软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(9):2760−2771 [doi: 10.13328/j.cnki.jos.005420]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

支持细粒度属性直接撤销的 CP-ABE 方案*

张文芳[1,2], 陈 桢[1,2], 刘旭东[1,2], 王小敏[1]

[1](西南交通大学 信息科学与技术学院,四川 成都 611756)

[2](信息安全与国家计算网格实验室(西南交通大学),四川 成都 611756)

通讯作者: 王小敏, E-mail: xmwang@swjtu.edu.cn

摘 要: 为了解决用户属性变化带来的权限访问控制问题,支持属性撤销的基于属性加密方案被提出.然而,现有的属性撤销机制大多存在撤销代价大、撤销粒度粗等问题,且已有的方案均存在安全隐患,即属性授权中心可以伪装成任意用户解密密文.为弥补上述不足,提出一种支持细粒度属性直接撤销的密文策略的基于属性加密方案(CP-ABE),并给出该方案的形式化定义与安全模型.所提方案中,用于生成用户密钥的秘密参数由系统中心和属性授权机构分别产生,可避免属性授权中心解密密文的安全隐患.同时,通过引入多属性授权中心进一步降低了安全风险.在属性撤销方面,通过设计高效的重加密算法并引入属性撤销列表,实现细粒度的属性直接撤销.安全证明和性能分析表明:所提方案在适应性选择密文攻击下具有不可区分性并能抵抗不可信授权中心的破译攻击,较同类方案具有更高的计算效率以及更细的属性撤销粒度.

关键词: 基于属性加密;密文策略;属性直接撤销;重加密;适应性选择密文攻击

中图法分类号: TP309

中文引用格式: 张文芳,陈桢,刘旭东,王小敏.支持细粒度属性直接撤销的 CP-ABE 方案.软件学报,2019,30(9):2760−2771. http://www.jos.org.cn/1000-9825/5420.htm

英文引用格式: Zhang WF, Chen Z, Liu XD, Wang XM. CP-ABE scheme supporting fine-grained attribute direct revocation. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2760−2771 (in Chinese). http://www.jos.org.cn/1000-9825/5420.htm

CP-ABE Scheme Supporting Fine-grained Attribute Direct Revocation

ZHANG Wen-Fang[1,2], CHEN Zhen[1,2], LIU Xu-Dong[1,2], WANG Xiao-Min[1]

[1](School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

[2](Laboratory of Information Science and National Computing Grid (Southwest Jiaotong University), Chengdu 610031, China)

Abstract: In the attribute-based cryptosystems, user's identity is extended as a set of attributes. In order to solve the access control problem caused by the change of users' attributes, attribute-based encryption (ABE) schemes with attribute revocation were proposed. However, there are some problems like high revocation cost or coarse-grained revocation in most of the existing ABE schemes. Besides, the attribute key escrow problem is serious, that is the attribute authority can impersonate any user to decrypt the ciphertexts since the user's attribute private key is generated by the attribute authority himself. In order to remedy the above mentioned problems, the study proposes a ciphertext-policy attribute-based scheme supporting fine-grained attribute direct revocation, whose formal definition and security model are also presented. In the proposal, user's attribute private key is generated by the system authority and multiple attribute authorities jointly, so that each attribute authority's privilege can be effectively limited. Furthermore, the proposal constructs an efficient re-encryption method based on the access tree, which, together with the attribute revocation list, can be used to realize fine-grained

* 基金项目: 国家自然科学基金(61872302); 四川省科技计划(2017GZDZX0002, 2018GZ0195, 2017SZYZF0002, 2019YFH0097); 国家铁路智能运输系统工程技术中心开放课题(RITS2018KF02)

Foundation item: National Natural Science Foundation of China (61872302); Sichuan Science and Technology Program (2017GZDZX0002, 2018GZ0195, 2017SZYZF0002, 2019YFH0097); Project Fund for the Center of National Railway Intelligent Transportation System Engineering and Technology (RITS2018KF02)

收稿时间: 2017-01-22; 修改时间: 2017-08-24; 采用时间: 2017-09-16

attribute direct revocation with low revocation cost. By the formal security proof, the proposal is proven to have the characteristics of indistinguish ability under the adaptive chosen cipher-text attack and can protect the system from being attacked by the incredible authority. Compared to the similar schemes, the proposal can achieve higher computation efficiency and finer-grained attribute direct revocation.

Key words: attribute-based encryption; ciphertext-policy; attribute direct revocation; re-encryption; adaptive chosen cipher-text attack

随着分布式存储与计算技术(如云存储和云计算)的迅速发展与成熟,研究具备匿名性特点的密码机制变得尤为重要.Sahai 和 Waters[1]将基于身份的加密算法加以扩展和改进,提出了基于模糊身份的加密方案.该方案首次引入属性的概念,用属性集合表示用户,以实现对其的匿名性保护;同时,基于特定的访问结构对数据进行加密,只有用户属性满足访问结构时,才能成功解密密文.在此基础上,相关学者展开了一系列基于属性的密码机制研究[2−4],并根据访问策略嵌入位置的不同,将属性基加密算法分为密文策略和密钥策略两类:密钥策略的属性基加密方案(key-policy attribute-based encryption,简称 KP-ABE)[2]将解密策略与用户的私钥绑定,密文策略的属性基加密方案(ciphertext-policy attribute-based encryption,简称 CP-ABE)[3]则将密文与解密策略绑定.

属性基加密方案使用属性集合来描述用户,然而在实际应用中,不同的用户往往具有部分相同的属性,而且这些属性存在属性到期、密钥泄露、属性变更等问题.因此,属性撤销成为属性基加密方案中亟需解决的问题,即:在用户属性变更时,如何及时更新用户权限,确保用户不能使用旧密钥解密密文.其中研究的难点在于在对某一用户的属性进行撤销时,不影响系统中拥有该属性的其他用户.此前,大多数的 ABE 方案[5−8]主要关注访问策略的表达能力,并未着重考虑属性撤销问题.2009 年,Attrapadung 等人[9,10]在已有 ABE 方案的基础上,结合基于身份的组播加密技术[11]与线性秘密共享(LSSS)技术[12],提出了 ABE 方案的两种撤销模式:间接撤销和直接撤销.

- 间接撤销由授权机构执行,采用半可信仲裁者方式或在密钥中加入时间信息,通过周期性地更换密钥实现属性撤销.目前的大多数方案都采用间接撤销[13−15],其优势在于加密时不需要获取撤销列表,使用比较灵活.但间接撤销的撤销代价比较大,且需要授权中心进行密钥更新,容易形成系统瓶颈;
- 在直接撤销模式下,发送方将撤销列表直接嵌入到密文中完成用户属性的撤销,因此不影响其他用户,但存在撤销粒度较粗的问题.而方案[10,16–18]只能解决用户撤销问题,即撤销某用户的所有权限,但不能针对部分权限进行修改,因此同样无法实现细粒度的属性撤销.

