EECS 575: Advanced Cryptography
Fall 2022
Lecture 8

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Generators (PRGs)
- PRGs with polynomial stretch
- Building PRGs (overview)
- Pseudorandom functions

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Generators (PRGs)
- PRGs with polynomial stretch
- Building PRGs (overview)
- Pseudorandom functions

Announcements

- Homework 2 is due 9/30
  - I have OH after class in 4709
- Happy new year to those who celebrated!

- Cryptography club

  victorcrypto.org

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Generators (PRGs)
- PRGs with polynomial stretch
- Building PRGs (overview)
- Pseudorandom functions

Computational indistinguishability

- Relax statistical ind. to "bounded" computation

$$Adv_{X,Y}(A) = |Pr[A(X)=1] - Pr[A(Y)=1]|$$

- $X = \{X_n\}_{n\in\mathbb{N}}$ $Y = \{Y_n\}_{n\in\mathbb{N}}$ $X \approx_c Y$

$\forall$ n.u.PPT A,

$$Adv_{X,Y}(A) = negl(n)$$

- $X \approx_c \{U_n\}_{n\in\mathbb{N}}$, X is pseudorandom

Composition Lemma

$x \approx_c y$, $\forall$ nuPPT B, $B(x) \approx_c B(y)$

sunglasses

"sunglasses lemma"

Hybrid Lemma

$X^i = \{X^i_n\}$ for $i \in [m]$ $(m = poly(n))$

IF $X^i \approx_c X^{i+1}$, then $X^1 \approx_c X^m$

$(\forall i \in [m-1])$

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Generators (PRGs)
- PRGs with polynomial stretch
- Building PRGs (overview)
- Pseudorandom functions

Pseudorandom Generators (PRGs)

$G : \{0,1\}^* \to \{0,1\}^*$ is PRG with output $\ell(n) > n$

If

- G efficiently computable
- $|G(x)| > |x|$ for all x
- $G(U_n) \approx_c U_{\ell(n)}$

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Generators (PRGs)
- PRGs with polynomial stretch
- Building PRGs (overview)
- Pseudorandom functions

Expanding a PRG

Theorem: If $\exists$ PRG G where $\ell(n) = n+1$,

then $\exists$ PRG $G_t : \{0,1\}^n \to \{0,1\}^{\ell(n)}$

for any $t(n) = \text{poly}(n)$

$G_t(s)$:

If $t = 0$:
  Return s
Else
  $(x \mid b) \leftarrow G(s)$
  Ret $b \mid G_{t-1}(x)$

1. Construct G_t ✓
2. Prove G_t a PRG
   - efficient, output $t(n)$ $\to$
   - pseudorandom

$$\{G_t(U_n)\} \approx_c \{U_{t(n)}\}$$

Expanding a PRG

Thm: $\{G_t(U_n)\} \approx_c \{U_{t(n)}\}$

Proof: Hybrid Lemma

H_0: $\{G_t(U_n)\}$

H_1: $U_1 \mid G_{t-1}(U_n)$

H_i: $U_{i+1} \mid G_{t-i-1}(U_n)$

H_{i+1}: $U_i \mid G_{t-i}(U_n)$

H_t: U_t

Need to show $H_i \approx_c H_{i+1}$ $\forall c$

S_i: $(y \in \{0,1\}^{n+1})$:

$x \mid b \leftarrow y$

Ret $U_{i-1} \mid b \mid G_{t-i}(x)$

Claim: if $y \leftarrow G(s)$, then $S_i = H_i$

if $y \leftarrow U_{n+1}$, then $S_i = H_{i+1}$

$G_t(s)$:

If $t = 0$:
  Return ε
Else
  $(x \mid b) \leftarrow G(s)$
  Ret $b \mid G_{t-1}(x)$

Composition lemma:

$S_i(G(s)) \approx_c S_i(U_{n+1})$ ☒

So $H_i \approx_c H_{i+1}$

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Generators (PRGs)
- PRGs with polynomial stretch
- Building PRGs (overview)
- Pseudorandom functions

How do we build PRGs?

From OWFs. But non-trivial.

- Hardcore predicate of OWP
  - Blum-Micali
  - Discrete log
- Goldreich-Levin
- OWF ⟺ HILL

Exercise: If G PRG, then G OWF

(Hint: use reduction)

Agenda for this lecture

- Announcements
- Recap from last time
- Pseudorandom Generators (PRGs)
- PRGs with polynomial stretch
- Building PRGs (overview)
- Pseudorandom functions

Pseudorandom functions

PRG → random-looking bits

PRF ⇒ random-looking Function

Need oracle indistinguishability

Let $\Theta = \{O_n\}$, $\Theta' = \{O'_n\}$ ensembles

over functions $\{0,1\}^{\ell_1(n)} \to \{0,1\}^{\ell_2(n)}$

$\Theta \approx_c \Theta'$ if $\forall$ nupt A $\qquad \ell_1, \ell_2 = poly(n)$

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

Pseudorandom functions

Say G pseudorandom if

$$G \approx_c \{U(\{0,1\}^{\ell_1(n)} \to \{0,1\}^{\ell_2(n)})\}$$

PRF family: $F = \{f_s : \{0,1\}^{\ell_1} \to \{0,1\}^{\ell_2}\}_{s \in \{0,1\}^n}$

is a PRF family if

- Efficient to sample s
- Efficient to evaluate $F_s(x)$
- $\{U(F)\}$ pseudorandom

($U(F)$ = random s, f_s)

Pseudorandom functions

Exercise: Let F_s be a PRF family.

Is $g_s(x) = F_s(x) \| 0$ a PRF family?

How to construct PRFs?

- From PRGs!