Computing Well Pairings For Elliptic Curve Group Points

Shakir Mahmoud Salman
Department of Mathematics
College of Basic Education
Diyala University

Abstract

This work introduce study for one of the relation between points on elliptic curve group which may can use it to attack some of elliptic curve cryptosystems kinds by solving the elliptic curve discrete logarithm problem (ECDLP) which are Weil pairings where we describe the basic concepts for elliptic curve group points operation and some type of elliptic curve that we can fined Weil pairing on it and also we explain all the terms concerning with this property and how to compute it by arithmetical example and introduce some of conclusions that we get it in this work .

Keywords :- elliptic curve ; pairing ; divisor ; rational function ; weil pairings .

حساب اقترانات ويل لزمرة نقاط المنحنى الاهليلجي

شاكر محمود سلمان
قسم الرياضيات
كلية التربية الأساسية
جامعة ديالى

الخلاصة

يقدم هذا البحث دراسة لواحدة من العلاقات الموجودة بين النقاط في زمرة نقاط المنحنى الاهليلجي والتي يمكن أن تستخدم لمهاجمة بعض أنظمة تشفير المنحنيات الاهليلجية عن طريق حل مسالة اللوغاريتم المنفصل في المنحنى الاهليلجي وهي

اقترانات ويل (Weil Pairing) حيث نستعرض المفاهيم الأساسية للعمليات الحسابية في زمرة نقاط المنحني الاهليلجي وبعض أنواع هذه المنحنيات التي يمكن إيجاد اقترانات ويل فيها , وكذلك سنوضح جميع المفاهيم المتعلقة بهذه الخاصية وكيفية حساب الاقترانات من خلال مثال عددي ثم نستعرض بعض الاستنتاجات التي تم التوصل إليها من خلال العمل .

كلمات مفتاحية:- منحنى اهليليجي , اقتران , قاسم , دالة نسبية , اقترانات وايل .

Introduction

Elliptic curve cryptography (ECC) was proposed independently in 1985 by N.Koblitz and V. Miller [6] . Since than, an immense amount of research has been dedicated to securing and accelerating its implementations . ECC has quickly received a lot of attention because of smaller key-length and increased theoretical robustness .

Elliptic curve cryptosystems depending the concept of elliptic curve discrete logarithm problem (ECDLP)where there is no known sub exponential algorithm to solve this problem in general [9]in some cases of several groups of elliptic curve points there are algorithms can solve (ECDLP) [1] .

A Computing some pairing in this group can help to solve (ECDLP) , the Weil pairing consider one of these pairings which we will discuss it in this article . Where we introduce some basic mathematical concepts about group of elliptic curve points and it's operation and how to define elliptic curve on finite complex field so we introduce the definition of Weil pairing and use it to solve elliptic curve discrete logarithm problem on several kind of elliptic curves which we will discuss it and latest we describe this way .

Essential Mathematical Concepts

In mathematics , an elliptic curve is an algebraic curve defined by equation of the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad ......(1)$$

Which is non singular , that is has no cusps or self intersections .

So in prime finite field elliptic curve defined by the form

$$E(F_p): y^2 = x^3 + ax + b \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

the curve is non singular curve mean that the discriminate of this equation is not equal to zero [10] where

$$\Delta = -16\,(\,4a^3 + 27b^2\,) \quad , where\ \ \Delta\ is\ curve's\ discriminant \qquad \ldots\ldots\ldots\ldots\ldots\ldots(3)$$

The graph of a nonsingular curve has tow components if its discriminate is positive and one component if it is negative , as in the figure 1 .

