Hash functions from superspecial genus-2 curves using Richelot isogenies

Wouter Castryck, **Thomas Decru**, and Benjamin Smith

NutMiC 2019, Paris

June 24, 2019

Background

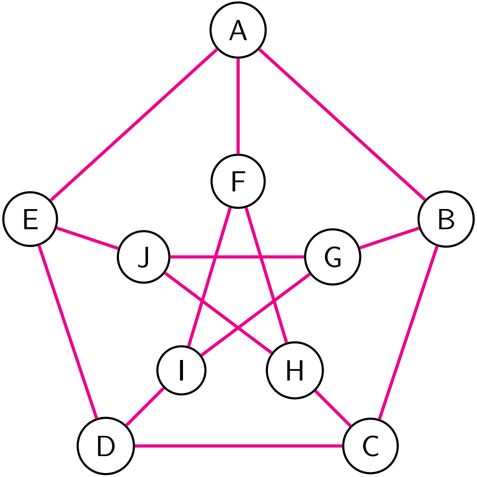
- 2006: hash functions based on supersingular elliptic curves (Charles, Goren, Lauter)
- 2011: key exchange protocol based on supersingular elliptic curves called SIDH (Jao, De Feo)

Background

- 2006: hash functions based on supersingular elliptic curves (Charles, Goren, Lauter)
- 2011: key exchange protocol based on supersingular elliptic curves called SIDH (Jao, De Feo)
- 2018: hash function based on supersingular genus-2 curves (Takashima)
- 2019: collisions in genus-2 hash, create genus-2 SIDH (Flynn, Ti)
- 2019: we fix collisions and smooth out a bunch of technicalities

