Hyper-and-elliptic-curve cryptography
(which is not the same as:
hyperelliptic-curve cryptography
and elliptic-curve cryptography)

Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Tanja Lange
Technische Universiteit Eindhoven

“Through our inefficient use of energy (gas guzzling vehicles,
badly insulated buildings,
poorly optimized crypto, etc)
we needlessly throw away almost
a third of the energy we use.”
—Greenpeace UK
Hyper-and-elliptic-curve cryptography
(which is not the same as:
hyperelliptic-curve cryptography
and elliptic-curve cryptography)

Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Tanja Lange
Technische Universiteit Eindhoven

“Through our inefficient use of energy (gas guzzling vehicles,
badly insulated buildings,
poorly optimized crypto, etc)
we needlessly throw away almost a third of the energy we use.”
—Greenpeace UK (mostly)
Hyper-and-elliptic-curve cryptography

is not the same as:
hyperelliptic-curve cryptography
and elliptic-curve cryptography

Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Tanja Lange
Technische Universiteit Eindhoven

“Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, poorly optimized crypto, etc) we needlessly throw away almost a third of the energy we use.”
—Greenpeace UK (mostly)

DH speed records

Sandy Bridge cycles for high-security constant-time $a; P 7! aP$ ("?" if not SUPERCOP-verified):

2012 Hamburg: 153000?
2012 Longa–Sica: 137000?
2013 Bos–Costello–Hisil–Lauter: 122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez: 114800?
2013 Faz-Hernández–Longa–Sánchez: 96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe: 91320
Hyper-and-elliptic-curve cryptography
(which is not the same as:
hyperelliptic-curve cryptography
and elliptic-curve cryptography)

Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Tanja Lange
Technische Universiteit Eindhoven

“Through our inefficient use of energy (gas guzzling vehicles,
badly insulated buildings,
**poorly optimized crypto**, etc)
we needlessly throw away almost
a third of the energy we use.”
—Greenpeace UK (mostly)

DH speed records
Sandy Bridge cycles for high-security constant-time
(“?” if not SUPERCOP-verified):
2012 Hamburg: 153000?
2012 Longa–Sica: 137000?
2013 Bos–Costello–Hisil–Lauter: 122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez: 114800?
2013 Faz-Hernández–Longa–Sánchez: 96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe:
“Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, poorly optimized crypto, etc) we needlessly throw away almost a third of the energy we use.”
—Greenpeace UK (mostly)
“Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, **poorly optimized crypto**, etc) we needlessly throw away almost a third of the energy we use.”
—Greenpeace UK (mostly)

<table>
<thead>
<tr>
<th>Year</th>
<th>Authors</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Hamburg</td>
<td>153000</td>
</tr>
<tr>
<td>2012</td>
<td>Longa–Sica</td>
<td>137000</td>
</tr>
<tr>
<td>2013</td>
<td>Bos–Costello–Hisil–Lauter</td>
<td>122716</td>
</tr>
<tr>
<td>2013</td>
<td>Oliveira–López–Aranha–Rodríguez-Henríquez</td>
<td>114800</td>
</tr>
<tr>
<td>2013</td>
<td>Faz-Hernández–Longa–Sánchez</td>
<td>96000</td>
</tr>
<tr>
<td>2014</td>
<td>Bernstein–Chuengsatiansup–Lange–Schwabe</td>
<td>91320</td>
</tr>
</tbody>
</table>
Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, poorly optimized crypto, etc) we needlessly throw away almost a third of the energy we use. —Greenpeace UK (mostly)

<table>
<thead>
<tr>
<th>Year</th>
<th>Participants</th>
<th>Time (cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Hamburg</td>
<td>153000?</td>
</tr>
<tr>
<td>2012</td>
<td>Longa–Sica</td>
<td>137000?</td>
</tr>
<tr>
<td>2013</td>
<td>Bos–Costello–Hisil–Lauter</td>
<td>122716</td>
</tr>
<tr>
<td>2013</td>
<td>Oliveira–López–Aranha–Rodríguez-Henríquez</td>
<td>114800?</td>
</tr>
<tr>
<td>2013</td>
<td>Faz–Hernández–Longa–Sánchez</td>
<td>96000?</td>
</tr>
<tr>
<td>2014</td>
<td>Bernstein–Chuengsatiansup–Lange–Schwabe</td>
<td>91320</td>
</tr>
</tbody>
</table>

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult.
14M for $X: \mathbb{P}(\mathbb{P})^7$ etc.
2006 Gaudry: even faster.
25M for $X: \mathbb{P}(\mathbb{Q})^7 \mathbb{P}(\mathbb{P})^7$ and $X: \mathbb{P}(\mathbb{Q}+\mathbb{P})$, including 6M by surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $\mathbb{F}_{2^{127^1}}$. 


Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, poorly optimized crypto, etc) we needlessly throw away almost a third of the energy we use."

—Greenpeace UK (mostly)

<table>
<thead>
<tr>
<th>Year</th>
<th>Name of Authors</th>
<th>DH Speed (CPU cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Hamburg</td>
<td>153000?</td>
</tr>
<tr>
<td>2012</td>
<td>Longa–Sica</td>
<td>137000?</td>
</tr>
<tr>
<td>2013</td>
<td>Bos–Costello–Hisil–Lauter</td>
<td>122716</td>
</tr>
<tr>
<td>2013</td>
<td>Oliveira–López–Aranha–Rodríguez-Henríquez</td>
<td>114800?</td>
</tr>
<tr>
<td>2013</td>
<td>Faz-Hernández–Longa–Sánchez</td>
<td>96000?</td>
</tr>
<tr>
<td>2014</td>
<td>Bernstein–Chuengsatiansup–Lange–Schwabe</td>
<td>91320</td>
</tr>
</tbody>
</table>

Critical for 122716:
1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar multiplication.
14M for $X(P) \rightarrow X(2P), X(Q + P)$.

14M for $X(P) \rightarrow X(2P), X(Q + P)$.

14M for $X(P) \rightarrow X(2P), X(Q + P)$.

14M for $X(P) \rightarrow X(2P), X(Q + P)$.

14M for $X(P) \rightarrow X(2P), X(Q + P)$.

14M for $X(P) \rightarrow X(2P), X(Q + P)$.
Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, poorly optimized crypto, etc) we needlessly throw away almost a third of the energy we use. —Greenpeace UK (mostly)

DH speed records

Sandy Bridge cycles for high-security constant-time $a, P \rightarrow aP$ (“?” if not SUPERCOP-verified):

- 2012 Hamburg: 153000?
- 2012 Longa–Sica: 137000?
- 2013 Bos–Costello–Hisil–Lauter: 122716
- 2013 Faz-Hern´andez–Longa–S´anchez: 96000?
- 2014 Bernstein–Chuengsatiansup–Lange–Schwabe: 91320

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult.
14M for $X(P) \rightarrow X(2P)$.

2006 Gaudry: even faster.
25M for $X(P), X(Q), X(Q + P) \rightarrow X(2P), X(Q + P)$, including 6M by surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $\mathbb{F}_{2^{127}-1}$. 
DH speed records

Sandy Bridge cycles for high-security constant-time $a, P \mapsto aP$ ("?" if not SUPERCOP-verified):

2012 Hamburg:      153000?
2012 Longa–Sica:    137000?
2013 Bos–Costello–Hisil–Lauter:  122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez:  114800?
2013 Faz-Hernández–Longa–Sánchez:       96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe:  91320

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult.

14M for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster.

25M for $X(P), X(Q), X(Q - P) \mapsto X(2P), X(Q + P)$, including 6M by surface coefficients.

2012 Gaudry–Schost:

1000000-CPU-hour computation found secure small-coefficient surface over $F_{2^{127-1}}$. 
Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult.

14M for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster.

25M for $X(P), X(Q), X(Q - P) \mapsto X(2P), X(Q + P)$, including 6M by surface coefficients.

2012 Gaudry–Schost:

1000000-CPU-hour computation found secure small-coefficient surface over $\mathbb{F}_{2^{127}-1}$. 

<table>
<thead>
<tr>
<th>Year</th>
<th>Authors</th>
<th>Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Hamburg</td>
<td>153000?</td>
</tr>
<tr>
<td>2012</td>
<td>Longa–Sica</td>
<td>137000?</td>
</tr>
<tr>
<td>2013</td>
<td>Bos–Costello–Hisil–Lauter–Yang</td>
<td>122716</td>
</tr>
<tr>
<td>2013</td>
<td>Oliveira–López–Aranha–Rodríguez–Henríquez</td>
<td>114800?</td>
</tr>
<tr>
<td>2013</td>
<td>Faz–Hernández–Longa–Sánchez–Yang</td>
<td>96000?</td>
</tr>
<tr>
<td>2014</td>
<td>Bernstein–Chuengsatiansup–Lange–Schwabe</td>
<td>91320</td>
</tr>
</tbody>
</table>
DH speed records
Sandy Bridge cycles for high-security constant-time a; P 7! aP
("?" if not SUPERCOP-verified):
2012 Hamburg: 153000?
2012 Longa–Sica: 137000?
2013 Bos–Costello–Hisil–Lauter: 122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez: 114800?
2013 Faz-Hernández–Longa–Sánchez: 96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe: 91320

Critical for 122716, 91320:
1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult.
14 M for \( X(P) \ Leadsto X(2P) \).
2006 Gaudry: even faster.
25 M for \( X(P), X(Q), X(Q - P) \ Leadsto X(2P), X(Q + P) \), including 6 M by surface coefficients.
2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over \( \mathbb{F}_{2^{127} - 1} \).
Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult.
14$M$ for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster.
25$M$ for $X(P), X(Q), X(Q - P) \mapsto X(2P), X(Q + P)$, including 6$M$ by surface coefficients.

2012 Gaudry–Schost:
1000000-CPU-hour computation found secure small-coefficient surface over $\mathbf{F}_{2^{127} - 1}$.
Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult.

14M for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster.

