Elliptic Curve Pairings

EE 694 : Credit Seminar
by

Thakore Varun Pragnesh (213079002)

under the guidance of

Prof. Saravanan Vijayakumaran

Department of Electrical Engineering
Indian Institute of Technology, Bombay
Mumbai 400 076

1 Introduction

An elliptic curve pairing is a function that takes as input two points on an elliptic curve and outputs an element of some multiplicative abelian group. A pairing satisfies several properties, the most important of which is bilinearity. The bilinearity of pairings enable many applications in cryptography, for example, three-party Diffie Hellman key agreement where the bilinearity property of pairings is used to share a common key between three users.

This report provides an overview on elliptic curve parings. It introduces Divisors which are used to define the Weil and Tate pairings. It presents Miller's Algorithm which is used to compute pairings.

2 Divisors

Let K denote a field and $\overline{K}$ its algebraic closure. Let E be an elliptic curve defined over field K. For each point $P \in E(\overline{K})$, define a formal symbol $[P]$. A **divisor** D on E is a finite linear combination of such symbols with integer coefficients.

$$D = \sum_j a_j[P_j], \quad a_j \in \mathbf{Z}$$

The **degree** and **sum** of a divisor is defined as

$$deg(D) = \sum_j a_j \in \mathbf{Z}$$
$$sum(D) = \sum_j a_j P_j \in E(\overline{K})$$

The **support** of a divisor D, denoted $supp(D)$, is the set

$$supp(D) = \{P_j \in E(\overline{K}) : a_j \neq 0\}$$

The set of all divisors on E is denoted by $Div(E)$ and forms a group, where group operation is addition and identity is the zero divisor $0 \in Div(E)$. The divisors of degree zero forms a subgroup of $Div(E)$ denoted by $Div^0(E)$, $Div^0(E) \subset Div(E)$.
Let E be given by $y^2 = x^3 + ax + b$. A **function** on E is a rational function

$$f(x, y) \in \overline{K}(x, y)$$

that is defined for at least one point in $E(\overline{K})$(so, for example, the rational function $1/(y^2 - x^3 - ax - b)$ is not allowed). The function takes values in $\overline{K} \cup \infty$.

A function is said to have a **zero** at a point P if it takes the value 0 at P, and it has a **pole** at P if it takes the ∞ at P. We need to define the order of the zero or pole. Let P be a point. There is a function u_P, called a **uniformizer** at P, with $u_P(P) = 0$ and such that every $f(x, y)$ can be written in the form

$$f = {u_P}^r g, \quad with \quad r \in \mathbf{Z} \quad and \quad g(P) \neq 0, \infty$$

The **order** of f at P is defined as

$$ord_P(f) = r$$

Exmaple 2.1
Let E be $y^2 = x^3 - x$ and $f(x, y) = x$. Let us consider the point $P = (0, 0)$, we know that the function y is a uniformizer at P, thus $u_P = y$.

$$f(x, y) = x = y^2 \frac{1}{x^2 - 1} = {u_P}^r g$$

where $g = 1/(x^2 - 1)$ is non-zero and finite at P. Therefore $ord_{(0,0)}(x) = 2$. □

If f is a function on E that is not identically 0, define the **divisor** of f as

$$div(f) = \sum_{P \in E(\overline{K})} ord_P(f)[P] \quad \in Div(E)$$

This is a finite sum and hence a divisor.

Theorem 2.1
Let E be an elliptic curve and let f be a function on E that is not identically 0

1. f has only finitely many zeroes and poles
2. $deg(div(f)) = 0$
3. If f has no zeroes or poles ($div(f) = 0$), then f is a constant

For proof see, [2, Th 7.7.1]. □

Theorem 2.2
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

$$sum(D) = \mathcal{O}$$

For proof see, [5, Th 11.2]. □

We will now describe the evaluation of a function at a divisor. If $div(f)$ and D have disjoint supports then evaluation of f at D is defined as

$$f(D) = \prod_j f(P_j)^{a_j}$$

The disjoint supports is necessary for $f(D)$ to be non-trivial.
We call divisors D_1 and D_2 **equivalent**, denoted as $D_1 \sim D_2$, if $D_1 = D_2 + div(f)$ for some function f.

