支持云代理重加密的CP-ABE方案

赵开强[1],康 萍[1],刘 彬[1],郭 真[1],冯朝胜[1,2],卿 昱[3]
(1. 四川师范大学计算机科学学院,四川成都 610101;
2. 电子科技大学网络与数据安全四川省重点实验室,四川成都 610054;
3. 中国电子科技集团公司第30研究所,四川成都 610041)

摘 要: 针对现有的面向CP-ABE(Ciphertext-Policy Attribute-Based Encryption)的代理重加密方案因代理方可以解密代理重加密密文且可以任意修改访问策略而难以支持云代理重加密的问题,本文提出支持云代理重加密的CP-ABE方案即CP-ABE-CPRE(CP-ABE Scheme with Cloud Proxy Re-Encryption)方案. 该方案利用版本号标识不同阶段的私钥和密文来支持属性撤销,只有在用户私钥版本号和密文版本号相匹配且用户属性满足访问策略时,用户才能解密密文. 当撤销用户属性时,云服务器无需修改访问策略就可以更新被撤销属性对应的保密值. 该方案还通过懒惰更新和批量更新减少密文和用户私钥更新次数,提升更新效率. 理论分析和实验结果分析都表明,CP-ABE-CPRE在计算开销和存储开销上均优于相关已有方案. 安全性分析表明,CP-ABE-CPRE能够对抗针对性选择明文攻击(sCPA, selective Chosen Plaintext Attack).

关键词: 基于属性加密;访问控制;云代理重加密;云计算;sCPA
基金项目: 国家自然科学基金(No.61373163);国防科技重点实验室基金(No.6142103010709)
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112(2023)03-0728-08
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210445

A CP-ABE Scheme with Cloud Proxy Re-Encryption

ZHAO Kai-qiang[1], KANG Ping[1], LIU Bin[1], GUO Zhen[1], FENG Chao-sheng[1,2], QING Yu[3]
(1. *Department of Computer Science, Sichuan Normal University, Chengdu, Sichuan* 610101, *China*;
2. *Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*;
3. *The No.*30 *Institute of China Electronic Technology Corporation, Chengdu, Sichuan* 610041, *China*)

Abstract: Aiming at the problem that the existing CP-ABE (Ciphertext-Policy Attribute-Based Encryption) proxy re-encryption scheme is difficult to support cloud proxy re-encryption because the proxy can decrypt the re-encrypted ciphertext and modify the access policy arbitrarily, we propose a CP-ABE-CPRE (CP-ABE Scheme with Cloud Proxy Re-Encryption) scheme. CP-ABE-CPRE supports attribute revocation by using version numbers to identify private key and ciphertext at different stages. Only when the user private key's edition number matches the ciphertext's and the user's attributes meet the access policy, the user can decrypt the ciphertext. When revoking an attribute, cloud can update the confidential data corresponding to the attribute needed revoking without modifying the access policy. Moreover, this scheme also reduces the number of ciphertext and user private key updates through lazy and batch updates, and improves update efficiency. Analysis of theoretical and experimental results both show that CP-ABE-CPRE is superior to related existing solutions in terms of computational and storage cost. And security analysis shows that CP-ABE-CPRE resists the selective chosen plaintext attack.

Key words: attribute-based encryption; access control; cloud proxy re-encryption; cloud computing; sCPA
Foundation Item(s): National Natural Science Foundation of China (No.61373163); National Defense Science and Technology Foundation of Key Laboratory (No.6142103010709)

收稿日期:2021-04-07;修回日期:2022-04-10;责任编辑:梅志强

1 引言

如何在云计算环境下高效地完成文件的重加密是CP-ABE(Ciphertext-Policy Attribute-Based Encryption)一直面临的难题. 用户被撤销时,被撤销用户满足的访问策略对应的密文都需重新加密. 并且,现有的CP-ABE代理重加密方案主要关注的是将重加密委托给可信的代理方而非半可信的云服务提供商. 针对该问题,本文将版本控制技术引入到CP-ABE的代理重加密的设计之中,提出一种支持云代理重加密的CP-ABE方案,即CP-ABE-CPRE.

2005年,Sahai和Waters在模糊身份加密方案[1]中首次提出ABE(Attribute-Based Encryption)的概念,该方案用属性来标记用户特征和密文. 后来的发展中ABE主要形成了KP-ABE(Key-Policy Attribute-Based Encryption)[2]和CP-ABE[3]两个分支. Bethencourt等[3]于2007年首次提出密文策略基于属性加密(CP-ABE)算法,该算法在用户私钥中隐藏属性,在密文中隐藏访问策略. CP-ABE算法中主要有Bethencourt等方案[3]中用到的树结构和Waters等[4]2011年提出的线性秘密共享方案(LSSS, linear secret sharing scheme)两种访问控制结构. 2014年,Balu等[5]提出用LISS代替LSSS,并给出具体方案构造,解决了Waters等[4]方案中属性出现次数受限的问题.

