II. Pseudorandom generators & encryption

perfect secrecy

- too much (adversary learns nothing, has unlimited resources)
- too little (only eavesdropping allowed)
- too expensive (true randomness)

➔ pseudorandomness, restricted adversaries, different types of attacks.

Notation

- S set: $x \leftarrow S$, x chosen uniformly from S.
- A probabilistic algorithm: $x \leftarrow A(w)$, x chosen according to distribution generated by A on input w.

Private key encryption schemes

Definition 2.1 A private key encryption scheme Π consists of three probabilistic polynomial time algorithms Gen, Enc, Dec.

1. Gen on input 1^n outputs a key $k \in \{0,1\}^n$, $k \leftarrow Gen(1^n)$

2. Enc on input a key k and a plaintext message $m \in \{0,1\}^*$, outputs a ciphertext c, $c \leftarrow Enc_k(m)$.

3. Dec on input a key k and a ciphertext $c \in \{0,1\}^*$, outputs a plaintext message m, $m \leftarrow Dec_k(c)$.

Property $\forall k, m : Pr[Dec_k(Enc_k(m)) = m] = 1$.

If Enc with $k \leftarrow Gen(1^n)$ works only for $m \in \{0,1\}^{l(n)}$, $l : \mathbb{N} \rightarrow \mathbb{N}$ a polynomial, then Π is called **fixed-length encryption scheme**.

Negligible functions

Definition 2.2 A function $\mu : \mathbb{N} \to \mathbb{R}^+$ is called negligible, if

$$\forall c \in \mathbb{N}\ \exists n_0 \in \mathbb{N}\ \forall n \geq n_0\ \mu(n) \leq 1/n^c.$$

The indistinguishability game

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

1. A key k is chosen with Gen.
2. A chooses 2 plaintexts $m_0, m_1 \in P$ with $|m_0| = |m_1|$
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.

Indistinguishable encryptions

Definition 2.3 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ has indistinguishable encryptions (against eavesdropping adversaries) if for every probabilistic polynomial time algorithm A there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that

$$\Pr\left[\text{PrivK}_{A,\Pi}^{\text{eav}}(n) = 1\right] \leq 1/2 + \mu(n).$$

Remarks

1. Only consider polynomial time adversaries, not unbounded adversaries as in perfect secrecy.

2. Allow success probability slightly, i.e. negligibly larger than 1/2 (perfect secrecy =1/2).

Indistinguishable encryptions and prediction

Theorem 2.4 Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a fixed length encryption scheme with message length $l : \mathbb{N} \to \mathbb{N}$ that has indistinguishable encryptions. For all ppts A there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that for all $n \in \mathbb{N}$, and all $1 \le i \le l(n)$

$$\Pr\left[A\left(1^n, \text{Enc}_k(m)\right) = m_i\right] \le 1/2 + \mu(n),$$

where $m \leftarrow \{0,1\}^{l(n)}$, $m = m_1 \ldots m_{l(n)}$, $k \leftarrow \text{Gen}(1^n)$.

From prediction to distinction

A on input 1^n

- $m_0 \leftarrow I_0^n$, $m_1 \leftarrow I_1^n$.
- Upon receiving c, simulate $\tilde{A}$ on c, $b' \leftarrow \tilde{A}(c)$.
- Output b'.

$$I_0^n = \left\{m \in \{0,1\}^{l(n)} : m_i = 0\right\}$$

$$I_1^n = \left\{m \in \{0,1\}^{l(n)} : m_i = 1\right\}$$

Pseudorandom generators

Definition 2.5 Let $l : \mathbb{N} \to \mathbb{N}$ be a polynomial with $l(n) > n$ for all $n \in \mathbb{N}$. A deterministic polynomial time algorithm G is a pseudorandom generator if

1. $\forall s \in \{0,1\}^* \quad |G(s)| = l(|s|)$,
2. For every ppt D there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that $\forall n \in \mathbb{N}$
$$\left|\Pr[D(r)=1] - \Pr[D(G(s))=1]\right| \leq \mu(n),$$
where $r \leftarrow \{0,1\}^{l(n)}$ and $s \leftarrow \{0,1\}^n$.

l is called the expansion factor of G.

PRGs and encryption

Construction 2.6 Let $l : \mathbb{N} \to \mathbb{N}$ be a polynomial with $l(n) > n$ for all $n \in \mathbb{N}$ and let G be a deterministic algorithm with $|G(s)| = l(|s|)$ for all $s \in \{0,1\}^*$. Define fixed length encryption scheme $\Pi_G = (\text{Gen}, \text{Enc}, \text{Dec})$ with message length l by

$$\text{Gen}(1^n): \quad k \leftarrow \{0,1\}^n,$$

$$\text{Enc}_k(m): \quad c \leftarrow m \oplus G(k), m \in \{0,1\}^{l(n)},$$

$$\text{Dec}_k(c): \quad m \leftarrow c \oplus G(k), m \in \{0,1\}^{l(n)}.$$

Theorem 2.7 If G is a pseudorandom generator, then Π_G has indistinguishable encryption against eavesdropping adversaries.

The indistinguishability game

Let A be a probabilistic polynomial time algorithm (ppt).

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.

Indistinguishable encryptions

Definition 2.3 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ has indistinguishable encryptions (against eavesdropping adversaries) if for every probabilistic polynomial time algorithm A there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that

$$\Pr\left[\text{PrivK}^{\text{eav}}_{A,\Pi}(n) = 1\right] \le 1/2 + \mu(n).$$

From adversaries to distinguishers

D on input $w \in \{0,1\}^{l(n)}$ and 1^n

1. Simulate $A(1^n)$ to obtain messages $m_0, m_1 \in \{0,1\}^{l(n)}$.
2. $b \leftarrow \{0,1\}$, $c := w \oplus m_b$.
3. Simulate $A(1^n, c)$ to obtain b'. If $b = b'$, output 1, otherwise output 0.

Multiple messages

A probabilistic polynomial time algorithm (ppt).

Multiple messages eavesdropping game $\mathrm{PrivK}^{mult}_{A,\Pi}(n)$

1. $k \leftarrow \mathrm{Gen}(1^n)$
2. A on input 1^n generates two vectors of messages $M_0 = (m_0^1, \ldots, m_0^t)$, $M_1 = (m_1^1, \ldots, m_1^t)$ with $|m_0^i| = |m_1^i|$ for all i.
3. $b \leftarrow \{0,1\}$, $c_i \leftarrow \mathrm{Enc}_k(m_b^i)$. $C = (c_1, \ldots, c_t)$ is given to A.
4. $b' \leftarrow A(1^n, C)$.
5. Output of experiment is 1, if $b = b'$, otherwise output is 0.

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

Security for multiple encryptions

Definition 2.8 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ has indistinguishable multiple encryptions (against eavesdropping adversaries) if for every probabilistic polynomial time algorithm A there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that

$$\Pr\left[\text{PrivK}_{A,\Pi}^{\text{mult}}(n) = 1\right] \leq 1/2 + \mu(n).$$

Theorem 2.9 There exist encryption schemes with indistinguishable encryptions (against eavesdropping adversaries) that do not have indistinguishable multiple encryption (against eavesdropping adversaries).