为了实现细粒度的属性直接撤销,学者们先后提出了一系列改进方案[19−24].Hur[19]采用二叉树方法,提出了一种支持属性直接撤销的 CP-ABE 方案.然而,该方案缺乏严格的安全模型和安全性证明,并且无法抵抗合谋攻击.王鹏翩等人[20]通过为用户分配两个访问树的方法实现了属性的细粒度撤销,但该方案只能在密文中嵌入一个属性的撤销信息,无法满足属性变化频繁的实际应用需求.文献[21]中,Ibraimi 等人通过半可信第三方持有部分密钥与撤销列表的方式实现属性的即时撤销,但需要确保第三方的高度可信与实时在线.上述所有支持撤销的属性基加密方案不仅在属性撤销上存在或多或少的不足,更普遍存在一个安全隐患:属性授权中心掌握所有用户的私钥,因此可以伪装成任意一名用户解密密文[25].一旦授权中心被攻破,用户存储在云端的加密信息即可被非法获取并使用.

本文针对现有方案的不足,提出一种抗不可信授权中心破译攻击的支持细粒度属性直接撤销的 CP-ABE 方案.该方案采用访问树结构实现访问策略,当用户属性满足访问树判别条件时,即可解密密文.针对不可信授权中心的问题,本方案中用于生成用户私钥的秘密参数β和 t_j 分别由系统中心 SA(system authority)和属性授权机构 AA(attribute of authority)产生,从而约束了不可信授权中心的攻击能力,有效避免了密文破译攻击.在属性撤销方面,本方案采用属性授权中心实时更新属性撤销名单,并结合密文重加密的方式,可以对任意用户的任意属性单独进行撤销,而不影响其他用户,以确保属性的细粒度撤销.同时,通过在密文中嵌入与用户撤销属性相关的秘密信息,产生与属性撤销名单一一对应的密文,保证密文只能够被有效用户解密.与 Attrapadung 方案[10]相比,本文方案能够实现细粒度的属性直接撤销.本文对属性可直接撤销的 CP-ABE 方案进行了严格的形式化安全定义,并在随机预言机模型下证明所提方案在适应性选择密文攻击下具备密文不可区分性,并能抵抗不可

信授权中心的破译攻击.性能分析表明:本文方案在保证更细的撤销粒度和系统安全性前提下,算法效率也具有一定的优势.

本文第 1 节介绍相关的预备知识.第 2 节给出属性可直接撤销的 CP-ABE 方案及其安全性的形式化定义.第 3 节提出支持细粒度属性直接撤销的 CP-ABE 方案.第 4 节从正确性、安全性、效率等 3 个方面对所提方案进行证明和分析.最后对全文进行总结.

1 预备知识

本节给出基于属性加密方案的相关定义与困难问题假设.

1.1 拉格朗日插值法

若已知 $f(x)$在互不相同的 d 处的函数值,即函数过 d 个已知的点,那么能够构造出 $d-1$ 阶的 x 的多项式函数 $f(x)$,且此 $f(x)$是存在且唯一确定的,其求解方法如下:

$$f(x)=\sum_{i=1}^{d} f(x_i)\left(\prod_{j=1,j\neq i}^{d}\frac{x-x_j}{x_i-x_j}\right) \tag{1}$$

称公式(1)为拉格朗日插值多项式.

1.2 访问树

访问树是访问结构的一种表达形式,不仅支持门限方式的访问策略,也支持表达“与”、“或”等逻辑运算.为方便表述,对于访问树中的任意节点 x,有如下定义.

- $Parent(x)$:节点 x 的父节点,对根节点 $root$ 外的所有节点有效;
- $Children(x)$:节点 x 的子节点集合;
- $Num(x)$:节点 x 的子节点个数;
- $index(x)$:节点 x 在同一层次节点中的序号,即为其父节点的子节点集合中的编号;
- $attr(x)$:节点 x 表征的属性,当且仅当 x 为叶子节点时有效.

访问树中的每一个非叶子节点都表征一个门限,门限值 n_x 满足 $1\leqslant n_x\leqslant Mum(x)$.“或”门的门限值 $n_x=1$,“与”门的门限值 $n_x=Num(x)$.

定义 2(访问结构(access structure)). 令参与方集合为 $P=\{P_1,P_2,\ldots,P_n\}$,访问结构 A 是 2^P 的一个非空集合.访问结构 A 中的集合称为授权集合,不在访问结构 A 中的集合称为非授权集合.

1.3 困难问题假设

定义 3(判定性 q-BDHE 假设(decision q bilinear Diffie-Hellman exponent assumption)). 设群 G_1,G_2 是 p 阶循环群,双线性映射 $e:G_1\times G_1\rightarrow G_2$,给定随机生成元 g,随机数 $s,a\in Z_p$,计算:

$$Y=(g,g^s,g^a,g^{(a^2)},\ldots,g^{(a^n)},g^{(a^{n+2})},\ldots,g^{(a^{2n})}).$$

给定随机数 $V\in_R G_2$,若不存在有效算法 C 能够在多项式时间内以不可忽略的优势区分 V 与 $e(g,g)^{a^{n+1}s}$,则假设成立.

定义 4(DDH 问题假设(decision Diffie-Hellman problem)). 设群 G_1,G_2 是 p 阶循环群,双线性映射 $e:G_1\times G_1\rightarrow G_2$,随机生成元为 g,随机数 $x,y,z\in Z_p$,给定元组$\langle g,g^x,g^y,g^{xy}\rangle$和$\langle g,g^x,g^y,g^z\rangle$,若不存在有效算法 C 能够在多项式时间内以不可忽略的优势判断 z 是否等于 $xy \bmod p$,则假设成立.

2 算法形式化定义与安全模型

2.1 形式化定义

本节给出可撤销的密文策略属性基加密方案的形式化定义.CP-ABE 方案中,密文与断言$(\Gamma,term)$相关联,其

中,Γ代表属性集合,Φ代表满足 *term* 的Γ的非空子集.假设ω为解密者的属性集合,只有存在$\omega'\in\Phi$使得$\omega'\subseteq\omega$,解密者才能成功解密密文.

直接可撤销的密文策略的基于属性加密(CP-ABE)方案涉及 3 个实体:系统中心、属性授权机构、用户,由以下 6 个算法构成.

(1) 初始化算法 $Setup(1^{\lambda})\rightarrow(PK,MK)$:由系统中心运行的概率性随机算法,输入安全参数 1^{λ},系统中心输出公开参数 *PK* 和系统主密钥 *MK*;

(2) 密钥生成算法 $KeyGen(ID,\omega,MK)\rightarrow SK_{ID,\omega}$:由属性授权机构运行的概率性随机算法,输入 *MK*、用户的身份 *ID* 及其属性集合ω,属性授权机构输出用户的私钥 $SK_{ID,\omega}$;

(3) 加密算法 $Encrypt(\Gamma_{\omega^*},M,R,PK)\rightarrow CT$:由数据拥有者运行的一个概率性随机算法,输入系统公开参数 *PK*、明文消息 *M*、访问策略 Γ_{ω^*} 和属性撤销信息 *R*,输出密文 *CT*;

(4) 重加密算法 $ReEncrypt(\Gamma_{\omega^*},M,R,PK)\rightarrow CT$:由系统中心运行的概率性随机算法,输入系统公开参数 *PK*、密文 *CT*、访问策略 Γ_{ω^*} 和属性撤销信息 *R*,输出新密文 *CT*;

(5) 解密算法 $Decrypt(\Gamma_{\omega^*},SK_{ID,\omega},CT,R)\rightarrow M$:由解密者运行的一个确定性算法,输入私钥 $SK_{ID,\omega}$、与访问策略 Γ_{ω^*} 对应的密文 *CT* 和属性撤销信息 *R*,如果 $\Gamma_{\omega^*}(\omega)=1$,且 $SK_{ID,\omega}$不涉及 *R* 中的撤销事件时,则输出明文消息 *M*,否则输出错误符号$\perp$;

(6) 撤销算法 $Revocation(MK,ID_k,\lambda_k,attr(j))\rightarrow R$:由属性授权机构运行的确定性算法,输入待撤销属性 $attr(j)$及用户 ID_k,输出属性撤销信息 *R*.

