计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20150580
52(10):2281-2292,2015

隐私保护且支持用户撤销的属性基加密方案

李继国　石岳蓉　张亦辰
(河海大学计算机与信息学院　南京　211100)
(ljg1688@163.com)

A Privacy Preserving Attribute-Based Encryption Scheme with User Revocation

Li Jiguo, Shi Yuerong, and Zhang Yichen
(*College of Computer & Information, Hohai University, Nanjing* 211100)

Abstract　Since Sahai and Waters proposed the concept of attribute-based encryption, ciphertext-policy attribute-based encryption (CP-ABE) system has drawn more and more attentions due to its widespread use of scenes. The consumption of the battery is not economical for users who use attribute-based encryption on mobile devices because of the large number of bilinear pairing operations. Due to dynamic for user's attributes and the openness of the access structure in the cloud environment, it may lead to the attribute failure and user privacy leakage. In order to solve above problems, we construct an attribute-based encryption scheme, which protects the privacy for the users by fully hidden access structure and supports flexible user revocation by key updating mechanisms. Meanwhile, we outsource the high computational cost of the bilinear pairing operations to the cloud storage providers, which reduces the computational expense of users for mobile devices. In order to curb cloud misconduct or malicious attacks on the cloud, we provide the verification function of the converted ciphertext which ensures the converted encrypted cipher text is not replaced illegally. The proposed scheme is more suitable for secure mobile cloud applications.

Key words　attribute-based encryption system; ciphertext-policy; privacy preserving; user revocation; cloud computing

摘　要　自从Sahai和Waters提出了基于属性加密的概念,密文策略的属性基加密(ciphertext-policy attribute-based encryption, CP-ABE)体制因其使用场景的广泛性受到了各界的青睐.对于使用移动设备进行属性基加解密的用户而言,大量的双线性对运算带来的电池耗费是不经济的;同时,由于在云环境系统下用户属性的动态性和访问结构的公开性,也会导致属性失效和用户隐私泄露的问题.为了解决上述问题,构造了一个隐私保护的且支持用户撤销的属性基加密方案,达到了完全隐藏访问结构并通过密钥更新机制灵活地实现用户撤销;同时,该方案将计算代价较高的双线性对操作外包给云存储提供方执行,以降低移动设备用户的计算代价,为了遏制云端的不端行为或对云端恶意攻击,提供了对转换密文的验证功能,保证了转换后密文未被非法替换,使之更适用于安全的手机云应用.

关键词　属性基加密体制;密文策略;隐私保护;用户撤销;云计算

中图法分类号　TP309

收稿日期:2015-06-15;**修回日期**:2015-08-13

基金项目:国家自然科学基金项目(61272542);江苏高校优势学科建设工程资助项目;中央高校基本科研业务费专项资金项目(2013B07014);江苏省"六大人才高峰"项目(2009182);河海大学新世纪优秀人才计划项目

云计算作为新型服务模式的代表以其低成本、快速部署和灵活调整规模等优势得到了工业界和学术界的高度关注. 面对云服务提供商不断爆出的安全事故,人们对云计算环境中的用户数据安全性和隐私性的忧虑与日俱增[1]. 一旦将数据存储在云中,对数据的控制权就不在用户的掌握之中,而是转移到了云存储提供方的手中,某些不法分子可能利用非法手段从中获取客户的隐私资料. 为了保护敏感信息,将数据以加密的形式存储在云端是个可行的办法,而传统的公钥密码系统不能满足在云环境下的访问控制、安全和效率要求. 为了解决该问题,Sahai 和 Waters[2] 提出了基于属性加密体制的概念. 属性基加密机制可以很好地实现对不同用户访问权限的控制和高效的信息分享,从而受到了各界的青睐.

在密文策略的属性基加密(ciphertext-policy attribute-based encryption, CP-ABE)系统[3]中,每个用户与一系列的描述性属性集合相关(比如性别、VIP 等级、工种等),密文与访问结构相关联,而每个用户的私钥与一系列的描述性属性集合相关,当且仅当在私钥和相应的密文之间存在一个匹配时可以解密消息. 密文策略的属性基加密体制因其使用场景的广泛性以及数据拥有者具有自主制定访问控制权而受到了广泛关注.

由于属性策略的动态性,在云环境下不仅要考虑用户数据的安全性,而且也要考虑用户属性的撤销问题. 文献[4-6]中,通过授权中心发布一个具有有效阈值期的属性或者密钥解决属性的撤销问题. 这种撤销机制可能给系统带来安全隐患,例如前向保密问题和后向保密问题. Hur 等人[7] 提出一个支持即时属性撤销的数据外包属性基加密方案,该方案通过可信第三方来管理属性撤销列表. Wang 等人[8] 通过采用分层域的方式为用户分发密钥,并实现了属性撤销. Yu 等人[9] 提出了一种云存储环境下的密文策略的属性基加密方案,它通过使用懒散的代理重加密(lazy proxy re-encryption)技术来提供一种新型的密钥撤销方法. 这为之后如何在分布式存储系统中构造支持属性撤销的属性基加密方案[10-11]提供了思路. 这种撤销方式,必须重新计算相关访问结构的密文,且计算量与属性的个数呈线性关系,对于移动用户而言成本太高,并不适用于手机端用户. 文献[12]通过在用户的私钥和密文中嵌入代理重加密技术,从而大大降低了昂贵的密钥更新带来的撤销开销.

在属性基加密中,由于将一系列描述用户属性的集合作为公钥,而加密者在制定访问策略生成密文时,通常将这个访问规则和密文一起发布,因此系统中任意试图解密的用户都能够推出一些敏感信息(甚至推出可能的接收者),这使得用户的个人数据置于高泄露风险中(比如针对商家发布的密文可以分析其潜在的盈利模式,或者针对用户发布的密文分析出其敏感个人信息). Shi 等人[13] 提出谓词加密方案为这一问题提供了新思路. Nishide 等人[14] 构造了一个使用通配符以达到部分隐藏访问结构的方案. Li 等人[15] 提出了匿名密文策略属性基加密方案,该方案在生成属性私钥时通过盲化用户身份来达到匿名性. Lai 等人[16-17] 提出了 2 个高效、表达能力强的密文策略属性基加密方案. 在系统初始阶段只公布属性名称,由于数据拥有者在加密时隐藏了属性值,故能保护用户部分隐私,并在完全安全模型下证明了方案的安全性.

随着当今社会步入移动互联网时代,更多地使用移动端设备访问云存储环境下的数据成为了一种发展趋势. 对于使用移动端设备的用户而言,系统在提供安全性的基础上必须不能增加其计算负担和通信负担,而传统的属性基加密方案在解密操作中大量的双线性对运算会带来较大电池的耗费,所以将部分计算外包给云存储提供方进行操作有很大的经济性、很好的系统可扩展性和访问性. Green 等人[18] 提出一种将计算代价较高的数据加密操作外包到云端的方案,对于在使用移动设备的用户而言,将降低用户端的计算代价. 为了保护用户隐私,Han 等人[19] 构造了隐私保持的分布式密钥策略属性基加密方案. 为了提高效率,张洁等人[20] 提出了完全安全且密文长度固定的分层内积加密方案. 最近,Liu 等人[21-23] 和 Ning 等人[24-25] 对 CP-ABE 方案中的黑盒可追踪性、白盒可追踪性和支持大属性域等方面进行了系统、深入的研究. 提出的方案不仅可追踪泄露解密密钥的恶意用户而且对恶意用户追踪的系统存储开销为常量,更加适合于实际应用需求,推动了属性基密码的发展.

针对密文策略属性基加密方案的用户撤销的必要性、访问结构的隐私性和计算效率问题,本文构造了一个支持隐私保护和用户撤销的属性基加密方案,保证了系统的安全性. 在方案中,密钥的生成是通过数据拥有者和授权中心进行的,当系统存在用户撤销时,通过提供一组密钥更新机制进一步确保系统的安全性,且由云存储提供方进行重加密操作

以保护存储在云端的敏感数据,降低了用户的计算消耗.该方案允许满足属性集合的授权用户访问云端数据,以一种安全的方式将数据外包给云存储提供方,将计算代价高的加解密操作交给云存储提供方执行,以降低移动设备端的用户总通信成本.为了遏制云端的不端行为或对云端恶意攻击,提供了对转换密文的验证功能,保证了转换后密文未被非法替换且避免造成不良后果.为了达到完全隐藏访问结构,属性名及属性值不公开,即解密者不知道自己的哪些属性可以解密密文,本文采用多值属性与或门来表达访问结构,提高了系统的灵活性.

1 预备知识

定义 1. 双线性映射[26].设置 G 和 G_T 为 2 个阶为 p 的乘法循环群,其中 p 是一个大素数.一个双线性映射 $e:G\times G\rightarrow G_T$ 应具有如下性质:

1) 双线性. $\forall g\in G$, $\forall h\in G$, $\forall a,b\in\mathbb{Z}_p$,有 $e(g^a,h^b)=e(g,h)^{ab}$.

2) 非退化性. $\exists g\in G$,使得 $e(g,g)\neq 1$.

