Last lecture

"more secure" encryption scheme

computational secure
encryption scheme

PRG for any poly ℓ

PRG with $\ell(\lambda)=\lambda+1$

OWP w/ hard-core bit

OWF w/ hard-core bit

This lecture

OWF

OWP

Weak OWF

Def (OWF) $f: \{0,1\}^* \to \{0,1\}^*$

- easy to compute

  $\exists$ p.p.t algo to compute f

- hard to invert

  $\forall$ p.p.t. A

  $\Pr[\mathrm{Invert}_{A,f}(\lambda)=1]$

  $= \mathrm{negl}(\lambda)$

$\underline{\mathrm{Invert}_{A,f}(\lambda)}$

$x \xleftarrow{\$} \{0,1\}^\lambda$

compute $f(x)$

$A(f(x)) \to x'$

A wins iff $f(x') = f(x)$

equ. $x' \in f^{-1}(f(x))$

E.g. candidate OWF

$$f(p, q) = \left(\begin{matrix}\text{smallest prime} \\ \text{greater than } p\end{matrix}\right) \cdot \left(\begin{matrix}\text{smallest prime} \\ \text{greater than } q\end{matrix}\right)$$

$$f(a_1, a_2, \cdots, a_\lambda, I) = \left(a_1 \cdots a_\lambda, \sum_{i \in I} a_i\right)$$

$$I \subseteq \{1, \cdots, \lambda\}$$

$$f(\underset{\text{prime}}{p}, \underset{\text{generator in } \mathbb{Z}_p^*}{g}, a) = (p, g, g^a \bmod p)$$

f is a PRG

OWF: f

- length-regular OWF

  $\exists \ell : \mathbb{N} \to \mathbb{N} \quad |f(x)| = \ell(|x|)$

- length-preserving OWF $\quad |f(x)| = |x|$

- one-way permutation (OWP)

  $\forall \lambda \quad f$ is a permutation over $\{0,1\}^\lambda$

- hard-core bit $\quad h : \{0,1\}^* \to \{0,1\}$

  h is a hard-core bit of f

  - h is poly-time computable
  - hard to guess from $f(x)$

$\forall$ p.p.t A

$$\left| \Pr[\mathrm{Hardcore}_{A,f,h}(\lambda) = 1] - \frac{1}{2} \right| \leq \mathrm{negl}(\lambda)$$

$$\boxed{\begin{array}{l} \mathrm{Hardcore}_{A,f,h}(\lambda) \\ \hline x \xleftarrow{\$} \{0,1\}^\lambda \\ A(f(x)) \to b \\ A \text{ win iff } b = h(x) \end{array}}$$

f is a OWF

① $f'(\underbrace{x}_{\lambda}, \underbrace{i}_{\log\lambda}) = (\underbrace{f(x)}_{\ell(\lambda)}, \underbrace{i}_{\log\lambda}, \underbrace{x_i}_{1})$

② $f''(\underbrace{x}_{\lambda/2}, \underbrace{y}_{\lambda/2}) = f(x)$

③ $f'''(x, y) = (f(x), y)$

THM

$\exists$ owf $\Longrightarrow$ $\exists$ owf with a hard-core bit function

---

THM assume f is a OWF

then f' is a OWF

h is a hard-core bit of f'

$$f'(x, y) = (f(x), y)$$

$$h(x, y) = \sum_i x_i y_i \mod 2$$

THM assume f is a OWF

then f' is a OWF

h is a hard-core bit of f'

$$f'(x,y) = (f(x), y)$$

$$h(x,y) = \sum_i x_i y_i \bmod 2$$

Pf. Assume p.p.t A, poly q

for infinitely many $\lambda \in \mathbb{N}$

$$\Pr_{(x,y) \xleftarrow{\$} \{0,1\}^\lambda}\left[A(f'(x,y)) = h(x,y)\right] \geq \frac{1}{2} + \frac{1}{q(\lambda)}$$

Try to construct another A' that inverts f with non-negligible prob.