Exmaple 2.2
Consider an elliptic curve $E : y^2 = x^3 + ax + b$ and a line $l : y = \lambda x + \nu$ as shown in the following figure. By substituting $l : y = \lambda x + \nu$ into $E : y^2 = x^3 + ax + b$ we get three zeroes which are the points P, Q and $-(P + Q)$.

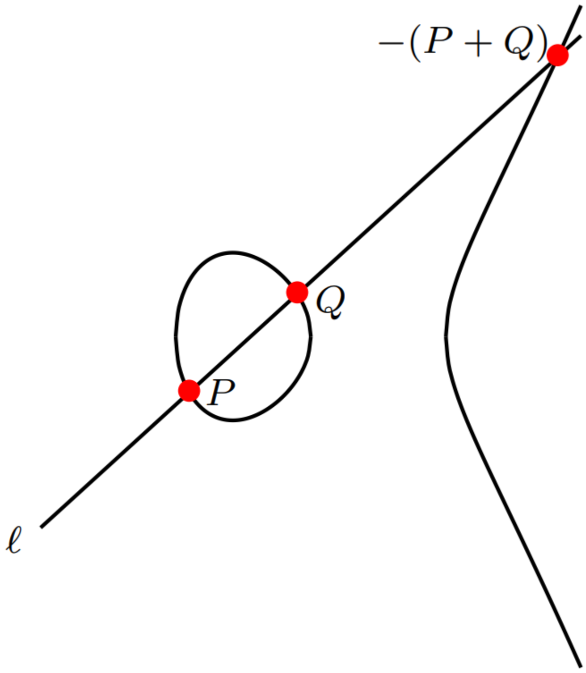

Figure 1: [1, Example 3.0.2]

Here we have only considered the affine coordinates. To consider l on E at $\mathcal{O} = (0 : 1 : 0)$ we need to convert from affine coordinates to projective coordinates by substituting $x = X/Z$ and $y = Y/Z$. This gives $(\frac{\lambda X+\nu Z}{Z})^2 = (\frac{X}{Z})^3 + a\frac{X}{Z} + b$ which shows there is a pole of order 3 at $Z = 0$. Thus l has divisor $div(l) = [P] + [Q] + [-(P + Q)] - 3[\mathcal{O}]$. □

We will now define the group of n-**torsion** points which will be required in the definition of pairings. Let E be an elliptic curve defined over a field K. Let n be a positive integer. The group of n-**torsion** points is defined as

$$E[n] = \{P \in E(\overline{K}) | nP = \mathcal{O}\}$$

We will now state the **Weil reciprocity** theorem which is required to prove several properties of elliptic curve pairings.

Theorem 2.3 (Weil reciprocity)
Let f and g be non-zero functions on a curve such that $div(f)$ and $div(g)$ have disjoint supports. Then $f(div(g)) = g(div(f))$.
For proof see, [3, Th IX.3]. □

3 Weil Pairing

Let $S, T \in E[n]$. Let D_S and D_T be divisors of degree 0 such that

$$sum(D_S) = S \qquad sum(D_T) = T$$

and such that D_S and D_T have disjoint supports. Let f_S and f_T be functions such that

$$div(f_S) = nD_S \qquad div(f_T) = nD_T$$

The **Weil Pairing** is defined as

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

$$e_n(S,T) = \frac{f_T(D_S)}{f_S(D_T)}$$

where μ_n is the set of nth root of unity.