定义 2. 访问结构[27].设 n 个参与者集合为 $\{P_1,P_2,\cdots,P_n\}$,其中授权的参与者子集为 $\Gamma\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$,非授权的参与者子集为 $\Gamma^c=2^{\{P_1,P_2,\cdots,P_n\}}\setminus\Gamma$. B,C 表示 $\{P_1,P_2,\cdots,P_n\}$ 子集,对于任意 B,C,若 $B\in\Gamma$ 且 $B\subseteq C$,则 $C\in\Gamma$ 成立,那么就说集合 Γ 是一个单调的访问结构.一个访问结构是 $\{P_1,P_2,\cdots,P_n\}$ 的非空子集集合(或单调集合),即 $\Gamma\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\setminus\{\varnothing\}$.设 X 表示参与者任意子集,若 $X\in\Gamma$,则称其为授权的集合,反之则称为非授权的集合.本文所用的访问结构为多值属性的与或门形式.

定义 3. 判定性双线性 Diffie-Hellman (DBDH) 假设.挑战者根据安全参数 κ 选择素数阶为 p 的乘法循环群 G,g 为群 G 的生成元,双线性映射为 e,挑战者随机选择 $a,b,c\in\mathbb{Z}_p^*$.当给定元组 $[g,g^a,g^b,g^c]$ 时,一个概率的多项式时间敌手 $\mathcal{A}$ 区分群 G 的有效元组 $e(g,g)^{abc}$ 与群 G 中的随机元素 R 是否相等,称为 DBDH 问题.

敌手 $\mathcal{A}$ 解决群 G 中的 DBDH 问题是困难的,称为 DBDH 假定.敌手 $\mathcal{A}$ 解决 DBDH 问题优势为

$$|Pr[\mathcal{A}(g,g^a,g^b,g^c,A=e(g,g)^{abc})=0]-Pr[\mathcal{A}(g,g^a,g^b,g^c,A=R)=0]|<\varepsilon.$$

定义 4. 离散对数困难问题假设.令 G 为素数阶 p 的乘法循环群,g 为群 G 的生成元,$e:G\times G\rightarrow G_T$ 为双线性映射.随机选取 $x\in\mathbb{Z}_p^*$,给定元组 $[G,G_T,p,e,g,g^x]$,不存在概率多项式时间敌手 $\mathcal{A}$ 以不可忽略的优势计算出 x. $\mathcal{A}$ 解决离散对数优势为 $Adv_{\mathcal{A}}=|Pr[\mathcal{A}(G,G_T,p,e,g,g^x)=x]|<\varepsilon$.

2 属性基加密方案形式化描述

方案包含 4 个实体:1)数据拥有者负责生成自己的私钥 SK_{DO} 并发送其公钥 PK_{DO} 到公共区域,指定相应的访问结构并上载密文到云存储提供方(CSP);2)CSP 负责为系统中的合法用户存储密文数据(原始密文、更新后的密文、转换后的密文等),这里假设 CSP 是诚实的,但是好奇的;3)授权中心负责系统的初始化、合法用户的密钥生成、系统版本号以及密文和密钥的更新操作;4)数据用户从授权中心处获得组私钥和其用户私钥,从 CSP 处下载密文,并对密文的正确性进行验证,当且仅当其属性列表与密文中内嵌的访问结构相匹配且密文未被替换时成功解密密文.该方案的形式化定义描述如下:

1) 开始算法.授权中心以属性集合 U 以及系统安全参数 κ 为输入,该算法返回系统公开参数 $params$ 和系统主密钥 MK.授权中心发布系统公开参数 $params$、组公钥 GPK、版本号 vn,并保存主密钥 MK、组私钥 GSK.数据拥有者选择 SK_{DO} 作为私钥,计算公钥 PK_{DO} 并发送到公共区域.算法形式化描述为 $\text{Setup}(2^\kappa)\rightarrow(params,MK,GSK,SK_{DO})$.

2) 密钥生成算法.该算法以用户的属性列表 L、系统主密钥 MK 以及系统公开参数 $params$ 作为输入,返回用户的私钥 SK_L.算法形式化描述为 $\text{KeyGen}(params,MK,L)\rightarrow SK_L$.

3) 加密算法.数据拥有者以访问结构 W、消息 m 以及系统公共参数 $params$ 为输入,返回密文 CT.算法形式化描述为 $\text{Encrypt}(params,M,W)\rightarrow CT$.

4) 解密算法.数据用户以密文 CT、私钥 SK_L 以及系统公开参数 $params$ 作为输入,运行该算法,如果 $L\models W$ 且通过对密文正确性验证,数据用户可以正确解密密文 CT 得到消息 m.否则输出 $\perp$.算法形式化描述为 $\text{Decrypt}(params,CT,SK_L)\rightarrow m/\perp$.

当系统中的用户需要撤销时,还需要如下算法:

1) 重加密算法.授权中心运行该算法,在安全信道下发送新的组私钥 GSK_{vn} 给系统中的合法用户,其中 vn 为此时版本号标识,并更新授权用户的部分私钥 $D_{2,vn}$,同时授权中心计算重加密密钥为 ck_{vn} 发送给 CSP,CSP 计算新的密文 CT_{vn}.算法形式

化描述为 ReKey($params$, GSK_x)→ck_{vn}, CT_{vn}, $D_{2,vn}$.

2) 转换密钥生成算法. 该算法以系统公共参数 $params$ 和用户私钥 SK_L 为输入,返回转换密钥 TK_L 和恢复私钥 HK_L. 算法形式化描述为 TKGen($params$,SK_L)→TK_L,HK_L.

3) 转换部分密文算法. 该算法以系统公开参数 $params$、密文 CT 和转换密钥 TK_L 为输入,返回转换后的密文 CT'. 算法形式化描述为 TK-Encrypt($params$,CT,TK_L)→CT'.

4) 转换后解密算法. 该算法以系统公共参数 $params$、密文 CT、转换后的密文 CT' 和用户恢复私钥 HK_L 为输入,如果 $L\models W$,通过密文正确性验证则可以正确解密密文 CT 得到消息 m,否则算法失败并输出 $\perp$. 算法形式化描述为 TK-Decrypt($params$,CT,CT',HK_L)→$m/\perp$.

3 属性基加密方案安全性定义

3.1 安全模型

基于文献[14,18],本文的安全模型定义如下:

1) 初始化阶段. 敌手 $\mathcal{A}$ 提交 2 个挑战的访问结构 W_0,W_1,并将其发送给挑战者 $\mathcal{B}$.

2) 开始阶段. 挑战者运行开始算法,返回系统公开参数 $params$ 给 $\mathcal{A}$.

3) 询问阶段 1. 挑战者首先创建一个空集合 D 和空表 T,敌手 $\mathcal{A}$ 提交相应的属性给挑战者,以便在属性集合中进行私钥询问,其中 $L\models W_0^* \wedge L\models W_1^*$ 或者 $L\not\models W_0^* \wedge L\not\models W_1^*$.

① 私钥询问. 挑战者运行密钥生成算法并设置 $D=D\cup\{L\}$,返回私钥 SK_L 给 $\mathcal{A}$. 其中 $\mathcal{A}$ 可以进行多次询问.

② 转换密钥询问. 挑战者在表 T 中查找元组(L, SK_L, TK_L, HK_L),若存在则返回转换密钥 TK_L;否则,挑战者运行密钥生成算法、转换密钥生成算法,并且在表 T 中存储元组(L, SK_L, TK_L, HK_L),返回转换密钥 TK_L 给敌手 $\mathcal{A}$. 如果敌手 $\mathcal{A}$ 在属性集合 L 下进行了私钥询问,则不允许 $\mathcal{A}$ 继续进行转换密钥询问.

4) 挑战阶段. 敌手 $\mathcal{A}$ 提交 2 个相同长度的消息 M_0, M_1. 挑战者进行公平的抛硬币实验选择随机值 $b\in\{0,1\}$,并运行加密算法生成密文 CT^*,挑战者将密文 CT^* 返回给敌手 $\mathcal{A}$. 这里注意到,如果 $L\models W_0^* \wedge L\models W_1^*$,意味着 $M_0=M_1$.

5) 询问阶段 2. 敌手 $\mathcal{A}$ 重复挑战上述询问阶段 1 的询问. 如果 $M_0\neq M_1$,敌手 $\mathcal{A}$ 不能提交属性列表 $L\in D$ 使得 $L\models W_0^* \wedge L\models W_1^*$.

6) 猜测阶段. 敌手 $\mathcal{A}$ 输出对随机值 b 的一个猜测 b'. 如果 $b=b'$,表示猜测成功,否则失败.

定义 5. 如果存在概率多项式时间敌手 $\mathcal{A}$,在最多时间 t 内进行至多 q 次密钥询问,以可忽略的优势 $Adv_{\mathcal{A}}=|Pr[b=b']-\frac{1}{2}|\leqslant\varepsilon$ 赢得上述游戏,则称 CP-ABE 加密方案是(t,q,ε)安全的.

