第 43 卷 第 10 期 计 算 机 工 程 2017 年 10 月
Vol. 43 No. 10 Computer Engineering October 2017

·安全技术· 文章编号：1000-3428(2017)10-0109-06 文献标志码：A 中图分类号：TP309

一种支持属性撤销的外包属性加密方案

刘竹松，彭佳鹏

（广东工业大学 计算机学院，广州 510006）

摘 要：针对传统基于密文策略的属性加密方案在密钥生成、密文解密和属性撤销阶段计算开销大的问题，提出一种具有属性撤销功能的外包属性加密方案。在加密过程中使用线性秘密共享机制作为访问结构，将密钥生成和密文解密的部分计算外包，通过为每个用户的私钥设置版本号实现用户属性的撤销，同时证明方案在可重复的选择密文攻击下是安全的。实验结果表明，该方案的计算开销较低，并且能较好地实现密文策略的属性撤销功能。

关键词：访问控制；属性加密；外包；属性撤销；安全性

中文引用格式：刘竹松，彭佳鹏. 一种支持属性撤销的外包属性加密方案[J]. 计算机工程，2017，43(10)：109-114.

英文引用格式：LIU Zhusong，PENG Jiapeng. An Outsourced Attribute-Based Encryption Scheme Supporting Attribute Revocation[J]. Computer Engineering，2017，43(10)：109-114.

An Outsourced Attribute-Based Encryption Scheme Supporting Attribute Revocation

LIU Zhusong，PENG Jiapeng

（School of Computers，Guangdong University of Technology，Guangzhou 510006，China）

【Abstract】 Traditional Ciphertext-Policy Attribute-Based Encryption（CP-ABE） schemes have large computational overhead in key generation，decryption and attribute revocation processes. Aiming at this problem，this paper proposes an outsourced CP-ABE scheme which supports attribute revocation. It utilizes linear secret sharing mechanism as an access structure in the process of encryption and outsources parts of the work in the process of key generation and decryption process. In addition，it achieves attribute revocation by adding a unique number into each user's key. Meanwhile，it proves the security of the proposed scheme under the Repeatable Chosen-Ciphertext Attack（RCCA）. Experimental results demonstrate the efficient performance of the proposed scheme in attribute revocation and low computational overhead.

【Key words】 access control；Attribute-Based Encryption（ABE）；outsourcing；attribute revocation；security

DOI：10.3969/j.issn.1000-3428.2017.10.019

0 概述

随着云计算的发展，数据的存储量越来越大，网络传输速度日益增长，越来越多的数据拥有者将数据存储在云端。云存储服务商的不可靠性以及庞大的存储数据量对云环境下的数据存储和访问提出了更高的安全要求，其中针对用户的访问控制是非常重要的一环，研究者对此进行了一系列的研究。属性加密[1]是目前被广泛应用的访问控制技术，数据拥有者把相关访问结构和信息进行加密，只有拥有的属性集满足此访问结构的用户才能访问信息。近年来，国内外研究者相继提出了一系列方案。为减轻用户的计算开销，文献[2]提出了外包属性加密方案，即用户把大部分的解密工作交由外包解密服务提供商完成，但方案没有减轻属性权威的计算开销，也没有实现属性撤销的功能。文献[3]方案通过生成外包密钥减轻了属性权威的负担，并进一步提高了外包安全性，但也没有实现属性撤销的功能。文献[4-6]提出的方案支持属性的撤销，使用的是代理重加密技术。但因为在云环境下数据量很大，用户的属性集也会很庞大，该方案在进行用户属性撤销时需要重加密具有相关属性的密文，并对其他拥有此属性的用户进行密钥升级，计算量较大。文献[7]提出的基于密文的属性加密方案，通过属性权威更新密文和提供新的密钥来支持属性撤销，但给属性权威带来很大的计算负担，同时也增加了属性权威和用户间的通信代价。文献[8-10]提出了多权威的属性加密方案，有效地提高了系统安全性，但系统的计算开销十分庞大，而且在进行属性撤销时也极为不便。文献[11]提出了基于动态属性的加密方案，

基金项目：国家自然科学基金(61572144)；广东省重大科技专项(2016B030306004，2015B010110001，2014B010117004)；广州市科技计划项目(201604010099，201508010065)。

