Computing Cyclic Isogenies in Genus 2 with Applications in Cryptography

Alina Dudeanu[1] Dimitar Jetchev[1] Damien Robert[2]

[1]EPF Lausanne

[2]INRIA Bordeaux

May 20, 2014

Introduction

Elliptic and Hyperelliptic Curves

- Applications: Public key cryptosystems (e.g. Diffie-Hellman key exchange protocol, ElGamal).

General security assessment:

- DLP: Given a multiplicative group $G =< g >$ of large order r and $h \in G$, find x such that $h = g^x$.
- Classical DLP: $G = \mathbf{F}_p^*$, with p prime.
- Subexponential attacks.

Curve-based security assessment:

- ECDLP: Given an elliptic curve E (genus 1) over some $\mathbf{F}_p$, then $G = E(\mathbf{F}_p)$.
- HECDLP: Given an hyperelliptic curve C of genus g over some $\mathbf{F}_p$ and its Jacobian $Jac(C)$, then $G = Jac_{\mathbf{F}_p}(C)$.
- Exponential attacks

Introduction

Elliptic and Hyperelliptic Curves

- Applications: Public key cryptosystems (e.g. Diffie-Hellman key exchange protocol, ElGamal).

General security assessment:

- DLP: Given a multiplicative group $G = < g >$ of large order r and $h \in G$, find x such that $h = g^x$.
- Classical DLP: $G = \mathbf{F}_p^*$, with p prime.
- Subexponential attacks.

Curve-based security assessment:

- ECDLP: Given an elliptic curve E (genus 1) over some $\mathbf{F}_p$, then $G = E(\mathbf{F}_p)$.
- HECDLP: Given an hyperelliptic curve C of genus g over some $\mathbf{F}_p$ and its Jacobian $Jac(C)$, then $G = Jac_{\mathbf{F}_p}(C)$.
- Exponential attacks

Introduction

Elliptic and Hyperelliptic Curves

- Applications: Public key cryptosystems (e.g. Diffie-Hellman key exchange protocol, ElGamal).

General security assessment:

- DLP: Given a multiplicative group $G =< g >$ of large order r and $h \in G$, find x such that $h = g^x$.
- Classical DLP: $G = \mathbf{F}_p^*$, with p prime.
- Subexponential attacks.

Curve-based security assessment:

- ECDLP: Given an elliptic curve E (genus 1) over some $\mathbf{F}_p$, then $G = E(\mathbf{F}_p)$.
- HECDLP: Given an hyperelliptic curve C of genus g over some $\mathbf{F}_p$ and its Jacobian $Jac(C)$, then $G = Jac_{\mathbf{F}_p}(C)$.
- Exponential attacks

Genus 1 Curves

- ECC:
  $\mathbf{F}_p$, where p is a prime of recommended size.
  an elliptic curve E over $\mathbf{F}_p$ with given $\#E(\mathbf{F}_p)$.
- Question
  Is the discrete logarithm problem equally hard on all curves having the same number of points?
- Answer
  "Yes", with some probability and constraints for the case of ordinary elliptic curves.

Theorem (Tate)

E_1, E_2 defined over $\mathbf{F}_p$ have $\#E_1(\mathbf{F}_p) = \#E_2(\mathbf{F}_p)$ iff there exists an $\mathbf{F}_p$-isogeny $\phi\colon E_1 \to E_2$.

An isogeny is a morphism of the form $\phi : E_1 \to E_2$ of some degree over $\mathbf{F}_p$ (rational map, regular at any point on E_1) with $\phi(\mathcal{O}_1) = \mathcal{O}_2$.

Genus 1 Curves

- ECC:
  $\mathbf{F}_p$, where p is a prime of recommended size.
  an elliptic curve E over $\mathbf{F}_p$ with given $\#E(\mathbf{F}_p)$.
- Question
  Is the discrete logarithm problem equally hard on all curves having the same number of points?
- Answer
  "Yes", with some probability and constraints for the case of ordinary elliptic curves.

Theorem (Tate)

E_1, E_2 defined over $\mathbf{F}_p$ have $\#E_1(\mathbf{F}_p) = \#E_2(\mathbf{F}_p)$ iff there exists an $\mathbf{F}_p$-isogeny $\phi\colon E_1 \to E_2$.

An isogeny is a morphism of the form $\phi : E_1 \to E_2$ of some degree over $\mathbf{F}_p$ (rational map, regular at any point on E_1) with $\phi(\mathcal{O}_1) = \mathcal{O}_2$.

Genus 1 Curves

- ECC:
  $\mathbf{F}_p$, where p is a prime of recommended size.
  an elliptic curve E over $\mathbf{F}_p$ with given $\#E(\mathbf{F}_p)$.
- Question
  Is the discrete logarithm problem equally hard on all curves having the same number of points?
- Answer
  "Yes", with some probability and constraints for the case of ordinary elliptic curves.

Theorem (Tate)

E_1, E_2 defined over $\mathbf{F}_p$ have $\#E_1(\mathbf{F}_p) = \#E_2(\mathbf{F}_p)$ iff there exists an $\mathbf{F}_p$-isogeny $\phi\colon E_1 \to E_2$.

An isogeny is a morphism of the form $\phi : E_1 \to E_2$ of some degree over $\mathbf{F}_p$ (rational map, regular at any point on E_1) with $\phi(\mathcal{O}_1) = \mathcal{O}_2$.

