零知识证明的分层次案例化教学设计*

张艳硕 李泽昊
北京电子科技学院,北京市 100070

摘 要:零知识证明,指证明者能够在不向验证者提供任何有用的信息的情况下,使验证者相信某个论断是正确的。它在网络技术高速发展的当今社会发挥着重要作用,目前已广泛应用于数据的隐私保护、身份认证、去中心化存储、区块链、数字金融等领域,在未来的应用或将更加广泛。本文旨在提出零知识证明的分层次案例化教学设计,给出针对不同层次与水平的零知识证明教学设计,由浅入深,用简单有趣的例子去讲解零知识证明,让更多不同层次的人群了解并掌握零知识证明技术及其应用。

关键词:零知识证明;分层;案例;教学设计
中图分类号:TN918.1-4 文献标识码:A 文章编号:1672-464X(2020)4-92-10

1 引言

零知识证明(Zero—Knowledge Proof)[1],是由 S.Goldwasser、S.Micali 及 C.Rackoff 在 20 世纪 80 年代初提出的。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,使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议,即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息,但证明过程不能向验证者泄漏任何关于被证明消息的信息。大量事实证明,零知识证明在密码学中非常有用。如果能够将零知识证明用于验证,将可以有效解决许多问题。

零知识证明的思想被广泛运用在密码学和区块链领域,Zcash[2]是首个使用零知识证明机制的区块链系统,它可提供完全的支付保密性,同时仍能够使用公有区块链来维护一个去中心化网络。著名的比特币交易系统就利用了此原理。如今区块链技术与信息安全技术高速发展,零知识证明在未来更是有着广泛的运用。

由此可见,让更多不同层次和水平人群了解零知识证明,理解其基本概念和原理是必要的,这有助于人们了解这项技术,也可以以此产生更多了解此技术的人才。本文旨在提出零知识证明的分层次案例化教学设计,针对不同层次和水平人群提出不同的零知识证明案例化教学设计,由浅入深,用简单有趣的例子去讲解零知识证明,让不同层次和水平人群更好地了解零知识证明,为零知识证明的普及和科学研究打下基础。

* 基金项目:北京电子科技学院 2018 年教研基金“精研密码新型技术,助力密码学科竞赛”和 2020 年教育部新工科项目“新工科背景下数学课程群的教学改革与实践”教育部信息安全一流专业建设点项目资助

** 作者简介:张艳硕(1979—),男,副教授,博士,从事密码数学理论研究.Email:zhang_yanshuo@163.com;李泽昊(2000—),男,本科在读,信息安全专业.Email:969493466@qq.com。

2　零知识证明

2.1　零知识证明的发展历程

零知识证明发源较早，早在 16 世纪的文艺复兴时期，意大利有两位数学家为竞争一元三次方程求根公式发现者的桂冠，就采用了零知识证明的方法。在漫长的历史中，零知识证明的概念逐渐清晰，应用也越来越多样化。近年来，电子计算机和网络技术高速发展，零知识证明的思想变得更加受到重视，零知识证明的应用范围也更加广泛。未来零知识证明或将有更多发展和更加广阔的应用空间。

2.2　零知识证明的定义与性质

零知识证明[1]，指证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。在有必要证明一个命题是否正确，又不需要提示与这个命题相关的任何信息时，零知识证明系统(也叫做最小泄露证明系统)是不可或缺的。零知识证明系统包括两部分：宣称某一命题为真的示证者(Prover)和确认该命题确实为真的验证者(Verifier)。证明是通过这两部分之间的交互来执行的。这种思想源自交互式证明系统[3]。在零知识协议的结尾，验证者只有当命题为真时才会确认。但是，如果示证者宣称一个错误的命题，那么验证者完全可能发现这个错误。

零知识证明(Zero—Knowledge Proof)起源于最小泄露证明[4]。设 P 表示掌握某些信息，并希望证实这一事实的实体，设 V 是证明这一事实的实体。假如某个协议向 V 证明 P 的确掌握某些信息，但 V 无法推断出这些信息是什么，称 P 实现了最小泄露证明。不仅如此，如果 V 除了知道 P 能够证明某一事实外，不能够得到其他任何知识，称 P 实现了零知识证明，相应的协议称作零知识协议。