作者简介：刘竹松(1979—)，男，副教授、博士、CCF 会员，主研方向为数据安全、云计算、大数据；彭佳鹏，硕士研究生。

收稿日期：2016-09-23 **修回日期：**2016-10-24 **E-mail：**25421944@qq.com

解决了属性相对固定、更新较难的问题,但不能实现属性的动态撤销。文献[12]提出了一个完全隐藏访问结构的密文策略属性加密方案,相比传统方案能更深层地隐藏访问策略,但不具备属性更新功能。文献[13]则提出了一种支持属性撤销的属性加密方案。

针对上述方案属性权威计算开销过大且不支持属性撤销的问题,本文提出一种基于密文环境的属性加密(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)方案,在文献[2]方案和文献[3]方案的基础上,进一步降低属性权威计算的负担,并且增加属性撤销的功能。本文方案为每个用户对应的私钥生成一个版本号,当进行属性撤销时,只需要更新此用户私钥的版本号,无需更新密文和升级其他用户的私钥,从而减小计算开销。同时将密钥生成的大部分计算交由外包机构,以减少属性权威计算。最后分析验证本文方案在选择明文攻击(Chosen-Plaintext Attack, CPA)和可重复的选择密文攻击(Replayable Chosen-Ciphertext Attack,RCCA)下是安全的,同时也满足前向安全性和后向安全性。

1 研究背景

1.1 访问结构

设$\{P_1,P_2,\cdots,P_n\}$是参与方的集合,一个集合$A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$满足条件$\forall B,C$:如果$B\in A$且$B\subseteq C$就有$C\in A$,那么它就是单调的。设一个访问结构是集合$A$,它是幂集$2^{\{P_1,P_2,\cdots,P_n\}}$的非空子集。这样对于用户属性集合$S$,属于$A$的集合被称作授权集合,不属于$A$的则被称作非授权集合。

1.2 双线性映射

设G和G_T是2个阶为素数p的乘法循环群,G的生成元是g且映射$e:G\times G=G_T$是双线性映射,具备下列性质:

1)双线性:对于所有的$u,v\in G$和$a,b\in\mathbb{Z}_p$有$e(u^a,v^b)=e(u,v)^{ab}$。

2)非退化:$e(g,g)\neq 1$。

3)可计算:对于所有的$u,v\in G$,存在有效算法计算$e(u,v)$。

1.3 线性秘密共享机制

一个定义在实体集P上的线性秘密共享机制是指:

1)集合P中每个元素所获得的共享部分可以形成一个$\mathbb{Z}_p$上的向量。

2)存在一个l行n列的矩阵$\boldsymbol{M}$使得对于所有的$i=1$到l,$\rho(i)$表示一个元素并对应P的第i行。对于向量$\boldsymbol{v}=(s,r_2,r_3,\cdots,r_n)$,假设$s\in\mathbb{Z}_p$是一个要被分享的秘密,$r_2,r_3,\cdots,r_n\in\mathbb{Z}_p$是随机选取的,则$\boldsymbol{Mv}$得到的向量为这$l$个元素所分享的信息,其中$(\boldsymbol{Mv})_i$属于元素$\rho(i)$。

3)设有一个针对访问结构A的线性秘密共享机制,如果对授权属性集$S\in A$,使$I\subset\{1,2,\cdots,l\}$定义为$I=\{i:\rho(i)\in S\}$,会有常数集合$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$,如果$\{\lambda_i\}$依据$\boldsymbol{M}$合法的分享秘密$s$,会有$\sum_{i\in I}\omega_i\lambda_i=s$,这些常数$\omega_i$可根据矩阵$\boldsymbol{M}$在多项式时间内被求得。

1.4 困难性假设

定义1 q-parallel BDHE(Bilinear Diffie-Hellman Exponent)问题

令G为阶为素数p的有限群,生成元是g,取$a,s,b_1,b_2,\cdots,b_n\in\mathbb{Z}_p$。如果敌手得到如下信息:

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

则认为敌手对于$e(g,g)^{a^{q+1}s}\in G_T$与群G_T上的一个随机元素是计算不可区分的。

2 系统模型和安全性定义

2.1 系统模型

本文的系统模型由表1中各方组成。其中,DO负责上传数据;AA负责用户属性集的管理和密钥生成等操作;KGSP负责部分密钥的生成;CSP负责数据的存储和密文部分解密的工作;User访问数据时进行最终的解密。

表1 文中各个机构的缩写

缩写	描述
DO	数据拥有者
AA	属性权威
KGSP	外包密钥生成服务提供商
CSP	云存储服务提供商同时提供外包解密服务
User	用户

相比较传统的属性加密方案,本文方案增加了外包密钥生成和外包密文解密,有效地减少了AA和User的计算开销,同时也较为高效地实现了用户属性的撤销。系统模型如图1所示。

