Lecture 3

EECS 575

- Announcements
- Computational security
- One-way function
- OWF candidates, reductions

Announcement

- HW1 due Fri., Sep 16
- HW2 released Sep 16

Computational Security

- Security against "bounded" attacks
- Bounded computational power can't break

Model of computation

- Turing machines
- Running time
  - "basic" operations: adds, multiplies, loads, stores

$T(n) = O(n^c)$

input size ↑ polynomial (asymptotically)

"poly-time"

- randomized: has a random tape $r \leftarrow \{0,1\}^*$

$A(x; r)$ PPT

Model, cont'd.

- Non-uniformity

  "advice" about problem

Formally, A non-uniform if

$\exists\ w_1, w_2, \ldots w_k, \ldots$

$A(x)$ receives $w_{|x|}$ advice

$|w_{|x|}| = O(n^c)$

$P/poly$

nuPPT

Negligible functions

Non-negative func $f(n) > 0$

$f(n)$ is negl(n) if

$f(n) = o(n^{-c})$ for all c

Question

Is product of negl and non-negl:

(a) always non-negl

(b) always negl

(c) neither

$f(n) = e^{-n}$

$g(n) = e^{n}$

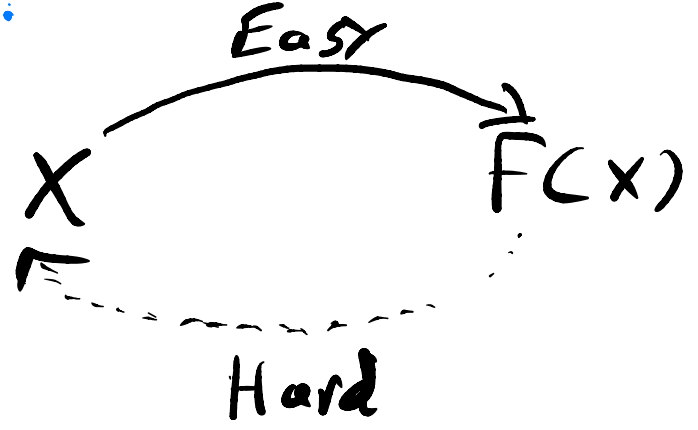
$h(n) = n$

$f(n)g(n) = 1$

$f(n)h(n) = e^{-n} \cdot n$

One-way functions

Intuition:



F(n)

$f(n): \{0,1\}^* \to \{0,1\}^*$ is OWF if

1. Easy to compute:

   $\exists F$ deterministic, poly-time TM

   s.t. $F(x) = f(x) \quad \forall x$

2. Hard to invert $\forall$ nuppt I,

$$Adv_f(I) := Pr\left[I(1^n, F(x)) \in F^{-1}(f(x)) \right]$$

$F: \{0,1\}^n \to \{0,1\}^n$ $\quad x \leftarrow \{0,1\}^n$ $\quad 1^n$ = input length

$= negl(n)$

$= 0$ Just guess!

Let $f(x)$ be OWF. Is $g(x) = f(x)||0$ also OWF?

Yes! By reduction:

If break $g(x)$, can break $f(x)$

$f(x)$ OWF $\Rightarrow$ $g(x)$ OWF

$\neg g(x)$ OWF $\Rightarrow$ $\neg f(x)$ OWF

Imagine we have $\mathcal{I}_g$, $Adv_g(\mathcal{I}_g) = \text{poly}(n)$

Build $\mathcal{I}_f$ from $\mathcal{I}_g$

$\mathcal{I}_f(1^n, y)$:

$y' = y \| 0$

$x \leftarrow \mathcal{I}_g(1^{n+1}, y')$

Ret x

advice string?

Claim:

$\mathcal{I}_f$ inverts F w/ non-negl prob.

Post on Piazza

OWF candidates

$$f_{ss} : (\mathbb{Z}_N)^n \times \{0,1\}^n \to (\mathbb{Z}_N)^n \times \mathbb{Z}_N$$

$$f_{ss}(a_1, \ldots, a_n, b_1, \ldots, b_n)$$

$$:= (a_1, \ldots, a_n), \sum b_i a_i \bmod N$$

$$= (a_1, \ldots, a_n), \sum_{\substack{i \text{ s.t.} \\ b_i = 1}} a_i \bmod N$$

$$f_{ss}((0, \ldots 0, x), (\ldots, 1)) = x^y$$

multiplication:

$$F_{mult} : \mathbb{N}^2 \to \mathbb{N}$$

$$f_{mult}(x, y) = \begin{cases} 1 & \text{if } x = 1 \vee y = 1 \\ xy \end{cases}$$

Are f_{ss} and f_{mult} OWFs?