25M for $X(P), X(Q), X(Q - P)$ $\mapsto X(2P), X(Q + P)$, including 6M by surface coefficients.

2012 Gaudry–Schost:

1000000-CPU-hour computation found secure small-coefficient surface over $F_{2^{127} - 1}$.
Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult.

$14 \, M \text{ for } X(P), X(Q), X(Q - P)$, including surface coefficients.

2006 Gaudry: even faster.

$25 \, M \text{ for } X(P), X(Q), X(Q - P); X(Q + P)$, including surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $F_{2^{127}}$.
1986 Chudnovsky–Chudnovsky:
traditional Kummer surface
allows fast scalar mult.
14 $M$ for $X(P)$.

2006 Gaudry:
even faster.
25 $M$ for $X(P)$; $X(Q)$, $X(Q - P)$, including small-coefficient surfaces.

2012 Gaudry–Schost:
1000000-CPU-hour computation
found secure small-coefficient surfaces over $F_{2^{127}}$.

Strategies to build $dim-2 J = F_p$ with known $\# J(F_p)$, large $p$:

- CM Pila new
- fast build yes no yes
- any curve no yes yes
- many curves no yes yes
- secure curves yes yes yes
- twist-secure yes yes yes
- Kummer yes yes yes
- small coeff no yes yes
- fastest DH no yes yes
- fastest keygen no no yes
- complete add no no yes
Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky:
traditional Kummer surface
allows fast scalar mult.

14 $M$ for $X(P)$.

2006 Gaudry: even faster.
25 $M$ for $X(P)$; $X(Q)$; $X(Q+P)$.

7 $M$ by surface coefficients.

2012 Gaudry–Schost:
1000000-CPU-hour computation
found secure small-coefficient
surface over $F_{2^{127}}$.

### Strategies to build dim-2 $J = F_p$ with known $\#J(F_p)$, large $p$:

<table>
<thead>
<tr>
<th>CM</th>
<th>Pila</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast build</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>any curve</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>many curves</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>secure curves</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>twist-secure</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kummer</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>small coeff</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest DH</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest keygen</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>
Strategies to build dim-2 $J/F_p$ with known $\#J(F_p)$, large $p$:

<table>
<thead>
<tr>
<th></th>
<th>CM</th>
<th>Pila</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast build</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>any curve</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>many curves</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>secure curves</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>twist-secure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kummer</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>small coeff</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>fastest DH</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>fastest keygen</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
Strategies to build dim-2 $J/\mathbb{F}_p$ with known $\#J(\mathbb{F}_p)$, large $p$:

<table>
<thead>
<tr>
<th></th>
<th>CM</th>
<th>Pila</th>
<th>Stn</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast build</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>any curve</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>many curves</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>secure curves</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>twist-secure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kummer</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>small coeff</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest DH</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest keygen</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
Strategies to build dim-2 $J/F_p$ with known $\#J(F_p)$, large $p$:

<table>
<thead>
<tr>
<th></th>
<th>CM</th>
<th>Pila</th>
<th>Stn</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast build</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>any curve</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>many curves</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>secure curves</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>twist-secure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kummer</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>small coeff</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest DH</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest keygen</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

Hyper-and-elliptic-curve crypto

Typical example: Define $H : y^2 = (z_1)(z + 1)(z + 2)$

$(z_1 = 2)(z + 3 = 2)(z_2 = 3)$ over $F_p$ with $p = 2^{127} - 309$;

$J = \text{Jac } H$; traditional Kummer surface $K$; traditional $X$; $J \rightarrow K$.

Small $K$ coeffs (20 : 1 : 20 : 40).
Strategies to build dim-2 \( J/\mathbb{F}_p \) with known \( \#J(\mathbb{F}_p) \), large \( p \):

<table>
<thead>
<tr>
<th></th>
<th>CM</th>
<th>Pila</th>
<th>Stn</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast build</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>any curve</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>many curves</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>secure curves</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>twist-secure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kummer</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>small coeff</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest DH</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest keygen</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

Hyper-and-elliptic-curve crypto

Typical example: Define \( H : y^2 = (z - 1)(z + 1)(z + 2)(z - 1/2)(z + 3/2)(z - 2) \) over \( \mathbb{F}_p \) with \( p = 2^{127} - 309 \);
\( J = \text{Jac} H \); traditional Kummer surface \( K \); traditional \( X : J \to K \).
Small \( K \) coeffs (20 : 1 : 20 : 40).
Strategies to build dim-2 $J/F_p$ with known $\#J(F_p)$, large $p$:

<table>
<thead>
<tr>
<th>Fast build</th>
<th>CM</th>
<th>Pila</th>
<th>Stn</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>any curve</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>many curves</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>secure curves</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>twist-secure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kummer</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>small coeff</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest DH</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest keygen</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

Hyper-and-elliptic-curve crypto

Typical example: Define $H : y^2 = (z - 1)(z + 1)(z + 2)(z - 1/2)(z + 3/2)(z - 127309)$ over $F_p$ with $p = 2^{127} - 309$.

$J = \text{Jac } H$; traditional Kummer surface $K$; traditional $X : J \neq K$.

Small $K$ coeffs (20 : 1 : 20 : 40).
Strategies to build dim-2 $J/F_p$
with known $\#J(F_p)$, large $p$:

<table>
<thead>
<tr>
<th></th>
<th>CM</th>
<th>Pila</th>
<th>Stn</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast build</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>any curve</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>many curves</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>secure curves</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>twist-secure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kummer</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>small coeff</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest DH</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest keygen</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

Hyper-and-elliptic-curve crypto

Typical example: Define $H : y^2 = (z - 1)(z + 1)(z + 2)$
$(z - 1/2)(z + 3/2)(z - 2/3)$
over $F_p$ with $p = 2^{127} - 309$;
$J = \text{Jac } H$; traditional Kummer surface $K$; traditional $X : J \to K$.
Small $K$ coeffs (20 : 1 : 20 : 40).
### Strategies to build dim-2 $J/\mathbb{F}_p$ with known $\#J(\mathbb{F}_p)$, large $p$:

<table>
<thead>
<tr>
<th>Feature</th>
<th>CM</th>
<th>Pila</th>
<th>Stn</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast build</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>any curve</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>many curves</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>secure curves</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>twist-secure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kummer</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>small coeff</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest DH</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>fastest keygen</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

### Hyper-and-elliptic-curve crypto

Typical example: Define

$$H : y^2 = (z - 1)(z + 1)(z + 2)(z - 1/2)(z + 3/2)(z - 2/3)$$

over $\mathbb{F}_p$ with $p = 2^{127} - 309$; $J = \text{Jac } H$; traditional Kummer surface $K$; traditional $X : J \rightarrow K$. Small $K$ coeffs ($20 : 1 : 20 : 40$).

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Costset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.
Strategies to build dim-2 $J/F_p$ with known $\#J(F_p)$, large $p$:

<table>
<thead>
<tr>
<th></th>
<th>CM</th>
<th>Pila</th>
<th>Stn</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>new</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>curves</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>secure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kcoeff</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>fastest</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>DH</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>keygen</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>complete add</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

Hyper-and-elliptic-curve crypto

Typical example: Define $H : y^2 = (z - 1)(z + 1)(z + 2) (z - 1/2)(z + 3/2)(z - 2/3)$ over $F_p$ with $p = 2^{127} - 309$; $J = \text{Jac } H$; traditional Kummer surface $K$; traditional $X : J \to K$. Small $K$ coeffs (20 : 1 : 20 : 40).

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

Security $2^{125}$ against rho.

Order of $\ell$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is $12152941675747802266549093$ $122563150387$.

Twist security $2^{75}$.

(Want more twist security? Switch to $p = 2^{127} - 94825$; cofactors 16 $3269239$, 4.)
Strategies to build dim-2 $J = \mathbb{F}_p$ with known $\# J (\mathbb{F}_p)$, large $p$:

<table>
<thead>
<tr>
<th>M</th>
<th>Pila</th>
<th>Stn</th>
<th>new</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>s</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>s</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>s</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>no</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

Hyper-and-elliptic-curve crypto

Typical example: Define

$H : y^2 = (z - 1)(z + 1)(z + 2)$

$(z - 1/2)(z + 3/2)(z - 2/3)$

over $\mathbb{F}_p$ with $p = 2^{127} - 309$;

$J = \text{Jac} \; H$; traditional Kummer surface $K$; traditional $X : J \to K$.

Small $K$ coeffs (20 : 1 : 20 : 40).

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

Security $\approx 2^{125}$ against rho.

Order of $\ell$ in $(\mathbb{Z}/p\mathbb{Z})^*$

$12152941675747802266549093$ $122563150387$.

Twist security $\approx 2^{75}$.

(Want more twist security? Switch to $p = 2^{127} - 94825$; cofactors 16 : 3269239, 4.)
Hyper-and-elliptic-curve crypto

Typical example: Define

\[ H : y^2 = (z - 1)(z + 1)(z + 2) \]
\[ \quad (z - 1/2)(z + 3/2)(z - 2/3) \]

over \( \mathbb{F}_p \) with \( p = 2^{127} - 309 \);

\( J = \text{Jac } H \); traditional Kummer surface \( K \); traditional \( X : J \rightarrow K \).

Small \( K \) coeffs \( (20 : 1 : 20 : 40) \).

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

\( \#J(\mathbb{F}_p) = 16 \ell \)

where \( \ell \) is the prime

\[ 18092513943330655349329 \]
\[ 407607485536491946060108 \]
\[ 289531455285792829679923 \].

Security \( \approx 2^{125} \) against rho.

Order of \( \ell \) in \( (\mathbb{Z}/p)^* \) is

\[ 121529416757478022665490 \]
\[ 122563150387 \].

Twist security \( \approx 2^{75} \).