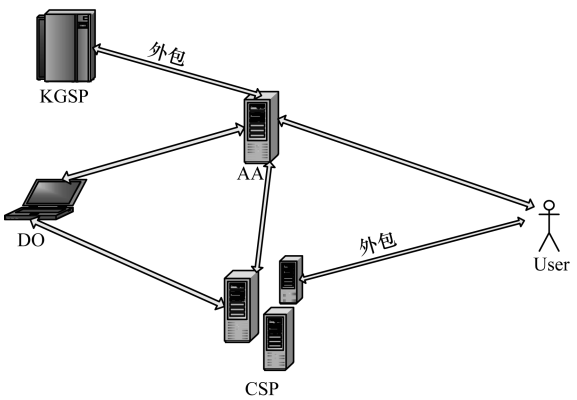

图1 系统模型

相关算法如下:

Setup(λ):初始化算法输入一个安全参数 λ,输出属性全集参数 θ,公钥 PK 和主密钥 MSK。

$\text{KeyGen}_{\text{AA}}(MSK,S)$:AA 负责的部分密钥生成算法输入主密钥 MSK 和用户属性集 S,输出 TK_{AA},用户参数 z,用户私钥版本号 v,参数 t_1 和 t_2。

$\text{KeyGen}_{\text{KGSP}}(PK,t_1,t_2,S)$:KGSP 负责的部分密钥生成算法输入 PK,t_1 和 t_2 以及 S,输出 TK_{KGSP}。

$\text{KeyBlind}(TK_{\text{AA}},TK_{\text{KGSP}})$:密钥整合算法输入 TK_{AA} 和 TK_{KGSP},输出转换密钥 $TK=(TK_{\text{AA}},TK_{\text{KGSP}})$ 和用户私钥 SK。

$\text{Encrypt}(PK,CM,(\boldsymbol{M},\rho),\theta)$:加密算法输入公开密钥 PK,信息 CM 和属性全集参数 θ 依照访问控制策略 $(\boldsymbol{M},\rho)$ 对信息 CM 进行加密输出得到密文 CT。

$\text{Transform}_{\text{out}}(TK,CT)$:转化算法输入转换密钥 TK 和密文 CT,如果 TK 对应的用户属性集不满足 CT 的访问结构,则输出为 $\perp$。当满足访问结构时,进行部分解密输出部分解密密文 CT'。

$\text{Decrypt}_{\text{out}}(SK,CT')$:解密算法输入私钥 SK 和部分解密密文 CT'。如果 CT' 为 $\perp$,则输出为 $\perp$,否则输出解密之后的结果。

$\text{AttributeRev}(z,v,S')$:属性撤销算法输入用户参数 z 和其私钥版本号 v 以及新的用户属性集 S',输出升级密钥 SUK 和新的转换密钥 TK'。

2.2　安全性定义

传统的选择密文攻击(Chosen Ciphertext Attack,CCA)不允许密文发生任何的改变,而外包的目的就是压缩密文,所以,本文方案采用文献[14]提出的 RCCA 模型,该模型允许修改密文但不能改变基本信息。相关定义和游戏方案如下:

定义 2　带外包功能的 RCCA-secure ABE

如果一个带有外包功能的 CP-ABE 是 RCCA-secure 的,那么对于所有多项式时间敌手在以下定义的 RCCA 游戏中至多有可忽略的优势。

Setup:挑战者运行初始化算法生成公开密钥 PK 发送给挑战者。

Phase1:挑战者初始化一个空表 T,一个空集 D 和一个整数 $j=0$。挑战者可以重复地进行下面的查询:

$\text{Create}(I_{\text{key}})$:挑战者设置 $j=j+1$。它对 I_{key} 运行外包密钥生成算法生成密钥对 (SK,TK),然后将 (j,I_{key},SK,TK) 存储到表 T 中,并将转换密钥 TK 发送给敌手。Create 操作可以重复的用相同输入进行运算。

$\text{Corrupt}(i)$:如果在表 T 中存在第 i 项,挑战者从中取出 (i,I_{key},SK,TK),并将 I_{key} 加入集合 D 中,然后把 SK 发送给敌手。如果没有这一项则返回 $\perp$。

