Discrete Logarithm

Lukas Helminger

Mathematical Foundations of Cryptography – WT 2020/21

Outline

Literature

The slides are based on the following books

- **The Arithmetic of Elliptic Curves**, Joseph H. Silverman
- **An Introduction to Mathematical Cryptography**, Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H.
- **Elliptic Curves: Number Theory and Cryptography**, Lawrence C. Washington
- **Elliptische Kurven in der Kryptographie.**, Annette Werner

Motivation

- Suggested by Miller, Koblitz in 1980's
- Smaller key size compared to RSA
- Recommended cryptographic primitive (standard)

Elliptic Curve Cryptography

Elliptic Curves

Definition

An elliptic curve E over the field $\mathbb{F}$ is the set of solutions of an equation of the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

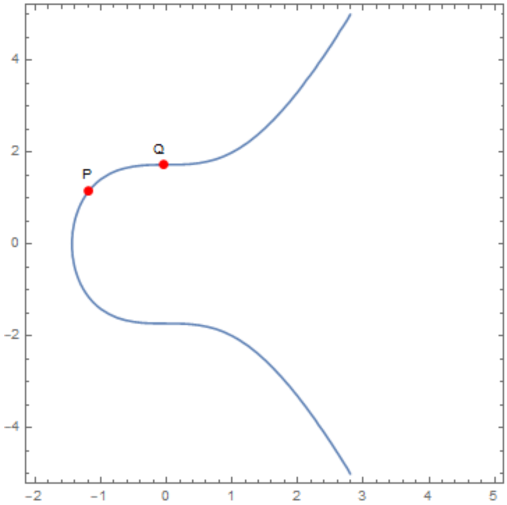
where $a, b \in \mathbb{F}$, with the discriminant $\Delta := -16(4a^3 + 27b^2) \neq 0$, i.e.

$$E = \{(x : y : z) \in \mathbb{P}^2(\bar{\mathbb{F}}) \mid y^2z = x^3 + axz^2 + bz^3\}.$$

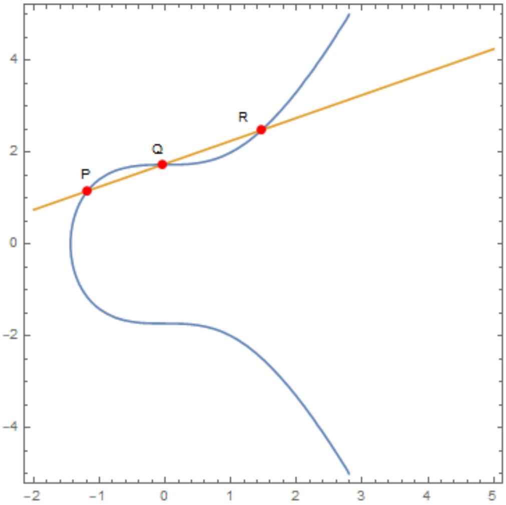
Affine plane: $E : y^2 = x^3 + ax + b$
Rational points:

$$E(\mathbb{F}) := \{O\} \cup \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 = x^3 + ax + b\}$$

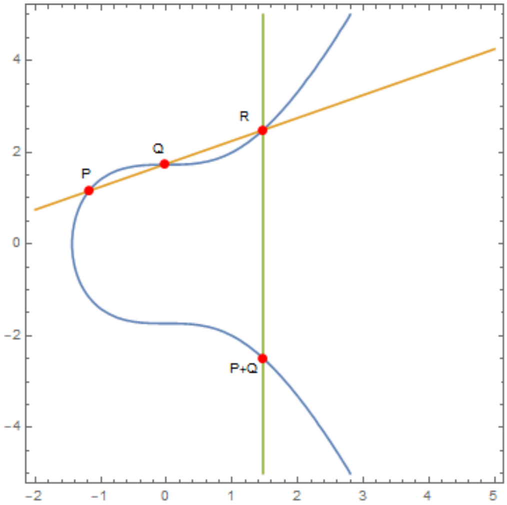
The Group Law



The Group Law



The Group Law



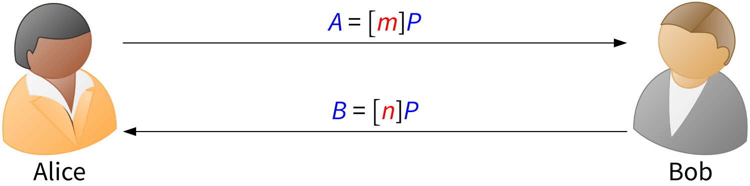
Mulitplicatio-by-m map

Let E be an elliptic curve over $\mathbb{F}$, and let m be an integer. The multiplication-by-m map $[m] : E \to E$ is defined for $P \in E$ as follows

$$[m]P := \begin{cases} \overbrace{P + \cdots + P}^{m \text{ terms}} & m > 0 \\ O & m = 0 \\ \underbrace{-P - \cdots - P}_{-m \text{ terms}} & m < 0 \end{cases}.$$

