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

06/12/2022

Isogeny-based key exchanges

Based on class group actions

1. CRS (1997-2004)
2. CSIDH (2018)
3. OSIDH (2020)

Not based on class group actions

1. SIDH (2011)
2. B-SIDH (2020)

Isogeny-based key exchanges

Based on class group actions

1. CRS (1997-2004)
2. CSIDH (2018)
3. OSIDH (2020)

Not based on class group actions

1. SIDH (2011)
2. B-SIDH (2020)

1. pSIDH (2022)

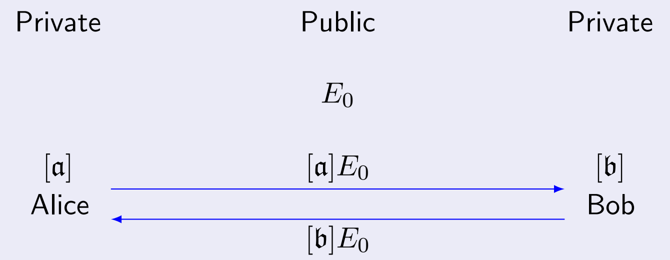
Key exchange from a class group action

Private	Public	Private
	E_0	
Alice		Bob

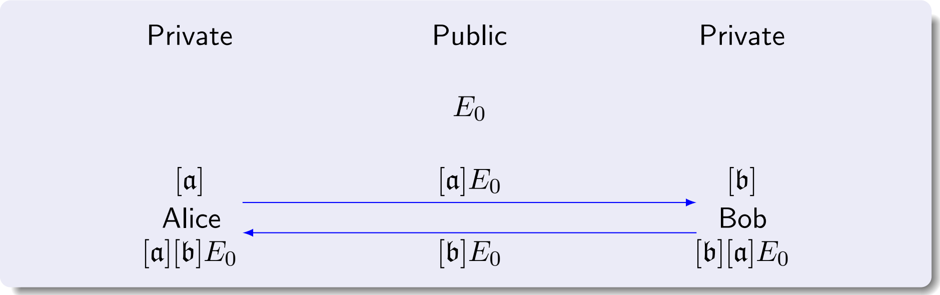
Key exchange from a class group action

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

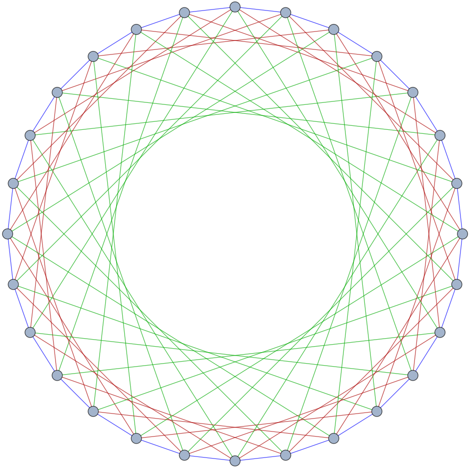
Key exchange from a class group action



Key exchange from a class group action

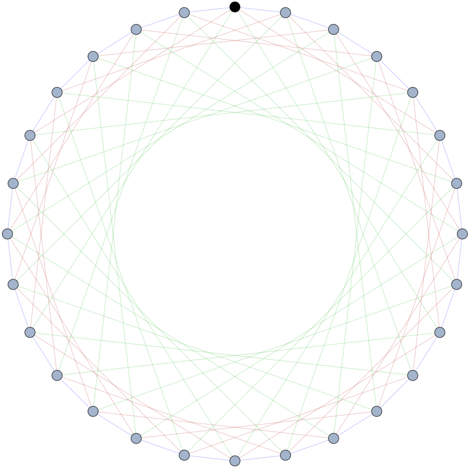


CSIDH

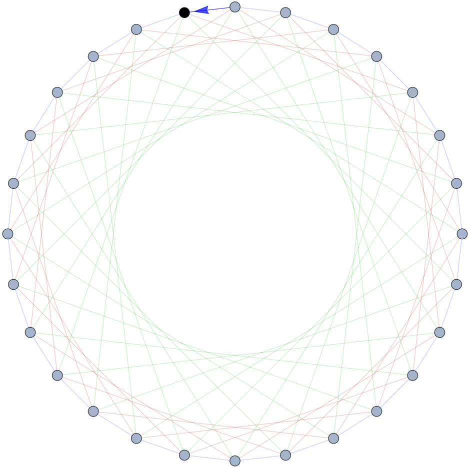


Connected component of a union of supersingular 3-, 5-, and 7-isogeny graphs over some prime field $\mathbb{F}_p$.

