Kani's Lemma over quadratic twists

Searching for universal gluing

Max Duparc

Swissogeny Days

Elliptic curves

Elliptic curve isomorphism duality

Elliptic curves are either:

standard curves

$$E_A: zy^2 = x^3 + Ax^2z + xz^2 = x(x - \alpha z)(x - \alpha^{-1}z)$$

quadratic twists

$$E_A^{\top}$$
: $Bzy^2 = x^3 + Ax^2z + xz^2$

with $B \in \mathbb{F}_q$ non-quadratic residue.

Properties

- $E_A \cap E_A^{\top} = \langle (0:0:1), (\alpha:0:1) \rangle$.
- \bullet E_A supersingular then

$$\mathcal{E}_A(\mathbb{F}_{p^{2n}})\cong \mathbb{Z}_{p^n\pm 1}^2$$
 and $\mathcal{E}_A^ op(\mathbb{F}_{p^{2n}})\cong \mathbb{Z}_{p^n\mp 1}^2$

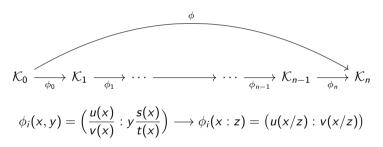
Kummer line

Let $\mathcal{K}_A = (E_A \cup E_A^\top)/_{\pm 1}$ be the **Kummer line**

$$\theta: E_A \cup E_A^\top \longrightarrow \mathcal{K}_A = \mathbb{P}^1$$
$$(x:y:z) \longrightarrow (x:z)$$
$$0 \longrightarrow (1:0)$$

DUPARC (EPFL) $(2^n, 2^n)$ over twists 2/14

Dim 1 isogeny

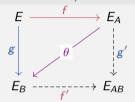


ightharpoonup Can evaluate isogeny over the quadratic twist (up to ± 1).

3 / 14

Kani's Lemma

Lemma (Kani's Lemma)



$$\deg(f) + \deg(g) = a + b = N$$
$$\gcd(a, b) = 1$$

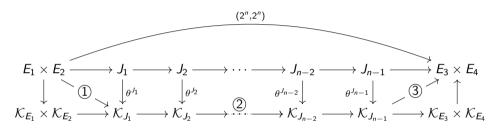
$$E_A \times E_B \xrightarrow{F:=\begin{pmatrix} \widehat{f} & -\widehat{g} \\ g' & f' \end{pmatrix}} E \times E_{AB}$$

$$\ker(F) = \left\{ \left(f(P), -g(P) \right) \middle| P \in E[N] \right\}$$
$$= \left\{ \left([N - b]P, -\theta(P) \right) \middle| P \in E_A[N] \right\}$$

In this presentation:

- ▶ We extend Kani's Lemma on the quadratic twist with $N = 2^{\bullet}$.
- ▶ We also propose a more efficient gluing.

[DMPR23]: $(2^n, 2^n)$ isogenies between product of elliptic curves



- 1. **Gluing**: Elliptic curves $\xrightarrow{(2,2)}$ Kummer surface.
- 2. **Generic**: Kummer surface $\xrightarrow{(2,2)}$ Kummer surface.
- 3. **Spliting**: Kummer surface $\xrightarrow{(2,2)}$ Elliptic curves.
- ▶ <u>Problem</u>: Gluing does not naturally work on the quadratic twist.

Theta structure: Simplified

Definition (Theta structure)

Let A be a principally polarised abelian variety of dimension g. A 2-theta structure is an embedding into the **Kummer variety** \mathcal{K}_A :

$$\theta^A: A_{l+1} \longrightarrow \mathcal{K}_A \subseteq \mathbb{P}^{2^g-1}$$

that is induced by a symplectic basis¹ $\langle S_1, \dots, S_g \rangle \oplus \langle T_1, \dots, T_g \rangle$ of A[2].