Elliptic Curve Diffie-Hellman Key Agreement

Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$.
Then Alice chooses a secret integer m, and Bob chooses a secret integer n.



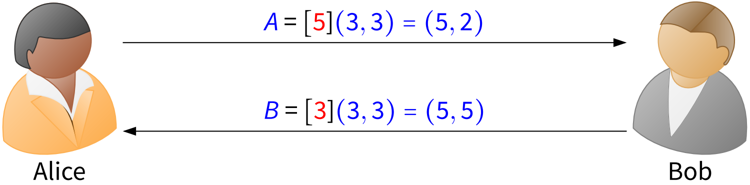
Their shared key is

$$K = [mn]P = [m]B = [n]A$$

DH Example

Elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{F}_7$ and generator $P = (3,3) \in E(\mathbb{F}_7)$. $m = 5$, $n = 3$.

n	0	1	2	3	4	5	6	7
nP	O	$(3,3)$	$(1,4)$	$(5,5)$	$(0,0)$	$(5,2)$	$(1,3)$	$(3,4)$



$K = [5 \cdot 3](3,3) = (3,4)$

(Elliptic Curve) Discrete Logarithm Problem

Definition (ECDLP)

Given an elliptic curve E over $\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ and point $Q \in \langle P \rangle$.
Find:

$$[x]P = Q$$

Definition (DLP)

Let $(G, \cdot)$ be a finite cyclic group and $g \in G$ a generator of G. Further, let $a \in G$ be arbitrarily. The challenge is to find an $x \in \mathbb{Z}$ such that

$$g^x = a.$$

Examples

- Let $G = (\mathbb{Z}/31\mathbb{Z})^\times$. One can show that $\overline{3}$ is a generator of the cyclic group. Further, let $a = \overline{14}$. Then the DLP is to find $x \in \mathbb{Z}$ such that
$$\overline{3}^x = \overline{14}.$$
- Elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{F}_7$ and generator $P = (3,3) \in E(\mathbb{F}_7)$. $m = 5$, $n = 3$.

n	0	1	2	3	4	5	6	7
nP	O	$(3,3)$	$(1,4)$	$(5,5)$	$(0,0)$	$(5,2)$	$(1,3)$	$(3,4)$

$K = [5 \cdot 3](3,3) = (3,4)$ Would have to solve:
$$[x](3,3) = (3,4).$$

Dlog Algorithms

Subsection 1

Babystep-Giantstep

Shanks's Babystep-Giantstep Algorithm

1. $m \leftarrow \lceil \sqrt{n} \rceil$
2. Create two lists:

$$\text{BS: } 1, g, g^2, \ldots, g^{m-1}$$
$$\text{GS: } a, a\left(g^{-m}\right), a\left(g^{-m}\right)^2, \ldots, a\left(g^{-m}\right)^{m-1}$$

3. Find a match between the list BS and GS,
   say $g^i = a \cdot (g^{-m})^j$.
4. $x' \leftarrow i + jm$

BSGS Example

$G = (\mathbb{Z}/31\mathbb{Z})^\times$, then $m = \lceil \sqrt{30} \rceil = 6$. We want to solve the following DLP

$$\overline{3}^x = \overline{14}$$

The baby steps are:

q	0	1	2	3	4	5
$\overline{3}^i$	$\overline{1}$	$\overline{3}$	$\overline{9}$	$\overline{27}$	$\overline{19}$	$\overline{26}$

The giant steps are:

r	0	1	2	3	4	5
$\overline{14} \cdot \overline{3}^{-6j}$	$\overline{14}$	$\overline{28}$	$\overline{25}$	$\overline{19}$	$\overline{7}$	$\overline{14}$

Therefore the solution to the DLP is $x = 3 \cdot 6 + 4 = 22$.