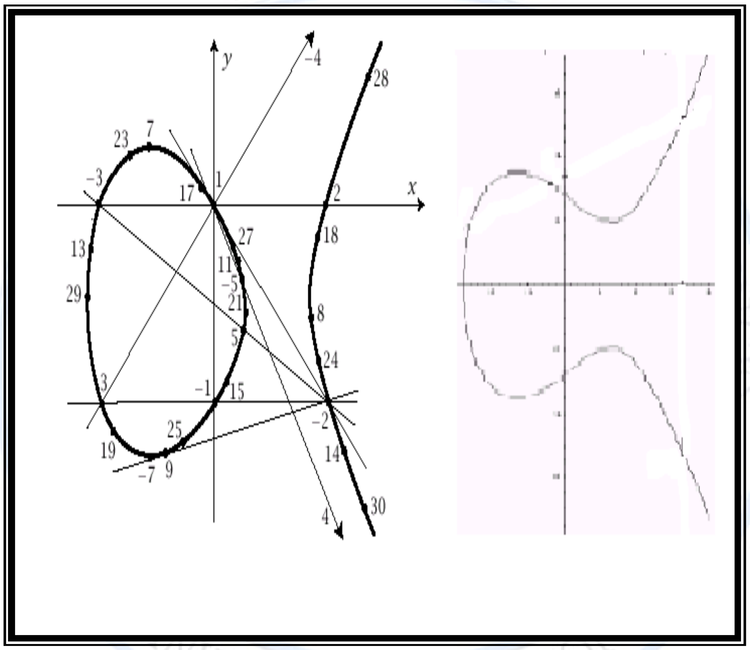

Figure (1) the relation between the graph of elliptic curve and it's discriminate

The j-invariant is another concept for elliptic curve which is the number can we compute it from the general equation for elliptic curve and use it for knowing the isomorphism among different elliptic curves in the algebraically closed field [10] .

For the curve described in equation (2) which denoted by $j\,(\,E\,)$ is:

$$j\,(\,E\,) = -1728\,(\,4a\,)^3 / \Delta \qquad \ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

There are different forms for this concept which computed depending on definition of field that the curve defined on it and the equation generates it .

The more important property in elliptic curve is the group and its operation which we get it from the points of elliptic curve .

Group Structure

The pairs of affine coordinates (x, y) where $x \in F_p$ and $y \in F_p$ from the plane $F_p \times F_p$ which satisfy the equation of elliptic curve is point of this curve, moreover , these point construct abelian group under special binary operation [4] and the identity element for this group is point at infinity , we denoted it by O_E .

For every two points on a curve $(P \in E(F_p))$ and $(Q \in E(F_p))$ it is possible to find a third point $R = P \oplus Q$ where $(R \in E(F_p))$ such that certain relations hold for all points on the elliptic curve :

- $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$
- $P \oplus O_E = O_E \oplus P = P$
- $\textit{There exists } (-P) \textit{ such that } -P \oplus P = P \oplus (-P) = O_E$
- $P \oplus Q = Q \oplus P$

and thus the set of all points is additive abelian group $(E(F_p), \oplus)$ where :

If $P = (x_1, y_1)$, $Q = (x_2, y_2)$ *and* $R = (x_3, y_3)$ where $R = P \oplus Q$ then

$$x_3 = \lambda^2 - 2x_1 \quad , \quad y_3 = \lambda(x_1 - x_3) - y_1 \ ;$$

$$\lambda = \frac{3x_1^2 + a}{2y_2}$$

Where $P = Q$; and if $P \neq Q$ then

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

Notice that since λ defined in a field F_p that is λ is well defined [12]

The point at infinity O_E can we prove it on elliptic curve by geometrical method because it consider their projective coordinate is (0 , 0 ,1) and to transform it to affine coordinate made it point at infinity . [10] .

Bilinear Mapping

In this subsection we briefly review the basic fact about bilinear maps which are :

1- G_1 and G_1 are two (additive) cyclic group of prime order p .

2- g_1 is a generator of G_1 and g_2 is a generator of G_2 .

3- φ is a computable isomorphism from G_1 to G_2 with $\varphi(g_1) = g_2$

4- e is computable bilinear map where $e : G_1 \times G_2 \rightarrow G_T$.

5- G_T is multiplication cyclic group of order p .

