## 1零知识证明定义

证明一个命题是正确的，但又不会验证者知道其中包含的信息。

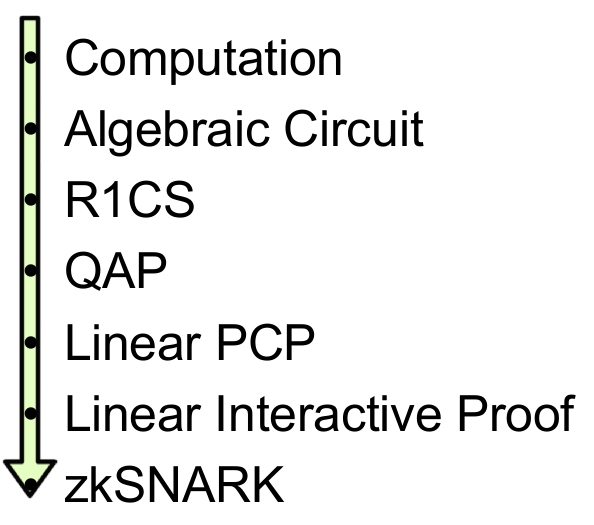
### 1.1交互式证明

验证者会多次询问证明者相关的信息，但不能完全

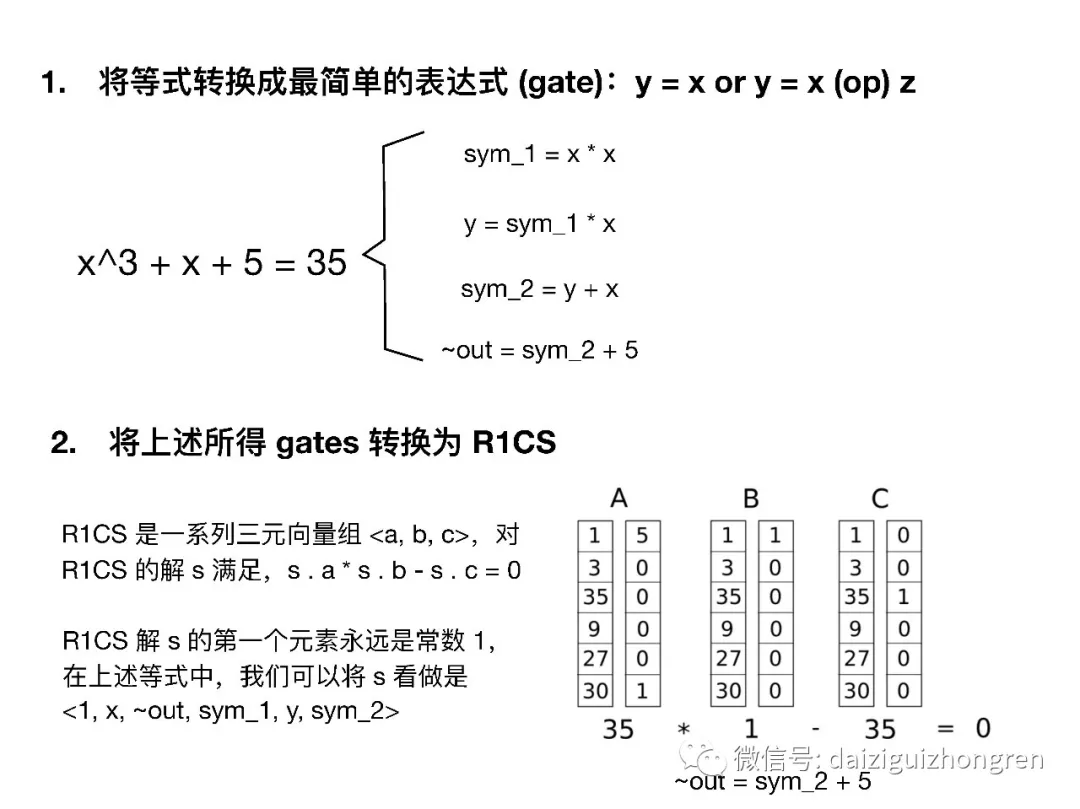
