EECS 575: Advanced Cryptography
Fall 2021
Lecture 4

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Collections of one-way functions
- Number theory background
- The Rabin collection

Agenda for this lecture

- Announcements
- Collections of one-way functions
- Number theory background
- The Rabin collection

Announcements

- Homework 2 is due ~~9/22~~ 9/20
- I will have office hours on Zoom from noon-1pm today
- Lecture topic vote

Agenda for this lecture

- Announcements
- Collections of one-way functions
- Number theory background
- The Rabin collection

Recap from last time

- One-way functions
  Easy to compute, hard to invert
- Definition of OWFs, proof by reduction

Collections of One-Way Functions

Why do we need our collections?

Previous def'n

A function $F: \{0,1\}^n \to \{0,1\}^n$ is one-way if ....

Collections of One-Way Functions

A collection of OWFs is a family $F = \{f_s \mid D_s \to R_s\}_{s \in \mathcal{S}}$ satisfying:

- Easy to sample a function: $\exists$ ppt alg. $\mathbf{S}$ such that $\mathbf{S}()$ outputs $s \in \mathcal{S}$ (set of all possible parameters) → defines a f'n
- Easy to sample from the domain: $\exists$ ppt alg D s.t. $D(s)$ outputs $x \in D_s$ according to some dist

Collections of One-Way Functions

- Easy to evaluate f'n:
  $\exists$ deterministic poly-time F s.t.
  $F(s, x) = f_s(x)$ for all $s \in \mathcal{S}$, $x \in D_s$
- Hard to invert: $\forall$ nupat $\mathcal{I}$,

$$\Pr_{\substack{s \leftarrow \mathcal{S}(\lambda) \\ x \leftarrow D(s)}}\left[\mathcal{I}(s, f_s(x)) \in f_s^{-1}(f_s(x))\right] = \mathrm{negl}(\lambda)$$

Agenda for this lecture

- Announcements
- Collections of one-way functions
- Number theory background
- The Rabin collection

Number Theory Background

Greatest common divisor

gcd(a,b) is the largest integer that divides both, i.e. gcd(a,b) = d if d|a and d|b

Example

gcd(6,10) = 2

gcd(6,11) = 1

Alternatively, gcd(a,b) = 1 $\Rightarrow \exists x$ s.t. $ax \equiv 1 \bmod b$

Extended Euclidean Algorithm

Bézout coefficients: x, y s.t. $ax + by = \gcd(a,b)$

EEA(a,b):

Input a, b: $a \geq b > 0$

Output: Bézout coeffs for a, b

If $b \mid a$ then

  Return $(0, 1)$

else

  Let $a = b \cdot q + r$, $r \in \{1, \ldots, b-1\}$

  $(x', y') \leftarrow EEA(b, r)$ ← mod-swap

  Return $(y', x' - q \cdot y')$

Thm: $\forall a, b \; \exists x, y$ s.t.

$ax + by = \gcd(a,b)$

$\gcd(b, r) = bx' + ry'$

$= bx' + (a - bq)y'$

$= ay' + (x' - qy')b$

$a = bq + r$

$\gcd(a,b) = \gcd(b,r)$

$r = a - bq$

$r = \delta m - \delta n q$

$r = \delta(m - nq)$

Extended Euclidean Algorithm

Thm (informal): EEA is efficient

If $2^n \geq a > b \geq 0$, EEA makes at most $2n$ recursive calls

Proof: see notes

Chinese Remainder Theorem

Ring of integers mod $N = pq$

Algebraic object where you have $(+, \cdot)$

$\mathbb{Z}_N = \{0, \ldots, N-1\}$ $(+, \cdot)$ are integer add/mult mod N

$\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$ (CRT)

View members of LHS as pair of members of $\mathbb{Z}_p$ and $\mathbb{Z}_q$

In $\mathbb{Z}_p \times \mathbb{Z}_q$, add/mult component-wise

Chinese Remainder Theorem

CRT isomorphism can be computed in both directions

$h : \mathbb{Z}_N \to \mathbb{Z}_p \times \mathbb{Z}_q$

$h(x) = (x \bmod p, x \bmod q)$

$h^{-1}(x,y) : \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_N$

Given elts c_p, c_q. $[h(c_p) = (1,0)$, $h(c_q) = (0,1)]$

write

$h^{-1}(x,y) = x c_p + y c_q \bmod N$

CRT basis elements allows to compute c_p, c_q

Run EEA(p,q)

x, y Bezout

$px + qy = 1$

$c_q \quad c_p$

Chinese Remainder Theorem

CRT is additive / multiplicative.

E.g. $h(7 \cdot 9) = h(7) \cdot h(9) \rightarrow (9 \bmod 3, 9 \bmod 5)$

$\mathbb{Z}_{15}$

$(7 \bmod 3, 7 \bmod 5)$

$(1, 2) \cdot (0, 4)$

$(0, 3)$

$h(7 \cdot 9) = h(63)$

$= (63 \bmod 3, 63 \bmod 5)$

$(0, 3)$

Chinese Remainder Theorem

Multiplicative group $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N \mid gcd(x, N) = 1\}$

What is $|\mathbb{Z}_N^*|$? $\varphi(N)$ # integers $\leq N$ with $gcd(x, N) = 1$

Prime $N = p$ $\varphi(N) = p - 1$

$N = pq$ we have $\varphi(N) = \varphi(p) \cdot \varphi(q)$

$= (p-1)(q-1)$

Finally $\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$

Agenda for this lecture

- Announcements
- Collections of one-way functions
- Number theory background
- The Rabin collection

Rabin's Function

Background: Quadratic residues

$$QR_N^* = \{ y \in \mathbb{Z}_N^* : \exists x \in \mathbb{Z}_N^* \text{ s.t. } y = x^2 \bmod N \}$$

$\forall x \in \mathbb{Z}_p^*$, $x^2 = (-x)^2$

For prime $N = p$, $|QR_p^*| = \frac{p-1}{2}$

For $N = pq$, $QR_N^* \cong QR_p^* \times QR_q^*$

$$\Rightarrow |QR_N^*| = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Rabin's Function

$f_N : \mathbb{Z}_N^* \to QR_N^*$, is $f_N(x) = x^2 \bmod N$

Thm: Let S be sampling a/g. for param. N of Rabin collection. If factoring S's outputs is hard, then Rabin is OWF collection

Proof: Next time