

Faster $(2, 2)$ -isogenies for Faster Festive Encryption

Luciano Maino

University of Bristol
S3×E4

14th November, 2023

- “FESTA: Fast Encryption from Supersingular Torsion Attacks”,
with Andrea Basso, and Giacomo Pope. (Asiacrypt 2023)
<https://eprint.iacr.org/2023/660>
- “An Algorithmic Approach to $(2, 2)$ -isogenies in the Theta Model and Applications to Isogeny-based Cryptography”,
with Pierrick Dartois, Giacomo Pope, and Damien Robert.
<https://eprint.iacr.org/2023/1747>

Overview

1 FESTA

2 Security

3 $(2, 2)$ -isogenies in the Theta Model

4 Conclusions

Outline

1 FESTA

2 Security

3 $(2, 2)$ -isogenies in the Theta Model

4 Conclusions

Attack-based Encryption

- SIDH was introduced by De Feo, Jao, and Plut in 2011.

Attack-based Encryption

- SIDH was introduced by De Feo, Jao, and Plut in 2011.
- Petit (2017) describes an attack on some parameter sets
 - ↪ SÉTA: **S**upersingular **E**ncryption from **T**orsion **A**ttacks (2019)

De Feo, de Saint Guilhem, Fouotsa, Kutas, Leroux, Petit, Silva, and Wesolowski

Attack-based Encryption

- SIDH was introduced by De Feo, Jao, and Plut in 2011.
- Petit (2017) describes an attack on some parameter sets
 - ↪ SÉTA: **S**upersingular **E**ncryption from **T**orsion **A**ttacks (2019)
De Feo, de Saint Guilhem, Fouotsa, Kutas, Leroux, Petit, Silva, and Wesolowski
- New attacks on SIDH (2022)
 - ↪ FESTA: **F**ast **E**ncryption from **S**upersingular **T**orsion **A**ttacks

Attack-based Encryption

- SIDH was introduced by De Feo, Jao, and Plut in 2011.
- Petit (2017) describes an attack on some parameter sets
 - ↪ SÉTA: **S**upersingular **E**ncryption from **T**orsion **A**ttacks (2019)
De Feo, de Saint Guilhem, Fouotsa, Kutas, Leroux, Petit, Silva, and Wesolowski
- New attacks on SIDH (2022)
 - ↪ FESTA: **F**ast **E**ncryption from **S**upersingular **T**orsion **A**ttacks

SIDH Attacks in a Nutshell

Given $(\varphi(P), \varphi(Q))$ under a secret isogeny $\varphi: E \rightarrow E'$ of degree d , where $\langle P, Q \rangle = E[n]$, and n is sufficiently large, it is possible to recover φ .

Trapdoor Function

Triple of algorithms $(\text{KeyGen}, f, f^{-1})$

- $\text{KeyGen}(\lambda) \xrightarrow{\$} (\text{sk}, \text{pk})$
- $f(\text{pk}, x) \rightarrow y$
- $f^{-1}(\text{sk}, y) \rightarrow x$

Trapdoor Function

Triple of algorithms $(\text{KeyGen}, f, f^{-1})$

- $\text{KeyGen}(\lambda) \xrightarrow{\$} (\text{sk}, \text{pk})$
- $f(\text{pk}, x) \rightarrow y$
- $f^{-1}(\text{sk}, y) \rightarrow x$

Correct

For all pk and x , $f^{-1}(\text{sk}, f(\text{pk}, x)) = x$.

Trapdoor Function

Triple of algorithms $(\text{KeyGen}, f, f^{-1})$

- $\text{KeyGen}(\lambda) \xrightarrow{\$} (\text{sk}, \text{pk})$
- $f(\text{pk}, x) \rightarrow y$
- $f^{-1}(\text{sk}, y) \rightarrow x$

Correct

For all pk and x , $f^{-1}(\text{sk}, f(\text{pk}, x)) = x$.

