L_0+L_1$	$(k+1)L_0$	$(2m+2n+1)L_0$	6r	/	√	×	LSSS
[3]	$\leqslant 4L_0+L_1$	$(n+2)L_0+\log m$	$(2m+4n+1)L_0$	r+2	/	√	√	$\mathrm{AND}^*_{+,-}$
新方案	$\leqslant 4L_0+L_1$	$(n+1)L_0+\log m+\|Z_p^*\|$	$(2m+N+1)L_0$	r+2	/	√	√	AND^*_m

从表 4 可以看出, 在已有的结果中, 方案[3,18–20,22–23]具有恒定大小的密文, 然而只有方案[3]支持属性撤销机制. 此外, 方案[18–20]的AND策略不支持通配符. 方案[4,28,29]仅仅实现了间接的属性撤销机制, 而且密文长度会随着访问策略的复杂性或者属性域的大小线性增长. 方案[31]仅仅实现了直接的用户撤销机制, 无法实现细粒度的属性撤销机制. 方案[3,35]实现了直接的细粒度属性撤销机制. 此外, 方案[31,35]的密文长度会随着访问策略的复杂性和属性撤销事件的数目线性增长, 其属性撤销机制也不适用于云计算环境. 方案[35]的解密代价本质上是与属性撤销事件的次数相关联的. 事实上, 方案[31,35]的属性撤销机制的实施完全依赖于数据拥有者, 因此当撤销事件发生时, 并不能保证已经存储到云平台上的数据的安全性. 尽管拥有恒定的计算量, 而且支持适用于云计算的直接的属性撤销机制, 方案[3]仅仅支持策略

$\mathrm{AND}^{*}_{+,-}$. 新方案在保证密文长度恒定并实现直接的属性撤销机制的同时, 可以支持 AND^{*}_{m} 策略. 与方案[3]类似, 新方案的一个不足之处是, 云存储服务器需要执行部分计算任务. 根据引言部分的分析, AND^{*}_{m} 比 $\mathrm{AND}^{*}_{+,-}$ 更加实用. 因此, 总的来看, 新方案更加适用于用户属性变化频繁且带宽资源受限的实际应用.

6 结论

本文构造了一个密文长度恒定的 CP-ABE 方案, 并且在随机预言机模型中证明了新方案是安全的. 所提出的方案支持具有多个属性取值和通配符的 AND 策略 AND^{*}_{m}, 提供了直接的属性撤销机制. 性能分析表明, 新方案特别适用于用户属性变化频繁且带宽资源受限的应用环境.

References

[1] Sahai A, Waters B. Fuzzy identity-based encryption[C]. In: Advances in Cryptology—EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457–473.

[2] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]. In: Proceedings of the 2006 ACM Conference on Computer and Communications Security—CCS 2006. ACM, 2006: 89–98.

[3] Zhang Y H, Chen X F, Li J, et al. FDR-ABE: attribute-based encryption with flexible and direct revocation[C]. In Proceedings of the 2013 International Conference on Intelligent Networking and Collaborative Systems—INCoS 2013. IEEE, 2013: 38–45.

[4] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]. In Proceedings of the 2007 IEEE Symposium on Security and Privacy—SP 2007. IEEE, 2007: 321–334.

[5] Cheung L, Newport C. Provably secure ciphertext policy ABE[C]. In: Proceedings of the 2007 ACM Conference on Computer and Communications Security—CCS 2007. ACM, 2007: 456–465.

[6] Chase M. Multi-authority attribute based encryption[C]. In Proceedings of the 2013 Theory of Cryptography Conference—TCC 2007. Springer Berlin Heidelberg, 2007: 515–534.

[7] Liu Z, Cao Z F, Huang Q, et al. Fully secure multi-authority ciphertext-policy attribute-based encryption without random[C]. In Proceedings of the 2011 European Symposium on Research in Computer Security—ESORICS 2011. Springer Berlin Heidelberg, 2011: 278–297.

[8] Lewko A, Waters B. Decentralizing attribute-based encryption[C]. In: Advances in Cryptology—EUROCRYPT 2011. Springer Berlin Heidelberg, 2011: 568–588.

[9] Li J, Ren K, Zhu B, et al. Privacy-aware attribute-based encryption with user accountability[C]. In Proceedings of the 2009 International Conference on Information Security—ISC 2009. Springer Berlin Heidelberg, 2009: 347–362.

[10] 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]. In: Proceedings of the 2013 ACM Conference on Computer and Communications Security—CCS 2013. ACM, 2013: 475–486.

[11] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[C]. In: Advances in Cryptology—EUROCRYPT 2008. Springer Berlin Heidelberg, 2008: 146–162.

[12] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]. In Proceedings of the 2008 International Conference on Applied Cryptography and Network Security—ACNS 2008. Springer Berlin Heidelberg, 2008: 111–129.

[13] Lai J Z, Deng R H, Li Y J. Expressive CP-ABE with partially hidden access structures[C]. In: Proceedings of the 2012 ACM Symposium on Information, Computer and Communication Security—ASIACCS 2012. ACM, 2012: 18–19.