(Want more twist security? Switch to \( p = 2^{127} - 94825 \) \( 94825 \);
cofactors \( 16 \cdot 3269239, 4 \)).
Hyper-and-elliptic-curve crypto

Typical example: Define

\[ H : y^2 = (z - 1)(z + 1)(z + 2) \]
\[ (z - 1/2)(z + 3/2)(z - 2/3) \]
over \( \mathbb{F}_p \) with \( p = 2^{127} - 309; \)
\( J = \text{Jac } H; \) traditional Kummer surface \( K; \) traditional \( X : J \to K. \)
Small \( K \) coeffs \((20 : 1 : 20 : 40). \)

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

\[ \#J(\mathbb{F}_p) = 16\ell \]
where \( \ell \) is the prime
18092513943330655534932966
40760748553649194606010814
289531455285792829679923.

Security \( \approx 2^{125} \) against rho.

Order of \( \ell \) in \((\mathbb{Z}/p)^*\) is
12152941675747802266549093
122563150387.

Twist security \( \approx 2^{75}. \)

(Want more twist security? Switch to \( p = 2^{127} - 94825; \)
cofactors 16 \cdot 3269239, 4.)
Hyper-and-elliptic-curve crypto

Typical example: Define

\[ H: y^2 = (z - 1)(z + 1)(z + 2)(z - 1/2)(z + 3/2)(z - 2/3) \]

with \( p = 2^{127} - 309; \)

\( H; \) traditional Kummer

\( K; \) traditional \( X: J \to K. \)

coeffs (20 : 1 : 20 : 40).

Note: There are typos in the

in/Mumford/Kummer

as in 2007 Gaudry, 2010

2013 Bos–Costello–

Hisil–Lauter. We have simpler,

computer-verified formulas.

\[ \#J(\mathbb{F}_p) = 16l \]

where \( l \) is the prime

18092513943330655534932966
40760748553649194606010814
289531455285792829679923.

Security \( \approx 2^{125} \) against rho.

Order of \( l \) in \( (\mathbb{Z}/p)^* \) is

12152941675747802266549093
122563150387.

Twist security \( \approx 2^{75} \).

(Want more twist security?
Switch to \( p = 2^{127} - 94825; \)
ocfactors 16 \cdot 3269239, 4.)

Fast point-counting

Define \( \mathbb{F}_{p^2} = \mathbb{F}_p[i] = (i^2 + 1); \)

\( r = (7 + 4i)^2 = 33 + 56i; \)

\( s = 159 + 56i; ! = p^{384}; \)

\( C: y^2 = rx^6 + sx^4 + sx^2 + r. \)
Hyper-and-elliptic-curve crypto

Typical example: Define

\[ H : y^2 = (z - 1)(z + 1)(z + 2)(z - 1 = 2)(z + 3 = 2)(z^2 = 3) \]

over \( F_{p^2} \) with \( p = 2^{127} - 309 \);

\( J = \text{Jac}_H \); traditional Kummer surface \( K \); traditional \( X : J \to K \).

Small \( K \) coeffs \((20 : 1 : 20 : 40)\).

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

\[ \#J(F_p) = 16l \]

where \( l \) is the prime

\[ 18092513943330655534932966 \]
\[ 40760748553649194606010814 \]
\[ 289531455285792829679923. \]

Security \( \approx 2^{125} \) against rho.

Order of \( l \) in \((\mathbf{Z}/p)^*\) is

\[ 12152941675747802266549093 \]
\[ 122563150387. \]

Twist security \( \approx 2^{75} \).

(Want more twist security? Switch to \( p = 2^{127} - 94825; \) cofactors \( 16 \cdot 3269239, 4 \).)
Hyper-and-elliptic-curve crypto

Typical example: Define

\[ H : y^2 = (z^1)(z + 1)(z + 2)(z^1 = 2)(z + 3 = 2)(z^2 = 3) \]

over \( F_p \) with \( p = 2^{127} - 2 \).

\( J = \text{Jac}_H; \) traditional Kummer surface \( K; \) traditional \( X \):
\( J \hookrightarrow K. \)

Small \( K \) coeffs (20 : 1 : 20 : 40).

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

# \( J(F_p) = 16 \)
where \( l \) is the prime

\[ 18092513943330655534932966 \]
\[ 40760748553649194606010814 \]
\[ 289531455285792829679923. \]

Security \( \approx 2^{125} \) against rho.

Order of \( l \) in \( (\mathbb{Z}/p)^* \) is

\[ 12152941675747802266549093 \]
\[ 122563150387. \]

Twist security \( \approx 2^{75} \).

(Want more twist security?
Switch to \( p = 2^{127} - 94825; \) cofactors \( 16 \cdot 3269239, 4. \))

Fast point-counting

Define \( F_{p^2} = F_p[i]/(i^2 + 1) \)
\[ r = (7 + 4i)^2 = 33 + 56i; \]
\[ s = 159 + 56i; \omega = \sqrt{-384}; \]
\( C : y^2 = rx^6 + sx^4 + sx^2 + \).
\# J(F_p) = 16 \ell

where \ell is the prime
1809251394333055534932966
40760748553649194606010814
289531455285792829679923.

Security \approx 2^{125} against rho.

Order of \ell in (\mathbb{Z}/p)^* is
12152941675747802266549093
122563150387.

Twist security \approx 2^{75}.

(Want more twist security? Switch to \( p = 2^{127} - 94825; \)
cofactors 16 \cdot 3269239, 4.)

Fast point-counting

Define \( F_{p^2} = F_p[i]/(i^2 + 1); \)
\( r = (7 + 4i)^2 = 33 + 56i; \)
\( s = 159 + 56i; \omega = \sqrt{-384}; \)
\( C : y^2 = rx^6 + sx^4 + sx^2 + r. \)
\#J(F_p) = 16 \ell
where \ell is the prime
18092513943330655534932966
40760748553649194606010814
289531455285792829679923.

Security \approx 2^{125} against rho.

Order of \ell in \((\mathbb{Z}/p)^*\) is
12152941675747802266549093
122563150387.

Twist security \approx 2^{75}.

(Want more twist security?
Switch to \(p = 2^{127} - 94825;\)
cofactors 16 \cdot 3269239, 4.)

Fast point-counting
Define \(F_{p^2} = F_p[i]/(i^2 + 1);\)
\(r = (7 + 4i)^2 = 33 + 56i;\)
\(s = 159 + 56i; \omega = \sqrt{-384};\)
\(C : y^2 = rx^6 + sx^4 + sx^2 + r.\)

\((x, y) \mapsto (x^2, y)\) takes \(C\) to \(E:\)
\(y^2 = rx^3 + sx^2 + sx + \overline{r}.\)
# \(J(\mathbf{F}_p) = 16\ell\)

where \(\ell\) is the prime

\[
18092513943330655534932966 \\
40760748553649194606010814 \\
289531455285792829679923.
\]

Security \(\approx 2^{125}\) against rho.

Order of \(\ell\) in \((\mathbf{Z}/p)^*\) is

\[
12152941675747802266549093 \\
122563150387.
\]

Twist security \(\approx 2^{75}\).

(Want more twist security?
Switch to \(p = 2^{127} - 94825\);
cofactors 16 · 3269239, 4.)

Fast point-counting

Define \(\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2 + 1)\);

\[
r = (7 + 4i)^2 = 33 + 56i; \\
s = 159 + 56i; \omega = \sqrt{-384}; \\
C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r}.
\]

\((x, y) \mapsto (x^2, y)\) takes \(C\) to \(E : y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}\).

\((x, y) \mapsto (1/x^2, y/x^3)\) takes \(C\) to \(y^2 = \bar{r}x^3 + \bar{s}x^2 + sx + r\).
\#J(F_p) = 16\ell

where \ell is the prime
18092513943330655534932966
40760748553649194606010814
289531455285792829679923.

Security \approx 2^{125} against rho.

Order of \ell in (\mathbb{Z}/p)^* is
12152941675747802266549093
122563150387.

Twist security \approx 2^{75}.

(Want more twist security? Switch to \( p = 2^{127} - 94825; \) cofactors 16 \cdot 3269239, 4.)

Fast point-counting

Define \( F_{p^2} = F_p[i]/(i^2 + 1); \)

\( r = (7 + 4i)^2 = 33 + 56i; \)

\( s = 159 + 56i; \ omega = \sqrt{-384}; \)

\( C : y^2 = rx^6 + sx^4 + s \bar{x}^2 + r. \)

\( (x, y) \mapsto (x^2, y) \) takes \( C \) to \( E : \)

\( y^2 = rx^3 + sx^2 + s \bar{x} + r. \)

\( (x, y) \mapsto (1/x^2, y/x^3) \) takes \( C \) to \( y^2 = r x^3 + s \bar{x}^2 + sx + r. \)

\( (z, y) \mapsto \left( \frac{1 + iz}{1 - iz}, \frac{\omega y}{(1 - iz)^3} \right) \)

takes \( H \) over \( F_{p^2} \) to \( C. \)
$J$ is isogenous to the Weil restriction $W$ of $E$, so computing $# J(F_p)$ is fast.  

\[ J = 16\ell \]

$\ell$ is the prime

3943330655534932966
8553649194606010814
5285792829679923.

$\approx 2^{125}$ against rho.

If $\ell$ in $(\mathbb{Z}/p)^*$ is

167574780226654903
50387.

security $\approx 2^{75}$.

Want more twist security?

So $p = 2^{127} - 94825$;

is $16 \cdot 3269239, 4.$)

**Fast point-counting**

Define $F_{p^2} = F_p[i]/(i^2 + 1)$;

$r = (7 + 4i)^2 = 33 + 56i$;

$s = 159 + 56i$; $\omega = \sqrt{-384}$;

$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x, y) \mapsto (x^2, y)$ takes $C$ to $E$:

$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes $C$ to

$y^2 = \overline{r}x^3 + \overline{s}x^2 + sx + r$.

$(z, y) \mapsto \left( \frac{1 + iz}{1 - iz}, \frac{\omega y}{(1 - iz)^3} \right)$

takes $H$ over $F_{p^2}$ to $C$.  