### 1.2非交互式证明

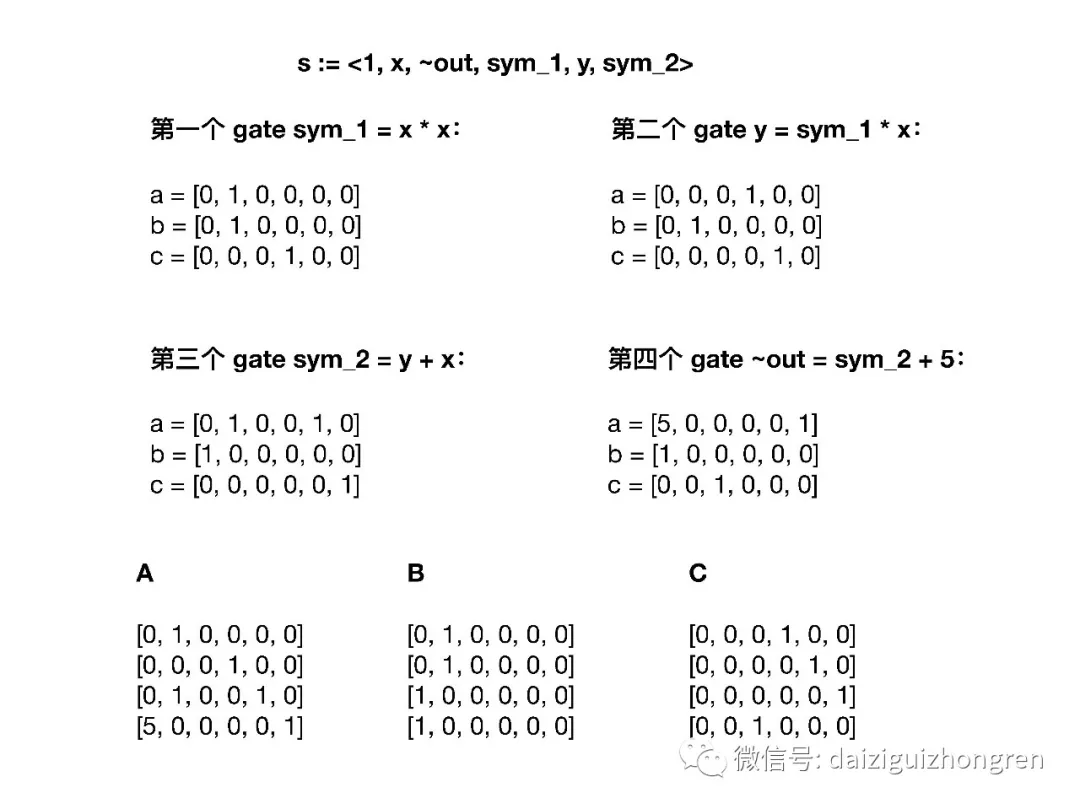
由证明者生成π，Prove() -> π, 证明者将π发送给验证方，验证者验证π的正确性，verify(π)->{true , false}