One-way

Given pk and y , finding x st $f(\text{pk}, x) = y$ is hard.

$$\begin{pmatrix} P_b \\ Q_b \end{pmatrix}_{E_0}$$

FESTA Trapdoor

$$\begin{pmatrix} P_b \\ Q_b \end{pmatrix} E_0 \xrightarrow{\varphi_A} E_A \quad \text{sk} = (\alpha, \varphi_A)$$

FESTA Trapdoor

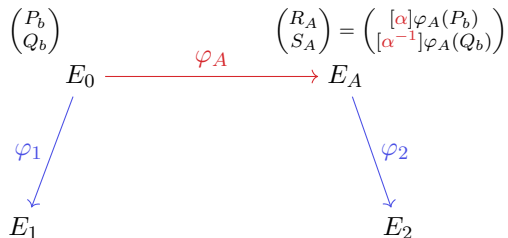
$$\begin{array}{ccc} \begin{pmatrix} P_b \\ Q_b \end{pmatrix} & & \begin{pmatrix} R_A \\ S_A \end{pmatrix} = \begin{pmatrix} [\alpha] \varphi_A(P_b) \\ [\alpha^{-1}] \varphi_A(Q_b) \end{pmatrix} \\ E_0 \xrightarrow{\varphi_A} & & E_A \end{array} \quad \text{sk} = (\alpha, \varphi_A)$$

FESTA Trapdoor

$$\begin{array}{ccc} \begin{pmatrix} P_b \\ Q_b \end{pmatrix} & & \begin{pmatrix} R_A \\ S_A \end{pmatrix} = \begin{pmatrix} [\alpha] \varphi_A(P_b) \\ [\alpha^{-1}] \varphi_A(Q_b) \end{pmatrix} \\ E_0 \xrightarrow{\varphi_A} & & E_A \end{array}$$

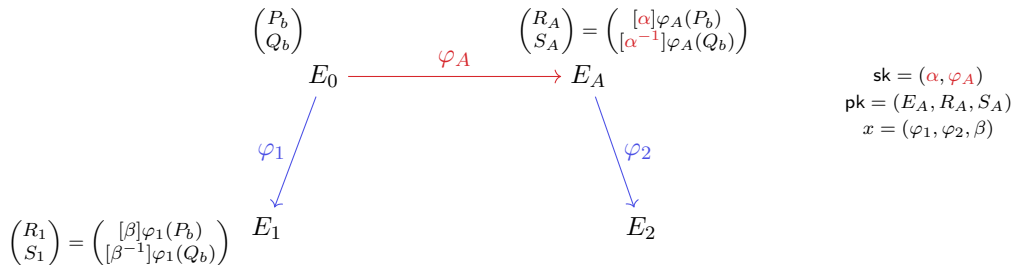
$$\begin{aligned} \text{sk} &= (\alpha, \varphi_A) \\ \text{pk} &= (E_A, R_A, S_A) \end{aligned}$$

FESTA Trapdoor

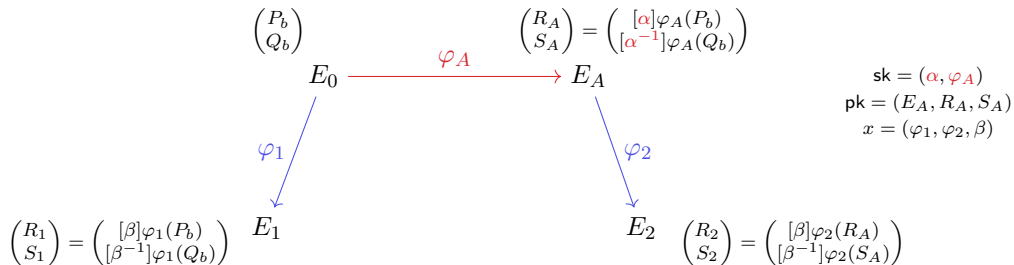


$$\begin{aligned} \text{sk} &= (\alpha, \varphi_A) \\ \text{pk} &= (E_A, R_A, S_A) \\ x &= (\varphi_1, \varphi_2, \beta) \end{aligned}$$

