EE 720 Lecture Notes

Autumn 2023

Saravanan Vijayakumaran

August 15, 2023

Table of contents

Preface

These notes were created to support the course *EE720: An Introduction to Number Theory and Cryptography* at IIT Bombay. This course runs in the Electrical Engineering department and is offered to both undergraduate and postgraduate students.

I have taught EE720 three times (2018–2020) using the excellent textbook Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell. Time constraints allowed me to cover only a small subset of the book's content. I used other sources to teach topics from abstract algebra in more detail.

These notes are meant to **supplement** the book by Katz & Lindell. They will contain the following.

- Proofs of some results stated without proof in the book.
- Expanded coverage of some material relevant to the course.

Saravanan Vijayakumaran
July 2023

> **Warning**
>
> These notes are a work in progress and may contain errors. Please email the author at sarva@ee.iitb.ac.in to report any errors.

About Me

My name is Saravanan Vijayakumaran. I am an Associate Professor in the Department of Electrical Engineering at IIT Bombay. I am currently (mid 2023) interested in cryptocurrency blockchains and applications of zero-knowledge proofs.

Chapter 1

Perfectly Secret Encryption

1.1 Proof of Lemma 2.7

Lemma 1.1. *Encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is perfectly secret if and only if it is perfectly indistinguishable.*

1.1.1 Forward Direction

- Suppose a scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secret.
- Consider an adversary $\mathcal{A}$ who picks two messages m_0, m_1 and gives it to Π.
- Π picks a bit b randomly and a key k. It gives $c = \mathsf{Enc}_k(m_b)$ to $\mathcal{A}$.
- $\mathcal{A}$ outputs b'.
- We want to prove that $\Pr[b = b'] = \frac{1}{2}$. Note abuse of notation; lower case letters for random variables.

1.1.1.1 Deterministic Adversary

- If $\mathcal{A}$ is deterministic, then there exists a partition C_0, C_1 of $\mathcal{C}$ such that $\mathcal{C}_0 \cap \mathcal{C}_1 = \emptyset$ and

$$\mathcal{A}(c) = \begin{cases} 0 & \text{if } c \in \mathcal{C}_0, \\ 1 & \text{if } c \in \mathcal{C}_1. \end{cases}$$

Then we have

$$\begin{aligned} \Pr[b = b'] &= \frac{\Pr[\mathcal{A}(C) = 0 \mid b = 0] + \Pr[\mathcal{A}(C) = 1 \mid b = 1]}{2} \\ &= \frac{\Pr[C \in \mathcal{C}_0 \mid b = 0] + \Pr[C \in \mathcal{C}_1 \mid b = 1]}{2} \end{aligned}$$

Consider the first term in the numerator

$$\begin{aligned}\Pr[C \in \mathcal{C}_0 \mid b = 0] &= \Pr[C \in \mathcal{C}_0 \mid M = m_0] \\ &= \sum_{c \in \mathcal{C}_0} \Pr[C = c \mid M = m_0] = \sum_{c \in \mathcal{C}_0} \Pr[C = c] \\ &= \Pr[C \in \mathcal{C}_0]\end{aligned}$$

Similarly, the second term in the numerator is equal to $\Pr[C \in \mathcal{C}_1]$. Plugging these back into the previous equation, we get

$$\Pr[b = b'] = \frac{\Pr[C \in \mathcal{C}_0] + \Pr[C \in \mathcal{C}_1]}{2} = \frac{1}{2}.$$

1.1.1.2 Probabilistic Adversary (not exclusive from previous case)

Suppose the adversary is probabilistic.

$$\Pr[b = b'] = \frac{\Pr[\mathcal{A}(C) = 0 \mid b = 0] + \Pr[\mathcal{A}(C) = 1 \mid b = 1]}{2}$$

Consider the first term in the numerator.

$$\begin{aligned}\Pr[\mathcal{A}(C) = 0 \mid b = 0] &= \sum_{c \in \mathcal{C}} \Pr[\mathcal{A}(C) = 0 \mid b = 0, C = c] \Pr[C = c \mid b = 0] \\ &= \sum_{c \in \mathcal{C}} \Pr[\mathcal{A}(C) = 0 \mid C = c] \Pr[C = c \mid b = 0] \\ &= \sum_{c \in \mathcal{C}} \Pr[\mathcal{A}(C) = 0 \mid C = c] \Pr[C = c] \\ &= \Pr[\mathcal{A}(C) = 0].\end{aligned}$$

where the second equality follows because the adversary's decision is independent of the message once we condition on the ciphertext, and the third equality follows from Lemma 2.5 and the assumption of perfect secrecy.

Similarly, we have $\Pr[\mathcal{A}(C) = 1 \mid b = 1] = \Pr[\mathcal{A}(C) = 1]$. Plugging these back into the previous equation, we get

$$\Pr[b = b'] = \frac{\Pr[\mathcal{A}(C) = 0] + \Pr[\mathcal{A}(C) = 1]}{2} = \frac{1}{2}.$$

1.1.2 Reverse Direction

To be done as part of Assignment 1