Notes for 9/18. cryptography

Last Lecture:

- Perfect Secrecy
- OTP (one-time pad)

Today:

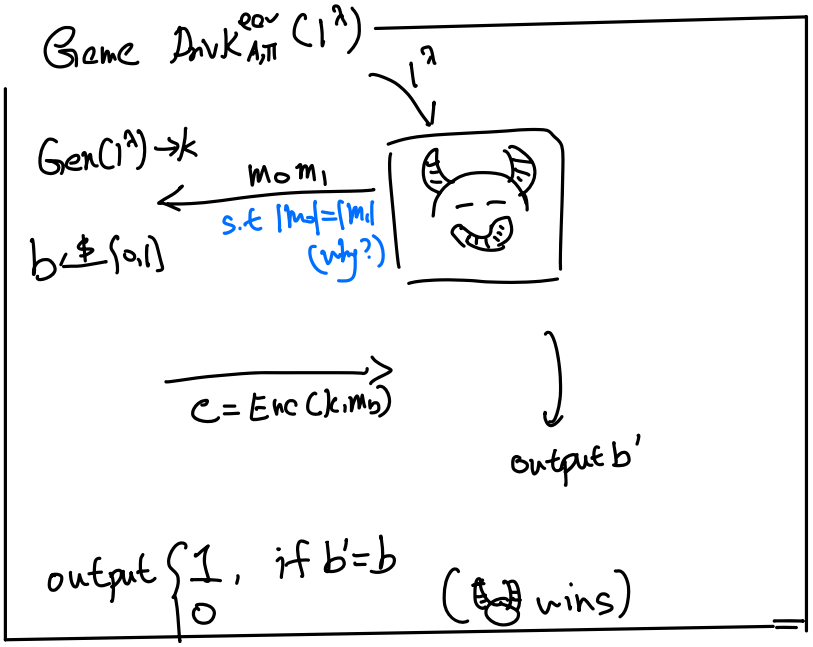
(Computational) Indistinguishability encryption in the presence of an eavesdropper.

Define game : $PrivK^{eav}_{A,\Pi}$

private key

adversary

scheme (Gen, Enc, Dec)

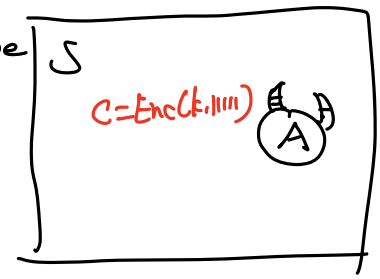


Π is an indistinguishability encryption . in p. o. an, eav.