Theorem 3.1
The Weil Pairing maps to the set of nth root of unity and is independent of the choice of divisors D_S and D_T and functions f_S and f_T.
PROOF We will first show that the Weil Pairing maps to the set of nth root of unity.

$$e_n(S,T)^n = \left(\frac{f_T(D_S)}{f_S(D_T)}\right)^n = \frac{f_T(nD_S)}{f_S(nD_T)} = \frac{f_T(div(f_S))}{f_S(nD_T)} = \frac{f_S(div(f_T))}{f_S(nD_T)} = \frac{f_S(nD_T)}{f_S(nD_T)} = 1$$

This proves that $e_n(S,T)$ maps to the set of nth root of unity.
Now we will show that the Weil Pairing is independent of the choice of divisors D_S and D_T. Let D'_S be another divisor such that $sum(D'_S) = S$ and $deg(D'_S) = 0$ and D'_S and D_T have disjoint supports. We know that $\exists f'_S$ such that $div(f'_S) = nD'_S$. Since $D'_S \sim D_S$ we can write $D'_S = D_S + div(h)$ for some function h. Thus,

$$\begin{aligned} nD'_S &= nD_S + ndiv(h) \\ div(f'_S) &= div(f_S) + div(h^n) \\ f'_S &= f_S \cdot h^n \end{aligned}$$

Now,

$$\frac{f_T(D'_S)}{f'_S(D_T)} = \frac{f_T(D_S) \cdot f_T(div(h))}{f_S(D_T) \cdot h^n(D_T)} = \frac{f_T(D_S) \cdot f_T(div(h))}{f_S(D_T) \cdot h(nD_T)} = \frac{f_T(D_S) \cdot f_T(div(h))}{f_S(D_T) \cdot h(div(f_T))} = \frac{f_T(D_S)}{f_S(D_T)}$$

This proves that pairing does not depend on the choice of D_S, an analogous argument can be used to prove the same for D_T.

Now we will show that the Weil Pairing is independent of the choice of functions f_S and f_T. Let f'_S be another function such that $div(f'_S) = nD_S$. Since f'_S and f_S have the same divisor, they are equal upto a constant i.e. $f'_S = c \cdot f_S$. Now for $D_T = \sum_j a_j[P_j]$,

$$f'_S(D_T) = \prod_j f'_S(P_j)^{a_j} = \prod_j (c \cdot f_S(P_j))^{a_j} = c^{\sum_j a_j} \prod_j f_S(P_j)^{a_j} = f_S(D_T)$$

where the last step follows from $deg(D_T) = 0$ i.e. $\sum_j a_j = 0$. This proves that Weil Pairing is independent of the choice of f_S, an analogous argument can be used to prove the same for f_T. □

Theorem 3.2 (Bilinearity Property)
e_n is bilinear in each variable, this meas that for all $S_1, S_2, S, T_1, T_2, T \in E[n]$

$$e_n(S_1 + S_2, T) = e(S_1, T) \cdot e(S_2, T)$$

$$e_n(S, T_1 + T_2) = e(S, T_1) \cdot e(S, T_2,)$$

PROOF We prove linearity in the first factor; linearity in the second goes analogously. Let $S \in E[n]$ such that $S = S_1 + S_2$ and D_S be divisor of degree 0 such that $sum(D_S) = S_1 + S_2$. Let $T \in E[n]$ and D_T be divisor of degree 0 such that $sum(D_T) = T$ and D_S and D_T have disjoint supports. We know that $\exists f_S$ and f_T such that $div(f_S) = nD_S$ and $div(f_T) = nD_T$.
Let D_{S_1} be a divisor of degree 0 such that $sum(D_{S_1}) = S_1$ and $div(f_{S_1}) = nD_{S_1}$. Let D_{S_2} be another divisor of degree 0 such that $sum(D_{S_2}) = S_2$ and $div(f_{S_2}) = nD_{S_2}$. Now $D_S \sim (D_{S_1} + D_{S_2})$ thus for some function h,

$$\begin{aligned} D_S &= D_{S_1} + D_{S_2} + div(h) \\ nD_S &= nD_{S_1} + nD_{S_2} + ndiv(h) \\ div(f_S) &= div(f_{S_1}) + div(f_{S_2}) + div(h^n) \\ f_S &= f_{S_1} \cdot f_{S_2} \cdot h^n \end{aligned}$$

