Horizontal racewalking using radical isogenies

Wouter Castryck[1,4] Thomas Decru[1] **Marc Houben**[1,2,3]
Frederik Vercauteren[1]

[1]imec-COSIC, KU Leuven, Belgium

[2]Departement of Mathematics, KU Leuven, Belgium

[3]Mathematical Institute, Leiden University, The Netherlands

[4]Department of Mathematics: Algebra and Geometry, Ghent University, Belgium

13/12/2022

Motivation

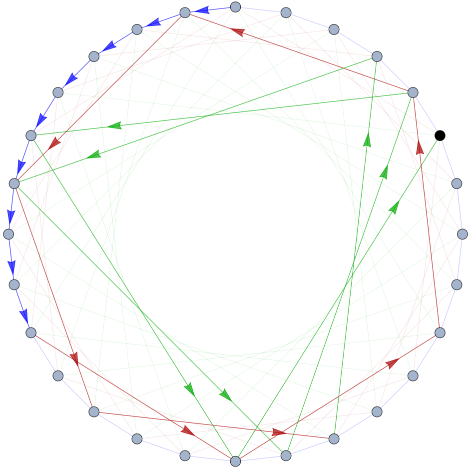
Functionalities based on long chains of isogenies

1. Key exchanges (CSIDH, CRS) $\leftarrow$
2. Verifiable delay functions
3. Signatures (CSI-FiSh)
4. Oblivious transfer
5. Delay encryption

Key exchange from a class group action

Private	Public	Private
	E_0	
$[\mathfrak{a}]$	$[\mathfrak{a}]E_0$ →	$[\mathfrak{b}]$
Alice		Bob
$[\mathfrak{a}][\mathfrak{b}]E_0$	← $[\mathfrak{b}]E_0$	$[\mathfrak{b}][\mathfrak{a}]E_0$

CSIDH



Connected component of a union of supersingular 3-, 5-, and 7-isogeny graphs over some prime field $\mathbb{F}_p$.

Computing a chain of N-isogenies

Problem

Given a cyclic isogeny $\varphi : E \to E' = E/\langle P \rangle$ of degree N, find P' on E' such that the composition $E \xrightarrow{\varphi} E' \to E'/\langle P' \rangle$ is cyclic of degree N^2.

Possible solution

Sample a random point T on E', and hope that $P' = (\#E'/N)T$ works.

Alternative solutions

1. Extract a root of the modular polynomial $\Phi_N(j(E'), X)$ different from $j(E)$.
2. Extract a root of the N-division polynomial on E'.

Radical 5-isogenies

Any elliptic curve with a point of P order 5 can be written as

$$E : y^2 - (1-b)xy - by = x^3 - bx^2, \text{ where } P = (0,0).$$

Write down the (general) equation for $E/\langle P\rangle$ using Vélu's formulae:

$$y^2+(1-b)xy-by = x^3-bx^2-5b(b^2+2b-1)x-b(b^4+10b^3-5b^2+15b-1).$$

Find the coordinates of an appropriate 5-torsion point P' on E':

$$\begin{aligned} x_0' &= 5\alpha^4+(b-3)\alpha^3+(b+2)\alpha^2+(2b-1)\alpha-2b, \\ y_0' &= 5\alpha^4+(b-3)\alpha^3+(b^2-10b+1)\alpha^2+(13b-b^2)\alpha-b^2-11b, \end{aligned}$$

where $\alpha = \sqrt[5]{b}$. Translate P' to $(0,0)$ to obtain

$$E' : y^2-(1-b')xy-b'y = x^3-b'x^2, \text{ where } b' = \alpha\frac{\alpha^4+3\alpha^2+4\alpha^2+2\alpha+1}{\alpha^4-2\alpha^3+4\alpha^2-3\alpha+1}.$$

New method

Problem

Given a cyclic isogeny $\varphi : E \to E' = E/\langle P \rangle$ of degree N, find P' on E' such that the composition $E \xrightarrow{\varphi} E' \to E'/\langle P' \rangle$ is cyclic of degree N^2.