[14] Zhang Y H, Chen X F, Li J, et al. Anonymous attribute-based encryption supporting efficient decryption test[C]. In: Proceedings of the 2013 ACM Symposium on Information, Computer and Communication Security—ASIACCS 2013. ACM, 2013: 511–516.

[15] Green M, Hohenberger S, Waters B. Outsourcing the decryption of abe ciphertexts[C/OL]. In: USENIX Security Symposium 2011. http://static.usenix.org/events/sec11/tech/full_papers/Green.pdf.

[16] Lai J Z, Deng R H, Guan C W, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343–1354.

[17] Li J, Chen X F, Li J W, et al. Fine-grained access control system based on outsourced attribute-based encryption[C]. In Proceedings of the 2013 European Symposium on Research in Computer Security—ESORICS 2013. Springer Berlin Heidelberg, 2013: 592–609.

[18] Emura K, Miyaji A, Nomura A. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]. In Proceedings of the 2009 International Conference on Information Security Practice and Experience—ISPEC 2009. Springer Berlin Heidelberg, 2009: 13–23.

[19] Emura K, Miyaji A, Omote K, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[J].

International Journal of Applied Cryptography, 2010, 2(1): 46–59.

[20] Rao Y, Dutta R. Recipient anonymous ciphertext-policy attribute based encryption[C]. In Proceedings of the 2013 International Conference on Information Systems Security—ICISS 2013. Springer Berlin Heidelberg, 2013: 329–344.

[21] Han J G, Susilo W, Mu Y, et al. Attribute-based oblivious access control[J]. The Computer Journal, 2012, 55(10): 1202–1215.

[22] Chen C, Zhang Z F, Feng D G. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost[C]. In Proceedings of the 2011 International Conference on Provable Security—ProvSec 2011. Springer Berlin Heidelberg, 2011: 84–101.

[23] Zhou Z B, Huang D J, Wang Z J. Efficient privacy-preserving ciphertext-policy attribute based encryption and broadcast encryption[J]. IEEE Transactions on Computers, 2013, DOI:10.1109/TC.2013.200.

[24] Herranz J, Laguillaumie F, Ràfols C. Constant size ciphertexts in threshold attribute-based encryption[C]. In Proceedings of the 2010 International Conference on Practice and Theory in Public Key Cryptography—PKC 2010. Springer Berlin Heidelberg, 2010: 19–34.

[25] Ge A J, Zhang R, Chen C, et al. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts[C]. In Proceedings of the 2012 Australasian Conference Information Security and Privacy—ACISP 2012. Springer Berlin Heidelberg, 2012: 336–349.

[26] Attrapadung N, Libert B. Functional encryption for inner product: achieving constant-size ciphertexts with adaptive security or support for negation[C]. In Proceedings of the 2010 International Conference on Practice and Theory in Public Key Cryptography—PKC 2010. Springer Berlin Heidelberg, 2010: 384–402.

[27] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation[C]. In Proceedings of the 2008 ACM Conference on Computer and Communications Security—CCS 2008. ACM, 2008: 417–426.

[28] Yu S C, Wang C, Ren K, et al. Attribute based data sharing with attribute revocation[C]. In: Proceedings of the 2010 ACM Symposium on Information, Computer and Communication Security—ASIACCS 2010. ACM, 2010: 261–270.

[29] 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, 22(7): 1214–1221.

[30] Cheng Y, Wang Z Y, Ma J, et al. Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage[J]. Journal of Zhejiang University-SCIENCE C, 2013, 14(2): 85–97.

[31] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys[C]. In: Advances in Cryptology—CRYPTO 2005. Springer Berlin Heidelberg, 2005: 258–275.

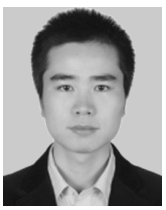
[32] Wang P P, Feng D G, Zhang L W. Towards attribute revocation in key-policy attribute based encryption[C]. In Proceedings of the 2011 International Conference on Cryptology and Network Security—CANS 2011. Springer Berlin Heidelberg, 2011: 272–291.

[33] 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.
王鹏翩, 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.

[34] Attrapadung N, Imai H. Conjunctive broadcast and attribute-based encryption[C]. In Proceedings of the 2009 International Conference on Pairing-Based Cryptography—Pairing 2009. Springer Berlin Heidelberg, 2009: 248–265.

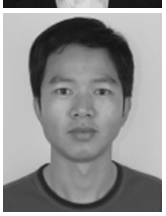
[35] Fiat A, Naor M. Broadcast encryption[C]. In: Advances in Cryptology—CRYPTO '93. Springer Berlin Heidelberg, 1993: 480–491.

作者信息



张应辉(1985–), 博士, 讲师. 主要研究领域为公钥密码学、云存储安全、无线网络安全.
E-mail: yhzhaang@163.com

郑东(1964–), 博士, 教授. 主要研究领域为基于编码的密码学、云存储安全.
E-mail: zhengdong@xupt.edu.cn



李进(1981–), 博士, 教授. 主要研究领域为公钥密码学、云计算安全.
E-mail: jinli71@gmail.com

李晖(1968–), 博士, 教授. 主要研究领域为密码学、信息与编码理论、云计算安全.
E-mail: lihui@mail.xidian.edu.cn