第5章 基于属性的密码体制

5.1 基于属性的密码体制的一般概念

加密可被认为是加密者与接收者(用户或设备)共享数据的一种方法,但仅限于加密者明确知道他想要共享数据的用户。然而,在许多应用中,加密者并不明确知道想要共享数据的用户。例如,加密者意欲在某个特定时间段与具有某个特定IP地址的用户共享数据,加密者就必须把自己的秘密钥给这些特定的用户。这种共享数据的方式只能实现一对一的加密,因而是粗粒度的,限制了加密者以细粒度方式和其他用户共享加密数据。基于属性的加密(Attribute-Based Encryption, ABE)机制是传统公钥加密的一种延伸,由Sahai和Waters在2005年欧密会上提出[34],其中加密者能够在加密算法中表达他想要如何分享数据,他可根据接收用户的凭证制定一些策略,并根据这些策略共享数据。因此,可实现一对多或多对多的加密。用户的凭证用属性集合描述,属性是描述用户的信息要素,通常指用户本身所拥有的特性或身份标识,如学生的属性可包括所在的院系、专业、类别、年级等。

基于属性的加密机制又分为基于密钥策略的属性加密(Key-Policy Attribute-Based Encryption, KP-ABE)和基于密文策略的属性加密(Ciphertext-Policy Attribute-Based Encryption, CP-ABE),在KP-ABE中,密文包含属性集合,而密钥则与该属性集合的访问策略相关联,只有当密文的属性集合满足密钥所关联的访问策略时才能解密。CP-ABE则相反,其中接收者的密钥与属性集合相关联,而密文则包含该属性集合上的访问策略,只有当接收者密钥所关联的属性集合满足密文所包含的访问策略时才能解密。如图5-1所示,其中TA(Trusted Authority)是建立系统的可信机构。KP-ABE与CP-ABE的区别如表5-1所示。

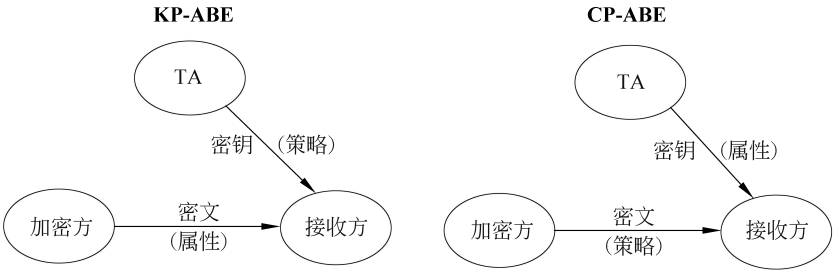

图5-1 KP-ABE与CP-ABE的关系

表 5-1　KP-ABE 与 CP-ABE 的区别

比　较　项	KP-ABE	CP-ABE
密文	密文包含属性	密文包含策略
密钥	密钥关联策略	密钥关联属性
策略	策略掌握在中心 TA 手中(稳定)	策略掌握在自己(加密者)手中(灵活)
应用模式	收费点播模式	传统访问控制模式
计算量	计算量小	计算量大

IBE 方案可看作一种特殊的 KP-ABE 方案，如图 5-2 所示。其中，密文包含的属性为接收者的身份 ID′。密钥所关联的访问策略为：密文包含的接收者身份 ID′与密钥的属主身份 ID 一样，即 ID′＝ID 时，可以解密。

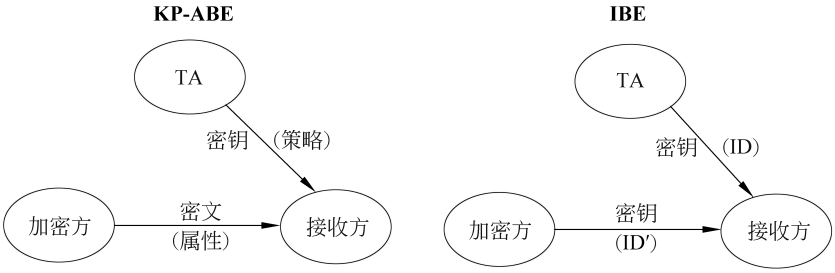

图 5-2　KP-ABE 与 IBE 的关系

因为策略集合远大于属性集合，因此在 KP-ABE 中，按照属性集合加密，计算量要小于 CP-ABE 中按照策略加密。

访问结构是实现访问策略的集合表示，是由属性集合$\{P_1, P_2, \cdots, P_n\}$的一些非空子集构成的单调集合(见 1.5.1 节定义 1-18)，表示为$\mathbb{A}$。$\mathbb{A}$中的元素 r 满足访问策略，称为授权集合，表示为 $\gamma \in \mathbb{A}$。不在$\mathbb{A}$中的元素则不满足访问策略，称为非授权集合，表示为 $\gamma \notin \mathbb{A}$。