Now,

$$\begin{aligned} e_n(S, T) &= \frac{f_T(D_S)}{f_S(D_T)} \\ e_n(S_1 + S_2, T) &= \frac{f_T(D_{S_1}) \cdot f_T(D_{S_2}) \cdot f_T(div(h))}{f_{S_1}(D_T) \cdot f_{S_2}(D_T) \cdot h^n(D_T)} = e(S_1, T) \cdot e(S_2, T) \qquad \square \end{aligned}$$

4 Tate Pairing

Let E be an elliptic curve over $\mathbb{F}_q$. Let n be an integer such that $n|q-1$. Let $P \in E(\mathbb{F}_q)[n]$ and D_P be a divisor of degree 0 such that $sum(D_P) = P$. Let f_P be a function such that $div(f_P) = nD_P$. Let Q be a point representing a coset in $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$. Let D_Q be a divisor of degree 0 such that $sum(D_Q) = Q$ and such that D_P and D_Q have disjoint supports.

The **Tate Pairing** is defined as

$$\langle \cdot, \cdot \rangle_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^n$$

$$\langle P, Q \rangle_n = f_P(D_Q)$$

The **modified Tate Pairing** is defined as

$$\langle \cdot, \cdot \rangle_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mu_n$$

$$\tau_n = f_P(D_Q)^{\frac{q-1}{n}}$$

where μ_n is theset of nth root of unity.

Theorem 4.1

The Tate Pairing is independent of the choice of divisor D_Q and function f_P.

PROOF We will now show that Tate Pairing is independent of the choice of divisor D_Q. Let f_P be a function satisfying $div(f_P) = nD_P$ and $D'_Q \sim D_Q \sim ([Q] - [\mathcal{O}])$ such that the support of both D'_Q and D_Q is disjoint from support of $div(f_P)$. Then we can write $D'_Q = D_Q + div(h)$ for some function h defined over $\mathbb{F}_q$ such that $div(f_P)$ and $div(h)$ have disjoint supports. Now,

$$\begin{aligned}
f(D'_Q) &= f(D_Q + div(h)) \\
&= f(D_Q) \cdot f(div(h)) \\
&= f(D_Q) \cdot h(div(f)) \\
&= f(D_Q) \cdot h(nD_P) \\
&= f(D_Q) \cdot h(D_P)^n \\
f(D'_Q) &= f(D_Q) \quad (mod(\mathbb{F}_q^*)^n)
\end{aligned}$$

where the last equation follows from $h(D_P) \in \mathbb{F}_q^*$. This proves that Tate pairing is independent of the choice of divisor D_Q.

To prove that Tate pairing is independent of the choice of function f_P. We know that f_P is unique upto a constant. Thus the proof follows similarly as Theorem 3.1. □

Theorem 4.2 (Bilinearity Property)
The Tate Pairing satisfies bilinearity property

$$\langle P_1 + P_2, Q\rangle_n \equiv \langle P_1, Q\rangle_n \cdot \langle P_2, Q\rangle_n$$

$$\langle P, Q_1 + Q_2\rangle_n \equiv \langle P, Q_1\rangle_n \cdot \langle P, Q_2\rangle_n$$

where $P, P_1, P_2 \in E(\mathbb{F}_q)[n]$ and $Q, Q_1, Q_2 \in E(\mathbb{F}_q)$
PROOF We will first prove linearity in the first factor. Let $P = P_1 + P_2$. Let D_{P_1} be a divisor of degree 0 such that $sum(D_{P_1}) = P_1$ and $div(f_{P_1}) = nD_{P_1}$. Let D_{P_2} be another divisor of degree 0 such that $sum(D_{P_2}) = P_2$ and $div(f_{P_2}) = nD_{P_2}$. Now $D_P \sim (D_{P_1} + D_{P_2})$ thus for some function h,

$$\begin{aligned} D_P &= D_{P_1} + D_{P_2} + div(h) \\ nD_P &= nD_{P_1} + nD_{P_2} + ndiv(h) \\ div(f_P) &= div(f_{P_1}) + div(f_{P_2}) + div(h^n) \\ f_P &= f_{P_1} \cdot f_{P_2} \cdot h^n \end{aligned}$$