为解决CP-ABE中的共享访问策略更新问题,2009年,Liang等[6]在CP-ABE中引入代理重加密技术,该方案通过委托第三方代理将共享密文从加密状态转换为另一种访问策略下加密状态的共享密文,整个过程不暴露明文信息和用户私钥. 2010年,Luo等[7]提出了CP-ABE代理重加密方案,在密文中增加一个子项来控制当前密文能否被重加密. 2015年,Li等[8]提出了一种具有CCA(Chosen Ciphertext Attack)安全的CP-ABE代理重加密方案,但该方案代理方能利用重加密密钥重加密该用户的其他密文. 同年,为降低本地生成重加密密钥的计算负担,Kawai[9]提出将其委托给授权中心来完成,但会造成授权机构计算瓶颈问题,还让用户失去了对重加密的控制. 2015年,Liang等[10]为解决同年提出的代理重加密方案[11]中重加密计算开销大的问题,将云服务器作为代理来进行重加密. 2020年,杨等[12]提出支持外包加解密可验证的CP-ABE方案,为代理重加密的外包验证提供了思路. 在Liang等[10]之前的方案因无法解决外包中秘密泄露的问题而不支持云代理重加密. 2018年,为实现解密能力的细粒度委托,Zeng等[13]提出云存储下的支持条件代理重加密的CP-ABE方案,其中委托人能将密文的解密权从指定的发送方委托给受委托人. 2019年,冯等[14]提出支持多特性的代理重加密方案,该方案同时支持单向性、非交互性、可重复性、可控性和可验证性. 2019年Deng等[15]基于矩阵提出了从ABE到IBE(Identity-Based Encryption)的灵活代理重加密方案,方案在构造时将IBE算法中的系统参数全部被包含在ABE中,实现灵活的授权访问. 2020年,Zheng等[16]为保证物联网中用户敏感数据的安全,提出支持用户高效撤销的基于属性数据共享方案,支持用户的高效加入、撤销和再加入. 同年,Lin等[17]提出云上物联网数据外包代理重加密方案,为物联网中的数据外包引入了一个安全的代理重加密协议. 2021年,Guo等[18]提出一种非交互式的可靠代理重加密方案,该方案利用鉴定算法判断云服务器是否腐败,实现对云的可追责性.

2010年,Yu等[19]提出了云计算中的安全、可扩展和支持细粒度数据访问控制的KP-ABE方案,并在其中引入懒惰重加密技术. 2013年,Tysowski等[20]提出了基于重加密密钥管理的混合属性CP-ABE方案. 该方案基于属性版本号和用户组实现用户撤销,但方案存在明显的安全漏洞. 首先,组内用户可以直接构造出与外包加密相关的密文子项,抵消掉密文中的外包加密部分;其次,该方案无法抵御协作攻击,组内不满足访问策略的用户可以和组外满足访问策略的用户合谋解密. 2017年,Li等[21]同样基于用户组概念提出支持云代理重加密的CP-ABE方案,实现高效的用户撤销. 然而,该方案在证书分发阶段的全局一致子项会引起非法用户间合谋放大属性集合的问题,且安全性证明不完备. 2019年,Li等[22]提出支持用户和属性撤销的基于属性外包加密方案,并将其应用于雾计算来提升密文更新效率,但该方案重加密的计算开销较大.

2 系统模型

2.1 系统框架

系统框架图如图1,系统包含四个实体.

(1)授权机构(Trusted Authority, TA):全可信实体. 主要负责输出系统公钥、主密钥和用户私钥,并负责重加密部分密钥的生成. (2)云服务提供商(Cloud service provider, CSP):半可信实体. 提供强大的存储和计算能力. (3)数据拥有者(Data Owner, DO):定义访问策略,执行加密,并将密文上传到CSP. (4)数据消费者(Data User, DU):从TA获取用户私钥,从CSP下载共享密文,并执行解密.

2.2 属性撤销

本节介绍无需修改访问策略的属性撤销方法. 为访问树中的叶子节点对应的属性选择相应的保密值并设置版本号,发生属性撤销时仅更新被撤销属性对应的保密值,并将属性版本加一. 只有当用户私钥中的属性版本与加密所基于的访问策略中的属性版本相匹配且属性满足访问策略的用户才能解密,用户解密存在以下三种情况:(1)用户私钥与共享密文版本相同;(2)

用户私钥版本低于共享密文版本;(3)用户私钥版本高于共享密文版本.

用户需要同时获得最新版本用户私钥和最新版本共享密文才能进行解密. 当用户向云服务器申请共享密文时,云服务器代理更新密文和用户私钥至最新版本发送给用户用于解密.

