Faster computation of isogenies of large prime degree.

D. J. Bernstein, L. De Feo, **A. Leroux**, B. Smith

ANTS 2020

Isogenies between montgomery elliptic curves

For Montgomery curves

$$E_{/k} : y^2 = x^3 + Ax^2 + x$$

the cyclic isogeny φ of odd prime degree n with kernel $\mathcal{G} = \langle P \rangle$ is the algebraic map defined by:

$$\begin{aligned} \varphi \quad : \quad & E \longrightarrow E/\mathcal{G} \\ & (x, y) \longmapsto \left(\frac{g(x)}{h(x)}, y \left(\frac{g(x)}{h(x)} \right)' \right) \end{aligned}$$

Isogenies between montgomery elliptic curves

For Montgomery curves

$$E_{/k} : y^2 = x^3 + Ax^2 + x$$

the cyclic isogeny φ of odd prime degree n with kernel $\mathcal{G} = \langle P \rangle$ is the algebraic map defined by:

$$\begin{aligned} \varphi \quad : \quad & E \longrightarrow E/\mathcal{G} \\ & (x, y) \longmapsto \left(\frac{g(x)}{h(x)}, y \left(\frac{g(x)}{h(x)} \right)' \right) \end{aligned}$$

where:

$$\frac{g(X)}{h(X)} = (-1)^{n-1} X^n \prod_{i=1}^{n-1} \frac{1/X - x([i]P)}{X - x([i]P)}$$

A summary of the result

Isogeny evaluation problem over a field k

Input: Generator $P \in E(k)$ of order n for cyclic kernel $\mathcal{G} = \langle P \rangle$, a point $Q \in E(k)$.

Output: The codomain $E/\mathcal{G}$ and the image point $\varphi(Q)$;

A summary of the result

Isogeny evaluation problem over a field k

Input: Generator $P \in E(k)$ of order n for cyclic kernel $\mathcal{G} = \langle P \rangle$, a point $Q \in E(k)$.

Output: The codomain $E/\mathcal{G}$ and the image point $\varphi(Q)$;

Kernel polynomial Evaluation

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

A summary of the result

Isogeny evaluation problem over a field k

Input: Generator $P \in E(k)$ of order n for cyclic kernel $\mathcal{G} = \langle P \rangle$, a point $Q \in E(k)$.

Output: The codomain $E/\mathcal{G}$ and the image point $\varphi(Q)$;

Kernel polynomial Evaluation

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

A summary of the result

Isogeny evaluation problem over a field k

Input: Generator $P \in E(k)$ of order n for cyclic kernel $\mathcal{G} = \langle P \rangle$, a point $Q \in E(k)$.

Output: The codomain $E/\mathcal{G}$ and the image point $\varphi(Q)$;

Algo. Complexity: $\widetilde{O}(\sqrt{n})$.

Kernel polynomial Evaluation

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1} (\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1} (\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Pollard '74: Original idea.

Chudnovsky^2 '88: n-th term of a holonomic sequence.

$\vdots$

Bostan '20: n-th term of a q-holonomic sequence.

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1} (\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Eval. on $\prod_{i=0}^{s-1} \prod_{j=0}^{s-1} (\alpha - \zeta^i \zeta^{s \cdot j})$ in BSGS fashion with resultants ($n = s^2$).

Pollard '74: Original idea.

Chudnovsky^2 '88: n-th term of a holonomic sequence.

⋮

Bostan '20: n-th term of a q-holonomic sequence.

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1}(\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Eval. on $\prod_{i=0}^{s-1}\prod_{j=0}^{s-1}(\alpha - \zeta^i\zeta^{s\cdot j})$ in BSGS fashion with resultants ($n = s^2$).

1. $B(Y) = \prod_{i=0}^{s-1}(Y - \zeta^i)$.

Pollard '74: Original idea.

Chudnovsky^2 '88: n-th term of a holonomic sequence.

⋮

Bostan '20: n-th term of a q-holonomic sequence.

