DOI:10.7544/issn1000-1239.2020.20190254
57(5):1057-1069,2020

支持用户权限动态变更的可更新属性加密方案

严新成[1] 陈 越[1] 巴 阳[1] 贾洪勇[2] 王仲辉[3]
[1](战略支援部队信息工程大学 郑州 450001)
[2](郑州大学软件与应用科技学院 郑州 450001)
[3](西部战区陆军参谋部附属单位 兰州 730030)
(imtodshine@163.com)

Updatable Attribute-Based Encryption Scheme Supporting Dynamic Change of User Rights

Yan Xincheng[1], Chen Yue[1], Ba Yang[1], Jia Hongyong[2], and Wang Zhonghui[3]
[1](*Strategic Support Force Information Engineering University*, *Zhengzhou* 450001)
[2](*School of Software and Applied Technology*, *Zhengzhou University*, *Zhengzhou* 450001)
[3](*Subordinate Unit of the Army Staff*, *Western Theater Command*, *Lanzhou* 730030)

Abstract Attribute-based encryption has great advantages in achieving fine-grained secure sharing for cloud data. Due to the dynamic changes of user access rights in cloud storage, data re-encryption is an effective method to ensure the forward security of ciphertext when the attribute or user private key is revoked, but the corresponding computation overhead and communication overhead of data uploading and downloading are too large. To address these issues, an updatable attribute-based encryption scheme is proposed to support dynamic changes of user rights (SDCUR-UABE). By constructing the attribute version key and user version key in ciphertext-policy attribute-based encryption, only the corresponding components of transformation key in user's private key need to be updated when the user attribute is revoked. Similarly, when a system attribute is revoked, the corresponding attribute version key needs to be updated to implement replaceable update of part components for the ciphertext and key. Next, only the user version key needs to be updated when the user private key is revoked. Therefore the expensive computation and communication overhead caused by ciphertext update based on data re-encryption can be avoided. Besides, key segmentation is used to realize data decryption outsourcing to reduce the user's decryption overhead in the construction of the scheme. Theoretical analysis and experimental verification show that the proposed scheme can effectively solve the computing efficiency and communication overhead of ciphertext update when the user rights are dynamically changed in the cloud storage system, and greatly reduce the computational complexity of user decryption under the premise of guaranteeing forward security for ciphertext.

Key words cloud storage; attribute-based encryption; decryption outsourcing; attribute revocation; private key revocation

摘 要 属性加密在实现云数据细粒度安全共享方面具有较大优势.由于云存储中用户访问权限动态变化,当属性或用户私钥撤销时,数据重加密是保证密文前向安全性的有效方法,但相应的计算开销及数

收稿日期:2019-04-23;**修回日期**:2019-09-09
基金项目:国家自然科学基金项目(61702549);河南省科技攻关计划项目(172102210017)
This work was supported by the National Natural Science Foundation of China (61702549) and the Science and Technology Program of Henan Province (172102210017).
通信作者:陈越(cyue2008@126.com)

据上传下载的通信开销过大.针对上述问题,提出一种支持用户权限动态变更的可更新属性加密方案(updatable attribute-based encryption scheme supporting dynamic change of user rights, SDCUR-UABE).通过在密文策略属性加密中构造属性及用户版本密钥,在撤销用户属性时只需更新用户私钥对应的转换密钥构件;撤销系统属性时需要更新属性版本密钥来实现对密文密钥部分构件的可替换更新;撤销用户私钥时只需更新用户版本密钥.由此避免了基于数据重加密实现密文更新带来的巨大计算开销及通信开销.此外,在方案构造中利用密钥分割实现数据解密外包来降低用户的解密开销.理论分析及实验验证表明:在保证密文前向安全性的前提下,该方案能够有效解决云存储系统中用户权限动态变更时密文更新的计算效率与通信开销问题,同时减轻了用户解密的计算量.

关键词 云存储;属性加密;解密外包;属性撤销;私钥撤销

中图法分类号 TP309

云计算技术的大规模应用使得存储数据的隐私保护问题日益凸显.随着用户对数据的安全性和访问控制灵活性提出了更高要求,属性加密技术在解决此类问题上发挥着越来越重要的作用.

在实际应用中,由于用户权限具有动态变化的特性,用户属性发生变更或用户退出系统时,进行用户属性撤销或私钥撤销对于系统安全至关重要,这是属性加密所必须解决的问题,也是研究的一个难点.通常的解决方法是将访问策略中包含被撤销属性的所有密文进行更新,但存在计算及通信开销较大的问题.比如,在系统运行过程中当出现大量用户权限变更频繁(如系统属性撤销、用户属性撤销以及用户退出、用户私钥泄露)时,密文更新带来的巨大计算量易造成系统瓶颈.因此需要考虑一种高效的更新方法,在保证密文安全性的同时能够以较低计算开销来应对属性撤销或用户私钥撤销.

1 相关工作

近年来,许多学者已经关注属性基加密安全数据共享中属性撤销及用户私钥撤销的需求,并在应对高效属性撤销及密文更新的问题上做了大量研究工作.

密文策略属性加密中的属性撤销问题首次在文献[1]中提出,需要用户与属性授权中心多次交互;文献[2]在文献[1]的基础上为每个用户和属性添加截止日期,解决了密钥多次协商问题.但要求保持用户和授权中心实时在线;文献[3]提出的方案限制了用户剩余属性的解密权限,不符合数据属主设置访问策略的初衷;文献[4]通过实现用户私钥及密文同步更新来达到用户属性撤销的目的,但访问结构单一;文献[5]未考虑系统属性撤销;文献[6]在用户属性及用户私钥撤销时均需要更新部分密文,计算开销较大.

文献[7]提出的属性撤销方案中公钥参数与用户数量线性相关,易造成公钥参数过长;文献[8]在实现属性撤销时只需进行密文密钥部分更新,但用户属性撤销实质上是移除被撤销属性对应的权限,剩余属性权限应保留,此时可以通过直接更新用户私钥的方式实现;文献[9]基于 shamir 秘密共享及访问树结构提出了属性撤销方案,但在秘密共享的效率上低于线性秘密分享方案(linear secret sharing scheme, LSSS)[10];文献[11]基于文献[12]构造免密钥托管的密钥产生协议,但要求用户属性撤销后不具备任何访问权限,这和实际情况不相符,且方案不能支持高效的系统属性撤销.

文献[13]在撤销属性过程中采用懒惰重加密技术更新密文,计算及通信开销较大;文献[14]利用代理重加密技术将属性撤销实现系统属性撤销,但未给出用户属性撤销及用户私钥撤销算法;文献[15]提出的方案在密钥维护代价方面有待改进,需要考虑如何降低密钥更新的工作量以及实现属性直接撤销;文献[16]利用属性组的概念有效地解决了属性撤销的问题,但组管理器需要更新其他用户的密钥;文献[17]提出一种支持关键字搜索与属性撤销的属性加密方案,可以在分布式多属性授权中心下实现细粒度的搜索授权;文献[18]通过设置代理解密密钥列表实现用户私钥撤销,但未给出属性撤销的实现方法;文献[19]能够实现属性级用户撤销,但需要将被撤销属性对应的密文进行更新,若访问策略涉及被撤销属性的密文数量较多时,云端密文更新计算开销过大.

文献[20]中,中央控制在解密过程中通过直接拒绝为撤销列表中的用户返回中间密文达到撤销用户的目的.虽然所构造方案利用安全两方计算技术解决了密钥托管问题,但此时密文的安全性过度依赖于中央控制的可靠性,被撤销用户若通过某种手

段获取密文后仍然具备密文解密能力,因此降低了存储密文的安全性;文献[21]通过对被撤销属性对应的密文进行更新实现用户属性撤销;文献[22]利用属性撤销加密原语和 Merkle 散列树来实现细粒度的访问控制和可验证的数据删除;文献[23]提出了 LU-MA-ABE(large universe and multi-authority attribute-based encryption)方案,同时支持解密外包,属性撤销以及策略更新;文献[24]在雾计算系统中提出基于多授权中心属性签密的数据访问控制方案(data access control scheme based on multi-authority attribute-based signcryption with computation outsourcing and attribute revocation, OMDAC-ABSC),支持匿名身份认证,属性撤销以及公开验证.但上述文献并未就系统属性撤销及用户私钥撤销展开研究.

通过上述国内外相关研究进展分析,现阶段实现支持间接属性撤销的用户权限变更主要依赖于密文密钥的更新.虽然基于属性版本密钥更新可以实现相关密文密钥的同步演化,避免数据重加密的带来的计算开销,但对于用户属性撤销而言,若数据中心包含大量涉及被撤销属性的密文,则计算代价过高.本文基于密文策略属性加密展开研究,通过为用户及属性设置版本密钥,设计支持高效用户属性撤销、用户私钥撤销及系统属性撤销的数据外包密文策略属性加密方案,即 SDCUR-UABE(updatable attribute-based encryption scheme supporting dynamic change of user rights),由此实现高效的用户权限动态变更,并利用密钥分割技术将数据解密外包来降低用户解密开销.