Genus 1 Curves

- ECC:
  $\mathbf{F}_p$, where p is a prime of recommended size.
  an elliptic curve E over $\mathbf{F}_p$ with given $\#E(\mathbf{F}_p)$.
- Question
  Is the discrete logarithm problem equally hard on all curves having the same number of points?
- Answer
  "Yes", with some probability and constraints for the case of ordinary elliptic curves.

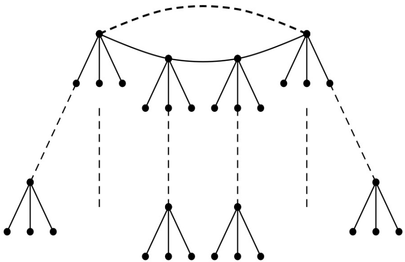
Theorem (Tate)

E_1, E_2 defined over $\mathbf{F}_p$ have $\#E_1(\mathbf{F}_p) = \#E_2(\mathbf{F}_p)$ iff there exists an $\mathbf{F}_p$-isogeny $\phi\colon E_1 \to E_2$.

An isogeny is a morphism of the form $\phi : E_1 \to E_2$ of some degree over $\mathbf{F}_p$ (rational map, regular at any point on E_1) with $\phi(\mathcal{O}_1) = \mathcal{O}_2$.

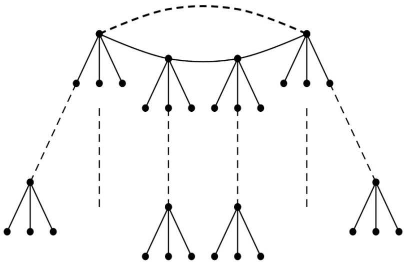
Isogeny Graph

- $\#E(\mathbf{F}_p) = 1 + p - t$ where t is the trace of Frobenius π
- $\mathrm{End}(E)$ - order in $K = \mathbf{Q}(\sqrt{-d_t})$, with $c_t^2 d_t = t^2 - 4p$.
- $\mathcal{O}_K \supseteq \mathrm{End}(E) \supseteq \mathbf{Z}[\pi]$



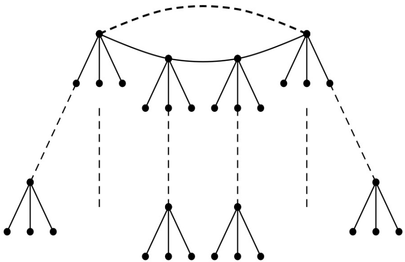
Isogeny Graph

- $\#E(\mathbf{F}_p) = 1 + p - t$ where t is the trace of Frobenius π
- $\mathrm{End}(E)$ - order in $K = \mathbf{Q}(\sqrt{-d_t})$, with $c_t^2 d_t = t^2 - 4p$.
- $\mathcal{O}_K \supseteq \mathrm{End}(E) \supseteq \mathbf{Z}[\pi]$



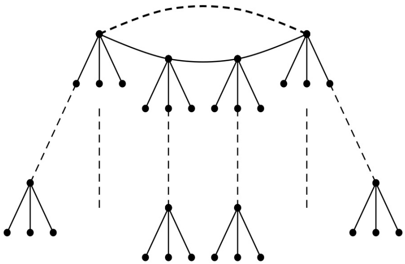
Isogeny Graph

- $\#E(\mathbf{F}_p) = 1 + p - t$ where t is the trace of Frobenius π
- $\mathrm{End}(E)$ - order in $K = \mathbf{Q}(\sqrt{-d_t})$, with $c_t^2 d_t = t^2 - 4p$.
- $\mathcal{O}_K \supseteq \mathrm{End}(E) \supseteq \mathbf{Z}[\pi]$



Isogeny Graph

- $\#E(\mathbf{F}_p) = 1 + p - t$ where t is the trace of Frobenius π
- $\mathrm{End}(E)$ - order in $K = \mathbf{Q}(\sqrt{-d_t})$, with $c_t^2 d_t = t^2 - 4p$.
- $\mathcal{O}_K \supseteq \mathrm{End}(E) \supseteq \mathbf{Z}[\pi]$



Genus 2 Curves

Why?

Similar cost when doing arithmetic, smaller fields by a factor 2.

- Jacobians of curves over $\mathbf{F}_p$ that have the same characteristic polynomial of Frobenius = an $\mathbf{F}_p$-isogeny class.
- Jacobians are principally polarised abelian varieties (together with embeddings in $\mathbf{P}^N$). An isogeny links both the varieties and their polarizations.
- A principal polarization is crucial in recovering a curve equation from an abelian variety that is a Jacobian.

Same Question

Is the DL equally hard on isomorphic classes of Jacobians in the same isogeny graph?

Genus 2 Curves

Why?

Similar cost when doing arithmetic, smaller fields by a factor 2.

- Jacobians of curves over $\mathbf{F}_p$ that have the same characteristic polynomial of Frobenius = an $\mathbf{F}_p$-isogeny class.
- Jacobians are principally polarised abelian varieties (together with embeddings in $\mathbf{P}^N$). An isogeny links both the varieties and their polarizations.
- A principal polarization is crucial in recovering a curve equation from an abelian variety that is a Jacobian.

