软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(10):2805−2816 [doi: 10.3724/SP.J.1001.2012.04184]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种支持完全细粒度属性撤销的 CP-ABE 方案*

王鹏翩[1,2+], 冯登国[1], 张立武[1,2]

[1](信息安全国家重点实验室(中国科学院 软件研究所),北京 100190)

[2](信息安全共性技术国家工程中心,北京 100190)

CP-ABE Scheme Supporting Fully Fine-Grained Attribute Revocation

WANG Peng-Pian[1,2+], FENG Deng-Guo[1], ZHANG Li-Wu[1,2]

[1](State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100190, China)

[2](National Engineering Research Center of Information Security, Beijing 100190, China)

+ Corresponding author: E-mail: wangpengpian@is.iscas.ac.cn

Wang PP, Feng DG, Zhang LW. CP-ABE scheme supporting fully fine-grained attribute revocation. *Journal of Software*, 2012,23(10):2805−2816 (in Chinese). http://www.jos.org.cn/1000-9825/4184.htm

Abstract: Attribute revocation is crucial to use of ABE. The existing ABE schemes that support attribute revocation under the direct revocation model can only revoke the whole attributes that the user possesses by revoking the user's identity, so the attribute revocation is coarse-grained. This paper proposes the model of CP-ABE that supports fully fine-grained attribute revocation. Based on the dual encryption system proposed by Waters, a concrete CP-ABE scheme that fully supports fine-grained attribute revocation is constructed over the composite order bilinear groups, and the study proves its security under the standard model. Compared to the existing related schemes, this scheme is much more flexible and can revoke an arbitrary number of attributes that user possesses.
Key words: attribute revocation; direct revocation mode; attribute based encryption; cipher policy

摘 要: 属性撤销是基于属性的加密(attribute based encryption,简称 ABE)在实际应用中所必须解决的问题.在直接撤销模式下,已有的支持属性撤销的 ABE 方案只能以撤销用户身份的方式对用户所拥有的全部属性进行撤销,而无法做到针对属性的细粒度撤销.提出了直接模式下支持完全细粒度属性撤销的 CP-ABE(cipher policy ABE)模型,在合数阶双线性群上,基于双系统加密的思想构造了具体的方案,并在标准模型下给出了严格的安全性证明.该方案能够对用户所拥有的任意数量的属性进行撤销,解决了已有方案中属性撤销粒度过粗的问题.
关键词: 属性撤销;直接撤销模式;基于属性的加密;密文策略
中图法分类号: TP309 **文献标识码**: A

基于属性的加密(attribute based encryption,简称 ABE)最早由 Sahai 等人提出[1],由于 ABE 具有内在的"一对多"的良好性质,因此能够对密文进行细粒度的访问控制.已有的 ABE 方案根据解密策略绑定的位置大致可以分为两类:一类是 KP(key policy)-ABE 方案[2−5],即将解密策略与用户私钥绑定;一类是 CP(cipher policy)-ABE 方

* 基金项目: 国家自然科学基金(60803129); 下一代互联网商用及设备产业化专项资金(CNGI-09-03-03); 信息网络安全公安部重点实验室(公安部第三研究所)开放基金(C11604)

收稿时间: 2011-09-15; 修改时间: 2011-11-17; 定稿时间: 2012-01-17

案[3−7],即将解密策略与密文绑定.

在实际应用中,属性的撤销是 ABE 所必须解决的问题,也是 ABE 研究的一个难点[8].目前,大多数的 ABE 方案主要关注于如何支持表述能力更为丰富的解密策略,而没有特别地考虑属性撤销问题.Attrapadung 等人[4,5]通过将 ABE 与组播加密相结合,首次明确提出了 ABE 的两种撤销模式,即间接撤销模式和直接撤销模式:在间接撤销模式下,需要通过影响用户的私钥来完成属性的撤销,例如引入可信第三方[9]以及周期性更新用户的私钥[10].间接撤销模式虽然撤销较为灵活,但其撤销代价较大,也容易形成系统瓶颈,目前支持属性撤销的 ABE 方案多数都是通过间接撤销模式完成的;在直接撤销模式下,发送方通过将撤销列表嵌入到密文中来完成对用户属性的撤销,因此能够在不更新任何一个用户私钥的情况下完成撤销,撤销代价相对较小.Attrapadung 等人以 Waters 等人[11]所提出的基于身份的支持用户撤销的组播加密方案为基础,构造了支持以直接撤销模式对用户属性进行撤销的 ABE 方案.除直接撤销模式和间接撤销模式外,Yu 等人[12]基于代理重加密技术,提出了一个特殊的通过同时改变系统公钥和用户私钥的方式来完成撤销的 CP-ABE 方案,但其撤销代价也较大,且其本质上也属于间接撤销模式.

需要注意的是,Attrapadung 等人的方案实际上只能够对用户的身份进行撤销,即对用户所拥有的全部属性进行撤销,而无法做到细粒度地对用户的某一个属性单独进行撤销,撤销粒度较粗.Hur 等人[13]在 Bethencourt 等人方案[6]的基础上,基于用户二叉树提出了一个支持完全细粒度属性撤销的 CP-ABE 方案.虽然该方案是以直接模式进行撤销,但该方案本质上已经偏离了 ABE 的概念,且该方案并未进行严格的安全模型定义以及安全性证明,存在着灵活性差、密钥维护代价高、无法抗合谋攻击等缺点,借鉴意义有限.在我们之前的工作中[14],通过为每一个用户分配两个分享不同秘密值的访问树,实现了直接撤销模式下支持细粒度属性撤销的 KP-ABE 方案,但该方案只支持在密文中嵌入一个属性的用户撤销列表,属性的撤销粒度仍然较粗.

本文针对已有支持属性撤销 ABE 方案的不足,提出了直接撤销模式下支持完全细粒度属性撤销的 CP-ABE 模型.即在密文中可以嵌入任意多个属性的用户撤销列表,并给出了严格的安全性定义.最后,基于 Waters 等人[15]所提出的双系统加密的思想,并借鉴 Lewko 等人[16]的基于合数阶双线性群构造的适应性安全 ABE 方案,通过采用 Attrapadung 等人方案中的第一种撤销方式,给出了一个具体的支持完全细粒度属性撤销 CP-ABE 构造方案以及相应的安全性证明.

1 预备知识

1.1 访问结构

定义 1[17]. 令 $P=\{P_1,P_2,...,P_n\}$是参与方的集合,一个访问结构$\mathbb{A}$是 2^P 的一个非空子集,即$\mathbb{A}\subseteq 2^P\backslash\{\varnothing\}$.若访问结构$\mathbb{A}$是单调的,则有:$\forall B,C$,若 $B\in\mathbb{A}$且 $B\subseteq C$,则有 $C\in\mathbb{A}$.访问结构$\mathbb{A}$中的集合称为授权集合,不在访问结构$\mathbb{A}$中的集合称为非授权集合.

为简化表述,记 $\overline{\mathbb{A}}$ 为访问结构$\mathbb{A}$所涉及的参与方的集合($\mathbb{A}$中所有授权集合的并集),即 $\overline{\mathbb{A}}=\bigcup_{X\in\mathbb{A}} X$.

