Southeast Asian Bulletin of Mathematics (2017) 41: 301–310

Southeast Asian Bulletin of Mathematics
© SEAMS. 2017

Some Property of Weil Pairing on an Elliptic Curve

Tomoko Adachi
Department of Information Science, Toho University, Miyama 2-2-1, Funabashi, Chiba, Japan
Email: adachi@is.sci.toho-u.ac.jp

Hiroki Adachi
Toho University, Japan
Email: tgv2215_hiro@yahoo.co.jp

Received 28 August 2014
Accepted 28 December 2014

Communicated by K.P. Shum

AMS Mathematics Subject Classification(2000): 11G07, 14H52

Abstract. Weil pairing plays an important role in elliptic curve cryptosystems, when we discuss about discrete log problem on an elliptic curve E defined over F_q, where q is a prime or a prime power. However, its calculation is very complex. In this paper, we give some property when we calculate the Weil pairing of an elliptic curve.

Keywords: Weil pairing; Elliptic Curve; Miller's Algorithm.

1. Introduction

Weil pairing play an important role in elliptic curve cryptosystems. Elliptic curve cryptosystems were proposed independently by Miller [4] and by Koblitz [2]. We have public key cryptosystems based on the discrete logarithm in the multiplicative group of a finite field. We do the same in the group under addition of points of an elliptic curve E defined over a finite field F_q, where q is a prime or a prime power. Menezes et al. [3] found a new approach to the discrete log problem on an elliptic curve E defined over F_q. Namely, they used the Weil pairing to embed the group E into the multiplicative group of some extension field F_{q^k}. Boneh and Franklin [1] gave an idea of Identity-based encryption from the Weil pairing. Okamoto and Takashima [6] gave a new idea of functional encryption of an elliptic curve. The Weil pairing of an elliptic curve is utilized

to cryptosystems, since the calculation on an finite group of an elliptic curve is very complex and that of the Weil pairing is more complex.

The goal of this paper is to find some property of the Weil pairing in order to reduce the calculation of the Weil pairing. In this paper, we give some property of Weil pairing on an elliptic curve.

2. Weil Pairing of an Elliptic Curve

In this section, we describe elliptic curve and the Weil pairing. We refer to [7]. For recent study in elliptic curves and singular curves over finite fields, see [8].

Let K be a field, let $\bar{K}$ be a fixed algebraic closure of K, let a_1, a_3, a_2, a_4, $a_6 \in \bar{K}$, and let $\mathcal{O} = (\infty, \infty)$ be an extra point out at infinity. We generally write the Weierstrass equation for an elliptic curve as follows;

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

$\mathcal{O}$ is considered as a point of E. If a_1, a_3, a_2, a_4, $a_6 \in K$, then E is said to be defined over K and is denoted by E/K.

If $\mathrm{char}(\bar{K}) \neq 2, 3$, the equation 1 is simple formed to

$$E : y^2 = x^3 + ax + b, \tag{2}$$

where $a, b \in \bar{K}$. Here, $D := 4a^3 + 27b^2 \neq 0$ holds.

Definition 2.1. [5] *Let E/K be an elliptic curve. The following quotient field is called the function field of E.*

$$\bar{K}(E) := \bar{K}[X]/\{f \in K[X] : f(P) = 0 \quad \forall P \in E\}$$

Definition 2.2. [7] *Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' be the line through R and $\mathcal{O}$. Then L' intersects E at R, $\mathcal{O}$, and a third point. We denote that third point by $P \oplus Q$.*

Proposition 2.3. [7] *The law $\oplus$ of Definition has the following properties.*

(a) *If a line L intersects E at the points P, Q, R, then $(P \oplus Q) \oplus R = \mathcal{O}$.*
(b) *$P \oplus \mathcal{O} = \mathcal{P}$ for all $P \in E$.*
(c) *$P \oplus Q = Q \oplus P$ for all $P, Q \in E$.*
(d) *Let $P \in E$. There is a point of E, denoted by $\ominus P$, satisfying $P \oplus (\ominus P) = \mathcal{O}$.*
(e) *Let $P, Q, R \in E$. Then $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$. In other words, the law $\oplus$ makes E into an abelian group with identity element $\mathcal{O}$.*

(f) *Suppose that E is defined over K. Then*

$$E(K) := \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \mathcal{O}$$

is a subgroup of E.

