Perfect Secrecy and One Time Pad Notes

Songyue Wang (sywang@cs.hku.hk)
HKU-COMP3357
Spring 2023

1 Perfect Secrecy

1.1 Definition of Perfect Secrecy

An encryption scheme (Gen, Enc,Dec) with message space M is perfectly secret if for every probability distribution over M, every message $m \in M$, and every ciphertext $c \in C$ for which $Pr[C = c] > 0$:

$$Pr[M = m|C = c] = Pr[M = m] \tag{1}$$

For an adversary with **unlimited computational power**, the ciphertext **does not leak any** information about the underlying message.

2 One Time Pad

2.1 Definition of One Time Pad

- *Gen*: choose a uniform binary string from $K = \{0, 1\}^l$.
- *Enc*: given key k and message $m \in \{0, 1\}^l$, compute cipher text $c := k \oplus m$.
- *Dec*: given key k and message $c \in \{0, 1\}^l$, compute plaintext $m := k \oplus c$.

2.2 Proof of Perfect Secrecy for OTP

For arbitary $c \in C$, $m' \in M$ and uniformed selected $k \in \{0, 1\}^l$, we compute:

$$Pr[C = c|M = m'] = Pr[Enc_k(m') = c] = 2^{-l} \tag{2}$$

$$\begin{aligned} Pr[C = c] &= \sum_{m' \in M} Pr[C = c|M = m'] \cdot Pr[M = m'] \\ &= 2^{-l} \cdot \sum_{m' \in M} Pr[M = m'] \\ &= 2^{-l} \end{aligned} \tag{3}$$

Use Bayes' Theorem,

$$\begin{aligned} Pr[M = m|C = c] &= \frac{Pr[C = c|M = m] \cdot Pr[M = m]}{Pr[C = c]} \\ &= \frac{2^{-l} \cdot Pr[M = m']}{2^{-l}} \\ &= Pr[M = m] \end{aligned} \tag{4}$$

Regardless of the cipher text, the adversary can only guess the message with **priori probabilities** (no extra information leaked).

2.3 Points to Note

- Reusing the same pad will be unsecure.

We have 2 messages with equal length, which are encrypted with the same pad:

$$\begin{aligned} m_1 \oplus k = c_1 \\ m_2 \oplus k = c_2 \end{aligned} \tag{5}$$

The adversary can simply XOR two cipher texts:

$$c_1 \oplus c_2 = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2 \tag{6}$$

If some bits in $m_1 \oplus m_2$ are 0, it can be concluded that the the corresponding bits in m_1 and m_2 are the same, if $m_1 \oplus m_2$ is an all-zero bit string, we know the same message is being sent twice.

- The OTP inherits the limitation of perfect secret encryption scheme. If the mssage space is M and key space is K, then $|K| \geq |M|$.

Proof:
Assume $|K| < |M|$, and $M(c) \stackrel{\text{def}}{=} m|m = Dec_k(c)$ for some $k \in K$.
As $|M(c)| \leq |K|$, there is some $m' \in M$ s.t. $m' \notin M(c)$ Therefore for these messages,

$$Pr[M = m'|C = c] = 0 \tag{7}$$

Which is not equal to **priori probabilities**.