在最小泄露协议中零知识证明需要满足下述三个性质[4]：

(1)正确性。P 无法欺骗 V。换言之，若 P 不知道一个定理的证明方法，则 P 使 V 相信他会证明定理的概率很低。

(2)完备性。V 无法欺骗 P。若 P 知道一个定理的证明方法，则 P 使 V 以绝对优势的概率相信他能证明。

在零知识协议中，除满足上述两个条件以外，还满足下述的第三个性质。

(3)零知识性。V 无法获取任何额外的知识。

将性质(1)和(2)称为零知识证明的正确性和完备性，而性质(3)称为零知识性。

2.3　零知识证明的重要性

数据隐私是当今社会最重要的课题之一。保护与个人身份有关的各种各样的个人资料极为重要，并会不断增加其重要性。当今时代网络技术不断发展，收集，传输和记录数据的难度和成本大大降低，这造成隐私的泄露可能大大增加。某些服务商在提供服务时也以用户提供某些数据作为前提，但这也加重了隐私泄露的风险。零知识证明或可能在未来成为解决隐私泄露的方案。

零知识证明还被广泛应用于多个领域，如据的隐私保护、身份认证、去中心化存储、区块链、数字金融等，并且未来应用或更加广泛。由此可见，掌握零知识证明的原理和应用就显得格外重要。

3　零知识证明的现行教学设计及其不足

零知识证明的现行教学设计大致是通过正规专业课程进行，通过信息学与计算机专业知识进行讲解。其内容较为复杂，涉及较多方面的专业知识，如数学，信息学，计算机科学等，专业性强较难理解。主要通过专业理论知识对其概念和原理进行讲解，然后讲解其在各领域的详细应用过程。

类似于以上教学设计，专业性较强，较难理解，也较为枯燥。对于较低水平学生，无法很好地起到教学科普的作用。对于非本专业学生，也不能留下深刻印象，无法达到较好的教学目的。

零知识证明属于数据安全领域，其现行教学设计有较大缺陷，其教学难度不易控制[5]。零知识证明是信息与计算科学专业、计算机应用与技术、信息安全等专业的教学内容。其应用内容有一定的难度，对于没有学过相关知识的非专业学生来讲，随着教学的深入，会感到不容易接受。因此在教学内容的编排上，必须要考虑到学生的理解和接受程度。同时，由于零知识证明涉及密码学，其涉及面广泛，若要深刻地理解零知识证明，要求有较高的数学基础和逻辑思维能力。

对于不同阶段的理工科大学生群体，必须合理地组织教学内容，教学难度和深度。并采用灵活丰富的教学手段，用较为有趣的案例进行教学。这样能够突出重点、建立基础，并能形成体系，为进一步的扩展提供契机。

对于大学理工科新生，他们也需要学习和了解相关密码知识。将零知识证明讲解清楚，可以充分发挥科普的优势，这也为密码知识的不断发展提供动力和源泉。讲好零知识证明及其应用也能为他们未来对密码技术有更好的理解。

4 针对不同学习阶段的教学设计

零知识证明相关的知识深度和广度较高，应用广泛，要深入理解难度较高，但其概念简单，易于理解，对于不同阶段和专业的大学生可以利用不同的教学设计，使不同阶段和专业的学生对零知识证明的概念及其应用有不同程度的掌握。下面将分不同学龄和专业层次，通过给出实例的方式，介绍不同的零知识证明教学方案，让不同阶段和知识水平的学生了解零知识证明的概念和相关应用。

4.1 针对大学工科类专业新生的教学设计

此阶段新生逻辑思维和数学基础较为薄弱，但能对事物产生兴趣，对于此阶段学生可以着重通过有趣的例子进行讲解，使其基本了解零知识证明的概念。

下面给出两种可行的教学设计，分别基于故事和游戏，可根据实际情况和学生的能力及学习程度选择合适的教学设计进行教学。

4.1.1 基于故事的教学设计

首先介绍零知识证明的概念基础，提出问题，让学生产生兴趣，可以引用阿里巴巴与四十大盗的童话故事，提如下问题:

阿里巴巴被强盗抓住了，强盗向他索要开启山洞大门的咒语。此时阿里巴巴面临一个问题，如果把密码告诉强盗，自己就没有利用价值了，可能被强盗杀死。如果不告诉强盗咒语，强盗以为自己不知道咒语，还是可能被杀。怎么能做到让他们相信自己确实知道咒语，但又不让他们知道咒语是什么?

