# Computational Security

- Unbounded computational power
  - ↳ Still provides security (Information Theoretic Security)
- Computational Security
  - the adversary is probabilistic polynomial time. (PPT)
  - the adversary can break the security with negligible probability

An adversary can break the security of $\Pi$ in with 100 years of computation with prob $\frac{1}{2^{100}}$.

# Probabilistic Polynomial Time

- Probabilistic adv (use randomness)
- I/P of the adversary is $x$, then the running time of the adversary is at most $p(|x|)$ for some polynomial $p$.

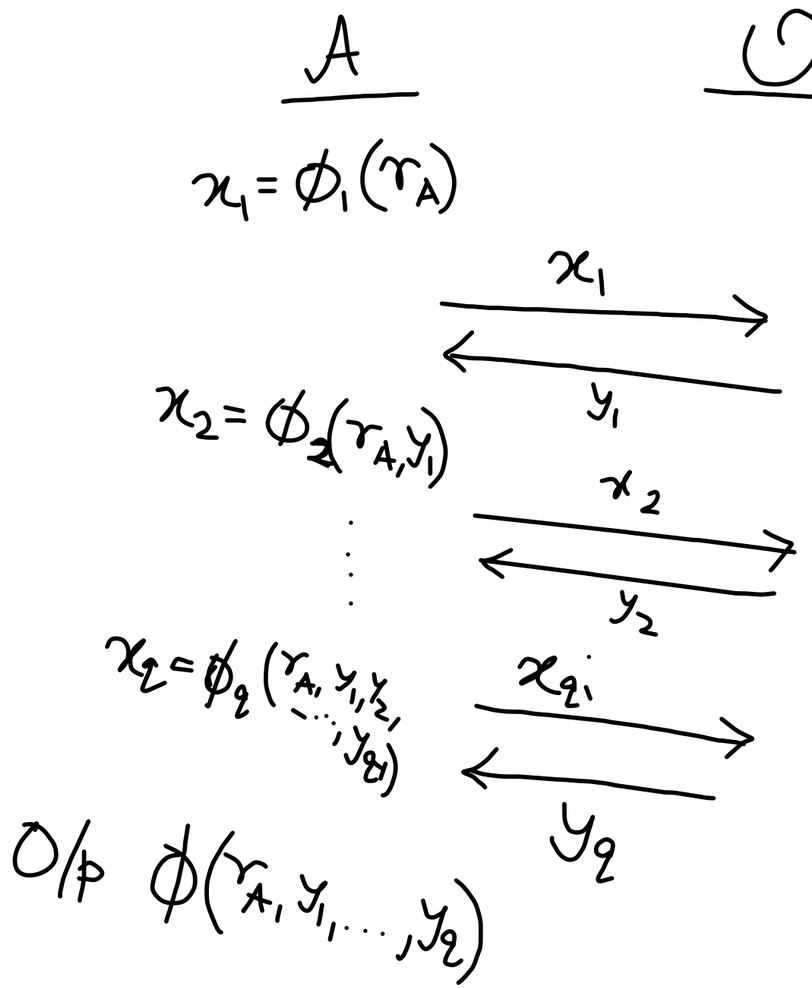
$|x|=n$

$A(x)$

↳ $(n^2+n+1)$ (PPT)

↳ $2^n$ ($\neq$ PPT)

# Oracle Adversary $A$




$$A \to (r_A, \phi_1, \phi_2, \ldots, \phi_q, \phi)$$

## Adaptive

- each query is dependent on previous responses.

# Negligible Function

A function $f$ is called negligible if $\forall$ polynomial $p$, $\exists N$ s.t. $\forall n > N$,

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

$f : \mathbb{N} \to \mathbb{R}^+$

$f(n) = n$ (X)

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

$f(n) = \frac{1}{n^{20}}$ (X)

$f(n) = \frac{1}{2^n}$ (✓)

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

# Necessity of the Relaxation

① Poly Adversary:

- input: $c$
- $\mathcal{M}(c) = \{m \mid Dec_k(c) = m\}$, for all $k$.
- $\mathcal{M}(c) \subset \mathcal{M}$

Running time = $|\mathcal{K}|$.

