·网络空间安全· 文章编号:1000-3428(2021)07-0095-06 文献标志码:A 中图分类号:TP391

一种支持属性撤销的密文策略属性基加密方案

王静宇,周雪娟
(内蒙古科技大学 信息工程学院,内蒙古 包头 014010)

摘 要: 针对传统属性基加密方案中单授权中心计算开销大以及安全性较差等问题,通过引入多个授权中心以及安全两方计算协议等技术,提出一种支持细粒度属性级撤销和用户级撤销的密文策略属性基加密方案。引入多个属性授权中心以颁发并更新属性版本秘钥,同时秘钥生成中心与云存储服务器之间进行安全两方计算等操作,生成并更新用户密钥,从而进行细粒度属性级撤销。在云存储服务器中,对用户列表中的用户唯一秘值及唯一身份值进行操作以实现用户级撤销,同时通过多个授权中心抵抗合谋攻击,并将部分计算工作外包给云端。分析结果表明,与基于AND、访问树和LSSS策略的方案相比,该方案有效增强了系统的安全功能,同时显著降低了系统的计算复杂度。

关键词: 访问控制;密文策略属性基加密;多授权中心;细粒度属性级撤销;用户级撤销

开放科学(资源服务)标志码(OSID):

中文引用格式: 王静宇,周雪娟.一种支持属性撤销的密文策略属性基加密方案[J].计算机工程,2021,47(7):95-100.
英文引用格式: WANG J Y, ZHOU X J. An attribute-based encryption scheme for ciphertext policy that supports attribute revocation[J].Computer Engineering,2021,47(7):95-100.

An Attribute-based Encryption Scheme for Ciphertext Policy that Supports Attribute Revocation

WANG Jingyu, ZHOU Xuejuan
(School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou, Inner Mongolia 014010, China)

【Abstract】 The traditional single-authorization Attribute-Based Encryption (ABE) schemes are limited by the high computing overhead and the poor security. Based on secure two-party computing protocols, this paper proposes a multi-authorization ciphertext policy ABE scheme, which supports fine-grained attribute-level revocation and user-level revocation. The scheme introduces multiple authorization centers to issue and update the secret key of the version. At the same time, secure two-party computation is performed between the secret key generation center and the cloud storage server to generate and update the user key for fine-grained attribute-level revocation. In the cloud storage server, the unique secret value and the unique identity value of each user in the list is operated to realize user-level revocation. In addition, the scheme employs multiple authorization centers to resist collusive attacks, and outsources part of computing tasks to the cloud. The scheme is put to a security test and compared with multiple schemes, including those based on AND, access tree and LSSS strategy. The experimental results show that the proposed scheme effectively enhances system security, and significantly reduces the computing complexity of the system.

【Key words】 access control; ciphertext policy Attribute-Based Encryption (ABE); multiple authorization centers; fine-grained attribute-level revocation; user revocation
DOI: 10. 19678/j. issn. 1000-3428. 0058105

0 概述

近年来,大数据技术发展迅速,对社会生活的影响与日俱增。但大数据技术在带来诸多便利的同时,也暴露出诸多安全隐私问题,目前解决该问题的关键是安全高效的数据加/解密。对此,文献[1]提出了属性基加密(Attribute Based Encryption,ABE)方案,其中心思想是系统根据用户的角色或身份,给其分配不同的一

基金项目: 国家自然科学基金(61662056)。
作者简介: 王静宇(1976—),男,教授、博士,主研方向为信息安全、大数据访问控制;周雪娟,硕士研究生。
收稿日期: 2020-04-17 **修回日期:** 2020-06-22 **E-mail:** 13734728816@126.com

组属性集从而保证用户拥有不同的访问权限。根据访问策略所在位置的不同,属性基加密方案可分为密钥策略属性基加密(KP-ABE)[2]和密文策略属性基加密(CP-ABE)[3]。属性的频繁撤销不仅会导致系统计算负担过重,而且会引起数据安全问题。如何应对大数据访问控制中属性撤销带来的负面影响成为当下最受关注的研究热点之一。

