Algorithms for solving DLP / ECDLP

- Generic alg. – applicable to arbitrary groups

a) Exhaustive search: Check for all $a \in \{0, \dots, n-1\}$, $n \in ord(P)$ whether $Q = a \cdot P$
Complexity $O(n)$: worst case: n computations

b) Babystep – Giantstep – Alg (Shanks)
Let $m = \lceil \sqrt{n} \rceil$
There exist unique $q, r \in \{0, \dots, m-1\}$ s.t. $a = q \cdot m + r$

$Q = a \cdot P = q \cdot m \cdot P + r \cdot P \Leftrightarrow Q - r \cdot P = q \cdot m \cdot P$

Compute all values $Q - r \cdot P$, $0 \leq r \leq m-1$ and store them (Babysteps)
If $Q - r \cdot P = \mathcal{O}$, for some r we are done $(a = r)$
Otherwise compute $m \cdot P$ and then successively $q \cdot m \cdot P$ and compare to $Q - r P$. (Giant steps)
Complexity: m Babysteps, m Giantsteps, m values to be stored
$\sim O(\sqrt{n})$ memory & computing complexity

c) Pohlig – Hellman – Method.
<u>Assumption</u>: Factorization of n is known: $n = \prod_{i=1}^{r} p_i^{l_i}$
<u>Idea</u>: Solve DLPs in subgroups of order $p_i^{l_i}$, hence, compute $a_i \mod p_i^{l_i}$, then use CRT to compute $a \mod n$
The DLP in the subgroup of order $p_i^{l_i}$ can be reduced to l_i DLPs in the subgroup of order p_i.
Solve these DLPs with b) (For more details see MOV)

<u>Complexity</u> $\sum_{i=1}^{r} l_i \big(\underbrace{\log(n)}_{\text{reduction}} + \underbrace{\sqrt{p_i}}_{\text{BSGS}}\big) + \underbrace{(\log(n))^2}_{\text{CRT}}$ operations

→ Complexity depends on the largest prime divisor of n
→ for cryptographic purposes choose groups with a large prime divisor
→ If n is prime it is just b)

d) <u>Pollard ρ - Method</u>

<u>Idea</u>: Find numbers $c, d, c', d' \in \mathbb{Z}$ s.t.

$$cP + d \cdot Q = c'P + d' \cdot Q$$

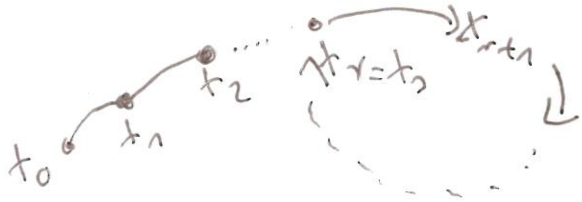
$$\Rightarrow (c - c')P = (d' - d) \cdot Q = (d' - d) \cdot a \cdot P$$

$$\Rightarrow c - c' \equiv (d' - d) \cdot a \pmod n$$

If $\gcd(d' - d, n) = 1$, compute $a = (d' - d)^{-1}(c - c') \bmod n$

To find such numbers, construct pseudo-random sequences (c_i, d_i)

$X_i = c_i \cdot P + d_i \cdot Q$. On a finite set a collision will occur



Therefore, the method is called ρ-method (As the values of x_i look like a rho.)

Complexity: $O(\sqrt{n})$ (cf. Birthday paradoxon)

- Specialized method using some more structure

e) Reduction algorithm for ECDLP (MOV / Frey - Rück)

Reduce ECDLP in $E(\mathbb{F}_q)$ to a DLP in $\mathbb{F}_{q^k}^*$ for some $k \in \mathbb{N}$ (embedding degree)

↳ Can be avoided by choice of E leading to large k.

f) Index Calculus (similar to sieving methods for factorizing integers)

<u>Idea</u>: Use a factorbase $\alpha^a = \prod_{i=1}^{t} p_i^{\lambda_i}$, where α is a generator, a is a random number and $(p_1, \dots, p_t)$ is a factor base of t primes.

It follows that $a = \sum_{i=1}^{t} \lambda_i \log_\alpha(p_i)$.

