Perfect Secrecy

S. Zhong    Y. Zhang

Computer Science and Technology Dept.

2016 Fall
1. Brief reminders from probability:

2. Perfectly-Secret Encryption
   - Definition

3. The One-Time Pad (Vernam’s Cipher)

4. Limitations of Perfect Secrecy

5. Shannon’s Theorem
Let $X$ and $Y$ be two random variables, and let $\mathcal{X}$ and $\mathcal{Y}$ be the value spaces of $X$ and $Y$ respectively.

- The conditional probability of $X$ given $Y$ is
  \[
  Pr[X = x | Y = y] = \frac{Pr[X = x \& Y = y]}{Pr[Y = y]}. 
  \]

- $X$ and $Y$ are independent iff (if and only if) for all $x$ and $y$:
  \[
  Pr[X = x \& Y = y] = Pr[X = x] \cdot Pr[Y = y]. 
  \]

- Thus, $X$ and $Y$ are independent iff for all $x$ and $y$:
  \[
  Pr[X = x | Y = y] = Pr[X = x]. 
  \]
Let $X$ and $Y$ be two random variables, and let $\mathcal{X}$ and $\mathcal{Y}$ be the range spaces of $X$ and $Y$ respectively.

- **Bayes’ theorem:**

$$Pr[X = x | Y = y] = \frac{Pr[X = x] \cdot Pr[Y = y | X = x]}{Pr[Y = y]}.$$
Defining an encryption scheme

An encryption scheme $\Pi$, also called a cipher or a cryptosystem, is defined by three algorithms $\text{Gen}$, $\text{Enc}$, and $\text{Dec}$, as well as a specification of a finite message space $\mathcal{M}$ with $|\mathcal{M}| > 1$.

- **Gen**: a probabilistic algorithm that outputs a key $k$ uniformly chosen from a finite key space $\mathcal{K}$.
  
  \[ k \leftarrow \text{Gen}. \]

- **Enc**: an algorithm that takes as input a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext $c$:
  
  \[ c \leftarrow \text{Enc}_k(m) \text{(probabilistic)} \text{ OR } c := \text{Enc}_k(m) \text{(deterministic)}. \]

- **Dec**: a deterministic algorithm that takes as input a ciphertext $c$ from the set of all ciphertexts $\mathcal{C}$ and a key $k \in \mathcal{K}$, and outputs a message $m \in \mathcal{M}$.
  
  \[ m := \text{Dec}_k(c). \]
Probabilistic analysis on an encryption scheme (before encryption)

Consider the similar shift cipher $\Pi_{\text{shft1}}$:

**Gen:** $k \leftarrow \{0, \ldots, 25\}$.

**Enc:** $C = M + k \mod 26$.

$M = \{0, \ldots, 25\} \text{or}\{a, \ldots, z\}$.

- Q1: Say our message $M$ follows the distribution

  $Pr[M = b] = 0.6$ and $Pr[M = g] = 0.4$.

  What the probability that the ciphertext is $Z$ given $M$ as above?

- A: $Pr[C = Z] = Pr[M = b \land K = 24] + Pr[M = g \land K = 19]$
  
  $= Pr[M = b] \cdot Pr[K = 24] + Pr[M = g] \cdot Pr[K = 19]$

  $= 0.6 \cdot 1/26 + 0.4 \cdot 1/26 = 1/26$. 
Q2: Now we sample a message $M$ follows the distribution $Pr[M = b] = 0.6$ and $Pr[M = g] = 0.4$, encrypt it and get a ciphertext $Z$. What is the probability that $M = b$?

A: Based on Bayes’ Theorem, we have

$$Pr[M = b | C = Z] = \frac{Pr[M = b] \cdot Pr[K = 24 | M = b]}{Pr[C = Z]}$$

$$= \frac{Pr[M = b] \cdot \frac{1}{26}}{\frac{1}{26}} = Pr[M = b] = 0.6$$
Probabilistic analysis on another encryption scheme

Consider a similar shift cipher $\Pi_{\text{shift2}}$:

**Gen:** $k \leftarrow \{0, \ldots, 25\}$.

**Enc:** $C = M + k \mod 26$.

$\mathcal{M} = \{0, \ldots, 25\}^3 \text{or} \{a, \ldots, z\}^3$.