在CP-ABE方案中,密文与特定的访问策略相关联,用户私钥则与一组属性有关,即数据拥有者可以任意指定哪些数据可被哪些特定的用户查看。比起KP-ABE系统,CP-ABE则更适合处理生活中大部分的数据安全问题。该方案最早由文献[3]提出,但是缺少属性撤销功能。文献[4-5]提出给每个属性加上一个有效期,由授权中心定期更新属性的最新版本,但该方案缺乏实时更新性,系统安全性较低。文献[6]提出利用非完全可信的第三方服务器进行用户属性撤销,但是要求第三方服务器时刻在线,因此撤销不够灵活且对系统要求过高。文献[7]提出了一种支持属性直接撤销的方案,该方案无法抵抗合谋攻击,安全性较低。文献[8-10]提出的方案均为用户级撤销,缺乏细粒度的属性级撤销。文献[11]提出一种使用单一授权机构管理所有用户属性、并为所有用户颁发解密密文的密钥,虽有第三方服务器帮助进行加解密操作,但是单一的授权中心容易降低系统安全性与运行效率。文献[12]提出了首个多权限访问控制系统,但是该系统的中央授权机构拥有的主密钥能够解密所有密文,削弱了系统的安全性,同时撤销问题仍未得到解决。文献[13-14]提出使用多个授权机构产生用户秘钥,解决了秘钥托管和属性撤销问题,但仍然没有解决系统计算量过大的缺陷。

针对上述问题,本文借鉴文献[15]提出的属性撤销思想,在改进文献[16]中算法的基础上,提出一种灵活的属性撤销方案,采用安全两方计算协议以及多个属性授权中心进行细粒度属性撤销、密钥托管以及用户级撤销,以提高系统安全性能及属性撤销效率。

1 预备知识

1.1 双线性映射

定义1 映射 $e: G_0 \times G_0 \to G_1$,其中 G_0 和 G_1 是阶为 q 的乘法循环群。g 为乘法循环群的生成元。满足以下性质:

1)双线性:$\forall g \in G_0, \forall a,b \in \mathbb{Z}_p^*$ 有 $e(g^a \cdot g^b)=e(g^b \cdot g^a)=e(g \cdot g)^{ab}$。

2)非退化性:$\exists g \in G_0$,使 $e(g \cdot g) \neq 1$。

3)可计算性:存在有效的方法计算 $e(g \cdot g)$。

1.2 访问结构

定义2 设由系统中所有属性组成的集合为 P,且 $P=\{P_1,P_2,\cdots,P_n\}$,同时访问结构 $A \in 2^{(P_1,P_2,\cdots,P_n)}/\{\varphi\}$ 意为包含在 P 中的非空集合。若 A 是单调的访问结构,当 $\forall B$,且 $B \in A, B \subseteq C$ 时,则 $C \in A$。

1.3 Shamir秘密共享方案

定义3 Shamir提出采用拉格朗日多项式插值的门限秘密共享方案。该方案将秘密 s 无规律分成 k 份,其中任意不少于 $t(1 \leqslant t \leqslant k)$ 份可以通过拉格朗日插值重构出 s,但任意少于 $t-1$ 份的分割数据都不能重构出 s。同时,为每个分割出来的秘密分配节点 $(x_1,y_1),(x_2,y_2),\cdots,(x_k,y_k)$,则其中 t 个节点可以确定出唯一的由秘密共享中心生成阶为 $t-1$ 的多项式 $y=f(x)$。

1)秘密分割

(1)秘密分享中心分发一组被分割的秘密 s 给每一位参与者 $q_i(1 \leqslant i \leqslant t)$,且随机选择 $k-1$ 个系数 $a_1,a_2,\cdots,a_{k-1}$,定义随机多项式 $f(x)=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+\cdots+a_1x+a_0$。

(2)随机选择 t 个非零且不重叠的元素 $x_1,x_2,\cdots,x_t$,且公开 x_i,得出 $y_i=f(x_i)(1 \leqslant i \leqslant t)$,因此有 t 个 (x_i,y_i),但保留 y_i。

2)秘密重构

采用拉格朗日重构的思想,将 t 个参加者所拥有的多项式节点 $(x_i,y_i)(1 \leqslant i \leqslant t)$ 作为输入,输出多项式 $f(x)=\sum_{m=1}^{t} y_m g_m(x)$,其中 $g_m(x)=\prod_{m=1,m\neq n}^{t} \frac{x-x_m}{x_n-x_m}$,$f(0)=a_0=s$,即可重构秘密 s。

