EECS 575: Advanced Cryptography
Fall 2021
Lecture 8

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- PRGs imply one-way functions
- Pseudorandom functions (PRFs)
- PRF from a length-doubling PRG

Agenda for this lecture

- Announcements
- Recap from last time
- PRGs imply one-way functions
- Pseudorandom functions (PRFs)
- PRF from a length-doubling PRG

Announcements

- Homework 3 is due 10/4.
  - Take-home exam 1 will be released that day!
- Lecture topic vote, final tally:
  1. Cryptocurrencies/Blockchains
  2. Lattice-based cryptography
  3. Fully-homomorphic encryption
  4. Advanced ZK (zkSNARKs)
  5. Verifiable computation

Topics for last two lectures!

Probably not fine

Agenda for this lecture

- Announcements
- Recap from last time
- PRGs imply one-way functions
- Pseudorandom functions (PRFs)
- PRF from a length-doubling PRG

Recap from last time

Pseudorandom generators:

PRG G with output length $\ell(n) \geq n+1$

"Stretches" input to output

- one-bit stretch implies many-bit
- OWP + HCP: if OWP w/ hcp h

  $\Rightarrow$ Blum-Micali $(f(x), h(x))$ is PRG w/ one-bit stretch

Discrete log owf:

$\rightarrow (g^x \bmod p, [x > \frac{p-1}{2}])$

Agenda for this lecture

- Announcements
- Recap from last time
- PRGs imply one-way functions
- Pseudorandom functions (PRFs)
- PRF from a length-doubling PRG

PRGs and OWFs

OWPs w/ hcp => PRGs

Does each OWP have HCP? Yes.

Do OWFs imply PRGs?
Take OWF F, use Blum-n.call:

(F(x), h(x))

IS this necessarily PRG if F OWF?
No, because F's output might be non-uniform

OWFs => PRGs

Hastad, Impagliazzo, Luby, Levin

HILL

Show PRGs => OWFs, so PRGs = OWFs

Goldreich 3.3.8 - PRGs imply OWFs

$|\Pr[D(G(U_n))=1] - \Pr[D(U_{2n})=1]|$ is

G PRG $\Rightarrow$ f OWF

f not OWF $\Rightarrow$ G not PRG

Let G be a PRG with $\ell(n) = 2n$

The function F def'd by letting

$$F(x,y) = G(x), \quad |x| = |y|$$

is a OWF.

Proof: By reduction. Suppose $\mathcal{I}$ for F. Build distng. D

$D(q \in \{0,1\}^{2n})$:

$B \leftarrow \mathcal{I}(q)$

If $F(B) = q$:

Return 1

Else Return 0

$\Pr[D(G(U_n))=1] = \Pr[\mathcal{I} \text{ wins}] > 1/p(n)$

$\Pr[D(U_{2n})=1] = \Pr[\mathcal{I} \text{ inverts } U_{2n}] \leq \frac{2^n}{2^{2n}} = \frac{1}{2^n}$

$|\Pr[D(G(U_n))=1] - \Pr[D(U_{2n})=1]| \geq \frac{1}{p(n)} - \frac{1}{2^n} \geq \frac{1}{2p(n)}$ ☒

Agenda for this lecture

- Announcements
- Recap from last time
- PRGs imply one-way functions
- Pseudorandom functions (PRFs)
- PRF from a length-doubling PRG

Pseudorandom Functions (PRFs)

PRG = "stretches" its output.

PRF = keyed function,
"looks like" random
functions if you
don't have the key.

PRGs hard to use in higher-level protocols: what's the key?

How many bits to write down $f: \{0,1\}^n \to \{0,1\}$? 2^n

Eg. $n=3$ 3-bits → 1 bit 10| ← single Function

How many functions? 2^{2^n} possible functions !!

Random function: sample from 2^{2^n} possibilities.

Pseudorandom Functions (PRFs)

Efficient adversaries can't look at the whole f'n

Oracle indistinguishability: (intuition: "random access mem." for primitives)

Let $\Theta = \{O_n\}$ and $\Theta' = \{O'_n\}$ be ensembles over functions from $\{0,1\}^{\ell_1(n)}$ to $\{0,1\}^{\ell_2(n)}$ for $\ell_1(n), \ell_2(n) = poly(n)$

Say that $\Theta \approx_c \Theta'$ if $\forall$ nupt D,

$$Adv^{dist}_{\Theta,\Theta'}(D) = \left| \Pr_{f \leftarrow O_n}[D^f(1^n) = 1] - \Pr_{f \leftarrow O'_n}[D^f(1^n) = 1] \right| = negl(n)$$

Like with PRGs, we say $\Theta = \{O_n\}$ is pseudo random if $\Theta \approx_c U(\{0,1\}^{\ell_1(n)} \to \{0,1\}^{\ell_2(n)})$

Pseudorandom Functions (PRFs)

PRF Family: A family $\{F_s : \{0,1\}^{\ell_1(n)} \to \{0,1\}^{\ell_2(n)}\}$ is a PRF family if:

- Efficient to eval: $\exists$ deterministic poly-time F s.t. $F(s,x) = F_s(x)$ for all inputs $s \in \{0,1\}^n$, $x \in \{0,1\}^{\ell_1(n)}$
- Pseudorandom:

$$\left| \Pr_{s \in \{0,1\}^n}[D^{F_s}(1^n) = 1] - \Pr_{\substack{\text{Unif } f \\ \ell_1(n) \text{ to } \ell_2(n)}}[D^{f}(1^n) = 1] \right| = \text{negl}(n)$$

$\forall$ nuppt D

Question: Let f be a PRF family. Is $g_s(x) = F_s(x) \| 0$ a PRF family?

Agenda for this lecture

- Announcements
- Recap from last time
- PRGs imply one-way functions
- Pseudorandom functions (PRFs)
- PRF from a length-doubling PRG

PRF from a length-doubling PRG

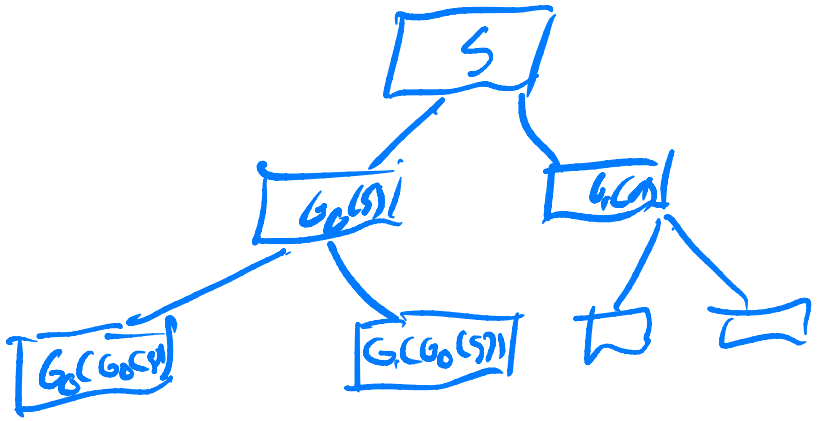
Do PRGs $\Rightarrow$ PRFs? Yes; [GGM]

Start with G, a length-doubling PRG

View G as a pair of length-preserving f'n's:

$$G(s) = G_0(s) \,||\, G_1(s)$$

Intuition: make a tree



PRF $F_S(x)$ = treat $x = x_1 x_2 \cdots x_n$, output

$G_{x_n}(\cdots G_{x_2}(G_{x_1}(s))\cdots)$