The Elliptic Curve Discrete Logarithm Problem

Enric Florit Zacarías

These notes are a small survey made for self-study on the Discrete Logarithm Problem. I have done a review of general methods first, and then stepped into ECDLP. Some basic knowledge from group theory, modular arithmetic and elliptic curves should be sufficient to understand the content.

1 Statement

Let G be a cyclic group and $g \in G$ a generator. Given an element $a \in G$, to solve the discrete logarithm problem is to find $n \in \mathbb{Z}$ such that

$$a = g^n.$$

This definition is analogous to the logarithm one can perform in fields such as $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}_p$.

We will only deal with (cyclic subgroups of) finite groups, and n can be seen modulo the order of the group. In this text we shall note $n = L_g(a)$, or $n = L(a)$ whenever we fix a generator.

2 Index calculus in $\mathbb{F}_p^\times$

Proposition 2.1. *The group $\mathbb{F}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic (of order $p-1$) for every prime p. If g is a generator of $\mathbb{F}_p^\times$ we call it a primitive root modulo p.*

This is a motivation for studying the discrete logarithm problem, and in fact the DLP for general groups (other than $\mathbb{Z}/N\mathbb{Z}$) is sometimes [1] refered to as the generalized DLP. Therefore the most basic setting for the DLP are the integers modulo p. We want to find n such that

$$a \equiv g^n \mod p.$$

1. Find a primitive root g modulo p.
2. Pick a *factor base* $B \subset \mathbb{Z}/p\mathbb{Z}$ (usually the factors are primes).
3. Find relations of the form
$$g^{k_i} \equiv \pm \prod_{b\in B} b^{r_{b,i}} \mod p, \ 0 \le i \lesssim |B|.$$
4. Translate these to relations of the form
$$k_i \equiv L(\pm 1) + \sum_{b \in B} r_{b,i} L(b) \mod p-1.$$
Notice that $L(1) \equiv 1$ and $L(-1) \equiv \frac{p-1}{2}$. This is a linear system in the unknowns $L(b),\ b \in B$. Solve it and store the results.
5. Find j such that $g^j a$ can be factored as product of elements in B,
$$g^j a \equiv \prod_{b\in B} b^{s_b} \mod p.$$
6. We find $n \equiv L(a) \equiv \sum_{b\in B} s_b L(b) - j \mod p-1$.

This method works because we are using a set of representatives $\{0, 1, \ldots, p-1\}$ of the group, which can be factored if we see them in $\mathbb{Z}$. This shows the importance of the chosen representation of our group. However, we still need efficient ways to perform steps (3) and (5).

Proposition 2.1 is also true in all this groups: $(\mathbb{Z}/4\mathbb{Z})^\times, (\mathbb{Z}/p^k\mathbb{Z})^\times, (\mathbb{Z}/2p^k\mathbb{Z})^\times$, with p an odd prime. But we have stated the method only for $\mathbb{F}_p$ because in the other settings, one is working in a ring with zero divisors instead of a field. We actually have a similar problem working modulo $p-1$, which can be solved via the Chinese Remainder Theorem (see [4] Sutherland's remark 11.4).

Another result will be important when we deal with elliptic curves:

Proposition 2.2. *Given a prime p and an integer $m \geq 1$, the group $\mathbb{F}_{p^m}^\times$ is cyclic.*

More sofisticated versions of index calculus exist for all finite fields.

3 Generic algorithms for the DLP

3.1 Baby step, Giant step

Assume now that G is finite of order $N := |G|$.

1. Fix $m \geq \sqrt{N}$ and compute g^m.
2. **Baby steps:** Compute and store g^i for $0 \leq i < m$.
3. **Giant steps:** Compute ag^{-jm} for $j = 0, 1, \dots, m-1$ until it matches one of the g^i.
4. If $g^i = ag^{-jm}$, then $n \equiv i + jm \mod N$.

As long as $m \geq \sqrt{N}$, we will find a match. Indeed, every expression $i + jm$ is and euclidian division, which will sweep every value less than or equal to $m^2 \geq N$.