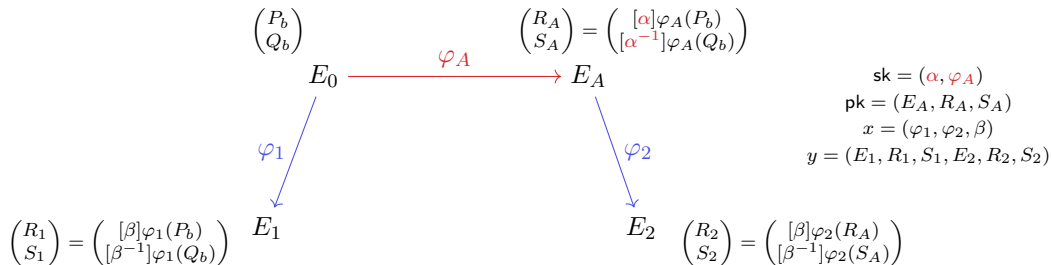
FESTA Trapdoor



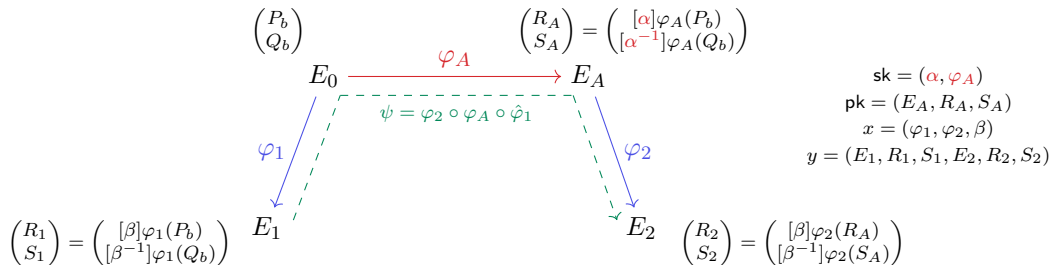
FESTA Trapdoor



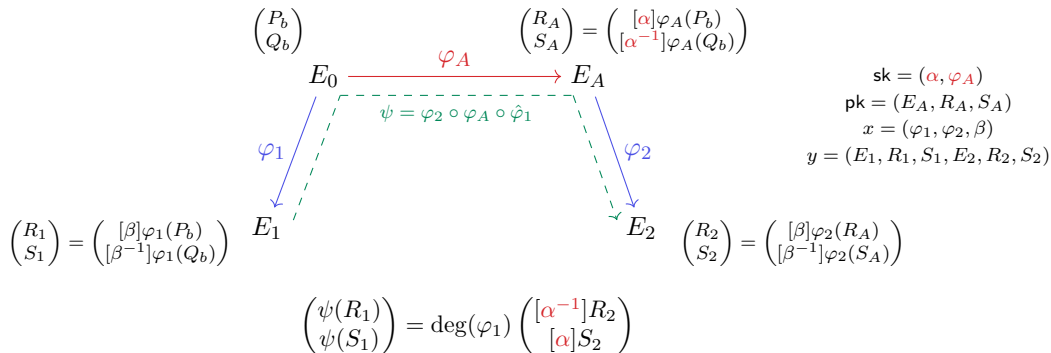
FESTA Trapdoor



FESTA Trapdoor



FESTA Trapdoor



- $\varphi_{N_1}: E_0 \rightarrow E_1, \varphi_{N_2}: E_0 \rightarrow E_2$ s.t. $\gcd(N_1, N_2) = 1$
- $K := \langle ([N_2]\varphi_{N_1}(P), [N_1]\varphi_{N_2}(P)), ([N_2]\varphi_{N_1}(Q), [N_1]\varphi_{N_2}(Q)) \rangle$, where $\langle P, Q \rangle = E_0[N_1 + N_2]$

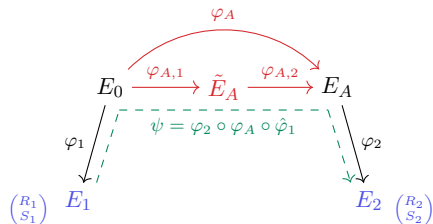
Theorem

The $(N_1 + N_2, N_1 + N_2)$ -polarised isogeny Φ with kernel K has matrix form

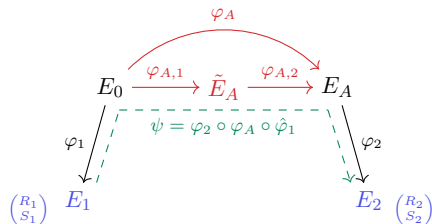
$$\begin{pmatrix} \widehat{\varphi}_{N_1} & -\widehat{\varphi}_{N_2} \\ g_{N_2} & \widehat{g}_{N_1} \end{pmatrix},$$

where g_{N_i} are N_i -isogenies such that $\varphi_{N_2} \circ \widehat{\varphi}_{N_1} = g_{N_1} \circ g_{N_2}$.