4 个常用的概念如下：

- 主密钥：由 TA 掌握，用于为接收方产生解密密钥。
- 会话密钥：TA 为接收方产生的解密密钥。
- 密钥指数：用主密钥产生会话密钥时使用的随机数。
- 加密指数：发送方加密明文时使用的随机数。

KP-ABE 方案由以下 4 个算法组成：

(1) 初始化。

TA 执行，为随机化算法，输入安全参数 κ 和属性总体的描述，输出系统参数 params 和主密钥 msk，表示为(params，msk)←Init(κ)。

(2) 加密。

发送方执行，为随机化算法，输入消息 M、系统参数 params 以及属性集 γ，输出密文 CT，表示为 CT＝$\mathcal{E}_\gamma(M)$。

(3) 密钥产生。

TA 执行,为随机化算法,输入系统参数 params、主密钥 msk 以及访问结构$\mathbb{A}$,输出会话密钥 sk,表示为 sk←ABEGen($\mathbb{A}$)。

TA 在密钥产生过程中实施策略的具体方式是用秘密分割方案在属性总体上对主密钥进行分割,使得只有授权集合可以隐含地恢复主密钥。"隐含"是指在指数上恢复被加密指数随机化了的主密钥。

(4) 解密。

接收方执行,为确定性算法,输入系统参数 params、会话密钥 sk(访问结构$\mathbb{A}$对应的密钥)及密文 CT(包含属性集合 γ),如果 $\gamma\in\mathbb{A}$,解密算法将解密 CT 并返回消息 M,表示为 $M=\mathcal{D}_{sk}(CT)$。

KP-ABE 的安全模型与 IBE 机制类似,仍是由挑战者和敌手的交互式游戏刻画。

将 KP-ABE 方案记为 Π,Π 的 IND 游戏(称为 IND-KP-ABE-CPA 游戏)如下:

(1) 初始化。由挑战者运行,产生系统参数 params 和主密钥 msk,将 params 给敌手。

(2) 阶段 1(训练)。敌手发出对访问结构$\mathbb{A}$的秘密钥产生询问;挑战者运行秘密钥产生算法,产生与$\mathbb{A}$对应的秘密钥 d,并把它发送给敌手。这一过程可重复多项式有界次。

(3) 挑战。敌手提交两个长度相等的消息 M_0、M_1 和一个意欲挑战的属性集合 γ^*,其中 γ^* 不满足阶段 1 中的每一个访问结构$\mathbb{A}$;挑战者选择随机数 $\beta\leftarrow_R\{0,1\}$,以 γ^* 加密 M_β,将密文 C^* 给敌手。

(4) 阶段 2(训练)。重复阶段 1 的过程,敌手发出对另外的访问结构$\mathbb{A}$的秘密钥产生询问,唯一的限制是挑战阶段产生的属性集合 γ^* 均不满足该访问结构$\mathbb{A}$,表示为 $\gamma^*\notin\mathbb{A}$;挑战者以阶段 1 中的方式进行回应。这一过程可重复多项式有界次。

(5) 猜测。敌手输出猜测 $\beta'\in\{0,1\}$,如果 $\beta'=\beta$,则敌手攻击成功。

敌手的优势定义为安全参数 κ 的函数:

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{\text{KP-ABE}}(\kappa)=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$$

如果敌手在初始化阶段前声称一个意欲挑战的属性集合 γ^*,则称这个系统是选定属性安全的。

IND-KP-ABE-CPA 游戏的形式化描述如下:

$\underline{\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{IND-KP-ABE-CPA}}(\kappa)}$:

$\gamma^*\leftarrow A$;/选定属性的

(params,msk)←Init(κ);

$(M_0,M_1,\gamma^*)\leftarrow\mathcal{A}^{\text{ABEGen}(\cdot)}$(params);

/如果是选定属性的,此时无 γ^*

/ABEGen(·)改为 $\text{ABEGen}_{\neq\gamma^*}(\cdot)$

$\beta\leftarrow_R\{0,1\}$,$C^*=\mathcal{E}_{\gamma^*}(M_\beta)$;

$\beta'\leftarrow\mathcal{A}^{\text{ABEGen}_{\neq\gamma^*}(\cdot)}(C^*)$;

如果 $\beta'=\beta$,则返回 1;否则返回 0.