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1}(\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Eval. on $\prod_{i=0}^{s-1}\prod_{j=0}^{s-1}(\alpha - \zeta^i\zeta^{s\cdot j})$ in BSGS fashion with resultants ($n = s^2$).

1. $B(Y) = \prod_{i=0}^{s-1}(Y - \zeta^i)$.
2. $G(Y) = \prod_{j=0}^{s-1}(\alpha - Y \cdot \zeta^{j\cdot s})$.

Pollard '74: Original idea.

Chudnovsky^2 '88: n-th term of a holonomic sequence.

⋮

Bostan '20: n-th term of a q-holonomic sequence.

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1}(\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Eval. on $\prod_{i=0}^{s-1}\prod_{j=0}^{s-1}(\alpha - \zeta^i\zeta^{s\cdot j})$ in BSGS fashion with resultants ($n = s^2$).

1. $B(Y) = \prod_{i=0}^{s-1}(Y - \zeta^i)$.
2. $G(Y) = \prod_{j=0}^{s-1}(\alpha - Y \cdot \zeta^{j\cdot s})$.
3. $h(\alpha) = \mathrm{Res}_Y(B, G)$.

Pollard '74: Original idea.

Chudnovsky^2 '88: n-th term of a holonomic sequence.

⋮

Bostan '20: n-th term of a q-holonomic sequence.

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1}(\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Eval. on $\prod_{i=0}^{s-1}\prod_{j=0}^{s-1}(\alpha - \zeta^i\zeta^{s\cdot j})\prod_{k=0}^{m-1}(\alpha - \zeta^{n+k})$ in BSGS fashion with resultants ($n = s^2+m$ and $m = O(\sqrt{n})$).

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1}(\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Eval. on $\prod_{i=0}^{s-1}\prod_{j=0}^{s-1}(\alpha - \zeta^i\zeta^{s\cdot j})\prod_{k=0}^{m-1}(\alpha - \zeta^{n+k})$ in BSGS fashion with resultants ($n = s^2+m$ and $m = O(\sqrt{n})$).

1. $B(Y) = \prod_{i=0}^{s-1}(Y - \zeta^i)$.

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1}(\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Eval. on $\prod_{i=0}^{s-1}\prod_{j=0}^{s-1}(\alpha - \zeta^i\zeta^{s\cdot j})\prod_{k=0}^{m-1}(\alpha - \zeta^{n+k})$ in BSGS fashion with resultants ($n = s^2+m$ and $m = O(\sqrt{n})$).

1. $B(Y) = \prod_{i=0}^{s-1}(Y - \zeta^i)$.
2. $G(Y) = \prod_{j=0}^{s-1}(\alpha - Y \cdot \zeta^{j\cdot s})$.

Warm-up: the multiplicative group example

Input: An element $\zeta \in k$ and a value $\alpha \in k$.

Output: The evaluation $h(\alpha) = \prod_{i=0}^{n-1}(\alpha - \zeta^i)$

Algo. Complexity: $\widetilde{O}(\sqrt{n})$

Eval. on $\prod_{i=0}^{s-1}\prod_{j=0}^{s-1}(\alpha - \zeta^i\zeta^{s\cdot j})\prod_{k=0}^{m-1}(\alpha - \zeta^{n+k})$ in BSGS fashion with resultants ($n = s^2+m$ and $m = O(\sqrt{n})$).

1. $B(Y) = \prod_{i=0}^{s-1}(Y - \zeta^i)$.
2. $G(Y) = \prod_{j=0}^{s-1}(\alpha - Y \cdot \zeta^{j\cdot s})$.
3. $h(\alpha) = \mathrm{Res}_Y(B, G)\prod_{k=0}^{m-1}(\alpha - \zeta^{n+k})$.

Can we do the same?

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

Algo. Complexity: ?

Can we do the same?

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

Algo. Complexity: ?

We used the progression

$$\zeta^i,\ \zeta^{s \cdot j} \mapsto \zeta^i \cdot \zeta^{s \cdot j} = \zeta^{i + s \cdot j}$$

Can we do the same?