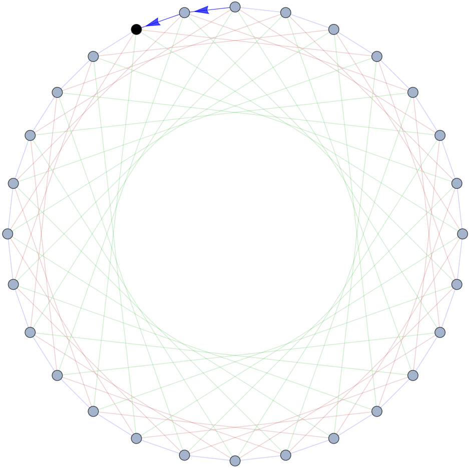
CSIDH



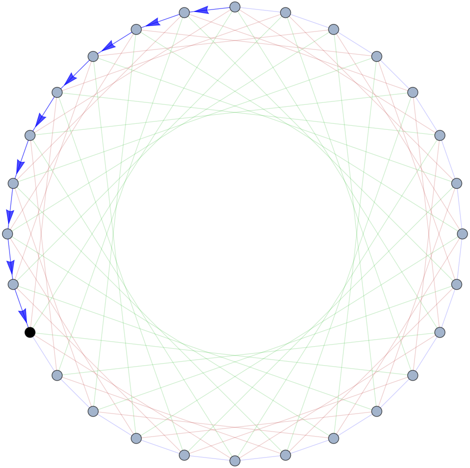
CSIDH



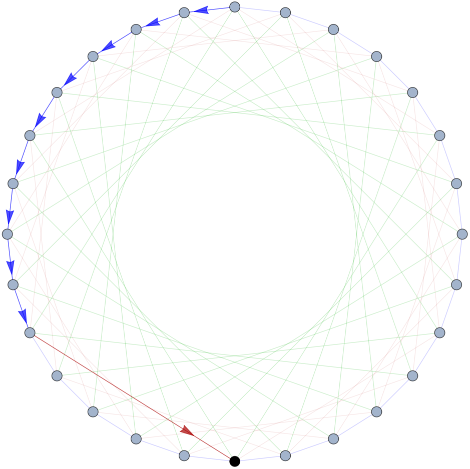
CSIDH



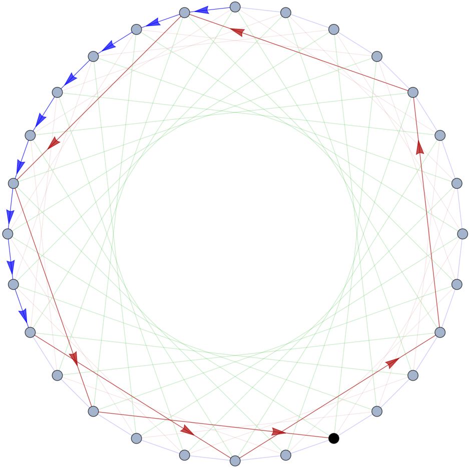
CSIDH



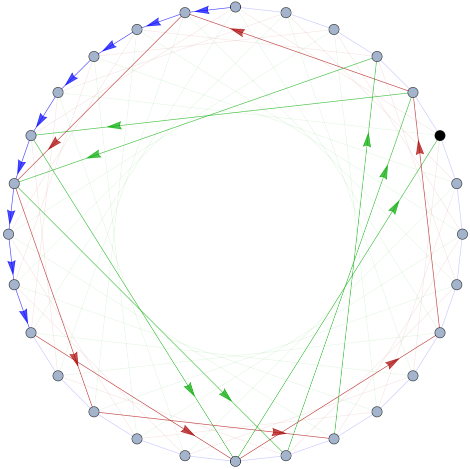
CSIDH



CSIDH



CSIDH



Computing a chain of N-isogenies

Problem

Given an 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.

Computing a chain of N-isogenies

Problem

Given an 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 Q on E', and hope that $P' = (\#E'/N)Q$ works.

Computing a chain of N-isogenies

Problem

Given an 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 Q on E', and hope that $P' = (\#E'/N)Q$ works.

Alternative solutions

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

Computing a chain of N-isogenies

Problem

Given an 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 Q on E', and hope that $P' = (\#E'/N)Q$ 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

Radical 5-isogenies

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

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

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 $E/\langle P\rangle$:

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

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 $E/\langle P \rangle$:

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

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 $\alpha = \sqrt[5]{b}$.

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 $E/\langle P \rangle$:

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

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

In general, we have the *Tate normal form*,

