CSE 575: Advanced Cryptography
Fall 2024
Lecture 4

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- OWF collections
- Number theory background
- Rabin’s OWF collection
- Proving one-wayness of Rabin

Agenda for this lecture

- Announcements
- OWF collections
- Number theory background
- Rabin's OWF collection
- Proving one-wayness of Rabin

Announcements

- Say hello to Luke!
- HW1 now due Wednesday, 9/11

Agenda for this lecture

- Announcements
- OWF collections
- Number theory background
- Rabin's OWF collection
- Proving one-wayness of Rabin

OWF Collections

$$F = \{ f_s : D_s \to R_s \}_{s \in \$}$$

- Easy to sample f'n
  $\exists$ PPT S sampler from $\$$
- Easy to sample domain:
  $\exists$ PPT $D(s)$, outputs $x \in D_s$
- Easy to evaluate
  $\forall s$, same property as OWF holds
- Hard to invert: $\forall$ nuPPT $\mathcal{I}$:

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

Agenda for this lecture

- Announcements
- OWF collections
- Number theory background
- Rabin's OWF collection
- Proving one-wayness of Rabin

Number Theory

- Greatest Common Divisor (GCD)

  $a, b \in \mathbb{Z}$ $\quad gcd(a,b) = d$

  largest int s.t. $d|a$ and $d|b$

- $\forall a, b \in \mathbb{Z} \quad \exists x, y \in \mathbb{Z}$ s.t. $ax + by = gcd(a,b)$

  Bezout

- a, b coprime if $gcd(a,b) = 1$

  $ax + by = 1$

  $ax \equiv 1 \mod b$

Euclid's algorithm

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

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**

$a \cdot 0 + b \cdot 1 = \gcd(a, b) = b$

Integer long division is efficient

Piazza

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

1. Correct: always returns BCs.

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

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

$= bx' + ay' - bqy' = ay' + b(x' - qy')$ ☒

Chinese Remainder Theorem

Let $N = pq$

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

arithmetic is component-wise
$(a,b) + (x,y) = (a+x, b+y)$
likewise for mult

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

$$h^{-1}(x,y) = c_p x + c_q y$$ where c_p, c_q are CRT coefficients

$$h(c_p x + c_q y) = h(c_p) \cdot h(x) + h(c_q) \cdot h(y)$$

$h(c_p) = (1,0)$

$h(c_q) = (0,1)$

$(1,0) \cdot (x \bmod p,\ \cancel{x \bmod q})$

$(x \bmod p,\ 0)$

$+ (0,\ y \bmod q)$

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

Chinese Remainder Theorem

$N = pq$

How to compute CRT coeffs?

Compute BCs of p, q : x, y

$px_1 + qy_1 = 1$

$c_p = 1 - px = qy$

$c_q = 1 - qy = px$

$h^{-1}(a, b) = c_p a + c_q b$

$(1-px)a + (1-qy)b$

$= qya + pxb$

$h(qya + pxb) = (qya + pxb \bmod p,\ qya + pxb \bmod q)$

$(1-px)a = a$

$h(c_p a + c_q b)$

$= (a, b)$

The multiplicative group $\mathbb{Z}_N^*$

$N = pq$

Totient Function $\varphi(N) = |\{x < N : \gcd(x, N) = 1\}|$

$\varphi(p) = p - 1$

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

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

Group $\mathbb{Z}_N^* = \{x \in \{1, \ldots, N-1\} \mid \gcd(x, N) = 1\}$

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

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

$= N - p - q + 1$

Inverses

$\forall x \in \mathbb{Z}_N^*$ $\exists a$ s.t. $ax = 1 \bmod N$

The multiplicative group $\mathbb{Z}_N^*$

Quadratic residues QR_N^*

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

$N = pq$, $|QR_N^*| = \frac{\varphi(N)}{4}$ $\left[4 \mid (p-1)(q-1) \right]$

$\Rightarrow QR_N^* \cong QR_p^* \times QR_q^*$

The multiplicative group $\mathbb{Z}_N^*$

$\mathbb{Z}_{15}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$

$\mathbb{Z}_N^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$\phi(15) = (3-1)(5-1) = 8$

Q R_N^* :

$1^2 = 1$

$2^2 = 4$

$4^2 = 1$

$7^2 = 4$

$8^2 = 4$

$11^2 = 1$

$13^2 = 4$

$14^2 = 1$

Agenda for this lecture

- Announcements
- OWF collections
- Number theory background
- Rabin’s OWF collection
- Proving one-wayness of Rabin

Rabin’s function

Agenda for this lecture

- Announcements
- OWF collections
- Number theory background
- Rabin's OWF collection
- Proving one-wayness of Rabin

Factoring => Rabin is OWF