Elliptic and Hyperelliptic Curve Cryptography

Renate Scheidler

Research supported in part by NSERC of Canada
Comprehensive Source

Handbook of Elliptic and Hyperelliptic Curve Cryptography
Overview

- Motivation
- Elliptic Curve Arithmetic
- Hyperelliptic Curve Arithmetic
- Point Counting
- Discrete Logarithm Algorithms
- Other Models
Motivation — Why (Hyper-)Elliptic Cryptography?

Requirements on groups for discrete log based cryptography

- Large group order (plus other restrictions)
- Compact representation of group elements
- Fast group operation
- Hard Diffie-Hellman/discrete logarithm problem
Motivation — Why (Hyper-)Elliptic Cryptography?

Requirements on groups for discrete log based cryptography

- Large group order (plus other restrictions)
- Compact representation of group elements
- Fast group operation
- Hard Diffie-Hellman/discrete logarithm problem

Elliptic and low genus hyperelliptic curves do well on all of these!
Elliptic Curves

Let $K$ be a field (in crypto, $K = \mathbb{F}_q$ with $q$ prime or $q = 2^n$)
Elliptic Curves

Let $K$ be a field (in crypto, $K = \mathbb{F}_q$ with $q$ prime or $q = 2^n$)

**Weierstraß equation** over $K$:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad \text{(**)}$$

with $a_1, a_2, a_3, a_4, a_6 \in K$
Elliptic Curves

Let $K$ be a field (in crypto, $K = \mathbb{F}_q$ with $q$ prime or $q = 2^n$)

Weierstraß equation over $K$:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

(*)

with $a_1, a_2, a_3, a_4, a_6 \in K$

Elliptic curve: Weierstraß equation & non-singularity condition: there are no simultaneous solutions to (*) and

$$2y + a_1x + a_3 = 0$$

$$a_1y = 3x^2 + 2a_2x + a_4$$
Elliptic Curves

Let $K$ be a field (in crypto, $K = \mathbb{F}_q$ with $q$ prime or $q = 2^n$)

Weierstraß equation over $K$:

\[ E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \]  

(*)

with $a_1, a_2, a_3, a_4, a_6 \in K$

Elliptic curve: Weierstraß equation & non-singularity condition: there are no simultaneous solutions to (*) and

\[
2y + a_1x + a_3 = 0
\]
\[
a_1y = 3x^2 + 2a_2x + a_4
\]

Non-singularity $\iff \Delta \neq 0$ where $\Delta$ is the discriminant of $E$
Non-Examples

Two Weierstraß equations with a singularity at (0, 0)

\[ y^2 = x^3 \quad \text{and} \quad y^2 = x^2(x - 1) \]
An Example

\[ E : y^2 = x^3 - 5x \text{ over } \mathbb{Q} \]
Elliptic Curves, $\text{char}(K) \not= 2, 3$

The variable transformations

$$y \rightarrow y - (a_1 x + a_3)/2, \text{ then } x \rightarrow x - (a_1^2 + 4a_2)/12 :$$

yield an elliptic curve in **short** Weierstraß form:

$$E : \quad y^2 = x^3 + Ax + B \quad (A, B \in K)$$

Discriminant $\Delta = 4A^3 + 27B^2 \not= 0$ (cubic in $x$ has distinct roots)
Elliptic Curves, $\text{char}(K) \neq 2, 3$

The variable transformations

$$y \rightarrow y - (a_1x + a_3)/2, \text{ then } x \rightarrow x - (a_1^2 + 4a_2)/12 :$$

yield an elliptic curve in **short** Weierstraß form:

$$E : \quad y^2 = x^3 + Ax + B \quad (A, B \in K)$$

Discriminant $\Delta = 4A^3 + 27B^2 \neq 0$ (cubic in $x$ has distinct roots)

For any field $L$ with $K \subseteq L \subseteq \overline{K}$:

$$E(L) = \{(x_0, y_0) \in L \times L \mid y_0^2 = x_0^3 + Ax_0 + B\} \cup \{\infty\}$$

set of **$L$-rational points** on $E$
An Example

\[ E(\mathbb{Q}) = \{(x_0, y_0) \in \mathbb{Q} \times \mathbb{Q} \mid y_0^2 = x_0^3 - 5x_0\} \cup \{\infty\} \]

\[ P_1 = (-1, 2), \ P_2 = (0, 0) \in E(\mathbb{Q}) \]
The Mysterious Point at Infinity

In $E$, replace $x$ by $x/z$, $y$ by $y/z$, then multiply by $z^3$:

$$E_{\text{proj}} : y^2z = x^3 + Axz^2 + Bz^3$$
The Mysterious Point at Infinity

In $E$, replace $x$ by $x/z$, $y$ by $y/z$, then multiply by $z^3$:

$$E_{\text{proj}} : y^2z = x^3 + Axyz^2 + Bz^3$$

Points on $E_{\text{proj}}$:

$[x : y : z] \neq [0 : 0 : 0]$ normalized so the last non-zero entry is 1
The Mysterious Point at Infinity

In $E$, replace $x$ by $x/z$, $y$ by $y/z$, then multiply by $z^3$:

$$E_{\text{proj}} : y^2z = x^3 + Axz^2 + Bz^3$$

Points on $E_{\text{proj}}$:

$$[x : y : z] \neq [0 : 0 : 0]$$ normalized so the last non-zero entry is 1

<table>
<thead>
<tr>
<th>Affine Points</th>
<th>Projective Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x, y)$</td>
<td>$[x : y : 1]$</td>
</tr>
<tr>
<td>$\infty$</td>
<td>$[0 : 1 : 0]$</td>
</tr>
</tbody>
</table>
Arithmetic on $E$

**Goal:** Make $E(L)$ into an additive (Abelian) group

The identity is the point at infinity
Arithmetic on $E$

**Goal:** Make $E(L)$ into an additive (Abelian) group

The identity is the point at infinity

By **Bezout’s Theorem**, any line intersects $E$ in three points

- Need to count multiplicities
- If one of the points is $\infty$, the line is “vertical”
Arithmetic on \( E \)

**Goal:** Make \( E(L) \) into an additive (Abelian) group

The identity is the point at infinity

By **Bezout’s Theorem**, any line intersects \( E \) in three points
  - Need to count multiplicities
  - If one of the points is \( \infty \), the line is “vertical”

Motto: “Any three collinear points on \( E \) sum to zero”

AKA **Chord & Tangent Addition Law**
Arithmetic on $E$ — Inverses

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, \hspace{1cm} $P = (-1, -2)$

