

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang  
Scribe: Iftikhar A Burhanuddin  
burhanud@usc.edu  
Classes #9 - March 05, 2002

**Administrivia:** Scribe notes for classes #8 are online at the course web-page: <http://www-rcf.usc.edu/~mdhuang/cs599>

**Today's class:**

1. Explicit Definition of Weil Pairing
2. Functions and Divisors
3. Constructing functions using the doubling trick
4. Properties of Weil Pairing

**I. Explicit Definition of Weil Pairing:**

Let  $l$  be a positive integer, not necessarily a prime. Given an elliptic curve  $E$  over a field  $K$ ,  $E/K$  the Weil pairing is defined as follows:

$$e_l : E[l] \times E[l] \rightarrow \mu_l \subseteq \overline{K}$$

where  $E[l]$  is the group of  $l$ -torsion points of  $E/K$ ,  $\mu_l$  is the group of the  $l$ -th roots of unity in  $K$  and is a subgroup of  $\overline{K}$ , the algebraic closure of  $K$ , which contains all elements algebraic over  $K$ . Please note that  $K$  can be any of a large choice of fields but we'll be applying this pairing to the field of our primary interest - finite fields.

This pairing has two interesting properties. Say  $X, Y, Z \in E[l]$  and  $\oplus$  denotes addition on the curve and  $\cdot$  denotes multiplication in  $\mu_l$

1. Bilinearity:

$$e_l(X \oplus Y, Z) = e_l(X, Z) \cdot e_l(Y, Z)$$
$$e_l(X, Y \oplus Z) = e_l(X, Y) \cdot e_l(X, Z)$$

2. Non-degeneracy:

$$\text{for all } X \in E[l], e_l(X, Y) = 1 \Leftrightarrow Y = O \text{ (the point at } \infty)$$

**II. Functions and Divisors**

A divisor is a formal, finite sum of points in  $E(\overline{K})$ . Say divisor  $D$ , is given by  $D = \sum_i a_i P_i$ , where  $P_i \in E(\overline{K})$ ,  $a_i \in \mathbf{Z}$  then degree of  $D$  is defined to be the sum of the coefficients,  $deg(D) := \sum_i a_i$

The set of divisors of the curve  $E$ ,  $Div(E)$  forms a group and the divisors of degree 0,  $Div^0(E)$  form a subgroup of  $Div(E)$ .

$$Div^0(E) = \{D \mid deg(D) = 0\}$$

Let  $f$  be a (rational) function on  $E$ , then the divisor  $div(f)$ , sometimes simply denoted by  $(f)$  is defined as

$$div(f) = \sum_i a_i P_i - \sum_i b_i Q_i \in Div^0(E)$$

where  $a_i, b_i > 0$ ,  
 $P_i$  is a zero of order  $a_i$   
 $Q_i$  is a pole of order  $b_i$

*Remark:* Divisors are a way of keeping track of zeros and poles of a function of a curve and are related to the jacobian of a curve.

*Fact:* Let  $f, g$  be functions on  $E$  then  $div(f.g) = div(f) + div(g)$

*Example 1:* Suppose  $P = (\alpha, \beta) \in E(\overline{K})$ ,  $-P = (-\alpha, \beta) \Rightarrow P \oplus (-P) = O$  and let  $l$  denote the line which passes through  $P$  and  $-P$ . Then  $div(l) = P + (-P) - 2O$

*Example 2:* Consider  $P, Q, R \in E(\overline{K})$  and  $P \oplus Q = R$  and let  $l$  represent the line which passes through  $P, Q$  and  $-R$ , then  $div(l) = P + Q + (-R) - 3O$

**Lemma 1:** Suppose  $P_1, P_2, P_3 \in E(\overline{K})$  and  $P_1 \oplus P_2 = P_3$  then there exists a rational function (which is a quotient of two linear functions)  $f$ , such that

$$P_1 + P_2 = div(f) + P_3 + O$$

subtracting  $2O$  from both sides  
 $\Rightarrow [P_1 - O] + [P_2 - O] = div(f) + [P_3 - O]$

