An Algorithmic Approach to $(2,2)$-isogenies in the Theta Model and Applications to Isogeny-based Cryptography

Pierrick Dartois, Luciano Maino, Giacomo Pope and Damien Robert

Asiacrypt 2024

12th December, 2024

Motivation

- SIDH attacks relied on the computation of chains of 2-isogenies between elliptic products.
  - $\hookrightarrow$ In dimension two: Richelot formulae and specific algorithms for gluing and splitting.
- SIDH attacks have introduced a new representation for isogenies between elliptic curves.
  - $\hookrightarrow$ KEMs: FESTA and QFESTA.
  - $\hookrightarrow$ SQIsign variants.

Motivation

- SIDH attacks relied on the computation of chains of 2-isogenies between elliptic products.
  - ↪ In dimension two: Richelot formulae and specific algorithms for gluing and splitting.
- SIDH attacks have introduced a new representation for isogenies between elliptic curves.
  - ↪ KEMs: FESTA and QFESTA.
  - ↪ SQIsign variants.

Problem

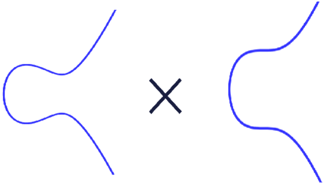
We needed a faster way to compute $(2,2)$-isogenies between elliptic products.

Background

- The correct higher-dimensional generalisation of elliptic curves is *principally polarised abelian varieties*.

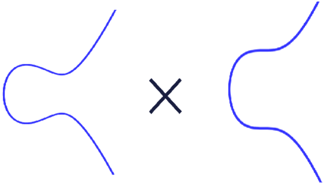
Background

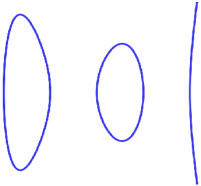
- The correct higher-dimensional generalisation of elliptic curves is *principally polarised abelian varieties.*
- In dimension two, we have *principally polarised abelian surfaces* (PPASes).
  - Products of elliptic curves,



Background

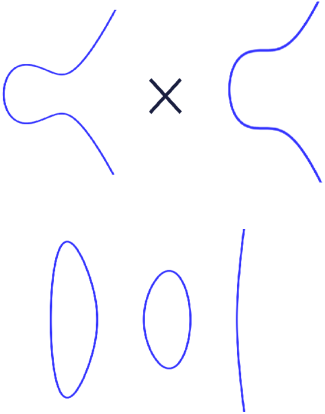
- The correct higher-dimensional generalisation of elliptic curves is *principally polarised abelian varieties*.
- In dimension two, we have *principally polarised abelian surfaces* (PPASes).
  - Products of elliptic curves,
  - Jacobians of genus-2 curves.





Background

- The correct higher-dimensional generalisation of elliptic curves is *principally polarised abelian varieties.*
- In dimension two, we have *principally polarised abelian surfaces* (PPASes).
  - Products of elliptic curves,
  - Jacobians of genus-2 curves.
- Isogenies between PPASes have kernels of rank two.
- An (N, N)-isogeny is an isogeny between PPASes whose kernel $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.



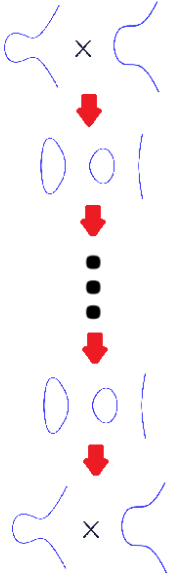
Chains of $(2,2)$-isogenies between elliptic products

Goal: Compute the $(2^n, 2^n)$-isogeny $\Phi : E_1 \times E_2 \to E_1' \times E_2'$