$J$ is isogenous to the Weil restriction $W$ of $E$, so computing $# J(F_p)$ is fast.
Fast point-counting

Define $F_{p^2} = F_p[i]/(i^2 + 1)$;
$r = (7 + 4i)^2 = 33 + 56i$;
$s = 159 + 56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r}$.

$(x, y) \mapsto (x^2, y)$ takes $C$ to $E$:
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes $C$ to $y^2 = \bar{r}x^3 + \bar{s}x^2 + sx + r$.

$(z, y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$
takes $H$ over $F_{p^2}$ to $C$. 

$J$ is isogenous to the Weil restriction $W$ of $E$, so computing $\#J(F_p)$ is fast.
Fast point-counting

Define \( F_{p^2} = F_p[i]/(i^2 + 1) \);
\( r = (7 + 4i)^2 = 33 + 56i \);
\( s = 159 + 56i \); \( \omega = \sqrt{-384} \);
\( C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r} \).

\((x, y) \mapsto (x^2, y)\) takes \( C \) to \( E \):
\( y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r} \).

\((x, y) \mapsto (1/x^2, y/x^3)\) takes \( C \) to
\( y^2 = \bar{r}x^3 + \bar{s}x^2 + sx + r \).

\((z, y) \mapsto \left( \frac{1 + iz}{1 - iz}, \frac{\omega y}{(1 - iz)^3} \right)\)
takes \( H \) over \( F_{p^2} \) to \( C \).

\( J \) is isogenous to
Weil restriction \( W \) of \( E \), so computing \( \#J(F_p) \) is fast.
Fast point-counting

Define $F_{p^2} = F_p[i]/(i^2 + 1)$;
$r = (7 + 4i)^2 = 33 + 56i$;
$s = 159 + 56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \bar{s}x^2 + \bar{r}$.

$(x, y) \mapsto (x^2, y)$ takes $C$ to $E$:
$y^2 = rx^3 + sx^2 + \bar{s}x + \bar{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes $C$ to $y^2 = \bar{r}x^3 + \bar{s}x^2 + sx + r$.

$(z, y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$ takes $H$ over $F_{p^2}$ to $C$. 

$J$ is isogenous to$\quad$Weil restriction $W$ of $E$, so $\quad$computing $\#J(F_p)$ is fast.
Fast point-counting

Define \( F_{p^2} = F_p[i]/(i^2 + 1) \);
\( r = (7 + 4i)^2 = 33 + 56i \);
\( s = 159 + 56i; \omega = \sqrt{-384} \);
\( C : y^2 = rx^6 + sx^4 + sx^2 + r \).

\((x, y) \mapsto (x^2, y)\) takes \( C \) to \( E : y^2 = rx^3 + sx^2 + sx + r \).

\((x, y) \mapsto (1/x^2, y/x^3)\) takes \( C \) to
\( y^2 = rx^3 + sx^2 + sx + r \).

\((z, y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)\)
takes \( H \) over \( F_{p^2} \) to \( C \).

\( J \) is isogenous to
Weil restriction \( W \) of \( E \), so computing \( \#J(F_p) \) is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.
Fast point-counting

Define $F_{p^2} = F_p[i]/(i^2 + 1)$;
$r = (7 + 4i)^2 = 33 + 56i$;
$s = 159 + 56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + sx^2 + r$.

$(x, y) \mapsto (x^2, y)$ takes $C$ to $E$ :
$y^2 = rx^3 + sx^2 + sx + r$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes $C$ to
$y^2 = r x^3 + sx^2 + sx + r$.

$(z, y) \mapsto \left( \frac{1 + iz}{1 - iz}, \frac{\omega y}{(1 - iz)^3} \right)$
takes $H$ over $F_{p^2}$ to $C$.

$J$ is isogenous to
Weil restriction $W$ of $E$, so
computing $\#J(F_p)$ is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

Handles all elliptic curves
over $F_{p^2}$ with full 2-torsion
(and more elliptic curves).

Geometrically: all elliptic curves;
codim 1 in hyperelliptic curves.
Fast point-counting

\[ F_{p^2} = \mathbb{F}_p[i]/(i^2 + 1); \]
\[ (4i)^2 = 33 + 56i; \]
\[ + 56i; \quad \omega = \sqrt{-384}; \]
\[ r = rx^6 + sx^4 + sx^2 + \bar{r}. \]
\[ (x^2, y) \text{ takes } C \text{ to } E : \]
\[ y^2 = r x^3 + s x^2 + sx + \bar{r}. \]
\[ (1/x^2, y/x^3) \text{ takes } C \text{ to } \]
\[ y^2 = 3 + \bar{s} x^2 + sx + r. \]
\[ \left( \frac{1 + iz \omega y}{1 - iz} \right) \]
\[ \text{over } \mathbb{F}_{p^2} \text{ to } C. \]

\[ J \text{ is isogenous to } \]
\[ \text{Weil restriction } \mathcal{W} \text{ of } E, \text{ so } \]
\[ \text{computing } \#J(\mathbb{F}_p) \text{ is fast.} \]

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

Handles all elliptic curves
over \( \mathbb{F}_{p^2} \) with full 2-torsion
(and more elliptic curves).

Geometrically: all elliptic curves;
codim 1 in hyperelliptic curves.

New: not just point-counting
Alice generates secret \( a^2 \mathbb{Z} \).
Bob generates secret \( b^2 \mathbb{Z} \).

Alice computes \( aG \) using standard \( \mathcal{G} \).
Top speed: Edwards coordinates.

Alice sends \( aG \) to Bob.

Bob views \( aG \) in \( \mathcal{W}(\mathbb{F}_p) \),
applies isogeny \( \mathcal{W}(\mathbb{F}_p) ! J(\mathbb{F}_p) \),
computes \( b(aG) \) in \( J(\mathbb{F}_p) \).
Top speed: Kummer coordinates.
Define \( F_{p^2} = F_p[i] = (i^2 + 1); \) 
\( r = \sqrt{-384}; \) 
\( s = 159 + 56i; \) 
\( \lambda = 33 + 56i; \) 
\( \lambda^4 + sx^2 + r. \)

This takes \( C \) to \( E : \)
\( \frac{\omega y}{(1 - iz)^3} \)
to \( C. \)

\( J \) is isogenous to
Weil restriction \( W \) of \( E \), so computing \( \#J(F_p) \) is fast.

2003 Scholten:
this strategy for building many genus-2 curves with fast point-counting.

Handles all elliptic curves over \( F_{p^2} \) with full 2-torsion (and more elliptic curves).

Geometrically: all elliptic curves; codim 1 in hyperelliptic curves.

New: not just point-counting
Alice generates secret \( a \in \mathbb{Z} \).
Bob generates secret \( b \in \mathbb{Z} \).
Alice computes \( aG \) using standard \( G \) over \( F_{p^2} \).
Top speed: Edwards coordinates.

Alice sends \( aG \) to Bob.
Bob views \( aG \) in \( W(F_p) \), applies isogeny \( W(F_p) \) to \( J(F_p) \), computes \( b(aG) \) in \( J(F_p) \).
Top speed: Kummer coordinates.
Fast point-counting

Define $F_p^2 = F_p[i] = (i^2 + 1)$;

$r = (7 + 4i)^2 = 33 + 56i$;

$s = 159 + 56i$;

$C : y^2 = r x^6 + sx^4 + sx^2 + r$.

$(x; y)$ takes $C$ to $E$:

$y^2 = r x^3 + sx^2 + sx + r$.

$(z; y)$ takes $H$ over $F_p^2$ to $C$.

$J$ is isogenous to Weil restriction $W$ of $E$, so computing $\#J(F_p)$ is fast.

2003 Scholten: this strategy for building many genus-2 curves with fast point-counting.

Handles all elliptic curves over $\mathbb{F}_{p^2}$ with full 2-torsion (and more elliptic curves).

Geometrically: all elliptic curves; codim 1 in hyperelliptic curves.

New: not just point-counting

Alice generates secret $a \in \mathbb{Z}$.

Bob generates secret $b \in \mathbb{Z}$.

Alice computes $aG \in E(\mathbb{F}_{p^2})$, using standard $G \in E(\mathbb{F}_{p^2})$.

Top speed: Edwards coordinates.

Alice sends $aG$ to Bob.

Bob views $aG$ in $W(\mathbb{F}_p)$, applies isogeny $W(\mathbb{F}_p) \to J(\mathbb{F}_p)$, computes $b(aG) \in J(\mathbb{F}_p)$.

Top speed: Kummer coordinates.
$J$ is isogenous to Weil restriction $W$ of $E$, so computing $\#J(\mathbb{F}_p)$ is fast.

2003 Scholten:
this strategy for building many genus-2 curves with fast point-counting.

Handles all elliptic curves over $\mathbb{F}_{p^2}$ with full 2-torsion (and more elliptic curves).
Geometrically: all elliptic curves; codim 1 in hyperelliptic curves.

New: not just point-counting
Alice generates secret $a \in \mathbb{Z}$.
Bob generates secret $b \in \mathbb{Z}$.
Alice computes $aG \in E(\mathbb{F}_{p^2})$ using standard $G \in E(\mathbb{F}_{p^2})$.
Top speed: Edwards coordinates.
Alice sends $aG$ to Bob.
Bob views $aG$ in $W(\mathbb{F}_p)$, applies isogeny $W(\mathbb{F}_p) \to J(\mathbb{F}_p)$, computes $b(aG)$ in $J(\mathbb{F}_p)$.
Top speed: Kummer coordinates.
J is isogenous to restriction $W$ of $E$, so computing $\#J(F_p)$ is fast.

2003 Scholten: this strategy for building many genus-2 curves with fast point-counting.

Handles all elliptic curves over $F_p^2$ with full 2-torsion (and more elliptic curves).

Geometrically: all elliptic curves; codim 1 in hyperelliptic curves.

New: not just point-counting

Alice generates secret $a \in \mathbb{Z}$.
Bob generates secret $b \in \mathbb{Z}$.

