Adversarial Indistinguishability
Perfectly-Secret Encryption

Foundations of Cryptography
Computer Science Department
Wellesley College

Fall 2016

Table of contents

Introduction

Adversarial Indistinguishability

Vernam’s Cipher

Shannon’s Theorem
**Perfect Secrecy Revisited**

**Definition 2.3.** An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) over a 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 \(\Pr[C = c] > 0\):

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

**Lemma 2.4.** An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) over a message space \(\mathcal{M}\) is **perfectly secret** if and only if for every probability distribution over \(\mathcal{M}\), every \(m_0, m_1 \in \mathcal{M}\), and every ciphertext \(c \in \mathcal{C}\):

\[
\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1].
\]

*Another way of interpreting this definition is that a scheme is perfectly secret if the distributions over message and ciphertexts are independent.*

**Experiments in security**

**The eavesdropping indistinguishability experiment** \(\text{PrivK}^{\text{eav}}_{\mathcal{A}, \Pi}\)

1. The adversary \(\mathcal{A}\) outputs a pair of messages \(m_0, m_1 \in \mathcal{M}\).
2. A random key \(k\) is generated by running \(\text{Gen}\), and a random bit \(b \leftarrow \{0, 1\}\) is chosen. (These are chosen by some imaginary entity that is running the experiment with \(\mathcal{A}\).) Then, a ciphertext \(c \leftarrow \text{Enc}_k(m_b)\) is computed and given to \(\mathcal{A}\).
3. \(\mathcal{A}\) outputs a bit \(b'\).
4. The output of the experiment is defined to be 1 if \(b' = b\), and 0 otherwise. We write \(\text{PrivK}^{\text{eav}}_{\mathcal{A}, \Pi} = 1\) if the output is 1 and in this case we say that \(\mathcal{A}\) succeeded.

Observe that it is always possible for \(\mathcal{A}\) to succeed with probability one half. (Why?) The question is can \(\mathcal{A}\) do any better.
**Perfect indistinguishability**

*Definition 2.5.* Encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ is *perfectly indistinguishable* if for every adversary $\mathcal{A}$ it holds that

$$\Pr[\text{Priv}_{\mathcal{A},\Pi}^\text{eav} = 1] = \frac{1}{2}.$$  

*Lemma 2.6.* Encryption scheme $\Pi$ is perfectly secret if and only if it is perfectly indistinguishable.

*Remark.* You will have an opportunity to explore the proof of Lemma 2.6 in the next problem set.

---

**Vigenère is not perfectly indistinguishable**

*Example 2.7.* Let $\Pi$ denote the Vigenère cipher for the message space of two-character strings, and where the period is chosen uniformly in $\{1, 2\}$. We exhibit an adversary $\mathcal{A}$ for which $\Pr[\text{Priv}_{\mathcal{A},\Pi}^\text{eav} = 1] > \frac{1}{2}$.

Adversary $\mathcal{A}$ does:

1. Output $m_0 = aa$ and $m_1 = ab$.
2. Upon receiving the challenge ciphertext $c = c_1c_2$, do the following: if $c_1 = c_2$ output 0; else output 1.
Analyzing the adversary’s chances

Pr[Privₖₑavlₐ, π = 1]

= \frac{1}{2} \cdot Pr[Privₖₑavlₐ, π = 1 | b = 0] + \frac{1}{2} \cdot Pr[Privₖₑavlₐ, π = 1 | b = 1]

= \frac{1}{2} \cdot Pr[A \text{ outputs } 0 | b = 0] + \frac{1}{2} \cdot Pr[A \text{ outputs } 1 | b = 1]

A outputs 0 if and only if the two characters of the ciphertext

\( c = c_1c_2 \) are equal. When \( b = 0 \) then \( c_1 = c_2 \) if either (1) a key of

period 1 is chosen, or (2) a key of period 2 is chosen, and both

characters of the key are equal. So,

\[
Pr[A \text{ outputs } 0 | b = 0] = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26}.
\]

Plugging into the top equations gives

Pr[Privₖₑavlₐ, π = 1]

