

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang  
Scribe: Iftikhar A Burhanuddin  
burhanud@usc.edu  
Classes #8 - February 26, 2002

**Administrivia:** Scribe notes for classes #6 and #7 are online at the course webpage: <http://www-rcf.usc.edu/~mdhuang/cs599>

**Today's class:**

1. Some math background
2. A friendly introduction to functions and divisors
3. Weil Paring
4. MOV attack

**I. Some math background**

Say  $K$  is a field and  $\overline{K}$  is the algebraic closure of  $K$ . An element  $\gamma \in \overline{K}$  is defined as being algebraic over  $K$  if  $\gamma$  satisfies a polynomial with coefficients in  $K$ :  $F(\gamma) = 0$  for some  $F(x) \in K[x]$ .

*Remark:* Let  $K$  is a number field (that is, it is a finite extension of  $\mathbf{Q}$ ) and we try to solve for  $x$  in  $x^2 + 3 = 0$  we notice that the solutions  $x = \pm\sqrt{3}i$  are algebraic over  $\mathbf{Q}$  but don't live in  $\mathbf{Q}$  but reside in an extension of degree 2 over  $\mathbf{Q}$ , namely  $\mathbf{Q}(\sqrt{3}i)$  but everything in  $\mathbf{Q}$  is algebraic over  $\mathbf{Q}$  as it satisfies a linear polynomial in  $\mathbf{Q}[x]$ .

Suppose the curve  $E/K$  is defined by the polynomial  $y^2 = x^3 + ax + b$ , where  $a, b \in K$  and we are interested in points on the curve are of the following form  $E(\overline{K}) = \{(\alpha, \beta) \mid \beta^2 = \alpha^3 + a\alpha + b\}$  where  $\alpha, \beta$  are algebraic over  $K$ . (Observe that  $\alpha$  is algebraic  $\Leftrightarrow \beta$  is algebraic).

Let's try and classify the torsion points of  $E/K$ . The set of 2-torsion points is  $\{(\alpha, 0) \mid \alpha^3 + a\alpha + b = 0\} \cup \{O\}$ . The 3-torsion points satisfy this equation  $2.P \oplus P = O$ . More generally  $E[n] = \{P \mid n.P = O\}$ . This set of points is closed under addition on the curve (group law). Say  $P, Q \in E[n]$ , then  $n(P + Q) = n.P \oplus n.Q = O \oplus O = O$ . Also the inverse exists:  $n.P = O = n.(-P) = -(n.P)$ . And since the identity  $O \in E[n]$ , this set is a group, infact a finite abelian group.

$$E[n] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z} = \{a.P \oplus b.Q \mid P, Q \in E[n] \text{ and } 0 \leq a, b \leq n-1\}$$

Hence  $|E[n]| = n^2$ . So in some sense the  $n$ -torsion group is well understood. When  $n$  is odd, the  $x$ -coordinate satisfies a recursively defined polynomial.

*Remarks:*

1. If  $S, T \in E[2]$  then  $S, T, S \oplus T = R$  and  $O$  forms the 2-torsion group.

- Every element of  $E(\mathbf{F}_p)$  is a torsion point. If  $|E(\mathbf{F}_p)| = l$ , prime then  $E(\mathbf{F}_p) \leq E[n]$ , ( $\leq$  denotes the *subgroup of* relation).

## II. A friendly introduction to functions and divisors

Suppose  $E/K$  defined by  $y^2 = x^3 + ax + b$  and a function  $f$  is defined on points on  $E$ , that is  $P = (x, y)$ , where  $x, y$  are elements in  $\overline{K}$ . A point  $P$  is a *zero* for a function  $f$  if  $f(P) = 0$ . We'll not delve into precise definitions for poles and zeros and their orders but we'll look at illustrative examples.

*Some example functions:*

- $f(P) = x(P)$ , where  $x(P)$  is the  $x$ -coordinate of point  $P$ . What about  $x(P)$  when  $P$  is the point at infinity? The function  $x$  is said to have a *pole* at  $O$ .
- $f(P) = y(P)$ , where this function extracts the  $y$ -coordinate of point  $P$ . So the zeros of function  $y$  are the two non-zero 2-torsion points. By non-zero we mean the non point-at-infinity torsion points.
- $f(P) = \frac{1}{x}(P)$ , where the function evaluated at point  $P$  equals the inverse of the  $x$ -coordinate of point. If  $x(P) = 0$  then  $P$  is a pole for function  $\frac{1}{x}$ . Hence points which are zeros (poles) for  $x$  become poles (zeros) for  $\frac{1}{x}$ .