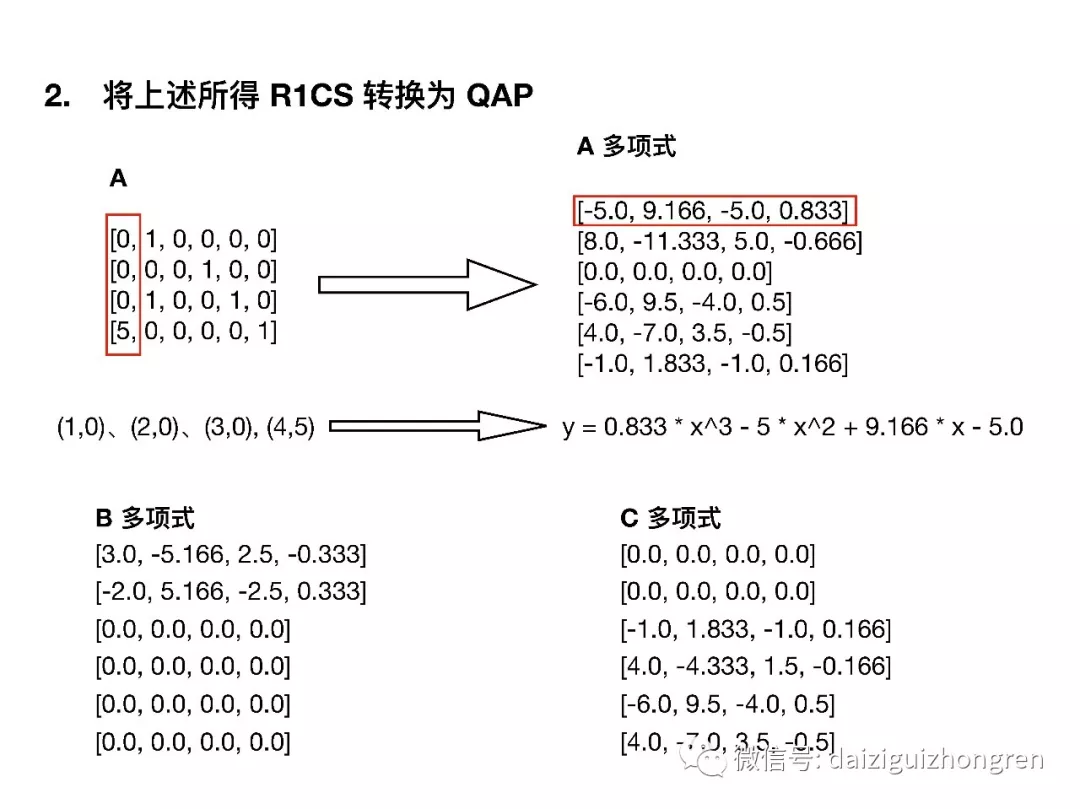
## 2 zk-snark原理介绍

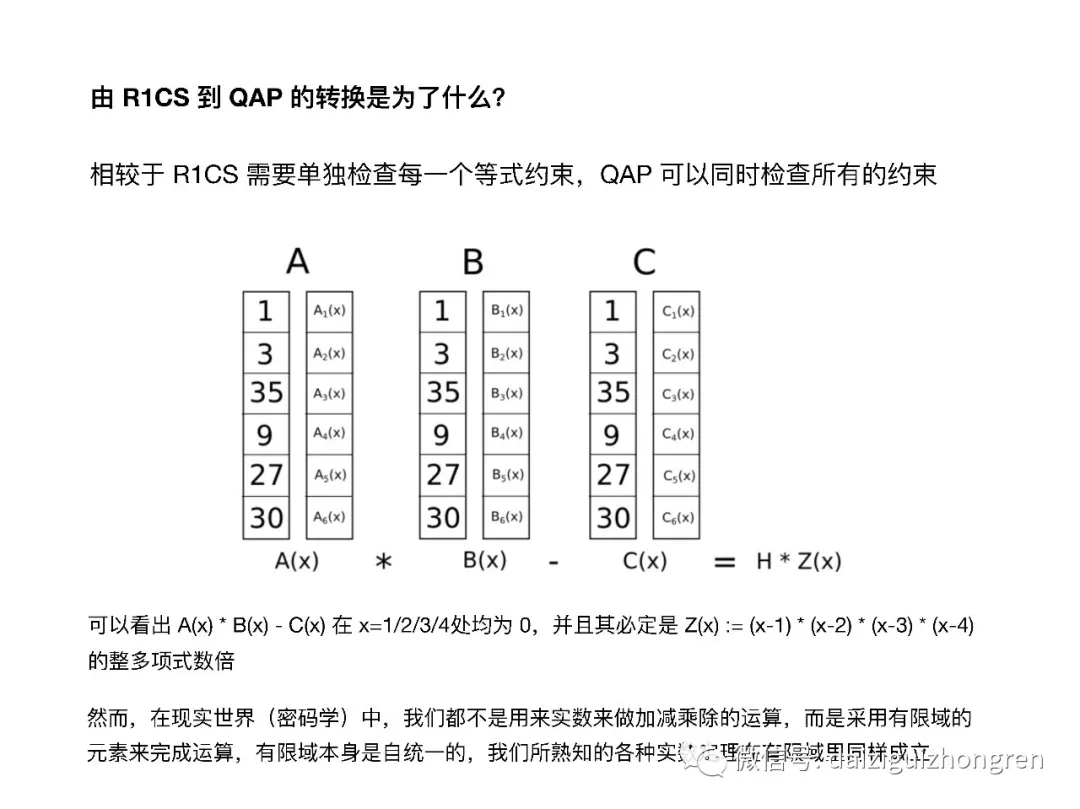


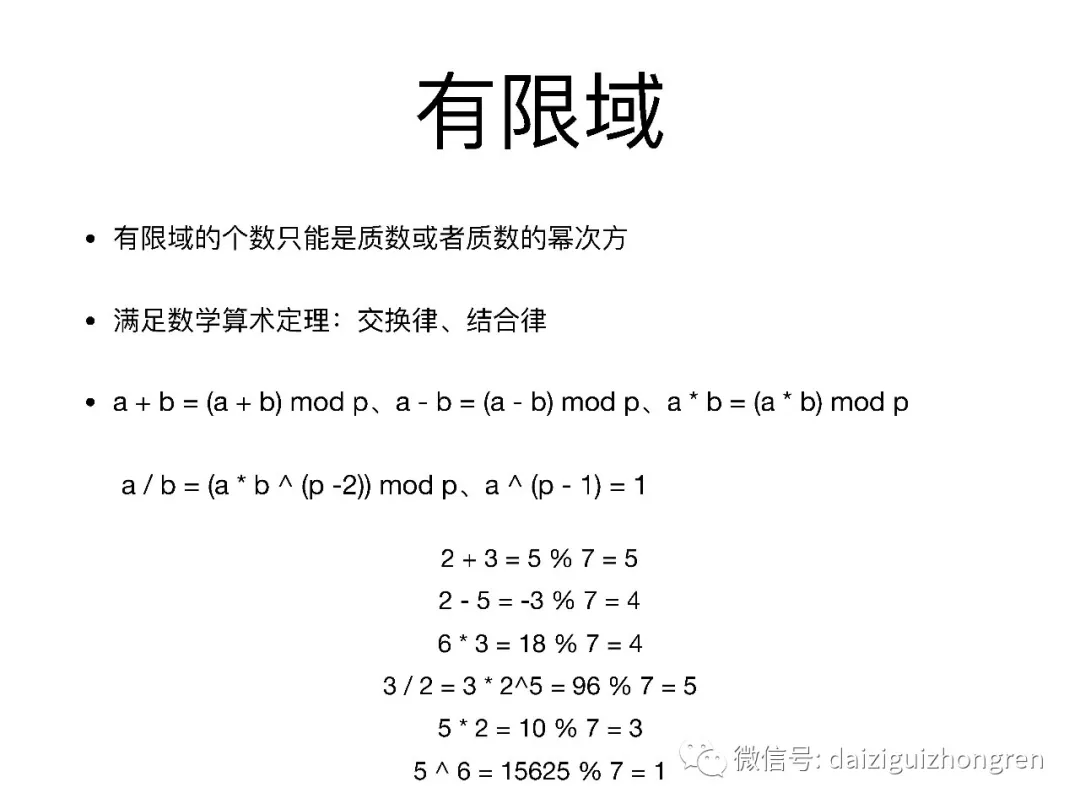
(计算等式)Computation ->(逻辑门)Algebraic Circuit->(R1约束系统)R1CS(Rank-1 Constraint System)->(二次运算程序)QAP(Quadratic Arithmetic Programs)->(双线性配对)Linear PCP->（线性交互证明）Linear Interactive Proof