Now,

$$\begin{aligned} \langle P, Q\rangle_n &= f_P(D_Q) \\ \langle P_1 + P_2, Q\rangle_n &= f_{P_1}(D_Q) \cdot f_{P_2}(D_Q) \cdot h^n(D_Q) \\ \langle P_1 + P_2, Q\rangle_n &\equiv \langle P_1, Q\rangle_n \cdot \langle P_2, Q\rangle_n \end{aligned}$$

Now we will prove linearity in the second factor. Let $Q = Q_1 + Q_2$. Let D_{Q_1} be a divisor of degree 0 such that $sum(D_{Q_1}) = Q_1$. Let D_{Q_2} be another divisor of degree 0 such that $sum(D_{Q_2}) = Q_2$. Now $D_Q \sim (D_{Q_1} + D_{Q_2})$. Thus,

$$\begin{aligned} \langle P, Q\rangle_n &= f_P(D_Q) \\ \langle P, Q_1 + Q_2\rangle_n &\equiv f_P(D_{Q_1}) \cdot f_P(D_{Q_2}) \\ \langle P, Q_1 + Q_2\rangle_n &\equiv \langle P, Q_1\rangle_n \cdot \langle P, Q_2\rangle_n \qquad \square \end{aligned}$$

5 Miller's Algorithm

The Weil and Tate parings are computed as $\frac{f_{n,P}(D_Q)}{f_{n,Q}(D_P)}$ and $f_{n,P}(D_Q)$ respectively. Thus to calculate the pairing we need to compute the function $f_{n,P}$. We will first see a naive method to calculate $f_{n,P}$.

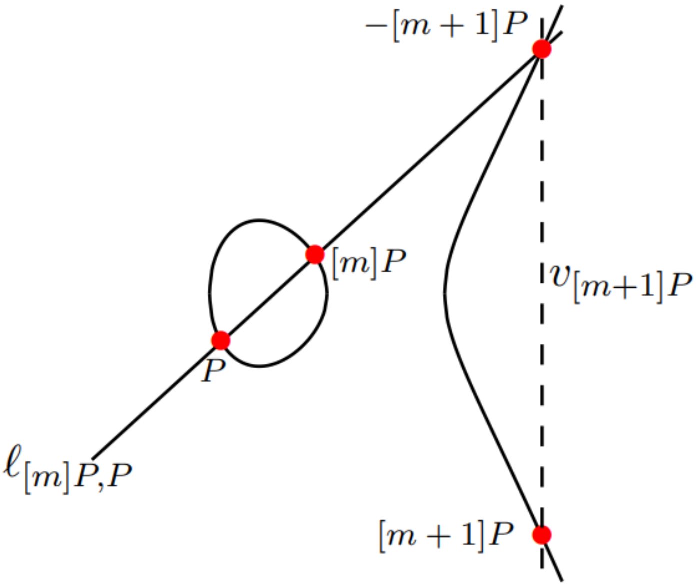

Figure 2: [1, Chapter 5]

The divisors for the lines shown in the figure are as follows:

$$div(l_{[m]P,P}) = (P) + ([m]P) + (-[m+1]P) - 3(\mathcal{O})$$
$$div(v_{[m+1]P}) = ([m+1]P) + (-[m+1]P) - 2(\mathcal{O})$$

Now using Theorem 2.2 we can write the divisor of a function $f_{m,P}$ as

$$div(f_{m,P}) = m(P) - ([m]P) - (m-1)(\mathcal{O})$$

Observe that $div(f_{m+1,P}) - div(f_{m,P}) = div(l_{[m]P,P}) - div(v_{[m+1]P})$. Thus we can compute $f_{m+1,P}$ from $f_{m,P}$ by using $f_{m+1,P} = f_{m,P}\frac{l_{[m]P,P}}{v_{[m+1]P}}$. Starting with $f_{2,P} = 2(P) - ([2]P) - (\mathcal{O})$ then, we can repeat the process roughly n-1 times to obtain the function $f_{n,P}$. Thus pairing evaluation function $f_{n,P}$ is the product

$$f_{n,P} = l_{[n-2]P,P} \cdot \prod_{i=1}^{n-3} \frac{l_{[i]P,P}}{v_{[i+1]P}}$$

The above method computes $f_{n,P}$ by successively increasing $f_{m,P}$ by 1 at each iteration. For practical applications n is large (at the very least 2^{160}) this makes the naive method computationally infeasible.

