Last Lecture:

Perfect Secrecy in the presence of an eavesdropper

Indistinguishability encryption in the presence of an eavesdropper

$$\mathrm{PrivK}^{eav}_{A,\Pi}$$

private key

adversary

encryption scheme

$$\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$$

generate key

encrypt

decrypt

$$\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$$

private key — adversary — encryption scheme

λ: security parameter

(informally, $\approx$ key length)

$\boxed{\begin{array}{lcl} \mathcal{A}(1^\lambda) & & k \leftarrow \mathrm{Gen}(1^\lambda) \\ & \xrightarrow{m_0\ m_1} & b \xleftarrow{\$} \{0,1\} \\ \text{choose } m_0\ m_1 & & \\ & \xleftarrow[c]{} & c \leftarrow \mathrm{Enc}(k, m_b) \\ \xrightarrow{\text{output } b'} & & \end{array}}$

game outputs $\begin{cases} 1 \text{ (means } \mathcal{A} \text{ wins) if } b' = b \\ 0 \text{ (means } \mathcal{A} \text{ loses) if } b' \neq b \end{cases}$

$$\underbrace{\mathrm{Priv}K}_{\text{private key}}{}^{\overline{eav}}_{\underbrace{A}_{\text{adversary}},\ \underbrace{\Pi}_{\text{encryption scheme}}}$$

negl(λ) is a family of functions

$$f \in \mathrm{negl}(\lambda) \iff f(\lambda) \in O\left(\frac{1}{\lambda^k}\right) \ \forall k$$

Def. Prefect Secrecy in the presence of the eavesdropper $\equiv \forall A \ \Pr\left[\mathrm{Priv}K^{eav}_{A,\Pi} \to 1\right] = \frac{1}{2}$

Def. Indistinguishability encryption in the presence of the eavesdropper $\equiv$ $\forall$ poly-time A

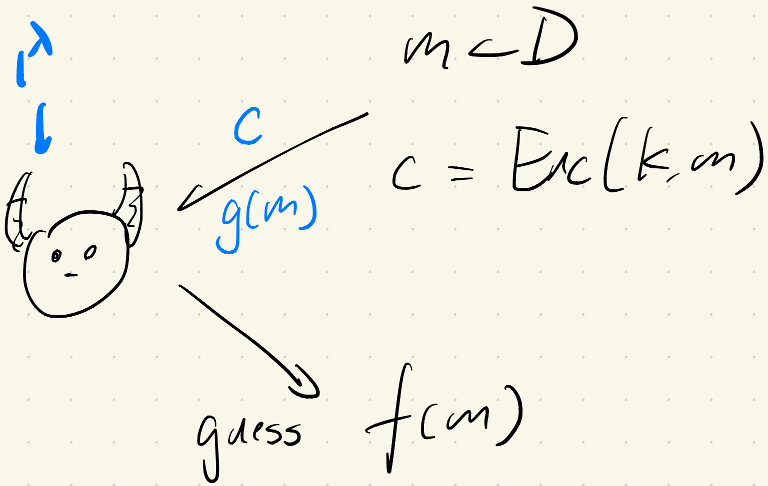
(a kind of computational security) $\Pr\left[\mathrm{Priv}K^{eav}_{A,\Pi}(1^\lambda) \to 1\right] = \frac{1}{2} \pm \mathrm{negl}(\lambda)$