3.2 可验证性

基于文献[28],可验证性安全游戏定义如下:

1) 开始阶段. 挑战者运行开始算法,返回系统公共参数 $params$ 给 $\mathcal{A}$.

2) 询问阶段 1. 挑战者首先创建一个空集合 D 和空表 T,敌手 $\mathcal{A}$ 提交相应的属性列表 S 给挑战者,以便在属性集合下进行私钥询问.

① 私钥询问. 挑战者运行密钥生成算法,返回私钥 SK_L 给 $\mathcal{A}$. 其中, $\mathcal{A}$ 可以进行多次询问.

② 转换密钥询问. 挑战者运行密钥生成算法、转换密钥生成算法,并且在表 T 存储元组(L,SK_L,TK_L,HK_L),返回转换密钥 TK_L 给敌手 $\mathcal{A}$. 如果敌手 $\mathcal{A}$ 在属性集合 L 下进行了私钥询问,则不允许 $\mathcal{A}$ 继续进行转换密钥询问.

3) 挑战阶段. 敌手 $\mathcal{A}$ 提交访问结构 W、明文消息 m^*,并运行加密算法生成转换后的密文 CT^*,挑战者将密文 CT^* 返回给敌手 $\mathcal{A}$.

4) 询问阶段 2. 敌手 $\mathcal{A}$ 重复询问阶段 1 的询问.

5) 输出阶段. $\mathcal{A}$ 输出属性集合 S^* 和转换后的密文 CT'^*,若 TK-Decrypt($params$,CT^*,CT'^*,$HK_{L\in S^*}$)$\notin\{m^*,\perp\}$,则敌手赢得游戏.

定义 6. 在上述安全模型下,如果不存在概率多项式时间敌手 $\mathcal{A}$,以不可忽略的优势赢得与挑战者之间的游戏,则称 CP-ABE 加密方案是可验证的.

4 隐私保护和用户撤销的属性基加密方案

提出一个隐私保护且支持用户撤销的属性基加密方案. 支持云环境下的高效数据外包操作,同时对密文转换的正确性进行了验证,使系统更加灵活且安全. 具体构造如下:

1) 开始算法. 令 $U=\{1,2,\cdots,n\}$ 为属性集合空间,κ 为系统安全参数,$e:G\times G\to G_T$ 为双线性映射. 其中,G 和 G_T 为素数阶 $p>2^\kappa$ 的乘法循环群; g,u,

$v,d\in G$. 授权中心随机选择 $\alpha\in\mathbb{Z}_p^*$,$\delta\in\mathbb{Z}_p^*$,计算 $Y=e(g,g)^{\alpha}$,g^{δ},为每个属性 att_i 选择随机值 $t_{i,j}\in\mathbb{Z}_p$ $(i\in[1,n],j\in[1,n_i])$,计算 $T_{i,j}=g^{t_{i,j}}$. 数据拥有者随机选择 $\beta\in\mathbb{Z}_p^*$ 作为私钥 SK_{DO},计算公钥 $PK_{\mathrm{DO}}=\{g^{\beta},g^{1/\beta}\}$. $H:G\rightarrow\mathbb{Z}_p^*$ 是抗碰撞 Hash 函数;$params=\{Y,p,G,G_T,e,g,u,v,d,g^{\delta},\{T_{i,j}\}\}$ 是系统参数,其中 $i\in[1,n]$,$j\in[1,n_i]$;系统主密钥为 $MK=\{\alpha,g^{\alpha},\delta\}$.

为了进一步提高安全性,授权中心选择随机值 $u_0\in Z_p^*$ 作为组私钥 GSK,并将其线下发送给注册的用户,计算 $GPK=g^{u_0}$ 作为组公钥,授权中心初始化组密钥版本号 $vn=0$.

2) 密钥生成算法. 令 $L=[L_1,L_2,\cdots,L_i,L_{i+1},\cdots,L_n]=[v_{1,j\in[1,n_i]},v_{2,j\in[1,n_i]},\cdots,v_{i,j\in[1,n_i]},v_{i+1,j\in[1,n_i]},\cdots,v_{n,j\in[1,n_i]}]$ 为某用户的属性列表. 授权中心选择随机值 $r\in\mathbb{Z}_p^*$,计算 $D_0=g^{\frac{\alpha-\gamma}{\beta}}$,授权中心为每个属性 att_i 随机选择 $\lambda_i\in\mathbb{Z}_p^*$,计算 $D_{i,1}=g^{r+\lambda_i t_{i,j}}$,$D_{i,2}=g^{\lambda_i}$,其中 $i\in[1,n]$,$j\in[1,n_i]$,为授权的用户计算 $D_2=(g^{1/\beta})^{u_0}$. 用户私钥为

$$SK_L=(D_0,\forall v_{i\in[1,n],j\in[1,n_i]}\in L:\{D_{i,1},D_{i,2}\},D_2).$$

3) 加密算法. 数据拥有者选择明文消息 $m\in G_T$ 在其指定的访问策略 $W=[W_1,W_2,\cdots,W_n]$ 下进行加密.

步骤 1. 数据拥有者选择随机消息 $m'\in G_T$,计算 $\hat{c}=u^{H(m)}v^{H(m')}d$. 数据拥有者对其将要进行分享的消息 m 进行操作,随机选择 $s\in\mathbb{Z}_p^*$,计算密文 $C_0=mY^s e(g,g)^{u_0 s}=m e(g,g)^{\alpha s+u_0 s}$,$C_1=g^{\beta s}$,$C_2=g^{\delta s}$.

对于选择的随机消息 m',数据拥有者随机选择 $s'\in\mathbb{Z}_p^*$,计算 $C_3=m'Y^{s'}e(g,g)^{u_0 s'}$,$C_4=g^{\beta s'}$,$C_5=g^{\delta s'}$.

步骤 2. 对于要加密的明文消息 m,设 s 为访问结构的根节点,设定所有的儿子节点为未标记,标记根节点为已标记,为每个未标记的非叶子节点递归运算.

若非叶子节点为“与”门,且其儿子节点状态为未标记,随机选择 $s_i\in\mathbb{Z}_p$,$1\leqslant s_i\leqslant p-1$,设置最后一个儿子节点的值为 $s_j=s-\sum_{i=1}^{j-1}s_i \bmod p$,并标记此节点为已标记.

反之若为“或”门,标记该节点下的任意节点的值为 s,并设置此节点为已标记.

对于叶子节点,加密者计算 $C_{i,j,1}=g^{s_i}$,$C_{i,j,2}=T_{i,j}^{s_i}$,并输出密文为

$$CT_{\mathrm{own1}}=\{C_0,C_1,C_2,\{C_{i,j,1},C_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]}\}.$$

同样地,对于随机消息 m',数据拥有者计算密文 $CT_{\mathrm{own2}}=\{C_3,C_4,C_5,\{\overline{C}_{i,j,1},\overline{C}_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]}\}$. 最终密文为 $CT=\{vn=0,\hat{c},CT_{\mathrm{own1}},CT_{\mathrm{own2}}\}$.

4) 解密算法. 当数据用户从云存储提供方(CSP)中得到密文 CT 后,检查密文 CT 和私钥 SK_L 的版本号的一致性,若任意一方破坏了一致性,数据用户就向授权中心申请更新私钥. 数据用户在不知道访问结构 W 的情况下试图用其私钥 SK_L 解密密文 CT. 对任意的 $1\leqslant i\leqslant n$,如果该用户属性列表满足访问结构即 $L\models W$,那么数据用户可以通过如下计算进行解密操作:

步骤 1. 计算 $F=\prod_{i=1}^{n}e(C_{i,j,2},D_{i,2})$,$O=\prod_{i=1}^{n}e(C_{i,j,1},D_{i,1})$,$S=e(C_1,D_0)$,$B=\prod_{i=1}^{n}e(C_1,D_2)$,计算得到 $m=\dfrac{C_0 F}{OSB}$.

解密操作的正确性验证如下:

$$F=\prod_{i=1}^{n}e(C_{i,j,2},D_{i,2})=\prod_{i=1}^{n}e(T_{i,j}^{s_i},g^{\lambda_i})=\prod_{i=1}^{n}e(g,g)^{t_{i,j}s_i\lambda_i},$$

$$O=\prod_{i=1}^{n}e(C_{i,j,1},D_{i,1})=\prod_{i=1}^{n}e(g^{s_i},g^{r+\lambda_i t_{i,j}})=\prod_{i=1}^{n}e(g,g)^{s_i r}\prod_{i=1}^{n}e(g,g)^{s_i t_{i,j}\lambda_i},$$

$$S=e(C_1,D_0)=e(g^{\beta s},g^{\frac{\alpha-\gamma}{\beta}})=e(g,g)^{(\alpha-\gamma)s},$$

$$B=e(C_1,D_2)=e(g^{\beta s},(g^{1/\beta})^{u_0})=e(g,g)^{u_0 s},$$

$$\frac{C_0 F}{OSB}=\frac{m e(g,g)^{\alpha s}e(g,g)^{u_0 s}\prod_{i=1}^{n}e(g,g)^{t_{i,j}s_i\lambda_i}}{\prod_{i=1}^{n}e(g,g)^{s_i r}\prod_{i=1}^{n}e(g,g)^{s_i t_{i,j}\lambda_i}e(g,g)^{(\alpha-\gamma)s}e(g,g)^{u_0 s}}=$$

$$\frac{m e(g,g)^{\alpha s}e(g,g)^{u_0 s}\prod_{i=1}^{n}e(g,g)^{t_{i,j}s_i\lambda_i}}{\prod_{i=1}^{n}e(g,g)^{s_i r}\prod_{i=1}^{n}e(g,g)^{s_i t_{i,j}\lambda_i}e(g,g)^{\alpha s}e(g,g)^{-\gamma s}e(g,g)^{u_0 s}}=m.$$

步骤2. 计算 $F'=\prod_{i=1}^{n} e(\bar{C}_{i,j,2}, D_{i,2})$, $O'=\prod_{i=1}^{n} e(\bar{C}_{i,j,1}, D_{i,1})$, $S'=e(C_4, D_0)$, $B'=\prod_{i=1}^{n} e(C_4, D_2)$, 计算得到 $m'=\frac{C_3 F'}{O' S' B'}$. 解密操作的正确性验证与步骤1类似,这里不再赘述.