Same Question

Is the DL equally hard on isomorphic classes of Jacobians in the same isogeny graph?

Genus 2 Curves

Why?

Similar cost when doing arithmetic, smaller fields by a factor 2.

- Jacobians of curves over $\mathbf{F}_p$ that have the same characteristic polynomial of Frobenius = an $\mathbf{F}_p$-isogeny class.
- Jacobians are principally polarised abelian varieties (together with embeddings in $\mathbf{P}^N$). An isogeny links both the varieties and their polarizations.
- A principal polarization is crucial in recovering a curve equation from an abelian variety that is a Jacobian.

Same Question

Is the DL equally hard on isomorphic classes of Jacobians in the same isogeny graph?

Genus 2 Curves

Why?

Similar cost when doing arithmetic, smaller fields by a factor 2.

- Jacobians of curves over $\mathbf{F}_p$ that have the same characteristic polynomial of Frobenius = an $\mathbf{F}_p$-isogeny class.
- Jacobians are principally polarised abelian varieties (together with embeddings in $\mathbf{P}^N$). An isogeny links both the varieties and their polarizations.
- A principal polarization is crucial in recovering a curve equation from an abelian variety that is a Jacobian.

Same Question

Is the DL equally hard on isomorphic classes of Jacobians in the same isogeny graph?

Genus 2 Curves

Why?

Similar cost when doing arithmetic, smaller fields by a factor 2.

- Jacobians of curves over $\mathbf{F}_p$ that have the same characteristic polynomial of Frobenius = an $\mathbf{F}_p$-isogeny class.
- Jacobians are principally polarised abelian varieties (together with embeddings in $\mathbf{P}^N$). An isogeny links both the varieties and their polarizations.
- A principal polarization is crucial in recovering a curve equation from an abelian variety that is a Jacobian.

Same Question

Is the DL equally hard on isomorphic classes of Jacobians in the same isogeny graph?

Isogeny Graphs of Principally Polarized Abelian Surfaces

Computing isogenies from kernel in genus 2 is a lot harder:

- Canonical coordinates
- Polarizations: prime degree isogenies do not preserve principal polarisations.
- Deciding isomorphisms: deciding if two non-polarized abelian surfaces are isomorphic is a computationally hard problem.
- Class field theory: endomorphism rings are orders in quartic number fields.

Main idea: use the theory of theta functions and the CM description of principally polarised abelian varieties

Isogeny Graphs of Principally Polarized Abelian Surfaces

Computing isogenies from kernel in genus 2 is a lot harder:

- Canonical coordinates
- Polarizations: prime degree isogenies do not preserve principal polarisations.
- Deciding isomorphisms: deciding if two non-polarized abelian surfaces are isomorphic is a computationally hard problem.
- Class field theory: endomorphism rings are orders in quartic number fields.

Main idea: use the theory of theta functions and the CM description of principally polarised abelian varieties

Isogeny Graphs of Principally Polarized Abelian Surfaces

Computing isogenies from kernel in genus 2 is a lot harder:

- Canonical coordinates
- Polarizations: prime degree isogenies do not preserve principal polarisations.
- Deciding isomorphisms: deciding if two non-polarized abelian surfaces are isomorphic is a computationally hard problem.
- Class field theory: endomorphism rings are orders in quartic number fields.

Main idea: use the theory of theta functions and the CM description of principally polarised abelian varieties

Isogeny Graphs of Principally Polarized Abelian Surfaces

Computing isogenies from kernel in genus 2 is a lot harder:

- Canonical coordinates
- Polarizations: prime degree isogenies do not preserve principal polarisations.
- Deciding isomorphisms: deciding if two non-polarized abelian surfaces are isomorphic is a computationally hard problem.
- Class field theory: endomorphism rings are orders in quartic number fields.

Main idea: use the theory of theta functions and the CM description of principally polarised abelian varieties

Isogeny Graphs of Principally Polarized Abelian Surfaces

Computing isogenies from kernel in genus 2 is a lot harder:

- Canonical coordinates
- Polarizations: prime degree isogenies do not preserve principal polarisations.
- Deciding isomorphisms: deciding if two non-polarized abelian surfaces are isomorphic is a computationally hard problem.
- Class field theory: endomorphism rings are orders in quartic number fields.

Main idea: use the theory of theta functions and the CM description of principally polarised abelian varieties

Isogeny Graphs of Principally Polarized Abelian Surfaces

Computing isogenies from kernel in genus 2 is a lot harder:

- Canonical coordinates
- Polarizations: prime degree isogenies do not preserve principal polarisations.
- Deciding isomorphisms: deciding if two non-polarized abelian surfaces are isomorphic is a computationally hard problem.
- Class field theory: endomorphism rings are orders in quartic number fields.

Main idea: use the theory of theta functions and the CM description of principally polarised abelian varieties

Current State of the Art

The work of Cosset et Robert on (ℓ, ℓ) isogenies:

- The kernel is isomorphic to $\frac{1}{\ell}\mathbf{Z}^2/\mathbf{Z}^2$.
- Similar formulas to Vélu.
- The (ℓ, ℓ) isogeny is the only isogeny that preserves the principal polarization of the source and target.
- Not all isogenies between isomorphism classes can be expressed with (ℓ, ℓ)-isogenies.
- **The graph associated to the isogeny class may not be connected**.

