Computational Security

Recap

1. Classical Ciphers
   - Broken
2. Perfect Secrecy
   - Information-theoretically Secure
   - $|K| \geq |M|$
     - Not Practical

Informally, if any adversary gets only tiny information about the plaintext with restricted Computational power.

$\mathcal{A}$ gets the plaintext corresponding to a ciphertext with probability $\frac{1}{2^{50}}$ in 200 years. $\Rightarrow$ Secure

Two Relaxations

- Efficient adversaries. (resource bounded)
- Adversary succeeds with a small probability.

Concrete Approach:

An encryption scheme is (t, ϵ)-secure if no efficient adversary can break the scheme in time t with probability ϵ.

Asymptotic Approach

An encryption scheme is secure if any probabilistic polynomial time (PPT) adversary can succeed in breaking the scheme only with negligible probability.

Polynomial Time:

$\{n \rightarrow$ security parameter

A runs in polynomial time if

$\forall x \in \{0,1\}^*$, A runs in poly($|x|$) no. of steps

$x = x_1 \ldots x_n \quad |x| = n$

$A \rightarrow (n^2+1)$ step / $\neq 2^n$ ~~(x)~~

n^2+1: $p(n)$

2^n: $exp(n)$

Negligible Function

20^{10}

10^{20}

f: Natural no $\longrightarrow$ real (+ve) number s.t.

for any polynomial p, $\exists N$: $\forall n \geq N$

$$f(n) < \frac{1}{p(n)}$$

Example: $f(n) = \frac{1}{n^2}$ $\quad p(n) = n^2 + 1$ (✓)

$f(n) = \frac{1}{2^n}$ $\quad p(n) = n^{10}$ (✗)

$f(n) = \frac{1}{2\sqrt{n}}$

$f(n) = \frac{1}{n \log n}$

$$\frac{1}{2^n} < \frac{1}{n^{10}}$$

$$n^{10} < 2^n$$

$n \geq 30$

$N = 30$

Necessity of these Relaxations

① PPT Adversary:

(m_1, c_1)
(m_2, c_2)
$\vdots$
(m_α, c_α)

$c \Rightarrow Dec_k(c) = m$

$\Downarrow$ get key k.

$k = 0 =$
$k = 1 =$
$\vdots$
$k = 2^n - 1 =$

$Enc_0(m_1) \stackrel{?}{=} c_1$
$Enc_1(m_1) \stackrel{?}{=} c_1$
$\vdots$
$Enc_{2^n-1}(m_1) \stackrel{?}{=} c_1$

If you allow unbounded computing power, adv will succeed with probability 1

② Success Probability is Negligible

- Assume A is computationally bounded.
- $A \rightarrow$ guess k $\qquad k \xleftarrow{\$} K$
  - $c \rightarrow Dec_k(c) = m$ ← this is the message

$$Pr[A \text{ succeeds}] = \frac{1}{|K|}$$

Computationally Secure Encryption (Notation)

A private-key encryption scheme $\Pi = (Gen, Enc, Dec)$

$k \leftarrow Gen(1^n)$

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

$m := Dec_k(c)$

$|k| \geq n$ → Why? We will see later

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

↳ fixed length Encryption Scheme

$\|$

$\underline{Gen}$

$k \xleftarrow{R} K$ → ignore Gen

Indistinguishability in the presence of Eavesdropper

$PrivK^{eav}_{A,\pi}(n)$

{ The o/p is 1, if $b = b'$
  0, o/w

$\Pr[PrivK^{eav}_{A,\pi}(n) = 1] \leq \frac{1}{2} + negl(n)$
$\forall A \nearrow$ (PPT)

Ch — 1^n → — A

$b \xleftarrow{\$} \{0,1\}$
$k \xleftarrow{\$} Gen(1^n)$
$c \leftarrow Enc_k(m_b)$

← m_0, m_1 — m_0, m_1 with $|m_0| = |m_1|$

→ c_b

← b'

Claim Indistinguishability ensures Ciphertext does not reveal any plaintext-bit Information