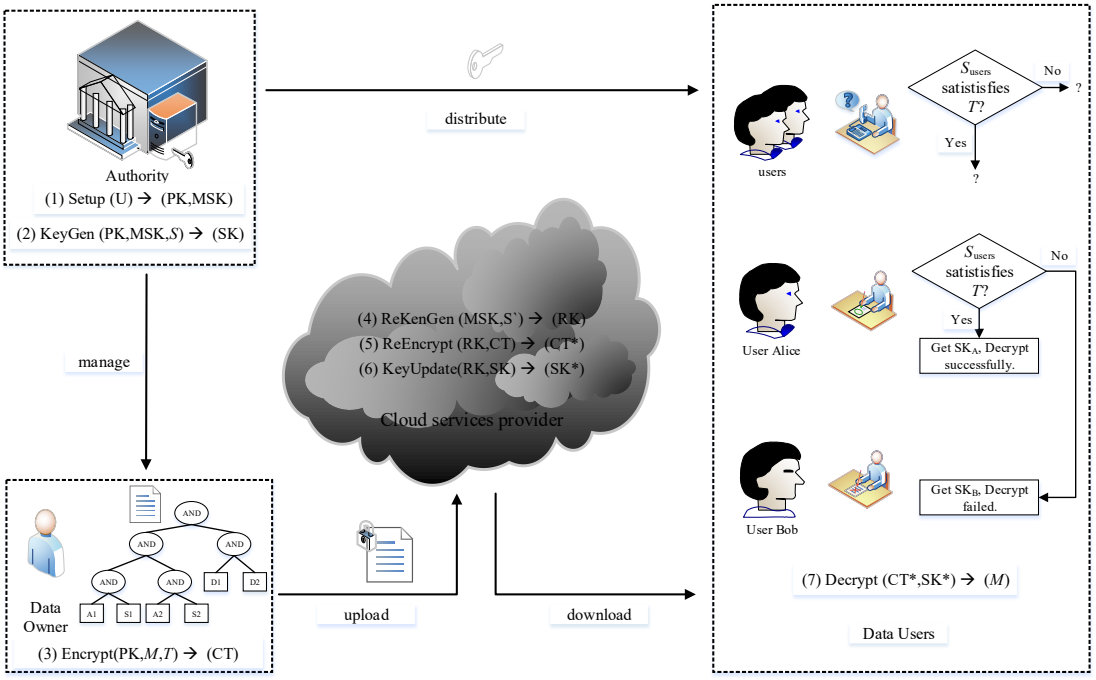

图1 系统结构图

3 方案构造

本文方案以Bethencourt等[3]方案为基础,详细算法如下.

(1) Setup(U)→(PK, MSK).

选择生成元为g,阶为素数p的双线性群G_0,为属性空间U中属性$\text{Attr}_1, \text{Attr}_2, \cdots, \text{Attr}_j, \cdots, \text{Attr}_i$选择随机数$t_1, t_2, \cdots, t_j, \cdots, t_i \in Z_p^*, i \in (1, u)$,$u$为属性空间长度. 定义双线性映射$e: G_0 \times G_0 \to G_T$,并随机选择$\alpha, \beta \in Z_p$,输出系统公钥PK,系统主密钥MSK:

$$\text{PK} = \{G_0, g, h = g^{\beta}, e(g,g)^{\alpha}\}$$

$$\text{MSK} = \left\{\text{MSK}' = \{g^{\alpha}, \beta\}, \text{MSK}'' = \{t_1, t_2, t_3, \cdots, t_u\}\right\}$$

(2) Keygen(PK, MSK, S)→SK.

定义从1开始的属性版本号$(v) = \{1, 2, 3, \cdots, n\}$,约定重加密次数不超过$n$. 为用户选择随机数$r \in Z_p^*, \forall i \in S$,选择随机数$r_i$,绑定属性$i$对应的保密值$t_i^{(v)} \in Z_p^*$,并计算属性公开值$T_i^{(v)} = g^{t_i^{(v)}}$. TA计算用户初始私钥:

$$\text{SK}^{(v)} = \left\{D = g^{\frac{\alpha + r}{\beta}},\ \forall i \in S: D_i^{(v)} = g^r \cdot (T_i^{(v)})^{r_i}, D_i' = g^{r_i}\right\}$$

(3) Encrypt(PK, M, T)→CT.

用户随机选择$s \in Z_p$,从访问树根节点R开始,自顶向下按如下规则分发秘密值s. 为树T中每个节点x定义多项式q_x,其中,多项式的阶$d_x = k_x - 1$(k_x表示门限值). 令$q_R(0) = s$,然后随机选择d_R个点完整定义q_R. 对除根节点R以外的其余节点x,令$q_x(0) = q_{\text{parent}(x)}(\text{index}(x))$,并随机选择$d_x$个点完整定义$q_x$. 计算:

$$\hat{C} = M \cdot e(g,g)^{\alpha s}, C = h^s$$

设Y为树T叶子节点的集合,对叶子节点计算:

$$\forall y \in Y: C_y = g^{q_y(0)}, C_y' = \left(T_i^{(v)}\right)^{q_y(0)}$$

完整密文如下:

$$\text{CT}^{(v)} = \{T, \hat{C} = M \cdot e(g,g)^{\alpha s}, C = h^s,$$
$$\forall y \in Y: C_y = g^{q_y(0)}, C_y' = (T_i^{(v)})^{q_y(0)}\}$$

(4) ReKeyGen(MSK, S′)→RK.

设属性当前版本为(j),DO发起重加密请求时,对被撤销属性i,TA选择新保密值$t_i^{(j+1)} \in Z_p^*$,作为属性i版本$(j+1)$的保密值,并计算重加密密钥RK,其中$S' \subseteq S$:

$$\text{RK} = (\forall i \in S': \text{RK}_i^{(j+1)} = t_i^{(j+1)} - t_i^{(j)})$$

计算版本$(j+1)$的属性公开值$\forall i \in S': T_i^{(j+1)} = g^{t_i^{(j+1)}}$,并将RK发送给CSP.

(5) ReEncrypt(RK, CT)→CT*.

DO发起重加密请求时,TA生成RK发送给CSP,

CSP保存重加密密钥到重加密密钥列表中,并记录相应版本号,数据消费者DU请求密文时分三种情形.

情形1,若重加密列表为空(未收到重加密请求),则CSP直接发送共享密文给请求密文的用户.

