CSCI 1510

This Lecture:

- Computational Security
- Concrete vs. Asymptotic
- Definition of Semantic Security

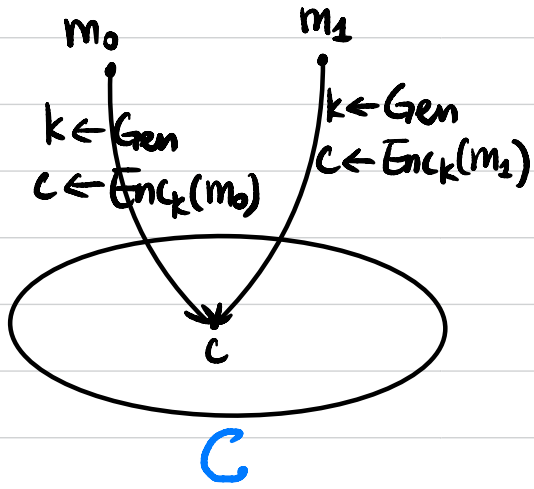
Last Lecture

Perfectly secure symmetric-key encryption

- Definitions 1, 2, 3

  $\forall m_0, m_1 \in \mathcal{M}, \forall c \in \mathcal{C}$:

  $\Pr[\text{Enc}_K(m_0) = c] = \Pr[\text{Enc}_K(m_1) = c]$



- Construction: OTP

- Limitations: $|\mathcal{M}| \leq |k|$.

How to relax the security definition?

Computational Security

Perfect Security:

① Absolutely no information is leaked

② $\mathcal{A}$ has unlimited computational power

Relaxation (Practical Purpose):

① "Tiny" information can be leaked

② $\mathcal{A}$ has limited computational power

How to formalize?

Computational Security

- Concrete Approach:

  A scheme is (t, ε)-secure if $\forall A$ running in time $\leq t$ succeeds in breaking the scheme with probability $\leq \varepsilon$.

  (A: classical computers; t: CPU cycles)

Example: $(2^{128}, 2^{-80})$-secure encryption scheme.

What's the problem?

Computational Security

- Asymptotic Approach:

  measuring how "hard" it is for $\mathcal{A}$ to break the scheme.

  Introduce a security parameter n (public)

  All honest parties run in time $\text{poly}(n)$.

  Security can be tuned by changing n.

poly(n) "negligible" in n

A scheme is (t, ε)-secure if $\forall \mathcal{A}$ running in time $\text{poly}(n)$ succeeds in breaking the scheme with probability $\text{negl}(n)$.

Polynomial & Negligible

"Efficient": probabilistic polynomial time (PPT)

Def A function $f: \mathbb{N} \to \mathbb{R}^+$ is **polynomial** if
$\exists c \in \mathbb{N}$ s.t. $f(n) \in O(n^c)$

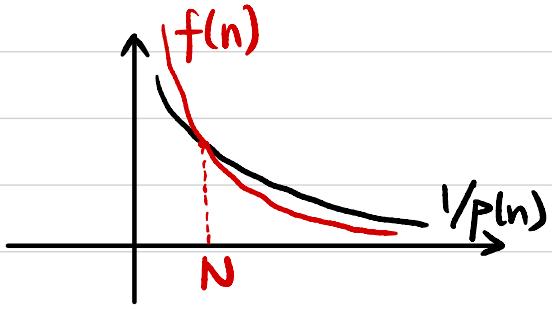
Example: $f(n) = 3n^6 + 5n^2 - 7 \in O(n^6)$

Def A function $f: \mathbb{N} \to \mathbb{R}^+$ is **negligible** if

$\forall$ polynomial p, $\exists N \in \mathbb{N}$ s.t. $\forall n > N$, $f(n) < \frac{1}{p(n)}$.

