

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang  
Scribe: Iftikhar A Burhanuddin  
burhanud@usc.edu  
Classes #11 - March 26, 2002

**Administrivia:** Scribe notes for class #10 are online at the course webpage: <http://www-rcf.usc.edu/~mdhuang/cs599>

**Today's class:**

1. Introduction to Hyperelliptic curves
2. Group Law on Hyperelliptic curves
3. Discrete logarithm problem on Hyperelliptic Curves

### **I. Introduction to Hyperelliptic curves:**

“An elementary Introduction to Hyperelliptic curves” is an appendix in our textbook [1]. We’ll take a conceptual approach to understand this topic.

A Hyperelliptic curve of genus  $g$  defined over a field  $F$  is given by

$$v^2 + h(u)v = f(u),$$

where  $h(u), f(u) \in \mathbf{F}[u]$ ,  $\deg h \leq g$ ,  $\deg f \leq 2g + 1$ , and  $f$  monic

More generally  $\deg f$  can be even but it’s a more complicated case to deal with and we’ll restrict our discussion to the *odd* degree case.

If  $\text{char } \mathbf{F} \neq 2$ , then a hyperelliptic curve of genus  $g$ , is given by

$$C : y^2 = f(x),$$

where  $\deg f = 2g + 1$ ,  $f$  monic

and for what follows we’ll assume that  $\text{char } \mathbf{F} > 2$ . In particular when  $g = 1$ ,  $\deg f = 3$ , we get an elliptic curve defined by equation  $y^2 = x^3 + ax + b$ .

A necessary and sufficient condition for our curve  $C$  defined by the polynomial  $f$  to be smooth is  $\gcd(f, f') = 1$ , that is the partial derivatives wrt  $x$  and  $y$  are not be simultaneously zero. Recall that a plane curve  $D(x, y) = 0$  is smooth/non-singular at point  $(a, b)$  iff  $\frac{\partial D}{\partial x}(a, b) \neq 0$  or  $\frac{\partial D}{\partial y}(a, b) \neq 0$ .

What is *genus*? Recall that  $\mathbf{F} < \mathbf{C}$  as a subfield. So if we plot  $F$  as a complex curve, we get a surface. The genus of a surface is number of holes on the surface and is an invariant associated with the curve. Genus can also be defined using the 0-Homology group. Example of a genus zero curve is the projective line or circle. Intuitively higher the genus more complicated the curve.

### **II. Group Law on Hyperelliptic curves:**

When we draw line we expect it to intersect an elliptic curve at 3 points and this gave us the addition law on EC. In genus  $g$  curves, we expect  $2g + 1$  points

on the curve and the line. On Hyperelliptic curves we forget about addition directly on points as it doesn't give us anything meaningful and we'll try adding *divisors* (modulo divisors of functions).

We'll do a quick recap of divisors and functions we discussed in lectures #8 and #9. Consider an elliptic curve given by  $y^2 = x^3 + ax + b$ . The functions  $x(P)$  and  $y(P)$  are defined on all points on the curve except at the point of infinity. These functions satisfy curve's equation:  $x(P)^3 + ax(P) + b = y(P)^2$ . Other examples of functions are  $2x + 1$ ,  $x^2 + 1$ ;  $\frac{x}{y}$ . The set of all rational functions in  $x$  and  $y$  on the curve forms a field with addition and multiplication defined *naturally*,  $(x + y)(P) = x(P) + y(P)$ ,  $(xy)(P) = x(P)y(P)$ .