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

New method

In general, we have the *Tate normal form*,

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

For $\alpha = \sqrt[N]{t_N(P,P)}$, we can write

$$b' = \sum_{i=0}^{N-1} u_i(b,c)\alpha^i, \qquad c' = \sum_{i=0}^{N-1} v_i(b,c)\alpha^i.$$

New method

In general, we have the *Tate normal form*,

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

For $\alpha = \sqrt[N]{t_N(P,P)}$, we can write

$$b' = \sum_{i=0}^{N-1} u_i(b,c)\alpha^i, \qquad c' = \sum_{i=0}^{N-1} v_i(b,c)\alpha^i.$$

Idea

Determine $u_i(b,c), v_i(b,c)$ over many (smallish) fields $\mathbb{F}_p$ by rational interpolation, then lift to $\mathbb{Q}$ using CRT.

New method

In general, we have the *Tate normal form*,

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

For $\alpha = \sqrt[N]{t_N(P,P)}$, we can write

$$b' = \sum_{i=0}^{N-1} u_i(b,c)\alpha^i, \qquad c' = \sum_{i=0}^{N-1} v_i(b,c)\alpha^i.$$

Idea

Determine $u_i(b,c), v_i(b,c)$ over many (smallish) fields $\mathbb{F}_p$ by rational interpolation, then lift to $\mathbb{Q}$ using CRT.

$\Longrightarrow$ extended formulas from $N \leq 13$ to $N \leq 37$.

Optimizing the formulae

Optimizing the formulae

Previously, on radical 8-isogenies...

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

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

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

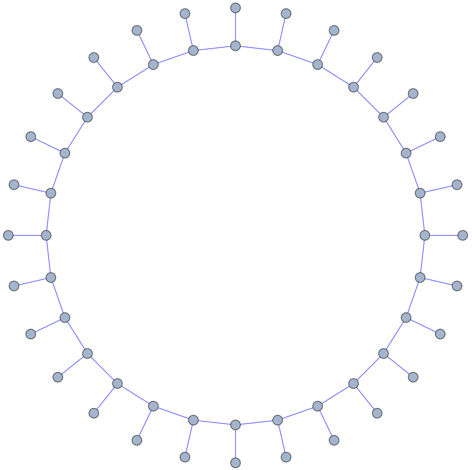


Figure: Connected component of a supersingular 2-isogeny graph over $\mathbb{F}_p$.

Benchmarks

1. Factor 3 improvement for chains of 2-isogenies over 512-bit prime fields.
2. 12% acceleration compared to CSURF-512.

Thank you!