Number Theory & Cryptographic Hardness Assumptions

Jacob Benjamin Cholewa   Ştefan Patachi

IT University of Copenhagen

June 2017

Outline

Outline

Introduction

One-way functions

"One goal of this chapter is to introduce various problems believed to be hard, and to present conjectured one-way functions based on those problems."

"[I]n the public-key setting all known constructions rely on hard number-theoretic problems."

The inverting experiment $Invert_{\mathcal{A},f}(n)$

1. Choose uniform $x \in \{0,1\}^n$, and compute $y := f(x)$.
2. $\mathcal{A}$ is given 1^n and y as input, and outputs x'.
3. The output of the experiment is defined to be 1 if $f(x') = y$, and 0 otherwise.

Definition 7.1

A function $f : \{0,1\}^* \leftarrow \{0,1\}^*$ is one-way if the following two conditions hold:

1. **(Easy to compute:**) There exists a polynomial-time algorithm M_f computing f; that is, $M_f(x) = f(x)$ for all x.
2. **(Hard to compute):** For every probabilistic polynomial-time algorithm $\mathcal{A}$, there is a negligible function *negl* such that

$$\Pr\left[Invert_{\mathcal{A},f}(n) = 1\right] \leq negl(n)$$

Outline

Introduction
Divisibility

For two integers $a, b \in \mathbb{Z}$, a divides b, written as $a \mid b$, if there exists an integer c such that $ac = b$.

The *greatest common divisor* of two integers a, b, written $gcd(a, b)$, is the largest integer c such that $c \mid a$ and $c \mid b$. We say that a and b are relatively prime if $gcd(a, b) = 1$.

A positive integer $p > 1$ is *prime* if it has no factors; that is, it has only two divisors: 1 and itself.

A positive integer greater than 1 that is not a prime is called a *composite*. That is because all composites can be uniquely expressed as a product of primes.

$$N = \prod p_i^{e_i}$$

where p_i are distinct primes and $e_i \geq 1$ for all i.

Outline

Proposition 8.1

Let a be an integer and let b be a positive integer. Then there exist unique integers q, r for which $a = qb + r$ and $0 \leq r < b$.

Modulo Reduction

We define $[a \bmod N]$ to be equal to this r. Note that $0 \leq [a \bmod N] < N$.

Modular Arithmetic

congruence Modulo

We say that a and b are *congruent modulo* N, written as $a \equiv b \mod N$, if $[a \mod N] = [b \mod N]$. Note that $a \equiv b \mod N$ if and only if $N \mid (a - b)$.

Example

$$36 \equiv 21 \mod 15 \text{ as } 15 \mid (36 - 21).$$

Congruence modulo is an equivalence functions as it is reflexive ($\forall a, a \equiv a \mod N$), symmetric ($a \equiv b \mod N \Rightarrow b \equiv a \mod N$), and transitive ($a \equiv b \mod N \wedge b \equiv c \mod N \Rightarrow a \equiv c \mod N$).

Modular Arithmetic

congruence Modulo

Congruence module respects addition and multiplication

Example

$$[25 \cdot 2 \bmod 5] = [25 \bmod 5] \cdot [2 \bmod 5] = 25 \cdot 2 \equiv 50 \bmod 5$$

Congruence module does not (in general) respect division.

Example

$$3 \cdot 2 \equiv 6 \equiv 15 \cdot 2 \bmod 24, \text{ but } 3 \not\equiv 15 \bmod 24.$$

However; If for a given integer b there exists an integer c such that $bc = 1 \bmod N$, then we say that b is *invertible* modulo N, and call c a inverse of b. When b is invertible then we define the inverse as b^{-1} and define division as

$$[a/b \bmod N] \stackrel{def}{=} \left[ab^{-1} \bmod N\right]$$

Proposition 8.7

Let b, N be integers, with $b \geq 1$ and $N > 1$. Then b is invertible modulo N if and only if $gcd(b, N) = 1$.