BSGS Analyses

Runtime:

1. $m \leftarrow \lceil \sqrt{n} \rceil$
2. BS: $1, g, g^2, \ldots, g^{m-1}$ $\qquad \mathcal{O}(m)$
   GS: $a, a\left(g^{-m}\right), a\left(g^{-m}\right)^2, \ldots, a\left(g^{-m}\right)^{m-1}$ $\qquad \mathcal{O}(m)$
3. Finding a match $\qquad \mathcal{O}(m \log m)$

$$\mathcal{O}\left(\sqrt{n}\right)$$

Space Complexity:
The lists in step (2) have length m, so we get $\mathcal{O}\left(\sqrt{n}\right)$.

Pohlig-Hellman

Let $|G| = n = \prod_{i=1}^{m} p_i^{e_i}$. Assume we have some oracle $O(g, a, p^e)$ which outputs the DL of a w.r.t. g in a group of order p^e.

Then for $i = 1, \ldots, m$ do:

1. $g' \leftarrow g^{N/p^{e_i}}$
2. $a' \leftarrow a^{N/p^{e_i}}$
3. $y_i \leftarrow O(g', a', p^{e_i})$

Use the CRT to solve

$$x \equiv y_1 \pmod{p_1^{e_1}} \quad , \ldots , \quad x \equiv y_m \pmod{p_m^{e_m}}.$$

Running time: $\mathcal{O}\left(\left(\sum_{i=1}^{m}\left(e_i\left(\log n + \sqrt{p_i}\right)\right)\right)\right)$

Subsection 3

Pollard ρ-Method

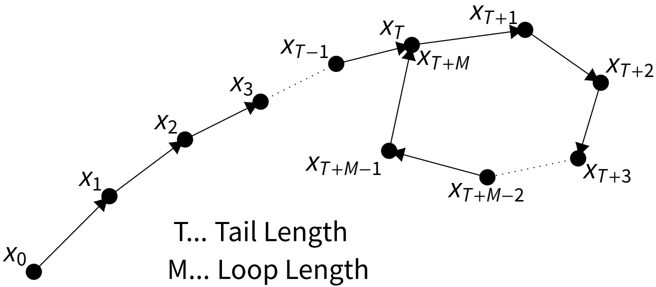
Definition and Notation

Definition

Let S be a finite set, let $f : S \to S$ and let $x \in S$. The sequence

$$x_0 = x, \quad x_1 = f(x_0), \quad x_2 = f(x_1), \quad x_3 = f(x_2), \quad \dots$$

is called the (forward) orbit of x by the map f and is denoted by $O_f^+(x)$.



T... Tail Length
M... Loop Length

Theorem (Cycle Detection)

Let S be a finite set containing n elements, let $f : S \to S$, and $x \in S$ be an initial point.

- a Suppose that the forward orbit $O_f^+(x) = \{x_0, x_1, x_2, \dots\}$ of x has a tail of length T and a loop length of M. Then

$$x_{2i} = x_i \qquad \text{for some } 1 \leq i < T + M.$$

  In particular we only need $\mathcal{O}(1)$ memory to find a collision.

- b If f is sufficiently random, then the expected value of $T + M$ is

$$\mathbb{E}(T + M) \approx 1.25\sqrt{n}.$$

  Hence, we are likely to find a collision in $\mathcal{O}(\sqrt{n})$ steps.

Pollard's ρ for the DLP

Partition G into S_1, S_2, S_3, where $1 \notin S_2$. Let $x_i \in G$, then we define $f : G \to G$ in the following way

$$f(x_i) = \begin{cases} gx_i & x_i \in S_1 \\ x_i^2 & x_i \in S_2 \\ ax_i & x_i \in S_3. \end{cases}$$

Note, if we start with $x_0 = 1$, every x_i can be written as $x_i = g^{\alpha_i} a^{\beta_i}$, where

$$\alpha_i = \begin{cases} \alpha_{i-1} + 1 \pmod{n} & x_i \in S_1 \\ 2\alpha_{i-1} \pmod{n} & x_i \in S_2 \\ \alpha_{i-1} & x_i \in S_3 \end{cases} \qquad \beta_i = \begin{cases} \beta_{i-1} & x_i \in S_1 \\ 2\beta_{i-1} \pmod{n} & x_i \in S_2 \\ \beta_{i-1} + 1 \pmod{n} & x_i \in S_3. \end{cases}$$

Pollard's ρ for the DLP (cont.)