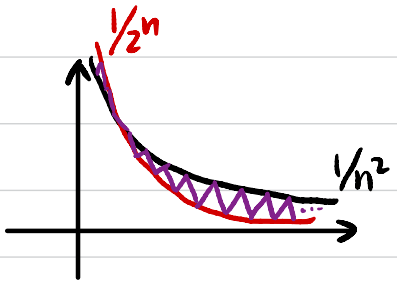
$\Leftrightarrow \forall c \in \mathbb{N}$, $f(n) \in o(n^{-c})$

Examples: 2^{-n}, $2^{-\sqrt{n}}$, $n^{-\log n}$



Exercise: Is this a negligible function?

$$f(n) := \begin{cases} 2^{-n} & \text{if } n \text{ is even} \\ 1/n^2 & \text{if } n \text{ is odd} \end{cases}$$



No, because $\exists$ polynomial $p(n) = n^2$ s.t.
$\forall N \in \mathbb{N}$. $\exists n > N$, s.t. $f(n) \geq \frac{1}{n^2}$

Negligible Function

Def A function $f: \mathbb{N} \to \mathbb{R}^+$ is negligible if

$$\forall \text{polynomial } p,\ \exists N \in \mathbb{N} \text{ s.t. } \forall n > N,\ f(n) < \frac{1}{p(n)}.$$

Claim 1 If f, g are negligible functions, then $f+g$ is also negligible.

proof: $\forall$ polynomial p, $\exists N_f \in \mathbb{N}$ s.t. $\forall n > N_f$, $f(n) < \frac{1}{2p(n)}$

$\exists N_g \in \mathbb{N}$ s.t. $\forall n > N_g$, $g(n) < \frac{1}{2p(n)}$

$N := \max(N_f, N_g)$. $\forall n > N$, $f(n) + g(n) < \frac{1}{p(n)}$.

Claim 2 If f is negligible, p is polynomial, then $f \cdot p$ is also negligible.

proof: $\forall$ polynomial q, $\exists N \in \mathbb{N}$ s.t. $\forall n > N$, $f(n) < \frac{1}{p(n) \cdot q(n)}$

$$\Rightarrow f(n) \cdot p(n) < \frac{1}{q(n)}.$$

Corollary If g is non-negligible, p is polynomial, then $\frac{g}{p}$ is also non-negligible.

Concrete → Asymptotic

A scheme is (t, ε)-secure if $\forall A$ running in time $\leq t$ succeeds in breaking the scheme with probability $\leq \varepsilon$.

Probabilistic polynomial time (PPT)

Security parameter n

poly (n)

A scheme is secure if $\forall$ PPT A succeeds in breaking the scheme with probability $\leq$ negligible.

negl (n)

Computationally Secure Encryption

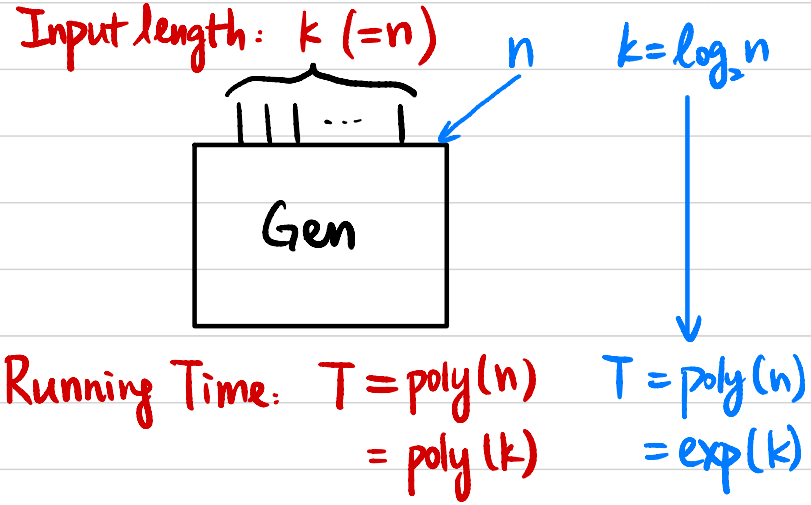
- **Syntax:**

A symmetric-key encryption scheme is defined by PPT algorithms (Gen, Enc, Dec):

$k \leftarrow Gen(1^n)$ (1^n: $11\cdots1$, n ones)

$c \leftarrow Enc_k(m)$ $\quad m \in \{0,1\}^*$

$m/\perp := Dec_k(c)$



- **Correctness:** $\forall n$, $\forall k$ output by $Gen(1^n)$, $\forall m \in \{0,1\}^*$