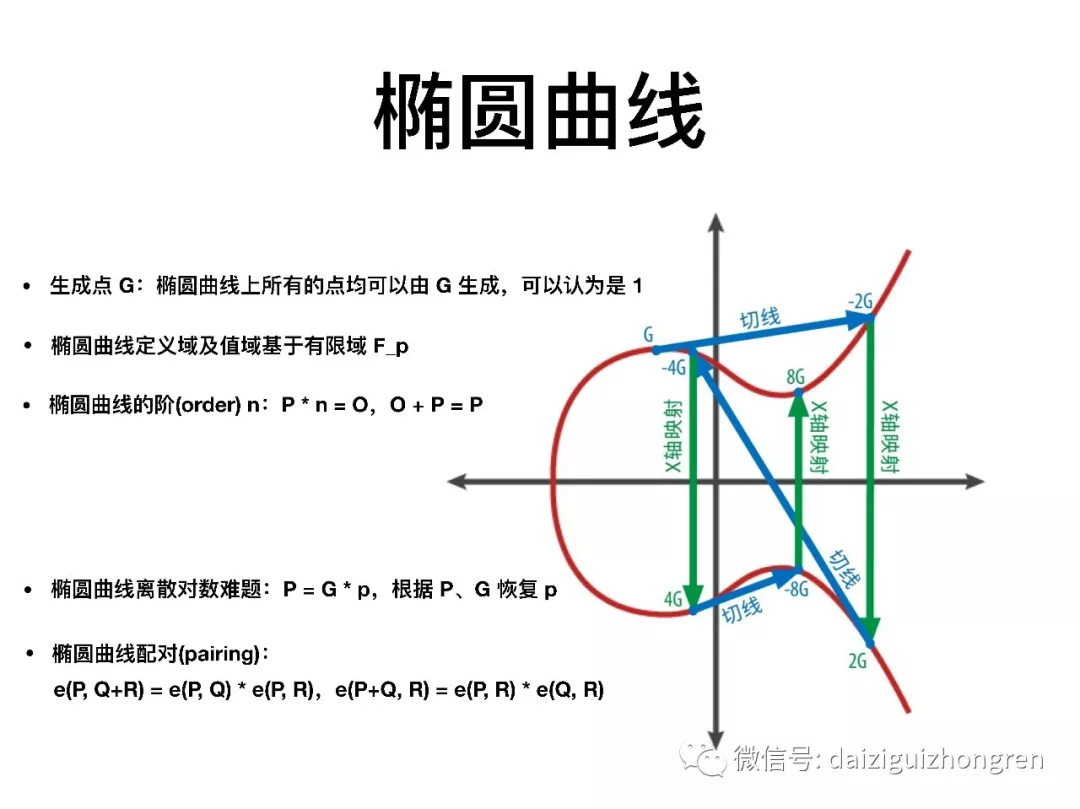


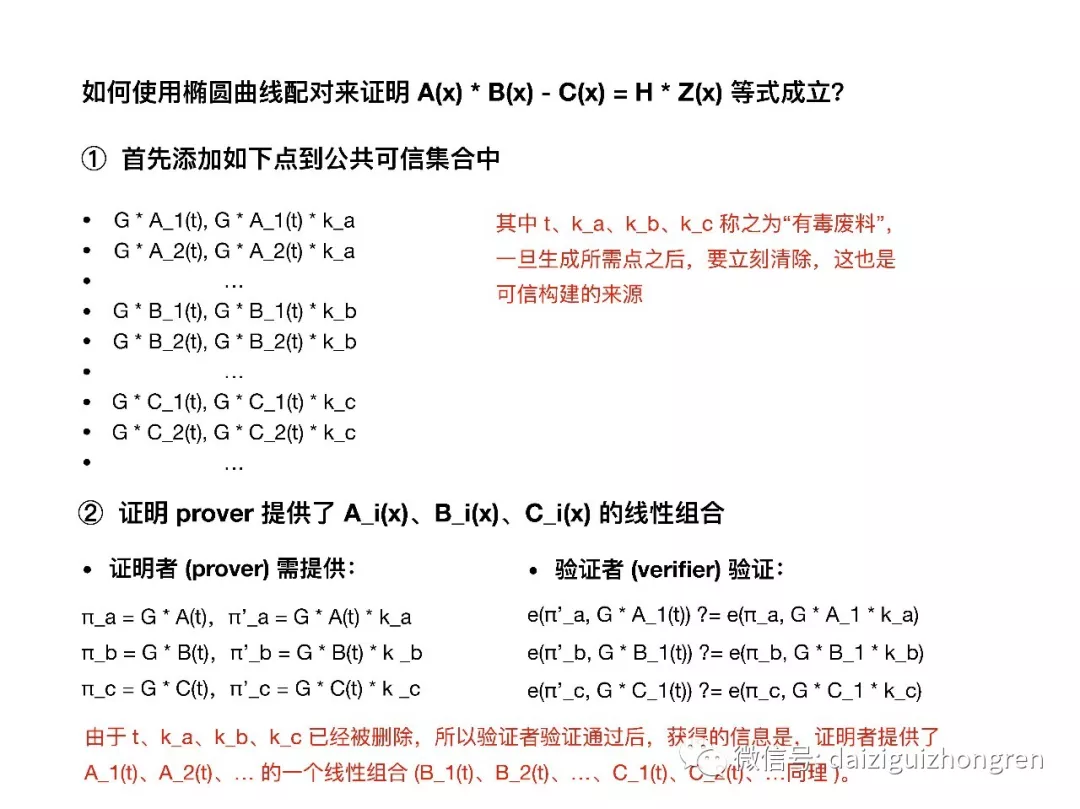