其中，$\mathcal{A}$右肩上的 ABEGen(·)表示敌手$\mathcal{A}$向挑战者做访问结构的秘密钥询问，$\text{ABEGen}_{\neq\gamma^*}(\cdot)$表示敌手$\mathcal{A}$向挑战者做访问结构$\mathbb{A}$的秘密钥询问，要求$\gamma^* \notin \mathbb{A}$。

敌手的优势为

$$\text{Adv}_{\Pi,\mathcal{A}}^{\text{KP-ABE}}(\kappa)=\left|\Pr[\text{Exp}_{\Pi,\mathcal{A}}^{\text{IND-KP-ABE-CPA}}(\kappa)=1]-\frac{1}{2}\right|$$

定义 5-1　如果对任何多项式时间的敌手$\mathcal{A}$在上述游戏中的优势是可忽略的，则称此 KP-ABE 加密机制是语义安全的。

CP-ABE 方案由以下 4 个算法组成：

(1) 初始化。为随机化算法，输入安全参数κ和属性总体的描述，输出系统参数 params 和主密钥 msk，表示为$(\text{params},\text{msk})\leftarrow\text{Init}(\kappa)$。

(2) 加密。为随机化算法，输入消息 M、系统参数 params 以及属性总体上的访问结构$\mathbb{A}$，输出密文 CT，CT 中隐含地包含访问结构$\mathbb{A}$，表示为 $\text{CT}=\mathcal{E}_{\mathbb{A}}(M)$。仅当接收方拥有满足访问结构的属性集合时才能解密该密文。

发送方实施的策略：首先为每一消息选择一个加密指数，然后用秘密分割方案在密文上分割加密指数，使得只有授权集合可以隐含地恢复加密指数。“隐含”是指在指数上恢复被加密指数随机化了的主密钥。

(3) 密钥产生。为随机化算法，输入系统参数 params、主密钥 msk 以及用来描述密钥的属性集γ，输出会话密钥 sk，表示为 $\text{sk}\leftarrow\text{ABEGen}(\gamma)$。

(4) 解密。接收方执行，为确定性算法，输入系统参数 params、会话密钥 sk(属性集合γ对应的密钥)及密文 CT(包含访问结构$\mathbb{A}$)，如果γ满足访问结构$\mathbb{A}$(即$\gamma\in\mathbb{A}$)，解密算法将 CT 解密并返回消息 M，表示为 $M=\mathcal{D}_{\text{sk}}(\text{CT})$。

CP-ABE 机制的安全模型与 IBE 机制类似，其中允许敌手对任意的密钥(除了用来解密挑战密文的密钥以外)进行询问。敌手会选择挑战一个满足访问结构$\mathbb{A}^*$的密文，并且能够对任何不满足访问结构$\mathbb{A}^*$的属性集合γ进行密钥询问。记 CP-ABE 方案为Π，Π的 IND 游戏(称为 IND-CP-ABE-CPA 游戏)如下：

(1) 初始化。由挑战者运行，产生系统参数 params 并将其给敌手。

(2) 阶段 1(训练)。敌手发出对属性集合γ的秘密钥产生询问；挑战者运行秘密钥产生算法，产生与γ对应的秘密钥 d，并把它发送给敌手。这一过程可重复多项式有界次。

(3) 挑战。敌手提交两个长度相等的消息 M_0 和 M_1。此外，敌手选定一个意欲挑战的访问结构$\mathbb{A}^*$，其中敌手在阶段 1 中询问过的属性集合均不能满足此访问结构。挑战者选择随机数$\beta\leftarrow_R\{0,1\}$并以$\mathbb{A}^*$加密 M_β，将密文 C^* 给敌手。

(4) 阶段 2(训练)。敌手发出对另外的属性集合γ的秘密钥产生询问，唯一的限制是这些γ均不满足挑战阶段的访问结构$\mathbb{A}^*$；挑战者以阶段 1 中的方式进行回应。这一过程可重复多项式有界次。

(5) 猜测。敌手输出猜测$\beta'\in\{0,1\}$，如果$\beta'=\beta$，则敌手攻击成功。

敌手的优势定义为安全参数κ的函数：

$$\text{Adv}_{\Pi,\mathcal{A}}^{\text{CP-ABE}}(\kappa)=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$$

如果敌手在初始化阶段前声称一个意欲挑战的访问结构$\mathbb{A}^*$,则称这个系统是选定访问结构安全的。

IND-CP-ABE-CPA 游戏的形式化描述如下:

$\underline{\mathrm{Exp}_{\Pi,\mathcal{A}}^{\text{IND-CP-ABE-CPA}}(\kappa)}$:

$\mathbb{A}^* \leftarrow \mathcal{A}$;/选定访问结构的

$(\text{params}, \text{msk}) \leftarrow \text{Init}(\kappa)$;

$(M_0, M_1, \mathbb{A}^*) \leftarrow \mathcal{A}^{\text{ABEGen}(\cdot)}(\text{params})$;

/如果是选定访问结构的,此时没有$\mathbb{A}^*$;

/ABEGen(·)修改为 $\text{ABEGen}_{\neq \mathbb{A}^*}(\cdot)$

$\beta \leftarrow_R \{0,1\}, C^* = \mathcal{E}_{\mathbb{A}^*}(M_\beta)$;

$\beta' \leftarrow \mathcal{A}^{\text{ABEGen}_{\neq A^*}(\cdot)}(C^*)$;

如果 $\beta' = \beta$,则返回 1;否则返回 0.