1.4 安全两方计算协议

定义4[17] 在一个安全系数普遍较低的分布式网络环境中,参与者A与B在协同计算后得到某函数 $p(x_1,x_2)$ 的值,其中 x_1 和 x_2 分别是两个参与者的秘值。最终参与者A与B均可根据协议得到自己预期的结果值,但是不知道除自身外的任何信息,亦不能根据中间信息推导出其他信息,该协议保证了参与者个人隐私以及系统的安全。

2 算法定义及安全模型

本文方案主要由5类实体构成,分别为:数据拥有者(Data Owner,DO),云存储服务器(Cloud Service Provider,CSP),密钥生成中心(Key Generation Center,KGC),属性授权中心(Attribute Authorization Center,AAC),数据使用者(Data User,DU)。

2.1 算法定义

本文算法由以下几个主要函数构成:

1)Setup():KGC利用安全参数初始化运算获得系统的公钥PK,私钥SK。CSP产生DU的各种参数值。

2)Data Encrypt(PK,m,T):DO使用公钥PK、明文信息 m,以及访问控制策略 T 进行数据加密,生成密文CT并将其发送给CSP。

3)Data KeyGen(PK,MK,ϕ_u,U_{ij}):首先,多个 AAC_i 计算生成 U_{ij},并将最后结果发给CSP,之后,CSP与KGC使用安全两方计算协议计算后生成用户私钥 SK_u。

4）Data Decrypt（SK_u，CT）：合法用户DU使用自己私钥SK_u解密密文CT，当所拥有的一组属性集$\phi_u \in T$时，即可解出明文m。

5）Revocation（）：此阶段进行用户级撤销和属性级撤销。删除DU的参数进行用户级撤销。更改属性版本秘钥以及用户秘钥进行属性级撤销。

2.2　安全性假设

下面给出支持撤销的CP-ABE方案在选择明文攻击（Indistinguishablity under Chosen Plaintext Attack，IND-CPA）下的安全模型，以及攻击者A与挑战者B之间的攻击游戏流程。

准备阶段：攻击者A向挑战者B挑战访问控制策略T^*以及用户撤销列表R_x。

初始化：挑战者B运行Setup（），输出主密钥MK，公钥PK，且发送PK给攻击者A，留存MK。

阶段1：攻击者A随机指定一组属性集$\phi_u^* \notin T^*$，接下来向挑战者B请求相对应的解密私钥$SK_{\phi_u^*}^*$。挑战者B运行KeyGen（PK，MK，ϕ_u，U_{ij}）算法，输入ϕ_u^*，输出属性版本秘钥$U_{\phi_u^*}'$以及解密私钥$SK_{\phi_u^*}^*$，并将其发送给攻击者A。

挑战：攻击者A向挑战者B提交两个等长的消息m_a，m_b。B随机选取$P \in \{a,b\}$，并运行KeyGen（PK，MK，ϕ_u，U_{ij}）算法，将得到的密文$CT_{\phi_u^*}^*$返回给攻击者A。

阶段2：同阶段1，A继续向B发送询问报文。

猜测：A猜测数值p^*，若$p^* \in \{a,b\}$且$p^* = p$，则敌手赢。同时A获得游戏成功的优势定义为：

$$\mathrm{Adv}_{\mathrm{IND-CPA}}(A) = \left| \Pr\left[p^* - p\right] - 1/2 \right| \quad (1)$$

若在某个概率多项时间内敌手赢得游戏的优势可以被忽略，则称本文方案满足IND-CPA安全。

3　方案概述

本文方案在CP-ABE的基础上，结合安全两方计算协议与多属性授权中心，解决用户级撤销及属性级撤销。方案流程如图1所示。

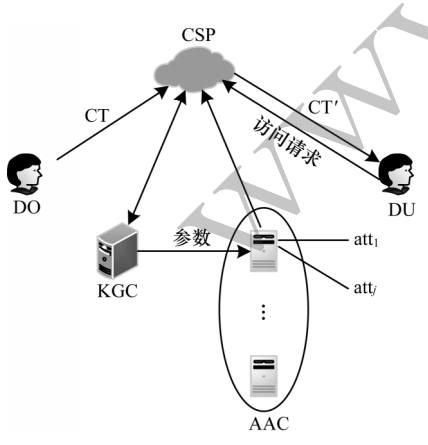

图1　支持属性撤销的CP-ABE方案流程

Fig.1　CP-ABE solution process that supports attribute revocation

方案具体步骤如下：

1）用户秘钥生成。各个属性授权中心生成对应属性的属性版本秘钥U_{ij}，并将其交由CSP，CSP与KGC用各自的参数进行安全两方计算，将生成的结果交由DU，DU即可得到自身用户秘钥SK_u。