A bilinear map is a map $e : G_1 \times G_2 \rightarrow G_T$, which has the following properties :-

1-Bilinear : *for all* $U \in G_1$, $V \in G_2$ *and* $a, b \in Z$;

$$e(a \cdot U , b \cdot V) = e(U,V)^{ab}$$

2-Nondegenerate : $e(G_1, G_2) \neq 1$. [1] .

2.3 *Torsion Subgroup*

The operation of integer times a point and that we know to compute the order of the curve E (F_p) . we can look at the order of points .The order of a point is the smallest integer m (if exists) such that $mP = O_E$ if such an integer does not exist the point is said to have infinite order .

Torsion points are points of finite order . To be more precise P is said to be a r-torsion point (were r is a positive integer if $r \cdot P = O_E$. [10]

If the curve is defined over a finite field F_q , then all rational points are torsion points , since their order divides the order of the curve (this is a fundamental at group theory) and that the order of the curve is finite as we have seen in the previous section . For later developments , we will need to classify torsion points and get information about their structure , which leads us do the following definition :-

Definition 1 :-

Let r be a positive integer . The set

$$E[r]=\{P\in E(\overline{F_p})\,such\,that\ \ r\cdot P=O_E\ \}$$

From a group which is called the r-torsion group .Where $\overline{F_q}$ is algebraic closure field .

The r-torsion group consist of all r-torsion points of the curve E defined over the algebraically closed set .Note That r is not necessarily The order of The points. it can be multiple of The order . Indeed if p has order n Then n is the smallest integer such That $n\cdot P=O_E$ but her all integer k ; $k_n\cdot P=O_E$ as well there P belongs only to $\mathbf{E(n)}$ but to all $E(r)$ such that $n\mid r$ as well . [4]

Sometimes we need to deal with a specific subset of this algebraic closure $E(\overline{F_p})$ like to the base filed $E(F_P)$ or it's extension .

Definition 2 :

Let G be an extension of F_p we can define a group

$$E(G)[r]=E[r]\cap E[G]=\{\ P\in E[G]\ \mid\ r\cdot P=O_E\ \}$$

Now we can give structure of $E[r]$ depending or r and the characteristic p of the field .

- If r is a power of p then either $E[r]=O_E$ (if E is supersingular) or $E[r]$ is isomorphic to Z_r (when E is not supersingular).
- If p and r are coprime then $E[r]$ is isomorphism with $Z_r\times Z_r$ in particular it means that $E[r]$ has r^2 elements but with no element of order r^2 . [3]

For more about superingular curve and distribution on prime field see [4]

Elliptic Curve Over Complex Field

The formulation of elliptic curve as the embedding of a tours in the complete projective plane hollows naturally form a curious property at weiersstrass's elliptic function these function and their derivative are related by the formula :

$$\wp'(z)^2=4\wp(z)^3-g_2\wp(z)-g_3$$

where g_1 , g_2 are constant , $\wp(z)$ is the weierstrass elliptic function and $\wp'(z)$ it's derivative [3] .

It should be clear that this relation is in the form at an elliptic curve over the complex numbers . the weierstrass function are doubly-periodic; that is they are period with respect to a lattice Λ in essence the weierstress function are naturally defined on a tours $T = C / \Lambda$ this tours may be embedded in the complete projective plan by means at the map

$$Z \to (1 \ , \ \wp(z), \wp'(z) \ )$$

this is group isomorphism. Carrying the natural group structure of the tours into the projective plan. It is also an isomorphism of Riemann surfaces, and so topologically a give elliptic carve like a tours .If the lattice Λ is related to a lattice $c \cdot \Lambda$ where multiplication it by a non-zero complex number c , then the corresponding carves are isomorphic.