着重强调阿里巴巴不能让强盗知道咒语这一点，即不能泄露任何有价值的信息这一点，这样就着重强调了零知识证明的概念精髓。学生充分思考后，可以给出以下答案作为参考:

阿里巴巴对强盗头领提议，让强盗和自己离开一定的距离，但又能互相看到，强盗举起双手后，阿里巴巴就念咒语开启山洞大门，当强盗把双手放下后，阿里巴巴就念咒语关上山洞大门，如果阿里巴巴逃跑，强盗就用弓箭射死他。对于强盗头领来说，这显然可以接受。对于阿里巴巴，他没有泄露开门的咒语，但是证明了自己知道咒语。这样，阿里巴巴在没有告诉强盗头领开门咒语的情况下，又向强盗证明了自己确实知道开门咒语。

最后再次强调零知识证明的概念，并可以让学生在日常生活中尝试使用零知识证明，以更加熟练零知识证明的概念。

4.1.2 基于游戏的教学设计

还可以用数独游戏让学生更深切地体会零知识证明的应用方法:

首先介绍规则: 数独[6] 是一种运用纸、笔进行演算的逻辑游戏。玩家需要根据 9×9 盘面上的已知数字,推理出所有剩余空格的数字,并满足每一行、每一列、每一个粗线宫(3* 3) 内的数字均含 1-9,不重复。然后先进行示例,再让同学们练习数独,找到乐趣,然后继续游戏,让同学们两人一组,互相出数独题目,并解答。

若无法解答则会产生疑问: 可能对方出的题目本身就是无解的。

这时提出疑问: 如何向同伴证明自己出的数独题目有解,但又不泄露答案呢?

设小明是证明者,小红是验证者,小明做好很多数字卡片,在桌面上将谜面的数用正面摆放,谜底的数用反面摆放。

小明问小红,要验证哪一种,是行(row) ,列(column) 还是 3* 3 的方格(box) 。

小明按照小红的话,将每一行或列或九宫格的所有卡片放入不透明袋子中,打散交给小红。(如图 1)

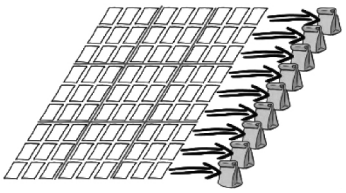

图 1　将卡片放入袋子

小红打开,看到每个袋子中都正好是 9 张 1-9 的卡片(如图 2) 。

图 2　拿出卡片并验证

因为是小红选择的标准,所以一定程度上证明是可信的,如果小红不相信,则再反复几次,继续由小红决定,换不同的行,列,方格进行验证。这个例子中,小明没有向小红透露数独的解,但是足以证明该数独题目是有解的,自己并没有捉弄小红。

通过这样的体验,学生就可以大致了解通过零知识证明的原理来证明自己的数独题目有解,在游戏和实验中体验零知识证明的趣味性。

讲解的过程,可以注意以下几点:

第一是充分吸引学生学习的兴趣。通过讲解简单生动的案例,充分吸引学生的学习兴趣,为未来对学生相关领域的深入学习和研究打下基础。

第二是讲解要生动,不宜过难。对于工科类新生,教学到了解零知识证明的相关定义即可,若无法深入理解,可不必继续后面的案例和零知识证明的深层次应用等内容。

4.2　针对大学理科类专业新生的教学设计

此类型学生对于数学知识和逻辑思维有较好的基础,但并不具备深入学习的条件,此时可以举出与数学和科学家的故事,在科普零知识证明的同时,加强对数学等科学的学习兴趣,使学生们未来更好地对有关领域进行学习,锻炼逻辑思维,让学生产生兴趣的同时理解零知识证明。

下面给出两种可行的教学设计,分别基于历史史实和经典数学证明,可根据实际情况和学生的能力及学习程度选择合适的教学设计进行教学。

4.2.1　基于历史史实的教学设计

步骤 1: 通过介绍历史史实[7] ,介绍数学家,提出以下问题。

意大利有两位数学家为竞争一元三次方程求根公式发现者的桂冠,数学家塔尔塔里雅和菲奥都宣称自己掌握了这个求根公式,为了证明自己没有说谎,又不把公式的具体内容公布出来(可能在当时数学公式也是一种技术秘密) ,应该怎样做呢?