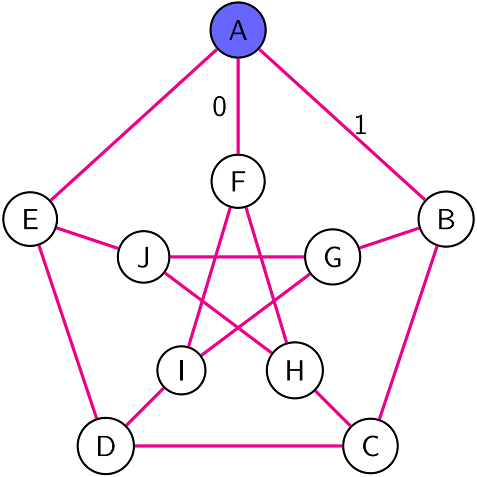
Hash functions from expander graph

Input: 110



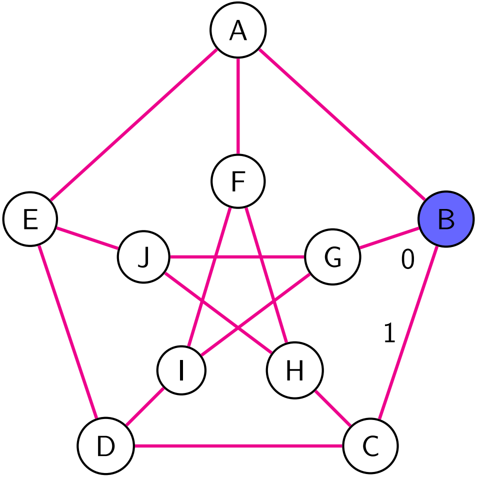
Hash functions from expander graph

Input: 110



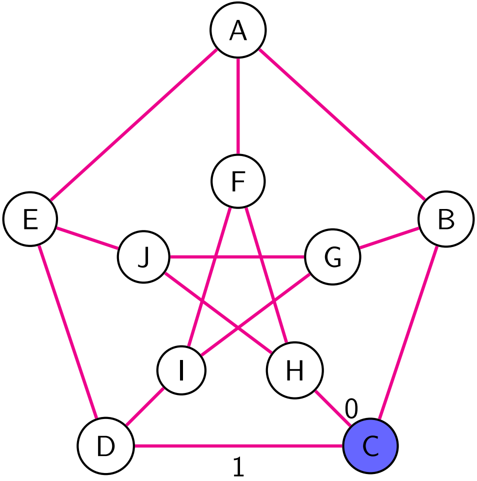
Hash functions from expander graph

Input: 110



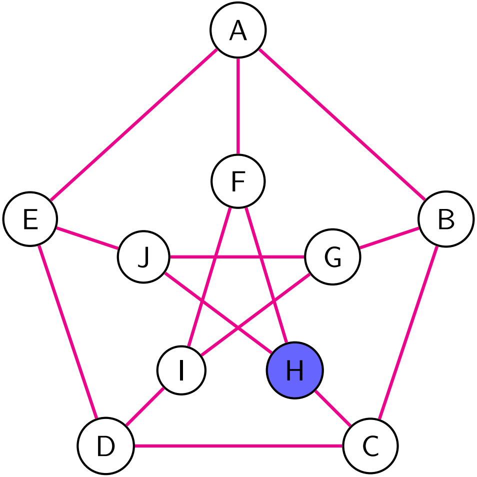
Hash functions from expander graph

Input: 110



Hash functions from expander graph

Input: 110; Output: H



Supersingular ℓ-isogeny graph over $\mathbb{F}_{p^2}$

Construct the graph $G(p, \ell)$ as follows:

- Vertices: all supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to $\cong$
- Edges: all ℓ-isogenies between them

Supersingular ℓ-isogeny graph over $\mathbb{F}_{p^2}$

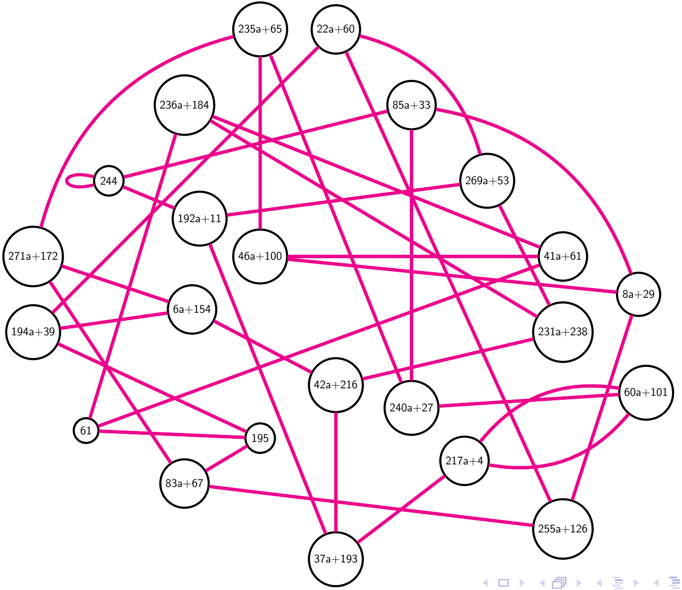
Construct the graph $G(p, \ell)$ as follows:

- Vertices: all supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to $\cong$
- Edges: all ℓ-isogenies between them

Some properties:

- Amount of vertices $\sim p/12$
- Good expander graph
- Every node has $\ell + 1$ edges

$G(277,2)$ with $\mathbb{F}_{277^2} \cong \mathbb{F}_{277}(a) \cong \mathbb{F}_{277}[x]/(x^2+274x+5)$



Security

Problem

Given two supersingular elliptic curves E and E' defined over $\mathbb{F}_{p^2}$, find an ℓ^k-isogeny between them.

Security

Problem

Given two supersingular elliptic curves E and E' defined over $\mathbb{F}_{p^2}$, find an ℓ^k-isogeny between them.

Problem

Given any supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, find a curve E' and two distinct isogenies of degree ℓ^k and $\ell^{k'}$ between them.

General idea

2-isogenies between supersingular elliptic curves

$$\downarrow$$

(2,2)-isogenies between principally polarized superspecial abelian surfaces

Elliptic curves

Definition

An elliptic curve, say E, over a field K of odd characteristic, is an algebraic curve defined by an equation of the form

$$E : y^2 = f(x),$$

where $f(x)$ is a squarefree polynomial in $K[x]$ of degree 3 or 4.

