EE 720: An Introduction to Number Theory and Cryptography (Spring 2020)

Lecture 4 — January 23, 2020

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Perfect adversarial indistinguishability

2 Recap

- Perfectly secret encryption schemes

3 Some Exercises on Perfect Secrecy

- Prove that if only a single character is encrypted, then the shift cipher is perfectly secret. Show that it is not perfectly secret when used to encrypt more than one character.
- What is the largest message space $\mathcal{M}$ for which the substitution cipher provides perfect secrecy?
- Prove that the Vigenére cipher using a key period t is perfectly secret when used to encrypt messages of length t. Show that it is not perfectly secret when used to encrypt messages of length more than t.

4 Perfect adversarial indistinguishability

- Another equivalent definition of perfect secrecy.
- Based on an *experiment* involving an adversary passively observing a ciphertext and then trying to guess which of two possible messages was encrypted.
- Will serve as a starting point for defining computational security in the next few lectures.
- Consider the following experiment $\texttt{PrivK}^{\texttt{eav}}_{\mathcal{A},\Pi}$:
  - Let $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ be an encryption scheme with message space $\mathcal{M}$.
  - Let $\mathcal{A}$ be an adversary (an algorithm).
  - The adversary $\mathcal{A}$ outputs a pair of arbitrary messages $m_0, m_1 \in \mathcal{A}$.
  - A key k is generated using $\texttt{Gen}$, and a uniform bit $b \in \{0, 1\}$ is chosen. Ciphertext $c \leftarrow \texttt{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. This ciphertext c is called the *challenge ciphertext*.

- $\mathcal{A}$ outputs a bit b'.
- The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\texttt{PrivK}^{\texttt{eav}}_{\mathcal{A},\Pi} = 1$ if the output of the experiment is 1 and in this case we say that $\mathcal{A}$ succeeds.

- It is trivial for $\mathcal{A}$ to succeed with probability $\frac{1}{2}$ by outputting a random guess or a fixed bit. Perfect indistinguishability requires that it is impossible for $\mathcal{A}$ to do any better.

Definition. *Encryption scheme* $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *with message space* $\mathcal{M}$ *is perfectly indistinguishable if for every* $\mathcal{A}$ *it holds that*

$$\Pr\left[\mathit{PrivK}^{eav}_{\mathcal{A},\Pi} = 1\right] = \frac{1}{2}.$$

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

Proof.

- (**Forward direction**, $A \implies B$) Assume that Π is perfectly secret and that the adversary is deterministic. Prove that Π is perfectly indistinguishable. Prove it assuming the adversary is probabilistic.

- (**Reverse direction**, $B \implies A$) Proving $B \implies A$ is equivalent to proving $A^c \implies B^c$. Assume that Π is not perfectly secret. Prove that Π is not perfectly indistinguishable.

$\square$

5 References and Additional Reading

- Section 2.3 from Katz/Lindell