CSCI 1510

- Limitations of Perfect Security
- Definition of Computational Security : Concrete vs. Asymptotic
- Definition of Semantic Security

Last Lecture

Perfectly secure symmetric-key encryption

- Definitions 1, 2, 3

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

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

- Construction: OTP

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

How to relax the security definition?

Limitations of Perfect Security

Thm If $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is a perfectly secure encryption scheme with message space $\mathcal{M}$ & key space $\mathcal{K}$, then $|\mathcal{M}| \le |\mathcal{K}|$.

Proof: Assume $|\mathcal{K}| < |\mathcal{M}|$.

Pick an arbitrary $c \in \mathcal{C}$ where $\Pr[C=c] > 0$.

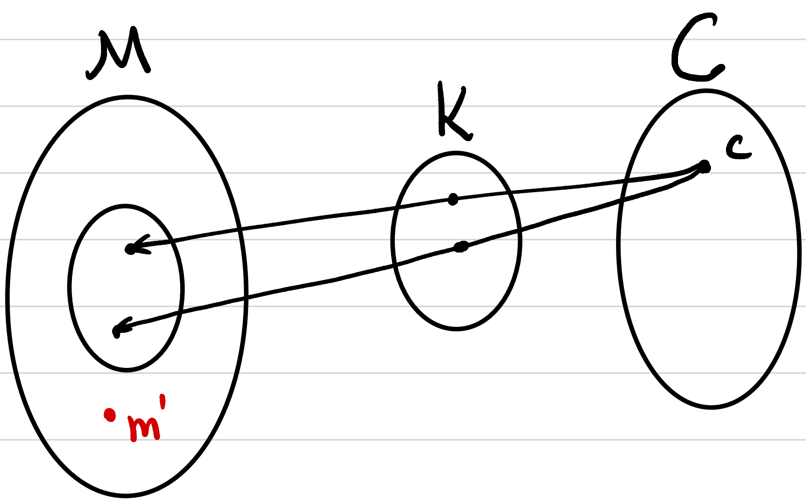
$\mathcal{M}(c) := \{ m \mid m = \mathrm{Dec}_k(c) \text{ for some } k \in \mathcal{K} \}$.

$|\mathcal{M}(c)| \le |\mathcal{K}| < |\mathcal{M}|$.

$\exists m' \in \mathcal{M}$ s.t. $m' \notin \mathcal{M}(c)$.

$\Pr[M=m' \mid C=c] = 0 \neq \Pr[M=m']$.

possible for some distribution over $\mathcal{M}$



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:

(quantum computers?)

classical computers

cpu cycles

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

Example: $(2^{128}, 2^{-60})$-secure encryption scheme.

What's the problem?

① Moore's Law?

② Specific about A's computing power

$(5 \text{ years}, 2^{-40}) \rightarrow$ 2 years?

10 years?

Computational Security

- Asymptotic Approach:

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

  Introduce a security parameter n (public)

  All honest parties run in time poly(n). exp(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 poly(n) succeeds in breaking the scheme with probability negl(n).

Polynomial & Negligible

"Efficient": Probabilistic polynomial time (PPT)

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

$$\exists c \in \mathbb{N} \text{ s.t. } f(n) \in O(n^c)$$

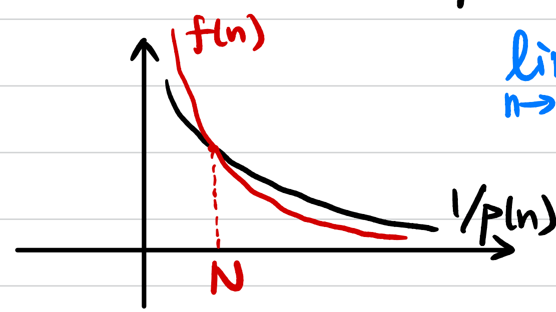
Example: $f(n) = 3n^6 + 5n^2 - 7 \in O(n^6)$

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

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

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

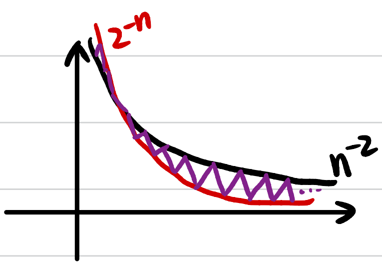
$$\lim_{n\to\infty} \frac{f(n)}{1/p(n)} = 0$$



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

Exercise: Is this a negligible function?