This algorithm has the downside of requiring the storage of $\mathcal{O}(\sqrt{N})$ values.

3.2 Pollard's ρ

Let G be finite, $f\colon G \to G$ a certain function. If we pick $P_0 \in G$ and define

$$P_{i+1} := f(P_i), \ i \geq 0,$$

then by the pigeonhole principle there will be some $i_0 \neq j_0$ such that $P_{i_0} = P_{j_0}$. We try to exploit this fact to solve computational problems by choosing appropriate functions f.

3.2.1 Integer factoring

The algorithm's description for integer factoring is easier to understand than the setting for DLP, but the underlying principle is the same.

Let N be an integer we want to factor. Pick an initial $x_0 \in 0, 1, \dots, N-1$, usually 2, and let $f(x) := x^1 + 1 \mod N$.

Then for some $i_0 \neq j_0$, the numbers x_{i_0} and x_{j_0} will be congruent *modulo a prime p dividing N*, and hopefully not modulo N. Then $d := \gcd(x_{i_0} - x_{j_0}, N)$ is divisible by p, and a factor of N.

Using Floyd's Tortoise and Hare, we may write the following algorithm:

```
x := 2, y := 2, d := 1
while d=1:
        x := f(x)
        y := f(f(y))
        d := gcd(|x-y|, N)
return d
```

This method has the reputation for factoring the eighth Fermat number $F_8 = 2^{2^8} + 1$ in 1981.

3.2.2 Logarithms

We follow the exposition in Washington's book [5]. Start by dividing G into k disjoint subsets $S_1, S_2, \dots, S_k$ of approximately the same size (take $k \simeq 20$). Choose $2k$ random integers $r_i, s_i \mod N$, $i = 1, \dots, k$. Let

$$m_i := g^{r_i} a^{s_i},$$

and define $f(x) := x \cdot m_i$ if $x \in S_i$.

As the initial point, take $P_0 := g^{r_0} a^{s_0}$ for some integers $r_0, s_0 \mod N$. We need to keep track of the expression of $P_{j+1} = f(P_j)$ as product of powers of g and a. I.e., if $P_j = g^{u_j} a^{v_j}$, then

$$P_{j+1} = f(P_j) = P_j m_i = g^{u_j + r_i} a^{v_j + s_i}.$$

Once a loop is reached, we will have

$$g^\alpha a^\beta = g^A a^B \implies a^{\beta - B} = g^{A - \alpha} \implies a^{n(\beta - B)} = a^{A - \alpha}$$

and therefore $n(\beta - B) \equiv A - \alpha \mod N$. If we let $d := \gcd(\beta - B, N)$, then

$$n \equiv \frac{A-\alpha}{\beta - B} \mod \frac{N}{d},$$

and we only have to try a few possible values of n.

3.3 Pollard's λ

Pollard's λ algorithm is essentially a parallelized version of the rho algorithm. We pick r starting points $P_0^{(1)}, \ldots, P_0^{(r)}$, and perform random walks (in parallel) as in Pollard's ρ. Points satisfying some condition (called distinguished points) are reported to a central process. When two equal points with different expressions arrive to the central unit, the relation found can be used to find n, just as in the final stage of the ρ algorithm.

3.4 Pollard's Kangaroo Algorithm

This algorithm can be used to look for the order n in a (contiguous) subset $\{\alpha, \ldots, \beta\} \subset \mathbb{Z}/N\mathbb{Z}$. It is said that the ρ algorithm is faster if we are looking at the whole $\{0, 1, \ldots, N-1\}$ set.

Choose a set of integers $S \subset \mathbb{Z}$ (unrelated to α, β) and a function $f \colon G \to S$. Fix L, and compute the following finite sequence:

$$x_0 = g^\beta; \; x_{i+1} = x_i g^{f(x_i)} \text{ for } i = 0, 1, \ldots, N-1.$$

If we say $d = \sum_{i=0}^{N-1} f(x_i)$, then $x_N = x_0 g^d = g^{\beta + d}$.