2.2 安全模型

在此给出适用于本文算法的安全特性的形式化定义.

定义 5. 一个基于属性的加密方案$\Pi=(Set,KGen,Rev,Enc,ReE,Dec)$在选择密文攻击下是不可区分的,如果没有概率多项式时间的敌手 *A* 以一个不可忽略的优势ε在以下游戏中获胜.

(1) 初始化:挑战者 *C* 运行初始化算法,利用系统安全参数产生公共参数 *PK* 和主密钥 *MK*.如果敌手 *A* 为恶意系统中心 SA,*C* 将 *PK* 和秘密参数$\langle\alpha,\beta,\lambda_i\rangle$发送给 *A*,*MK* 保密;如果敌手 *A* 为恶意属性授权机构 AA_k,*C* 将 *PK*,*MK* 和秘密参数α发送给 *A*,秘密参数$\langle\beta,\lambda_i\rangle$保密.敌手 *A* 输出挑战访问策略 Γ_{ω^*} 和属性撤销列表 *R*;

(2) 阶段 1:敌手 *A* 适应性地执行一系列预言机询问.

a) 私钥解析询问:选择用户 ID_i 及其属性集ω_i,向 *C* 询问对应用户的私钥,要求 $ID_i\in R$ 或ω_i 不满足访问策略 Γ_{ω^*},*C* 运行 *KeyGen* 算法产生私钥 SK_{ω_i},并将 SK_{ω_i} 发送给 *A*;

b) 密文解析询问:选择密文 *CT*,向 *C* 询问在访问策略 Γ_{ω^*} 下 *CT* 对应的明文 *M*,*C* 运行 *Decrypt* 算法恢复出明文 *M*,并发送给 *A*;

(3) 挑战:敌手 *A* 选择两条长度相等的明文 M_0,M_1 发送给挑战者.挑战者 *C* 随机选取 $b\in\{0,1\}$,运行 $Encrypt(\Gamma_{\omega^*},M_b,R,PK)$算法,生成消息 M_b 在访问策略 Γ_{ω^*} 下的询问密文 CT^*,并返回结果给 *A*;

(4) 阶段 2:如阶段 1 所示,*A* 继续执行私钥解析询问和密文解析询问;

(5) 猜测:敌手 *A* 输出对 *b* 的猜测 *b*′.如果满足以下条件,则敌手 *A* 在游戏中获胜.

i) $b'=b$;

ii) *A* 未对$(\Gamma_{\omega^*},CT^*,R)$进行密文解析询问.

定义 6. 一个基于属性的加密方案$\Pi=(Set,KGen,Rev,Enc,ReE,Dec)$能够抵抗不可信授权中心的破译攻击,如果没有概率多项式时间的敌手 *A* 以一个不可忽略的优势ε在以下游戏中获胜.

(1) 初始化:挑战者 *C* 运行初始化算法,利用系统安全参数产生公共参数 *PK* 和主密钥 *MK*.如果敌手 *A* 为恶意系统中心 SA,*C* 将 *PK* 和秘密参数$\langle\alpha,\beta,\lambda_i\rangle$发送给 *A*,*MK* 保密;如果敌手 *A* 为恶意属性授权机构

AA_k,C 将 PK,MK 和秘密参数α发送给 A,秘密参数$\langle\beta,\lambda_i\rangle$保密.敌手 A 输出挑战访问策略 Γ_{ω^*} 和属性撤销列表 R;

(2) 阶段 1:敌手 A 适应性地执行一系列预言机询问.

a) 私钥解析询问:选择用户 ID_i 及其属性集ω_i,向 C 询问对应用户的私钥,要求 $ID_i\in R$ 或ω_i 不满足访问策略 Γ_{ω^*},C 运行 $KeyGen$ 算法产生私钥 SK_{ω_i},并将 SK_{ω_i} 发送给 A;

b) 密文解析询问:选择密文 CT,向 C 询问在访问策略 Γ_{ω^*} 下 CT 对应的明文 M,C 运行 $Decrypt$ 算法恢复出明文 M,并发送给 A;

(3) 挑战:C 运行 $Encrypt(\Gamma_{\omega^*},M^*,R,PK)$算法生成消息 M^*在访问策略 Γ_{ω^*} 下的密文 CT^*,并返回结果给 A;

(4) 阶段 2:如阶段 1 所示,A 继续执行私钥解析询问与密文解析询问;

(5) 攻击:游戏最后,A 输出消息 M',如果满足以下条件,则 A 在游戏中获胜.

i) $M'=M^*$;

ii) A 未对$(\Gamma_{\omega^*},CT^*,R)$进行密文解析询问.

3 细粒度属性直接可撤销的 CP-ABE 加密方案

本文在 Attrapadung 等人方案[10]的基础上,提出一种属性可直接撤销的 CP-ABE 方案,所提 CP-ABE 方案支持加密方定制访问树结构.方案由初始化、密钥生成、属性撤销、加密、重加密、解密这 6 个阶段组成.

3.1 初始化$Setup(1^\lambda)$

系统中心 SA(system authority)选择一个双线性映射 $e:G_1\times G_1\to G_2$,其中,G_1,G_2 是两个 q 阶循环群.然后,选取生成元 $g,h,v\in G_1$,随机数$\alpha,\beta\in Z_q$,并且计算 $Z=e(g,g)^{\beta},v^{\beta}$.最后输出系统公开参数 $PK=\langle g,v^{\beta},e,Z,q\rangle$.对于系统中的每一名认证用户 ID_i,SA 选取唯一的秘密参数$\lambda_i\in Z_q$,通过安全信道发送λ_i,β至用户,发送α,h 至各个属性授权机构 AA_k,其中,$k\in\{1,...,n\}$为各属性属权机构的编号,n 为系统中属性授权机构的数量.

定义属性域 U,U 中的元素为属性映射的整数(mod q).对于任意属性 $j\in U$,若属性授权机构 AA_k 拥有其密钥分发权限,即 $j\in AA_k$,则 AA_k 选择秘密随机数 $t_j\in Z_q^*$,计算 $T_j=g^{t_j}$.最后输出属性公钥 $PK=\langle\{T_j\}_{j\in AA_k}\rangle_{k\in\{1,2,...,n\}}$、属性私钥 $MK=\langle\{t_j\}_{j\in AA_k}\rangle_{k\in\{1,2,...,n\}}$.

3.2 密钥生成$KeyGen(\lambda_i,\omega,MK)$

具有属性集ω的用户 ID_i 向属性授权机构 AA_k 发送λ_i 并申请对应私钥,AA_k 针对任意属性 $j\in\omega\cap AA_k$,计算:

$$S_{i,j}=g^{\frac{\alpha\lambda_i}{t_j}}h^{\frac{\alpha}{t_j}},W_i=g^{\alpha\lambda_i}.$$

用户 ID_i 收到 $S_{i,j},W_i$ 后,计算 $W_i^*=W_i\cdot g^{-\beta}=g^{\alpha\lambda_i-\beta}$.最终用户 ID_i 的私钥为 $SK_{ID_i,\omega}=\langle\lambda_i,W_i^*,S_{i,1},...,S_{i,|\omega|}\rangle$.