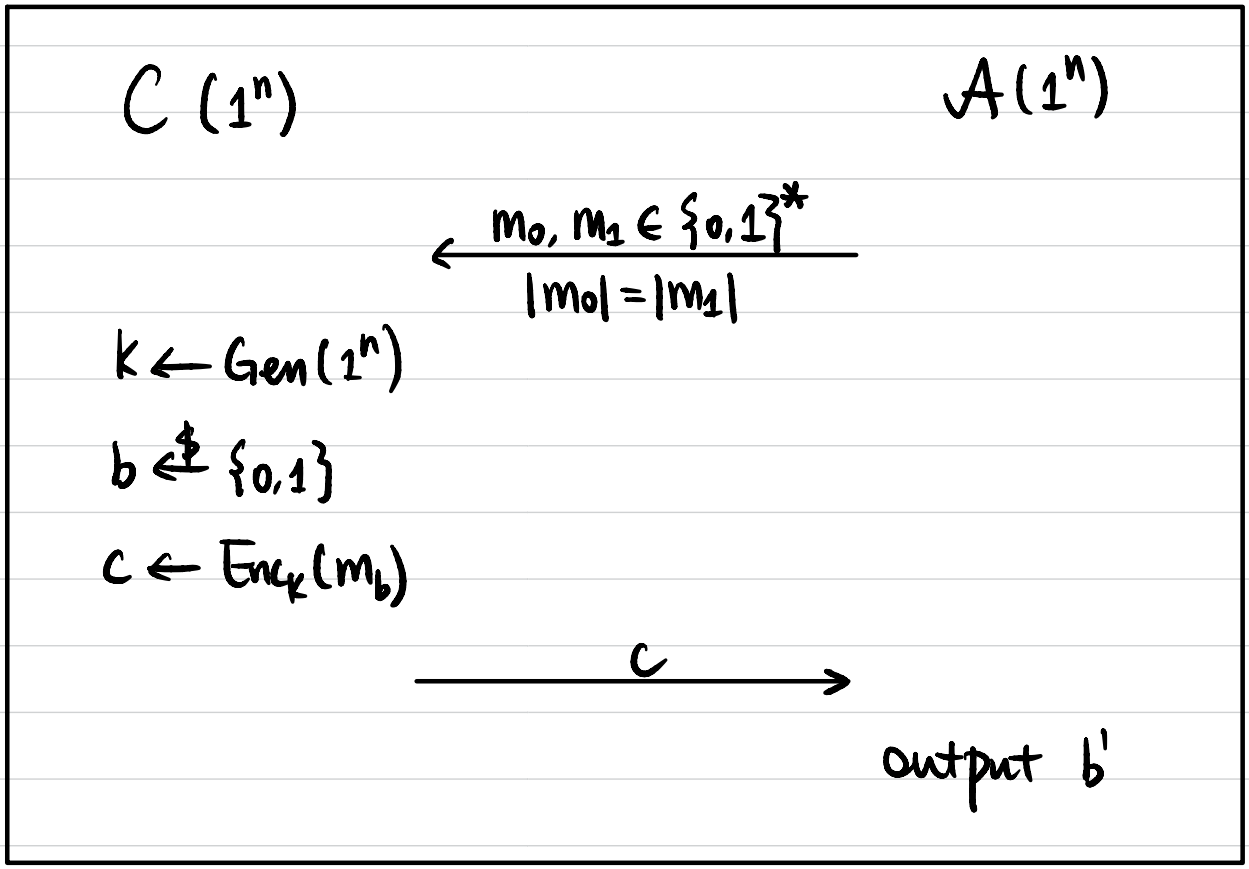
$$Dec_k(Enc_k(m)) = m$$

Computationally Secure Encryption

Def 1 A symmetric-key encryption scheme (Gen, Enc, Dec) is **semantically secure** if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$$

