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

Lecture 3 — January 22, 2020

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Principles of Modern Cryptography (Contd)

1.1 Threat Models

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

  Adversary is able to obtain the decryption of ciphertexts of its choice. Aims to deduce information about the underlying plaintext of some *other* ciphertext produced using the same key.

1.2 Precise Assumptions

Most modern cryptographic constructions cannot be proven secure unconditionally. Proofs of security rely on assumptions which need to made explicit and mathematically precise.

1.3 Proofs of Security

Proofs of security provide security guarantees relative to the definition being considered the specified assumptions being used.

2 Perfectly Secret Encryption

- Let us look at encryption schemes that are provably secure even against an adversary with unbounded computational power. Such schemes are called *perfectly secret*. The existence of such schemes is not obvious because we are allowing the adversary to launch brute-force attacks (for e.g., try all possible keys for any key length).
- This work was done by Shannon in the 1940s, so not exactly modern cryptography which is post 1970s. But Shannon was way ahead of his time.
- Recall the syntax of encryption: $m \in \mathcal{M}, k \in \mathcal{K}, k = \texttt{Gen}, c = \texttt{Enc}_k(m), m = \texttt{Dec}_k(c)$
- $c \leftarrow \texttt{Enc}_k(m)$ may be probabilistic but $\texttt{Dec}_k(c) = m$ 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 $\texttt{Gen}$. 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 $k \in \mathcal{K}$.
- Example: Consider the shift cipher with message set $\mathcal{M} = \{\texttt{kim}, \texttt{ann}, \texttt{boo}\}$ with probabilities 0.5, 0.2, 0.3 respectively. What is $\Pr[C = \texttt{dqq}]$? What is $\Pr[M = \texttt{ann} \mid C = \texttt{dqq}]$?

2.1 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 (*$\texttt{Gen}$*,* $\texttt{Enc}$*,* $\texttt{Dec}$*) 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.

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

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

Lemma. *An encryption scheme (*$\texttt{Gen}$*,* $\texttt{Enc}$*,* $\texttt{Dec}$*) with message space* $\mathcal{M}$ *is perfectly secret if and only if* $\Pr[\texttt{Enc}_K(m) = c] = \Pr[\texttt{Enc}_K(m') = c]$ *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 $\Pr[C = c \mid M = m] = \Pr[\texttt{Enc}_K(m) = c]$. Use Bayes' theorem to show that $\Pr[M = m \mid C = c] = \Pr[M = m]$. Exploit the fact that for every $m' \in \mathcal{M}$ we have $\delta_c = \Pr[C = c \mid M = m'] = \Pr[\texttt{Enc}_K(m') = c]$. □

3 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* $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ *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 $\mathcal{M}$. Consider the set

$$\mathcal{M}(c) = \{m \mid m = \mathtt{Dec}_k(c) \text{ for some } k \in \mathcal{K}\}$$

and consider its size. Rest of the proof on board. □

4 References and Additional Reading

- Sections 2.1,2.2,2.3 from Katz/Lindell