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

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

$$E_A(\mathbb{F}_{p^{2n}}) \cong \mathbb{Z}^2_{p^n \pm 1} \text{ and } E_A^\top(\mathbb{F}_{p^{2n}}) \cong \mathbb{Z}^2_{p^n \mp 1}$$

Kummer line

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

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

Dim 1 isogeny

$$
\begin{tikzcd}
\mathcal{K}_0 \arrow[r, "\phi_0"'] \arrow[rrrrrr, bend left, "\phi"] & \mathcal{K}_1 \arrow[r, "\phi_1"'] & \cdots \arrow[r] & \cdots \arrow[r, "\phi_{n-1}"'] & \mathcal{K}_{n-1} \arrow[r, "\phi_n"'] & \mathcal{K}_n
\end{tikzcd}
$$

$$\phi_i(x, y) = \left(\frac{u(x)}{v(x)} : y\frac{s(x)}{t(x)}\right) \longrightarrow \phi_i(x : z) = \big(u(x/z) : v(x/z)\big)$$

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

Kani's Lemma

Lemma (Kani's Lemma)

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "g"'] & E_A \arrow[d, dashed, "g'"] \arrow[dl, "\theta"] \\ E_B \arrow[r, dashed, "f'"'] & E_{AB} \end{tikzcd}$$

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

$$\gcd(a, b) = 1$$

$$\implies$$

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

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

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

$$
\begin{tikzcd}
E_1 \times E_2 \arrow[r] \arrow[d] \arrow[dr, "①"] \arrow[rrrrrr, bend left, "{(2^n,2^n)}"] & J_1 \arrow[r] \arrow[d, "\theta^{J_1}"] & J_2 \arrow[r] \arrow[d, "\theta^{J_2}"] & \cdots \arrow[r] & J_{n-2} \arrow[r] \arrow[d, "\theta^{J_{n-2}}"'] & J_{n-1} \arrow[r] \arrow[d, "\theta^{J_{n-1}}"'] & E_3 \times E_4 \\
\mathcal{K}_{E_1} \times \mathcal{K}_{E_2} \arrow[r] & \mathcal{K}_{J_1} \arrow[r] & \mathcal{K}_{J_2} \arrow[r] & \cdots \arrow[phantom, "②"] \arrow[r] & \mathcal{K}_{J_{n-2}} \arrow[r] & \mathcal{K}_{J_{n-1}} \arrow[r] \arrow[ur, "③"] & \mathcal{K}_{E_3} \times \mathcal{K}_{E_4} \arrow[u]
\end{tikzcd}
$$

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.

- Problem: 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** $\mathcal{K}_A$:

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

that is *induced by a symplectic basis*[1] $\langle S_1, \cdots, S_g \rangle \oplus \langle T_1, \cdots, T_g \rangle$ of $A[2]$.

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

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

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

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

[1] $w(S_i, S_j) = 1 = w(T_i, T_j)$ and $w(S_i, T_j) = (-1)^{\delta_{i,j}}$

Duplication formula

- Hadamard transform $\mathcal{H}$ induces a duality:

$$\mathcal{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$\begin{array}{ccc} \theta^A & \xleftrightarrow{\qquad\qquad\mathcal{H}\qquad\qquad} & \widetilde{\theta}^A \\ \wr & & \wr \\ \langle S_1, S_2 \rangle \oplus \langle T_1, T_2 \rangle & \xleftrightarrow{\quad\mathcal{H}\quad} & \langle T_1, T_2 \rangle \oplus \langle S_1, S_2 \rangle \end{array}$$

- Let $K = \langle T_1, \cdots, T_g \rangle \subset A[2]$ and $\phi : A \to B$ the $(\overbrace{2, 2, \cdots, 2}^{g \text{ times}})$ isogeny with $\ker(\phi) = K$. We then have the **Duplication Formula**:

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

Gluing

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

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

$$P \to \mathbf{N} \cdot \big(\theta(P_1) \otimes \theta(P_2)\big)$$

$$\begin{tikzcd} E_1 \times E_2 \arrow[rr, "\phi"] \arrow[d, "\theta\times\theta"'] \arrow[drr, "\textbf{gluing}"] & & J_1 \arrow[d, "\theta^{J_1}"] \\ \mathcal{K}_{E_1} \times \mathcal{K}_{E_2} \arrow[r, "①"'] & \mathcal{K}_{E_1 \times E_2} \arrow[r, "②"'] & \mathcal{K}_{J_1} \end{tikzcd}$$

$\mathbf{N} \in \mathrm{GL}_4(\mathbb{F}_q)$ such that $\ker(\phi)[2]$ is $\langle T_1, T_2 \rangle$ for $\theta^{E_1 \times E_2}$

2. Apply the following **duplication formula**:

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

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

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

The Gluing algorithm

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

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

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

- Total cost: $66\mathbf{M}+12\mathbf{S}+2\mathbf{C}+58\mathbf{A}$.

