

# Divisor Class Halving on Hyperelliptic Curves

Peter Birkner

Department of Mathematics and Computer Science  
Eindhoven University of Technology

EIDMA Seminar Combinatorial Theory  
7 March, 2007

# Motivation

- To construct a cryptosystem we need a **one-way function** to encrypt our information.
- A one-way function is **easy to compute** but **hard to invert**.

Let  $(G, \oplus)$  be a cyclic group with a generator  $g \in G$  and let  $f : \mathbb{Z} \rightarrow G$  be the function  $n \mapsto [n]g = \underbrace{g \oplus \dots \oplus g}_{n\text{-times}}$ .

Now, we are looking for groups  $(G, \oplus)$  where  $f$  is a one-way function, i. e.

- we can efficiently compute  $[n]g$ ,
- for a given  $h \in G$  it is hard to find a  $k \in \mathbb{Z}$  such that  $h = [k]g$ .

Inverting the function  $f$  is called the **Discrete Logarithm Problem (DLP)** in  $G$ .

# Aim of the Talk

- 1 Present a class of groups where the function  $f$  is hard to invert, i. e. the DLP is hard to solve.

These groups are divisor class groups of hyperelliptic curves over binary fields (Part I).

- 2 Provide efficient arithmetic in these groups to make the function  $f$  easy to compute, i. e. make the scalar multiplication  $[n]g$  fast.

Therefore, we will look at doubling and halving of divisor classes in particular (Part II, III).

# Part I: The Divisor Class Group of a Hyperelliptic Curve

## Definition

Let  $K$  be a field and  $\bar{K}$  an algebraic closure of  $K$ . A *hyperelliptic curve  $C$  of genus  $g$  over  $K$*  with at least one  $K$ -rational Weierstraß point can be given by an equation of the form

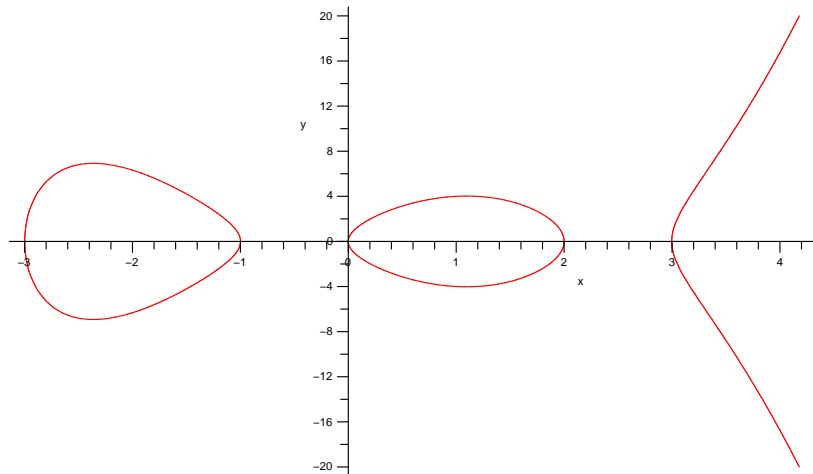
$$C : y^2 + h(x)y = f(x),$$

where

- $h \in K[x]$  is a polynomial of degree at most  $g$ ,
- $f \in K[x]$  is a monic polynomial of degree  $2g + 1$ ,
- no point on  $C$  over  $\bar{K}$  satisfies both partial derivatives  $2y + h = 0$  and  $h'y - f' = 0$ .

# Example: A Hyperelliptic Curve over the Reals

$$C : y^2 = x^5 - x^4 - 11x^3 + 9x^2 + 18x \text{ over } \mathbb{R}$$
$$= x(x-2)(x-3)(x+1)(x+3)$$



## Definition

Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$ .

- ① A **divisor  $D$  on  $C$**  is a formal sum of points on  $C$ :

$$D := \sum_{P \in C(\bar{K})} n_P P \quad (n_P \in \mathbb{Z}, n_P = 0 \text{ for almost all } P \in C(\bar{K}))$$

- ② The **degree** of a divisor  $D$  on  $C$  is

$$\deg(D) := \sum_{P \in C(\bar{K})} n_P.$$

The group of **degree zero divisors on  $C$**  is denoted by  $\text{Div}_C^0(\bar{K})$ .