Define two more sequences:

$$y_0 = a; \; y_{i+1} = y_i g^{f(y_i)} \text{ for } i = 0, 1, \ldots, N-1,$$

$$d_k = \sum_{i=0}^{k-1} f(y_i).$$

Note that $y_i = y_0 g^{d_i} = a g^{d_i}$.

We will stop computing terms of $\{y_i\}_i$ and $\{d_i\}_i$ whenever:

(a) $y_j = x_N$ for some j, in which case $g^{\beta+d} = a g^{d_j} \implies n \equiv \beta + d - d_j \mod N$; or

(b) $d_i > \beta - \alpha + d$, in which case the algorithm fails to find n. We may try again changing S, $\{\alpha, \ldots, \beta\}$, or the function f.

3.5 Pohlig-Hellman

Assume $G = \langle g \rangle$ is cyclic of order N, and that we know the factorization of N[1],

$$N = \prod_i q_i^{e_i}.$$

The idea is to find $n \mod q_i^{e_i}$ for each i, and then combine the information by means of the Chinese Remainder Theorem.

Fix $q^e || N$ (i.e., $q^e | N$ but $q^{e+1} \not| N$). Write n in base q, with $0 \leq n_i < q$:

$$n = n_0 + n_1 q + n_2 q^2 + \cdots,$$

we will find n_i successively. The following steps are performed (the algorithm can be written in a more compact way, but this exposition made in Washington's book [5] is clearer to understand):

1. First compute $T = \left\{ g^{j\left(\frac{N}{q}\right)}; \; 0 \leq j \leq q-1 \right\}$.

2. Compute $a^{N/q}$, which will equal some $g^{n_0(N/q)} \in T$.

3. If $e = 1$, stop. Otherwise continue.

4. Let $a_1 = a g^{-n_0}$.

5. Compute a_1^{N/q^2}, which will equal some $g^{n_1(N/q)} \in T$.

[1] We may perform the algorithm if we only know a few prime factors of N, and we will get *some* information, but we will only know the exact logarithm if we have the full factorization.

6. If $e = 2$, stop. Otherwise continue.
7. Suppose we have computed $n_0, n_1, \dots, n_{r-1}$ and $a_1, \dots, a_{r-1}$. Let $a_r = a_{r-1} g^{-n_{r-1} q^{r-1}}$.
8. Determine n_r such that $a_r^{N/q^{r+1}} = g^{n_r(N/q)} \in T$.
9. If $r = e - 1$, stop. Otherwise go back to step 7.

Sketch of Pohlig-Hellman proof: we have

$$a = g^n \implies a^{N/q} = g^{(N/q)(n_0+n_1q+n_2q^2+\dots)} = g^{n_0(N/q)} + N(n_1 + n_2q + n_3q^2 + \dots) = g^{n_0(N/q)}.$$

Similarly, $ag^{-n_0} = g^{n-n_0} \implies (ag^{-n_0})^{N/q^2} = g^{n_1(N/q)}$; and so on for $n_2, n_3, \dots$. We stop at $r = e - 1$, since N/q^{e+1} is no longer an integer, and we already know $n \mod q^e$.

Pohlig-Hellman works well if all primes dividing N are small. However, if q is a large prime dividing N, then it is difficult to list the elements in T, since $|T| = q$.

Therefore, for cryptographical applications based on the DLP, we should pick N to either

a) only have *large* prime factors, or

b) be a large prime.

4 The ECDLP

First, let's fix some notation. K will be a field, $\bar{K}$ its algebraic closure, $Gal(\bar{K}|K)$ the Galois group of $\bar{K}$ over K, and an element $\sigma \in Gal(\bar{K}|K)$ acts on an object (element of the field or point in a curve) x as a superindex, x^σ. $charK$ is the characteristic of K, and for any integer n, $charK \nmid n$ means that either $charK = 0$ or $charK > 0$ and it does not divide n.

E/K will be an elliptic curve defined over K (this is, an equation for the curve has its coefficients in K), and for every field $L \supseteq K$, $E(L)$ will be the set of L-rational points of E. We will denote the neutral element of the elliptic curve ∞. If $K = \mathbb{F}_q$ (the finite field with $q = p^r$ elements, p a prime), then $Frob_q$ denotes the Frobenius automorphism of E that raises each component of a point to its qth power.