= \frac{1}{2} \cdot Pr[A \text{ outputs } 0 | b = 0] + \frac{1}{2} \cdot Pr[A \text{ outputs } 1 | b = 1]

When \( b = 1 \) then \( c_1 = c_2 \) if a key of period 2 is chosen and the

first character of the key is one more than the second. So,

\[
Pr[A \text{ outputs } 1 | b = 1] = 1 - Pr[A \text{ outputs } 0 | b = 1] = 1 - \frac{1}{2} \cdot \frac{1}{26}.
\]

Pr[Privₖₑavlₐ, π = 1] = \frac{1}{2} \cdot \left( \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26} + 1 - \frac{1}{2} \cdot \frac{1}{26} \right) = 0.75
Introduction

Adversarial Indistinguishability

Vernam’s Cipher

Shannon’s Theorem

The one-time pad (random polyalphabetic cipher)

• We assume that an attacker has at least some knowledge of the statistical characteristics of the plaintext.

• If these statistics survive in the ciphertext, the cryptanalysis may be able to greatly restrict the key space.

• In 1917, Vernam patented a cipher now called the one-time pad that masked all statistical characteristics of the plaintext. Indeed, although there was no proof of it at the time, the cipher obtains perfect secrecy.

The one-time pad encryption scheme

Fix an integer \( \ell > 0 \). Then the message space \( \mathcal{M} \), key space \( \mathcal{K} \), and ciphertext space \( \mathcal{C} \) are all equal to \( \{0, 1\}^\ell \).

1. Gen chooses a string from \( \mathcal{K} = \{0, 1\}^\ell \) according to the uniform distribution.

2. Enc: given a key \( k \in \{0, 1\}^\ell \) and a message \( m \in \{0, 1\}^\ell \), output \( c := k \oplus m \).

3. Dec: given a key \( k \in \{0, 1\}^\ell \) and a ciphertext \( c \in \{0, 1\}^\ell \), output \( m := k \oplus c \).

Note that the scheme is perfectly correct. Why?

*Here \( a \oplus b \) denotes the bitwise exclusive-or of two binary strings \( a, b \).
The one-time pad is perfectly-secret

**Theorem 2.9.** The one-time pad encryption scheme is perfectly-secret.

**Proof.** Fix some distribution over $\mathcal{M}$ and fix an arbitrary $m \in \mathcal{M}$ and $c \in \mathcal{C}$. Then

$$
\begin{align*}
\Pr[C = c \mid M = m] &= \Pr[M \oplus K = c \mid M = m] \\
&= \Pr[m \oplus K = c] = \Pr[K = m \oplus c] = \frac{1}{2^\ell}.
\end{align*}
$$

Since this holds for all distributions and all $m$, we have that for every probability distribution over $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$ and every $c \in \mathcal{C}$,

$$
\Pr[C = c \mid M = m_0] = \frac{1}{2^\ell} = \Pr[C = c \mid M = m_1],
$$

and by Lemma 2.4, the encryption scheme is perfectly secret.

---

So why use anything else

**Theorem 2.10.** Let $(\text{Gen}, \text{Enc}, \text{Dec})$ be a perfectly-secret encryption scheme over a message space $\mathcal{M}$, and let $\mathcal{K}$ be the key space as determined by $\text{Gen}$. Then $|\mathcal{K}| \geq |\mathcal{M}|$.

In particular, if the key space consists of fixed-length keys, and the message space consists of all messages of some fixed length, this implies that the key must be at least as long as the message.

(And reusing one-time pads is a really bad idea.)
**Back to the theorem (and its proof)**

**Theorem 2.10.** Let \((\text{Gen}, \text{Enc}, \text{Dec})\) be a perfectly-secret encryption scheme over a message space \(\mathcal{M}\), and let \(\mathcal{K}\) be the key space as determined by \(\text{Gen}\). Then \(|\mathcal{K}| \geq |\mathcal{M}|\).