• **Example**: Let E_A and $P = (x : y : z) \in E_A$. Then:

$$\theta^{E_A}(P) = (a(x-z) : b(x+z)) = \begin{pmatrix} a & -a \\ b & b \end{pmatrix} \theta(P)$$

with $(a^2 : b^2) = (\alpha + 1 : \alpha - 1)$

$$\theta^{E_A} \sim \langle (\alpha:0:1) \rangle \oplus \langle (0:0:1) \rangle$$

DUPARC (EPFL)

 $^{^{1}}w(S_{i}, S_{i}) = 1 = w(T_{i}, T_{i}) \text{ and } w(S_{i}, T_{i}) = (-1)^{\delta_{i,j}}$

Duplication formula

• Hadamard transform \mathcal{H} induces a duality:

• Let $K = \langle T_1, \cdots, T_g \rangle \subset A[2]$ and $\phi : A \to B$ the $(2, 2, \cdots, 2)$ isogeny with $\ker(\phi) = K$. We then have the **Duplication Formula**:

$$\mathcal{H}\Big(\theta^A\big(P+Q\big)\odot\theta^A\big(P-Q\big)\Big)=\widetilde{\theta}^B\big(\phi(P)\big)\odot\widetilde{\theta}^B\big(\phi(Q)\big)$$

Duparc (EPFL) $(2^n, 2^n)$ over twists 7/14

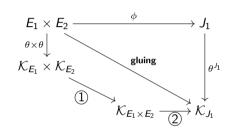
Gluing

Let
$$P = (P_1, P_2) \in E_1 \times E_2$$
.

1. $E_1 \times E_2 \xrightarrow{\textcircled{1}} \mathcal{K}_{E_1 \times E_2}$ is defined as:

$$P o \mathbf{N} \cdot ig(heta(P_1) \otimes heta(P_2)ig)$$

 $\mathbf{N} \in \mathsf{GL}_4(\mathbb{F}_q)$ such that $\ker(\phi)[2]$ is $\langle T_1, T_2
angle$ for $heta^{E_1 imes E_2}$



2. Apply the following duplication formula:

$$\mathcal{H}\Big(\theta^{E_1\times E_2}\big(P\big)\odot\theta^{E_1\times E_2}\big(P\big)\Big)=\widetilde{\theta}^{J_1}\big(\phi(P)\big)\odot\widetilde{\theta}^{J_1}\big(0\big)$$

Problem: $E_1 \times E_2$ reducible, we may have $\mathcal{H}\left(\theta^{E_1 \times E_2}(0) \odot \theta^{E_1 \times E_2}(0)\right) = 0 \iff \widetilde{\theta}^{J_1}(0)_i = 0.$

▶ Can only retrieve 3 component of $\widetilde{\theta}^{J_1}(\phi(P))$.

Duparc (EPFL) $(2^n, 2^n)$ over twists 8/14

The Gluing algorithm

$$\begin{split} \mathcal{H}\Big(\theta^{E_1\times E_2}\big(P\big)\odot\theta^{E_1\times E_2}\big(P\big)\Big) &= \widetilde{\theta}^{J_1}\big(\phi(P)\big)\odot\widetilde{\theta}^{J_1}\big(0\big)\\ \mathcal{H}\Big(\theta^{E_1\times E_2}\big(P+X\big)\odot\theta^{E_1\times E_2}\big(P+X\big)\Big) &= \widetilde{\theta}^{J_1}\big(\phi(P+X)\big)\odot\widetilde{\theta}^{J_1}\big(0\big) \end{split}$$

• Say $\widetilde{\theta}^{J_1}(0) = (0:\beta:\gamma:\delta)$ and $\widetilde{\theta}^{J_1}(\phi(P)) = (x:y:z:w)$. Then:

$$\widetilde{\theta}^{J_1}(\phi(P)+\phi(X))\odot\widetilde{\theta}^{J_1}(0)=\left(0:\underbrace{x\beta}_{\text{sol.}}:w\gamma:z\delta\right)$$

► Total cost: 66M + 12S + 2C + 58A.

Problem: What is P + X when $P \in E^{\top}$ and $X \in E$?

Solution

Key insight

$$\mathcal{H}\Big(heta^{ extsf{E}_1 imes extsf{E}_2}ig(P+Qig)\odot heta^{ extsf{E}_1 imes extsf{E}_2}ig(P-Qig)\Big)=\widetilde{ heta}^{J_1}ig(\phi(P)ig)\odot\widetilde{ heta}^{J_1}ig(\phi(Q)ig)$$

- 1. $\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)$ is always defined over \mathbb{F}_q .
 - ▶ Following Riemann Position Theorem.
- 2. This separate $\phi(P)$ and $\phi(Q)$.
 - ▶ Q can be outside $ker(\phi)[4]$.
- 3. It can be efficiently computed.