**Example:**  $D = 2P_1 + 3P_2$ ,  $\deg(D) = 2 + 3 = 5$

# The Function Field of a Hyperelliptic Curve

## Definition

Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$ .

- The **coordinate ring of  $C$  over  $K$**  is the quotient ring

$$K[C] := K[x,y]/(y^2+h(x)y-f(x)).$$

Similarly, the coordinate ring of  $C$  over  $\bar{K}$  is

$$\bar{K}[C] := \bar{K}[x,y]/(y^2+h(x)y-f(x)).$$

An element of  $\bar{K}[C]$  is called a **polynomial function on  $C$** .

- The **function field  $\bar{K}(C)$  of  $C$  over  $\bar{K}$**  is the field of fractions of  $\bar{K}[C]$ . The elements of  $\bar{K}(C)$  are called **rational functions on  $C$** .

## Definition

Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$  and let  $P \in C(\overline{K})$ . A rational function  $u \in \overline{K}(C)$  with  $u(P) = 0$  is called a **uniformising parameter for  $P$** , if the following property holds:

For each  $0 \neq a \in \overline{K}[C]$  there exists an integer  $d$  and a function  $s \in \overline{K}(C)$  such that  $a = u^d s$  and  $s(P) \notin \{\infty, 0\}$ .

## Theorem

For each  $P \in C(\overline{K})$  there exists an uniformising parameter for  $P$ .

# Order of a Rational Function

## Definition

- ① Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$ . Let  $P \in C(\overline{K})$  with uniformising parameter  $u \in \overline{K}(C)$  and let  $0 \neq a \in \overline{K}[C]$  be a **polynomial function on  $C$** . Now,  $a$  can be written as

$$a = u^d s.$$

The (unique) integer  $d$  is called the **order of  $a$  at  $P$** .

- ② Let  $r = a/b \in \overline{K}(C)^*$  be a **rational function** on  $C$  and  $P \in C(\overline{K})$ . The **order of  $r$  at  $P$**  is defined as

$$\text{ord}_P(r) := \text{ord}_P(a) - \text{ord}_P(b).$$

## Definition

Let  $r \in \overline{K}(C)^*$  be a rational function on  $C$ . The **divisor of  $r$**  is

$$\operatorname{div}(r) := \sum_{P \in C(\overline{K})} (\operatorname{ord}_P(r)) P.$$

## Definition

A divisor  $D$  is called **principal** if  $D = \operatorname{div}(r)$  for some rational function  $r \in \overline{K}(C)^*$ . The set of principal divisors on  $C$  is denoted by **Princ( $C$ )**.

A principal divisor has degree zero. So,  $\operatorname{Princ}(C)$  is a subgroup of  $\operatorname{Div}_C^0(\overline{K})$ .

# The Divisor Class Group

## Definition

The **divisor class group of  $C$**  is the quotient group

$$\text{Pic}_C^0(\bar{K}) := \text{Div}_C^0(\bar{K}) / \text{Princ}(C).$$

It is also called the **Picard group of  $C$** . The elements of  $\text{Pic}_C^0(\bar{K})$  are called divisor classes of  $C$ .

Since our curves have only one point at infinity, the divisor class group is isomorphic to the **ideal class group of  $C$** .

## Theorem (Mumford)

Let  $C$  be a hyperelliptic curve of genus  $g$  over a field  $K$ . Each nontrivial divisor class of  $C$  over  $K$  can be represented by a **unique pair of polynomials**  $u, v \in K[x]$ , where

- 1  $u$  is monic,
- 2  $\deg v < \deg u \leq g$ ,
- 3  $u \mid v^2 + vh - f$ .

In the genus 2 case each divisor class can be represented by the 4 coefficients  $u_1, u_0, v_1, v_0$  of the polynomials  $u$  and  $v$ .