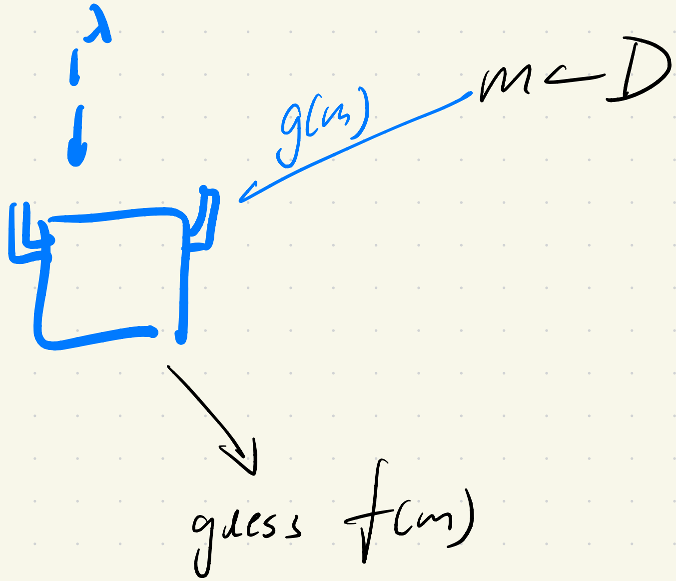
Semantic Secrecy

Distribution D_λ ~ message space

$\forall$ poly-time samplable D

$\forall f, g \in P$ $\quad\forall$ p.p.t. $\quad\exists$ p.p.t.





$$\left| \Pr[\ \text{guess } f(m) \text{ correctly}\ ] - \Pr[\ \text{guess } f(m) \text{ correctly}\ ] \right| \le negl(\lambda)$$

Indistinguishability ⟹ Semantic Security

Assume Π is not semantically secure.

$\Downarrow$

$\exists \underbrace{D, f, g, A}_{\text{poly-time}}$

A'

$A'(g(m)) \xrightarrow{\text{guess}} f(m)$

$m' \leftarrow D_\lambda,\ k \leftarrow Gen(1^\lambda)$

$c \leftarrow Enc(k, m')$

$A(g(m), c)$

Construct an distinguish /adversary in the indistinguishability game

$m_0 \leftarrow D_\lambda \quad m_1 \leftarrow D_\lambda$

$\xrightarrow{m_0, m_1}$

challenger

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

$c = Enc(k, m_b)$

$\xleftarrow{c}$

$A(g(m_0), c) \stackrel{?}{=} f(m_0)$

output $\begin{cases} 0 & \text{if guess correctly} \\ 1 & \text{if guess incorrectly} \end{cases}$

$$\Pr[\text{wins}] = \frac{1}{2} + \frac{1}{2}\Big(\Pr[A \text{ guess correctly in semantic security game}] - \Pr[A' \text{ guess correctly in the semant game}]\Big)$$

$f \in negl(\lambda)$

$\forall k \quad f \in O\left(\frac{1}{\lambda^k}\right)$

$\forall k \; \exists c, L \quad \forall \lambda > L$

$$f(\lambda) \leq \frac{c}{\lambda^k}$$

$f \in negl(\lambda)$

$\exists k, \; \forall c, L \quad \exists \lambda > L$

$$f(\lambda) > \frac{c}{\lambda^k}$$

$$f \notin negl(\lambda) \Longleftarrow f \in \Omega\left(\frac{1}{\lambda^k}\right)$$

(fix-length) Encryption Scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$

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

$\mathrm{Gen}(1^\lambda)$: sample $k \leftarrow \{0,1\}^\lambda$

$\mathrm{Enc}(k, m) = m \oplus g(k)$

$\mathrm{Dec}(k, c) = c \oplus g(k)$

$\mathrm{Gen}(1^\lambda)$: $r \leftarrow \{0,1\}^{\ell(\lambda)}$

$\mathrm{Enc}(r, m)$: $r \oplus m$

$\mathrm{Dec}(r, c)$: $r \oplus c$

---

g is a secure PRG $\Longrightarrow$ above is $\Big\{$ semantically secure / indistinguishability encryption in the presence of eavesdropper

$k \leftarrow \{0,1\}^\lambda$

$\xrightarrow{m_0 \;\, m_1}$

$\xleftarrow{\;c\;}$

$c = m_b \oplus g(k)$

guess b'

$\Pr[\text{guess correctly}] \geq \frac{1}{2} + \frac{1}{\mathrm{poly}(\lambda)}$

$r \leftarrow \{0,1\}^{\ell(\lambda)}$

$\xrightarrow{m_0 \;\, m_1}$

$\xleftarrow{\;c\;}$

$c = m_b \oplus r$

guess b'

$\Pr[\text{guess correctly}] = \frac{1}{2}$

Assumption: pseudorandom generator (PRG) exists

Def (PRG): PRG is function $g : \{0,1\}^* \to \{0,1\}^*$

i) poly-time

ii) $|g(x)| = \ell(|x|)$

$x \in \{0,1\}^\lambda \implies g(x) \in \{0,1\}^{\ell(\lambda)}$

iii) $r \leftarrow \{0,1\}^\lambda$ "g(r) looks uniform"

