Perfectly Secret Encryption

Jacob Benjamin Cholewa

Stud. MSc. Software Development

March 2017
Outline

Definitions
Perfect Secrecy
Perfect indistinguishability

Perfect secrecy in practice
The One-Time Pad
Limitations of Perfect Secrecy
Outline

Definitions

Perfect Secrecy
Perfect indistinguishability

Perfect secrecy in practice

The One-Time Pad
Limitations of Perfect Secrecy
Definitions
Common terms

- **Gen** is a probabilistic algorithm that outputs some $k \in \mathcal{K}$.
- $Enc_k(m)$ takes some message $m \in \mathcal{M}$ and encrypts it with $k$.
- $Dec_k(c)$ takes some ciphertext $c \in \mathcal{C}$ and decrypts it with $k$. 
The probability that $Gen$ outputs some $k$ is denoted by $Pr[K = k] = p$.

Perfect correctness entails that $Pr[Dec_k(Enc_k(m)) = m] = 1$. 
Definition 2.3
An encryption schema \((Gen, Enc, Dec)\) 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 \(Pr[C = c] > 0\):

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

Alternative definition
For every \(m, m' \in \mathcal{M}\) and every \(c \in \mathcal{C}\)

\[
Pr[Enc_k(m) = c] = Pr[Enc_k(m') = c]
\]
Outline

Definitions

Perfect Secrecy
Perfect indistinguishability

Perfect secrecy in practice
The One-Time Pad
Limitations of Perfect Secrecy
Definitions

Perfect indistinguishability

The adversarial indistinguishability experiment $\text{Priv}_{A,\Pi}^{\text{eav}}$

1. The adversary $A$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.
2. A key $k$ is generated using $\text{Gen}$, and a uniform bit $b \in \{0,1\}$ is chosen. Ciphertext $c \leftarrow \text{Enc}_k(m_b)$ is computed and given to $A$. We refer to $c$ as the challenge ciphertext.
3. $A$ outputs a bit $b'$.
4. The output of the experiment is defined to be 1 if $b = b'$, or otherwise 0. We write $\text{Priv}_{A,\Pi}^{\text{eav}} = 1$ if the output of the experiment is 1 and in this case we say that $A$ succeeds.
Definition 2.5
Encryption schema $\Pi = (Gen, Enc, Dec)$ with message space $\mathcal{M}$ is perfectly indistinguishable if for every $\mathcal{A}$ it holds that

$$\Pr [PrivK_{\mathcal{A},\Pi}^{eav} = 1] = \frac{1}{2}$$
Definitions
Perfect indistinguishability (example)

Exercise
Let $\Pi$ denote the Mono-Alphabetic Substitution cipher. How can we construct an adversary $A$ such that

$$Pr[\text{PrivK}_{A,\Pi}^{eav} = 1] > \frac{1}{2}$$

and thereby proof that $\Pi$ is not perfectly indistinguishable?
Answer

Adversary $A$ does:

1. Output $m_0 = aa$ and $m_1 = ab$.
2. Upon receiving the challenge ciphertext $c = c_1 c_2$, do the following: if $c_1 = c_2$ output 0, else output 1.

It is trivial to see that the adversary always succeeds and thus

$$Pr \left[ PrivK_{A,\Pi}^{eav} = 1 \right] = 1$$
Outline

Definitions
   Perfect Secrecy
   Perfect indistinguishability

Perfect secrecy in practice
   The One-Time Pad
   Limitations of Perfect Secrecy
The One-Time Pad (Vernam Cipher)

Definition

Construction 2.8
Fix an integer \( \ell > 0 \). The message space \( \mathcal{M} \), key space \( \mathcal{K} \), and ciphertext space \( \mathcal{C} \) are all equal to \( \{0, 1\}^{\ell} \).

- **Gen**: the key-generation algorithm chooses a key from \( \mathcal{K} = \{0, 1\}^{\ell} \) according to the uniform distribution.

- **Enc**: given a key \( k \in \{0, 1\}^{\ell} \) and a message \( m \in \{0, 1\}^{\ell} \), then the encryption algorithm outputs the ciphertext \( c := k \oplus m \).

- **Dec**: given a key \( k \in \{0, 1\}^{\ell} \) and a ciphertext \( c \in \{0, 1\}^{\ell} \), the decryption algorithm outputs the message \( m := k \oplus c \).
The One-Time Pad (Vernam Cipher)

Proof

Exercise
How can we proof that the One-Time Pad has perfect secrecy? What assumptions are needed?
Definitions
Perfect Secrecy

Definition 2.3
An encryption schema \((\text{Gen}, \text{Enc}, \text{Dec})\) 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 \(\Pr[C = c] > 0\):

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

Alternative definition
For every \(m, m' \in \mathcal{M}\) and every \(c \in \mathcal{C}\)

\[
\Pr[\text{Enc}_k(m) = c] = \Pr[\text{Enc}_k(m') = c]
\]
The One-Time Pad (Vernam Cipher)
Proof (continued)

Proof

\[
Pr[M = m \mid C = c] = \frac{Pr[C = c \mid M = m] \cdot Pr[M = m]}{Pr[C = c]}
\]

\[
= 2^{-\ell} \cdot Pr[M = m] \cdot \frac{2^{-\ell}}{2^{-\ell}}
\]

\[
= Pr[M = m]
\]

Assumptions

What happens if we use the same key more than once?

\[
c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m'
\]
Outline

Definitions
Perfect Secrecy
Perfect indistinguishability

Perfect secrecy in practice
The One-Time Pad
Limitations of Perfect Secrecy
The key and message space

Definition

Theorem 2.10
If \((\text{Gen}, \text{Enc}, \text{Dec})\) is a perfectly secret encryption schema with message space \(\mathcal{M}\) and key space \(\mathcal{K}\), then \(|\mathcal{K}| \geq |\mathcal{M}|\).
The key and message space

Proof

Theorem 2.10
Assume $|K| < |M|$ and let $\mathcal{M}(c)$ be the set of all possible messages that are possible decryptions of $c$.

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

If Dec is deterministic then clearly $|\mathcal{M}(c)| \leq |K|$. If $|K| < |M|$, then there is some $m' \in \mathcal{M}$ such that $m' \notin \mathcal{M}(c)$. But then

$$Pr[M = m' \mid C = c] = 0 \neq Pr[M = m']$$
Theorem 2.11
Let \((\text{Gen}, \text{Enc}, \text{Dec})\) be an encryption schema with message space \(\mathcal{M}\), for which \(|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|\). The schema is perfectly secret if and only if:

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

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 \(c\).
Shannon’s Theorem

Proof

For any distribution over $\mathcal{M}$, any $m \in \mathcal{M}$ with probability $Pr[M = m] \neq 0$, and any $c \in \mathcal{C}$, we have

$$Pr[M = m \mid C = c] = \frac{Pr[C = c \mid M = m] \cdot Pr[M = m]}{Pr[C = c]}$$

$$= \frac{Pr[\text{Enc}_k(m) = c] \cdot Pr[M = m]}{Pr[C = c]}$$

$$= \frac{|\mathcal{K}|^{-1} \cdot Pr[M = m]}{|\mathcal{K}|^{-1}} = Pr[M = m]$$