Current State of the Art

The work of Cosset et Robert on (ℓ, ℓ) isogenies:

- The kernel is isomorphic to $\frac{1}{\ell}\mathbf{Z}^2/\mathbf{Z}^2$.
- Similar formulas to Vélu.
- The (ℓ, ℓ) isogeny is the only isogeny that preserves the principal polarization of the source and target.
- Not all isogenies between isomorphism classes can be expressed with (ℓ, ℓ)-isogenies.
- **The graph associated to the isogeny class may not be connected**.

Current State of the Art

The work of Cosset et Robert on (ℓ, ℓ) isogenies:

- The kernel is isomorphic to $\frac{1}{\ell}\mathbf{Z}^2/\mathbf{Z}^2$.
- Similar formulas to Vélu.
- The (ℓ, ℓ) isogeny is the only isogeny that preserves the principal polarization of the source and target.
- Not all isogenies between isomorphism classes can be expressed with (ℓ, ℓ)-isogenies.
- **The graph associated to the isogeny class may not be connected**.

Current State of the Art

The work of Cosset et Robert on (ℓ, ℓ) isogenies:

- The kernel is isomorphic to $\frac{1}{\ell}\mathbf{Z}^2/\mathbf{Z}^2$.
- Similar formulas to Vélu.
- The (ℓ, ℓ) isogeny is the only isogeny that preserves the principal polarization of the source and target.
- Not all isogenies between isomorphism classes can be expressed with (ℓ, ℓ)-isogenies.
- **The graph associated to the isogeny class may not be connected**.

Current State of the Art

The work of Cosset et Robert on (ℓ, ℓ) isogenies:

- The kernel is isomorphic to $\frac{1}{\ell}\mathbf{Z}^2/\mathbf{Z}^2$.
- Similar formulas to Vélu.
- The (ℓ, ℓ) isogeny is the only isogeny that preserves the principal polarization of the source and target.
- Not all isogenies between isomorphism classes can be expressed with (ℓ, ℓ)-isogenies.
- The graph associated to the isogeny class may not be connected.

Current State of the Art

The work of Cosset et Robert on (ℓ, ℓ) isogenies:

- The kernel is isomorphic to $\frac{1}{\ell}\mathbf{Z}^2/\mathbf{Z}^2$.
- Similar formulas to Vélu.
- The (ℓ, ℓ) isogeny is the only isogeny that preserves the principal polarization of the source and target.
- Not all isogenies between isomorphism classes can be expressed with (ℓ, ℓ)-isogenies.
- **The graph associated to the isogeny class may not be connected**.

Algorithm of Computing Cyclic Isogenies

Input:

- a prime p and a prime ℓ
- C a hyperlliptic curve of genus 2 defined over $\mathbf{F}_p$ given in Rosenhain form:

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

  s. t. $\mathrm{End}_{\overline{\mathbf{F}}_p}(\mathrm{Jac}(C)) \simeq \mathcal{O}$ with $\mathcal{O}$ order in $K := \mathbf{Q}(\pi)$.
  The quadratic field $K_0 = \mathbf{Q}(\sqrt{D}) \subset K$ and $\mathcal{O}_0 := \mathcal{O} \cap K_0$.
- a totally positive element $\beta \in \mathcal{O}_0$ of norm prime ℓ
- a generator P in Mumford coordinates of the isogeny kernel G s.t. $\beta \cdot P = O$.

Output: C'- a hyperelliptic curve defined over $\mathbf{F}_p$ s.t. $\mathrm{Jac}(C') \simeq_{\mathbf{F}_p} B$, with B the target of an ℓ-isogeny of kernel G.

Algorithm of Computing Cyclic Isogenies

Input:

- a prime p and a prime ℓ
- C a hyperlliptic curve of genus 2 defined over $\mathbf{F}_p$ given in Rosenhain form:

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

  s. t. $\mathrm{End}_{\overline{\mathbf{F}}_p}(\mathrm{Jac}(C)) \simeq \mathcal{O}$ with $\mathcal{O}$ order in $K := \mathbf{Q}(\pi)$.
  The quadratic field $K_0 = \mathbf{Q}(\sqrt{D}) \subset K$ and $\mathcal{O}_0 := \mathcal{O} \cap K_0$.
- a totally positive element $\beta \in \mathcal{O}_0$ of norm prime ℓ
- a generator P in Mumford coordinates of the isogeny kernel G s.t. $\beta \cdot P = O$.

Output: C'- a hyperelliptic curve defined over $\mathbf{F}_p$ s.t. $\mathrm{Jac}(C') \simeq_{\mathbf{F}_p} B$, with B the target of an ℓ-isogeny of kernel G.

Algorithm of Computing Cyclic Isogenies

Input:

- a prime p and a prime ℓ
- C a hyperlliptic curve of genus 2 defined over $\mathbf{F}_p$ given in Rosenhain form:

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

  s. t. $\mathrm{End}_{\overline{\mathbf{F}}_p}(\mathrm{Jac}(C)) \simeq \mathcal{O}$ with $\mathcal{O}$ order in $K := \mathbf{Q}(\pi)$. The quadratic field $K_0 = \mathbf{Q}(\sqrt{D}) \subset K$ and $\mathcal{O}_0 := \mathcal{O} \cap K_0$.
- a totally positive element $\beta \in \mathcal{O}_0$ of norm prime ℓ
- a generator P in Mumford coordinates of the isogeny kernel G s.t. $\beta \cdot P = O$.