情形2,若重加密列表长度为1(一次重加密请求),则CSP代理执行一次重加密. 具体更新操作如下:

利用RK更新属性相关密文子项,其中更新前密文版本为(j),版本(j)到$(j+1)$的重加密操作:

$$\begin{aligned}&\forall y\in Y'\colon C_y'\\&=(T_i^{(j)})^{q_y(0)}\cdot\left(C_y=(g^{q_y(0)})^{t_i^{(j+1)}-t_i^{(j)}}\right)\\&=(T_i^{(j+1)})^{q_y(0)}\end{aligned}$$

更新后完整密文为:

$$\begin{aligned}\mathrm{CT}^{(j+1)}=\{&T,\hat{C}=M\cdot e(g,g)^{\alpha s},C=h^s,\\&\forall y\in Y\colon C_y=g^{q_y(0)},C_y'=(T_i^{(j+1)})^{q_y(0)}\}\end{aligned}$$

情形3,若重加密列表长度大于1(多次重加密请求),则CSP执行批量代理重加密操作. 假定发起两次重加密请求(多个版本类推),更新操作如下:

假定属性i的重加密密钥经历了$(j+1)$和$(j+2)$两个版本,则对应的阶段重加密密钥为$\mathrm{RK}_i^{(j+1)}=t_i^{(j+1)}-t_i^{(j)}$,$\mathrm{RK}_i^{(j+2)}=t_i^{(j+2)}-t_i^{(j+1)}$,通过一次加法运算得到最终的重加密密钥. 最终,代理重加密操作与情形2类似.

(6) $\mathrm{KeyUpdate}(\mathrm{RK},\mathrm{SK})\to\mathrm{SK}^*$.

CSP在更新密文后,再更新对应用户私钥,并连同更新的密文发送给用户. 对$\forall i\in S'$,从版本(j)到$(j+1)$的私钥更新操作为(新属性集合为S'):

$$\begin{aligned}D_i^{(j+1)}&=g^r\cdot(T_i^{(j)})^{r_i}\cdot(D_i')^{t_i^{(j+1)}-t_i^{(j)}}\\&=g^r\cdot(T_i^{(j+1)})^{r_i}\end{aligned}$$

不同更新次数下的私钥更新思路与密文一致.

(7) $\mathrm{Decrypt}(\mathrm{CT}^*,\mathrm{SK}^*)\to M$.

定义函数$\mathrm{DecryptNode}(\mathrm{CT}^*,\mathrm{SK}^*,x)$. 解密时,若用户私钥匹配访问策略,则输出一个$G_T$域上的群元素,否则,输出$\perp$,具体解密过程如下所述. 如果$x$为叶子节点,解密算法如下:

$$\begin{aligned}\mathrm{DecryptNode}(\mathrm{CT}^*,\mathrm{SK}^*,x)&=\frac{e(D_i,C_x)}{e(D_i',C_x')}\\&=\frac{e(g^r\cdot(T_i^{(j)})^{r_i},g^{q_y(0)})}{e(g^{r_i},(T_i^{(j)})^{q_y(0)})}\\&=e(g,g)^{rq_y(0)}\end{aligned}$$

x为非叶子节点,对x的所有孩子节点z,都调用函数$\mathrm{DecryptNode}(\mathrm{CT}^*,\mathrm{SK}^*,z)$,并将其输出记为$F_z$. 令$S_x$为任意$k_x$大小的孩子节点$z$的集合,且$F_z\neq\perp$. 若节点不满足访问策略,函数返回$\perp$. 否则,解密如下,其中$i=\mathrm{index}(z)$,$s_x'=\{\mathrm{index}(z)\colon z\in S_x\}$:

$$\begin{aligned}F_x&=\prod_{z\in S_x}F_z^{\Delta_{i,S_x'}(0)}\\&=\prod_{z\in S_x}e(g,g)^{rq_z(0)\Delta_{i,S_x'}(0)}\\&=\prod_{z\in S_x}e(g,g)^{rq_{\mathrm{parent}(\mathrm{index}(x))}\Delta_{i,S_x'}(0)}\\&=\prod_{z\in S_x}e(g,g)^{rq_x(i)\Delta_{i,S_x'}(0)}\\&=e(g,g)^{rq_x(0)}\end{aligned}$$

密文版本号为(1)时(未重加密),若属性集S满足访问树T,则设$\mathrm{A}=\mathrm{DecryptNode}(\mathrm{CT},\mathrm{SK},R)$;当密文被重加密更新到版本$(j)$时,若属性集$S'$满足访问树$T$,设$\mathrm{A}=\mathrm{DecryptNode}(\mathrm{CT}^*,\mathrm{SK}^*,R)$. 最终可通过如下公式解密明文$M$:

$$\frac{\hat{C}}{\frac{e(C,D)}{A}}=\frac{M\cdot e(g,g)^{\alpha s}\cdot e(g,g)^{rs}}{e(g,g)^{(\alpha+r)s}}=M$$

4　安全性证明

定理1　若文献[3]中方案在一般群模型和随机预言模型下能达到针对性选择明文安全,则本文所提方案也能在一般群模型和随机预言模型下达到针对性选择明文安全.

证明　若敌手A能以不可忽略的优势攻破CP-ABE-CPRE方案,则能以同样的优势攻破文献[3]中方案.

准备阶段　敌手A向模拟器B提交一个访问树T^*和满足T^*的必备属性i^*(其版本号由v_{i^*}到$v_{i^*}+1$),模拟器B将T^*作为挑战访问树发送给文献[3]中方案的挑战者E.

初始化　挑战者E执行文献[3]方案中的Setup算法生成$\mathrm{PK}'=\{G_0,g,h=g^\beta,e(g,g)^\alpha\}$($\mathrm{MSK}'=\{g^\alpha,\beta\}$由$E$秘密保存)并发送给模拟器$B$,$B$为属性生成$\mathrm{MSK}''=\{t_i^{(v_i)}\}_{1\le i\le u}$并秘密保存(主密钥$\mathrm{MSK}=\mathrm{MSK}'\cup\mathrm{MSK}''$,$v_i$为属性$i$最新的版本号),计算$T^{(v)}=\{T_i^{(v_i)}=g^{t_i^{(v_i)}}\}_{1\le i\le u}$,将$\mathrm{PK}=\mathrm{PK}'\cup T^{(v)}$发送给敌手$A$.