4.1 Torsion points

Let E/K be an elliptic curve and let N be a positive integer. We are interested in

$$E[N] = \{P \in E(\bar{K});\ NP = \infty\},$$

wich is a subgroup of $E(\bar{K})$.

Theorem 4.1. *Let E/K be an elliptic curve and let N be a positive integer with $charK \nmid N$. Then*

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}.$$

If $charK = p > 0$ and $p|N$, let $N = p^r N'$ with $p \nmid N'$. Then

$$E[N] \cong \mathbb{Z}/N'\mathbb{Z} \oplus \mathbb{Z}/N'\mathbb{Z} \text{ or } \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N'\mathbb{Z}.$$

4.2 The Weil pairing

Let E/K be an elliptic curve and $charK \nmid N$. Then $E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$. We may fix a $\mathbb{Z}/N\mathbb{Z}$-basis $\{T_1, T_2\}$ of $E[N]$. We can express any point in this group by means of a linear combination of T_1, T_2. This would allow us to map pairs of points to a value via the determinant:

$$\det(aT_1 + bT_2, cT_1 + dT_2) = ad - bc.$$

This has the problem of not being galois invariant (i.e., if $\sigma \in Gal(\bar{K}|K)$, its action doesn't necessarily commute with det). We are going to define a pairing that does, in addition to having similar properties to the determinant.

Let $\mu_N = \{x \in \bar{K};\ x^N = 1\}$ be the group of Nth roots of unity in $\bar{K}$, which is cyclic of order N.

Theorem 4.2. *Let E/K be an elliptic curve, $charK \nmid N$. There exists a pairing*

$$e_N \colon E[N] \times E[N] \longrightarrow \mu_N,$$

*called the **Weil pairing**, satisfying the following properties:*

a) e_N is bilinear, this is, for all $S, S_1, S_2, T, T_1, T_2 \in E[N]$,

$$e_N(S_1+S_2,T) = e_N(S_1,T)e_N(S_2,T)$$
$$e_N(S,T_1+T_2) = e_N(S,T_1)e_N(S,T_2).$$

b) e_N is alternating: $e_N(T,T)=1$, and $e_N(S,T)=e_N(T,S)^{-1}$ for all $S,T \in E[N]$.

c) e_N is nondegenerate, meaning that if $e_N(S,T)=1$ for all $T \in E[N]$ then $S=\infty$ (and the same happens if we consider the other variable).

d) e_N is compatible with the Galois action, for all $\sigma \in Gal(\bar{K}|K)$, $S,T \in E[N]$,

$$e_N(S,T)^\sigma = e_N(S^\sigma, T^\sigma).$$

Corollary 4.3. *Let $\{T_1,T_2\}$ be a basis of $E[N]$. Then $e_N(T_1,T_2)$ is a primitive Nth root of unity. Moreover, if $E[N] \subset E(K)$, then $\mu_N \subset K$.*

Proof. Let $\zeta = e_N(T_1,T_2)$, $\zeta^d = 1$ for some d. Then properties (1) and (3) of the pairing imply

$$e_N(T_1,dT_2) = \zeta^d = 1$$
$$e_N(T_2,dT_2) = e_N(T_2,T_2)^d = 1.$$

For all $S \in E[N]$, $S = aT_1 + bT_2$, and so

$$e_N(S,dT_2) = e_N(T_1,dT_2)^a e_N(T_2,dT_2)^b = 1,$$

wich implies $dT_2 = \infty$. Therefore $N|d$, and so ζ is a primitive Nth root of unity.

Now let $\sigma \in Gal(\bar{K}|K)$. If $E[N] \subset E(K)$ then $T_1, T_2 \in E(K)$, and we have

$$\zeta = e_N(T_1,T_2) = e_N(T_1^\sigma, T_2^\sigma) = e_N(T_1,T_2)^\sigma = \zeta^\sigma.$$

Therefore (as $charK \nmid N$) $\zeta \in K \implies \mu_N \subset K$. □

We won't need this, but a consequence of the last statement is that $E[N] \not\subset E(\mathbb{Q})$ for $n \geq 3$.