*Proof:* Given  $P_1, P_2, P_3$ , there exists a line  $l$  such that  $div(l) = P_1 + P_2 + (-P_3) - 3O$ . Also there exists a line  $l'$  such that  $div(l') = P_3 + (-P_3) - 2O \Rightarrow div(l'^{-1}) = -P_3 - (-P_3) + 2O$ . Let  $f = l.l'^{-1}$  then  $div(f) = div(l.l'^{-1}) = div(l) + div(l'^{-1}) = P_1 + P_2 - P_3 - O \quad \diamond$

Now let's consider a function  $\sigma$  defined as follows:

$$\begin{aligned} \sigma : Div(E) &\rightarrow E(\overline{K}) \\ \sum_i a_i P_i &\mapsto \oplus_i a_i P_i \end{aligned}$$

*Remark:* More generally, suppose  $D \in Div^0(E)$ , if  $\sigma(D) = P$  then there exists a function  $f$ , such that  $D = div(f) + [P - O]$ .

*Example:* Say  $P, Q \in E(\overline{K})$ , then  $\sigma(P - Q) = P \oplus (-Q)$

The *support* of a divisor  $D$  is the set of points in the formal sum and is denoted by  $\text{supp } D$ . *Example:* i)  $D = P - O$ ,  $\text{supp } D = \{P, O\}$ , ii) support of  $(P \oplus X) - X$  is  $\{P \oplus X, X\}$ , iii)  $D = P + Q + R - 3O$ , then  $\text{supp } D = \{P, Q, R, O\}$

For all  $P \in E[l]$ ,  $P \neq Q$  choose a divisor  $D_P \in Div^0(E)$  so that  $\sigma(D_P) = P$  and  $\text{supp } D_P \cap \text{supp } D_Q = \emptyset$  for all  $P, Q \in E[l]$ ,  $P \neq Q$

$P - O$  is a good candidate for  $D_P$  but to meet the disjoint support criterion we'll take  $D_P = (P \oplus X_P) - X_P$  where  $X_P \in E(\overline{K})$ ,  $X_P \neq X_Q$  if  $P \neq Q$ , that is, for each torsion point we select a different  $X$ . In fact there are infinitely many ways to build  $D_P$ .

So now given  $D = \sum_i a_i P_i \in \text{Div}^0(E)$  and a function  $f$  on  $E$  such that no point in the support of  $D$  is a zero or pole for  $f$ , it makes sense to evaluate  $f$  at  $D$ .

Let's define  $f$  evaluated at  $D$  as follows  $f(D) := \prod_i f(P_i)^{a_i}$

*Example:*  $f(P - Q) = \frac{f(P)}{f(Q)}$  and  $P$  and  $Q$  are neither zeros or poles of  $f$ .

*Remark:* Suppose  $D \in \text{Div}^0(E)$  then there's no effect if we multiplied  $f(D)$  by a constant  $c$

$$cf(D) = \prod_i c^{a_i} f(P_i)^{a_i} = c^{\sum_i a_i} \prod_i f(P_i)^{a_i} = c^0 \prod_i f(P_i)^{a_i} = f(D)$$

We've seen how to construct divisors  $D_P$ , for each  $l$ -torsion point such that  $\sigma(D_P) = P$  and  $\text{supp } D_P \cap \text{supp } D_Q = \emptyset$ , for all  $P \neq Q$ . Next we'll see how to construct  $f_P$  for  $P \in E[l]$  such that  $\text{div}(f_P) = lD_P$ . Once we've seen that we can evaluate  $f_P(D_Q)$  and  $f_Q(D_P)$  and then we'll be ready to define Weil Pairing as follows:

$$e_l(P, Q) = \begin{cases} 1, & P = Q \\ \frac{f_P(Q)}{f_Q(P)}, & \text{otherwise} \end{cases}$$

### III. Constructing functions using the doubling trick:

**Goal:** To construct  $f_P$  such that  $\text{div}(f_P) = lD_P$

Recall that  $\sigma(D) = P \in E(\overline{K})$ , where  $D \in \text{Div}^0(E)$  then there exists  $f$  such that  $D = \text{div}(f) + [P - O]$ . In particular if  $\sigma(D) = O$ , then there exists a function  $f$  such that  $D = \text{div}(f)$ .

