Isogeny interpolation and the computation of isogenies from higher-dimensional representations

David Jao & Jeanne Laflamme

December 2024

UNIVERSITY OF WATERLOO

Outline

- SIDH
- Castryck-Decru Attack
- Theta Coordinates and `Avisogenies`
- Using `Avisogenies` to implement the attack
- Timings

SIDH

Public parameters:

E_0: supersingular curve defined over $\mathbb{F}_{p^2}$

$p = 2^a 3^b - 1$

$E_0[2^a] = \langle P_A, Q_A \rangle$

$E_0[3^b] = \langle P_B, Q_B \rangle$

SIDH

Alice

- generates $k_A \in \mathbb{Z}$
- Computes $S_A = P_A + k_A Q_A$

$\longrightarrow E_A, \phi_A(P_B), Q_A(Q_B)$

Her secret isogeny is
$\phi_A : E_0 \longrightarrow E_A$
where $\ker \phi_A = \langle S_A \rangle$

$\deg \phi_A = 2^a$

Bob

- generates $k_B \in \mathbb{Z}$
- Computes $S_B = P_B + k_B Q_B$

$E_B, \phi_B(P_A), \phi_B(Q_A) \longleftarrow$

His secret isogeny is
$\phi_B : E_0 \longrightarrow E_B$
where $\ker \phi_B = \langle S_B \rangle$

$\deg \phi_B = 3^b$

$\phi_A' : E_B \longrightarrow E_{AB}$
where $\ker \phi_A' = \langle \phi_B(P_A) + k_A \phi_B(Q_A) \rangle$

$$\begin{tikzcd}
E_0 \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "\phi_B'"] \\
E_B \arrow[r, "\phi_A'"] & E_{AB}
\end{tikzcd}$$

$\phi_B' : E_A \longrightarrow E_{AB}$
where $\ker \phi_B' = \langle \phi_A(P_B) + k_B \phi_A(Q_B) \rangle$

SIDH

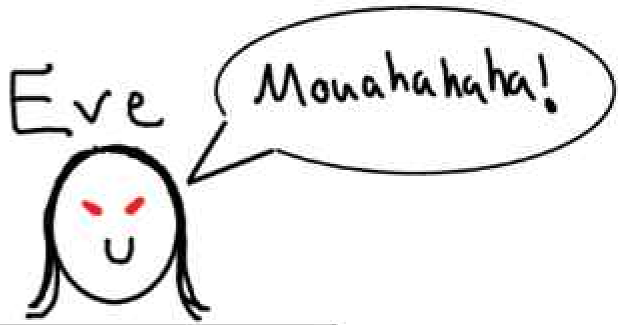
$$\phi_A : E_0 \longrightarrow E_A$$

"Pure" isogeny problem: Given E_0 and E_A, recover $\ker \phi_A$

SIDH

$$\phi_A : E_0 \longrightarrow E_A$$

"Pure" isogeny problem: Given E_0 and E_A, recover $\mathrm{Ker}\,\phi_A$



E_0, E_A
$\phi_A(P_B), \phi_A(Q_B)$

$(E_0[3^b] = \langle P_B, Q_B \rangle)$

Dimension 2 Varieties

- Product of Elliptic Curves $E_1 \times E_2$ (rare)
- Jacobian of a genus 2 hyperelliptic curve Jac(C) (common)

$\Rightarrow$ 4 types of isogenies in dimension 2:

- "Glue" isogeny $\Phi : E_1 \times E_2 \rightarrow Jac(C)$
- generic isogeny $\Phi : Jac(C_1) \rightarrow Jac(C_2)$
- "split" isogeny: $\Phi : Jac(C) \rightarrow E_1 \times E_2$
- Product isogeny: $\Phi : E_1 \times E_2 \rightarrow E_3 \times E_4$