在此过程中,由于各属性授权机构 AA_k 无法得到秘密参数β,而系统中心 SA 无法获取属性私钥 t_j 的信息,因此可以确保不可信的属性授权机构和系统中心均无法解密用户密文.

3.3 属性撤销$Revocation(MK,ID_k,\lambda_k,attr(j))$

各属性授权中心 AA_k 公开维护一个用户属性撤销列表 R_k.

当用户 ID_{rev} 的属性 $attr(j)$被撤销时,将λ_{rev} 加入属性 $attr(j)$的撤销列表 $List_{attr(j)}$中并计算 $\{L_{attr(j),rev}=g^{\alpha\lambda_{rev}}v^{\beta t_j}h^{\alpha}\}$,最终将属性 $attr(j)$的相关撤销信息 $(attr(j),\{\lambda_{rev},L_{attr(j),rev}\}_{rev\in List_{attr(j)}})$ 加入 R_k.

- 若属性无相关撤销用户,则计算 $L_{attr(j)}=v^{\beta t_j}h^{\alpha}$,将二元组加入 R_k;
- 若用户 ID_{rev} 被撤销,则计算该用户所有属性的 $L_{attr(j),rev}$,并添加至 R_k.

3.4 加密*Encrypt*(Γ_{ω^*},*M*,*R*,*PK*)

获取所有属性授权机构 AA_k 最新的属性撤销列表 $R_k=\{(j,\{\lambda_{rev},L_{j,rev}\}_{rev\in List_j})\}$.加密方选择随机数 $s,r\in Z_q^*$,计算 $C_0=M\cdot Z^{sr}$,$C^*=g^{sr}$.

加密方选择访问树策略 Γ_{ω^*},如下所示,从根节点 *root* 开始由上至下为每个内部节点选取 n_x-1 阶多项式 q_x.

- 根节点 *root*:$q_{root}(0)=s$,其余 $n_{root}-1$ 个系数随机选取;
- 内部节点 x:$q_x(0)=q_{parent}(index(x))$;
- 叶子节点 $leaf_j$: $q_{leaf_j}(0)=q_x(index(leaf_j))$;
- 对于任意属性 $j\in\omega^*$,$List_j=\varnothing$,计算 $C_{1,j}=T_j^{q_{leaf_j}(0)\cdot r}$,$C_{2,j}=L_j^{q_{leaf\,j}(0)\cdot r}$;
- 对于任意属性 $j\in\omega^*$,$List_j\neq\varnothing$,遍历 j 的撤销列表 $List_j$,选择$|List_j|$个随机数 $u_1,...,u_{|List_j|}$,满足 $u_1+...+u_{|List_j|}=q_{leaf_j}(0)$,计算 $\{C_{1,j,rev}=T_j^{u_{rev}\cdot r},C_{2,j,rev}=L_{j,rev}^{u_{rev}\cdot r}\}_{j\in\omega^*,rev\in List_j}$;
- 最后输出密文 $CT=\langle C_0,C^*,\{C_{1,j},C_{2,j}\}_{j\in\omega^*,List_j=\varnothing},\{C_{1,j,rev},C_{2,j,rev}\}_{j\in\omega^*,rev\in List_j}\rangle$.

3.5 重加密*ReEncrypt*(Γ_{ω^*},*M*,*R*,*PK*)

已知密文 $CT=\langle C_0,C^*,\{C_{1,j},C_{2,j}\}_{j\in\omega^*,List_j=\varnothing},\{C_{1,j,rev},C_{2,j,rev}\}_{j\in\omega^*,rev\in List_j}\rangle$,当访问结构涉及的属性发生撤销事件时,用户需对密文进行重加密.

- 若撤销前,属性 $j\in\omega^*$,$List_j=\varnothing$,则选择随机数 u_{rev}^*,计算重加密密文: $C_{1,j,rev}=C_{1,j}\cdot T_j^{-u_{rev}^*\cdot r}$,$C_{2,j,rev}=C_{2,j}\cdot L_j^{-u_{rev}^*\cdot r}=L_j^{(q_{leaf_j}(0)-u_{rev}^*)\cdot r}$,$C_{1,j,rev^*}=T_j^{u_{rev}^*\cdot r}$,$C_{2,j,rev^*}=L_j^{u_{rev}^*\cdot r}$,替换原有密文即可;
- 若撤销前,属性 $j\in\omega^*$,$List_j\neq\varnothing$,则选择随机数 u_{rev}^*,计算重加密密文 $C_{1,j,rev}=C_{1,j,rev}\cdot T_j^{-u_{rev}^*\cdot r}=T_j^{(u_{rev}-u_{rev}^*)\cdot r}$,$C_{2,j,rev}=C_{2,j,rev}\cdot L_j^{-u_{rev}^*\cdot r}=L_j^{(u_{rev}-u_{rev}^*)\cdot r}$,$C_{1,j,rev^*}=T_j^{u_{rev}^*\cdot r}$,$C_{2,j,rev^*}=L_j^{u_{rev}^*\cdot r}$,替换原有密文即可.

3.6 解密*Decrypt*(Γ_{ω^*},$SK_{ID,\omega}$,*CT*,*R*)

解密算法如下递归进行:对于访问树 Γ_{ω^*} 中的每个叶子节点 $leaf_j$,查询属性撤销列表 *R*.

- 若该属性无相关撤销信息,即 $j\in\omega\cap\omega^*$,$List_j=\varnothing$,计算:

$$DecryptNode(CT,SK_{ID,\omega},leaf_j)=\frac{e(S_{i,j}\cdot v^{\beta},C_{1,j})}{e(g,C_{2,j})}=e(g,g)^{\alpha r\lambda_i\cdot q_{leaf_j}(0)};$$

- 若该属性具有撤销信息,即 $j\in\omega\cap\omega^*$,$List_j\neq\varnothing$,计算:

$$DecryptNode(CT,SK_{ID_i,\omega},leaf_j)=\prod_{rev\in List_j}\left(\frac{e(S_{i,j}\cdot v^{\beta},C_{1,j,rev})}{e(g,C_{2,j,rev})}\right)^{\frac{\lambda_i}{\lambda_i-\lambda_{rev}}}=e(g,g)^{\alpha r\lambda_i q_{leaf_j}(0)}.$$

对于访问树 Γ_{ω^*} 的非叶子节点 x,设该节点的子节点为 z,调用 $DecryptNode(CT,SK_{ID,\omega},z)$的计算结果,记为 F_z.令 S_x 为任意 n_x 个 $F_z\neq\perp$的子节点 z 的集合,$F(x)$计算如下:

$$\begin{aligned}F(x)&=\prod\nolimits_{z\in S_x}F(z)^{\Delta_{i,S_x}(0)}\\&=\prod\nolimits_{z\in S_x}(e(g,g)^{\alpha r\lambda_i\cdot q_z(0)})^{\Delta_{i,S_x}(0)}\\&=\prod\nolimits_{z\in S_x}(e(g,g)^{\alpha r\lambda_i\cdot q_{parent(z)}(index(z))})^{\Delta_{i,S_x}(0)}\\&=\prod\nolimits_{z\in S_x}(e(g,g)^{\alpha r\lambda_i\cdot q_x(i)})^{\Delta_{i,S_x}(0)}\\&=e(g,g)^{\alpha r\lambda_i q_x(0)}.\end{aligned}$$

当且仅当用户 ID 所拥有的属性集ω满足 Γ_{ω^*},用户才能递归计算出 $F(root)=e(g,g)^{\alpha\lambda_i rs}$.