The points $P' \in E'$ are characterized by the property

$$\hat{\varphi}(P') = \lambda P \text{ for some } \lambda \in (\mathbb{Z}/N\mathbb{Z})^{\times}.$$

Assume $\lambda = 1$. Then we can write

$$P' = \varphi(Q), \text{ for some } Q \in E[N^2] \text{ such that } NQ = P.$$

In fact, if $R \in E$ is such that $E[N] = \langle P, R \rangle$, then

$$P' \in \{\varphi(Q), \varphi(Q + R), \ldots, \varphi(Q + (N-1)R)\}.$$

Let E/K be an elliptic curve, $P \in E(K)$ of order N, and $Q \in E(\overline{K})$ such that $NQ = P$. We can find $x(P') = x(\varphi(Q))$ by Vélu's formulae:

$$x(P') = \sum_{i=0}^{N-1} x(Q + iP) - \sum_{i=0}^{N-1} x(iP), \qquad \beta_0 := \sum_{i=0}^{N-1} x(Q + iP).$$

Let $R \in E(\overline{K})$ such that $E[N] = \langle P, R \rangle$, and set

$$\beta_j := \sum_{i=0}^{N-1} x(Q + jR + iP).$$

Let $\zeta_N \in \overline{K}$ be an N-th root of unity, and consider the linear system

$$\begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{N-1} \end{pmatrix} := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{N-1} & \zeta_N^{2(N-1)} & \cdots & \zeta_N^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}.$$

Let $\zeta_N \in \overline{K}$ be an N-th root of unity, and consider the linear system

$$\begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{N-1} \end{pmatrix} := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{N-1} & \zeta_N^{2(N-1)} & \cdots & \zeta_N^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}.$$

Galois magic™

For all $0 \leq d \leq N-1$, we have $\gamma_d^N \in K$ and $(\gamma_d/\gamma_1^d) \in K$.

Defining $\alpha := \gamma_1$ and $C_d := (\gamma_d/\gamma_1^d)$, we have that $\alpha^N \in K$ and

$$\beta_0 = \sum_{i=0}^{N} x(Q+iP) = \frac{1}{N}\sum_{d=0}^{N-1} \gamma_d = \frac{1}{N}\sum_{d=0}^{N-1} \left(\frac{\gamma_d}{\gamma_1^d}\right)\gamma_1^d = \frac{1}{N}\sum_{d=0}^{N-1} C_d\,\alpha^d \in K(\alpha).$$

Idea

Determine a formula for C_d over many (smallish) finite fields $\mathbb{F}_p$, then lift to $\mathbb{Q}$ using CRT.

Idea

Determine a formula for C_d over many (smallish) finite fields $\mathbb{F}_p$, then lift to $\mathbb{Q}$ using CRT.

Let $E/\mathbb{F}_p$ be an elliptic curve in Tate normal form

$$E : y^2 + (1-c)xy - bx = x^3 - bx^2, \text{ where } (b,c) \in X_1(N)(\mathbb{F}_p).$$

We determine $C_d(b,c)$ by *rational interpolation*: compute many samples $((b,c), C_d)$ and interpolate a rational expression.

Let $p \equiv 1 \pmod{N^4}$ and $E/\mathbb{F}_p$ an elliptic curve with trace $t = 2$, so that $N^4 \mid \#E(\mathbb{F}_p) = p + 1 - t$ and $N \mid p - 1$. Assuming that $E[N^2] = \mathbb{Z}/N^2\mathbb{Z} \times \mathbb{Z}/N^2\mathbb{Z}$, all quantities Q, P, R, ζ_N are defined over $\mathbb{F}_p$.

Problem

Given p, t, construct an elliptic curve $/\mathbb{F}_p$ with trace t, possibly with extra restriction on the N-torsion.

Let E/K be an elliptic curve, $P \in E(K)$ of order N, and $Q \in E(\overline{K})$ such that $NQ = P$. We can find $x(P')$ by determining

$$\beta_0 := \sum_{i=0}^{N} x(Q + iP).$$

Let $R \in E(\overline{K})$ such that $E[N] = \langle P, R \rangle$, and set

$$\beta_j := \sum_{i=0}^{N} x(Q + jR + iP).$$

Let $\zeta_N \in \overline{K}$ be an N-th root of unity, and consider the linear system

$$\begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{N-1} \end{pmatrix} := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{N-1} & \zeta_N^{2(N-1)} & \cdots & \zeta_N^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}.$$

Let E/K be an elliptic curve, $P \in E(K)$ of order N, and $Q \in E(\overline{K})$ such that $NQ = P$. We can find $x(P')$ by determining

$$\beta_0 := \sum_{i=0}^{N} x(Q + iP).$$

Let $R \in E(\overline{K})$ such that $E[N] = \langle P, R \rangle$, and set

$$\beta_j := \sum_{i=0}^{N} x(Q + jR + iP).$$

Let $\zeta_N \in \overline{K}$ be an N-th root of unity, and consider the linear system

$$\begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{N-1} \end{pmatrix} := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{N-1} & \zeta_N^{2(N-1)} & \cdots & \zeta_N^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}.$$