The line through $P$ and $\infty$ is $x = -1$
Arithmetic on $E$ — Inverses

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, \hspace{1cm} $P = (-1, -2)$

It intersects $E$ in the third point $R = (-1, 2) = -P$
Arithmetic on $E$ — Addition

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$,

$P_1 = (-1, -2), \quad P_2 = (0, 0)$

The line through $P_1$ and $P_2$ is $y = 2x$
Arithmetic on $E$ — Addition

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, \hspace{1cm} $P_1 = (-1, -2), \hspace{0.5cm} P_2 = (0, 0)$

It intersects $E$ in the third point $G = (5, 10)$
Arithmetic on $E$ — Addition

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$,

$P_1 = (-1, -2), \quad P_2 = (0, 0)$

\[ R = -G = (5, -10) = P + Q \]
Arithmetic on $E$ — Doubling

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, \hspace{1cm} $P = (-1, -2)$

The line tangent to $E$ at $P$ is $y = \frac{19}{26}x - \frac{33}{26}$
Arithmetic on $E$ — Doubling

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, \hspace{1cm} $P = (-1, -2)$

It intersects $E$ in the third point $G = \left(\frac{9}{4}, \frac{3}{8}\right)$
Arithmetic on $E$ — Doubling

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$,

$P = (-1, -2)$

The sum $R$ is the inverse of $G$, i.e.

$$R = -G = \left(\frac{9}{4}, -\frac{3}{8}\right) = 2P$$
Arithmetic on Short Weierstraß Form — Summary

\[ P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2) \quad (P_1 \neq -P_2; \quad P_1, P_2 \neq \infty) \]

\[ -P_1 = (-x_1, y_1) \]

\[ P_1 + P_2 = \left( \lambda^2 - x_1 - x_2, \quad -\lambda^3 + \lambda(x_1 + x_2) - \mu \right) \text{ where} \]

\[
\lambda = \begin{cases} 
\frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\
\frac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2
\end{cases}
\]

\[
\mu = \begin{cases} 
\frac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\
\frac{-x_1^3 + Ax_1 + 2B}{2y_1} & \text{if } P_1 = P_2
\end{cases}
\]
Beyond Elliptic Curves

Recall Weierstraß equation:

\[
E : y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6
\]

\[
\begin{align*}
\text{deg}(f) &= 3 = 2 \cdot 1 + 1 \text{ odd} \\
\text{deg}(h) &= 1 \text{ for } \text{char}(K) = 2; \ h = 0 \text{ for } \text{char}(K) \neq 2
\end{align*}
\]
Beyond Elliptic Curves

Recall Weierstraß equation:

\[ E : y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6 \]

\[ \underbrace{h(x)}_{\text{deg } h = 1 \text{ for } \text{char}(K) = 2} \quad \underbrace{f(x)}_{\text{deg } f = 3 = 2 \cdot 1 + 1 \text{ odd}} \]

\[ \text{deg}(f) = 3 = 2 \cdot 1 + 1 \text{ odd} \]
\[ \text{deg}(h) = 1 \text{ for } \text{char}(K) = 2; \ h = 0 \text{ for } \text{char}(K) \neq 2 \]

Generalization: \( \text{deg}(f) = 2g + 1, \ \text{deg}(h) \leq g \)

\( g \) is the **genus** of the curve
Beyond Elliptic Curves

Recall Weierstraß equation:

\[ E : y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6 \]

\[ h(x) \quad f(x) \]

\[ \text{deg}(f) = 3 = 2 \cdot 1 + 1 \text{ odd} \]
\[ \text{deg}(h) = 1 \text{ for } \text{char}(K) = 2; \ h = 0 \text{ for } \text{char}(K) \neq 2 \]

Generalization: \( \text{deg}(f) = 2g + 1, \ \text{deg}(h) \leq g \)

\( g \) is the **genus** of the curve

\( g = 1: \) elliptic curves

\( g = 2: \ \text{deg}(f) = 5, \ \text{deg}(h) \leq 2 \quad — \quad \text{also good for crypto} \)
Hyperelliptic Curves

Hyperelliptic curve of genus $g$ over $K$:

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

- $h(x), f(x) \in K[x]$
- $f(x)$ monic and $\deg(f) = 2g + 1$ is odd
- $\deg(h) \leq g$ if $\text{char}(K) = 2$; $h(x) = 0$ if $\text{char}(K) \neq 2$
- non-singularity
Hyperelliptic Curves

Hyperelliptic curve of genus $g$ over $K$:

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

- $h(x), f(x) \in K[x]$
- $f(x)$ monic and $\deg(f) = 2g + 1$ is odd
- $\deg(h) \leq g$ if $\text{char}(K) = 2$; $h(x) = 0$ if $\text{char}(K) \neq 2$
- non-singularity

$\text{char}(K) \neq 2$: $y^2 = f(x)$, $f(x)$ monic, of odd degree, square-free
Hyperelliptic Curves

Hyperelliptic curve of genus \( g \) over \( K \):

\[
H : y^2 + h(x)y = f(x)
\]

- \( h(x), f(x) \in K[x] \)
- \( f(x) \) monic and \( \deg(f) = 2g + 1 \) is odd
- \( \deg(h) \leq g \) if \( \text{char}(K) = 2 \); \( h(x) = 0 \) if \( \text{char}(K) \neq 2 \)
- non-singularity

\( \text{char}(K) \neq 2 \):

\[
y^2 = f(x), \quad f(x) \text{ monic, of odd degree, square-free}
\]

Set of \( L \)-rational points on \( H \) (\( K \subseteq L \subseteq \overline{K} \)):

\[
H(L) = \{(x_0, y_0) \in L \times L \mid y_0^2 + h(x_0)y = f(x_0)\} \cup \{\infty\}
\]
An Example

\[ H : y^2 = x^5 - 5x^3 + 4x - 1 \text{ over } \mathbb{Q}, \text{ genus } g = 2 \]
An Example

\((-2, -1), (2, -1), (3, -11) \in H(\mathbb{Q})\)
Group of divisors on $H$:

$$
\text{Div}_H(\overline{K}) = \langle H(\overline{K}) \rangle = \left\{ \sum_{\text{finite}} m_P P \mid m_P \in \mathbb{Z}, \ P \in H(\overline{K}) \right\}
$$
Divisors

- Group of \textbf{divisors} on $H$:

\[
\text{Div}_H(K) = \langle H(K) \rangle = \left\{ \sum_{\text{finite}} m_P P \mid m_P \in \mathbb{Z}, P \in H(K) \right\}
\]