最后,通过如下计算恢复明文 M:

$$M=\frac{C_0\cdot e(C^*,W_i^*)}{F(root)}.$$

4 方案分析

4.1 正确性分析

用户能够成功解密的条件是用户的属性集ω满足访问树结构 Γ_{ω^*},且用户用于解密的属性不在撤销名单中.利用拉格朗日插值定理,可以递归地恢复出 s,进而解密出明文,具体推导过程如下:

$$M=\frac{C_0\cdot e(C^*,W_i^*)}{F(root)}=\frac{M\cdot Z^{sr}\cdot e(g^{sr},g^{\alpha\lambda_i-\beta})}{e(g,g)^{\alpha\lambda_i rs}}=\frac{M\cdot e(g,g)^{\beta sr}\cdot e(g^{sr},g^{\alpha\lambda_i-\beta})}{e(g,g)^{\alpha\lambda_i rs}}=M.$$

4.2 安全性分析

定理 1. 在随机预言机模型及 q-BDHE 问题假设下,本文提出的基于属性的加密方案在适应性选择密文攻击下是密文不可区分的.

证明:假设存在敌手 A 以不可忽略的优势ε攻破上述方案的密文不可区分性,则可以构造一个有效的算法 C,以不可忽略的优势解决 q-BDHE 问题.记攻击者 A 访问私钥解析预言机、密文解析预言机的次数分别为 q_k,q_D.

假定给算法 C 一个 q-BDHE 问题的实例:给定 $Y=(g,g^s,g^a,g^{(a^2)},...,g^{(a^q)},g^{(a^{q+2})},...,g^{(a^{2q})})$ 与随机数 $V\in_R G_2$,C 的目标是调用 A 为子程序,区分出随机数 V 与 $e(g,g)^{a^{q+1}s}$.C 仿真如下.

(1) 初始化:挑战者 C 随机选择元素 s,a,计算 $Y'=(g,g^s,g^a,g^{(a^2)},...,g^{(a^n)},g^{(a^{n+2})},...,g^{(a^{2n})})$.然后,挑战者 C 运行 $Setup(1^\lambda)$算法,抛掷一枚公平的二元随机硬币$\mu\in\{0,1\}$:若μ=0,令$\beta=a^{n+1}$,计算 $Z=e(g,g)^{a^{n+1}}$,其中,n 表示属性个数;否则,随机选择元素 $V\in G_2$.挑战者将 $Y=(Y',V)$发送给 A.令 $t_j=a^j$,$j\in[1,n)$,产生公钥 $PK=\langle g,v^\beta,e,Z,q,\{T_j\}_{j\in U}\rangle$与系统主密钥 MK,将公钥发送给敌手 A,敌手 A 输出挑战身份 $\bar{\lambda}$、挑战访问策略 Γ_{ω^*} 和属性撤销列表 R;

(2) 阶段 1:敌手 A 进行多项式界次数的预言机询问.

a) 私钥解析询问:C 维护一个含有数组 $(\omega_i,\lambda_i,W_i,\{S_{i,j}\}_{j\in\omega_i})$ 的列表 key^{list}.当 A 选择用户 ID_i 及其属性集ω_i,向 C 询问对应用户的私钥时,C 检查列表 key^{list} 中是否有对应的询问结果:如果有,则返回对应值 $(W_i,\{S_{i,j}\}_{j\in\omega_i})$;否则,$C$ 操作如下.

- ✧ 若 $\Gamma_{\omega^*}(\omega_i)\neq 1$,对于属性 $j\in\omega_i$,令α=a,计算 $S_{i,j}=g^{\frac{a\lambda_i}{t_j}}h^{\frac{a}{t_j}}=g^{\frac{\lambda_i}{a^{j-1}}}$,$W_i=g^{a\lambda_i-a^{n+1}}$.$C$ 返回结果给 A,并记录 $(\omega_i,\lambda_i,W_i,\{S_{i,j}\}_{j\in\omega_i})$ 到列表 key^{list};
- ✧ 否则,$\Gamma_{\omega^*}(\omega_i)=1$,当$\lambda_i\in R$ 时,预言仿真过程同上;
- ✧ 否则,$\Gamma_{\omega^*}(\omega_i)=1$且$\lambda_i\notin R$,$C$ 停止并输出“FAILURE”(该事件用 E_1 表示);

b) 密文解析询问:C 维护一个含有数组 $(\omega_i,\lambda_i,\Gamma_{\omega^*},M_k,CT_k)$ 的列表 Dec^{list}.当 A 在访问结构 Γ_{ω^*} 下发送一个挑战用户λ_i、一个属性集合ω_i 与密文 CT_k 给挑战者 C 进行密文解析询问时,C 检查列表 Dec^{list} 中是否有对应的询问结果:如果有,则返回对应明文 M_k;否则,C 操作如下.

- ✧ 若 $\Gamma_{\omega^*}(\omega_i)=1$,$\lambda_i\notin R$ 且 $CT_k\neq CT^*$,C 运行 $Decrypt(\Gamma_{\omega^*},SK_{ID,\omega},CT,R)$算法,解密出明文 M_k,返回给 A,并记录相应信息到列表 Dec^{list};
- ✧ 否则,C 停止并输出“FAILURE”(该事件用 E_2 表示);

(3) 挑战:敌手 A 挑战方案的不可区分性:A 分别选择两条长度相等的明文 M_0,M_1.挑战者 C 随机选取 $b\in$

{0,1},运行 $Encrypt(\Gamma_{\omega^*},M_b,R,PK)$算法,生成消息 M_b 在访问策略 Γ_{ω^*} 下的密文 CT^*,并返回结果给 A;若μ=0,则令 r=1, $C_0 = M_b \cdot Z^{sr} = M_b \cdot e(g,g)^{a^{n+1}s}$, $C^*=g^{sr}=g^s$;若μ=1,则令 $C_0=V^{sr}$,$C^*=g^{sr}$;

(4) 阶段 2:如阶段 1 所示,A 继续执行多项式界次数的私钥解析和密文解析询问;

(5) 猜测:敌手 A 输出对 b 的猜测 b'.

若 $b=b'$,C 输出对μ的猜测μ'=0;否则,输出对μ的猜测μ'=1.所以,C 成功输出 $\mu \overset{?}{=} \mu'$ 作为对 q-BDHE 问题的一个实例的解答.

分析 C 在这个游戏中的优势:

i) 预言机的回答是有效的,除非事件 E_1,E_2 发生;

ii) 如果 A 能够区分密文与密文间的不同,则 C 能解决 q-BDHE 问题的一个实例.