步骤3. 通过如下方法测试密文是否被替换,验证 $\hat{c}=u^{H(m)} v^{H(m')} d$,若是,则输出消息 m;否则,输出 $\perp$. 尽管密文消息 CT_{own2}, $\hat{c}$ 为冗余部分,但保证了消息的正确性.

5) 重加密算法. 当系统中的用户需要撤销时,为了保证安全性其系统权限应被收回,此时,授权中心选择新的随机值 $u_x \in \mathbb{Z}_p^*$ 作为新的组私钥 GSK_x,其中,x 为此时版本号标识,当系统中的合法用户需要访问数据时通过安全的线下通道发送给他们,同样地更新授权用户的私钥部分 $D_{2,vn}=(g^{1/\beta})^{u_x}$,此时云存储提供方将向授权中心请求重加密操作以便此时授权的用户可以正确解密,密文从版本 $vn=0$ 更新到 $vn=x$,授权中心计算重加密密钥为 $ck_{vn}=\{g^{\frac{u_x-u_0}{\delta}}\}$,并发送给 CSP,CSP 计算版本号为 $vn=x$ 的新密文 CT_{vn}.

对于密文的第1部分 $CT_{\text{own1},vn}$,计算如下:

$$C_{0,vn}=C_0\, e(C_2, ck_{vn})=m\, e(g,g)^{\alpha s+u_0 s}\, e(g^{\delta s}, g^{\frac{u_x-u_0}{\delta}})=m\, e(g,g)^{\alpha s+u_x s}.$$

对于密文的第2部分 $CT_{\text{own2},vn}$,进行如下计算:

$$C_{3,vn}=C_3\, e(C_5, ck_{vn})=m'\, e(g,g)^{\alpha s'+u_0 s'}\, e(g^{\delta s'}, g^{\frac{u_x-u_0}{\delta}})=m\, e(g,g)^{\alpha s'+u_x s'}.$$

更新后密文 $CT_{vn}=\{CT_{\text{own1},vn}, CT_{\text{own2},vn}\}$ 如下:

$$CT_{\text{own1},vn}=\{vn=x, \hat{c}, C_{0,vn}, C_1, C_2, \{C_{i,j,1}, C_{i,j,2}\}_{i\in[1,n], j\in[1,n_i]}\},$$

$$CT_{\text{own2},vn}=\{vn=x, \hat{c}, C_{3,vn}, C_4, C_5, \{\bar{C}_{i,j,1}, \bar{C}_{i,j,2}\}_{i\in[1,n], j\in[1,n_i]}\}.$$

更新后的密文解密操作的正确性验证如下:

$$\frac{C_{0,vn}\prod_{i=1}^{n} e(C_{i,j,2}, D_{i,2})}{\prod_{i=1}^{n} e(C_{i,j,1}, D_{i,1})\, e(C_1, D_0)\, e(C_1, D_{2,vn})}=\frac{m\, e(g,g)^{\alpha s+u_x s}\prod_{i=1}^{n} e(g,g)^{t_{i,j} s_i \lambda_i}}{\prod_{i=1}^{n} e(g,g)^{s_i r}\prod_{i=1}^{n} e(g,g)^{s_i t_{i,j} \lambda_i}\, e(g,g)^{(\alpha-\gamma)s}\, e(g^{\beta s}, g^{1/\beta})^{u_x}}=m,$$

$$\frac{C_{3,vn}\prod_{i=1}^{n} e(\bar{C}_{i,j,2}, D_{i,2})}{\prod_{i=1}^{n} e(\bar{C}_{i,j,1}, D_{i,1})\, e(C_4, D_0)\, e(C_4, D_{2,vn})}=\frac{m'\, e(g,g)^{\alpha s'+u_x s'}\prod_{i=1}^{n} e(g,g)^{t_{i,j} s'_i \lambda_i}}{\prod_{i=1}^{n} e(g,g)^{s'_i r}\prod_{i=1}^{n} e(g,g)^{s'_i t_{i,j} \lambda_i}\, e(g,g)^{(\alpha-\gamma)s'}\, e(g^{\beta s'}, g^{1/\beta})^{u_x}}=m'.$$

6) 转换密钥生成算法. 该算法以用户私钥 $SK_L=(D_0, \forall v_{i\in[1,n], j\in[1,n_i]}\in L: \{D_{i,1}, D_{i,2}\}, D_2)$ 和系统公共参数 $params$ 为输入,随机选择 $z\in\mathbb{Z}_p^*$,以如下方法计算转换密钥 $TK_L=\{D'_0=D_0^{1/z}, D'_2=D_2^{1/z}, \{D'_{i,1}=D_{i,1}^{1/z}, D'_{i,2}=D_{i,2}^{1/z}\}_{i\in[1,n], j\in[1,n_i]}\}$,并保存 $HK_L=z$ 作为恢复密钥.

7) 转换部分密文算法. 该算法以系统公共参数 $params$、密文 $CT=\{CT_{\text{own1}}, CT_{\text{own2}}\}$ 以及转换密钥 $TK_L=\{D'_0, D'_2, \{D'_{i,1}, D'_{i,2}\}_{i\in[1,n]}\}$ 作为输入,计算转换后的部分密文如下:

$$K'_{\text{own1}}=\frac{\prod_{i=1}^{n} e(C_{i,j,1}, D'_{i,1})\, e(C_1, D'_0)\, e(C_1, D'_2)}{\prod_{i=1}^{n} e(C_{i,j,2}, D'_{i,2})}=\frac{\prod_{i=1}^{n} e(g^{s_i}, g^{\frac{r+\lambda_i t_{i,j}}{z}})\, e(g^{\beta s}, g^{\frac{\alpha-\gamma}{z\beta}})\, e(g^{\beta s}, g^{\frac{u_0}{z\beta}})}{\prod_{i=1}^{n} e(g^{t_{i,j} s_i}, g^{\frac{\lambda_i}{z}})}=e(g,g)^{\frac{\alpha s+u_0 s}{z}}.$$

$$K'_{\text{own2}}=\frac{\prod_{i=1}^{n}e(\overline{C}_{i,j,1},D'_{i,1})\ e(C_4,D'_0)\ e(C_4,D'_2)}{\prod_{i=1}^{n}e(\overline{C}_{i,j,2},D'_{i,2})}=$$

$$\frac{\prod_{i=1}^{n}e(g^{s'_i},g^{\frac{r+\lambda_i t_{i,j}}{z}})\ e(g^{\beta s'},g^{\frac{\alpha-\gamma}{z\beta}})\ e(g^{\beta s'},g^{\frac{u_0}{z\beta}})}{\prod_{i=1}^{n}e(g^{t_{i,j}s'_i},g^{\frac{\lambda_i}{z}})}=$$

$$e(g,g)^{\frac{\alpha s'+u_0 s'}{z}}.$$

则 $CT'=\{vn=0,K'=\hat{c},K_1=C_0,K'_{\text{own1}},K_2=C_3,K'_{\text{own2}}\}$为转换后密文.

8) 转换后解密算法. 该算法以系统公共参数 $params$、密文 CT、转换后的密文 CT'和用户恢复私钥 $HK_L=z$ 为输入,若 $K'\neq\hat{c}$, $K_1\neq C_0$, $K_2\neq C_3$,则算法输出$\perp$. 如果 $L\models W$,数据用户可以通过 $m=K_1/K'^{z}_{\text{own1}}$,$m'=K_2/K'^{z}_{\text{own2}}$,并验证 $K'=u^{H(m)}v^{H(m')}d$ 来正确解密密文 CT 得到消息 m;否则,算法失败并输出$\perp$.

