# 应用密码学研究生课程

Kurt Pan

2023 年 5 月 24 日

# 目录

目录

# 第 1 章

# 公钥工具

我们首先通过介绍几个基本工具来开始讨论公钥密码学，这些工具将在本书的其余部分中使用。这些工具的主要应用将在接下来的几章中出现，我们将在那里使用它们进行公钥加密、数字签名和密钥交换。由于我们在本章中使用了一些基本的代数和数论，因此建议读者首先简单地浏览一下附录 A。

我们从一个简单的玩具问题开始：在两方之间生成一个共享的秘密密钥，以便被动窃听敌手不能猜测出他们的共享密钥。敌手可以监听网络流量，但不能修改在途的消息或注入他自己的消息。在后面的章节中，我们开发了在存在可能干扰网络流量的主动攻击者的情况下进行密钥交换所需的全部设备。

我们在开始时就强调，对窃听的安全性通常不足以应对真实世界的应用，因为有能力监听网络流量的攻击者通常也能够篡改它；然而，这个玩具窃听模型是介绍新公钥工具的好方法。

## 1.1 玩具问题：匿名密钥交换

## 1.2 单向陷门函数

## 1.3 基于 RSA 的陷门置换方案

## 1.4 Diffie-Hellman 密钥交换

## 1.5 离散对数及相关假设

## 1.6 来自数论原语的抗碰撞哈希函数

# 参考文献


[ALM+98] Sanjeev Arora et al. *Proof verification and the hardness of approximation problems*. Journal of the ACM (JACM) 45.3 (1998), pp. 501–555.

[AS98] Sanjeev Arora and Shmuel Safra. *Probabilistic checking of proofs: A new characterization of NP*. Journal of the ACM (JACM) 45.1 (1998), pp. 70–122.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. *Non-deterministic exponential time has two-prover interactive protocols*. Computational complexity 1 (1991), pp. 3–40.

[LFK+92] Carsten Lund et al. *Algebraic methods for interactive proof systems*. Journal of the ACM (JACM) 39.4 (1992), pp. 859–868.

[Sch89] Claus-Peter Schnorr. *Efficient Identification and Signatures for Smart Cards*. Annual International Cryptology Conference. 1989.

[Sha92] Adi Shamir. *IP = PSPACE*. Journal of the ACM (JACM) 39.4 (1992), pp. 869–877.

参考文献