总而言之,如果事件 E_1,E_2 都没有发生,则 A 能攻破所提方案的不可区分性.现在计算 C 能解决 q-BDHE 问题的优势:当μ=0 时, $C_0 = M_b \cdot Z^{sr} = M_b \cdot e(g,g)^{a^{n+1}s}$ 是一条合法密文,攻击者可以发挥全部攻击优势ε=Pr[$b=b'$]−1/2,则μ=0 时,C 获胜的概率为 Pr[$b=b'|\mu$=0]=Pr[$b=b'$]=ε+1/2;当μ=1 时,$C_0=M_bV^{sr}$ 相当于 G_2 上随机选取的元素,不包含明文 M_b 的任何信息,因此攻击者失去攻击优势,则μ=1 时,C 获胜的概率为 Pr[$b=b'|\mu$=1]=Pr[$b\neq b'$]=1/2.综上所述,C 能解决 q-BDHE 问题的优势为

$$\Pr[b=b']-1/2=\Pr[b=b'|\mu=0]\cdot\Pr[\mu=0]+\Pr[b=b'|\mu=1]\cdot\Pr[\mu=1]-1/2=(\varepsilon+1/2)\cdot1/2+1/2\cdot1/2-1/2=\varepsilon/2.$$ □

定理 2. 在随机预言机模型及 DDH 问题假设下,本文提出的基于属性的加密方案能够抵抗不可信授权中心的破译攻击.

证明:假设存在敌手 A 以不可忽略的优势ε攻破上述方案,则可以构造一个有效的算法 C,以$\varepsilon'\approx\varepsilon/2$ 的优势解决 DDH 问题.记攻击者 A 访问私钥解析预言机、密文解析预言机的次数分别为 q_k,q_D.

假定给算法 C 一个 DDH 问题的实例:输入 $g^x,g^y,g^z\in G_1$,挑战者 C 的目标是以 A 作为子程序,判断 $z=xy \bmod q$ 是否成立.C 仿真过程如下所示.

(1) 初始化:挑战者 C 运行 $Setup(1^\lambda)$算法,产生公钥 $PK=\langle g,v^\beta,e,Z,q,\{T_j\}_{j\in U}\rangle$与系统主密钥 MK.C 抛掷一枚公平的二元随机硬币$\mu\in\{0,1\}$:若μ=0,令 $z=\beta$,计算 $Z=e(g,g)^z$;否则,随机选择 $x,y\in Z_q$,计算 $Z=e(g,g)^{xy}$.若敌手 A 为恶意系统中心 SA,C 将 PK 和秘密参数$\langle\alpha,\beta,\lambda_i\rangle$发送给 A,MK 保密;若敌手 A 为恶意属性授权机构 AA_k,C 将 PK,MK 和秘密参数α发送给 A,秘密参数$\langle\beta,\lambda_i\rangle$保密.敌手 A 输出挑战访问策略 Γ_{ω^*} 和属性撤销列表 R;

(2) 阶段 1:敌手 A 进行多项式界次数的预言机询问.

a) 私钥解析询问:C 维护一个含有数组 $(\omega_i,\lambda_i,W_i,\{S_{i,j}\}_{j\in\omega_i})$ 的列表 key^{list}.当 A 选择用户 ID_i 及其属性集ω_i、向 C 询问对应用户的私钥时,C 检查列表 key^{list} 中是否有对应的询问结果:如果有,则返回对应值 $(W_i,\{S_{i,j}\}_{j\in\omega_i})$;否则,$C$ 操作如下.

- ✧ 若 $\Gamma_{\omega^*}(\omega_i)\neq1$,对于属性$j\in\omega_i$,令$\alpha=a$,计算 $S_{i,j}=g^{\frac{a\lambda_i}{t_j}}h^{\frac{a}{t_j}}=g^{\frac{\lambda_i}{a^{j-1}}}$,$W_i=g^{a\lambda_i-a^{n+1}}$.$C$ 返回结果给 A,并记录 $(\omega_i,\lambda_i,W_i,\{S_{i,j}\}_{j\in\omega_i})$ 到列表 key^{list};
- ✧ 否则, $\Gamma_{\omega^*}(\omega_i)=1$,当$\lambda_i\in R$ 时,预言仿真过程同上;
- ✧ 否则, $\Gamma_{\omega^*}(\omega_i)=1$ 且$\lambda_i\notin R$,C 停止并输出“FAILURE”(该事件用 E_1 表示);

b) 密文解析询问:C 维护一个含有数组 $(\omega_i,\lambda_i,\Gamma_{\omega^*},M_k,CT_k)$ 的列表 Dec^{list}.当 A 在访问结构 Γ_{ω^*} 下发送一个挑战用户λ_i、一个属性集合ω_i 与密文 CT_k 给挑战者 C 进行密文解析询问时,C 检查列表 Dec^{list} 中是否有对应的询问结果:如果有,则返回对应明文 M_k;否则,C 操作如下.

- ✧ 若 $\Gamma_{\omega^*}(\omega_i)=1$,$\lambda_i\notin R$ 且 $CT_k\neq CT^*$,C 运行 $Decrypt(\Gamma_{\omega^*},SK_{ID,\omega},CT,R)$算法,解密出明文 M_k,返回给 A,并记录相应信息到列表 Dec^{list};
- ✧ 否则,C 停止并输出“FAILURE”(该事件用 E_2 表示);

(3) 挑战:A 分别选择两条长度相等的明文 M_0,M_1.挑战者 C 随机选取 $b\in\{0,1\}$,运行 $Encrypt(\Gamma_{\omega^*},M_b,R,PK)$ 算法,生成消息 M_b 在访问策略 Γ_{ω^*} 下的密文 CT^*,将 CT^* 发送给 A;

(4) 阶段 2:如阶段 1,攻击者进行多项式次预言机询问;

(5) 猜测:攻击者 A 输出对 b 的猜测 b',若 $b=b'$ 则 A 赢得游戏,则 C 成功输出 $\mu=\mu'$ 作为对 DDH 问题的一个实例的解答,即该方案无法抵抗不可信授权中心的破译攻击.

分析 C 在这个游戏中的优势.

i) 只要事件 E_1,E_2 不发生,则预言机返回的的结果是正确的;

ii) 若 A 赢得游戏,则 C 能够解决给定 DDH 问题的实例.

总而言之,如果事件 E_1,E_2 都没有发生,则 A 能攻破所提方案的不可区分性.现在计算 C 能解决 DDH 问题的优势:当 $\mu=0$ 时,$C_0=M_b\cdot Z^{sr}=M_b\cdot e(g,g)^{zsr}$ 是一条合法密文,攻击者可以发挥全部攻击优势 $\varepsilon=\Pr[b=b']-1/2$,则 $\mu=0$ 时,C 获胜的概率为 $\Pr[b=b'|\mu=0]=\Pr[b=b']=\varepsilon+1/2$;当 $\mu=1$ 时,$C_0=M_b\cdot e(g,g)^{xysr}$ 相当于 G_2 上随机选取的元素,因此攻击者失去攻击优势,则 $\mu=1$ 时,C 获胜的概率为 $\Pr[b=b'|\mu=1]=\Pr[b\neq b']=1/2$.综上所述,$C$ 能解决 DDH 问题的优势为

$$\Pr[b=b']-1/2=\Pr[b=b'|\mu=0]\times\Pr[\mu=0]+\Pr[b=b'|\mu=1]\times\Pr[\mu=1]-1/2=(\varepsilon+1/2)\times1/2+1/2\times1/2-1/2=\varepsilon/2.$$ □

若所提方案无法抵抗不可信授权中心的破译攻击,则该方案是适应性选择密文攻击下的不可展性不安全的.因为若敌手以一种可控的方式,通过修改密文来修改相应的明文,则它可以对挑战密文进行修改,然后通过预言机的帮助获取修改后密文对应的明文,最后,利用明文间的相互关系输出挑战密文对应的明文.由于公钥密码体制适应性选择密文攻击下的不可区分性等价于适应性选择密文攻击下的不可展性,因此敌手无法在多项式时间内解密挑战密文,所以本文所提的基于属性的加密方案能够抵抗不可信授权中心的破译攻击.