2）属性级撤销。KGC将随机选取的重加密参数Φ发送给除DO外的各个实体，以此来更新各自实体的相关参数。每个AAC_i更新和被撤销属性相关的属性版本秘钥U_{ij}，CSP更新和被撤销属性相关的密文CT，KGC与CSP进行安全两方计算，更新与被撤销属性相关的用户的秘钥SK_u。

3）用户级撤销。CSP给每一位合法用户DU分配唯一身份值UID_i及唯一秘值r_t。并将其存入用户列表R_x中，若进行用户级撤销时，CSP将用户的身份值移出用户列表，并删除唯一秘值，该用户将不能再访问加密数据。

该方案包含的主要函数如下：

1）Setup（）

$H:\{0,1\}^* \to G_1$是一个哈希函数，用来将字符串属性映射到G_1的随机元素上。CSP随机选择$\beta \in \mathbb{Z}_p^*$，设$h = g^\beta$，则CSP的公钥$\mathrm{pk}_c = h$，私钥为$\mathrm{mk}_c = \beta$。密钥生成中心KGC随机选择$\alpha \in Z_p^*$，则KGC的公钥为$\mathrm{pk}_k = e(g,g)^\alpha$，私钥为$\mathrm{mk}_k = g^\alpha$。则系统公钥$\mathrm{PK} = \{G_1, g, h = g^\beta, e(g,g)^\alpha\}$，主密钥为$\mathrm{MK} = \{\alpha, \beta\}$。

CSP为每个用户分配唯一身份值UID_i，并添加进用户列表R_x中，根据其身份或者角色分配一组属性集ϕ_u，以及唯一随机秘值$r_t \in \mathbb{Z}_P^*$。KGC为每个AAC_i分配唯一随机值$V_i \in \mathbb{Z}_p^*$。

2）Data Encrypt（PK，m，T）

该算法由DO操作，首先，使用访问结构和访问树表示DO制定的访问控制策略，访问结构中的属性作为叶子节点，门限逻辑运算符作为中间节点，且树的根节点为R，以此来构建访问控制树T。该算法采用自上而下的方式从根节点R开始为树T中所有节点x（包括非叶子节点和叶子节点）产生一个阶为d_x的多项式q_x，n_x为非叶子节点阈值，且多项式的阶d_x和节点阈值n_x之间的关系为$d_x = n_x - 1$。随机选取$s \in \mathbb{Z}_p^*$，设置根节点多项式为$q_R(0) = s$，同时计算$\tilde{C} = m \cdot e(g,g)^{\alpha s}$，$C = \mathrm{h}^s$。针对其它节点，设置多项式为$q_x(0) = q_{p(x)}(\mathrm{index}(x))$，$\mathrm{index}(x)$的值表示其父节点$p(x)$的第$\mathrm{index}(x)$个左孩子节点。

在树T中，设J为所有和叶子节点相联系的属性的集合，计算每个叶子节点$j \in \mathrm{J}$所对应的$C_j = g^{q_j(0)}$和$C_j^* = H(j^{q_j(0)})$。密文CT则为：

$$\mathrm{CT} = \{T, \tilde{C} = m \cdot e(g,g)^{\alpha s}, C = h^s, \forall j \in \mathrm{J}: C_j = g^{q_j(0)}, C_j^* = H(j)^{q_j(0)}\} \quad (2)$$

3）Data KeyGen（PK，MK，ϕ_u，U_{ij}）

（1）属性版本密钥生成

该算法由AAC运行。每个AAC_i管理若干个不同属性，每个属性仅由一个AAC_i管理。每个AAC_i给其所管理的每个属性各随机选取任意值$V_{ij}^* \in \mathbb{Z}_p^*$，故属性版本密钥为$U_{ij}=V_i/V_{ij}^*$。并将其发送给CSP。