Computing $\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)$ efficiently

• Given $P \neq Q \in E_A \cup E_A^{\top}$, then x_{\oplus} and x_{\ominus} are "conjugate".

Lemma

 $\exists \mathsf{u},\mathsf{v},\mathsf{w} \in \mathbb{F}_q$ s.t. $(x_\oplus,z_\oplus) = \theta(P+Q)$ and $(x_\ominus,z_\ominus) = \theta(P-Q)$ are of the form:

$$\begin{cases} x_{\oplus} = u - \delta_{P} \delta_{Q} v \\ x_{\ominus} = u + \delta_{P} \delta_{Q} v \\ z_{\oplus} = z_{\ominus} = w \end{cases}$$

with $\delta_P = (\sqrt{B})^{\mathbf{1}_{P \in E_A^\top}}$.

$$\begin{cases} u = z_{Q}z_{P}(\delta_{Q}^{2}y_{Q}^{2}z_{P}^{2} + \delta_{P}^{2}y_{P}^{2}z_{Q}^{2}) - (Az_{P}z_{Q} + x_{P}z_{Q} + x_{Q}z_{P})(x_{Q}z_{P} - x_{P}z_{Q})^{2} \\ v = z_{P}^{2}z_{Q}^{2}y_{Q}y_{P} \\ w = (x_{Q}z_{P} - x_{P}z_{Q})^{2}z_{P}z_{Q} \end{cases}$$

Computing
$$\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)$$

Theorem

Let
$$P, Q \in (E_1 \cup E_1^\top) \times (E_2 \cup E_2^\top)$$
 with $P = (P_1, P_2)$ and $Q = (Q_1, Q_2)$ such that $\delta = \delta_{P_1} \delta_{Q_1} = \delta_{P_2} \delta_{Q_2}$:
$$\theta^{E_1 \times E_2} (P + Q) \odot \theta^{E_1 \times E_2} (P - Q) = \left((\mathbf{N}\vec{u}) \odot (\mathbf{N}\vec{v}) \right) - \delta^2 \left((\mathbf{N}\vec{v}) \odot (\mathbf{N}\vec{v}) \right)$$

with
$$\vec{u} = \begin{pmatrix} u_1 u_2 + \delta^2 v_1 v_2 \\ u_1 w_2 \\ w_1 u_2 \\ w_1 w_2 \end{pmatrix}$$
 and $\vec{v} = \begin{pmatrix} v_1 u_2 + u_1 v_2 \\ v_1 w_2 \\ w_1 v_2 \\ 0 \end{pmatrix}$

▶ If $Q \in E_1 \times E_2$, works for $P \in (E_1 \times E_2) \cup (E_1^\top \times E_2^\top)$.

Improved Gluing

• Precomputation:

- Compute Q s.t. $\theta^{J_1}(\phi(Q)) = (\alpha : \beta : \gamma : \delta)$ with $\alpha\beta\gamma\delta \neq 0$
- Save Q and $(\alpha^{-1} : \beta^{-1} : \gamma^{-1} : \delta^{-1})$.

New Gluing:

• To evaluate P, simply use:

$$\mathcal{H}\Big(\theta^{E_1\times E_2}\big(P+Q\big)\odot\theta^{E_1\times E_2}\big(P-Q\big)\Big)=\widetilde{\theta}^{J_1}\big(\phi(P)\big)\odot\widetilde{\theta}^{J_1}\big(\phi(Q)\big)$$

- ▶ Can evaluate all $P \in (E_1 \times E_2) \cup (E_1^\top \times E_2^\top)$.
 - Covers all useful case for Kani's Lemma.
- ► Total cost: $61M + 12S + 2C (+10C) + 52A.^2$

¹Ex: $Q \notin (E_1 \times E_2)[4]$ and $Q = (Q_1, Q_2)$ with $Q_i \neq 0$.

 $^{^{2}}$ vs. 66M + 12S + 2C + 58A

Conclusion

- Using Kani's Lemma over quadratic twist can be efficiently computed.
 - Useful for SQIPrime, POKE, DeuringVRF...
- This method can be made universal: i.e. $P \in (E_1 \cup E_1^\top) \times (E_2 \cup E_2^\top)$. (but slower)
- Question: Where are the zeros of $\theta^{J_1}(P)$ with $P=(P_1,0),(0,P_2)$?

$$\mathcal{H}\Big(heta^A(P+Q)\odot heta^A(P-Q)\Big)=\widetilde{ heta}^B(\phi(P))\odot\widetilde{ heta}^B(\phi(Q))$$

Happy to discuss your comments and questions!