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

Algo. Complexity: ?

We used the progression

$$\zeta^i,\ \zeta^{s\cdot j} \mapsto \zeta^i \cdot \zeta^{s\cdot j} = \zeta^{i+s\cdot j}$$

Problem: No formula for $x([i]P),\ x([s\cdot j]P) \mapsto x([i+s\cdot j]P)$;

Can we do the same?

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

Algo. Complexity: ?

We used the progression

$$\zeta^i,\ \zeta^{s\cdot j} \mapsto \zeta^i \cdot \zeta^{s\cdot j} = \zeta^{i+s\cdot j}$$

Problem: No formula for $x([i]P),\ x([s\cdot j]P) \mapsto x([i+s\cdot j]P)$;

Solution: But Biquadratic expressions for

$$x([i]P),\ x([j\cdot s]P) \mapsto \begin{cases} x([i+s\cdot j]P)\cdot x([i-s\cdot j]P) \\ x([i+s\cdot j]P) + x([i-s\cdot j]P) \end{cases}$$

Can we do the same?

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

Algo. Complexity: ?

We used the progression

$$\zeta^i,\ \zeta^{s\cdot j} \mapsto \zeta^i \cdot \zeta^{s\cdot j} = \zeta^{i+s\cdot j}$$

Problem: No formula for $x([i]P),\ x([s\cdot j]P) \mapsto x([i+s\cdot j]P)$;

Solution: But Biquadratic expressions for

$$x([i]P),\ x([j\cdot s]P) \mapsto \begin{cases} x([i+s\cdot j]P)\cdot x([i-s\cdot j]P) \\ x([i+s\cdot j]P) + x([i-s\cdot j]P) \end{cases}$$

BSGS eval. to $h(\alpha) = \prod_{i\in I}\prod_{j\in J}(\alpha - x([i+s\cdot j]P))(\alpha - x([i-s\cdot j]P))$

Can we do the same?

Input: A point $P \in E(k)$ of order n, a value $\alpha \in k$.

Output: Eval. of kernel polynomial $h(\alpha) = \prod_{i=1}^{n-1} (\alpha - x([i]P))$.

Algo. Complexity: $\widetilde{O}(\sqrt{n})$.

We used the progression

$$\zeta^i,\ \zeta^{s\cdot j} \mapsto \zeta^i \cdot \zeta^{s\cdot j} = \zeta^{i+s\cdot j}$$

Problem: No formula for $x([i]P),\ x([s\cdot j]P) \mapsto x([i+s\cdot j]P)$;

Solution: But Biquadratic expressions for

$$x([i]P),\ x([j\cdot s]P) \mapsto \begin{cases} x([i+s\cdot j]P)\cdot x([i-s\cdot j]P) \\ x([i+s\cdot j]P) + x([i-s\cdot j]P) \end{cases}$$

BSGS eval. to $h(\alpha) = \prod_{i\in I}\prod_{j\in J}(\alpha - x([i+s\cdot j]P))(\alpha - x([i-s\cdot j]P))$

Biquadratic expressions

The group law on the elliptic curve gives:

$$(X - x(P \oplus Q))(X - x(P \ominus Q)) = X^2 + \frac{F_1(x(P), x(Q))}{F_0(x(P), x(Q))} X + \frac{F_2(x(P), x(Q))}{F_0(x(P), x(Q))}$$

Biquadratic expressions

The group law on the elliptic curve gives:

$$(X - x(P \oplus Q))(X - x(P \ominus Q)) = X^2 + \frac{F_1(x(P), x(Q))}{F_0(x(P), x(Q))} X + \frac{F_2(x(P), x(Q))}{F_0(x(P), x(Q))}$$

where

$$\begin{aligned} F_0(X, Y) &= (X - Y)^2 \\ F_1(X, Y) &= -2((XY + 1)(X + Y) + 2AXY) \\ F_2(X, Y) &= (XY - 1)^2 \end{aligned}$$