1.2 线性秘密分享方案

定义 2[17]. 令 $P=\{P_1,P_2,...,P_n\}$是参与方的集合,(A,ρ)代表着一个访问结构$\mathbb{A}$,其中,A 是一个 $l\times k$ 的矩阵;ρ是一个从$\{1,2,...,l\}$到 P 的映射,即将矩阵 A 中的每一行映射到一个参与方.一个线性秘密分享方案(linear secret sharing schemes,简称 LSSS)包含两种有效的算法:

- **秘密分享算法**. 若要分享一个秘密值 s,首先从 Z_p 中随机选取 $k-1$ 个值 $v_1,v_2,...,v_{k-1}$,与 s 组成一个 k 维的向量 $\vec{v}=(s,v_1,v_2,...,v_{k-1})$.令 $\overrightarrow{A_i}$ 为矩阵 A 第 i 行所代表的向量,然后将 $\sigma_i=\overrightarrow{A_i}\cdot\vec{v}$ 作为参与方$\rho(i)$所获得的秘密分享值.
- **秘密恢复算法**. 若一个参与方的集合$\omega\in\mathbb{A}$,令 $L=\{i|\rho(i)\in\omega\}$,则可以根据 A 有效地计算出一组恢复系

数$\{\mu_i\}_{i\in L}$,使得$\sum_{i\in L}\mu_i\cdot\sigma_i=s$.

1.3 合数阶群上的双线性映射

定义 3[15]. 令 $N=p_1p_2p_3$(p_1,p_2,p_3为素数且两两不同),G,G_T是N阶循环群,g为G的一个生成元,e是$G\times G\to G_T$的一个映射,若e满足以下 3 个性质,则称e是一个有效的从G到G_T的双线性映射:

(1) 双线性:$\forall a,b\in Z_N, e(g^a,g^b)=e(g,g)^{ab}$;

(2) 非退化性:$\exists g\in G$,使得$e(g,g)$的阶为N;

(3) 可计算性:$\forall u,v\in G, e(u,v)$都是可以有效计算的.

需要注意的是,合数阶群上的双线性映射具有如下性质:令G_{p_1},G_{p_2},G_{p_3}分别代表群G中阶为p_1,p_2,p_3的子群,设$h_i\in G_{p_i}, h_j\in G_{p_j}$,若$i\neq j$,则有$e(h_i,h_j)=1$.

1.4 困难性假设

定理 1[18]. 令 $N=p_1,p_2,\ldots,p_m$为两两不同的素数,且任意$i\in\{1,2,\ldots,m\}$,有$p_i>2^\lambda$.令$N=\prod_{i=1}^{m}p_i$, G,G_T是N阶循环群,e是$G\times G\to G_T$的一个双线性映射,$\{A_i\}$为群G上的一组随机变量,$\{B_i\},T_0,T_1$为群G_T上的一组随机变量,且这些随机变量的阶都不超过t.在一般群模型下考虑如下实验:

将$(N,G,G_T,e,\{A_i\},\{B_i\})$给定一个算法$\mathcal{A}$,然后从$T_0,T_1$中随机选择一个元素$T_b$返回给算法$\mathcal{A}$.算法$\mathcal{A}$输出对$b$的猜测$b'$.定义算法$\mathcal{A}$的猜测优势为$|\Pr[b'=b]-1/2|$.

若T_0,T_1独立于$\{B_i\}\cup\{e(A_i,A_j)\}$,则如果$\mathcal{A}$在上述的一般群模型下的实验中最多只进行了$q$次操作,并具有$\delta$的攻击优势,则可以构造一个算法$\mathcal{B}$,以至少$\delta-O(q^2t/2^\lambda)$的概率分解$N$.

本节中,下面 3 个假设都基于定理 1 进行证明,其中,假设 1 和假设 2 的证明见文献[19].

假设 1[19]. 令 $N=p_1p_2p_3$(p_1,p_2,p_3为素数且两两不同),G,G_T是N阶循环群,e是$G\times G\to G_T$的一个双线性映射.从G_{p_1}中随机选取一个生成元g,从G_{p_3}中随机选取一个生成元Y.给定(N,G,G_T,e,g,Y),若不存在一种算法能够在多项式时间内区分G_{p_1}与$G_{p_1p_2}$上的元素,则该假设成立.

假设 2[19]. 令 $N=p_1p_2p_3$(p_1,p_2,p_3为素数且两两不同),G,G_T是N阶循环群,e是$G\times G\to G_T$的一个双线性映射.首先从G_{p_1}中随机选取一个生成元g,从G_{p_2}中随机选取一个生成元X,从G_{p_3}中随机选取一个生成元Y,然后从Z_N中随机选择 4 个元素s,c_1,c_2,d.给定$(N,G,G_T,e,g,g^sX^{c_1},Y,X^{c_2}Y^d)$,若不存在一种算法能够在多项式时间内区分$G$与$G_{p_1p_3}$上的元素,则该假设成立.

假设 3. 令 $N=p_1p_2p_3$(p_1,p_2,p_3为素数且两两不同),G,G_T是N阶循环群,e是$G\times G\to G_T$的一个双线性映射.首先从G_{p_1}中随机选取一个生成元g,从G_{p_2}中随机选取一个生成元X,从G_{p_3}中随机选取一个生成元Y,然后从Z_N中随机选择 4 个元素s,c_1,c_2,α.给定$(g,X,Y,g^sX^{c_1},\{g_i=g^{\alpha^i}\}_{i\in\{1,2,\ldots,n,n+2,\ldots,2n\}},g^{\alpha^{n+1}}X^{c_2},T)$,若不存在一种算法能够在多项式时间内区分$e(g,g)^{\alpha^{n+1}\cdot s}$与$G_T$上的一个随机元素,则该假设成立.

证明:利用定理 1 对该假设进行证明(其中的符号表示见文献[18]).令$X_1=X^{c_1}, X_2=X^{c_2}$,则假设 3 可以表述为如下形式:

$$
\begin{aligned}
&A_1=(1,0,0), A_2=(0,1,0), A_3=(0,0,1),\\
&A_4=(S,C_1,0), A_5=(B,0,0), A_6=(B^2,0,0),\ldots.,\\
&A_{n+4}=(B^n,0,0), A_{n+6}=(B^{n+2},0,0),\ldots,\\
&A_{2n+4}=(B^{2n},0,0), A_{2n+5}=(B^{n+1},C_2,0),\\
&T_0=[B^{n+1}S,0,0],\\
&T_1=[Z_1,Z_2,Z_3].
\end{aligned}
$$

对于T_1:由于T_1是从群G_T上随机选取的一个元素,Z_1,Z_2,Z_3不在任何一个A_i中出现,因此T_1独立于$\{e(A_i,A_j)\}$.

对于 T_0:注意到其中的第 1 个分量 $B^{n+1}S$ 只能通过 $e(A_4,A_{2n+5})$得到,但计算 $e(A_4,A_{2n+5})$的同时会得到第 2 个分量 $e(X_1,X_2)$,由于 X_1,X_2 不在除 A_4,A_{2n+5} 之外的任何一个 A_i 中出现,因此 $e(X_1,X_2)$的值无法计算.由此可知,T_0 也独立于$\{e(A_i,A_j)\}$.

根据定理 1,由于 T_0,T_1 独立于$\{B_i\}\cup\{e(A_i,A_j)\}$,因此,若 N 的分解是困难的,则该假设在一般群模型下是安全的.