From here on, we drop the special symbols $\oplus$ and $\ominus$ and simply write $+$ and $-$ for the group operation on an elliptic curve E. For an integer m and $P \in E$, we let

$$[m]P := \begin{cases} P + \cdots + P & m > 0 \\ -m(-P) & m < 0 \\ \mathcal{O} & m = 0. \end{cases}$$

Definition 2.4. [7] *Let E be an elliptic curve and let m be a positive integer. The m-torsion subgroup of E, denoted by $E[m]$, is the set of points of E of order m,*

$$E[m] := \{P \in E : [m]P = \mathcal{O}\}.$$

The torsion subgroup of K, denoted by E_{tors}, is the set of points of finite order,

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

If E is defined over K, then $E_{tors}(K)$ denotes the points of finite order in $E(K)$.

Proposition 2.5. [7] *Let E be an elliptic curve and let m be an nonzero integer.*

(a) $\deg[m] = m^2$.

(b) *If $m \neq 0$ in K, i.e., if either $char(K) = 0$ or $p = char(K) > 0$ and $p \not| m$, then*

$$E[m] = Z/mZ \times Z/mZ$$

(c) *If $char(K) = p > 0$, then one of the following is true:*
(c-1) *$E[p^e] = \{\mathcal{O}\}$ for all $e = 1, 2, 3, \ldots$.*
(c-2) *$E[p^e] = Z/p^eZ$ for all $e = 1, 2, 3, \ldots$.*

The divisor group of an elliptic curve E, denoted by $\mathrm{Div}(E)$, is the free abelian group generated by the points of E. Thus a divisor $D \in \mathrm{Div}(E)$ is a formal sum

$$D = \sum_{P \in E} n_P(P) \qquad n_P \in Z,$$

where all integers n_P are equal to 0 but finitely many $P \in E$. The degree of D is defined by

$$\deg D = \sum_{P \in E} n_P.$$

The divisors of degree 0 form a subgroup of $\mathrm{Div}(E)$, which we denote by

$$\mathrm{Div}^0(E) = \{D \in \mathrm{Div}(E) : \deg D = 0\}.$$

Assume that the elliptic curve E is smooth, that is, $D \neq 0$, and let $f \in \bar{K}(E)$. Then we can associate to f the divisor $\mathrm{div} f$ given by

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P).$$

Definition 2.6. [7] *A divisor $D \in Div(E)$ is principal if it has the form $D = div(f)$ for some $f \in \bar{K}(E)$. Two divisors are linearly equivalent, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The divisor class group (or Picard group) of E, denoted by $Pic(E)$, is the quotient of $Div(E)$ by its subgroup of principal divisors.*

Let E/K be an elliptic curve. From here, we fix an integer $m \geq 2$, which we assume to be prime to $p = \mathrm{char}(K)$ if $p > 0$.

We define the Weil e_m-pairing

$$e_m : E[m] \times E[m] \longrightarrow \mu_m \tag{3}$$

by setting

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

where $X \in E$ is any point such that $G(X + S)$ and $g(X)$ are both defined and nonzero. μ_m denotes the group of m-th roots of unity. Note that although the function g is well-defined only up multiplication by an element of $\bar{K}^*$, the value of $e_m(S, T)$ does not depend on this choice.

Proposition 2.7. [7] *The Weil e_m-pairing has the following properties:*

(a) *It is bilinear:*

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

$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2).$$

(b) *It is alternating:* $e_m(T, T) = 1$.
So, in particular, $e_m(S, T) = e_m(T, S)^{-1}$.