sample random $x \in \{0,1\}^{\lambda/2}$

$$\Pr_{x \leftarrow \{0,1\}^{\lambda/2}}\left[\Pr_{y \leftarrow \{0,1\}^{\lambda/2}}\left[A(f'(x,y)) = h(x,y)\right] \geq \frac{1}{2} + \frac{1}{q(\lambda)\cdot 2}\right] \geq 1 - \frac{\frac{1}{2} - \frac{1}{q(\lambda)}}{\frac{1}{2} - \frac{1}{q(\lambda)\cdot 2}}$$

$$\geq \frac{1}{\mathrm{poly}(\lambda)}$$

Assume $\Pr_{y \leftarrow \{0,1\}^{\lambda/2}} \left[A(f'(x,y)) = h(x,y) \right] \geq \frac{1}{2} + \frac{1}{q(\lambda) \cdot 2}$

$\text{Event}_i \equiv g_i = \langle x, y_i \oplus 10000 \rangle$

given $f(x)$ find x

sample $y_1\ y_2 \cdots y_m$ ask $A(f'(x, y_{\{1\}} \oplus 10000)) \to g_1$

$A(f'(x, y_{\{2\}} \oplus 10000)) \to g_2$

$A(f'(x, y_{\{1,2\}} \oplus 100\cdots)) \to g_m$

Rand $z_1 \cdots z_{\log m}$

correct values of $\langle x, z_i \rangle$

for each non-empty $S \subseteq [\log m]$, $y_S = \sum_{i \in S} z_i$

$\langle x, y_S \rangle = \left\langle x, \sum_{i \in S} z_i \right\rangle$

$= \sum_{i \in S} \langle x, z_i \rangle$

g_i = a guess of $\langle x, y_i \oplus 10000 \rangle$

$g_i \oplus \langle x, y_i \rangle$ = a guess of $\underbrace{\langle x, 10000 \rangle}_{= x_1}$

independent R.V. $X_1 \cdots X_n$ over $[0,1]$

Chernoff bound: $\Pr\left[\left|\frac{1}{n}\sum_i X_i - \frac{1}{n}\sum_i \mathbb{E}[X_i]\right| > \delta\right] \le 2e^{-\frac{\delta^2}{2}n}$

Markov Bound: R.V. X over $[0, +\infty)$

$$\Pr[X > a] \le \frac{\mathbb{E}[X]}{a}$$

Cheb... Bound: pair-wise independent R.V. $X_1 \cdots X_n$

$$\Pr\left[\left|\sum_i X_i - \sum_i \mathbb{E}[X_i]\right| > \delta\right] \le \frac{\sum_i \mathrm{Var}[X_i]}{\delta^2}$$

$$= \Pr\left[\left(\sum_i (X_i - \mathbb{E}[X_i])\right)^2 > \delta^2\right]$$

THM $\exists$ OWP w/ hard-core bit $\Longrightarrow$ $\exists$ PRG

Pf. f is a OWP and h is its hard-core bit

$$G(x) = f(x) \| h(x) \quad \text{is a PRG}$$

Cor. $\exists$ OWP $\Longrightarrow$ $\exists$ PRG

THM $\exists$ OWF $\Longrightarrow$ $\exists$ PRG

Def (Weak OWF) $f: \{0,1\}^* \to \{0,1\}^*$

① f is poly-time computable

② $\exists$ poly q $\forall$ p.p.t. A $\forall$ sufficiently large λ

$$\Pr_{x \xleftarrow{\$} \{0,1\}^\lambda}\left[A(f(x)) \in f^{-1}(f(x))\right] \leq 1 - \frac{1}{q(\lambda)}$$

THM $\exists$ weak OWF $\Longrightarrow$ $\exists$ OWF (computational) indistinguishable multiple message in the presence of eavesdropper