- **Q1:** Say our message $M$ follows the distribution

  $$Pr[M = \text{ann}] = 0.6 \text{ and } Pr[M = \text{bob}] = 0.4.$$  

  What the probability that the ciphertext is $DQQ$ given $M$ as above?

  - **A:** $Pr[C = DQQ] = Pr[M = \text{ann} \land K = 3] = 0.6 \cdot 1/26 = 3/130$.

- **Q2:** Now we sample a message $M$ follows the distribution

  $Pr[M = \text{ann}] = 0.6 \text{ and } Pr[M = \text{bob}] = 0.4.$, encrypt it and get a ciphertext $DQQ$. What the probability that $M = \text{ann}$?

  - **A:** 100%.

  Based on Bayes’ Theorem,

  $$Pr[M = \text{ann} | C = DQQ] = \frac{Pr[M=\text{ann}] \cdot Pr[K=3 | M=\text{ann}]}{Pr[C=DQQ]} = 1.$$
Definition 2.1 (Perfectly Secret Encryption).

An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) over a massage space \(\mathcal{M}\) is perfect secret if for every possible distribution over \(\mathcal{M}\),

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

holds for every \(m \in \mathcal{M}\) and every \(c \in \mathcal{C}\) that \(Pr[C = c] > 0\).
According to the definition, it is easy to know $\Pi_{shft2}$ is not perfectly-secret:

$$Pr[M = \text{ann}|C = DQQ] = 1 \neq Pr[M = \text{ann}] = 0.6.$$  

Q: Is $\Pi_{shft1}$ perfectly-secret?  
A: Probably yes, but we still need to prove it.
Revisiting $\Pi_{shft1}$ and $\Pi_{shft2}$

**Theorem 2.2.**

$\Pi_{shft1}$ is a perfectly-secret encryption scheme.

**Proof:** For any $m \in M = \{0, \ldots, 25\}$, any $c \in C$ and any possible distribution over $M$ we have:

\[
Pr[M = m|C = c] = \frac{Pr[M = m \land C = c]}{Pr[C = c]} = \frac{Pr[M = m] \cdot Pr[C = c|M = m]}{Pr[M = 0 \land C = c] + \ldots + Pr[M = 25 \land C = c]}
\]

\[
= \frac{Pr[M = m] \cdot Pr[k = c - m \mod 26]}{Pr[M = 0] \cdot Pr[C = c|M = 0] + \ldots + Pr[M = 25] \cdot Pr[C = c|M = 25]}
\]

\[
= Pr[M = m]Pr[k = c \mod 26] + \ldots + Pr[M = 25]Pr[k = c - 25 \mod 26] = Pr[M = m].
\]
An equivalent definition of perfect secrecy

We have an equivalent and useful formulation of perfect secrecy.

**Lemma 2.3.**

An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) over message space \(\mathcal{M}\) is perfectly secret if and only if for every \(m, m' \in \mathcal{M}\), and every \(c \in \mathcal{C}\):

\[
Pr[C = c|M = m] = Pr[C = c|M = m'].
\]

- This formulation states that the probability distribution over \(\mathcal{C}\) is independent of the plaintext.
- “It’s impossible to distinguish an encryption of \(m_0\) from an encryption of \(m_1\)”
An equivalent definition of perfect secrecy

Proof:
“⇐”: Assume \( Pr[C = c|M = m] = Pr[C = c|M = m'] \) holds for every possible \( m, m' \in \mathcal{M} \). We have:

\[
Pr[M = m|C = c] = Pr[M = m \land C = c]/Pr[C = c] = \frac{Pr[M = m] \cdot Pr[C = c|M = m]}{\sum_{m' \in \mathcal{M}} Pr[M = m' \land C = c]} \]

\[
= \frac{Pr[M = m] \cdot Pr[C = c|M = m]}{\sum_{m' \in \mathcal{M}} Pr[M = m'] \cdot Pr[C = c|M = m']} = Pr[M = m]
\]
An equivalent definition of perfect secrecy

