Attacks on Discrete-Log Cryptography on Elliptic Curves

By

Khai Dong

* * * * * * * * *

Submitted in partial fulfillment of the requirements for

Honors in the Department of Mathematics

Union College

February 27, 2024

ABSTRACT

KHAI DONG Attacks on Discrete-Log Cryptography on Elliptic Curves.

Department of Mathematics, February 27, 2024.

ADVISOR: HATLEY, JEFFREY

This paper discusses the M.O.V. attack [2], which uses the Weil Pairing to solve a discrete logarithm problem over a specific elliptic curve E by reducing it to a discrete logarithm problem over a finite field $\mathbb{F}_{p^m}$ for some $m \in \mathbb{N}$. The effectiveness of this attack relies on efficiently solving discrete logarithm problems over the field $\mathbb{F}_{p^m}$, which requires m to be sufficiently small. A large portion of this paper is dedicated to proving the existence of the Weil Pairing, an alternating, bilinear, non-degenerate, and Galois invariant pairing, which is the foundation of the M.O.V. attack.

NOTATION

We shall use the following notations throughout this paper:

- $\mathbb{N} = \{1, 2, 3, \dots\}$, being the set of natural numbers
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, being the set of integers
- $\mathbb{Q}$, being the set of rationals
- $[n] := \{0, 2, 3, \dots, n-1\}$

Contents

1. INTRODUCTION

This paper discusses the M.O.V. attack [2], which uses the Weil Pairing to solve a discrete logarithm problem over a specific elliptic curve E by reducing it to a discrete logarithm problem over a finite field $\mathbb{F}_{p^m}$ for some $m \in \mathbb{N}$. The effectiveness of this attack relies on efficiently solving discrete logarithm problems over the field $\mathbb{F}_{p^m}$, which requires m to be sufficiently small.

A large portion of this paper is dedicated to proving the existence of the Weil Pairing, an alternating, bilinear, non-degenerate, and Galois invariant pairing, which is the foundation of the M.O.V. attack.

In Section 2, we provide background about elliptic curves. Section 3 provides some general information on discrete logarithm problems and shows how such problems can be formulated using elliptic curves. Section 3 also provides some details on Index Calculus, a method to solve discrete logarithm problems over finite fields. Finally, Section 4 proves the existence of the Weil Pairing, describes how this pairing can be utilized to solve discrete logarithm problems over elliptic curves, and shows examples of these attacks.

2. ELLIPTIC CURVES

Definition 1. Let $\mathbb{F}$ be a field. An **elliptic curve** E over $\mathbb{F}$ is the graph of an equation of the form

$$E : y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{F}$ are constants and $y^2 = x^3 + Ax + B$ is non-singular. Geometrically, this means the graph of E has no cusps, self-intersections, or isolated

points.

The equation $y^2 = x^3 + Ax + B$ is referred to as the **Weierstrass form** for an elliptic curve.

By convention, if not stated otherwise, we consider an elliptic curve to be defined over $\mathbb{Q}$, the set of rational numbers. Moreover, due to elliptic curve origin in projective geometry, we consider the point ∞ to be on any elliptic curve E. Intuitively, it is useful to think of ∞ as a point on the top or at the bottom of the y-axis.

Definition 2. Let $\mathbb{F}$ be a field and E be an elliptic curve over $\mathbb{F}$. We define

$$E(\mathbb{F}) = \{\infty\} \cup \{(x, y) \in (\mathbb{F})^2 : y^2 = x^3 + Ax + B\}.$$

2.1. **ADDITION OF POINTS ON ELLIPTIC CURVES.** We first demonstrate that with 2 points $P_1, P_2 \in E(\mathbb{Q})$, we can generate a third point $P_3 \in E(\mathbb{Q})$ (Figure 2.1). We do this by drawing the line L through P_1 and P_2. If $P_1 = P_2$, we take the tangent line at P_1 (or equivalently, P_2) as L. Then, if L cuts E at a third point P_3', (for ease of notation, we call this point $P_3' = P_1P_2$). We then reflect P_3' across the x-axis to obtain P_3. Otherwise, if L is parallel to the y-axis, $P_3 = \infty$.

In more detail, let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and

$$E : y^2 = x^3 + Ax + B. \tag{1}$$

Firstly, we assume $P_1 \neq P_2$ and that neither points are ∞ (points P_1 and P_2 have rational coordinates). We have 2 cases

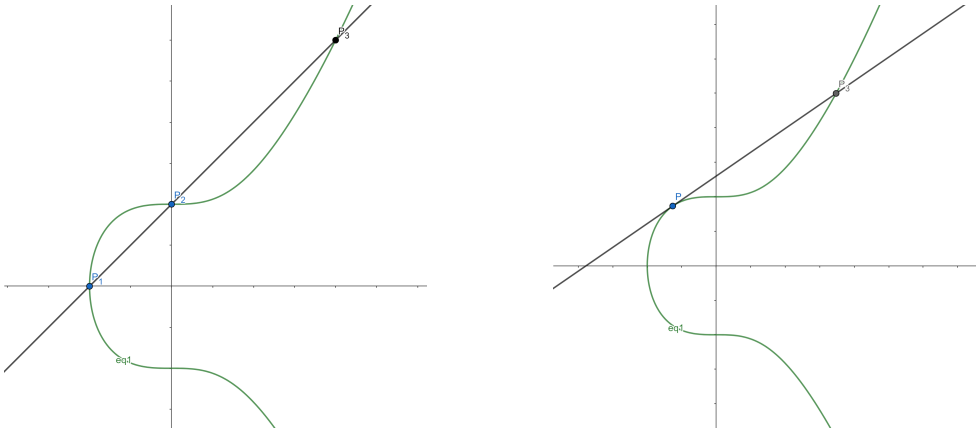

FIGURE 2.1. Adding Points on an Elliptic Curve

- If $x_2 \neq x_1$, then line L through P_1 and P_2 has the slope

$$m = \frac{y_2 - y_1}{x_2 - x_1},$$

and the equation of line L is

$$y = m(x - x_1) + y_1. \tag{2}$$

We then substitute the Equation 2 into Equation 1 to get

$$\begin{aligned} &(m(x - x_1) + y_1)^2 = x^3 + Ax + B \\ \iff &x^3 - m^2x^2 + (A + 2m^2x_1 - 2my_1)x \\ &\qquad + (B + 2mx_1y_1 - m^2x_1^2 - y_1^2) = 0. \end{aligned}$$