Concrete Inversion

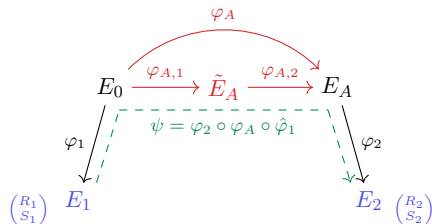


Concrete Inversion



- $d_{A,i} = \deg(\varphi_{A,i})$, $d_i = \deg(\varphi_i)$
- $m_1^2 d_{A,1} d_1 + m_2^2 d_{A,2} d_2 = 2^b$
- $\varphi_{N_1} = [m_1] \circ \varphi_1 \circ \hat{\varphi}_{A,1}$,
 $\varphi_{N_2} = [m_2] \circ \varphi_2 \circ \varphi_{A,2}$
- $d_i > 2^{2\lambda}$, $d_{A,1} \cdot d_{A,2} > 2^{2\lambda}$

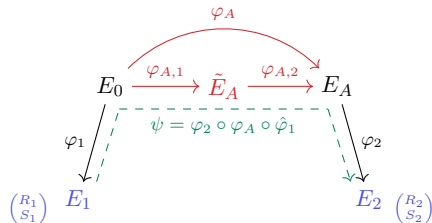
Concrete Inversion



- $d_{A,i} = \deg(\varphi_{A,i})$, $d_i = \deg(\varphi_i)$
- $m_1^2 d_{A,1} d_1 + m_2^2 d_{A,2} d_2 = 2^b$
- $\varphi_{N_1} = [m_1] \circ \varphi_1 \circ \hat{\varphi}_{A,1}$,
 $\varphi_{N_2} = [m_2] \circ \varphi_2 \circ \varphi_{A,2}$
- $d_i > 2^{2\lambda}$, $d_{A,1} \cdot d_{A,2} > 2^{2\lambda}$

$$K := \left\langle \begin{pmatrix} ([m_2 d_{A,2} d_2] R_1, [d_1 m_1 \alpha^{-1}] R_2), \\ ([m_2 d_{A,2} d_2] S_1, [d_1 m_1 \alpha] S_2) \end{pmatrix} \right\rangle,$$

Concrete Inversion



- $d_{A,i} = \deg(\varphi_{A,i})$, $d_i = \deg(\varphi_i)$
- $m_1^2 d_{A,1} d_1 + m_2^2 d_{A,2} d_2 = 2^b$
- $\varphi_{N_1} = [m_1] \circ \varphi_1 \circ \widehat{\varphi}_{A,1}$,
 $\varphi_{N_2} = [m_2] \circ \varphi_2 \circ \varphi_{A,2}$
- $d_i > 2^{2\lambda}$, $d_{A,1} \cdot d_{A,2} > 2^{2\lambda}$

$$K := \left\langle \begin{pmatrix} ([m_2 d_{A,2} d_2] R_1, [d_1 m_1 \alpha^{-1}] R_2), \\ ([m_2 d_{A,2} d_2] S_1, [d_1 m_1 \alpha] S_2) \end{pmatrix} \right\rangle,$$

$$\Phi = \begin{pmatrix} [m_1] \circ \varphi_{A,1} \circ \widehat{\varphi}_1 & -[m_2] \circ \widehat{\varphi}_{A,2} \circ \widehat{\varphi}_2 \\ [m_2] \circ g_{d_2 d_{A,2}} & [m_1] \circ \widehat{g}_{d_{A,1} d_1} \end{pmatrix}$$

Outline

1 FESTA

2 Security

3 $(2, 2)$ -isogenies in the Theta Model

4 Conclusions

Guessing some torsion

Let $\varphi : E_0 \rightarrow E$, and $\begin{pmatrix} R \\ S \end{pmatrix} = \begin{pmatrix} [\alpha]\varphi(P) \\ [\alpha^{-1}]\varphi(Q) \end{pmatrix}$

Guessing some torsion

Let $\varphi : E_0 \rightarrow E$, and $\begin{pmatrix} R \\ S \end{pmatrix} = \begin{pmatrix} [\alpha]\varphi(P) \\ [\alpha^{-1}]\varphi(Q) \end{pmatrix}$

Let n such that $2^n \geq 2\sqrt{\deg(\varphi)}$.

The idea is to guess $\alpha \pmod{2^n}$ and apply Robert's attack in dimension 4 (or 8).

Guessing some torsion

Let $\varphi : E_0 \rightarrow E$, and $\begin{pmatrix} R \\ S \end{pmatrix} = \begin{pmatrix} [\alpha]\varphi(P) \\ [\alpha^{-1}]\varphi(Q) \end{pmatrix}$

Let n such that $2^n \geq 2\sqrt{\deg(\varphi)}$.