2 预备知识

2.1 双线性映射

假设 G_0,G_1 是 2 个阶为大素数 p 的乘法循环群,双线性映射 $e:G_0\times G_0\rightarrow G_1$ 具有 3 个性质:

1) 双线性性.对任意 $g_1,g_2\in G_0$ 以及 $a,b\in\mathbb{Z}_p$,都有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$.

2) 非退化性.存在 $g_0\in G_0$,使得 $e(g_0,g_0)\neq 1$.

3) 可计算性.对任意 $g_1,g_2\in G_0$,存在多项式时间算法计算 $e(g_1,g_2)$.

2.2 线性秘密共享方案(LSSS)

每一个单调的布尔表达式都可以转化为一个等价的 LSSS 秘密共享方案[21],一个参与方集合 Q 上的 LSSS 秘密共享矩阵是$\mathbb{Z}_p$域上线性的,如果它具有 2 个性质:

1) 各方共享的秘密形成一个$\mathbb{Z}_p$域上的矩阵;

2) 秘密共享方案存在一个共享生成矩阵 $\boldsymbol{M}_{l\times m}$,对所有 $i=1,2,\cdots,l$,$\boldsymbol{M}$ 的第 i 行 $\boldsymbol{M}_i$ 被标识为参与方 $\rho(i)$($\rho:\{1,2,\cdots,l\}\rightarrow Q$),同时有列向量 $\boldsymbol{v}=(s,r_2,r_3,\cdots,r_m)^{\mathrm{T}}$,其中 $s\in\mathbb{Z}_p$是将要共享的秘密值,而 $r_2,r_3,\cdots,r_m\in\mathbb{Z}_p$是随机数.则向量 $\boldsymbol{M}\cdot\boldsymbol{v}$ 为秘密 s 的 l 个共享子秘密,且$(\boldsymbol{M}\cdot\boldsymbol{v})_i$ 属于$\rho(i)$.

假定一个 LSSS 秘密共享方案的访问结构为 Λ.令 $S\in\Lambda$ 为一个授权属性集合,定义 $I\subset\{1,2,\cdots,l\}$且 $I=\{i:\rho(i)\in S\}$.存在常量$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$对任意合法共享秘密$\{\lambda_i\}$,有 $\sum_{i\in I}(\omega_i\lambda_i)=\sum_{i\in I}\omega_i(\boldsymbol{M}_i\cdot\boldsymbol{v})=\boldsymbol{\varepsilon}\cdot\boldsymbol{v}=s$,其中 $\boldsymbol{\varepsilon}=(1,0,\cdots,0)$.这些常量值$\{\omega_i\}$可以在与共享生成矩阵 $\boldsymbol{M}$ 的大小相关的多项式时间内计算出来,而对于未授权的集合,这些常量值不存在.

2.3 判定性 q-Parallel BDHE 假设

选择一个阶为大素数 p 的群 G_0,其生成元为 g.随机选取 $a,s,b_1,b_2,\cdots,b_q\in\mathbb{Z}_p$,给定敌手参数:

$$y=(g,g^s,g^a,\cdots,g^{(a^q)},g^{(a^{q+2})},\cdots,g^{(a^{2q})},$$
$$\forall 1\leqslant j\leqslant q:\ g^{sb_j},g^{a/b_j},\cdots,g^{(a^q/b_j)},g^{(a^{q+2}/b_j)},\cdots,g^{(a^{2q}/b_j)},$$
$$\forall 1\leqslant j,k\leqslant q,k\neq j:\ g^{asb_k/b_j},g^{a^2sb_k/b_j},\cdots,g^{(a^qsb_k/b_j)}),$$

对于敌手而言,区分 $e(g,g)^{a^{q+1}s}\in G_1$ 和 G_1 中的某个随机元素 R 是困难的.

定义算法 $\mathcal{B}$ 的输出为$d\in\{0,1\}$,若输出概率满足$|Pr[\mathcal{B}(y,T=e(g,g)^{a^{q+1}s})=0]-Pr[\mathcal{B}(y,T=R)=0]|\geqslant\varepsilon$,则称 $\mathcal{B}$ 解决群 G_0 中判定性 q-Parallel BDHE 假设的优势为 ε.如果不存在多项式时间算法 $\mathcal{B}$ 能够以不可忽略的优势攻破判定 q-Parallel BDHE 困难问题,我们称判定 q-Parallel BDHE 假设成立.

3 SDCUR-UABE 方案设计

3.1 系统模型

本文提出的 SDCUR-UABE 方案系统模型如图 1 所示.系统主要由属性授权中心(attribute authority, AA)、云存储服务器(cloud storage server, CSS)、代理解密服务器(proxy decryption server, PDS)、数据属主(data owner, DO)和数据用户(data user, DU)5 个部分组成,分别提供密钥生成、密文存储、代理解密、数据加密和数据解密服务.DO 可通过终端进行数据加密并上传至 CSS,而 DU 可

通过云端下载数据并解密.在数据解密时,系统将计算开销较大的部分运算外包给代理解密服务器来降低 DU 计算开销.由于代理解密服务器和云服务商是诚实并好奇的,它们既会诚实地按照指示正确地执行步骤,也会出于好奇在工作过程中窥探用户数据隐私.因此在方案设计中,代理服务器所持有的代理解密密钥并不能将密文还原成明文,而用户上传的数据在云存储服务器中也始终以密文形式存储.各参与方的职责在 3.2 节方案构建中进行具体描述.

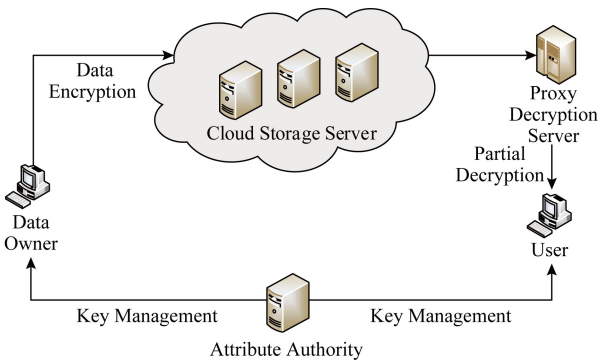


Fig. 1 System model of SDCUR-UABE

图 1 SDCUR-UABE 方案系统模型

3.2 方案构建

定义双线性映射 $e:G_0\times G_0\rightarrow G_1$ 以及散列函数 $H_1:\{0,1\}^*\rightarrow G_0$.其中,$\{0,1\}^*$ 代表任意长度的二进制串.本文方案包含 5 个阶段:

1) $Setup(\lambda,U)\rightarrow(PK,MK,PK_x)$.

初始化过程,由属性授权中心执行.输入为安全参数及全局描述.为覆盖最一般的情形,令 $U=\{0,1\}^*$,随机选择 $\alpha,a,\beta\in\mathbb{Z}_p$,设置主私钥 $MK=(\beta,g^\alpha)$,公开参数 $PK=(g,e(g,g)^a,g^a,H_1)$.属性授权中心为系统属性集中的每个属性 x 设置属性版本 $V_x\in\mathbb{Z}_p$(可以与时间相关)以及公开属性密钥 $PK_x=g^{V_x}$.

2) $KeyGen(MSK,S)\rightarrow(SK,TK)$.

密钥产生过程,由属性授权中心执行.选择随机的变量 $t,z\in\mathbb{Z}_p^*$,首先设置转换密钥

$$TK=(PK,L=g^{\beta t/z},$$
$$\{K_x\}_{x\in S}=\{(H_1(x)\times g^{V_x})^{\beta t/z}\}_{x\in S}).$$

然后设置用户版本密钥 $VK_u=g^{\alpha/\beta}g^{at}$ 以及用户私钥 $SK=(z,TK)$.

3) $Encrypt(PK,m\in\{0,1\}^k,(\boldsymbol{M}^*,\rho))\rightarrow CT$.

数据加密阶段,由数据属主执行.输入为公开参数 PK 以及消息 m.此外,输入 LSSS 类型的访问策略 $(\boldsymbol{M},\rho)$,函数 ρ 将矩阵 $\boldsymbol{M}$ 的每一行映射到一个属性,其中 $\boldsymbol{M}$ 是一个 $l\times n$ 的矩阵.算法随机选择列向量 $\boldsymbol{v}=(s,r_2,r_3,\cdots,r_n)\in\mathbb{Z}_p^n$,用于共享秘密 s.对于所有的 $i=1,2,\cdots,l$,有 $\lambda_i=(\boldsymbol{M}\cdot\boldsymbol{v})_i$,其中 $\boldsymbol{M}_i$ 是矩阵 $\boldsymbol{M}$ 的第 i 行.另外,算法随机选择变量 $r_1,r_2,\cdots,r_l\in\mathbb{Z}_p$,产生密文 $CT=(C,C',(C_i,D_i))$,其中:

$$C=m\times e(g,g)^{as},\tag{1}$$
$$C'=g^{\beta s/z},\tag{2}$$
$$(C_i,D_i)=((C_1=g^{a\lambda_1}\times(H_1(\rho(1))\times g^{V_{\rho(1)}})^{-r_1},D_1=g^{r_1}),\cdots,(C_l=g^{a\lambda_l}\times(H_1(\rho(l))\times g^{V_{\rho(l)}})^{-r_l},D_l=g^{r_l}))\tag{3}$$

以及对访问矩阵的描述 $(\boldsymbol{M},\rho)$.