- Subgroup of \textbf{degree zero divisors} on $H$:

\[
\text{Div}^0_H(K) = \langle [P] \mid P \in H(K) \rangle = \left\{ \sum_{\text{finite}} m_P [P] \mid m_P \in \mathbb{Z}, P \in H(K) \right\}
\]

where \([P] = P - \infty\)
Divisors

- Group of **divisors** on $H$:

$$\text{Div}_H(K) = \langle H(K) \rangle = \left\{ \sum_{\text{finite}} m_P P \mid m_P \in \mathbb{Z}, P \in H(K) \right\}$$

- Subgroup of $\text{Div}_H(K)$ of **degree zero divisors** on $H$:

$$\text{Div}^0_H(K) = \langle [P] \mid P \in H(K) \rangle = \left\{ \sum_{\text{finite}} m_P [P] \mid m_P \in \mathbb{Z}, P \in H(K) \right\}$$

where $[P] = P - \infty$

- Subgroup of $\text{Div}^0_H(K)$ of **principal divisors** on $H$:

$$\text{Prin}_H(K) = \left\{ \sum_{\text{finite}} v_P(\alpha) [P] \mid \alpha \in K(x, y), P \in H(K) \right\}$$
The Jacobian

**Jacobian** of $H$: \[ \text{Jac}_H(K) = \text{Div}_H^0(K)/\text{Prin}_H(K) \]

Motto: “Any complete collection of points on a function sums to zero”
The Jacobian

**Jacobian** of $H$:

\[
\text{Jac}_H(K) = \text{Div}_H^0(K)/\text{Prin}_H(K)
\]

Motto: “Any complete collection of points on a function sums to zero”

\[
H(K) \leftrightarrow \text{Jac}_H(K) \quad \text{via} \quad P \mapsto [P]
\]
The Jacobian

**Jacobian** of $H$: \[ \text{Jac}_H(K) = \text{Div}_H^0(K)/\text{Prin}_H(K) \]

Motto: “Any complete collection of points on a function sums to zero”

\[ H(K) \leftrightarrow \text{Jac}_H(K) \text{ via } P \mapsto [P] \]

For elliptic curves: \[ E(K) \cong \text{Jac}_E(K) \rightarrow E(K) \text{ is a group} \]
The Jacobian

**Jacobian** of $H$:

\[ \text{Jac}_H(K) = \text{Div}_H^0(K) / \text{Prin}_H(K) \]

Motto: “Any complete collection of points on a function sums to zero”

\[ H(K) \leftrightarrow \text{Jac}_H(K) \quad \text{via} \quad P \mapsto [P] \]

For elliptic curves: \( E(K) \cong \text{Jac}_E(K) \quad (\Rightarrow \ E(K) \text{ is a group}) \)

**Identity**: \([\infty] = \infty - \infty\)
The Jacobian

Jacobian of $H$: \[ \text{Jac}_H(\overline{K}) = \text{Div}_H^0(\overline{K})/\text{Prin}_H(\overline{K}) \]

Motto: “Any complete collection of points on a function sums to zero”

\[ H(\overline{K}) \leftrightarrow \text{Jac}_H(\overline{K}) \quad \text{via} \quad P \mapsto [P] \]

For elliptic curves: \( E(\overline{K}) \cong \text{Jac}_E(\overline{K}) \) \( \implies E(\overline{K}) \) is a group

Identity: \( [\infty] = \infty - \infty \)

Inverses: The points

\[ P = (x_0, y_0) \quad \text{and} \quad \overline{P} = (x_0, -y_0 - h(x_0)) \]

on $H$ both lie on the function $x = x_0$, so

\[ -[P] = [\overline{P}] \]
Semi-Reduced and Reduced Divisors

Every class in $\text{Jac}_H(\overline{K})$ contains a divisor $\sum_{\text{finite}} m_P[P]$ such that:

- all $m_P > 0$
- if $P = \overline{P}$, then $m_P = 1$
- if $P \neq \overline{P}$, then only one of $P$, $\overline{P}$ can appear in the sum

(replace $- [P]$ by $[\overline{P}]$) (as $2[P] = 0$) (as $[P] + [\overline{P}] = 0$)
Semi-Reduced and Reduced Divisors

Every class in $\text{Jac}_H(\overline{K})$ contains a divisor $\sum_{\text{finite}} m_P [P]$ such that

- all $m_P > 0$
- if $P = \overline{P}$, then $m_P = 1$
- if $P \neq \overline{P}$, then only one of $P, \overline{P}$ can appear in the sum

(replace $-[P]$ by $[\overline{P}]$) (as $2[P] = 0$) (as $[P] + [\overline{P}] = 0$)

Such a divisor is **semi-reduced**.
Semi-Reduced and Reduced Divisors

Every class in $\text{Jac}_H(\overline{K})$ contains a divisor $\sum_{\text{finite}} m_P[P]$ such that

- all $m_P > 0$ (replace $-[P]$ by $[\overline{P}]$)
- if $P = \overline{P}$, then $m_P = 1$ (as $2[P] = 0$)
- if $P \neq \overline{P}$, then only one of $P$, $\overline{P}$ can appear in the sum (as $[P] + [\overline{P}] = 0$)

Such a divisor is **semi-reduced**. If $\sum m_P \leq g$, then it is **reduced**.
Semi-Reduced and Reduced Divisors

Every class in \( \text{Jac}_H(\bar{K}) \) contains a divisor \( \sum_{\text{finite}} m_P [P] \) such that

- all \( m_P > 0 \) (replace \( -[P] \) by \( [\bar{P}] \))
- if \( P = \bar{P} \), then \( m_P = 1 \) (as \( 2[P] = 0 \))
- if \( P \neq \bar{P} \), then only one of \( P, \bar{P} \) can appear in the sum (as \( [P] + [\bar{P}] = 0 \))

Such a divisor is **semi-reduced**. If \( \sum m_P \leq g \), then it is **reduced**.