查询阶段1　任意属性集S_i不满足T^*时,A可重复地查询S_i对应的私钥. B将S_i连同S_i中每个属性i的哈希值$T_i^{(v_i)}=g^{t_i^{(v_i)}}$发送给$E$. E调用算法$\mathrm{Keygen}(\mathrm{MSK}',S_i)$生成属性集$S_i$对应的私钥$\mathrm{SK}_i=\left(D=g^{\frac{\alpha+r}{\beta}},\forall i\in S\colon D_i^{(v_i)}=g^r\cdot(T_i^{(v_i)})^{r_i},D_i'=g^{r_i}\right)$并返回给$B$,$B$将$\mathrm{SK}_i$发送给敌手$A$.

挑战　敌手A向模拟器B提交两个等长的消息M_0和M_1. B将M_0和M_1发送给E. E随机选择$b\in\{0,1\}$,查询T^*所包含属性的哈希值,调用加密算法

Encrypt(PK, M_b, T)→CT 加密 M_b，得到密文 CT=$\left(T, \hat{C}=M\cdot e(g,g)^{\alpha s}, C=h^s, \forall y\in Y: C_y=g^{q_y(0)}, C'_y{}^{(v)}=(T_i^{(v_i)})^{q_y(0)}\right)$，并发送给模拟器 B. 由于属性 i^* 的版本号由 v_{i^*} 更新到 $v_{i^*}+1$，调用重加密秘钥生成算法 ReKeyGen(MSK, S') 和重加密算法 ReEncrypt(RK, CT) 更新密文，将更新后的密文 CT* 发送给敌手 A.

查询阶段 2 敌手 A 除重复阶段 1 的查询，还进行如下查询：

用户私钥更新查询：当 S_i 包含属性 i^* 且不满足 T^* 时，ReKeyGen(MSK, S') 和 KeyUpdate(RK, SK) 算法被调用来更新私钥.

用户私钥查询：若 S_i 满足 T^*，提交给 E 的 i^* 对应的哈希值是 $T_{i^*}^{(v_{i^*})}$ 而非 $T_{i^*}^{(v_{i^*}+1)}$.

猜测 敌手 A 输出猜测值 $b'=b$，若 $b\in\{0,1\}$，则敌手 A 赢得游戏. 敌手 A 赢得游戏的优势定义为 $\Pr[b'=b]-\frac{1}{2}$.

若敌手 A 能以不可忽略的优势攻破 CP-ABE-CPRE 方案，则能以同样的优势攻破文献[3]中方案. 而文献[3]中方案被证明在一般群模型和随机预言模型下能达到 sCPA 安全，故 CP-ABE-CPRE 方案能在一般群模型和随机预言模型下达到 sCPA 安全.

5 理论分析

5.1 特性分析

本节将对比分析 CP-ABE-CPRE 方案与相关已有方案的特性. 对比结果如表 1，CP-ABE-CPRE 方案支持所有特性，其余方案支持的特性较少.

5.2 性能分析

本节以计算和存储开销为指标，将本文方案与文献[20~22]中所提方案进行对比分析. 给出需要用到的符号及其意义，如表 2 所示.

5.2.1 计算开销

本小节从私钥生成、加密、重加密和解密方面分析本文所提方案和对比方案的计算开销，计算性能对比结果如表 3.

CP-ABE-CPRE 方案在生成用户私钥时，对与属性无关私钥子项计算开销为 E_{G_0}，对每个用户属性需要计算开销为 $3E_{G_0}$，总开销为 $(1+3|S_u|)\cdot E_{G_0}$. DO 在加密时，CP-ABE-CPRE 方案对树中每个中间节点需要 1 次 G_T 上的指数运算和 1 次 G_0 上的指数运算，对密文共享访问树中每个叶子节点需要 2 次 G_0 上的指数运算，总开销为 $(1+2|S_N|)\cdot E_{G_0}+E_{G_T}$. 重加密时，CP-ABE-CPRE 方案对共享访问树的每个叶子节点更新需要 1 次 G_0 域上的指数运算，总开销为 $|S_N|\cdot E_{G_0}$. 解密时，CP-ABE-CPRE 方案对每个叶子节点需要 2 次双线性配对运算（假设共享访问树为仅含 AND 结构的满二叉树），对除叶子节点和根节点之外的中间节点需要执行 1 次 G_T 上的指数运算，解密根节点需要 1 次配对运算，解密总开销为 $(2|S_u|+1)\cdot B_e+(|S_N|-2)\cdot E_{G_T}$.

表 1 方案特性对比

方案	云代理重加密	可重复重加密	批量重加密	懒惰重加密	属性撤销	用户撤销
文献[20]	Yes	Yes	No	No	No	Yes
文献[21]	Yes	Yes	No	No	No	Yes
文献[22]	No	No	No	No	Yes	Yes
本文方案	Yes	Yes	Yes	Yes	Yes	Yes

表 2 性能分析符号一览表

符号	意义
E_{G_0}	群 G_0 上一次指数运算时间开销
E_{G_T}	群 G_T 上一次指数运算时间开销
B_e	双线性配对运算时间开销
$\|S_u\|$	用户属性个数
$\|S_N\|$	密文共享访问树中叶子节点个数
$\|G_0\|$	一个 G_0 群元素大小
$\|G_T\|$	一个 G_T 群元素大小

5.2.2 存储开销

本小节从用户秘钥和共享密文分析本文所提方案和对比方案的存储开销. 存储开销对比见表 4.