if $\forall$ p.p.t. A

$Pr[PrivK^{eav}_{A,\Pi}(1^\lambda) = 1] \leq \frac{1}{2} + negl(\lambda)$

Let S^* be

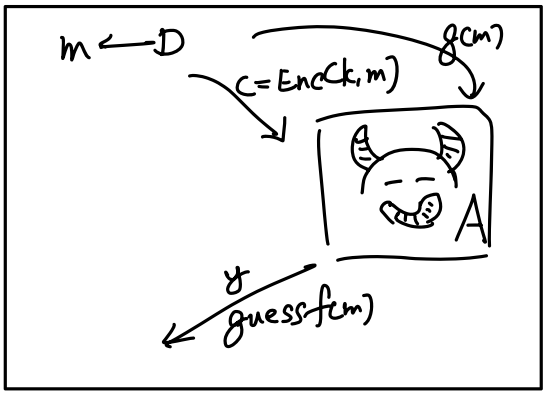


Let D_m be uniform over $\{m_0, m_1\}$

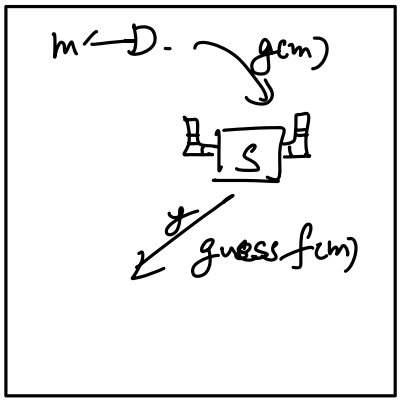
(computational) Semantic Security

$\forall$ Distribution D over message, $f, g,$ $\exists$ Simulator S

poly-time samplable $\in P$ ppt ppt



A wins if $y = f(m)$



S wins if $y = f(m)$

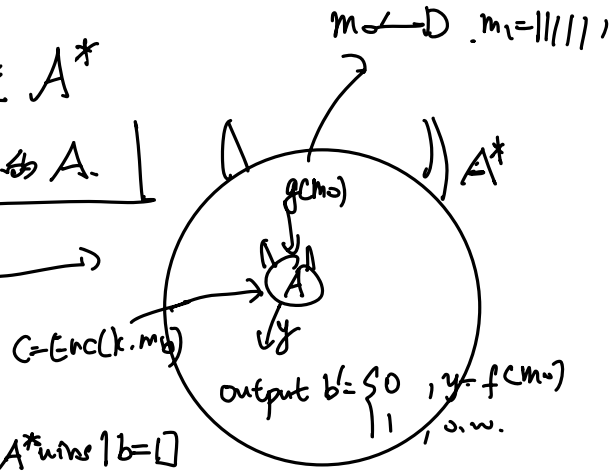
$$Pr[S \text{ wins}] \geq Pr[A \text{ wins}] - negl(\lambda)$$

Semantic ⇒ Indistinguishable

若不满足 Semantic，在 Indistinguishable 中构造 A^*

生构造 S. S为输入 $c = Enc(k, 111111)$ 给 A.

A^* 先输出 $m_0 \leftarrow D$, $m_1 = 111111\cdots1$



$$\frac{1}{2} + negl(\lambda) \geq Pr[A^* \text{ wins}] = \frac{1}{2} Pr[A^* \text{ wins} \mid b=0] + \frac{1}{2} Pr[A^* \text{ wins} \mid b=1]$$

$$= \frac{1}{2} Pr[A \text{ wins}] + \frac{1}{2}(1 - Pr[S \text{ wins}])$$

$$= \frac{1}{2} + \frac{1}{2}(Pr[A \text{ wins}] - Pr[S \text{ wins}])$$

(Thus: $\leq negl(\lambda)$)

Pseudorandom Generator

$g: \{0,1\}^* \to \{0,1\}^*$ $\quad \{0,1\}^n \to \{0,1\}^{\ell(n)}$

stretch function $\ell: \mathbb{N} \to \mathbb{N}$

$|g(x)| = \ell(|x|)$ $\quad \ell(n) > n$

e.g. $\ell(n) = n+1$

$\ell(n) = 2n$

$\ell(n) = n^2$

▷ g is poly-time computable

▷ $|g(x)| = \ell(|x|) > |x|$

▷ Pseudorandomness ∴

Pseudorandomness:

$\forall$ p.p.t. Distinguisher D

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

Π is an example where $\lvert K \rvert < \lvert M \rvert$	OTP
$K = \{0,1\}^\lambda$	
$M = C = \{0,1\}^{\ell(\lambda)}$	
$\mathrm{Gen}(1^\lambda)$ sample $k \subset \{0,1\}^\lambda$	$\mathrm{Gen}: k \leftarrow$
$\mathrm{Enc}(k,m) = g(k) \oplus m$	$\mathrm{Enc}(k,m) = k \oplus m$
$\mathrm{Dec}(k,c) = g(k) \oplus c$	$\mathrm{Dec}(k,c) = k \oplus c$

$\Leftrightarrow$

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

Proof that Π is secure.

if A is an adversary, Construct a distinguisher with A.