Genus two curves

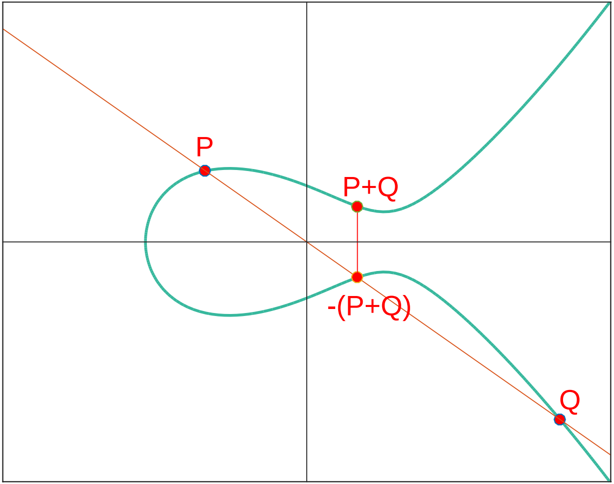
Definition

A hyperelliptic curve of genus two, say C, over a field K of odd characteristic, is an algebraic curve defined by an equation of the form

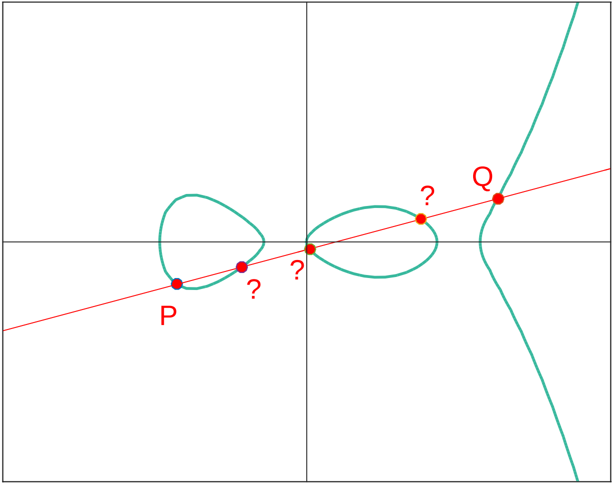
$$C : y^2 = f(x),$$

where $f(x)$ is a squarefree polynomial in $K[x]$ of degree 5 or 6.

