CSE 575: Advanced Cryptography
Fall 2024
Lecture 3

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Computational model
- One-way functions
- Number theory background

Agenda for this lecture

- Announcements
- Computational model
- One-way functions
- Number theory background

Announcements

- Hired IA – Luke Miga
- HW1 is online, due Monday 9/9

Dow 1018

News


nist.gov/news-events/news/2024/08/ni...
Relaunch to update
An official website of the United States government
Here's how you know
NIST
Search NIST
Men
NEWS
NIST Releases First 3 Finalized Post-Quantum Encryption Standards

Agenda for this lecture

- Announcements
- Computational model
- One-way functions
- Number theory background

Model of Computation: Algorithms

- Running time
  all "primitive" ops constant
- Randomness
  - read-only random tape
- non-uniformity
  "advice" about problem

Model of Computation: Asymptotics

Polynomial := $T(n)$ is poly if $\exists c$ s.t.

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

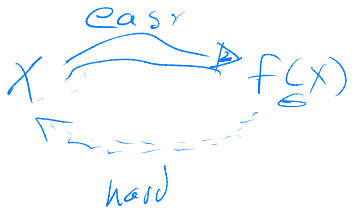
negligible $\gamma(n)$ if $\forall$ constants $c > 0$

$$\gamma(n) = o(n^{-c})$$

n is security parameter

Agenda for this lecture

- Announcements
- Computational model
- One-way functions
- Number theory background



One-Way Functions

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

- Easy to compute
  $\exists$ uniform deterministic p-time F
  s.t. $F(x) = f(x)$ $\forall x$
- Hard to invert $\forall$ nuPPT $\mathcal{I}$,

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

- 1^n input
- win by outputting any preimage
- easy to sample domain
  easy to recognize "wins"
- Average-case

$f: D \to R$

$w(n)$

Question about OWFs

Let $f(x)$ be OWF. Is

$g(x) := f(x) \| 0$ OWF?

Proof by reduction

A candidate OWF

$$f_{mult} : [1, 2^n] \times [1, 2^n] \longrightarrow [1, 2^{2n}]$$

$$f_{mult}(x,y) := \begin{cases} 1 & \text{if } x = 1 \text{ or } y = 1 \\ x \cdot y & \text{otherwise} \end{cases}$$

Looks like factoring!

Is f_{mult} OWF? No!

Can output $(N/2, 2)$

A candidate OWF

Let $\Pi_n = \{p \mid p \in [1, 2^n] \text{ and } p \text{ prime}\}$

Factoring Assumption: $\forall$ nuPPT $\mathcal{A}$

$$\Pr_{p,q \leftarrow \Pi_n}[\mathcal{A}(p \cdot q) = (p, q)] = \text{negl}(n)$$

Define $f'_{mult} : \Pi_n \times \Pi_n \longrightarrow [1, 2^{2n}]$

Thm: If FA holds, f'_{mult} is OWF

Proof: Exercise.

Fixing our candidate OWF

Can we sample random primes efficiently?

Yes!

Sample random integer, check if prime.

If yes, done

If no, GOTO 1

$\pi(N)$ = # primes $< N$

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

Agenda for this lecture

- Announcements
- Computational model
- One-way functions
- Number theory background

Number Theory

Euclid's algorithm

Algorithm 1 Algorithm ExtendedEuclid(a, b) for computing the greatest common divisor of a and b.

Input: Positive integers $a \geq b > 0$.

Output: $(x, y) \in \mathbb{Z}^2$ such that $ax + by = \gcd(a, b)$.

1: **if** $b \mid a$ **then**
2: **return** $(0, 1)$
3: **else**
4: Let $a = b \cdot q + r$ for $r \in \{1, \ldots, b-1\}$
5: $(x', y') \leftarrow$ ExtendedEuclid(b, r)
6: **return** $(y', x' - q \cdot y')$
7: **end if**

Chinese Remainder Theorem

Announcements

- Homework/exam schedule is (tentatively) done:
  - HW1: put online 9/5, due 9/16
    HW2: put online 9/16, due 9/30
    Take-home exam #1: put online 10/3, due 10/10
    HW3: put online 10/7, due 10/21
    HW4: put online 10/21, due 11/4
    HW5: put online 11/4, due 11/18
    HW6: put online 11/16, due 11/28*
    Take-home exam #2: put online 11/28, due 12/5