Simulation and Zero-knowledge

2021年3月29日 13:29

Simulation Paradigm (Real - ideal Paradigm)

- Simulation Definition for Encryption:

Informal: Seeing Ciphertext gives almost no information.

$$\{Enc_k(c)\} \approx Sim(\ \ ) \to \{ct\}$$

Formally,

[Goldwassen, Micali 82].

Enc is "semantically secure" if:

$\exists$ ppt. Simulator S, (s.t. $\forall$ p.p.t Adv $\exists$ negl. ε.)

s.t. $\forall n \in N$, $\forall m \in M_m$ (message length)

$$\{Enc_k(m)\} \approx \{S(1^{|m|})\}$$

For multiple msgs $m_1, \cdots, m_h$. $h \in poly(n)$.

$$\{Enc_k(m_1), \cdots, Enc_k(m_h)\} \approx_c \{S(1^{|h|}, 1^{|m|})\}$$

Example (from last lec)

$M = K = \{0,1\}^n$.

$Gen \to k$ for a PRF: $\{0,1\}^n \to \{0,1\}^n$.

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

$$Dec(c) = F_k(c_2) \oplus c_1 = m.$$

Theorem This encryption scheme satifies Semantic Secrecy

Proof. $\exists$ Construct such a simulator. S

S: tosses strings $R \leftarrow \{0,1\}^n$, $r \leftarrow \{0,1\}^n$.

outputs (R, r)

As for multiple msgs, use Hybrid Argument ~

Claim: $\boxed{\text{Indistinguishable Enc} = \text{Semantic Enc}}$

proof. Ind $\Rightarrow$ Sem

$$S(1^n)_{k \in K} = Enc_k(0^n).$$

proof. Ind $\Rightarrow$ Sem

$$S(1^n)_{k \leftarrow K} = Enc_k(0^n).$$

$$\forall m \in M. \quad Enc_k(m) \approx Enc_k(0^n)$$

Sem $\Rightarrow$ Ind.

$$Enc_k(m_1, r) \approx S(1^n) \approx Enc_k(m_2, r)$$

Interactive Proof

Prover $\xrightarrow{\pi}$ Verifier

NP: Language $L \in NP$ if.

$x \in L$, $\exists w$. poly machine A. s.t. $A(x, w) = 1$

Graph (non) - Isomorphism

$G_1(V_1, E_1) \quad G_2(V_2, E_2)$.

$G_1 \cong G_2$ if $\exists \pi: V \to V$ s.t. $\pi(V_1) = V_2$

and. $E_2 = \{(\pi(v_1), \pi(v_2)): v_1, v_2 \in V_1\}$

$G_1 \not\cong G_2$

Prover $\longrightarrow$ Verifier

$\pi(G_b)$

$\pi \leftarrow S_{|V|}$

$b \leftarrow \{1,2\}$

b'

$\vdots$

n times.

If iso success with Prob $\frac{1}{2^n}$.

Witness = $\{\pi(G_b), b' \dots\}$

Interactive Proof. L, x, (P, V)

p.p.t.

Completeness if $x \in L$

$Pr[\text{Prover}(x) \to \rho$, s.t. $Ver(x, \pi) = 1] = 1$

Soundness if $x \notin L$.

$Pr[\text{Prover}(x) \to \rho$, s.t. $Ver(x, \pi) = 1] <$ negl.

(ρ is all interaction)

Zero - Knowledge

For honest V, $\exists$ p.p.t Simulator S. such that

$$S(x) \approx_c \text{Witness}$$

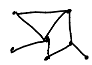
instance

For malicious V. $\exists$ p.p.t Simulator S. s.t.

$S(x, V) \approx_c$ Witness

Zero-Knowledge Proof for NPC

- 3-coloring



$G = (V, E)$

$P \xrightarrow{\pi\,(\text{color})} V$

$\xleftarrow[(e \in E)]{\text{open edge } e}$

$\xrightarrow{\text{open } e}$

Use for π (color) and "open e"

1. Commitment

Sender Receiver

$\xrightarrow{\text{Commit}(m, r) = c}$ msg random

$\xrightarrow{\text{Open}: m, r}$ Check if $c = \text{Commit}(m, r)$

Property:

- Hiding: $\forall m_0, m_1$

$\{\text{Commit}(m_0, r)\} \approx_c \{\text{Commit}(m_1, r)\}$

- Binding: $\forall m_0, m_1 \in \mathcal{M}$. $m_0 \neq m_1$. and $\forall r_0, r_1$.

$\text{Commit}(m_0, r_0) \neq \text{Commit}(m_1, r_1)$

One construction:

OWP f. hardcore bit b

$m \in \{0,1\}$.

$r \leftarrow U_n$.

$\text{Commit}(m, r) = f(r) \| b(r) \oplus m$.

2. Proof for Zero-Knowledge.

Construct Sim:

- Commit (Random Coloring)
- Query V. if e works, output e. and then open e.

otherwise goto Commit

Then $\text{Sim}(G, V) \approx_c \text{View}(P, V)$

(Proved by Hybrid Argument).

$\text{Commit}(m, r)$.