References I



Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert, An algorithmic approach to (2,2)-isogenies in the theta model and applications to isogeny-based cryptography, Cryptology ePrint Archive, Paper 2023/1747, 2023.



Sabrina Kunzweiler, Luciano Maino, Tomoki Moriva, Christophe Petit, Giacomo Pope, Damien Robert, Miha Stopar, and Yan Bo Ti, Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3. Cryptology ePrint Archive, Paper 2024/1732, 2024.



Damien Robert, Some notes on algorithms for abelian varieties, Cryptology ePrint Archive, Paper 2024/406, 2024.

The Riemann relation

Theorem (Riemann positions)

Let $z_1, z_2, z_3, z_4 \in \mathbb{F}_q$ such that $z_1 + z_2 + z_3 + z_4 = 2z$ and $z_i' = z - z_i$. Then, for all $\chi \in \widehat{\mathbb{Z}}_2^2$, $k_1, k_2, k_3, k_4 \in \mathbb{Z}_2^2$ such that $k_i' = m - k_i$, we have that

$$\left(\sum_{t} \chi(t) \theta_{k_1+t}(z_1) \theta_{k_2+t}(z_2)\right) \left(\sum_{t} \chi(t) \theta_{k_3+t}(z_3) \theta_{k_4+t}(z_4)\right) = \left(\sum_{t} \chi(t) \theta_{k'_1+t}(z'_1) \theta_{k'_2+t}(z'_2)\right) \left(\sum_{t} \chi(t) \theta_{k'_3+t}(z'_3) \theta_{k'_4+t}(z'_4)\right)$$

- Does not help.
 - Only provides tautological or 0 = 0 equality.
 - Using 4-theta structure, we get that:

$$\sum_t \chi(t) heta_t(P+T) heta_t(P-T) = \pm 2 \sqrt{\left(\sum_t \chi(t) heta_t(P) heta_t(P)
ight) \left(\sum_t \chi(t) heta_t(T) heta_t(T)
ight)}$$

Duparc (EPFL) $(2^n, 2^n)$ over twists 2

Consequence of the theorem

P_1	P_2	Q_1	Q_2	Protocol
0	0	0	0	Addition & Field exten.
0	0	1	1	Field exten.
1	1	0	0	Field exten.
0	1	0	1	Addition
1	0	1	0	Addition
0	1	1	0	Field exten.
1	0	0	1	Field exten.
1	1	1	1	Addition & Field exten.

Table: Table of which algorithm to retrieve $\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)$, depending on the position of P_1, P_2, Q_1 and Q_2 . 0 if in E_i and 1 if in E_i^{\top} .

Theta structure: Simplified

Definition (Theta structure)

Let A be a principally polarised abelian variety of dimension g. A n-theta structure is an embedding into the **Kummer variety** \mathcal{K}_A :

$$\theta^A:A_{/\pm 1}\longrightarrow \mathcal{K}_A\subseteq \mathbb{P}^{n^g-1}$$

that is induced by a symplectic structure over A[n].

- 1. $\theta^A(0)$ characterized A up to isomorphism.
 - n = 2, g = 1: Let E_A and $P = (x : y : z) \in E_A$. Then:

$$\theta^{E_A}(0) = (a:b) \text{ with } (a^2:b^2) = (\alpha+1:\alpha-1)$$

$$\theta^{E}(P) = (a(x-z):b(x+z))$$

Duparc (EPFL) $(2^n, 2^n)$ over twists 4/8

Kummer surfaces

- 1. $\theta^A(0)$ characterized A up to isomorphism.
 - Case n = g = 2: $\theta^A(0) = (a:b:c:d)$, $(A:B:C:D) = \mathcal{H}(a^2:b^2:c^2:d^2)$ then, A is isomorphic to the abelian surface defined by

$$\begin{split} p(X_1,X_2,X_3,X_4) &= X_1^4 + X_2^4 + X_3^4 + X_4^4 - 2EX_1X_2X_3X_4 - F(X_1^2X_4^2 + X_2^2X_3^2) - G(X_1^2X_3^2 + X_2^2X_4^2) - H(X_1^2X_2^2 + X_3^2X_4^2) \\ F &= (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2) \\ &\qquad \qquad G &= (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2) \\ &\qquad \qquad H &= (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2) \\ E &= 256abcdA^2B^2C^2D^2/(a^2d^2 - b^2c^2)(a^2c^2 - b^2d^2)(a^2b^2 - c^2d^2) \end{split}$$

DUPARC (EPFL) $(2^n, 2^n)$ over twists 5/8

 $^{^2\}mathcal{H}$ denote the Hadamard transformation.