Alice computes $aG \in E(F_p^2)$ using standard $G \in E(F_p^2)$.
Top speed: Edwards coordinates.

Alice sends $aG$ to Bob.

Bob views $aG$ in $W(F_p)$, applies isogeny $W(F_p) \to J(F_p)$, computes $b(aG)$ in $J(F_p)$.
Top speed: Kummer coordinates.

In general: use isogenies $\phi: W \to J$ and $\psi: J \to W$ to dynamically move computations between $E(F_p^2)$ and $J(F_p)$.

But do we have fast formulas for $\phi$ and for dual isogeny $\psi$?
In general: use isogenies $\iota : \mathcal{W} \to \mathcal{J}$ and $\iota' : \mathcal{J} \to \mathcal{W}$ to dynamically move computations between $\mathcal{E}(\mathbb{F}_{p^2})$ and $\mathcal{J}(\mathbb{F}_p)$.

But do we have fast formulas for $\iota'$ and for dual isogenies?

New: not just point-counting

Alice generates secret $a \in \mathbb{Z}$.
Bob generates secret $b \in \mathbb{Z}$.

Alice computes $aG \in \mathcal{E}(\mathbb{F}_{p^2})$ using standard $G \in \mathcal{E}(\mathbb{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends $aG$ to Bob.

Bob views $aG$ in $\mathcal{W}(\mathbb{F}_p)$, applies isogeny $\mathcal{W}(\mathbb{F}_p) \to \mathcal{J}(\mathbb{F}_p)$, computes $b(aG)$ in $\mathcal{J}(\mathbb{F}_p)$.
Top speed: Kummer coordinates.
New: not just point-counting

Alice generates secret $a \in \mathbb{Z}$.
Bob generates secret $b \in \mathbb{Z}$.

Alice computes $aG \in E(\mathbb{F}_{p^2})$ using standard $G \in E(\mathbb{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends $aG$ to Bob.

Bob views $aG$ in $W(\mathbb{F}_p)$,
applies isogeny $W(\mathbb{F}_p) \to J(\mathbb{F}_p)$,
computes $b(aG)$ in $J(\mathbb{F}_p)$.
Top speed: Kummer coordinates.

In general: use isogenies $\iota: W \to J$ and $\iota': J \to W$ to
dynamically move computations between $E(\mathbb{F}_{p^2})$ and $J(\mathbb{F}_p)$.

But do we have fast formulas for $\iota'$ and for dual isogeny $\iota^{-1}$?
New: not just point-counting

Alice generates secret $a \in \mathbb{Z}$.
Bob generates secret $b \in \mathbb{Z}$.

Alice computes $aG \in E(\mathbb{F}_{p^2})$ using standard $G \in E(\mathbb{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends $aG$ to Bob.

Bob views $aG$ in $W(\mathbb{F}_p)$,
applies isogeny $W(\mathbb{F}_p) \rightarrow J(\mathbb{F}_p)$,
computes $b(aG)$ in $J(\mathbb{F}_p)$.
Top speed: Kummer coordinates.

In general: use isogenies $\iota : W \rightarrow J$ and $\iota' : J \rightarrow W$ to dynamically move computations between $E(\mathbb{F}_{p^2})$ and $J(\mathbb{F}_p)$.

But do we have fast formulas for $\iota'$ and for dual isogeny $\iota$?
New: not just point-counting

Alice generates secret $a \in \mathbb{Z}$.
Bob generates secret $b \in \mathbb{Z}$.

Alice computes $aG \in E(\mathbb{F}_{p^2})$ using standard $G \in E(\mathbb{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends $aG$ to Bob.

Bob views $aG$ in $W(\mathbb{F}_p)$, applies isogeny $W(\mathbb{F}_p) \to J(\mathbb{F}_p)$, computes $b(aG)$ in $J(\mathbb{F}_p)$.
Top speed: Kummer coordinates.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbb{F}_{p^2})$ and $J(\mathbb{F}_p)$.

But do we have fast formulas for $\iota'$ and for dual isogeny $\iota$?

Scholten: Define $\phi : H \to E$ as

$$(z, y) \mapsto \left( \frac{(1 + iz)^2}{(1 - iz)^2}, \frac{\omega y}{(1 - iz)^3} \right).$$

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$. 

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbb{F}_{p^2})$ and $J(\mathbb{F}_p)$.
Alice generates secret $a \in \mathbb{Z}$.
Bob generates secret $b \in \mathbb{Z}$.

Alice computes $aG \in E(\mathbb{F}_{p^2})$ using standard $G \in E(\mathbb{F}_{p^2})$.

Top speed: Edwards coordinates.

Alice sends $aG$ to Bob.
Bob views $aG$ in $W(\mathbb{F}_p)$, applies isogeny $W(\mathbb{F}_p) \not\cong J(\mathbb{F}_p)$, computes $b(aG)$ in $J(\mathbb{F}_p)$.

Top speed: Kummer coordinates.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbb{F}_{p^2})$ and $J(\mathbb{F}_p)$.

But do we have fast formulas for $\iota'$ and for dual isogeny $\iota$?

Scholten: Define $\phi : H \to E$ as $(z, y) \mapsto \left( \frac{(1 + iz)^2}{(1 - iz)^2}, \frac{\omega y}{(1 - iz)^3} \right)$.

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

The conventional continuation:
1. Prove that $\iota$ is an isogeny by analyzing fibers of $\iota$.
2. Observe that $\iota' \equiv \iota$ for some isogeny $\iota$.
3. Compute formulas for $\iota'$ and for dual isogeny $\iota$.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbb{F}_{p^2})$ and $J(\mathbb{F}_p)$.

But do we have fast formulas for $\iota'$ and for dual isogeny $\iota$?

Scholten: Define $\phi : H \to E$ as $(z, y) \mapsto \left( \frac{(1 + iz)^2}{(1 - iz)^2}, \frac{\omega y}{(1 - iz)^3} \right)$.

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

The conventional continuation:
1. Prove that $\iota$ is an isogeny by analyzing fibers of $\iota$.
2. Observe that $\iota' \equiv \iota$ for some isogeny $\iota$.
3. Compute formulas for $\iota'$ and for dual isogeny $\iota$.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbb{F}_{p^2})$ and $J(\mathbb{F}_p)$.

But do we have fast formulas for $\iota'$ and for dual isogeny $\iota$?

Scholten: Define $\phi : H \to E$ as $(z, y) \mapsto \left( \frac{(1 + iz)^2}{(1 - iz)^2}, \frac{\omega y}{(1 - iz)^3} \right)$.

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.
In general: use isogenies
\( \iota : W \to J \) and \( \iota' : J \to W \) to
dynamically move computations
between \( E(F_{p^2}) \) and \( J(F_p) \).

But do we have **fast formulas**
for \( \iota' \) and for dual isogeny \( \iota \)?

Scholten: Define \( \phi : H \to E \) as
\[(z, y) \mapsto \left( \frac{(1 + iz)^2}{(1 - iz)^2}, \frac{\omega y}{(1 - iz)^3} \right).\]

Composition of \( \phi_2 : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2) \) and standard \( E \to W \)
is composition of standard
\( H \times H \to J \) and some \( \iota' : J \to W \).

The conventional continuation:
1. Prove that \( \iota' \) is an isogeny by analyzing fibers of 2.
2. Observe that \( \iota \iota' = 2 \) for some isogeny \( \iota \).
3. Compute formulas for \( \iota \iota' \): take
   \( P_i = (z_i, y_i) \) on \( H \),
   \( z_i \in F_{p^2} \)
   \((y_1^2 - f(z_1), y_2^2 - f(z_2)) \in J(F_p) \),
   \( f \) is the discriminant.

   **Composition:**
   \( \phi \phi : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2) \) and standard \( E \to W \)
is composition of standard
   \( H \times H \to J \) and some \( \iota' : J \to W \).

   **Elimination:**
   Eliminate \( z_1, z_2, y_1 \) in favor of Mumford coordinates.
In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbb{F}_{p^2})$ and $J(\mathbb{F}_p)$.

But do we have fast formulas for $\iota'$ and for dual isogeny $\iota$?

Scholten: Define $\phi : H \to E$ as
$$(x, y) \mapsto \left(\frac{(1 + ix)^2}{(1 - ix)^2}, \frac{\omega y}{(1 - ix)^3}\right).$$

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

The conventional continuation:

1. Prove that $\iota'$ is an isogeny by analyzing fibers of $\phi_2$.
2. Observe that $\iota \circ \iota' = 2$ for some isogeny $\iota$.
3. Compute formulas for $\iota'$: $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbb{F}_p(z_1, z_2)[y_1, y_2]/(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of $\phi$ with addition formulas on $E$; eliminate $z_1, z_2, y_1, y_2$ in favor of Mumford coordinates.
In general: use isogenies 
\( \iota : W \to J \) and \( \iota' : J \to W \) to 
dynamically move computations 
between \( E(\mathbb{F}_{p^2}) \) and \( J(\mathbb{F}_p) \).

But do we have fast formulas 
for \( \iota' \) and for dual isogeny \( \iota \)?

Scholten: Define \( \phi : H \to E \) as 
\[
(z, y) \mapsto \left( \frac{(1 + iz)^2}{1 - iz}^2, \frac{\omega y}{(1 - iz)^3} \right).
\]

Composition of \( \phi_2 : (P_1, P_2) \mapsto \phi(P_1) + \phi(P_2) \) and standard \( E \to W \) 
is composition of standard 
\( H \times H \to J \) and some \( \iota' : J \to W \).

