Hyperelliptic Curve Cryptography

A SHORT INTRODUCTION

Definition (HEC over K):

- Curve with equation $y^2 + h(x)y = f(x)$ with $h, f \in K[X]$
- Genus $g \Rightarrow \deg h(x) \leq g, \quad \deg f(x) = 2g + 1$
- f monic
- Nonsingular

Nonsingularity

- Definition (Algebraically closed field K):

$$P \in K[X],\ P\ non-constant \Rightarrow P\ has\ a\ root.$$

- Definition (Algebraic closure of K):

Smallest algebraically closed field containing K

Nonsingularity (definition)

A hyperelliptic curve $y^2 + h(x)y = f(x)$ with coefficients in field K

is said to be **nonsingular** if no point on the curve over the algebraic

closure $\overline{K}$ of K satisfies both partial derivatives of the curve equation, ie

$2y + h(x) = 0$ and $h'(x)y = f'(x)$.

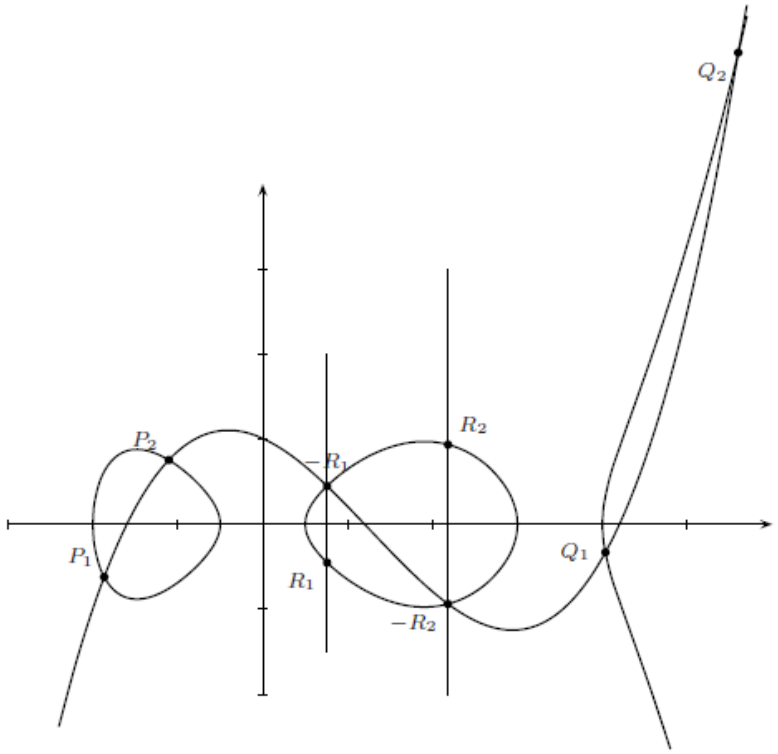
In particular, note that $f'(x) = 0 \Leftrightarrow x$ multiple root of f, and hence for

odd characteristics $y^2 = f(x)$ non singular $\Leftrightarrow f$ has no multiple roots.

Group law

Figure 14.1 Group law on genus 2 curve over the reals $\mathbb{R}$, $y^2 = f(x), \deg f = 5$ for $(P_1 + P_2) \oplus (Q_1 + Q_2) = R_1 + R_2$.

[1]



- More intersections in general than the EC case ⇒more than 3 points if we intersect with a line
- We do not even have a group structure in general, so we need something else

Divisors (definition)

- D is called a **divisor** of a HEC C if $D = \sum_{P \in C(\overline{K})} n_P P$ with $n_P \in \mathbb{Z}$ and only finitely many $n_p \neq 0$

- The **degree** of D is $\deg(D) = \sum_{P \in \mathrm{C}(\overline{K})} n_P$

E.g. given $D = P_1 + 2P_2$, $\deg(D) = 3$

- $Div_C^0(\overline{K})$ is the group of degree 0 divisors on C

Divisors

- Let r be a rational function in $\bar{K}(C)$ (field of fractions in $\bar{K}[x,y]/(y^2+h(x)y-f(x))$. The **order** of r at P is given by

$$\mathrm{ord}_P(r) = \begin{cases} n \text{ if } P \text{ zero of order } n \\ -n \text{ if } P \text{ pole of order } n \\ 0 \text{ if neither} \end{cases}$$

- The **divisor** of r is given by

$$\mathrm{div}(r) = \sum_{P \in C(\bar{K})} \mathrm{ord}_P(r) \cdot P$$

e.g. $r(x) = \frac{(x-2)^2}{(x+1)x^3}$: $P_1 = 2$ is a zero of order 2, $P_2 = -1$ a pole of order 1 and $P_3 = 0$ a pole of order 3, so $\mathrm{div}(r) = 2\,P_1 - P_2 - 3P_3$