Rewriting the kernel polynomial

$$h(\alpha) = \prod_{i \in I} \prod_{j \in J} (\alpha - x([i + s \cdot j]P))(\alpha - x([i - s \cdot j]P))$$

Rewriting the kernel polynomial

$$h(\alpha) = \prod_{i \in I} \prod_{j \in J} (\alpha - x([i + s \cdot j]P))(\alpha - x([i - s \cdot j]P))$$

$$= \prod_{i \in I} \prod_{j \in J} \frac{\alpha^2 F_0(x([i]P), x[s \cdot j]P) + \alpha F_1(x([i]P), x[s \cdot j]P) + F_2(x([i]P), x[s \cdot j]P)}{F_0(x([i]P), x[s \cdot j]P)}$$

Rewriting the kernel polynomial

$$h(\alpha) = \prod_{i \in I} \prod_{j \in J} (\alpha - x([i + s \cdot j]P))(\alpha - x([i - s \cdot j]P))$$

$$= \prod_{i \in I} \prod_{j \in J} \frac{\alpha^2 F_0(x([i]P), x[s \cdot j]P) + \alpha F_1(x([i]P), x[s \cdot j]P) + F_2(x([i]P), x[s \cdot j]P)}{F_0(x([i]P), x[s \cdot j]P)}$$

1. $B(Y) = \prod_{i \in I} (Y - x([i]P))$

Rewriting the kernel polynomial

$$h(\alpha) = \prod_{i \in I} \prod_{j \in J} (\alpha - x([i + s \cdot j]P))(\alpha - x([i - s \cdot j]P))$$

$$= \prod_{i \in I} \prod_{j \in J} \frac{\alpha^2 F_0(x([i]P), x[s \cdot j]P) + \alpha F_1(x([i]P), x[s \cdot j]P) + F_2(x([i]P), x[s \cdot j]P)}{F_0(x([i]P), x[s \cdot j]P)}$$

1. $B(Y) = \prod_{i \in I} (Y - x([i]P))$
2. $G_1(Y) = \prod_{j \in J} (F_0(Y, x([j \cdot s]P))$

Rewriting the kernel polynomial

$$h(\alpha) = \prod_{i \in I} \prod_{j \in J} (\alpha - x([i + s \cdot j]P))(\alpha - x([i - s \cdot j]P))$$

$$= \prod_{i \in I} \prod_{j \in J} \frac{\alpha^2 F_0(x([i]P), x[s \cdot j]P) + \alpha F_1(x([i]P), x[s \cdot j]P) + F_2(x([i]P), x[s \cdot j]P)}{F_0(x([i]P), x[s \cdot j]P)}$$

1. $B(Y) = \prod_{i \in I} (Y - x([i]P))$
2. $G_1(Y) = \prod_{j \in J} (F_0(Y, x([j \cdot s]P))$
3. $G_2(Y) = \prod_{j \in J} \prod (\alpha^2 F_0(Y, x[s \cdot j]P) + \alpha F_1(Y, x[s \cdot j]P) + F_2(Y, x[s \cdot j]P))$

Rewriting the kernel polynomial

$$h(\alpha) = \prod_{i \in I} \prod_{j \in J} (\alpha - x([i + s \cdot j]P))(\alpha - x([i - s \cdot j]P))$$

$$= \prod_{i \in I} \prod_{j \in J} \frac{\alpha^2 F_0(x([i]P), x[s \cdot j]P) + \alpha F_1(x([i]P), x[s \cdot j]P) + F_2(x([i]P), x[s \cdot j]P)}{F_0(x([i]P), x[s \cdot j]P)}$$