4.3 Divisors and construction of the Weil pairing

In the following we will introduce the necessary tool to construct the Weil pairing and to prove its properties.

Definition 4.4. *Let E/K be an elliptic curve. For each point $P \in E(\bar{K})$, define a formal symbol $[P]$. The group of divisors of E is*

$$Div(E) := \bigoplus_{P \in E(\bar{K})} [P]\mathbb{Z} = \{\sum_i a_i[P_i] \text{ finite sum; } a_i \in \mathbb{Z}\}.$$

We define the *degree* and *sum* of a divisor $D = \sum_i a_i[P_i]$ as

$$deg(D) = \sum_i a_i \in \mathbb{Z}$$
$$sum(D) = \sum_i a_i P_i \in E(\bar{K}).$$

Both maps are morphisms. The kernel of $sum(\cdot)$ is the degree-zero-part of the divisor group of E, denoted $Div^0(E)$. The restricted map

$$sum \colon Div^0(E) \to E(\bar{K})$$

is surjective, because $sum([P]-[\infty]) = P$.

If f is a nonzero function in the function field of the curve, $f \in \bar{K}(E)^\times$, we define

$$div(f) := \sum_{P \in E(\bar{K})} ord_P(f)[P] \in Div^0(E).$$

This is actually a (zero-degree) divisor because of the following:

Proposition 4.5. *Let C/K be a smooth curve and $f \in \bar{K}(C)^\times$. Then there are only finitely many points of C at which f has a pole or zero; and if f has no poles, then $f \in \bar{K}$. Finally, $deg(div(f)) = 0$.*

We shall define the Picard group of E and it's zero-degree part:

$$Pic(E) := {}^{Div(E)}\!\big/_{div(\bar{K}(E)^\times)}$$
$$Pic^0(E) := {}^{Div^0(E)}\!\big/_{div(\bar{K}(E)^\times)}.$$

The following two results say that the group $E(\bar{K})$ is isomorphic to $Pic^0(E)$.

Theorem 4.6. *Let E be an elliptic curve. Let D be a divisor on E with $deg(D) = 0$. Then there is a function f on E with $div(f) = D$, if and only if $sum(D) = \infty$.*

Corollary 4.7. *The map sum: $Pic^0(E) \to E(\bar{K})$ is an isomorphism of groups.*

To construct the pairing, we need a result about rational maps between curves.

Theorem 4.8. *Let $\phi\colon C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Assume now $charK \nmid n$, and so $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Let's construct the Weil pairing. Fix $T \in E[n]$. By Theorem 4.6 there exists $f \in \bar{K}(E)$ such that

$$div(f) = n[T] - n[\infty].$$

Choose $T' \in E[n^2]$ such that $nT' = T$ (the map $[n]$ is surjective). There exists a function g such that

$$div(g) = \sum_{R \in E[n]} [T' + R] - [R],$$

because its sum is $n^2T' = nT = \infty$. The function g does not depend on the choice of T', because any two choices for T' differ by an element $R \in E[n]$. Therefore we can also write

$$g = \sum_{nT''=T} [T''] - \sum_{nR=\infty} [R].$$

Consider now the map $f \circ [n]$. Then for every $P = T' + R$, $nP = T$; and obviously $nR = \infty$ (for all $R \in E[n]$). Therefore

$$div(f \circ [n]) = n\left(\sum_R [T' + R]\right) - n\left(\sum_R [R]\right) = div(g^n).$$

Multiplying by a constant in $\bar{K}^\times$, we may assume $f \circ [n] = g^n$.

Let $S \in E[n]$. Then for every $X \in E(\bar{K})$,

$$g(X + S)^n = f(n(X + S)) = f(nX) = g(X)^n.$$

Therefore $g(X + S)/g(X)$ is an nth root of unity. In particular, this quotient takes values from the finite set μ_n, and so does the morphism

$$\begin{aligned} E &\to \mathbb{P}^1 \\ X &\mapsto \frac{g(X+S)}{g(X)}. \end{aligned}$$

Thus the map must be constant[2].

