EECS 575: Advanced Cryptography
Fall 2022
Lecture 5

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 out, due 9/30
- Late policy:
  - 5% off per late day
  - Max one week late
  - Point penalty can be waived *with cause*

Agenda for this lecture

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

Recap from last time

One-way functions: f is OWF if

- Easy to compute
- Hard to invert

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

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

- Proofs by reduction

  If $\langle X \rangle$ secure, then $\langle Y \rangle$ secure

  If $\langle Y \rangle$ not secure, then $\langle X \rangle$ not secure

Collections of One-Way Functions

OWFs lack keys/params.

Real crypto has keys/params!

Motivates OWF collections

Collections of One-Way Functions

Family $F = \{F_s : D_s \to R_s\}_{s \in \{0,1\}^*}$

- Easy to sample a f'n:
  $\exists$ ppT $\$$ s.t. $s \leftarrow \$(1^n)$
- Easy to sample from domain
  $\exists$ ppT Samp s.t. $x \leftarrow Samp(s)$ ← Hard to sample
- Easy to compute (hold $\forall s$)
- Hard to invert: $\forall$ nuppt $\mathcal{I}$,

$$\Pr_{s \leftarrow \$(),\, x \leftarrow Samp(s)}\left[\mathcal{I}(s, F_s(x)) \in F_s^{-1}(F_s(x))\right] \leq negl(n)$$

↳ negl frac could be easy!

Agenda for this lecture

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

Number Theory Background

"$d \in \mathbb{Z}$ divides $b \in \mathbb{Z}$ $d|b$, if

$\exists q \in \mathbb{Z}$ s.t. $b = dq$

For $a, b \in \mathbb{Z}$, $\exists$ "greatest common divisor"

$d = \gcd(a,b)$ s.t.

$d|a$ and $d|b$

and no $e > d$ divides both.

If $d = 1$, say a, b are coprime.

For $a, b \in \mathbb{Z}$, $\exists x, y \in \mathbb{Z}$ s.t.

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

(Bézout)

Extended Euclidean Algorithm

EEA(a, b): (output x, y) ←

IF b | a:
  Return (0, 1) ⟶ $a \cdot 0 + b \cdot 1 = b$

Else
  write $a = q \cdot b + r$ [$\in \{0, \ldots, b-1\}$]
  $(x', y') \leftarrow$ EEA(b, r)
  Ret $(y', x' - q \cdot y')$

$$17 \overline{)253} \quad 20 + \frac{9}{17}$$

$$\frac{9}{17}$$

Extended Euclidean Algorithm

```
EEA(a, b):
IF b|a:
    Return (0, 1)
Else
    write a = q·b + r  [∈ {0, ..., b-1}]
    (x', y') ← EEA(b, r)
    Ret (y', x' - q·y')
```

Claim: EEA is correct and runs in poly(log a + log b)

Proof: Exercise / notes

Claim:

EEA makes at most $2n$ recursive calls for n-bit a, b

Proof: Exercise

Chinese Remainder Theorem

Ring $\mathbb{Z}_N$ → Integers mod N

$N = p \cdot q$ (product of two primes)

$\mathbb{Z}_p$, $\mathbb{Z}_q$. $\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$

"Isomorphic"

Bijection that "respects" add/mult

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

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

$h(a \cdot b) = h(a) \cdot h(b)$

$h(a+b) = h(a) + h(b)$

Chinese Remainder Theorem

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

c_p, c_q a CRT "basis":

$h(c_p) = (1, 0) \in \mathbb{Z}_p \times \mathbb{Z}_q$

$h(c_q) = (0, 1) \in \mathbb{Z}_p \times \mathbb{Z}_q$

$h^{-1}(x, y) = x c_p + y c_q \in \mathbb{Z}_N$

Holds for polynomials!

Chinese Remainder Theorem

How to compute CRT basis?

Exercise! EEA(p, q)

EEA lets us compute

$ax + by = gcd(a, b)$ ⇒ Compute $a^{-1} \bmod b$

If a, b coprime

$ax + by = 1$ ← hold over $\mathbb{Z}$

$a^{-1} \bmod b$ ⇒ $ax = 1 \bmod b$

$ax = 1 + \lambda b$ $\quad ax - 1 = \lambda b$

$ax - \lambda b = 1$

Chinese Remainder Theorem

Euler's Totient Function $\varphi(N)$

$= |\{x \in \mathbb{Z} \mid x < N, \gcd(x,N) = 1\}|$

$\varphi(p) = p-1$

$\varphi(p^a) = (p-1)p^{a-1}$

$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ if $\gcd(a,b) = 1$

$\mathbb{Z}_N^*$: elts $\mathbb{Z}_N$ with mult inverse

$a^{-1} \bmod N$ $\quad ax + by = 1$

$|\mathbb{Z}_N^*| = \varphi(N) = (p-1)(q-1)$

Chinese Remainder Theorem

$\mathbb{Z}_N^*$ Subgroup of "quadratic residues"

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

$\mathbb{Z}_p^*$, $|QR_p^*| = \frac{p-1}{2}$

$y \in QR_p^* \quad \exists x \text{ s.t. } x^2 = y \bmod p$

$(-x)^2 = y \bmod p$

$$|QR_N^*| = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \frac{|\mathbb{Z}_N^*|}{4}$$

$x \to x^2 \bmod N$

is 4-to-1

Agenda for this lecture

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

Rabin's Function