Theta structure and torsion points

- 2. Images through θ^A of translation by A[n] are characterised by the weil pairing over A[n].
 - $\mathbb{Z}_n^{2g} \cong A[n] \cong \mathbb{Z}_n^g \times \widehat{\mathbb{Z}_n^g}$ we can write $A[n] \ni X \sim (x, \chi)$ s.t.:

$$w(X_1, X_2) = \chi_2(x_1)/\chi_1(x_2)$$

$$\theta_j^A(P+X) = \chi(j)\theta_{x+j}^A(P)$$

• Elliptic curves: $E[2] = \langle (0:0:1), (\alpha:0:1) \rangle$ the standard basis. Then, for P = (x:y:z):

$$\theta^{E}(P) = (a(x-z) : b(x+z))$$

$$\theta^{E}((0:0:1)) = (-a:b)$$
 $\theta^{E}((\alpha:0:1)) = (ab^{2}:ba^{2}) = (b:a)$

$$(0:0:1) \sim (0,(-1)^{\vec{1}\cdot\vec{i}})$$
 $(\alpha:0:1) \sim (1,(-1)^{\vec{0}\cdot\vec{i}})$

 ${}^{0}\widehat{G} = \operatorname{Hom}(G, \mathbb{S}^{1})$

 $(2^n, 2^n)$ over twists

Theta structure of surfaces

• Surfaces: $A[2] = \langle S_1, S_2 \rangle \oplus \langle T_1, T_2 \rangle$ a symplectic basis³. Then, for $\theta^A(0) = (a : b : c : d)$:

$$\theta^{A}(S_{1}) = (b:a:d:c) \qquad \qquad \theta^{A}(T_{1}) = (a:-b:c:-d)$$

$$\theta^{A}(S_{2}) = (c:d:a:b) \qquad \qquad \theta^{A}(T_{2}) = (a:b:-c:-d)$$

$$S_{1} = (01,(-1)^{0\vec{0}\cdot\vec{i}}), \quad S_{2} = (10,(-1)^{0\vec{0}\cdot\vec{i}}) \qquad \qquad T_{1} = (00,(-1)^{0\vec{1}\cdot\vec{i}}), \quad T_{2} = (00,(-1)^{1\vec{0}\cdot\vec{i}})$$

$$\theta^{A}_{i} \text{ theta structure} \longleftrightarrow S_{1}, S_{2}, T_{1}, T_{2} \text{ symplectic basis.}$$

3. The Hadamard transform \mathcal{H} induces a duality in theta structure:

$$\theta_i^A \longleftarrow \stackrel{\mathcal{H}}{\longleftarrow} \longrightarrow \widetilde{\theta}_i^A$$

$$S_1, S_2; T_1, T_2 \longleftarrow \stackrel{\mathcal{H}}{\longleftarrow} T_1, T_2; S_1, S_2$$

 $^{3}w(T_{1},T_{2})=1=w(S_{1},S_{2})$ and $w(T_{i},S_{i})=(-1)^{\delta_{i,j}}$

DUPARC (EPEL)

 $(2^n, 2^n)$ over twists

Theta structure and isogenies

- 4. θ -structures are compatible with isogenies.
 - Let $K = \langle T_1, \cdots, T_g \rangle \subset A[2]$ and $\phi : A \to B$ the $(2, 2, \cdots, 2)$ isogeny with $\ker(\phi) = K$. We then have the **Duplication Formula**:

$$\mathcal{H}\Big(heta^Aig(P+Qig)\odot heta^Aig(P-Qig)\Big)=\widetilde{ heta}^Big(\phi(P)ig)\odot\widetilde{ heta}^Big(\phi(Q)ig)$$

• Example: Let P = Q = 0. Then

$$\mathcal{H}ig(heta^A(0)\odot heta^A(0)ig)=\widetilde{ heta}^B(0)\odot\widetilde{ heta}^B(0)$$

$$A \simeq \theta^A(0) \longrightarrow \theta^B(0) \simeq B$$