**Theorem**

Every class in \( \text{Jac}_H(\bar{K}) \) contains a unique reduced divisor.
Example — Reduction

\[ H : y^2 = x^5 - 5x^3 + 4x - 1 \] over \( \mathbb{Q} \), \( D = [R_1] + [R_2] + [R_3] \) with

- \( R_1 = (-2, -1) \)
- \( R_2 = (2, -1) \)
- \( R_3 = (3, -11) \)
Example — Reduction

\( R_1, R_2, R_3 \) all lie on the quadratic \( y = -2x^2 + 7 \)
Example — Reduction

This quadratic meets $H$ in the two additional points $G_1$, $G_2$ where

$G_1 = \left( \frac{1}{2} (1 + \sqrt{17}), -2 - \sqrt{17} \right), \quad G_2 = \left( \frac{1}{2} (1 - \sqrt{17}), -2 + \sqrt{17} \right)$

Thus, $[R_1] + [R_2] + [R_3] + [G_1] + [G_2] = 0$ in $\text{Jac}_H(\mathbb{Q})$
Example — Reduction

\[ [R_1] + [R_2] + R_3] = [B_1] + [B_2] \text{ with } B_1 = [\overline{G_1}], \ B_2 = [\overline{G_2}] \]

The reduced divisor in the class of \( D \) is \( E = [B_1] + B_2 \) where

\[
B_1 = \left( \frac{1}{2} (1 + \sqrt{17}), 2 + \sqrt{17} \right), \quad \quad B_2 = \left( \frac{1}{2} (1 - \sqrt{17}), 2 - \sqrt{17} \right),
\]
Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$.
Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

The $r$ points $P_i$ all lie on a curve $y = \nu(x)$ with $\deg(\nu) = r - 1$
Reduction in General

Let \( D = \sum_{i=1}^{r} [P_i] \) be a semi-reduced divisor on \( y^2 + h(x)y = f(x) \)

The \( r \) points \( P_i \) all lie on a curve \( y = \nu(x) \) with \( \deg(\nu) = r - 1 \)

\[ \nu(x)^2 + h(x)h(x) = f(x) \] polynomial of degree \( \max\{2r - 2, 2g + 1\} \)
Reduction in General

Let \( D = \sum_{i=1}^{r} [P_i] \) be a semi-reduced divisor on \( y^2 + h(x)y = f(x) \)

The \( r \) points \( P_i \) all lie on a curve \( y = \nu(x) \) with \( \deg(\nu) = r - 1 \)

\( \nu(x)^2 + h(x)h(x) = f(x) \) polynomial of degree \( \max\{2r - 2, 2g + 1\} \)

**Case** \( r \geq g + 2 \): replace the \( r \) points \( P_1, \ldots, P_r \) in \( D \) by the inverses of the other \( (2r - 2) - r = r - 2 \) points on this degree \( 2r - 2 \) polynomial
Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$

$v(x)^2 + h(x)h(x) = f(x)$ polynomial of degree $\max\{2r - 2, 2g + 1\}$

**Case** $r \geq g + 2$: replace the $r$ points $P_1, \ldots, P_r$ in $D$ by the inverses of the other $(2r - 2) - r = r - 2$ points on this degree $2r - 2$ polynomial

**Case** $r = g + 1$: replace the $g + 1$ points $P_1, \ldots, P_r$ in $D$ by the inverses of the other $2g + 1 - (g + 1) = g$ points on this degree $2g + 2$ polynomial
Reduction in General

Let $D = \sum_{i=1}^{r} [P_i]$ be a semi-reduced divisor on $y^2 + h(x)y = f(x)$

The $r$ points $P_i$ all lie on a curve $y = v(x)$ with $\deg(v) = r - 1$

$v(x)^2 + h(x)h(x) = f(x)$ polynomial of degree $\max\{2r - 2, 2g + 1\}$

Case $r \geq g + 2$: replace the $r$ points $P_1, \ldots, P_r$ in $D$ by the inverses of the other $(2r - 2) - r = r - 2$ points on this degree $2r - 2$ polynomial.

Case $r = g + 1$: replace the $g + 1$ points $P_1, \ldots, P_r$ in $D$ by the inverses of the other $2g + 1 - (g + 1) = g$ points on this degree $2g + 2$ polynomial.

After $\left\lfloor \frac{r - g}{2} \right\rfloor$ steps a reduced divisor is obtained \(\Box\)
Mumford Representation

Let $D = \sum_{i=1}^{r} m_i[P_i]$ be a semi-reduced divisor, $P_i = (x_i, y_i)$.

The **Mumford representation** of $D$ is $D = (u(x), v(x))$ where

\[
u(x), v(x) \in \overline{K}[x], \; u \text{ monic, } \deg(v) < \deg(u), \; u \mid v^2 + hv - f\]
Let \( D = \sum_{i=1}^{r} m_i[P_i] \) be a semi-reduced divisor, \( P_i = (x_i, y_i) \)

The **Mumford representation** of \( D \) is \( D = (u(x), v(x)) \) where

\[
\begin{align*}
u(x), v(x) &\in \overline{K}[x], \quad \text{monic, } \deg(v) < \deg(u), \quad u \mid v^2 + hv - f \\
\end{align*}
\]

\[
\begin{align*}
\frac{d}{dx} \left[ v(x)^2 + v(x) h(x) - f(x) \right]_{x=x_i} &= 0 \quad \text{(0 \leq j \leq m_i - 1)} \\
\end{align*}
\]

So \( u(x_i) = 0 \) and \( v(x_i) = y_i \) with multiplicity \( m_i \) for \( 1 \leq i \leq r \)
Mumford Representation

Let \( D = \sum_{i=1}^{r} m_i [P_i] \) be a semi-reduced divisor, \( P_i = (x_i, y_i) \)

The **Mumford representation** of \( D \) is \( D = (u(x), v(x)) \) where

\[ u(x), v(x) \in \overline{K}[x], \ u \text{ monic, } \deg(v) < \deg(u), \ u \mid v^2 + hv - f \]

\[
\begin{align*}
    u(x) &= \prod_{i=1}^{r} (x - x_i)^{m_i} \\
    \left( \frac{d}{dx} \right)^j \left[ v(x)^2 + v(x) h(x) - f(x) \right]_{x=x_i} &= 0 \quad (0 \leq j \leq m_i - 1)
\end{align*}
\]

So \( u(x_i) = 0 \) and \( v(x_i) = y_i \) with multiplicity \( m_i \) for \( 1 \leq i \leq r \)

Mumford representation uniquely determines \( D \)
Let $D = \sum_{i=1}^{r} m_i [P_i]$ be a semi-reduced divisor, $P_i = (x_i, y_i)$

The **Mumford representation** of $D$ is $D = (u(x), v(x))$ where

$u(x), v(x) \in \overline{K}[x], \quad u \text{ monic}, \quad \deg(v) < \deg(u), \quad u \mid v^2 + hv - f$

\[
\begin{align*}
  u(x) &= \prod_{i=1}^{r} (x - x_i)^{m_i} \\
  \left( \frac{d}{dx} \right)^j \left[ v(x)^2 + v(x) h(x) - f(x) \right]_{x=x_i} &= 0 \quad (0 \leq j \leq m_i - 1)
\end{align*}
\]

