Computing cyclic isogenies between abelian surfaces over finite fields

Marius Vuille

joint with A. Dudeanu, D. Jetchev and D. Robert

AGCCT, 22.06.2017

Context

H1 $(A, \mathcal{L}_0)$ ordinary and simple, principally polarized abelian surface over $\mathbb{F}_q$
($A = \mathrm{Jac}(H)$, H genus 2 hyperelliptic curve over $\mathbb{F}_q$)

Context

H1 $(A, \mathcal{L}_0)$ ordinary and simple, principally polarized abelian surface over $\mathbb{F}_q$
($A = \mathrm{Jac}(H)$, H genus 2 hyperelliptic curve over $\mathbb{F}_q$)

H2 G finite subgroup-scheme over $\mathbb{F}_q$ of prime order $\ell \nmid q$
($\Rightarrow G(\overline{\mathbb{F}}_q)$ cyclic) and such that A/G principally polarizable

Context

- H1 $(A, \mathcal{L}_0)$ ordinary and simple, principally polarized abelian surface over $\mathbb{F}_q$
  ($A = \text{Jac}(H)$, H genus 2 hyperelliptic curve over $\mathbb{F}_q$)
- H2 G finite subgroup-scheme over $\mathbb{F}_q$ of prime order $\ell \nmid q$
  ($\Rightarrow G(\overline{\mathbb{F}}_q)$ cyclic) and such that A/G principally polarizable

Want to compute the isogeny

$$f\colon A \to A/G, \text{ i.e.,}$$

- compute H' genus 2 hyperelliptic curve over $\mathbb{F}_q$ such that $A/G \cong \text{Jac}(H')$ (as p.p.a.v)
- for $x \in \text{Jac}(H)(\mathbb{F}_q)$, compute $f(x) \in \text{Jac}(H')(\mathbb{F}_q)$

Main result

Theorem (Dudeanu, Jetchev, Robert, V.)

Given the equation of a curve H and given a generator t of G (in Mumford coordinates) such that $A = \mathrm{Jac}(H)$ and G satisfy H1 and H2, for each choice of p.p. on A/G we can compute the isogeny $f\colon A \to A/G$ (on points $x \in A(\mathbb{F}_q)$ of order coprime to ℓ).

Remarks

- We have an implementation of the first part (computing H') on Magma, second part will follow.

Remarks

- We have an implementation of the first part (computing H') on Magma, second part will follow.
- Will see more about choices of principal polarization on A/G.

Applications

- transporting DLP

Applications

- transporting DLP
- point counting in dimension 2

Applications

- transporting DLP
- point counting in dimension 2
- computing endomorphsim rings

Polarizability of A/G

$(A, \mathcal{L}_0)$ ordinary and simple, principally polarized abelian surface over $\mathbb{F}_q$

Polarizability of A/G

$(A, \mathcal{L}_0)$ ordinary and simple, principally polarized abelian surface over $\mathbb{F}_q$

- $K := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$ - quartic CM-field

Polarizability of A/G

$(A, \mathcal{L}_0)$ ordinary and simple, principally polarized abelian surface over $\mathbb{F}_q$

- $K := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$ - quartic CM-field
- $\mathrm{End}^+_{\overline{\mathbb{F}}_q}(A) \subset \mathrm{End}_{\overline{\mathbb{F}}_q}(A)$ - real endomorphisms (stable under Rosati involution)

Polarizability of A/G

- $\beta \in \mathrm{End}^{+}_{\overline{\mathbb{F}}_q}(A)$ totally positive real endomorphism

$$\begin{array}{ccc} A & \xrightarrow{\ \beta\ } & A \\ & & \Big\downarrow{\scriptstyle \varphi_{\mathcal{L}_0}} \\ & & A^{\vee} \end{array}$$

Polarizability of A/G

- $\beta \in \mathrm{End}^{+}_{\overline{\mathbb{F}}_q}(A)$ totally positive real endomorphism

$$\begin{array}{ccc} A & \xrightarrow{\beta} & A \\ & & \big\downarrow{\scriptstyle \varphi_{\mathcal{L}_0}} \\ & & A^{\vee} \end{array}$$