Definition 8.9

An abelian group is a finite set $\mathbb{G}$, with $|\mathbb{G}|$ denoting the order of the set, along with a binary operator $\circ$ for which the following conditions hold:

- **(Closure:)** For all $g, h \in \mathbb{G}, g \circ h \in \mathbb{G}$.
- **(Existence of inverses:)** There exists an identity $e \in \mathbb{G}$ such that for all $g \in \mathbb{G}, e \circ g = g = g \circ e$.
- **(Associativity:)** For all $g, h, j \in \mathbb{G}, (g \circ h) \circ j = g \circ (h \circ j)$.
- **(Commutativity:)** for all $g, h \in \mathbb{G}, g \circ h = h \circ g$.

Example

Let $N > 1$ be an integer. The set $0, ..., N-1$ with respect to addition modulo N is an abelian group of order N, where the identity of the group is 0. We denote this group $\mathbb{Z}_N$.

Groups

Group exponentiation

It is often useful to describe the group operation applied m times to a fixed element g, where m is a positive integer. When using additive notation we express this $m \cdot g$; that is

$$m \cdot g \stackrel{def}{=} \underbrace{g + \cdots + g}_{m \text{ times}}$$

Thankfully, the notation adheres to familiar arithmetic rules such as:

$$(mg) + (m'g) = g \cdot (m + m')$$
$$m \cdot (m'g) = g \cdot (mm')$$
$$1 \cdot g = g$$

Groups

Group exponentiation

When using multiplicative notation we express this g^m; that is

$$g^m \stackrel{def}{=} \underbrace{g \cdots g}_{m \text{ times}}$$

Thankfully, the notation adheres to familiar arithmetic rules such as:

$$\begin{aligned} g^m \cdot g^{m'} &= g^{m+m'} \\ (g^m)^{m'} &= g^{mm'} \\ g^m \cdot h^m &= (gh)^m \\ g^1 &= g \end{aligned}$$

Lemma 8.13

Let $\mathbb{G}$ be a group and $a, b, c \in \mathbb{G}$. If $ac = bc$, then $a = b$.

Proof.

We know that $ac = bc$. Multiplying both sides with the unique inverse c^{-1} of c, we obtain $a = b$. In detail:

$$(ac)c^{-1} = (bc)c^{-1} \Rightarrow a(cc^{-1}) = b(cc^{-1}) \Rightarrow a = b$$

$\square$

Theorem 8.14

Let $\mathbb{G}$ be a finite group, with $m = |\mathbb{G}|$ as the order of the group. Then for any element $g \in \mathbb{G}, g^m = 1$.

Proof.

Fix an arbitrary $g \in \mathbb{G}$, and let $g_1, ..., g_m$ be the elements of $\mathbb{G}$. We claim that

$$g_1 \cdots g_m = (gg_1) \cdots (gg_m)$$

Remember that $gg_i = gg_j \Rightarrow g_i = g_j$. Following arithmetic rules we can 'pull out' all occurrences of g and obtain

$$g_1 \cdots g_m = (gg_1) \cdots (gg_m) = g^m \cdot (g_1 \cdots g_m)$$

$\square$

Corollary 8.17

Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}|$. Let $e > 0$ be an integer, and define the function $f_e : \mathbb{G} \to \mathbb{G}$ by $f_e(g) = g^e$. If $gcd(e, m) = 1$, then f_e is a permutation. Moreover, if $d = e^{-1} \mod m$, then f_d is the inverse of f_e. (Recall proposition 8.7: $gcd(e, m) = 1$ implies that e is invertible modulo m).

Proof.

Since $\mathbb{G}$ is finite, the second part of the claim implies the first; this, we need only show that f_d is the inverse of f_e. This is true because for any $g \in \mathbb{G}$ we have

$$f_d(f_e(g)) = f_d\left(g^e\right) = \left(g^e\right)^d = g^{ed} = g$$

$\square$

As discussed, the set $\mathbb{Z}_N = \{0, ..., N-1\}$ is a group under addition modulo N. Now we define the group under multiplication under modulo N, for any $N > 1$, to be given as

$$\mathbb{Z}_N^* \stackrel{def}{=} \{b \in \{1, ..., N-1\} \mid gcd(b, N) = 1\}$$

Proposition 8.18

Let $N > 1$ be an integer. Then $\mathbb{Z}_N^*$ is an abelian group under multiplication modulo N.