4.3 性能分析

本节就密钥长度、密文长度、加密阶段和解密阶段的计算代价、撤销机制、访问策略、重加密功能、能否解决授权中心不可信问题等方面与文献[10,13,16−18,21−24]中的方案进行对比,以评估本方案的性能.比较结果见表 1.

Table 1 Performance comparison of the proposal against other schemes

表 1 本方案与其他方案性能比较

方案	密钥长度(bit)	密文长度(bit)	加密计算量	解密计算量	撤销机制	访问策略	是否支持重加密	能否解决授权中心不可信问题
文献[10]	$(\|C\|+4)\|G_1\|$	$(2+\|B\|+2r)\|G_1\|$	$(1+2\|B\|+3r)T_{exp}$	$(1+2\|B\|+2r)T_{bp}+(\|B\|+r)T_{exp}$	用户撤销	LSSS	×	×
文献[13]	$(2\|A\|+1)\|G_1\|$	$(2+\|A\|)\|G_1\|$	$(2+\|A\|)T_{exp}$	$(1+\|A\|)T_{bp}$	属性间接撤销	$AND_{+,-}$	√	×
文献[16]	$(2\|B\|+2)\|G_1\|$	$(\|B\|+r+2)\|G_1\|$	$(\|B\|+r+2)T_{exp}+(1+r)T_{bp}$	$(3\|D\|+2)T_{bp}+\|D\|T_{exp}$	用户撤销	LSSS	√	×
文献[17]	$(2\|C\|+3)\|G_1\|$	$(4\|B\|+1)\|G_1\|$	$(6\|B\|+1)\ T_{exp}+1\ T_{bp}$	$(2\|D\|+2)T_{exp}+3\|D\|T_{bp}$	用户撤销	LSSS	×	√
文献[18]	$(\|C\|+4)\|G_1\|$	$(2\|B\|+r+3)\|G_1\|$	$(3\|B\|+r+3)T_{exp}+1T_{bp}$	$(\|D\|+2)T_{exp}+(2\|D\|+3)T_{bp}$	用户撤销	LSSS	√	×
文献[21]	$(2\|C\|+1)\|G_1\|$	$(2+\|B\|)\|G_1\|$	$(1+\|B\|)T_{exp}+1T_{bp}$	$(2\|D\|+1)T_{bp}$	属性直接撤销	访问树	×	×
文献[22]	$(2\|C\|+1)\|G_1\|$	$(3\|B\|+2r+2)\|G_1\|$	$(2+3\|B\|+4r)T_{exp}+1T_{bp}$	$(4\|D\|+2r+1)T_{bp}$	属性直接撤销	LSSS	×	×
文献[23]	$(\|A\|+1)\|G_1\|$	$5\|G_1\|$	$(2\|B\|+4)T_{exp}+(1+\|B\|)T_{bp}$	$(4+r)T_{bp}$	属性直接撤销	$AND_{+,-}$	√	×
文献[24]	$(\|C\|+1)\|G_1\|$	$5\|G_1\|$	$5T_{exp}+1T_{bp}$	$(4+r)T_{bp}$	属性直接撤销	AND_m	√	×
本文方案	$(\|C\|+2)\|G_1\|$	$(2\|B\|+2)\|G_1\|$	$(2\|B\|+2)T_{exp}$	$(2\|D\|+1)T_{bp}$	属性直接撤销	访问树	√	√

表 1 中,T_{bp} 表示一次双线性对运算所需的时间复杂度,T_{exp} 表示一次 G_1 群上的模幂运算所需的时间复杂

度,$|A|$表示所有属性的数量,$|B|$表示访问策略中声明的属性的数量,$|C|$表示用户拥有属性的数量,$|D|$表示用户解密使用的属性的数量,r 表示撤销事件的数量.

从表 1 可以看出:在已有的结果中,本方案的密钥长度仅次于文献[24]中的方案.文献[13,23]需要给每个用户颁发所有属性相应的密钥,因此密钥长度较长;而文献[10,16−18,21,22]中的方案与本方案类似,只需要给每个用户颁发自身属性相应的密钥,减少了密钥长度.同时,为了确保能够抵抗合谋攻击,本方案引进了一个私有变量,因此比文献[24]中的方案增加了 $1|G_1|$bit.

为了实现对用户属性的细粒度撤销,本方案采用在密文中直接嵌入撤销信息的方法,需要产生与属性撤销名单一一对应的密文,因此在密文长度上本方案并不具备优势,为$(2|B|+2)|G_1|$bit.虽然文献[23,24]中的方案的密文长度较小且具有恒定大小,为 $5|G_1|$,但这两个方案只支持 AND 结构的访问策略,不够灵活,并且大部分计算任务需要由属性授权中心执行,在用户与属性数目较大时,易造成性能瓶颈.文献[13,21]中的方案的密文长度比本文方案略短,但文献[13]中的方案采用了间接撤销模式,而文献[21]中的方案则通过与半可信第三方的交互来实现属性的直接撤销,通信代价较大.文献[10,16,18]中的方案的密文长度与本方案相近,但这 3 个方案只支持用户撤销,不支持属性撤销,撤销粒度粗.文献[17,22]中的方案为了抵抗合谋攻击,需要对密文进行随机化处理,因此这两个方案密文长度较大,分别为$(4|B|+1)|G_1|$bit 和$(3|B|+2r+2)|G_1|$bit.总体而言,在保证良好的系统安全性、灵活性以及更细的属性撤销粒度前提下,本文方案具有较短的密文长度.

综合加密与解密的计算量,文献[24]中的方案的计算代价最少,为 $5T_{exp}+(5+r)T_{bp}$,但该方案将大量的计算任务交由属性授权中心执行,其安全性高度依赖于属性授权中心的可靠性,且该方案的解密计算量与属性撤销频率呈线性关系,不适用于属性变化频繁的云计算环境中.相比于其他方案,本方案在计算代价上具有较大优势,仅比文献[21]中的方案增加了$(|B|+1)T_{exp}$.而文献[21]中的方案使用了两部分密钥,且解密时需要跟属性授权中心进行认证,增加了通信代价.方案[13]采用属性的间接撤销,需要在属性变化时颁发新的密钥,并且计算代价与所有属性的集合大小相关,当属性集合过大时,解密方可能无法负荷相应的计算量.而文献[10,16−18,22,23]中的方案都存在计算代价大且与属性撤销频率呈线性关系的问题.本文方案不仅实现了细粒度属性的直接撤销,并且采用了访问树结构,能够保证密文的灵活使用,在计算效率上也进行了优化,更加实用.

从功能性进行分析,主要集中于细粒度属性直接撤销,而重加密是实现上述功能的重要方法,即:当用户属性撤销事件发生时,对已经生成并发布的密文重新进行加密,以避免属性被撤销用户解密该密文.文献[10,17,21,22]并不支持重加密,文献[13,16,18,23,24]中的方案虽然具备重加密功能,但是存在撤销粒度粗(如文献[16,18]中的方案),或访问策略表达能力弱(如文献[13,23,24]中的方案)的缺点.本文方案在树状访问结构基础上,通过引入属性撤销列表,给出了高效的重加密算法,从而实现了细粒度的属性直接撤销功能.在安全性方面,本文方案能够防止不可信授权中心的侵权行为,而绝大多数方案都不具备该特性,因此,本文方案在安全性上得以加强.

