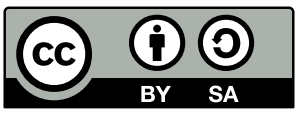
使用哈希函数构造密码学证明

Alessandro Chiesa

Eylon Yogev

译者：Kurt Pan

May 27, 2024



Contents

前言 iv
序言 vi

前言

简洁证明系统是一种非凡的工具。我们用一个简单的例子来简要解释它们是什么。假设爱丽丝有一个做了一些有趣事情的公共程序 P，比如会依次输出 π 的十进制数字，首先是 3，然后是 1，然后是 4，依此类推。爱丽丝在她的笔记本电脑上运行这个程序，程序输出了 π 的第一百万位小数，这正好是 5。她非常兴奋，于是告诉了她所有的朋友。爱丽丝的一个朋友鲍勃有点怀疑。他检查了程序 P 的代码，确认它确实是在正确地计算 π 的数字。但他担心爱丽丝只是猜测了第一百万位数字是什么而并没有实际运行程序。鲍勃决定自己验证一下这个计算。他设置好他的笔记本电脑运行 P ，并等待它重新确认爱丽丝的发现。

当鲍勃等待他的笔记本电脑从头开始重新运行整个计算时，他开始觉得这毫无意义。如果他们的朋友卡罗尔也不信任他们中的任何一个，她也将不得不重新运行整个计算以说服自己 P 确实正确运行了。如果大卫不信任他们三个人中的任何一个，他也将不得不重新运行整个计算。这是大量的重复劳动。他们所有人都在一遍又一遍地重做相同的计算。

有没有更好的方法？ 简洁证明系统提供了一个非凡的解决方案。它使得爱丽丝能够计算出程序 P 正确运行并且其输出如所声称的那样的证明。这个证明是**简洁的**，意味着它很短且验证速度很快。在实践中，简洁证明只有几千字节长，验证只需几毫秒。这里应当停下来对此感到惊叹：无论爱丽丝计算的是 π 的第一百万位还是第一十亿位数字，证明她计算是正确的证明总是只有几千字节长且只需几毫秒就能验证。

令人惊奇的是，这适用于任意程序 P，即使它需要爱丽丝提供辅助输入。爱丽丝可以运行程序并发布其输出以及程序正确运行的简洁证明。然后，只需几毫秒的工作，鲍勃、卡罗尔、大卫以及其他任何人都可以检查这个证明，并确信爱丽丝正确地运行了这个程序。他们无需重新运行计算。这个简洁证明甚至可以是**零知识**的，意思是证明不会透露爱丽丝的辅助输入的任何信息，但它仍然可以让所有人相信程序确实在这个输入上正确运行了。

近年来，简洁证明系统的研究已经发展成为一个庞大的研究领域，许多研究者都贡献了许多美妙的想法。推动这一快速进展的原因之一是这些工具的商业化应用，例如对去中心化系统扩容。另一个原因是这一领域为新的技术创新提供了肥沃的土壤。有多种构造简洁证明的方法，给研究者提供了许多探索的方向。同时，工程师们也有强烈的需求希望构造编程框架，使得非专家也能轻松使用这些工具。总体而言，这是一个由研究者和开发者组成的充满活力的社区，这一领域的工作既令人兴奋又充满乐趣。

本书涵盖了一种特定的简洁证明系统构造方法，称为**基于哈希的证明**。这些证明系统在概念上是最简单的，不需要复杂的数学知识，因此对广泛的读者群体都具有吸引力。此外，这些证明系统的安全性依赖于哈希函数的相对简单的性质。对于标准的密码学哈希函数，这些性质被认为即使在敌手拥有大规模量子计算机的情况下也能成立。因此，这些证明系统是**后量子**的：即使在构建出大规模量子计算机之后，它们仍将保持安全。

基于哈希的证明系统的理论已经相当成熟且被透彻理解。然而，直到现在，还没有一本书提供所有的详细信息。这就是本书的目的。本书开始部分精确定义了构成简洁证明系统的元素。接下来，本书转向从几个抽象的信息论对象构建简洁证明系统。一个广泛使用的例子是从一个重要对象——**交互式预言机证明（Interactive Oracle Proof，简称 IOP）**构造简洁证明系统。该构造完全依赖于哈希函数。书中逐步构造必要的工具，然后清晰描述了该构造及其安全性证明。

本书是对证明系统领域的重大贡献。它适合喜欢对材料进行清晰且精确处理的读者。我相信，一旦你读了这本书，你会想要了解更多关于这个领域的知识。本书是进入简洁证明世界的一个很好的起点，带你踏上一段有趣的旅程。

Dan Boneh
2024 年 4 月
斯坦福大学

序言

> “证明对我们的生活至关重要，而对于所有基本的事物，我们应该有所预料，对证明是什么的回答将永远是一个发展中的过程。“
>
> Silvio Micali, 计算可靠证明

本书讨论的是**密码学证明**，即用于证明和验证计算的正确执行的简洁且零知识的（稍后将详细介绍）协议。密码学证明是计算机科学中的一个基本对象，处于密码学和计算复杂性理论的交汇之处。由于实际应用的推动，在学术界和工业界受到了极大的关注。密码学证明结合了计算理论中一些最优美的思想和最强大的工具，是深奥的数学思想在新技术中起关键作用的一个显著例子。

本书提供了一个基于（理想）哈希函数构造的密码学证明的严格介绍，既是学生自学的教材，也是从业者的参考书。这包括了基于（理想）哈希函数的简洁非交互论证（SNARGs）的著名构造。例如，STARKs（可扩展透明知识论证）就是此类 SNARGs 的一个例子。

最新版本 本书的最新版本可以在以下网站找到：

`https://hash-based-snargs-book.github.io/`

该网站还链接了本书源代码的 Git 库，包括最新的更正和补充内容。我们非常欢迎对本书的评论（无论正面或负面的！），以及任何的更正或建议。您可以直接在 GitHub 上的库里提交 issues 或 PR，或者直接通过电子邮件联系我们。