Computation of ℓ-Isogenies in $\tilde{O}(\sqrt{\ell})$

Antonin Leroux

DGA, Institut Polytechnique de Paris, Ecole Polytechnique

Joint work with D. J. Bernstein, L. De Feo, B. Smith

Summary

1. Computing Isogenies

2. A Generalization

Computing Isogenies

Isogeny formula on Montgomery Elliptic Curves

Cyclic isogeny φ of **odd degree** with kernel $G = \langle P \rangle \subset E[\ell]$ on

$$E/_{\mathbb{F}_q} : y^2 = x^3 + Ax^2 + x$$

is[1] $\varphi : (x, y) \mapsto (f(x), c_0 y f'(x))$ with

$$f(x) = x \prod_{g \in G} \frac{x x_g - 1}{x - x_g}$$

[1] See Renes, "Computing Isogenies Between Montgomery Curves Using the Action of (0, 0)"

Isogeny formula on Montgomery Elliptic Curves

Cyclic isogeny φ of **odd degree** with kernel $G = \langle P \rangle \subset E[\ell]$ on

$$E_{/\mathbb{F}_q} : y^2 = x^3 + Ax^2 + x$$

is[1] $\varphi : (x, y) \mapsto (f(x), c_0 y f'(x))$ with

$$f(x) = x \prod_{g \in G} \frac{x x_g - 1}{x - x_g}$$

Efficiently evaluate $P_G(x) = \prod_{g \in G}(x - x_g) \Rightarrow$ Efficiently compute φ.

[1] See Renes, "Computing Isogenies Between Montgomery Curves Using the Action of (0, 0)"

Decomposing the polynomial in a BSGS fashion

Goal: Evaluate $P_G(x)$.

[2] all complexities are given in terms of $\mathbb{F}_q$ operations

Decomposing the polynomial in a BSGS fashion

Goal: Evaluate $P_G(x)$.

Complexity[2]**: Naive** method in $O(\ell)$, **today** in $\tilde{O}(\sqrt{\ell})$.

[2] all complexities are given in terms of $\mathbb{F}_q$ operations

Decomposing the polynomial in a BSGS fashion

Goal: Evaluate $P_G(x)$.

Complexity[2]**: Naive** method in $O(\ell)$, **today** in $\tilde{O}(\sqrt{\ell})$.

Take $m = \lfloor\sqrt{\ell}\rfloor$ and $\begin{cases} G_1 = \left\{P, [2]P ...., [m-1]P\right\} \\ G_2 = \left\{[2m]P, [4m]P, ..., [m(m-1)]P\right\} \end{cases}$

[2]all complexities are given in terms of $\mathbb{F}_q$ operations

Decomposing the polynomial in a BSGS fashion

Goal: Evaluate $P_G(x)$.

Complexity[2]**: Naive** method in $O(\ell)$, **today** in $\tilde{O}(\sqrt{\ell})$.

Take $m = \lfloor \sqrt{\ell} \rfloor$ and $\begin{cases} G_1 = \left\{ P, [2]P ...., [m-1]P \right\} \\ G_2 = \left\{ [2m]P, [4m]P, ..., [m(m-1)]P \right\} \end{cases}$

$$P_G(x) = \prod_{P_1 \in G_1, P_2 \in G_2} (x - x_{P_1 \oplus P_2})(x - x_{P_1 \ominus P_2}) R(x) = P_{G_1, G_2}(x) R(x)$$

[2]all complexities are given in terms of $\mathbb{F}_q$ operations

Decomposing the polynomial in a BSGS fashion

Goal: Evaluate $P_G(x)$.

Complexity[2]**: Naive** method in $O(\ell)$, **today** in $\tilde{O}(\sqrt{\ell})$.

Take $m = \lfloor \sqrt{\ell} \rfloor$ and $\begin{cases} G_1 = \left\{ P, [2]P...., [m-1]P \right\} \\ G_2 = \left\{ [2m]P, [4m]P, ..., [m(m-1)]P \right\} \end{cases}$

$$P_G(x) = \prod_{P_1 \in G_1, P_2 \in G_2} (x - x_{P_1 \oplus P_2})(x - x_{P_1 \ominus P_2}) R(x) = P_{G_1, G_2}(x) R(x)$$

$R(x) = P_{G_1}(x) P_{G_2}(x) \prod_{0 \le 2i+1 \le m} (x - x_{[(2i+1)m]P}) \prod_{m^2 \le i \le \ell - 1} (x - x_{[i]P})$

[2] all complexities are given in terms of $\mathbb{F}_q$ operations

Decomposing the polynomial in a BSGS fashion

Goal: Evaluate $P_G(x)$.

Complexity[2]: Naive method in $O(\ell)$, **today** in $\tilde{O}(\sqrt{\ell})$.