5 安全性分析和证明

本文提出的 CP-ABE 方案能够抵抗合谋攻击,因为要恢复出消息 m 必须要恢复出因子 $e(g,g)^{\alpha s}$,而因子 $e(g,g)^{\alpha s}$依赖于对密文部件 C_1 和私钥部件 D_0 进行的双线性对运算,$e(C_1,D_0)=e(g^{\beta s},g^{\frac{\alpha-\gamma}{\beta}})=\frac{e(g,h)^{\alpha s}}{e(g,h)^{s\gamma}}$. 由于算法针对不同的用户生成不同的秘密值 γ,所以 $e(g,h)^{s\gamma}$为盲化因子,因此该方案能够抵抗合谋攻击. 在该方案中通过选择组公钥 GPK 提供了属性撤销机制,适用于用户撤销,为系统提供了又一重安全保障. 用户只有在拥有组私钥 GSK,且其属性列表符合密文中的访问结构时才能正确解密. 若系统中的可信用户泄露了组私钥 GSK,因为该方案具有抗合谋攻击性,所以方案的安全性依然依赖于用户的属性列表是否能够满足访问结构. 对于 CSP,因其不知道数据拥有者的密钥 SK_{DO}和用户的私钥 SK_L,是无法解密用户存储到云端的密文. 此外,当系统中存在用户撤销时,数据拥有者可以向 CSP 申请重加密密文以便避免因 GSK 的泄露来带来的安全隐患. 尽管 CSP 使用重加密密钥对密文进行重加密,但因重加密密钥 ck_{vn} 依赖于离散对数困难问题,CSP 在重加密过程中不会获取任何有用消息.

定理 1. 如果 DBDH 假设在群(G,G_T,p,e)中成立,那么不存在概率多项式时间敌手 $\mathcal{A}$,在最多时间 t 内,进行至多 q 次密钥询问的情况下以不可忽略的优势 ε 攻破本文提出的方案.

为了证明安全性,我们定义了 2 个游戏 $Game_0$,$Game_1$. 游戏 $Game_0$ 和上述方案在真实情况下挑战密文 CT^* 生成方式相同;而在游戏 $Game_1$ 中,挑战密文 $CT^*=\{\hat{c},CT_{\text{own1}},CT_{\text{own2}}\}$选取随机值 $\hat{c}\in G$ 作为验证消息,挑战密文的其他部分生成和游戏 $Game_0$ 中一样. 本文通过如下 2 个引理证明方案的安全性,引理 1 证明游戏 $Game_0$, $Game_1$ 的不可区分性;引理 2 证明敌手 $\mathcal{A}$ 赢得游戏 $Game_1$ 的优势可以忽略.

引理 1. 如果 DBDH 假设在群(G,G_T,p,e)中成立,那么不存在概率的多项式时间敌手 $\mathcal{A}$,在选择集合安全模型下以不可忽略的优势 ε 区分游戏 $Game_0$ 和游戏 $Game_1$.

证明. 假设存在一个多项式时间敌手 $\mathcal{A}$,在选择集合模型下以不可忽略的优势 ε 区分游戏 $Game_0$ 和 游戏 $Game_1$,则可以找到一个高效的模拟器 $\mathcal{B}$,它在敌手 $\mathcal{A}$ 的帮助下成功解决 DBDH 问题.

挑战者选择随机生成元 $g\in G$ 和双线性群(e,p,G,G_T),挑战者随机地进行抛硬币实验选择随机数 $\tau\in\{0,1\}$,若 $\tau=0$,挑战者将元组$(g^a,g^b,g^c,V)=(g^a,g^b,g^c,e(g,g)^{abc})$发送给模拟器 $\mathcal{B}$;否则,挑战者将元组 $(g^a,g^b,g^c,e(g,g)^w)$发送给模拟器 $\mathcal{B}$,其中 $a,b,c,w\in_R\mathbb{Z}_p$.

1) 初始化阶段. 敌手 $\mathcal{A}$ 提交 2 个即将挑战的访问结构 W_0, W_1,并发送给模拟器 $\mathcal{B}$,模拟器 $\mathcal{B}$ 随机地进行抛硬币实验选取随机数 $\tau\in\{0,1\}$.

2) 开始设置阶段. 模拟器 $\mathcal{B}$ 生成版本号 $vn=0$ 的系统公共参数,计算 $Y=e(g^a,g^b)=e(g,g)^{ab}$,即 $\alpha=ab$,其中 g 为群 G 的生成元,$\mathcal{B}$ 随机选择值 $x,y,z,\delta\in\mathbb{Z}_p^*$ 和抗碰撞 Hash 函数 $H:G\to\mathbb{Z}_p^*$,计算 $u=g^x$,$v=g^y$,$d=g^z$,g^δ. $\mathcal{B}$ 随机选择 $\beta\in\mathbb{Z}_p^*$ 并计算$\{g^\beta,g^{1/\beta}\}$. 对属性集合中的每个属性,$\mathcal{B}$ 随机选择 $t_{i,j}\in\mathbb{Z}_p$ $(i\in[1,n],j\in[1,n_i])$,计算 $T_{i,j}=g^{t_{i,j}}$. 模拟器 $\mathcal{B}$ 选择随机值 $u_0\in\mathbb{Z}_p^*$ 作为组私钥 GSK,计算 $GPK=g^{u_0}$ 作为组公钥,并初始化组密钥版本号 $vn=0$. $\mathcal{B}$ 将如下系统公共参数发送给敌手 $\mathcal{A}$.

$$params=\{Y,p,G,G_T,e,g,u,v,d,g^\delta,g^\beta,g^{1/\beta},\{T_{i,j}\}\},$$

其中,$i\in[1,n]$,$j\in[1,n_i]$.

3) 挑战前询问阶段 1. 敌手 $\mathcal{A}$ 提交的属性列表 L 给挑战者,以供向挑战者询问私钥,其中 $L\not\models W_0\wedge L\not\models W_1$.

① 私钥询问. $\mathcal{B}$ 选择为每个属性 $i\in[1,n]$ 随机选择 $\lambda_i'\in\mathbb{Z}_p^*$，设置 $r=-\lambda_i' t_{i,j}-\alpha'$，并按照如下方法计算私钥 $\{D_0,\{D_{i,1},D_{i,2}\},D_2\}$.

$D_0=(g^{1/\beta})^{\alpha+\lambda_i' t_{i,j}+\alpha'}=(g^{1/\beta})^{(\alpha+\alpha')+\lambda_i' t_{i,j}}=g^{\frac{\gamma+\lambda_i' t_{i,j}}{\beta}}$，其中 $\gamma=\alpha+\alpha'$，α' 为随机数.

$D_{i,1}=g^{\gamma+\lambda_i' t_{i,j}}=g^{-\lambda_i' t_{i,j}-\alpha'+\lambda_i' t_{i,j}}=g^{-\alpha'}$，

$D_{i,2}=g^{\lambda_i'}$，

$D_2=(g^{1/\beta})^{u_0}$，

至此，私钥 $SK_L=(D_0,\{D_{i,1},D_{i,2}\},D_2)$ 的所有有效部件已被构造出来.

② 转换密钥询问. $\mathcal{B}$ 在表 T 中查找元组 (L,SK_L,TK_L,HK_L)，若存在则返回转换密钥 TK_L；否则，$\mathcal{B}$ 随机选择 $z\in\mathbb{Z}_p^*$，设置转换密钥 TK_L 如下：

$\overline{D}_0'=g^{\frac{z-\gamma}{\beta}}$，$\overline{D}_2'=(g^{1/\beta})^{u_0}$，$\overline{D}_{i,1}'=g^{-\alpha'}$，$\overline{D}_{i,2}'=g^{\lambda_i'}$.

在这里，$\mathcal{B}$ 并不知道实际的恢复密钥 $HK_L=\dfrac{u_0+\alpha}{u_0+z}$ 值.

4) 挑战阶段. 敌手 $\mathcal{A}$ 提交 2 个相同长度的挑战消息 $m_0,m_1\in G$，并发送给模拟器 $\mathcal{B}$. 如果 $m_0=m_1$，则模拟器 $\mathcal{B}$ 停止并输出一个随机猜测. 挑战者选择 2 个随机消息 $m_0',m_1'\in G$，随机选择 $\xi\in\{0,1\}$，返回在消息 m_ξ 下加密的密文如下：

$C_0=m_\xi e(g,g)^{\alpha c}\,e(g,g)^{u_0 c}=m_\xi e(g,g)^{\alpha c+u_0 c}$，

$C_1=g^{\beta c}$，

$C_2=g^{\delta c}$，

$\hat{c}=u^{H(m_\xi)}v^{H(m_\xi')}d$.

对于密文部件 $\{C_{i,j,1},C_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]}$，设 c 为访问结构的根节点，设定所有的儿子节点为未标记，标记根节点为已标记，为每个未标记的非叶子节点递归地进行如下运算：

若非叶子节点为“与”门，且其儿子节点状态为未标记，选择随机值 $h_i\in\mathbb{Z}_p(1\leqslant h_i\leqslant p-1)$，设置最后一个儿子节点的值为 $h_j=c\Big/\sum_{i=1}^{j-1}h_i$，并标记此节点.

反之若为“或”门，标记该节点下的任意节点的值为 c，并设置此节点为已标记.

对于叶子节点，加密者计算 $C_{i,j,1}=g^{h_i}$，$C_{i,j,2}=T_{i,j}^{h_i}$，则 $\{C_0,C_1,C_2,\{C_{i,j,1},C_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]}\}$ 为密文.