$\mathrm{PrivK}^{\mathrm{multi}}_{A,\Pi}(\lambda)$

A outputs $\begin{matrix} m_{0,1}, & m_{0,2}, & m_{0,3} & \cdots \\ m_{1,1} & m_{1,2} & m_{1,3} & \cdots \end{matrix}$

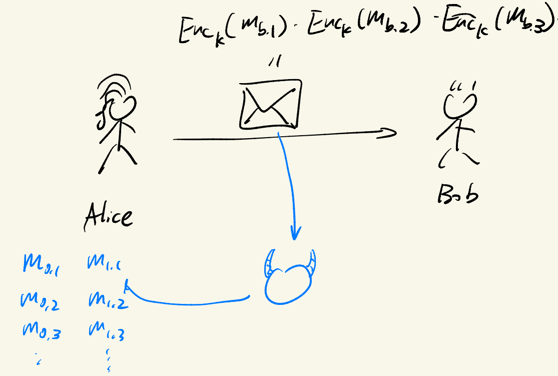
$k \leftarrow \mathrm{Gen}(1^\lambda) \quad b \xleftarrow{\$} \{0,1\}$

$c_i \leftarrow \mathrm{Enc}_k(m_{b,i})$

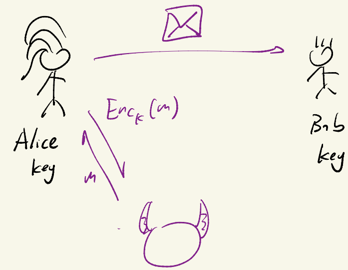
give $c_1 \cdot c_2 \cdots$ to A

A guess b'

A wins if $b' = b$



$\mathrm{PrivK}^{CPA}_{A,\Pi}$ chosen plaintext attack



$k \leftarrow \mathrm{Gen}(1^\lambda)$

$A(1^\lambda) \xrightarrow{m_i}$ challenger

$\xleftarrow{\mathrm{Enc}(k, m_i)}$

for $i = 1, \dots, \mathrm{poly}(\lambda)$
$A(1^\lambda)$ send m_i, receives $\mathrm{Enc}(k, m_i)$

$\xrightarrow{m'_0 \ m'_1}$ $\quad b \xleftarrow{\$} \{0,1\}$

$\xleftarrow{\mathrm{Enc}(k, m'_b)}$

$\xrightarrow{m_i}$

$\xleftarrow{\mathrm{Enc}(k, m_i)}$

guess b'

A wins iff $b' = b$

Def. Π is CPA-secure

$\forall$ p.p.t. A

$$\left| \Pr\left[\mathrm{PrivK}^{CPA}_{A,\Pi}(\lambda) = 1 \right] - \frac{1}{2} \right| \leq \mathrm{negl}(\lambda)$$

$\mathrm{PrivK}^{\text{multi-CPA}}_{A,\pi}$

$A(1^\lambda)$ Challenger

$k \leftarrow \mathrm{Gen}(1^\lambda)$

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

$\xrightarrow{\quad m_{i,0} \quad m_{i,1} \quad}$

$\xleftarrow{\quad \mathrm{Enc}_k(m_{i,b}) \quad}$

repeat poly(λ) times

guess b'