If we had used exponential adv then we have the following generic attacks:

Adversary

1) Ciphertext only

2) Known Plaintext - Ciphertext

$(m_1, c_1), (m_2, c_2) \ldots, (m_q, c_q)$

- Guess $k$
- Check whether $Enc_k(m_1) = c_1$ and ---- $Enc_k(m_q) = c_q$

② The adversary may break the security with negligible probability.

$(m_1, c_1), \ldots, (m_q, c_q)$

Adversary

- Guess $k$.
- If $Enc_k(m_1) = c_1, \ldots, Enc_k(m_q) = c_q$
  return $k$.

$\Pr[\text{guess is correct}] = \frac{1}{|\mathcal{K}|}$

# Computational Security

- Concrete version: A scheme $\Pi$ is $(t, \epsilon)$ - secure.
  - $t$ is the max$^m$ running time of the adv
  - $\epsilon$ is the prob with which adv may win.
- Asymptotic version:
  - Fix a security parameter $n$.
  - A scheme $\Pi$ is $(p(n), \mu(n))$ - secure.
    - $p$ → polytime
    - $\mu$ → negligible

$\Pi \rightarrow \left(n^4, \frac{1}{2^n}\right)$

$n = 64$

# Computationally Secure Encryption

$\Pi = (Gen, Enc, Dec)$

$k \leftarrow Gen(1^n)$, $|k| \geq n$

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

$m \leftarrow Dec(c, k)$.

Correctness: $\forall k, m, \quad Dec(Enc(m,k), k) = m$.

$|m| = \ell(n)$

↳ Fixed length encryption

$k$ $\underbrace{11\cdots1}_{64}$

$n = 64$

$k \xleftarrow{\$} \{0,1\}^{128}$

# Computationally Secure Encryption

$\Pi = (Gen, Enc, Dec)$

$k \leftarrow Gen(1^n)$, $|k| \geq n$

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

$m \leftarrow Dec(c, k)$.

Correctness: $\forall k, m, \quad Dec(Enc(m,k), k) = m$.

$|m| = \ell(n)$

↳ Fixed length encryption

$k$ $\underbrace{11\cdots1}_{64}$

$n = 64$

$k \xleftarrow{\$} \{0,1\}^{128}$

# Computational Indistinguishability

$\boxed{PrivK^{eav}_{\pi,A}}$

| Ch | | A |
|---|---|---|
| $k \leftarrow Gen(1^n)$ | | |
| $b \xleftarrow{\$} \{0,1\}$ | | |
| | $\leftarrow$ $m_0, m_1$ , $\lvert m_0\rvert = \lvert m_1\rvert$ | |
| $c \leftarrow Enc(k, m_b)$ | | |
| | $\rightarrow$ $c$ | |
| | $\leftarrow$ $\hat{b}$ | |

$\Pi$ is computationally indistinguishable $(p(n), \mu(n))$

if $Pr[PrivK^{eav}_{\pi,A} = 1] = Pr[b = \hat{b}]$

$\leq \frac{1}{2} + \mu(n)$,

for all A running in at most $p(n)$ steps.

# Semantic Security

↓

(π leaks no additional information)

**Weaker Version:** (π leaks negligible information about any plaintext bit.)

$\forall i$, $\forall$ poly-time $A$,

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

$\pi \rightarrow$ Secure.

# Semantic Security

↓

(π leaks no additional information)

(WSS)

Weaker Version: (π leaks negligible information about any plaintext bit.)

$\forall i$, $\forall$ poly-time $A$,

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

$\pi \rightarrow$ Secure.

If $\Pi$ is computationally indistinguishable,
then $\Pi$ is WSS.

(Proof by Reduction)

Assume $\Pi$ is not WSS.

$\Rightarrow \exists\ \mathcal{A}$ s.t. $\mathcal{A}$ breaks WSS Security of $\Pi$

$\Rightarrow$ $\exists\ \mathcal{B}$ s.t. $\mathcal{B}$ uses this adv $\mathcal{A}$ to break CI