$\text{Decrypt}(i,CT)$:如果在表 T 中存在第 i 项,挑战者从中取出 (i,I_{key},SK,TK) 并将 (SK,TK) 发送给敌手。如果没有这一项则返回 $\perp$。

Challenge:敌手提交 2 个相等长度的信息 CM_0 和 CM_1,同时敌手生成一个访问结构 I^*_{enc} 使得对于所有的 $I_{\text{key}}\in D$ 都满足访问结构 I^*_{enc}。挑战者投掷硬币 $b\in\{0,1\}$,然后基于 I^*_{enc} 加密 CM_b 得到密文 CT^* 发送给敌手。

Phase2:重复 Phase 1 的操作并有如下限制。敌手不能进行 Corrupt 查询,因为敌手进行此操作会使其得到一个满足访问结构 I^*_{enc} 的 I_{key},从而被添加到集合 D 中,使得敌手得到 SK 用来解密密文;进行一次小的 Dercypt 查询,Dercypt 查询会在 Phase 1 中被响应,但如果输出结果是 CM_0 或 CM_1 中的一个,挑战者会回复特殊的消息来应对测试。

Guess:敌手输出对 b 的猜测 b',即敌手判断密文 CT^* 是 CM_0 加密得到的还是 CM_1 加密得到的。定义敌手在这个游戏中的优势为 $\Pr[b=b']-\frac{1}{2}$。

3　本文方案

3.1　设计原理

实际应用中本文方案的具体流程如下:首先 DO 运行加密算法利用相关访问结构加密信息得到密文,将密文和访问结构上传到 CSP 上。用户初次访问 CSP 上的文件时需要向 AA 申请密钥。AA 根据用户的属性集生成转换密钥 TK 和用户私钥 SK,将 TK 发送给 CSP,将 SK 发送给用户。用户访问 CSP 上的密文时,如果其对应的 TK 所对应的属性集满足密文的访问结构,CSP 就将会运行转换算法然后将部分解密的密文发送给用户,用户得到部分解密的密文后执行解密操作得到明文。当 AA 需要撤销某个用户的某些属性时,会为这个用户的私钥 SK 生成新的版本号,AA 生成一个升级密钥 SUK 并将其发送给用户,令其升级 SK 得到新的私钥 SK'。AA 生成新的转换密钥 TK' 发送给 CSP,令其删除原来的转换密钥 TK,并使用新的转换密钥 TK'。外包密钥生成、外包解密和属性撤销流程如图 2 ~ 图 4 所示。