## Composition & Reduction (Cantor/Koblitz)

IN:  $\overline{D}_1 = [u_1, v_1], \overline{D}_2 = [u_2, v_2], C : y^2 + h(x)y = f(x)$

OUT:  $\overline{D} = [u, v]$  reduced with  $\overline{D} = \overline{D}_1 + \overline{D}_2$

- 1 compute  $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
- 2 compute  $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2 (v_1 + v_2 + h)$
- 3 let  $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
- 4  $u = \frac{u_1 u_2}{d^2} \quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + f)}{d} \pmod{u}$
- 5 let  $u' = \frac{f - v h - v^2}{u} \quad b' = (-h - v) \pmod{u'}$
- 6 if  $\deg u' > g$  put  $u := u', v := v'$  goto step 5
- 7 make  $u$  monic

## Part II: Efficient Doubling of Divisor Classes in Characteristic 2 and Genus 2

# Classification of Binary Genus 2 Curves

Let  $C : y^2 + h(x)y = f(x)$  be a hyperelliptic curve of genus 2 over  $\mathbb{F}_{2^d}$ . We need to have  $h \neq 0$  to avoid singular curves.

The 2-rank of those curves is determined by the **degree of  $h$** :

- **Type I** if  $\deg h = 2$ . This case splits into **Type Ia** where  $h$  has no root in  $\mathbb{F}_{2^d}$  and **Type Ib** where such a root does exist. These curves have 2-rank equal to 2.
- **Type II** if  $\deg h = 1$ . These curves have 2-rank equal to 1.
- **Type III** if  $\deg h = 0$ . These curves have 2-rank equal to 0, they are supersingular.

In the remainder of this talk we focus on Type II curves.

# Doubling in the General Case

<b>Doubling, deg <math>u = 2</math></b>			
Input	$[u, v], u = x^2 + u_1 x + u_0, v = v_1 x + v_0$		
Output	$[u', v'] = 2[u, v]$		
Step	Expression	odd	even
1	compute $\tilde{v} \equiv (h + 2v) \bmod u = \tilde{v}_1 x + \tilde{v}_0$ : $\tilde{v}_1 = h_1 + 2v_1 - h_2 u_1, \tilde{v}_0 = h_0 + 2v_0 - h_2 u_0$ ;		
2	compute resultant $r = \text{res}(\tilde{v}, u)$ : $w_0 = v_1^2, w_1 = u_1^2, w_2 = \tilde{v}_1^2, w_3 = u_1 \tilde{v}_1, r = u_0 w_2 + \tilde{v}_0 (\tilde{v}_0 - w_3)$ ;	2S, 3M ( $w_2 = 4w_0$ )	2S, 3M (see below)
3	compute almost inverse $inv' = invr$ : $inv'_1 = -\tilde{v}_1, inv'_0 = \tilde{v}_0 - w_3$ ;		
4	compute $k' = (f - hv - v^2)/u \bmod u = k'_1 x + k'_0$ : $w_3 = f_3 + w_1, w_4 = 2u_0, k'_1 = 2(w_1 - f_4 u_1) + w_3 - w_4 - h_2 v_1$ ; $k'_0 = u_1(2w_4 - w_3 + f_4 u_1 + h_2 v_1) + f_2 - w_0 - 2f_4 u_0 - h_1 v_1 - h_2 v_0$ ;	1M	2M (see below)
5	compute $s' = k' inv' \bmod u$ : $w_0 = k'_0 inv'_0, w_1 = k'_1 inv'_0, s'_1 = (inv'_0 + inv'_1)(k'_0 + k'_1) - w_0 - w_1(1 + u_1), s'_0 = w_0 - u_0 w_1$ ;	5M	5M
6	compute $s'' = x + s_0/s_1$ and $s_1$ : $w_1 = 1/(rs'_1) (= 1/r^2 s_1), w_2 = rw_1 (= 1/s'_1), w_3 = s_1^2 w_1 (= s_1)$ ; $w_4 = rw_2 (= 1/s_1), w_5 = w_4^2, s_0'' = s_0' w_2$ ;	I, 2S, 5M	I, 2S, 5M
7	compute $l' = s'' u = x^3 + l'_2 x^2 + l'_1 x + l'_0$ : $l'_2 = u_1 + s_0'', l'_1 = u_1 s_0'' + u_0, l'_0 = u_0 s_0''$ ;	2M	2M
8	compute $u' = s^2 + (h + 2v)s/u + (v^2 + hv - f)/u^2$ : $u'_0 = s_0''^2 + w_4(h_2(s_0'' - u_1) + 2v_1 + h_1) + w_5(2u_1 - f_4), u'_1 = 2s_0'' + h_2 w_4 - w_5$ ;	S, 2M	S, M
9	compute $v' \equiv -h - (l + v) \bmod u' = v'_1 x + v'_0$ : $w_1 = l'_2 - u'_1, w_2 = u'_1 w_1 + u'_0 - l'_1, v'_1 = w_2 w_3 - v_1 - h_1 + h_2 u'_1$ ; $w_2 = u'_0 w_1 - l'_0, v'_0 = w_2 w_3 - v_0 - h_0 + h_2 u'_0$ ;	4M	4M
<b>total</b>		<b>each I, 5S, 22M</b>	