假设 3 证毕. □

1.5 双系统加密

为了使 IBE 达到适应性安全,Waters 等人[16]提出了双系统加密的概念,其核心思想是:首先引入一些攻击游戏,通过适当地构造半功能密钥以及半功能密文,使得真实的攻击游戏与这些攻击游戏不可区分;然后,在最终的攻击游戏中通过对一条随机消息进行加密,使得敌手不具有任何攻击优势.双系统加密是实现适应性安全的一条有效途径,在 Waters 等人思想的基础上,Lewko 等人[19]基于合数阶双线性群构造了适应性安全的 ABE 方案.随后,Lewko 与 Waters[20]基于双系统加密给出了一个选择性安全的非中心式 CP-ABE 方案.双系统加密并没有一个严格而通用的形式化表述,本节我们只给出双系统加密的一些基本性质:

- 半功能密钥可以对正常的密文进行解密;
- 正常的密钥可以对半功能密文进行解密;
- 半功能密钥不能对半功能密文进行解密.

具体的构造以及说明将在第 3 节中加以阐述.

2 模型定义

2.1 方案模型

一个支持完全细粒度属性撤销的 CP-ABE 方案由 4 种多项式时间算法(*Setup*,*KeyGen*,*Encrypt*,*Decrypt*)组成:

- $Setup(1^\lambda,m,n)\rightarrow(MSK,PK)$:输入安全参数 1^λ、属性的数量 m、用户的数量 n;输出系统公钥 PK 和主私钥 MSK.其中,PK 隐含了系统的属性集合 $I=\{1,2,...,m\}$和用户身份集合 $U=\{1,2,...,n\}$;
- $KeyGen(ID,\omega,MSK,PK)\rightarrow SK_{ID,\omega}$:输入一个属性集合$\omega\subseteq I$、用户的标识 $ID\in U$ 以及主私钥 MSK 和公钥 PK;输出用户 ID 关于属性集合ω的私钥 $SK_{ID,\omega}$;
- $Encrypt(M,\mathbb{A},\{R_i\}_{i\in\bar{\mathbb{A}}},PK)\rightarrow C$:输入明文 M、访问结构$\mathbb{A}$和其中所涉及的每一个属性 i 的用户撤销列表 $R_i\subseteq U$,以及系统的公钥 PK;输出为密文 C.其中,C 包含了访问结构$\mathbb{A}$和其中每一个属性的用户撤销列表 $\{R_i\}_{i\in\bar{\mathbb{A}}}$;
- $Decrypt(SK_{ID,\omega},C,PK)\rightarrow M$:输入用户私钥 $SK_{ID,\omega}$、密文 C、系统公钥 PK.令 $\omega'=\{i\mid i\in\omega\cap\bar{\mathbb{A}},ID\notin R_i\}$,即 ω'为用户 ID 所拥有的与访问结构$\mathbb{A}$相关的未被撤销的属性集合,若ω'满足访问结构$\mathbb{A}$,则输出明文 M.

2.2 安全模型

通过一个攻击游戏来定义支持完全细粒度属性撤销的 CP-ABE 方案的安全模型.

- Init:敌手选择一个挑战的访问结构$\mathbb{A}^*$,并对其所涉及的任一属性 i,指定该属性的用户撤销列表 R_i^*;
- Setup:挑战者运行 CP-ABE 方案的 Setup 算法,并将系统公钥 PK 返回给敌手;
- Phase 1:敌手可以询问用户 ID 关于属性集合ω的私钥,但要求 $\omega'=\{i\mid i\in\omega\cap\overline{\mathbb{A}^*},ID\notin R_i^*\}$ 不能满足访问结构$\mathbb{A}^*$,即敌手所询问的私钥不能直接成功解密最终的询问密文.最后,挑战者将 $SK_{ID,\omega}$返回给敌手;
- Challenge:敌手选择两条长度相等的明文 M_0,M_1.挑战者从 M_0 和 M_1 中随机选择一条明文 M_θ进行加

密,并将最终计算出的询问密文返回给敌手;

- Phase 2:与 Phase 1 相同,敌手继续提交用户私钥的询问;
- Guess:敌手输出对θ的猜测θ'.若$\theta'=\theta$,则敌手获胜;

定义敌手的攻击优势 Adv 为 $\Pr[\theta'=\theta]-1/2$.

定义 4(安全性定义). 一个支持完全细粒度属性撤销的 CP-ABE 方案是安全的,当且仅当对于上述的攻击游戏,任何多项式时间的敌手的攻击优势是可忽略的.

3 具体方案

3.1 基本思想

在我们的构造方案中,如果在加密一条明文时使用了属性 i,那么如果用户 ID 拥有属性 i 所对应的私钥 SK_i 且 ID 不在属性 i 的用户撤销列表 R_i 中,则可以计算出与属性 i 相关且与该 ID 的私钥绑定的一个解密信息片段.当且仅当用户所拥有的未被撤销的属性满足密文的访问结构时,用户才能使用这些与其私钥绑定的解密信息片段恢复出明文.

本文方案借鉴了 Attrapadung 等人[4]方案中的用户撤销方法,基于 LSSS 来实现.相比较已有的基于素数阶群实现的 CP-ABE 方案,我们的方案主要有两点不同:一是加密时,与属性相关的秘密分享值不直接作用于属性上,而是作用在与该属性相关的用户撤销列表信息上;二是出于安全性证明的考虑,我们的方案工作在合数阶双线性群上,其安全性证明也依赖于双系统加密的安全性证明框架.

需要说明的是,我们的方案与已有的基于合数阶双线性群实现的 ABE 方案一样,虽然方案基于合数阶双线性群构造,但方案本身实际工作在 G_{p_1} 子群上,G_{p_3} 子群只是用于对密钥的随机化,而 G_{p_2} 子群只是用于安全性证明中半功能密钥以及半功能密文的构造,在实际的构造方案中并不使用.

3.2 具体实现

令 $N=p_1p_2p_3$(p_1,p_2,p_3 为素数且两两不同),G,G_T 是阶为 N 的群,e 是 $G\times G\to G_T$ 的一个双线性映射.令 G_{p_1} 为 G 中阶为 p_1 的子群,g 为 G_{p_1} 的生成元;令 G_{p_3} 为 G 中阶为 p_3 的子群,Y 为 G_{p_3} 的生成元.

$Setup(m,n)$:令属性集合 $I=\{1,2,...,m\}$,用户集合 $U=\{1,2,...,n\}$.首先,对于任意属性 $i\in I$,从 Z_N 中随机选取两个元素 t_i,γ_i,计算 $T_i=g^{t_i}$,$h_i=g^{\gamma_i}$;其次,从 Z_N 中随机选取一个元素 α,对于任意 $i\in\{1,2,...,n,n+2,...,2n\}$,计算 $g_i=g^{(\alpha^i)}$;最后,从 Z_N 中随机选取一个元素 a,并最终发布公钥参数 PK 为

$$PK=(N,g,g^a,\{T_i\}_{i\in I},\{h_i\}_{i\in I},\{g_i\}_{i\in\{1,2,...,n,n+2,...,2n\}}).$$

系统主私钥 MSK 为

$$MSK=(\alpha,a,\{t_i,\gamma_i\}_{i\in U},Y),$$

其中,t_i,T_i 用于与属性本身相关的计算,γ_i,h_i 用于与用户属性撤销相关的计算,α,g_i 用于与用户身份信息相关的计算,Y 用于对用户的私钥进行随机化.

