Infrastructure versus Jacobian in Real Hyperelliptic Curves

Monireh Rezai Rad

Supervised by: Renate Scheidler and Michael Jacobson

Department of Mathematics and Statistics

University of Calgary

Alberta Number Theory Days 2016

April 17, 2016

Outline

Motivation

Why real hyperelliptic curves?

- Real hyperelliptic curves are more general than imaginary ones,
- they support a second baby step operation which is much faster than giant step,
- support two structures: Jacobian and infrastructure.

Question: *Which one is more efficient?*

Hyperelliptic Curves

Definition

A hyperelliptic curve of genus g over a finite field $\mathbb{F}_q$ is a non-singular, irreducible equation of the form

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

where $h, f \in \mathbb{F}_q[x]$ satisfy certain conditions.

For example, $h(x) = 0$ if $char(\mathbb{F}_q) \neq 2$.

Imaginary and Real Model

Hyperelliptic curves come in two models:

- Imaginary Model
  - f monic and $deg(f) = 2g + 1$,
  - $deg(h) \leq g$ if q even.

Imaginary and Real Model

Hyperelliptic curves come in two models:

- Imaginary Model
  - f monic and $deg(f) = 2g + 1$,
  - $deg(h) \leq g$ if q even.
- Real Model
  - If q odd: f monic and $deg(f) = 2g + 2$,
  - If q even: h monic and $deg(h) = g + 1$,
    - f monic and $deg(f) \leq 2g + 1$, or
    - $deg(f) = 2g + 2$, and $sgn(f) = e^2 + e$,$(e \in F_q^*)$.

Imaginary and Real Model

Hyperelliptic curves come in two models:

- Imaginary Model
  - f monic and $deg(f) = 2g + 1$,
  - $deg(h) \leq g$ if q even.
- Real Model
  - If q odd: f monic and $deg(f) = 2g + 2$,
  - If q even: h monic and $deg(h) = g + 1$,
    - f monic and $deg(f) \leq 2g + 1$, or
    - $deg(f) = 2g + 2$, and $sgn(f) = e^2 + e$,$(e \in F_q^*)$.

The imaginary model has one point ∞ at infinity.
The real model has two points at infinity, ∞^+ and ∞^-.

Why (Hyper-)Elliptic Cryptography?

They provide the same level of security as traditional groups like $\mathbb{F}_q$ with a much smaller group size.

Requirements on groups for discrete log based cryptography

- Large group order.
- Compact representation of group elements.
- Fast group operation.
- Hard Diffie-Hellman/discrete logarithm problem.

Divisors

Definition

A **divisor** D is a formal sum of points in C

$$D = \sum_{P \in C} n_P P \ , \ n_P \in \mathbb{Z}$$

where all $n_P = 0$, except for finitely many.

Jacobian - Divisors and Jacobian

Definition

The divisor class group $Cl^0(C)$ or the **Jacobian** is defined to be the quotient group of degree zero divisors modulo the principal divisors.

Jacobian - Divisors and Jacobian

Definition

The divisor class group $Cl^0(C)$ or the **Jacobian** is defined to be the quotient group of degree zero divisors modulo the principal divisors.

Hasse-Weil Theorem

The Jacobian of a hyperelliptic curve C of genus g over a finite field $\mathbb{F}_q$ is a finite group and

$$|Cl^0(C)| \approx q^g.$$

Jacobian - Divisors and Jacobian

Definition

The divisor class group $Cl^0(C)$ or the **Jacobian** is defined to be the quotient group of degree zero divisors modulo the principal divisors.

Hasse-Weil Theorem

The Jacobian of a hyperelliptic curve C of genus g over a finite field $\mathbb{F}_q$ is a finite group and

$$|Cl^0(C)| \approx q^g.$$

Bingo!

We have a finite group of a large order.

Mumford Representation

Definition

A **reduced** divisor D is an affine effective divisor with some certain properties which $\deg(D) \leq g$

Mumford Representation

Definition

A **reduced** divisor D is an affine effective divisor with some certain properties which $\deg(D) \leq g$

Mumford Representation

Each reduced divisor can be represented by two polynomials $[u, v]$ where $u, v \in \mathbb{F}[x]$ and $\deg(u) \leq g$, namely the **Mumford** representation.