Divisors

$\sum m_P \} = 0$ $\quad D_2 = \sum n_P P$ $\} \deg 0$
$\sum n_P \quad D_1 = \sum m_P P$
$\hookrightarrow D_1 + D_2$ has deg 0 too

- A divisor D is said to be **principal** if $\exists r$ s.t. $D = \mathrm{div}(r)$. The set of principal divisors on C is $\mathrm{Princ}(C)$.
- It can be shown that $\forall r \in \bar{K}(C), \deg(\mathrm{div}(r)) = 0$ and hence $\mathrm{Princ}(C)$ is a subgroup of $\mathrm{Div}_C^0(\bar{K})$.
- In practice, $\deg(\mathrm{div}(r)) = 0$ means we will need to throw in O, the point at infinity. For example consider the curve $C: y^2 = f(x)$ of genus 1 over $\mathbb{C}$. Then $\deg(f) = 3$. Given $g(x, y) = \frac{y}{x-2}$, the zero of g is 0, and as $\deg(f) = 3$ then there are 3 points on the curve with $y = 0$; call them P_1, P_2, P_3. Additionally g has points with $x = 2$ as poles. Assuming $f(2) \neq 0$, then there are two such points on C, Q_1 & Q_2. Then $\mathrm{div}(g) = P_1 + P_2 + P_3 - Q_1 - Q_2 - O$.

Divisors

- We define the Picard (or divisor class) group of C as
$$\mathrm{Pic}_C^0(\overline{K}) = \mathrm{Div}_C^0(\overline{K}) \,/\, \mathrm{Princ}(C)$$

- $\exists J(C)$ abelian variety of dimension g s.t. $J(C) \cong \mathrm{Pic}_C^0(\overline{K})$. $J(C)$ is called the **Jacobian** of C.

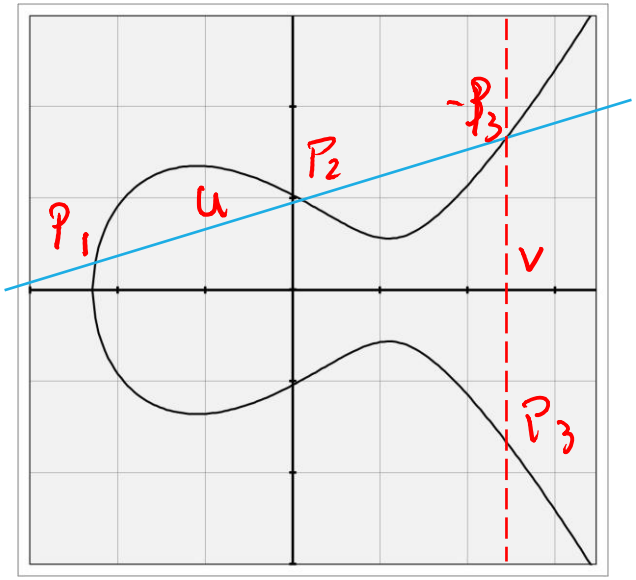
- What is important here is that the group we will be using is $J(C)$. The group law will operate on divisor classes. A divisor class would then be written uniquely as $\sum_{i=1}^{r} P_i - rO$, $P_i \in C \setminus \{O\}, r \leq g$, with $P_i \neq -P_j = \left(x_j, -h\left(x_j\right) - y_j\right)$ for $i \neq j$.

- Theorem (Hasse-Weil): if C is a HEC of genus g over F_q,
$$(\sqrt{q} - 1)^{2g} \leq \#J(C) \leq (\sqrt{q} + 1)^{2g}$$

Divisors (concretely)

- Step 1: if $n > 1$ points, write a polynomial of degree $n - 1$; the number of other points of intersections with the curve is $\max(\deg(f), 2(n-1)) - n$.
- Step 2: Inflect (ie take the opposite of these points) to reduce the sum.
- Step 3: repeat until you reach a number of points $\leq g$. This will allow one to form a divisor class / reduced divisor.