$KeyGen(ID,\omega,MSK,PK)$:用户 $ID\in U,\omega\subseteq I$.首先,从 Z_N 中随机选取一个元素 t,从 G_{p_3} 中随机选取一个元素 Y_0,计算 $K_0=g^tY_0$;然后,对于任意 $i\in\omega$,从 Z_N 中随机选取一个元素 r_i,从 G_{p_3} 中随机选取两个元素 $Y_{i,1},Y_{i,2}$,计算:

$$K_{i,1}=g^{a\cdot t+\alpha^{ID}\gamma_i+t_ir_i}Y_{i,1},$$

$$K_{i,2}=g^{r_i}Y_{i,2}.$$

易见,用户私钥中所有与属性相关的部分(即每一个属性所对应的 $K_{i,1}$ 部分)都嵌入了其身份信息,$K_{i,1}$ 将属性 i 与用户 ID 相绑定.

令 $K_i=(K_{i,1},K_{i,2})$,则最终生成的用户私钥 $SK_{ID,\omega}$ 为

$$SK_{ID,\omega}=(K_0,\{K_i\}_{i\in\omega}).$$

$Encrypt(M,(A_{l\times k},\rho),\{R_{\rho(x)}\}_{x\in\{1,2,...,l\}},PK)$:首先,从 Z_N^k 中随机选取一个向量 $\vec{v}=(s,v_2,v_3,...,v_k)$,并计算:

$$C_0=M\cdot e(g_1,g_n)^s,$$
$$C_1=(g^a)^s.$$

对于 A 中的每一行 x,令 $\overrightarrow{A_x}$ 为 A 的第 x 行所代表的向量, $\lambda_x=\overrightarrow{A_x}\cdot\vec{v}$, $S_{\rho(x)}=U-R_{\rho(x)}$ (设 $S_{\rho(x)}\neq\varnothing$),计算:

$$C_{x,0}=g^{\lambda_x},$$
$$C_{x,1}=T_{\rho(x)}^{\lambda_x}.$$

- 若 $S_{\rho(x)}\neq U$,即 $R_{\rho(x)}\neq\varnothing$:从 Z_N 中随机选取两个元素 η_x,s_x,计算:

$$C_{x,2}=g^{\eta_x}\left(h_{\rho(x)}\prod_{j\in S_{\rho(x)}}g_{n+1-j}\right)^{\lambda_x},$$
$$C_{x,3}=g^{s_x},$$
$$C_{x,4}=g^{\eta_x}\left(\prod_{j\in R_{\rho(x)}}g_{n+1-j}\right)^{s_x},$$

其中,$\eta_x,s_x,C_{x,3},C_{x,4}$ 用于对属性撤销信息 $C_{x,2}$ 的随机化,防止潜在的由于敌手直接计算出与身份信息无关的 $e(g_1,g_n)^{\lambda_x}$ 的值而导致的合谋攻击;

- 若 $S_{\rho(x)}=U$,即 $R_{\rho(x)}=\varnothing$:直接计算:

$$C_{x,2}=\left(h_{\rho(x)}\prod_{j\in S_{\rho(x)}}g_{n+1-j}\right)^{\lambda_x}.$$

为表述统一起见,此时令 $C_{x,3}=C_{x,4}=1$,即 $\eta_x=s_x=0$.

最终的密文 C 为

$$C=(C_0,C_1,\{(C_{x,0},C_{x,1},C_{x,2},C_{x,3},C_{x,4},R_{\rho(x)})\}_{x\in\{1,2,\ldots,l\}}).$$

Decrypt$(SK_{ID,\omega},C,PK)$:首先令 $L=\{x|\rho(x)\in\omega,ID\notin R_{\rho(x)}\}$,则 $\omega'=\{\rho(x)\}_{x\in L}$.假设 ω' 满足访问结构 $(A_{l\times k},\rho)$,则对于任意 $x\in L$,计算 D_x.

$$D_x=\frac{e(K_{\rho(x),1},C_{x,0})}{e(K_{\rho(x),2},C_{x,1})}\cdot\frac{e\left(C_{x,0},\prod_{j\in S_{\rho(x)},j\neq ID}g_{n+1-j+ID}\right)}{e(g_{ID},C_{x,2})}\cdot\frac{e(g_{ID},C_{x,4})}{e\left(C_{x,3},\prod_{j\in R_{\rho(x)}}g_{n+1-j+ID}\right)}$$
$$=\frac{e(g^{a\cdot t},g^{\lambda_x})}{e(g_1,g_n)^{\lambda_x}}.$$

令 μ_x 为 A 中第 x 行所对应的恢复系数,最终恢复明文 M.

$$M=C_0\cdot\frac{1}{e(K_0,C_1)}\cdot\prod_{x\in L}D_x^{\mu_x}.$$

正确性:

$$C_0\cdot\frac{1}{e(K_0,C_1)}\cdot\prod_{x\in L}D_x^{\mu_x}=M\cdot e(g_1,g_n)^s\cdot\frac{1}{e(g^t,g^{a\cdot s})}\cdot\frac{e\left(g^{a\cdot t},g^{\sum_{x\in L}\lambda_x\mu_x}\right)}{e(g_1,g_n)^{\sum_{x\in L}\lambda_x\mu_x}}=M.$$

说明:若解密者对于第 x 行所对应的属性被撤销,则其只能恢复出 $e(g^{a\cdot t},g^{\lambda_x})\cdot e(g_1,g_n)^{s_x}$ 这样一个随机值(s_x 是随机选取的).因此,解密者对于第 x 行所对应的属性是否被撤销,都无法直接计算出 $e(g^{a\cdot t},g^{\lambda_x})$ 的值.即,恢复明文所需的信息片段 $e(g_1,g_n)^{\lambda_x}$ 是与用户的私钥绑定的.

3.3 安全性证明

定理 2. 若困难性假设 1~假设 3 成立,则我们的方案是安全的.

本节的以下部分给出上述定理的详细证明,证明过程基于双系统加密中安全性证明的思想.首先,构造半功能密文以及半功能密钥;然后,基于半功能密文和半功能密钥构造一系列特殊的攻击游戏(在最终的特殊攻击游戏中,挑战者是对一条随机消息进行加密,因而敌手的攻击优势是可忽略的);最后,基于第 1.4 节中所定义的假设 1~假设 3,证明真实的攻击游戏与这些特殊的攻击游戏是不可区分的,进而证明敌手在真实的攻击游戏中的攻击优势也是可忽略的.

半功能密文:令 G_{p_2} 为 G 中阶为 p_2 的子群,X 为 G_{p_2} 的生成元.从 Z_N^k 中随机选取两个向量:

$$\vec{v}=(s,v_2,v_3,...,v_{k'}),$$
$$\vec{u}=(c,u_2,u_3,...,u_k),$$

则半功能密文 C'为

$$C'_0=C_0,$$
$$C'_1=(g^sX^c)^a,$$
$$\left\{C'_{x,0}=g^{\overrightarrow{A_x}\cdot\vec{v}}X^{\overrightarrow{A_x}\cdot\vec{u}},C'_{x,1}=(C'_{x,0})^{\rho(x)},C'_{x,2}=g^{\eta_x}\cdot\left(h_{\rho(x)}\prod_{j\in S_{\rho(x)}}g_{n+1-j}\right)^{\overrightarrow{A_x}\cdot\vec{v}}\cdot X^{\left(\gamma_i+\sum_{j\in S_{\rho(x)}}\alpha^{n+1-j}\right)\cdot\overrightarrow{A_x}\vec{u}},C'_{x,3}=C_{x,3},C'_{x,4}=C_{x,4}\right\}.$$

半功能密钥:半功能密钥分为两种形式:首先,从 G_{p_2} 中随机选取一个元素 X_0,从 G_{p_3} 中随机选取一个元素 Y_0,对于用户所拥有的任何一个属性 i,从 G_{p_2} 中随机选取两个元素 $X_{i,1},X_{i,2}$;然后,从 G_{p_3} 中随机选取两个元素 $Y_{i,1},Y_{i,2}$;最后,从 Z_N 中随机选取 1 个元素 r_i:

- 第 1 种形式的半功能密钥为 $K'_0=g^tX_0Y_0,\{K'_{i,1}=g^{a\cdot t+\alpha^{ID}\gamma_i+t_ir_i}X_{i,1}Y_{i,1},K'_{i,2}=g^{r_i}X_{i,2}Y_{i,2}\}$;
- 第 2 种形式的半功能密钥为 $K'_0=g^tY_0,\{K'_{i,1}=g^{\alpha^{ID}\gamma_i+t_ir_i}X_{i,1}Y_{i,1},K'_{i,2}=g^{r_i}Y_{i,2}\}$.