Output: C'- a hyperelliptic curve defined over $\mathbf{F}_p$ s.t. $\mathrm{Jac}(C') \simeq_{\mathbf{F}_p} B$, with B the target of an ℓ-isogeny of kernel G.

Algorithm of Computing Cyclic Isogenies

Input:

- a prime p and a prime ℓ
- C a hyperlliptic curve of genus 2 defined over $\mathbf{F}_p$ given in Rosenhain form:

  $$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

  s. t. $\mathrm{End}_{\overline{\mathbf{F}}_p}(\mathrm{Jac}(C)) \simeq \mathcal{O}$ with $\mathcal{O}$ order in $K := \mathbf{Q}(\pi)$.
  The quadratic field $K_0 = \mathbf{Q}(\sqrt{D}) \subset K$ and $\mathcal{O}_0 := \mathcal{O} \cap K_0$.
- a totally positive element $\beta \in \mathcal{O}_0$ of norm prime ℓ
- a generator P in Mumford coordinates of the isogeny kernel G s.t. $\beta \cdot P = O$.

Output: C'- a hyperelliptic curve defined over $\mathbf{F}_p$ s.t. $\mathrm{Jac}(C') \simeq_{\mathbf{F}_p} B$, with B the target of an ℓ-isogeny of kernel G.

Algorithm of Computing Cyclic Isogenies

Input:

- a prime p and a prime ℓ
- C a hyperlliptic curve of genus 2 defined over $\mathbf{F}_p$ given in Rosenhain form:

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

  s. t. $\mathrm{End}_{\overline{\mathbf{F}}_p}(\mathrm{Jac}(C)) \simeq \mathcal{O}$ with $\mathcal{O}$ order in $K := \mathbf{Q}(\pi)$.
  The quadratic field $K_0 = \mathbf{Q}(\sqrt{D}) \subset K$ and $\mathcal{O}_0 := \mathcal{O} \cap K_0$.
- a totally positive element $\beta \in \mathcal{O}_0$ of norm prime ℓ
- a generator P in Mumford coordinates of the isogeny kernel G s.t. $\beta \cdot P = O$.

Output: C'- a hyperelliptic curve defined over $\mathbf{F}_p$ s.t. $\mathrm{Jac}(C') \simeq_{\mathbf{F}_p} B$, with B the target of an ℓ-isogeny of kernel G.

Algorithm of Computing Cyclic Isogenies

Input:

- a prime p and a prime ℓ
- C a hyperlliptic curve of genus 2 defined over $\mathbf{F}_p$ given in Rosenhain form:

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

  s. t. $\mathrm{End}_{\overline{\mathbf{F}}_p}(\mathrm{Jac}(C)) \simeq \mathcal{O}$ with $\mathcal{O}$ order in $K := \mathbf{Q}(\pi)$.
  The quadratic field $K_0 = \mathbf{Q}(\sqrt{D}) \subset K$ and $\mathcal{O}_0 := \mathcal{O} \cap K_0$.
- a totally positive element $\beta \in \mathcal{O}_0$ of norm prime ℓ
- a generator P in Mumford coordinates of the isogeny kernel G s.t. $\beta \cdot P = O$.

Output: C'- a hyperelliptic curve defined over $\mathbf{F}_p$ s.t. $\mathrm{Jac}(C') \simeq_{\mathbf{F}_p} B$, with B the target of an ℓ-isogeny of kernel G.

Diagram

Let $f\colon A \to B$. Let $\beta\colon A \to A$ s.t. $\ker(f) \subset \ker(\beta)$ maximal isotropic.

$$\begin{tikzcd}
A \arrow[drr, "\varphi_{\mathcal{L}_0}"'] & & A \arrow[ll, "\beta"'] \arrow[rr, "f"] & & B \arrow[d, "\varphi_{\mathcal{M}_0}"] \\
& & A^* & & B^*. \arrow[ll, "f^*"']
\end{tikzcd} \tag{1}$$

Algorithm Steps

1. Compute a theta null point of A of level $(2,2)$.
2. Compute a totally positive element $\beta \in \mathcal{O}_{K_0}$ of norm ℓ that corresponds to the endomorphism on A whose kernel contains G.
3. Compute a theta null point of B of level $(2,2)$ by applying the isogeny theorem together with Koizumi's formulae
4. Deduce an equation of a rational smooth genus 2 curve C' whose $Jac(C') \simeq_{\mathbf{F}_p} B$.

Algorithm Steps

1. Compute a theta null point of A of level $(2,2)$.
2. Compute a totally positive element $\beta \in \mathcal{O}_{K_0}$ of norm ℓ that corresponds to the endomorphism on A whose kernel contains G.
3. Compute a theta null point of B of level $(2,2)$ by applying the isogeny theorem together with Koizumi's formulae
4. Deduce an equation of a rational smooth genus 2 curve C' whose $Jac(C') \simeq_{\mathbf{F}_p} B$.