The idea is to guess $\alpha \pmod{2^n}$ and apply Robert's attack in dimension 4 (or 8).

$$\begin{pmatrix} R' \\ S' \end{pmatrix} = [2^{n-b}] \begin{pmatrix} R \\ S \end{pmatrix}$$

We need to find a $\beta \leq 2^n$ st

$$[2^{b-n}] \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} = \begin{pmatrix} [\beta]R' \\ [\beta^{-1}]S' \end{pmatrix}$$

Guessing some torsion

Let $\varphi : E_0 \rightarrow E$, and $\begin{pmatrix} R \\ S \end{pmatrix} = \begin{pmatrix} [\alpha]\varphi(P) \\ [\alpha^{-1}]\varphi(Q) \end{pmatrix}$

Let n such that $2^n \geq 2\sqrt{\deg(\varphi)}$.

The idea is to guess $\alpha \pmod{2^n}$ and apply Robert's attack in dimension 4 (or 8).

$$\begin{pmatrix} R' \\ S' \end{pmatrix} = [2^{n-b}] \begin{pmatrix} R \\ S \end{pmatrix}$$

We need to find a $\beta \leq 2^n$ st

$$[2^{b-n}] \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} = \begin{pmatrix} [\beta]R' \\ [\beta^{-1}]S' \end{pmatrix}$$

Remark

Assuming the cost of running Robert's attack is negligible, $\deg(\varphi) > 2^{2\lambda}$.

$$m_1^2 d_{A,1} d_1 + m_2^2 d_{A,2} d_2 = 2^b$$

$$b := 632,$$

$$d_1 := (3^3 \cdot 19 \cdot 29 \cdot 37 \cdot 83 \cdot 139 \cdot 167 \cdot 251 \cdot 419 \cdot 421 \cdot 701 \cdot 839 \cdot 1009 \cdot 1259 \cdot 3061 \cdot 3779)^2,$$

$$d_2 := 7 \cdot (5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 41 \cdot 43 \cdot 71 \cdot 89 \cdot 127 \cdot 211 \cdot 281 \cdot 503 \cdot 631 \cdot 2309 \cdot 2521 \cdot 2647 \cdot 2729)^2,$$

$$d_{A,1} := (59 \cdot 6299 \cdot 6719 \cdot 9181)^2,$$

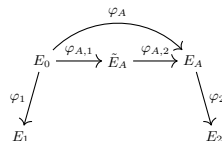
$$d_{A,2} := (3023 \cdot 3359 \cdot 4409 \cdot 5039 \cdot 19531 \cdot 22679 \cdot 41161)^2,$$

$$m_1 := 1492184945093476592520242083925044182103921,$$

$$m_2 := 25617331336429939300166693069,$$

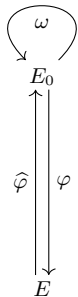
$$f := 107.$$

$p = 2^b d_1 (d_{A,1} d_{A,2})_{\text{sf}} d_2 f - 1$ is 1292-bit long



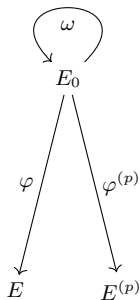
Generalised Lollipop Attack (Castrick-Vercauteren 2023)

Let $\varphi : E_0 \rightarrow E$, and $\begin{pmatrix} R \\ S \end{pmatrix} = \begin{pmatrix} [\alpha]\varphi(P) \\ [\alpha^{-1}]\varphi(Q) \end{pmatrix}$



Generalised Lollipop Attack (Castricky-Vercauteren 2023)

Let $\varphi : E_0 \rightarrow E$, and $\begin{pmatrix} R \\ S \end{pmatrix} = \begin{pmatrix} [\alpha]\varphi(P) \\ [\alpha^{-1}]\varphi(Q) \end{pmatrix}$



- $\psi := \varphi^{(p)} \circ \omega \circ \hat{\varphi}$
- If $\begin{pmatrix} \pi \circ \omega(P) \\ \pi \circ \omega(Q) \end{pmatrix} = \begin{pmatrix} [\beta_P]P \\ [\beta_Q]Q \end{pmatrix}$,

$$\begin{pmatrix} \psi(R) \\ \psi(S) \end{pmatrix} = [\deg \varphi] \begin{pmatrix} [\beta_P]\pi(R) \\ [\beta_Q]\pi(S) \end{pmatrix}$$