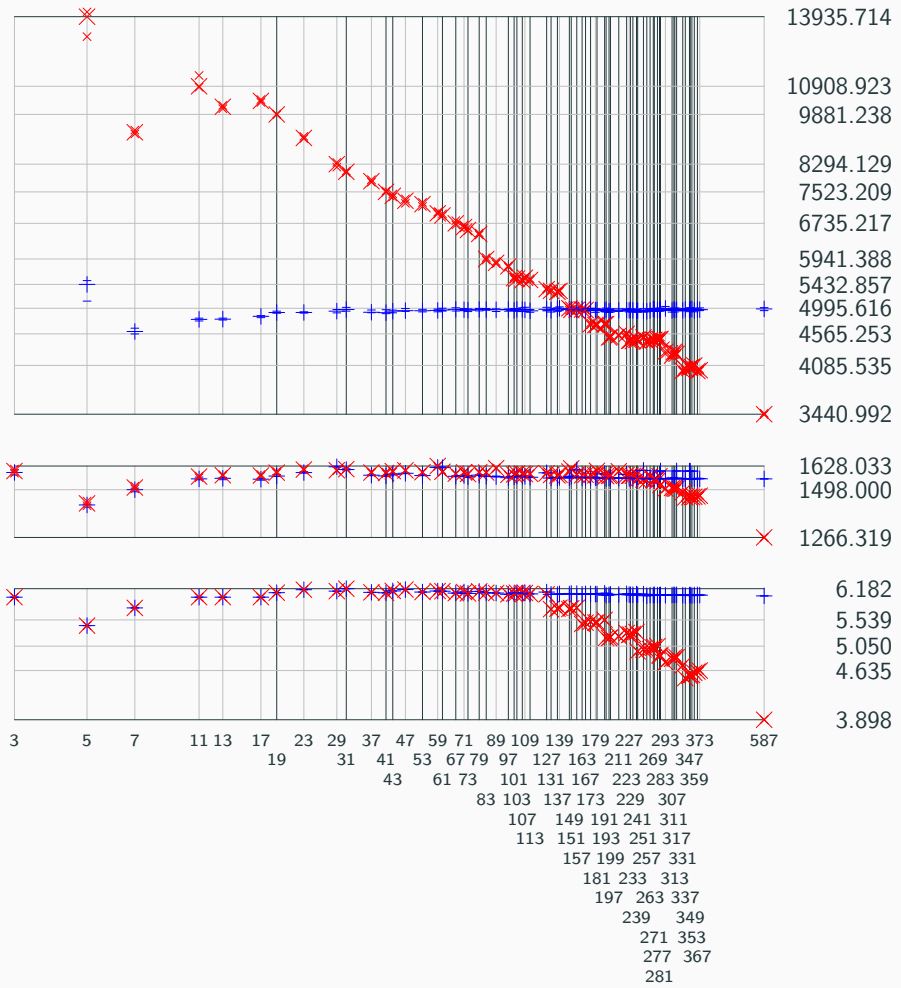
1. $B(Y) = \prod_{i \in I} (Y - x([i]P))$
2. $G_1(Y) = \prod_{j \in J} (F_0(Y, x([j \cdot s]P))$
3. $G_2(Y) = \prod_{j \in J} \prod (\alpha^2 F_0(Y, x[s \cdot j]P) + \alpha F_1(Y, x[s \cdot j]P) + F_2(Y, x[s \cdot j]P))$
4. $h(\alpha) = Res_Y(B, G_2)/Res_Y(B, G_1)$

Questions?

https://velusqrt.isogeny.org

Concrete Performances (small degrees)

Performance of new vs. old algorithm. Time to eval. an isogeny.