其中,$\mathcal{A}$右肩上的 ABEGen(·)表示敌手$\mathcal{A}$向挑战者做属性集合的秘密钥询问,$\text{ABEGen}_{\neq \mathbb{A}^*}(\cdot)$表示敌手$\mathcal{A}$向挑战者做不满足$\mathbb{A}^*$的属性集合 γ 的秘密钥询问。

敌手的优势为

$$\text{Adv}_{\Pi,\mathcal{A}}^{\text{CP-ABE}}(\kappa) = \left| \Pr[\text{Exp}_{\Pi,\mathcal{A}}^{\text{IND-CP-ABE-CPA}}(\kappa) = 1] - \frac{1}{2} \right|$$

定义 5-2 如果对任何多项式时间的敌手$\mathcal{A}$在上述游戏中的优势是可忽略的,则称此 CP-ABE 加密机制是语义安全的。

与 IBE 方案类似,ABE 方案的安全模型也分为选定属性(或访问结构)安全的和完全安全的。完全安全的模型用对偶加密系统实现。

本章分别介绍模糊身份的 KP-ABE 加密方案[34]、基于访问树结构的 KP-ABE 方案[35]、基于 LSSS 的 CP-ABE 加密方案[36]、基于对偶加密系统的完全安全的 CP-ABE 方案[37]。

5.2 基于模糊身份的 KP-ABE 方案

基于模糊身份的加密方案简称 Fuzzy IBE(Fuzzy Identity-Based Encryption),是 Sahai 和 Waters 于 2005 年提出的,是对使用生物特征数据作为身份信息的 IBE 方案的改进。该方案通过引入门限方案的思想,将用户的生物特征作为身份信息,可实现容错的基于身份的加密。若用户拥有身份 ω 对应的秘密钥,就可解密身份 ω' 加密的消息,当且仅当在某种度量下,ω 和 ω' 在某个距离之内。作为身份信息的生物特征,其距离度量可取海明距离、集合差、编辑距离。而如果将身份 ω 取为属性集合,则 Fuzzy IBE 系统可用于基于密钥策略的属性加密(KP-ABE)。

5.2.1 Fuzzy IBE 的安全模型及困难性假设

Fuzzy IBE 的选定身份(Fuzzy Selective-ID)模型与基于身份的标准模型类似,区别

在于前者仅允许敌手询问与目标身份在某个距离范围外的身份的秘密钥，其中距离度量取集合差。设 ω 和 ω' 是两个集合，它们的对称差是集合 $\omega\Delta\omega'=\{x\in\omega\cup\omega'\mid x\notin\omega\cap\omega'\}$，$\omega$ 和 ω' 之间的集合差定义为 $|\omega\Delta\omega'|$。为使集合差大于某个门限值，$|\omega\cap\omega'|$ 必须小于某个定值。这样就可以把集合差转换为集合交来描述。

设 $\mathcal{A}$ 表示一个攻击者，$\mathcal{A}$ 可以对任一身份做秘密钥产生询问，限制条件是该身份与要攻击的身份交集少于 d 个元素。

下面是 Fuzzy IBE 机制(记为 Π)安全游戏。

(1) 敌手声称意欲挑战的身份 α。

(2) 初始化。由挑战者运行，产生系统参数 params 和主密钥 msk，将 params 给敌手。

(3) 阶段 1(训练)。敌手对满足 $|\gamma_j\cap\alpha|<d$ 的身份 γ_j 进行秘密钥询问。

(4) 挑战。敌手提交两个长度相等的消息 M_0 和 M_1。挑战者选择随机数 $\beta\leftarrow_R\{0,1\}$，以 α 加密 M_β，将密文 C^* 给敌手。

(4) 阶段 2(训练)。重复阶段 1 的过程。

(5) 猜测。敌手输出猜测 $\beta'\in\{0,1\}$，如果 $\beta'=\beta$，则敌手攻击成功。

敌手的优势定义为安全参数 κ 的函数：

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{\mathrm{ABE}}(\kappa)=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$$