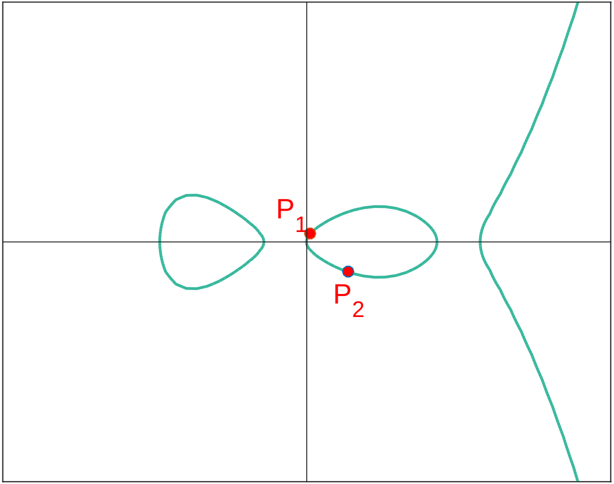
Elliptic curves group law



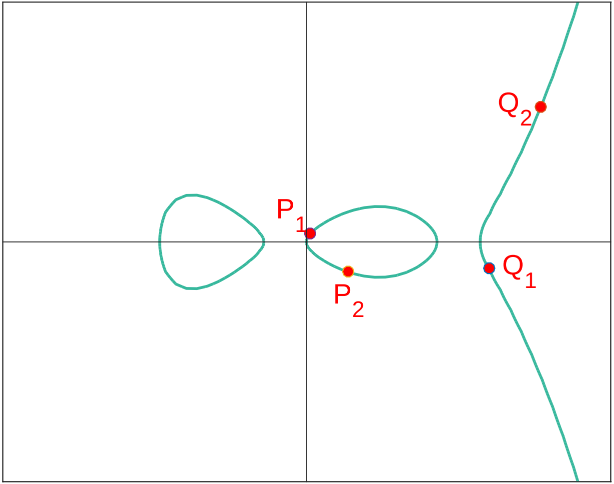
Genus two curves group law



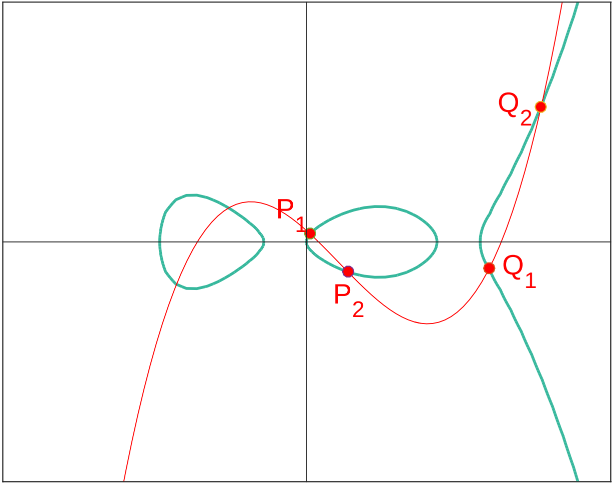
Genus two curves group law



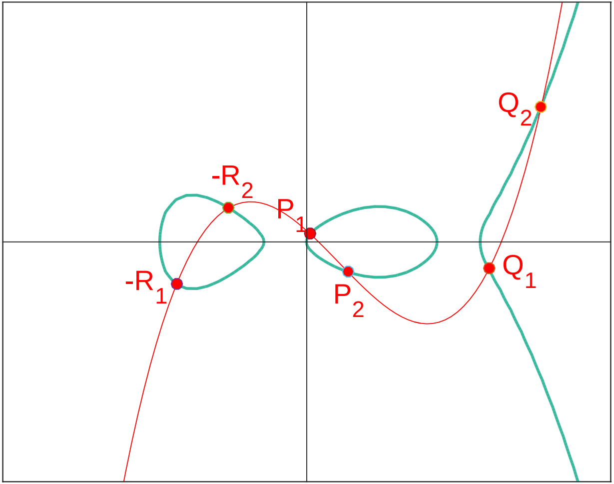
Genus two curves group law



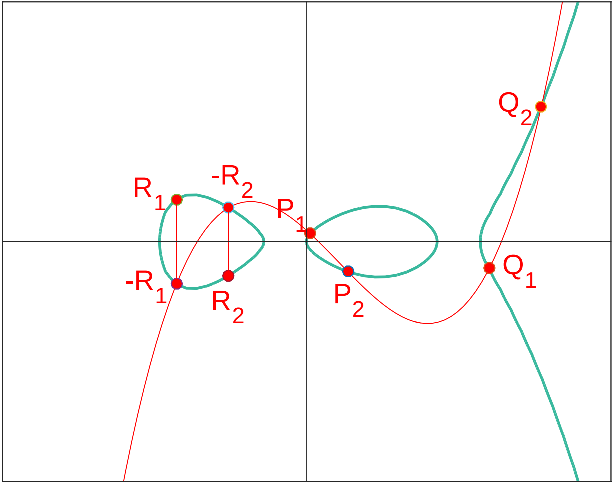
Genus two curves group law



Genus two curves group law



Genus two curves group law



Abelian surfaces

Definition

An **abelian surface** is a two-dimensional projective algebraic variety that is also an algebraic group.

Always isomorphic to one of the following:

- jacobian of a (hyperelliptic) genus-2 curve
- product of two elliptic curves

Principal polarization

Definition

A **principal polarization** is an isomorphism λ from an abelian variety A to its dual, which is of the form

$$\begin{aligned} \lambda_{\mathcal{L}} : A(\bar{k}) &\rightarrow \mathrm{Pic}(A) \\ a &\mapsto t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}, \end{aligned}$$

for some ample sheaf $\mathcal{L}$ on $A(\bar{k})$.