Next consider a linear function  $L$  defined on  $E$ :

$$\begin{aligned} L &: \alpha x + \beta y + \gamma, \text{ where } \alpha, \beta, \gamma \in \overline{K} \\ L &: E(\overline{K}) \rightarrow \overline{K} \\ (x, y) &\longrightarrow \alpha x + \beta y + \gamma \end{aligned}$$

So  $L$  is a function on the curve and a zero of  $L$  is a point on the curve  $E$  and also a point on the line defined by  $L$ .

More generally we can take  $f$  to be a rational function, that is,  $f(x, y) = \frac{F(x, y)}{G(x, y)}$ , where  $F(x, y), G(x, y) \in \overline{K}[x, y]$ ,  $G$  is not the zero polynomial and  $F$  and  $G$  share no factors in common.

*Some properties:*

- $div(f) = div(F) - div(G)$ . Hence  $div(\frac{1}{x}) = -div(x)$ .  $div(f)$  is defined below.
- The set of functions on the curve form a field.

Say for point  $P$ ,  $F(P) = G(P) = 0$ . If  $P$  is a zero of order 2 for  $F$  and a zero of order 1 for  $G$ , then  $P$  is a zero of order 1 for  $f$ . On the other hand if  $P$  is a zero of order 2 for  $F$  and a zero of order 3 for  $G$ , then  $P$  is a pole of order 1 for  $f$ .

*Examples of orders of poles/zeros of points wrt linear functions:*

1.  $L'$  which intersects at three distinct points  $P, Q$  and  $R$  has a zero of order 1 at  $P, Q, R$  and a pole of order 3 at  $O$ .
2.  $L''$  is tangent to the curve at  $P$  and intersects the curve at  $R \neq P$  has a zero of order 2 at  $P$ , a zero of order 1 at  $R$  and a pole of order 3 at  $O$ .
3.  $L'''$  is a vertical tangent to the curve at point  $P$  and doesn't touch/intersect the curve anywhere else in the affine part of the curve has a zero of order 2 at  $P$  and a pole of order 3 at  $O$ .

A *divisor* is a finite formal sum of points  $P_i$ 's on the curve,  $\sum a_i P_i$ . The divisor for a function  $f$  on  $E$  is denoted by  $div(f)$  or simply  $(f)$  and is defined as follows  $div(f) = \sum_{i=0}^{n-1} a_i P_i - \sum_{i=0}^{m-1} b_i Q_i$ , where  $a_i, b_i \in \mathbf{Z}_{>0}$ ,  $P_i$  is a zero of  $f$  of degree  $a_i$ ,  $Q_i$  is a pole of  $f$  of order  $b_i$ , and  $f$  has  $n$  zeros and  $m$  poles.

*Fact:*  $\sum_{i=0}^{n-1} a_i - \sum_{i=0}^{m-1} b_i = 0$

Hence the divisors of the functions we talked about earlier are as follows:  $div(L') = P + Q + R - 3O$ ,  $div(L'') = 2P + R - 3O$ ,  $div(L''') = 2P - 2O$ . If  $f$  doesn't intersect (affine part of) the curve at all then  $div(f)$  is the empty/zero divisor.

*Remarks:*

1. Please note that a divisor is a formal sum of points and should not be mistaken for addition  $\oplus$  on the curve.
2. We get a degenerate case if we take our function  $f$  to be  $y^2 - x^3 - ax - b$ , the defining polynomial of the curve as  $f$  takes every point on the curve to the zero element of  $\overline{K}$ .

For point  $P \in E(\overline{K})$  we would like to construct a function  $f_P$  on  $E$  such that  $div(f_P) = n \cdot P - N \cdot O$  for any  $n \in \mathbf{N}_{>0}$ , that is the function has a zero of order  $n$  at  $P$  and a pole of order  $n$  at  $O$ .

*Claim:* We can construct  $f_P$  in  $O(\log n)$  rounds by a doubling trick. We'll give a constructive proof and talk about constructing and evaluating  $f_P$  efficiently in lecture #9. So we'll assume that the claim is true for the remaining part of the lecture.