We can define the Weil pairing

$$e_n(S,T) := \frac{g(X+S)}{g(X)},$$

independent of X. This freedom in the choice of X will be used in proving the properties of the pairing. Note that although g may vary by a constant in $\bar{K}^\times$, this doesn't affect the definition of the pairing. The function g *does* depend on T, we could also write f_T and g_T.

We are ready to prove the properties of the Weil pairing.

[2] This kind of reasoning is introduced in the second chapter of Silverman's AEC[3].

a) **Bilinear**. For the first variable, we have

$$e_n(S_1+S_2,T)=\frac{g(X+S_1+S_2)}{g(X)}=\frac{g(X+S_1+S_2)}{g(X+S_1)}\frac{g(X+S_1)}{g(X)}=e_n(S_1,T)e_n(S_2,T).$$

For the second, let T_1,T_2, $T_3=T_1+T_2$, and consider the functions f_1,f_2,f_3,g_1,g_2,g_3 as constructed before. Also, consider the function h such that

$$div(g)=[T_3]-[T_1]-[T_2]+[\infty].$$

Then $div\left(\frac{f_3}{f_1f_2}\right)=ndiv(h) \implies \exists c\in \bar{K}^\times$ such that

$$f_3=c\cdot f_1\cdot f_2\cdot h^n.$$

Composing with the map $[n]$, using $g_i^n=f_n\circ[n]$ and taking nth roots, we get $g_3=c'\cdot g_1\cdot g_2\cdot(h\circ[n])$. Therefore

$$\begin{aligned}e_n(S,T_1+T_2)=\frac{g_3(X+S)}{g_3(X)}&=\frac{g_1(X+S)g_2(X+S)h(nX+nS)}{g_1(X)g_2(X)h(nX)}\\&=\frac{g_1(X+S)g_2(X+S)}{g_1(X)g_2(X)}=e_n(S,T_1)e_n(S,T_2).\end{aligned}$$

b) **Alternating**. By last property,

$$e_n(S+T,S+T)=e_n(S,S)e_n(S,T)e_n(T,S)e_n(T,T).$$

This implies we only need to show $e_n(T,T)=1$ for all $T\in E[n]$.

Let $\tau_P\colon E\to E$ be the translation by $P\in E$ map (it is a rational map, but not an isogeny, unless $P=\infty$ and $\tau_P=id_E$). Then

$$div\left(\prod_{i=0}^{n-1}f\circ\tau_{iT}\right)=n\sum_{i=0}^{n-1}[1-iT]-[-iT]=0$$

$\implies \prod_{i=0}^{n-1}f\circ\tau_{iT}$ is constant, and if $T'\in E$ is such that $nT'=T$, then $\prod_{i=0}^{n-1}g\circ\tau_{iT'}$ is also constant. Therefore we may apply it to $X+T'$ and X, and

$$\prod_{i=0}^{n-1}g(X+(1+i)T')=\prod_{i=0}^{n-1}g(X+iT'),$$

which cancelling terms gives us $g(X+nT')=g(X)$. Thus

$$\frac{g(X+T)}{g(X)}=1.$$

c) **Non-degenerate**. Assume we have $g(X+S)=g(X)$ for all $S\in E[n]$. Then there exists $h\in\bar{K}(E)^\times$ such that $g=h\circ[n]$. Raising to n we have $(h\circ[n])^n=g^n=f\circ[n]$. Since $[n]$ is surjective on $E(\bar{K})$, we have $f=h^n$. Therefore, $ndiv(h)=div(f)=n[T]-n[\infty]$, and $div(h)=[T]-[\infty]\implies T=\infty$.