Isomorphism classes of elliptic carves are specified by the j-invariant. [10] the elliptic carve may be written in complex number as :

$$y^2 = x(x-1)(x-2) \quad where$$

$$g_2 = \frac{4^{1/3}}{3}(\lambda^2 - \lambda + 1) \quad and \quad g_3 = \frac{1}{27}(\lambda + 1)(2\lambda^2 - 5\lambda + +2)$$

$$and\ hence\ \Delta = g_2^3 - 2g_3^2 = \lambda^2(\lambda - 1)^3$$

Notice the above form sometimes called the modular lambda function [3]

Elliptic carve over C can be written as : $C / \langle 1 , \tau \rangle$ where $\tau \in C$ is a complex number with imaginary part $\tau > 0$ here $\langle 1 , \tau \rangle$ is the lattice $\{ n + m\tau \ ; n, m \in Z \ \}$

Every point of $E = C / \langle 1 , \tau \rangle$ can be represent as $a + b\tau$ where $0 \le a \ , \ b < 1$ to discuss the group law see [7]

Rational Functions

One of the many map between two curves is rational function which we need it in this work , before we discuss it definition we must look to the following definition :

Definition 3 :

Let V_1 and V_2 in P^2 be projective varieties . A rational map from V_1 to V_2 is a map of the form :

$$\phi : V_1 \to V_2 \ ; \ \phi = [f_1, f_2, f_3, \ldots\ldots\ldots, f_n]$$

where $f_1, f_2, f_3, \ldots\ldots\ldots, f_n \in \overline{K}(V_1)$ have property that for every point $P \in V_1$ at which $f_1, f_2, f_3, \ldots\ldots\ldots, f_n$ are all defined

$\phi(P) = [f_1(P), f_2(P), f_3(P), \ldots\ldots\ldots, f_n(P)] \in V_2$ [10].

The rational map $\phi : V_1 \to V_2$ is not necessarily a function on all of V_1 , however , it is sometimes possible to evaluate $\phi(P)$ at point P of V_1 where some of f_i is not regular by replacing each f_i to gf_i for an appropriate $g \in \overline{K}(V_1)$ [10] .

The rational function on elliptic curve can we see in another form of definition in [9] . we have then an equivalence relationship and we can define the ring and the associated field of fractions is the field of rational functions of E . [9].

Divisors

Divisors are one of the tools which we need to understand it before we get to pairings . As usual we first begin with a formed definition and then try to give a concrete explanation .

Let E be an elliptic curve defined over a field K , for each point $P \in E(\overline{K})$ we defined a formal symbol *[P]*

Definition 4 :

A divisor D on E is a finite linear combination of the previous symbols with integer coefficients :

$$D = \sum_j a_j [P_j] \quad ; \ a_j \in Z$$

A divisor is no thing but an element of the free abelian group generated by the symbol *[P]* .The group of divisors is denoted by *Div(E)* and we defined two function of divisor :

- The degree of D is an integer which value is :

$$\deg \left(\sum a_j [P_j]\right) = \sum_j a_j$$

- The sum of D is a point of $E(\overline{K})$, and defined this by :

$$sum\left(\sum_j a_j [P_j]\right) = \sum_j a_j P_j$$

The subgroup of divisors of degree 0 , which is denoted $Div^0(E)$, is particular interest [10] .

If we have a function f which has pole of order 1 at P , a zero of order 2 in Q and pole of order 1 at O_E this can be expressed using divisors simply by saying :

$$div(f) = 2[Q] - [P] - [O_E].$$

more precisely , given any rational function f we define $Div(f)$ as :

$$div(f) = \sum_{p \in E(\bar{K})} ord_p(f)[P]$$

where $ord_p(f)$ is the order of the point P .

Since there are only finitely many zeros poles and in equal quantities , hence $Div(f)$ is always in $Div^0(E)$. The divisor of a function is said to be a principal divisor and the group of principal divisors is denoted $prin(E)$ and we obviously have : $prin(E) \subset Div^0(E)$.