Solving this cubic polynomial, we obtain P_1, P_2, and $P_3' = (x', y')$ where

$$x' = m^2 - x_1 - x_2 \quad \text{and} \quad y' = m(x' - x_1) + y_1.$$

We reflect P_3' across the x-axis to obtain $P_3 = (x_3, y_3)$ where

$$x_3 = m^2 - x_1 - x_2 \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1.$$

We remarked that in this case, since P_1 and P_2 have rational coordinates and the slope of line L is rational, P_3' and P_3 have rational coordinates.

- If $x_1 = x_2$, then L is a vertical line through P_1 and P_2, which will intersect E at $P_3 = \infty$.

Then, we assume $P_1 = P_2 = (x_1, y_1) \neq \infty$. We choose L to be the tangent line at P_1. To find L, we use implicit differentiation on Equation 1:

$$\begin{aligned} & y^2 = x^3 + Ax + B \\ \implies & \frac{d}{dx}(y^2) = \frac{d}{dx}(x^3 + Ax + B) \\ \iff & 2y\frac{dy}{dx} = 3x^2 + A \iff \frac{dy}{dx} = \frac{3x^2 + A}{2y}. \end{aligned}$$

If $y_1 \neq 0$, substituting P_1 into $\frac{dy}{dx}$, we have the slope of L,

$$m = \frac{dy}{dx}(P_1) = \frac{3x_1^2 + A}{2y_1},$$

and the equation of L being

$$y = m(x - x_1) + y_1.$$

Following the same procedure as before, we obtain $P_3 = (x_3, y_3)$ where

$$x_3 = m^2 - x_1 - x_2 \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1.$$

Otherwise, if $y_1 = 0$, the line is vertical and $P_3 = \infty$.

Finally, we consider the case when either P_1 or P_2 is ∞. If $P_1 = \infty$ and $P_2 \neq \infty$. The line L through P_1 and P_2 is a vertical line that cuts E at P_2' which is the reflection of P_2 across the x-axis. Reflecting P_2' across the x-axis gives $P_3 = P_2$. Similarly, if $P_1 \neq \infty$ and $P_2 = \infty$, $P_3 = P_1$. If $P_1 = P_2 = \infty$, we define $P_3 = \infty$.

We remark that throughout this section, E can be over any field $\mathbb{F}$ since the procedure remains the same as a field $\mathbb{F}$ supports addition, subtraction, multiplication, and division by definition, which means our procedure above holds. Hence, we formally define this binary operation on P_1 and P_2 as follows:

Definition 3. Let $\mathbb{F}$ be a field and E be an elliptic curve over $\mathbb{F}$. Suppose $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are points on $E(\mathbb{F})$. If $P_1 \neq \infty$ and $P_2 \neq \infty$, we define $P_1 +_E P_2 = P_3 = (x_3, y_3)$ as follows:

- If $x_1 \neq x_2$, then

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{and } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

- If $x_1 = x_2$ and $y_1 \neq y_2$, then $P_3 = \infty$.
- If $P_1 = P_2$ and $y_1 \neq 0$, then

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{and } m = \frac{3x_1^2 + A}{2y_1}.$$

- If $P_1 = P_2$ and $y_1 = 0$, then $P_3 = \infty$

Otherwise, if $P_1 = \infty$, $P_3 = P_1$, and if $P_2 = \infty$, $P_3 = P_2$.

If the elliptic curve is clear from context, we denote $P_1 + P_2 = P_3$ instead.

Moreover, we remark that $+_E$ is commutative since the line L through P_1 and P_2 is the same regardless of the order of P_1 and P_2. This can trivially be proven by looking at the formula to compute P_3 in the definition.

2.2. THE GROUP $E(\mathbb{F})$.

Theorem 1. *Let $\mathbb{F}$ be a field and E be an elliptic curve over $\mathbb{F}$. The set*

$$E(\mathbb{F}) = \{\infty\} \cup \{(x, y) \in \mathbb{F}^2 : y^2 = x^3 + Ax + B\}.$$

forms an abelian group under the binary operation $+_E$.

Proof. Since $+_E$ is commutative, we only have to show that $E(\mathbb{F})$ is a group.
(closure) The closure condition is trivially true by looking at the equation of P_3 in the definition of $+_E$ as $\mathbb{F}$, being a field, is closed under addition, subtraction, multiplication, and division.
(identity) ∞ is the identity of the group by definition.
(inverse) Let $P = (x, y) \in E(\mathbb{F})$ be an arbitrary point. Let $P' = (x, -y)$. If $y = 0$, then $P = P'$. Thus, $P + P' = \infty$. Otherwise, P and P' share the x-coordinate and $y \neq 0$. Thus, $P + P' = \infty$. Therefore, in all cases, P' is the inverse of P, thus, proved the inverse existence.
(associativity) We omit this proof due to its algebra-intensive nature. The full proof can be found in [5, Chapter 2.4]. □

2.3. TORSION POINTS.

Definition 4. Let E be an elliptic curve over a field $\mathbb{F}$. Let $n \in \mathbb{N}$. We define the set of n-torsion points of E as

$$E[n] = \{P \in E(\overline{\mathbb{F}}) : nP = \infty\},$$

where $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}$.