Algorithm Steps

1. Compute a theta null point of A of level $(2, 2)$.
2. Compute a totally positive element $\beta \in \mathcal{O}_{K_0}$ of norm ℓ that corresponds to the endomorphism on A whose kernel contains G.
3. Compute a theta null point of B of level $(2, 2)$ by applying the isogeny theorem together with Koizumi's formulae
4. Deduce an equation of a rational smooth genus 2 curve C' whose $Jac(C') \simeq_{\mathbf{F}_p} B$.

Algorithm Steps

1. Compute a theta null point of A of level $(2,2)$.
2. Compute a totally positive element $\beta \in \mathcal{O}_{K_0}$ of norm ℓ that corresponds to the endomorphism on A whose kernel contains G.
3. Compute a theta null point of B of level $(2,2)$ by applying the isogeny theorem together with Koizumi's formulae
4. Deduce an equation of a rational smooth genus 2 curve C' whose $Jac(C') \simeq_{\mathbf{F}_p} B$.

Algorithm Steps

1. Compute a theta null point of A of level $(2, 2)$.
2. Compute a totally positive element $\beta \in \mathcal{O}_{K_0}$ of norm ℓ that corresponds to the endomorphism on A whose kernel contains G.
3. Compute a theta null point of B of level $(2, 2)$ by applying the isogeny theorem together with Koizumi's formulae
4. Deduce an equation of a rational smooth genus 2 curve C' whose $Jac(C') \simeq_{\mathbf{F}_p} B$.

Computing the theta null point of A

- We work over $\mathbf{C}$.
- Let $A := \mathrm{Jac}(C)$ and let $\mathcal{L}_0$ be a pp on A.
- $\exists \Lambda \subset \mathbf{C}^2$ lattice rank 4 s.t. $A \simeq T := \mathbf{C}^2/\Lambda$.
- $\exists \mathcal{L}_0 \Rightarrow \exists \Omega \in \mathcal{M}_2(C)$, $\Omega = \Omega^T$ and $\mathcal{I}(\Omega) > 0$ s.t. $\Lambda = \Omega\mathbf{Z}^2 + \mathbf{Z}^2$.
- The Riemann theta function associated to Ω is $\Theta : \mathbf{C}^2 \to \mathbf{C}$ where

$$\Theta(z, \Omega) := \sum_{x \in \mathbf{Z}^2} e^{\pi i x^T \Omega x + 2\pi i x^T z}.$$

Computing the theta null point of A

- We work over **C**.
- Let $A := \mathrm{Jac}(C)$ and let $\mathcal{L}_0$ be a pp on A.
- $\exists \Lambda \subset \mathbf{C}^2$ lattice rank 4 s.t. $A \simeq T := \mathbf{C}^2/\Lambda$.
- $\exists \mathcal{L}_0 \Rightarrow \exists \Omega \in \mathcal{M}_2(C)$, $\Omega = \Omega^T$ and $\mathcal{I}(\Omega) > 0$ s.t. $\Lambda = \Omega \mathbf{Z}^2 + \mathbf{Z}^2$.
- The Riemann theta function associated to Ω is $\Theta : \mathbf{C}^2 \to \mathbf{C}$ where

$$\Theta(z, \Omega) := \sum_{x \in \mathbf{Z}^2} e^{\pi i x^T \Omega x + 2\pi i x^T z}.$$

Computing the theta null point of A

- We work over $\mathbf{C}$.
- Let $A := \mathrm{Jac}(C)$ and let $\mathcal{L}_0$ be a pp on A.
- $\exists \Lambda \subset \mathbf{C}^2$ lattice rank 4 s.t. $A \simeq T := \mathbf{C}^2/\Lambda$.
- $\exists \mathcal{L}_0 \Rightarrow \exists \Omega \in \mathcal{M}_2(C)$, $\Omega = \Omega^T$ and $\mathcal{I}(\Omega) > 0$ s.t. $\Lambda = \Omega\mathbf{Z}^2 + \mathbf{Z}^2$.
- The Riemann theta function associated to Ω is $\Theta : \mathbf{C}^2 \to \mathbf{C}$ where

$$\Theta(z, \Omega) := \sum_{x \in \mathbf{Z}^2} e^{\pi i x^T \Omega x + 2\pi i x^T z}.$$

Computing the theta null point of A

- We work over $\mathbf{C}$.
- Let $A := \mathrm{Jac}(C)$ and let $\mathcal{L}_0$ be a pp on A.
- $\exists \Lambda \subset \mathbf{C}^2$ lattice rank 4 s.t. $A \simeq T := \mathbf{C}^2/\Lambda$.
- $\exists \mathcal{L}_0 \Rightarrow \exists \Omega \in \mathcal{M}_2(C)$, $\Omega = \Omega^T$ and $\mathcal{I}(\Omega) > 0$ s.t. $\Lambda = \Omega \mathbf{Z}^2 + \mathbf{Z}^2$.
- The Riemann theta function associated to Ω is $\Theta : \mathbf{C}^2 \to \mathbf{C}$ where

$$\Theta(z, \Omega) := \sum_{x \in \mathbf{Z}^2} e^{\pi i x^T \Omega x + 2\pi i x^T z}.$$

