Symmetric Crypto  Lec 2.  (Apr 4'24)

Outline:
- Recap
- Game-based Defn.
- PRG extension (BM'84)
- Hybrid Arguments
- PRFs from PRG (GGM'84)
- Wrap up

RECAP:
Goldreich-Levin
OWF $\rightarrow$ PRG
(1-bit stretch)
Last class

Today
Blum-Micali
PRG
(poly(1))-stretch

GGM
PRF

LR
PRP/
Block Cipher
Def: A PRG $G : S \rightarrow R$ is a deterministic, poly-time algorithm that given a seed $s \in S$ (seed space) as input, outputs $\mathbf{r} \in R$ (output space).

$G$ is secure, if for all efficient adversaries $A$,

$$\left| \Pr[A(r) = 1 : s \leftarrow S, r \leftarrow G(s)] - \Pr[A(r) = 1 : r \leftarrow R] \right| \leq \text{neg}(\lambda)$$

Here, the probability space is over random choice of $s, r$, and randomness of $A$.

Last lecture: Secure PRG $G : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$

with 1-bit stretch from a OWF using hard core bits (GIL)

Today: Given a secure PRG:

$G : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$, we build another PRG,

$G' : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$, where $l$ is a poly, $l(n) > n+1$
Game-based definition of PRG security: -

In the above definition, the adversary A needs to act as a distinguisher between two distributions:

\[ \frac{\mathcal{S}}{Y} \text{ vs. } \frac{\mathcal{R}}{Y} \]

We can reframe this as a game between A and a challenger:

**Experiment 0:**

- **Challenger:**
  - \( S \) \( \subseteq \mathcal{S} \)
  - \( r \leftarrow \mathcal{G}(S) \)

- **A:**
  - \( r \)

**Experiment 1:**

- **Challenger:**
  - \( \mathcal{R} \)
  - \( r \leftarrow \mathcal{G}(\mathcal{R}) \)

- **A:**
  - \( r \)
Let $W_0$: Event that $A$ outputs 1 in $\text{Exp} \, 0$.

Let $W_1$: $\ldots$ $\ldots$ $\ldots$ $\text{Exp} \, 1$.

Then, we define:

$$\text{PRGAdv} [A, G_1] = \text{Advantage of } A \text{ in the PRG security game for } G_1$$

$$= \left| \Pr (W_0) - \Pr (W_1) \right|$$

where the probability space is over the random choices of the Challenger and $A$.

$G_1$ is secure if, for efficient adversaries $A$,

$$\text{PRGAdv} [A, G_1] \leq \text{negl}(\lambda).$$

(Identical to the distribution-based defn. above.

PRG Extension: -- (Blum-Micali '84)

Let $G_1 : \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ be a secure PRG.

We will construct $G_3 : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$.
We can sequentially compose $G_1$, to get many random-looking bits.

Formally, $G_1^i(\mathbf{g} \in \{0,1\}^n)$:

$\mathbf{g}_0 = \mathbf{g}$

For each $i \in \{1,2,\ldots,\ell(m)\}$:

$(\mathbf{g}_i, b_i) \leftarrow G_1(\mathbf{g}_{i-1})$

$\text{OPL} (b_1, \ldots, b_{\ell(m)})$

Is $G_1^i$ a secure PRG? 

1) Efficient? Let $t(n)$ be the runtime of $G_1$. Then, $G_1^i$ runtime is:

$l(m) \cdot t(n) + O(l(m))$ is poly.
Thm. For every adv A playing the PRG game for $G_1$, let an adversary $B$ that plays the PRG game for $G_1$, s.t.

$$\text{PRG Adv} (A, G_1) = l(n) \cdot \text{PRG Adv} (B, G_1).$$

Proof. Informally:

(i) For random $s$, the OIP of $G_1$ looks random, so, we can replace $(b_1, b_2)$ by random elements:

$$s, \in \{0, 1\}^n$$

(ii) Now, $s$, is random, so we can
replace $(s_2, b_2)$ by random elements:

\[ s_2 \leftarrow \{0, 1\}^n, \]

\[ b_2 \leftarrow \{0, 1\} \]

and so on. (we can do this for each)

**HOW TO FORMALIZE THE ABOVE INTUITION?**

**Hybrid Arguments**: Recall we defined 2 games, Expo, Exp1 in the PRG1 security defn.

**Expo**: $H_0$ samples

$S \leftarrow \{0, 1\}^n$ and gives $r = G_1(s)$ to $A$.