We note that $E[n]$ contains points with coordinates in $\overline{\mathbb{F}}$ and not just in $\mathbb{F}$.

Theorem 2. *Let E be an elliptic curve over a field $\mathbb{F}$ and $n \in \mathbb{N}$. If* $\mathrm{char}\mathbb{F} \nmid n$ *or* $\mathrm{char}\mathbb{F} = 0$*, then*

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

Due to the proof's complex nature, we omit the proof for Theorem 2 in this paper. It can be found in [5, Section 3.2].

2.4. **DIVISORS.**

Definition 5. Let E be an elliptic curve over a field $\mathbb{F}$. For each point $P \in E(\overline{\mathbb{F}})$, we define a formal symbol $[P]$. Then, we define a **divisor** D on E as the formal sum

$$D = \sum_i a_i[P_i],$$

where $a_i \in \mathbb{Z}$ and $P_i \in E(\overline{\mathbb{F}})$. Hence, a divisor is an element of a free abelian group generated by points in $E(\overline{\mathbb{F}})$. We denote this group $\mathrm{Div}(E)$.

Definition 6. Let E be an elliptic curve over a field $\mathbb{F}$. Let

$$D = \sum_i a_i[P_i]$$

be a divisor on E. We define the **degree** and **sum** of the divisor D, respectively, as follows:

$$\deg(D) = \sum_i a_i \qquad \text{and} \qquad \mathrm{sum}(D) = \sum_i a_i P_i.$$

We note that the sum function takes sums of points on the elliptic curve E as defined in Section 2.1.

Definition 7. Let E be an elliptic curve over a field $\mathbb{F}$. We define a **function** f on E as a function $f(x, y) \in \overline{\mathbb{F}}(x, y)$ that is defined in at least 1 point on $E(\overline{\mathbb{F}})$. The function f takes values in $\overline{\mathbb{F}} \cup \{\infty\}$.

Definition 8. Let E be an elliptic curve over a field $\mathbb{F}$, f be a function on E, and $P \in E(\overline{\mathbb{F}})$. Then, f is said to have a **zero** at P if $f(P) = 0$ and to have a **pole** at P if $f(P) = \infty$.

However, we would want to know more refined information about the poles and zeros of a function f, particularly, the order of the zeros or poles.

Definition 9. Let E be an elliptic curve over a field $\mathbb{F}$. Let $P \in E(\overline{\mathbb{F}})$. We can prove that there exists a function u_P where $u_P(P) = 0$, called a **uniformizer** at P such that every function f can be written as

$$f = u_P^r g, \qquad \text{where } r \in \mathbb{Z} \text{ and } g(P) \neq 0, \infty.$$

We define the **order** of f at P by $\mathrm{ord}_P(f) = r$.

The way to choose a uniformizer for point P is described in [5, Section 11.1], and thus proven the existence of u_P for all $P \in E(\overline{\mathbb{F}})$.
We remarked that if f has a zero at P, $\mathrm{ord}_P(f) > 0$. If f has a pole at P, then $1/f$ has a zero at P. Hence, if f has a pole at P, then $\mathrm{ord}_P(f) < 0$. Otherwise, if f has neither zero nor pole at P, then $\mathrm{ord}_P(f) = 0$.

Now we introduce a special type of divisor.

Definition 10. Let E be an elliptic curve over a field $\mathbb{F}$ and f be a function on E. We define the **divisor of** f to be

$$\text{div}(f) = \sum_{P \in E(\overline{\mathbb{F}})} \text{ord}_P(f)[P] \in \text{Div(E)}.$$

We also call a divisor of this form a **principal divisor**.

The following results are particularly helpful in this paper. However, we omit the proofs of these statements due to their complexity. These proofs can be found in [5, Section 11.1].

Proposition 1. *Let E be an elliptic curve over a field $\mathbb{F}$ and f be a non-zero function on E. Then,*

- *f has only finitely many zeros and poles.*
- $\deg(\text{div}(f)) = 0$.
- *If f has no zeros or poles, f is a constant.*

Theorem 3. *Let E be an elliptic curve over a field $\mathbb{F}$. Let D be a divisor on E where* $\deg(D) = 0$. *Then, there exists a function f on E with* $\text{div}(f) = D$ *if and only if* $\text{sum}(\text{div}(f)) = \infty$.

For example, referring back to Section 2.1, given points P_1, P_2 on E and a line L through P_1 and P_2, we notice that P_3', the third intersection between L and E, is $-(P_1 + P_2)$. Thus, $\text{sum}(\text{div}(L)) = P_1 + P_2 - (P_1 + P_2) = \infty$.

3. DISCRETE LOGARITHM PROBLEMS

Definition 11. Let G be a group. Let $a, b \in G$ such that there exists $k \in \mathbb{N}$ such that

$$a^k = b.$$

The **discrete logarithm problem** is to find k. Since by the Lagrange Theorem, $a^{|G|} = 1$, the answer k should be regarded as defined $\mod |G|$.

Classically, the discrete logarithm problem is defined on the multiplicative group $\mathbb{F}_q^\times$ of a finite field. However, any group G would work in defining these problems. Classically, to ensure a full range of possible values for k, we choose G to be cyclic and a to be a generator of G; however, this may not required. In cryptography, the discrete logarithm problems have several applications [5, Chapter 6]; the security of many cryptosystems depends on the hardness of discrete logarithm problems. Over the years, various methods to solve these discrete logarithm problems have been developed to give insights into the hardness of such problems. These methods, however, only work in specific conditions or are not efficient.

