密文策略属性基基加密(CP-ABE)

Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization

setup

1. 生成pairing相关公共参数 $< e, g, G_1, G_T, Z_r >$。
2. 选取随机数$\alpha \in Z_r$，并计算$Y = e(g,g)^{\alpha}$。
3. 选取随机数$\beta \in Z_r$，计算g^{β}。
4. 系统主密钥g^{α}，公钥$pk = \langle Y, g^{\beta} \rangle$。
5. 每个属性对应一个G_1群元素，可以预先选取，也可以使用的时候再对属性进行哈希计算（使用统一的hash算法）。

keygen

1. 选取一个随机数t，计算$D = g^{\alpha} g^{\beta t}$，$D_0 = g^t$。
2. 对用户属性列表中attList的每一个属性i，计算$D_i = H(i)^t$。
3. 用户私钥$sk = \langle D, D_0, \{D_i\}_{i \in attList} \rangle$。

encrypt

1. 选取随机数$s \in Zr$，针对明文消息$M \in G_T$，计算$C = Me(g,g)^{\alpha s}, C_0 = g^s$。
2. 将s作为秘密，沿着访问树进行拆分，使得对于叶子节点属性i,对应的秘密分片为λ_i。对于每个叶子节点属性，计算$C_i^1 = g^{\beta \lambda_i} H(i)^{-r_i}, C_i^2 = g^{r_i}$。
3. 密文为$ct = \langle C, C_0 \{C_i^1, C_i^2\}_{i \in leafNodes} \rangle$。

decrypt

1. 秘钥的属性集合S满足密文访问树T的情况下才能解密。
2. 对于秘钥属性集合S和密文访问T的叶子节点属性集合中重合的属性i，计算 $P_i = e(C_i^1, D_0) e(C_i^2, D_i) = e(g,g)^{\beta t \lambda_i}$。
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密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$e(g,g)^{\beta t s}$的形式恢复。
5. 另外计算$e(C_0, D) = e(g,g)^{\alpha s} e(g,g)^{\beta t s}$，进一步求得$e(g,g)^{\alpha s}$。
6. $C / e(g,g)^{\alpha s} = M$

算法实现注意事项

1. 属性用整数表示，用同样的哈希计算方法将属性映射值群G_1上。