Suppose  $P \in E[l]$ , we've seen how to construct a divisor  $D_P$  such that  $\sigma(D_P) = P$ . Now  $\sigma(lD_P) = l.P = O$  (as  $P$  is a  $l$ -torsion point) then there exists a function  $f_P$  such that  $\text{div}(f_P) = lD_P$  and this gives us a proof of existence.

$\sigma(D_P) = \sigma([P - O]) \Rightarrow$  there exists  $f$  such that  $D_P = \text{div}(f) + [P - O]$   
To be specific let's take  $D_P = X - Y$ . So

$$X - Y = \text{div}(f) + [P - O] \Rightarrow [X - O] + [(-Y) - O] = \text{div}(g) + [P - O]$$

by *Lemma 1*. Also we know that there exists  $L$  such that

$$\text{div}(L) = Y + (-Y) - 2O \Rightarrow (-Y) - O = \text{div}(L) - [Y - O]$$

Substituting we get

$$\begin{aligned} [X - O] + \text{div}(L) - [Y - O] &= \text{div}(g) + [P - O] \\ \Rightarrow \text{div}(L) + [X - Y] &= \text{div}(g) + [P - O] \\ \Rightarrow [X - Y] &= \text{div}(g) - \text{div}(L) + [P - O] \\ &= \text{div}(g.L^{-1}) + [P - O] \end{aligned}$$

Observe that the degree of resulting function  $g.L^{-1}$  is bounded as it is of the form  $\frac{L_1}{L_2 L_3}$ , where  $L_1, L_2, L_3$  are linear functions.

Consider  $D_P = \text{div}(f) + [P - O]$ . Multiplying both sides by 2 gives

$$2D_P = 2\text{div}(f) + 2[P - O] = \text{div}(f^2) + 2[P - O]$$

*Example:* Suppose  $l = 4$ , given an  $l$ -torsion point  $P$ , let's construct a function using a "Doubling Trick" such that the divisor of the function is  $4D_P$  where  $\sigma(D_P) = P$ .

We know that  $\sigma(2[P - O]) = 2P$  and there exists  $f_1$  such that  $2[P - O] = \text{div}(f_1) + [(2P) - O]$

Substituting we get

$$2D_P = \text{div}(f^2) + \text{div}(f_1) + [(2P) - O] = \text{div}(f^2 \cdot f_1) + [(2P) - O]$$

Multiplying by 2 gives

$$4D_P = \text{div}((f^2 \cdot f_1)^2) + 2[(2P) - O]$$

The new function  $(f^2 \cdot f_1)^2$  is of bigger degree.

$$\sigma(2[(2P) - O]) = 4P = \sigma[(4P) - O]$$

then there exists  $f_2$  such that  $2[(2P) - O] = \text{div}(f_2) + [(4P) - O]$ . Substituting we get

$$4D_P = \text{div}((f^2 \cdot f_1)^2) + \text{div}(f_2) + [(4P) - O]$$

Say  $P$  is a 4-torsion point, so we've constructed a function whose divisor is  $4D_P$