$\underline{\Pi^m}$: $\Pi = (Enc, Dec)$ be an encryption scheme (fixed length $\ell(n)$) has indistinguishability in the presence of eavesdropper. Then for all A, $i \in \{1, \ldots, \ell(n)\}$. $\boxed{m \xleftarrow{\$} \{0,1\}^{\ell(n)}}$

$$Pr\left[A(1^n, \underset{Enc_k(m)}{c}, i) = m_i\right] \leq \frac{1}{2} + negl(n).$$

$-$ (1)

Claim Indistinguishability ensures Ciphertext does not reveal any plaintext-bit Information

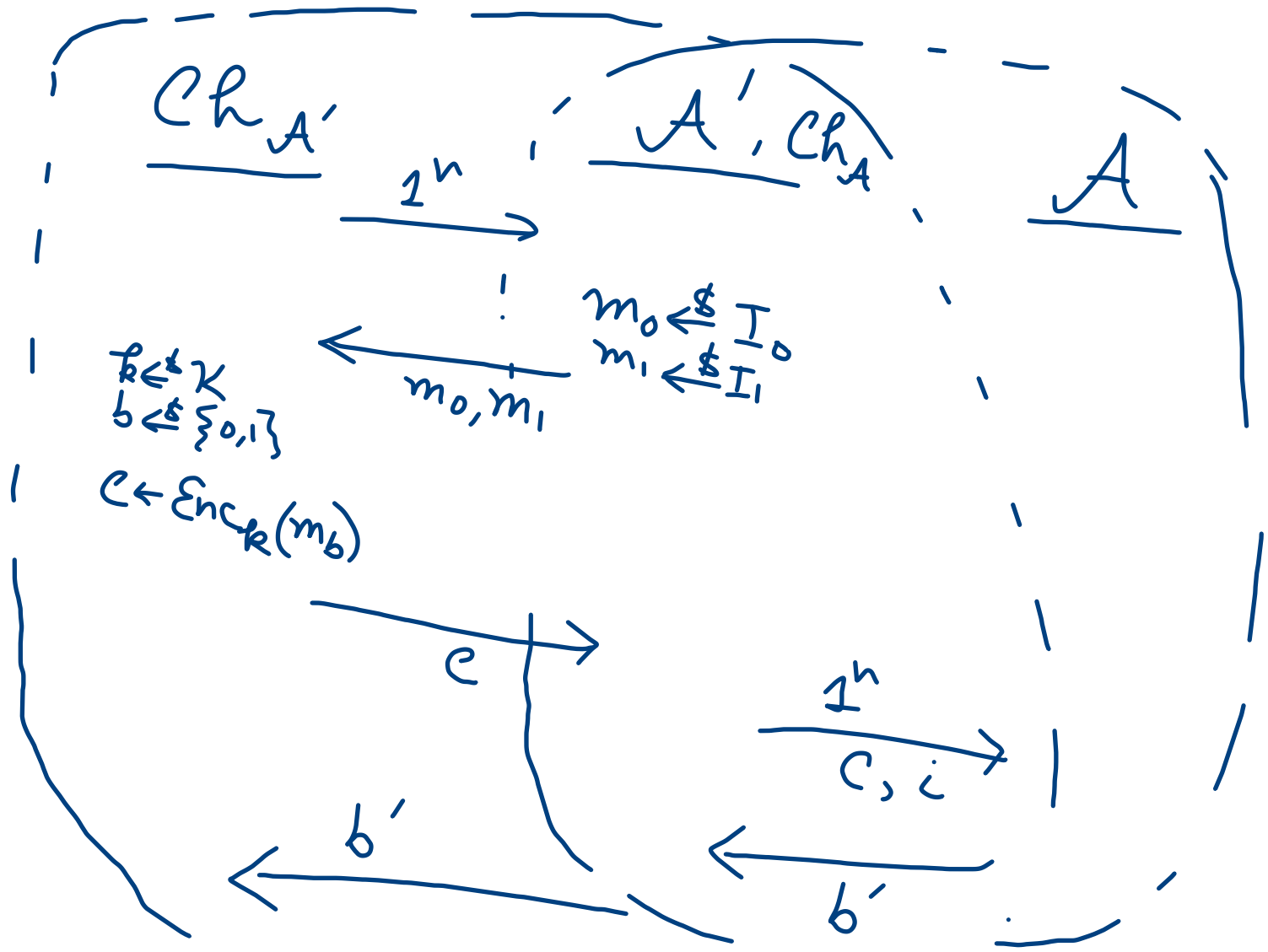
Π^m: $\Pi = (Enc, Dec)$ be an encryption scheme (fixed length $\ell(n)$) has indistinguishability in the presence of eavesdropper. Then for all A, $i \in \{1, \ldots, \ell(n)\}$. $\boxed{m \leftarrow^{\$} \{0,1\}^{\ell(n)}}$

$$Pr\left[A(1^n, \underbrace{c}_{Enc_k(m)}, i) = m_i\right] \leq \frac{1}{2} + negl(n).$$