Chains of $(2,2)$-isogenies between elliptic products

Goal: Compute the $(2^n, 2^n)$-isogeny $\Phi : E_1 \times E_2 \to E_1' \times E_2'$
We compute Φ as a chain of $(2,2)$-isogenies:

$$\Phi = \Phi_n \circ \ldots \circ \Phi_1$$

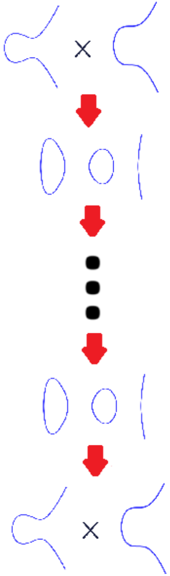


Chains of $(2,2)$-isogenies between elliptic products

Goal: Compute the $(2^n, 2^n)$-isogeny $\Phi : E_1 \times E_2 \to E_1' \times E_2'$
We compute Φ as a chain of $(2,2)$-isogenies:

$$\Phi = \Phi_n \circ \ldots \circ \Phi_1$$

- Gluing isogeny $\Phi_1 : E_1 \times E_2 \to \mathsf{Jac}(\mathcal{C})$ (Howe, Leprévost, and Poonen, 2000).
- Splitting Isogeny $\Phi_n : \mathsf{Jac}(\mathcal{C}) \to E_1' \times E_2'$ (Smith, 2005).
- Richelot Isogenies $\Phi_i : \mathsf{Jac}(\mathcal{C}_i) \to \mathsf{Jac}(\mathcal{C}_{i+1})$, for $i = 2, \ldots, n-1$ (Smith, 2005).



Efficient formulae for $(2, 2)$-isogenies

- Represent PPASes via the *theta model*.
- Very efficient formulae to perform arithmetic.
- We adapt these formulae to our use case.
- Compared to the state of the art:
  - Codomain computation is **ten** times faster.
  - Isogeny evaluation is **twenty** times faster.
- We can now compute "cryptographic-size" isogenies in matter of ms.

Theta structures

Let $\mathcal{A}$ be a principally polarised abelian surface.

Theta structures

Let $\mathcal{A}$ be a principally polarised abelian surface.
Let $\mathcal{A}[4] = \langle S_1', S_2' \rangle \oplus \langle T_1', T_2' \rangle$ be a symplectic 4-torsion basis

- $e(S_1', T_1') = e(S_2', T_2') = \mu$,
- $e(S_1', S_2') = e(T_1', T_2') = e(S_1', T_2') = e(S_2', T_1') = 1$.

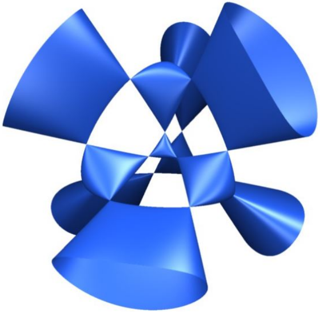
Theta structures

Let $\mathcal{A}$ be a principally polarised abelian surface.
Let $\mathcal{A}[4] = \langle S_1', S_2' \rangle \oplus \langle T_1', T_2' \rangle$ be a symplectic 4-torsion basis

- $e(S_1', T_1') = e(S_2', T_2') = \mu$,
- $e(S_1', S_2') = e(T_1', T_2') = e(S_1', T_2') = e(S_2', T_1') = 1$.

$\langle S_1', S_2' \rangle \oplus \langle T_1', T_2' \rangle \rightsquigarrow \theta_{00}, \theta_{10}, \theta_{01}, \theta_{11}$

$$P \in \mathcal{A} \to (\theta_{00}(P) : \theta_{10}(P) : \theta_{01}(P) : \theta_{11}(P)) \in \mathbb{P}^3$$



Taken from nLab.

Theta structures

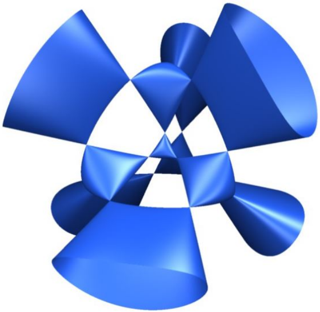
Let $\mathcal{A}$ be a principally polarised abelian surface.
Let $\mathcal{A}[4] = \langle S_1', S_2' \rangle \oplus \langle T_1', T_2' \rangle$ be a symplectic 4-torsion basis

- $e(S_1', T_1') = e(S_2', T_2') = \mu$,
- $e(S_1', S_2') = e(T_1', T_2') = e(S_1', T_2') = e(S_2', T_1') = 1$.