定义 5-3　如果对任何多项式时间的敌手 $\mathcal{A}$ 在上述游戏中的优势是可忽略的，则称此 Fuzzy IBE 加密机制是安全的。

下面的 Fuzzy IBE 方案的安全性基于修改版的 DBDH 假设，记为判定性 MBDH (Modified Bilinear Diffie-Hellman)。回忆 DBDH 假设，挑战者随机选择 $a,b,c\leftarrow_R\mathbb{Z}_p$，不存在多项式时间的敌手能以不可忽略的优势区分以下两个分布总体：

$$\{(g,A=g^a,B=g^b,C=g^c,Z=\hat{e}(g,g)^{abc})\}$$

$$\{(g,A=g^a,B=g^b,C=g^c,Z=\hat{e}(g,g)^{z})\}$$

随机选择 $a,b,c\leftarrow_R\mathbb{Z}_p$，定义以下两个分布总体：

$$\mathcal{P}_{\mathrm{MBDH}}=\{(g,A=g^a,B=g^b,C=g^c,Z=\hat{e}(g,g)^{\frac{ab}{c}})\}$$

$$\mathcal{R}_{\mathrm{MBDH}}=\{(g,A=g^a,B=g^b,C=g^c,Z=\hat{e}(g,g)^{z})\}$$

判定性 MBDH 问题是指，敌手 $\mathcal{B}$ 得到 T，判断 $T\in\mathcal{P}_{\mathrm{MBDH}}$ 还是 $T\in\mathcal{R}_{\mathrm{MBDH}}$。优势定义为

$$|\Pr[\mathcal{B}(T\in\mathcal{P}_{\mathrm{MBDH}})=1]-\Pr[\mathcal{B}(T\in\mathcal{R}_{\mathrm{MBDH}})=1]|$$

MBDH 假设：没有多项式时间的敌手能以不可忽略的优势解决 MBDH 问题。

已知 c，可由推广的欧几里得算法求 $\frac{1}{c}$，因此 MBDH 问题和 DBDH 问题等价。

5.2.2　基于模糊身份的加密方案

基于模糊身份的加密方案将身份看作属性集合，参数设置如下：g 是阶为素数 p 的群 $\mathbb{G}_1$ 的生成元，$\hat{e}:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$ 为双线性映射。κ 为安全参数，代表群的大小。对 $i\in\mathbb{Z}$

$_p$及$\mathbb{Z}_p$中元素的集合S,定义拉格朗日系数为$\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$。属性总体记为$\mathcal{U}$,大小记为$|\mathcal{U}|$,其元素用$\mathbb{Z}_p^*$中的前$|\mathcal{U}|$个元素$1,2,\cdots,|\mathcal{U}|(\bmod p)$表示。身份为$\mathcal{U}$的元素构成的子集。访问策略是将主密钥$y$由$(d,|\mathcal{U}|)$门限秘密分割方案进行分配,由身份$\omega'$产生的密文仅由满足$|\omega\cap\omega'|\geqslant d$的身份$\omega$才能解密。

基于模糊身份的加密方案如下:

(1) 初始化:

$\underline{\text{Init}(\kappa)}$:

$t_1,t_2,\cdots,t_{|\mathcal{U}|},y\leftarrow_R\mathbb{Z}_p$;

$\text{params}=(T_1=g^{t_1},T_2=g^{t_2},\cdots,T_{|\mathcal{U}|}=g^{t_{|\mathcal{U}|}},Y=\hat{e}(g,g)^y)$;

$\text{msk}=(t_1,t_2,\cdots,t_{|\mathcal{U}|},y)$.

注意:主密钥与每个属性成分关联。

(2) 密钥产生(其中$\omega\subseteq\mathcal{U}$):

$\underline{\text{ABEGen}(\text{msk},\omega)}$:

随机选取一个$d-1$次多项式q,满足$q(0)=y$;

$D_i=g^{\frac{q(i)}{t_i}},i\in\omega$;

$d_\omega=\{D_i\}_{i\in\omega}$.

注意:d_ω作为对ω产生的秘密钥,秘密钥的每个成分D_i与主密钥分割后的份额$q(i)$关联。

(3) 加密(用接收方的属性ω'作为公开钥,其中$M\in\mathbb{G}_2$):

$\underline{\mathcal{E}_{\omega'}(M)}$:

$s\leftarrow_R\mathbb{Z}_p$;/加密指数

$\text{CT}=(\omega',C'=M\cdot Y^s,\{C_i=T_i^s\}_{i\in\omega'})$.

注意:加密指数与公开参数关联,而公开参数与属性元素关联,所以加密指数与属性元素关联。

(4) 解密(用ω解密CT,其中$|\omega\cap\omega'|\geqslant d$):

$\underline{\mathcal{D}_{d_\omega}(\text{CT})}$:

在$\omega\cap\omega'$选d个元素,构成集合S;

返回$\dfrac{C'}{\prod_{i\in S}(\hat{e}(D_i,C_i))^{\Delta_{i,S}(0)}}$.