4) $Transform(TK,CT)\rightarrow parCT$.

代理解密阶段,由代理解密服务器运行.算法输入为某个属性集合 S 对应的 $TK=(PK,L,\{K_x\}_{x\in S})$,以及对应于 $(\boldsymbol{M},\rho)$ 的密文 $CT=(C,C',(C_i,D_i))$.若属性集合 S 不满足设定的访问结构,则输出 $\perp$.若满足,则定义集合 $I=\{i:\rho(i)\in S\}$,且满足 $I\subset\{1,2,\cdots,l\}$.存在常量 $\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$,对任意合法共享秘密份额 $\{\lambda_i\}$,都有 $\sum_{i\in I}(\omega_i\lambda_i)=\sum_{i\in I}\omega_i\times(\boldsymbol{M}_i\cdot\boldsymbol{v})=\boldsymbol{\varepsilon}\cdot\boldsymbol{v}=s$ 成立.计算半解密密文为

$$parCT=\left(e\left(\prod_{i\in I}C_i^{\omega_i},L\right)\times\prod_{i\in I}e(D_i^{\omega_i},K_{\rho(i)})\right)=$$
$$e\left(\prod_{i\in I}g^{a\omega_i\lambda_i}(H_1(\rho(i))\times g^{V_{\rho(i)}})^{-r_i\omega_i},g^{\beta t/z}\right)\times$$
$$\left(\prod_{i\in I}e(g^{r_i\omega_i},(H_1(\rho(i))\times g^{V_{\rho(i)}})^{\beta t/z})\right)=$$
$$e\left(\prod_{i\in I}g^{a\omega_i\lambda_i},g^{\beta t/z}\right)\times$$
$$e\left(\prod_{i\in I}(H_1(\rho(i))\times g^{V_{\rho(i)}})^{-r_i\omega_i},g^{\beta t/z}\right)\times$$
$$\left(\prod_{i\in I}e(g^{r_i\omega_i},(H_1(\rho(i))\times g^{V_{\rho(i)}})^{\beta t/z})\right)=$$
$$e(g,g)^{(a\beta t/z)\cdot\sum_{i\in I}(\omega_i\lambda_i)}=e(g,g)^{at\beta s/z}.\tag{4}$$

5) $UserVerandDec(C',VK_u,parCT)\rightarrow CT'$.

用户验证阶段,由属性授权中心执行,输入为密文构件 C',用户版本密钥 VK_u 及半解密密文 $parCT$ 并计算:

$$CT'=e(C',VK_u)/parCT=$$
$$e(g^{\beta s/z},g^{\alpha/\beta}g^{at})/e(g,g)^{at\beta s/z}=e(g,g)^{as/z}.\tag{5}$$

6) $Decrypt(SK,CT')\rightarrow m$.

数据解密阶段,客户端执行,输入为用户私钥及半解密密文并计算:

$$m'=C/CT'^{SK_u}=m\times e(g,g)^{as}/(e(g,g)^{as/z})^z=m.\tag{6}$$

3.3 用户权限变更

用户权限变更包括用户属性撤销、系统属性撤

销以及用户私钥撤销 3 种情况,相对应的用户权限的变化情况分析为:用户某属性因为到期或者其他原因被撤销时,不能影响该用户剩余属性集的解密能力以及拥有该属性的其他用户的解密权限;撤销系统某属性影响拥有该属性的所有用户的解密能力,同时需要对访问策略涉及该属性的所有密文进行更新;用户私钥撤销即撤销该用户的所有访问权限(可以看做是用户属性撤销的特殊情形,等价于撤销该用户所有属性).

3.3.1 用户属性撤销

撤销用户 A 某属性 att 时(对应属性版本为 V_{att}),AA 为用户 A 产生一个升级密钥 $UUK=g^{(V'_{att}-V_{att})\beta t/z}$ 并发送给相应的代理解密服务器.代理解密服务器将用户 A 私钥对应的 TK 中关联被撤销属性的密钥构件 K_x 升级为 $K'_x=K_x\times UUK$,其他部分不变,即:

$$TK'=(PK,L=g^{\beta t/z},\{K_x\}_{x\in S}). \tag{7}$$

对于 $\forall x\in S, x\neq att$,有:

$$\{K_x\}_{x\in S}=\{(H_1(x)\times g^{V_x})^{\beta t/z}\}_{x\in S}; \tag{8}$$

对于 $x=att$,有:

$$\{K'_x\}_{x\in S}=\{K_x\times UUK\}_{x\in S}=\{(H_1(x)\times g^{V'_x})^{\beta t/z}\}_{x\in S}. \tag{9}$$

由于用户属性撤销而非私钥撤销,因此用户 A 剩余属性集的解密能力以及拥有该属性的其他用户的解密权限不变,此时无需更新用户版本密钥.为保证密文的前向安全性,可以从 3 个方面讨论方案正确性.

1) 撤销 att 前可解密,撤销之后亦可解密.

由代理解密过程知,在半解密密文 $parCT$ 以及 $CT'=e(C',VK_u)/parCT$ 计算过程中,私钥分量 TK 的更新只影响 $e\left(\prod_{i\in I}C_i^{\omega_i},L\right)$ 中 $e\left(\prod_{i\in I}g^{a\omega_i\lambda_i},g^{\beta t/z}\right)$ 的计算,即 $e(g,g)^{(a\beta t/z)\cdot\sum_{i\in I}(\omega_i\lambda_i)}$. 由 LSSS 秘密共享方案知,若剩余属性集合仍满足访问结构(即$(\boldsymbol{M},\rho)$),则存在常量$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$使得 $\sum_{i\in I}(\omega_i\lambda_i)=s$,即不影响后续解密.

2) 撤销 att 前可解密,撤销之后不可解密.

同理,若撤销 att 前可解密,说明在上述过程中最后环节存在常量$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$使得 $\sum_{i\in I}(\omega_i\lambda_i)=s$,而撤销属性 att 后(可能是关键属性),使得剩余属性集合不满足访问矩阵,因此不存在常量$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$来恢复共享秘密 s.上述情形成立.

3) 撤销 att 前不可解密,撤销之后不可解密.

同理,若撤销 att 前不可解密,说明在上述过程中最后环节不存在常量$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$来恢复共享秘密 s.由于访问结构的单调性,显然撤销属性 att 后剩余属性集合仍不满足访问矩阵,即无法完成解密.上述情形成立.

用户属性撤销过程可由属性授权中心独立完成,只需对用户私钥的部分构件进行更新即可,无需对其他用户私钥对应的转换密钥以及访问策略涉及被撤销属性的密文进行更新,能够极大降低因用户属性撤销引起的权限变更的相关计算开销.

3.3.2 系统属性撤销

系统属性撤销和用户属性撤销类似.由于系统属性撤销涉及包含该属性的所有用户,因此对相应的用户需要分发新的私钥分量 TK,同时对访问矩阵中涉及被撤销属性的密文进行更新.

需要说明的是系统属性撤销后,在访问策略不变的情形下,包含被撤销属性的用户解密权限降低,可能会背离数据属主定义策略的初衷,但通过本节提出的属性撤销算法,能够在保证已有密文的前向安全性基础上保留数据属主原有访问策略的可解密用户范围,而非简单地将撤销属性的部分构件去掉.应满足:之前有属性 att 且可/不可访问的,撤销 att 后还能/不可访问;对于之前没有 att 且可访问/不可访问的用户,在系统属性 att 撤销后仍能保持原有权限.此时用户版本密钥无需更新.

这里,通过对转换密钥和涉及被撤销属性的密文中属性版本的更新,实现系统属性撤销,保证撤销前密文的前向安全性.具体过程为:

撤销系统某属性 att 时(对应属性版本为 V_{att}),AA 首先为该属性随机产生一个新的版本 V'_{att},然后通知所有 DO 将当前属性密钥 PK_{att} 更新为$\{g^{V'_{att}}\}$.

AA 为所有拥有属性 att 的用户产生一个升级密钥 $UUK=g^{(V'_{att}-V_{att})\beta t/z}$ 并发送给相应的代理解密服务器.由于每个用户的解密私钥 z 不同,因此对应的 UUK 也不相同,任何用户都不能用别人的 UUK 来为自己的代理解密密钥 TK 升级.代理解密服务器将属性集包含 att 的各个用户私钥对应的 TK 中关联被撤销属性的密钥构件 K_x 升级为 $K'_x=K_x\times UUK$,其他部分不变.我们有:

$$TK'=(PK,L=g^{\beta t/z},\{K_x\}_{x\in S}). \tag{10}$$

对于 $\forall x\in S, x\neq att$,有:

$$\{K_x\}_{x\in S}=\{(H_1(x)\times g^{V_x})^{\beta t/z}\}_{x\in S}; \tag{11}$$

对于 $x=att$,有:

$$\{K'_x\}_{x\in S}=\{K_x\times UUK\}_{x\in S}=\{(H_1(x)\times g^{V'_x})^{\beta t/z}\}_{x\in S}. \tag{12}$$

然后 AA 为所有访问策略中包含属性 att 的密文产生升级密钥 $CUK=D_i^{-(V'_{a_j}-V_{a_j})}$ 并发送给云存储服务器,用于将密文中对应属性 att 的密文构件 C_i 升级为 $C'_i=C_i\times CUK$,升级后的密文为 $CT=(C,C',(C_i,D_i))$,其中:

$$C=m\times e(g,g)^{as},C'=g^{\beta s/z}. \tag{13}$$

$\forall\rho(i)\neq att$,

$$(C_i,D_i)=(C_i=g^{a\lambda_i}\times(H_1(\rho(i))\times g^{V_{\rho(i)}})^{-r_i},D_i=g^{r_i}); \tag{14}$$

$\forall\rho(i)=att$,

$$(C_i,D_i)=(C'_i=C_i\times CUK=g^{a\lambda_i}\times(H_1(\rho(i))\times g^{V'_{\rho(i)}})^{-r_i},D_i=g^{r_i}). \tag{15}$$

系统属性撤销过程需要为拥有待撤销属性的用户进行代理解密密钥部分更新,并为访问策略中包含待撤销属性的密文进行相应更新.但通过本节提出的属性撤销算法,能够在保证已有密文的前向安全性基础上保留数据属主原有访问策略的可解密用户范围.为实现上述目标,可从 4 个方面讨论方案正确性.