$\langle S_1', S_2' \rangle \oplus \langle T_1', T_2' \rangle \rightsquigarrow \theta_{00}, \theta_{10}, \theta_{01}, \theta_{11}$

$$P \in \mathcal{A} \to (\theta_{00}(P) : \theta_{10}(P) : \theta_{01}(P) : \theta_{11}(P)) \in \mathbb{P}^3$$

The projective point $(\theta_{00}(0) : \theta_{10}(0) : \theta_{01}(0) : \theta_{11}(0))$ is enough to describe $\mathcal{A}$.



Taken from nLab.

Some operators

The Hadamard transform

$$\mathcal{H}(x, y, z, w) := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$$

We define $(\tilde{\theta}_{00}(P) : \tilde{\theta}_{10}(P) : \tilde{\theta}_{01}(P) : \tilde{\theta}_{11}(P)) = \mathcal{H}\left(\theta_{00}(P), \theta_{10}(P), \theta_{01}(P), \theta_{11}(P)\right)$ to be the *dual coordinates* of P.
Also $\mathcal{H} \circ \mathcal{H}(x, y, z, w) = (x, y, z, w)$.

Some operators

The Hadamard transform

$$\mathcal{H}(x,y,z,w) := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$$

We define $(\tilde{\theta}_{00}(P) : \tilde{\theta}_{10}(P) : \tilde{\theta}_{01}(P) : \tilde{\theta}_{11}(P)) = \mathcal{H}\left(\theta_{00}(P), \theta_{10}(P), \theta_{01}(P), \theta_{11}(P)\right)$ to be the *dual coordinates* of P.

Also $\mathcal{H} \circ \mathcal{H}(x,y,z,w) = (x,y,z,w)$.

The squaring operator:

$$\mathcal{S}(x,y,z,w) := (x^2, y^2, z^2, w^2).$$

Some operators

The Hadamard transform

$$\mathcal{H}(x,y,z,w) := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$$

We define $(\tilde{\theta}_{00}(P) : \tilde{\theta}_{10}(P) : \tilde{\theta}_{01}(P) : \tilde{\theta}_{11}(P)) = \mathcal{H}\left(\theta_{00}(P), \theta_{10}(P), \theta_{01}(P), \theta_{11}(P)\right)$ to be the *dual coordinates* of P.
Also $\mathcal{H} \circ \mathcal{H}(x,y,z,w) = (x,y,z,w)$.
The squaring operator:

$$\mathcal{S}(x,y,z,w) := (x^2, y^2, z^2, w^2).$$

The $\star$ operator:

$$(x,y,z,w) \star (x', y', z', w') = (xx', yy', zz', ww').$$

Duplication formula

Let $\mathcal{A}[4] = \langle S_1', S_2' \rangle \oplus \langle T_1', T_2' \rangle$ be a symplectic 4-torsion basis.

Duplication formula

Let $\mathcal{A}[4] = \langle S_1', S_2' \rangle \oplus \langle T_1', T_2' \rangle$ be a symplectic 4-torsion basis.
Let $\Phi : \mathcal{A} \to \mathcal{B}$, $\ker \Phi = \langle T_1, T_2 \rangle$, where $T_i = [2]T_i'$.
For all $P, Q \in \mathcal{A}$

$$\left(\theta_i^{\mathcal{A}}(P+Q)\right)_i \star \left(\theta_i^{\mathcal{A}}(P-Q)\right)_i = \mathcal{H}\left(\left(\tilde{\theta}_i^{\mathcal{B}}(\Phi(P))\right)_i \star \left(\tilde{\theta}_i^{\mathcal{B}}(\Phi(Q))\right)_i\right).$$