假设敌手进行了 q 次私钥查询,对于任意 $1\leqslant k\leqslant q$,定义以下两类攻击游戏:

- $Game_{k,1}$:在攻击游戏 $Game_{k,1}$ 中,对于敌手的前 k–1 次私钥查询请求,挑战者将返回第 2 种形式的半功能密钥;对于敌手的第 k 次私钥查询请求,挑战者将返回第 1 种形式的半功能密钥;对于敌手的第 k 次之后的私钥查询请求,挑战者将返回正常形式的密钥.在挑战阶段,挑战者将计算一条半功能密文返回给敌手;
- $Game_{k,2}$:在攻击游戏 $Game_{k,2}$ 中,对于敌手的前 k 次私钥查询请求,挑战者将返回第 2 种形式的半功能密钥;对于敌手的第 k 次之后的私钥查询请求,挑战者将返回正常形式的密钥.在挑战阶段,挑战者将计算一条半功能密文返回给敌手.

特别地,定义如下 3 个攻击游戏:

- $Game_{real}$:该游戏即为第 2.2 节中所定义的真实攻击游戏;
- $Game_0$:该游戏与 $Game_{real}$ 基本一致,其唯一的区别在于,在 $Game_0$ 的挑战阶段,挑战者将计算一条半功能密文返回给敌手.因此,$Game_0$ 实际上等同于 $Game_{0,2}$;
- $Game_{final}$:该游戏与 $Game_{q,2}$ 基本一致,其唯一的区别在于,在 $Game_{final}$ 的挑战阶段,挑战者将选择一条随机的消息进行加密,并最终将半功能密文返回给敌手.因此,在 $Game_{final}$ 中,敌手的攻击优势 $Game_{final}Adv$ 是可忽略的.

在以下的安全性证明中,我们将基于第 1.4 节中的 3 个假设,通过 4 个引理证明上述的这些游戏是不可区分的,以此将敌手在 $Game_{real}$ 中的攻击优势 $Game_{real}Adv$ 规约到其在 $Game_{final}$ 中的攻击优势 $Game_{final}Adv$.

引理 1. 若存在一个多项式时间的敌手$\mathcal{A}$,能够以不可忽略的优势ϵ区分 $Game_{real}$ 和 $Game_0$,则可以构造一个多项式时间的算法$\mathcal{B}$,以ϵ的优势攻破假设 1.

证明:挑战者将(g,Y,T)发送给$\mathcal{B}$.

Init:$\mathcal{B}$运行敌手$\mathcal{A}$,$\mathcal{A}$输出一个要挑战的访问结构$(A_{l\times k}^*,\rho)$,并且对于任意$x\in\{1,2,...,l\}$,$\mathcal{A}$指定属性$\rho(x)$的用户撤销列表$R_{\rho(x)}^*$.

Setup:令用户集合$U=\{1,2,...,n\}$,属性集合$I=\{1,2,...,m\}$.对于任意属性$i\in I$,首先从Z_N中随机选取一个元素t_i,计算$T_i=g^{t_i}$;其次,令$\omega^*=\{\rho(x)\}_{x\in\{1,2,...,l\}}$,若$i\notin\omega^*$,则从$Z_N$中随机选取一个元素$\gamma_i$,计算$h_i=g^{\gamma_i}$;若$i\in\omega^*$,则从$Z_N$中随机选取一个元素$\beta_i$,令$S_i=U-R_i$,$\gamma_i=\beta_i-\sum_{j\in S_i}\alpha^{n+1-j}$,则$h_i=g^{\beta_i}\left(\prod_{j\in S_i}g_{n+1-j}\right)^{-1}$;然后,从$Z_N$中随机选取一个元素$\alpha$,对于任意$i\in\{1,2,...,n,n+2,...,2n\}$,计算$g_i=g^{(\alpha^i)}$;最后,从$Z_N$中随机选取一个元素$a$,并最终发布公钥参数$PK$为

$$PK=(N,g,g^a,\{T_i\}_{i\in I},\{h_i\}_{i\in I},\{g_i\}_{i\in\{1,2,...,n,n+2,...,2n\}}).$$

系统主私钥MSK为

$$MSK=(\alpha,a,\{t_i,\gamma_i\}_{i\in U},Y).$$

Phase 1:由于$\mathcal{B}$完全拥有主私钥MSK,因此对于敌手$\mathcal{A}$的任何私钥询问请求,$\mathcal{B}$都可以模拟生成.

Challenge:敌手$\mathcal{A}$提交两条明文消息M_0和M_1,$\mathcal{B}$首先从Z_N中随机选取$k-1$个元素$v_2',v_3',...,v_k'$,令向量$\vec{v}'=(1,v_2',v_2',...,v_k')$,然后从$M_0$和$M_1$中随机选取一条消息$M_\theta$计算询问密文$C^*$:

$$C_0^*=M_\theta\cdot e(g^{\alpha^{n+1}},T),$$

$$C_1^*=T^a,$$

$$\left\{C_{x,0}^*=T^{\vec{A}_x^*\cdot\vec{v}'},C_{x,1}^*=(C_{x,0}^*)^{\rho(x)},C_{x,2}^*=g^{\eta_x}\cdot T^{\beta_{\rho(x)}\cdot\vec{A}_x^*\cdot\vec{v}'},C_{x,3}=g^{s_x},C_{x,4}=g^{\eta_x}\left(\prod_{j\in R_{\rho(x)}^*}g_{n+1-j}\right)^{s_x},R_{\rho(x)}^*\right\}_{x\in\{1,2,...,l\}}.$$

Phase 2:重复 Phase 1 阶段的操作.

Guess:敌手$\mathcal{A}$输出对θ的猜测θ':

- 若$T\in G_{p_1}$,设$T=g^s$,则$\vec{v}=s\cdot\vec{v}'$.易见,此时询问密文C^*是一条正常的密文,$\mathcal{B}$与敌手$\mathcal{A}$进行的是$Game_{real}$;
- 若$T\in G_{p_1p_2}$,设$T=g^sX^c$,则$\vec{u}=c\cdot\vec{v}'$.易见,此时询问密文C^*是一条半功能密文,$\mathcal{B}$与敌手$\mathcal{A}$进行的是$Game_0$.