Mumford Representation

Definition

A **reduced** divisor D is an affine effective divisor with some certain properties which $\deg(D) \leq g$

Mumford Representation

Each reduced divisor can be represented by two polynomials $[u, v]$ where $u, v \in \mathbb{F}[x]$ and $\deg(u) \leq g$, namely the **Mumford** representation.

Yes!

A compact representation

Is this Representation unique?

For a divisor class $[D] \in Cl^0(C)$,

- If C is imaginary then

$$D \equiv D' - deg(D')\infty$$

where $D' = [u, v]$ is a reduced divisor.

Is this Representation unique?

For a divisor class $[D] \in Cl^0(C)$,

- If C is imaginary then

$$D \equiv D' - deg(D')\infty$$

where $D' = [u, v]$ is a reduced divisor.

- If C is real then

$$D \equiv D' + n\infty^+ + m\infty^- - D_\infty$$

where $D' = [u, v]$ is reduced, $0 \leq n \leq g - \deg(u)$, and

$$D_\infty = \lceil \frac{g}{2} \rceil \infty^+ + \lfloor \frac{g}{2} \rfloor \infty^-.$$

Is this Representation unique?

For a divisor class $[D] \in Cl^0(C)$,

- If C is imaginary then

$$D \equiv D' - deg(D')\infty$$

where $D' = [u, v]$ is a reduced divisor.

- If C is real then

$$D \equiv D' + n\infty^+ + m\infty^- - D_\infty. \tag{1}$$

where $D' = [u, v]$ is reduced, $0 \le n \le g - \deg(u)$, and

$$D_\infty = (\lceil \frac{g}{2} \rceil \infty^+ + \lfloor \frac{g}{2} \rfloor \infty^-$$

(1) is called **the balanced** representative for $[D]$ and is denoted by $([u, v], n)$.

Jacobian - Example

Example

For any real hyperelliptic curve of genus g, we have the following balanced representations:

a) The balanced representative of the principal divisor class is $([1,0], \lceil g/2 \rceil)$.
b) The balanced representative of $[\infty^+ - \infty^-]$ is $([1,0], \lceil g/2 \rceil + 1)$.
c) The balanced representative of $[\infty^- - \infty^+]$ is $([1,0], \lceil g/2 \rceil - 1)$.

Infrastructure

Infrastructure

A reduce ideal of the coordinate ring $\mathbb{F}_q[C]$ is represented by two polynomials $[u, v]$ satisfying some certain conditions such as $\deg(u) \leq g$. Moreover the polynomial u is monic, unique, and v is unique modulo u.

Infrastructure

The infrastructure of C is defined to be the set $\mathcal{R}$ of all reduced principal ideals of $Fq[C]$. Moreover,

$$|\mathcal{R}| \approx |Cl^0(C)|.$$

Distance

Infrastructure and Distance

For every ideal $\mathfrak{a} = (\alpha) \in \mathcal{R}$, the **distance** of $\mathfrak{a}$ is defined to be

$$\delta(\mathfrak{a}) = \deg(\alpha).$$

The distance imposes an ordering on $\mathcal{R}$:

$$\mathcal{R} = \{\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_r\}, \quad 0 = \delta_1 < \delta_2 < \cdots < \delta_r < R \ ,$$

where $\mathfrak{a}_1 = (1)$ and $\delta_i = \delta(\mathfrak{a}_i)$.
We have $\delta_1 = 0$, $\delta_2 = g + 1$. Also,

$$\delta_{i+1} = \delta_i + g + 1 - \deg(u_i) \tag{2}$$

Jacobian Arithmetic Using Balanced Divisors

For any two balanced divisors D_1 and D_2 on C, the balanced representative of the class of $D_1 + D_2$ is denoted by $D_1 \oplus D_2$.

Algorithm 1 Divisor Class Addition

Input: Two balanced divisors $D_1 = (D_1', n_1)$ and $D_2 = (D_2', n_2)$.

Output: A balanced divisor $D_3 = (D_3', n_3) = D_1 \oplus D_2$.