1) 用户持有属性 att,撤销前可解密,撤销之后亦可解密.

撤销系统属性 att 之前,转换密钥 TK 为

$$TK=(PK,L=g^{\beta t/z},\{K_x\}_{x\in S}=\{(H_1(x)\times g^{V_x})^{\beta t/z}\}_{x\in S}. \tag{16}$$

用户符合解密条件可正常解密;撤销系统属性 att 之后,通过将属性密钥 PK_{att} 更新为 $\{g^{V'_{att}}\}$,对于 $x=att$,将转换密钥的构件进行升级为

$$\{K'_x\}_{x\in S}=\{K_x\times UUK\}_{x\in S}=\{(H_1(x)\times g^{V_{x'}})^{\beta t/z}\}_{x\in S}. \tag{17}$$

同时升级密文构件,即 $\forall\rho(i)=att$,

$$(C_i,D_i)=(C'_i=C_i\times CUK=g^{a\lambda_i}\times(H_1(\rho(i))\times g^{V'_{\rho(i)}})^{-r_i},D_i=g^{r_i}). \tag{18}$$

由于转换密钥和密文中涉及 att 的构件是同步更新,因此保证了系统属性 att 撤销之后拥有属性 att 且撤销前可解密的用户仍然能够解密密文.

2) 用户持有属性 att,撤销前不可解密,撤销之后亦不可解密.

同理,撤销系统属性 att 之后,上述情形用户私钥对应的转换密钥中涉及 att 的构件以及密文中包含 att 的构件为同步更新,在系统属性撤销前该类型用户不具备解密条件,撤销之后仍然不具备解密条件.

3) 用户属性集不包含 att,撤销前可解密,撤销之后亦可解密.

由于用户属性集不包含 att,则系统属性 att 撤销之后属性密钥 PK_{att} 更新为 $\{g^{V'_{att}}\}$,关于 att 的用户转换密钥对应的构件以及密文中访问策略涉及 att 的构件同步更新,对用户解密权限不影响,即撤销前可解密,撤销之后亦可解密.

4) 用户属性集不包含 att,撤销前不可解密,撤销之后亦不可解密.

同理可以说明,系统属性 att 撤销前后上述用户解密权限不变.

3.3.3 用户私钥撤销

当系统中某些用户被判定为“恶意用户”或者某些用户因其他原因退出系统时,需要通过撤销该用户私钥以保证该用户可解密密文的安全性.

此时属性授权中心 AA 只需对被撤销用户版本密钥进行更新,当前私钥无需变动.即更新用户版本密钥为 $VK'_u=g^{\alpha/\beta}g^{at'}$.在用户解密验证阶段,需要计算 $e(C',VK_u)/parCT$,即 $e(g^{\beta s/z},g^{\alpha/\beta}g^{at})/e(g,g)^{at\beta s/z}$.用户版本密钥更新之前,和密文处于同一个时间周期,$e(g,g)^{at\beta s/z}$ 可以消去.而版本密钥更新后即需要计算 $e(g^{\beta s/z},g^{\alpha/\beta})e(g^{\beta s/z},g^{at'})/e(g,g)^{at\beta s/z}$,由于时间周期 t 值不同,在执行 $Decrypt(SK,CT')$ 过程时,显然无法恢复消息 m.

4 安全性分析

4.1 安全模型

现在我们定义 SDCUR-UABE 方案的敌手 $\mathcal{A}$ 和挑战者 C 之间的 CPA 安全游戏.

初始化:挑战者 C 运行 3.2 节 $Setup$ 算法并将公开参数 PK 传给敌手 $\mathcal{A}$,主私钥 MK 自己保留.

阶段 1. 敌手 $\mathcal{A}$ 向挑战者 C 进行多项式有限次的属性集合 $S_1,S_2,\cdots,S_{q_1}$ 对应的私钥问询.挑战者 C 将这些私钥发送给敌手 $\mathcal{A}$.

挑战. 在这个阶段,敌手 $\mathcal{A}$ 从希望被挑战的消息空间中选择 2 个等长的明文消息 m_0,m_1 并提交.此外敌手提交一个要挑战的访问结构 $\boldsymbol{M}^*$ 且阶段 1 中的属性集合 $S_1,S_2,\cdots,S_{q_1}$ 均不满足该访问结构.挑战者随机掷硬币 $b\in\{0,1\}$ 并返回给敌手 $\mathcal{A}$ 在访问结构 $\boldsymbol{M}^*$ 下加密 m_b 形成的密文 CT^*.

阶段 2. 重复阶段 1 的私钥询问过程,其中问询的属性集合 $S_{q_1+1},S_{q_1+2},\cdots,S_q$ 对应的私钥均不满足要挑战的访问结构 $\boldsymbol{M}^*$.

猜测. 在这个阶段中,敌手 $\mathcal{A}$ 输出一个对 b 的猜测 $b'\in\{0,1\}$.

在这个攻击游戏中敌手 $\mathcal{A}$ 获胜的概率定义为

$$|Pr[b'=b]-1/2|. \tag{19}$$

定义 1. SDCUR-UABE 方案是安全的,如果在多项式时间内没有敌手能够以不可忽略的优势赢得上述游戏.

4.2 安全性证明

定理 1. 若判定性 q-Parallel BDHE 假设成立,那么没有多项式时间的敌手能够选择性地攻破本文提出的 SDCUR-UABE 方案,其中挑战矩阵为 $\boldsymbol{M}^*$,大小为 $l^* \times n^*$,其中 $l^*, n^* \leqslant q$.

证明. 假设存在一个多项式时间的敌手 $\mathcal{A}$ 能够在上述安全模型中能够以优势 $\varepsilon = Adv_{\mathcal{A}}$ 选择性地攻破 SDCUR-UABE 方案,设其挑战矩阵为 $\boldsymbol{M}^*$ $(l^* \times n^*)$,其中 $l^*, n^* \leqslant q$,那么我们可以构建模拟器 $\mathcal{B}$ 能够以不可忽略的优势攻破判定性 q-Parallel BDHE 假设.

初始化. 模拟器 $\mathcal{B}$ 以判定性 q-Parallel BDHE 假设中的 y, T 为输入,敌手 $\mathcal{A}$ 提交访问策略$(\boldsymbol{M}^*, \rho^*)$,矩阵 $\boldsymbol{M}^*$ 的列数为 n^*.

建立. 在该阶段模拟器 $\mathcal{B}$ 随机选择 $\alpha' \in \mathbb{Z}_p$ 并计算 $e(g,g)^{\alpha} = e(g^{a^q}, g^{a^q}) e(g,g)^{\alpha'}$,即有 $\alpha = \alpha' + a^{q+1}$.选择一个随机预言机 h 并建立一个列表.当调用 h 时,如果 $h(x)$已经存在列表中,则直接返回结果;如果 $h(x)$不存在列表中,则随机选择 $z_x \in \mathbb{Z}_p$.设 X 是满足 $\rho^*(i) = x$ 这一条件的 i 的集合,则设置:

$$h_x = g^{z_x} \prod_{i \in X} g^{a \boldsymbol{M}^*_{i,1}/b_i} \times g^{a^2 \boldsymbol{M}^*_{i,2}/b_i} \cdots g^{a^{n^*} \boldsymbol{M}^*_{i,n^*}/b_i}, \quad (20)$$

如果 $X = \varnothing$,则设置 $h_x = g^{z_x}$.由于 z_x 是随机选取的,因此上述参数是随机分布的.

阶段 1. 在该阶段模拟器 $\mathcal{B}$ 回答敌手关于属性集为 S 的私钥问询,其中 S 不满足访问矩阵 $\boldsymbol{M}^*$.