同样地，对于随机消息 $m_0',m_1'\in G$（挑战者对其按上述过程进行加密，这里不再赘述），并返回密文 $\{C_3,C_4,C_5,\{\overline{C}_{i,j,1},\overline{C}_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]}\}$.

模拟器 $\mathcal{B}$ 将密文 CT^* 发送给 $\mathcal{A}$.

5) 挑战后询问阶段 2. 敌手 $\mathcal{A}$ 重复挑战前询问阶段 1 的询问，$\mathcal{B}$ 如挑战前询问阶段 1 一样回应敌手 $\mathcal{A}$.

6) 猜测阶段. 敌手 $\mathcal{A}$ 输出一个关于随机值 ξ 的一个猜测 ξ'. 如果 $\xi'=\xi$，则模拟器 $\mathcal{B}$ 输出其对 τ 的猜测结果 $\tau'=0$；反之，如果 $\xi'\neq\xi$，则 $\mathcal{B}$ 输出其对 τ 的猜测结果 $\tau'=1$. 有如下 2 种情况：

① 当 $V=e(g,g)^{abc}$ 时，根据 DBDH 问题假设，敌手 $\mathcal{A}$ 在游戏中猜测到 $\xi'=\xi$ 的可能性至少为 ε，则有 $Pr[\xi'=\xi|V=e(g,g)^{abc}]\geqslant\dfrac{1}{2}+\varepsilon$. 当 $\xi'=\xi$ 时，模拟器 $\mathcal{B}$ 提交他对 τ 的猜测 τ'，那么 $Pr[\tau'=\tau|V=e(g,g)^{abc}]=\dfrac{1}{2}+\varepsilon$.

② 当 $V=e(g,g)^{v}$ 时，根据 DBDH 问题假设，值 V 为计算随机数 w 得到的，这意味着敌手 $\mathcal{A}$ 无法得到关于 ξ 的任何消息，即当 $\xi'\neq\xi$ 时，敌手 $\mathcal{A}$ 无法区分出 ξ，即 $Pr[\xi'\neq\xi|V=e(g,g)^{w}]=\dfrac{1}{2}$. 当 $\xi'\neq\xi$ 时，模拟器 $\mathcal{B}$ 提交他对 τ 的猜测 $\tau'=1$，那么 $Pr[\tau'=\tau|V=e(g,g)^{w}]=\dfrac{1}{2}$.

综上，$\mathcal{B}$ 成功解决 DBDH 困难问题的概率为

$$Adv=\frac{1}{2}(Pr[\tau'=\tau|V=e(g,g)^{abc}]+Pr[\tau'=\tau|V=e(g,g)^{w}])-\frac{1}{2}\geqslant\frac{\varepsilon}{2}.$$

证毕.

引理 2. 如果 DBDH 假设在群 (G,G_T,p,e) 中成立，则不存在概率多项式时间敌手 $\mathcal{A}$，在选择集合安全模型下以不可忽略的优势 ε 赢得游戏 $Game_1$.

证明. 在选择集合模型下，假设存在一个概率多项式时间敌手 $\mathcal{A}$，在最多时间 t 内，进行至多 q 次密钥询问的情况下以不可忽略的优势 ε 赢得游戏 $Game_1$，则可以找到一个高效的模拟器 $\mathcal{B}$，在敌手 $\mathcal{A}$ 的帮助下成功解决 DBDH 问题. 该引理的安全性证明如下：

挑战者随机选择生成元 $g\in G$ 和双线性群 (e,p,G,G_T)，挑战者随机地进行抛硬币实验选择随机数 $\tau\in\{0,1\}$. 若 $\tau=0$，挑战者将元组 $(g^a,g^b,g^c,V)=(g^a,g^b,g^c,e(g,g)^{abc})$ 发送给模拟器 $\mathcal{B}$；否则，挑战者将元组 $(g^a,g^b,g^c,e(g,g)^{w})$ 发送给模拟器 $\mathcal{B}$，其中 $a,b,c,w\in_R\mathbb{Z}_p$.

1) 初始化阶段. 敌手 $\mathcal{A}$ 提交 2 个即将挑战的访问结构 W_0，W_1，并发送给模拟器 $\mathcal{B}$，$\mathcal{B}$ 随机地进行抛硬币实验选取随机数 $\tau\in\{0,1\}$.

2) 开始设置阶段. $\mathcal{B}$ 计算 $Y=e(g^a,g^b)=e(g,g)^{ab}$,即 $\alpha=ab$. $\mathcal{B}$ 随机选择 $x,y,z,\beta,t_{i,j},u_0,\delta\in\mathbb{Z}_p^*$ ($i\in[1,n],j\in[1,n_i]$),设置抗碰撞 Hash 函数为 $H:G\rightarrow\mathbb{Z}_p^*$,$\mathcal{B}$ 计算 $u=g^x$,$v=g^y$,$d=g^z$,$\{g^\beta,g^{1/\beta}\}$,$T_{i,j}=g^{t_{i,j}}$,g^{u_0},g^δ. 模拟器 $\mathcal{B}$ 将如下系统公共参数发送给 $\mathcal{A}$.

$$params=\{Y,p,G,G_T,e,g,u,v,d,g^\beta,g^{1/\beta},g^\delta,\{T_{i,j}\}\},$$

其中,$i\in[1,n],j\in[1,n_i]$.

3) 询问阶段 1. 敌手 $\mathcal{A}$ 提交属性列表 L 给挑战者,以供向挑战者询问私钥,其中 $L\not\models W_0\wedge L\not\models W_1$. 模拟器 $\mathcal{B}$ 初始化列表 T、空集合 D. $\mathcal{B}$ 回应敌手 $\mathcal{A}$ 的私钥询问过程、转换密钥询问过程与引理 1 中类似. 针对敌手 $\mathcal{A}$ 的私钥询问,$\mathcal{B}$ 返回相应的私钥给敌手 $\mathcal{A}$,针对敌手 $\mathcal{A}$ 的转换密钥询问,$\mathcal{B}$ 返回相应的转换密钥给敌手 $\mathcal{A}$,同样,模拟器 $\mathcal{B}$ 并不知道实际的恢复密钥 HK_L 值. 注意,如果敌手 $\mathcal{A}$ 在属性集合 L 下进行了私钥询问,则不允许 $\mathcal{A}$ 继续在属性集合 L 下进行转换密钥询问.

4) 挑战阶段. 敌手 $\mathcal{A}$ 提交 2 个相同长度的挑战消息 $m_0,m_1\in G$,并发送给 $\mathcal{B}$. 如果 $m_0=m_1$,则 $\mathcal{B}$ 放弃此次实验并输出一个随机猜测. 挑战者进行公平的抛硬币实验选择随机值 $\xi\in\{0,1\}$,返回在消息 m_ξ 的密文如下:

$$C_0=m_\xi e(g,g)^{\alpha c}e(g,g)^{u_0 c}=m_\xi e(g,g)^{\alpha c+u_0 c},$$

$$C_1=g^{\beta c},$$

$$C_2=g^{\delta c}.$$

对于密文部件 $\{C_{i,j,1},C_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]}$,$\mathcal{B}$ 按照引理 1 中的方法生成相应的密文,这里不再赘述.

根据本文游戏的定义,$\mathcal{B}$ 选择一个随机消息 $m'\in G$,计算密文部件如下:

$$C_3=m'_\xi e(g,g)^{\alpha c}e(g,g)^{u_0 c}=m'_\xi e(g,g)^{\alpha c+u_0 c},$$

$$C_4=g^{\beta c},$$

$$C_5=g^{\delta c}.$$

对于密文部件 $\{\overline{C}_{i,j,1},\overline{C}_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]}$,$\mathcal{B}$ 按照引理 1 中的方法生成相应的密文,这里不再赘述.

最后,$\mathcal{B}$ 随机选择 $\hat{c}\in G$ 作为验证消息,并将密文 $CT^*=\{\hat{c},C_0,C_1,C_2,C_3,C_4,C_5\{C_{i,j,1},C_{i,j,2}\},\{\overline{C}_{i,j,1},\overline{C}_{i,j,2}\}_{i\in[1,n],j\in[1,n_i]}\}$ 发送给敌手 $\mathcal{A}$.

5) 询问阶段 2. 敌手 $\mathcal{A}$ 重复询问阶段 1 的询问,模拟器 $\mathcal{B}$ 如挑战前询问阶段 1 一样回应敌手 $\mathcal{A}$.

6) 猜测阶段. 敌手 $\mathcal{A}$ 输出一个关于随机值 ξ 的一个猜测 ξ'. 如果 $\xi'=\xi$,则模拟器 $\mathcal{B}$ 输出其对 τ 的猜测结果 $\tau'=0$;反之,如果 $\xi'\neq\xi$,则模拟器 $\mathcal{B}$ 输出其对 τ 的猜测结果 $\tau'=1$. 有如下 2 种情况:

① 当 $V=e(g,g)^{abc}$ 时,根据 DBDH 问题假设,敌手 $\mathcal{A}$ 在游戏中猜测到 $\xi'=\xi$ 的概率至少为 ε,则有 $Pr[\xi'=\xi|V=e(g,g)^{abc}]\geqslant\frac{1}{2}+\varepsilon$. 当 $\xi'=\xi$ 时,模拟器 $\mathcal{B}$ 提交他对 τ 的猜测 $\tau'=0$,那么 $Pr[\tau'=\tau|V=e(g,g)^{abc}]=\frac{1}{2}+\varepsilon$.