Take $m = \lfloor \sqrt{\ell} \rfloor$ and $\begin{cases} G_1 = \Big\{ P, [2]P...., [m-1]P \Big\} \\ G_2 = \Big\{ [2m]P, [4m]P, ..., [m(m-1)]P \Big\} \end{cases}$

$$P_G(x) = \prod_{P_1 \in G_1, P_2 \in G_2} (x - x_{P_1 \oplus P_2})(x - x_{P_1 \ominus P_2}) R(x) = P_{G_1,G_2}(x) R(x)$$

$R(x) = P_{G_1}(x) P_{G_2}(x) \prod_{0 \leq 2i+1 \leq m} (x - x_{[(2i+1)m]P}) \prod_{m^2 \leq i \leq \ell-1} (x - x_{[i]P})$
Evaluating $R(x)$ is in $\mathbf{O}(\sqrt{\ell})$.

[2] all complexities are given in terms of $\mathbb{F}_q$ operations

The algebraic group law

Biquadratic expression of the group law:

$$\begin{cases} x_{P_1 \oplus P_2} x_{P_1 \ominus P_2} = \frac{(1 - x_{P_1} x_{P_2})^2}{(x_{P_1} - x_{P_2})^2} \\ x_{P_1 \oplus P_2} + x_{P_1 \ominus P_2} = 2 \frac{x_{P_1} + x_{P_2} + x_{P_1} x_{P_2} (2A + x_{P_1} + x_{P_2})}{(x_{P_1} - x_{P_2})^2} \end{cases}$$

The algebraic group law

Biquadratic expression of the group law:

$$\begin{cases} x_{P_1 \oplus P_2} x_{P_1 \ominus P_2} = \frac{(1 - x_{P_1} x_{P_2})^2}{(x_{P_1} - x_{P_2})^2} \\ x_{P_1 \oplus P_2} + x_{P_1 \ominus P_2} = 2 \frac{x_{P_1} + x_{P_2} + x_{P_1} x_{P_2} (2A + x_{P_1} + x_{P_2})}{(x_{P_1} - x_{P_2})^2} \end{cases}$$

Grouping terms in pairs yields

$$(x - x_{P_1 \oplus P_2})(x - x_{P_1 \ominus P_2}) = \frac{h(x, x_{P_1}, x_{P_2})}{b(x_{P_1}, x_{P_2})} \tag{1}$$

Rewriting P_{G_1,G_2}

When x is **fixed**:

$$P_{G_1,G_2}(x) = \prod_{P_1 \in G_1, P_2 \in G_2} \frac{h(x, x_{P_1}, x_{P_2})}{b(x_{P_1}, x_{P_2})} = \prod_{P_1 \in G_1} \frac{H(x_{P_1})}{B(x_{P_1})}$$

where $H(Y) = \prod_{P_2 \in G_2} h(x, Y, x_{P_2})$ has degree $2|G_2|$ in Y, same for B.

Rewriting P_{G_1,G_2}

When x is **fixed**:

$$P_{G_1,G_2}(x) = \prod_{P_1 \in G_1, P_2 \in G_2} \frac{h(x, x_{P_1}, x_{P_2})}{b(x_{P_1}, x_{P_2})} = \prod_{P_1 \in G_1} \frac{H(x_{P_1})}{B(x_{P_1})}$$

where $H(Y) = \prod_{P_2 \in G_2} h(x, Y, x_{P_2})$ has degree $2|G_2|$ in Y, same for B.

We focus on **evaluating** H at $(x_{P_1})_{P_1 \in G_1}$, the same idea works for B.

Multi-point Evaluation

A very classical **multi-point evaluation** algorithm, allows us to evaluate $\prod_{i=1}^{n}(X - a_i)$ at $b_1, ..., b_n$ in $\tilde{O}(n)$.

Multi-point Evaluation

A very classical **multi-point evaluation** algorithm, allows us to evaluate $\prod_{i=1}^{n}(X - a_i)$ at $b_1, ..., b_n$ in $\tilde{O}(n)$.

Applying this on H when $|G_1| = |G_2| \simeq \sqrt{\ell} \Rightarrow \left(H(x_{P_1})\right)_{P_1 \in G_1}$ is evaluated in $\tilde{O}(\sqrt{\ell})$

Multi-point Evaluation

A very classical **multi-point evaluation** algorithm, allows us to evaluate $\prod_{i=1}^{n}(X - a_i)$ at $b_1, ..., b_n$ in $\tilde{O}(n)$.