(c) *It is non-degenerate:*

$$\textit{If} \quad e_m(S, T) = 1 \quad \textit{for all} \quad S \in E[m], \quad \textit{then} \quad T = O.$$

(d) *It is Galois invariant:*

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma) \qquad \textit{for all} \quad \sigma \in G_{\bar{K}/K}.$$

(e) *It is compatible:*

$$e_{mm'}(S,T) = e_m([m']S,T) \quad \textit{for all } S \in E[mm'] \textit{ and } T \in E[m].$$

3. Identity-Based Encryption Scheme From the Weil Pairing

In this section, we describe a basic identity-based encryption from the Weil pairing. It is not secure against an adaptive chosen cipher-text attack. However, it is an important idea and the basic scheme is to make the presentation easy.

This scheme is specified by the following four randomized algorithms. We let k be the security parameter given to the setup algorithm.

The message space is $\mathcal{M} = \{0,1\}^n$. The cipher-text space is $\mathcal{C} = E/F_p \times \{0,1\}^n$. The system parameters are p, n, P, P_{pub}, G and H. The master-key is $s \in Z_q^*$.

(a) Setup. The algorithm works as follows:
  (a-1) Choose a large k-bit prime p such that $p = 2 \bmod 3$ and $p = 6q-1$ for some prime $q > 3$. Let E be the elliptic curve defined by $y^2 = x^3 + 1$ over F_p. Choose an arbitrary $P \in E/F_p$ of order q.
  (a-2) Pick a random $s \in Z_q^*$ and set $P_{pub} = sP$.
  (a-3) Choose a cryptographic hash function $H : F_{p^2} \to \{0,1\}^n$ for some n. Choose a cryptographic hash function $G : \{0,1\}^* \to F_p$. The security analysis will view H and G as random oracles.

(b) Extract. For a given string ID $\in \{0,1\}^*$, the algorithm builds a private key d as follows:
  (b-1) Use the map from a given string ID $\in \{0,1\}^*$ to a point $Q_{\mathrm{ID}} \in E/F_p$ of order q. At first, compute $y_0 = G(\mathrm{ID})$ and $x_0 = ({y_0}^2 - 1)^{1/3} \bmod p$. Next, let $Q = (x_0, y_0) \in E/F_p$, and set $Q_{\mathrm{ID}} = 6Q$. Then Q_{ID} has order q as required.
  (b-2) Set the private key $d_{\mathrm{ID}} = sQ_{\mathrm{ID}}$ where s is the master key.

(c) Encrypt. To encrypt $M \in \mathcal{M}$ under the public key ID do the following:
  (c-1) Use the map from the public key ID into a point $Q_{\mathrm{ID}} \in E/F_p$ of order q. At first, compute $y_0 = G(\mathrm{ID})$ and $x_0 = ({y_0}^2 - 1)^{1/3} \bmod p$. Next, let $Q = (x_0, y_0) \in E/F_p$, and set $Q_{\mathrm{ID}} = 6Q$. Then Q_{ID} has order q as required.
  (c-2) Choose a random $r \in Z_q$.
  (c-3) Set the cipher-text to be $C = \langle rP, M \oplus H(g_{\mathrm{ID}}^r) \rangle$ where $g_{\mathrm{ID}}^r = \hat{e}(Q_{\mathrm{ID}}, P_{pub}) \in F_{p^2}$.

(d) Decrypt. Let $C = \langle U, V \rangle \in \mathcal{C}$ be a cipher-text encrypted using the public key ID. If $U \in E/F_p$ is not a point of order q, reject the cipher-text. Otherwise, to decrypt C using the private key d_{ID} compute $V \oplus H(\hat{e}(d_{\mathrm{ID}}, U)) = M$.

Here, the map $\hat{e}$ in (c-3) is Weil pairing. It is defined by equation (3), and has properties of Proposition 2.7. Since Weil pairing is a bilinear map, it is utilized to identity-based encryption scheme.

4. Computing the Weil Pairing

The definition of the Weil pairing requires functions having specified divisors. In this section, we describe to computing the Weil pairing. Miller's algorithm computes such functions in linear time, and makes pairings practical for use in applications to cryptography. We refer to [5].

