EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)

Lecture 3 — January 10, 2019

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Perfectly Secret Encryption

- Perfectly secret encryption schemes are *provably secure* against an adversary with unbounded computational power.
- Recall the syntax of encryption: $m \in \mathcal{M}, k \in \mathcal{K}, k \leftarrow \texttt{Gen}, c \leftarrow \texttt{Enc}_k(m), m := \texttt{Dec}_k(c)$
- $c \leftarrow \texttt{Enc}_k(m)$ may be probabilistic but $\texttt{Dec}_k(c)$ is equal to m with probability 1. This is called perfect correctness.
- Let M be a random variable denoting the message (plaintext) being encrypted.
- Let K be a random variable denoting the value of the key output by Gen. Almost always a uniform random variable on $\mathcal{K}$.
- K and M are assumed to be independent.
- Let C be a random variable denoting the ciphertext.
- Fixing an encryption scheme and a distribution over $\mathcal{M}$ determines a distribution over $\mathcal{C}$ given by choosing a key $k \in \mathcal{K}$.

1.1 Perfect Secrecy

- Assume that adversary knows
  - Probability distribution over $\mathcal{M}$
  - Encryption scheme
  - Ciphertext transmitted
- Ciphertext text should reveal nothing about the plaintext.

Definition (KL page 29)**.** *An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$:*

$$\Pr[M = m \mid C = c] = \Pr[M = m].$$

In other words, the *a posteriori* probability that some message $m \in \mathcal{M}$ was sent, conditioned on the ciphertext that was observed, should be the same as the *a priori* probability that m was sent.

Equivalent formulation of perfect secrecy: The probability distribution of the ciphertext does not depend on the plaintext, i.e.

$$\Pr\left[\mathtt{Enc}_K(m) = c\right] = \Pr\left[\mathtt{Enc}_K(m') = c\right]$$

This implies that the ciphertext contains no information about the plaintext.

Lemma. *An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if and only if* $\Pr\left[\mathtt{Enc}_K(m) = c\right] = \Pr\left[\mathtt{Enc}_K(m') = c\right]$ *holds for every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$.*

Proof. ($\Rightarrow$) If a scheme is perfectly secret, $\Pr[C = c \mid M = m] = \Pr[C = c] = \Pr[C = c \mid M = m']$.

($\Leftarrow$) The case of $\Pr[M = m] = 0$ is trivial. For $\Pr[M = m] > 0$, note that $\Pr[C = c \mid M = m] = \Pr\left[\mathtt{Enc}_K(m) = c\right]$. Use Bayes' theorem to show that $\Pr[M = m \mid C = c] = \Pr[M = m]$. □

2 One-Time Pad

- Patented by Vernam in 1917. At that time, he did not know that it was a perfectly secret encryption scheme.
- Shannon introduced the notion of perfect secrecy in the 1940s and proved that the one-time pad achieves it.
- Construction 2.8 on page 33 of KL
- Proof of perfect secrecy
- Drawbacks
  - Key needs to be as long as the message
  - Only secure if the key is used only once. While we have not defined a notion of security when multiple messages are encrypted, consider the case when two message m and m' are one-time pad encrypted using the same key k. Then $c \oplus c' = m \oplus k \oplus m' \oplus k = m \oplus m'$. This leaks information about the plaintexts.
- The key length drawback of the one-time pad is actually a drawback of any perfectly secret encryption scheme.

Theorem (Page 35 of KL)**.** *If* (Gen, Enc, Dec) *is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.*

Proof. Obtain a contradiction to perfect secrecy when $|\mathcal{K}| < \mathcal{M}$. Assume a uniform distribution on $\mathcal{M}$. □

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 References and Additional Reading

- Sections 2.1,2.2,2.3 from Katz/Lindell