computationally indistinguishable

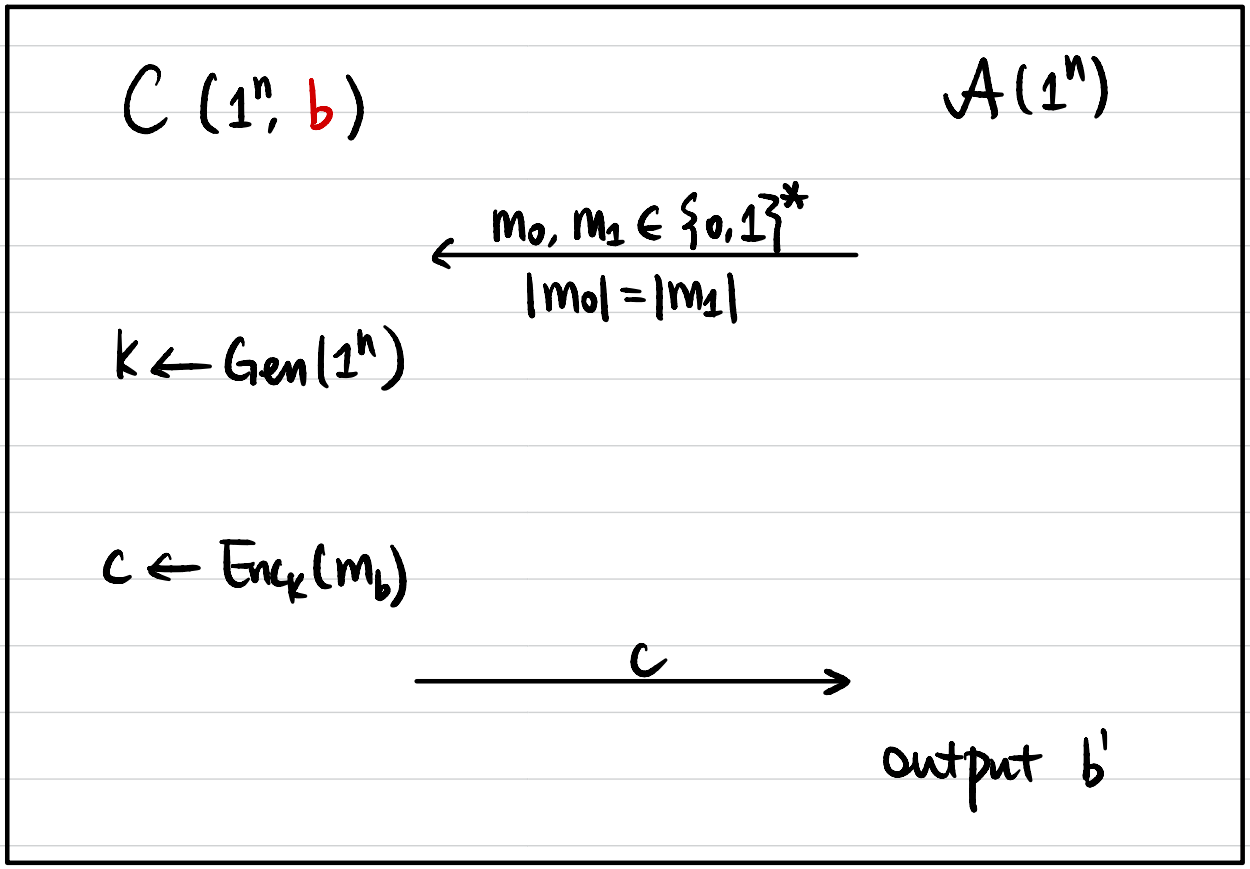


Computationally Secure Encryption

Def 2 A symmetric-key encryption scheme (Gen, Enc, Dec) is **semantically secure** if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

computationally indistinguishable

$$\left| \Pr[b' = 1 \mid b = 0] - \Pr[b' = 1 \mid b = 1] \right| \leq \varepsilon(n)$$



Computationally Secure Encryption

Def 1 A symmetric-key encryption scheme (Gen, Enc, Dec)

is **semantically secure** if $\forall$ **PPT** $\mathcal{A}$:

$$\Pr[b = b'] \leq \frac{1}{2} + \text{negl}(n)$$ in Game 1.

Def 2 $$\left|\Pr[b' = 1 \mid b = 0] - \Pr[b' = 1 \mid b = 1]\right| \leq \text{negl}(n)$$ in Game 2.

