Computational Indistinguishability $\iff$ Semantic Security

Thm If $\Pi = (Gen, Enc, Dec)$ is computational Indistinguishable under eavesdropping adversary then it achieves Semantic Security

$\forall A, \exists A'$:

$\forall h, f \Rightarrow$

$$\left| \Pr_{\substack{k, \\ m \leftarrow Samp(1^n), \\ r_A}} \left[A\left(1^n, Enc_k(m), h(m)\right) = f(m) \right] - \Pr_{\substack{m \leftarrow Samp(1^n) \\ r_{A'}}} \left[A'\left(1^n, |m|, h(m)\right) = f(m) \right] \right| \leq negl(n).$$

(Proof ⇒ later)

Computational Indistinguishability $\iff$ Semantic Security

Thm If $\Pi = (Gen, Enc, Dec)$ is computational Indistinguishable under eavesdropping adversary then it achieves Semantic Security

$\forall A, \exists A'$:

$\forall h, f \Rightarrow$

$$\left| \Pr_{\substack{k, \\ m \leftarrow Samp(1^n), \\ r_A}} \left[A\left(1^n, Enc_k(m), h(m)\right) = f(m) \right] - \Pr_{\substack{m \leftarrow Samp(1^n) \\ r_{A'}}} \left[A'\left(1^n, |m|, h(m)\right) = f(m) \right] \right| \leq negl(n).$$

(Proof ⇒ later)

Pseudo-Random Generator (PRG)

fix poly $\rightarrow \ell(\cdot)$

$G \rightarrow$ deterministic poly time algo s.t. it takes as i/p an n-bit string say s, & outputs $G(s)$, an $\ell(n)$-bit string.

$$G: \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$$

G is a PRG if

1) $\forall n,\ \ell(n) > n$.

2) $\forall$ PPT algo $\mathcal{D}$,

$$\left| \Pr_{s \xleftarrow{R} \{0,1\}^n}[\mathcal{D}(G(s)) = 1] - \Pr_{r \xleftarrow{R} \{0,1\}^{\ell(n)}}[\mathcal{D}(r) = 1] \right| \leq \text{negl}(n).$$

Pseudo-Random Generator (PRG)

fix poly $\rightarrow \ell(\cdot)$

$G \rightarrow$ deterministic poly time algo s.t. it takes as i/p an n-bit string say s, & outputs $G(s)$, an $\ell(n)$-bit string.

(s ↓ seed)

$$G: \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$$

G is a PRG if

1) $\forall n,\ \ell(n) > n$.

2) $\forall$ PPT algo $\mathcal{D}$,

$$\left| \Pr_{s \xleftarrow{R} \{0,1\}^n}[\mathcal{D}(G(s)) = 1] - \Pr_{r \xleftarrow{R} \{0,1\}^{\ell(n)}}[\mathcal{D}(r) = 1] \right| \leq \text{negl}(n).$$

$G(s) = s \| msb(s)$

$G: \{0,1\}^n \to \{0,1\}^{n+1}$

msb → most significant bit

$msb(100\cdots) = 1$

Is G pseudoramdom?

$s = s_1 s_2 \cdots s_n$

$G(s) = s_1 s_2 \cdots s_n s_1$

$x = x_1 \cdots x_{n+1}$

↳ $G(s)$

↳ $\not\in$

$\mathcal{D}$

1. Check if $x_1 \stackrel{?}{=} x_{n+1}$ or not
2. Return 1 if $x_1 = x_{n+1}$

$\left| Pr[\mathcal{D}(G(s)) = 1] - Pr[\mathcal{D}(r) = 1] \right|$

$= \left(1 - \frac{1}{2}\right)$

$= \frac{1}{2}$

G → not PRG

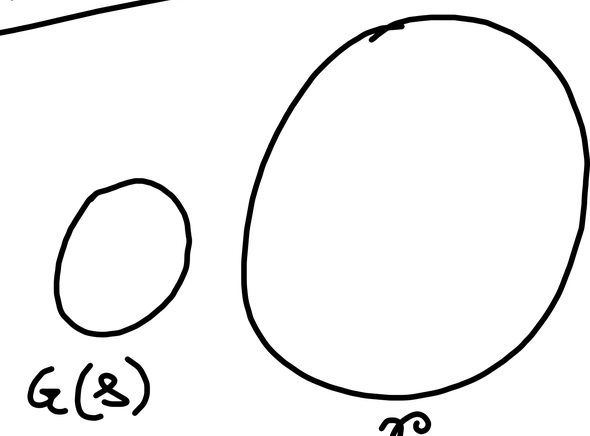
$$G : \{0,1\}^n \to \{0,1\}^{2n}$$

f
- Computing $f(x)$ is easy
- Computing $f^{-1}(y)$ is difficult

$\mathcal{D}$

exp

1. Compute $G(s)$ for $s = 0, \ldots, 2^n - 1$ $\to S$
2. Return 1 if the string belongs S



Assumption: There exists PRGs. [If One-way function exists, then PRG exist]

Construction

$G: \{0,1\}^n \to \{0,1\}^{\ell(n)}$

$\Pi = (Gen, Enc, Dec)$

$Gen(1^n)$: $k \xleftarrow{\$} \{0,1\}^n$

$Enc(m,k)$: $c \leftarrow G(k) \oplus m$ | $m \in \{0,1\}^{\ell(n)}$

$Dec(c,k)$: $m := G(k) \oplus c$

Thm: If G is PRG, then Π is computationally indist under eavesdropping adv.

Ch_G | $\mathcal{A}_G / Ch_\pi$ | $\mathcal{A}_\pi$

$\omega \xleftarrow{\$} \{0,1\}^{2n}$

$\omega = G(k)$

$\omega \in \{0,1\}^{\ell(n)}$

$b \xleftarrow{\$} \{0,1\}$

$c = \omega \oplus m_b$

(m_0, m_1)

$b \xleftarrow{\$} \{0,1\}^n$

$\omega \xleftarrow{\$} \{0,1\}^{\ell(n)}$

m_0, m_1

$c = m_b \oplus \omega$

c

$\hat{b}$

$\Pr[\hat{b} = b] = \frac{1}{2}$

c

$\hat{b}$

if $\hat{b} = b$ then $b' = 1$ else $b' = 0$

b'

$b \xleftarrow{\$} \{0,1\}^n$

m_0, m_1

$c = G(k) \oplus m_b$ c

$\hat{b}$

$\Pr[\hat{b} = b] = \Pr[Priv^{eav}_{\pi, \mathcal{A}_\pi} \Rightarrow 1]$

① $\Pr_{\omega \xleftarrow{\$} \{0,1\}^{\ell(n)}}[\mathcal{D}(\omega) = 1] = \frac{1}{2}$

② $\Pr_{k \xleftarrow{\$} \{0,1\}^n}[\mathcal{D}(G(k) = 1] = \Pr[Priv^{eav}_{\pi, \mathcal{A}_\pi} \Rightarrow 1]$

If $\left| \Pr[\mathcal{D}(G(k) = 1]] - \Pr[\mathcal{D}(\omega) = 1] \right| \leq negl(n)$

$\Pr[Priv_{\pi, \mathcal{A}(\pi)} = 1] \leq \frac{1}{2} + negl(n)$.