Lemma 4.1. [5] *For $P_1, P_2 \in E$ and $f_1, f_2 \in \bar{K}(E)$, let $Div^0(E) \ni D_1 = (P_1) - (\mathcal{O}) + div(f_1)$, $D_2 = (P_2) - (\mathcal{O}) + div(f_2)$. Then it holds*

$$D_1 + D_2 = (P_3) - (\mathcal{O}) + div(f_1 f_2 f_3),$$

where $P_3 = P_1 + P_2$ and $f_3 \in \bar{K}(E)$ is represented $f_3 = \ell/v$ by the line ℓ which connect to P_1 and P_2, and by the line v which connect to P_3 and $\mathcal{O}$.

Algorithm 4.2. [5] Div-add$((P_1, f_1), (P_2, f_2))$

In: $\mathrm{Div}^0(E) \ni D_1 = (P_1) - (\mathcal{O}) + \mathrm{div}(f_1)$, $D_2 = (P_2) - (\mathcal{O}) + \mathrm{div}(f_2)$
$(P_1, P_2 \in E, \quad f_1, f_2 \in \bar{K}(E))$

Out: $\mathrm{Div}^0(E) \ni D_1 + D_2 = (P_3) - (\mathcal{O}) + \mathrm{div}(f)$
$(E \ni P_3 = P_1 + P_2, \quad f \in \bar{K}(E))$

(1) $P_3 = P_1 + P_2$
(2) $f_3 = \ell/v$
(3) Output $(P_3, f_1 f_2 f_3)$

Algorithm 4.3. [5]

In: a positive integer $m = \sum_{i=0}^{n-1} m_i 2^i \quad (m_i \in \{0,1\}, m_{n-1} \neq 0), \quad P \in E[m]$

Out: $f_1 \in \bar{K}(E)) \quad (\mathrm{div}(f_1) = m(P) - m(\mathcal{O})$

(1) Chose $f_0 \in \bar{K}(E))$.
(2) $(Y, f) = \text{div-add}((P, f_0), (P, f_0)). \qquad f_2 = {f_0}^2$.
(3) For $i = n-2, \cdots, 0$, do
  if $m_i = 1$, then
    $(Y, f) = \text{Div-add}(\text{Div-add}((Y, f), (Y, f)), (P, f_0))$.
    $f_2 = {f_2}^2 * f_0$.
  else $(Y, f) = (\text{Div-add}((Y, f), (Y, f))$
    $f_2 = {f_2}^2$.
  next i
(4) Output f/f_2 $(= f_1)$

5. Our Result : Some Property of Weil Pairing

In this section, we describe our new result. Although we do programming of Algorithm 4.3 in section 4, we find that the output – the function $f_1 = f/f_2$ – has features quite its own for the input – a positive integer m.

Table 1: Results of $m = 1 \sim 15$.

m	$m_{(2)}$	Y	f	f_2	f_1
1	1	$2P$	$f_0^2(l/v)$	f_0^2	l/v
2	10	$4P$	$f_0^4(l/v)^3$	f_0^4	$(l/v)^3$
3	11	$5P$	$f_0^5(l/v)^4$	f_0^5	$(l/v)^4$
4	100	$8P$	$f_0^8(l/v)^7$	f_0^8	$(l/v)^7$
5	101	$9P$	$f_0^9(l/v)^8$	f_0^9	$(l/v)^8$
6	110	$10P$	$f_0^{10}(l/v)^9$	f_0^{10}	$(l/v)^9$
7	111	$11P$	$f_0^{11}(l/v)^{10}$	f_0^{11}	$(l/v)^{10}$
8	1000	$16P$	$f_0^{16}(l/v)^{15}$	f_0^{16}	$(l/v)^{15}$
9	1001	$17P$	$f_0^{17}(l/v)^{16}$	f_0^{17}	$(l/v)^{16}$
10	1010	$18P$	$f_0^{18}(l/v)^{17}$	f_0^{18}	$(l/v)^{17}$
11	1011	$19P$	$f_0^{19}(l/v)^{18}$	f_0^{19}	$(l/v)^{18}$
12	1100	$20P$	$f_0^{20}(l/v)^{19}$	f_0^{20}	$(l/v)^{19}$
13	1101	$21P$	$f_0^{21}(l/v)^{20}$	f_0^{21}	$(l/v)^{20}$
14	1110	$22P$	$f_0^{22}(l/v)^{21}$	f_0^{22}	$(l/v)^{21}$
15	1111	$23P$	$f_0^{23}(l/v)^{22}$	f_0^{23}	$(l/v)^{22}$