Applying this on H when $|G_1| = |G_2| \simeq \sqrt{\ell} \Rightarrow (H(x_{P_1}))_{P_1 \in G_1}$ is evaluated in $\tilde{O}(\sqrt{\ell})$
$\Rightarrow \prod_{P_1 \in G_1} H(x_{P_1})$ computed in $\tilde{O}(\sqrt{\ell})$ (same for B)

Multi-point Evaluation

A very classical **multi-point evaluation** algorithm, allows us to evaluate $\prod_{i=1}^{n}(X - a_i)$ at $b_1, ..., b_n$ in $\tilde{O}(n)$.

Applying this on H when $|G_1| = |G_2| \simeq \sqrt{\ell} \Rightarrow (H(x_{P_1}))_{P_1 \in G_1}$ is evaluated in $\tilde{O}(\sqrt{\ell})$
$\Rightarrow \prod_{P_1 \in G_1} H(x_{P_1})$ computed in $\tilde{O}(\sqrt{\ell})$ (same for B)
$\Rightarrow P_{G_1,G_2}(x)$ is calculated in $\tilde{O}(\sqrt{\ell})$

Multi-point Evaluation

A very classical **multi-point evaluation** algorithm, allows us to evaluate $\prod_{i=1}^{n}(X - a_i)$ at $b_1, ..., b_n$ in $\tilde{O}(n)$.

Applying this on H when $|G_1| = |G_2| \simeq \sqrt{\ell} \Rightarrow (H(x_{P_1}))_{P_1 \in G_1}$ is evaluated in $\tilde{O}(\sqrt{\ell})$
$\Rightarrow \prod_{P_1 \in G_1} H(x_{P_1})$ computed in $\tilde{O}(\sqrt{\ell})$ (same for B)
$\Rightarrow P_{G_1,G_2}(x)$ is calculated in $\tilde{O}(\sqrt{\ell})$
$\Rightarrow$ Evaluation of P_G at x in $\tilde{O}(\sqrt{\ell})$.

Experimental Results

ℓ	q	E	Before	After
11677	$744\ell - 1$	$y^2 = x^3 + x$	14.880s	0.160s
62501	$48\ell - 1$	$y^2 = x^3 + 6x^2 + x$	✗	1.120s

Table 1: Magma implementation, comparison between my implementation of the two methods

A Generalization

Can we generalize it?

Goal: Compute $P_G(x) = \prod_{g \in G}(x - f(g))$, where $f : G \to \mathbb{F}_q$.

[3]an additive version of this is presented in D. Chudnovsky and G. Chudnovsky, "Computer algebra in the service of mathematical physics and number theory"

Can we generalize it?

Goal: Compute $P_G(x) = \prod_{g \in G}(x - f(g))$, where $f : G \to \mathbb{F}_q$.

Multiplicative group[3]: $G \cong \mu_\ell$, $f = Id$

$$P_G(x) = \prod_{i=1}^{\ell}(X - \zeta^i)$$

[3] an additive version of this is presented in D. Chudnovsky and G. Chudnovsky, "Computer algebra in the service of mathematical physics and number theory"

Can we generalize it?

Goal: Compute $P_G(x) = \prod_{g \in G}(x - f(g))$, where $f : G \to \mathbb{F}_q$.

Multiplicative group[3]: $G \cong \mu_\ell$, $f = Id$

$$P_G(x) = \prod_{i=1}^{\ell}(X - \zeta^i)$$

Elliptic curve: $G = \langle P \rangle \subset E[\ell]$, $f(P) = x_P$

$$P_G(x) = \prod_{i=1}^{\ell}(x - x_{[i]P})$$

[3] an additive version of this is presented in D. Chudnovsky and G. Chudnovsky, "Computer algebra in the service of mathematical physics and number theory"

Can we generalize it?

Goal: Compute $P_G(x) = \prod_{g \in G}(x - f(g))$, where $f : G \to \mathbb{F}_q$.

Multiplicative group[3]: $G \cong \mu_\ell$, $f = Id$

$$P_G(x) = \prod_{i=1}^{\ell}(X - \zeta^i)$$

Elliptic curve: $G = \langle P \rangle \subset E[\ell]$, $f(P) = x_P$

$$P_G(x) = \prod_{i=1}^{\ell}(x - x_{[i]P})$$

Abelian variety of higher genuses?

[3] an additive version of this is presented in D. Chudnovsky and G. Chudnovsky, "Computer algebra in the service of mathematical physics and number theory"

References

D. Chudnovsky and Gregory Chudnovsky. "Computer algebra in the service of mathematical physics and number theory". In: *International Journal of Computer Mathematics - IJCM* (Jan. 1990).

Joost Renes. "Computing Isogenies Between Montgomery Curves Using the Action of (0, 0)". In: *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*. 2018, pp. 229–247. DOI: 10.1007/978-3-319-79063-3_11. URL: https://doi.org/10.1007/978-3-319-79063-3%5C_11.