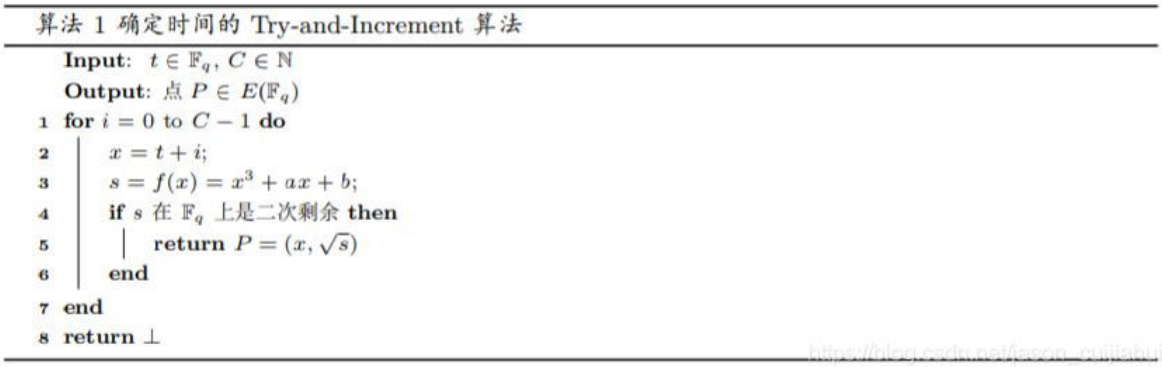
Report

在本项目中，实现了一个朴素的ECMH策略，要实现一个ECMH策略，最基本的就是实现hash列表的交换性，结合性等：如hash（{a}）+hash（{b}）=hash（{b}）+hash（{a}）=hash（{a，b}）因此，如何把hash的消息映射到椭圆曲线的点上是重中之重，在这里我使用了一种比较朴素的方法：



算法 1 确定时间的 Try-and-Increment 算法

Input: $t \in \mathbb{F}_q, C \in \mathbb{N}$
Output: 点 $P \in E(\mathbb{F}_q)$

```
for i = 0 to C − 1 do
    x = t + i;
    s = f(x) = x^3 + ax + b;
    if s 在 F_q 上是二次剩余 then
        return P = (x, √s)
    end
end
return ⊥
```

其中t是消息的hash值（在这里采用sha256的方法）C是自己取的值，我取为n

判断是否是二次剩余的方法在这里我是用欧拉定理，即判断

$$a^{\frac{p-1}{2}} = 1$$

使用s计算y的算法为：

$$\mathrm{y} = \mathrm{s}^{\frac{\mathrm{p}+1}{4}} \bmod \mathrm{p}$$

因此我们就可以定义combine 和 remove操作分别为点加和点减，可以结合SM2类中相关算法加以实现，具体结果如下所示：

```
C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Python39\python.exe -u "c:\Users\86180\Desktop\SM2-ECMH\sm2_ECMH.py"
--------------------------准备combine操作--------------------------
当前集合为： ['Feng Xiangdi'] 对应的点为： (98614918984154830144678945975731224550404777164876842752539643719615745414992, 263942748508777971013737317152836238750074181184160540209448873812028582723277)
当前集合为： ['cybersecurity'] 对应的点为： (45517304204206417385122539864414278298529159958161873524619980236109122646456, 35751141645107420413680751470625137874556414866304023177912105081833926851049)
--------------------------进行combine操作--------------------------
当前集合为： ['Feng Xiangdi', 'cybersecurity'] 对应的点为： (97876383724363666982590411642203982790998961143420853807894782627011529604 41, 883158922908274334527867347674785885420489784773389604457300233320634030605 05)
--------------------------结束combine操作--------------------------
--------------------------准备combine操作--------------------------
当前集合为： ['Feng Xiangdi', 'cybersecurity'] 对应的点为： (97876383724363666982590411642203982790998961143420853807894782627011529604 41, 883158922908274334527867347674785885420489784773389604457300233320634030605 05)
当前集合为： ['Shandong University'] 对应的点为： (11453774045834000589778374683784898366630654485216961142392663810866563011246 5, 78062634317704622905034037799697667558371728092078670957560994192208875639115)
--------------------------进行combine操作--------------------------
当前集合为： ['Feng Xiangdi', 'cybersecurity', 'Shandong University'] 对应的点为： (43346784015451644716331988679637976352722578034885327346860269262342289316695, 49152209672397782514686327618004267035291645123793037762730522845595375306734)
--------------------------结束combine操作--------------------------
--------------------------准备remove操作--------------------------
当前集合为： ['Feng Xiangdi', 'cybersecurity', 'Shandong University'] 对应的点为： (43346784015451644716331988679637976352722578034885327346860269262342289316695, 49152209672397782514686327618004267035291645123793037762730522845595375306734)
当前集合为： ['Feng Xiangdi'] 对应的点为： (98614918984154830144678945975731224550404777164876842752539643719615745414992, 263942748508777971013737317152836238750074181184160540209448873812028582723277)
--------------------------进行remove操作--------------------------
当前集合为： ['cybersecurity', 'Shandong University'] 对应的点为： (10176513464448454776502652114337700407683548818441401692660937406995211479787 1, 97545711159973195860300100326595880073033492119911548280117611542720274627947)
--------------------------结束remove操作--------------------------
```