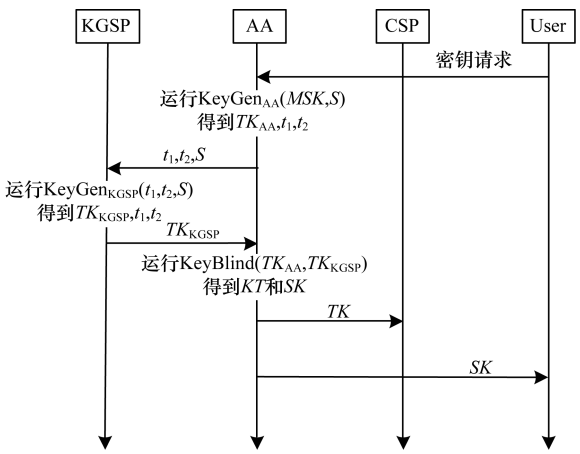

图 2　外包密钥生成流程

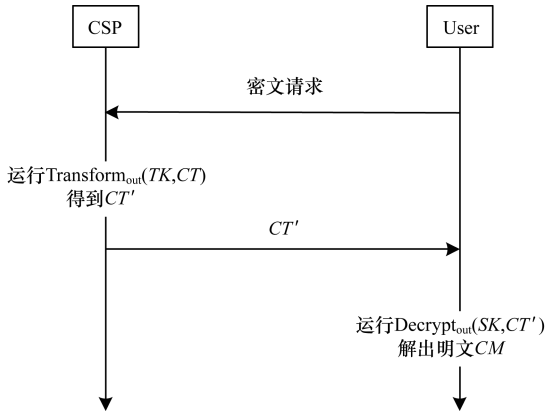

图 3 外包解密流程

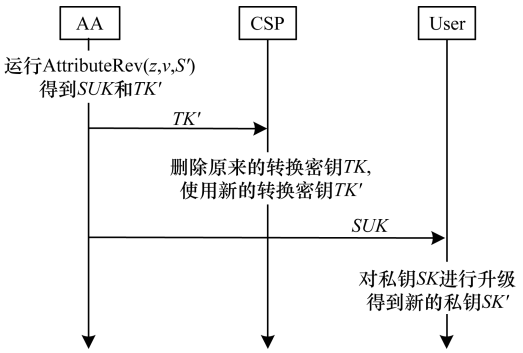

图 4 属性撤销流程

3.2 方案描述

本文方案具体描述如下：

Setup(λ)：Setup 算法首先输入一个安全参数 λ 和一个属性全集描述 $U=\{0,1\}^*$，并为该组属性集生成对应的属性全集参数 $\theta\in\mathbb{Z}_p$，不同属性全集的 θ 值不同。选择一个阶为素数 p 且生成元为 g 的群 G，选择哈希函数 F，它可将 U 中的元素映射为 G 中的一个元素。选择随机数 $\alpha,\beta,a\in\mathbb{Z}_p$。AA 生成主密钥 MSK 仅对属性权威可见，$MSK=(\alpha,\beta,\theta,PK)$，生成公开密钥 PK 对所有人可见：$PK=(g,e(g,g)^{\alpha},g^{a},F)$。

KeyGen$_{AA}$(MSK,S)：对于用户初次的私钥请求，AA 首先在 $\mathbb{Z}_p$ 上为用户选择随机数 z 作为用户参数，每个用户的 z 值唯一且用户之间 z 值不同。计算参数 $t_1=\alpha/z,t_2=\beta/z$ 并将值传给 KGSP，AA 选择随机数 $v\in\mathbb{Z}_p$ 作为用户私钥的版本号，最后生成部分转换密钥：$TK_{AA}=(K_\theta=F(\theta)^{t_2}\cdot g^{t_1(1-v)/\theta})$。

KeyGen$_{KGSP}$(PK,t_1,t_2,S)：KGSP 根据公开公钥 PK，AA 传来的 t_1,t_2 的值和用户属性集 S 生成外包部分转换密钥 TK_{KGSP} 并将其发送给 AA。

$$\begin{aligned}TK_{KGSP}&=(K=g^{t_1}g^{at_2},L=g^{t_2},\{K_x\}_{x\in S}\\&=\{F(x)^{t_2}\}_{x\in S})\end{aligned}$$

KeyBlind(TK_{AA},TK_{KGSP})：AA 得到 KGSP 传来的 TK_{AA}，生成转换密钥 TK 发送给 CSP，生成 $SK=(z/v)$ 发送给用户。

$$\begin{aligned}TK&=(TK_{AA},TK_{KGSP})=(K=g^{t_1}g^{at_2},L=g^{t_2},\{K_x\}_{x\in S}\\&=\{(F(x)^{t_2}\}_{x\in S},F,K_\theta=F(\theta)^{t_2}\cdot g^{t_1(1-v)/\theta})\end{aligned}$$

Encrypt(PK,CM,($\boldsymbol{M}$,ρ),θ)：加密算法输入公开密钥 PK、信息 CM 和属性全集参数 θ，依照访问控制结构($\boldsymbol{M}$,ρ)对信息 CM 进行加密。$\boldsymbol{M}$ 是一个 $l\times n$ 的共享生成矩阵，函数 ρ 将矩阵 $\boldsymbol{M}$ 的每一行映射为一个属性。算法首先随机产生一个矢量 $\boldsymbol{v}=(s,y_2,\cdots,y_n)$，$s\in\mathbb{Z}_p$ 是一个需要被分享的秘密，$y_2,y_3,\cdots,y_n$ 是在 $\mathbb{Z}_p$ 上随机选取的，对 $i=1,2,\cdots,l$，计算 $\lambda_i=v\cdot\boldsymbol{M}_i$，其中 $\boldsymbol{M}_i$ 是 $\boldsymbol{M}$ 的第 i 行向量，另外再从 $\mathbb{Z}_p$ 中选则 l 个随机数 $r_1,r_2,\cdots,r_l$。用户经过加密计算得到密文 $CT=(C,C',(C_1,D_1),(C_2,D_2),\cdots,(C_l,D_l),(C_\theta,D_\theta))$，并把 CT 和($\boldsymbol{M}$,ρ)发送到 CSP 上，CT 的完整表示如下：

$$\begin{aligned}CT&=(C=CM\cdot e(g,g)^{s\alpha},C'\\&=g^{s},(C_1=g^{a\lambda_1}\cdot F(\rho(1))^{-r_1},D_1=g^{r_1}),\cdots,\\&(C_2=g^{a\lambda_2}\cdot F(\rho(2))^{-r_2},D_2=g^{r_2}),\\&(C_l=g^{a\lambda_l}\cdot F(\rho(l))^{-r_l},D_l=g^{r_l}),\\&(C_\theta=g^{s}\cdot F(\theta)^{-s\theta},D_\theta=g^{s\theta}))\end{aligned}$$