So $u(x_i) = 0$ and $v(x_i) = y_i$ with multiplicity $m_i$ for $1 \leq i \leq r$

Mumford representation uniquely determines $D$

**Example:** If $P = (x_0, y_0)$, then $D = [P] = (x - x_0, y_0)$
Divisor Reduction Using Mumford Representations

Input: $D = (u, v)$

Output: The reduced divisor $D' = (u', v')$ in the class of $D$
Divisor Reduction Using Mumford Representations

**Input:** \( D = (u, v) \)

**Output:** The reduced divisor \( D' = (u', v') \) in the class of \( D \)

```plaintext
while \( \deg(u) > g \) do
    \[
    u' = \frac{f - vh - v^2}{u}, \quad v' \equiv -v - h \pmod{u'}
    \]
    \[
    u = u', \quad v = v'
    \]
end while

return \( (u', v') \)
```
Divisor Reduction — Example

\[ H : y^2 = x^5 - 5x^3 + 4x - 1 \text{ over } \mathbb{Q} \]

\[ D = [(-2, -1)] + [(2, 1)] + [(3, -11)] = (u, v) \]
Divisor Reduction — Example

\[ H : \quad y^2 = x^5 - 5x^3 + 4x - 1 \text{ over } \mathbb{Q} \]

\[ D = [(-2, -1)] + [(2, 1)] + [(3, -11)] = (u, v) \text{ with} \]

\[ u(x) = (x + 2)(x - 2)(x - 3) = x^3 - 3x^2 - 4x + 2 \]

\[ v(x) = -2x^2 + 7 \quad (\text{from before}) \]
Divisor Reduction — Example

$H : \ y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$

$D = [(-2, -1)] + [(2, 1)] + [(3, -11)] = (u, v)$ with

$u(x) = (x + 2)(x - 2)(x - 3) = x^3 - 3x^2 - 4x + 2$
$v(x) = -2x^2 + 7$ (from before)

$u'(x) = \frac{(x^5 - 5x^3 + 4x - 1) - (-2x^2 + 7)^2}{x^3 - 3x^2 - 4x + 2} = x^2 - x - 4$
$v'(x) \equiv -(-2x^2 + 7) \ (\text{mod } x^2 - x - 4) = 2x + 1$

$D' = (u', v')$ is the reduced divisor in the class of $D$
Divisor Reduction — Example

\[ H : \quad y^2 = x^5 - 5x^3 + 4x - 1 \text{ over } \mathbb{Q} \]

\[ D = [(-2, -1)] + [(2, 1)] + [(3, -11)] = (u, v) \text{ with} \]

\[ u(x) = (x + 2)(x - 2)(x - 3) = x^3 - 3x^2 - 4x + 2 \]
\[ v(x) = -2x^2 + 7 \quad \text{(from before)} \]

\[ u'(x) = \frac{(x^5 - 5x^3 + 4x - 1) - (-2x^2 + 7)^2}{x^3 - 3x^2 - 4x + 2} = x^2 - x - 4 \]
\[ v'(x) \equiv -(-2x^2 + 7) \pmod{x^2 - x - 4} = 2x + 1 \]

\[ D' = (u', v') \text{ is the reduced divisor in the class of } D \]

Recall \[ D' = \left[ \left( \frac{1}{2}(1 + \sqrt{17}), 2 + \sqrt{17} \right) \right] + \left[ \left( \frac{1}{2}(1 - \sqrt{17}), 2 - \sqrt{17} \right) \right] \]
Divisor Addition Using Mumford Representations

\[ D_1 = (u_1, v_1), \quad D_2 = (u_2, v_2) \] divisors on \( H : y^2 + h(x)y = f(x) \)
Divisor Addition Using Mumford Representations

\[ D_1 = (u_1, v_1), \quad D_2 = (u_2, v_2) \text{ divisors on } H : y^2 + h(x)y = f(x) \]

Simplest case: for any \([P]\) occurring in \(D_1\), \([\overline{P}]\) does not occur in \(D_2\) and vice versa — then \(D_1 + D_2\) is semi-reduced
Divisor Addition Using Mumford Representations

\[ D_1 = (u_1, v_1), \quad D_2 = (u_2, v_2) \] divisors on \[ H : y^2 + h(x)y = f(x) \]

Simplest case: for any \([P]\) occurring in \(D_1\), \([-P]\) does not occur in \(D_2\) and vice versa — then \(D_1 + D_2\) is semi-reduced

Then \(D_1 + D_2 = (u, v)\) where \(u = u_1u_2\) and
\[
\begin{align*}
v &= v_1 \pmod{u_1} \\
v &= v_2 \pmod{u_2}
\end{align*}
\]
Divisor Addition Using Mumford Representations

\[ D_1 = (u_1, v_1), \quad D_2 = (u_2, v_2) \text{ divisors on } H : y^2 + h(x)y = f(x) \]

Simplest case: for any \([P]\) occurring in \(D_1\), \([\overline{P}]\) does not occur in \(D_2\) and vice versa — then \(D_1 + D_2\) is semi-reduced

Then \(D_1 + D_2 = (u, v)\) where \(u = u_1u_2\) and

\[
v = \begin{cases} 
    v_1 \pmod{u_1} \\
    v_2 \pmod{u_2} 
\end{cases}
\]

In general: suppose \(P = (x_0, y_0)\) occurs in \(D_1\) and \(\overline{P}\) occurs in \(D_2\).
Divisor Addition Using Mumford Representations

\[ D_1 = (u_1, v_1), \quad D_2 = (u_2, v_2) \text{ divisors on } H : y^2 + h(x)y = f(x) \]

Simplest case: for any \( [P] \) occurring in \( D_1 \), \( [\overline{P}] \) does not occur in \( D_2 \) and vice versa — then \( D_1 + D_2 \) is semi-reduced

Then \( D_1 + D_2 = (u, v) \) where \( u = u_1u_2 \) and \( v = \begin{cases} v_1 \pmod{u_1} \\ v_2 \pmod{u_2} \end{cases} \)

In general: suppose \( P = (x_0, y_0) \) occurs in \( D_1 \) and \( \overline{P} \) occurs in \( D_2 \). Then \( u_1(x_0) = u_2(x_0) = 0 \) and \( v_1(x_0) = y_0 = -v_2(x_0) - h(x_0) \), so \( x - x_0 \mid u_1(x), \ u_2(x), \ v_1(x) + v_2(x) + h(x) \)
Divisor Addition Using Mumford Representations

\[ D_1 = (u_1, v_1), \quad D_2 = (u_2, v_2) \] divisors on \( H : y^2 + h(x)y = f(x) \)

Simplest case: for any \( [P] \) occurring in \( D_1, [\overline{P}] \) does not occur in \( D_2 \) and vice versa — then \( D_1 + D_2 \) is semi-reduced