The conventional continuation:

1. Prove that \( \iota' \) is an isogeny 
by analyzing fibers of \( \phi_2 \).

2. Observe that \( \iota \circ \iota' = 2 \) 
for some isogeny \( \iota \).

3. Compute formulas for \( \iota' \): take 
\( P_i = (z_i, y_i) \) on \( H : y^2 = f(z) \) 
over \( \mathbb{F}_p(z_1, z_2)[y_1, y_2] \) 
\( / (y_1^2 - f(z_1), y_2^2 - f(z_2)) \);
compose definition of \( \phi \) 
with addition formulas on \( E \); 
eliminate \( z_1, z_2, y_1, y_2 \) 
in favor of Mumford coordinates.
In general: use isogenies $W \to J$ and $J \to W$ to dynamically move computations between $E(F_{p^2})$ and $J(F_{p^2})$.

But do we have fast formulas for $0:J\to W$ and for dual isogeny $\phi_2$?

Scholten: Define:

$$H \to E((z, y) \mapsto (\frac{(1 + iz)^2}{1 - (iz)^3}, (\frac{1}{iy}(1 - iz)))^2);$$

Composition of $\phi_2: (P_1, P_2) \to (P_1 + P_2)$ and standard $E \to W$ is composition of standard $H \to J$ and some $\phi: J \to W$.

The conventional continuation:

1. Prove that $0$ is an isogeny by analyzing fibers of $\phi_2$.
2. Observe that $\phi \circ \phi = \phi_2$ for some isogeny $\phi$.
3. Compute formulas for $\phi$; take $P_i = (z_i, y_i)$ on $H: y^2 = f(x)$ over $F_{p^2}$.
4. Simplify formulas for $\phi$ using, e.g., 2006 Monagan–Pearce "rational simplification" method.
5. Find $\phi: \text{norm} \to \text{conorm}$ etc.
In general: use isogenies $J \to W$ and $0: J \to W$ to dynamically move computations between $E(F_p^2)$ and $J(F_p^2)$. But do we have fast formulas for $0$ and for dual isogeny $J \to W$?

Scholten: Define $H \to E$ as

$$\begin{align*}
H & \to E \\
y^2 & = f(z) \\
& \in \mathbb{F}_p(z_1, z_2)[y_1, y_2]
\end{align*}$$

Composition of $2$: $(P_1; P_2) \mapsto (P_1 + P_2)$ and standard $E \to W$ is composition of standard $H \to J$ and some $0: J \to W$.

The conventional continuation:

1. Prove that $\iota'$ is an isogeny by analyzing fibers of $\phi_2$.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny $\iota$.

3. Compute formulas for $\iota'$: take $P_i = (z_i, y_i)$ on $H: y^2 = f(z)$ over $\mathbb{F}_p(z_1, z_2)[y_1, y_2]$/\(y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of $\phi$ with addition formulas on $E$; eliminate $z_1, z_2, y_1, y_2$ in favor of Mumford coordinates.

4. Simplify formulas for $\iota$ using, e.g., 2006 Monagan–Pearce “rational simplification” method.

5. Find $\iota$: norm–conorm etc.
In general: use isogenies $\phi_1$ and $\phi_2$ to dynamically move computations between $E(K_{p^2})$ and $J(K_{p^2})$.

But do we have fast formulas for $\phi_0$ and for dual isogeny $\phi'_0$?

Scholten: Define $H$ as:

$$(z, y) \mapsto (1 + iz)^{2(1 - iz)}; y(1 - iz)^3.$$ 

Composition of $2$:

$$(P_1; P_2) \mapsto (P_1) + (P_2)$$

and standard $E \to W$ is composition of standard $H \to J$ and some $\phi'_0: J \to W$.

The conventional continuation:

1. Prove that $\phi'_1$ is an isogeny by analyzing fibers of $\phi_2$.
2. Observe that $\phi \circ \phi'_1 = 2$ for some isogeny $\phi$.
3. Compute formulas for $\phi'_1$: take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbb{F}_p(z_1, z_2)[y_1, y_2]$

$$/(y_1^2 - f(z_1), y_2^2 - f(z_2)).$$

compose definition of $\phi$

with addition formulas on $E$;

eliminate $z_1, z_2, y_1, y_2$

in favor of Mumford coordinates.

4. Simplify formulas for $\phi'_1$ using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find $\phi$: norm–conorm etc.
The conventional continuation:

1. Prove that $\iota'$ is an isogeny by analyzing fibers of $\phi_2$.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny $\iota$.

3. Compute formulas for $\iota'$: take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbb{F}_p(z_1, z_2)[y_1, y_2] \backslash (y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of $\phi$ with addition formulas on $E$; eliminate $z_1, z_2, y_1, y_2$ in favor of Mumford coordinates.

4. Simplify formulas for $\iota'$ using, e.g., 2006 Monagan–Pearce “rational simplification” method.

5. Find $\iota$: norm–conorm etc.
The conventional continuation:

1. Prove that \( \iota' \) is an isogeny by analyzing fibers of \( \phi_2 \).

2. Observe that \( \iota \circ \iota' = 2 \) for some isogeny \( \iota \).

3. Compute formulas for \( \iota' \): take \( P_i = (z_i, y_i) \) on \( H : y^2 = f(z) \) over \( \mathbb{F}_p(z_1, z_2)[y_1, y_2] \):

\[
\frac{y_1^2 - f(z_1), y_2^2 - f(z_2)}{(y_1^2 - f(z_1), y_2^2 - f(z_2))};
\]

compose definition of \( \phi \) with addition formulas on \( E \);
eliminate \( z_1, z_2, y_1, y_2 \) in favor of Mumford coordinates.

4. Simplify formulas for \( \iota' \) using, e.g., 2006 Monagan–Pearce “rational simplification” method.

5. Find \( \iota : \text{norm–conorm etc.} \)

Much easier: We applied \( \phi_2 \) to random points in \( H(\mathbb{F}_p) \times H(\mathbb{F}_p) \), interpolated coefficients of \( \iota' \).
Similarly interpolated formulas for \( \iota \); verified composition.

Easy computer calculation.

“Wasting brain power is bad for the environment.”
1. Prove that $0$ is an isogeny by analyzing fibers of $2$.

2. Observe that $0 = \ldots$ definition of with addition formulas on $E$; eliminate $z_1; z_2; y_1; y_2$ in favor of Mumford coordinates.

3. Compute formulas for $0$: take $P_i = (z_i; y_i)$ on $H: y^2 = f(z)$ over $F_p$.

4. Simplify formulas for $0$ using, e.g., 2006 Monagan–Pearce “rational simplification” method.


"Wasting brain power is bad for the environment."

Much easier: We applied $\phi_2$ to random points in $H(F_p) \times H(F_p)$, similarly interpolated formulas for $\phi$, verified composition.

Easy computer calculation.

"2006 Monagan–Pearce "rational simplification" method."
1. Prove that $0$ is an isogeny by analyzing fibers of $\phi_2$.

2. Observe that $\phi_0^\circ \iota = 2$.

3. Compute formulas for $\iota$: take $P_i = (z_i; y_i)$ on $H$:
   
   $$ y^2 = f(z_1; z_2) \quad \text{over } F_p, $$
   
   compose definition of $\phi$ with addition formulas on $E$;
   eliminate $z_1; z_2; y_1; y_2$ in favor of Mumford coordinates.

4. Simplify formulas for $\iota'$ using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find $\iota$: norm–conorm etc.

New: small coefficients $K$ defined by 3 coeffs.

Only 2 degrees of freedom in $E$.

Can't expect small-height coeffs.

... unless everything lifts to $\mathbb{Q}$.

Much easier: We applied $\phi_2$ to random points in $H(F_p) \times H(F_p)$, interpolated coefficients of $\iota'$.

Similarly interpolated formulas for $\iota$; verified composition.

Easy computer calculation.

"Wasting brain power is bad for the environment."
1. Prove that \( \lambda \) is an isogeny by analyzing fibers of \( \Phi \).

2. Observe that \( \lambda^0 = 2 \) for some isogeny \( \lambda \).

3. Compute formulas for \( \lambda \): take \( P_i = (z_i; y_i) \) on \( H \):
   \[ y_2^2 = f(z_1); y_2^2 = f(z_2); \]

   compose definition of \( \lambda \) with addition formulas on \( E \);

   eliminate \( z_1, z_2, y_1, y_2 \)

   in favor of Mumford coordinates.

4. Simplify formulas for \( \lambda' \) using, e.g., 2006 Monagan–Pearce “rational simplification” method.

5. Find \( \lambda \): norm–conorm etc.

   Much easier: We applied \( \phi_2 \) to random points in \( H(F_p) \times H(F_p) \),
   interpolated coefficients of \( \lambda' \).

   Similarly interpolated formulas for \( \lambda \); verified composition.

   Easy computer calculation.

   “Wasting brain power is bad for the environment.”

New: small coefficients
\( K \) defined by 3 coeffs.
Only 2 degrees of freedom in \( E \).
Can’t expect small-height coeffs.
... unless everything lifts to \( \mathbb{Q} \).
4. Simplify formulas for $\iota'$ using, e.g., 2006 Monagan–Pearce “rational simplification” method.

5. Find $\iota$: norm–conorm etc.

Much easier: We applied $\phi_2$ to random points in $H(F_p) \times H(F_p)$, interpolated coefficients of $\iota'$. Similarly interpolated formulas for $\iota$; verified composition.

Easy computer calculation.

“Wasting brain power is bad for the environment.”

New: small coefficients $K$ defined by 3 coeffs. Only 2 degrees of freedom in $E$. Can’t expect small-height coeffs. ... unless everything lifts to $Q$. 
4. Simplify formulas for $\iota'$ using, e.g., 2006 Monagan–Pearce “rational simplification” method.

5. Find $\iota$: norm–conorm etc.

Much easier: We applied $\phi_2$ to random points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$, interpolated coefficients of $\iota'$. Similarly interpolated formulas for $\iota$; verified composition.

Easy computer calculation.

“Wasting brain power is bad for the environment.”

---

New: small coefficients $K$ defined by 3 coeffs. Only 2 degrees of freedom in $E$.

Can’t expect small-height coeffs. ... unless everything lifts to $Q$.