Send $r = (b_1, b_2, \ldots, b_{\ell(n)})$ to $A$.

We'll now define a sequence of hybrid games, $H_0 = \text{Expo}, H_1, \ldots, H_{\ell(n)}$, where we'll slightly change the challenger's behavior in each hybrid.
Hybrid 1: 

Given samples $s_1, b_1 \in \{0,1\}^n$,

where $s_1 \in \{0,1\}^n \rightarrow G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow \cdots \rightarrow G_m \rightarrow \{0,1\}^n$.

$b_i \in \{0,1\}$

$b_2$

$b_3$

$b_4 \in \{0,1\}^n$

etc.

give $m = (b_1, b_2, \ldots, b_m)$ to $A$.

(Informally, no adv should be able to distinguish $b_i$ for $\{0,1\}^n$ due to security of PRG $G_i$.)

Hybrid $j$: 

Hybrid $j$: 

Given samples $s_j \in \{0,1\}^n$,

where $s_j \in \{0,1\}^n \rightarrow G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow \cdots \rightarrow G_m \rightarrow \{0,1\}^n$

$(b_1, b_2, \ldots, b_j \in \{0,1\}^n, b_{j+1}, \ldots, b_m)$

Hybrid $m$: 

$(b_1, b_2, \ldots, b_m \in \{0,1\}^n)$

$\equiv \text{Exp} 1$ in PRG security defn.

For $i \in \{0,1, \ldots, l(n)\}$, define $p_i$ as the probability that $A$ outputs 1 in Hybrid game $H_i$.

By defn.
\[
\text{PRG1 Adv}[A, G_1] = |Pr\{\text{adv} - Pr\{M_1\}|
\]

= \left| \Pr[1 \rightarrow 0] - \Pr[0 \rightarrow 1] \right|

Now, we'll construct the \text{adv} B playing the PRG1 security game for \( G_1 \).

In the game that B is playing, \( \text{ExpO} : \tau = G_1(s) \) for random seed \( s \).
i.e. $b_1 \ldots b_{w-1}$: random, but

$b_w$, \ldots, been generated as in $H_{w-1}$.

$r \stackrel{\$}{\leftarrow} (S_b, b_w)$

This is Hybrid $H_{w-1}$ from
A's perspective.

Exp 1: $r \stackrel{\$}{\leftarrow} (S_b, b_w)$

$\Rightarrow$ $b_1, \ldots, b_w$: random.

$\Rightarrow$ $B$ 'identically simulates' hybrid $H_w$ to A.

This means, $Pr$ A outputs 1 in $H_{j-1}$

$Pr$ ($W_0, B \mid w = j$) = $P_{j-1}$

event that

B outputs 1
in Expo

* B outputs whatever A outputs

* B is simulating $H_{j-1}$ in

the event $W_{0B} / w = j$, so,

A outputs 1 with prob $P_{j-1}$

$Pr( W_{1B} \mid w = j ) = P_j$ for all $j$...