$\ell(\lambda) = 2\lambda$

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

$\ell(\lambda) = \lambda^2$

$\ell(\lambda) = \lambda^{10000}$

$\forall$ p.p.t. D distinguisher

$$\left| \Pr_{s \leftarrow \{0,1\}^\lambda} [D(g(s)) \to 1] - \Pr_{r \leftarrow \{0,1\}^{\ell(\lambda)}} [D(r) \to 1] \right| \leq \mathrm{negl}(\lambda)$$

Assume g is a secure PRG

- $g_1(\underbrace{x}_{(\lambda-1)} \| \underbrace{b}_{1\text{-bit}}) = g(x) \| b$

$\ell_1(\lambda) = \ell(\lambda-1)+1$

- $g_2(\underbrace{x}_{\lceil \frac{\lambda}{2} \rceil\text{-bit}} \| \underbrace{y}_{\lfloor \frac{\lambda}{2} \rfloor\text{-bit}}) = g(x) \| g(y)$

$\ell_2(\lambda) = 2\,\ell(\frac{\lambda}{2})$

Pf. Assume g_1 isn't a secure PRG

Let D_1 be the distinguisher

Construct D base on D_1 that breaks g

$$\boxed{\begin{array}{l} D(z) \\ \quad \text{sample } b \leftarrow \{0,1\} \\ \quad \text{call } D_1(z \| b) \\ \quad \text{output whatever } D_1 \text{ outputs} \end{array}}$$

Extend + e stretch of PRG

(ℓ)

