项目说明 -- 零知识证明

✅Project: Write a circuit to prove that your CET6 grade is larger than 425.

零知识证明简介

零知识证明是一种证明方法，通过这种方法，一方（证明者）在不透露任何实际信息的情况下，可以向另一方（验证者）证明它知道一个秘密或一个声明是真实的。

根据零知识证明的定义可以得知零知识证明具有以下三个重要的性质：

1. 完备性（`Completeness`）：只要证明者拥有相应的知识，那么就能通过验证者的验证，即证明者有足够大的概率使验证者确信。；
2. 可靠性（`Soundness`）：如果证明者没有相应的知识，则无法通过验证者的验证，即证明者欺骗验证者的概率可以忽略。
3. 零知识性（`Zero-Knowledge`）：证明者在交互过程中仅向验证者透露是否拥有相应知识的陈述，不会泄露任何关于知识的额外信息。

根据零知识证明的方式，可以分为交互式和非交互式。交互式一般是通过挑战响应的方式，非交互式一般通过承诺方案来实现。

零知识证明六级成绩超过425

在交互式证明中，经常会用到Hash或者离散对数这种具有单向性的函数，我们就分别用这两种构造交互式的零知识证明方案。

根据题目描述，MoE发布的成绩结构是这样的：

$GRADE = (cn\_id, grade, year, sig\_by\_moe)$，我们认为MoE作为可信第三方，并且公钥是可验证的，利用MoE的私钥进行签名。

Hash方法构造方案：

成绩发布：

1. 生成随机数 r\k，对 r 做 g+k 次hash运算，其中g = grade，即计算$hash^{(g+k)}(r)$，同时考生储存$hash^{(k)}(r)$，也就是说考生可以计算得到$hash^{(k)}(r), hash^{(k+1)}(r)...hash^{(k+g)}(r)$
2. 使用MoE的私钥sk进行签名：$sig\_by\_moe = signature_{sk}(cn\_id||year||hash^{(g+k)}(r))$

零知识证明：

假如此时正在面试，考官要求学生提供零知识证明CET6成绩超过425（如果没超过，就当考官没说）

1. 考生向考官提供sig_by_moe，考官通过验证平台或其他方式，使用MoE的公钥验证签名，得到$hash^{(g+k)}(r)$
2. 考官发起挑战，要求学生提供$h = hash^{g+k-425}(r)$

3. 如果学生成绩大于425，那么$g+k-425>k$，即学生可以提供$h'=hash^{(g+k-425)}(r)$，考官验证 $h==h'$，如果相等则通过验证。

ECC方法构造方案

成绩发布：

1. 确定ECC曲线参数，大素数P、基点G
2. 生成随机数k，计算$R=(g+k)*G, g=grade$，考生保存kG，也就是说，考生可以计算得到$(k+1)G,(k+2)G...(k+g)G$
3. 使用MoE的私钥sk进行签名：$sig\_by\_moe=signature_{sk}(cn\_id||year||R)$

零知识证明：

假如此时正在面试，考官要求学生提供零知识证明CET6成绩超过425（如果没超过，就当考官没说）

1. 考生向考官提供sig_by_moe，考官通过验证平台或其他方式，使用MoE的公钥验证签名，得到$R=(g+k)*G$
2. 考官发起挑战，要求学生提供$r=(g+k-425)*G$
3. 如果学生成绩大于425，那么$g+k-425>k$，即学生可以提供$r'=(g+k-425)*G$，考官验证 $r==r'$，如果相等则通过验证。

合理性说明：

两个方案中都是利用成绩和随机数k做了一个计算链，同时允许考生知道其中的g个值，因为是单向函数，所以考生也只能提供这g个值。在零知识证明时，向考生请求g+k-425，那么考生的g必须大于425才能提供正确的值，因此可以实现正确性证明。