模拟器首先选择一个随机值 $r \in \mathbb{Z}_p$,并找到一个向量 $\boldsymbol{\omega} = (\omega_1, \omega_2, \cdots, \omega_{n^*}) \in \mathbb{Z}_p^{n^*}$ 使得 $\omega_1 = -1$ 并且对于满足 $\rho^*(i) \in S$ 所有的 i,都有 $\boldsymbol{\omega} \cdot \boldsymbol{M}^*_i = \boldsymbol{0}$.由 LSSS 定义知这样一个向量必然存在.注意若这样一个向量不存在,则向量$(1,0,\cdots,0)$为属性集 S 的长度.模拟器设置

$$L = g^{r/z} \prod_{i=1}^{n^*} (g^{(aq+1-i)/z})^{\omega_i} = g^{\beta t/z}, \quad (21)$$

即 $t = (r + \omega_1 a^q + \omega_2 a^{q-1} + \cdots + \omega_{n^*} a^{q-n^*+1})/\beta$.通过对 t 进行定义,可以看到 g^{at} 包含代数式项 $g^{-aq+1/\beta}$,在创建 VK_u 的过程中可以通过与 $g^{\alpha/\beta} = g^{\alpha'/\beta} \cdot g^{aq+1/\beta}$ 进行乘法运算消去.

模拟器计算 VK_u:

$$VK_u = g^{\alpha'/\beta} g^{ar/\beta} \prod_{i=2}^{n^*} (g^{(aq+2-i)/\beta})^{\omega_i}. \quad (22)$$

对于 $\forall x \in S$ 来计算 K_x.如果不存在 i 满足 $\rho^*(i) = x$,可令 $K_x = L^{z_x} \times L^{V_x}$.对于 $x \in S$ 且 x 在访问结构中出现的情形,必须保证 g^{a^{q+1}/b_i} 形式的项都能够被模拟.此外,有 $\boldsymbol{\omega} \cdot \boldsymbol{M}^*_i = 0$,因此这些项都能够消去.

仍然令 X 是满足 $\rho^*(i) = x$ 这一条件的 i 的集合,模拟器创建 K_x:

$$K_x = L^{z_x} L^{V_x} \prod_{i \in X} \prod_{j=1}^{n^*} (g^{(a^j/b_i)r} \times \prod_{k=1, k \neq j}^{n^*} (g^{a^{q+1+j-k}/b_i})^{\omega_k})^{\boldsymbol{M}^*_{i,j}}.$$

挑战. 敌手提交 2 个消息 m_0, m_1 给 $\mathcal{B}$.模拟器 $\mathcal{B}$ 随机选择 $b \in \{0,1\}$,并计算 $C = m_b \times T \times e(g^s, g^{\alpha'})$ 以及 $C' = g^s$.$\mathcal{B}$ 随机选择随机值 $y'_2, y'_3, \cdots, y'_{n^*}$,并使用向量 $\boldsymbol{v} = (s, sa + y'_2, sa^2 + y'_3, \cdots, sa^{n-1} + y'_{n^*}) \in \mathbb{Z}_p^{n^*}$ 来共享秘密.此外,模拟器选择随机值 $r'_1, r'_2, \cdots, r'_l \in \mathbb{Z}_p$.对于 $i = 1, 2, \cdots, n^*$,定义 R_i 为所有 $k \neq i$ 且满足 $\rho^*(i) = \rho^*(k)$的 k 的集合.挑战密文构件生成为

$$D_i = g^{-r'_i} g^{-sb_i}, \quad (23)$$

$$C_i = g^{V_{\rho^*(i)}} h_{\rho^*(i)}^{r'_i} (\prod_{j=2}^{n^*} (g^a)^{\boldsymbol{M}^*_{i,j} \cdot y'_j}) \times (g^{b_i \cdot s})^{V_{\rho^*(i)} - z_{\rho^*(i)}} \times (\prod_{k \in R_i} \prod_{j=1}^{n^*} (g^{a^j \cdot s \cdot (b_i/b_k)})^{\boldsymbol{M}^*_{k,j}}). \quad (24)$$

阶段 2. 和阶段 1 类似,敌手 $\mathcal{A}$ 继续向模拟器 $\mathcal{B}$ 提交一系列属性集合进行私钥问询,其限制与阶段 1 相同.

猜测. 敌手 $\mathcal{A}$ 最终输出一个对 b 的猜测 b'.如果 $b' = b$,模拟器输出 0 来猜测 $T = e(g,g)^{a^{q+1}s}$,否则输出 1 表示 T 是群 G_1 中的随机元素.当 $T = e(g,g)^{a^{q+1}s}$ 时模拟器 $\mathcal{B}$ 提供了一个有效的模拟,根据安全模型中敌手 $\mathcal{A}$ 的优势定义 $Adv_{\mathcal{A}} = |Pr[b' = b] - 1/2|$,可以得出:

$$Adv_{\mathcal{A}} = |Pr[b' = b] - \frac{1}{2}| = |Pr[\mathcal{B}(y, T = e(g,g)^{a^{q+1}s}) = 0] - \frac{1}{2}|. \quad (25)$$

当 T 是群 G_1 中的随机元素时,m_b 对于敌手而言是完全随机的,因此有 $Pr[\mathcal{B}(y, T = R) = 0] = \frac{1}{2}$.

此时模拟器 $\mathcal{B}$ 的优势为

$$Adv_{\mathcal{B}} = \frac{1}{2} Pr[\mathcal{B}(y, T = e(g,g)^{a^{q+1}s}) = 0] + \frac{1}{2} Pr[\mathcal{B}(y, T = R) = 0] - \frac{1}{2} = \frac{1}{2}\left(\frac{1}{2} + Adv_{\mathcal{A}}\right) + \frac{1}{4} - \frac{1}{2} = \frac{\varepsilon}{2}. \quad (26)$$

由于敌手 $\mathcal{A}$ 的优势 ε 是不可忽略的,因此模拟器 $\mathcal{B}$ 的优势也是不可忽略的,即可以构建模拟器 $\mathcal{B}$ 能够以不可忽略的优势攻破判定性 q-Parallel BDHE 困难问题. 证毕.

定理 2. 本文提出的 SDCUR-UABE 方案中设置的代理解密服务器不影响方案的安全性,且该方案能够抵抗用户与代理解密服务器之间的合谋攻击.

证明. 首先,方案中设置的代理解密服务器所持有的代理解密密钥 TK 为半解密密钥,其密钥构件 $L=g^{\beta t/z}$ 及 $\{K_x\}_{x\in S}=\{(H_1(x)\times g^{V_x})^{\beta t/z}\}_{x\in S}$ 与属性授权中心执行密钥产生算法所选择随机的变量 $t,z\in\mathbb{Z}_p^*$ 有关.进行代理解密时生成的半解密密文 $e(g,g)^{at\beta s/z}$ 对于非授权用户而言仍以密文形式存储,因而在降低合法用户解密开销的同时保证了密文的安全性.

考虑多个用户及代理解密服务器之间进行合谋的场景.正常进行代理解密计算过程为

$$parCT=\left(e\left(\prod_{i\in I}C_i^{\omega_i},L\right)\times\prod_{i\in I}e(D_i^{\omega_i},K_{\rho(i)})\right)=$$
$$e\left(\prod_{i\in I}g^{a\omega_i\lambda_i}(H_1(\rho(i))\times g^{V_{\rho(i)}})^{-r_i\omega_i},g^{\beta t/z}\right)\times$$
$$\left(\prod_{i\in I}e(g^{r_i\omega_i},(H_1(\rho(i))\times g^{V_{\rho(i)}})^{\beta t/z})\right)=$$
$$e(g,g)^{(a\beta t/z)\cdot\sum_{i\in I}(\omega_i\lambda_i)}=e(g,g)^{at\beta s/z}. \quad (27)$$

若上述过程用到某用户私钥对应的转换密钥 TK 的部分构件 $L'_u=g^{\beta t'/z'}$ 和 $K_{x_u}=(H_1(x_u)\times g^{V_{x_u}})^{\beta t'/z'}$,以及当前密文 CT.进行代理解密计算后生成的半解密密文:

$$parCT=e(g,g)^{(a\beta t/z)\cdot\sum_{i\in I}(\omega_i\lambda_i)}\times e((H_1(\rho(i))\times$$
$$g^{V_{\rho(i)}}),g)^{\beta r_i\omega_i(-t/z+t'/z')}=e(g,g)^{at\beta s/z}\times$$
$$e((H_1(\rho(i))\times g^{V_{\rho(i)}}),g)^{\beta r_i\omega_i(-t/z+t'/z')}. \quad (28)$$

由于用户各自持有的私钥为不同的随机变量 z_i 且变量 t 在用户私钥生成时随机选取,此时无法将表达式 $e((H_1(\rho(i))\times g^{V_{\rho(i)}}),g)^{\beta r_i\omega_i(-t/z+t'/z')}$ 消去,因此在计算过程中各自属性集不满足访问策略的合谋用户之间无法利用其他用户私钥对应的 TK 密钥(代理解密服务器持有)构件完成代理解密过程,即合谋攻击失败. 证毕.