$h(x)$

$b \| z \leftarrow g(x)$

output $b \| g(z)$

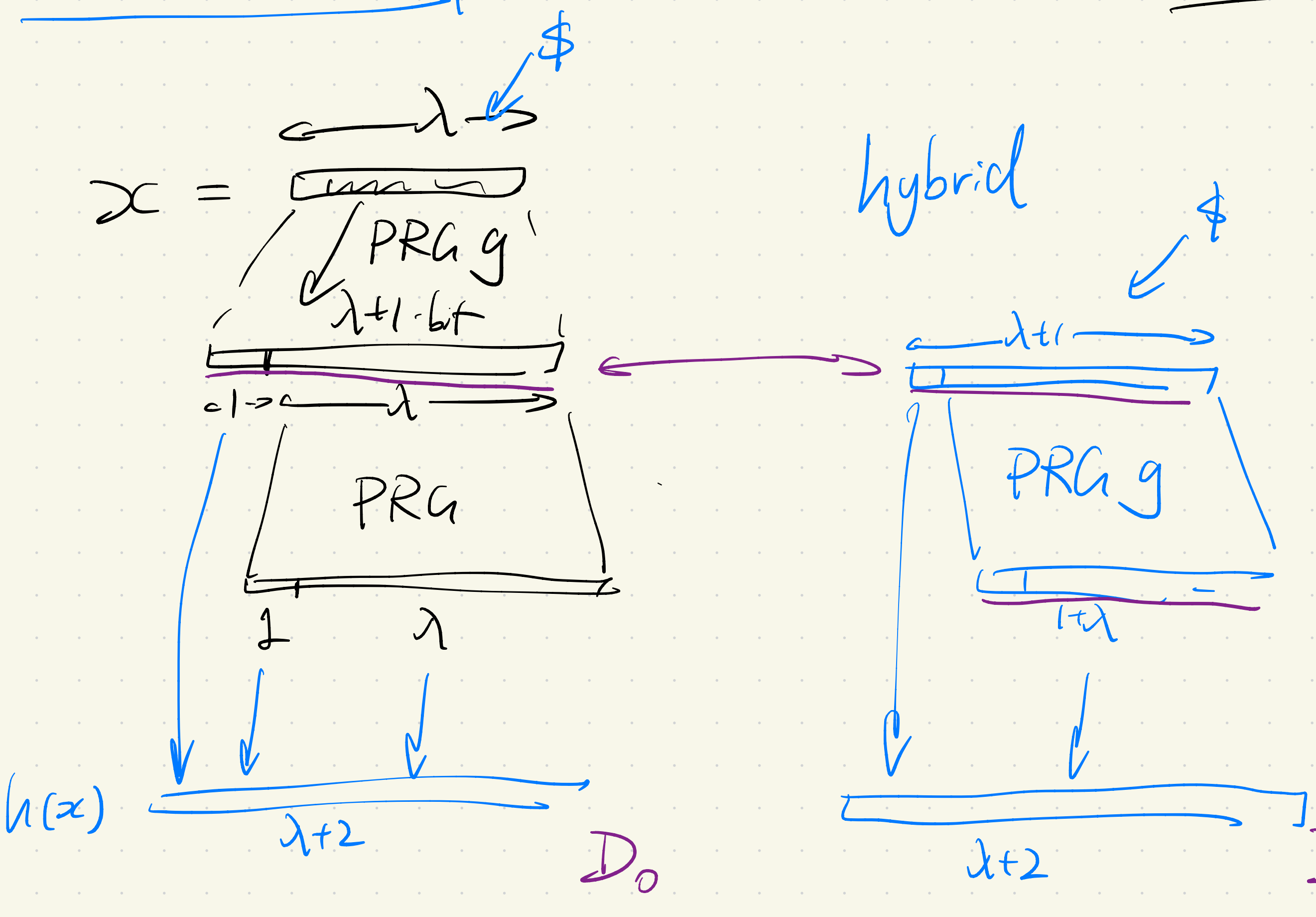
Assume exist PRG g: such that

$$|g(x)| = |x| + 1$$

$\Downarrow$

$\forall$ poly ℓ, exist PRG h

$$|h(x)| = \ell(|x|)$$



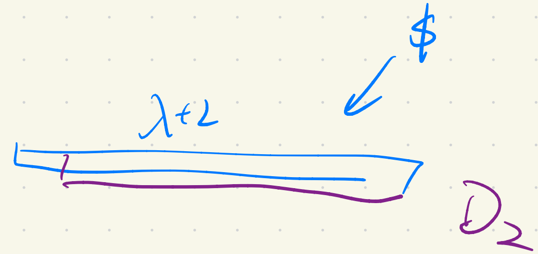
Assume $\exists$ p.p.t. A

$$\left| \Pr_{x \leftarrow D_0}[A(x) \to 1] - \Pr_{x \leftarrow D_1}[A(x) \to 1] \right| \geq \frac{1}{poly(\lambda)}$$

Construct A'