**Proof (cont’d):** “⇒” : When $m' = m$, “⇒” is always true. Now we only consider $m' \neq m$. For every such $m' \in \mathcal{M}$, we can construct a message distribution such that $Pr[M = m] = 0.7$ and $Pr[M = m'] = 0.3$. According to the definition of perfect secrecy, we know for every $c \in C$:

\[
Pr[M = m] = Pr[M = m | C = c]
\]
\[
= Pr[M = m \land C = c] / Pr[C = c]
\]
\[
= Pr[M = m | C = c] / Pr[C = c]
\]
\[
= \frac{Pr[M = m] \cdot Pr[C = c | M = m]}{Pr[M = m'] \cdot Pr[C = c | M = m'] + Pr[M = m] \cdot Pr[C = c | M = m']}
\]

Therefore we have

\[Pr[C = c | M = m] = 0.3Pr[C = c | M = m'] + 0.7Pr[C = c | M = m],\]

and

\[Pr[C = c | M = m] = Pr[C = c | M = m'].\]
Perfect adversarial indistinguishability

Now we give a game-based definition of perfect secrecy on an encryption scheme $\Pi = \{\text{Gen}, \text{Enc}, \text{Dec}\}$ with message space $\mathcal{M}$. The adversarial indistinguishability game/experiment $PrivK^{eav}_{A,\Pi}$ between the adversary and a challenger:

1. The adversary $A$ chooses a pair of messages $m_0, m_1 \in \mathcal{M}$, and sends them to the challenger.
2. The challenger runs $\text{Gen}$ to generate a key $k$, chooses a uniform bit $b \in \{0, 1\}$, and computes the challenge ciphertext by encrypting $m_b$:
   $$c \leftarrow \text{Enc}_k(m_b).$$
3. The challenger sends $c$ to the adversary.
4. Based on $c$, the adversary guess the correct value of $b$, and outputs $b'$ as its answer to the challenge.
5. The output/result of the game is defined to 1:
   $$PrivK^{eav}_{A,\Pi} = 1$$
   if $b' = b$ ($A$ succeeds in the game), and 0 otherwise.
Perfect adversarial indistinguishability

Definition 2.4.

Perfect adversary indistinguishability Encryption scheme \( \Pi = (Gen, Enc, Dec) \) with message space \( \mathcal{M} \) is perfectly indistinguishable if for every \( \mathcal{A} \) it holds that

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

The definition states that every adversary would do no better or worse in the game than making a uniformly random guess.
Lemma 2.5.

Encryption scheme $\Pi = (Gen, Enc, Dec)$ with message space $\mathcal{M}$ is perfectly secret if and only if it is perfectly indistinguishable.
Example: let $\Pi$ denote the Vigenere cipher for the message space of two-character strings, and where the period is chosen uniformly in $\{1, 2\}$. We claim $\Pi$ is NOT perfectly indistinguishable. To prove this, we construct an adversary $A$ for which $Pr[PrivK_{A,\Pi}^eav] > \frac{1}{2}$. Specifically $A$ does:

1. Choose $m_0 = aa$ and $m_1 = ab$.
2. Upon receiving the challenge ciphertext $c = c_1c_2$, output $b = 0$ if $c_1 = c_2$, and $b = 1$ otherwise.

Now what does $Pr[PrivK_{A,\Pi}^eav = 1]$ equal?
Perfect (adversarial) indistinguishability

\[
Pr[PrivK_{A,\Pi}^{eav} = 1] = 0.5Pr[PrivK_{A,\Pi}^{eav} = 1|b = 0] + 0.5Pr[PrivK_{A,\Pi}^{eav} = 1|b = 1] = 0.5Pr[A \text{ outputs } 0|b = 0] + 0.5Pr[A \text{ outputs } 1|b = 1]
\]

In addition,
\[
Pr[A \text{ outputs } 0|b = 0] = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26}
Pr[A \text{ outputs } 1|b = 1] = 1 - Pr[A \text{ outputs } 0|b = 1] = 1 - \frac{1}{2} \cdot \frac{1}{26}
\]

