完美保密

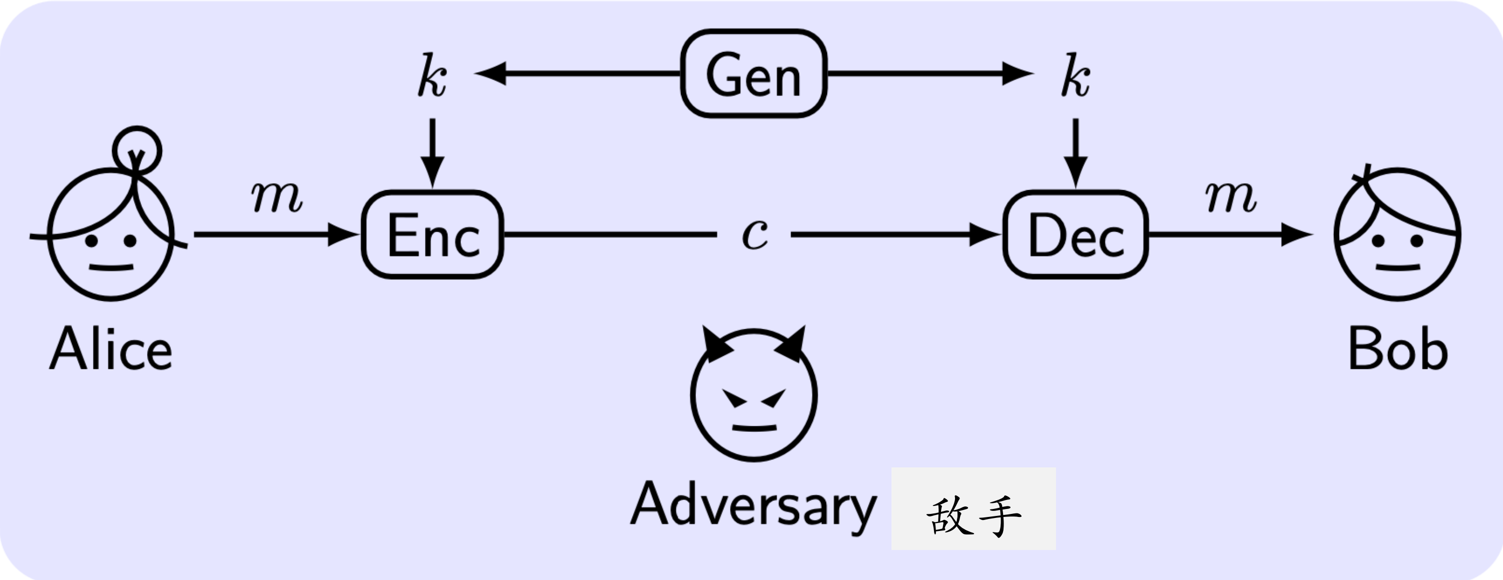
哈尔滨工业大学

张宇

2024春

目录

回顾加密词法



密钥 明文 密文

- key $k \in \mathcal{K}$, plaintext (or message) $m \in \mathcal{M}$, ciphertext $c \in \mathcal{C}$
- **Key-generation** algorithm $k \leftarrow \mathsf{Gen}$ 密钥生成算法
- **Encryption** algorithm $c := \mathsf{Enc}_k(m)$ 加密算法
- **Decryption** algorithm $m := \mathsf{Dec}_k(c)$ 解密算法
- **Encryption scheme**: $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 加密方案
- **Basic correctness requirement**: $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

基本正确性要求

完美保密定义

- 直觉：一个加密方案是安全的，那么敌手在获得密文后，密文应该对敌手猜测明文没有任何帮助。
- 换句话说，根据密文来猜测答案和不知道密文猜测答案对敌手来说是一样的。从概率的角度看，在获得密文后的某个明文后验似然（posteriori likehood）与该明文被发送的先验概率（priori probability）没有差别。

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 $\Pr[C = c] > 0$:

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

一比特异或加密

Is the below scheme perfectly secret?

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

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 $C = 1$.

$$\Pr[M = 1 | C = 1] = \Pr[C = 1 | M = 1] \cdot \Pr[M = 1] / \Pr[C = 1]$$

$$= \frac{\Pr[K = 1 \oplus 1] \cdot p}{\Pr[C = 1 | M = 1] \cdot \Pr[M = 1] + \Pr[C = 1 | M = 0] \cdot \Pr[M = 0]}$$

$$= \frac{1/2 \cdot p}{1/2 \cdot p + 1/2 \cdot (1 - p)} = p = \Pr[M = 1]$$

We can do the same for other cases.