Let E/K be an elliptic curve, $P \in E(K)$ of order N, and $Q \in E(\overline{K})$ such that $NQ = P$. We can find $x(P')$ by determining

$$\beta_0 := \sum_{i=0}^{N} x(Q + iP).$$

Let $R \in E(\overline{K})$ such that $E[N] = \langle P, R \rangle$, and set

$$\beta_j := \sum_{i=0}^{N} x(Q + jR + iP).$$

Let $\zeta_N \in \overline{K}$ be an N-th root of unity, and consider the linear system

$$\begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{N-1} \end{pmatrix} := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{N-1} & \zeta_N^{2(N-1)} & \cdots & \zeta_N^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}.$$

Let E/K be an elliptic curve, $P \in E(K)$ of order N, and $Q \in E(\overline{K})$ such that $NQ = P$. We can find $x(P')$ by determining

$$\beta_0 := \sum_{i=0}^{N} x(Q + iP).$$

Let $R \in E(\overline{K})$ such that $E[N] = \langle P, R \rangle$, and set

$$\beta_j := \sum_{i=0}^{N} x(Q + jR + iP).$$

Let $\zeta_N \in \overline{K}$ be an N-th root of unity, and consider the linear system

$$\begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{N-1} \end{pmatrix} := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{N-1} & \zeta_N^{2(N-1)} & \cdots & \zeta_N^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}.$$

Let E/K be an elliptic curve, $P \in E(K)$ of order N, and $Q \in E(\overline{K})$ such that $NQ = P$. We can find $x(P')$ by determining

$$\beta_0 := \sum_{i=0}^{N} x(Q + iP).$$

Let $R \in E(\overline{K})$ such that $E[N] = \langle P, R \rangle$, and set

$$\beta_j := \sum_{i=0}^{N} x(Q + jR + iP).$$

Let $\zeta_N \in \overline{K}$ be an N-th root of unity, and consider the linear system

$$\begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{N-1} \end{pmatrix} := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N & {\zeta_N}^2 & \cdots & {\zeta_N}^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & {\zeta_N}^{N-1} & {\zeta_N}^{2(N-1)} & \cdots & {\zeta_N}^{(N-1)^2} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}.$$

Idea

Determine a formula for C_d over many (smallish) finite fields $\mathbb{F}_p$, then lift to $\mathbb{Q}$ using CRT.

Let $E/\mathbb{F}_p$ be an elliptic curve in Tate normal form

$$E : y^2 + (1-c)xy - bx = x^3 - bx^2, \text{ where } (b,c) \in X_1(N)(\mathbb{F}_p).$$

We determine C_d in terms of b, c by *rational interpolation:* compute many samples $((b,c), C_d)$ and interpolate a rational expression.

Let $p \equiv 1 \pmod{N^4}$ and $E/\mathbb{F}_p$ an elliptic curve with trace $t = 2$, so that

$$N \mid p-1, \quad \text{and} \quad N^4 \mid \#E(\mathbb{F}_p) = p + 1 - t.$$

If additionally $E[N^2] \cong \mathbb{Z}/N^2\mathbb{Z} \times \mathbb{Z}/N^2\mathbb{Z}$, all quantities Q, P, R, ζ_N are defined over $\mathbb{F}_p$.

Problem (not really a problem because we know how to do it)

Given p and t, construct an elliptic curve $E/\mathbb{F}_p$ with trace t (preferably with additional control over the N^∞-torsion structure).

Elliptic curves over $\mathbb{C}$

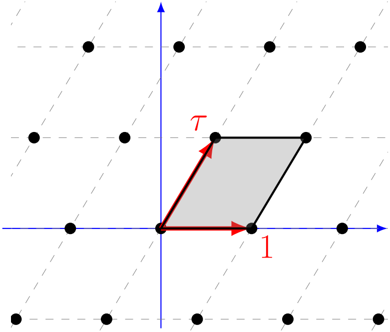
$\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\}$

$j : \mathbb{H} \to \mathbb{C}$, $\Lambda_1 \cong \Lambda_2 \iff j(\tau_1) = j(\tau_2)$.

Typically, $\mathrm{End}(\Lambda) = \mathrm{End}(\mathbb{Z}[\tau]) = \mathbb{Z}$.

If $a\tau^2 + b\tau + c = 0$ for coprime $a, b, c \in \mathbb{Z}$:

$\mathrm{End}(\Lambda) \cong \mathbb{Z}[a\tau] = \mathcal{O} \subseteq K = \mathbb{Q}(\tau)$.



The *Hilbert class polynomial* is:

$$\begin{aligned} H_\tau(X) &= \prod_{\sigma \in \mathrm{Gal}(K(j(\tau))/K)} (X - \sigma(j(\tau))) \\ &= \prod_{\substack{\Lambda \text{ lattice} \\ \mathrm{End}(\Lambda) \cong \mathcal{O}}} (X - j(\Lambda)) \quad \in \mathbb{Z}[X]. \end{aligned}$$

$K(j(\tau)) = K_{\mathcal{O}}$; the *ring class field* of $\mathcal{O}$.