Choose non-square $\Delta \in Q$; distinct squares $\rho_1, \rho_2, \rho_3$ of norm-1 elements of $Q(\sqrt{\Delta})$; $r \in Q(\sqrt{\Delta})$ with $-\rho_1\rho_2\rho_3 = \bar{r}/r$.

Define $s = -r(\rho_1 + \rho_2 + \rho_3)$.
Then $rx^3 + sx^2 + sx + \bar{r} = r(x - \rho_1)(x - \rho_2)(x - \rho_3).$
4. Simplify formulas for \( \nu' \) using, e.g., 2006 Monagan–Pearce “rational simplification” method.

5. Find \( \nu' \): norm–conorm etc.

Much easier: We applied \( \phi_2 \) to random points in \( H(F_p) \times H(F_p) \), interpolated coefficients of \( \nu' \).

Similarly interpolated formulas for \( \nu' \); verified composition.
Easy computer calculation.

“Wasting brain power is bad for the environment.”

New: small coefficients \( K \) defined by 3 coeffs.
Only 2 degrees of freedom in \( E \).
Can’t expect small-height coeffs.

... unless everything lifts to \( \mathbb{Q} \).
Choose non-square \( \Delta \in \mathbb{Q} \); distinct squares \( \rho_1, \rho_2, \rho_3 \) of norm-1 elements of \( \mathbb{Q}(\sqrt{\Delta}) \);

\( r \in \mathbb{Q}(\sqrt{\Delta}) \) with \(-\rho_1\rho_2\rho_3 = \bar{r}/r \).

Define \( s = -r(\rho_1 + \rho_2 + \rho_3) \).
Then \( rx^3 + sx^2 + \bar{s}x + \bar{r} = r(x - \rho_1)(x - \rho_2)(x - \rho_3) \).

Choose \( \mu, \lambda \in \mathbb{Q} \) and \( (\beta/H) \) such that:

Then the Scholten curve \( (r\beta^6 + s\beta^4 + \bar{s}\beta^2 + \bar{r}) \)

\( r(1 - \beta x)^6 \) has full 2-torsion over \( \mathbb{Q} \).

In many cases corresponding Rosenhain parameters \( \lambda \mu \) have \( \frac{\lambda \mu}{\nu} \) both squares in \( \mathbb{Q} \),
so \( K \) is defined over \( \mathbb{Q} \).

(Degenerate cases: see paper.)
4. Simplify formulas for $0$ using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find $\phi_2$ to $H(F_p) \times H(F_p)$.

- Interpolated formulas of $\phi_i$.
- Norm–conorm etc.
- As for $\phi_1$.

"Wasting brain power is bad for the environment."

New: small coefficients $K$ defined by 3 coeffs.

Choose $2 \mathbb{Q}(\Delta)$ with $2 \mathbb{Q}$ and $(2 \mathbb{Q} = \mathbb{Q})^2 = \mathbb{Q}$.

Then the Scholten curve
\[
(\alpha^2 - x)^6 + s \beta^4 \alpha^2 + s \beta^2 (1 - \beta_2) + s (1 - \beta_2)^2 (1 - \beta_2)^2
\]
has full 2-torsion over $\mathbb{Q}$.

In many cases corresponding Rosenhain parameters $\beta \in \mathbb{Q}(\sqrt{\Delta})$.

Then the Scholten curve $K$ defined by 3 coeffs.

Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ and $(\beta/\beta)^2 \neq \{\beta_1, \beta_2, \beta_3\}$.

Define $s = r (\rho_1 + \rho_2 + \rho_3)$.

Then $r \mathbb{Q}(\sqrt{\Delta})$ with $-\rho_1 \rho_2 \rho_3 = r^2$.

In many cases corresponding Rosenhain parameters $\beta \in \mathbb{Q}(\sqrt{\Delta})$.

Then the Scholten curve $K$ defined by 3 coeffs.

Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ and $(\beta/\beta)^2 \neq \{\beta_1, \beta_2, \beta_3\}$.

Define $s = r (\rho_1 + \rho_2 + \rho_3)$.

Then $r \mathbb{Q}(\sqrt{\Delta})$ with $-\rho_1 \rho_2 \rho_3 = r^2$.

In many cases corresponding Rosenhain parameters $\beta \in \mathbb{Q}(\sqrt{\Delta})$.

Then the Scholten curve $K$ defined by 3 coeffs.

Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ and $(\beta/\beta)^2 \neq \{\beta_1, \beta_2, \beta_3\}$.

Define $s = r (\rho_1 + \rho_2 + \rho_3)$.

Then $r \mathbb{Q}(\sqrt{\Delta})$ with $-\rho_1 \rho_2 \rho_3 = r^2$.

In many cases corresponding Rosenhain parameters $\beta \in \mathbb{Q}(\sqrt{\Delta})$.

Then the Scholten curve $K$ defined by 3 coeffs.

Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ and $(\beta/\beta)^2 \neq \{\beta_1, \beta_2, \beta_3\}$.

Define $s = r (\rho_1 + \rho_2 + \rho_3)$.

Then $r \mathbb{Q}(\sqrt{\Delta})$ with $-\rho_1 \rho_2 \rho_3 = r^2$.

In many cases corresponding Rosenhain parameters $\beta \in \mathbb{Q}(\sqrt{\Delta})$.

Then the Scholten curve $K$ defined by 3 coeffs.

Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ and $(\beta/\beta)^2 \neq \{\beta_1, \beta_2, \beta_3\}$.

Define $s = r (\rho_1 + \rho_2 + \rho_3)$.

Then $r \mathbb{Q}(\sqrt{\Delta})$ with $-\rho_1 \rho_2 \rho_3 = r^2$.

In many cases corresponding Rosenhain parameters $\beta \in \mathbb{Q}(\sqrt{\Delta})$.

Then the Scholten curve $K$ defined by 3 coeffs.

Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ and $(\beta/\beta)^2 \neq \{\beta_1, \beta_2, \beta_3\}$.

Define $s = r (\rho_1 + \rho_2 + \rho_3)$.

Then $r \mathbb{Q}(\sqrt{\Delta})$ with $-\rho_1 \rho_2 \rho_3 = r^2$.

In many cases corresponding Rosenhain parameters $\beta \in \mathbb{Q}(\sqrt{\Delta})$.

Then the Scholten curve $K$ defined by 3 coeffs.

Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ and $(\beta/\beta)^2 \neq \{\beta_1, \beta_2, \beta_3\}$.

Define $s = r (\rho_1 + \rho_2 + \rho_3)$.

Then $r \mathbb{Q}(\sqrt{\Delta})$ with $-\rho_1 \rho_2 \rho_3 = r^2$.

In many cases corresponding Rosenhain parameters $\beta \in \mathbb{Q}(\sqrt{\Delta})$.

Then the Scholten curve $K$ defined by 3 coeffs.

Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ and $(\beta/\beta)^2 \neq \{\beta_1, \beta_2, \beta_3\}$.
4. Simplify formulas for $0$ using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find $\rho_1$, $\rho_2$, $\rho_3$.

Much easier: We applied $2$ to random points in $H(F_p)$, $H(F_p)$, 
interpolated coefficients of $0$.

Similarly interpolated formulas for $\rho_1$, $\rho_2$, $\rho_3$; verified composition.

Easy computer calculation.

"Wasting brain power is bad for the environment."

New: small coefficients $K$ defined by $3$ coeffs.

Only $2$ degrees of freedom in $E$.

Can’t expect small-height coeffs.

... unless everything lifts to $Q$.

Choose non-square $\Delta \in Q$; distinct squares $\rho_1$, $\rho_2$, $\rho_3$ of norm-$1$ elements of $Q(\sqrt{\Delta})$;

$r \in Q(\sqrt{\Delta})$ with $-\rho_1 \rho_2 \rho_3 = \overline{r}/r$.

Define $s = -r(\rho_1 + \rho_2 + \rho_3)$.

Then $rx^3 + sx^2 + \overline{s}x + \overline{r} = r(x - \rho_1)(x - \rho_2)(x - \rho_3)$.

Choose $\beta \in Q(\sqrt{\Delta})$ with $\beta$, and $(\overline{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve

$(r\beta^6 + s\beta^4 \beta^2 + \overline{s}\beta^2 \beta^4 + \overline{r}\beta^6 + r(1-\beta z)^6 + s(1-\beta z)^4 (1-\mu z) + \overline{s}(1-\beta z)^2 (1-\beta z)^4 + \overline{r}(1-\beta z)^4)^2$ has full $2$-torsion over $Q$.

In many cases corresponding Rosenhain parameters $\lambda$, $\mu$, $\nu$ have $\lambda \mu$ and $\mu(\mu - 1)(\lambda - 1)$ both squares in $Q$, so $K$ is defined over $Q$.

(Degenerate cases: see paper.)
New: small coefficients

\( K \) defined by 3 coeffs.

Only 2 degrees of freedom in \( E \).

Can’t expect small-height coeffs. unless everything lifts to \( \mathbb{Q} \).

Choose non-square \( \Delta \in \mathbb{Q} \);
distinct squares \( \rho_1, \rho_2, \rho_3 \)
of norm-1 elements of \( \mathbb{Q}(\sqrt{\Delta}) \);
\( r \in \mathbb{Q}(\sqrt{\Delta}) \) with \(-\rho_1\rho_2\rho_3 = \bar{r}/r\).

Define \( s = -r(\rho_1 + \rho_2 + \rho_3) \).

Then \( rx^3 + sx^2 + \bar{s}x + \bar{r} = r(x - \rho_1)(x - \rho_2)(x - \rho_3) \).

Choose \( \beta \in \mathbb{Q}(\sqrt{\Delta}) \) with \( \beta \notin \mathbb{Q} \)
and \((\beta/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}\).

Then the Scholten curve
\[
(r\beta^6 + s\beta^4\beta^2 + s\beta^2\beta^4 + r\beta^6)y^2 = r(1-\beta z)^6 + s(1-\beta z)^4(1-\beta z)^2 + \bar{s}(1-\beta z)^2(1-\beta z)^4 + \bar{r}(1-\beta z)^6
\]
has full 2-torsion over \( \mathbb{Q} \).