We define $\phi(N) \stackrel{def}{=} |\mathbb{Z}_N^*|$ to be the order of the group $\mathbb{Z}_N^*$. Lets first consider the case where $N = p$ is prime. Then all elements in $\{1, ..., p-1\}$ are relatively prime to p, and so the order of $\mathbb{Z}_p^*$ is given as $\phi(p) = p - 1$.

In the case where N is a composite of two primes $N = pq$, then the order of the group $\mathbb{Z}_N^*$ is given as $\phi(N) = (p-1)(q-1)$ (proof is omitted for brevity).

Example

Take $N = 15 = 5 \cdot 3$. Then $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, and $\phi(15) = (5-1)(3-1) = 8$.

Outline

Cyclic Groups

Cyclic Groups and Generators p.316-319

Let $\mathbb{G}$ be a finite group or order m, for any $g \in \mathbb{G}$ we say:

$\langle g \rangle = \{g^0, g^1, ..., g^{i-1}\}$ is a subgroup of $\mathbb{G}$ with order i and $i|m$

where $i \leq m$ is the smallest positive integer with $g^i = 1$.

Properties

- if $i = m$ then $\mathbb{G} = \langle g \rangle$ is a cyclic group.
- if $\mathbb{G}$ is cyclic and m is prime, then all elements of $\mathbb{G}$, except 1, are generators.

Theorem 8.56

If p is prime then $\mathbb{Z}_p^*$ is a cyclic multiplicative group of order $p-1$.

Example 8.60

Consider the (multiplicative) group $\mathbb{Z}_7^*$, which is cyclic by Theorem 8.56. We have $\langle 2\rangle = \{1,2,4\}$, and so 2 is not a generator. However,

$$\langle 3\rangle = \{1,3,2,6,4,5\} = \mathbb{Z}_7^*$$

and so 3 is a generator of $\mathbb{Z}_7^*$. .

Outline

Cyclic Groups

The Discrete Logarithm p.319-320

The general notation of a cyclic group:

$$\mathbb{G} = \langle g \rangle = \{g^x, \text{ for each } x \in \mathbb{Z}_q\}$$

For a random sample $h \in \mathbb{G}$, we call $x = \log_g h$ the discrete logarithm of h with respect to g from the context of $\mathbb{G}$.

The discrete logarithm experiment p.319-320

- Run $\mathcal{G}(1^n) \to (\mathbb{G}, q, g)$
- Choose $h \in_{\mathrm{R}} \mathbb{G}$
- $\mathcal{A}$ is given $(\mathbb{G}, q, g, h)$ and returns $x \in \mathbb{Z}_q$
- Experiment outputs 1 if $g^x = h$, 0 otherwise

The discrete logarithm problem is hard relative to $\mathcal{G}$ if for all probabilistic polynomial-time algorithms $\mathcal{A}$

$$Pr[DLog_{\mathcal{A},\mathcal{G}}(n) = 1] \leq negl(n)$$

Outline

Computaional Diffie-Hellman

Given $(\mathbb{G}, q, g)$ and $h_1, h_2 \in \mathbb{G}$, that means $h_1 = g^{x_1}, h_2 = g^{x_2}$, it is hard to compute:

$$DH_g(h_1, h_2) = g^{x_1 \cdot x_2} = h_1^{x_2} = h_2^{x_1}$$

Decisional Diffie-Hellmann

Given $(\mathbb{G}, q, g)$ and $h_1, h_2, h' \in \mathbb{G}$, it is hard to distinguish whether

$$h' \stackrel{?}{=} DH_g(h_1, h_2)$$

Cyclic Groups

Diffie-Hellman Assumptions p.320-321

Definition 8.63

We say that the DDH problem is hard relative to $\mathcal{G}$ if for all probabilistic polynomial-time algorithms $\mathcal{A}$

$$|Pr[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] - Pr[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^{x \cdot y}) = 1]|$$

$$\leq negl(n)$$

Outline

Cyclic Group

Theorem 8.64

Let $p - 1 = r \cdot q$, with p and q primes. Define

$$\mathbb{G} = \{[h^r \mod p] | h \in \mathbb{Z}_p^*\}$$

Then $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$ or order q.

