EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 4 — January 17, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Proof that the one-time pad is perfectly secret
- Limitations of the one-time pad and perfectly secret schemes
- Exercises on perfect secrecy
- Perfect adversarial indistinguishability

2 Recap

- Perfectly secret encryption schemes
- One-time pad construction

3 One-Time Pad

- Recall construction
- 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 $\mathcal{M}$. □

4 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 mono-alphabetic 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.

5 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 $\mathtt{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi}$:
  - Let $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ 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 $\mathtt{Gen}$, and a uniform bit $b \in \{0, 1\}$ is chosen. Ciphertext $c \leftarrow \mathtt{Enc}_k(m_b)$ 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 $\mathtt{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi} = 1$ 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. Perfect indistinguishability requires that it is impossible for $\mathcal{A}$ to do any better.

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

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

Exercises

- Is the shift cipher perfectly indistinguishable? What if only a single character is encrypted?
- Is the Vigenére cipher with key length t perfectly indistinguishable when used to encrypt messages of length t?

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

6 References and Additional Reading

- Sections 2.1,2.2,2.3 from Katz/Lindell