这是因为

$$\prod_{i\in S}(\hat{e}(D_i,C_i))^{\Delta_{i,S}(0)}=\prod_{i\in S}(\hat{e}(g^{\frac{q(i)}{t_i}},g^{st_i}))^{\Delta_{i,S}(0)}=\prod_{i\in S}(\hat{e}(g,g)^{sq(i)})^{\Delta_{i,S}(0)}$$

$$=\hat{e}(g,g)^{s\sum_{i\in S}q(i)\Delta_{i,S}(0)}=\hat{e}(g,g)^{sy}$$

定理5-1 在选定身份模型下,如果存在多项式时间的敌手$\mathcal{A}$以ε的优势攻破该方案,则存在另一敌手$\mathcal{B}$以ε的优势解决判定性MBDH问题。

证明　设$\mathcal{B}$收到五元组 $T=(g,g^a,g^b,g^c,Z)$，它可能取自$\mathcal{P}_{\text{MBDH}}$，此时 $Z=\hat{e}(g,g)^{\frac{ab}{c}}$；也可能取自$\mathcal{R}_{\text{MBDH}}$，此时 Z 从$\mathbb{G}_2$中随机独立选取。$\mathcal{B}$的目标是区分哪种情况发生。如果 $Z=\hat{e}(g,g)^{\frac{ab}{c}}$，则$\mathcal{B}$输出 1；否则输出 0。$\mathcal{B}$在下面的选定身份游戏中与$\mathcal{A}$交互，假定属性总体$\mathcal{U}$是公开的。

游戏开始前，$\mathcal{B}$首先获得$\mathcal{A}$意欲挑战的身份 α。

(1) 初始化。$\mathcal{B}$产生系统参数：$Y=\hat{e}(g,A)=\hat{e}(g,g)^a$（隐含地取主密钥成分 $y=a$）；对所有的 $i\in\alpha$，随机选择 $v_i\leftarrow_R\mathbb{Z}_p$，令 $T_i=C^{v_i}=g^{cv_i}$（隐含地取主密钥成分 $t_i=cv_i$）；对所有的 $i\in\mathcal{U}-\alpha$，随机选择 $w_i\leftarrow_R\mathbb{Z}_p$，令 $T_i=g^{w_i}$（隐含地取主密钥成分 $t_i=w_i$）。设系统参数 params$=(T_1,T_2,\cdots,T_{|\mathcal{U}|},Y)$，将其发送给敌手$\mathcal{A}$。在$\mathcal{A}$看来，所有参数均为随机的。

注意，初始化过程采用的是分离策略，将属性总体$\mathcal{U}$划分为 α 和$\mathcal{U}-\alpha$。

(2) 阶段 1。$\mathcal{A}$对身份 γ 做秘密钥产生询问，其中 γ 满足$|\gamma\cap\alpha|<d$。$\mathcal{B}$按以下方式定义 Γ、Γ'和 S 3 个集合：

- $\Gamma=\gamma\cap\alpha$；
- Γ'是满足$\Gamma\subseteq\Gamma'\subseteq\gamma$且$|\Gamma'|=d-1$的集合；
- $S=\Gamma'\cup\{0\}$。

这样构造的 S 有 d 个点，可通过 S 由插值法（在指数上）构造 $d-1$ 次多项式 $q(x)$（常数项取主密钥成分 $y=a$），求出 $q(x)$在 γ 中的每一个值（指数上），从而可应答敌手对身份 γ 的秘密钥询问。

Γ、Γ'与挑战身份α 和γ 之间的关系如图 5-3 所示。

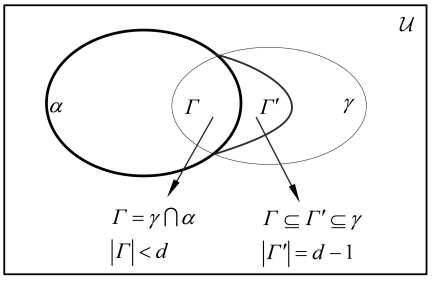

图 5-3　4 个集合之间的关系

然后$\mathcal{B}$按以下方式为 γ 产生秘密钥：

- 若 $i\in\Gamma$，随机选取 $s_i\leftarrow_R\mathbb{Z}_p$，计算 $D_i=g^{s_i}$（隐含地有 $q(i)=t_is_i=cv_is_i$）。
- 若 $i\in\Gamma'-\Gamma$，随机选取 $\lambda_i\leftarrow_R\mathbb{Z}_p$，计算 $D_i=g^{\frac{\lambda_i}{w_i}}$（隐含地有 $q(i)=\lambda_i$）。
- 若$i\in\gamma-\Gamma'$，计算$D_i=\left(\prod_{j\in\Gamma}C^{\frac{v_js_j\Delta_{j,S}(i)}{w_i}}\right)\left(\prod_{j\in\Gamma'-\Gamma}g^{\frac{\lambda_j\Delta_{j,S}(i)}{w_i}}\right)A^{\frac{\Delta_{0,S}(i)}{w_i}}$（隐含地取$q(0)=a$）。