$D(x)$:

$b \leftarrow \{0,1\}$ — m_0, m_1 — A

$x \oplus m_b$ → output b'

D outputs $b == b'$.

$$\Pr_{s \leftarrow \{0,1\}^\lambda}[D(g(s)) \to 1] = \Pr[A \text{ wins in } \mathrm{PrivK}^{\mathrm{eav}}_{A,\Pi}]$$

$$\Pr_{x \leftarrow \{0,1\}^{\ell(\lambda)}}[D(x) \to 1] = \Pr[A \text{ wins in } \mathrm{PrivK}^{\mathrm{eav}}_{A,\mathrm{OTP}}] = 1/2$$

□

Assume g is PRG:

1° Then $g'(x \| b) = g(x) \| b$ is a PRG

Pf: If not, D' efficiently distinguishes g', for infinitely many λ

$$\left| \Pr[D'(g'(x \| b)) \to 1] - \Pr[D'(y) \to 1] \right| \geq \frac{1}{\mathrm{poly}(\lambda)}$$

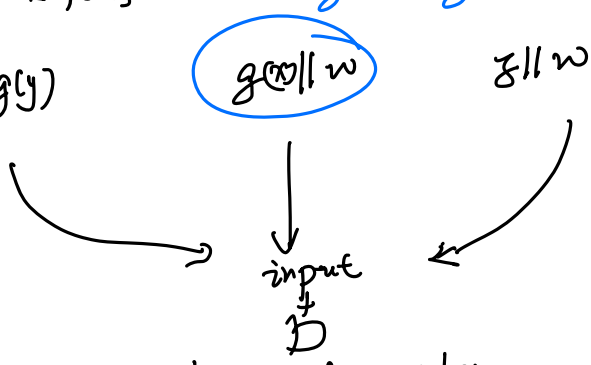
Construct $D(y)$

> sample $b \leftarrow \{0,1\}$
> compute $D'(y \| b)$
> output whatever D' outputs

2° Then $g'(x\|y) = g(x)\|g(y)$

$x\|y \xleftarrow{\$} \{0,1\}^{\lambda*2}$

$g(x)\|g(y)$ $\quad$ hybrid argument $\quad$ $g(x)\|w$ $\quad$ $g\|w \xleftarrow{\$} \{0,1\}^{\ell(\lambda)*2}$



Pf: If g' not PRG. Let D' be a distinguisher

Then Either $|Pr[D'(g(x)\|g(y))\to 1] - Pr[D'(g(x)\|w)\to 1]| \geq \frac{1}{p(\lambda)}$

or $|Pr[D'(g(x)\|w)\to 1] - Pr[D'(g\|w)\to 1]| \geq \frac{1}{p(\lambda)}$

for inf. many λ.

Define $D(w)$

sample x.

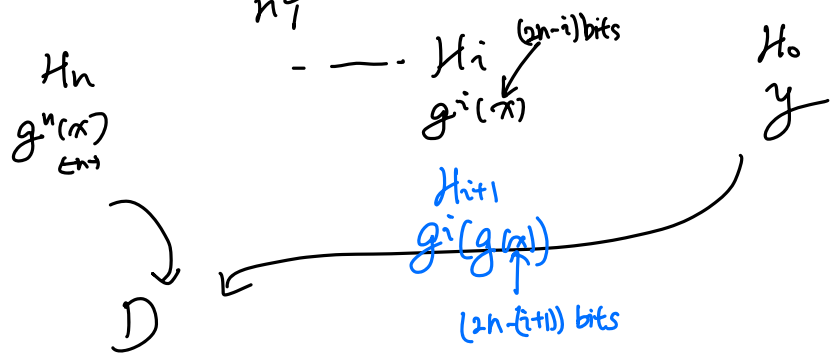
Output $D'(g(x)\|w)$ $\square$

$\exists$ PRG g with stretch $\ell(n)=n+1$

$\Rightarrow \exists$ PRG $\quad$ — $\ell(n)=n+2$

$\Rightarrow \exists$ — — — $\ell(n)=2n$

$g'(x) = g(g(\cdots g(x)\cdots))$ (n times)