The CM method

Let $E/\mathbb{F}_q$ be an elliptic curve, and let $\pi = \mathrm{Frob}_q \in \mathrm{End}(E)$. Then $\pi^2 - t\pi + q = 0$.

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \implies t^2 - 4q = \mathrm{Disc}(\mathbb{Z}[\pi]) = u^2\,\mathrm{Disc}(\mathrm{End}(E)),$$

for some $u \in \mathbb{Z}$.

Algorithm (CM method)

Given q, t, find $E/\mathbb{F}_q$ with trace t.

1. Find $u \in \mathbb{Z}$ and $D < 0$ such that $u^2 D = t^2 - 4q$.
2. Compute the Hilbert class polynomial $H_D(X) \in \mathbb{Z}[X]$.
3. Extract a root $j \in \mathbb{F}_q$ of $H_D \pmod{p}$.
4. Output $E_j/\mathbb{F}_q$ with $j(E_j) = j$ (or twist).

Moreover, $E[\ell^\infty]$ is determined by $v_\ell(u)$.

Summary

Algorithm

1. Find all prime numbers $p \equiv 1 \pmod{N^4}$ up to a certain bound.
2. For each prime p, determine the roots j_i of the Hilbert class polynomials H_D modulo p for all discriminants of the form $u^2 D = t^2 - 4p = 2^2 - 4p,$ where $N^2 \mid u$.
3. Pick a nice model for $X_1(N)$, e.g. $F_N(b, c) = 0$ where b, c are the Tate normal form parameters.
4. For each root j_i, determine the $\mathcal{E} \in X_1(N)(\mathbb{F}_p)$ for which $j(\mathcal{E}) = j_i$.
5. For each such $\mathcal{E}$, if the corresponding curve has trace $+2$, determine $C_d(\mathcal{E}) \in \mathbb{F}_p$ for all $d \in \{0, \dots, N-1\}$.
6. For each d, determine $C_d \in \mathbb{F}_p(X_1(N))$ by rational interpolation.
7. Lift to $\mathbb{Q}(X_1(N))$ using the Chinese Remainder Theorem.

$\Longrightarrow$ extended the range of formulae from $N \leq 13$ to $N \leq 37$.

Optimizing the formulae

Previously, on radical 8-isogenies...

$$A' = \frac{-A^3+6A^2-12A+8}{A^2}\alpha^7 + \frac{4A^3-24A^2+48A-32}{A^3+4A^2-4A}\alpha^6 + \frac{-4A^3+24A^2-48A+32}{A^3+4A^2-4A}\alpha^5 + \frac{2A^3-12A^2+24A-16}{A^3+4A^2-4A}\alpha^4 + \frac{A-2}{A}\alpha^3 + \frac{-2A^2+4A}{A^2+4A-4}\alpha^2 + \frac{3A^2-4}{A^2+4A-4}\alpha + \frac{-A^2+2A}{A^2+4A-4},$$

where $\alpha = \sqrt[8]{(-A^3+A^2)/(A^4-8A^3+24A^2-32A+16)}$.

New radical 8-isogeny formula

$$A' = \frac{-2A(A-2)\alpha^2 - A(A-2)}{(A-2)^2\alpha^4 - A(A-2)\alpha^2 - A(A-2)\alpha + A},$$

where $\alpha = \sqrt[8]{-A^2(A-1)/(A-2)^4}$.

Walking horizontally

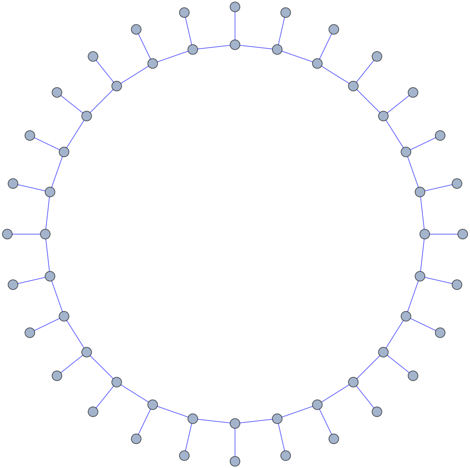


Figure: Connected component of a supersingular 2-isogeny graph over $\mathbb{F}_p$.

Benchmarks

1. Factor 3 speed-up for long chains of 2-isogenies over 512-bit prime fields.
2. 12% acceleration compared to previous implementation of CSIDH-512 using radical isogenies.

Thank you!