- isogeny $\varphi_{\mathcal{L}_0} \circ \beta$ arises as the polarization isogeny of an ample line bundle $\mathcal{L}_0^{\beta}$, i.e.,

$$\begin{array}{ccc} A & \xrightarrow{\beta} & A \\ & {\scriptstyle \varphi_{\mathcal{L}_0^{\beta}}} \searrow & \big\downarrow{\scriptstyle \varphi_{\mathcal{L}_0}} \\ & & A^{\vee} \end{array}$$

Polarizability of A/G

- $K(\mathcal{L}_0^\beta) := \ker\left(\varphi_{\mathcal{L}_0^\beta} \colon A \to A^\vee\right) = \ker\beta$ - abelian group with symplectic pairing, induced by commutator pairing of Mumford theta group

Polarizability of A/G

- $K(\mathcal{L}_0^\beta) := \ker\left(\varphi_{\mathcal{L}_0^\beta} \colon A \to A^\vee\right) = \ker\beta$ - abelian group with symplectic pairing, induced by commutator pairing of Mumford theta group
- Then : A/G principally polarizable if and only if $\exists \beta \in \mathrm{End}^+_{\overline{\mathbb{F}}_q}(A)$, β totally positive, such that $G \subset K(\mathcal{L}_0^\beta) = \ker\beta$ maximally isotropic.

Remarks

- Two distinct choices of totally positive real endomorphisms β and β' (satisfying $G \subset \ker \beta$ and $G \subset \ker \beta'$ maximally isotropic for the corresponding pairing) yield two distinct principal polarizations on A/G.

Remarks

- Two distinct choices of totally positive real endomorphisms β and β' (satisfying $G \subset \ker \beta$ and $G \subset \ker \beta'$ maximally isotropic for the corresponding pairing) yield two distinct principal polarizations on A/G.
- Adding β to the input of the algorithm uniquely determines the principal polarization on A/G and hence H' (up to isomorphism).

Example 1

- $(A, \mathcal{L}_0)$ p.p. abelian surface over $\mathbb{F}_q$, ℓ odd prime, $\ell \nmid q$, $\beta = [\ell]$ is a totally positive real endomorphism, $\deg \beta = \ell^4$

Example 1

- $(A, \mathcal{L}_0)$ p.p. abelian surface over $\mathbb{F}_q$, ℓ odd prime, $\ell \nmid q$, $\beta = [\ell]$ is a totally positive real endomorphism, $\deg \beta = \ell^4$
- $G \subset \ker \beta = A[\ell]$ maximally isotropic $\Rightarrow G \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$

Example 1

- $(A, \mathcal{L}_0)$ p.p. abelian surface over $\mathbb{F}_q$, ℓ odd prime, $\ell \nmid q$, $\beta = [\ell]$ is a totally positive real endomorphism, $\deg \beta = \ell^4$
- $G \subset \ker \beta = A[\ell]$ maximally isotropic $\Rightarrow G \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$
- Cosset-Robert compute $A \to A/G$, called an (ℓ, ℓ)-isogeny

Example 2

- $(A, \mathcal{L}_0)$ p.p. abelian surface over $\mathbb{F}_q$, $\beta \in \mathrm{End}^+_{\overline{\mathbb{F}}_q}(A) \setminus \mathbb{Z}$, β totally positive, $\deg \beta = \ell^2$, $\ell > 2$ prime, $\ell \nmid q$

Example 2

- $(A, \mathcal{L}_0)$ p.p. abelian surface over $\mathbb{F}_q$, $\beta \in \mathrm{End}^+_{\overline{\mathbb{F}}_q}(A) \setminus \mathbb{Z}$, β totally positive, $\deg \beta = \ell^2$, $\ell > 2$ prime, $\ell \nmid q$
- $G \subset \ker \beta$ maximally isotropic $\Rightarrow G \cong \mathbb{Z}/\ell\mathbb{Z}$

Example 2

- $(A, \mathcal{L}_0)$ p.p. abelian surface over $\mathbb{F}_q$, $\beta \in \mathrm{End}^+_{\overline{\mathbb{F}}_q}(A) \setminus \mathbb{Z}$, β totally positive, $\deg \beta = \ell^2$, $\ell > 2$ prime, $\ell \nmid q$
- $G \subset \ker \beta$ maximally isotropic $\Rightarrow G \cong \mathbb{Z}/\ell\mathbb{Z}$
- provided A is ordinary and simple and G is Galois-stable, we can compute $A \to A/G$, called a β-cyclic isogeny

