证明、论证与零知识

Kurt Pan

2023 年 5 月 5 日

目录

目录

Chapter 1

引言

本书讨论了可验证计算（VC）。可验证计算是指一种名为交互式证明（IPs）和论证的密码学协议，证明者能够向验证者提供证明者正确地执行了所请求的计算的保证。交互式证明和论证在 20 世纪 80 年代被提出，代表了一个陈述为真的“证明”包括什么概念上的重大扩展。传统上的证明是一个静态对象，可以很容易地通过逐步检查来检验正确性，因为证明的每个单独步骤都应该易于验证。相比之下，交互式证明允许证明者和验证者之间的进行交互，以及允许无效证明以微小但非零的概率通过验证。交互式证明和论证之间的区别在于，论证（而非交互式证明）允许存在对错误陈述的“证明”，只要找到这些“证明”需要巨大的计算能力就可以。[1]

20 世纪 80 年代中期和 90 年代初的著名理论结果表明，至少原则上讲，可验证计算协议可以达到惊人的成就：包括让手机可以去监控强大但不受信任（甚至恶意）的超级计算机的执行，让计算能力较弱的外设（例如，安全卡读卡器）将安全核心工作外包给强大的远程服务器，以及让数学家仅通过查看所谓证明中的几个符号就能对定理的正确性具有很高的信心。[2]

当 VC 协议具有一种称为零知识的性质时，它会在密码学环境中非常有用。零知识的意思是证明或论证除了其本身的有效性之外，不会泄露任何信息。

为了具体说明为什么零知识协议有用，考虑以下来自身份认证的典型例子。假如 Alice 选择了一个随机口令 x，公开了一个哈希值 $z = h(x)$，其中 h 是一个单向函数。这意味着给定一个对随机选择 x 的 $z = h(x)$，需要大量计算能力才能找到 z 在 h 下的原象，即一个满足 $h(x') = z$ 的 x'。假如 Alice 在之后想要说服 Bob 她是发布 z 的同一个人。她可以通过向 Bob 证明她知道一个满足 $h(x') = z$ 的 x' ，来实现这一点。这将使 Bob 相信 Alice 是发布 z 的同一个人，因为这意味着 Alice 要么一开始就知道 x，要么她反转了 h （这被认为是超出了 Alice 的计算能力）。

对密码学相关的高度特定化的陈述（如证明离散对数的知识 [Sch89]）的实用零知识协议已经有了数十年了。然而，通用零知识协议直到最近才变得足够高效，可以用于密码部署中。通用的意思是，协议设计技术适用于任意计算。这一令人兴奋的进展包括了漂亮的新协议的提出，并引发了各界对零知识证明和论证的浓厚兴趣。本书旨在以统一的方式让人们能够轻松理解这些协议设计的主要思想和方法。

[1] 比如说，一个不是 IP 的论证系统，可能会使用密码系统，使得作弊的证明者有可能找到一个可通过验证的对假陈述的“证明”，当且仅当证明者可以攻破密码系统。

[2] 只要证明以一种特定的、略微有些冗余的形式书写。具体见第9章中对概率可检验证明（PCPs）的讨论。

1.1 数学证明

1.2 我们将研究哪些非传统证明?

Chapter 2

随机性的力量：指纹和 Freivalds 算法

Chapter 3

定义和技术预备知识

Chapter 4

交互式证明系统

Chapter 5

使用 Fiat-Shamir 得到公开可验证非交互式论证

Chapter 6

前端：将计算机程序转化为电路

Chapter 7

基于交互式证明的首个电路可满足性简洁论证

Chapter 8

MIP 和简洁论证系统

Chapter 9

PCP 和简洁论证系统

Chapter 10

交互式预言证明

Chapter 11

零知识证明和论证系统

Chapter 12

基于离散对数困难性的 Σ-协议和承诺

Chapter 13

通过承诺并证明和遮盖多项式实现零知识

Chapter 14

基于离散对数困难性的多项式承诺

Chapter 15

基于配对的多项式承诺

Chapter 16

多项式承诺总结

Chapter 17

线性 PCP 和简洁论证

Chapter 18

SNARK 组合和递归

Chapter 19

实用论证系统鸟瞰

Bibliography

[Sch89] Claus-Peter Schnorr. *Efficient Identification and Signatures for Smart Cards*. Annual International Cryptology Conference. 1989 (cit. on p. 5).

BIBLIOGRAPHY