Principal polarization

Definition

~~A **principal polarization** is an isomorphism λ from an abelian variety A to its dual, which is of the form~~

$$\cancel{\begin{array}{rcl} \lambda_{\mathcal{L}} : A(\bar{k}) & \to & Pic(A) \\ a & \mapsto & t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}, \end{array}}$$

~~for some ample sheaf $\mathcal{L}$ on $A(\bar{k})$.~~

Read: we have equations!

- $y^2 = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$
- $(y^2 = x^3 + b_1x + b_0) \times (y^2 = x^3 + c_1x + c_0)$

Supersingular elliptic curves

E is supersingular iff

- the p-torsion of E is trivial,

Supersingular elliptic curves

E is supersingular iff

- the p-torsion of E is trivial,
- or $\mathrm{End}(E)$ is an order in a quaternion algebra,

Supersingular elliptic curves

E is supersingular iff

- the p-torsion of E is trivial,
- or $\mathrm{End}(E)$ is an order in a quaternion algebra,
- or the trace of Frobenius is divisible by p,

Supersingular elliptic curves

E is supersingular iff

- the p-torsion of E is trivial,
- or $\mathrm{End}(E)$ is an order in a quaternion algebra,
- or the trace of Frobenius is divisible by p,
- or the Newton polygon is a straight line segment with slope $1/2$,

Supersingular elliptic curves

E is supersingular iff

- the p-torsion of E is trivial,
- or $\mathrm{End}(E)$ is an order in a quaternion algebra,
- or the trace of Frobenius is divisible by p,
- or the Newton polygon is a straight line segment with slope $1/2$,
- or the dual of Frobenius is purely inseparable,

Supersingular elliptic curves

E is supersingular iff

- the p-torsion of E is trivial,
- or $\mathrm{End}(E)$ is an order in a quaternion algebra,
- or the trace of Frobenius is divisible by p,
- or the Newton polygon is a straight line segment with slope $1/2$,
- or the dual of Frobenius is purely inseparable,
- or the Hasse invariant is 0,
- $\ldots$

Superspecial genus two curves

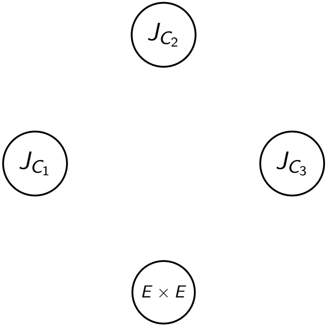
Definition

A p.p. abelian surface defined over a field with characteristic p is **superspecial** if the Hasse invariant is zero.

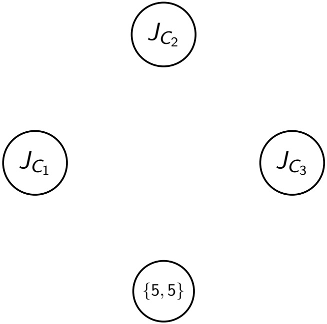
Why?

- Finite amount $\sim p^3/2880$
- All defined over $\mathbb{F}_{p^2}$

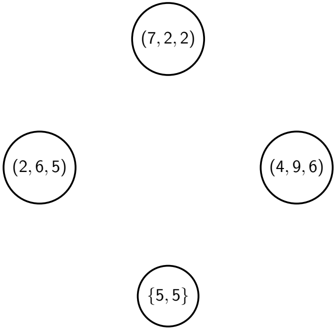
Superspecial abelian surfaces over $\mathbb{F}_{13^2}$



Superspecial abelian surfaces over $\mathbb{F}_{13^2}$



Superspecial abelian surfaces over $\mathbb{F}_{13^2}$



$(2,2)$-isogenies

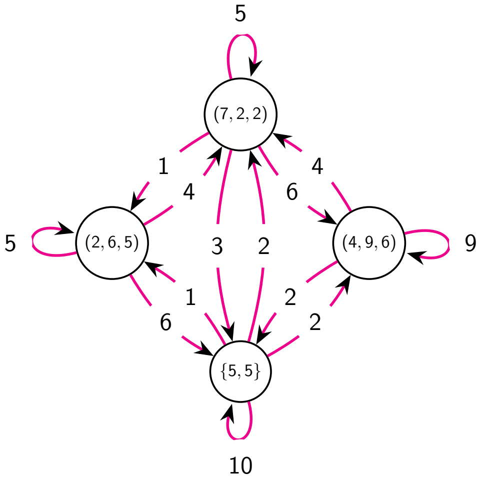
Definition

A $(2,2)$-**isogeny** ϕ is an isogeny such that $\ker\phi \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $\ker\phi$ is maximal isotropic with regards to the 2-Weil pairing.