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



Negligible Function

Def A function $f: \mathbb{N} \to \mathbb{R}^+$ is negligible if
$\forall$ polynomial p, $\exists N \in \mathbb{N}$ s.t. $\forall n > N$, $f(n) < \frac{1}{p(n)}$.

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

proof: $\forall$ polynomial p, $\exists N_1 \in \mathbb{N}$ s.t. $\forall n > N_1$, $f(n) < \frac{1}{2p(n)}$

$\exists N_2 \in \mathbb{N}$ s.t. $\forall n > N_2$, $g(n) < \frac{1}{2p(n)}$

$N := \max(N_1, N_2)$. $\forall n > N$, $f(n) + g(n) < \frac{1}{p(n)}$.

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 $\forall \mathcal{A}$ running in time $\le t$ succeeds in breaking the scheme with probability $\le \varepsilon$.

$\Downarrow$

Security parameter n

poly(n)

A scheme is secure if $\forall$ PPT $\mathcal{A}$ succeeds in breaking the scheme with probability $\le$ negligible.

negl(n)

Computationally Secure Encryption

- **Syntax:**

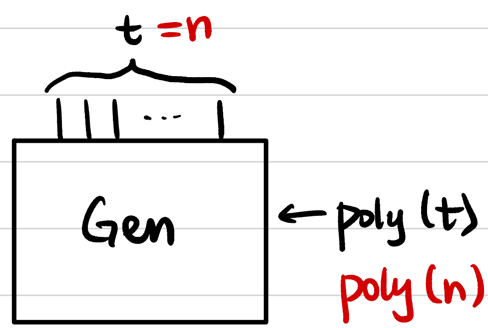
A symmetric-key encryption scheme is defined by PPT algorithms (Gen, Enc, Dec):

$\underbrace{11\cdots1}_{n}$

$$k \leftarrow \text{Gen}(1^n)$$

$$c \leftarrow \text{Enc}_k(m) \qquad m \in \{0,1\}^*$$

$$m/\perp := \text{Dec}_k(c)$$



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

$$\text{Dec}_k(\text{Enc}_k(m)) = m$$

Computationally Secure Encryption

Def 1 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

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

$C(1^n)$		$\mathcal{A}(1^n)$
	$\xleftarrow[\lvert m_0 \rvert = \lvert m_1 \rvert]{m_0, m_1 \in \{0,1\}^*}$	
$k \leftarrow \mathrm{Gen}(1^n)$		
$b \xleftarrow{\$} \{0,1\}$		
$c \leftarrow \mathrm{Enc}_k(m_b)$		
	$\xrightarrow{c}$	
		output b'

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

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

$C(1^n, b)$ $\qquad\qquad\qquad\qquad$ $\mathcal{A}(1^n)$

$$\xleftarrow[|m_0| = |m_1|]{m_0, m_1 \in \{0,1\}^*}$$

$k \leftarrow Gen(1^n)$

$c \leftarrow Enc_k(m_b)$

$$\xrightarrow{\quad c \quad}$$

output b'

Computationally Secure Encryption

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

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

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

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

Def 1 $\Rightarrow$ Def 2: If Π is secure under Def 1, then it's also secure under Def 2.

Assume Π is not secure under Def 2, then $\exists$ PPT $\mathcal{A}$, non-negligible function $\varepsilon(\cdot)$ s.t.

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

use $\mathcal{A}$ to break Def 1