Genus 1 example



$$D_1 = P_1 - O$$

$$D_2 = P_2 - O$$

$$\mathrm{div}(u) = P_1 + P_2 + (-P_3) - 3O$$

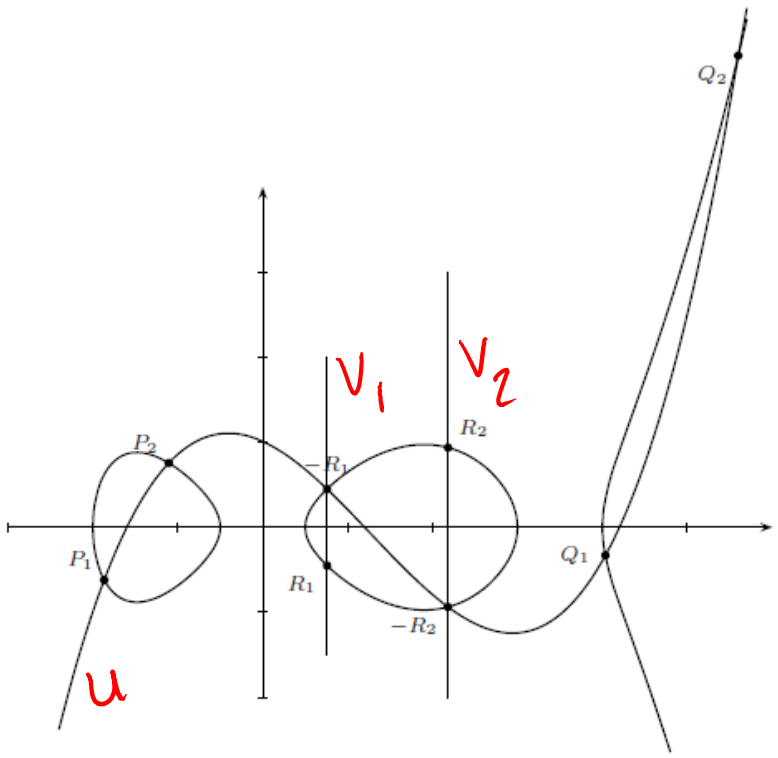
$$\mathrm{div}(v) = P_3 + (-P_3) - 2O$$

$$\mathrm{div}(u) - \mathrm{div}(v) = P_1 + P_2 - P_3 - O$$

$$0 = P_1 + P_2 - P_3 - O$$

Genus 2 example

Figure 14.1 Group law on genus 2 curve over the reals $\mathbb{R}$, $y^2 = f(x), \deg f = 5$ for $(P_1 + P_2) \oplus (Q_1 + Q_2) = R_1 + R_2$.



$D_1 = P_1 + P_2 - 2\mathcal{O}$

$D_2 = Q_1 + Q_2 - 2\mathcal{O}$

$div(u) = P_1 + P_2 + Q_1 + Q_2 + (-R_1) + (-R_2) - 6\mathcal{O}$

$div(v_1) = R_1 + (-R_1) - 2\mathcal{O}$

$div(v_2) = R_2 + (-R_2) - 2\mathcal{O}$

$div(u) - div(v_1) - div(v_2) = P_1 + P_2 + Q_1 + Q_2 - R_1 - R_2 - 2\mathcal{O}$

$D_1 + D_2 = D$

$D = R_1 + R_2 - 2\mathcal{O}$

Mumford representation

- Theorem: Given a HEC C of genus g over K, $\exists!\ (u, v)$ with $u, v \in K[x]$ s.t.
  - u is monic
  - $u \mid v^2 + vh - f$
  - $\deg(v) < \deg(u) \leq g$

- In particular, if $g = 2$, we can represent any divisor class by the coefficients u_1, u_0, v_1, v_0 of u and v.

- As u is monic, we can write u in $\bar{K}[x]$ as $u(x) = \Pi_{i=1}^{\deg(u)}(x - x_i)$. The middle condition in the theorem tells us that $\left(x_i, v(x_i)\right) \in C$. In general if (x_i, y_i) has multiplicity n, then for $0 \leq j \leq n - 1$,

$$\left(\frac{d}{dx}\right)^j [v(x)^2 + v(x)h(x) - f(x)]_{|x=x_i} = 0$$

Mumford representation

For example, consider $C: y^2 = x^5 + 3x^3 + 2x^2 + 3$ over F_5.

- Consider $P_1 = (1,2), P_2 = (3,0), P_3 = (1,3), P_4 = (4,1)$
- We want to reduce the divisors $D_1 = P_1 + P_2 - 2O$ and

$D_2 = P_3 + P_4 - 2O$ ie find a, b, c, d s.t. $D_1 = [a, b], D_2 = [c, d]$

- C has genus 2 so $\deg(\mathrm{b}) < \deg(a) \leq 2$. We know that at the x coordinates of P_1, P_2 ,a vanishes so $a = (x-1)(x-3) = x^2 + x + 3$ and $b(x_i) = y_i$, $b_1 + b_0 = 2$ and $3b_1 + b_0 = 0$ so $b = 4x + 3$.
- Similarly we have $c = (x-1)(x-4) = x^2 + 4$ and $d_1 + d_0 = 3$ and $4d_1 + d_0 = 1$ so $d = x + 2$.
- $D_1 = [x^2 + x + 3, 4x + 3], D_2 = [x^2 + 4, x + 2]$

Cantor's algorithm[1]

INPUT: Two divisor classes $\bar{D}_1 = [u_1, v_1]$ and $\bar{D}_2 = [u_2, v_2]$ on the curve $C : y^2 + h(x)y = f(x)$.
OUTPUT: The unique reduced divisor D such that $\bar{D} = \bar{D}_1 \oplus \bar{D}_2$.