$A'(b \| y)$

call $A(b \| g(y))$



assume secure PRG g s.t. $|g(x)| = |x| + 1$

$\forall$ poly ℓ

PRG h

$h(x)$

for $i = 1 \cdots \ell$

$y_i \| x \leftarrow g(x)$

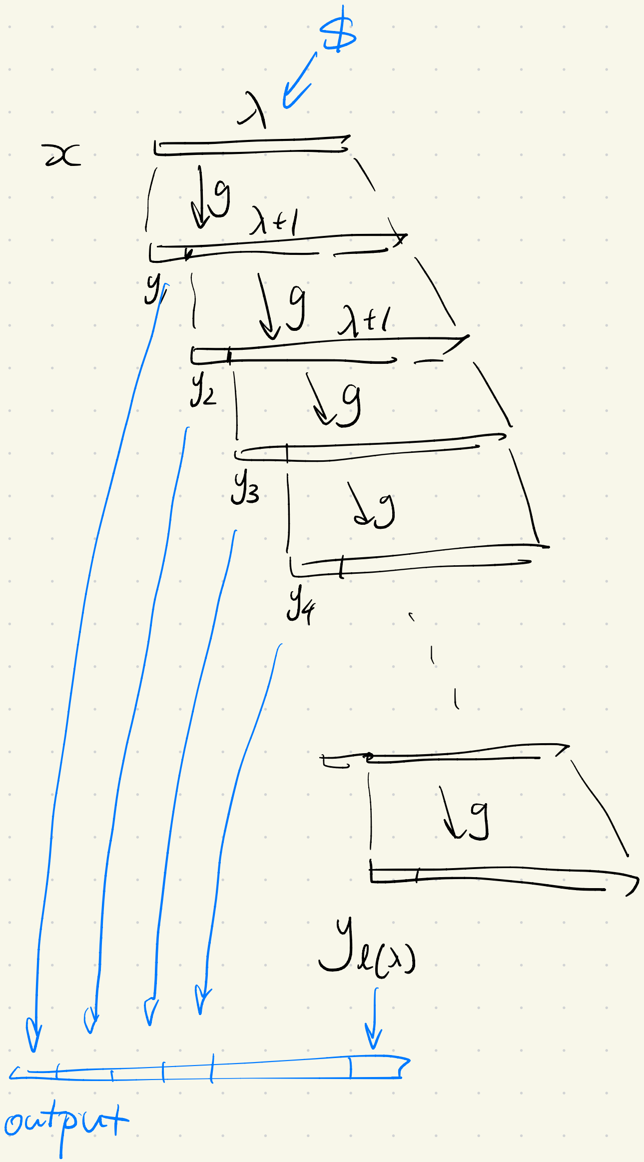
output $y_1 y_2 \cdots y_\ell$

