

# Perfectly Secret Encryption

Yu Zhang

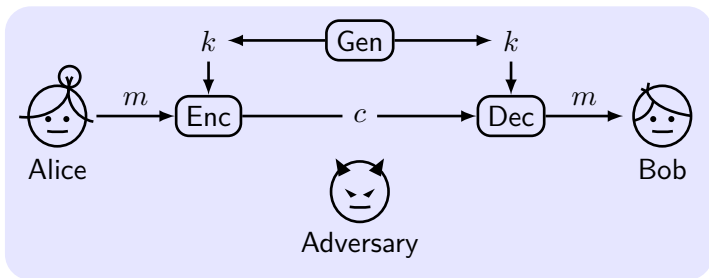
Harbin Institute of Technology

Cryptography, Autumn, 2020

- 1** Definitions and Basic Properties
- 2** The One-Time Pad (Vernam's Cipher)
- 3** Limitations of Perfect Secrecy
- 4** Shannon's Theorem
- 5** Eavesdropping Indistinguishability

- 1 Definitions and Basic Properties**
- 2 The One-Time Pad (Vernam's Cipher)
- 3 Limitations of Perfect Secrecy
- 4 Shannon's Theorem
- 5 Eavesdropping Indistinguishability

# Recall The Syntax of Encryption



- $k \in \mathcal{K}, m \in \mathcal{M}, c \in \mathcal{C}$ .
- $k \leftarrow \text{Gen}, c := \text{Enc}_k(m), m := \text{Dec}_k(c)$ .
- **Encryption scheme:**  $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ .
- **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

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

# Perfect Secrecy On One Bit

## XORing one bit is perfectly secret.

Let  $\Pr[M = 1] = p$  and  $\Pr[M = 0] = 1 - p$ . Let us consider a case that  $M = 1$  and  $C = 1$ .

$$\begin{aligned}\Pr[M = 1|C = 1] &= \Pr[C = 1|M = 1] \cdot \Pr[M = 1] / \Pr[C = 1] \\ &= \frac{\Pr[K = 1 \oplus 1] \cdot p}{\Pr[C = 1|M = 1] \cdot \Pr[M = 1] + \Pr[C = 1|M = 0] \cdot \Pr[M = 0]} \\ &= \frac{1/2 \cdot p}{1/2 \cdot p + 1/2 \cdot (1 - p)} = p = \Pr[M = 1]\end{aligned}$$

We can do the same for other cases.

Note that  $\Pr[M = 1|C = 1] \neq \Pr[M = 1, C = 1] = \Pr[C = 1|M = 1] \cdot \Pr[M = 1] = 1/2 \cdot p$ .

# An Equivalent Formulation

## Lemma 2

$\Pi$  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.<sup>1</sup>

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

---

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

# Perfect Indistinguishability

## Lemma 3

$\Pi$  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 2:  $\Pr[C = c | M = m] = \Pr[C = c]$ .

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

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





- 1 Definitions and Basic Properties
- 2 The One-Time Pad (Vernam's Cipher)**
- 3 Limitations of Perfect Secrecy
- 4 Shannon's Theorem
- 5 Eavesdropping Indistinguishability

# One-Time Pad (Vernam's Cipher)

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

## 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 3:  $\Pr[C = c | M = m_0] = \Pr[C = c | M = m_1]$ . □

- 1 Definitions and Basic Properties
- 2 The One-Time Pad (Vernam's Cipher)
- 3 Limitations of Perfect Secrecy**
- 4 Shannon's Theorem
- 5 Eavesdropping Indistinguishability

# Limitations of OTP and Perfect Secrecy

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

## Theorem 5

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

## Proof.

Assume  $|\mathcal{K}| < |\mathcal{M}|$ .  $\mathcal{M}(c) \stackrel{\text{def}}{=} \{\hat{m} \mid \hat{m} = \text{Dec}_k(c) \text{ for some } \hat{k} \in \mathcal{K}\}$ . Since for one  $k$ , there is at most one  $m$  such that  $m = \text{Dec}_k(c)$ ,  $|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}|$ . So  $\exists m' \notin \mathcal{M}(c)$ . Then

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

and so not perfectly secret. □

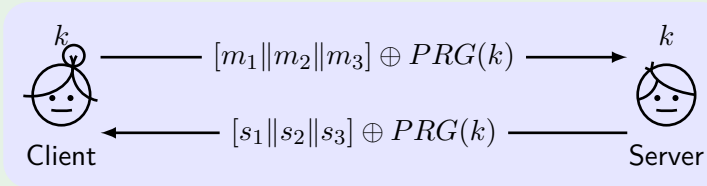
# Two Time Pad: Real World Cases

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)



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

- 1 Definitions and Basic Properties
- 2 The One-Time Pad (Vernam's Cipher)
- 3 Limitations of Perfect Secrecy
- 4 Shannon's Theorem**
- 5 Eavesdropping Indistinguishability

# Shannon's Theorem

## Theorem 6

For  $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ ,  $\Pi$  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  $k \in \mathcal{K}$ :  $c := \text{Enc}_k(m)$ .

## Proof.

$\Leftarrow$ :  $\Pr[C = c|M = m] = 1/|\mathcal{K}|$ , use Lemma 3.

$\Rightarrow$  (2): At least one  $k$ , otherwise  $\Pr[C = c|M = m] = 0$ ;  
at most one  $k$ , because  $\{\text{Enc}_k(m)\}_{k \in \mathcal{K}} = \mathcal{C}$  and  $|\mathcal{K}| = |\mathcal{C}|$ .

$\Rightarrow$  (1):  $k_i$  is such that  $\text{Enc}_{k_i}(m_i) = c$ .

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

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

# Application of Shannon's Theorem

**Is the below scheme perfectly secret?**

Let  $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1, 2, \dots, 255\}$

$\text{Enc}_k(m) = m + k \pmod{256}$

$\text{Dec}_k(c) = c - k \pmod{256}$

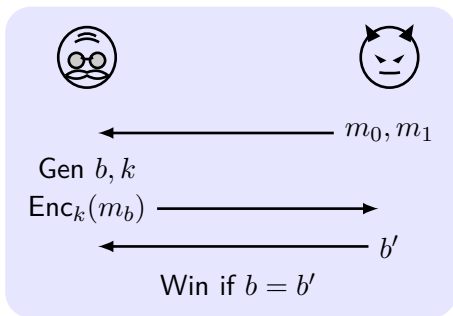


- 1 Definitions and Basic Properties
- 2 The One-Time Pad (Vernam's Cipher)
- 3 Limitations of Perfect Secrecy
- 4 Shannon's Theorem
- 5 Eavesdropping Indistinguishability**

# Eavesdropping Indistinguishability Experiment

$\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}}$  denote a **private-key** encryption experiment for a given  $\Pi$  over  $\mathcal{M}$  and an **eavesdropping** adversary  $\mathcal{A}$ .

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



## Definition 7

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

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

Which in the below schemes are perfectly secret?

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

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