Example 2

- $(A, \mathcal{L}_0)$ p.p. abelian surface over $\mathbb{F}_q$, $\beta \in \mathrm{End}^+_{\overline{\mathbb{F}}_q}(A) \setminus \mathbb{Z}$, β totally positive, $\deg \beta = \ell^2$, $\ell > 2$ prime, $\ell \nmid q$
- $G \subset \ker \beta$ maximally isotropic $\Rightarrow G \cong \mathbb{Z}/\ell\mathbb{Z}$
- provided A is ordinary and simple and G is Galois-stable, we can compute $A \to A/G$, called a β-cyclic isogeny
- conversely, given G Galois-stable of prime order ℓ, provided there exists β totally positive of degree ℓ^2 and such that $\beta(G) = 0$, we can compute $A \to A/G$

Example 2

$$\begin{array}{rl} & \mathrm{End}_{\overline{\mathbb{F}}_q}(A) \subset K \\ & \quad | \\ \beta \in & \mathrm{End}^{+}_{\overline{\mathbb{F}}_q}(A) \subset K_+ \\ & \quad | \\ [\ell] \in & \mathbb{Z} \subset \mathbb{Q} \end{array}$$

Projective embeddings

Theta coordinates

- $\mathcal{L} := \mathcal{L}_0^{\otimes n}$, $n \geq 3$, then fixing a basis $\{\theta_i\}_i$ of $\Gamma(A, \mathcal{L})$ gives an embedding

$$A \hookrightarrow \mathbb{P}^{n^2-1}$$

Projective embeddings

Theta coordinates

- $\mathcal{L} := \mathcal{L}_0^{\otimes n}$, $n \geq 3$, then fixing a basis $\{\theta_i\}_i$ of $\Gamma(A, \mathcal{L})$ gives an embedding
$$A \hookrightarrow \mathbb{P}^{n^2-1}$$
- different choice of basis changes image of A by an element of $\mathrm{Aut}(\mathbb{P}^{n^2-1})$

Projective embeddings

Theta coordinates

- $\mathcal{L} := \mathcal{L}_0^{\otimes n}$, $n \geq 3$, then fixing a basis $\{\theta_i\}_i$ of $\Gamma(A, \mathcal{L})$ gives an embedding
$$A \hookrightarrow \mathbb{P}^{n^2-1}$$
- different choice of basis changes image of A by an element of $\mathrm{Aut}(\mathbb{P}^{n^2-1})$
- additional structure $\Theta_{\mathcal{L}}$ on $(A, \mathcal{L})$, called theta structure, determines ONE basis

- $\mathcal{L} := \mathcal{L}_0^{\otimes n}$, $n \geq 3$, then fixing a basis $\{\theta_i\}_i$ of $\Gamma(A, \mathcal{L})$ gives an embedding
$$A \hookrightarrow \mathbb{P}^{n^2-1}$$

- different choice of basis changes image of A by an element of $\mathrm{Aut}(\mathbb{P}^{n^2-1})$
- additional structure $\Theta_{\mathcal{L}}$ on $(A, \mathcal{L})$, called theta structure, determines ONE basis
- $(A, \mathcal{L}, \Theta_{\mathcal{L}})$ - polarized abelian variety with theta structure
$$A \hookrightarrow \mathbb{P}^{n^2-1}, \quad x \mapsto \left(\theta_i^{\Theta_{\mathcal{L}}}(x)\right)_{i \in K_1(\mathcal{L})}$$

- theta coordinates of x with respect to $\Theta_{\mathcal{L}}$

- $f\colon (A, \mathcal{L}, \Theta_{\mathcal{L}}) \to (B, \mathcal{M}, \Theta_{\mathcal{M}})$ isogeny of polarized abelian varieties with theta structures

- $f: (A, \mathcal{L}, \Theta_{\mathcal{L}}) \to (B, \mathcal{M}, \Theta_{\mathcal{M}})$ isogeny of polarized abelian varieties with theta structures
- Then : $\exists \lambda \in \overline{\mathbb{F}}_q^{\times}$ such that $\forall x \in A(\overline{\mathbb{F}}_q)$ and $\forall i \in K_1(\mathcal{M})$

$$\theta_i^{\Theta_{\mathcal{M}}}(f(x)) = \lambda \cdot \sum_{\substack{j \in K_1(\mathcal{L}) \\ f(j)=i}} \theta_j^{\Theta_{\mathcal{L}}}(x)$$