Duplication formula

Let $\mathcal{A}[4] = \langle S_1', S_2' \rangle \oplus \langle T_1', T_2' \rangle$ be a symplectic 4-torsion basis.
Let $\Phi : \mathcal{A} \to \mathcal{B}$, $\ker \Phi = \langle T_1, T_2 \rangle$, where $T_i = [2]T_i'$.
For all $P, Q \in \mathcal{A}$

$$\left(\theta_i^{\mathcal{A}}(P+Q)\right)_i \star \left(\theta_i^{\mathcal{A}}(P-Q)\right)_i = \mathcal{H}\left(\left(\tilde{\theta}_i^{\mathcal{B}}(\Phi(P))\right)_i \star \left(\tilde{\theta}_i^{\mathcal{B}}(\Phi(Q))\right)_i\right).$$

We can obtain addition formulae:

- Differential addition: $8\mathbf{S} + 17\mathbf{M}$,
- Doubling: $8\mathbf{S} + 6\mathbf{M}$.

The same formulae as in (Gaudry, 2005).

The isogeny formula

Goal: To compute the isogeny $\Phi : \mathcal{A} \to \mathcal{B}$ with $\ker \Phi = \langle T_1, T_2 \rangle$, where $T_i = [2]T_i'$.

The isogeny formula

Goal: To compute the isogeny $\Phi : \mathcal{A} \to \mathcal{B}$ with $\ker \Phi = \langle T_1, T_2 \rangle$, where $T_i = [2]T_i'$.
Assume that we have an isotropic group $\langle T_1'', T_2'' \rangle$ such that $T_i' = [2]T_i''$.

The isogeny formula

Goal: To compute the isogeny $\Phi : \mathcal{A} \to \mathcal{B}$ with $\ker \Phi = \langle T_1, T_2 \rangle$, where $T_i = [2]T_i'$.
Assume that we have an isotropic group $\langle T_1'', T_2'' \rangle$ such that $T_i' = [2]T_i''$.
Define $(\alpha : \beta : \gamma : \delta) = (\tilde{\theta}^{\mathcal{B}}_{00}(0) : \tilde{\theta}^{\mathcal{B}}_{10}(0) : \tilde{\theta}^{\mathcal{B}}_{01}(0) : \tilde{\theta}^{\mathcal{B}}_{11}(0))$.

Goal: To compute the isogeny $\Phi : \mathcal{A} \to \mathcal{B}$ with $\ker \Phi = \langle T_1, T_2 \rangle$, where $T_i = [2]T_i'$.
Assume that we have an isotropic group $\langle T_1'', T_2'' \rangle$ such that $T_i' = [2]T_i''$.
Define $(\alpha : \beta : \gamma : \delta) = (\tilde{\theta}_{00}^{\mathcal{B}}(0) : \tilde{\theta}_{10}^{\mathcal{B}}(0) : \tilde{\theta}_{01}^{\mathcal{B}}(0) : \tilde{\theta}_{11}^{\mathcal{B}}(0))$.
One can prove:

$$\mathcal{H} \circ \mathcal{S}(\theta_{00}^{\mathcal{A}}(T_1''), \theta_{10}^{\mathcal{A}}(T_1''), \theta_{01}^{\mathcal{A}}(T_1''), \theta_{11}^{\mathcal{A}}(T_1'')) = (x\alpha, x\beta, y\gamma, y\delta),$$
$$\mathcal{H} \circ \mathcal{S}(\theta_{00}^{\mathcal{A}}(T_2''), \theta_{10}^{\mathcal{A}}(T_2''), \theta_{01}^{\mathcal{A}}(T_2''), \theta_{11}^{\mathcal{A}}(T_2'')) = (z\alpha, w\beta, z\gamma, w\delta),$$

for some unknown x, y, z, w.