CP-ABE-CPRE 方案对每个用户属性相关的私钥子项需要 $2|G_0|$ 存储空间，存储用户标识需要 $|G_0|$ 空间，总开销为 $(1+2|S_u|)\cdot|G_0|$. 产生密文时，对非叶子节点需要 $|G_0|+|G_T|$ 存储空间，对每一个叶子节点需要 $2|G_0|$ 存储空间，总开销为 $(1+2|S_N|)\cdot|G_0|+|G_T|$.

表 3 计算性能对比

方案	私钥生成	加密	重加密	解密
文献[20]	$(1+3\|S_u\|)\cdot E_{G_0}$	$(1+2\|S_N\|)\cdot E_{G_0}+B_e+E_{G_T}$	$E_{G_0}+B_e$	$(2\|S_u\|+3)\cdot B_e+(\|S_N\|-2)\cdot E_{G_T}$
文献[21]	$2B_e+(7+3\|S_u\|)\cdot E_{G_0}$	$(4+2\|S_N\|)\cdot E_{G_0}+2E_{G_T}$	B_e	$(2\|S_u\|+\|S_N\|+5)\cdot B_e+(\|S_N\|+2)\cdot E_{G_T}$
文献[22]	$(3+5\|S_u\|)\cdot E_{G_0}$	$(5+3\|S_N\|)\cdot E_{G_0}+E_{G_T}$	$8\|S_N\|\cdot E_{G_0}$	$(3\|S_u\|+6)\cdot B_e+(\|S_N\|-2)\cdot E_{G_T}$
本文方案	$(1+3\|S_u\|)\cdot E_{G_0}$	$(1+2\|S_N\|)\cdot E_{G_0}+E_{G_T}$	$\|S_N\|\cdot E_{G_0}$	$(2\|S_u\|+1)\cdot B_e+(\|S_N\|-2)\cdot E_{G_T}$

表4　存储开销对比

方案	用户私钥	加密密文
文献[20]	$(1+2\|S_u\|)\cdot\|G_0\|$	$(2+2\|S_N\|)\cdot\|G_0\|+\|G_T\|$
文献[21]	$(4+2\|S_u\|)\cdot\|G_0\|$	$(4+2\|S_N\|)\cdot\|G_0\|+\|G_T\|$
文献[22]	$(2+4\|S_u\|)\cdot\|G_0\|$	$(3+3\|S_N\|)\cdot\|G_0\|+\|G_T\|$
本文方案	$(1+2\|S_u\|)\cdot\|G_0\|$	$(1+2\|S_N\|)\cdot\|G_0\|+\|G_T\|$

6　实验分析

6.1　实验环境

本文基于CP-ABE工具包和JPBC密码学库,使用Java语言,利用512 bit的A类奇异曲线$y^2=x^3+x$构造160 bit的椭圆曲线群进行实验. 实验环境为Windows 10操作系统、AMD Ryzen 3 PRO 2200 G (3.5 GHz)、内存12 GB. 实验中对每组对比实验结果中取30次运算的平均值作为实验结果,以确保数据的可靠性.

6.2　计算开销

本节将从加密、重加密、私钥生成和解密对比本文方案与对比方案的计算开销. 实验中将属性个数作为变量,并设置范围为10到100,步长为10,且将访问树中阈值全部设置为AND节点.

在加密阶段CP-ABE-CPRE方案与对比方案的计算开销对比如图2. 在加密过程中四个方案的计算开销均随着属性个数的增加呈线性增长,但CP-ABE-CPRE方案需要计算的与属性无关的密文子项较少,因而在加密时间开销上具有优势.

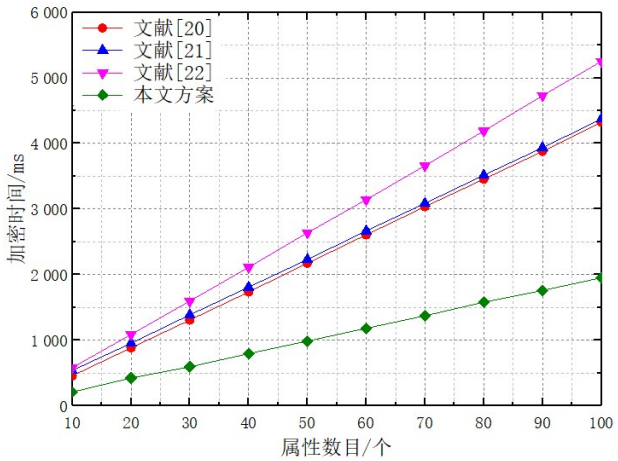

图2　加密时间开销对比

重加密对比结果如图3. 文献[20]和文献[21]方案通过用户组来实现用户级的撤销,其重加密开销与属性个数无关且重加密时间开销趋于常数. 而同样实现属性级撤销的文献[22]中方案与CP-ABE-CPRE方案相比,该方案对每一个被撤销的属性需要多计算一个密文子项. 故CP-ABE-CPRE方案相较于属性级撤销方案有明显计算优势.