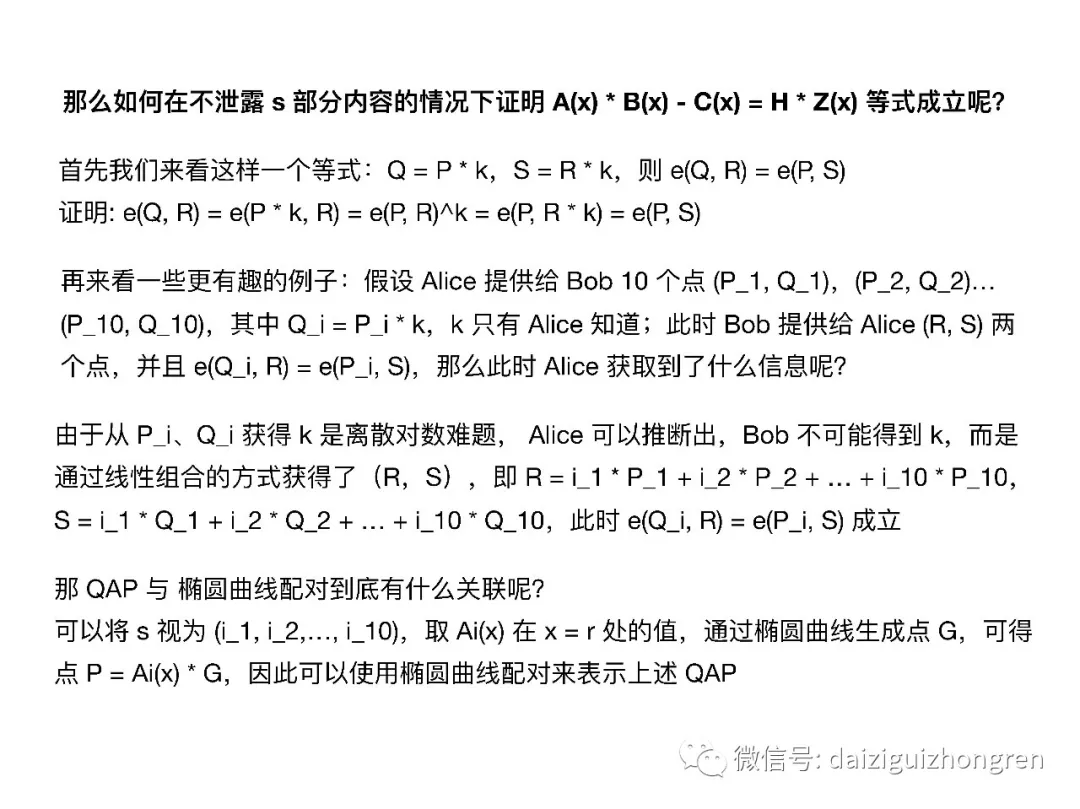
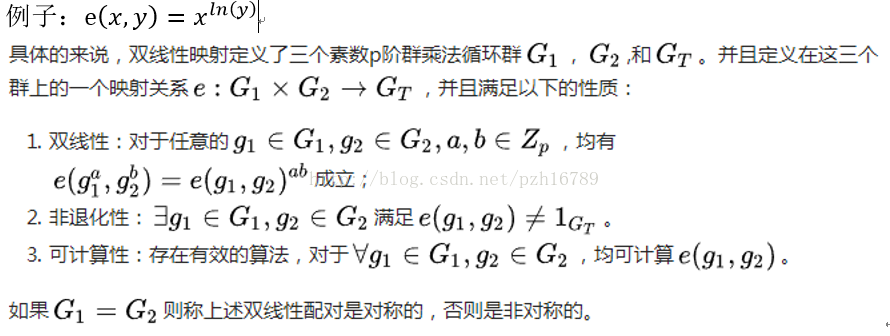