1: Addition $D' =$Comp(D_1', D_2') (Cantor Algorithm)
2: Reduction $D'' = \mathrm{red}(D')$
3: Balancing D'' and put in D_3 and update n_3
4: **return** (D_3, n_3)

Infrastructure Arithmetic

The infrastructure supports two main operations.

Baby step

computes $\mathfrak{a}_{i+1}$ from $\mathfrak{a}_i$

Infrastructure Arithmetic

The infrastructure supports two main operations.

Baby step

computes $\mathfrak{a}_{i+1}$ from $\mathfrak{a}_i$

Giant step denoted by $\otimes$

$(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{a} \otimes \mathfrak{b}$, with

$$\delta(\mathfrak{a} \otimes \mathfrak{b}) = \delta(\mathfrak{a}) + \delta(\mathfrak{b}) - d \quad \text{with} \quad 0 \leq d \leq 2g \quad .$$

Infrastructure Arithmetic

The infrastructure supports two main operations.

Baby step

computes $\mathfrak{a}_{i+1}$ from $\mathfrak{a}_i$

Giant step denoted by $\otimes$

$(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{a} \otimes \mathfrak{b}$, with

$$\delta(\mathfrak{a} \otimes \mathfrak{b}) = \delta(\mathfrak{a}) + \delta(\mathfrak{b}) - d \quad \text{with} \quad 0 \leq d \leq 2g \quad .$$

The giant step is the cantor algorithm by some *adjustment* baby steps.

$\mathcal{R}$ is "almost" an abelian group under $\otimes$, failing associativity only barely.

Great!
An efficient arithmetic

How the Jacobian and the Infrastructure Related?

$$\phi : \mathcal{R} \to Cl^0(C), \quad \phi(\mathfrak{a}) = [\mathrm{div}(\mathfrak{a}) + (g - \deg(\mathfrak{a}))\infty^- - D_\infty].$$

How the Jacobian and the Infrastructure Related?

$$\phi : \mathcal{R} \to Cl^0(C), \quad \phi(\mathfrak{a}) = [\mathrm{div}(\mathfrak{a}) + (g - \deg(\mathfrak{a}))\infty^- - D_\infty].$$

Theorem

The image of $\mathcal{R}$ under ϕ is equal to $G \cap B$, where $G = \langle [\infty^+ - \infty^-] \rangle$ and B is the set of all classes in $Cl^0(C)$ whose balanced representative is of the form $([u, v], 0)$.

Image of ϕ and Holes

Question: What is outside of the image?

Definition

The elements in $Cl^0(C)$ which is not in image of ϕ are called holes. In fact a hole does not correspond to any infrastructure element.

Image of ϕ and Holes

Question: What is outside of the image?

Definition

The elements in $Cl^0(C)$ which is not in image of ϕ are called holes. In fact a hole does not correspond to any infrastructure element.

The holes in the infrastructure correspond to balanced divisors with $n \neq 0$ which needs balancing step (extra cost) in their arithmetic. So we are interested to avoid holes.

Why do we care about holes?

Question: How common a hole?

- The probability a divisor class is represented by a hole divisor is $\frac{1}{q}$ for sufficiently large q.
- With probability $1 - \frac{1}{q}$ there is no hole between two successive infrastructure $\mathfrak{a}_i$ and $\mathfrak{a}_{i+1}$ for $i \geq 2$.

Why do we care about holes?

Question: How common a hole?

- The probability a divisor class is represented by a hole divisor is $\frac{1}{q}$ for sufficiently large q.
- With probability $1 - \frac{1}{q}$ there is no hole between two successive infrastructure $\mathfrak{a}_i$ and $\mathfrak{a}_{i+1}$ for $i \geq 2$.

Heuristics

For sufficiently large q, the following properties hold with probability $1 - O(q^{-1})$:

(H1) $\delta(\mathfrak{a}_{i+1}) - \delta(\mathfrak{a}_i) = 1$ for $1 \leq i \leq r$.