<b>Doubling deg <math>h = 1</math>, deg <math>u = 2</math></b>				
Input Output	$[u, v], u = x^2 + u_1x + u_0, v = v_1x + v_0; h_1^2, h_1^{-1}$ $[u', v'] = 2[u, v]$			
Step	Expression	$h_1 = 1$	$h_1^{-1}$ small	$h_1$ arbitrary
1	compute $rs_1$ : $z_0 = u_0^2, k'_1 = u_1^2 + f_3;$ $w_0 = f_0 + v_0^2 (= rs'_1/h_1^3);$	3S	3S	3S
2	compute $1/s_1$ and $s''_0$ : $w_1 = (1/w_0)z_0 (= h_1/s_1);$ $z_1 = k'_1 w_1, s''_0 = z_1 + u_1;$	1, 2M	1, 2M	1, 2M
3	compute $u'$ : $w_2 = h_1^2 w_1, u'_1 = w_2 w_1;$ $u'_0 = s''_0{}^2 + w_2;$	2S	S, 2M	S, 2M
4	compute $v'$ : $w_3 = w_2 + k'_1;$ $v'_1 = h_1^{-1}(w_3 z_1 + w_2 u'_1 + f_2 + v_1^2);$ $v'_0 = h_1^{-1}(w_3 u'_0 + f_1 + z_0);$	S, 3M	S, 3M	S, 5M
total		1, 6S, 5M	1, 5S, 7M	1, 5S, 9M

# Part III: Halving of Divisor Classes in Characteristic 2 and Genus 2

# What is Halving of a Divisor Class?

## Given:

- A hyperelliptic curve  $C$  given by an equation of form
$$C: y^2 + h(x)y = f(x)$$
over a field  $K$ ,
- The divisor class group  $\text{Pic}_C^0(K)$  of  $C$  with order  $2^k r$ , where  $r$  is odd,
- A divisor class  $\bar{D} = [u, v]$  in the order- $r$  subgroup  $S$  of  $\text{Pic}_C^0(K)$ .

**Problem:** Find a divisor class  $\bar{E} \in S$  such that  $[2]\bar{E} = \bar{D}$ .

# Why Halving on HEC?

- EC already have efficient point halving. So, it stands to reason to investigate halving on HEC, too.
- Efficient halving of divisor classes can make HEC cryptosystems faster:
  - Efficient halving can lead to faster scalar multiplication when using **half-and-add** instead of double-and-add.
  - Halving can be used by all known windowing methods.

# Example

Let  $\bar{D}$  be a divisor class in a order 17 subgroup of the Picard group of a hyperelliptic curve.

We want to compute  $[5]\bar{D}$ . This can be done using a double-and-add algorithm:

$$[2]\left([2]\bar{D}\right) + \bar{D} = [5]\bar{D} \quad (2 \text{ DBL}, 1 \text{ ADD})$$

But  $[5]\bar{D}$  can also be computed using the halving map:

$$[1/2]\left([1/2]P + P\right) = [3/4]P \quad (2 \text{ HLV}, 1 \text{ ADD})$$

because  $3/4 \equiv 5 \pmod{17}$ .