3.1. **ELLIPTIC-CURVE CRYPTOGRAPHY.** Since $E(\mathbb{F})$ is a group (by Theorem 1), we can define a discrete logarithm problem with $G = E(\mathbb{F})$. Hence, we can reformulate a discrete logarithm problem over an elliptic curve E as follows:

Definition 12. Let $\mathbb{F}_q$ be a finite field and E be an elliptic curve. Let $P, Q \in E(\mathbb{F}_q)$ such that there exists k such that $kP = Q$ (written additively by convention). A discrete logarithm problem over $E(\mathbb{F}_q)$ is to find k.

We remarked that this cryptographic scheme only requires us to know the field $\mathbb{F}_q$ (which can be described by an integer q), the elliptic curve E (which can be described by 2 integers A, B in Weierstrass form), and 2 points P, Q in $E(\mathbb{F}_q)$.

3.2. **THE INDEX CALCULUS.** This section introduces Index Calculus: a method that can efficiently solve discrete logarithm problems over finite fields. The method is particularly useful in breaking discrete logarithm cryptography over elliptic curves as such a problem can be reduced to a discrete logarithm problem over a finite field (Section 4).

Let $\mathbb{F}_q$ be a finite field where $q = p^n$ for some prime p. Let g be a generator of $\mathbb{F}_q^\times$; that is for every $h \in \mathbb{F}_q^\times$, there exists $k \in \mathbb{Z}_{q-1}$ where $g^k = h$. Let $h \in \mathbb{F}_q^\times$ be arbitrary. We define $L(h) = k$ being the discrete logarithm of h with respect to g and q; that is $g^{L(h)} = h \mod (q-1)$. Then, suppose we have $h_1, h_2 \in \mathbb{F}_q$. Then, we have

$$h_1 h_2 = g^{L(h_1)} g^{L(h_2)} = g^{L(h_1)+L_(h_2)}.$$

This means $L(h_1h_2) = L(h_1) + L(h_2) \mod (q-1)$. Therefore, if we pre-compute the discrete logarithm L for a sufficiently large set of $\{h_i\}_i \in [n]$ where $h = \prod_{i \in I \subseteq [n]} h_i^{\alpha_i}$ for some I and integers α_i's, we can compute

$$L(h) = \sum_{i \in I \subseteq [n]} \alpha_i L(h_i) \mod (q-1)$$

for any $h \in \mathbb{F}_q$. This analysis is the basis for the Index Calculus, where we pre-compute a set of $\{L(h_i)\}_{i \in [n]}$ to compute the desired $L(h)$.

In the case of field $\mathbb{F}_q$ where q is a prime, we choose the $\{h_i\}$ to be a set of small primes. However, we are more interested in the case where $q = p^n$, where p is a prime and $n \geq 2$ since solving a discrete logarithm problem over an elliptic curve using the pairings would require solving discrete logarithm

problems over $\mathbb{F}_{p^n}$ with $n \geq 2$ being the minimum.

We observe that elements of $\mathbb{F}_{p^n}$ are roots of $f(x) = x^{p^n} - x$ in the closure of $\mathbb{F}_p$. Let ω as a root of f. We have that all element of $\mathbb{F}_{p^n}$ has the form $\sum_{i=0}^{n-1} a_i \omega^i$ where $a_i \in \mathbb{F}_p$. This means we can choose $\{h_i\}$ to be a set of small primes in $\mathbb{F}_p$, ω, and their products. For more details, please refer to [1, p. 18]. We remark that by this construction, larger fields would require more time to perform Index Calculus, and this method might fail if the desired h can not factor into powers of elements of $\{h_i\}$.

4. THE M.O.V. ATTACK

In general, the M.O.V. (Menezes-Okamoto-Vanstone) attack [2] reduces the problem of discrete logarithm over $E(\mathbb{F}_p)$ to one in $\mathbb{F}_q$ where $q = p^m$ and m depends on $E(\mathbb{F}_p)$. As long as $\mathbb{F}_q$ is not too much larger than $\mathbb{F}_p$, we can efficiently solve the simpler discrete log problem over $\mathbb{F}_q$. To achieve such a reduction, we use the Weil Pairing.

4.1. **THE WEIL PAIRINGS.**

Definition 13. Let $\mathbb{F}$ be a field and $n \in \mathbb{N}$ such that $\text{char}\mathbb{F} \nmid n$. Then, we define

$$\mu_n = \{x \in \overline{\mathbb{F}} : x^n = 1\}$$

to be the group of n^{th} roots of unity in $\overline{\mathbb{F}}$. Since $\text{char}\mathbb{F} \nmid n$, $x^n = 1$ has exactly n roots in $\overline{\mathbb{F}}$. Any generator ζ of μ_n is called a **primitive n^{th} root of unity**.

Theorem 4. *Let $\mathbb{F}$ be a field, $n \in \mathbb{N}$, and E be an elliptic curve over $\mathbb{F}$. Assume* $\text{char}\mathbb{F} \nmid n$. *Then, there exists a pairing*

$$e_n : E[n] \times E[n] \to \mu_n,$$

called a ***Weil pairing****, that satisfied the following properties*

(1) e_n *is bilinear. This means that*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

and

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

where $S, T, S_1, S_2, T_1, T_2 \in E[n]$.

(2) e_n *is non-degenerate; that is, if* $e_n(S, T) = 1$ *for all* $T \in E[n]$*, then* $S = \infty$ *and if* $e_n(S, T) = 1$ *for all* $S \in E[n]$*, then* $T = \infty$.

