Perfectly Secret Encryption

Yu Zhang

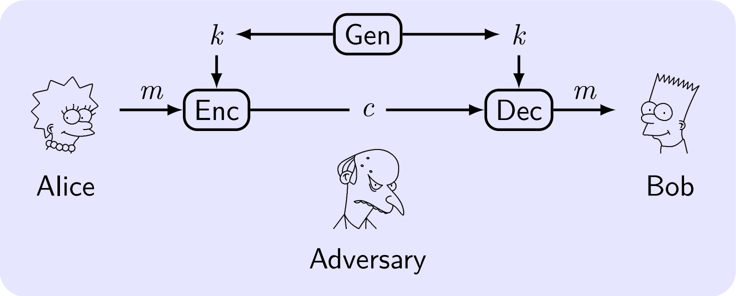
Harbin Institute of Technology

Cryptography, Autumn, 2015

Outline

Content

Recall The Syntax of Encryption



- $k \in \mathcal{K}, m \in \mathcal{M}, c \in \mathcal{C}$.
- $k \leftarrow \mathsf{Gen}$, $c := \mathsf{Enc}_k(m)$, $m := \mathsf{Dec}_k(c)$.
- **Encryption scheme**: $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.
- **Random Variable**: K, M, C for key, plaintext, ciphertext.
- **Probability**: $\Pr[K = k], \Pr[M = m], \Pr[C = c]$.
- What's the basic correctness requirement?

Definition of ‘Perfect Secrecy’

Intuition: An adversary knows the probability distribution over $\mathcal{M}$. c should have no effect on the knowledge of the adversary; the a *posteriori* likelihood that some m was sent should be no different from the a *priori* probability that m would be sent.

Definition 1

Π over $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, $\forall m \in \mathcal{M}$ and $\forall c \in \mathcal{C}$ for which $\Pr[C = c] > 0$:

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

Simplify: non-zero probabilities for $\forall m \in \mathcal{M}$ and $\forall c \in \mathcal{C}$.

Is the below scheme perfectly secret?

For $\mathcal{M} = \mathcal{K} = \{0, 1\}, \mathsf{Enc}_k(m) = m \oplus k$.

An Equivalent Formulation

Lemma 2

Π over $\mathcal{M}$ is perfectly secret $\iff$ for every probability distribution over $\mathcal{M}$, $\forall m \in \mathcal{M}$ and $\forall c \in \mathcal{C}$:

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

Proof.

$\Leftarrow$: Multiplying both sides by $\Pr[M = m] / \Pr[C = c]$, then use Bayes' Theorem.[1]
$\Rightarrow$: Multiplying both sides by $\Pr[C = c] / \Pr[M = m]$, then use Bayes' Theorem. $\square$

[1] If $\Pr[B] \neq 0$ then $\Pr[A|B] = (\Pr[A] \cdot \Pr[B|A]) / \Pr[B]$

Perfect Indistinguishability

Lemma 3

Π over $\mathcal{M}$ is perfectly secret $\iff$ for every probability distribution over $\mathcal{M}$, $\forall m_0, m_1 \in \mathcal{M}$ and $\forall c \in \mathcal{C}$:

$$\Pr[C = c | M = m_0] = \Pr[C = c | M = m_1].$$

Proof.

$\Rightarrow$: By Lemma **??**: $\Pr[C = c | M = m] = \Pr[C = c]$.

$\Leftarrow$: $p \stackrel{\text{def}}{=} \Pr[C = c | M = m_0]$.

$$\begin{aligned}\Pr[C = c] &= \sum_{m \in \mathcal{M}} \Pr[C = c | M = m] \cdot \Pr[M = m] \\ &= \sum_{m \in \mathcal{M}} p \cdot \Pr[M = m] = p = \Pr[C = c | M = m_0].\end{aligned}$$

$\square$

Content

One-Time Pad (Vernam's Cipher)

- $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$.
- Gen chooses a k randomly with probability exactly $2^{-\ell}$.
- $c := \mathsf{Enc}_k(m) = k \oplus m$.
- $m := \mathsf{Dec}_k(c) = k \oplus c$.

Theorem 4

The one-time pad encryption scheme is perfectly-secret.

Proof.

$$\begin{aligned}\Pr[C = c | M = m] &= \Pr[M \oplus K = c | M = m] \\ &= \Pr[m \oplus K = c] = \Pr[K = m \oplus c] = 2^{-\ell}.\end{aligned}$$

Then Lemma **??**: $\Pr[C = c | M = m_0] = \Pr[C = c | M = m_1]$. $\square$

Content

Limitations of OTP and Perfect Secrecy

Key k is as long as m, difficult to store and share k.

Theorem 5

Let Π be perfectly-secret over $\mathcal{M}$, and let $\mathcal{K}$ be determined by Gen*. Then $|\mathcal{K}| \geq |\mathcal{M}|$.*

Proof.