综上所述,本文方案采用树状访问结构实现了用户属性的细粒度直接撤销,在保证安全性的前提下,具有更高的撤销效率;同时,所提方案能够抵抗不可信授权中心的破译攻击,更加适用于用户属性变化频繁的云计算环境中.

5 结 论

本文提出一种支持细粒度属性直接撤销的 CP-ABE 方案,该方案采用树结构的访问策略,有效解决了现有方案撤销代价与安全性难以兼顾的问题.性能分析表明,新方案在密钥长度与计算量上具有一定优势,并且能够防止不可信授权中心解密用户隐私数据的行为,可以有效避免云计算环境中因数据共享带来的安全隐患.

References:

[1] Sahai A, Waters B. Fuzzy identity-based encryption. In: Ronald C, ed. Proc. of the 24th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005). Berlin: Springer-Verlag, 2005. 457−473.

[2] Goyal V, Pandey O, Amit S, Brent W. Attribute-Based encryption for fine-grained access control of encryption data. In: Proc. of the 13th ACM Conf. on Computer and Communications Security (CCS 2006). New York: ACM Press, 2006. 89−98.

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Proc. of 2007 IEEE Symp. on Security and Privacy. New York: IEEE, 2007. 321−334. [doi: 10.1109/SP.2007.11]

[4] Attrapadung N, Imai H. Dual-Policy attribute based encryption. In: Michel A, ed. Proc. of the 7th Applied Cryptography and Network Security (ACNS 2009). Heidelberg: Springer-Verlag, 2009. 168−185.

[5] Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2007. 195−203.

[6] Chase M. Multi-Authority attribute based encryption. In: Salil PV, ed. Proc. of the 4th Theory of Cryptography Conf. (TCC 2007). Berlin: Springer-Verlag, 2007. 515−534.

[7] Goyal V, Jain A, Pandey O, Sahai A. Bounded ciphertext policy attribute based encryption. In: Luca A, Ivan D, *et al*., eds. Proc. of the 35th Int'l Colloquium (ICALP 2008). Berlin: Springer-Verlag, 2008. 579−591.

[8] Wei JH, Liu WF, Hu XX. Forward-Secure ciphertext-policy attribute-based encryption scheme. Journal of Communications, 2014, 35(7):38−45 (in Chinese with English abstract).

[9] Attrapadung N, Imai H. Attribute-Based encryption supporting direct/indirect revocation modes. In: Matthew GP, ed. Proc. of the IMA Int'l Conf. on Cryptography and Coding (IMACC 2009). Berlin: Springer-Verlag, 2009. 278−300.

[10] Attrapadung N, Imai H. Conjunctive broadcast and attribute-based encryption. In: Hovav S, Brent W, eds. Proc. of the Int'l Conf. on Pairing-Based Cryptography (Pairing 2009). Berlin: Springer-Verlag, 2009. 248−265.

[11] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Victor S, ed. Proc. of the 25th Annual Int'l Cryptology Conf. (CRYPTO 2005). Berlin: Springer-Verlag, 2005. 258−275.

[12] Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Haifa: Israel Institute of Technology (Technion), 1996.

[13] Yu S, Wang C, Ren K. Attribute based data sharing with attribute revocation. In: Proc. of the 5th ACM Symp. on Information, Computer and Communications Security (ASIACCS 2010). New York: ACM Press, 2010. 261−270.

[14] Naruse T, Mohri M, Shiraishi Y. Attribute-Based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating. In: James JP, *et al*., eds. Proc. of the Future Information Technology. Berlin: Springer-Verlag, 2014. 119−125.

[15] Zu LH, Liu ZH, Li JJ. New ciphertext-policy attribute-based encryption with efficient revocation. In: Proc. of the 2014 IEEE Int'l Conf. on Computer and Information Technology. New York: IEEE, 2014. 281−287. [doi: 10.1109/CIT.2014.97]

[16] Shi YF, Zheng QJ, Liu JQ, Han Z. Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation. Information Sciences, 2015,295:221−231.

[17] Zhang K, Ma JF, Li H, *et al*. Multi-Authority attribute-based encryption with efficient revocation. Journal of Communications, 2017, 38(3):83−91 (in Chinese with English abstract).

[18] Wang H, Zheng ZH, Wu L, *et al*. New directly revocable attribute-based encryption scheme and its application in cloud storage environment. Cluster Computing, 2017,20(3):2385−2392.

[19] Hur J, Noh DK. Attribute-Based access control with efficient revocation in data outsourcing systems. IEEE Trans. on Parallel and Distributed Systems, 2011,22(7):1214−1221. [doi: 10.1109/TPDS.2010.203]

[20] Wang PP, Feng DG, Zhang LW. Towards attribute revocation in key-policy attribute based encryption. In: Lin D, *et al*., eds. Proc. of the 10th Int'l Conf. on Cryptology and Network Security (CANS 2011). Berlin: Springer-Verlag, 2011. 272−291.

[21] Ibraimi L, Pekovic M, Nikova S, *et al*. Mediated ciphertext-policy attribute-based encryption and its applications. In: Proc. of the 10th Int'l Workshop on Information Security Applications (WISA 2009). Berlin: Springer-Verlag, 2009. 309−323.

[22] Wang PP, Feng DG, Zhang LW. CP-ABE scheme supporting fully fine-grained attribute revocation. Ruan Jian Xue Bao/Journal of Software, 2012,23(10):2805−2816 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4184.htm

[23] Zhang YH, Chen XF, Li J, *et al*. FDR-ABE: Attribute-based encryption with flexible and direct revocation. In: Proc. of the 2013 Int'l Conf. on Intelligent Networking and Collaborative Systems. New York: IEEE, 2013. 38−45.

[24] Zhang YF, Zheng D, Li J, Li H. Attribute directly-revocable attribute-based encryption with constant ciphertext length. Journal of Cryptologic Research, 2014,1(5):465−480 (in Chinese with English abstract).

[25] Hong HS, Sun ZX. An efficient and traceable KP-ABS scheme with untrusted attribute authority in cloud computing. Journal of Cloud Computing: Advances, Systems and Application, 2016,5(2):1−8.

附中文参考文献:

[8] 魏江宏,刘文芬,胡学先.前向安全的密文策略基于属性加密方案.通信学报,2014,35(7):38−45.

[17] 张凯,马建峰,李辉,等.支持高效撤销的多机构属性加密方案.通信学报,2017,38(3):83−91.

[22] 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.软件学报,2012,23(10):2805−2816. http://www.jos.org.cn/1000-9825/4184.htm

[24] 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.密码学报,2014,1(5):465−480.

张文芳(1978－),女,山西太原人,博士,副教授,主要研究领域为公钥密码学,信息安全.

刘旭东(1990－),男,硕士生,主要研究领域为基于属性的密码体制,环签名.

陈桢(1990－),男,硕士,主要研究领域为基于属性的加密,签名机制.

王小敏(1974－),男,博士,教授,博士生导师,主要研究领域为信息安全,轨道交通信息系统安全.