- $f : (A, \mathcal{L}, \Theta_{\mathcal{L}}) \to (B, \mathcal{M}, \Theta_{\mathcal{M}})$ isogeny of polarized abelian varieties with theta structures
- Then : $\exists \lambda \in \overline{\mathbb{F}}_q^{\times}$ such that $\forall x \in A(\overline{\mathbb{F}}_q)$ and $\forall i \in K_1(\mathcal{M})$

$$\theta_i^{\Theta_{\mathcal{M}}}(f(x)) = \lambda \cdot \sum_{\substack{j \in K_1(\mathcal{L}) \\ f(j)=i}} \theta_j^{\Theta_{\mathcal{L}}}(x)$$

- given the theta coordinates of $x \in A(\overline{\mathbb{F}}_q)$ wrt $\Theta_{\mathcal{L}}$, this is a formula for computing the theta coordinates of $f(x) \in B(\overline{\mathbb{F}}_q)$ wrt $\Theta_{\mathcal{M}}$

- H genus 2 hyperelliptic curve over $\mathbb{F}_q$ such that $A = \mathrm{Jac}(H)$ is ordinary and simple
- β totally positive real endomorphism of degree ℓ^2
- $t \in A(\overline{\mathbb{F}}_q)$ of order ℓ, such that $\beta(t) = 0$ and $G = \langle t \rangle$ defined over $\mathbb{F}_q$ ($\Rightarrow G \subset \ker \beta$ maximally isotropic)

The algorithm

- Fact 1 : we can convert points $x \in \mathrm{Jac}(H)(\overline{\mathbb{F}}_q)$ from Mumford coordinates to theta coordinates, for $\mathcal{L}_0^{\otimes 4}$ and for "a particular" theta structure $\Theta_{\mathcal{L}_0^{\otimes 4}}$

The algorithm

- Fact 1 : we can convert points $x \in \mathrm{Jac}(H)(\overline{\mathbb{F}}_q)$ from Mumford coordinates to theta coordinates, for $\mathcal{L}_0^{\otimes 4}$ and for "a particular" theta structure $\Theta_{\mathcal{L}_0^{\otimes 4}}$
- Fact 2 : knowing the theta coordinates of $0_{A/G}$ for $\mathcal{M}_0^{\otimes 4}$ ($\mathcal{M}_0$ induced by $\mathcal{L}_0$ and β) and for "a particular" theta structure $\Theta_{\mathcal{M}_0^{\otimes 4}}$, we can recover an equation for H'

The algorithm

- Fact 1 : we can convert points $x \in \mathrm{Jac}(H)(\overline{\mathbb{F}}_q)$ from Mumford coordinates to theta coordinates, for $\mathcal{L}_0^{\otimes 4}$ and for "a particular" theta structure $\Theta_{\mathcal{L}_0^{\otimes 4}}$
- Fact 2 : knowing the theta coordinates of $0_{A/G}$ for $\mathcal{M}_0^{\otimes 4}$ ($\mathcal{M}_0$ induced by $\mathcal{L}_0$ and β) and for "a particular" theta structure $\Theta_{\mathcal{M}_0^{\otimes 4}}$, we can recover an equation for H'
- Fact 3 : we can convert points $y \in (A/G)(\overline{\mathbb{F}}_q)$ from theta coordinates (for $\mathcal{M}_0^{\otimes 4}$ and for $\Theta_{\mathcal{M}_0^{\otimes 4}}$) to Mumford coordinates for $\mathrm{Jac}(H')$

The algorithm

- Problem : $f : (A, \mathcal{L}_0^{\otimes 4}, \Theta_{\mathcal{L}_0^{\otimes 4}}) \to (A/G, \mathcal{M}_0^{\otimes 4}, \Theta_{\mathcal{M}_0^{\otimes 4}})$ is NOT an isogeny that preserves polarizations

The algorithm

- Problem : $f : (A, \mathcal{L}_0^{\otimes 4}, \Theta_{\mathcal{L}_0^{\otimes 4}}) \to (A/G, \mathcal{M}_0^{\otimes 4}, \Theta_{\mathcal{M}_0^{\otimes 4}})$ is NOT an isogeny that preserves polarizations
- can't apply the isogeny theorem

The algorithm

- Problem : $f : (A, \mathcal{L}_0^{\otimes 4}, \Theta_{\mathcal{L}_0^{\otimes 4}}) \to (A/G, \mathcal{M}_0^{\otimes 4}, \Theta_{\mathcal{M}_0^{\otimes 4}})$ is NOT an isogeny that preserves polarizations
- can't apply the isogeny theorem
- need some tricks

The algorithm
How?