Then \( D_1 + D_2 = (u, v) \) where \( u = u_1 u_2 \) and

\[ v = \begin{cases} 
  v_1 \pmod{u_1} \\
  v_2 \pmod{u_2} 
\end{cases} \]

In general: suppose \( P = (x_0, y_0) \) occurs in \( D_1 \) and \( \overline{P} \) occurs in \( D_2 \).
Then \( u_1(x_0) = u_2(x_0) = 0 \) and \( v_1(x_0) = y_0 = -v_2(x_0) - h(x_0) \), so \( x - x_0 \mid u_1(x), u_2(x), v_1(x) + v_2(x) + h(x) \)

\[
\begin{align*}
  d &= \gcd(u_1, u_2, v_1 + v_2 + h) = s_1 u_1 + s_2 u_2 + s_3 (v_1 + v_2 + h) \\
  u &= \frac{u_1 u_2}{d^2} \\
  v &\equiv \frac{1}{d} \left( s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + f) \right) \pmod{u}
\end{align*}
\]

(In the simplest case above, \( d = 1 \) and \( s_3 = 0 \))
Arithmetic in $\text{Jac}_H(\overline{K})$

**Input:** $D_1 = (u_1, v_1), D_2 = (u_2, v_2)$ reduced

**Output:** The reduced divisor $D' = (u', v')$ in the class of $D_1 + D_2$
Arithmetic in $\text{Jac}_H(\overline{K})$

**Input:** $D_1 = (u_1, v_1), \ D_2 = (u_2, v_2)$ reduced

**Output:** The reduced divisor $D' = (u', v')$ in the class of $D_1 + D_2$

1. **Addition:** compute a semi-reduced divisor $D = (u, v)$ in the class of $D_1 + D_2$
2. **Reduction:** compute the reduced divisor $D' = (u', v')$ in the class of $D$
Arithmetic in $\text{Jac}_H(\mathbb{K})$

**Input:** $D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$ reduced

**Output:** The reduced divisor $D' = (u', v')$ in the class of $D_1 + D_2$

1. **Addition:** compute a semi-reduced divisor $D = (u, v)$ in the class of $D_1 + D_2$
2. **Reduction:** compute the reduced divisor $D' = (u', v')$ in the class of $D$

**Methods**

- “Vanilla” method just discussed
- Cantor’s algorithm (“improved vanilla”)
- NUCOMP
- Explicit formulas (if $g$ is small, say $g = 2, 3, 4$)
Divisors defined over $K$

Let $\phi \in \text{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)
Divisors defined over $K$

Let $\phi \in \text{Gal}(\overline{K}/K)$  (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

$\phi$ acts on points on $H$: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$
Divisors defined over $K$

Let $\phi \in \text{Gal}(\bar{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

$\phi$ acts on points on $H$: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$

$\phi$ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$
Divisors defined over $K$

Let $\phi \in \text{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

$\phi$ acts on points on $H$: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$

$\phi$ acts on divisors: if $D = \sum m_P [P]$, then $\phi(D) = \sum m_P [\phi(P)]$

A divisor $D$ is defined over $K$ if $\phi(D) = D$
Divisors defined over $K$

Let $\phi \in \text{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

$\phi$ acts on points on $H$: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$

$\phi$ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$

A divisor $D$ is defined over $K$ if $\phi(D) = D$

Example:

$$D = (x^2 - x - 4, 2x + 1) \quad \text{on} \quad H : y^2 = x^5 - 5x^3 + 4x - 1 \quad \text{over} \quad \mathbb{Q}$$

$$= \left[ \left( \frac{1}{2} (1 + \sqrt{17}), 2 + \sqrt{17} \right) \right] + \left[ \left( \frac{1}{2} (1 - \sqrt{17}), 2 - \sqrt{17} \right) \right]$$

is defined over $\mathbb{Q}$ (invariant under automorphism $\sqrt{17} \mapsto -\sqrt{17}$)
Divisors defined over $K$

Let $\phi \in \text{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

$\phi$ acts on points on $H$: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$

$\phi$ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$

A divisor $D$ is **defined over $K$** if $\phi(D) = D$

**Example:**

$$D = (x^2 - x - 4, 2x + 1) \quad \text{on} \quad H : y^2 = x^5 - 5x^3 + 4x - 1 \quad \text{over} \quad \mathbb{Q}$$

$$= \left[ \left( \frac{1}{2}(1 + \sqrt{17}), 2 + \sqrt{17} \right) \right] + \left[ \left( \frac{1}{2}(1 - \sqrt{17}), 2 - \sqrt{17} \right) \right]$$

is defined over $\mathbb{Q}$ (invariant under automorphism $\sqrt{17} \leftrightarrow -\sqrt{17}$)

**Theorem**

$D = (u, v)$ is defined over $K$ if and only if $u(x), v(x) \in K[x]$. 
Divisors defined over $K$

Let $\phi \in \text{Gal}(\overline{K}/K)$ (for $K = \mathbb{F}_q$, think of Frobenius $\phi(\alpha) = \alpha^q$)

$\phi$ acts on points on $H$: if $P = (x_0, y_0)$, then $\phi(P) = (\phi(x_0), \phi(y_0))$

$\phi$ acts on divisors: if $D = \sum m_P[P]$, then $\phi(D) = \sum m_P[\phi(P)]$

A divisor $D$ is defined over $K$ if $\phi(D) = D$

Example:

$$D = (x^2 - x - 4, 2x + 1) \quad \text{on} \quad H : y^2 = x^5 - 5x^3 + 4x - 1 \quad \text{over} \quad \mathbb{Q}$$

$$= \left[ \left( \frac{1}{2} (1 + \sqrt{17}), 2 + \sqrt{17} \right) \right] + \left[ \left( \frac{1}{2} (1 - \sqrt{17}), 2 - \sqrt{17} \right) \right]$$

is defined over $\mathbb{Q}$ (invariant under automorphism $\sqrt{17} \leftrightarrow -\sqrt{17}$)

Theorem

$D = (u, v)$ is defined over $K$ if and only if $u(x), v(x) \in K[x]$.

Corollary

The group $\text{Jac}_H(\mathbb{F}_q)$ of divisor classes defined over $\mathbb{F}_q$ is finite.
Group Structure and Size

\[ E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q - 1) \]
Group Structure and Size

\[ E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q - 1) \]

Via a hand-wavy argument, \( y^2 = f(x) \) should have \( \approx q + 1 \) points
Group Structure and Size

\[ N = \mathbb{F}_q \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q - 1) \]

Via a hand-wavy argument, \( y^2 = f(x) \) should have \( \approx q + 1 \) points.

