Katz, Lindell
Introduction to Modern Cryptrography
Slides Chapter 2

Markus Bläser, Saarland University

Some notation

- Gen defines a *probability distribution* on the key space $\mathcal{K}$.
- K will usually be a random variable denoting the key output by Gen.
- $\Pr[\mathrm{K} = \mathrm{k}]$ is the probability that the key output by Gen is $\mathrm{k} \in \mathcal{K}$.

- M will usually be a random variable denoting the message from $\mathcal{M}$ to be encrypted.
  We assume some knowledge on the distribution of messages.
- $\Pr[\mathrm{M} = \mathrm{m}]$ denotes the probability that $\mathrm{m} \in \mathcal{M}$ shall be encrypted.

K and M are independent!

Some notation (2)

- Enc takes a key $k \in \mathcal{K}$ and message $m \in \mathcal{M}$ and outputs a ciphertext c.
- $c := \mathrm{Enc}_k(m)$ (deterministic)
- $c \leftarrow \mathrm{Enc}_k(m)$ (probabilistic)

- Dec takes a key $k \in \mathcal{K}$ and a ciphertext $c \in \mathcal{C}$ and outputs a message m.
- We assume *perfect correctness:* $\mathrm{Dec}_k(c) = m$ for every c potentially output by $\mathrm{Enc}_k(m)$.
- W.l.o.g. Dec is deterministic.

- distribution on $\mathcal{C}$: choose a key k with Gen and a message m according to the given distribution and output $c \leftarrow \mathrm{Enc}_k(m)$.
- C usually denotes a random variable with this distribution.

Perfect secrecy

Definition (Perfect secrecy, 2.3)

An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *perfectly secret* if for any probability distribution over $\mathcal{M}$, every $\mathrm{m} \in \mathcal{M}$, and every $\mathrm{c} \in \mathcal{C}$ with $\Pr[\mathrm{C} = \mathrm{c}] > 0$,

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

"The ciphertext does not tell you anything about the message."

Equivalent definitions

Lemma (2.4)

(Gen, Enc, Dec) *is perfectly secret iff*

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[\mathsf{Enc}_K(m') = c]$$

for all $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$.

"Two messages produce the same distribution on the ciphertexts."

Adversarial indistinguishability experiment

Scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, adversary $\mathcal{A}$

1. $\mathcal{A}$ outputs a pair $m_0, m_1 \in \mathcal{M}$
2. $k \in \mathcal{K}$ is generated using Gen.
   $b \in \{0, 1\}$ is chosen uniformly at random.
   $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. ("challenge")
3. $\mathcal{A}$ outputs bit b'
4. $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = \begin{cases} 1 & b = b' \\ 0 & \text{otherwise} \end{cases}$.
   $\mathcal{A}$ *succeeds* when results is 1.

eav = eavesdropper

Perfect indistinguishability

Definition (2.5)

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *perfectly indistinguishable* if for every $\mathcal{A}$:

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

"No advantage over random guessing."

Lemma (2.6)

Π *is perfectly secret iff it is perfectly indistinguishable.*

One-time pad (Vernam 1917)

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

- Gen generates a key uniformly at random
- Enc outputs $c := m \oplus k$ (on input (k, m))
- Dec outputs $m := c \oplus k$ (on input (k, c))

$\oplus$: bitwise exclusive-or

Theorem (2.9)

The one-time pad is perfectly secret.

Limitations of perfect secrecy

Theorem (2.10)

If $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is perfectly secret, then* $|\mathcal{K}| \geq |\mathcal{M}|$.

Perfect secrecy $\longrightarrow$ at least as many keys as messages