Write the scalar as  $\sum \frac{n_i}{2^i}$  instead of  $\sum n_i 2^i$  to use HLV.

Only **one** result about halving of divisor classes yet!

- Kitamura, Katagi, Takagi: A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two (ACISP 2005, ePrint 2004/255).
- Characteristic 2 case.
- They cover Type I curves and some special Type II curves.

- We focus on Type II curves over  $\mathbb{F}_{2^d}$ , where  $d$  is odd. Isomorphic transformations lead to a unique equation
$$C : y^2 + xy = x^5 + f_3x^3 + f_2x^2 + f_0,$$
with  $f_0 \in \mathbb{F}_{2^d}^*$ ,  $f_3 \in \mathbb{F}_{2^d}$  and  $f_2 \in \mathbb{F}_2$ .
- We have  $2 \cdot (2^d - 1) \cdot 2^d \approx 2^{2d+1}$  isomorphism classes of curves.
- Since the 2-rank of these curves is one, we can find curves  $C$  with  $\#\text{Pic}_C^0(\mathbb{F}_{2^d}) = 2r$ , where  $r$  is odd.
- Halving algorithm developed by inverting doubling formulae.

# From Doubling to Halving (1)

- Explicit formulae (by Lange and Stevens) to double a divisor class
- Given a divisor class  $\bar{E} = [u'_1, u'_0, v'_1, v'_0]$

$$u_1 = \left( \frac{u_0'^2}{f_0 + v_0'^2} \right)^2 \quad (1)$$

$$u_0 = \left( (u_1'^2 + f_3)\sqrt{u_1} + u_1' \right)^2 + \sqrt{u_1} \quad (2)$$

$$v_0 = \left( \sqrt{u_1} + u_1'^2 + f_3 \right) u_0 + u_0'^2 \quad (3)$$

$$v_1 = \left( \sqrt{u_1} + u_1'^2 + f_3 \right) + \sqrt{u_1} u_1 + f_2 + v_1'^2 \quad (4)$$

- Resulting divisor class  $\bar{D} = [2]\bar{E} = [u_1, u_0, v_1, v_0]$

## From Doubling to Halving (2)

- **Reverse doubling formulae** to perform halving!

- Start with (2) from doubling:

$$u_0 = \left( (u_1'^2 + f_3)\sqrt{u_1} + u_1' \right)^2 + \sqrt{u_1}$$

- Expand right-hand side and substitute  $U = u_1'^2$  :

$$U^2 u_1 + U = u_0 + f_3^2 u_1 + \sqrt{u_1}$$

- Solve quadratic equation in  $U$  over  $\mathbb{F}_{2^d}$  and get **two solutions** of  $u_1'$  by re-substituting  $u_1' = \sqrt{U}$

## From Doubling to Halving (3)

2 solutions  $\Rightarrow$  **2 possible divisor classes**. Which one is the right one?

- 2 divides the group order  $\Rightarrow$  2 preimages of  $\bar{D}$  under doubling:  $\bar{E}$  and  $\bar{E} + \zeta$ , where  $\zeta$  has order 2
- $[2]\bar{E} = \bar{D}$  and  $[2](\bar{E} + \zeta) = [2]\bar{E} + 0 = \bar{D}$
- Distinguish between  $\bar{E}$  and  $\bar{E} + \zeta$  by checking, if can be halved again ( $\zeta$  cannot be halved!)
- **Lemma**  
A divisor class  $\bar{D} = [u_1, u_0, v_1, v_0]$  can be halved  
 $\iff \text{Tr}(u_1(u_0 + \sqrt{u_1 + f_3^2 u_1})) = 0$ .