(3) $e_n(T, T) = 1$ *for all* $T \in E[n]$.

(4) $e_n(T, S) = e_n(S, T)^{-1}$ *for all* $S, T \in E[n]$.

(5) $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ *for all automorphism* σ *of* $\overline{\mathbb{F}}$ *s.t.,* $\sigma(A) = A$ *and* $\sigma(B) = B$.

(6) $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$ *for all endomorphism* α *of* E.

It's worth noting that the Weil Pairing is a particularly useful tool in studying elliptic curves as it is an alternating, non-degenerate, and bilinear pairing. This resembles the determinant of matrices. However, what makes the Weil pairing useful in this paper is that it is Galois invariant (5).

We first construct the pairing $e_n : E[n] \times E[n] \to \mu_n$. Let $S, T \in E[n]$. By Theorem 3, there exists a function f_T such that

$$\operatorname{div}(f_T) = n[T] - n[\infty]$$

since $\deg(n[T] - n[\infty]) = n - n = 0$ and $\text{sum}(n[T] - n[\infty]) = nT - n\infty = \infty$ since $T \in E[n]$. We consider the function $(f_T \circ n)(P) = f_T(nP)$. We know that f_T has a zero of order n at T and a pole of order n at ∞, by definition. We notice that $nP = \infty$ if and only if $P \in E[n]$, by definition of $E[n]$. Hence, $f_T \circ n$ has a pole of order n at any P in $E[n]$. We want to find all zeros of $f_T \circ n$. We have that $(f_T \circ n)(P) = 0$ if and only if $nP = T \iff n^2P = nT = \infty$. Thus, $(f_T \circ n)(P) = 0$ if and only if $P \in E[n^2]$.

Lemma 1. *Let $P \in E[n^2]$. If $(f_T \circ n)(P) = 0$, $P = T' + R$ for some $R \in E[n]$.*

Proof. By Theorem 2, $E[n^2]$ forms an abelian group. Since $P, T' \in E[n^2]$, we have that

$$P = T' + (P - T').$$

We claim that $P - T' \in E[n]$. This is true since

$$n(P - T') = nP - nT' = nP - T$$

since $nT' = T$. Since $(f_T \circ n)(P) = 0$, $nP = T$. Thus, $n(P - T') = \infty$. □

Thus, we have that

$$\text{div}(f_T \circ n) = n\left(\sum_{R \in E[n]} [T' + R]\right) - n\left(\sum_{P \in E[n]} [P]\right)$$

Then, we choose a $T' \in E[n^2]$ such that $nT' = T$. By Theorem 3 again, there exists a function g_T such that

$$\text{div}(g_T) = \sum_{R \in E[n]} ([T' + R] - [R]).$$

This is true since $\deg([T'+R]-[R]) = 0$ and $\text{sum}([T'+R]-[R]) = T'+R-R = T'$. By Theorem 2, $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. This means there are n^2 points $R \in E[n]$. Thus,

$$\text{sum}(\text{div}(g_T)) = n^2 T' = \infty$$

since $T' \in E[n^2]$. Then, we use a slightly different notation to obtain the divisors of g^n as

$$\begin{aligned}
\text{div}(f_T \circ n) &= n\Bigg(\sum_{R \in E[n]} [T'+R]\Bigg) - n\Bigg(\sum_{R \in E[n]} [R]\Bigg) \\
&= n\Bigg(\sum_{R \in E[n]} \big([T'+R] - [R]\big)\Bigg) \\
&= n \cdot \text{div}(g_T) \\
&= \text{div}(g_T^n).
\end{aligned}$$

Let $S, T \in E[n]$ be our initial S and T, and $P \in E(\overline{\mathbb{F}})$ be an auxiliary point. We have that

$$g_T(P+S)^n = (f_T \circ n)(P+S) = f_T(nP+nS) = f_T(nP) = g_T(P)^n.$$

This means

$$\left(\frac{g_T(P+S)}{g_T(P)}\right)^n = 1 \implies \frac{g_T(P+S)}{g_T(P)} \in \mu_n.$$

Thus, we define the Weil pairing $e_n : E[n] \times E[n] \to \mu_n$ as

$$e_n(S,T) = \frac{g_T(P+S)}{g_T(P)}.$$

We claim that this defined e_n is actually independent of the choice of point P.

Lemma 2. *Let $P_1, P_2 \in E(\overline{\mathbb{F}})$. Then,*

$$\frac{g_T(P_1+S)}{g_T(P_1)} = \frac{g_T(P_2+S)}{g_T(P_2)}.$$

We omit the proof of Lemma 2 since the proof is topology intensive. This can be found in [5, Section 11.2].

With the defined e_n, we present the proof of Theorem 4.

Proof. (1) Let $S_1, S_2 \in E[n]$. Since e_n is independent of the choice of P by Lemma 2, have that

$$\begin{aligned} e_n(S_1,T)e_n(S_2,T) &= \frac{g_T(P+S_1)}{g(P)}\frac{g_T(P+S_1+S_2)}{g_T(P+S_1)} \\ &= \frac{g_T(P+S_1+S_2)}{g_T(P)} = e_n(S_1+S_2,T). \end{aligned}$$

Hence, e_n is linear in the first variable. Then, let $T_1, T_2 \in E[n]$. We define $T_3 = T_1 + T_2$. Since $T_3 = T_1 + T_2$, by Theorem 3, there exists function h such that

$$\operatorname{div}(h) = [T_3] - [T_1] - [T_2] + [\infty].$$

Moreover, we also have that

$$\begin{aligned} \operatorname{div}\left(\frac{f_{T_3}}{f_{T_1}f_{T_2}}\right) &= n[T_3] - n[\infty] - n[T_2] + n[\infty] - n[T_1] + n[\infty] \\ &= n[T_3] - n[T_1] - n[T_2] + n[\infty] \\ &= n([T_3] - [T_1] - [T_2] + [\infty]) \\ &= n \cdot \operatorname{div}(h) = \operatorname{div}(h^n) \implies \operatorname{div}(f_{T_3}) = \operatorname{div}(f_{T_1}f_{T_2}h^n). \end{aligned}$$