Let $m_{(2)}$ to be a binary number of a positive integer m. Table 1 shows experiment results in the case of the input value m is from 1 to 15.

Now, we pay attention to the case that the maximal digit of $m_{(2)}$ is equal to one, and all others digits of $m_{(2)}$ are equal to zero. For example, $m_{(2)}$ is 1, 10, 100, 1000, $\cdots$, or 1000000000000000. Table 2 shows experiment results of the such case. In the such case, we observe index n of the function $f_1 = (l/v)^n$. Then, we obtain the following theorem.

Theorem 5.1. *Let m to be a positive integer, that is, input value. And let $m_{(2)}$ to be a binary number of m. Suppose that the maximal digit of $m_{(2)}$ is equal to one, and all others digits of $m_{(2)}$ are equal to zero, that is, there is an nonnegative integer a such that $m = 2^a$. Then, the index n of the output value $f_1 = (l/v)^n$, for the input $m = 2^a$, satisfies as follows:*

$$n = 2^{a+1} - 1. \tag{4}$$

Proof. By the mathematical induction method, we prove the theorem.

When $a = 0$, it is trivial.

Suppose that the equation (4) holds when $a = k$ for an nonnegative integer k. When $a = k + 1$, we obtain the following:

Table 2: Results of $m_{(2)} = 10 \cdots 0$.

m	$m_{(2)}$	f_1	n
$1 = 2^0$	1	l/v	$1 = 2 - 1$
$2 = 2^1$	10	$(l/v)^3$	$3 = 4 - 1$
$4 = 2^2$	100	$(l/v)^7$	$7 = 8 - 1$
$8 = 2^3$	1000	$(l/v)^{15}$	$15 = 16 - 1$
$16 = 2^4$	10000	$(l/v)^{31}$	$31 = 32 - 1$
$32 = 2^5$	100000	$(l/v)^{63}$	$63 = 64 - 1$
$64 = 2^6$	1000000	$(l/v)^{127}$	$127 = 128 - 1$
$128 = 2^7$	10000000	$(l/v)^{255}$	$255 = 256 - 1$
$256 = 2^8$	100000000	$(l/v)^{511}$	$511 = 512 - 1$
$512 = 2^9$	1000000000	$(l/v)^{1023}$	$1023 = 1024 - 1$
$1024 = 2^{10}$	10000000000	$(l/v)^{2047}$	$2047 = 2048 - 1$
$2048 = 2^{11}$	100000000000	$(l/v)^{4095}$	$4095 = 4096 - 1$
$4096 = 2^{12}$	1000000000000	$(l/v)^{8191}$	$8191 = 8192 - 1$
$8192 = 2^{13}$	10000000000000	$(l/v)^{16383}$	$16383 = 16384 - 1$
$16384 = 2^{15}$	100000000000000	$(l/v)^{32767}$	$32767 = 32768 - 1$
$32768 = 2^{16}$	1000000000000000	$(l/v)^{65535}$	$65535 = 65536 - 1$

$$
\begin{aligned}
n &= 1 + 2 + 4 + 8 + 16 + \cdots + 2^k + 2^{k+1} \\
&\quad \text{(By additional repetition of Algorithm 4.3.)} \\
&= (2^{k+1} - 1) + 2^{k+1} \\
&\quad \text{(By the assumption of the mathematical induction method.)} \\
&= 2 \times 2^{k+1} - 1 \\
&= 2^{(k+1)+1} - 1
\end{aligned}
$$

Hence, the equation (4) holds when $a = k + 1$. Therefore, the equation (4) holds, for an nonnegative integer a. ■

Next, we pay attention to the case that the maximal and minimal digits of $m_{(2)}$ are equal to one, and all others digits of $m_{(2)}$ are equal to zero. For example, $m_{(2)}$ is 11, 101, 1001, $\cdots$, or 1000000001. Table 3 shows experiment results of the such case. In the such case, we observe index n of the function $f_1 = (l/v)^n$. Then, we obtain the following theorem.