### III. The Weil Pairing:

Weil pairing has been used to *break* cryptosystems (trace 0 case of ECDLP [1]) and also lately to *make* cryptosystems (Dan Boneh's IBE cryptosystem [2]). This pairing is a bilinear, non-degenerate map which can be defined over number fields and finite fields as follows:

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

where  $\mu_n = \{\alpha \mid \alpha^n = 1, \alpha \in \overline{K}\}$ . In other words suppose  $P$  and  $Q$  are  $n$ -torsion points then  $e_n(P, Q)$  is an  $n$ th root of unity in  $\overline{K}$ , that is  $e_n(P, Q)^n = 1$

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

*Interesting properties of the Weil Pairing:*

1. Bilinear: For  $P_1, P_2, Q_1, Q_2 \in E[n]$

$$\begin{aligned} e_n(P_1 \oplus P_2, Q_1) &= e_n(P_1, Q_1) \cdot e_n(P_2, Q_1) \\ e_n(P_1, Q_1 \oplus Q_2) &= e_n(P_1, Q_1) \cdot e_n(P_1, Q_2) \end{aligned}$$

Note:  $E[n]$  is a group wrt  $\oplus$ , hence  $P_1, P_2 \in E[n] \Rightarrow P_1 \oplus P_2 \in E[n]$

2. Non-degenerate:

$$e_n(P, Q) = 1 \text{ for all } P \in E[n] \Rightarrow Q = 0$$

$$\text{since } e_n(P, 0) = e_n(P, 0 + 0) = e_n(P, 0) \cdot e_n(P, 0) \Rightarrow e_n(P, 0) = 1$$

#### IV. MOV attack:

Consider  $E/\mathbf{F}_p$  and say  $|E(\mathbf{F}_p)| = l$ , prime and therefore  $E(\mathbf{F}_p) \leq E[l]$  as a subgroup. Recall that  $E[l] = \mathbf{Z}/l\mathbf{Z} \oplus \mathbf{Z}/l\mathbf{Z}$  and  $|E[l]| = l^2$ . Therefore  $E[l] = E(\mathbf{F}_p) \oplus \mathbf{Z}/l\mathbf{Z} \cdot Q$  for some  $Q \in E[l]$

Say  $E(\mathbf{F}_p) = \mathbf{Z}/l\mathbf{Z} \cdot S$  for some  $S \in E(\mathbf{F}_p)$  and the Elliptic Curve Discrete Logarithm Problem is given  $T \in E(\mathbf{F}_p)$  to compute  $m$  such that  $T = m \cdot S$

Here's a candidate attack:

1. Compute  $e_l(S, Q)$
2. Next compute  $e_l(T, Q) = e_l(m \cdot S, Q) = e_l(S, Q)^m$  by bilinearity property.

And now we can compute  $m$  if we can compute discrete logarithms in  $\mu_l \leq \overline{\mathbf{F}}_p$ . As we evaluate the Weil Pairing we go up extensions. So how high (extension) up do we need to go...all the way upto  $\overline{\mathbf{F}}_p$ ? Actually an extension of  $\mathbf{F}_p$  that contains  $\mu_l$  will do. So we find  $k$  such that  $\mathbf{F}_{p^k}$  contains  $\mu_l$ , that is, we need  $l$  to divide  $|F_{p^k}^*| = p^k - 1$ .

Hence problem ECDLP reduces to DLP over some extension of our base field. And we have a sub exponential time algorithm for DLP over finite fields. But the obstacle is that typically  $k$  is very big and this attack doesn't give us a sub exponential time algorithm for ECDLP in general (as the running time of the algorithm is relative to the size of the field and in this case we are doing computation in a huge extension of  $\mathbf{F}_p$ ). But suppose  $l|p-1$  then  $k=1$ . When does this happen?  $|E(\mathbf{F}_p)| = p+1-t = l \Rightarrow t=2$ . Hence the  $l$ -th roots of unity in  $\overline{\mathbf{F}}_p$  are the elements of  $\mathbf{F}_p^*$  as  $l = p-1$  (by Flt). Hence in this case ECDLP reduces to DLP over the base field itself and hence can be solved in sub exponential time.

#### Bibliography:

1. A. Menezes, T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions on Information Theory*, 39 (1993), 1639-1646
2. D. Boneh and M. Franklin, Identity based encryption from the Weil pairing, *Crypto '2001*, *Lecture Notes in Computer Science*, Vol. 2139, Springer-Verlag, pp. 213-229, 2001