2 – Perfectly Secret Encryption

Eklavya Sharma

Random number generation: Requires high-entropy data and a process for creating unbiased independent bits from it.

Contents

1 Formal definitions of security

There are multiple definitions of security.

Let $\Pi = (\mathcal{M}, \mathcal{K}, \mathcal{C}, \mathsf{Gen}, e, d)$ be the encryption scheme under consideration. We will consider ciphertext-only attack by an adversary with unbounded computational power. Let $M \in \mathcal{M}, K \in \mathcal{K}, C \in \mathcal{C}$ be the random variables corresponding to the message, key and ciphertext.

Definition 1. Π *is secure iff*

$$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, (P[C = c] > 0 \implies P[M = m|C = c] = P[M = m])$$

Definition 2. Π *is secure iff*

$$\forall m \in \mathcal{M}, \forall m' \in \mathcal{M}, \forall c \in \mathcal{C}, P[C = c|M = m] = P[C = c|M = m']$$

Definition 3 (Perfect indistinguishability)**.** *The adversarial indistinguishability experiment* $PrivK^{eav}_{A,\Pi}$*:*

- *The adversary A outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.*
- *A key k is generated using* Gen*, and a uniform bit $b \in \{0, 1\}$ is chosen. Ciphertext $c = e_k(m_b)$, called the challenge ciphertext, is computed and given to A.*

- *A outputs a bit b'.*
- *The output of the experiment is defined as*

$$PrivK^{\text{eav}}_{A,\Pi} = \begin{cases} 1 & \text{if } b' = b \\ 0 & \text{if } b' = b \end{cases}$$

Π *is perfectly indistinguishable iff* $P[PrivK^{eav}_{A,\Pi} = 1] = \frac{1}{2}$.

Theorem 1. *All of the above definitions of security are equivalent.*

2 One-time Pad

The one-time pad is the encryption scheme where:

- $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^l$.
- Gen chooses a key uniformly randomly from $\mathcal{K}$.
- $e_k(x) = d_k(x) = x \oplus k$.

Theorem 2. *The one-time pad is a perfectly secure encryption scheme.*

3 Limitations of perfect security

Theorem 3. $(\mathcal{M}, \mathcal{K}, \mathcal{C}, \mathsf{Gen}, e, d)$ *is perfectly secure* $\implies |\mathcal{K}| \geq |\mathcal{M}|$.

Hint. Consider $\mathcal{M}(c) = \{d_k(c) : k \in \mathcal{K}\}$. Show that $|\mathcal{M} - \mathcal{M}(c)| > 0$. □

4 Shannon's theorem

Theorem 4. *Let* $\Pi = (\mathcal{M}, \mathcal{K}, \mathcal{C}, \mathsf{Gen}, e, d)$ *and* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. Π *is a perfectly secure encryption scheme iff both of the following are true:*

- Gen *chooses every key with equal probability* $1/|\mathcal{K}|$.
- $\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, |\{k : e_k(m) = c\}| = 1$.