This means there exists $c \in \overline{\mathbb{F}}^{\times}$ such that $f_{T_3} = c f_{T_1} f_{T_2} h^n$. Then, similar to before, we define $(f_{T_3} \circ n)(S) = f_{T_3}(nS)$. Thus, we have that

$$\begin{aligned} g_{T_3}^n = f_{T_3} \circ n \implies g_{T_3}^n &= c \cdot (f_{T_1} \circ n) \cdot (f_{T_2} \circ n) \cdot (h^n \circ n) \\ \implies g_{T_3}^n &= c \cdot g_{T_1}^n \cdot g_{T_2}^n \cdot (h^n \circ n) \\ \implies g_{T_3} &= c^{1/n} \cdot c g_{T_1} g_{T_2} (h \circ n). \end{aligned}$$

Then, we have that

$$\begin{aligned} e_n(S, T_1 + T_2) = e_n(S, T_3) &= \frac{g_{T_3}(P+S)}{g_{T_3}(P)} = \frac{c g_{T_1} g_{T_2} (h \circ n)(P+S)}{c g_{T_1} g_{T_2} (h \circ n)(P)} \\ &= \frac{g_{T_1}(P+S)}{g_{T_1}(P)} \cdot \frac{g_{T_2}(P+S)}{g_{T_2}(P)} \cdot \frac{h(n(P+S))}{h(nP)} = e_n(S, T_1) e_n(S, T_2), \end{aligned}$$

since $S \in E[n]$, that is $h(n(P+S)) = h(nP + nS) = h(nP)$. This finished our proof in bilinearity.

(3) Let τ_{jT} denotes the function $P \to P + jT$. Then, $f \circ \tau_{jT}$ denote the function $P \to f(P + jT)$. Then, we have that

$$\operatorname{div}(f \circ \tau_{jT}) = n[T - jT] - n[-jT].$$

Therefore,

$$\operatorname{div}\left(\prod_{j=0}^{n-1} f \circ \tau_{jT} \right) = \sum_{i=0}^{n-1} (n[T - jT] - n[-jT]) = 0.$$

By Theorem 3, $\prod_{j=0}^{n-1} f \circ \tau_{jT}$ is constant. Since $g^n = f \circ n$, we have that

$$\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right)^n = \prod_{j=0}^{n-1} f \circ n \circ \tau_{jT'}$$
$$= \prod_{j=0}^{n-1} f \circ \tau_{jT} \circ n \qquad \text{(since } nT' = T\text{)}$$

Since $\prod_{j=0}^{n-1} f \circ \tau_{jT}$ is constant, $\prod_{j=0}^{n-1} f \circ \tau_{jT} \circ n$ is constant. Thus, $\prod_{j=0}^{n-1} g \circ \tau_{jT'}$ is constant. Hence, the product evaluates to the same value at $P + T'$ and P. That is

$$\prod_{j=0}^{n-1} g(P + T' + jT') = \prod_{j=0}^{n-1} g(P + (j+1)T') = \prod_{j=0}^{n-1} g(P + jT').$$

Suppose we choose P such that all terms are finite and nonzero. By canceling the terms on both sides, we have that

$$g(P + nT') = g(P + T) = g(P) \qquad \text{(since } nT' = T\text{)}.$$

Thus,

$$e_n(T, T) = \frac{g(P+T)}{g(P)} = 1, \text{ as desired.}$$

(4) Let $S, T \in E[n]$. We consider

$$\begin{aligned} e_n(T,S)e_n(S,T) &= e_n(S,S)e_n(T,S)e_n(S,T)e_n(T,T) && \text{(by (3))} \\ &= e_n(S+T,S)e_n(S+T,T) = e_n(S+T,S+T) && \text{(by (1))} \\ &= 1 && \text{(by (3))} \end{aligned}$$

Since $e_n(T,S)e_n(S,T) = 1$, $e_n(T,S) = e_n(S,T)^{-1}$, as desired.

(2) Let $T \in E[n]$ such that $e_n(S,T) = 1$ for all $S \in E[n]$. This means that

$g_T(P+S) = g_T(P)$ for all $P \in E(\overline{\mathbb{F}})$ and $S \in E[n]$. By Proposition 9.34 [5, p. 300], there exists function h such that $g_T = h \circ n$. We omit such a Proposition from this paper since it is not involved anywhere except in this proof. Since $g_T = h \circ n$, we have that

$$g_T^n = (h \circ n)^n = f_T \circ n$$

Thus, we have $h^n = f$. Therefore,

$$n \cdot \operatorname{div}(h) = \operatorname{div}(f) = n[T] - n[\infty]$$
$$\implies n \cdot \operatorname{div}(h) = [T] - [\infty].$$

Since h is a function, by Theorem 3, $\operatorname{sum}(h) = T - \infty = T = \infty$, as desired. Let $S \in E[n]$ such that $e_n(S,T) = 1$ for all $T \in E[n]$. By (4), for all $T \in E[n]$, $e_n(T,S)^{-1} = 1 \iff e_n(T,S) = 1$. Then, non-degeneracy in S follows from non-degeneracy in T, that is $S = \infty$.