Castryck-Decru Attack

$$\begin{tikzcd} E_0 \arrow[r, "\phi_A"] \arrow[d, "\gamma"] & E_A \arrow[l, dashed, bend left, "\hat{\phi}_A"] \arrow[d, "\gamma'"] \\ E_0 \arrow[r, "\phi_A'"] \arrow[u, dashed, bend left, "\hat{\gamma}"] & C \end{tikzcd}$$

$\gamma : E_0 \to E_0$ has $\deg \gamma = 3^b - 2^a$

Define $\Phi : E_0 \times E_A \longrightarrow E_0 \times C$ as $\Phi = \begin{pmatrix} \hat{\gamma} & \hat{\phi}_A \\ -\phi_A' & \gamma' \end{pmatrix}$

$\deg \Phi = 3^b$

The choice of γ ensures that this is a valid isogeny (Kani's thm)

$$\ker \Phi = < (2^a P_B, -\phi_A(\hat{\gamma}(P_B))), (2^a Q_B, -\phi_A(\hat{\gamma}(Q_B))) >,$$

For $P \in E_A$, $\Phi(O, P) = \begin{pmatrix} \hat{\gamma} & \hat{\phi}_A \\ -\phi_A' & \gamma' \end{pmatrix} \begin{pmatrix} O \\ P \end{pmatrix} = \begin{pmatrix} \hat{\phi}_A(P) \\ \gamma'(P) \end{pmatrix}$

We can recover the image of $\hat{\phi}_A$ on any point!

Castryck-Decru Attack

$$\begin{tikzcd} E_0 \arrow[r, shift left, "\phi_A"] \arrow[d, shift left, "\gamma"] & E_A \arrow[l, shift left, dashed, "\hat{\phi}_A"] \arrow[d, "\gamma'"] \\ E_0 \arrow[r, "\phi_A'"] \arrow[u, shift left, dashed, "\hat{\gamma}"] & C \end{tikzcd}$$

$\gamma : E_0 \to E_0$ has $\deg \gamma = 3^b - 2^a$

Define $\Phi : E_0 \times E_A \longrightarrow E_0 \times C$ as $\Phi = \begin{pmatrix} \hat{\gamma} & \hat{\phi}_A \\ -\phi_A' & \gamma' \end{pmatrix}$

$\deg \Phi = 3^b$

The choice of γ ensures that this is a valid isogeny (Kani's thm)

$$\ker \Phi = < (2^a P_B, -\phi_A(\hat{\gamma}(P_B))), (2^a Q_B, -\phi_A(\hat{\gamma}(Q_B))) >,$$

For $P \in E_A$, $\Phi(O, P) = \begin{pmatrix} \hat{\gamma} & \hat{\phi}_A \\ -\phi_A' & \gamma' \end{pmatrix} \begin{pmatrix} O \\ P \end{pmatrix} = \begin{pmatrix} \hat{\phi}_A(P) \\ \gamma'(P) \end{pmatrix}$

We can recover the image of $\hat{\phi}_A$ on any point!

In fact, if P_A', Q_A' generate the 2^a-torsion on E_A then either $\hat{\phi}_A(P_A')$ or $\hat{\phi}_A(Q_A')$ generate the kernel of ϕ_A !!!

Recovering Alice's Isogeny

$$\Phi : E_0 \times E_A \longrightarrow E_0 \times C$$

$$\Phi = \begin{pmatrix} \hat{\gamma} & \hat{\phi}_A \\ -\phi_A' & \gamma' \end{pmatrix}$$

$$\begin{array}{l} E_0 \\ \\ E_A \end{array} \xrightarrow{\Phi_1} \mathrm{Jac}(C_1) \xrightarrow{\Phi_2} \mathrm{Jac}(C_2) \xrightarrow{\Phi_3} \cdots \xrightarrow{\Phi_{b-1}} \mathrm{Jac}(C_{b-1}) \xrightarrow{\Phi_b} \begin{array}{l} E_0 \\ \\ C \end{array}$$

- $\Phi_1 : E_0 \times E_A \to \mathrm{Jac}(C_1)$ is a glue isogeny
- $\Phi_b : \mathrm{Jac}(C_{b-1}) \to E_0 \times C$ is a split isogeny
- The rest $\Phi_i : \mathrm{Jac}(C_{i-1}) \to \mathrm{Jac}(C_i)$ are generic isogenies

$\deg \Phi = 3^b$

$\deg \Phi_i = 3$

What if...