$h(x)$

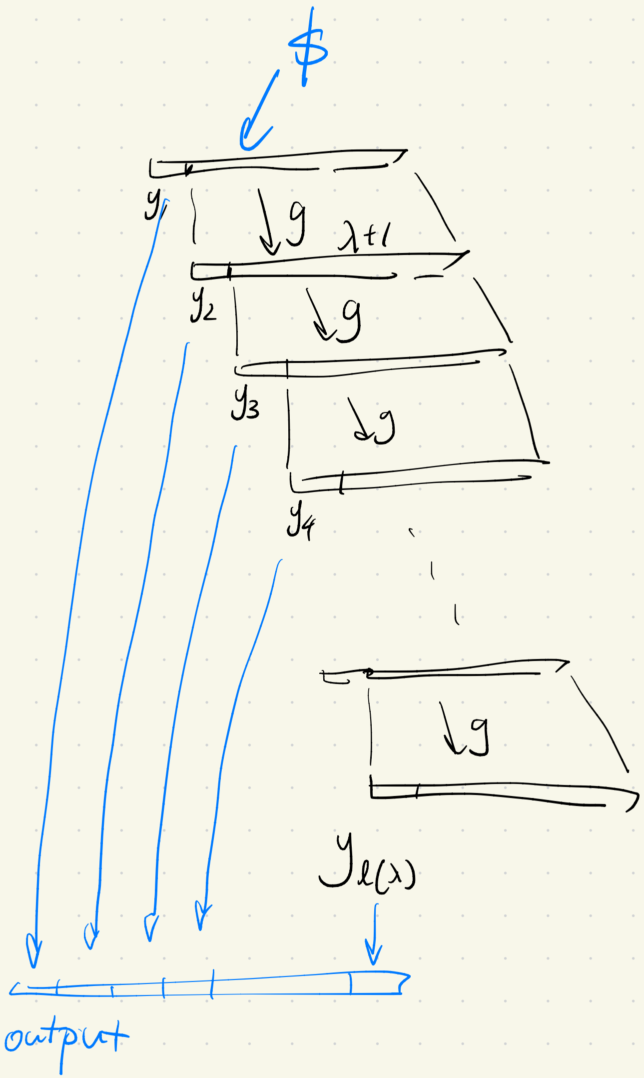
for $i = 1, 2, \cdots$

$y_i \| x \leftarrow g(x)$

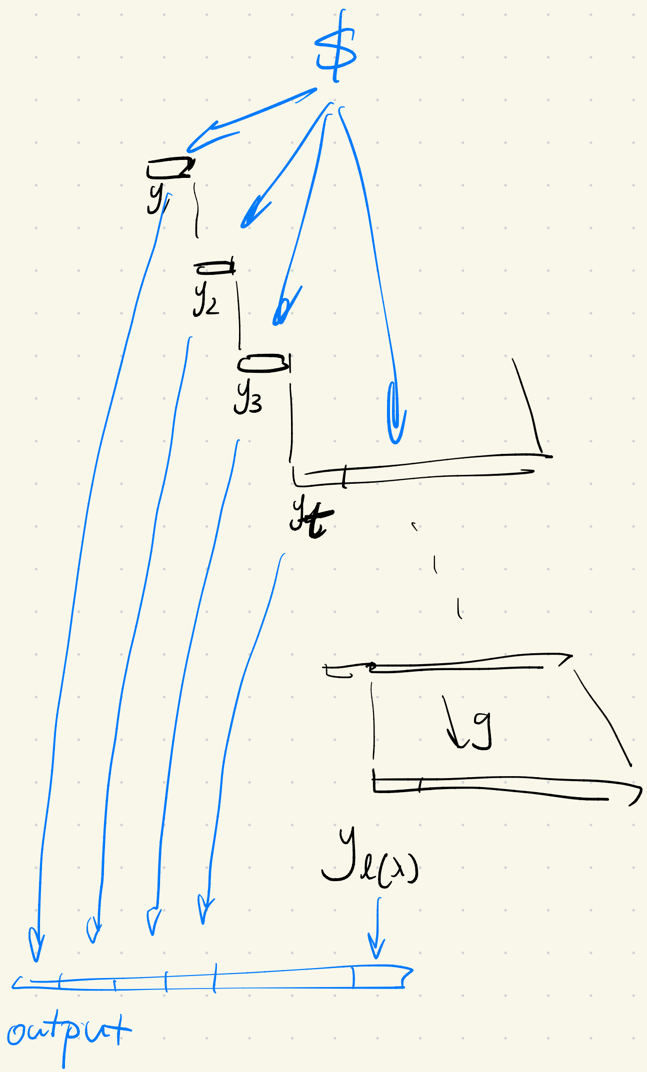
output y_i


$
λ
x
g
λ+1
y1
y2
y3
y4
yℓ(λ)
output

D_0

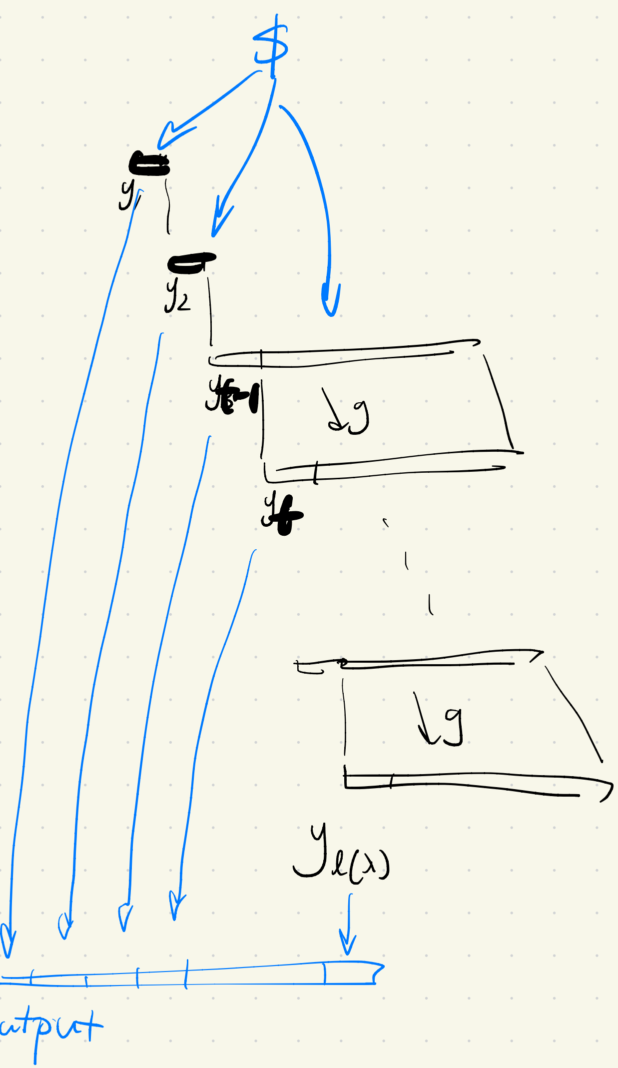