②当 $V=e(g,g)^v$ 时,根据 DBDH 问题假设,值 V 为计算随机数 w 得到的,这意味着敌手 $\mathcal{A}$ 无法得到关于 ξ 的任何消息,即当 $\xi'\neq\xi$ 时,敌手 $\mathcal{A}$ 无法区分出 ξ,即 $Pr[\xi'\neq\xi|V=e(g,g)^w]=\frac{1}{2}$. 当 $\xi'\neq\xi$ 时,模拟器 $\mathcal{B}$ 提交他对 τ 的猜测 $\tau'=1$,那么 $Pr[\tau'=\tau|V=e(g,g)^w]=\frac{1}{2}$.

综上,$\mathcal{B}$ 成功解决 DBDH 困难问题的概率为

$$Adv=\frac{1}{2}(Pr[\tau'=\tau|V=e(g,g)^{abc}]+Pr[\tau'=\tau|V=e(g,g)^w])-\frac{1}{2}\geqslant\frac{\varepsilon}{2}.$$ 证毕.

定理 2. 如果离散对数(discrete logarithm)假设在群 (G,G_T,p,e) 中成立,那么不存在概率多项式时间敌手 $\mathcal{A}$,在可验证性安全模型下以不可忽略的优势 ε 攻破本文提出的方案的可验证性.

证明. 假设存在一个概率多项式时间敌手 $\mathcal{A}$,在可验证性安全模型下以不可忽略的优势 ε 攻破该方案的可验证性,那么我们可以找到一个高效的模拟器 $\mathcal{B}$,在敌手 $\mathcal{A}$ 的帮助下以不可忽略的优势 ε 成功解决离散对数困难问题. 该定理的安全性证明如下:

挑战者随机选择生成元 $g\in G$ 和双线性群 (e,p,G,G_T),并选择随机值 $x\in\mathbb{Z}_p^*$,然后将元组 (e,p,G,G_T,g,g^x) 发送给模拟器 $\mathcal{B}$.

1) 开始阶段. $\mathcal{B}$ 运行开始算法,均匀随机地选择 $y,z\in\mathbb{Z}_p^*$ 和抗碰撞 Hash 函数 $H:G\rightarrow\mathbb{Z}_p^*$,计算 $v=g^y$,$d=g^z$ 并设置 $u=g^x$,$\mathcal{B}$ 选择值 $\alpha,\delta\in\mathbb{Z}_p^*$ 作为主私钥,计算 $e(g,g)^\alpha$,其中 g 为群 G 的生成元. $\mathcal{B}$ 选择随机值 β 并计算 $\{g^\beta,g^{1/\beta},g^\delta\}$. $\mathcal{B}$ 随机选择 $u_0\in\mathbb{Z}_p^*$ 作为组私钥 GSK,并计算 $GPK=g^{u_0}$ 作为组公钥. 对属性集合中的每个属性,$\mathcal{B}$ 随机选择 $t_{i,j}\in\mathbb{Z}_p$ ($i\in[1,n],j\in[1,n_i]$),并计算 $T_{i,j}=g^{t_{i,j}}$. $\mathcal{B}$ 返回系统公共参数给敌手 $\mathcal{A}$.

$$params=\{Y,p,G,G_T,e,g,u,v,d,g^{\beta},g^{1/\beta},g^{\delta},\{T_{i,j}\}\},$$

其中,$i\in[1,n]$,$j\in[1,n_i]$.

2) 询问阶段 1. 敌手 $\mathcal{A}$ 提交相应的属性列表给挑战者,以便在属性集合下进行私钥询问. 由于模拟器 $\mathcal{B}$ 保留随机值 α 作为主私钥,$\mathcal{B}$ 响应敌手 $\mathcal{A}$ 的密钥询问如下:

① 私钥询问. 模拟器 $\mathcal{B}$ 为每个属性 att_i 均匀随机地选择 $\lambda_i\in\mathbb{Z}_p^*$,并设置 $r=-\lambda_i' t_{i,j}-\alpha'$,则模拟器 $\mathcal{B}$ 回应敌手 $\mathcal{A}$ 的私钥询问如下:

对于私钥部件 D_0,D_2,模拟器 $\mathcal{B}$ 计算:

$$D_0=(g^{1/\beta})^{\alpha+\lambda_i' t_{i,j}+\alpha'}=(g^{1/\beta})^{(\alpha+\alpha')+\lambda_i' t_{i,j}}=g^{\frac{\gamma+\lambda_i' t_{i,j}}{\beta}},$$

$$D_2=(g^{1/\beta})^{u_0},$$

其中,$\gamma=\alpha+\alpha'$,α' 为随机数.

对于私钥部件 $\{D_{i,1},D_{i,2}\}_{i\in[1,n],j\in[1,n_i]}$,$\mathcal{B}$ 计算:

$$D_{i,1}=g^{\gamma+\lambda_i' t_{i,j}}=g^{-\lambda_i' t_{i,j}-\alpha'+\lambda_i' t_{i,j}}=g^{-\alpha'},$$

$$D_{i,2}=g^{\lambda_i'},$$

其中,$i\in[1,n]$,$j\in[1,n_i]$.

模拟器 $\mathcal{B}$ 将私钥 $SK_L=(D_0,\forall v_{i\in[1,n],j\in[1,n_i]}\in L:\{D_{i,1},D_{i,2}\},D_2)$ 返回给敌手 $\mathcal{A}$.

② 转换密钥询问. 模拟器 $\mathcal{B}$ 在表 T 中查找元组 (L,SK_L,TK_L,HK_L),若存在则返回转换密钥 TK_L;否则,$\mathcal{B}$ 随机选择 $z\in\mathbb{Z}_p^*$,回应敌手 $\mathcal{A}$ 的转换密钥询问如下:

$$\overline{D}_0'=g^{\frac{z-\gamma}{\beta}},\overline{D}_2'=(g^{1/\beta})^{u_0},\overline{D}_{i,1}'=g^{-\alpha'},\overline{D}_{i,2}'=g^{\lambda_i'},$$

其中 $i\in[1,n]$,$j\in[1,n_i]$. $\mathcal{B}$ 将转换密钥 $TK_L=\{D_0',D_2',\{D_{i,1}',D_{i,2}'\}_{i\in[1,n],j\in[1,n_i]}\}$ 给敌手 $\mathcal{A}$.

3) 挑战阶段. 敌手 $\mathcal{A}$ 提交一个属性集合 S^* 下访问结构 W^*、明文消息 $m^*\in G_T$,模拟器 $\mathcal{B}$ 运行加密算法生成转换后的密文 CT^*.

$\mathcal{B}$ 随机选择 $s\in\mathbb{Z}_p^*$,计算 $C_1=g^{\beta s}$,$C_2=g^{\delta s}$,$C_{i,j,1}=g^{s_i}$,$C_{i,j,2}=T_{i,j}^{s_i}$,其中 $i\in[1,n]$,$j\in[1,n_i]$,并计算 $C_0=m\,Y^s\,e(g,g)^{u_0 s}=m\,e(g,g)^{\alpha s+u_0 s}$.

$\mathcal{B}$ 选择随机消息 $m^{*\prime}\in G_T$,随机值 $s'\in\mathbb{Z}_p^*$,计算密文 $C_3=m^{*\prime}\,Y^{s'}e(g,g)^{u_0 s'}=m^{*\prime}\,e(g,g)^{\alpha s'+u_0 s'}$,$C_4=g^{\beta s'}$,$C_5=g^{\delta s'}$,$\overline{C}_{i,j,1}=g^{s_i'}$,$\overline{C}_{i,j,2}=T_{i,j}^{s_i'}$,其中,$i\in[1,n]$,$j\in[1,n_i]$.

模拟器 $\mathcal{B}$ 计算 $\hat{c}=u^{H(m')}\,v^{H(m^{*\prime})}\,d$,并将密文 CT^* 返回给 $\mathcal{A}$.

4) 询问阶段 2. 敌手 $\mathcal{A}$ 重复询问阶段 1 的询问,模拟器 $\mathcal{B}$ 如询问阶段 1 一样回应敌手 $\mathcal{A}$.

5) 输出阶段. 最后敌手 $\mathcal{A}$ 输出在属性集合 S^* 和转换后的密文 $CT'^*=\{K',K_1,K'_{\text{own1}},K_2,K'_{\text{own2}}\}$.