If we try to recover Bob's secret isogeny, we will be computing a chain of degree 2 isogenies instead. There exists implementation of the attack that recover both Alice's isogeny and Bob's isogeny but what if...

Public parameters:

E_0: supersingular curve defined over $\mathbb{F}_{p^2}$

$p = \ell_A^a \ell_B^b - 1$

$E_0[\ell_A^a] = \langle P_A, Q_A \rangle$

$E_0[\ell_B^b] = \langle P_B, Q_B \rangle$

Now if we want to recover Alice's secret isogeny, we need to compute a chain of degree ℓ_B isogenies in dimension 2. Can this be done if $\ell_B > 3$?

Theta Coordinates

Theta coordinates make use of theta functions which are derived from the Riemann theta function:

$$\theta(z, \Omega) = \sum_{n \in \mathbb{Z}_g} \exp(i\pi n^T \Omega n + 2i\pi n^T z).$$

They allow to embed an abelian variety into the projective plane.

Theta Coordinates

Points P on an elliptic curve E are embedded into $\mathbb{P}^1$ and so have two theta coordinates:

$$\theta^P = (\theta_0^P : \theta_1^P) \in \mathbb{P}^1.$$

Points $\mathbf{P}$ on a dimension 2 variety are embedded into $\mathbb{P}^3$ and so have four theta coordinates:

$$\theta^{\mathbf{P}} = (\theta_{00}^{\mathbf{P}} : \theta_{01}^{\mathbf{P}} : \theta_{10}^{\mathbf{P}} : \theta_{11}^{\mathbf{P}}) \in \mathbb{P}^3$$

Theta Null Points

The elliptic curve E itself can be represented with theta coordinates through the coordinates of the identity element on E. This is called the theta null point of E:

$$\theta^E = (\theta_0^E : \theta_1^E) \in \mathbb{P}^1$$

We can define the theta null point of a dimension 2 variety A in a similar way:

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

Avisogenies

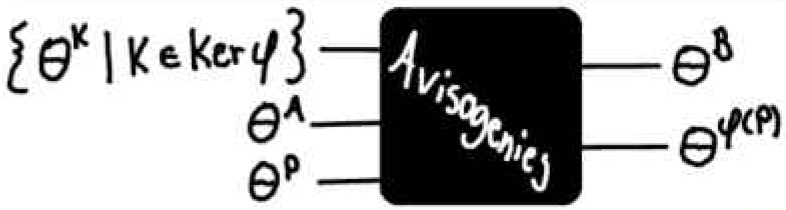
The isogeny formulas implemented in the package take as input:

- The theta null point of the variety
- The theta coordinates of all the points in the kernel of the isogeny

There are conversion formulas implemented to go from points on the Jacobian of a hyperelliptic curve to theta coordinates. However there are no implementations of conversions for products of Elliptic curves.

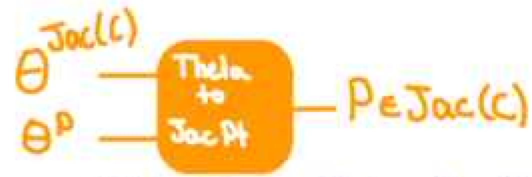
$\varphi : A \to B$
$P \mapsto \varphi(P)$
dimension 2 isogeny with $\deg\varphi = \ell$