Remark: there are 15 of these $(2,2)$-isogenies for every A, and at least 9 are to the same type of abelian surface, so

$$J_C \to J_{C'} \text{ or } E_1 \times E_2 \to E_1' \times E_2'$$

Superspecial p.p. abelian surface $(2,2)$-isogeny graph over $\mathbb{F}_{13^2}$



Superspecial p.p. abelian surface $(2,2)$-isogeny graph over $\mathbb{F}_{p^2}$

Isogeny graph $\mathcal{G}_p$:

- Vertices: all p.p. superspecial abelian surfaces over $\mathbb{F}_{p^2}$ up to isomorphism
  - genus-2 curves: absolute Igusa invariants $(j_1, j_2, j_3) \in \mathbb{F}_{p^2}^3$
  - products of elliptic curves: j-invariants $\{j_1, j_2\} \subset \mathbb{F}_{p^2}$
- Edges: all $(2,2)$-isogenies between them

Superspecial p.p. abelian surface $(2,2)$-isogeny graph over $\mathbb{F}_{p^2}$

Isogeny graph $\mathcal{G}_p$:

- Vertices: all p.p. superspecial abelian surfaces over $\mathbb{F}_{p^2}$ up to isomorphism
  - genus-2 curves: absolute Igusa invariants $(j_1, j_2, j_3) \in \mathbb{F}_{p^2}^3$
  - products of elliptic curves: j-invariants $\{j_1, j_2\} \subset \mathbb{F}_{p^2}$
- Edges: all $(2,2)$-isogenies between them

Intuitively:

- Interior of $\mathcal{G}_p$: $\sim p^3/2880$ genus-2 curves
- Boundary of $\mathcal{G}_p$: $\sim p^2/288$ products of elliptic curves

Restrict to jacobians of genus-2 curves

Ignore products of elliptic curves:

- $\mathcal{O}(1/p)$ chance of encountering
- formulas are less efficient
- what would output be? $\{j_1, j_2\}$ vs (j_1, j_2, j_3)

Richelot isogenies

$$C_0 : y^2 = \underbrace{(x-\alpha_1)(x-\alpha_2)}_{G_1}\underbrace{(x-\alpha_3)(x-\alpha_4)}_{G_2}\underbrace{(x-\alpha_5)(x-\alpha_6)}_{G_3}$$

Richelot isogenies

$$C_0 : y^2 = \underbrace{(x-\alpha_1)(x-\alpha_2)}_{G_1}\underbrace{(x-\alpha_3)(x-\alpha_4)}_{G_2}\underbrace{(x-\alpha_5)(x-\alpha_6)}_{G_3}$$

Take $\phi_1 : J_{C_0} \to J_{C_1}$ the $(2,2)$-isogeny with kernel

$$\{0, [(\alpha_1, 0) - (\alpha_2, 0)], [(\alpha_3, 0) - (\alpha_4, 0)], [(\alpha_5, 0) - (\alpha_6, 0)]\}$$

Richelot isogenies

$$C_0 : y^2 = \underbrace{(x-\alpha_1)(x-\alpha_2)}_{G_1}\underbrace{(x-\alpha_3)(x-\alpha_4)}_{G_2}\underbrace{(x-\alpha_5)(x-\alpha_6)}_{G_3}$$

Take $\phi_1 : J_{C_0} \to J_{C_1}$ the $(2,2)$-isogeny with kernel

$$\{0, [(\alpha_1,0)-(\alpha_2,0)], [(\alpha_3,0)-(\alpha_4,0)], [(\alpha_5,0)-(\alpha_6,0)]\}$$

$$\rightsquigarrow C_1 : y^2 = \delta^{-1}\underbrace{(G_2'G_3 - G_2G_3')}_{H_1}\underbrace{(G_3'G_1 - G_3G_1')}_{H_2}\underbrace{(G_1'G_2 - G_1G_2')}_{H_3}$$

