KP-ABE与CP-ABE的区别

qry

- KP-ABE的访问策略是在密钥中

所谓密钥政策加密系统是指，密钥对应于一个访问策略而密文对应于一个属性集合，解密当且仅当属性集合中的属性能够满足此访问结构。

- CP-ABE的访问策略是在密文中

所谓密文政策加密系统是指，密文对应于一个访问策略而密钥对应于属性集合，解密当且仅当属性集合中的属性能够满足此访问结构。

KP-ABE

Setup

PK : $T_1 = g^{t_1}, \ldots, T_{|\mathcal{U}|} = g^{t_{|\mathcal{U}|}}, Y = e(g,g)^y$

MK : $t_1, \ldots, t_{|\mathcal{U}|}, y$

Key Generation $(\mathcal{T}, \mathrm{MK})$

SK : $D_x = g^{\frac{q_x(0)}{t_i}}$ where $i = \mathrm{att}(x)$

Encryption (M, γ, PK)

（M为明文，γ为属性集）

$E = (\gamma, E' = MY^s, \{E_i = T_i^s\}_{i \in \gamma})$

Decryption (E, D)

$$= \begin{cases} e(D_x, E_i) = e(g^{\frac{q_x(0)}{t_i}}, g^{s \cdot t_i}) \\ = e(g,g)^{s \cdot q_x(0)} \quad \text{if } i \in \gamma \\ \\ \perp \text{ otherwise} \end{cases}$$

CP-ABE

Setup

$$\mathrm{PK} = \mathbb{G}_0, g, h = g^{\beta}, f = g^{1/\beta}, e(g,g)^{\alpha}$$

$$\mathrm{MK\ is}\ (\beta, g^{\alpha})$$

Encrypt(PK, M, $\mathcal{T}$)

（M为明文，T为访问控制树）

$$\mathrm{CT} = \Big(\mathcal{T},\ \tilde{C} = Me(g,g)^{\alpha s},\ C = h^s,$$
$$\forall y \in Y: \quad C_y = g^{q_y(0)}, C'_y = H(\mathsf{att}(y))^{q_y(0)}\Big).$$

KeyGen(MK, S)

（S为解密者的属性）

$$\mathrm{SK} = \Big(D = g^{(\alpha+r)/\beta},$$
$$\forall j \in S: \quad D_j = g^r \cdot H(j)^{r_j}, D'_j = g^{r_j}\Big).$$

Decrypt(CT, SK)

$$\mathrm{DecryptNode}(\mathrm{CT}, \mathrm{SK}, x) = \frac{e(D_i, C_x)}{e(D'_i, C'_x)}$$
$$= \frac{e\left(g^r \cdot H(i)^{r_i}, h^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})}$$
$$= e(g,g)^{r q_x(0)}.$$

$$\tilde{C}/(e(C,D)/A) = \tilde{C}/\left(e\left(h^s, g^{(\alpha+r)/\beta}\right)/e(g,g)^{rs}\right) = M.$$

- 因为KP-ABE在密文中只需要包含属性的标签，所以相比CP-ABE有着更快的加密速度。