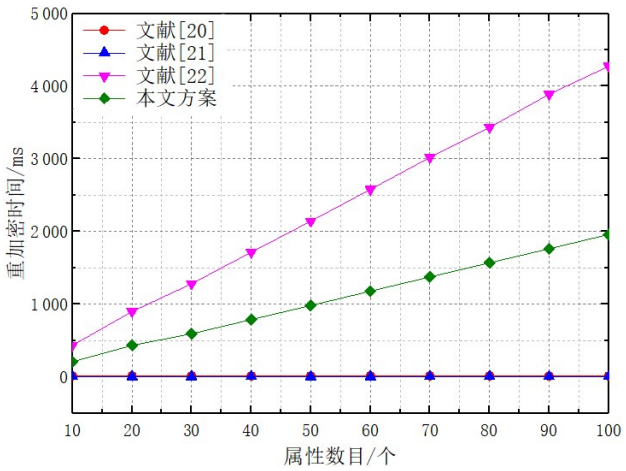

图3　重加密时间开销对比

私钥生成开销对比结果如图4. 文献[20]和文献[21]的私钥构造均需要构造与用户组相关的私钥子项;而文献[22]的用户私钥计算会多一个与属性相关的子项,故CP-ABE-CPRE方案在构造用户私钥计算开销上具有明显优势.

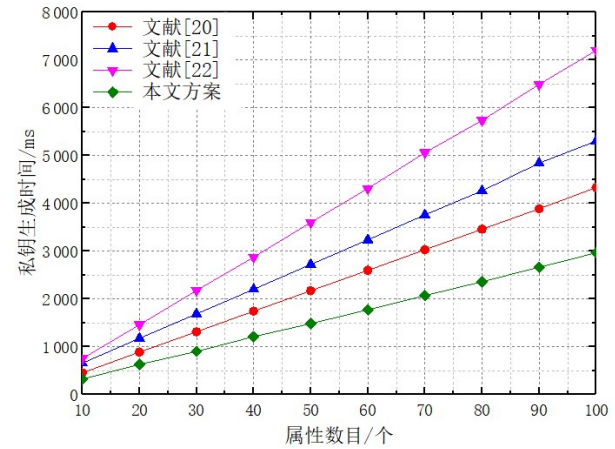

图4　私钥生成时间开销对比

解密对比如图5,文献[20]和文献[21]需要多解密用户组的加密,文献[22]对每一个属性需多解密一个子项,故CP-ABE-CPRE方案解密时具有优势.

6.3　存储开销

本节将对比分析CP-ABE-CPRE方案与对比方案在加解密过程中的密文和用户私钥的存储开销. 对比结果如图6和图7.

在相同访问策略下,四个方案加密存储开销差异较小. 但文献[20]和文献[21]方案需要存储用户组密文子项,文献[22]对每个叶子节点需多存储一个密文子项,因此,CP-ABE-CPRE方案在密文存储开销上具有优势,对比结果图6. 用户私钥存储开销的对比结果如图7,相同的原因产生与密文存储开销相似的结果.

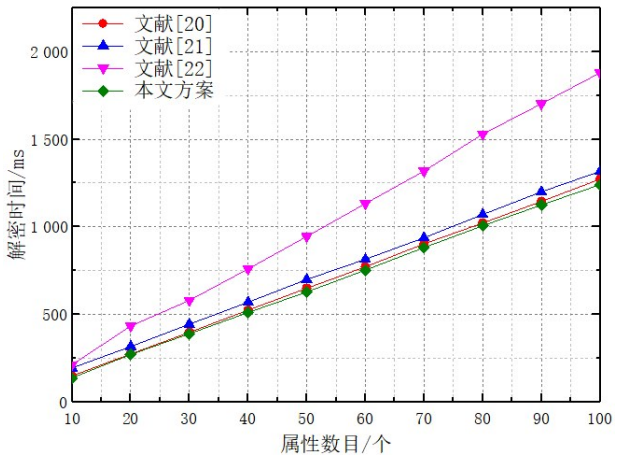

图5 解密时间开销对比

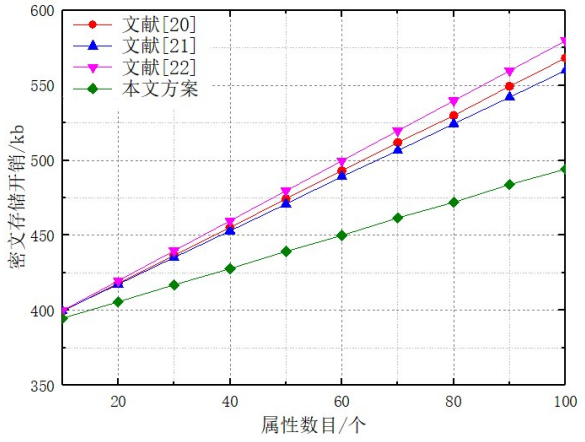

图6 密文存储开销对比

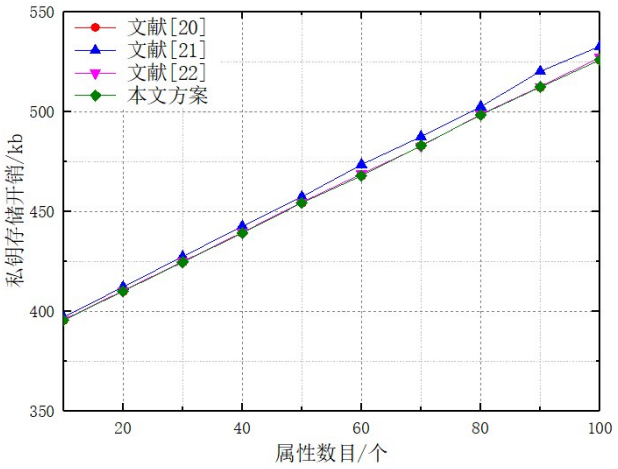

图7 私钥存储开销对比

7 结语

本文将代理重加密和版本控制技术结合并应用到CP-ABE方案的设计之中,提出CP-ABE-CPRE方案. 该方案用不同版本号的属性保密值标识不同撤销阶段的属性值,通过更新被撤销属性的版本实现无需修改访问策略的属性撤销. 懒惰更新和批量更新显著减少了用户交互次数,提升了更新效率. 性能分析表明,CP-ABE-CPRE方案有较高的计算效率和存储效率. 安全性分析表明,CP-ABE-CPRE方案达到sCPA安全. 未来将重点研究支持大属性空间的CP-ABE-CPRE方案.