Avoiding dual isogeny

Continuing with $y^2 = H_1 H_2 H_3$ gives the dual isogeny $\hat{\phi}_1$ and the composition is a $(2, 2, 2, 2)$-isogeny:

$$\begin{tikzcd} A_0 \arrow[r, bend left, "\phi_1"] & A_1 \arrow[l, bend left, "\hat{\phi}_1"] \end{tikzcd}$$

Avoiding small cycles

Continuing with one factor fixed, e.g. $y^2 = H_1\tilde{H}_2\tilde{H}_3$, gives a $(2,2)$-isogeny ϕ_2, with a composed $(4,2,2)$-isogeny:

$$A_0 \xrightarrow{\phi_1} A_1 \xrightarrow{\phi_2} A_2$$

Avoiding small cycles

Continuing with one factor fixed, e.g. $y^2 = H_1\tilde{H}_2\tilde{H}_3$, gives a $(2,2)$-isogeny ϕ_2, with a composed $(4,2,2)$-isogeny:

$$\begin{tikzcd}
 & A_1' \arrow[dr, "\phi_2'"] & \\
A_0 \arrow[ur, "\phi_1'"] \arrow[r, "\phi_1"] \arrow[dr, "\phi_1''"'] & A_1 \arrow[r, "\phi_2"] & A_2 \\
 & A_1'' \arrow[ur, "\phi_2''"'] &
\end{tikzcd}$$

Good isogeny extensions

Write $H_1 = L_1 L_2$, $H_2 = L_3 L_4$, $H_3 = L_5 L_6$ then the good extensions of ϕ_1 are determined by the quadratic factors

$$\begin{array}{ll}
(L_1 L_3, L_2 L_5, L_4 L_6), & (L_1 L_3, L_2 L_6, L_4 L_5), \\
(L_1 L_4, L_2 L_5, L_3 L_6), & (L_1 L_4, L_2 L_6, L_3 L_5), \\
(L_1 L_5, L_2 L_3, L_4 L_6), & (L_1 L_5, L_2 L_4, L_3 L_6), \\
(L_1 L_6, L_2 L_3, L_4 L_5), & (L_1 L_6, L_2 L_4, L_3 L_5).
\end{array}$$

Composing gives a $(4, 4)$-isogeny.

Security

Problem

Given two superspecial genus-2 curves C_1 and C_2 defined over $\mathbb{F}_{p^2}$, find a $(2^k, 2^k)$-isogeny between their jacobians.

Security

Problem

Given two superspecial genus-2 curves C_1 and C_2 defined over $\mathbb{F}_{p^2}$, find a $(2^k, 2^k)$-isogeny between their jacobians.

Problem

Given any superspecial genus-2 curve C_1 defined over $\mathbb{F}_{p^2}$, find

1. *a curve C_2 and a $(2^k, 2^k)$-isogeny $J_{C_1} \to J_{C_2}$,*
2. *a curve C_2' and a $(2^{k'}, 2^{k'})$-isogeny $J_{C_1} \to J_{C_2'}$,*

such that C_2 and C_2' are $\overline{\mathbb{F}}_p$-isomorphic.

Concluding remarks

Advantages:

- Processing 3 bits at once, with possible parallelization of 3 square root extractions
- Elliptic curves graph size $\mathcal{O}(p)$
  Genus-2 curves graph size $\mathcal{O}(p^3)$

  $\Rightarrow$ same security in smaller fields, e.g. $p \approx 2^{86}$ vs $p \approx 2^{256}$

Concluding remarks

Advantages:

- Processing 3 bits at once, with possible parallelization of 3 square root extractions
- Elliptic curves graph size $\mathcal{O}(p)$
  Genus-2 curves graph size $\mathcal{O}(p^3)$

  $\Rightarrow$ same security in smaller fields, e.g. $p \approx 2^{86}$ vs $p \approx 2^{256}$

Future research:

- Practical genus-2 SIDH key exchange?
- Expander properties of $\mathcal{G}_p$?