因此,若$\mathcal{A}$能够以不可忽略的优势ϵ区分$Game_{real}$和$Game_0$,则$\mathcal{B}$同样也能够以不可忽略的优势ϵ区分G_{p_1},$G_{p_1p_2}$上的元素. □

引理 2. 若存在一个多项式时间的敌手$\mathcal{A}$,能够以不可忽略的优势ϵ区分$Game_{k-1,2}$和$Game_{k,1}$,则可以构造一个多项式时间的算法$\mathcal{B}$,以ϵ的优势攻破假设 2.

证明:挑战者将$(g,g^sX^{c_1},Y,X^{c_2}Y^d,T)$发送给$\mathcal{B}$,其中,Init,Setup 以及 Guess 阶段与引理 1 一致.因此,该引理的证明只单独描述 Phase 1 和 Phase 2 阶段.

Phase 1:对于敌手$\mathcal{A}$前$k-1$次私钥询问请求,$\mathcal{B}$将返回第 2 种形式的半功能密钥.生成过程如下:$\mathcal{B}$首先从Z_N中随机选取一个元素t,从G_{p_3}中随机选取一个元素Y_0;其次,对于任意$i\in\omega$,从Z_N中随机选取一个元素r_i,从G_{p_3}中随机选取一个元素$Y_{i,2}$,然后计算:

$$K_0'=g^tY_0,$$

$$K_{i,1}'=g^{a\cdot t+\alpha^{ID}\gamma_i+t_i\cdot r_i}(X^{c_2}Y^d)^{r_i},$$

$$K_{i,2}'=g^{r_i}Y_{i,2}.$$

对于敌手$\mathcal{A}$的第k次私钥询问请求,按照如下方式生成:$\mathcal{B}$首先从Z_N中随机选取一个元素t',从G_{p_3}中随机选取一个元素Y_0';其次,对于任意$i\in\omega$,从Z_N中随机选取一个元素r_i',从G_{p_3}中随机选取两个元素$Y_{i,1}',Y_{i,2}'$,然后计算:

$$K'_0 = g^{t'} \cdot T \cdot Y'_0,$$
$$K'_{i,1} = g^{a \cdot t' + \alpha^{ID} \gamma_i} \cdot T^a \cdot T^{r'_i \cdot t_i} \cdot Y'_{i,1},$$
$$K'_{i,2} = T^{r'_i} \cdot Y'_{i,2}.$$

对于敌手$\mathcal{A}$第 k 次之后的私钥询问请求,则与引理 1 的 Phase 1 阶段相同.

Challenge:敌手$\mathcal{A}$提交两条明文消息 M_0 和 M_1,$\mathcal{B}$首先从 Z_N 中随机选取 $k-1$ 个元素 $v'_2, v'_3, ..., v'_k$,令向量 $\vec{v'} = (1, v'_2, v'_2, ..., v'_k)$,然后从 M_0 和 M_1 中随机选取一条消息 M_θ计算询问密文 C^*:

$$C_0^* = M_\theta \cdot e(g^{\alpha^{n+1}}, g^s X^{c_1}),$$
$$C_1^* = (g^s X^{c_1})^a,$$
$$\left\{ C_{x,0}^* = (g^s X^{c_1})^{\overrightarrow{A_x^*} \cdot \vec{v}}, C_{x,1}^* = (C_{x,0}^*)^{\rho(x)}, C_{x,2}^* = g^{\eta_x} \cdot (g^s X^{c_1})^{\beta_{\rho(x)} \cdot \overrightarrow{A_x^*} \cdot \vec{v}}, C_{x,3} = g^{s_x}, C_{x,4} = g^{\eta_x} \left(\prod_{j \in R^*_{\rho(x)}} g_{n+1-j} \right)^{s_x}, R^*_{\rho(x)} \right\}_{x \in \{1,2,...,l\}}.$$

Phase 2:重复 Phase 1 阶段的操作:

- 若 $T \in G$,设 $T = g^b X^{c'} Y^{d'}$,则敌手$\mathcal{A}$第 k 次私钥询问所获取的密钥是第 1 种形式的半功能密钥,$\mathcal{B}$与敌手$\mathcal{A}$进行的是 $Game_{k,1}$;
- 若 $T \in G_{p_1 p_3}$,设 $T = g^b Y^{d'}$,则敌手$\mathcal{A}$第 k 次私钥询问所获取的密钥是正常的密钥,$\mathcal{B}$与敌手$\mathcal{A}$进行的是 $Game_{k-1,2}$.

因此,若$\mathcal{A}$能够以不可忽略的优势ϵ区分 $Game_{k-1,2}$ 和 $Game_{k,1}$,则$\mathcal{B}$同样也能够以不可忽略的优势ϵ区分 G, $G_{p_1 p_3}$ 上的元素. □

引理 3. 若存在一个多项式时间的敌手$\mathcal{A}$,能够以不可忽略的优势ϵ区分 $Game_{k,1}$和 $Game_{k,2}$,则可以构造一个多项式时间的算法$\mathcal{B}$,以ϵ的优势攻破假设 2.

证明:挑战者将 $(g, g^s X^{c_1}, Y, X^{c_2} Y^d, T)$ 发送给$\mathcal{B}$,其中,Init,Setup,Challenge 以及 Guess 阶段与引理 2 一致.因此,该引理的证明只单独描述 Phase 1 和 Phase 2 阶段.

Phase 1:对于敌手$\mathcal{A}$前 $k-1$ 次私钥询问请求,$\mathcal{B}$将返回第 2 种形式的半功能密钥.生成过程和引理 2 中 Phase 1 阶段前 $k-1$ 次私钥生成过程一致.对于敌手$\mathcal{A}$的第 k 次私钥询问请求,按照如下方式生成:$\mathcal{B}$首先从 Z_N 中随机选取一个元素 t',从 G_{p_3} 中随机选取一个元素 Y'_0;其次,对于任意 $i \in \omega$,从 Z_N 中随机选取一个元素 r'_i, b_i,从 G_{p_3} 中随机选取两个元素 $Y'_{i,1}, Y'_{i,2}$,然后计算:

$$K'_0 = g^{t'} \cdot T \cdot Y'_0,$$
$$K'_{i,1} = g^{a \cdot t' + \alpha^{ID} \gamma_i} \cdot T^a \cdot T^{r'_i \cdot t_i} \cdot Y'_{i,1} \cdot (X^{c_2} Y^d)^{b_i},$$
$$K'_{i,2} = T^{r'_i} \cdot Y'_{i,2}.$$

对于敌手$\mathcal{A}$第 k 次之后的私钥询问请求,则与引理 1 的 Phase 1 阶段相同.

Phase 2:重复 Phase 1 阶段的操作:

- 若 $T \in G$,设 $T = g^b X^{c'} Y^{d'}$,则敌手$\mathcal{A}$第 k 次私钥询问所获取的密钥是第 1 种形式的半功能密钥,$\mathcal{B}$与敌手$\mathcal{A}$进行的是 $Game_{k,1}$;
- 若 $T \in G_{p_1 p_3}$,设 $T = g^b Y^{d'}$,则敌手$\mathcal{A}$第 k 次私钥询问所获取的密钥是第 2 种形式的半功能密钥,$\mathcal{B}$与敌手$\mathcal{A}$进行的是 $Game_{k,2}$.

因此,若$\mathcal{A}$能够以不可忽略的优势ϵ区分 $Game_{k,1}$ 和 $Game_{k,2}$,则$\mathcal{B}$同样也能够以不可忽略的优势ϵ区分 $G, G_{p_1 p_3}$ 上的元素. □

引理 4. 若存在一个多项式时间的敌手$\mathcal{A}$,能够以不可忽略的优势ϵ区分 $Game_{q,2}$ 和 $Game_{final}$,则可以构造一个多项式时间的算法$\mathcal{B}$,以ϵ的优势攻破假设 3.