这是因为

$$\begin{aligned}D_i&=\left(\prod_{j\in\Gamma}C^{\frac{v_js_j\Delta_{j,S}(i)}{w_i}}\right)\left(\prod_{j\in\Gamma'-\Gamma}g^{\frac{\lambda_j\Delta_{j,S}(i)}{w_i}}\right)A^{\frac{\Delta_{0,S}(i)}{w_i}}\\&=\left(\prod_{j\in\Gamma}g^{\frac{cv_js_j\Delta_{j,S}(i)}{w_i}}\right)\left(\prod_{j\in\Gamma'-\Gamma}g^{\frac{\lambda_j\Delta_{j,S}(i)}{w_i}}\right)g^{\frac{a\Delta_{0,S}(i)}{wi}}\end{aligned}$$

$$=\left(\prod_{j\in\Gamma}g^{\frac{q(j)\Delta_{j,S}(i)}{w_i}}\right)\left(\prod_{j\in\Gamma'-\Gamma}g^{\frac{q(j)\Delta_{j,S}(i)}{w_i}}\right)g^{\frac{q(0)\Delta_{0,S}(i)}{w_i}}$$

$$=g^{\sum\limits_{j\in\Gamma}\frac{q(j)\Delta_{j,S}(i)}{w_i}}g^{\sum\limits_{j\in\Gamma'-\Gamma}\frac{q(j)\Delta_{j,S}(i)}{w_i}}g^{\frac{q(0)\Delta_{0,S}(i)}{w_i}}$$

$$=g^{\frac{1}{w_i}\sum\limits_{j\in S}q(j)\Delta_{j,S}(i)}=g^{\frac{q(i)}{w_i}}$$

在敌手$\mathcal{A}$看来,$\mathcal{B}$按以上方式为γ产生的秘密钥与真实方案中的秘密钥是同分布的。

(3) 挑战。$\mathcal{A}$向$\mathcal{B}$提交两个挑战消息M_0和M_1。$\mathcal{B}$随机选$\beta\leftarrow_R\{0,1\}$,计算M_β的密文:

$$C^*=(\alpha,C'=M_\beta\cdot Z,\{C_i=B^{v_i}\}_{i\in\alpha})$$

如果$Z=\hat{e}(g,g)^{\frac{ab}{c}}$,设加密指数$s=\frac{b}{c}$,则有

$$C'=M_\beta\cdot Z=M_\beta\cdot\hat{e}(g,g)^{\frac{ab}{c}}=M_\beta\cdot\hat{e}(g,g)^{ys}=M_\beta\cdot Y^s$$

$$C_i=B^{v_i}=g^{bv_i}=g^{\frac{b}{c}cv_i}=g^{scv_i}=(T_i)^s$$

所以该密文是消息M_β在身份α下的加密结果。

如果Z从$\mathbb{G}_2$中随机独立选取,则$C'=M_\beta\cdot Z$是M_β的一次一密加密的密文。

(4) 阶段 2。与阶段 1 类似。

(5) 猜测。$\mathcal{A}$输出对β的猜测β'。如果$\beta'=\beta$,则$\mathcal{B}$输出 1,表示$T\in\mathcal{P}_{\text{MBDH}}$;如果$\beta'\neq\beta$,则$\mathcal{B}$输出 0,表示$T\in\mathcal{R}_{\text{MBDH}}$。

如果$T\in\mathcal{P}_{\text{MBDH}}$,则模拟过程中敌手$\mathcal{A}$的视图与其在真实攻击中的视图相同,于是$\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|>\varepsilon(\kappa)$;反之,如果$T\in\mathcal{R}_{\text{MBDH}}$,则$\Pr[\beta'=\beta]=\frac{1}{2}$。$\mathcal{B}$的优势为

$$|\Pr[\mathcal{B}(T\in\mathcal{P}_{\text{MBDH}})=1]-\Pr[\mathcal{B}(T\in\mathcal{R}_{\text{MBDH}})=1]|\geqslant\left|\left(\frac{1}{2}\pm\varepsilon(\kappa)\right)-\frac{1}{2}\right|=\varepsilon(\kappa)$$