Conversely if $D \in Div^0(E)$ then $D \in prin(E)$ if and only if $sum(D) = O_E$. [3]

Now suppose we have a divisor $D = \sum_j a_j[P_j]$ and rational function f . then we kind of extend f and define $f(D)$ to be

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

To explain that we consider P,Q and R three points on E such that lie on the same line $ax + by + c = 0$, where $b \neq 0$. Then the function $f(x, y) = ax + by + c$ has three zeros in P , Q and R and triple pole at O_E (see [8]) so we can write $div(f) = [P] + [Q] + [R] - 3[O_E]$ now if we consider the line between R and $-R$, it's equation is $x - x_R = 0$ (where x_R is the x-coordinate of R) so we have $div(x - x_R) = [R] + [-R] - 2[O_E]$

and hence we can say :

$$div(\frac{ax+by+c}{x-x_R}) = div(ax+by+c) - div(x-x_R) = [P]-[-R]-[O_E]$$

But P, Q and R on the same line that mean $P + Q = -R$ (see [4]) then we get :

$$[P]+[Q]=[P+Q]+[O_E]+div(\frac{ax+by+c}{x-x_R}) \ .$$

finally in this section we must note that $[P]+[Q]$ and $[P+Q]+[O_E]$ are equivalent .

The Weil Pairing

The Weil pairing is a mapping from pairs of points on an elliptic curve to $\overline{F_q}$. More specifically for us , it establishes an isomorphism between a group generated by P of order m and the m^{th} root of unity in F_{q^k} , suitable extension field of F_q [2] .

The Weil pairing operates on two points of $E(\overline{F_q})$ with the same order m the collection of all m-torsion points [2] .

Where $E[m] \subset E(F_{q^k})$ this will be a key for us to compute such a k . So we may define the Weil pairing as :

Let m be a positive integer coprime to p and let $\mu_m \subset \overline{K^*}$ be the group of m^{th} roots of unity . Let $P,Q \in E[m]$,let A and B be divisors of degree zero such that $A \sim (P)-(O_E)$, $B \sim (P)-(O_e)$ and A,B have disjoint support .

Let $f_A, f_B \in \overline{K}$ such that :

$$div(f_A) = mA \quad and \quad div(f_B) = mB$$

then f_A , f_B are exists because P and Q are both m-torsion points also $div(f_A)$ *and* B have disjoint supports , as do $div(f_B)$ *and* A .

The Weil pairing e_m is a function :

$$e_m : E[m] \times E[m] \rightarrow \mu_m$$

defined as :-

$$e_m(P,Q) = f_A(B)/f_B(A)$$

the value of $e_m(P,Q)$ is independent of the choice of A, B, f_A and f_B .

We list some useful properties of the Weil pairing :- [1]

1) ***Identity***: *for all* $P \in E[m]$, $e_m(P,P) = 1$
2) ***Alternation***: *for all* $P,Q \in E(m)$, $e_m(P,Q) = e_m(Q,P)^{-1}$
3) ***Bilinearity***: *for all* $P,Q,R \in E[m]$,

$$e_m(P \oplus Q, R) = e_m(P,R)e_m(Q,R)$$
$$e_m(P, Q \oplus R) = e_m(P,Q)e_m(P,R)$$

4) ***Non-degeneracy***: *if* $P \in E[m]$ *then* $e_m(P, O_E) = 1$
morever if $e_m(P,Q) = 1$ *for all* $Q \in E[m]$ *then* $P = O_E$
5) *If* $E[m] \subseteq E(k)$, *then* $e_m(P,Q) \in k$ *for all* $P,Q \in E[m]$
that is $\mu_m \subseteq k^*$)
6) ***compatible***: *if* $P \in E[m]$ *and* $Q \in E[mm']$, *then* $e_{mm'}(P,Q) = e_m(P, m'Q)$

we are not to give the rather technical proofs her and we must note that m must be relative prime to q ,so as to get the following properties :

<u>Theorem 1</u> :

Let $P \in E[m]$, m relatively prime to q

1) There exists a $Q \in E[m]$ *such that* $e_m(P,Q)$ is a primitive m^{th} root of unity .