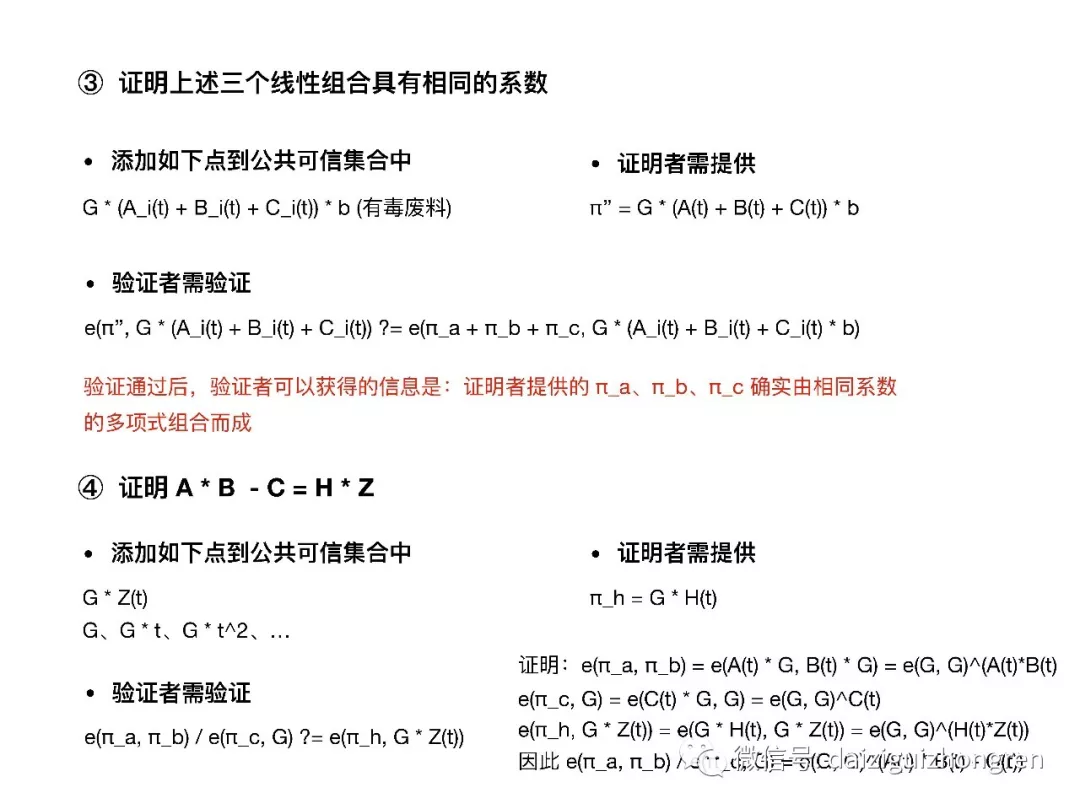












## 3隐私保护方案

### 3.1 同态hash加密方案