(5) Let σ be an automorphism of $\overline{\mathbb{F}}$ such that $\sigma(A) = A$ and $\sigma(B) = B$. Then, we apply σ on every point in constructing e_n. That is, let $S, T \in E[n]$. We define f_T^σ where

$$\operatorname{div}(f_T^\sigma) = n[\sigma T] - n[\infty].$$

Then, we can define define g_T^σ where

$$\operatorname{div}(g_T^\sigma) = \sum_{R \in E[n]} ([\sigma T' + \sigma R] - [\sigma R]) = \operatorname{div}(g_{\sigma_T} \circ \sigma)$$

Then, we have that

$$\sigma(e_n(S,T)) = \sigma\left(\frac{g_T(P+S)}{g_T(P)}\right) = \frac{g_T^\sigma(\sigma P + \sigma S)}{g_T^\sigma(\sigma P)} = e_n(\sigma S, \sigma T),$$

as desired.

(6) The proof of (6) can be found in [5, Section 11.2]. □

The following result is helpful in the next section.

Lemma 3. *Let $\{T_1, T_2\}$ be a $\mathbb{Z}$-basis of $E[n]$. Then, $e_n(T_1, T_2)$ is a primitive n^{th} root of unity.*

Proof. Define $\zeta = e_n(T_1, T_2) \in \mu_n$. Let d be the order of ζ. To show ζ is a primitive n^{th} root of unity, we are going to show that $d = n$.
Let $S \in E[n]$. This means there exists $a, b \in \mathbb{Z}$ such that $S = aT_1 + bT_2$. We consider

$$\begin{aligned} e_n(S, dT_2) &= e_n(aT_1 + bT_2, dT_2) \\ &= e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b && \text{(bilinearity)} \\ &= e_n(T_1, T_2)^{da} e_n(T_2, T_2)^{db} && \text{(bilinearity)} \\ &= \zeta^{da} 1^{db} = 1 \end{aligned}$$

Since S is arbitrary, non-degeneration holds. This means $dT_2 = \infty$, which implies $n \mid d$. This means $n = d$, as desired. □

4.2. **THE M.O.V. ATTACK.** We first note that e_n can be computed efficiently [3]. This section shows how we can use the Weil pairing to reduce the problem of discrete logarithm over $E(\mathbb{F}_p)$ to one in $\mathbb{F}_q$ where $q = p^m$.
Let E be an elliptic curve over $\mathbb{F}_p$ where p is prime. Let $P, Q \in E(\mathbb{F}_p)$. Let N be the order of P. Since p is prime, $\gcd(N, p) = 1$ since $N \in \mathbb{Z}_{p-1}$. We want to find k such that $Q = kP$. First, we claim that is possible to check if k exists using the Weil pairing.

Lemma 4. *There exists k such that $Q = kP$ if and only if $NQ = \infty$ and $e_N(P, Q) = 1$.*

Proof. ($\implies$) If $Q = kP$, then $NQ = kNP = \infty$. Moreover, we have that

$$e_N(P, Q) = e_N(P, kP) = e_N(P, P)^k = 1^k = 1.$$

($\impliedby$) If $NQ = \infty$, then $Q \in E[N]$. Since $\gcd(N, q) = 1$, by Theorem 2, $E[N] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. We choose point R such that $\{P, R\}$ is a $\mathbb{Z}$-basis for $E[N]$. Then, we can write

$$Q = kP + bR,$$

where $a, b \in \mathbb{Z}$. By Lemma 3, $e_N(P, R) = \zeta$ is a primitive N^{th} root of unity. Hence, we have that

$$e_N(P, Q) = e_N(P, aP + bR) = e_N(P, P)^k e_N(P, R)^b = \zeta^b.$$

This means $\zeta^b = e_N(P, Q) = 1$. Since ζ is a primitive N^{th} root of unity, $N|b$. Thus, $bR = \infty$ (since $R \in E[N]$). Therefore, $Q = kP + \infty = kP$, as desired. □

We check if k exists by simply evaluating NQ and $e_n(P, Q)$, both of which could be computed efficiently.

Proposition 2. *Let E be an elliptic curve over $\mathbb{F}_p$. Then, $E[N] \subseteq E(F_{p^m})$ for some $m \in \mathbb{N}$.*

Proof. Since $S \in E[N] \subseteq E(\overline{\mathbb{F}}_p)$ and there are finite $S \in E[N]$, we can extend $E(\mathbb{F}_p)$ by all elements in $E[N]$ to obtain $E(\mathbb{F}_{p^m})$ for some $m \in \mathbb{N}$, as desired. □

Proposition 3. *Let E be an elliptic curve over $\mathbb{F}_p$ and $E[N] \subseteq E(F_{p^m})$ for some $m \in \mathbb{N}$. Then, $\mu_N \subseteq \mathbb{F}_{p^m}$.*

The proof of a similar statement to this proposition is available in [5, Section 3.3]. With all the pieces, we introduce the M.O.V. attack:

(1) Pick a random $T \in E(\mathbb{F}_{q^m})$.

(2) Compute the order M of T.

(3) Let $d = \gcd(M, N)$, and let $T_1 = (M/d)T$. Then, the order of T_1 is d, which divides N, implying $T_1 \in E[N]$.

(4) Then, we compute $\zeta_P = e_N(P, T_1)$ and $\zeta_Q = e_N(Q, T_1)$. We note that

$$\begin{aligned}\zeta_P^d &= e_N(P, T_1)^d = e_N(P, dT_1) \\ &= e_N(P, \infty) = e_N(P, NP) = e_N(P, P)^N = 1,\end{aligned}$$

and

$$\begin{aligned}\zeta_Q^d &= e_N(Q, T_1) = e_N(Q, dT_1) \\ &= e_N(Q, \infty) = e_N(Q, \text{order}(Q)Q) = e_N(Q, Q)^{\text{order}(Q)} = 1.\end{aligned}$$

This means $\zeta_P, \zeta_Q \in \mu_d$. Since $d \mid N$, $\zeta_P, \zeta_Q \in \mu_d \subseteq \mu_N \subseteq \mathbb{F}_{q^m}$.