Choose a factorbase with small elements, s.t., sufficiently many group elements can be represented as a product of elements of this factorbase

Compute DLs for these elements:

Obtain a system of linear equations by taking enough random numbers a and getting enough equations to obtain the solution of $\log_\alpha(p_i)$.

The DL is calculated as follows:

Take random b, until $\alpha^b \cdot \beta = \prod_{i=1}^{t} p_i^{\lambda_i}$ can be found

$\Rightarrow$ $\cancel{b+}\log_\alpha(\beta) = \sum_{i=1}^{t} \lambda_i \log_\alpha(p_i) - b$

- Most efficient alg. known for $\mathbb{F}_p$ (and $\mathbb{F}_{q^k}^*$)

subexponentially complexity: $e^{\sqrt[3]{\frac{64}{9}}(\log(n))^{1/3}(\log(\log(n)))^{2/3}}$

comparison $\sqrt{n} = n^{1/2} = (e^{\ln(n)})^{1/2} = e^{1/2 \ln(2) \log(n)}$

- Index calculus cannot be applied to $E(\mathbb{F}_q)$; problem is the construction of the factor base.

<u>Cryptographically secure curves</u>

Choose a cyclic group $\langle P \rangle \leq E(\mathbb{F}_q)$, s.t.,

- $\langle P \rangle$ contains at least 2^{160} points ((a), (b), (d) not feasible)
- $\mathrm{ord}(P) = |\langle P \rangle|$ has a prime factor of size 2^{160} ((c) not feasible)
- embedding degree k should be large ((e) is not feasible)

Comparison DLP vs ECDLP

There exist more efficient alg. for solving the DLP in $\mathbb{F}_p^*$ and $\mathbb{F}_{q^k}^*$ than for $E(\mathbb{F}_q)$, hence, ECC has a security advantage. The following systems have the same security level

DL on $\mathbb{F}_p^*$	ECDL
p: 2048 bits	n: 224 bits (group order)

$\Rightarrow q$ has 224 bits

13.4 Cryptographic Applications

Having selected a cryptographically secure curve, carry out protocols based on the ECDLP.

Prerequisites: $\langle P \rangle \leq E(\mathbb{F}_q)$, $\mathrm{ord}(P) = n$, publically known

13.4.1 DH key exchange

see motivation

13.4.2 Mapping of integers to points of elliptic curves and vice versa

The mapping of integers to points on EC will be described in two steps. First a deterministic approach for a special case. Second, a probabilistic approach for the general case.

Deterministic procedure

Let: $E: Y^2 = X^3 + aX \cancel{+b}$ $a, b \in \mathbb{F}_p$

be an elliptic curve over $\mathbb{F}_p$ with $b=0$ and prime $p \equiv 3 \pmod{4}$

For a message $0 < M < p/2$ let $x = M$

- Calculate $z = x^3 + a \cdot x$
- If z is quadratic residue, calculate a square root $y \bmod p$ which can be easily done, cf. Prop 9.3.
- Otherwise, repeat the last two steps for $x = p - M$
- The point on the elliptic curve is (x, y).

This procedure is valid

If M or $p-M$ leads to a quadratic residue, the validity is obvious.
It remains to show that either M or $p-M$ is quadratic residue.
Let g be a generator, then there exists $0 < i < p$, s.t

$$M^3 + a \cdot M \equiv g^i \pmod{p}$$

If i is even, $z = M^3 + a \cdot M \bmod p$ is a quadratic residue.
Otherwise, if i is odd then

$$(p-M)^3 + a(p-M) \equiv -M^3 - aM \equiv -g^i \overset{(*)}{\equiv} g^{i + \frac{p-1}{2}} \pmod{p}$$

As $p \equiv 3 \pmod{4}$, $\frac{p-1}{2}$ is odd, i.e., $i + \frac{p-1}{2}$ is even
Hence, $z = (p-M)^3 + a(p-M) \bmod p$ is a quadratic residue

Remark on $(*)$

As $\mathbb{F}_p$ is a field, the square roots of $1 \equiv g^0 \equiv g^{p-1} \pmod{p}$ is either 1 or $-1 \equiv g^{\frac{p-1}{2}} \pmod{p}$. Hence, $-g^i \equiv g^{i + \frac{p-1}{2}} \pmod{p}$

Let (x, y) be a point on the EC, then the corresponding message is given as $M = \min\{x, p-x\}$