Take a point  $p = (\alpha, \beta)$  and consider the function  $x - \alpha$ . This function is going to vanish at  $P$  and  $\overline{P} = (\alpha, -\beta)$ ,  $\beta \neq 0$ .  $(x - \alpha)(P) = (x - \alpha)(\overline{P}) = 0 \rightarrow x(P) - \alpha = 0$ . We can think of  $\alpha$  as a constant function which maps every point to  $\alpha$ . So  $div(x - \alpha) = (\alpha, \beta) + (\alpha, -\beta) - 2O$

Say  $C$  is a plane curve and let

$$Div^0(C) := \{ \sum_{i=1}^k a_i P_i \mid P_i \in C(\overline{K}), a_i \in \mathbf{Z}, \sum_{i=1}^k a_i = 0 \} \text{ and}$$

$$Div^l(C) := \{ div(h) \mid h \text{ is a function on } C \}$$

The superscript  $l$  stands for linear equivalence.  $Div^l(C) \leq Div^0(C)$  as a proper subgroup except when  $g = 0$ , in which case they are equal. If  $C$  is an elliptic curve then  $Div^0(E)/Div^l(E) = E(\overline{K})$ .

Say  $D_1, D_2 \in Div^0(E)$ . We'll write  $D_1 \sim D_2 \Leftrightarrow [D_1] = [D_2] \Leftrightarrow D_1 - D_2 \in Div^l(E)$  where  $[D]$  denotes the divisor  $D$ 's congruence class.

$$\begin{array}{ccc} E(\overline{K}) & \cong & Div^0(E)/Div^l(E) \\ P & \rightarrow & [P - O] \end{array}$$

So  $[D] = [P - O] \Leftrightarrow$  there exists a function  $h$  such that  $D - (P - O) = div(h)$

For example, take function  $y$  as our  $h$  and we know that  $div(y) = Q_1 + Q_2 + Q_3 - 3O$ , where the  $Q_i$ 's are the non-zero 2-torsion points. So for a point  $P$ ,  $[Q_1 + Q_2 + Q_3] = [P - O]$ .

For a hyperelliptic curve  $C$  we can define the Jacobian of  $C$ ,

$$J_C := Div^0(C)/Div^l(C)$$

Example: Say  $C$  is a genus 2 curve defined by  $y^2 = (x - 1)(x - 2)(x - 3)(x - 4)(x - 5)$ . Taking  $x - 1$  as our function,  $div(x - 1) = 2(1, 0) - 2O$ . More generally if  $f(\alpha) \neq 0$ , then  $div(x - \alpha) = (\alpha, \beta) + (\alpha, -\beta) - 2O$ , where  $\beta^2 = f(\alpha)$ ,  $\beta \neq 0$ . Conversely if  $P = (\alpha, \beta)$  and  $\overline{P} = (\alpha, -\beta)$ ,  $\beta \neq 0$ , then  $P + \overline{P} - 2O$  maps to the divisor of a function. And  $P - O \sim -(\overline{P} - O) \Leftrightarrow P + \overline{P} \sim 2O$ . In other words we can replace  $P + \overline{P}$  by  $2O$ .

So for each congruence class we can find a *nice* unique representative of the form  $P_1 + P_2 + \dots + P_m - mO$ , where  $m \leq g$ , where  $g$  is the genus of the curve and where the divisor is in semi-reduced form, that is,  $P_i$ 's may not be distinct but  $P_i \neq \overline{P}_j$ .

In the case of elliptic curves  $m = g = 1$

$$\begin{array}{ccc} E(\overline{K}) & \cong & Div^0(E)/Div^l(E) \\ P & \rightarrow & [P - O] \end{array}$$

The image of  $E(\overline{K})$  under this map is a group. But the image of  $C(\overline{K})$  is not a group.

$$\begin{array}{ccc} C(\overline{K}) & \cong & Div^0(E)/Div^l(E) \\ P & \rightarrow & [P - O] \end{array}$$

$[P_1 - O] + [P_2 - O] = [P_1 + P_2 - 2O] \neq [P' - O]$  and  $[P_1 + P_2 - 2O]$  represents another class.