（2）用户密钥生成

该算法由CSP和KGC同时运行得出。CSP将参数（r_t，β）作为输入，KGC将参数α作为输入，CSP与KGC二者之间进行安全两方计算协议[17]，输出$x=(\alpha+r_t)\beta$，将计算结果发送给KGC[18]。KGC随机选择$\tau \in \mathbb{Z}_p^*$，将计算的结果$A=g^{x\tau}=g^{(\alpha+r_t)\beta\tau}$发送给CSP。当CSP接收到$g^{(\alpha+r_t)\beta\tau}$后，计算$B=A^{1/\beta^2}=g^{(\alpha+r_t)\tau/\beta}$，之后将$B$发送给KGC。

KGC在接收到B后，计算用户的部分密钥$SK_k=B^{1/\tau}=g^{(\alpha+r_t)/\beta}$。CSP将用户的一组属性集$\phi_u$以及属性版本密钥作为输入，输出用户部分私钥：

$$SK_c=(\forall\ j\in J, D_j=g^{r_t}\cdot H(j)^{U_{ij}}, D_j^*=g^{U_{ij}}) \tag{3}$$

用户分别接收到来自KGC和CSP的部分密钥后，合并生成用户自己的用户密钥：

$$SK_U=(SK_C,SK_K)=(D=g^{(\alpha+r_t)/\beta}, \forall j\in J:$$
$$D_j=g^{r_t}\cdot H(j)^{U_{ij}}, D_j^*=g^{U_{ij}}) \tag{4}$$

4）Data Decrypt（SK_u，CT）

该算法由DU执行，当用户获得加密数据后，采用递归的算法对数据进行解密。过程如下：

（1）若j为访问控制树T的叶子节点，用户的一组实体属性集$\phi_u \in T$，且$\phi_{ui}\in\phi_u$时，解密公式如下：

$$\text{DecryptNode}(CT,SK_u,x)=\frac{e(D_j,C_j)}{e(D_j^*,C_j^*)}=$$
$$\frac{e\left(g^{r_t}\cdot H(j)^{U_{ij}},g^{q_j(0)}\right)}{e\left(g^{U_{ij}},H(j)^{q_j(0)}\right)}=\frac{e\left(g^{r_t},g^{q_j(0)}\right)\cdot e\left(H(j)^{U_{ij}},g^{q_j(0)}\right)}{e\left(g^{q_j(0)},H(j)^{U_{ij}}\right)}=$$
$$e\left(g^{r_t},g^{q_j(0)}\right)=e(g,g)^{r_t q_j(0)} \tag{5}$$

当$\phi_{ui}\notin\phi_u$，则为⊥。

（2）若j为访问控制树T的非叶子节点，设$\mathbb{Z}_x$为大小为k_x的每个节点z的孩子节点集合，当$F_z\neq\perp$，则进行如下递归计算：

$$F_x=\prod_{z\in\mathbb{Z}_x}F_z^{\Delta_{i,\mathbb{Z}_x'}(0)}=\prod_{z\in Z_x}\left(e(g,g)^{r_t q_z(0)}\right)^{\Delta_{i,\mathbb{Z}_x'}(0)}=$$
$$\prod_{z\in Z_x}\left(e(g,g)^{r_t q_{(\text{parent}(z))}^{(\text{index}(z))}}\right)^{\Delta_{i,\mathbb{Z}_x'}(0)}=$$
$$\left(e(g,g)^{r_t q_j(i)}\right)^{\Delta_{i,\mathbb{Z}_x'}(0)}=e(g,g)^{r_t q_j(0)} \tag{6}$$

其中$i=\text{index}$，$Z_x'=(\text{index}(z)|z\in\mathbb{Z}_x)$。

当$\phi_u\in T$，则调用访问控制树T的根节点R，并进行如下计算：

$$A=\text{DecryptNode}(CT,SK_u,R)=$$
$$e(g,g)^{r_t q_R(0)}=e(g,g)^{r_t s} \tag{7}$$

（3）当用户属性集$\phi_u\in T$，即$T(\phi_u)=1$，则可解密被加密的数据。

$$\frac{\tilde{C}}{e(C,D)/A}=\frac{m\cdot e(g,g)^{\alpha s}}{e((g^{\beta})^s,g^{(\alpha+r_t)/\beta})/e(g,g)^{r_t s}}=m \tag{8}$$

5）Revocation（）

主要包含以下4个阶段：

（1）用户级撤销

当用户整体从系统中撤销时，CSP将其唯一身份值uid_i从用户列表R_x中删除，并删除唯一秘密值r_t。在该系统中，任意用户均可下载密文，但是只有存在于用户列表中的合法用户才可获得相关秘钥，进一步解密密文。保证了系统的安全性。