5 性能分析及实验验证

5.1 理论分析

本节对 SDCUR-UABE 方案在数据加解密、用户属性撤销、系统属性撤销以及用户私钥撤销过程的计算开销进行分析.定义符号含义如表 1 所示:

Table 1 Symbols and Meanings

表 1 符号及含义

Symbols	Meanings
$\lvert U\rvert$	Number of system attributes
$\lvert S\rvert$	Number of attributes in user attributes set
d	Number of attributes involved in access policy
exp	Exponentiation in group element
$\hat{e}$	Bilinear pairing operation
c	Multiplication operations or constants
SKE	A symmetric encryption operation
t	Threshold value
h	Height of the access tree
$\lvert A_p\rvert$	Number of user attributes satisfing access policy
$\lvert CT_{att}\rvert$	Number of ciphertexts with att in access policy
$\lvert AS_{att}\rvert$	Number of users with att in user attributes set
$\lvert CT\rvert$	Number of ciphertexts in CSP
$\lvert SK\rvert$	Number of secret keys in AA

由于方案将大量的解密运算外包给 CSS,用户解密时只需 1 次幂运算即可.综上,用户加密计算开销为 $(\lvert A_p\rvert+3)exp$,解密过程计算开销为 exp.

若撤销用户 A 某属性 att,首先在用户私钥对应的转换密钥的更新阶段,授权中心 AA 首先更新属性密钥需要一次幂操作,代理解密服务器使用更新密钥更新转换密钥只需要一次乘法操作即可完成.由 3.3.1 节分析可知,此时无需更新密文.

撤销系统某属性 att 时,需要对所有访问策略涉及 att 的密文进行更新.本文系统属性撤销过程中 AA 更新属性密钥需要一次幂操作,然后为访问策略里包含属性 att 的密文生成一个升级密钥 CUK 需要 1 次幂操作,此时 AA 计算开销为 $2exp$;接下来代理解密服务器使用更新密钥为属性集包含被撤销属性的所有用户更新相应的转换密钥(每次更新只需要一次乘法操作即可完成),计算开销可记为 $\lvert AS_{att}\rvert\times c$;此外,在保证已有密文的前向安全性基础上为保留数据属主原有访问策略的可解密用户范围,需要云存储服务器对密文访问结构中涉及被撤销属性的所有用户更新密文构件(根据获得的升级密钥更新一次密文只需要一次乘法操作即可完成),计算开销为 $\lvert CT_{att}\rvert\times c$.

如 3.3.3 节所述,当系统中某些用户被判定为"恶意用户"或者某些用户因某种原因退出系统时,需要通过撤销该用户私钥以保证该用户可解密密文的安全性.此时属性授权中心 AA 只需对被撤销用户版本密钥进行更新,当前私钥无需变动.即更新用户版本密钥为 $VK'_u=g^{\alpha/\beta}g^{at'}$ 即可(具体分析过程见

3.3.3 节),此时属性授权中心 AA 只需要进行一次乘法运算和一次幂运算即可,而用户私钥对应的转换密钥以及密文无需更新,及代理解密服务器和云存储服务器无需参与计算.本文方案和其他关于属性撤销的经典方案在安全假设、安全模型等各类情况的对比如表 2、表 3 所示.

Table 2 Comparison of Security and Computation Cost in User Attribute Revocation

表 2 安全性及用户属性撤销过程计算开销对比

Schemes	Security Assumption	Security Model	Decryption Outsourcing	User Decryption Overhead	User Attribute Revocation		
					Attribute Authority	Proxy Server	Cloud Storage Server
Ref [3]	Generic Group Model	CPA	Yes	$(\lvert A_p\rvert+1)\bar{e}$			
Ref [4]	DBDH	CPA	No	$(\lvert U\rvert+1)\bar{e}+\lvert U\rvert exp$	c	$\lvert S\rvert(\lvert AS_{att}\rvert-1)\ exp$	$(d\lvert CT_{att}\rvert)\ exp$
Ref [5]	BDH		No	$(2d+1)\bar{e}+(2d+2)exp$	$(2\lvert A_p\rvert+1)\ exp$		$\lvert CT_{att}\rvert(d+3)exp$
Ref [8]	q-parallel BDHE	CPA	No	$(2\lvert A_p\rvert+1)\bar{e}+\lvert A_p\rvert exp$	$4exp$		$2exp$
Ref [11]	q-parallel BDHE	CPA	No	$2\lvert A_p\rvert\bar{e}+(3\lvert A_p\rvert+2)exp$	$(\lvert S\rvert+4)exp$	c	
Ref [13]	q-parallel BDHE	CPA	No	$\bar{e}+5exp$	$\lvert AS_{att}\rvert exp$		$\lvert CT_{att}\rvert exp$
Ref [14]	q-parallel BDHE	CPA	No	$(2\lvert A_p\rvert+1)\bar{e}+$ $(2\lvert A_p\rvert+2)exp$	$(\lvert AS_{att}\rvert-1)\ exp$		$\lvert CT_{att}\rvert exp$
Ref [15]	DBDH	CPA	No	$(\lvert S\rvert+1)\bar{e}+(2\lvert S\rvert)exp$	c	$\lvert CT_{att}\rvert(d+2)exp$	
Ref [20]	q-parallel BDHE	CPA	Yes	$3exp$	$\lvert AS_{att}\rvert exp$		$\lvert CT_{att}\rvert exp$
Ref [23]	q-DPBDHE2	CPA	Yes	$(\lvert AS_{att}\rvert+5)\ exp$	$h\times SKE$	0	$8d\ exp$
Ref [24]	q-parallel BDHE	CCA	Yes	exp	$(t+4)exp$	0	$(2\lvert CT_{att}\rvert)\ exp+\lvert CT_{att}\rvert c$
Ref [25]	q-parallel BDHE	CPA	Yes	$3exp$			
Ours	q-parallel BDHE	CPA	Yes	exp	exp	c	0

Table 3 Comparison of Computation Cost in System Attribute Revocation and User Private Key Revocation

表 3 系统属性撤销及用户私钥撤销过程计算开销对比

Schemes	System Attribute Revocation			User Private Key Revocation		
	Attribute Authority	Proxy Server	Cloud Storage Server	Attribute Authority	Proxy Server	Cloud Storage Server
Ref [3]						
Ref [4]						
Ref [5]				$(2\lvert A_p\rvert+1)\ exp$		$\lvert CT_{att}\rvert(d+3)exp$
Ref [8]						
Ref [11]				$exp+c$	c	
Ref [13]	$(\lvert AS_{att}\rvert+1)\ exp$		$\lvert CT_{att}\rvert exp$	$(\lvert SK\rvert+1)\lvert S\rvert exp$		$\lvert CT\rvert\lvert S\rvert exp$
Ref [14]	$\lvert AS_{att}\rvert exp$		$\lvert CT_{att}\rvert exp$	$(\lvert SK\rvert+1)\lvert S\rvert exp$		$\lvert CT\rvert\lvert S\rvert exp$
Ref [15]						
Ref [20]				c	0	0
Ref [23]						
Ref [24]						
Ref [25]						
Ours	$3exp$	$\lvert AS_{att}\rvert c$	$\lvert CT_{att}\rvert c$	exp	0	0

由表 2、表 3 的对比结果可知,文献[4]缺乏解密外包机制导致用户解密计算开销较大,且在用户属性撤销时需要将未被撤销属性的用户私钥和所有访问策略涉及被撤销属性的密文进行更新;类似地,文献[5,8,11,13-15]均存在用户解密开销大的问题,一方面在用户属性撤销时需要同时更新密文密钥,另一方面没有考虑到用户权限变更中的系统属性或者用户私钥撤销情形.文献[20]将解密运算过程中复杂的双线性配对运算外包给云服务商来提高解密效率,但用户属性撤销实质是被撤销属性对应权限的移除,剩余属性权限应当保留,此时可以通过直接更新用户私钥的方式实现,在计算开销上优于"通过计算更新密钥对不包含被撤销属性的用户密钥与包含被撤销属性的密文进行更新"实现的用户属性撤销.

5.2 实验验证

通过理论分析,本文在加解密功能实现和用户权限变更的效率上具有较大优势.为了对方案的实

际性能进行评估,本节在密钥生成、数据加密、代理解密以及用户解密 4 个方面与 VFO-CP-ABE(fully outsourced ciphertext-policy attribute-based encryption with verifiability)方案[25]进行计算时间的仿真实验测试对比.该方案是一种支持可验证的完全外包密文策略属性基加密方案,能够同时实现密钥生成、数据加密以及解密阶段的外包计算功能,解决上述各阶段需要大量计算资源的问题,对于计算资源有限的用户优势更为明显.实验环境描述如下:

Windows 64 b 操作系统、Intel® Core™ i7-4770 CPU (3.4 GHz)、内存 12 GB、基于 JPBC(Java pairing-based cryptography)库进行实验代码的编写.

在参与对比方案的具体实现过程中使用(att_1 AND att_2 AND … AND att_n)形式的访问策略进行测试,其中 att_i 代表属性.参与测试的属性数量每次以 10 递增,选取从 10～100 共 10 种访问策略.对于每种策略重复进行多次独立测试,去掉最高值与最低值后取剩余数据平均值作为本次测试对象的实验结果.

实验测试结果如图 2 所示,图 2(a)～(d)分别展示了 SDCUR-UABE 方案与 VFO-CP-ABE 方案在密钥生成、数据加密、代理解密以及用户解密 4 个方面的计算开销对比.由于 VFO-CP-ABE 方案中转换密钥 TK 和取回密钥 RK 由解密用户进行 $KeyBlind(SK)$ 运算产生,而本文所提方案中转换密钥的产生由属性授权中心产生,无需用户参与.这里将 $KeyBlind(SK)$ 过程开销计入密钥产生阶段的总开销.从实验结果来看,在密钥生成阶段本文提出的 SDCUR-UABE 与 VFO-CP-ABE 计算开销相近;在加密阶段 SDCUR-UABE 方案的开销随访问策略中的属性数量增加而增大,而 VFO-CP-ABE 进行加密外包.解密过程包括代理服务器进行部分解密和数据用户解密 2 个阶段.该过程中 2 个方案的计算开销都较小,但从结果来看 SDCUR-UABE 方案更有优势.整体来说,本文提出的方案能够满足实际需求,且在解密运算上具有较高的效率.