(5) Solve the discrete log problem $\zeta_Q = \zeta_P^{k_d}$ in $\mathbb{F}_{p^m}$. This problem is well-defined since k is a solution to this problem:

$$\zeta_P^k = e_N(P, T_1)^k = e_N(kP, T_1) = e_N(Q, T_1) = \zeta_Q.$$

We can solve this problem with Index Calculus (Section 3.2). This gives $k_d = k \pmod d$. We only get $k \pmod d$ since the order of elements in μ_d is in $\mathbb{Z}_d$.

(6) Redo (1) - (5) until the least common multiple of the d's obtained is N. This determined $k \pmod N$ by the Chinese Remainder Theorem.

After some number of picks of T in step (1), we can solve the elliptic curve discrete log problem. It can be shown that $d = 1$ does not occur very often [2, Section 5.3.1]. However, the runtime of this method relies on the runtime of step (5) where we solve a discrete logarithm problem in $\mathbb{F}_{p^m}$, which may be slow if the size of $\mathbb{F}_{p^m}$ (or m) is not sufficiently small.

4.3. **EXAMPLE.** We consider the elliptic curve E over $\mathbb{F}_{11}$ with Weierstrass form

$$E : y^2 = x^3 + 2$$

We define a discrete logarithm problem over E using $P = (1, 5)$ and $Q = (4, 0)$. Firstly, we check if there exists a k such that $kP = Q$ using Lemma 4. Using SAGEMATH [4], we have that $N = \text{order}(P) = 12$ and, indeed, $12 \cdot (4, 0) = \infty$ over E and $e_{12}((1, 5), (4, 0)) = 1$; in fact, $k = 6$. Moreover, we have that $\mathbb{F}_{11^m} \cong \mathbb{F}_{11}/(x^{12} - 1)$. Since

$$\begin{aligned} x^{12} - 1 = (x + 1) \cdot (x + 10) \cdot (x^2 + 1) \cdot (x^2 + x + 1) \\ \cdot (x^2 + 5x + 1) \cdot (x^2 + 6x + 1) \cdot (x^2 + 10x + 1) \end{aligned}$$

in $\mathbb{F}_{11}$, $x^{12} - 1$ completely splits in $\mathbb{F}_{11}/(x^2 + 1) \cong \mathbb{F}_{11}/(x^{12} - 1) \cong \mathbb{F}_{11^2}$. Thus, $m = 2$. Let $\omega = \sqrt{-1}$ being a root of $x^2 + 1$. Then, elements of $\mathbb{F}_{11^2}$ have the form $a + b\omega$ where $a, b \in \mathbb{F}_{11}$.

We choose $T = (6\omega + 7, 8)$ of order $M = 4$. Thus, $d = \gcd(M, N) = \gcd(12, 4) = 4$ and $T_1 = 1T = (6\omega + 7, 8)$. Again, using SAGEMATH,

$e_{12}(P, T_1) = 7\omega + 8$ and $e_{12}(Q, T_1) = 10$. We obtain $k = 2 \pmod 4$.

Again, we choose $T = (9\omega + 5, 7)$ of order $M = 3$. Then, $d = \gcd(M, N) = \gcd(12, 3) = 3$ and $T_1 = 1T = (9\omega + 5, 7)$. We have $e_{12}(P, T_1) = \omega + 3$ and $e_{12}(Q, T_1) = 1$. Hence, $k = 0 \pmod 3$.

Since $\text{lcm}(3, 4) = 12 = N$, we stopped. By the Chinese Remainder Theorem, $k = 6 \pmod{12}$, as desired.

5. REMARKS

We pointed out that this attack can not deterministically solve any discrete logarithm problem over an elliptic curve. As mentioned above, if the size of the field $\mathbb{F}_{p^m}$, which the problem reduced into, is large, the Index Calculus will not work efficiently. Moreover, computing the order of a point in a group is as hard as integer factorization. Thus, N and M may not be obtained in a reasonable time. Moreover, at any iteration of the algorithm, we may only obtain $k \pmod d$ where $d = \gcd(M, N)$ whereas we want to obtain $k \pmod N$. This means if N is a large prime or order of large primes, even if we pick a good starting point T, computing M will not efficient, which lowers of efficiency of the attack.

REFERENCES

[1] Jason S. Howell. "The Index Calculus Algorithm for Discrete Logarithms". PhD thesis. Clemson Unversity, 1998. URL: https://people.clarkson.edu/~jhowell/math/msthesis.pdf.

[2] A.J. Menezes, T. Okamoto, and S.A. Vanstone. "Reducing elliptic curve logarithms to logarithms in a finite field". In: IEEE Transactions on Information Theory 39.5 (1993), pp. 1639–1646. DOI: 10.1109/18.259647.

[3] Victor S. Miller. "The Weil Pairing, and Its Efficient Calculation". In: Journal of Cryptology 17.4 (Sept. 2004), pp. 235–261. ISSN: 1432-1378. DOI: 10.1007/s00145-004-0315-8. URL: https://doi.org/10.1007/s00145-004-0315-8.

[4] W. A. Stein et al. Sage Mathematics Software (Version x.y.z). http://www.sagemath.org. The Sage Development Team. YYYY.

[5] Lawrence C. Washington. Elliptic Curves: Number Theory and Cryptography. 2nd ed. Chapman & Hall/CRC, 2008. ISBN: 9781420071467.