(H2) $\delta(\mathfrak{a} \otimes \mathfrak{b}) = \delta(\mathfrak{a}) + \delta(\mathfrak{b}) - \lceil g/2 \rceil$ for all $\mathfrak{a}, \mathfrak{b} \in \mathcal{R} \setminus \{0\}$.

How often we do balancing.

With probability $1 - O(q^{-1})$:

1. For an infrastructure element $\mathfrak{a} = [u, v]$ and it divisor class correspond $\deg(u) = g$.

How often we do balancing.

With probability $1 - O(q^{-1})$:

1. For an infrastructure element $\mathfrak{a} = [u, v]$ and its correspond divisor class $\deg(u) = g$.
2. $\phi(\mathfrak{a}_{i+1}) = \phi(\mathfrak{a}_i) + [\infty^+ - \infty^-]$, i.e the baby step on $\mathcal{R}$ heuristically corresponds to the balancing step in $Cl^0(C)$.

How often we do balancing.

With probability $1 - O(q^{-1})$:

1. For an infrastructure element $\mathfrak{a} = [u, v]$ and its correspond divisor class $\deg(u) = g$.
2. $\phi(\mathfrak{a}_{i+1}) = \phi(\mathfrak{a}_i) + [\infty^+ - \infty^-]$, i.e the baby step on $\mathcal{R}$ heuristically corresponds to the balancing step in $Cl^0(C)$.
3. For two balanced divisors D_1 and D_2, $\lceil g/2 \rceil$ reduction steps and no balancing steps are needed to compute the balanced divisor $D_1 \oplus D_2$.

Infrastructure with the New Distance

Question:

Can we make the infrastructure competitive to the Jacobian?

Infrastructure with the New Distance

Question:

Can we make the infrastructure competitive to the Jacobian?

Answer: YES

We define a new distance as $\gamma(\mathfrak{a}) = \delta(\mathfrak{a}) - \lceil g/2 \rceil$.

Infrastructure with the New Distance

Question:

Can we make the infrastructure competitive to the Jacobian?

Answer: YES

We define a new distance as $\gamma(\mathfrak{a}) = \delta(\mathfrak{a}) - \lceil g/2 \rceil$.

With the new distance $\mathcal{R}$ is a group under the assumption of heuristics (H1) and (H2) since

$$\gamma(\mathfrak{a}_i \otimes \mathfrak{a}_{i+1}) = \gamma(\mathfrak{a}_i) + \gamma(\mathfrak{a}_{i+1}).$$

Balanced divisors versus Infrastructure

1- The classic infrastructure needs adjustment baby steps after each multiplication while the Jacobian and the infrastructure with the new distance do not.

2- The scalar multiplication in the classic infrastructure needs initial adjustment steps while the Jacobian and the infrastructure with the new distance do not.

Balanced divisors versus Infrastructure

1- The classic infrastructure needs adjustment baby steps after each multiplication while the Jacobian and the infrastructure with the new distance do not.

2- The scalar multiplication in the classic infrastructure needs initial adjustment steps while the Jacobian and the infrastructure with the new distance do not.

Result

- The classic infrastructure is less efficient than the the Jacobian.
- The infrastructure with the new distance is identical to the Jacobian.

Operation counts for scalar multiplication

Operation counts for scalar multiplication in $G = \langle[\infty^+ - \infty^-]\rangle$ and $\mathcal{R}$.

Table: Operation counts for scalar multiplication

	Doubles	Adds	Baby Steps
Imaginary	l	$l/3$	-
Real, Inf	$2l$	$l/3+1$	$l/3+\lceil g/2\rceil$
Real, Jac	$2l-\lceil\log_2(c)\rceil$	$l/3$	$c+(l-\lceil\log_2(c)\rceil)/3$

Where $c = \lfloor g/2\rfloor + 1$.

Numerical result

Table: Scalar multiplication and key exchange timings over $\mathbb{F}_p$ (in milliseconds) when $g = 3$.

Security Level (in bits)	Total Diffie-Hellman		
	Imag	Real Jac	Real Infra
80	6.907	8.345	8.408
112	11.898	14.643	14.7045
128	13.8725	16.962	17.025
192	25.7395	30.9435	31.0795
256	41.8	50.1305	50.3215

Thank you for your attention!