EECS 575: Advanced Cryptography
Fall 2022
Lecture 3

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- One-way functions (OWFs)
- Proof by reduction for f’(x) = (f(x), f(f(x)))
- More on OWFs from factoring

Agenda for this lecture

- Announcements
- One-way functions (OWFs)
- Proof by reduction for f’(x) = (f(x), f(f(x)))
- More on OWFs from factoring

Announcements

- Homework 1 due 9/16
  - I have OH after class, Alexandra has OH Friday
- Homework 2 will be released 9/16

BBB 3901

Agenda for this lecture

- Announcements
- One-way functions (OWFs)
- Proof by reduction for f’(x) = (f(x), f(f(x)))
- More on OWFs from factoring

Recap from last time

One-Way Functions

$F: \{0,1\}^* \to \{0,1\}^*$ is OWF if

- Easy to compute

  $\exists F$ det. poly-time s.t.

  $\forall x,\ F(x) = f(x)$

- Hard to invert:

  $\forall$ nuPPT $\mathcal{I}$,

  $$\Pr_{x \leftarrow \$ \{0,1\}^n}\left[\mathcal{I}(1^n, f(x)) \in F^{-1}(f(x))\right] = \text{negl}(n)$$

Weak OWFs

f is "weak" OWF if:

- Easy to compute
- Hard to invert:

$$\exists \delta(n) = 1/\mathrm{poly}(n), \forall \mathcal{I}$$

$$\Pr_{x \leftarrow \{0,1\}^n}\left[\mathcal{I}(1^n, f(x)) \in f^{-1}(f(x))\right] \leq 1-\delta$$

Q: Does quantifier order matter?

Hardness Amplification for OWFs

Thm: If $\exists$ weak OWF, $\exists$ strong OWF

If f δ-weak OWF,

$$f'(x_1, \ldots, x_m) := (f(x_1), \ldots, f(x_m))$$

is strong OWF for $m \geq 2n/\delta(n)$

Proof:

Exercise !! ☺

Goldreich

Agenda for this lecture

- Announcements
- One-way functions (OWFs)
- Proof by reduction for f’(x) = (f(x), f(f(x)))
- More on OWFs from factoring

Proofs by reduction

Thm: If f is a OWF, then

$$F'(x) = (F(x), F(f(x)))$$

is a OWF.

Proof: By reduction/contrapositive

$I(1^n, y = f(x))$:

$y' \leftarrow f(y)$

$x \leftarrow I'(1^n, (y, y'))$

Ret x

E.g. $F'(x) = F(\bar{x})$?

Let I' be an inverter for f' s.t.

$\Pr_x[I'(1^n, f(x)) \in f'^{-1}(f'(x))] \geq 1/p(n)$

Need to show $\exists I$ s.t.

$\Pr_x[I(1^n, f(x)) \in f^{-1}(f(x))] \geq 1/p'(n)$

$\Pr[I \text{ inverts}] \geq \Pr[I' \text{ inverts}]$

$\geq 1/p(n)$ ☒

Take-Home Exercise

If f is a OWF, must $f'(x_1, x_2) = (f(x_1), f(x_2))$ also be a OWF?

Agenda for this lecture

- Announcements
- One-way functions (OWFs)
- Proof by reduction for f’(x) = (f(x), f(f(x)))
- More on OWFs from factoring

A Candidate One-Way Function

Multiplication

$$F_{mult}(x,y) = \begin{cases} 1 & \text{if } x=1 \vee y=1 \\ x \cdot y & \text{o/w} \end{cases}$$

Inverting f_{mult} is factoring.

For $x, y \leftarrow [1, 2^n]$, is $f_{mult}(x,y)$ OWF?

What if $x \cdot y$ is even?

Ret $(2, x \cdot y/2)$

$$P_1 := \Pr\left[I(1^n, F_{mult}(X,Y)) \in \{X,Y\} \right]$$

$X, Y \in \Pi_\eta$

$$\Pi_\eta = \{ x : x \in [1, 2^n] \wedge x \text{ is prime} \}$$

Factoring assumption:

$P_1 = \text{negl}(n)$ $\forall$ nuppt I

equivalently, F_{mult} is OWF

Concrete complexity of factoring?

$\approx e^{\sqrt[3]{n}}$ for Number Field Sieve

How to sample from Π_n?

GenPrime(n):

$a \leftarrow [1, 2^n]$ (1)

If a prime, ret a

Else goto (1)

Efficient primality test

2002: det. poly-time test

AKS

In practice?

Miller-Rabin (randomized)

Fake-positive prob.

For integer $N > 1$

$\pi(N) \geq \frac{N}{2 \log_2 N}$ Chebyshev

$\pi(n) \sim \frac{N}{\ln N}$ Density of primes

$$\frac{|\Pi_n|}{2^n} = \frac{\pi(2^n)}{2^n} \geq \frac{2^{n}}{2^n \cdot 2 \log_2 2^n} = \frac{1}{2n}$$

n: bit length

Fixing f_{mult}

Sampling Random Primes