Transform$_{out}$(TK,CT)：转化算法输入转换密钥 TK 和密文 CT，如果 TK 对应的属性集不满足 CT 的访问结构，则输出为 $\perp$。当满足访问结构时，使 $I\subset\{1,2,\cdots,l\}$ 定义为 $I=\{i:\rho(i)\in S\}$，会有常数集合 $\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$，如果 $\{\lambda_i\}$ 依据 $\boldsymbol{M}$ 合法地分享秘密 s，就会有 $\sum_{i\in I}\omega_i\boldsymbol{M}_i=\{1,0,\cdots,0\}$，即满足 $\sum_{i\in I}\omega_i\lambda_i=s$。转换算法计算公式如下：

$$\begin{aligned}&\frac{e(C',K)\cdot e(C',L)}{e(\prod_{i\in I}C_i^{\omega_i},L)\cdot\prod_{i\in I}e(D_i^{\omega_i},K_{\rho(i)})\cdot e(C_\theta,L)\cdot e(D_\theta,K_\theta)}\\&=\frac{e(g,g)^{st_1}e(g,g)^{ast_2}e(g,g)^{st_2}}{e(g,g)^{ast_2}e(g,g)^{st_2}e(g,g)^{st_1(1-v)}}\\&=e(g,g)^{st_1v}=e(g,g)^{s\alpha v/z}\end{aligned}$$

然后 CSP 将部分解密密文 CT' 发送给用户，$CT'=(C,e(g,g)^{s\alpha v/z})$。

Decrypt$_{out}$(SK,CT')：如果密文没有被部分解密，则输出为 $\perp$；否则设 T 为 $e(g,g)^{s\alpha v/z}$，即可解出明文 CM，$CM=C/T^{z/v}$。

AttributeRev(z,v,S')：当 AA 需要撤销某个用户的某些属性时，首先为此用户私钥随机生成新的版本号 $v'\in\mathbb{Z}_p$，并生成升级密钥 $SUK=v/v'$，把升级密钥发送给用户，用户执行升级操作得到新的私钥

SK',$SK' = SK \cdot SUK = (z/v) \cdot (v/v') = z/v'$。同时 AA 根据用户私钥新的版本号生成新的部分转换密钥 TK'_{AA},$TK'_{AA} = (K_\theta = F(\theta)^{t_2} \cdot g^{t_1(1-v')/\theta})$,再根据用户属性撤销之后拥有的新的属性集 S'要求 KGSP 执行 KeyGen_{KGSP} 操作生成新的外包部分转换密钥 TK'_{KGSP},并运行 KeyBlind 算法从而生成新的转换密钥 TK'并发送给 CSP,CSP 删除这个用户对应的原来的转换密钥 TK,使用新的转换密钥 TK'。

3.3　安全性证明

定理 1　如果文献[15]方案在 CPA 下是安全的,则本文方案在 CPA 下是安全的。

文献[15]已经证明在 q-parallel BDHE 假设下,没有多项式时间的敌手可选择的以不可忽略的优势破解它的方案,所以,本文方案在 CPA 下是安全的。

定理 2　如果文献[2]在 RCCA 下是安全的,则本文方案在 RCCA 下是安全的。

文献[2]已经证明在 q-parallel BDHE 假设下,没有多项式时间的敌手可选择的以不可忽略的优势破解它的方案,所以,本文方案在 RCCA 下是安全的。

定理 3　本方案是前向安全和后向安全的。

当某个用户的属性被撤销时,AA 会对此用户的私钥 SK 进行升级,并且要求 CSP 更新转换密钥 TK,用户因为他的 SK 版本号已经发生改变,所以不能解密相关的密文,所以本方案满足前向安全性。每一个新用户加入系统后,只要其拥有的属性集满足密文的访问结构,就可以通过私钥解密相关密文,因此,本文方案满足后向安全性。