- Compute $((x_i, \alpha_i, \beta_i), (x_{2i}, \alpha_{2i}, \beta_{2i}))$ until there is a collision $x_i = x_{2i}$, i.e. $g^{\alpha_i} a^{\beta_i} = g^{\alpha_{2i}} a^{\beta_{2i}}$. Hence,
$$g^{\alpha_i - \alpha_{2i}} = a^{\beta_{2i} - \beta_i} = g^{x(\beta_{2i} - \beta_i)}.$$
Therefore a solution to the given DLP is a solution of the congruence relation
$$x(\beta_{2i} - \beta_i) \equiv \alpha_i - \alpha_{2i} \pmod{n}.$$
- Apply the Eucledian algorithm to find the smallest positive integer solution s.
- Set $d = \gcd(\beta_{2i} - \beta_i, n)$, then basic theory about congruence relations tells x is one of the values
$$s, s + \frac{n}{d}, \ldots, s + (d-1)\frac{n}{d}.$$
- Try all possible values (usually d is small).

Pollard's ρ Example

Consider the subgroup G of $\mathbb{F}_{607}^*$ of order $n = 101$ generated by the element $g = \overline{64}$ and the DLP

$$\overline{64}^x = \overline{122}.$$

Define

$$\begin{aligned} S_1 &= \left\{\overline{x} \in \mathbb{F}_{607}^* : x \leq 201\right\}, \\ S_2 &= \left\{\overline{x} \in \mathbb{F}_{607}^* : 202 \leq x \leq 403\right\}, \\ S_3 &= \left\{\overline{x} \in \mathbb{F}_{607}^* : 404 \leq x \leq 606\right\}. \end{aligned}$$

Apply Pollard's Rho method:

Pollard's ρ Example (cont.)

i	x_i	α_i	β_i	x_{2i}	α_{2i}	β_{2i}
0	$\overline{1}$	0	0	$\overline{1}$	0	0
1	$\overline{122}$	0	1	$\overline{316}$	0	2
2	$\overline{316}$	0	2	$\overline{172}$	0	8
3	$\overline{308}$	0	4	$\overline{137}$	0	18
$\vdots$		$\vdots$			$\vdots$	
11	$\overline{182}$	0	55	$\overline{7}$	8	12
12	$\overline{352}$	0	56	$\overline{309}$	16	26
13	$\overline{76}$	0	11	$\overline{352}$	32	53
14	$\overline{167}$	0	12	$\overline{167}$	64	6

i.e. collision, when $i = 14$.

$$
\begin{aligned}
x(6-12) &\equiv 0-64 \pmod{101} \\
-6x &\equiv -64 \pmod{101} \\
95x &\equiv 37 \pmod{101}
\end{aligned}
$$

Since $\gcd(95, 101) = 1$, there is only one solution smaller than n.

$$x = 78.$$

Index-Calculus

Only works for the multiplicative group of a finite field, i.e. $\mathbb{F}_q^*$.
Setting of the DLP $\overline{g}, \overline{a} \in \mathbb{Z}_p^*$:

$$\overline{g}^x = \overline{a}.$$

The algorithm has two major steps:

1. Choose a bound $B \in \mathbb{N}$ and compute the discrete logarithm for all elements q in the factor base $F(B)$: $\overline{g}^{x_q} = \overline{q}$

2. Look for an exponent $y \in \{1, 2, \ldots, p-1\}$ such that the integer ag^y modulo p is B-smooth.

Dlog Algorithms (EC)

Subsection 1

MOV Algorithm

Torsion Group

Definition

Torsion Points Let $n \in \mathbb{N}$. The set of n-torsion points of the group E is denoted by

$$E[n] = \{P \in E : [n]P = O\}.$$

Note that this set is the kernel of the multiplication-by-n map.

Let $E : y^2 = x^3 - 7x + 6$ be an elliptic curve over $\mathbb{R}$. $E[2] = ?$.
$O \in E[2]$. So, let $P \in E[2] \setminus \{O\}$ be arbitrary. From $[2]P = O$, we know that O lies on the tangent of E at P. Let $aX + bY + cZ = 0$ be the equation defining the tangent. Since O is on this projective line, we get $b = 0$ and therefore the tangent is is vertical in the affine plane. This implies that the y-coordinate of P must be 0. To get the remaining points in $E[2]$, we now have to solve the cubic equation $0 = x^3 - 7x + 6$. By doing this we obtain

$$E[2] = \{O, (-3, 0), (1, 0), (2, 0)\}.$$

Pairings

Definition (Pairing)

Let $G_1 = \langle g_1 \rangle, G_2 = \langle g_2 \rangle$ and G_T be three groups of prime order p. A (bilinear) pairing is a map $e : G_1 \times G_2 \to G_T$, with the following properties:

Bilinearity: $e(g_1, g_2)^{ab} = e(g_1^b, g_2^a) \quad \forall a, b \in \mathbb{Z}_p$

Non-degeneracy: $e(g_1, g_2) \neq 1_{G_T}$, i.e. $e(g_1, g_2)$ generates G_T.