证明:挑战者将 $(g,X,Y,g^sX^{c_1},\{g_i=g^{\alpha^i}\}_{i\in\{1,2,...,n,n+2,...,2n\}},g^{\alpha^{n+1}}X^{c_2},T)$ 发送给$\mathcal{B}$,其中,Init 阶段以及 Guess 阶段与引理 1 一致.因此,该引理的证明只单独描述 Setup,Phase 1 以及 Phase 2 阶段.

Setup:令用户集合 U={1,2,...,n},属性集合 I={1,2,...,m}.对于任意属性 $i\in I$,首先从 Z_N 中随机选取一个元素 t_i,计算 $T_i=g^{t_i}$;其次,令 $\omega^*=\{\rho(x)\}_{x\in\{1,2,...,l\}}$,若 $i\notin\omega^*$,则从 Z_N 中随机选取一个元素γ_i,计算 $h_i=g^{\gamma_i}$;若 $i\in\omega^*$,则从 Z_N 中随机选取一个元素β_i,令 $S_i=U-R_i$, $h_i=g^{\beta_i}\left(\prod_{j\in S_i}g_{n+1-j}\right)^{-1}$,此时有 $\gamma_i=\beta_i-\sum_{j\in S_i}\alpha^{n+1-j}$,但$\mathcal{B}$并不知道该$\gamma_i$ 的值;最后,从 Z_N 中随机选取一个元素 a,并最终发布公钥参数 PK 为

$$PK=(N,g,g^a,\{T_i\}_{i\in I},\{h_i\}_{i\in I},\{g_i\}_{i\in\{1,2,...,n,n+2,...,2n\}}).$$

需要注意的是,$\mathcal{B}$不完全拥有主私钥.

Phase 1:对于敌手$\mathcal{A}$的私钥询问请求,$\mathcal{B}$将始终返回第 2 种形式的半功能密钥.生成过程如下:首先从 Z_N 中随机选取一个元素 t,从 G_{p_3} 中随机选取一个元素 Y_0,计算 $K_0'=g^tY_0$;其次,对于任意 $i\in\omega$:

a) 若 $i\notin\omega^*$,此时$\mathcal{B}$完全知道相应的γ_i 的值,$\mathcal{B}$首先从 G_{p_2} 中随机选取一个元素 $X_{i,1}$,其次从 G_{p_3} 中随机选取两个元素 $Y_{i,1},Y_{i,2}$,然后从 Z_N 中随机选取一个元素 r_i,最后计算:

$$K_{i,1}'=g^{a\cdot t+\alpha^{ID}\gamma_i+t_i\cdot r_i}X_{i,1}Y_{i,1},$$
$$K_{i,2}'=g^{r_i}Y_{i,2}.$$

b) 若 $i\in\omega^*$, $ID\in R_i^*$, 此时$\mathcal{B}$并不知道相应的γ_i 的值,$\mathcal{B}$首先从 G_{p_2} 中随机选取一个元素 $X_{i,1}$,其次从 G_{p_3} 中随机选取两个元素 $Y_{i,1},Y_{i,2}$,然后从 Z_N 中随机选取一个元素 r_i,最后计算:

$$K_{i,1}'=g^{a\cdot t}\cdot g_{ID}^{\beta_i}\cdot\left(\prod_{j\in S_i}g_{n+1+ID-j}\right)^{-1}\cdot g^{t_i\cdot r_i}X_{i,1}Y_{i,1},$$
$$K_{i,2}'=g^{r_i}Y_{i,2}.$$

注意到,由于 $ID\in R_i^*$, 因此 $ID\notin S_i$, $\prod_{j\in S_i}g_{n+1+ID-j}$ 中不会出现 g_{n+1} 这一项, $K_{i,1}',K_{i,2}'$ 是可以有效计算的.

c) 若 $i\in\omega^*$, $ID\notin R_i^*$:此时$\mathcal{B}$并不知道相应的γ_i的值,且有 $ID\in S_i$, $\prod_{j\in S_i}g_{n+1+ID-j}$ 中会出现 g_{n+1} 这一项,$\mathcal{B}$需要利用 $g^{\alpha^{n+1}}X^{c_2}$ 这一项来完成私钥的生成.$\mathcal{B}$首先从 G_{p_2} 中随机选取一个元素 $X_{i,1}'$,其次从 G_{p_3} 中随机选取两个元素 $Y_{i,1},Y_{i,2}$,然后从 Z_N 中随机选取一个元素 r_i,最后计算:

$$K_{i,1}'=g^{a\cdot t}\cdot g_{ID}^{\beta_i}\cdot\left(\prod_{j\in S_i,j\neq ID}g_{n+1+ID-j}\right)^{-1}\cdot(g^{\alpha^{n+1}}X^{c_2})^{-1}\cdot g^{t_i\cdot r_i}X_{i,1}'Y_{i,1},$$
$$K_{i,2}'=g^{r_i}Y_{i,2}.$$

Challenge:敌手$\mathcal{A}$提交两条明文消息 M_0 和 M_1,$\mathcal{B}$首先从 Z_N 中随机选取 k–1 个元素 $v_2',v_3',...,v_k'$,令向量 $\vec{v'}=(1,v_2',v_2',...,v_k')$, 然后从 M_0 和 M_1 中随机选取一条消息 M_θ计算询问密文 C^*:

$$C_0^*=M_\theta\cdot T,$$
$$C_1^*=(g^sX^{c_1})^a,$$
$$\left\{C_{x,0}^*=(g^sX^{c_1})^{\overrightarrow{A_x^*}\cdot\vec{v'}},C_{x,1}^*=(C_{x,0}^*)^{\rho(x)},C_{x,2}^*=g^{\eta_x}\cdot(g^sX^{c_1})^{\beta_{\rho(x)}\cdot\overrightarrow{A_x^*}\cdot\vec{v'}},C_{x,3}=g^{s_x},C_{x,4}=g^{\eta_x}\left(\prod_{j\in R_{\rho(x)}^*}g_{n+1-j}\right)^{s_x},R_{\rho(x)}^*\right\}_{x\in\{1,2,...,l\}}.$$

Phase 2:重复 Phase 1 阶段的操作:

- 若 $T=e(g,g)^{\alpha^{n+1}\cdot s}$,则挑战密文是一条合法的半功能密文,$\mathcal{B}$与敌手$\mathcal{A}$进行的是 $Game_{q,2}$;
- 若 T 是 G_T 上的一个随机元素,则挑战密文是对一条随机消息进行的加密,$\mathcal{B}$与敌手$\mathcal{A}$进行的是 $Game_{final}$.