（2）属性级撤销

KGC随机选取一个重加密参数Φ，并将其分配给每个AAC_i，CSP，以及和撤销属性相关的用户DU。接收到重加密参数的实体更新其参数，使其保证参数的最新性。

每个AAC_i更新其所管理的对应的撤销属性的秘参$V_{ij'}^*$，则撤销属性更新后的版本密钥为$U_{ij'}=V_i/V_{ij'}^*$

（3）用户密钥更新

AAC_i更新相关的撤销属性的最新版本秘钥，并将结果发送给CSP，随之，CSP与KGC进行安全两方计算得出用户的最新秘钥。最新版本的秘钥为：

$$SK_u=\{D=g^{(\alpha+r_t)/\beta}, D_{j'}=g^{r_t}H(\Phi j)^{U_{ij'}}, D_{j'}^*=g^{U_{ij'}},$$
$$\forall j\in J\backslash\{j'\}: D_j=g^{r_t}H(j)^{U_{ij}}, D_j^*=g^{U_{ij}}\} \tag{9}$$

（4）密文更新

CSP接收到KGC的更新参数后，迅速更新密文的相关组件，确保密文的安全性。

$$CT=\{T,\tilde{C}=m\cdot e(g,g)^{\alpha s}, C=h^s, \forall j\in J:$$
$$C_j'=H(\Phi j)^{q_j(0)}, j=j', C_j'=H(j)^{q_j(0)}, j\neq J,$$
$$C_j=g^{q_j(0)}\} \tag{10}$$

4 安全性证明与性能分析

4.1 多授权模型安全性分析

本方案中多属性授权中心可分为两个模块，即由多个属性授权中心AAC_i联合产生的属性版本密钥，以及云服务器和密钥生成中心联合生成的用户密钥。当撤销某个用户或者某个用户的属性时，任意属性授权中心都无法获得用户的属性版本密钥，且用户密钥是由两个实体通过安全两方协议共同产生，双方均无法获取对方的部分密钥，故无法解密密

文。同理,当合法用户加入到系统中时,属性授权中心会根据用户的一组属性集生成最新的属性版本密钥,因此确保了数据的向前向后安全性。

4.2 抗合谋攻击

证明:在本文的方案中,只有当DU的$\phi_u \in T$,才能计算出$e(g,g)^{\alpha s}$。当有若干个不同权限的用户串谋攻击,由云服务器分配给每个用户一个唯一随机秘值r_t,则产生不同的DU秘钥部分组件$D=g^{(\alpha+r_t)/\beta}$,$D_j=g^{r_t}\cdot H(j)^{u_{ij}}$,故合谋攻击不能获得用户秘钥。本方案可满足抗合谋攻击。

4.3 选择明文攻击

在随机预言机模型下基于DBDH[19](判定双线性Diffie-Hellman问题)困难假设进行安全性证明:

模型生成(g,g^a,g^b,g^c,z),$a,b,c,\theta\in\mathbb{Z}_p^*$,$z=e(g,g)^{\theta}$,计算$e(g,g)^{abc}$,判断是否$z=e(g,g)^{abc}$成立。当且仅当满足如下条件时:

$$\Pr\left[Q\left(g,g^a,g^b,g^c,e\left(g,g\right)^{abc}\right)=1\right]-\Pr\left[Q\left(g,g^a,g^b,g^c,e(g,g)^{\theta}\right)=1\right]\geqslant\varepsilon \tag{11}$$

一个概率多项式时间算法Q以优势为ε求解DBDH问题。

定理1 假设DBDH成立,则敌手就无法在多项式时间内求解DBDH问题,其中可忽略优势ε即可证明该方案的安全性。

准备阶段:敌手A选择访问控制树T^*及用户撤销列表$R_x=\{\mathrm{UID}_1,\mathrm{UID}_2,\cdots,\mathrm{UID}_i\}$。

初始化:B运行Setup()算法。

1)选择随机数$y\in\mathbb{Z}_p^*$,设$e(g,g)^{\alpha}=e(g,g)^{ab}e(g,g)^{y}$,则$\alpha=ab+y$。同时,设公参$e(M,N)=e(g,g)^{ab}$。

