

Cryptography

Course 3: discrete-log and elliptic-curve cryptography

Jean-Sébastien Coron

Université du Luxembourg

October 4, 2010

Discrete-log based cryptography

- Discrete-log based group
 - The multiplicative group \mathbb{Z}_p^*
- Discrete-log based encryption
 - ElGamal
- Elliptic-Curve cryptography

The multiplicative group \mathbb{Z}_p^*

- Let p be a prime integer.
 - The set \mathbb{Z}_p^* is the set of integers modulo p which are invertible modulo p .
 - The set \mathbb{Z}_p^* is a cyclic group of order $p - 1$ for the operation of multiplication modulo p .
- Generators of \mathbb{Z}_p^* :
 - There exists $g \in \mathbb{Z}_p^*$ such that any $h \in \mathbb{Z}_p^*$ can be uniquely written as $h = g^x \pmod p$ with $0 \leq x < p - 1$.
 - The integer x is called the *discrete logarithm* of h to the base g , and denoted $\log_g h$.

Finding a generator of \mathbb{Z}_p^*

- Finding a generator of \mathbb{Z}_p^* for prime p .
 - The factorization of $p - 1$ is needed. Otherwise, no efficient algorithm is known.
 - Factoring is hard, but it is possible to generate p such that the factorization of $p - 1$ is known.
- Generator of \mathbb{Z}_p^*
 - $g \in \mathbb{Z}_p^*$ is a generator of \mathbb{Z}_p^* if and only if $g^{(p-1)/q} \neq 1 \pmod p$ for each prime factor q of $p - 1$.
 - There are $\phi(p - 1)$ generators of \mathbb{Z}_p^*

Generating p and q

- Generate p such that $p - 1 = 2 \cdot q$ for some prime q .
 - Generate a random prime p .
 - Test if $q = (p - 1)/2$ is prime. Otherwise, generate another p .
- Finding a generator g for \mathbb{Z}_p^*
 - Generate a random $g \in \mathbb{Z}_p^*$ with $g \neq \pm 1$
 - Check that $g^q \neq 1 \pmod p$. Otherwise, generate another g .
 - Complexity :
 - There are $\phi(p - 1) = q - 1$ generators.
 - g is a generator with probability $\simeq 1/2$.

- Discrete logarithm problem :
 - Given g, h such that $h = g^x$ for $x \stackrel{R}{\leftarrow} \mathbb{Z}_{p-1}$, find x .
- Computing discrete logarithms in \mathbb{Z}_p^*
 - Hard problem: no efficient algorithm is known for large p .
 - Brute force: enumerate all possible x . Complexity $\mathcal{O}(p)$.
 - Baby step/giant step method: complexity $\mathcal{O}(\sqrt{p})$.

- We want to work in a prime-order subgroup of \mathbb{Z}_p^*
 - Generate p, q such that $p - 1 = 2 \cdot q$ and p, q are prime
 - Find a generator g of \mathbb{Z}_p^*
 - Then $g' = g^2 \pmod p$ is a generator of a subgroup G of \mathbb{Z}_p^* of prime order q .

- Key generation
 - Let G be a subgroup of \mathbb{Z}_p^* of prime order q and g a generator of G .
 - Let $x \xleftarrow{R} \mathbb{Z}_q$. Let $h = g^x \pmod p$.
 - Public-key : (g, h) . Private-key : x
- Encryption of $m \in G$:
 - Let $r \xleftarrow{R} \mathbb{Z}_q$
 - Output $c = (g^r, h^r \cdot m)$
- Decryption of $c = (c_1, c_2)$
 - Output $m = c_2 / (c_1^x) \pmod p$

- To recover m from $(g^r, h^r \cdot m)$
 - One must find h^r from $(g, g^r, h = g^x)$
- Computational Diffie-Hellmann problem (CDH) :
 - Given (g, g^a, g^b) , find g^{ab}
 - No efficient algorithm is known.
 - Best algorithm is finding the discrete-log

- Defines a new group different from \mathbb{Z}_p^*
 - Different assumption
 - Advantage: shorter keys
- Elliptic-curve equation over \mathbb{Z}_p :
 - $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Z}_p$
- Group structure
 - The set of points together with \mathcal{O} can define a group structure

- Let $P = (x_1, y_1) \neq \mathcal{O}$ and $Q = (x_2, y_2) \neq \mathcal{O}$. Then $P + Q = (x_3, y_3)$ with:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, & \text{if } P = Q \end{cases}$$

- $P = (x_1, y_1) \neq \mathcal{O} \Rightarrow -P = (x_1, -y_1)$

- **Double-and-add Algorithm:**
input P and $d = (d_{\ell-1}, \dots, d_0)$
output $Q = dP$

 $Q \leftarrow P$
for i from $\ell - 2$ downto 0 do
 $Q \leftarrow 2Q$
 if $d_i = 1$ then $Q \leftarrow Q + P$
output Q

- Ordinary elliptic-curves
 - $y^2 = x^3 + ax + b \pmod{p}$
 - Let n be the number of points, including \mathcal{O} .
 - We must have $n = k \cdot q$ where q is a large prime.
 - then work in subgroup of order q .
- Computing the group order n :
 - Schoof's algorithm.
 - Schoof-Elkies-Atkin algorithm.
 - or use standardized curves.

- Key generation
 - Let \mathbb{G} be an elliptic curve subgroup of prime order q and G a generator of \mathbb{G} .
 - Let $\alpha \xleftarrow{R} \mathbb{Z}_q$. Let $H = \alpha G$.
 - Public-key : (G, H) . Private-key : α
- Encryption of m :
 - Let $r \xleftarrow{R} \mathbb{Z}_q$
 - Output $c = (rG, (rH)_x \oplus m)$ where $(rH)_x$ denotes the x coordinate of rH .
- Decryption of $c = (C_1, c_2)$
 - Output $m = (\alpha C_1)_x \oplus c_2$