$D(y)$

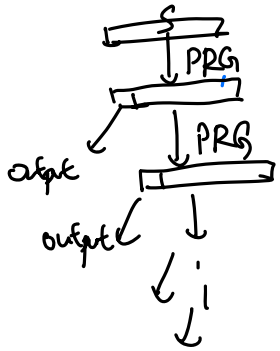
$g(g(\cdots g(y)\cdots))$ (i times)

output $D'(\cdot)$

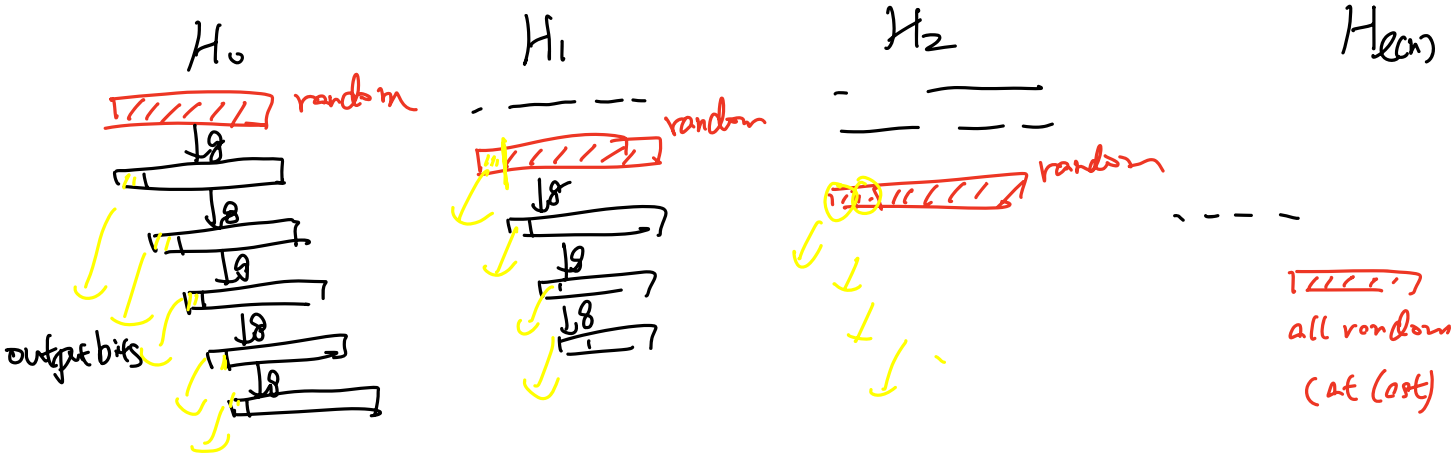
problems

: 量性相差 D.

: laborious

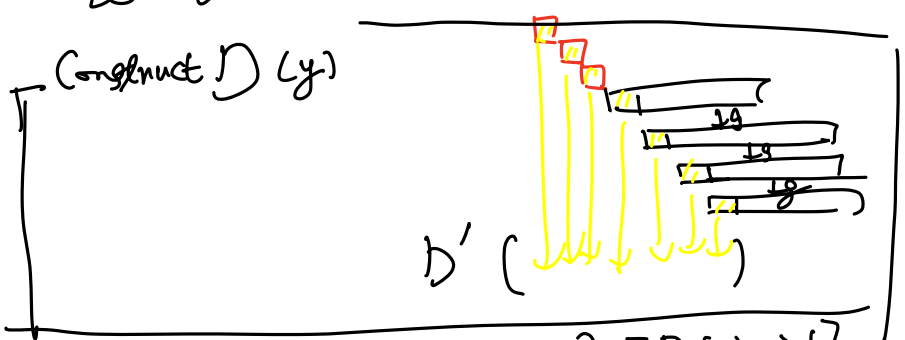


$g'(s)$. let $s_1 = s$.
for $i = 0, 1, 2, \ldots$
$s_{i+1} = g$(last n-bit of s_i)
output first bits of s_1, s_2



Assume g' is not a PRG

Let D' — —



$\Pr[D(g(s)) \to 1]$ $\qquad$ $\Pr[D(y) \to 1]$

$\|$ $\qquad$ $\|$

$\frac{1}{l(n)} \sum_{i=1}^{l(n)} [D' \to 1 \text{ in } H_i]$ $\qquad$ $\frac{1}{l(n)} \sum [D' \to 1 \text{ in } H_{i+1}]$

$H_0, H_1, \ldots, H_{l(n)-1}$ $\qquad$ $H_1, H_2, \ldots, H_{l(n)}$

* stream cipher 流密码 stateful v.s. stateless.