Hasse: \[ |E(\mathbb{F}_q)| = q + 1 - t \quad \text{with} \quad |t| \leq 2\sqrt{q} \]

Hasse-Weil: \[ |H(\mathbb{F}_q)| = q + 1 - t \quad \text{with} \quad |t| \leq 2g \sqrt{q} \]

Serre: \[ |t| \leq g \lfloor 2\sqrt{q} \rfloor \]
Group Structure and Size

\[ E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q-1) \]

Via a hand-wavy argument, \( y^2 = f(x) \) should have \( \approx q + 1 \) points

Hasse: \[ |E(\mathbb{F}_q)| = q + 1 - t \quad \text{with} \quad |t| \leq 2\sqrt{q} \]

Hasse-Weil: \[ |H(\mathbb{F}_q)| = q + 1 - t \quad \text{with} \quad |t| \leq 2g\sqrt{q} \]

Serre: \[ |t| \leq g\lfloor 2\sqrt{q} \rfloor \]

For the Jacobian:

\[(\sqrt{q} - 1)^{2g} \leq |\text{Jac}_H(\mathbb{F}_q)| \leq (\sqrt{q} + 1)^{2g}\]

So \[ |\text{Jac}_H(\mathbb{F}_q)| \approx q^g \]
Group Structure and Size

\[ E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{where} \quad n \mid \gcd(m, q-1) \]

Via a hand-wavy argument, \( y^2 = f(x) \) should have \( \approx q + 1 \) points

Hasse: \[ |E(\mathbb{F}_q)| = q + 1 - t \quad \text{with} \quad |t| \leq 2\sqrt{q} \]

Hasse-Weil: \[ |H(\mathbb{F}_q)| = q + 1 - t \quad \text{with} \quad |t| \leq 2g\sqrt{q} \]

Serre: \[ |t| \leq g\left[2\sqrt{q}\right] \]

For the Jacobian:

\[ (\sqrt{q} - 1)^{2g} \leq |\text{Jac}_H(\mathbb{F}_q)| \leq (\sqrt{q} + 1)^{2g} \]

So \[ |\text{Jac}_H(\mathbb{F}_q)| \approx q^g \]

If we want \( q^g \approx 2^{160} \):

\[
\begin{array}{c|c|c|c|c|c}
  g & 1 & 2 & 3 & 4 \\
  \hline
  q & 2^{160} & 2^{80} & 2^{53.33} & 2^{40}
\end{array}
\]
Point Counting Algorithms

Stay for next week’s workshop to learn more . . .
Point Counting Algorithms

Stay for next week’s workshop to learn more . . .

\[ K = \mathbb{F}_q, \ q = p^n \]

- **Square Root Methods**
  - Pollard kangaroo
  - Cartier-Manin

- \( \ell \)-adic Methods \((n = 1, \text{polynomial in } \log(p))\)
  - SEA and generalizations

- \( p \)-adic Methods \((p \text{ small, polynomial in } n)\)
  - Canonical lifts (Satoh, AGM)
  - Deformation theory
  - Cohomology
Point Counting Algorithms

Stay for next week’s workshop to learn more . . .

\[ K = \mathbb{F}_q, \ q = p^n \]

- **Square Root Methods**
  - Pollard kangaroo
  - Cartier-Manin
- **ℓ-adic Methods** \((n = 1, \text{ polynomial in } \log(p))\)
  - SEA and generalizations
- **p-adic Methods** \((p \text{ small, polynomial in } n)\)
  - Canonical lifts (Satoh, AGM)
  - Deformation theory
  - Cohomology

Point counting on certain curves is easy (e.g. Koblitz curves)
Point Counting Algorithms

Stay for next week’s workshop to learn more . . .

\[ K = \mathbb{F}_q, \quad q = p^n \]

- **Square Root Methods**
  - Pollard kangaroo
  - Cartier-Manin

- **\( \ell \)-adic Methods** \((n = 1, \text{polynomial in } \log(p))\)
  - SEA and generalizations

- **\( p \)-adic Methods** \((p \text{ small, polynomial in } n)\)
  - Canonical lifts (Satoh, AGM)
  - Deformation theory
  - Cohomology

Point counting on certain curves is easy (e.g. Koblitz curves)

Can also **construct** curves with good group orders via CM method (see Thursday’s talks by Drew Sutherland and Bianca Viray)
Discrete Logarithms

**Elliptic Curve DLP:** given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find $m$
Discrete Logarithms

**Elliptic Curve DLP:** given \( P, Q \in E(\mathbb{F}_q) \) with \( Q = mP \), find \( m \)

**Hyperelliptic Curve DLP:** given reduced divisors \( D, E \) so that \( E \) is equivalent to \( mD \), find \( m \)
Discrete Logarithms

**Elliptic Curve DLP:** given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find $m$

**Hyperelliptic Curve DLP:** given reduced divisors $D, E$ so that $E$ is equivalent to $mD$, find $m$

**Generic Methods** — Complexity $O(q^{g/2})$ group operations
- Baby step giant step — also requires $O(q^{g/2})$ space
- Pollard rho
- Pollard lambda (kangaroo)
Discrete Logarithms

**Elliptic Curve DLP:** given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find $m$

**Hyperelliptic Curve DLP:** given reduced divisors $D, E$ so that $E$ is equivalent to $mD$, find $m$

**Generic Methods** — Complexity $O(q^{g/2})$ group operations
  - Baby step giant step — also requires $O(q^{g/2})$ space
  - Pollard rho
  - Pollard lambda (kangaroo)

**Index Calculus Methods**
  - $g \gtrapprox \log(q)$ — sub-exponential
  - $3 \leq g \lesssim \log(q)$ — $O(q^{2-2/g})$
Discrete Logarithms

**Elliptic Curve DLP:** given $P, Q \in E(\mathbb{F}_q)$ with $Q = mP$, find $m$

**Hyperelliptic Curve DLP:** given reduced divisors $D, E$ so that $E$ is equivalent to $mD$, find $m$

**Generic Methods** — Complexity $O(q^{g/2})$ group operations
  - Baby step giant step — also requires $O(q^{g/2})$ space
  - Pollard rho
  - Pollard lambda (kangaroo)

**Index Calculus Methods**
  - $g \gtrsim \log(q)$ — sub-exponential
  - $3 \leq g \lesssim \log(q)$ — $O(q^{2-2/g})$

For $g = 1, 2$, generic methods are best! (As far as we know . . . )
Other Attacks & Parameter Choices

\[ K = \mathbb{F}_q \text{ with } q = p^n \]