Computing the theta null point of A

- We work over $\mathbf{C}$.
- Let $A := \mathrm{Jac}(C)$ and let $\mathcal{L}_0$ be a pp on A.
- $\exists \Lambda \subset \mathbf{C}^2$ lattice rank 4 s.t. $A \simeq T := \mathbf{C}^2/\Lambda$.
- $\exists \mathcal{L}_0 \Rightarrow \exists\, \Omega \in \mathcal{M}_2(C)$, $\Omega = \Omega^T$ and $\mathcal{I}(\Omega) > 0$ s.t. $\Lambda = \Omega \mathbf{Z}^2 + \mathbf{Z}^2$.
- The Riemann theta function associated to Ω is $\Theta : \mathbf{C}^2 \to \mathbf{C}$ where

$$\Theta(z, \Omega) := \sum_{x \in \mathbf{Z}^2} e^{\pi i x^T \Omega x + 2\pi i x^T z}.$$

Computing the theta null point of A

- We work over $\mathbf{C}$.
- Let $A := \mathrm{Jac}(C)$ and let $\mathcal{L}_0$ be a pp on A.
- $\exists \Lambda \subset \mathbf{C}^2$ lattice rank 4 s.t. $A \simeq T := \mathbf{C}^2/\Lambda$.
- $\exists \mathcal{L}_0 \Rightarrow \exists\, \Omega \in \mathcal{M}_2(C)$, $\Omega = \Omega^T$ and $\mathcal{I}(\Omega) > 0$ s.t. $\Lambda = \Omega \mathbf{Z}^2 + \mathbf{Z}^2$.
- The Riemann theta function associated to Ω is $\Theta : \mathbf{C}^2 \to \mathbf{C}$ where
$$\Theta(z, \Omega) := \sum_{x \in \mathbf{Z}^2} e^{\pi i x^T \Omega x + 2\pi i x^T z}.$$

Computing the theta null point of A

- For $n \in \mathbf{Z}_{>0}$ and $i \in \mathbf{Z}(n) := \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$, let $\theta_i(z) := \Theta(z + i, \frac{\Omega}{n})$.
- The space generated by $(\theta_i(z))_{i \in \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2}$ is the space of theta functions of level n.
- If $n = k^2$, there exists another basis given by theta functions of level (k, k), with indexes $a, b \in \mathbf{Z}(k)$.

When $n \geq 3$:

- $z \in T \longrightarrow (\theta_i(z))_{i \in \mathbf{Z}(n)} \in \mathbb{P}^{n^2-1}(\mathbf{C})$ is an embedding.
- $(\theta_i(0))_{i \in \mathbf{Z}(n)}$ identifies the abelian variety uniquely in $\mathbb{P}^{n^2-1}(\mathbf{C})$.

Computing the theta null point of A

- For $n \in \mathbf{Z}_{>0}$ and $i \in \mathbf{Z}(n) := \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$, let $\theta_i(z) := \Theta(z+i, \frac{\Omega}{n})$.
- The space generated by $(\theta_i(z))_{i \in \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2}$ is the space of theta functions of level n.
- If $n = k^2$, there exists another basis given by theta functions of level (k,k), with indexes $a, b \in \mathbf{Z}(k)$.

When $n \geq 3$:

- $z \in T \longrightarrow (\theta_i(z))_{i \in \mathbf{Z}(n)} \in \mathbb{P}^{n^2-1}(\mathbf{C})$ is an embedding.
- $(\theta_i(0))_{i \in \mathbf{Z}(n)}$ identifies the abelian variety uniquely in $\mathbb{P}^{n^2-1}(\mathbf{C})$.

Computing the theta null point of A

- For $n \in \mathbf{Z}_{>0}$ and $i \in \mathbf{Z}(n) := \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$, let $\theta_i(z) := \Theta(z + i, \frac{\Omega}{n})$.
- The space generated by $(\theta_i(z))_{i \in \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2}$ is the space of theta functions of level n.
- If $n = k^2$, there exists another basis given by theta functions of level (k, k), with indexes $a, b \in \mathbf{Z}(k)$.

When $n \geq 3$:

- $z \in T \longrightarrow (\theta_i(z))_{i \in \mathbf{Z}(n)} \in \mathbb{P}^{n^2-1}(\mathbf{C})$ is an embedding.
- $(\theta_i(0))_{i \in \mathbf{Z}(n)}$ identifies the abelian variety uniquely in $\mathbb{P}^{n^2-1}(\mathbf{C})$.

Computing the theta null point of A

- For $n \in \mathbf{Z}_{>0}$ and $i \in \mathbf{Z}(n) := \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$, let $\theta_i(z) := \Theta(z+i, \frac{\Omega}{n})$.
- The space generated by $(\theta_i(z))_{i \in \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2}$ is the space of theta functions of level n.
- If $n = k^2$, there exists another basis given by theta functions of level (k,k), with indexes $a, b \in \mathbf{Z}(k)$.

When $n \geq 3$:

- $z \in T \longrightarrow (\theta_i(z))_{i \in \mathbf{Z}(n)} \in \mathbb{P}^{n^2-1}(\mathbf{C})$ is an embedding.
- $(\theta_i(0))_{i \in \mathbf{Z}(n)}$ identifies the abelian variety uniquely in $\mathbb{P}^{n^2-1}(\mathbf{C})$.

Computing the theta null point of A

- For $n \in \mathbf{Z}_{>0}$ and $i \in \mathbf{Z}(n) := \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$, let $\theta_i(z) := \Theta(z+i, \frac{\Omega}{n})$.
- The space generated by $(\theta_i(z))_{i \in \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2}$ is the space of theta functions of level n.
- If $n = k^2$, there exists another basis given by theta functions of level (k, k), with indexes $a, b \in \mathbf{Z}(k)$.