2)针对每个属性ϕ'_{ui},随机选取$n_j\in Z_p^*$。当$\phi'_{ui}\notin T'$,设$h=N^{n_j^{-1}}$,则$\beta_j=bn_j^{-1}$。当$\phi'_{ui}\in T'$,设$h=g^{n_j}$,则$\beta_j=n_j$。

3)公钥$\mathrm{PK}=\{G,g,h=g^{\beta},e(g,g)^{\alpha}\}$,主密钥$\mathrm{MK}=\{\alpha,\beta\}$,B将公钥PK发送给敌手A,且自身保留主密钥MK。

阶段1:敌手A选择属性集$\phi=\{\phi_{i^*}\mid\phi_{i^*}\notin T_{i^*}\}$以及$\mathrm{UID}_{i^*}\notin R_x$,并请求相应的私钥。

1)B随机选取r'_t、u'_{ij}。且满足$r_t=br'_t-ab$,$u_{ij}=bu'_{ij}$,则$D=g^{(\alpha+r_t)/\beta}=g^{y+br'_t/\beta}$。

2)对每个属性ϕ_j,都有

$D_j=g^{r_t}\cdot H(j)^{u_{ij}}=g^{-ab}g^{br'_t}H(j)^{bu'_{ij}}$,$D_j^*=g^{u_{ij}}=g^{bu'_{ij}}$ 同时,挑战者将用户秘钥$\mathrm{SK}'_u=(D,D_j,D_j^*)$提交给敌手A。

挑战:敌手A向挑战者B提交两个等长的消息m_a,m_b。B随机选取$P\in\{a,b\}$,并运行KeyGen()算法。

随机选取$s'\in\mathbb{Z}_p^*$,计算

$$\tilde{c}_o=m_p\cdot e(g,g)^{\alpha(s+s')}=m_p\cdot e(g,g)^{(ab+y)(s+s')}=m_p\cdot e(g,g)^{abs}e(g,g)^{abs'}e(g,g)^{ys}e(g,g)^{ys'} \tag{12}$$

$$c_j=g^{q_j(0)} \tag{13}$$

$$c_j^*=H(j)^{q_j(0)} \tag{14}$$

$$c'_j=H(\Phi j)^{q_j(0)} \tag{15}$$

挑战者B将密文$\mathrm{CT}'=(\tilde{c}_o,c_j,c_j^*,c'_j)$发送给敌手A。

阶段2:同阶段1,A继续向B发送秘钥询问报文。

猜测:敌手A输出猜测$p^*\in\{0,1\}$。

1)若$p^*=p$,则$z=e(g,g)^{abc}$,即DBDH成立。表明敌手A可获得有效密文且优势为$\Pr=[p^*=p|z=e(g,g)^{abc}]=1/2+\varepsilon$。

2)若$p^*\neq p$,则表明敌手A无法获得有效的密文,$z=e(g,g)^{\theta}$,其优势为:

$$\Pr=[p^*\neq p\mid z=e(g,g)^{\theta}]=\frac{1}{2}$$

因此$\Pr\left[Q\left(g,g^a,g^b,g^c,e\left(g,g\right)^{abc}\right)=1\right]-\Pr\left[Q(g,g^a,g^b,g^c,e(g,g)^{\theta})=1\right]\geqslant\varepsilon$成立。

综上所述,若没有敌手在多项式时间内选择访问控制树T^*击败该方案,则证明该方案有较高的安全性。

5 效率分析

5.1 功能实现分析比较

本文中提出的方案与其他方案在秘钥托管、抗合谋、撤销机制等方面作出分析比较。从表1中可以得出结论:本文方案在系统安全等功能方面考虑得比较全面,基本问题得到解决。

表1 各方案功能实现分析比较

Table 1 Analysis and comparison of function realization of each scheme

方案	秘钥托管	抗合谋	撤销机制		访问策略
			用户级	属性级	
文献[13]方案	是	是	否	是	访问树
文献[20]方案	是	是	是	是	AND
文献[21]方案	—	—	否	是	LSSS
本文方案	是	是	是	是	访问树

5.2 效率比较

当进行用户级撤销时,仅由CSP将用户唯一身份值UID_i从用户列表R_x中删除,并删除唯一秘密值r_t,故用户级撤销的计算复杂度为$O(1)$。当进行属性级撤销时,被撤销的属性需更新最新的版本秘钥,故属性级撤销所需的计算复杂度为$O(6n)$。