Def 1 ⇒ Def 2: If $\Pi = (Gen, Enc, Dec)$ is secure under Def 1, then Π is also secure under Def 2.

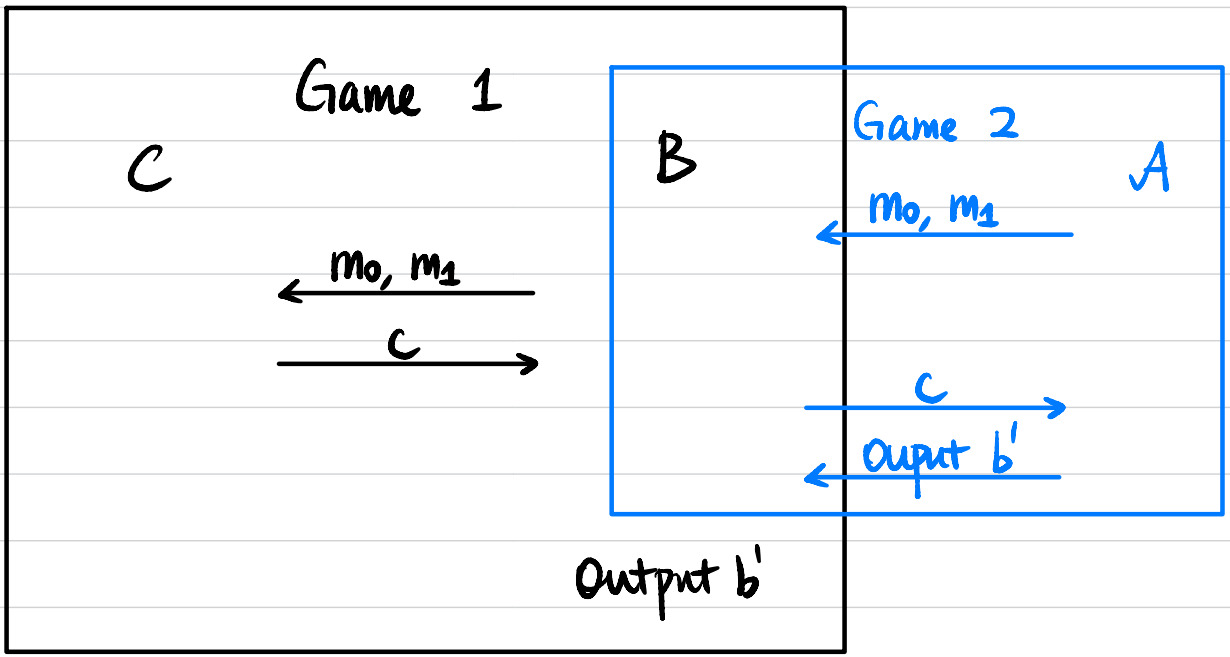
Proof: Assume Π is not secure under Def 2, then $\exists$ PPT A, non-negligible function $\gamma(\cdot)$ s.t.

$$\left| \Pr[b' = 1 \mid b = 0] - \Pr[b' = 1 \mid b = 1] \right| \geq \gamma(n) \quad \text{in Game 2.}$$

$$\Pr[b' = 1 \mid b = 0] = \alpha \qquad \Pr[b' = 1 \mid b = 1] = \beta \qquad |\alpha - \beta| \geq \gamma(n).$$

Assume $\beta - \alpha \geq \gamma(n)$:

We construct a PPT B to break Def 1



Proof (Continued):

$$\Pr[b=b' \text{ in Game 1}]$$

$$= \Pr[b=0] \cdot \Pr[b'=0 \mid b=0] + \Pr[b=1] \cdot \Pr[b'=1 \mid b=1]$$

$$= \frac{1}{2} \cdot (1-\alpha) + \frac{1}{2} \cdot \beta$$

$$= \frac{1}{2} + \frac{\beta - \alpha}{2}$$

$$\geq \frac{1}{2} + \frac{\gamma(n)}{2}$$

↑ non-negligible

If $\alpha - \beta \geq \gamma(n)$: Construct B to output $1-b'$

Def 2 ⇒ Def 1 :