Using (b) we get the non-degeneracy in the first variable.

d) **Galois invariant**. Let $\sigma\in Gal(\bar{K}|K)$. If f,g are the functions constructed fixing T, then f^σ,g^σ are the ones for T^σ. For instance,

$$div(f^\sigma)=n[T^\sigma]-n[\infty].$$

We have

$$\sigma(e_n(T,S))=\sigma\left(\frac{g(X+S)}{g(X)}\right)=\frac{g^\sigma(X^\sigma+S^\sigma)}{g^\sigma(X^\sigma)}=e_n(S^\sigma,T^\sigma).$$

□

4.4 The MOV attack

Let $K = \mathbb{F}_q$ be a finite field, consider an elliptic curve E/K. The use of this algorithm (by Menezes, Okamoto and Vanstone [2]) is to solve discrete logarithms $Q = kP$ when the base point P has order N coprime with the characteristic. This is done by translating the ECDLP to a DLP in a finite extension of the field via the Weil pairing e_N.

First we look at a characterization of the points in the cyclic group generated by a point. The proof will give us an idea for understanding the attack.

Lemma 4.9. *Given $Q \in E(\mathbb{F}_q)$, there exists k such that $Q = kP \iff NQ = \infty$ and $e_N(P,Q) = 1$.*

Proof. If $Q = kP$, then $NQ = kNP = \infty$. Also, $e_N(P,Q) = e_N(P,kP) = e_N(P,P)^k = 1$.

Conversely, assume $NQ = \infty$ and $e_N(P,Q) = 1$. Then $Q \in E[N]$. Because $\gcd(N,q) = 1$, we have $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$, let $R \in E[N]$ be such that $\{P, R\}$ is a base. Then $Q = aP + bR$. We have

$$1 = e_N(P,Q) = e_N(P,P)^a e_N(P,R)^b = \zeta^b,$$

which implies $N|b$ and so $bR = \infty$. Therefore $Q = aP$. □

Let's describe now the MOV attack. Choose m so that $E[N] \subset E(\mathbb{F}_{q^m})$. Such an m exists, because $E[N]$ is finite and $\bar{F}_q = \bigcup_{j\geq 1} F_{q^j}$. Then $\mu_N \subset \mathbb{F}_{q^m}$. The algorithm is the following:

1. Choose a random point $T \in E(\mathbb{F}_{q^m})$.
2. Compute the order M of T.
3. Let $d = \gcd(M,N)$, and let $T_1 = \frac{M}{d}T$, which has order d, which divides N. Thus $T_1 \in E[N]$.
4. Compute $\zeta_1 = e_N(P,T_1)$ and $\zeta_2 = e_N(Q,T_1)$ ($Q = kP \implies \zeta_2 = \zeta_1^k$). Then both ζ_1 and ζ_2 lie in $\mu_d \subseteq \mu_N \subset \mathbb{F}_{q^m}^\times$.
5. Solve the discrete logarithm problem $\zeta_2 = \zeta_1^k$ in $\mathbb{F}_{q^m}^\times$. This will give $k \mod d$.
6. Repeat with random points T until the least common multiple of the various d's is N. This determines $k \mod N$.

References

[1] Scott Vanstone Alfred Menezes Paul van Oorschot. *Handbook of applied cryptography.* 1st ed. Discrete Mathematics and Its Applications. CRC Press, 1996. ISBN: 9780849385230,0849385237.

[2] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. “Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field”. In: *Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing.* STOC '91. New Orleans, Louisiana, USA: ACM, 1991, pp. 80–89. ISBN: 0-89791-397-3. DOI: 10.1145/103418.103434. URL: http://doi.acm.org/10.1145/103418.103434.

[3] Joseph H. Silverman. *The arithmetic of elliptic curves.* 2nd ed. Graduate Texts in Mathematics 106. Springer-Verlag New York, 2009. ISBN: 0387094938,9780387094939.

[4] Andrew Sutherland. *18.783 Elliptic Curves.* Massachusetts Institute of Technology: MIT OpenCourseWare. Spring 2017. URL: https://ocw.mit.edu. License: Creative Commons BY-NC-SA.

[5] Lawrence C. Washington. *Elliptic curves: number theory and cryptography.* 2nd ed. Discrete Mathematics and Its Applications. Chapman and Hall/CRC, 2008. ISBN: 1420071467,9781420071467,9781420071474.