2) Let $\phi : \langle P \rangle \to \{\mu_m\}$, *whee* $\{\mu_m\} \subseteq F_{q^k}$, *be definedby* $R \to e_m(R,Q)$ then is group isomorphism .

proof : see [2]

To construct the pairing we begin with function field $\overline{F_q}(E)$ which is , informally the set of rational maps in x and y modulo the equation defending the elliptic curve whose coefficients lie in the algebraic closure of F_q .

***Example 1* :**

consider the elliptic curve $E(F_{13}): y^2 = x^3 + 7x$

The points of this curve and it's order are

Point	order	Point	order
$P_0 = O_E$	1	P_9= (5 ,11)	6
P_1= (0 ,0)	2	P_{10}= (8 ,3)	6
P_2= (2 ,3)	6	P_{11}= (8 ,10)	6
P_3= (2 ,10)	6	P_{12}= (9 ,5)	3
P_4= (3 ,3)	3	P_{13}= (9 ,8)	3
P_5= (3 ,10)	3	P_{14}= (10 ,2)	3
P_6= (4 ,1)	3	P_{15}= (10 ,11)	3
P_7= (4 ,12)	3	P_{16}= (11 ,2)	6
P_8= (5 ,2)	6	P_{17}= (11 ,11)	6

Let $D = 6(P_8) - 6(O_E)$ where D is principal

To fined a rational function f such that div (f) =D then

$$(P_8)-(O_E)=(P_8)-(O_E)+div(1)$$

$$2(P_8)-2(O_E)=[(P_8)-(O_E)]+[(P_8)-(O_E)]$$

$$=(P_7)-(O_E)+div(\frac{-x+y+}{x-4})$$

$$4(P_8)-4(O_E)=[2(P_8)-2(O_E)]+[2(P_8)-2(O_E)]$$

$$=(P_6)-(O_E)+div(\frac{(-x+y+3)^2}{(x-4)^2}\cdot\frac{(y+8x+8)}{(x-4)})$$

$$6(P_8)-6(O_E)=[2(P_8)-2(O_E)]+[4(P_8)-4(O_E)]$$

$$=div(\frac{(-x+y+3)^3}{(x-4)^3}\cdot\frac{(y+8x+8)}{(x-4)}\cdot\frac{(x-4)}{1})$$

So , the desired function form is :

$$f=\frac{(-x+y+3)^3}{(x-4)^3}(y+8x+8)$$

but $f_{13}(x,y)$ is undefined at the points P_6 and P_7 for that we considered the rational function defined at these points where :