讨论用户属性撤销过程的计算开销.这里主要对涉及相关运算的属性授权中心和云存储服务器的计算开销进行测试.由表 3 分析结果可知,选取用于对比的 LU-MA-ABE 方案[23]和 OMDAC-ABSC 方案[24]

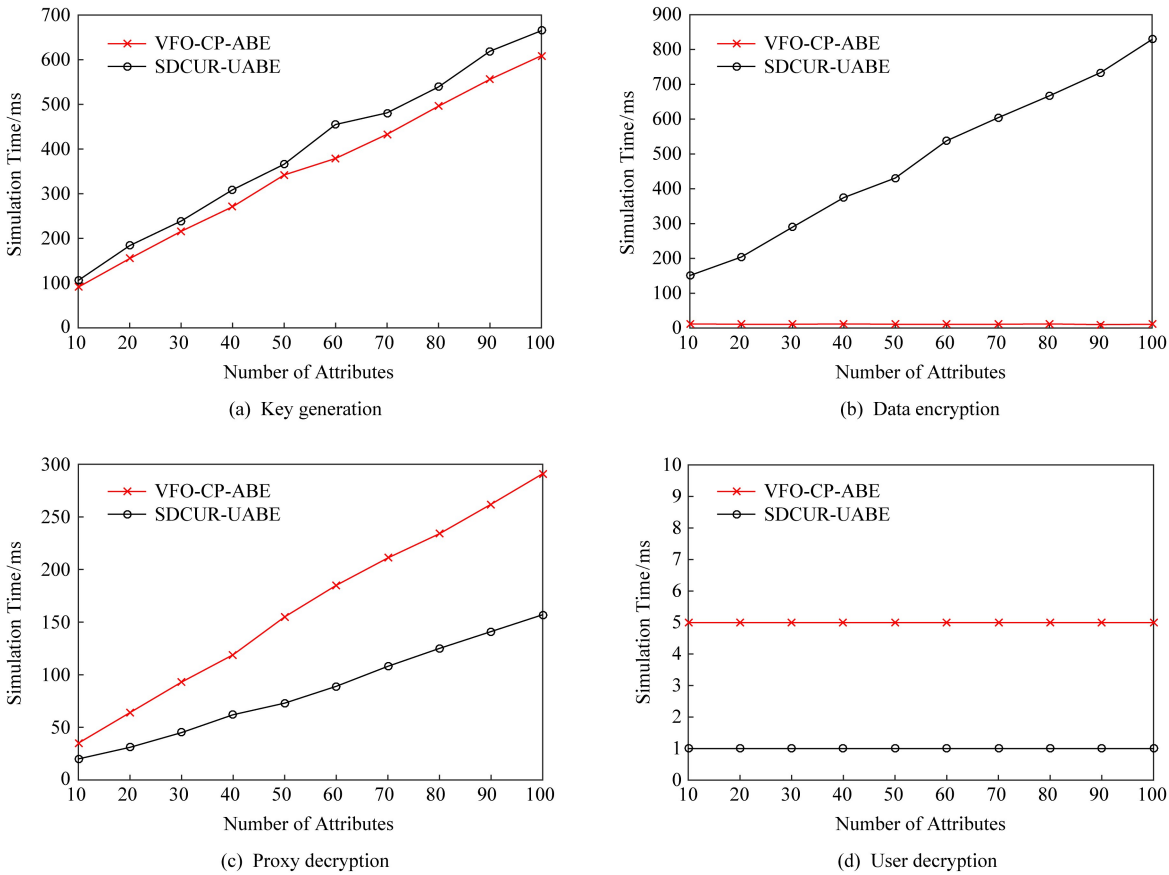


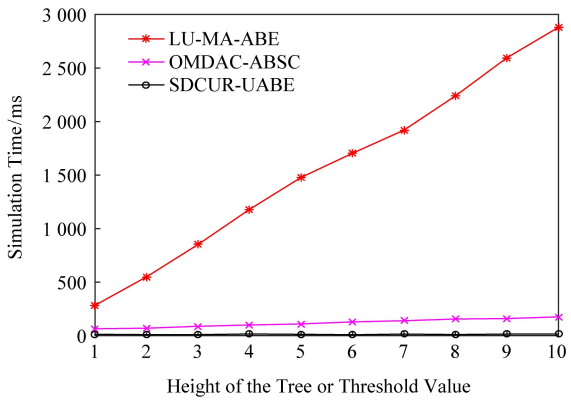
Fig. 2 Comparison of computation cost for key steps of SDCUR-UABE

图 2 SDCUR-UABE 方案中关键步骤计算开销对比

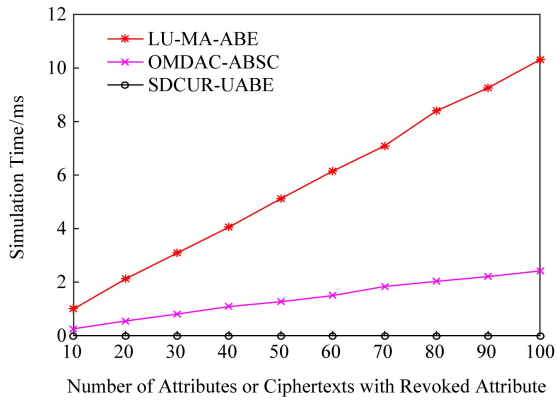
均支持高效属性撤销.用户属性撤销时,LU-MA-ABE 和 OMDAC-ABSC 方案中无需代理服务器参与运算,而本文中分析代理服务器的开销为常数(如乘法运算等),计算量较小,在实验仿真中开销可忽略.

需要说明的是 LU-MA-ABE 方案在每次进行属性撤销时候需要对新选取的属性组密钥进行被撤销属性的最小覆盖集(minimum covering set, MCS)元素个数次的对称加密.根据其定义的用于属性组密钥分发的二进制状态树,最小覆盖集元素个数 N_{MCS} 为树的高度 h,即 $N_{MCS}=h$.在实验过程中选取的对称加密密钥长度为 128 b,并基于 sun.misc.BASE64Encoder 和 sun.misc.BASE64Decoder 实现对属性组密钥的对称加解密.LU-MA-ABE 和 OMDAC-ABSC 方案中属性授权中心的计算开销分别依赖于二进制状态树的高度和门限值的大小,这里选取从 1～10 共 10 种不同的变化(递增值为 1);而云存储服务器进行密文更新过程计算开销分别依赖于访问结构中涉及的属性数量以及访问结构中涉及被撤销属性的密文数量,这里选取从 10～100 共 10 种不同的变化(递增值为 10).

用户属性撤销过程中 AA 的计算开销实验对比结果如图 3(a)所示.由于 LU-MA-ABE 方案需要对属性组密钥进行加密,计算开销较大,且随着状态树的高度增加呈线性增长;OMDAC-ABSC 方案中 AA 主要进行幂运算,相对 LU-MA-ABE 方案开销较小,但也随着门限值的增加而增大.而本文中用户属性撤销时 AA 只需要进行固定次数的幂运算,因此计算开销较小.从实验结果来看,测试的相关参与方的计算开销和理论分析一致.图 3(b)展示了该过程中云存储服务器 CSS 的计算开销对比,其中本文提出的 SDCUR-UABE 方案无需对密文进行更新,因此在用户属性撤销中更为高效.



(a) Computation overhead of AA in user attribute revocation



(b) Computation overhead of CSS in user attribute revocation

Fig. 3 Comparison of computation overhead in user attribute revocation

图 3 用户属性撤销过程计算开销对比

图 4 和图 5 分别展示了 SDCUR-UABE 方案在系统属性撤销和用户私钥撤销时的计算开销的仿真实验结果.由于大部分方案并未在用户属性撤销的同时对系统属性撤销和用户私钥撤销展开讨论,因此这里只是对本文提出的方案在系统属性撤销和用户私钥撤销过程的性能进行测试和说明.从表 3 的理论分析可以看出,在这 2 个阶段中,AA 均只需要进行固定次数的幂运算,计算开销较小;而代理服务器和云存储服务器在用户私钥撤销时无需参与运算,在系统属性撤销时候只需要进行固定次数的乘法运算,计算开销可以忽略.从仿真实验结果来看,SDCUR-UABE 方案在计算性能上能够满足系统属性撤销和用户私钥撤销的实际需求,且具有较高的效率,能够有效应对加密云存储中频繁的用户权限变更的情形.

