I. Perfect secrecy

Definition 0 A private or symmetric encryption scheme consists of three algorithms Gen, Enc, Dec.

1. The key generation algorithm outputs a key k, according to some distribution on the key space K.

2. The encryption algorithm Enc, on input a key k and a plaintext message m from message space P, outputs a ciphertext c, $Enc_k(m) =: c$.

3. The decryption algorithm Dec, on input a key k and a ciphertext c from a cipher space C, outputs a plaintext message m, $Dec_k(c) =: m$.

$\forall k \in K, m \in P$: $Dec_k(Enc_k(m)) = m$

Basic concepts

$\Pr[P=m]$ denotes probability distribution on P.

$\Pr[K=k]$ denotes probability distribution on K (given by Gen).

distributions are independent

induced distribution on C:

$$\Pr[C=c] = \sum_{\{(m,k):Enc_k(m)=c\}} \Pr[P=m \wedge K=k]$$

$$= \sum_{\{(m,k):Enc_k(m)=c\}} \Pr[P=m]\cdot\Pr[K=k]$$

$$\Pr\left[P=m \middle| C=c\right] = \Pr\left[P=m \wedge C=c\right]/\Pr\left[C=c\right]$$

$$= \sum_{\{k:Enc_k(m)=c\}} \Pr\left[P=m\right]\cdot\Pr\left[K=k\right]/\Pr\left[C=c\right]$$

Definition

Definition 1.1 An encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space P, key space K, and cipher space C is perfectly secret if for every distribution over P, every $m \in P$, and every $c \in C$ with $\Pr[C = c] > 0$:

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

Equivalent definition

Definition 1.2 Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be an encryption scheme with message space P, key space K, and cipher space C. For $m \in P$ and $c \in C$ we set

$$\Pr[\text{Enc}_K(m) = c] := \sum_{\{k \in K | \text{Enc}_k(m) = c\}} \Pr[K = k].$$

Lemma 1.3 Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be an encryption scheme with message space P, key space K, and cipher space C. Let $\Pr[P = \cdot]$ be a distribution on P. For every $c \in C$ and every $m \in P$ with $\Pr[P = m] > 0$:

$$\Pr[\text{Enc}_K(m) = c] = \Pr[C = c \mid P = m].$$

Equivalent definition

Lemma 1.4 An encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space P, key space K, and cipher space C is perfectly secret if and only if for every $m_0, m_1 \in P$, and every $c \in C$:

$$\Pr[\text{Enc}_K(m_0) = c] = \Pr[\text{Enc}_K(m_1) = c].$$

Remark The equivalent formulation for perfect secrecy uses no distributions on P.

One-time-pad

$l \in \mathbb{N},\ P = C = K = \{0,1\}^l$

- Gen: chooses $k \in \{0,1\}^l$ uniformly
- Enc: $\mathrm{Enc}_k(m) := m \oplus k$
- Dec: $\mathrm{Dec}_k(c) := c \oplus k$

Theorem 1.5 The one-time-pad is perfectly secret.

Shannon's theorem

Theorem 1.6 Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be an encryption scheme with $|P| = |C| = |K|$. Scheme Π is perfectly secret if and only if

1. Gen chooses every $k \in K$ with probability $1/|K|$.
2. For every $m \in P, c \in C$ there exists a unique key $k \in K$ with $\text{Enc}_k(m) = c$.

The indistinguishability game

Eavesdropping indistinguishability game $\mathrm{PrivK}^{eav}_{A,\Pi}$

1. A key k is chosen with Gen.
2. A chooses 2 plaintexts $m_0, m_1 \in P$.
3. $b \leftarrow \{0,1\}$ chosen uniformly. $c := \mathrm{Enc}_k(m_b)$ and c is given to A.
4. A outputs bit b'.
5. Output of experiment is 1, if $b = b'$, otherwise output is 0.

Write $\mathrm{PrivK}^{eav}_{A,\Pi} = 1$, if output is 1. Say A has succeded or A has won.

Theorem 1.7 $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is perfectly secret if and only if for every adversary A $\Pr\left[\mathrm{PrivK}^{eav}_{A,\Pi} = 1\right] = 1/2$.