4　方案比较

4.1　性能分析

将本文的方案与文献[2]方案和文献[3]方案进行比较,用 P 表示一次配对运算,E_G 表示一次在 G 上的多次幂运算。假设一次多次幂运算相当于 2 次单次幂运算且两者运算时间也大致相同。ω 表示属性集,d 表示解密时所需的最小属性数量,3 种方案的计算开销比较如表 2 所示。

表 2　计算开销比较

方案	密钥生成		解密	
	AA	KGSP	DSP/CSP	User
文献[2]方案	$2\lvert\omega\rvert E_G$	–	$2dP + 2dE_G$	E_G
文献[3]方案	$2E_G$	$2\lvert\omega\rvert E_G$	$2dP + 2dE_G$	E_G
本文方案	E_G	$2\lvert\omega\rvert E_G$	$2dP + 2dE_G$	E_G

与文献[2]方案的比较结果显示,本文方案中的 AA 的计算开销为常量,远小于对比方案,减轻了 AA 的负担,并且支持用户属性的撤销;与文献[3]方案的比较结果显示,本文方案在密钥生成阶段 AA 的计算开销进一步降低仅为 E_G,在其他实体没有明显提高计算开销的前提下,实现了用户属性较为高效的撤销,适用范围更广泛。

4.2　实验比较

为更直观地比较不同方案之间的计算开销,本文实现了本文方案以及文献[3]方案,实验在 Linux 系统下运行,主机配置 3.20 GHz 的 Intel(R) Core(TM) 2 Duo CPU 和 4 GB 的 RAM。图 5 ~ 图 7 是本文方案和文献[3]方案在密钥生成、加密和解密阶段计算时间的比较,图 8 显示了本文方案在属性撤销阶段撤销不同数量的属性的计算时间。

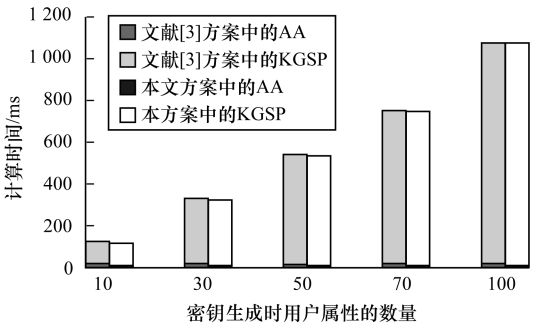

图 5　密钥生成计算时间比较

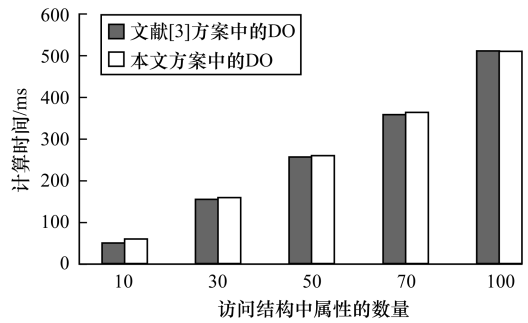

图 6　加密计算时间比较

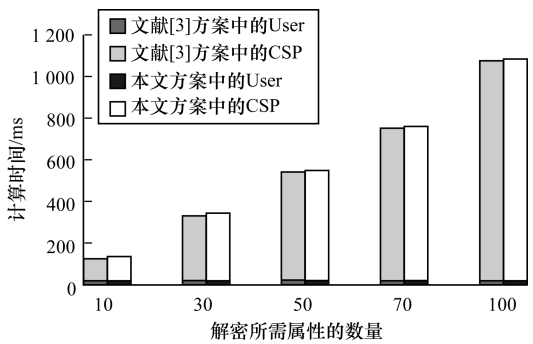

图 7　解密计算时间比较

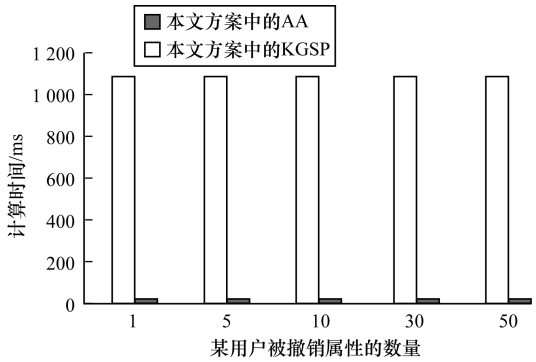

图 8 属性撤销计算时间

由图 5 可以看出,本文方案和文献[3]方案都对密钥生成的工作进行外包,因此,2 种方案的 KGSP 在密钥生成阶段的计算时间大致相同。但本文方案中 AA 的计算时间小于文献[3]方案,从而进一步减轻了 AA 在密钥生成阶段的负担。