Compute isogeny

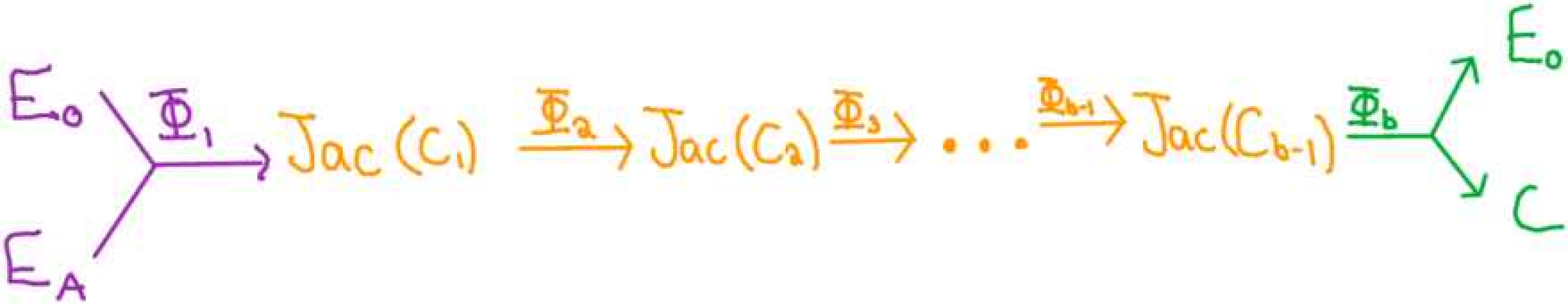


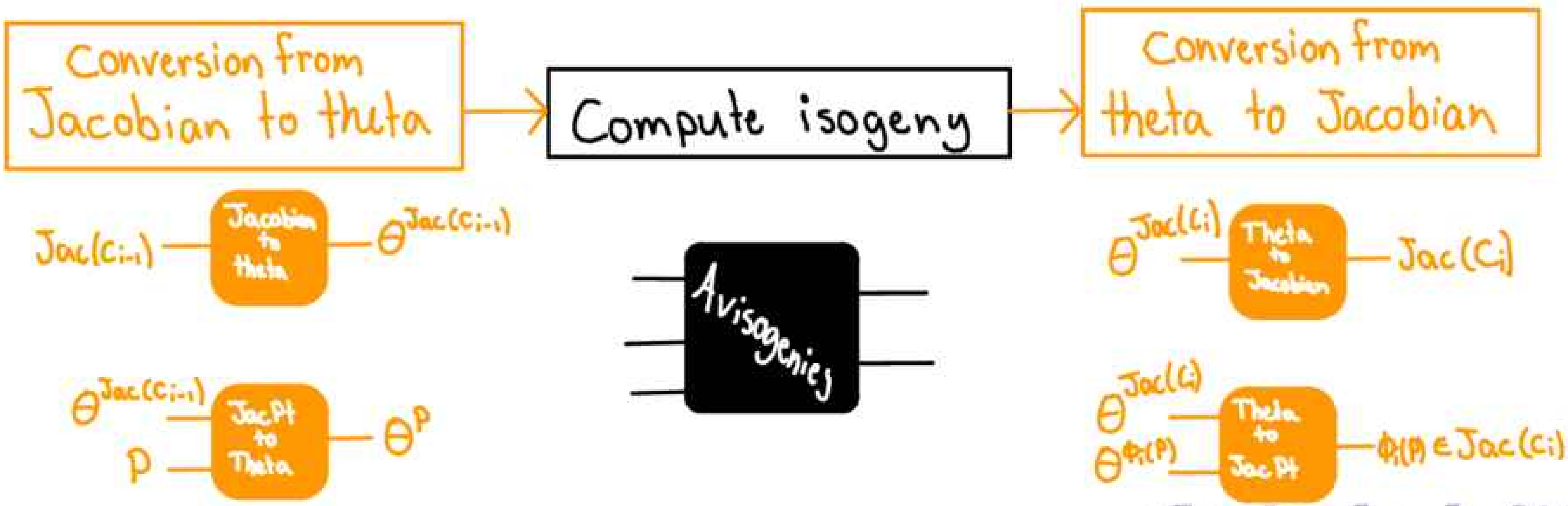
Conversion from Jacobian to theta

Conversion from theta to Jacobian



Generic Case

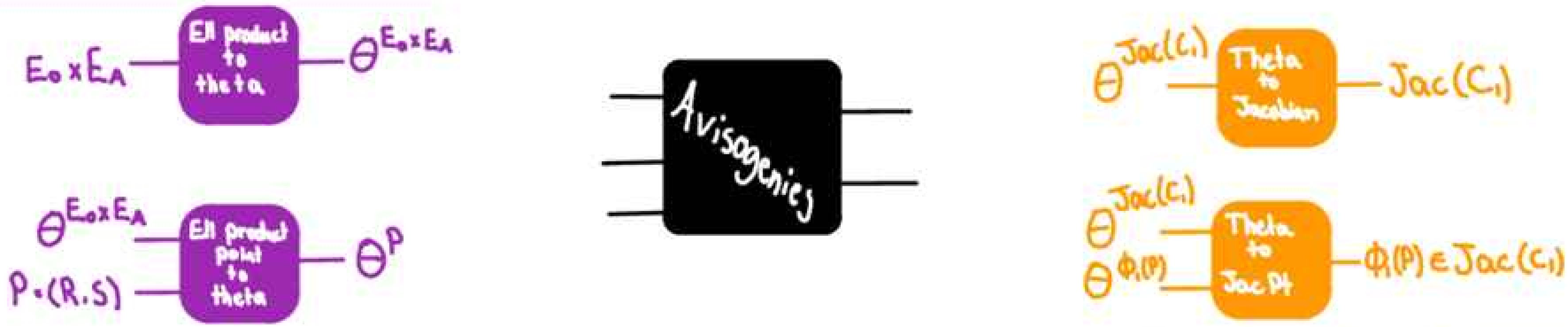




Glue Case

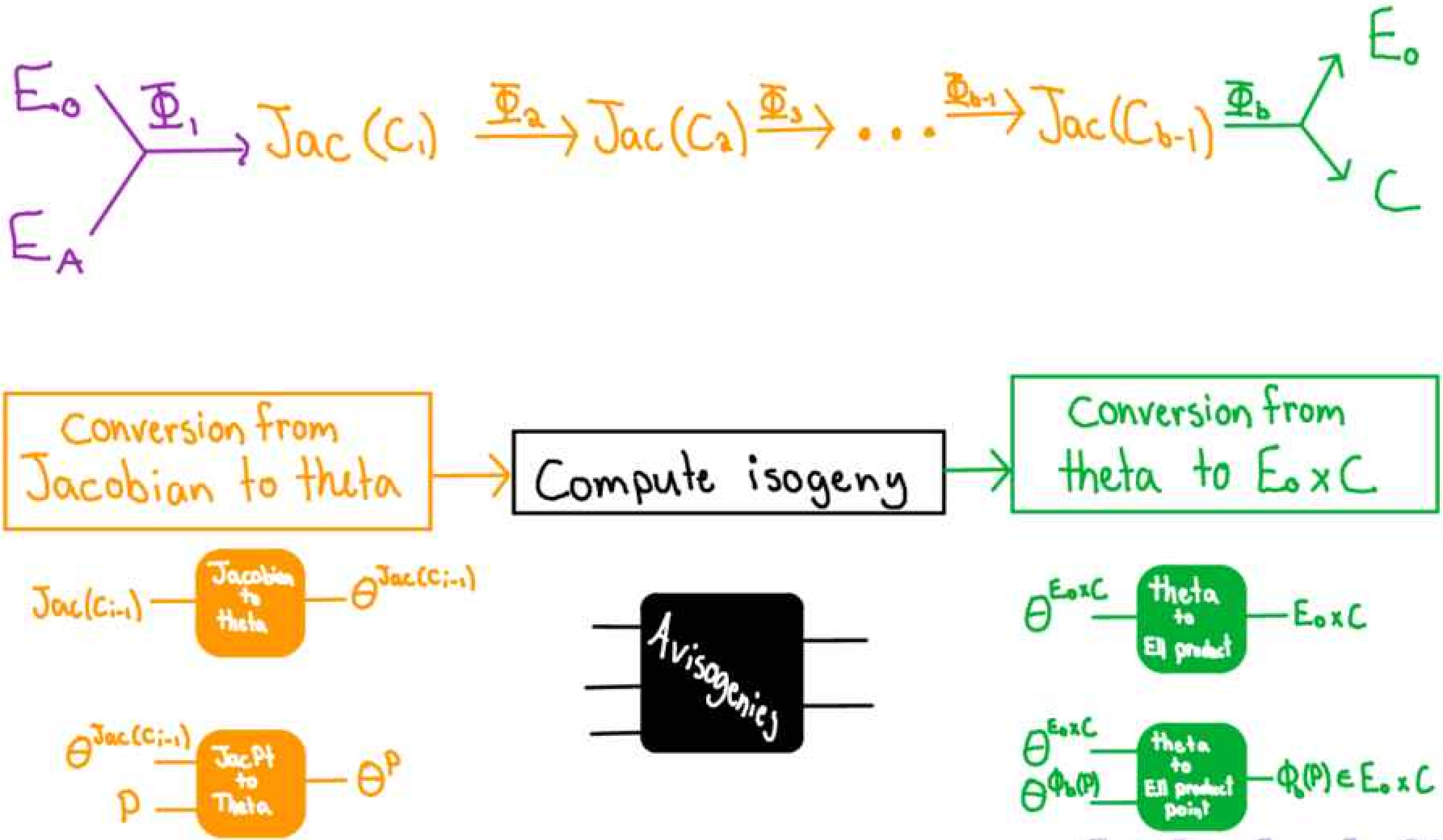
$$\begin{tikzcd} E_0 \arrow[dr, dash] & & & & & & E_0 \\ & \cdot \arrow[r, "\Phi_1"] & Jac(C_1) \arrow[r, "\Phi_2"] & Jac(C_2) \arrow[r, "\Phi_3"] & \cdots \arrow[r, "\Phi_{b-1}"] & Jac(C_{b-1}) \arrow[r, dash, "\Phi_b"] & \cdot \arrow[u] \arrow[d] \\ E_A \arrow[ur, dash] & & & & & & C \end{tikzcd}$$

$$\boxed{\text{Conversion from } E_0 \times E_A \text{ to theta}} \longrightarrow \boxed{\text{Compute isogeny}} \longrightarrow \boxed{\text{Conversion from theta to Jacobian}}$$



$(R \in E_0,\ S \in E_A)$

Split Case



E0
EA
Φ1
Jac(C1)
Φ2
Jac(C2)
Φ3
Φb-1
Jac(Cb-1)
Φb
E0
C
Conversion from Jacobian to theta
Compute isogeny
Conversion from theta to E0 x C
Jac(Ci-1)
Jacobian to theta
ΘJac(Ci-1)
Avisogenies
ΘE0xC
theta to Ell product
E0 x C
ΘJac(Ci-1)
P
Jac Pt to Theta
ΘP
ΘE0xC
ΘΦb(P)
theta to Ell product point
Φb(P) ∈ E0 x C

Theta Null Point of E_0

$$E_0 : y^2 = f(x) \text{ where, } f(x) = (x - e_1)(x - e_2)(x - e_3)$$

$$\theta^{E_0} = (\theta_0^{E_0} : \theta_1^{E_0})$$

$$\theta_0^{E_0} = \sqrt{e_1 - e_3} + \sqrt{e_1 - e_2}$$
$$\theta_1^{E_0} = \sqrt{e_2 - e_3}.$$