参考文献

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

[2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]//Proceedings of the 13th ACM Conference On Computer And Communications Security. New York, ACM, 2006: 89-98.

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

[4] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C]//International Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer, 2011: 53-70.

[5] BALU A, KUPPUSAMY K. An expressive and provably secure ciphertext-policy attribute-based encryption[J]. Information Sciences, 2014, 276: 354-362.

[6] LIANG X H, CAO Z F, LIN H, et al. Attribute based proxy re-encryption with delegating capabilities[C]//Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. New York, ACM, 2009: 276-286.

[7] LUO S, HU J B, CHEN Z. Ciphertext policy attribute-based proxy re-encryption[C]//International Conference on Information and Communications Security. Berlin, Heidelberg: Springer, 2010: 401-415.

[8] LI J J, LIU Z H, ZU L H. Chosen-ciphertext secure multi-use unidirectional attribute-based proxy re-encryptions[C]// 2014 Ninth Asia Joint Conference on Information Security. Piscataway: IEEE, 2014: 96-103.

[9] KAWAI Y. Outsourcing the re-encryption key generation: flexible ciphertext-policy attribute-based proxy re-encryption[M]//Information Security Practice and Experience. Cham: Springer International Publishing, 2015: 301-315.

[10] LIANG K T, AU M H, LIU J K, et al. A secure and effi-

cient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing[J]. Future Generation Computer Systems, 2015, 52: 95-108.

[11] LIANG K T, FANG L M, SUSILO W, et al. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security[C]//2013 5th International Conference on Intelligent Networking and Collaborative Systems. Piscataway: IEEE, 2013: 552-559.

[12] 杨贺昆, 冯朝胜, 晋云霞, 等. 支持可验证加解密外包的CP-ABE方案[J]. 电子学报, 2020, 48(8): 1545-1551.
YANG H K, FENG C S, JIN Y X, et al. ACP-ABE scheme with verifiable outsourced encryption and decryption[J]. Acta Electronica Sinica, 2020, 48(8): 1545-1551. (in Chinese)

[13] ZENG P, CHOO K K R. A new kind of conditional proxy re-encryption for secure cloud storage[J]. IEEE Access, 2018, 6: 70017-70024.

[14] 冯朝胜, 罗王平, 秦志光, 等. 支持多种特性的基于属性代理重加密方案[J]. 通信学报, 2019, 40(6): 177-189.
FENG C S, LUO W P, QIN Z G, et al. Attribute-based proxy re-encryption scheme with multiple features[J]. Journal on Communications, 2019, 40(6): 177-189. (in Chinese)

[15] DENG H, QIN Z, WU Q H, et al. Flexible attribute-based proxy re-encryption for efficient data sharing[J]. Information Sciences, 2020, 511: 94-113.

[16] ZHENG D, QIN B D, LI Y N, et al. Cloud-assisted attribute-based data sharing with efficient user revocation in the Internet of Things[J]. IEEE Wireless Communications, 2020, 27(3): 18-23.

[17] LIN H Y, HUNG Y M. An improved proxy re-encryption scheme for IoT-based data outsourcing services in clouds [J]. Sensors (Basel, Switzerland), 2020, 21(1): 67.

[18] GUO H, ZHANG Z F, XU J, et al. Accountable proxy re-encryption for secure data sharing[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(1): 145-159.

[19] YU S C, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//2010 Proceedings IEEE INFOCOM. Piscataway: IEEE, 2010: 1-9.

[20] TYSOWSKI P K, HASAN M A. Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds[J]. IEEE Transactions on Cloud Computing, 2013, 1(2): 172-186.

[21] LI J, YAO W, ZHANG Y, et al. Flexible and fine-grained attribute-based data storage in cloud computing[J]. IEEE Transactions on Services Computing, 2017, 10(5): 785-796.

[22] LI L, WANG Z, LI N. Efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT[J]. IEEE Access, 2020, 8: 176738-176749.

作者简介

赵开强　男, 1996年01月出生于四川省巴中市. 四川师范大学在读研究生. 研究方向为信息安全与云计算.
E-mail: 18483621260@163.com

康　萍　女, 1998年03月出生于四川省南充市. 四川师范大学在读研究生. 研究方向为信息安全与云计算.
E-mail: iskangping@foxmail.com

刘　彬　男, 1996年10月出生于四川省宜宾市. 四川师范大学在读研究生. 研究方向为区块链、联邦学习与信息安全.
E-mail: liubin10@foxmail.com

郭　真　女, 1997年09月出生于四川省成都市. 四川师范大学在读研究生. 研究方向为信息安全与云计算.
E-mail: ssbguo@foxmail.com

冯朝胜(通讯作者)　男, 1971年01月出生于四川省广元市. 教授、硕士生导师. 研究方向为云计算安全.
E-mail: csfenggy@163.com

卿　昱　女, 1970出生于四川,中国电子科技集团公司第三十研究所研究员,硕士生导师. 研究方向为网络与信息安全.