步骤 2: 学生进行思考后给出以下史实:

双方各出 30 个一元三次方程给对方解,谁能全部解出,就说明谁掌握了这个公式。比赛结果显示,塔尔塔里雅解出了菲奥出的全部 30 个

方程，而菲奥一个也解不出。于是人们相信塔尔塔里雅是一元三次方程求根公式的真正发现者。在这个案例中，知道一元三次方程解法的数学家就在没有泄露任何信息的情况下，证实了自己拥有方程的解法。

4.2.2 基于经典数学证明的教学设计

若有条件且学生理解能力较强，还可以给出思考题目，证明以下定理：

定理[8]：无理数的无理数次方可以是有理数。

给出提示：使用简单的实例，运用零知识证明的方法隐藏证明过程某些数是有理数还是无理数的性质。

一个可行的经典证明方法如下：设 $A=\sqrt{2}^{\sqrt{2}}$。可得 $A^{\sqrt{2}}=2$。2 是有理数，而 $\sqrt{2}$ 是无理数。若 A 是有理数，则原命题得证，若 A 为无理数，则因为 $A^{\sqrt{2}}=2$，命题也能得证。

在此案例中，并不知道 A 究竟是有理数还是无理数，但是同样完成了证明。因为不管 A 是有理数还是无理数，都可以得到无理数的无理数次方可能是有理数这样的结论。即在隐藏了 A 是什么数的情报的条件下，也成功让题目得到证明，这也是零知识证明的一个例子。

讲解时可以着重讲解 A 的重要性，即并不知道 A 是有理数还是无理数，但是仍然可以让最后命题得到证明，即隐藏了 A 是有理数还是无理数这一事实。可以借此加深学生对零知识证明的关键概念的理解，即在不泄露任何有价值信息的情况下进行证明这一点。

通过这样的讲解和示例运用，能够较好地让学生了解零知识证明的简单原理和用法。鼓励学生在未来的生活与学习中灵活运用零知识证明，达到学以致用的目的。

4.3 针对大学高年级本科生的教学设计

针对高年级本科生，可以用较为正式的案例讲解零知识证明的概念，然后通过几个其他案例，让有此类学生深入了解零知识证明与普通证明的区别。

引用简单经典的零知识证明的例子和应用。

有一个缺口环形的长廊，出口和入口距离非常近（在目距之内），但走廊中间某处有一道只能用钥匙打开的门，A 要向 B 证明自己拥有该门的钥匙（如图 3）。采用零知识证明，有以下方法：B 看着 A 从入口进入走廊，然后又从出口走出走廊，这时 B 没有得到任何关于这个钥匙的信息，但是完全可以证明 A 拥有钥匙。

此示例简单明了，很好地讲述了零知识证明的原理和定义。

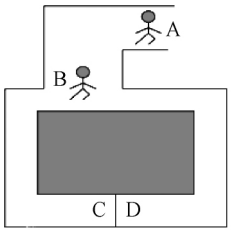

图 3 环形走廊

高年级本科生具有较强的逻辑思维能力和辨别能力，可以让此类学生对以下几个例子进行辨析，对照哪个是零知识证明，哪个是普通证明。

（1）A 要向 B 证明自己拥有某个房间的钥匙，假设该房间只能用钥匙打开锁，而其他任何方法都打不开。这时有 2 个方法：

①A 把钥匙出示给 B，B 用这把钥匙打开该房间的锁，从而证明 A 拥有该房间的正确的钥匙。

②B 确定该房间内有某一物体，A 用自己拥有的钥匙打开该房间的门，然后把物体拿出来出示给 B，从而证明自己确实拥有该房间的钥匙。

后面的②方法属于零知识证明。A 在 B 始终没有看到钥匙的情况下完成了证明。

（2）A 拥有 B 的公钥，A 没有见过 B，而 B 见过 A 的照片，偶然一天两个人见面，B 认出了 A，但 A 不能确定面前的人是否是 B，这时 B 要向 A 证明自己是 B，也有 2 个方法。

① B 把自己的私钥给 A，A 用公钥对某个数

据加密，然后用 B 的私钥解密，如果正确，则证明对方确实是 B。

② A 给出一个随机值，并使用 B 的公钥对其加密，然后将加密后的数据交给 B，B 用自己的私钥解密并展示给 A，如果与 A 给出的随机值相同，则证明对方是 B。