Suppose  $l = 2l_1 + 1$ , odd number and inductively we have constructed a function  $F_1$  such that  $l_1 D_P = \text{div}(F_1) + [(l_1 P) - O]$ . Multiplying by 2, gives us

$$2l_1 D_P = \text{div}(F_1^2) + 2[(l_1 P) - O]$$

On the hand

$$\sigma(2[(l_1 P) - O]) = (2l_1 P) = \sigma[(2l_1 P) - O]$$

then there exists  $g$ , such that  $2[(l_1 P) - O] = \text{div}(g) + [(2l_1 P) - O]$ . Substituting we get

$$2l_1 D_P = \text{div}(F_1^2 g) + 2[(l_1 P) - O]$$

Adding  $D_P$  on both sides we get

$$l D_P = \text{div}(F_1^2 g) + 2[(l_1 P) - O] + D_P$$

Now

$$\sigma(2[(l_1 P) - O] + D_P) = 2l_1 P + P = l P = O$$

then there exists  $h$ , such that

$$\text{div}(h) = (2l_1P) - O + D_P \Rightarrow lD_P = \text{div}(F_1^2gh)$$

$F_1$  is made up of  $O(\log l)$  many functions and our final function  $F_1^2gh$  has  $O(\log)$  many functions.

Let's try another example, suppose  $l = 11$ . We saw that

$$4D_P = \text{div}((f^2f_1)^2f_2) + [(4P) - O]$$

Hence

$$\sigma([(4P) - O]) + D_P = 5P = \sigma[(5P) - O](*)$$

then there exists  $f_3$  such that  $[4P - O] + D_P = (f_3) + [(5P) - O]$ . Adding  $D_P$  on both sides to  $(*)$  gives us

$$5D_P = \text{div}((f_2f_1)^2f_2) + \text{div}(f_3) + [(5P) - O]$$

And let  $F_1 = (f^2f_1)^2 + f_2f_3$  and now we can use  $F_1$  to construct  $11D_P$

So every reduction step we add 2 more functions i.e. another function of bounded degree.

*Problem:*

These functions sit in a field which contains the ground field and the (coordinates of the)  $l$ -torsion points:  $K(E[l])$ . If  $[K(E[l]):K]$ , the degree of the extension of  $K(E[l])$  over  $K$ , is reasonable bounded, we are in good shape to do computation. One such scenario is when we consider super singular curves when  $[K(E[l]) : K] \leq 6$ . In general the degree is (exponentially) big.

Hence we've seen an algorithm to evaluate  $f_P(D_Q)$  in  $O(\log l)$  field operations over  $K(E[l])$ .

#### IV. Properties of Weil Pairing:

We'll prove that  $(\frac{f_P(D_Q)}{f_Q(D_P)})^l = 1$ , and hence show how the Weil Pairing  $e_l(P, Q)$  is an  $l$ -th root of unity?

*Weil Reciprocity:* Suppose  $f, g$  two rational functions on  $E$ ,  $\text{div}(f)$  and  $\text{div}(g)$  have disjoint supports, then  $f(\text{div}(g)) = g(\text{div}(f))$ , that is the evaluation of  $f$  at  $\text{div}(g)$  equals the evaluation of  $g$  at  $\text{div}(f)$ . The proof is non-trivial and we take it to be a *fact*.

$$\begin{aligned} (f_P(D_Q))^l &= f_P(lD_Q) = f_P(\text{div}(f_Q)) = f_Q(\text{div}(f_P)) = f_Q(lD_P) = (f_Q(D_P))^l \\ &\Rightarrow (\frac{f_P(D_Q)}{f_Q(D_P)})^l = 1 \quad \diamond \end{aligned}$$

#### Bilinearity:

Let  $P, Q, R \in E[l]$ . As  $E[l]$  is a group  $P \oplus Q$  is also  $l$ -torsion point. We'll prove that the following equation is valid.