In many cases corresponding
Rosenhain parameters \( \lambda, \mu, \nu \)

have \( \frac{\lambda\mu}{\nu} \) and \( \frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)} \)
both squares in \( \mathbb{Q} \),
so \( K \) is defined over \( \mathbb{Q} \).

(Degenerate cases: see paper.)
Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbb{Q}$ and $(\beta/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve
\[
(r\beta^6 + s\beta^4\beta^2 + s\beta^2\beta^4 + r\beta^6)y^2 = r(1-\beta x)^6 + s(1-\beta x)^4(1-\beta x)^2 + \bar{s}(1-\bar{\beta} x)^2(1-\beta x)^4 + \bar{r}(1-\beta x)^6
\]
has full 2-torsion over $\mathbb{Q}$.

In many cases corresponding Rosenhain parameters $\lambda, \mu, \nu$ have $\frac{\lambda\mu}{\nu}$ and $\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$ both squares in $\mathbb{Q}$, so $K$ is defined over $\mathbb{Q}$.

(Degenerate cases: see paper.)

Example: Choose $\Delta = 1; 1 = (i)$, $2 = ((3 + 4i) = 5)^2$, $3 = ((5+12i) = 13)^2$; $r = 33+56i$, $s = 159 + 56i$, $\bar{s} = i$.

One Rosenhain choice is $\lambda = 10, \mu = 5, \nu = 8$, $\mu = 25$.

Then $\frac{\lambda\mu}{\nu}$ and $\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$ both squares in $\mathbb{Q}$.

Larger example: $r = 8648575 15615600i$, $s = 40209279 33245520i$; coeffs $(6137 : 833 : 2275 : 2275)$. 
New: small coefficients
K defined by 3 coeffs.
Only 2 degrees of freedom in E.
Can't expect small-height coeffs.

Choose non-square \( \Delta \in Q \); distinct squares \( 1, 2, 3 \) of norm-1 elements of \( Q(\sqrt{\Delta}) \); \( r_2 Q(\sqrt{\Delta}) \) with \( 1 = 2 = 3 = r \).

Define \( s = r(1 + 2 + 3) \).

Then \( r x^3 + sx^2 + sx + r = r(x^3)(x^2)(x) \).

Example: Choose \( \Delta = 1; 1 = (i)^2, 2 = ((3 + 4i) = 5)^2, 3 = ((5+12i) = 13)^2; r = 33+56i, s = 159 + 56i, \) and \( \beta/\beta^2 \notin \{p_1, p_2, p_3\} \).

Choose \( \beta \in Q(\sqrt{\Delta}) \) with \( \beta \notin Q \).

Then the Scholten curve has full 2-torsion over \( Q \).

In many cases corresponding Rosenhain parameters \( \lambda, \mu, \nu \) have \( \lambda \mu \) and \( \mu(\mu - 1)(\nu - 1)(\lambda - \mu) \) both squares in \( Q \), so \( K \) is defined over \( Q \).

(Degenerate cases: see paper.)

Larger example:
\( r = 8648575 - 15615600i, \) \( s = 40209279 - 33245520i \); coeffs \( (6137 : 833 : 2275 : 2275) \).

Example: Choose \( \Delta = (5 + 12i)^2/13 \); \( p_1 = (i)^2, p_2 = ((3 + 4i) = 5)^2, p_3 = (5 + 12i)^2/13 \).

One Rosenhain choice is \( \mu = 833, \nu = 2275, \lambda = 10, \) \( \lambda \mu = 108350, \nu(\nu - 1)(\lambda - \mu) = 560241600 \).

Then \( \frac{\lambda\mu}{2^2} = 55527, \frac{\nu(\nu - 1)(\lambda - \mu)}{2} = 28012080 \).

and

\[ \frac{r}{p_1 p_2 p_3} = \frac{r}{r}. \]
Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbb{Q}$ and $(\beta/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve
$$ (r\beta^6 + s\bar{\beta}^4\beta^2 + s\beta^2\bar{\beta}^4 + \bar{r}\beta^6)y^2 = r(1-\bar{\beta}z)^6 + s(1-\bar{\beta}z)^4(1-\beta z)^2 + \bar{s}(1-\bar{\beta}z)^2(1-\beta z)^4 + \bar{r}(1-\beta z)^6 $$
has full 2-torsion over $\mathbb{Q}$.

In many cases corresponding Rosenhain parameters $\lambda, \mu, \nu$ have $\frac{\lambda \mu}{\nu}$ and $\frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)}$ both squares in $\mathbb{Q}$, so $K$ is defined over $\mathbb{Q}$.

(Degenerate cases: see paper.)

Example: Choose $\Delta = -1$;
$\rho_1 = (i)^2$, $\rho_2 = ((3 + 4i)/5)^2$,
$\rho_3 = ((5+12i)/13)^2$; $r = 33+56i$, $s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is $\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\frac{\lambda \mu}{\nu} = \frac{1}{2^2}$
and $\frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)} = \frac{1}{40^2}$

Larger example:
$r = 8648575 - 15615600i$,
Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbb{Q}$ and $(\bar{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve

$$(r\bar{\beta}^6 + s\bar{\beta}^4\beta^2 + s\bar{\beta}^2\beta^4 + r\beta^6)y^2 = r(1-\beta z)^6 + s(1-\beta z)^4(1-\beta z)^2 + s(1-\beta z)^2(1-\beta z)^4 + r(1-\beta z)^6$$

has full 2-torsion over $\mathbb{Q}$.

In many cases corresponding Rosenhain parameters $\lambda, \mu, \nu$ have

$$\frac{\lambda\mu}{\nu} \quad \text{and} \quad \frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)}$$

both squares in $\mathbb{Q}$, so $K$ is defined over $\mathbb{Q}$.

(Degenerate cases: see paper.)

Example: Choose $\Delta = -1$;

$\rho_1 = (i)^2$, $\rho_2 = ((3 + 4i)/5)^2$,

$\rho_3 = ((5+12i)/13)^2$; $r = 33 + 56i$,

$s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is

$\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\frac{\lambda\mu}{\nu} = \frac{1}{2^2}$

and $\frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)} = \frac{1}{40^2}$.

Larger example:

$r = 8648575 - 15615600i$,

$s = -40209279 - 33245520i$;

coeffs $(6137 : 833 : 2275 : 2275)$. 
Choose $\beta \in \mathbb{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbb{Q}$, and $\beta^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve
\[
(r \beta^4 + s \beta^2 \beta^4 + \bar{r} \beta^6) y^2 = \bar{s}(1 - \bar{r} \beta z)^4 (1 - \bar{r} \beta z)^2 + \bar{s}(1 - \beta z)^4 (1 - \beta z)^2 (1 - \beta z)^4 + r (1 - \beta z)^6
\]
has full 2-torsion over $\mathbb{Q}$.

In many cases corresponding Rosenhain parameters 
\[
1; 2; 3
\]
both squares in $\mathbb{Q}$, so $K$ is defined over $\mathbb{Q}$.

(Degenerate cases: see paper.)

**Example:** Choose $\Delta = -1$; $\rho_1 = (i)^2$, $\rho_2 = ((3 + 4i)/5)^2$, $\rho_3 = ((5 + 12i)/13)^2$; $r = 33 + 56i$, $s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is $\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\frac{\lambda \mu}{\nu} = \frac{1}{2^2}$ and $\frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)} = \frac{1}{40^2}$.

Larger example:
\[
r = 8648575 - 15615600i,
\]
\[
s = -40209279 - 33245520i;
\]
coeffs $(6137 : 833 : 2275 : 2275)$. 
Choose $\Delta$ with $\beta \notin \mathbb{Q}$.

Then the Scholten curve

$$r^2 - s^2 \beta^4 + r\beta^6) y^2 = (\beta z)^4(1 - \beta z)^2 + (\beta z)^4 + r(1 - r z)^6$$

has full 2-torsion over $\mathbb{Q}$.

In many cases corresponding Rosenhain parameters

$$\rho_1 = (i)^2, \rho_2 = ((3 + 4i)/5)^2, \rho_3 = ((5+12i)/13)^2; r = 33 + 56i, s = 159 + 56i, \beta = i.$$ 

One Rosenhain choice is

$$\lambda = 10, \mu = 5/8, \nu = 25.$$ 

Then

$$\frac{\lambda \mu}{\nu} = \frac{1}{2^2}$$

and

$$\frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)} = \frac{1}{40^2}.$$ 

Larger example:

$$r = 8648575 - 15615600i,$$
$$s = -40209279 - 33245520i;$$
coeffs (6137 : 833 : 2275 : 2275).
Example: Choose $\Delta = -1$; 
$\rho_1 = (i)^2$, $\rho_2 = ((3 + 4i)/5)^2$, 
$\rho_3 = ((5 + 12i)/13)^2$; $r = 33 + 56i$, 
$s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is 
$\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then \[ \lambda \mu \nu = \frac{1}{2^2} \]
and \[ \frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)} = \frac{1}{40^2}. \]

Larger example: 
$r = 8648575 - 15615600i$, 
$s = -40209279 - 33245520i$; 
coeffs $(6137 : 833 : 2275 : 2275)$. 

Example: Choose $\Delta = -1$; 
$\rho_1 = (i)^2$, $\rho_2 = ((3 + 4i)/5)^2$,  
$\rho_3 = ((5+12i)/13)^2$; $r = 33 + 56i$, 
$s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is 
$\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then \[
\frac{\lambda \mu}{\nu} = \frac{1}{2^2}
\]
and \[
\frac{\mu(\mu - 1)(\lambda - \nu)}{\nu(\nu - 1)(\lambda - \mu)} = \frac{1}{40^2}.
\]

Larger example:
$r = 8648575 - 15615600i$,  
$s = -40209279 - 33245520i$;  
coeffs (6137 : 833 : 2275 : 2275).