$
g
λ+1
y1
y2
y3
y4
yℓ(λ)
output

D_1

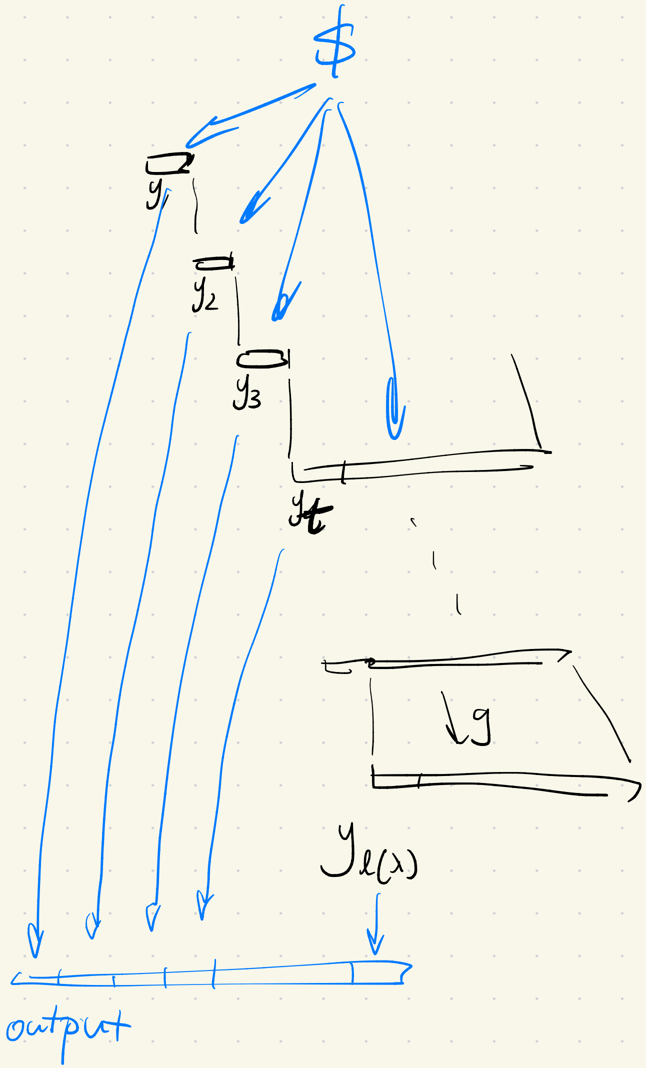

$
y1
y2
y3
yt
g
yℓ(λ)
output

D_t

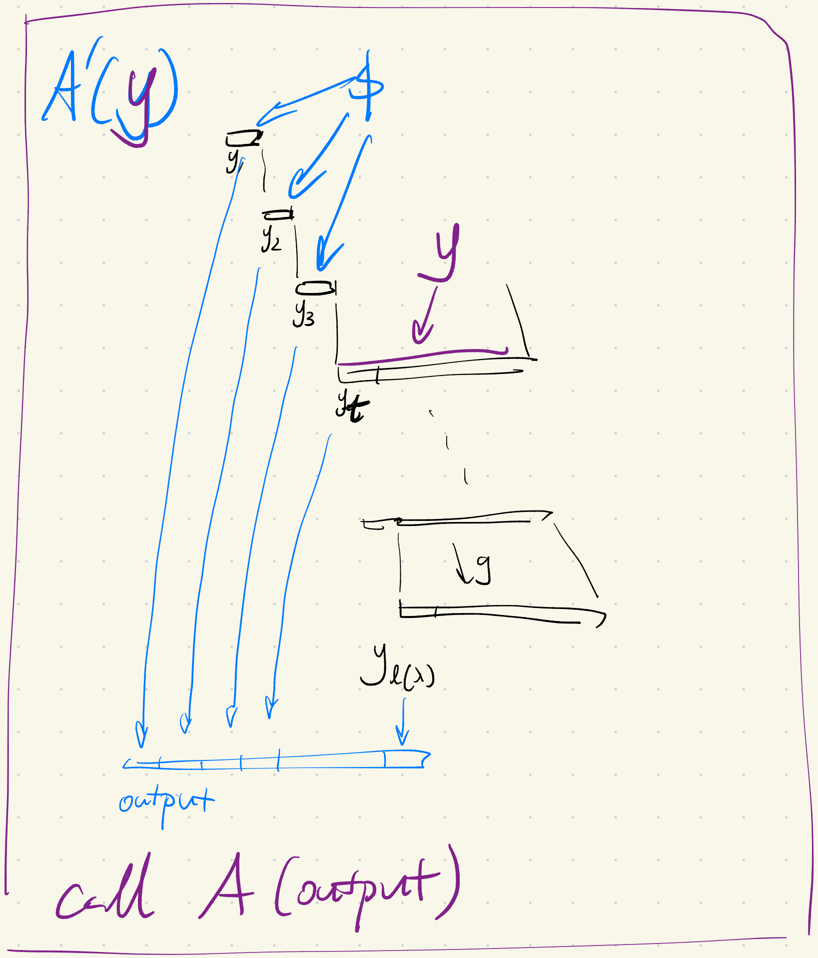
Construct distinguisher A' that distinguish $g(s)$ and r