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

Let's start with the definition of the Weil Pairing and try simplifying the numerator and denominator.

$$e_l(P \oplus Q, R) = \frac{f_{P \oplus Q}(D_R)}{f_R(D_{P \oplus Q})}$$

First note that  $\sigma(D_P + D_Q) = P \oplus Q = \sigma(D_{P \oplus Q})$  and hence there exists a function  $h$  such that  $D_{P \oplus Q} + \text{div}(h) = D_P + D_Q$  ( $\boxtimes$ )

$$\begin{aligned} \text{div}(f_P f_Q) &= \text{div}(f_P) + \text{div}(f_Q) \\ &= lD_P + l\text{div}(h) \text{ from } (\boxtimes) \\ \Rightarrow \text{div}(f_P f_Q) &= lD_{P \oplus Q} + l\text{div}(h) = f_{P \oplus Q} + \text{div}(h^l) \\ \Rightarrow \text{div}(f_{P \oplus Q}) &= \text{div}(f_P f_Q h^{-l}) \end{aligned}$$

Therefore

$$\begin{aligned} f_{P \oplus Q}(D_R) &= (f_P f_Q h^{-l})(D_R) \\ &= f_P(D_R) f_Q(D_R) h^{-l}(D_R) \\ &= f_P(D_R) f_Q(D_R) h^{-l}(lD_R) \\ &= f_P(D_R) f_Q(D_R) h^{-l}(\text{div}(f_R)) \end{aligned}$$

Next observe that

$$\begin{aligned} f_R(D_{P \oplus Q}) &= f_R(D_P + D_Q - \text{div}(h)) \text{ from } (\boxtimes) \\ &= f_R(D_P) f_R(D_Q) f_R(\text{div}(h^{-1})) \end{aligned}$$

Finally plugging the simplified versions of the numerator and the denominator we get,

$$\begin{aligned} e_l(P \oplus Q, R) &= \frac{f_{P \oplus Q}(D_R)}{f_R(D_{P \oplus Q})} \\ &= \frac{f_P(D_R) f_Q(D_R)}{f_R(D_P) f_R(D_Q)} \\ &= e_l(P, Q) e_l(Q, R) \quad \diamond \end{aligned}$$

Recall that

$$e_l : E[l] \times E[l] \longrightarrow \mu_l$$

Say given  $T, P \in E[l]$  and they are related by  $T = mP$ , we are interested in computing  $m$ . Choosing another point  $Q \in E[l]$  we can compute  $\alpha = e_l(T, Q)$  and  $\beta = e_l(P, Q)$ .

We know that  $\alpha = e_l(T, Q) = e_l(mP, Q) = (e_l(P, Q))^m = \beta^m$  by property of Weil Pairing. So ECDLP among torsion points becomes equivalent to solving DLP in  $K(E[l])$ .

If  $K$  is a finite field, then each element of  $K$  is some torsion point and so we can employ this method. Moreover  $\mathbf{F}_p(E[l]) = \mathbf{F}_{p^i}$  for some  $i$ . So ECDLP is equivalent to solving DLP over an extension of the base field  $\mathbf{F}_p$ .

So given elliptic curve  $E/\mathbf{F}_p$  and points  $S, T$ , here's an algorithm to compute the  $m$  in  $T = mS$

1. Say  $l = | \langle S \rangle |$  and  $R \in E[l]$  such that  $R \notin \langle S \rangle \Leftrightarrow e_l(S, R) \neq 1$ .  
Picking  $R$  can be a *slight* problem.
2. Compute  $\alpha = e_l(T, R)$
3. Compute  $\beta = e_l(S, R)$
4. Solve for  $m$  in  $\beta^m = \alpha$  in  $\mathbf{F}_p(E[l])$

So the running time is sub exponential in the size of  $\mathbf{F}_p(E[l])$  and in general the degree of the extension  $[\mathbf{F}_p(E[l]) : \mathbf{F}_p]$  is large and doesn't give us better than exponential in the size of  $\mathbf{F}_p$ . One exception being the super singular case.

*Remark:* A refinement to the algorithm is that the problem encountered in step 1 can be avoided by working in  $\mathbf{F}_p(\mu_l)$