(定理 5-1 证毕)

5.2.3 大属性集上的基于模糊身份的加密方案

在 5.2.2 节的方案中,公开参数随着属性集的大小$|\mathcal{U}|$而线性增长。若属性总体为$\mathbb{Z}_p^*$,则 params 大到使方案失去实际意义。本方案用插值法在g(生成元)的指数上构造一个n次多项式,其中n是加密的最大的身份长度(即表示身份的最多的属性个数),由此得到一个函数$T(x)$,用此函数表达属性x。因此建立 params 时,不用显式地表达每个属性。通过大属性集上一个抗碰撞的哈希函数$H:\{0,1\}^*\rightarrow\mathbb{Z}_p^*$,可以把任意串映射到$\mathbb{Z}_p^*$上。该方案的安全性基于判定性 BDH 假设(见 4.3.1 节)。

参数设置与 5.2.2 节相同,加密身份固定长度为n,即身份由$\mathbb{Z}_p^*$中的n个元素构成。如果取一个将任意串映射到$\mathbb{Z}_p^*$的抗碰撞的哈希函数H,则身份可取为n个任意的元素。访问策略仍是将主密钥y按$(d,|\mathcal{U}|)$门限秘密分割方案进行分配,由身份ω'产生的密文仅由满足$|\omega\cap\omega'|\geqslant d$的身份$\omega$解密。

该方案的具体构造如下:

(1) 初始化:

$\underline{\text{Init}(\kappa)}$：

$y \leftarrow_R \mathbb{Z}_p$；/ 主密钥

$g_2 \leftarrow_R \mathbb{G}_1$；

$t_1, t_2, \cdots, t_{n+1} \leftarrow_R \mathbb{G}_1$；

N 定义为集合$\{1, 2, \cdots, n+1\}$；

$T(x)$ 定义为函数 $g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(x)}$；

params $=(g, g_2, t_1, t_2, \cdots, t_{n+1})$；/$g$ 是$\mathbb{G}_1$的生成元

msk $= y$.

其中定义的函数 $T(x) = g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(x)}$，可看作存在某个 n 次多项式 $h(x)$ 使得 $T(x) = g_2^{x^n} g^{h(x)}$。

(2) 密钥产生(其中 $\omega \subseteq \mathcal{U}$)：

$\underline{\text{ABEGen}(\text{msk}, \omega)}$：

随机选取一个 $d-1$ 次多项式 q，满足 $q(0) = y$；

对每一 $i \in \omega$

{

$r_i \leftarrow_R \mathbb{Z}_p$；/密钥指数

$D_i = g_2^{q(i)} T(i)^{r_i}$，$d_i = g^{r_i}$

}；

$d_\omega = \{D_i, d_i\}_{i \in \omega}$.

注意：d_ω 作为对 ω 产生的秘密钥，其每个成分 D_i 与主密钥的分割份额 $q(i)$ 关联。

(3) 加密(用接收方的属性 ω' 作为公开钥，其中 $M \in \mathbb{G}_2$)：

$\underline{\mathcal{E}_{\omega'}(M)}$：

$s \leftarrow_R \mathbb{Z}_p$；/加密指数

$\text{CT} = (\omega', C' = M \cdot \hat{e}(g, g_2)^{ys}, C'' = g^s, \{C_i = T(i)^s\}_{i \in \omega'})$

注意：加密指数与属性的每个元素关联。

(4) 解密(用 ω 解密 CT，其中 $|\omega \cap \omega'| \geqslant d$)：

$\underline{\mathcal{D}_{d_\omega}(\text{CT})}$：

在 $\omega \cap \omega'$ 中选取 d 个元素，构成集合 S；

返回 $C' \prod_{i \in S} \left(\frac{\hat{e}(d_i, C_i)}{\hat{e}(D_i, C'')} \right)^{\Delta_{i,S}(0)}$.

这是因为

$$C' \prod_{i \in S} \left(\frac{\hat{e}(d_i, C_i)}{\hat{e}(D_i, C'')} \right)^{\Delta_{i,S}(0)} = M \cdot \hat{e}(g, g_2)^{ys} \prod_{i \in S} \left(\frac{\hat{e}(g^{r_i}, T(i)^s)}{\hat{e}(g_2^{q(i)} T(i)^{r_i}, g^s)} \right)^{\Delta_{i,S}(0)}$$

$$= M \cdot \hat{e}(g, g_2)^{ys} \prod_{i \in S} \left(\frac{\hat{e}(g^{r_i}, T(i)^s)}{\hat{e}(g_2^{q(i)}, g^s) \hat{e}(T(i)^{r_i}, g^s)} \right)^{\Delta_{i,S}(0)}$$