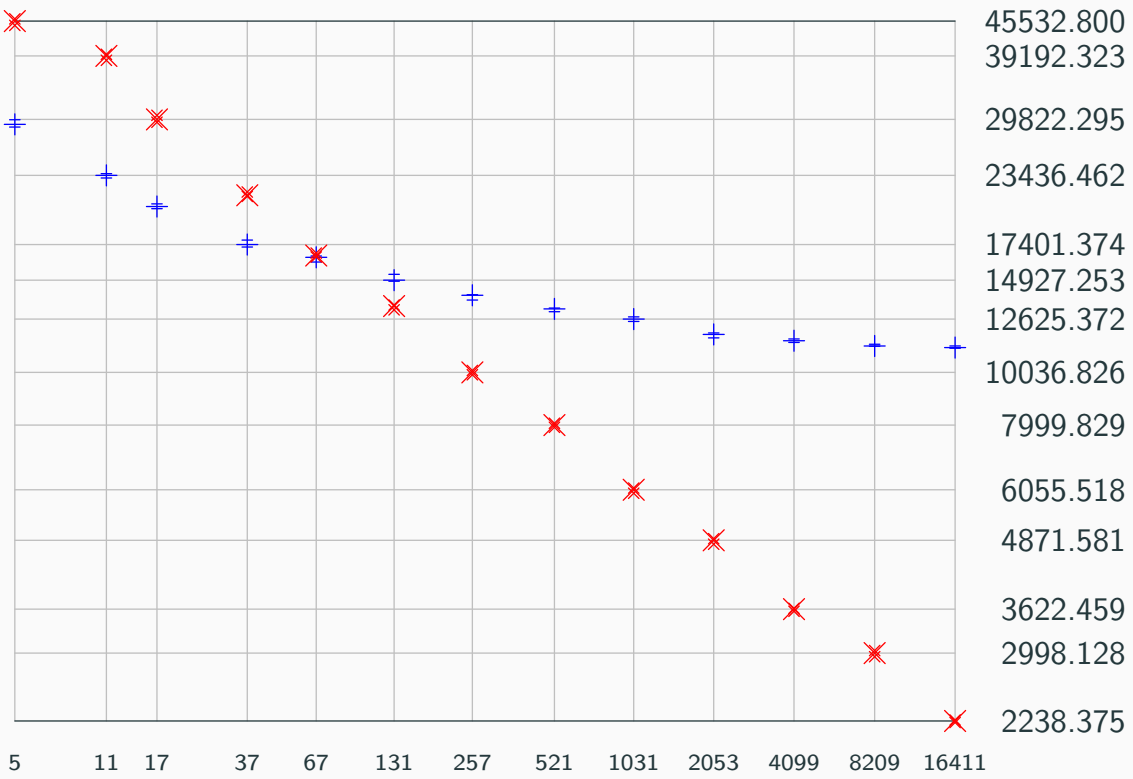
x-axis: isogeny degree n,
y-axis (divided by $n+2$):

Top: Cycle counts of pure C implem. on Flint.

Middle: Cycle counts of assembly optim. implem. based on original CSIDH-512.

Bottom: $\mathbb{F}_p$ mul. counts of the assembly optim. implem.

Concrete Performances (large degree)



Performance comparison of new vs. old algorithm in a Julia/Nemo implementation on a 256-bits base field.

x-axis: isogeny degree. y-axis: cycle counts.

Application to isogeny-based cryptography

Performance cross point is currently around $n \approx 100$

Application to isogeny-based cryptography

Performance cross point is currently around $n \approx 100$

Concrete improvements for:

Application to isogeny-based cryptography

Performance cross point is currently around $n \approx 100$

Concrete improvements for:

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18): $n \leq 587$

$1\ \%$ improvement for CSIDH-512 ($10\ \%$ for CSIDH-1024).

Application to isogeny-based cryptography

Performance cross point is currently around $n \approx 100$

Concrete improvements for:

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18): $n \leq 587$

1 % improvement for CSIDH-512 (10 % for CSIDH-1024).

B-SIDH (Costello '19): n in the millions.

First secure implementation: from minutes to seconds for key exchange.

Application to isogeny-based cryptography

Performance cross point is currently around $n \approx 100$

Concrete improvements for:

CSIDH (Castryck, Lange, Martindale, Panny, Renes '18): $n \leq 587$

1 % improvement for CSIDH-512 (10 % for CSIDH-1024).

B-SIDH (Costello '19): n in the millions.

First secure implementation: from minutes to seconds for key exchange.

others: Galbraith, Petit, Silva '17,

Delpech de Saint Guilhem, Kutas, Petit, Silva '19,

. . . (to be assessed).