The isogeny formula

Goal: To compute the isogeny $\Phi : \mathcal{A} \to \mathcal{B}$ with $\ker \Phi = \langle T_1, T_2 \rangle$, where $T_i = [2]T_i'$.
Assume that we have an isotropic group $\langle T_1'', T_2'' \rangle$ such that $T_i' = [2]T_i''$.
Define $(\alpha : \beta : \gamma : \delta) = (\tilde{\theta}_{00}^{\mathcal{B}}(0) : \tilde{\theta}_{10}^{\mathcal{B}}(0) : \tilde{\theta}_{01}^{\mathcal{B}}(0) : \tilde{\theta}_{11}^{\mathcal{B}}(0))$.
One can prove:

$$\mathcal{H} \circ \mathcal{S}(\theta_{00}^{\mathcal{A}}(T_1''), \theta_{10}^{\mathcal{A}}(T_1''), \theta_{01}^{\mathcal{A}}(T_1''), \theta_{11}^{\mathcal{A}}(T_1'')) = (x\alpha, x\beta, y\gamma, y\delta),$$
$$\mathcal{H} \circ \mathcal{S}(\theta_{00}^{\mathcal{A}}(T_2''), \theta_{10}^{\mathcal{A}}(T_2''), \theta_{01}^{\mathcal{A}}(T_2''), \theta_{11}^{\mathcal{A}}(T_2'')) = (z\alpha, w\beta, z\gamma, w\delta),$$

for some unknown x, y, z, w.
Hence, we can recover the dual theta-null point $(\alpha : \beta : \gamma : \delta)$ for $\mathcal{B}$, and in turn the theta-null point $\mathcal{H}(\alpha : \beta : \gamma : \delta)$ on $\mathcal{B}$.

Operation counting

Isogeny Type	Doubling	Codomain		Evaluation
		Precomputations	Codomain	
Normalised	$8\mathbf{S} + 6\mathbf{M}$	$4\mathbf{S} + 24\mathbf{M} + 1\mathbf{I}$	$8\mathbf{S} + 10\mathbf{M} + 1\mathbf{I}$	$4\mathbf{S} + 3\mathbf{M}$
Projective	$8\mathbf{S} + 8\mathbf{M}$	$5\mathbf{S} + 14\mathbf{M}$	$8\mathbf{S} + 7\mathbf{M}$	$4\mathbf{S} + 4\mathbf{M}$
Gluing	$12\mathbf{S} + 12\mathbf{M}$	—	$8\mathbf{S} + 13\mathbf{M} + 1\mathbf{I}$	$8\mathbf{S} + 10\mathbf{M} + 1\mathbf{I}$

Details I skated over

- The formulae I showed assume we have T_1'' and T_2'' such that $\ker(\Phi) = [4]\langle T_1'', T_2'' \rangle$.
- The correction formula requires $100\mathbf{M} + 8\mathbf{S} + 4\mathbf{I}$
- At the end of the chain, we are left with an elliptic product in theta coordinates.
- Switching to the Montgomery model for the two curves is not expensive.

Performance

Table 1: Running times of computing the codomain and evaluating a $(2^n, 2^n)$-isogeny between elliptic products over the base field $\mathbb{F}_{p^2}$. Times were recorded on a Intel Core i7-9750H CPU with a clock-speed of 2.6 GHz with turbo-boost disabled.

		Codomain			Evaluation		
$\log p$	n	Theta Rust	Theta SageMath	Richelot SageMath	Theta Rust	Theta SageMath	Richelot SageMath
254	126	**2.13 ms**	108 ms	1028 ms	**161 μs**	5.43 ms	114 ms
381	208	**9.05 ms**	201 ms	1998 ms	**411 μs**	8.68 ms	208 ms
1293	632	**463 ms**	1225 ms	12840 ms	**17.8 ms**	40.8 ms	1203 ms

Conclusion

- We have shown formulae to compute $(2^n, 2^n)$-isogenies between elliptic products.
- Significant improvements in isogeny-based cryptography.
- Generalisation to four-dimensional elliptic products (Dartois, 2024).

Thanks for your attention!

Questions?