- apply isogeny theorem to β-contragredient isogeny

$$\widehat{f} \colon A/G \to A$$

(endowed with suitable polarizations and theta structures)

The algorithm
How?

- apply isogeny theorem to β-contragredient isogeny

$$\widehat{f} \colon A/G \to A$$

(endowed with suitable polarizations and theta structures)

- apply isogeny theorem to some endomorphism

$$F \colon (A/G)^4 \to (A/G)^4$$

(endowed with suitable polarizations and theta structures)

- apply isogeny theorem to β-contragredient isogeny

$$\widehat{f}\colon A/G \to A$$

(endowed with suitable polarizations and theta structures)

- apply isogeny theorem to some endomorphism

$$F\colon (A/G)^4 \to (A/G)^4$$

(endowed with suitable polarizations and theta structures)

- try to recover theta coordinates for $(A/G, \mathcal{M}_0^{\otimes 4}, \Theta_{\mathcal{M}_0^{\otimes 4}})$ from theta coordinates for $(A/G)^4$ (with suitable polarization and theta structure)

Example

- over $\mathbb{F}_{23}$, consider

$$H : y^2 = x^5 + x^4 + 3x^3 + 22x^2 + 19x$$

- $\beta = -38(\pi + \pi^\dagger) + 215$, totally positive real endomorphism of degree 17^2 (π is the Frobenius, † is the Rosati involution)
- $G \subset \ker \beta$ cyclic of order 17, Galois-stable and generated by $t \in \mathrm{Jac}(H)(\mathbb{F}_{23^{16}})$ (c.f. next slide)
- $\Rightarrow$ we compute the β-cyclic isogeny

$$\mathrm{Jac}(H) \to \mathrm{Jac}(H)/G \cong \mathrm{Jac}(H'),$$

where

$$H' : y^2 = 5x^6 + 18x^5 + 18x^4 + 8x^3 + 20x$$

Example

- Let $\mathbb{F}_{23^{16}} = \mathbb{F}_{23}(a)$, where

$$a^{16} + 19a^7 + 19a^6 + 16a^5 + 13a^4 + a^3 + 14a^2 + 17a + 5 = 0.$$

- Let $t = (x^2 + u_1x + u_0, v_1x + v_0) \in \mathrm{Jac}(H)(\mathbb{F}_{23^{16}})$, where

$$\begin{aligned}
u_1 =& 10a^{15} + 9a^{14} + 17a^{13} + 5a^{12} + 14a^{11} + 19a^{10} + 14a^9 + 14a^8 \\
&+ 5a^7 + 22a^6 + a^5 + 19a^4 + 13a^3 + 2a^2 + 15a + 7, \\
u_0 =& 6a^{15} + 11a^{14} + 17a^{13} + 19a^{12} + 10a^{11} + a^{10} + 21a^9 + 15a^8 \\
&+ 18a^7 + 21a^6 + 5a^5 + 18a^4 + 4a^3 + 6a^2 + 3a + 19, \\
v_1 =& 19a^{15} + 11a^{14} + 18a^{13} + 3a^{12} + 20a^{11} + 11a^{10} + 8a^9 + a^8 \\
&+ 19a^7 + 5a^6 + 14a^5 + 3a^4 + 4a^3 + 10a^2 + 22a + 22, \\
v_0 =& a^{15} + 10a^{14} + 11a^{13} + 22a^{12} + 3a^{11} + 14a^{10} + 21a^9 + 5a^8 \\
&+ 9a^7 + 17a^5 + 20a^4 + 6a^3 + 8a^2 + 13a + 5
\end{aligned}$$

- Then $\beta(t) = 0$ and $G = \langle t \rangle$ is Galois stable since $\pi(t) = [6]t$.

Thank you!