因此,若$\mathcal{A}$能够以不可忽略的优势ϵ区分 $Game_{q,2}$ 和 $Game_{final}$,则$\mathcal{B}$同样也能够以不可忽略的优势ϵ区分 $e(g,g)^{\alpha^{n+1}\cdot s}$ 与 G_T 上的一个随机元素. □

由引理 1 可知,真实的攻击游戏 $Game_{real}$ 与 $Game_0$ 是不可区分的(基于假设 1);由引理 2 可知,$Game_0$ 与 $Game_{1,1}$,$Game_{1,2}$ 与 $Game_{2,1}$,...,$Game_{q-1,2}$ 与 $Game_{q,1}$ 是不可区分的(基于假设 2);由引理 3 可知,$Game_{1,1}$ 与 $Game_{1,2}$,$Game_{2,1}$ 与 $Game_{2,2}$,...,$Game_{q,1}$ 与 $Game_{q,2}$ 是不可区分的(基于假设 2);结合引理 2 和引理 3,易见 $Game_0$ 与 $Game_{q,2}$ 是不可区分的,进而结合引理 1 可知,$Game_{real}$ 与 $Game_{q,2}$ 是不可区分的.同时,由引理 4 可知,$Game_{q,2}$ 与 $Game_{final}$ 是不可区分的(基于假设 3),因此最终可以得出 $Game_{real}$ 和 $Game_{final}$ 是不可区分的.

通过定义可知,在 $Game_{final}$ 中,挑战者是对一条随机的消息进行加密,因而敌手的攻击优势 $Game_{final}Adv$ 是可以忽略的.由于 $Game_{real}$ 和 $Game_{final}$ 的不可区分性,可以得出:敌手在 $Game_{real}$ 中的攻击优势 $Game_{real}Adv$ 也是可忽略的.因此,我们的方案是安全的.定理 2 证毕. □

4 结束语

本文针对已有支持属性撤销的 ABE 方案中存在的属性撤销粒度过粗的问题,提出了直接撤销模式下支持完全细粒度属性撤销的 CP-ABE 模型,并给出了安全性定义.以 Waters 等人所提出的双系统加密为基础,在合数阶双线性群上给出了一个具体的构造.该方案可以通过 Amada 等人[21]所提出的通用转换方法达到 CCA 的安全性.但需要注意的是,该方案的公钥参数与用户数量线性相关,在实际应用中,容易造成公钥参数过长.Attrapadung 等人所提出方案中的第 2 种撤销方式能够克服这一不足,如何基于这种撤销方式实现一个公钥参数与用户数量无关的、且支持完全细粒度属性撤销的 CP-ABE 方案,是我们下一步所要着重考虑的问题.同时,如何将基于合数阶双线性群的构造方案转换为基于素数阶双线性群的构造方案,也是我们下一步工作所要考虑的问题.

References:

[1] Sahai A, Waters B. Fuzzy identity-based encryption. In: Cramer R, ed. Advances in Cryptology—EUROCRYPT 2005. Berlin: Springer-Verlag, 2005. 457−473. [doi: 10.1007/11426639_27]

[2] Goyal V, Pandey O, Sahai A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Proc. of the 13th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2006. 89−98. [doi: 10.1145/1180405.1180418]

[3] Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2007. 195−203. [doi: 10.1145/1315245.1315270]

[4] Attrapadung N, Imai H. Conjunctive broadcast and attribute-based encryption. In: Shacham H, Waters B, eds. Proc. of the Pairing-Based Cryptography—Pairing 2009. Berlin: Springer-Verlag, 2009. 248−265. [doi: 10.1007/978-3-642-03298-1_16]

[5] Attrapadung N, Imai H. Attribute-Based encryption supporting direct/indirect revocation modes. In: Parker MG, ed. Proc. of the Cryptography and Coding. Berlin: Springer-Verlag, 2009. 278−300. [doi: 10.1007/978-3-642-10868-6_17]

[6] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Proc. of the 2007 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2007. 321−334. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4223236 [doi: 10.1109/SP.2007.11]

[7] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Catalano D, Catalano N, eds. Proc. of the Public Key Cryptography (PKC 2011). Berlin: Springer-Verlag, 2011. 53−70. [doi: 10.1007/978-3-642-19379-8_4]

[8] Su JS, Cao D, Wang XF, Sun YP, Hu QL. Attribute based encryption schemes. Journal of Software, 2011,22(6):1299−1315 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3993.htm [doi: 10.3724/SP.J.1001.2011.03993]

[9] Hanaoka Y, Hanaoka G, Shikata J, Imai H. Identity-Based hierarchical strongly key-insulated encryption and its application. In: Roy B, ed. Advances in Cryptology—ASIACRYPT 2005. Berlin: Springer-Verlag, 2005. 495−514. [doi: 10.1007/11593447_27]

[10] Boldyreva A, Goyal V, Kumar V. Identity-Based encryption with efficient revocation. In: Proc. of the 15th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2008. 417−426. [doi: 10.1145/1455770.1455823]

[11] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup V, ed. Advances in Cryptology—CRYPTO 2005. Berlin: Springer-Verlag, 2005. 258−275. [doi: 10.1007/11535218_16]

[12] Yu SC, Wang C, Ren K, Lou WJ. Attribute based data sharing with attribute revocation. In: Proc. of the 5th ACM Symp. on Information, Computer and Communications Security. New York: ACM Press, 2010. 261−270. [doi: 10.1145/1755688.1755720]

[13] Hur JD, Noh K. Attribute-Based access control with efficient revocation in data outsourcing systems. IEEE Trans. on Parallel and Distributed Systems, 2011,22(7):1214−1221. [doi: 10.1109/TPDS.2010.203]

[14] Wang PP, Feng DG, Zhang LW. Towards attribute revocation in key-policy attribute based encryption. In: Lin DD, Tsudik G, Wang XY, eds. Proc. of the 10th Int'l Conf. on Cryptography and Network Security. Berlin: Springer-Verlag, 2011. 272−291. [doi: 10.1007/978-3-642-25513-7_19]

[15] Boneh D, Goh E, Nissim K. Evaluating 2-DNF formulas on ciphertexts. In: Kilian J, ed. Proc. of the Theory of Cryptography (TCC 2005). Berlin: Springer-Verlag, 2005. 325−341. [doi: 10.1007/978-3-540-30576-7_18]

[16] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi S, ed. Advances in Cryptology—CRYPTO 2009. Berlin: Springer-Verlag, 2009. 619−636. [doi: 10.1007/978-3-642-03356-8_36]

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

[18] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart N, ed. Advances in Cryptology—EUROCRYPT 2008. Berlin: Springer-Verlag, 2008. 146−162. [doi: 10.1007/978-3-540-78967-3_9]

[19] Lewko A, Okamoto T, Sahai A, Takashima K, Waters B. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert H, ed. Advances in Cryptology—EUROCRYPT 2010. Berlin: Springer-Verlag, 2010. 62−91. [doi: 10.1007/ 978-3-642-13190-5_4]

[20] Lewko A, Waters B. Decentralizing attribute-based encryption. In: Paterson K, ed. Advances in Cryptology—EUROCRYPT 2011. Berlin: Springer-Verlag, 2011. 568−588. [doi: 10.1007/978-3-642-20465-4_31]

[21] Amada S, Attrapadung N, Hanaoka G, Kunihiro N. Generic constructions for chosen-ciphertext secure attribute based encryption. In: Catalano D, Catalano N, eds. Proc. of the Public Key Cryptography (PKC 2011). Berlin: Springer-Verlag, 2011. 71−89. [doi: 10.1007/978-3- 642-19379-8_5]

附中文参考文献:

[8] 苏金树,曹丹,王小峰,孙一品,胡乔林.属性基加密机制.软件学报,2011,22(6):1299−1315. http://www.jos.org.cn/1000-9825/3993.htm [doi: 10. 3724/SP.J.1001.2011.03993]

王鹏翩(1985－),男,河南登封人,博士生,主要研究领域为网络与系统安全.

张立武(1976－),男,博士,高级工程师,主要研究领域为信息与系统安全.

冯登国(1965－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为密码学,信息安全.