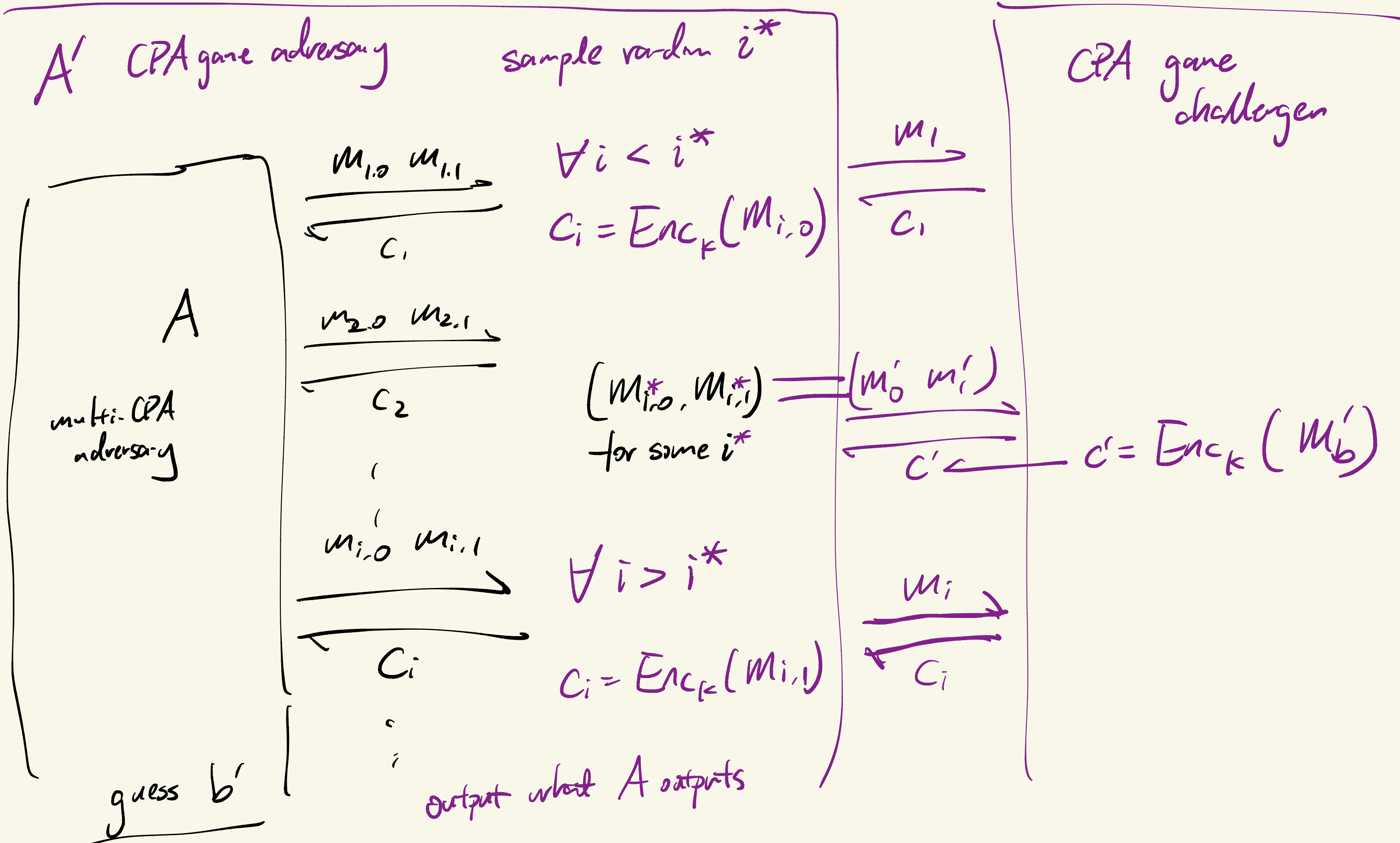
A win iff $b' = b$

THM

CPA security $\Longleftrightarrow$ multi CPA security

Pf. Assume A wins $\mathrm{PrivK}^{\text{multi-CPA}}_{A,\pi}$ w/ non-negl prob,

Construct another A' win $\mathrm{PrivK}^{\text{CPA}}_{A',\pi}$


A' CPA game adversary
sample random i*
CPA game challenger
A
multi-CPA adversary
m_{1,0} m_{1,1}
c_1
∀ i < i*
c_i = Enc_k(m_{i,0})
m_1
c_1
m_{2,0} m_{2,1}
c_2
(m_{i*,0}, m_{i*,1})
for some i*
(m'_0 m'_1)
c'
c' = Enc_k(m'_b)
m_{i,0} m_{i,1}
∀ i > i*
c_i
c_i = Enc_k(m_{i,1})
m_i
c_i
guess b'
output what A outputs