Say  $C : y^2 = f(x)$  defined over a finite field  $\mathbf{F}_q$ .  $deg f = 2g + 1$ . Given two divisors  $D_1, D_2 \in Div^0(C)$ , which represent two equivalence classes. To compute  $m$  such that  $mD_1 \sim D_2 \Leftrightarrow m[D_1] = [D_2]$ , that is  $mD_1 - D_2 \in Div^l(C)$ , where  $m[D] := [mD]$

$D_1, D_2$  should be  $\mathbf{F}_q$ -rational, that is  $D_1, D_2$  should involve  $\mathbf{F}_q$  rational points. Say  $[D_1] = [P_1 + \dots + P_m - mO]$ ,  $m \leq g$ , where  $P_i = (\alpha_i, \beta_i) \in C(\mathbf{F}_q)$ ,  $1 \leq i \leq m$ . We can associate  $[D_1]$  with a pair of single variable polynomials  $(u, v)$  as follows:  $u(X) = \prod_{i=1}^m (X - \alpha_i)$  and  $v(X)$  is a polynomial such that  $v(\alpha_i) = \beta_i$ . The  $D$ 's are  $\mathbf{F}_q$ -rational if  $u(X), v(X) \in \mathbf{F}_q[X]$ . Note that there is no restriction on the  $P_i$ s.

*Remark:* The Galois action on points is stable, that is  $P_1^\sigma + \dots + P_m^\sigma = P_1 + \dots + P_m$ .  $P_1^\sigma$  may not equal  $P_1$  but the sums are equal.

$$J_C(\mathbf{F}_q) = \{ [D] \mid D \in Div^0(C)/Div^l(C), [D] \text{ is } \mathbf{F}_q \text{ rational} \}$$

It turns out that  $J_C(\mathbf{F}_q)$  is a finite abelian group. The identity is the 0 class which represents  $Div^l(C)$ . Say  $[D] = div(h)$ , the inverse of  $[D]$  is given by  $[-D] = div(h^{-1})$  such that  $[D] + [-D] = 0$ . Suppose  $[D_1] = [P_1 + \dots + P_m - mO]$ ,  $[D_2] = [Q_1 + \dots + Q_k - kO]$ , where  $m, k \leq g$  then  $[D_1 + D_2] = [P_1 + \dots + P_m + Q_1 + \dots + Q_k - mO - kO]$  and  $m + k$  may be greater than  $g$ . And we want to find the unique representative for  $[D_1 + D_2]$  which has  $t \leq g$  zeros and a unique pole of order  $t$  at  $O$ . For details regarding addition on the Jacobian of a Hyperelliptic curve refer to the appendix of [1]. The running time of the addition algorithm is polynomial in  $g$  and  $\log q$  and part of the algorithm is to reduce to the unique representative form.

The group order  $|J_C(\mathbf{F}_q)|$  falls in the following range

$$(\sqrt{q} - 1)^{2g} \leq J_C(\mathbf{F}_q) \leq (\sqrt{q} + 1)^{2g}$$

So the order is about  $q^g$  and the group order grows exponentially with the genus. Therefore even if  $q$  is small but the genus of the curve  $g$  is big we'll end up with a *big* group.

### III. Discrete logarithm problem on Hyperelliptic Curves:

So we saw that as the genus increases,  $|J_C(\mathbf{F}_q)|$  increases but does the discrete log problem become more difficult? No! There is sub exponential algorithm (in  $\log q^g$ ) to solve HCDLP when  $g \gg \log q$ . The algorithm hinges on the *smoothness* of divisors (which depends on the smoothness of the associated polynomials) in particular even if  $D_1$  and  $D_2$  are not smooth, linear combinations  $[sD_1 + tD_2]$  may be  $\sqrt{\log q}$ -smooth. Note this method breaks down when  $g$  is fixed and hence doesn't tell us anything about ECDLP. For more details refer [2].

**Bibliography:**

1. Neal Koblitz, Algebraic Aspects of Cryptography (Algorithms and Computation in Mathematics, Vol 3), Springer-Verlag, January 1998
2. Leonard M. Adleman, Jonathan DeMarrais, Ming-Deh A. Huang, A Subexponential Algorithm for Discrete Logarithms over Hyperelliptic Curves of Large Genus over  $\text{GF}(q)$ , TCS 226(1-2): 7-18 (1999)