由图 6 可以看出,为支持用户属性的撤销,数据拥有者需要进行额外的计算,因此,在加密阶段本文方案的计算时间略大于文献[3]方案,但随着访问结构中属性数量的增加,计算时间也趋于相近。

由图 7 可以看出,在解密阶段,本文方案和文献[3]方案都采用了外包解密技术,因为增加属性撤销功能所带来的额外解密计算,使得在解密阶段本文方案总的计算开销稍大于文献[3]方案,但 2 个方案中 User 的计算开销大致相同。

图 8 为本文方案在属性撤销阶段撤销不同数量属性的计算时间柱状图,假定系统总的属性集合不变,每次撤销的是某个用户的某些属性。由于每次进行属性撤销时 AA 向 KGSP 传入的是更新后的用户属性集,因此在进行属性撤销时系统总的计算时间是不变的,AA 的计算时间也为常量,当需要撤销用户的多个属性时,本文方案较好地实现了属性撤销的功能。

综上所述,本文方案不仅实现了密钥生成和密文解密的外包,而且能够支持用户属性的撤销,减轻了 AA 和 User 的计算开销。

5 结束语

本文提出一种外包属性加密方案,该方案不仅可以进行外包密钥生成和外包解密,同时也支持用户属性的撤销。不同于传统的代理重加密技术,本文方案通过为每个用户的私钥生成一个版本号来进行属性撤销,将线性秘密共享机制作为访问结构,从而更好地进行信息加密。下一步将基于该方案在用户属性的细粒度撤销和安全性方面进行深入研究。

参考文献

[1] SAHAI A,WATERS B. Fuzzy Identity-based Encryption[C]// Proceedings of Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin,Germany: Springer,2005:457-473.

[2] GREEN M,HOHENBERGER S,WATERS B. Outsourcing the Decryption of ABE Ciphertexts[C]//Proceedings of the 20th USENIX Conference on Security. Berkeley,USA: USENIX Association Berkeley,2011:34.

[3] LI Jin,HUANG Xinyi,LI Jingwei,et al. Securely Outsourcing Attribute-based Encryption with Checkability[J]. IEEE Transactions on Parallel and Distributed Systems,2014,25(8):2201-2210.

[4] YU Shucheng,WANG Cong,REN Kui,et al. Attribute Based Data Sharing with Attribute Revocation[C]// Proceedings of the 5th ACM Symposium on Information,Computer and Communications Security. New York,USA: ACM Press,2010:261-270.

[5] HUR J,NOH D K. Attribute-based Access Control with Efficient Revocation in Data Outsourcing Systems[J]. IEEE Transactions on Parallel and Distributed Systems,2011,22(7):1214-1221.

[6] HUR J. Improving Security and Efficiency in Attribute-based Data Sharing[J]. IEEE Transactions on Knowledge and Data Engineering,2013,25(10):2271-2282.

[7] YANG Kan,JIA Xiaohua. Security for Cloud Storage Systems[M]. Berlin,Germany: Springer,2014.

[8] CHASE M. Multi-authority Attribute Based Encryption[C]// Proceedings of Cryptography Conference. Berlin,Germany: Springer,2007:515-534.

[9] CHASE M,CHOW S S M. Improving Privacy and Security in Multi-authority Attribute-based Encryption[C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. New York,USA: ACM Press,2009:121-130.

[10] 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.

[11] 邓宇乔. 基于动态属性的加密方案[J]. 计算机工程,2014,40(4):136-140.

[12] 刘雪艳,郑等凤. 基于素数群完全隐藏访问结构的 CP-ABE 方案[J]. 计算机工程 2016,42(10):140-145.

[13] 李 勇,曾振宇,张晓菲. 支持属性撤销的外包解密方案[J]. 清华大学学报(自然科学版),2013,53(12):1664-1669.

[14] CANETTI R,KRAWCZYK H,NIELSEN J B. Relaxing Chosen-Ciphertext Security[C]//Proceedings of Annual International Cryptology Conference. Berlin,Germany: Springer,2003:565-582.

[15] WATERS B. Ciphertext-policy Attribute-based Encryption: An Expressive,Efficient,and Provably Secure Realization[C]// Proceedings of International Workshop on Public Key Cryptography. Berlin,Germany: Springer,2011:53-70.

编辑 金胡考