Theorem 5.2. *Let m to be a positive integer, that is, input value. And let $m_{(2)}$ to be a binary number of m. Suppose that the maximal and minimal digits of $m_{(2)}$ are equal to one, and all others digits of $m_{(2)}$ are equal to zero, that is, there is a positive integer a such that $m = 2^a + 1$. Then, the index n of the output value $f_1 = (l/v)^n$, for the input $m = 2^a + 1$, satisfies as follows:*

$$n = 2^{a+1}. \tag{5}$$

Table 3: Results of $m_{(2)} = 10 \cdots 01$.

m	$m_{(2)}$	f_1	n
$3 = 2^1 + 1$	11	$(l/v)^4$	$4 = 2^2$
$5 = 2^2 + 1$	101	$(l/v)^8$	$8 = 2^3$
$9 = 2^3 + 1$	1001	$(l/v)^{16}$	$16 = 2^4$
$17 = 2^4 + 1$	10001	$(l/v)^{32}$	$32 = 2^5$
$33 = 2^5 + 1$	100001	$(l/v)^{64}$	$64 = 2^6$
$65 = 2^6 + 1$	1000001	$(l/v)^{128}$	$128 = 2^7$
$129 = 2^7 + 1$	10000001	$(l/v)^{256}$	$256 = 2^8$
$257 = 2^8 + 1$	100000001	$(l/v)^{512}$	$512 = 2^9$
$513 = 2^9$	1000000001	$(l/v)^{1024}$	$1024 = 2^{10}$

Proof. By the mathematical induction method, we prove the theorem.

When $a = 1$, it is trivial.

Suppose that the equation (5) holds when $a = k$ for a positive integer k. When $a = k + 1$, we obtain the following:

$$\begin{aligned} n &= 1 + 2 + 4 + 8 + 16 + \cdots + 2^k + 2^{k+1} + 1 \\ &\quad \text{(By additional repetition of Algorithm 4.3.)} \\ &= (2^{k+1} - 1) + 2^{k+1} + 1 \\ &\quad \text{(By Theorem 5.1.)} \\ &= 2 \times 2^{k+1} - 1 + 1 \\ &= 2^{(k+1)+1} \end{aligned}$$

Hence, the equation (5) holds when $a = k + 1$. Therefore, the equation (5) holds, for an nonnegative integer a. ∎

References

[1] D. Boneh, M.K. Franklin, Identity-based encryption from the weil pairing, *SIAM J. Comput.* **32** (2003) 586–615.

[2] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation* **48** (1987) 203–209.

[3] A.J. Menezes, T. Okamoto, S.A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory* **39** (5) (1993) 80–89.

[4] V.S. Miller, Use of elliptic curves in cryptography, In: H.C. Williams(eds), *Advances in Cryptology–Crypto '85*, Springer-Verlag, Berlin, 1986, 417–426.

[5] A. Miyaji, *Cryptography In Algebraic Aspects, – From Basic Number Theory to Implementing Elliptic Curve Cryptography*, Nippon Hyoron Sha Co., Ltd., Tokyo, 2012.

[6] T. Okamoto, K. Takashima, Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, In: T. Rabin (Eds.), *CRYPTO 2010*, Springer-Verlag, Berlin, 2010, 191–208,

[7] J.H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd Edition, Springer-Verlag, New York, 2009.

[8] A. Tekcan, Elipitic curves and some singular curves over finite fields, *Southeast Asian Bull. Math.* **35** (2011) 859–867.

Copyright of Southeast Asian Bulletin of Mathematics is the property of Southeast Asian Bulletin of Mathematics and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.