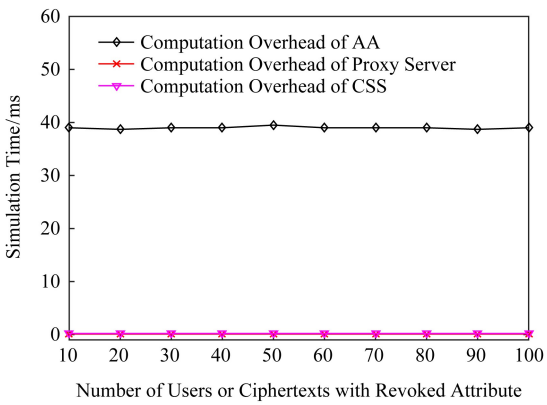


Fig. 4 Computation overhead in system attribute revocation

图 4 系统属性撤销过程计算开销

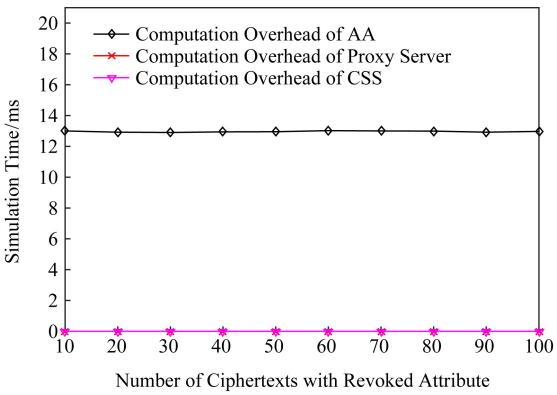


Fig. 5 Computation overhead in user private key revocation

图 5 用户私钥撤销过程计算开销

6 结束语

针对云存储系统中因用户权限动态变更带来的密文密钥更新计算开销过大等问题,本文在密文策略属性加密的基础上通过构造属性版本密钥和用户版本密钥设计了 SDCUR-UABE 方案.撤销用户属性时,无需对其他用户私钥及访问策略中涉及被撤销属性的密文进行更新,有效降低了密钥授权中心与云存储服务器的计算开销;撤销系统属性时,通过更新属性版本密钥并生成转换密钥及密文更新所需要的更新密钥,实现对密文密钥关键构件的可替换更新,有效解决了通用方法中基于密钥分发和重加密实现密文密钥更新带来的计算开销大的问题以及未能保证密文前向安全性问题;撤销用户私钥时,只需要将用户版本密钥进行更新,无需更新密文,避免了存储密文重加密带来的巨大计算及通信开销.此外,方案在设计过程中将解密运算开销较大的部分外包给代理解密服务器,在保证数据安全性的前提下降低了客户端的解密运算开销.理论分析及实验验证表明,本文提出的 SDCUR-UABE 方案能够实现用户属性、系统属性以及用户私钥的高效撤销,同时保证密文的前后向安全性和用户解密的高效性,从而有效解决了属性基加密云存储系统中因用户权限动态变更所导致的密文密钥更新计算开销过大等问题.

参 考 文 献

[1] Pirretti M, Traynor P, Mcdaniel P, et al. Secure attribute-based systems [C] //Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 99-112

[2] 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

[3] Luan I, Petkovic M, Nikova S, et al. Mediated ciphertext-policy attribute-based encryption and its application [C] //Proc of the 10th Int Workshop on Information Security Applications. Berlin: Springer, 2009: 309-323

[4] 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

[5] Hur J, Dong K N. Attribute-Based access control with efficient revocation in data outsourcing systems [J]. IEEE Transactions on Parallel & Distributed Systems, 2010, 22 (7): 1214-1221

[6] Wang Guojun, Liu Qin, Wu Jie, et al. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers [J]. Computers & Security, 2011, 30(5): 320-331

[7] Wang Pengpian, Feng Dengguo, Zhang Liwu. CP-ABE scheme supporting fully fine-grained attribute revocation [J]. Journal of Software, 2012, 23(10): 2805-2816 (in Chinese)
(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)

[8] Yang Kan, Jia Xiaohua, Ren Kaili. Attribute-based fine-grained access control with efficient revocation in cloud storage systems [C] //Proc of the 8th ACM SIGSAC Symp on Information, Computer and Communications Security. New York: ACM, 2013: 523-528

[9] Huang Qinlong, Ma Zhaofeng, Yang Yixian, et al. EABDS: Attribute-based secure data sharing with efficient revocation in cloud computing [J]. Chinese Journal of Electronics, 2015, 24(4): 862-868

[10] Liu Mengjun, Liu Shubo, Wang Ying, et al. Optimizing the decryption efficiency in LSSS matrix-based attribute-based encryption without given policy [J]. Acta Electronica Sinica, 2015, 43(6): 1065-1072 (in Chinese)
(刘梦君, 刘树波, 王颖, 等. 基于 LSSS 共享矩阵无授权策略的属性密码解密效率提高方案[J]. 电子学报, 2015, 43 (6): 1065-1072)

[11] Xia Zhihua, Zhang Liangao, Liu Dandan. Attribute-based access control scheme with efficient revocation in cloud computing [J]. China Communications, 2016, 13(7): 92-99

[12] Hur J. Improving security and efficiency in attribute-based data sharing [J]. IEEE Transactions on Knowledge & Data Engineering, 2013, 25(10): 2271-2282

[13] Qian Huiling, Li Jiguo, Zhang Yichen, et al. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation [J]. International Journal of Information Security, 2015, 14(6): 487-497

[14] Naruse T, Mohri M, Shiraishi Y. Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating [J]. Human-centric Computing and Information Sciences, 2015, 5(1): 8-20

[15] Yan Xixi, Tang Yongli. Attribute-based encryption scheme with efficient revocation in data outsourcing systems [J]. Journal on Communications, 2015, 36(10): 92-100 (in Chinese)
(闫玺玺, 汤永利. 数据外包环境下一种支持撤销的属性基加密方案[J]. 通信学报, 2015, 36(10): 92-100)

[16] Li Jiguo, Yao Wei, Han Jinguang, et al. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage [J]. IEEE Systems Journal, 2018, 12(2): 1767-1777

[17] Cui Jie, Zhou Han, Zhong Hong, et al. AKSER: Attribute-based keyword search with efficient revocation in cloud computing [J]. Information Sciences, 2018, 423: 343-352

[18] Zhang Kai, Ma Jianfeng, Li Hui, et al. Multi-authority attribute-based encryption with efficient revocation [J]. Journal on Communications, 2017, 38(3): 83-91 (in Chinese)
(张凯, 马建峰, 李辉, 等. 支持高效撤销的多机构属性加密方案[J]. 通信学报, 2017, 38(3): 83-91)

[19] Wang Jianhua, Wang Guangbo, Xu Kaiyong. Ciphertext policy attribute-based encryption scheme supporting attribute level user revocation under large universe [J]. Journal of Electronics & Information Technology, 2017, 39(12): 3013-3022 (in Chinese)
(王建华, 王光波, 徐开勇. 标准模型下可证明安全的支持大规模属性集与属性级用户撤销的 CP-ABE 方案[J]. 电子与信息学报, 2017, 39(12): 3013-3022)

[20] Zhao Zhiyuan, Zhu Zhiqiang, Wang Jianhua, et al. Revocable attribute-based encryption with escrow-free in cloud storage [J]. Journal of Electronics & Information Technology, 2018, 40(1): 1-10 (in Chinese)
(赵志远, 朱智强, 王建华, 等. 云存储环境下无密钥托管可撤销属性基加密方案研究[J]. 电子与信息学报, 2018, 40(1): 1-10)

[21] Wang Guangbo, Liu Haitao, Wang Chenlu, et al. Revocable attribute based encryption in cloud storage [J]. Journal of Computer Research and Development, 2018, 55(6): 1190-1200 (in Chinese)
(王光波, 刘海涛, 王晨露, 等. 云存储环境下可撤销属性加密[J]. 计算机研究与发展, 2018, 55(6): 1190-1200)

[22] Xue Liang, Yu Yong, Li Yannan, et al. Efficient attribute-based encryption with attribute revocation for assured data deletion [J]. Information Sciences, 2019, 479: 640-650

[23] Liu Zechao, Jiang Z L, Wang Xuan, et al. Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating [J]. Journal of Network and Computer Applications, 2018, 108: 112-123

[24] Xu Qian, Tan Chengxiang, Fan Zhijie, et al. Secure data access control for fog computing based on multi-authority attribute-based signcryption with computation outsourcing and attribute revocation [J]. Sensors, 2018, 18(5): 1609-1646

[25] Zhao Zhiyuan, Wang Jianhua, Xu Kaiyong, et al. Fully outsourced attribute-based encryption with verifiability for cloud storage [J]. Journal of Computer Research and Development, 2019, 56(2): 442-452 (in Chinese)
(赵志远, 王建华, 徐开勇, 等. 面向云存储的支持完全外包属性基加密方案[J]. 计算机研究与发展, 2019, 56(2): 442-452)

Yan Xincheng, born in 1991. PhD candidate. His main research interests include cloud data privacy protection and secure data sharing based on cryptography.

Chen Yue, born in 1965. PhD, professor and PhD supervisor. His main research interests include network and information security.

Ba Yang, born in 1989. PhD candidate. His main research interests include blockchain and data security, applied cryptography.

Jia Hongyong, born in 1978. PhD, lecturer. His main research interests include applied cryptography and hierarchical data access control.

Wang Zhonghui, born in 1976. BSc, senior engineer. His main research interests include information security, computer application.