- Case of $E_0 : y^2 = x^3 + 6x^2 + x$ (no need for this)
- The 2^b -torsion basis is computed as in
(Zanon, Simplicio Jr, Pereira, Doliskani, and Barreto, 2017)
 - Full basis scenario $\deg(\omega) < 2^{2b} / \deg(\varphi)^2$:
 $\mathcal{O}(\min\{2^{-4\lambda}, 2^{-b}\})$
 - Image of a single point $\deg(\omega) < 2^b / \deg(\varphi)$:
 $\mathcal{O}(2^{-4\lambda})$
- Polynomial-time attack if $2^b \gtrsim pd^3$

Outline

- 1 FESTA
- 2 Security
- 3 $(2, 2)$ -isogenies in the Theta Model
- 4 Conclusions

- On an elliptic curve E , we implicitly have some additional structure
- By Riemann–Roch, the following

$$\begin{aligned} E &\xrightarrow{\sim} \mathrm{Pic}^0(E) \\ P &\mapsto (P) - (0_E) \end{aligned}$$

is an isomorphism between the elliptic curve and its dual.

- In practice, this isomorphism is described by a *line bundle* $\mathcal{L}((0_E))$.

- On an elliptic curve E , we implicitly have some additional structure
- By Riemann–Roch, the following

$$\begin{aligned} E &\xrightarrow{\sim} \mathrm{Pic}^0(E) \\ P &\mapsto (P) - (0_E) \end{aligned}$$

is an isomorphism between the elliptic curve and its dual.

- In practice, this isomorphism is described by a *line bundle* $\mathcal{L}((0_E))$.
- We have just described a (principal) *polarisation*!

- On an elliptic curve E , we implicitly have some additional structure
- By Riemann–Roch, the following

$$\begin{aligned} E &\xrightarrow{\sim} \operatorname{Pic}^0(E) \\ P &\mapsto (P) - (0_E) \end{aligned}$$

is an isomorphism between the elliptic curve and its dual.

- In practice, this isomorphism is described by a *line bundle* $\mathcal{L}((0_E))$.
- We have just described a (principal) *polarisation*!

Generalisation

The correct generalisation to higher dimension is principally polarised abelian varieties.

- Let A be an abelian variety. A *polarisation* is an isogeny $\xi : A \rightarrow \hat{A}$ coming from a line bundle \mathcal{L}_A . A *principal polarisation* is a polarisation that is also an isomorphism.
- Let (A, ξ_A) and (B, ξ_B) be two principally polarised abelian varieties. The isogeny $f : A \rightarrow B$ is a N -isogeny if $[N] \circ \xi_A = \hat{f} \circ \xi_B \circ f$.

- Let A be an abelian variety. A *polarisation* is an isogeny $\xi : A \rightarrow \hat{A}$ coming from a line bundle \mathcal{L}_A . A *principal polarisation* is a polarisation that is also an isomorphism.
- Let (A, ξ_A) and (B, ξ_B) be two principally polarised abelian varieties. The isogeny $f : A \rightarrow B$ is a N -isogeny if $[N] \circ \xi_A = \hat{f} \circ \xi_B \circ f$.
- In dimension 2, we have only two types of principally polarised abelian surfaces:
 - products of elliptic curves
 - Jacobians of hyperelliptic genus-2 curves
- We note the N -isogenies in dimension 2 by (N, N) .

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

Goal: Compute the $(2^b, 2^b)$ -isogeny $f : E_1 \times E_2 \rightarrow E'_1 \times E'_2$

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

Goal: Compute the $(2^b, 2^b)$ -isogeny $f : E_1 \times E_2 \rightarrow E'_1 \times E'_2$

We compute f as a chain of $(2, 2)$ -isogenies:

$$f = f_b \circ \dots \circ f_1$$

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

Goal: Compute the $(2^b, 2^b)$ -isogeny $f : E_1 \times E_2 \rightarrow E'_1 \times E'_2$

We compute f as a chain of $(2, 2)$ -isogenies:

$$f = f_b \circ \dots \circ f_1$$

The state of the art:

- Gluing isogeny $f_1 : E_1 \times E_2 \rightarrow \text{Jac}(\mathcal{C})$ (Howe, Leprévost, and Poonen, 2000)
- Splitting Isogeny $f_b : \text{Jac}(\mathcal{C}) \rightarrow E'_1 \times E'_2$ (Smith, 2005)
- Richelot Isogenies $f_i : \text{Jac}(\mathcal{C}_i) \rightarrow \text{Jac}(\mathcal{C}_{i+1})$, for $i = 2, \dots, b - 1$ (Smith, 2005)

Let A be a principally polarised abelian surface, e.g. a product of two elliptic curves.
Let $A[4] = \langle S'_1, S'_2, T'_1, T'_2 \rangle$ be a symplectic 4-torsion basis

- $e(S'_1, T'_1) = e(S'_2, T'_2) = \mu$
- $e(S'_1, S'_2) = e(T'_1, T'_2) = e(S'_1, T'_2) = e(S'_2, T'_1) = 1$

Let A be a principally polarised abelian surface, e.g. a product of two elliptic curves.