**Proof.** Suppose \(|\mathcal{K}| < |\mathcal{M}|\). Consider the uniform distribution over \(\mathcal{M}\) and let \(c \in \mathcal{C}\). Define

\[
\mathcal{M}(c) \overset{\text{def}}{=} \{ \hat{m} \mid \hat{m} = \text{Dec}_k(c) \text{ for some } \hat{k} \in \mathcal{K} \}.
\]

Clearly \(|\mathcal{M}(c)| \leq |\mathcal{K}|\) since for each message \(\hat{m} \in \mathcal{M}(c)\) there is at least one key \(\hat{k} \in \mathcal{K}\) for which \(\hat{m} = \text{Dec}_\hat{k}(c)\). Under the assumption that \(|\mathcal{K}| < |\mathcal{M}|\), there is some \(m' \in \mathcal{M}\) such that \(m' \notin \mathcal{M}(c)\). But then

\[
\Pr[M = m' \mid C = c] = 0 \neq \Pr[M = m']
\]

and the scheme is not perfectly secret.

---

**Shannon’s Characterization of Perfect Secrecy**

- In his work on perfect secrecy, Claude Shannon also provided a characterization of perfectly secret encryption scheme.
- This theorem is a useful tool for proving (or disproving) perfect secrecy of suggested schemes.
- We investigate a version in the following slides.
**Shannon’s Theorem**

**Theorem 2.11.** Let \((\text{Gen}, \text{Enc}, \text{Dec})\) be a perfectly-secret encryption scheme with message space \(\mathcal{M}\), for which \(|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|\). The scheme is perfectly secret if and only if:

1. Every key \(k \in \mathcal{K}\) is chosen with (equal) probability \(1/|\mathcal{K}|\) by the algorithm Gen.

2. For every \(m \in \mathcal{M}\) and every \(c \in \mathcal{C}\), there exists a unique key \(k \in \mathcal{K}\) such that \(\text{Enc}_k(m)\) outputs \(c\)

**Proof of Shannon’s Theorem \((\Leftarrow)\)**

**Proof.** \((\Leftarrow)\) Fix \(c \in \mathcal{C}\) and \(m \in \mathcal{M}\). Let \(k\) be the unique key for which \(\text{Enc}_k(m) = c\). Then

\[
\Pr[C = c \mid M = m] = \Pr[K = k] = 1/|\mathcal{K}|,
\]

So

\[
\Pr[C = c] = \sum_{m \in \mathcal{M}} \Pr[\text{Enc}_K(m) = c] \cdot \Pr[M = m] = 1/|\mathcal{K}|.
\]

Thus for any \(m \in \mathcal{M}\) with \(\Pr[M = m] \neq 0\), and any \(c \in \mathcal{C}\), we have

\[
\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]} = \frac{\Pr[\text{Enc}_K(m) = c] \cdot \Pr[M = m]}{\Pr[C = c]} = \frac{|\mathcal{K}|^{-1} \cdot \Pr[M = m]}{|\mathcal{K}|^{-1}} = \Pr[M = m].
\]
Proof of Shannon’s Theorem (⇒)

Proof. (⇒) Fix \( c \in \mathcal{C} \). There must be some message \( m^* \) for which \( \Pr[\text{Enc}_K(m^*) = c] \neq 0 \). Lemma 2.4 implies that \( \Pr[\text{Enc}_K(m) = c] \neq 0 \) for every \( m \in \mathcal{M} \).

Thus, for each \( m_i \in \mathcal{M} \) there is a nonempty set of keys \( \mathcal{K}_i \) such that \( \text{Enc}_K(m_i) = c \) if and only if \( k \in \mathcal{K}_i \). Moreover when \( i \neq j \) then \( \mathcal{K}_i \) and \( \mathcal{K}_j \) must be disjoint or correctness fails. Since \( |\mathcal{K}| = |\mathcal{M}| \), each \( \mathcal{K}_i \) must consist of a single key \( k_i \) establishing condition (2). By Lemma 2.4, for any \( m_i, m_j \in \mathcal{M} \)

\[
\Pr[K = k_i] = \Pr[\text{Enc}_K(m_i) = c] = \Pr[\text{Enc}_K(m_j) = c] = \Pr[K = k_i].
\]

Since \( k_i \neq k_j \) for \( i \neq j \), this means each key is chosen with probability \( 1/|\mathcal{K}| \) as required by condition (1). \( \square \)