so,

$PRG\text{ Adv} [B, G] = |Pr[W_{0B}] - Pr[W_{1B}]|.$

By total probability: -
\[
\begin{align*}
&= \left[ \frac{\sum_{j=1}^{\ell(n)} \Pr(\text{w}_{0:j} | w = j) \cdot \Pr(w = j)}{\ell(n)} \right] \\
&\quad - \left[ \frac{\sum_{j=1}^{\ell(n)} \Pr(\text{w}_{1:j} | w = j) \cdot \Pr(w = j)}{\ell(n)} \right] \\
&\quad \text{Since } w \text{ is sampled uniformly from } \{1, \ldots, \ell(n)\}, \\
&\quad = \left[ \frac{\Pr_0 + \Pr_1 + \cdots + \Pr_{\ell(n)-1}}{\ell(n)} \right] \\
&\quad \quad - \left[ \frac{\Pr_1 - \Pr_2 - \cdots - \Pr_{\ell(n)-1} - \Pr_{\ell(n)}}{\ell(n)} \right] \\
&\quad = \left[ \frac{\Pr_0 - \Pr_{\ell(n)}}{\ell(n)} \right] \\
&\quad = \frac{1}{\ell(n)} \cdot \text{PRG}^{\text{Adv}}[A, G] \\
&\quad \text{i.e. } \text{PRG}^{\text{Adv}}[A, G] = \frac{1}{\ell(n)} \cdot \text{PRG}^{\text{Adv}}[B, G]. \\
&\quad \text{So, if } G \text{ is secure, meaning } \text{PRG}^{\text{Adv}}[B, G] \\
&\quad \text{is } \text{negl}(X) \text{ if } B, \\
&\quad \text{then, } G' \text{ must also be secure} \\
&\quad \text{bc } \ell(n) \cdot \text{negl}(X) \text{ is } \text{negl}(\ell(n)). \\
&\quad \text{Hence, } G' \text{ is a secure PRG}. 
\end{align*}
\]
**PRFs**: (pseudo random functions)

**PRF** $F: K \times X \rightarrow Y$: deterministic, efficient key, input, output space, space. Informally, for a random key $K$,

$F(K, \cdot)$ should look like a random function from $X$ to $Y$.

$\text{Func}(X, Y) =$ space of all functions from $X$ to $Y$.

E.g., if $K = \{0, 1\}^{128} = X = Y$,

$\# \text{ keys} = 2^{128} \neq \# \text{ PRFs}.$

But $\# \text{ functions in Func}(X, Y) = |Y|^{128} = (2^{128})^{2^{128}}$.

i.e. $\text{Func}(X, Y) >> 128 \times 128$.

**PRF security game**:
Exp 0:

\[ f(x_i) = F(k, x_i) \]

Adv. can make poly. # queries on arbitrary \( x_i \).

Exp 1:

Let \( W_0 \): Event that \( A \) outputs 1 in Exp 1.

Advantage of \( A \) w.r.t. PRF \( F \):

\[ \text{PRFAdv} [A, F] = |\Pr[W_0] - \Pr[W_1]| \]

\( A \) is called a \( Q \)-query adversary if it makes up to \( Q \) queries to the chal.
A PRF $F$ is secure if for efficient adversaries $A$, 
\[ \text{PRF-Adv}[A, F] \leq \text{negl}(\lambda). \]

**PRF from PRG**: (Goldreich, Goldwasser, Micali)

Given a PRG $G : S \rightarrow S \times S$, we can construct a PRF:

**Visualize $G$ as:**

```
        G7
       / \  \\
      /   \  \\
     /     \  \\
    /       \  \\
   /         \  \\
  /           \  \\
S0  S1
```

**"length-doubling"**

Let's say $S_0 = G_7(s)$

$S_1 = G_7(S_0)$.

We'll make

**PRF $F : S \times \{0, 1\}^l \rightarrow S$** as follows:

**Key space = $S$.** But strings, let's say $l = \lambda$.

$F(s, x) : \text{let } x = (x_1, \ldots, x_e)$

*E.g.* $l = 3$ and $x = [1, 0, 1]$

```
        G7
       / \  \\
      /   \  \\
     /     \  \\
    /       \  \\
   /         \  \\
  /           \  \\
S0  S1
```

```
S00 S10 S01 S11
```

```
S000 S001 S010 S011 S100 S101 S110
```

```
S0000 S0001 S0010 S0011 S0100 S0101 S0110 ...
```

*So on*
\[ F(8, 101) = 8_{101} \]

\[ = G_1, (G_{10}, (G_1, (8))) \]

\[ (x_3, x_2, x_1) \]

* For \( x = x_1, \ldots, x_e \), traverse the path in the above tree of evaluations.