Miller's algorithm overcomes this through the following observation. Rather than adding one zero and pole via multiplying $f_{m,P}$ by linear functions, we can double the number of zeros at P and poles at $\mathcal{O}$ by squaring $f_{m,P}$.

$$\begin{aligned} div(f_{m,P}^2) &= 2m(P) - 2([m]P) - 2(m-1)(\mathcal{O}) \\ div(f_{2m,P}) &= 2m(P) - ([2m]P) - (2m-1)(\mathcal{O}) \\ div(f_{2m,P}) - div(f_{m,P}^2) &= 2([m]P) - ([2m]P) - (\mathcal{O}) \end{aligned}$$

Thus we can advance from $f_{m,P}$ to $f_{2m,P}$ using

$$f_{2m,P} = f_{m,P}^2 \cdot \frac{l_{[m]P,[m]P}}{v_{[2m]P}}$$

$$\begin{tikzcd} f_{m,P} \arrow[r, "\cdot\frac{\ell_{[m]P,P}}{v_{[m+1]P}}"] \arrow[rrrrr, bend right, "f_{m,P}^2\cdot\frac{\ell_{[m]P,[m]P}}{v_{[2m]P}}"'] & f_{m+1,P} \arrow[r, "\cdot\frac{\ell_{[m+1]P,P}}{v_{[m+2]P}}"] & \cdots & \cdots \arrow[r, "\cdot\frac{\ell_{[2m-2]P,P}}{v_{[2m-1]P}}"] & f_{2m-1,P} \arrow[r, "\cdot\frac{\ell_{[2m-1]P,P}}{v_{[2m]P}}"] & f_{2m,P} \end{tikzcd}$$

Figure 3: Naive Method vs Miller's Algorithm [1, Section 5.3]

The degree of $f_{m,P}$ grows linearly in the size of m, so the function $f_{m,P}$ becomes too large to store explicitly as m increases. Thus at every stage Miller's algorithm evaluates $f_{m,P}(D_Q)$. At any intermediate stage, we will not store $f_{m,P}$ but rather it's evaluation at D_Q i.e. $f_{m,P}(D_Q) \in \mathbb{F}_q$.

The following shows Miller's Algorithm:
Input: $P \in E(\mathbb{F}_q)[n]$, $D_Q \sim (Q) - (\mathcal{O})$ with support disjoint from $div(f_{n,P})$ and $n = (n_{r-1}...n_1n_0)_2$ with $n_{r-1} = 1$.
Output: $f_{n,P}(D_Q) \leftarrow f$

```
$R \leftarrow P$,$f \leftarrow 1$
for $i = r-2$ to 0 do
    Compute the line functions $l_{R,R}$ and $v_{[2]R}$ for doubling $R$
    $R \leftarrow [2]R$
    $f \leftarrow f^2 \cdot \frac{l_{R,R}}{v_{[2]R}}(D_Q)$
    if $n_i = 1$ then
        Compute the line functions $l_{R,P}$ and $v_{R+P}$ for adding $R$ and $P$
        $R \leftarrow R + P$
        $f \leftarrow f \cdot \frac{l_{R,P}}{v_{R+P}}(D_Q)$
    end if
end for
return $f$
```

References

[1] Craig Costelo. *Pairings for beginners.*

[2] Steven D Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, 2012.

[3] Steven D Galbraith. “Pairings”. In: *book Advances in elliptic curve cryptography* (2005).

[4] Martijn Maas. “Pairing-based cryptography”. In: *Master’s thesis, Technische Universiteit Eindhoven* (2004).

[5] Lawrence C Washington. *Elliptic curves: number theory and cryptography.* Chapman and Hall/CRC, 2008.