An example – Elliptic products

Elliptic curves

In the case of an elliptic curve E:

$$P \in E \to (\theta_0(P) : \theta_1(P)) \in \mathbb{P}^1.$$

An example – Elliptic products

Elliptic curves

In the case of an elliptic curve E:

$$P \in E \to (\theta_0(P) : \theta_1(P)) \in \mathbb{P}^1.$$

Consider $E : y^2 = x^3 + Ax^2 + x$ and let α be a solution of $\alpha + 1/\alpha = A$.

An example – Elliptic products

Elliptic curves

In the case of an elliptic curve E:

$$P \in E \to (\theta_0(P) : \theta_1(P)) \in \mathbb{P}^1.$$

Consider $E : y^2 = x^3 + Ax^2 + x$ and let α be a solution of $\alpha + 1/\alpha = A$.
Define $a = \sqrt{1+\alpha}$ and $b = \sqrt{\alpha - 1}$.

$$E \rightsquigarrow (a : b) \in \mathbb{P}^1$$

An example – Elliptic products

Elliptic curves

In the case of an elliptic curve E:

$$P \in E \to (\theta_0(P) : \theta_1(P)) \in \mathbb{P}^1.$$

Consider $E : y^2 = x^3 + Ax^2 + x$ and let α be a solution of $\alpha + 1/\alpha = A$.
Define $a = \sqrt{1+\alpha}$ and $b = \sqrt{\alpha - 1}$.

$$E \rightsquigarrow (a : b) \in \mathbb{P}^1$$

$$P = (X : Z) \mapsto (\theta_0(P) : \theta_1(P)) = (a(X-Z) : b(X+Z))$$

An example – Elliptic products

Elliptic curves

In the case of an elliptic curve E:

$$P \in E \to (\theta_0(P) : \theta_1(P)) \in \mathbb{P}^1.$$

Consider $E : y^2 = x^3 + Ax^2 + x$ and let α be a solution of $\alpha + 1/\alpha = A$.
Define $a = \sqrt{1+\alpha}$ and $b = \sqrt{\alpha - 1}$.

$$E \rightsquigarrow (a : b) \in \mathbb{P}^1$$

$$P = (X : Z) \mapsto (\theta_0(P) : \theta_1(P)) = (a(X - Z) : b(X + Z))$$

Product theta structure on $E_1 \times E_2$

$$(P_1, P_2) \in E_1 \times E_2 \mapsto (\theta_0^{E_1}(P_1)\theta_0^{E_2}(P_2) : \theta_1^{E_1}(P_1)\theta_0^{E_2}(P_2) : \theta_0^{E_1}(P_1)\theta_1^{E_2}(P_2) : \theta_1^{E_1}(P_1)\theta_1^{E_2}(P_2))$$

The isogeny formula – Evaluation

We can also evaluate the isogeny Φ at any point P:

$$(\tilde{\theta}^{\mathcal{B}}_{00}(\Phi(P)), \tilde{\theta}^{\mathcal{B}}_{10}(\Phi(P)), \tilde{\theta}^{\mathcal{B}}_{01}(\Phi(P)), \tilde{\theta}^{\mathcal{B}}_{11}(\Phi(P))) = (\alpha^{-1}, \beta^{-1}, \gamma^{-1}, \delta^{-1}) \star \mathcal{H} \circ \mathcal{S}\left((\theta^{\mathcal{A}}_i(P))_i\right),$$

from which we can compute

$$(\theta^{\mathcal{B}}_{00}(\Phi(P)), \theta^{\mathcal{B}}_{10}(\Phi(P)), \theta^{\mathcal{B}}_{01}(\Phi(P)), \theta^{\mathcal{B}}_{11}(\Phi(P))) = \mathcal{H}(\tilde{\theta}^{\mathcal{B}}_{00}(\Phi(P)), \tilde{\theta}^{\mathcal{B}}_{10}(\Phi(P)), \tilde{\theta}^{\mathcal{B}}_{01}(\Phi(P)), \tilde{\theta}^{\mathcal{B}}_{11}(\Phi(P))).$$