# 模糊身份基加密(Fuzzy IBE)

https://eprint.iacr.org/2004/086.pdf

## 预备知识

### 拉格朗日插值算法

给定$d$个点$(x_0, y_0), (x_1, y_1), \ldots, (x_{d-1}, y_{d-1})$，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$(x_1, q(x_1)), (x_2, q(x_2)), \ldots, (x_n, q(x_n))$，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 $< e, g, G_1, G_T, Z_r >$。
2. 确定属性全集$U$为整数集合$\{1, 2, \ldots, |U|\}$，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$msk = \langle t_1, t_2, \ldots t_{|U|}, y \rangle$，公钥$pk = \langle T_1, T_2, \ldots, T_{|U|}, Y \rangle$。

## keygen

1. 随机选择一个$d-1$次多项式$q(x)$，使得$q(0) = y$。
2. 针对用户属性集合$S$中的每个属性$i$，计算$q(i)$，进一步计算$D_i = g^{\frac{q(i)}{t_i}}$。
3. 用户私钥$sk = \{D_i\}_{i \in S}$。

## encrypt

1. 选取随机数$s \in Zr$，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. 如果用户属性集合$S$和明文属性集合$W$重合属性个数不小于$d$，可按如下方法解密。
2. 从所有重合属性中选取$d$个构成属性集合$I$。
3. 针对$I$中的每个属性$i$，计算$P_i = e(E_i, D_i)^{\delta_i(0)} = e(g, g)^{sq(i)\delta_i(0)}$，其中$\delta_i(0)$是拉格朗日因子。
4. $\prod_{i \in I} P_i = e(g, g)^{s \sum_{i \in I} q(i)\delta_i(0)} = e(g, g)^{sy}$

5. $E'/\prod_{i\in I} P_i = M$

# 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. 多项式求值和拉格朗日插值在群Zr上进行，因此相应的int值在计算前要转换为Zr Element。
3. 对于重复使用的值，一定要记得使用getImmutable()或者duplicate()。尤其是在for循环中。