Formally, \( F(s, (x_1, \ldots, x_e)) : \)

\[
t \leftarrow s \\
\text{for } i \leftarrow \{1, \ldots, e\} : \\
t \leftarrow G_1(x_i(t)) \\
\text{off } t.
\]

Is \( F \) a secure PRF?

1) Efficiency: \( l \) evals of \( G_1 \) \( \checkmark \)

\[ = \text{poly}(1) \]

2) Security:

Thm: For every \( q \)-query PRF adv. \( A \), we can construct a PRG adv \( B \), s.t.

\[ \text{PRFAdv}[A, F] = l \cdot q \cdot \text{PRGAdv}[B, G] \]

\[ \Rightarrow F \text{ is a secure PRF} \]
Proof Sketch:

Given $A$: an adv. for the PRF game for $F$, we'll construct $B$: an adv. for the PRG game for $G_i$.

We'll use the Hybrid argument!

Naively, we could replace each PRG call by random, one-by-one:

$H_0 = \text{Expo for } A$: $H_1$, $H_2$, ...

$\text{Chal samples: } s_0, s_i \in \mathcal{S}$

$B_0, B_i \leftarrow \mathcal{S}$

Note, there are $2^{i-1}$ PRGs on level $i$ of tree.

$\Rightarrow \# \text{Hybrids: } 1 + 2 + 2^2 + \ldots + 2^{l-1}$

$\Rightarrow 2^l - 1$. \( \text{This is a problem...} \)
Now, we'll construct $B$, an adversary for the PRG game against $G_1$:

$B$'s advantage:

By similar argument as that for \text{PRG+poly} construction,
\[
\text{PRG}_{\text{Adv}}[B, G] = \left\{ \frac{1}{2^{k-1}} \left[ \sum_{j=1}^{2^k-1} \Pr(Z_{w_0B} | w = j) \cdot \Pr(w = j) - \sum_{j=1}^{2^k-1} \Pr(Z_{w_1B} | w = j) \cdot \Pr(w = j) \right] \right\}
\]

(skipped in class:)

Also, in Exp 0 of B,

\[B \text{ identically simulates } H_{j-1} \text{ conditioned on } w = j.\]

In Exp 1 for B, it identically simulates \(H_j\), conditioned on \(w = j\).

Let \(P_j\) : Probability that \(A\) outputs 1 in \(H_j\).

Then,

\[
\text{PRG}_{\text{Adv}}[B, G] = \frac{1}{2^{k-1}} \left[ \sum_{j=1}^{2^k-1} P_j + P_{j+1} + \ldots + P_{2^k-2} \right] - \frac{1}{2^{k-1}} \left[ P_1 + \ldots + P_{2^k-1} \right] = \frac{1}{2^{k-1}} \text{PRF}_{\text{Adv}}(A, F).
\]
**Issue:** Recall, \( l = 1 \).

Even if \( \text{PRFAdv}(A, F) \) is non-negligible,

B's advantage is still negligible!

\( \Rightarrow \) B does NOT break G's security.

\( \Rightarrow \) This proves NOTHING about F's security... 😞
Note, $A$ is $O$-query bounded, where $O = \text{poly}(n)$.

If $B$ only needs to simulate PRGs in the paths of these $Q$ queries.

$\Rightarrow$ There will be max $Q$ such PRGs in each level.

$\Rightarrow$ Just need $2Q$ hybrids!!

Full proof in book (Sec. 4.6)

**Symmetric Crypto - Summary:**

- OWF $\rightarrow$ PRG$^1$
- PRG$^1$ $\rightarrow$ PRG + poly
- PRG + poly $\rightarrow$ PRF
- PRF $\rightarrow$ PRP/
- PRP/ Block Cipher

Deterministic Counter Mode

Switching Lemma

Next class

By definition: Truncate

Deterministic Lemma

PRF but a permutation