CSE 575: Advanced Cryptography
Fall 2024
Lecture 6

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Computational indistinguishability
- Composition lemma, hybrid lemma
- Pseudorandom generators (PRGs)
- PRGs with arbitrary stretch

Agenda for this lecture

- Announcements
- Computational indistinguishability
- Composition lemma, hybrid lemma
- Pseudorandom generators (PRGs)
- PRGs with arbitrary stretch

Announcements

- HW2 online, due 9/26

Agenda for this lecture

- Announcements
- Computational indistinguishability
- Composition lemma, hybrid lemma
- Pseudorandom generators (PRGs)
- PRGs with arbitrary stretch

Computational indistinguishability

Statistical distance

$$\Delta(X,Y) = \sup_{A \in \Omega} |X(A) - Y(A)|$$ "max"

$$= \frac{1}{2} \sum_{E \in \Omega} |P_{D_X}[E] - P_{D_Y}[E]|$$

SD is a metric:

- reflexive
  $\Delta(X,X) = 0$
- symmetric
  $\Delta(Y,X) = \Delta(X,Y)$
- $\Delta(X,Z) \leq \Delta(X,Y) + \Delta(Y,Z)$?

X Y are stat. ind. if:

$\forall n$ $\Delta(X_n, Y_n) = negl(n)$

Statistical ind.

Let $x = \{X_n\}_{n \in \mathbb{N}}$ and $y = \{Y_n\}$ be dist. ensembles

Computational indistinguishability

E.g. $X_n = U_n$, $Y_n = U_n \setminus \{0^n\}$

$A = \{0^n\}$

$A(X_n, Y_n) = 2^{-n} = \text{negl}(n)$.

Computational indistinguishability

Dists X, Y, A

$$Adv_{X,Y}(A) = \left| Pr_X[A(X)=1] - Pr_Y[A(Y)=1] \right|$$

For x, y, $x \approx_c y$ if $\forall$ nuPPT A,

$$Adv_{x_n, y_n}(A) = negl(n).$$

Pseudorandom: x is PR if

$x \approx_c U$

[where $U = \{U_n\}_{n \in \mathbb{N}}$]

Agenda for this lecture

- Announcements
- Computational indistinguishability
- Composition lemma, hybrid lemma
- Pseudorandom generators (PRGs)
- PRGs with arbitrary stretch

Composition lemma

Let X, Y be $\approx_c$. Let S be n.PPT.

Then $S(X) \approx_c S(Y)$.

Proof:

$\exists A, p$ s.t. $Adv_{S(X),S(Y)}(A) \geq \frac{1}{p(n)}$

$B^A(y)$:

$t \leftarrow S(y)$

Ret $A(t)$

$Pr_x[B^A = 1] = Pr_{S(x)}[A = 1]$

$Pr_y[B^A = 1] = Pr_{S(y)}[A = 1]$

$\Rightarrow Adv_{X,Y}(B) \geq \frac{1}{p(n)}$ ☒

Hybrid lemma

Fischlin Paper on Piazza

Let x^i for $i = 1$ to m be dist. ens. where m is constant + indep. of n.

If $x^{i-1} \approx_c x^i$, then $x^0 \approx_c x^m$.

Proof:

Let $p_i = \Pr[D(x^i) = 1]$. Then

$$Adv_{x^0, x^m}(D) = |p_0 - p_m| \leq \sum_i |p_{i-1} - p_i|$$

$$= \sum_i Adv_{x^{i-1}, x^i}(D)$$

Need that sum of const. # negl's is also negl.

$\nu_i(n)$?

$\nu(n) = \sum \nu_i(n)$. Need $\forall c > 0$ $\exists n_0$ s.t. $\nu(n) \leq n^{-c}$ for all $n \geq n_0$.

Have n_i for each i. $\nu_i(n) \leq n^{-c}/m$ $\forall n \geq n_i$

Let $n_0 = \max n_i$ ∎

Agenda for this lecture

- Announcements
- Computational indistinguishability
- Composition lemma, hybrid lemma
- Pseudorandom generators (PRGs)
- PRGs with arbitrary stretch

Pseudorandom generators (PRGs)

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

- Easy to compute
- $|G(x)| = \ell(|x|) > |x| \quad \forall x$
- Ensemble $\{G(U_n)\}$ is Pseudorandom:

$$\{G(U_n)\} \approx_c \{U_{\ell(n)}\}$$

If $G(x)$ PRG, is $H(x) = \overline{G(x)}$ PRG?

Yes. Use composition lemma.

Agenda for this lecture

- Announcements
- Computational indistinguishability
- Composition lemma, hybrid lemma
- Pseudorandom generators (PRGs)
- PRGs with arbitrary stretch

PRGs with arbitrary stretch

Thm: If $\exists$ PRG with $\ell(n) = n+1$, then $\exists$ PRGs with stretch $poly(n)$ $\forall$ polys.

Proof:

$G_t(s)$:

If $t=0$
  Ret ε

else
  $x \| b = G(s)$
  Ret $b \| G_{t-1}(x)$

(can fix $t=0$ with different base case)

Hybrid argument

$H_0 = G_t(U_n)$

$H_1 = U_1 \| G_{t-1}(U_n)$

$\vdots$

$H_i = U_i \| G_{t-i}(U_n)$

$H_t = U_t$