Theta Null Point of $E_0 \times E_A$

$$\theta^{E_0} = (\theta_0^{E_0} : \theta_1^{E_0}), \quad \theta^{E_A} = (\theta_0^{E_A} : \theta_1^{E_A})$$

The theta null point of $A = E_0 \times E_A$ is

$$\theta^A = (\theta_{00}^A : \theta_{01}^A : \theta_{10}^A : \theta_{11}^A)$$

where

$$\begin{aligned}
\theta_{00}^A &= \theta_0^{E_0} \cdot \theta_0^{E_A} \\
\theta_{01}^A &= \theta_0^{E_0} \cdot \theta_1^{E_A} \\
\theta_{10}^A &= \theta_1^{E_0} \cdot \theta_0^{E_A} \\
\theta_{11}^A &= \theta_1^{E_0} \cdot \theta_1^{E_A}
\end{aligned}$$

Theta coordinates of a point $\mathbf{P} \in E_0 \times E_A$

Let $\mathbf{P} = (R, S)$. We can find the theta coordinates θ^R and θ^S of the elliptic curve points R and S using functions in `Avisogenies`. Then, similarly as before, the theta coordinates of $\mathbf{P}$ are given by

$$\theta^{\mathbf{P}}_{00} = \theta^R_0 \cdot \theta^S_0$$
$$\theta^{\mathbf{P}}_{01} = \theta^R_0 \cdot \theta^S_1$$
$$\theta^{\mathbf{P}}_{10} = \theta^R_1 \cdot \theta^S_0$$
$$\theta^{\mathbf{P}}_{11} = \theta^R_1 \cdot \theta^S_1$$

Recovering $E_0' \times C$

$$\theta^{E_0'} = (\theta_0^{E_0'} : \theta_1^{E_0'}), \quad \theta^C = (\theta_0^C : \theta_1^C)$$

The theta null point of $B = E_0' \times C$ is

$$\theta^B = (\theta_{00}^B : \theta_{01}^B : \theta_{10}^B : \theta_{11}^B)$$

where

$$\begin{aligned}
\theta_{00}^B &= \theta_0^{E_0'} \cdot \theta_0^C \\
\theta_{01}^B &= \theta_0^{E_0'} \cdot \theta_1^C \\
\theta_{10}^B &= \theta_1^{E_0'} \cdot \theta_0^C \\
\theta_{11}^B &= \theta_1^{E_0'} \cdot \theta_1^C
\end{aligned}$$

Recovering $E_0' \times C$

Since we are working with projective coordinates, we can take

$$\theta^{E_0'} = (\theta^B_{00} : \theta^B_{10})$$
$$\theta^C = (\theta^B_{00} : \theta^B_{01})$$

and then invert the formulas in the gluing step to recover E_0' and C. We can proceed similarly to recover points on the curves from their theta coordinates.

Timings

ℓ_A	ℓ_B	a	b	p	time
2	5	93	104	$2^{93}5^{104} - 1 \approx 2^{335}$	83 s
		216	115	$2^{216}5^{115} - 1 \approx 2^{484}$	2 mins
		109	216	$2^{109}5^{216} - 1 \approx 2^{611}$	4 mins
	7	113	106	$2^{113}7^{106} - 1 \approx 2^{411}$	38 mins
	11	99	80	$2^{99}11^{80} - 1 \approx 2^{376}$	$\approx$ 3 hours
3	5	79	88	$4 \cdot 3^{79}5^{88} - 1 \approx 2^{326}$	72 s
	7	102	73	$4 \cdot 3^{102}7^{73} - 1 \approx 2^{369}$	21 mins
5	7	107	102	$4 \cdot 5^{107}7^{102} - 1 \approx 2^{537}$	50 mins

Table: Timings of the attack for different choices of parameters

Thank you!