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

Solution

Key insight

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

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

$\exists$u,v,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 $\delta = \delta_{P_1}\delta_{Q_1} = \delta_{P_2}\delta_{Q_2}$:

$$\theta^{E_1\times E_2}(P+Q)\odot\theta^{E_1\times E_2}(P-Q) = \Big((\mathbf{N}\vec{u})\odot(\mathbf{N}\vec{u})\Big) - \delta^2\Big((\mathbf{N}\vec{v})\odot(\mathbf{N}\vec{v})\Big)$$

$$\text{with } \vec{u} = \begin{pmatrix} u_1u_2 + \delta^2 v_1v_2 \\ u_1w_2 \\ w_1u_2 \\ w_1w_2 \end{pmatrix} \text{ and } \vec{v} = \begin{pmatrix} v_1u_2 + u_1v_2 \\ v_1w_2 \\ w_1v_2 \\ 0 \end{pmatrix}$$

- 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[1] 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:

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

- ▶ 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: $61\mathbf{M} + 12\mathbf{S} + 2\mathbf{C}$ $(+10\mathbf{C})$ $+ 52\mathbf{A}$.[2]

[1] Ex: $Q \notin (E_1 \times E_2)[4]$ and $Q = (Q_1, Q_2)$ with $Q_i \neq 0$.
[2] vs. $66\mathbf{M} + 12\mathbf{S} + 2\mathbf{C} + 58\mathbf{A}$

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 $P = (P_1, 0), (0, P_2)$?

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

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 Moriya, 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:

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

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:

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

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

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

$$p(X_1, X_2, X_3, X_4) = X_1^4 + X_2^4 + X_3^4 + X_4^4 - 2EX_1X_2X_3X_4 - F(X_1^2X_4^2 + X_2^2X_3^2) - G(X_1^2X_3^2 + X_2^2X_4^2) - H(X_1^2X_2^2 + X_3^2X_4^2)$$

$$F = (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2) \qquad G = (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2)$$

$$H = (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2)$$

$$E = 256abcdA^2B^2C^2D^2/(a^2d^2 - b^2c^2)(a^2c^2 - b^2d^2)(a^2b^2 - c^2d^2)$$

[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 $P = (x:y:z)$:

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

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

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

---

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

Theta structure of surfaces

- **Surfaces:** $A[2] = \langle S_1, S_2 \rangle \oplus \langle T_1, T_2 \rangle$ a symplectic basis[3]. Then, for $\theta^A(0) = (a : b : c : d)$:

$$\theta^A(S_1) = (b : a : d : c) \qquad \theta^A(T_1) = (a : -b : c : -d)$$

$$\theta^A(S_2) = (c : d : a : b) \qquad \theta^A(T_2) = (a : b : -c : -d)$$

$$S_1 = (01, (-1)^{\vec{00}\cdot\vec{i}}),\ S_2 = (10, (-1)^{\vec{00}\cdot\vec{i}}) \qquad T_1 = (00, (-1)^{\vec{01}\cdot\vec{i}}),\ T_2 = (00, (-1)^{\vec{10}\cdot\vec{i}})$$

$$\theta_i^A \text{ theta structure} \longleftrightarrow S_1, S_2, T_1, T_2 \text{ symplectic basis.}$$

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

$$\theta_i^A \xleftrightarrow{\quad\mathcal{H}\quad} \widetilde{\theta}_i^A$$

$$S_1, S_2; T_1, T_2 \xleftrightarrow{\quad\mathcal{H}\quad} T_1, T_2; S_1, S_2$$

[3] $w(T_1, T_2) = 1 = w(S_1, S_2)$ and $w(T_i, S_j) = (-1)^{\delta_{i,j}}$

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 $(\overbrace{2, 2, \cdots, 2}^{g \text{ times}})$ isogeny with $\ker(\phi) = K$. We then have the **Duplication Formula**:

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

- **Example:** Let $P = Q = 0$. Then

$$\mathcal{H}\Big(\theta^A(0) \odot \theta^A(0)\Big) = \widetilde{\theta}^B(0) \odot \widetilde{\theta}^B(0)$$

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