注意：加密事件逻辑是从明文和密钥得到密文，而不是相反

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

等价定义

在完美保密中，密文出现概率独立于明文的某个量。

Lemma 2

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

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

不可区分性（indistiguishability）：任意明文被加密，某密文出现的概率相同，即给定2个明文与1个密文，不足以区分出是哪个明文加密得到了密文。

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* $\forall c \in \mathcal{C}$:

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

一次一密（One Time Pad）

- $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$.
- 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.

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

Then Lemma 3: $\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1]$. $\square$

完美保密局限性

- 密钥与明文一张长，难以存储和共享

Theorem 5

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

- 采用反证法证明，假设密钥数量比明文数量少$|\mathcal{K}| < |\mathcal{M}|$，则不可能实现完美保密。
- 将从一个密文c解密得到的所有明文集合，表示为$\mathcal{M}(c) \stackrel{\text{def}}{=} \{\hat{m} | \hat{m} = \mathsf{Dec}_k(c) \text{ for some } \hat{k} \in \mathcal{K}\}$。
- 对于一个密钥k，最多有个一个明文m使得$m = \mathsf{Dec}_k(c)$。这是因为如果有多个明文的话，就根本不是一个加密方案。
- 因此，从一个密文解密出来的明文数量不会超过密钥数量，也就不超过明文总数：$|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}|$.
- 那么，一定存在一个明文m'是无法由c解密出来的，即 $\Pr[M = m' | C = c] = 0 \neq \Pr[M = m']$。因此，不是完美保密。

二次加密：案例

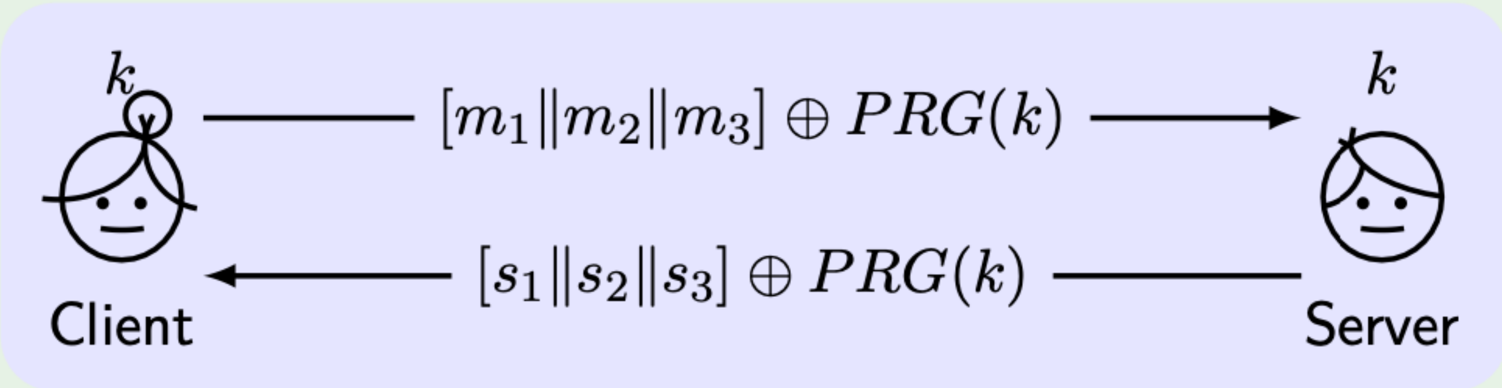
- 双方通信，每个传递方向应使用不同密钥

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.

香农定理

- 更具可操作性的完美保密定义

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 3.
$\Rightarrow$ (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 $\Pr[K = k_i] = \Pr[C = c] = 1/|\mathcal{K}|$. □

香农定理应用

Is the below scheme perfectly secret?

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

- 是，理由如下：
  - 满足明文空间、密文空间、密钥空间一样规模
  - 满足条件1：密钥是等概率随机产生的
  - 满足条件2：对于任意明文和密文对，存在唯一的密钥使得该明文加密成该密文。

课上练习

Which in the below schemes are perfectly secret?

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

本节小结

信息论意义上的安全——完美保密。完美保密的安全在信息论上是无需前提假设的，但其存在实践上的局限性，是完美中的不完美。

- 完美保密 = 完美不可区分
  - 知道密文对猜测明文没有帮助
  - 给定明文对推测密文没有帮助
  - 任意明文加密成某个密文的概率是相同的
- 完美保密是可实现的：一次一密
- 香农定理（可操作的完美保密）