接下来由我来介绍我们组的选做题——零知识证明，负责这部分的组员还有曹越、张万里、姚子晨和李新。

我们将从背景介绍、数学原理、协议举例三个方面展开。

首先是背景介绍

（第一页从这里开始）（黑字均为ppt原文，蓝字为额外/简化文案）

（第一页）零知识证明，它指的是证明者能够在不向验证者提供任何有用的信息的情况下，通过多轮交互，使验证者相信某个论断是正确的。

零知识证明包含有两层含义，首先是对某个命题或声明的交互证明，其次要求证明是“零知识”，要求除了命题本身的真假外，验证者不能获得任何其它额外的知识。零知识证明实现了两个似乎完全矛盾的任务,且零知识属性不会随着使用而退化，这可能是它在实践中最吸引人的地方。

我们通过一个例子来感受一下，Alice知道打开CD之间密门的咒语。她想对Bob证明这一点， 但她不想泄露咒语。

（第二页）那么他们可以这样验证：首先，bob站在a点，alice一直走进洞穴，到达点C或点D。在Alice消失在洞穴中之后，Bob 走到点B。 Bob向Alice喊，要她从左或右通道出来。Alice答应条件，如果有必要她就用咒语打开密门。 重复以上步骤n次。如果alice每次都能正确走出，那么bob可以相信alice掌握咒语。

（第三页）接下来是数学原理部分。

我们将分别介绍交互式零知识证明和非交互式零知识证明。

（第四页）前面的例子就是一次典型的交互式零知识证明。我们将交互式零知识证明协议三个基本属性用较为通俗的语言描述如下：

完备性：只要证明者P拥有相应正确知识，就能够通过验证者V的验证，即P有足够大的概率使V确信。

可靠性：如果证明者P没有相应正确知识，则无法通过验证者V的验证，即P成功欺骗V的概率可忽略。

零知识性：证明者P在交互的过程中仅向验证者V揭露其是否拥有相应正确知识，而不会泄露任何关于知识的额外信息。

在前面的示例中，如果Alice拥有打开密门的知识，则Alice每次都会从正确的通道中走出，这称为完备性。如果Alice不具备打开密门的相关咒语，则Alice有不小的概率无法从正确的门走出，这称为可靠性。在此协议中，Bob无法得知开门的咒语，这称为零知识性。

零知识证明协议的一般结构分为四个阶段，分别是提供承诺、发起挑战、回应挑战、验证回应后决定通过验证或发起下一次挑战。可以通过控制循环次数降低欺骗成功的概率。

我们就之前的例子，进行16次循环验证，可以看到，欺骗成功的概率非常的低。我们还给出一个形而上的零知识性证明，假设alice也不知道口令是什么，他每次都通过时光机按照bob的要求修改自己的选择，那么我们可以得到<==。

==============================================================

（第五页）交互式零知识证明协议依赖于验证者的随机尝试，需要证明者和验证者进行多次交互才能完成，效率较低。非交互式零知识证明将交互次数减少到一次，可实现离线证明和公开验证。可以运用在区块链等零知识证明应用场景中。

下面同样用一个例子来理解非交互式零知识证明。

Alice为了向Bob证明他已经解决了一个数独难题，为此Alice创建了一个防篡改的机器。Alice将生成好的数独答案放入到机器中，机器可以向Bob发送证明。机器遵循以下公开可验证的协议：

首先，Alice在机器中放入尚未被解决的原始数独题目，数独中的谜题卡片三张正面朝上。

（第六页）接下来，Alice上机器将他的答案正面朝下放置在相应的单元格上。最后Bob向机器获取证明，机器返回给Bob27个袋子，袋内分别是每行、每列、每个九宫格所包含的数字的卡片。Bob分别对这27个袋子进行检查，如果每个袋子中的卡片都包含数字1到9，而且没有任何数字丢失或重复，那么Bob可以确认Alice的确解开了数独，并且Bob并没有从机器返回的证明中获取任何关于数独解的知识。

下面我们以三色地图问题这一个典型的例子，来帮助大家直观感受什么是零知识证明。

三色地图问题，用三种颜色给一个地图染色，来保证任意两个相邻的地区都是不同的颜色。

可以将这个「三色地图问题」抽象为一个「将连通图的各个顶点进行三染色的问题」。

下面我们设计这样一个交互协议：

Alice在这个协议里扮演的身份是证明者，她掌握着地图三染色的一个特解，而且要在不暴露自己手中的地图染色方案的前提下，使验证者Bob认识到自己掌握着这样的一个解。

Bob在这个协议中扮演的身份是验证者，他的任务是通过有限轮数的交互，探测出Alice是真的持有一份三染色的方案，还是她做了弊，手中的方案并不能满足任意两个相邻的地区都是不同的颜色。