本文方案中采用的安全两方计算协议所需计算

复杂度为$O(5n)$,属性版本秘钥由各个属性授权中心产生,故计算复杂度为$O(n)$,故生成用户秘钥所需计算复杂度为$O(6n)$。

由此可以看出本文方案在解密花费以及撤销花费中,将部分计算任务交由CSP进行,极大地降低了系统计算复杂度。各方案效率的对比结果如表2所示。

表2 效率分析比较

Table 2 Analysis and comparison of efficiency

方案	生成秘钥花费	解密花费		撤销花费	
		CSP	USER	用户级撤销	属性级撤销
文献[20]方案	$3te$	—	$3tp$	np	$3(n+1)p$
本文方案	$O(6n)$	$O(n)$	$O(n)$	$O(1)$	$O(6n)$

在表2中,te为指数运算所需的花费,tp为双线性对运算所需的花费,p为在z_p^*,G_0,G_1中元素的大小。

6 结束语

本文提出一种支持属性撤销的CP-ABE方案,通过安全两方计算协议,生成并更新用户秘钥,从而实现细粒度级的用户级和属性级撤销,同时引进多个属性授权中心,在撤销某用户或某用户属性时,任意属性授权中心都无法获得用户的属性版本密钥。实验结果表明,该方案能有效降低撤销操作的计算复杂度,并增强了系统安全性。未来研究将继续优化细粒度撤销所需的计算开销,以进一步降低系统的计算复杂度。

参考文献

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[M]. Berlin, Germany: Springer, 2005.

[2] 胡海英,商威. 一种可撤销的KP-ABE方案[J]. 计算机系统应用,2013,22(9):123-128.
HU H, SHANG W. One revocable KP-ABE scheme[J]. Computer Systems Applications, 2013, 22(9): 123-128. (in Chinese)

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

[4] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation modes[C]//Proceedings of 2008 ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2008: 417-426.

[5] WAN Z, LIU J, DENG R H. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 743-754.

[6] YU S, WANG C, REN K, 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.

[7] 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.

[8] LEWKO A, SAHAI A, WATERS B. Revocation systems with very small private keys[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2005: 273-285.

[9] YANG L, ZHU J, WANG X, et al. Optimized ciphertext-policy attribute-based encryption with efficient revocation[J]. International Journal of Security & Its Applications, 2013, 7(6): 385-394.

[10] XU Z, MARTIN K M. Dynamic user revocation and key refreshing for attribute-based encryption in cloud storage[C]//Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Washington D. C., USA: IEEE Press, 2012: 844-849.

[11] 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.
LIU Z S, PENG J P. An outsourcing attribute encryption scheme for attribute revocation[J]. Computer Engineering, 2017, 43(10): 109-114. (in Chinese)

[12] CHASE M. Multi-authority attribute based encryption[C]//Proceedings of Theory of Cryptography Conference. Washington D. C., USA: IEEE Press, 2007: 515-534.

[13] HAN K, LI Q, DENG Z. Security and efficiency data sharing scheme for cloud storage[J]. Chaos, Solitons & Fractals, 2016, 86: 107-116.

[14] LI W, XUE K, XUE Y, et al. TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage[J]. IEEE Transactions on Parallel & Distributed Systems, 2016, 27: 1484-1496.

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

[16] YANG K, JIA X, REN K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems[C]//Proceedings of the 8th ACM SIGSAC Symposium on Information. New York, USA: ACM Press, 2013: 523-525.

[17] 唐瑜穗. 卷积隐藏技术下的安全双方计算模型的安全性与复杂性分析[D]. 贵州:贵州大学,2016.
TANG Y S. Analysis on the security and complexity of the secure two-party computation model under convolutional hidden technology[D]. Guizhou: Guizhou University, 2016. (in Chinese)

[18] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//Proceedings of 2009 ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2009: 121-130.

[19] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[EB/OL]. [2020-03-02]. https://crypto. stanford. edu/~dabo/papers/bfibe. pdf.

[20] LI X, TANG S, XU L, et al. Two-factor data access control with efficient revocation for multi-authority cloud storage systems[J]. IEEE Access, 2017, 5: 393-405

[21] LIU Z, JIANG Z, WANG X, et al. Practical attribute-based encryption: outsourcing decryption, attribute revocation and policy updating[J]. Journal of Network & Computer Applications, 2018, 108: 112-123.

编辑 卞颖颖