— (1)

Proof Idea:

- Assume there exists $\mathcal{A}$ that violates (1).
- Then, we will construct $\mathcal{A}'$ that violates indist under eavesdropping.



$$I_0 = \{m \mid m_i = 0\}$$
$$I_1 = \{m \mid m_i = 1\}$$

$$Pr\left[Priv^{eav}_{\mathcal{A}',\pi}(n) = 1\right]$$
$$= Pr[\mathcal{A}(1^n, Enc_k(m_i)) = m_i]$$
$$= \frac{1}{2} + negl(n)$$

(Contradiction)

Ah

x →

A'

x →

← 2x

→ 2x

← 4x

A (can compute 2x)

4x ←

Close to "Semantic security"

Thm Let $\Pi = (\underbrace{Enc, Dec}_{Gen,})$ be a private-key encryption (fixed length - ℓ) that is indistinguishable under eavesdropping adversary. Then for any Adversary A, $\exists A'$ (PPT)

any set $S \subseteq \{0,1\}^\ell$, any $f: \{0,1\}^\ell \to \{0,1\}^*$ (efficiently computable) the following holds:

$$\Pr\left[A\left(1^n, Enc_k(m)\right), h(m)\right) = f(m)\right] - \Pr\left[A'\left(1^n, h(m), |m|\right) = f(m)\right] \leq negl(n)$$

$k \xleftarrow{R} K$, $m \xleftarrow{R} S$, $r \xleftarrow{R}$

$m \xleftarrow{R} S$

$m \leftarrow Samp(1^n)$

$Ch_{A''}$ $\quad A''/Ch^{A} \quad$ A

$m \xleftarrow{\$} S$
$m_0 = m$
$m_1 = 1^n$

$b \xleftarrow{\$} \{0,1\}$ ←

$c \leftarrow Enc_k(m_b)$

c →

$Enc_k(m)$ / $Enc_k(1^n)$

$1^n, c$ →

z ←

If $z \stackrel{?}{=} f(m)$
If yes then $b' = 0$
O/W $b' = 1$

b' ←

$$Pr\left[PrivK^{eav}_{A'',\Pi} = 1\right]$$

$$= Pr\left[b' = b\right]$$

Problems

(2) Enc Deterministic (redefining the key-space)

$\Downarrow$

$Pr[C = c | M = m]$ for all m, c

Enc

$k \leftarrow \mathcal{K}$ <--- $\omega \leftarrow_{\$} R$

$c \leftarrow Enc_k(m)$ < $Enc'_k(m;\omega)$

$m := Dec_k(c)$

$(k, \omega) \leftarrow \mathcal{K} \times R$

$c := Enc'_{k,\omega}(m) = Enc'_k(m;\omega)$

$m := Dec_{k,\omega}(c)$

③ Perfect Secrecy $\overset{?}{\Longrightarrow}$ $Pr[C=c_0] = Pr[C=c_1]$

OTP:

$\mathcal{M} = \{ m \mid |m| = \ell \text{ and } msb(m) = 0 \}$

$K \xleftarrow{\$} \{0,1\}^\ell$

Will it be perfectly Secure?