Proof

- $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$
- order of $\mathbb{G}$ is q if $\exists f_r : \mathbb{Z}_p^* \to \mathbb{G}$ and f_r is a $r - to - 1$ function

Cyclic Group

Subgroups of $\mathbb{Z}_p^*$ p.322-324

Properties

- because q is prime, all elements of $\mathbb{G}$ except 1 are generators
- to choose uniform element from $\mathbb{G}$:

$$\text{pick } h \in_{\mathrm{R}} \mathbb{Z}_p^*, \text{ output } [h^r \mod p]$$

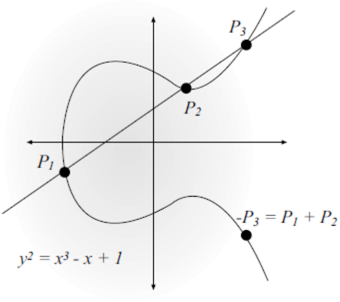
- to check if any element $h \in \mathbb{Z}_p^*$ is also in $\mathbb{G}$, check

$$h^q \stackrel{?}{=} 1 \mod p$$

Outline

Cyclic Group

Elliptic Curves p.325-332



- $P + \mathcal{O} = \mathcal{O} + P = P$
- if $P = (x, y)$ then $-P = (x, -y)$
- $P - P = \mathcal{O}$

$$4A^3 + 27B^2 \neq 0 \mod p$$

Definition

$E(\mathbb{Z}_p) = \{(x, y) | x, y \in \mathbb{Z}_p \text{ and } y^2 = x^3 + Ax + B \mod p\} \cup \{\mathcal{O}\}$

Cyclic Group

Elliptic Curves p.325-332

Calculations

To compute the addition of $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, we calculate $P_1 + P_2 = P_3(x_3, y_3)$:

1. calculate the slope $m = \left[\frac{y_2 - y_1}{x_2 - x_1} \mod p\right]$
2. the line P_1P_2 is $y = m \cdot (x - x_1) + y_1 \mod p$
3. coordinates of P_3 are
   $x_3 = [m^2 - x_1 - x_2 \mod p]$ & $y_3 = [m(x_1 - x_3) - y_1 \mod p]$

When $P_1 = P_2$ then $2P_1 = P_3(x_3, y_3)$ where:

- $x_3 = [m^2 - 2x_1 \mod p]$ & $y_3 = [m(x_1 - x_3) - y_1 \mod p]$
- $m = \left[\frac{3x_1^2 + A}{2y_1}\right]$

Affine Coordinates vs. Projective coordinates

- affine coordinates: $P = (x, y) = (X/Z \mod p, Y/Z \mod p)$
- projective coordinates: $P = (X, Y, Z)$

Addition of $P_1 + P_2 =$

$$P_3 = \left(m^2 - \frac{X_1}{Z_1} - \frac{X_2}{Z_2}, m\left(\frac{X_1}{Z_1} - m^2 + \frac{X_1}{Z_1} + \frac{X_2}{Z_2}\right) - \frac{Y_1}{Z_1}, 1\right)$$

$$m = \frac{\frac{Y_2}{Z_2} - \frac{Y_1}{Z_1}}{\frac{X_2}{Z_2} - \frac{X_1}{Z_1}} = \frac{Y_2 Z_1 - Y_1 Z_2}{X_2 Z_1 - X_1 Z_2}$$

Cyclic Group

Elliptic Curves Efficiency p.325-332

Projective Coordinates

$$P_3 = \left(vw, u(v^2 X_1 Z_2 - w) - v^3 Y_1 Z_2, Z_1 Z_2 v^3\right)$$

$$u = Y_2 Z_1 - Y_1 Z_2$$

$$v = X_2 Z_1 - X_1 Z_2$$

$$w = u^2 Z_1 Z_2 - v^3 - 2v^2 X_1 Z_2$$

Point compression

- only coordinate x is needed
- y is computable from the elliptic curve $E : y^2 = f(x) \mod p$
- one extra bit b needed for deciding what value y_b to use