## From Doubling to Halving (4)

Check, if first or second solution of QE leads to  $\bar{E}$

- Compute  $u'_0$  and  $u'_1$  using the **first** solution
- Then use lemma to check if  $u'_1$  and  $u'_0$  belong to a divisor class that can be halved ( $\bar{E}$ ) or not ( $\bar{E} + \zeta$ )
- If  $\bar{E}$ , continue computing  $v'_0$  and  $v'_1$  (**Done!**)
- If  $\bar{E} + \zeta$ , re-compute  $u'_1$  and  $u'_0$  with the **second** solution and then compute  $v'_0$  and  $v'_1$  (**Done!**)

# The Halving Algorithm

---

**Algorithm 1** Divisor Class Halving (HLV)

---

INPUT: Divisor class  $\bar{D} = [u, v]$ , where  $u = x^2 + u_1x + u_0$ ,  $v = v_1x + v_0$  and the pre-computed values  $f_3^2, \sqrt{f_0}$

OUTPUT: Halved divisor class  $\bar{E} = [u', v']$  such that  $\bar{D} = 2\bar{E}$

- 1:  $q_1 \leftarrow \sqrt{u_1}$ ,  $q_2 \leftarrow 1/q_1$ ,  $q_3 \leftarrow q_2^2$ ,  $q_4 \leftarrow u_0q_3$ ,  $q_5 \leftarrow \sqrt{q_2}$  ▷ 1I, 1M, 2SR, 1S
  - 2:  $q_6 \leftarrow \sqrt{q_4}$ ,  $c \leftarrow u_1(q_6 + q_5 + f_3)$  ▷ 1SR, 1M
  - 3:  $t' \leftarrow \sum_{i=0}^{(d-3)/2} c^{2(2i+1)}$  ▷ 1HT
  - 4:  $u'_1 \leftarrow t'q_2$ ,  $t \leftarrow u_1^2$ ,  $s_1 \leftarrow v_0 + (q_1 + t + f_3)u_0$  ▷ 2M, 1S
  - 5:  $u'_0 \leftarrow \sqrt{s_1}$ ,  $b \leftarrow \text{Trace}(u'_1(u'_0 + t + f_3))$  ▷ 1M, 1SR, 1TR
  - 6: **if**  $b = 0$  **then**
  - 7:      $v'_0 \leftarrow q_5u'_0 + \sqrt{f_0}$  ▷ 1M
  - 8: **else**
  - 9:      $t \leftarrow t + q_3$ ,  $u'_1 \leftarrow u'_1 + q_2$
  - 10:     $u'_0 \leftarrow u'_0 + q_6$ ,  $v'_0 \leftarrow q_5u'_0 + \sqrt{f_0}$  ▷ 1M
  - 11: **end if**
  - 12:  $v'_1 \leftarrow \sqrt{v_1 + q_1 \left( (q_1 + t + f_3)(t + f_3) + u_1 \right) + f_2}$  ▷ 2M, 1SR
  - 13: **return**  $[x^2 + u'_1x + u'_0, v'_1x + v'_0]$  ▷ Total: 1I, 8M, 5SR, 2S, 1HT, 1TR
-

# Complexity of Halving on Genus 2 Curves

- Efficient halving algorithm for divisor classes
- Type II curves with equation  $y^2 + xy = x^5 + f_3x^3 + f_2x^2 + f_0$
- Base field is  $\mathbb{F}_{2^d}$  ( $d$  odd)

	<b>Type II curve</b> $y^2 + xy = x^5 + f_3x^3 + f_2x^2 + f_0$	<b>Special curve</b> (see KKT, Appendix D) $y^2 + xy = x^5 + f_0$
Kitamura Katagi, Takagi	1I, 15M, 3SR, 3S, 2HT, 2TR	1I, 12M, 5SR, 2S, 1HT, 1TR
Our work	1I, 8M, 5SR, 2S, 1HT, 1TR	

# Outlook: The Genus 3 Case

# The Genus 3 Case

- For genus 3, the curve  $y^2 + cy = f(x)$  over  $\mathbb{F}_{2^d}$  is **not supersingular!** Hence, it can be used for cryptography.
- The 2-rank of these curves is zero. Hence, doubling and halving can be performed in the whole Picard group because each divisor class has a unique preimage under doubling.
- The most frequent case of divisor class doubling on genus 3 curves is already done by
  - Guyot, Kaveh and Patankar,
  - Pelzl, Wollinger, Guajardo and Paar,
  - Xinxin Fan.
- Joint work with N. Thériault (University of Waterloo) on genus 3 halving is in progress.

Thank you for your attention!