D_{t-1}



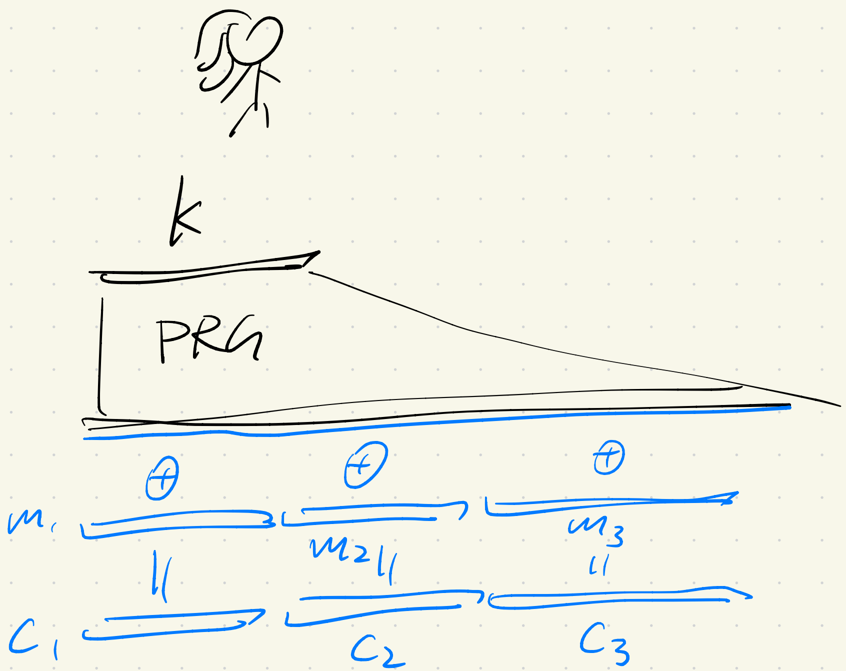
D_t

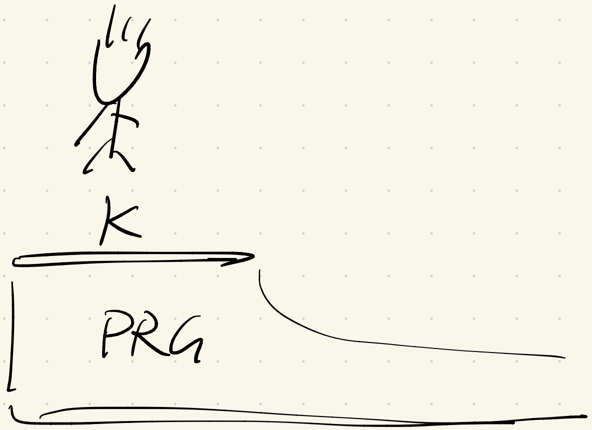


Assume $\exists$ p.p.t. A that distinguishes D_{t-1} D_t

Stream Cipher

stateful v.s. stateless





Next Lecture: One-way Function:

$$f: \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$$

$$f: \{0,1\}^\lambda \rightarrow \{0,1\}^{\ell(\lambda)}$$

- f is poly-time computable
- "Given $f(x)$, hard to find x' s.t. $f(x') = f(x)$"

  -- find $x' \in f^{-1}(f(x))$"