$$f = \frac{(-x+y+3)^3}{(x-4)^3}\cdot\frac{(x+y-3)^3}{(x+y-3)^3}\cdot(y+8x+8)$$

$$= \frac{(y^2-x^2+6x-9)^3}{(x-4)^3}\cdot\frac{(y+8x+8)}{(x+y-3)^3}$$

$$= \frac{(x^3+7x-x^2+6x-9)3}{(x-4)^3}\cdot\frac{(y+8x+8)}{(x+y-3)^3}$$

$$= \frac{(x^3-x^2+4)^3}{(x-4)^3}\cdot\frac{(y+8x+8)}{(x+y-3)^3}$$

$$= \frac{(x-4)^3(x-5)^6}{(x-4)^3}\cdot\frac{(y+8x+8)}{(x+y-3)^3}$$

$$= (x-5)^6\,\frac{(y+8x+8)}{(x+y-3)^3}$$

which defined at P_6

Now for compute the Weil pairings let $P = P_4 = (3,3)$ and $Q = P_6 = (4,1)$

We shall compute $e_3(P,Q)$

Firstly we choose random points $T=(8\ ,3)$, $U=(5,2)$ and compute

$P+T=(2,10)$ *and* $Q+U=(5,11)$

then the divisors are

$$3(P+T)-3(O_E)=(P_1)-(O_E)+div\left(\frac{(8x+y)(x+y+1)}{x(x+3)}\right)$$

$$3(T)-3(O_E)=(P_1)-(O_E)+div\left(\frac{(11x+y)(8x+y+11)}{x(x+4)}\right)$$

$$3(Q+U)-3(O_E)=(P_1)-(O_E)+div\left(\frac{(3x+y)(x+y+10)}{x(x+9)}\right)$$

$$3(U)-3(O_E)=(P_1)-(O_E)+div\left(\frac{(10x+y)(12x+y+3)}{x(x+9)}\right)$$

But f_A *and* f_B are functions with

$$div(f_A)=3(P+T)-3(T)\ ,\ div(f_B)=3(Q+U)-3(U)$$

subtracting this give us :

$$f_A = \frac{(8x+y)(x+y+1)(x+4)}{(x+3)(11x+y)(8x+y+11)} \quad , \quad f_B = \frac{(3x+y)(x+y+10)}{(10x+y)(12x+y+3)}$$

then that easy to compute :

$$e_m(P,Q) = \frac{f_A(Q+U)}{f_A(U)} \cdot \frac{f_B(T)}{f_B(P+T)} = 9$$

not that the element *9* has order *3* in F_{13} .

Conclusion

In this article we have describe a simple fact about Weil pairing and it's application and how to computation of this pairing .From that we get some fact that any one deal with this concept must know it where if m is chosen poorly the Weil pairing can degenerate badly and the isomorphism mapping is important for this pairing .

So, the difficulty actual computing of the Weil pairing of two points is finding f_p and f_q when we work on algebraically closed field F_q that the extension field F_q must be suitable , this mean that if we have an instance of (ECDLP) we can with this pairing map it to an instance (DLP) in extension field F_{q^k} if k is not too large then we can solve (DLP) by one of known algorithm for that and hence the Weil pairing becoming important for public key cryptosystem .

The another difficulty of computing the pairing is how to chose the rational functions and how to chose *A* and *B* coefficient on elliptic curve .

The more research for supersingularity of elliptic curve and isomorphism among curves in the same field and defined elliptic curve over complex finite field we see necessary for study the Weil pairing .

References

1. K.Araki , T. Satoh & S. Miura (**Overview Of Elliptic curve Cryptography)** Proc.199A8,International Workshop on Practice and Theory in Public Key Cryptography (PKC' 98) LNCS, Vol 1431,Springer-Verlag 1998, pp. 29-49.
2. N. Boston & S. Knoop **(Supersingular Curves and Weil Pairing in Elliptic Curve Cryptography)** Math. 842 , final project 2004 .
3. J . E. Cremona **(Algorithms For Modular Elliptic Curves)** second edition , Cambridge University , press , Cambridge 2007
4. J . E. Cremona , T .A. Fisher , C.O'Neill , M Stoll **(Explicit *n*-descent on Elliptic Curves)** II Geometry J.reine angew . Math . 632 (2009) , 63-48
5. K. Eisentrager , K. Lauter & P.L. Montgomery **(Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation)** . CT-RSA 2003, Lecture Notes in Computer Science, Vol. 2612, pp. 343-354, Springer-Verlag, 2003
6. E.V. Flynn , C. Grattoni **(Descent via isogeny on elliptic curves with large rational torsion Subgroups)** J. Symb. Comp. 43 (2008), 293–303.
7. S.D. Galbraith **(The Weil Pairing on Elliptic Curves Over C)** September 2005
8. S. F. Ibraheem **(Using transformation in Elliptic Curve Equations)** M.Sc. thesis , University of Technology , Baghdad 2005 .
9. A.J. Menezes **(Elliptic Curve Public Key Cryptosystems)** Klawer Academic , publish 1993 .
10. J.H. Silverman **(The Arithmetic of Elliptic Curves)** Graduate Text in Mathematics (GTM) 106,Springer-Verlag 1986.
11. S. Stamminger **(Explicit 8-desent on Elliptic curves)** Ph.D thesis , international University Bremen 2005
12. WWW.Certicom.com .