由于恢复密钥 z 是由 $\mathcal{B}$ 随机选择的,则 $\mathcal{B}$ 进行如下计算可得 $m^*=K_1/K'^{z}_{\text{own1}}$,$m^{*\prime}=K_2/K'^{z}_{\text{own2}}$. 若敌手 $\mathcal{A}$ 赢得了游戏,则 $\mathcal{B}$ 可以通过如下推导:

$$g^{xH(m^*)+yH(m^{*\prime})+z}=u^{H(m^*)}\,v^{H(m^{*\prime})}\,d=\hat{c}=K'=u^{H(m)}\,v^{H(m')}\,d=g^{xH(m)+yH(m')+z}.$$

由于 $\mathcal{B}$ 知道 $y,z,m^*,m^{*\prime},m,m'$,其中 $m\neq m^*$,根据抗碰撞 Hash 函数中存在碰撞的概率,易知 $H(m)\neq H(m^*)$,而 $x=\dfrac{y(H(m')-H(m^{*\prime}))}{H(m^*)-H(m)}$,$\mathcal{B}$ 解决了离散对数困难问题. 证毕.

6 方案比较

本节将本文所提方案与文献[9,14,18,29]中的方案进行对比. 主要比较了方案是否支持属性撤销、访问结构是否隐藏、访问结构的表达能力、是否支持外包验证等. 比较的结果如表 1 所示:

Table1 Comparison of Schemes

表 1 方案比较

Scheme	Type	Verifiable Outsourcing	Attribute Revocation	Anonymity	Access Structure
Ref[9]	CP-ABE	No	Yes	No	AND Gates
Ref[29]	CP-ABE	No	No	Fully Hidden	AND, OR Gates
Ref[18]	KP-ABE/CP-ABE	Only Outsourcing	No	No	LSSS
Ref[14]	CP-ABE	No	No	Partially Hidden	AND Gates
Our Scheme	CP-ABE	Yes	Yes	Fully Hidden	AND, OR Gates

从表 1 可以看出,文献[9,14,29]中的方案不能同时支持属性撤销和保护用户隐私;文献[18]的方案虽然提供了外包操作,但并未验证转换密文的正确性,系统的灵活性较弱;而本文所提方案支持用户撤销,且能够完全隐藏访问结构,并提供了对外包密文的验证功能.

7 结束语

本文构造了一个隐私保护且支持用户撤销的属性基加密方案,在标准困难问题下证明了方案的安全性和可验证性,并与相关方案进行了比较.方案使用组密钥实现了用户撤销,为系统的安全性提供了第二重保护.该方案完全隐藏了访问结构,因而恶意的用户无法通过访问策略分析出潜在的用户隐私信息;同时,对使用移动设备端的用户提供数据外包和验证操作,使之更适合于安全的手机云计算.

如何设计一个更适用于现实场景的云计算环境下的多授权中心的属性基加密方案是一个可以深入研究的课题.此外,目前在属性基加密体制中考虑到密钥泄露问题的方案寥寥无几,在目前严峻的数据安全形势下,希望能够在发生部分密钥泄露的情况下仍保证系统的安全性,所以设计抗泄露属性基加密方案也是今后数据安全发展的重点.

参 考 文 献

[1] Feng Dengguo, Zhang Min, Zhang Yan, et al. Study on cloud computing security [J]. Journal of Software, 2011, 22 (1): 71-83 (in Chinese)
(冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83)

[2] Sahai A, Waters B. Fuzzy identity-based encryption [G] // LNCS 3494: Proc of EUROCRYPT'05. Berlin: Springer, 2005: 457-473

[3] Cheung L, Newport C. Provably secure ciphertext policy ABE [C] //Proc of the 14th ACM Conf on Computer and Communications Security. New York: ACM, 2007: 456-465

[4] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2007: 321-334

[5] Pirretti M, Traynor P, McDaniel P, et al. Secure attribute-based systems [J]. Journal of Computer Security, 2010, 18 (5): 799-837

[6] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation [C] //Proc of the 15th ACM Conf on Computer and Communications Security. New York: ACM, 2008: 417-426

[7] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Trans on Parallel and Distributed Systems, 2011, 22 (7): 1214-1221

[8] Wang Guojun, Liu Qin, Wu Jie. Hierarchical attribute-base encryption for fine-grained access control in cloud storage services [C] //Proc of the 17th ACM Conf on Computer and Communications Security. New York: ACM, 2010: 735-737

[9] Yu Shucheng, Wang Cong, Ren Kui, et al. Attribute based data sharing with attribute revocation [C] //Proc of the 5th ACM Symp on Information, Computer and Communications Security. New York: ACM, 2010: 261-270

[10] Zhu Jun, Zhang Futai, Song Xiaodong. A new certificateless proxy re-encryption scheme [C] //Proc of IEEE Int Conf on Web Information Systems and Mining. Piscataway, NJ: IEEE, 2010: 53-58

[11] Ibraimi L, Petkovic M, Nikova S, et al. Mediated ciphertext-policy attribute based encryption and its application [G] // LNCS 5932: Proc of Information Security Applications. Berlin: Springer, 2009: 309-323

[12] Do J M, Song Y J, Park N. Attribute based proxy re-encryption for data confidentiality in cloud computing environments [C] //Proc of the Int Conf on Computers, Networks, Systems and Industrial Engineering. Piscataway, NJ: IEEE, 2011: 248-251

[13] Shi E, Bethencourt J, Chan THH, et al. Multi-dimensional range query over encrypted data [C] //Proc of IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2007: 350-364

[14] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [G] // LNCS 5037: Proc of Applied Cryptography and Network Security. Berlin: Springer, 2008: 111-129

[15] Li Jin, Ren Kui, Zhu Bo, et al. Privacy aware attribute based encryption with user accountability [G] // LNCS 5735: Proc of Information Security. Berlin: Springer, 2009: 347-362

[16] Lai Junzuo, Deng Huijie, Li Yingjiu. Fully secure cipertext-policy hiding CP-ABE [G] // LNCS 6672: Proc of Information Security Practice and Experience. Berlin: Springer, 2011: 24-39

[17] Lai Junzuo, Deng Huijie, Li Yingjiu. Expressive CP-ABE with partially hidden access structures [C] //Proc of the 7th ACM Symp on Information, Computer and Communications Security. New York: ACM, 2012: 18-25

[18] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C] //Proc of the USENIX Security Symp. Berkeley, CA: USENIX Association, 2011: 3-23

[19] Han J, Susilo W, Mu Y, et al. Privacy-preserving decentralized key-policy attribute-based encryption [J]. IEEE Trans on Parallel and Distributed Systems, 2012, 23(11): 2150-2162

[20] Zhang Jie, Ge Aijun, Ma Chuangui. Fully secure hierarchical inner product encryption with constant-size ciphertexts [J]. Journal of Computer Research and Development, 2015, 52 (3): 691-701 (in Chinese)

(张洁, 葛爱军, 马传贵. 完全安全且固定密文长度的分层内积加密方案[J]. 计算机研究与发展, 2015, 52(3): 691-701)

[21] Liu Zhen, Cao Zhenfu, Wong D S. Black-box traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on eBay [C] //Proc of the ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2013: 475-486

[22] Liu Zhen, Cao Zhenfu, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures [J]. IEEE Trans on Information Forensics and Security, 2013, 8(1): 76-88

[23] Liu Zhen, Cao Zhenfu, Wong D S. Traceable CP-ABE: How to trace decryption devices found in the wild [J]. IEEE Trans on Information Forensics and Security, 2015, 10(1): 55-68

[24] Ning Jianting, Cao Zhenfu, Dong Xiaolei, et al. Large universe ciphertext-policy attribute-based encryption with white-box traceability [G] // LNCS 8713: Proc of ESORICS 2014. Berlin: Springer, 2014: 55-72

[25] Ning Jianting, Dong Xiaolei, Cao Zhenfu, et al. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes [J]. IEEE Trans on Information Forensics and Security, 2015, 10(6): 1274-1288

[26] Shamir A. Identity-based cryptosystems and signature schemes [G] // LNCS 196: Proc of CRYPTO 84. Berlin: Springer, 1985: 47-53

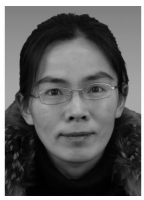
[27] Beimel A. Secure schemes for secret sharing and key distribution [D]. Haifa, Israel: Israel Institute of Technology, 1996

[28] Lai Junzuo, Deng Huijie, Guan Chaowen, et al. Attribute-based encryption with verifiable outsourced decryption [J]. IEEE Trans on Information Forensics and Security, 2013, 8(8): 1343-1354

[29] Balu A, Kuppusamy K. Privacy preserving ciphertext policy attribute based encryption [G] // CCIS 89: Proc of the Recent Trends in Network Security and Applications. Berlin: Springer, 2010: 402-409

Li Jiguo, born in 1970. Professor and PhD supervisor. His main research interests include cryptography theory and technology, cloud computing security.

Shi Yuerong, born in 1990. Received her BSc degree and MSc degree in computer science and technology from Hohai University in 2012 and 2015 respectively. Her main research interests include cryptography theory and technology, cloud computing security.



Zhang Yichen, born in 1971. PhD candidate in the College of Computer & Information of Hohai University. Her main research interests include cryptography theory and technology, cloud computing security.