- **Pohlig-Hellman** — ensure that \( |\text{Jac}_H(\mathbb{F}_q)| \) has a large prime factor
Other Attacks & Parameter Choices

\[ K = \mathbb{F}_q \text{ with } q = p^n \]

- **Pohlig-Hellman** — ensure that \(|\text{Jac}_H(\mathbb{F}_q)|\) has a large prime factor

- **Additive Reduction**: if \(p\) divides \(|\text{Jac}_H(\mathbb{F}_q)|\), then there is an explicit homomorphism \(\text{Jac}_H(\mathbb{F}_q)[p] \rightarrow (\mathbb{F}_q^{2g-1}, +)\) — ensure that \(\gcd(q, |\text{Jac}_H(\mathbb{F}_q)|) = 1\)
Other Attacks & Parameter Choices

\[ K = \mathbb{F}_q \text{ with } q = p^n \]

- **Pohlig-Hellman** — ensure that \(|\text{Jac}_H(\mathbb{F}_q)|\) has a large prime factor

- **Additive Reduction**: if \( p \) divides \(|\text{Jac}_H(\mathbb{F}_q)|\), then there is an explicit homomorphism \( \text{Jac}_H(\mathbb{F}_q)[p] \to (\mathbb{F}_q^{2g-1}, +) \) — ensure that \( \gcd(q, |\text{Jac}_H(\mathbb{F}_q)|) = 1 \)

- **Multiplicative Reduction** (MOV): pairings can be used to map the DLP in \( \text{Jac}_H(\mathbb{F}_q) \) into \( (\mathbb{F}_{q^k}^*, \times) \) where \( q^k \equiv 1 \pmod{r} \) for a prime \( r \) dividing \( |\text{Jac}_H(\mathbb{F}_q)| \) — ensure that \( k \) is large (For pairing-based crypto, however, we want \( k \) small — see Tuesday’s and Wednesday’s talks)
Other Attacks & Parameter Choices

\[ K = \mathbb{F}_q \text{ with } q = p^n \]

- **Pohlig-Hellman** — ensure that \(|\text{Jac}_H(\mathbb{F}_q)|\) has a large prime factor

- **Additive Reduction**: if \( p \) divides \(|\text{Jac}_H(\mathbb{F}_q)|\), then there is an explicit homomorphism \( \text{Jac}_H(\mathbb{F}_q)[p] \rightarrow (\mathbb{F}_q^{2g-1}, +) \) — ensure that \( \gcd(q, |\text{Jac}_H(\mathbb{F}_q)|) = 1 \)

- **Multiplicative Reduction** (MOV): pairings can be used to map the DLP in \( \text{Jac}_H(\mathbb{F}_q) \) into \((\mathbb{F}_{q^k}^*, \times)\) where \( q^k \equiv 1 \pmod{r} \) for a prime \( r \) dividing \(|\text{Jac}_H(\mathbb{F}_q)|\) — ensure that \( k \) is large (For pairing-based crypto, however, we want \( k \) small — see Tuesday’s and Wednesday’s talks)

- **Weil Descent**: If \( n = kd \) is composite, one may have \( \text{Jac}_H(\mathbb{F}_{p^{kd}}) \leftrightarrow \text{Jac}_C(\mathbb{F}_{p^d}) \) where \( C \) has higher genus — use \( n = 1 \) or \( n \) prime
Some Other Models

- **Hessians**: $x^3 + y^3 - 3dxy = 1$

- **Edwards models**: $x^2 + y^2 = c^2(1 + dx^2y^2)$ ($q$ odd) and variations

\[ x^3 + y^3 = 1 \]

\[ x^2 + y^2 = 10(1 - x^2y^2) \]
Even Degree Models

\[ H : y^2 + h(x)y = f(x) \]

- \( h(x), f(x) \in K[x] \)
- \( \deg(h) = g + 1 \) if \( \text{char}(K) = 2 \); \( h(x) = 0 \) if \( \text{char}(K) \neq 2 \)
- \( \deg(f) = 2g + 2 \) is even
- \( \text{sgn}(f) = s^2 + s \) with \( s \in K \) if \( \text{char}(K) = 2 \); \( f(x) \) is monic if \( \text{char}(K) \neq 2 \)
- non-singularity
Even Degree Models

\[ H : y^2 + h(x)y = f(x) \]

- \( h(x), f(x) \in K[x] \)
- \( \deg(h) = g + 1 \) if \( \text{char}(K) = 2 \); \( h(x) = 0 \) if \( \text{char}(K) \neq 2 \)
- \( \deg(f) = 2g + 2 \) is even
- \( \text{sgn}(f) = s^2 + s \) with \( s \in K \) if \( \text{char}(K) = 2 \); \( f(x) \) is monic if \( \text{char}(K) \neq 2 \)
- non-singularity

\[ \text{char}(K) \neq 2: \quad y^2 = f(x), \quad f(x) \text{ monic, of even degree, square-free} \]
Even Degree Models

\[ H : \ y^2 + h(x)y = f(x) \]

- \( h(x), f(x) \in K[x] \)
- \( \deg(h) = g + 1 \) if \( \text{char}(K) = 2 \); \( h(x) = 0 \) if \( \text{char}(K) \neq 2 \)
- \( \deg(f) = 2g + 2 \) is even
- \( \text{sgn}(f) = s^2 + s \) with \( s \in K \) if \( \text{char}(K) = 2 \); \( f(x) \) is monic if \( \text{char}(K) \neq 2 \)
- non-singularity

\( \text{char}(K) \neq 2 \): \( y^2 = f(x), \) \( f(x) \) monic, of even degree, square-free

Elliptic quartic, \( \text{char}(K) \neq 2, 3 \):

\[ y^2 = x^4 + ax^2 + bx + c \quad (a, b, c \in K) \]

(\( b = 0 \): Jacobi Quartic)
Examples

\[ E : y^2 = x^4 - 6x^2 + x + 6 \]
\[ g = 1 \]

\[ H : y^2 = x^6 - 13x^4 + 44x^2 - 4x - 1 \]
\[ g = 2 \]
Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography.
Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography

- Use $q$ prime or $q = 2^n$
Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography.

- Use $q$ prime or $q = 2^n$.

- Good parameter choices are known and easy.
Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography

- Use $q$ prime or $q = 2^n$

- Good parameter choices are known and easy

- Cryptographically suitable curves can be constructed in practice
Conclusion

- Genus 1 and genus 2 curves over $\mathbb{F}_q$ represent a very good setting for DLP based cryptography

- Use $q$ prime or $q = 2^n$

- Good parameter choices are known and easy

- Cryptographically suitable curves can be constructed in practice

* * * Thank You! * * *