1. $d_1 \leftarrow \gcd(u_1, u_2)$ $\qquad [d_1 = e_1 u_1 + e_2 u_2]$
2. $d \leftarrow \gcd(d_1, v_1 + v_2 + h)$ $\qquad [d = c_1 d_1 + c_2(v_1 + v_2 + h)]$
3. $s_1 \leftarrow c_1 e_1$, $s_2 \leftarrow c_1 e_2$ and $s_3 \leftarrow c_2$
4. $u \leftarrow \dfrac{u_1 u_2}{d^2}$ and $v \leftarrow \dfrac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$
5. **repeat**
6. $\quad u' \leftarrow \dfrac{f - vh - v^2}{u}$ and $v' \leftarrow (-h - v) \bmod u'$
7. $\quad u \leftarrow u'$ and $v \leftarrow v'$
8. **until** $\deg u \leqslant g$
9. make u monic
10. **return** $[u, v]$

Cantor algorithm

- ∃ better algorithms for fixed g and h. Notably, for binary fields, we can reduce the operations to $I + 5S + 22M$ (Lange,2004).[2]
- Additionally if $\deg(h) = 1$ we can get down to $I + 5S + 9M$.[2][3]
- As with the EC case we can change coordinate systems to get even better results and avoid inversions altogether (e.g. if $h(x) = x$, doubling in affine coordinates is $I + 5M + 6S$ but in projective coord, $22M + 6S$)[3]

In practice

- HECC can be used to implement the same algorithms as HEC
- $g \geq 3$ turns out to be vulnerable to index-calculus [4][5]
- To achieve a security level of 2^{128}, the base fields in ECC will have about 2^{256} elements as compared to 2^{128} for HECC with $g = 2$, leading to a speed-up factor of 3 [6]
- In a certain class of HECs (Kummer surfaces), HECC with $g = 2$ will have only twice as many operations as EC[7]
- Interestingly enough, Gaudry, Hess and Smart showed in 2000 that the ECDLP over F_{2^k} can be reduced to the DLP of a Jacobian over a subfield of F_{2^k} leading to subexponential times unless k large enough[8]

Future of HECC

- Focused on $g = 2$
- Recently, Bernstein and al. showed how HECC could take advantage of modern CPU architecture (using vectorization) to break DH speed records. [9]
- HECC being faster than ECC for certain operations and slower for others (e.g. ephemeral DH where $g = 1$ is faster for fixed-based multiplications such as the ones involved in the key generation and slower for variable-based multiplications, such as the ones needed for the shared-secret computation), Bernstein and Lange proposed a new approach to (H)ECC, “hyper-and-elliptic curve cryptography” in which a single appropriate group is used to compute both kinds of operations.[10]

References

[1] Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., & Vercauteren, F. (Eds.). (2005). *Handbook of elliptic and hyperelliptic curve cryptography*. CRC press.

[2] Lange, Tanja. "Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae." *IACR Cryptology ePrint Archive* 2002 (2002): 121.

[3] Wollinger, Thomas, and Vladyslav Kovtun. "Fast explicit formulae for genus 2 hyperelliptic curves using projective coordinates." *null*. IEEE, 2007.

[4] Gaudry, P., Thomé, E., Thériault, N., & Diem, C. (2007). A double large prime variation for small genus hyperelliptic index calculus. *Mathematics of Computation*, *76*(257), 475-492.

[5] Adleman, L. M., DeMarrais, J., & Huang, M. D. (1994). A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In *Algorithmic number theory*(pp. 28-40). Springer Berlin Heidelberg.

[6] Joppe W. Bos, Craig Costello, H□useyin Hisil, Kristin Lauter, Fast cryptography in genus 2, in Eurocrypt (2013), 194{210.

[7] Gaudry, P. Variants of the Montgomery form based on Theta functions (2006)

[8] Gaudry, P. (2000, January). An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology—EUROCRYPT 2000* (pp. 19-34). Springer Berlin Heidelberg.

[9] Bernstein, D. J., Chuengsatiansup, C., Lange, T., & Schwabe, P. (2014). Kummer strikes back: new DH speed records. In *Advances in Cryptology–ASIACRYPT 2014* (pp. 317-337). Springer Berlin Heidelberg.

[10] Bernstein, D. J., & Lange, T. (2014). Hyper-and-elliptic-curve cryptography.*LMS Journal of Computation and Mathematics*, *17*(A), 181-202.