Probabilistic Encryption

2021年3月22日 13:21

Recap:

- One-time pad from PRG. $Enc_k(m) = PRG(k) \oplus m$.

limitations: 1. Each key can only be used once

2. Deterministic.

Define (Secure Encryption) (Private)

(k, m, Gen, Enc, Dec) is a Secure Encryption, if:

$\forall m, m' \in M,\ k \in K.$

$$\{Enc_k(m)\} \approx_c \{Enc_k(m')\}. \quad \times$$

for multiple cypertext,

$\forall m_1, m_1', \cdots, m_h, m_h' \in M,\ h \in poly(n)$

$$k \leftarrow K.\ \{Enc_k(m_1), \cdots, Enc_k(m_h)\} \approx_c \{Enc_k(m_1'), \cdots, Enc_k(m_h')\}$$

This definition enforces randomness on encryption,

because an attack: $m_1 = m_1' = m_2 \neq m_2'$ distinguish two distribution.

Achieve this by PRF ?

$$F = \{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \leftarrow K_{PRF}}$$

$K_{Enc} = K_{PRF}$

$Gen = k \leftarrow K_{PRF}$

random r,

$Enc_k(m, r) = m \oplus F_k(r),\ r$

$Dec_k(c) = F_k(r) \oplus c$

Proof: Hybrid Argument

$$\{Enc_k(m_1), \cdots, Enc_k(m_h)\}$$

$$\downarrow$$

$$\{\underbrace{m_1 \oplus F_k(r_1)}\,|\,r_1, \cdots, m_h \oplus F_k(r_h)\,|\,r_h\}$$

$m_1 \oplus R_1 | r_1 \to R_1 | r_1 \to r_1$

$\{ m_1 \oplus r_k(1) \| r_1, \cdots, m_k \oplus r_k(k) \| r_k \}$

$m_1 \oplus R_1 | r_1 \rightarrow R_1 / r_1 \rightarrow r_{2n}$.

$(\mathcal{M}, K, Gen, Enc, Dec)$: Public Key Encryption

- K: $\overset{\text{public}}{pk}$, $\overset{\text{secret}}{sk}$.
- $Gen(1^n) \rightarrow pk, sk$.
- $Enc_{pk}(m) \rightarrow c$
- $Dec_{sk}(c) \rightarrow m$

A public key encryption is secure if : $\forall m, m' \in \mathcal{M}$.

$$\{pk, Enc_{pk}(m)\} \approx_c \{pk, Enc_{pk}(m')\}$$

We don't need to define $m_1 \sim m_k$

Since given pk, you can create $Enc_{pk}(m_i)$ by yourself !

Given a Trapdoor OWP.

$F = \{F_i : \{0,1\}^n \rightarrow \{0,1\}^n\}_{i \leftarrow K_{Trapdoor}, \overset{\text{trapdoor.}}{t_i}}$

$Gen(1^n)$: $pk = f_i$, $sk = t_i$. $\leftarrow$ hard core bit $b_i : \{0,1\}^n \rightarrow \{0,1\}$

$Enc_{pk}(\underset{m_1 \cdots m_n}{m}, r) = \quad f_i(r),\ b_i(r) \oplus m_1$

$Dec_{pk}(c) = \quad$ Invert $f_i(r) \Rightarrow b_i(r) \oplus C = m_1$