第②中方法属于零知识证明。B 没有泄露自己的私钥，但完成了证明。

由浅入深给出例子，让学生了解到更多更加实际的运用场景并进行分辨，加深其理解，激发其学习和研究的兴趣。

还可以进一步讲解目前零知识证明运用的方方面面，以及每天都会遇到的一些事物上。介绍一些最新的零知识证明的运用场景，如最新的区块链，虚拟货币。让其了解零知识证明在未来的作用。

5　零知识证明在应用中的分层次案例化教学

零知识证明的运用较为广泛，其在数据的隐私保护、身份认证、去中心化存储、数字金融等很多方面被广泛运用，并且未来很可能有更多应用的可能。依靠零知识证明，可以在对方无法知晓自己任何隐私的基础上，证明自己拥有一定的情报。

对于大学本科生和研究生，可以先用上文的方法讲解零知识证明的概念，进而对零知识证明的相关应用进行讲解。

5.1　针对大学工科类专业新生的教学设计

针对此类学生，可以设计较为贴近生活又简单明了的案例来进行教学设计，让这类学生更加了解零知识证明的基本概念和一些简单的应用，以及零知识证明与网络与信息技术，区块链，虚拟货币等最新技术的联系，达到教学目的。

提出以下问题：非色盲向色盲患者证明自己不是色盲？思考后，可做以下解答[9]：

假设 A 有一个红球和黄球，她的一个色盲朋友 B 并不相信 A 的球颜色不同。A 把两个球给 B，B 每只手拿一个球，然后 A 转过身背对 B，B 抛一枚硬币，如果正面朝上，则保持不动，否则交换左右手的球。A 转过身，B 问 A 是否交换过球。如此重复多次，如果 A 都回答正确，则 B 相信这两个球是不同颜色的，A 并不是色盲。

此时应该强调此案例与零知识证明的联系：B 是色盲，并不能真正取得球的颜色这一信息，但是通过让 B 知道，交换球后 A 是可以判断的这一事实的方式，向 B 证明了自己不是色盲，而零知识证明也是如此：隐藏有价值的信息不让对方知晓，但是也证明了自己拥有这些的信息。

此后还可以介绍一些最新的零知识证明的运用场景，如最新的区块链，虚拟货币。让学生了解零知识证明在未来的作用。要注意介绍应用场景应该仅限于介绍应用的方面，只要贴近生活，生动易懂即可，不必深入理解其深层原理。

5.2　针对大学理科类新生的教学设计

此阶段学生可以在理解零知识证明的概念后继续了解简单的应用实例，可以用现阶段流行的区块链技术作为案例进行教学。

先讲解零知识证明的概念，然后讲解零知识证明在区块链，比特币网络中的应用。

Zcash 网络是一个可行的案例，可以给出这样的例子：

在比特币网络中，用户需要将交易明文广播给所有矿工，由他们来校验交易的合法性。但是基于隐私的考虑，不能把交易的具体内容公布出来。

Zcash 实现了隐私交易，作为首个使用零知识证明机制的区块链系统，它可提供完全的支付保密性，同时仍能够使用公有区块链来维护一个去中心化网络。Zcash 交易自动隐藏区块链上所有交易的发送者、接受者及数额，只有那些拥有查看密钥的人才能看到交易的内容，用户拥有完全的控制权，他们可自行选择向其他人提供查看密钥。

用以下示例讲解其详细原理:

王五要向赵六转 1BTC,此时王五拥有一张 1BTC 的支票,要转账给赵六时,先给赵六新建一张 1BTC 的支票,这时王五和赵六都有了一张支票。这两张“支票”都是有效的。王五的支票开始就存在于整个 Zcash 网络,赵六的支票在生成后也会被广播到全网。为了隐藏交易者信息,要对两张支票进行加密处理,两张支票都隐藏了持有者(王五、赵六)的名字。同时,因为资产只能有一份,所有矿工手里还有一个作废列表。王五要同时广播自己的“支票代号”,录入作废列表中。其中王五的支票是原先存在的,王五的支票代号 R1 和赵六的支票是在交易过程中被王五广播的。