Definition (Weil-Pairing)

Let E be an elliptic curve over $\mathbb{F}$ and $n \in \mathbb{N}$, then there exists a map

$$e_n : E[n] \times E[n] \longrightarrow \mu_n\left(\bar{\mathbb{F}}\right) := \{x \in \bar{\mathbb{F}}^* : x^n = 1\}$$

which is bilinear, called the Weil-pairing.

Digression: Roots of unity

Definition (Root of Unity)

Let $\mathbb{F}$ be a field and $n \in \mathbb{N}$. An element $x \in \mathbb{F}$ is called n-th root of unity in $\mathbb{F}$ if

$$x^n = 1.$$

The set of n-th roots of unity in $\mathbb{F}$ is denoted by $\mu_n(\mathbb{F})$.

- $\mu_n(\mathbb{F})$ is a cyclic subgroup of $(\mathbb{F}^*, \cdot)$
- The generators of $\mu_n(\mathbb{F})$ are called primitive n-th roots of unity.

Pairings (cont.)

Corollary

Let E be an elliptic curve over a finite field $\mathbb{F}$ and let $P \in E$ be a point of order n. Then there exists a point $Q \in E[n]$ such that $e_n(P, Q)$ is a primitive n-th root of unity. In particular, if $E[n] \subset E(\mathbb{F})$, then $\mu_n(\bar{\mathbb{F}}) \subset \mathbb{F}^*$.

MOV Algorithm

Given: Elliptic curve E over $\mathbb{F}_q$ ($q = p^r$), with $Q \in \langle P \rangle$ and $\#\langle P \rangle = n$.
Find: $k \in \mathbb{Z}$:

$$[k]P = Q$$

1. Determine a number l with $E[n] \subset E(\mathbb{F}_{q^l})$.
2. Compute a point $R \in E[n]$ such that $a = e_n(P, R)$ is a primitive n-th root of unity, i.e. a has order n in $\mu_n(\overline{\mathbb{F}}_q)$.
3. Compute $b = e_n(Q, R)$.
4. Solve the DLP: $b = a^k$ in $\mathbb{F}_{q^l}^*$.

Suprersingular Curves

Definition (Supersingular)

An elliptic curve E over a finite field $\mathbb{F}_q$ is called supersingular, if $\mathrm{char}(\mathbb{F}_q)$ divides $t = q + 1 - \#E(\mathbb{F}_q)$.

Proposition

Let E be a supersingular elliptic curve over $\mathbb{F}_q$ and $t = q + 1 - \#E(\mathbb{F}_q)$. Then $E[n] \subset E(\mathbb{F}_{q^l})$, if l is chosen according to the table below. The number d to the corresponding l is the exponent of the group $E(\mathbb{F}_{q^l})$, i.e. the smallest natural number d such that $[d]R = O$ for all $R \in E(\mathbb{F}_{q^l})$.

t	0	$\pm\sqrt{q}$	$\pm\sqrt{2q}$	$\pm\sqrt{3q}$	$\pm 2\sqrt{q}$
l	2	3	4	6	1
d	$q+1$	$\sqrt{q^3} \pm 1$	q^2+1	q^3+1	$\sqrt{q} \mp 1$

Anomalous Curves

Definition

An elliptic curve E over $\mathbb{F}_p$ is called anomalous if $\#E(\mathbb{F}_p) = p$.

The SSSA algorithm computes the discrete logarithm in anomalous curves in $O(\log(p)^3)$ steps.

Implication for key sizes

Fastest generic algorithms: $\mathcal{O}\left(\sqrt{n}\right)$
Fastest algorithm for $\mathbb{F}_p^*$: $L_p[\frac{1}{2}, \sqrt{2}] = \exp((\sqrt{2} + o(1)) \ln p)^{1/2} (\ln \ln p)^{1/2})$

Security	RSA	DH/DSA	ECDH/ECDSA
128	3072	3072	256
256	15360	15360	512