Let $A[4] = \langle S'_1, S'_2, T'_1, T'_2 \rangle$ be a symplectic 4-torsion basis

- $e(S'_1, T'_1) = e(S'_2, T'_2) = \mu$
- $e(S'_1, S'_2) = e(T'_1, T'_2) = e(S'_1, T'_2) = e(S'_2, T'_1) = 1$

$$\langle S'_1, S'_2, T'_1, T'_2 \rangle \rightsquigarrow \theta_{00}, \theta_{10}, \theta_{01}, \theta_{11}$$

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

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

An example – Elliptic Products

In $S^3 \times E^3$, Sarkis gave conversion formulae between Montgomery curves and its theta squared model.

Picking any square root of the squared theta-null coordinates, we obtain a theta structure on the elliptic curve.

$$E \rightsquigarrow (a : b) \in \mathbb{P}^2$$

An example – Elliptic Products

In $S^3 \times E^3$, Sarkis gave conversion formulae between Montgomery curves and its theta squared model.

Picking any square root of the squared theta-null coordinates, we obtain a theta structure on the elliptic curve.

$$E \rightsquigarrow (a : b) \in \mathbb{P}^2$$

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

An example – Elliptic Products

In $S_3 \times E_3$, Sarkis gave conversion formulae between Montgomery curves and its theta squared model.

Picking any square root of the squared theta-null coordinates, we obtain a theta structure on the elliptic curve.

$$E \rightsquigarrow (a : b) \in \mathbb{P}^2$$

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

Product theta structure on $E_1 \times E_2$

$$(P_1, P_2) \in E_1 \times E_2 \mapsto$$

$$(\theta_0^{E_1}(P_1)\theta_0^{E_2}(P_2) : \theta_1^{E_1}(P_1)\theta_0^{E_2}(P_2) : \theta_0^{E_1}(P_1)\theta_1^{E_2}(P_2) : \theta_1^{E_1}(P_1)\theta_1^{E_2}(P_2))$$

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 $(\tilde{\theta}_{00}(P) : \tilde{\theta}_{10}(P) : \tilde{\theta}_{01}(P) : \tilde{\theta}_{11}(P)) = \mathcal{H}(\theta_{00}(P), \theta_{10}(P), \theta_{01}(P), \theta_{11}(P))$ 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 $(\tilde{\theta}_{00}(P) : \tilde{\theta}_{10}(P) : \tilde{\theta}_{01}(P) : \tilde{\theta}_{11}(P)) = \mathcal{H}(\theta_{00}(P), \theta_{10}(P), \theta_{01}(P), \theta_{11}(P))$ 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 $(\tilde{\theta}_{00}(P) : \tilde{\theta}_{10}(P) : \tilde{\theta}_{01}(P) : \tilde{\theta}_{11}(P)) = \mathcal{H}(\theta_{00}(P), \theta_{10}(P), \theta_{01}(P), \theta_{11}(P))$ 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 $f : A \rightarrow B$, $\ker f = \langle T_1, T_2 \rangle$, where $T_i = [2]T'_i$. (Remember the decomposition $\langle S'_1, S'_2, T'_1, T'_2 \rangle$)

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

We can obtain addition formulae

- Differential addition: **8S + 17M**
- Doubling: **8S + 6M**

The same formulae as in (Gaudry, 2005)

The isogeny formula

Goal: To compute the isogeny $f : A \rightarrow B$ with $\ker f = \langle T_1, T_2 \rangle$, where $T_i = [2]T'_i$.