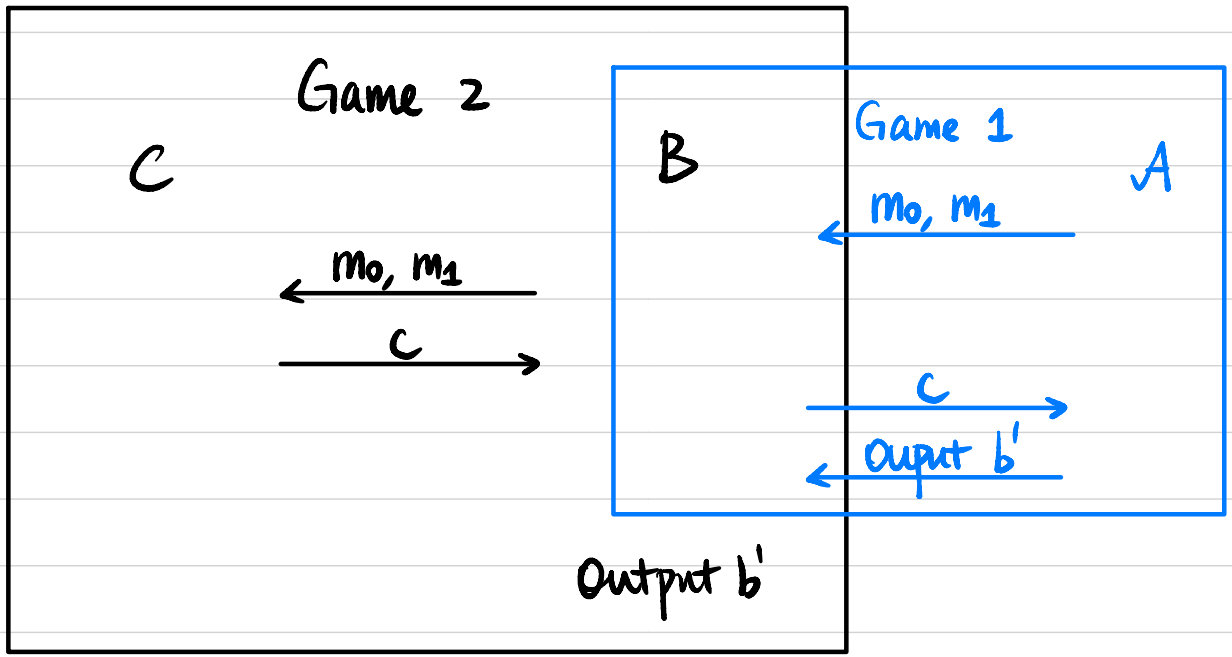
If Π is secure under Def 2, then it's also secure under Def 1.

Proof: Assume Π is not secure under Def 1, then

$\exists$ PPT A, non-negligible function $\gamma(\cdot)$ s.t.

$$\Pr[b=b'] \geq \frac{1}{2} + \gamma(n) \quad \text{in Game 1.}$$

We construct a PPT B to break Def 2



We want to bound $\left| \Pr[b'=1 \mid b=0] - \Pr[b'=1 \mid b=1] \right|$

$\Pr[b'=1 \mid b=0] = \alpha$

$\Pr[b'=1 \mid b=1] = \beta$

Proof (Continued):

We know $\Pr[b=b' \text{ in Game 1 by } \mathcal{A}] \geq \frac{1}{2} + \gamma(n)$

$$= \Pr[b=0] \cdot \Pr[b'=0 \mid b=0] + \Pr[b=1] \cdot \Pr[b'=1 \mid b=1]$$

$$= \frac{1}{2} \cdot (1-\alpha) + \frac{1}{2} \cdot \beta$$

$$= \frac{1}{2} + \frac{\beta-\alpha}{2}$$

$$\frac{1}{2} + \frac{\beta-\alpha}{2} \geq \frac{1}{2} + \gamma(n)$$

$$\Rightarrow \quad \beta-\alpha \geq 2 \cdot \gamma(n)$$

↑ non-negligible

$$\left| \Pr[b'=1 \mid b=0] - \Pr[b'=1 \mid b=1] \right| = |\alpha-\beta| \geq \text{non-negl}(n).$$