矿工们能获取的信息相当有限,但是这并不影响矿工对交易有效性的判断。

判断的逻辑如下[10]:矿工拿到王五给的支票代号 R1,去作废列表中检索,假如作废列表中已经存在 R1,则证明 R1 所对应的支票早已失效;若作废列表中并不存在 R1,则证明 R1 对应的支票仍旧有效,此时矿工把 R1 录入作废列表中,把新生成的支票录入支票列表中。所以记账的过程就是对原有支票登记失效,并存入现有支票的过程。

在此过程中,可以发现,每笔交易矿工能接收到的东西只有一个支票代号,和一张新的支票,而且这两样东西都是被加密的。所以矿工并不知道转账双方是谁,也不知道转账金额是多少。

通过以上案例,学生对零知识证明在区块链和比特币网络中的应用就会产生一些理解,将零知识证明的概念和当下较为流行的应用联系,有助于更好地让学生了解零知识证明。

要注意几点:不必完全清晰地还原零知识证明在区块链,虚拟货币网络中的完整运用,只需介绍其大致原理。本阶段学生只需大致理解即可。在讲解的同时,可以扩展一些区块链的知识,涉及零知识证明,也可以多介绍一些零知识证明的运用方面。目的是让学生了解零知识证明在一些新兴网络与信息技术中的普遍性与重要性。

5.3 针对大学高年级本科生的教学设计

在学会生了解零知识证明的概念后,可以为此阶段学生讲解另一新兴领域中零知识证明的运用。

即零知识证明在安全多方计算中的作用。

步骤 1:讲解安全多方计算的概念。

安全多方运算指一组参与者希望共同计算某个约定的函数,函数的输入参数有多个,每个参与者提供函数的一个输入;每个人都知道这个函数返回的值,但不知道其他参与者输入的信息。在安全多方计算中,每个参与者都需要证明自己参与运算的数据是真实的,但又不能泄露自己的信息,这就运用到了零知识证明。

步骤 2:举出姚氏百万富翁问题[11] 作为一个可行案例如下。

两个百万富翁 Alice 和 Bob 相遇,设 Alice 有 i 元,Bob 有 j 元,他们希望知道谁更有钱,但是出于隐私,都不想让对方知道自己到底拥有多少财富,如何在不借助第三方的情况下,如何达成比较?

步骤 3:学生思考后给出以下简化的解决流程。

先把问题简化,假如 i 和 j 是 1 到 10 之间的数。

(1) 首先 Bob 挑选一个非常大的整数 x,然后用 Alice 的公钥 a 加密。得到 $k = Enc(x)$;

(2) Bob 把 $k - j + 1$ 发给 Alice;

(3) Alice 拿到这个数后,计算以下这些数:

$Dec\{k-j+1\}, Dec\{k-j+2\}, \cdots, Dec\{k-j+10\}$

然后除以一个素数 p 取余得到:

$z_1 = Dec\{k-j+1\}(modp), z_2 = Dec\{k-j+1(modp)\}, \cdots, z_{10} = Dec(k-j+1)(modp)$

(4) Alice 的钱是 i，那么 Alice 做以下计算:

$z_1 = z_1, z_2 = z_2, \cdots, z_i = z_i, z_{i+1} = z_{i+1} + 1, \cdots, z_{10} = z_{10} + 1$

(5) Alice 把这串数字发给 Bob。

Bob 只需看第 j 个数字，如果等于 $x(modp)$ 就说明 $i \geq j$ 否则说明 $i < j$. 然后 bob 把结果返给 Alice。

在以上实例中，Bob 和 Alice 都不知道对方具体的财产是多少，但是却得知了到底谁的财产更多。这个实例应用零知识证明隐藏了对方的具体财产，但也可以保证最终的比较结果是正确的。

讲解过程可以借助姚氏百万富翁问题作为实例，用较为生动的语言让学生理解零知识证明在安全多方运算中的运用，让学生体会到零知识证明的神奇之处。注重应用，可以让学生对姚氏百万富翁问题进行验证。注意将理论与实际相结合，即结合零知识证明的概念与本例中的现实运用，突出趣味性，激发学生深入学习的兴趣。

5.4　针对大学研究生阶段的教学设计

在了解零知识证明基本概念后，讲解 zk-SNARKs 网络的基本原理。

步骤 1: 讲解 zk-SNARK 的基本含义和概念。

zk-SNARK 是“zero knowledge Succinct Non-interactive ARgument of Knowledge”的缩写，即简洁非交互式零知识证明。zk-SNARK 是一种较为简单、易操作，无交互的零知识证明技术。