那么Alice如何才能既不泄露她的染色方法，同时又能向Bob证明她知道染色方法？

下面我们通过六个步骤来了解一下Alice的解决方法：

————————翻页————————

（从此处开始，可以照着PPT直接读，PPT的文字已经精简化、通俗化了）

第一步：

Alice先要对她所掌握的三染色地图进行一些「变换」，把颜色做一次代换。

由此，Alice便得到了一个新的三染色答案。

此时她把新的图中的每一个顶点都用纸片盖上，然后出示给Bob看。

————————翻页————————

第二步:

Bob随机挑选一条「边」，然后告诉Alice。

————————翻页————————

第三步:

Alice揭开边两端的纸片，让Bob检查，Bob发现这两个顶点的颜色确实是不同的，那么Bob认为这一次检验通过。

这时候，Bob只看到了图的局部，也许Alice并没有掌握三染色的答案（知识），而只是她编造的答案中，刚好这两个顶点颜色不同呢？

————————翻页————————

第四至六步，这里其实是一个循环执行n次的操作:

Bob为了验证Alice是否真的掌握了知识，可以重复多次进行前面的操作：

Alice再做一次颜色代换，并把所有的顶点盖上纸片。Bob再次挑选一条边，然后让Alice揭开纸片验证。

————————翻页————————

那么我们来关注一下这个例子中的两个重点：

首先是Alice作弊成功的概率，也就是说是否能满足“证明”。

经过n轮之后，Alice成功作弊的概率为：

Pr[(G,c)||ThreeColor(G,c)=0]<(1−1/|E|)^n

也就是说，假设Alice编造的答案非常“高明”，仅有一条边不能满足两端的节点异色，也就是说在一个|E|条边的图中，在一次抽选检测中Alice仅有1/|E|的概率会被Bob识破。那么在n轮检测之后，Alice成功作弊的概率为(1−1/|E|)^n。然而实际上，Alice编造的答案很难做到如此高明，因而作弊成功的概率Pr<(1−1/|E|)^n。

如果n足够大，如n=128,这个概率Pr会变得非常小，以至于可忽略。

————————翻页————————

其次是Bob是否获取了知识，也就是说是否能满足“零知识”。

Bob每次看到的局部染色情况都是Alice变换过后的结果，无论Bob看多少次，都不能拼出一个完整的三染色答案出来。实际上，Bob在这个过程中虽然获得了很多「信息」，但是这就好比Alice发给Bob一堆随机数一样，没有获得真正的「知识」，也即，没有获得可以帮助Bob直接破解Alice秘密的能力。

————————翻页————————

由三色地图问题这一典型的例子可见，「知识」这个词的定义与验证者的计算能力相关，如果在零知识证明交互的过程中，验证者所获得的信息并不能增加其对于证明者的秘密的直接破解能力，那么这一过程中传递的信息不能被称为「知识」，也即，交互过程是零知识的。

交互式零知识协议只能取信于一个验证者，非交互式零知识证明（NIZK ），如果存在，非交互式零知识可以取信于多个验证者，以至所有人。非交互式零知识证明（NIZK ），如果存在，要比交互式证明强大得多，因此非交互式零知识证明现今很流行（如比特币、区块链）。下面简单介绍两种交互认证协议，一种非交互协议。

Schnorr协议：首先用户A和验证方B获取系统参数（p,q,β）（选取素数p，使p-1可以被素数q整除，β为乘法阶为q的生成元），用户A选择唯一身份和私钥a，并且计算*ν =* mod p)作为公钥，然后A通过传统方式（如出示证件等）向T验证身份，将公钥*ν*给T，最终获得由T签发的和*ν*绑定的证书，在这个过程中，可信任的第三方机构T向双方发布可以验证公钥的函数（可以验证对消息m的签名）。

之后A可向B验证身份，首先A选取随机数r，并计算x ≡ ，将（，x）发送B，然后，B在验证证书中公钥的真实性后，发送一个从未使用过的随机数e给A进行提问,A接受到e后，计算y ≡ a ∙ e + r ( mod p)发送给B，最后B计算z ≡ ∙ ，如果z=x，则B接受A的身份。

（贴了举例）

GQ协议：首先仍是系统参数选取，第三方T选取RSA型素数p和q，并产生n=p\*q，然后T选取一个公钥*ν*，并通过RSA加密算法计算出私钥s，然后向所有用户颁布（*ν，*n），其次是用户参数A获取身份，然后计算=f(，其中f是一个公开的冗余函数，之后T将保护私钥信息的数据 ≡交给A，之后协议可以执行交互，流程与上一个流程基本相同，值得注意的是最后B验证是z不可为0（防止攻击者选取随机数r=0）

（贴了举例）

Fiat-shamir变换: Fiat-shamir变换最早来自于1986年的来自于 Amos Fiat 与 Adi Shamir发表的美密会论文,对于任意的 「Public-Coin 协议」，都可以用 Fiat-Shamir 变换来把整个协议「压缩」成一步交互，也就是一个非交互式的证明系统。PPT上是一个例子，对比来看是将A要发送的信息一次性全部发送，将B需要提问的信息换为一个由公钥和共同已知的R构成的哈希值。

优缺点：（看情况，直接说）