The isogeny formula

Goal: To compute the isogeny $f : A \rightarrow B$ with $\ker f = \langle T_1, T_2 \rangle$, 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 $f : A \rightarrow B$ with $\ker f = \langle T_1, T_2 \rangle$, 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 $(\alpha : \beta : \gamma : \delta) = (\tilde{\theta}_{00}^B(0) : \tilde{\theta}_{10}^B(0) : \tilde{\theta}_{01}^B(0) : \tilde{\theta}_{11}^B(0))$

The isogeny formula

Goal: To compute the isogeny $f : A \rightarrow B$ with $\ker f = \langle T_1, T_2 \rangle$, 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 $(\alpha : \beta : \gamma : \delta) = (\tilde{\theta}_{00}^B(0) : \tilde{\theta}_{10}^B(0) : \tilde{\theta}_{01}^B(0) : \tilde{\theta}_{11}^B(0))$

Trust me, we did the maths:

$$\mathcal{H} \circ \mathcal{S}(\theta_{00}^A(T''_1), \theta_{10}^A(T''_1), \theta_{01}^A(T''_1), \theta_{11}^A(T''_1)) = (x\alpha, x\beta, y\gamma, y\delta),$$

$$\mathcal{H} \circ \mathcal{S}(\theta_{00}^A(T''_2), \theta_{10}^A(T''_2), \theta_{01}^A(T''_2), \theta_{11}^A(T''_2)) = (z\alpha, w\beta, z\gamma, w\delta),$$

for some unknown x, y, z, w .

The isogeny formula

Goal: To compute the isogeny $f : A \rightarrow B$ with $\ker f = \langle T_1, T_2 \rangle$, 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 $(\alpha : \beta : \gamma : \delta) = (\tilde{\theta}_{00}^B(0) : \tilde{\theta}_{10}^B(0) : \tilde{\theta}_{01}^B(0) : \tilde{\theta}_{11}^B(0))$

Trust me, we did the maths:

$$\mathcal{H} \circ \mathcal{S}(\theta_{00}^A(T''_1), \theta_{10}^A(T''_1), \theta_{01}^A(T''_1), \theta_{11}^A(T''_1)) = (x\alpha, x\beta, y\gamma, y\delta),$$

$$\mathcal{H} \circ \mathcal{S}(\theta_{00}^A(T''_2), \theta_{10}^A(T''_2), \theta_{01}^A(T''_2), \theta_{11}^A(T''_2)) = (z\alpha, w\beta, z\gamma, w\delta),$$

for some unknown x, y, z, w .

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

The isogeny formula

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

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

from which we can compute

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

Operation Counting

Isogeny Type	Doubling	Codomain		Evaluation
		Generic	Optimised	
Generic	$8\mathbf{S} + 6\mathbf{M}$	$8\mathbf{S} + 29\mathbf{M} + 1\mathbf{I}$	$8\mathbf{S} + 9\mathbf{M} + 1\mathbf{I}$	$4\mathbf{S} + 3\mathbf{M}$
Gluing	$12\mathbf{S} + 12\mathbf{M}$	$8\mathbf{S} + 13\mathbf{M} + 1\mathbf{I}$		$8\mathbf{S} + 5\mathbf{M} + 1\mathbf{I}$

Details I skated over

- The formulae I showed you assume that $\ker(f)[4] = \langle T'_1, T'_2 \rangle$.
- 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.

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.

$\log p$	n	Codomain			Evaluation		
		Theta Rust	Theta SageMath	Richelot SageMath	Theta Rust	Theta SageMath	Richelot SageMath
254	126	2.85 ms	108 ms	1028 ms	161 μs	5.43 ms	114 ms
381	208	11.2 ms	201 ms	1998 ms	411 μs	8.68 ms	208 ms
1293	632	495 ms	1225 ms	12840 ms	17.8 ms	40.8 ms	1203 ms

Apple M1 PRO CPU clocked at 3.2 GHz using a single performance core

```
=====
Running FESTA_128
=====
```

```
=====
Keygen took: 4.703 seconds
=====
```

```
=====
Encrypt took: 3.067 seconds
=====
```

```
=====
Decrypt took: 2.823 seconds
=====
```

Outline

1 FESTA

2 Security

3 $(2, 2)$ -isogenies in the Theta Model

4 Conclusions

- These $(2, 2)$ -isogeny formulae can speed-up all the protocols currently relying on chains of $(2, 2)$ -isogenies, e.g. IS-CUBE (Moriya 2023, $S3 \times E2$) and QFESTA (Onuki-Nakagawa, 2023)
- What about (ℓ, ℓ) -isogenies and $(2, 2, 2, 2)$ -isogenies?

Thanks for your
attention!

Questions?