进而讲解一些区块链中使用 zk-SNARKs 的案例，如 Zcash 网络的基本实现和原理，以便学生更好理解 zk-SNARKs 网络中的零知识证明运用和原理。

若学生学习能力较高，逻辑思维和理解能力较强，则可以较为详细地举出 zk-SNARK 的具体实现原理，相关知识和实例，以达成案例化教学的目的。

步骤 2: 可进行对 zk-SNARKs 进行如下讲解。

比特币和以太坊网络都使用公共地址来代替验证者和证明者的真实身份，使得交易部分匿名; 只有发送和接收地址，以及交易数量是公众知道的。但是，通过区块链上提供的各种信息，如交互记录等，可以发现地址的真实身份，存在隐私暴露的隐患。

用了零知识证明之后，发送方、接收方和第三方的细节信息可以保持匿名，同时保证交易有效。

最早使用零知识证明技巧的区块链叫做 Zcash，实际的做法叫做 zk-SNARKs，这是许多零知识证明的做法之一，也是最有名的一个。

zk-SNARKs[12] 是“零知识简洁无交互知识认证”的简称，是一种在无需泄露数据本身情况下证明某些数据运算的一种零知识证明。

zk-SNARKs 技术缩减了证明所需的时间和验证它们所需的计算量。它能够证明有效交易的条件已经满足，而不需要透露交易所涉及的地址或交易量的任何关键信息。

Zcash 可以将交易纪录上的汇款者、收款者和金额都经过加密隐藏起来，因此矿工无从得知这些交易上的细节，但仍然可以验证交易。不过，目前多数使用者在 Zcash 上的交易，还是选择未经加密的作法，因为花费的成本比较高。

另外，以太坊(Ethereum) 上的智能合约目前也已经可以运用 zk-SNARKs 这套零知识证明的作法。但以太坊不完全是从隐私的角度切入，而是从节省运算成本的角度应用零知识证明。

透过 zk-SNARKs，以太坊矿工可以不用再重新执行交易的运算，而是只要对方提得出证明即可。就像一个人不需要真的知道另一个人是否会高一到高三的数学，而只要看到高中毕业证就能确定他懂高中数学。不过，这只有在制作证明的成本，远低于实际运算成本的情况下才划算。

zk-SNARKs 将需要验证的交易内容转化为两个多项式乘积相等的证明，并结合同态加密等高级技术，在执行事务验证的同时保护隐藏的事

务量。其过程可简单描述为:

将代码分解为可验证的逻辑验证步骤,然后将这些步骤分解为由加减乘除组成的计算流程。

进行一系列变换,将待验证代码转换为多项式方程,如 $t(x)\ h(x) = w(x)\ v(x)$。

为了使证明更加简洁,验证者事先随机选择几个检查点 s,检查这些点上的方程是否为真。

通过同态编码或加密,验证者在计算方程时不知道实际输入值,但仍然可以验证。

在等式的左右两边,乘以一个不等于 0 的密值 k。当验证 $(t(s)\ h(s)\ k) = (w(s)\ v(s)\ k)$ 时,具体的 $t(s)$、$h(s)$、$w(s)$、$v(s)$ 是不可知的,可以对信息进行保护。

当前履行 zk-SNARKs 算法的一个缺陷是需要在 advanced 中内置参数。如果这些参数泄露,整个网络将面临毁灭性的破坏。因此,用户必须信任在使用这些网络时不会泄露的信息。

注意将讲解重点放在 zk-SNARKs 算法的零知识性质上,可以不必深入讲解其内在运行原理。

零知识证明的运用远不仅于此,零知识证明还在数据的隐私保护、身份认证、去中心化存储、数字金融等很多方面被广泛运用,并且未来很可能有更多应用的可能。可以结合社会生活和学术的多个方面,通过介绍一些精妙的加密的算法利用零知识证明在生活中实现数据安全的例子,让更多人了解零知识证明。

6 零知识证明的实验分层次案例化教学

对于大学本科高年级学生及研究生,其理解能力较强,能够很好地进行编程和实践操作,所以对于这两个阶段学生,加入实践内容,使其更好地理解零知识证明的过程和运行原理,通过对认证系统进行验证或设计认证系统,学生可以更好地对零知识证明的内容进行实际操作和理解,从而达到实践教学的目的。