⑤ Ch

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

$t \xleftarrow{\$} \{1,2,3\}$

$k_i \xleftarrow{\$} \mathbb{Z}_{26}$

$t=1$	m_0 / k_0	m_1 / k_0	m_2 / k_0
$t=2$	m_0 / k_0	m_1 / k_1	m_2 / k_0
$t=3$	m_0 / k_0	m_1 / k_1	m_2 / k_2

A

$m_0 = aab$ / aaa

$m_1 = abb$

a a b

k_0 k_1 k_0

$a+k_0$ $a+k_1$

$c_b = c_1 c_2 c_3$

If $c_1 = c_2 = c_3$ then $\hat{b} \leftarrow 0$

else $\hat{b} \leftarrow 1$

$\hat{b}$

b

$$\Pr\left[\text{PrivK}^{eav}_{A,\pi} = 1\right]$$

$$= \frac{1}{2}\Pr[X=1 \mid b=0] + \frac{1}{2}\Pr[X=1 \mid b=1]$$

$$\Pr[X=1 \mid b=0] = \Pr[\hat{b}=0 \mid b=0]$$

$$= \frac{1}{3}\Pr[\hat{b}=0 \mid b=0, t=1] + \frac{1}{3}\Pr[\hat{b}=0 \mid b=0, t=2] + \frac{1}{3}\Pr[\hat{b}=0 \mid b=0, t=3]$$

$$= \frac{1}{3}\cdot 1 + \frac{1}{3}\cdot\frac{1}{26} + \frac{1}{3}\cdot\frac{1}{26}\cdot\frac{1}{26}$$

$$\frac{1}{2}\left(1 - \Pr[X=0 \mid b=1]\right)$$

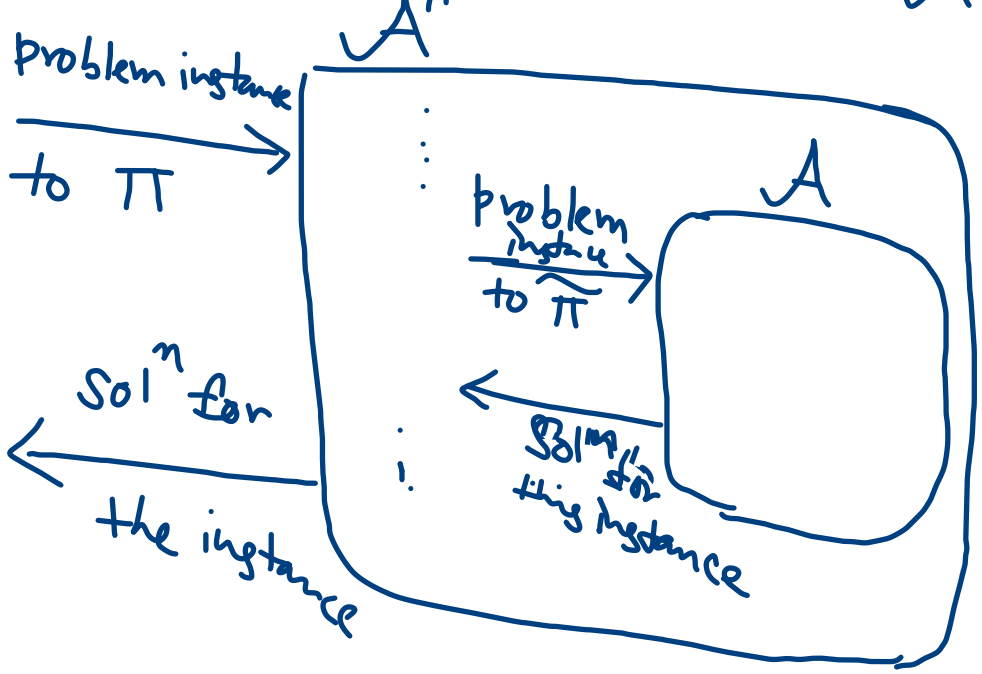
$$\frac{1}{3}\Pr[k_0 = k_1]$$

Reduction

Assumption: Π is secure / Problem P is difficult to solve.

Goal: $\tilde{\Pi}$ is secure / Problem Q is difficult to solve

Approach:
- $\tilde{\Pi}$ is not secure. $\exists$ adv $\mathcal{A}$ that breaks security of $\tilde{\Pi}$.
- Construct $\mathcal{A}''$ s.t. $\mathcal{A}''$ breaks Π.



- Success prob of $\mathcal{A} \to \epsilon(n)$
- If $\mathcal{A}$ succeeds then $\mathcal{A}''$ succeeds with prob $\epsilon'(n)$
- Then $\mathcal{A}''$ succeeds w.p. $\epsilon(n).\epsilon'(n)$