Assume $|\mathcal{K}| < |\mathcal{M}|$. $\mathcal{M}(c) \stackrel{\text{def}}{=} \{\hat{m} | \hat{m} = \mathsf{Dec}_k(c) \text{ for some } \hat{k} \in \mathcal{K}\}$, and $|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}|$. So $\exists m' \notin \mathcal{M}(c)$. Then

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

and so not perfectly secret. □

Two Time Pad: Real World Cases

Only used once for the same key, otherwise

$$c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m'.$$

Learn m from $m \oplus m'$ due to the redundancy of language.

MS-PPTP (Win NT)

k  Client

$$\xrightarrow{\quad [m_1 \| m_2 \| m_3] \oplus PRG(k) \quad}$$

$$\xleftarrow{\quad [s_1 \| s_2 \| s_3] \oplus PRG(k) \quad}$$

k  Server

Improvement: use two keys for C-to-S and S-to-C separately.

Content

Shannon's Theorem

Theorem 6

For $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$, Π *is perfectly secret* $\iff$

1. *Every* $k \in \mathcal{K}$ *is chosen with probability* $1/|\mathcal{K}|$ *by* Gen.
2. $\forall m \in \mathcal{M}$ *and* $\forall c \in \mathcal{C}$, $\exists$ *unique* $k \in \mathcal{K}$*:* $c := \mathsf{Enc}_k(m)$.

Proof.

$\Leftarrow$: $\Pr[C = c | M = m] = 1/|\mathcal{K}|$, use Lemma **??**.
$\Rightarrow (2)$: At least one k, otherwise $\Pr[C = c | M = m] = 0$;
at most one k, because $\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}} = \mathcal{C}$ and $|\mathcal{K}| = |\mathcal{C}|$.
$\Rightarrow (1)$: k_i is such that $\mathsf{Enc}_{k_i}(m_i) = c$.

$$\begin{aligned}
\Pr[M = m_i] &= \Pr[M = m_i | C = c] \\
&= (\Pr[C = c | M = m_i] \cdot \Pr[M = m_i]) \,/\, \Pr[C = c] \\
&= (\Pr[K = k_i] \cdot \Pr[M = m_i]) \,/\, \Pr[C = c],
\end{aligned}$$

so $\Pr[K = k_i] = \Pr[C = c] = 1/|\mathcal{K}|$. $\square$

Application of Shannon's Theorem

Is the below scheme perfectly secret?

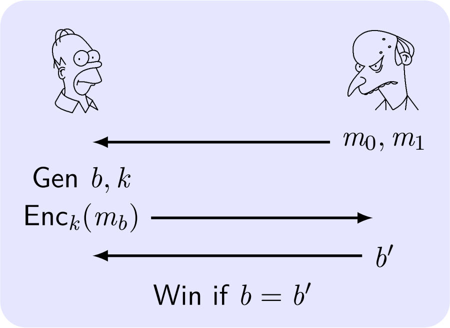
Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1, 2, \ldots, 255\}$
$\mathsf{Enc}_k(m) = m + k \mod 256$
$\mathsf{Dec}_k(c) = c - k \mod 256$

Content

Eavesdropping Indistinguishability Experiment

$\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ denote a **priv**ate-**k**ey encryption experiment for a given Π over $\mathcal{M}$ and an **eav**esdropping adversary $\mathcal{A}$.

1. $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.
2. $k \leftarrow \mathsf{Gen}$, a random bit $b \leftarrow \{0, 1\}$ is chosen. Then $c \leftarrow \mathsf{Enc}_k(m_b)$ is given to $\mathcal{A}$.
3. $\mathcal{A}$ outputs a bit b'
4. If $b' = b$, $\mathcal{A}$ succeeded $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1$, otherwise 0.



Adversarial Indistinguishability

Definition 7

Π over $\mathcal{M}$ is **perfectly secret** if for every $\mathcal{A}$ it holds that

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

Which in the below schemes are perfectly secret?

- $\mathsf{Enc}_{k,k'}(m) = \mathsf{OTP}_k(m) \| \mathsf{OTP}_{k'}(m)$
- $\mathsf{Enc}_k(m) = reverse(\mathsf{OTP}_k(m))$
- $\mathsf{Enc}_k(m) = \mathsf{OTP}_k(m) \| k$
- $\mathsf{Enc}_k(m) = \mathsf{OTP}_k(m) \| \mathsf{OTP}_k(m)$
- $\mathsf{Enc}_k(m) = \mathsf{OTP}_{0^n}(m)$
- $\mathsf{Enc}_k(m) = \mathsf{OTP}_k(m) \| LSB(m)$

Summary

- Perfect secrecy = Perfect indistinguishability = Adversarial indistinguishability
- Perfect secrecy is attainable. The One-Time Pad (Vernam's cipher)
- Shannon's theorem