可以进行以下实验:

实验名称: 基于零知识证明的认证系统。

实验内容: 基于 Feige-Fiat-Shamir 认证协议,完成一个认证系统。

实验环境: Windows 环境、VC、虚拟环境。

实验步骤:

(1) 掌握零知识证明、认证系统、基于零知识的认证系统概念与原理;

(2) 编程实现 Feige-Fiat-Shamir 认证协议;

(3) 基于 Feige-Fiat-Shamir 认证协议,完成一个简单的认证系统(本科高年级学生可以跳过该步骤,直接对认证协议进行验证);

(4) 验证 Feige-Fiat-Shamir 认证协议的正确性。

实验思考: 如何实现并行的 Feige-Fiat-Shamir 认证协议,如何基于并行的 Feige-Fiat-Shamir 认证协议完成一个认证系统。

注意,教学时应该根据不同的学生群体运用不同难度的教学。对于高年级本科生,考虑其程序设计能力和对协议的理解水平,可以不用对认证协议进行设计,直接对其进行验证。研究生能力较高,可以通过设计并验证的方式,使其对零知识证明协议有更好的理解和掌握。

通过实践教学,可以让有能力的学生进行深层次的学习,达到深层次的理解和融会贯通的能力,在未来能够编程实现零知识证明在相关领域解决问题。

7 总结

本文针对不同阶段和专业类型大学生,提供了零知识证明的分层次案例化教学设计,旨在让更多学生以更加生动形象的方式,了解和学习零知识证明。进行案例化教学时,要着重讲述案例,以生动活泼的案例,引出零知识证明的定义和应用,并且应该对于不同的教学对象采用不同的教学方法,做到因材施教。教学中要避免使用过于困难的材料,尽量让教学生动易懂,同时激

发学习兴趣，让更多人了解零知识证明及其广阔应用场景。

参考文献

[1] Goldwasser S, Micali S, Rackoff C. The Knowledge Complexity of Interactive Proof Systems [J]. SIAM Journal on Computing, 1989, 18(1): 186-208.

[2] 赵殷豪. 基于区块链的匿名技术研究 [D]. 北京: 北京交通大学, 2019.

[3] Pieprzyk J, Hardjono T, Seberry J. 计算机安全基础 [M]. 北京: 中国水利水电出版社, 2006.

[4] 曹天杰, 张永平, 汪楚娇. 安全协议 [M]. 北京: 北京邮电大学出版社, 2009.

[5] 马民生, 冯俊昌. 数据安全教学方法的研究与探讨 [J]. 计算机教育, 2009(10): 99-101.

[6] 诸葛民. 数独游戏规则 [M]. 北京: 中国纺织出版社: 2008.

[7] 肖云霞. 一元三次方程求解史话 [J]. 数学之友, 2011(3): 74-76.

[8] 龚立清. 无理数的无理数次幂一定是无理数 [J]. 中学数学, 1988(9): 27.

[9] 张引兵. 零知识证明及其应用研究 [D]. 淮北: 淮北师范大学, 2011.

[10] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用 [J]. 通信学报, 2020, 41(1): 134-151.

[11] 李顺东, 戴一奇, 游启友. 姚氏百万富翁问题的高效解决方案 [J]. 电子学报, 2005(5): 769-773.

[12] 管章双. 基于零知识证明的账户模型区块链系统隐私保护研究 [D]. 济南: 山东大学, 2020.

Hierarchical Case Teaching Design of Zero Knowledge Proof

ZHANG Yanshuo　LI Zehao

Beijing Electronic Science and Technology Institute, Beijing　100070, P.R.China

Abstract: Zero knowledge proof means that the verifier can make the verifier believe that an assertion is correct without providing any useful information to the verifier. Zero knowledge proof plays an important role in today's society with the rapid development of network technology. It is widely used in data privacy protection, identity authentication, decentralized storage, blockchain, digital finance and other fields, and will be more widely used in the future. The purpose of this paper is to put forward the hierarchical case teaching design of zero knowledge proof, and give the teaching design of zero knowledge proof for different stages and levels.

Keywords: zero knowledge proof; stratified; cases; instructional design

(责任编辑: 鞠　磊)