Then, we have:
\[
Pr[PrivK_{A,\Pi}^{eav} = 1] = \frac{1}{2} \left( \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26} + 1 - \frac{1}{2} \cdot \frac{1}{26} \right) = 0.75 > \frac{1}{2}
\]

Therefore, \(\Pi\) is not perfectly indistinguishable.
The One-Time Pad, a perfectly-secret encryption scheme

The One-Time Pad

Let $a \oplus b$ denote the bitwise exclusive-or (XOR) of two binary strings $a$ and $b$, the One-Time Pad is as follows:

1. Fix an integer $l > 0$. $\mathcal{M} = \{0, 1\}^l$, $\mathcal{K} = \{0, 1\}^l$, $\mathcal{C} = \{0, 1\}^l$.
2. Gen: $K \leftarrow \mathcal{K}$, i.e. $Pr[K = k] = 1/2^l$ for every $k \in \mathcal{K}$.
3. $\text{Enc}_K(M)$: $C := M \oplus K$.
4. $\text{Dec}_K(C)$: $M := C \oplus K$.

Correctness: $M = C \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M$.
Secrecy: ?
Secrecy of One-Time Pad

**Theorem 3.1.**
The One-Time Pad is a perfectly-secret encryption scheme.

**Proof:** Fix arbitrary input distribution over $\mathcal{M}$, for every possible $m$ and $c$,

\[
Pr[M = m|C = c] \\
= Pr[M = m, C = c]/Pr[C = c] \\
= Pr[K = m \oplus c] \cdot Pr[M = m]/\sum_{m' \in \mathcal{M}} (Pr[M = m'] \cdot Pr[C = c|M = m']) \\
= Pr[K = m \oplus c] \cdot Pr[M = m]/\sum_{m' \in \mathcal{M}} (Pr[M = m'] \cdot Pr[K = m' \oplus c]) \\
= 2^{-l}Pr[M = m]/(2^{-l} \sum_{m' \in \mathcal{M}} Pr[M = m']) \\
= 2^{-l}Pr[M = m]/2^{-l} \\
= Pr[M = m]
\]
Limitations of One-Time Pad

Perfect secrecy sounds perfect. But any drawbacks?

- the key is required to be as long as the message.
  \[ M = 0111000011110001110101101000000000000011001 \ldots \]
  \[ K = 100011100001110001110001110101010000000000011 \ldots \]

- only secure if used once (with the same key).
  \[ C_1 = M_1 \oplus K; \quad C_2 = M_2 \oplus K \Rightarrow C_1 \oplus C_2 = M_1 \oplus M_2. \]

- only secure against ciphertext-only attack.
  \[ M = 101, \quad Enc_K(M) = 111 \Rightarrow K = 010 \]
Theorem 4.1. 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:** Consider the uniform distribution over \(\mathcal{M}\) (as the input), we know there is a \(c \in \mathcal{C}\) such that \(Pr[C = c] > 0\). According to the definition of perfect secrecy, we know for every \(m \in \mathcal{M}\),

\[
Pr[M = m | C = c] = Pr[M = m] = \frac{1}{|\mathcal{M}|} > 0,
\]

which implies there is at least one key \(k\) for each \(m\) such that \(\text{Dec}_k(c) = m\). Accordingly, there are at least \(|\mathcal{M}|\) different keys in \(\mathcal{K}\), one for each different \(m \in \mathcal{M}\). Thus, we have \(|\mathcal{K}| \geq |\mathcal{M}|\).
Theorem 5.1 (Shannon’s Theorem).

Let \((\text{Gen}, \text{Enc}, \text{Dec})\) be an encryption scheme over a message space \(\mathcal{M}\) for which \(|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|\). This scheme 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 single key \(k \in \mathcal{K}\) such that \(\text{Enc}_k(m)\) outputs \(c\).

- Only applies when \(|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|\).
- Useful for deciding whether a given scheme is perfectly secret.
Katz, J. and Lindell, Y..

Chapter 2 of “Introduction to modern cryptogrophy” (2nd ed).

*Chapman & Hall/CRC, 2014*