

秘钥策略基加密(KP-ABE)

[Attribute-based encryption for fine-grained access control of encrypted data](#)

预备知识

拉格朗日插值算法

给定 d 个点 $(x_0, y_0), (x_1, y_1), \dots, (x_{d-1}, y_{d-1})$ ，可以决定一个 $d - 1$ 次多项式。该多项式可以表示为：

$$q(x) = \sum_{i=0}^{d-1} y_i \delta_i(x)$$

其中，拉格朗日因子 $\delta_i(x) = \prod_{j=0, j \neq i}^{d-1} \frac{x - x_j}{x_i - x_j}$

Shamir秘密共享

将秘密 s 分割后共享给 n 个人，至少 k 个人组合后才可以恢复秘密 s 。分享方案：

选取 $k - 1$ 次随机多项式 $q(x)$ 并使得 $q(0) = s$ ，计算 $(x_1, q(x_1)), (x_2, q(x_2)), \dots, (x_n, q(x_n))$ ，将对应的 $q(x_i)$ 分享给第 i 个用户。

k 个用户通过其秘密分片进行拉格朗日插值后恢复 $q(x)$ ，进而计算出 $q(0)$ 。

setup

1. 生成pairing相关公共参数 $\langle e, g, G_1, G_T, Z_r \rangle$ 。
2. 确定属性全集 U 为整数集合 $\{1, 2, \dots, |U|\}$ ，以及系统门限值 d 。
3. 针对每个属性 i 选择随机数 $t_i \in Z_r$ 作为主密钥组件，计算 $T_i = g^{t_i}$ 作为对应的公钥组件。
4. 选取随机数 $y \in Z_r$ ，并计算 $Y = e(g, g)^y$ 。
5. 最终，系统主密钥 $msk = \langle t_1, t_2, \dots, t_{|U|}, y \rangle$ ，公钥 $pk = \langle T_1, T_2, \dots, T_{|U|}, Y \rangle$ 。

keygen

1. 将秘密 y 根据访问树 T 自顶向下共享，得到叶子节点的属性 i 对应的秘密分片为 $q(i)$ ，进一步计算 $D_i = g^{\frac{q(i)}{t_i}}$ 。
2. 用户私钥 $sk = \{D_i\}_{i \in leaf(T)}$ 。

encrypt

1. 选取随机数 $s \in Z_r$ ，针对明文消息 $M \in G_T$ ，计算 $E' = M \cdot Y^s = M \cdot e(g, g)^{ys}$ 。
2. 针对明文属性集合 W 中的每个属性 i ，计算 $E_i = T_i^s$ 。
3. 密文为 $ct = \langle E', \{E_i\}_{i \in W} \rangle$ 。

decrypt

1. 秘文的属性集合 W 满足解密秘钥访问树 T 的情况下才能解密。
2. 同一属性对应的密文组件和秘钥组件做配对，针对 W 中的每个属性 i ，计算 $P_i = e(E_i, D_i) = e(g, g)^{sq(i)}$ 。
3. 从根节点开始，做递归计算。注意，这个过程中秘密是嵌入在指数中的，所以在实现的过程中将整个 P_i 作为秘密分片来处理。因此，计算过程中中间节点的秘文分片的计算形式是将每个子节点的分片基于拉格朗日差值

因子做指数运算后，再进行连乘运算。

4. 最终根节点的秘密值可以以 $e(g, g)^{sy}$ 的形式恢复。

5. $E'/e(g, g)^{sy} = M$

算法实现注意事项

1. 属性用整数表示。实际应用中通过索引表将每一个整数和一个字符串属性对应起来。
2. 判断一个int类型是否属于int数组，和判断一个String是否属于String数组所用方法的区别。
3. 访问树作为函数参数比较简单直观。也可以考虑以序列化的方式来做。