When $n \geq 3$:

- $z \in T \longrightarrow (\theta_i(z))_{i \in \mathbf{Z}(n)} \in \mathbb{P}^{n^2-1}(\mathbf{C})$ is an embedding.
- $(\theta_i(0))_{i \in \mathbf{Z}(n)}$ identifies the abelian variety uniquely in $\mathbb{P}^{n^2-1}(\mathbf{C})$.

Computing the theta null point of A

- For $n \in \mathbf{Z}_{>0}$ and $i \in \mathbf{Z}(n) := \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$, let $\theta_i(z) := \Theta(z+i, \frac{\Omega}{n})$.
- The space generated by $(\theta_i(z))_{i \in \frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2}$ is the space of theta functions of level n.
- If $n = k^2$, there exists another basis given by theta functions of level (k,k), with indexes $a, b \in \mathbf{Z}(k)$.

When $n \geq 3$:

- $z \in T \longrightarrow (\theta_i(z))_{i \in \mathbf{Z}(n)} \in \mathbb{P}^{n^2-1}(\mathbf{C})$ is an embedding.
- $(\theta_i(0))_{i \in \mathbf{Z}(n)}$ identifies the abelian variety uniquely in $\mathbb{P}^{n^2-1}(\mathbf{C})$.

Computing the theta null point of A

- Over $\mathbf{F}_p$, given $\{0, 1, \lambda, \mu, \nu\}$, we deduce the theta null point of level $(2, 2)$ (over some extension of $\mathbf{F}_p$) via Thomae's formulae.
- For any $x \in A$, the algebraic theta coordinates are deduced from Mumford coordinates.
- (ℓ, ℓ) isogenies: $A \xleftarrow{[\ell]} A \xrightarrow{f} B$

$$(2,2) \qquad (2\ell, 2\ell) \qquad (2,2).$$

- ℓ cyclic isogenies: $A \xleftarrow{\beta} A \xrightarrow{f} B$

$$(2,2) \qquad (2\ell, 2) \qquad (2,2).$$

Computing the theta null point of A

- Over $\mathbf{F}_p$, given $\{0, 1, \lambda, \mu, \nu\}$, we deduce the theta null point of level $(2, 2)$ (over some extension of $\mathbf{F}_p$) via Thomae's formulae.
- For any $x \in A$, the algebraic theta coordinates are deduced from Mumford coordinates.
- (ℓ, ℓ) isogenies: $A \xleftarrow{[\ell]} A \xrightarrow{f} B$

$$(2,2) \qquad (2\ell, 2\ell) \qquad (2,2).$$

- ℓ cyclic isogenies: $A \xleftarrow{\beta} A \xrightarrow{f} B$

$$(2,2) \qquad (2\ell, 2) \qquad (2,2).$$

Computing the theta null point of A

- Over $\mathbf{F}_p$, given $\{0, 1, \lambda, \mu, \nu\}$, we deduce the theta null point of level $(2, 2)$ (over some extension of $\mathbf{F}_p$) via Thomae's formulae.
- For any $x \in A$, the algebraic theta coordinates are deduced from Mumford coordinates.
- (ℓ, ℓ) isogenies: $A \xleftarrow{[\ell]} A \xrightarrow{f} B$

$$(2,2) \qquad (2\ell, 2\ell) \qquad (2,2).$$

- ℓ cyclic isogenies: $A \xleftarrow{\beta} A \xrightarrow{f} B$

$$(2,2) \qquad (2\ell, 2) \qquad (2,2).$$

Computing the theta null point of A

- Over $\mathbf{F}_p$, given $\{0, 1, \lambda, \mu, \nu\}$, we deduce the theta null point of level $(2, 2)$ (over some extension of $\mathbf{F}_p$) via Thomae's formulae.
- For any $x \in A$, the algebraic theta coordinates are deduced from Mumford coordinates.
- (ℓ, ℓ) isogenies: $A \xleftarrow{[\ell]} A \xrightarrow{f} B$

$$(2, 2) \qquad (2\ell, 2\ell) \qquad (2, 2).$$

- ℓ cyclic isogenies: $A \xleftarrow{\beta} A \xrightarrow{f} B$

$$(2, 2) \qquad (2\ell, 2) \qquad (2, 2).$$

Computing the theta null point of A

- Over $\mathbf{F}_p$, given $\{0, 1, \lambda, \mu, \nu\}$, we deduce the theta null point of level $(2, 2)$ (over some extension of $\mathbf{F}_p$) via Thomae's formulae.
- For any $x \in A$, the algebraic theta coordinates are deduced from Mumford coordinates.
- (ℓ, ℓ) isogenies: $A \xleftarrow{[\ell]} A \xrightarrow{f} B$

$$(2,2) \qquad (2\ell, 2\ell) \qquad (2,2).$$

- ℓ cyclic isogenies: $A \xleftarrow{\beta} A \xrightarrow{f} B$

$$(2,2) \qquad (2\ell, 2) \qquad (2,2).$$

Computing a theta null point of the target B

- Compute the action of β on A by applying a Koizumi type formulas with $F \in \mathrm{GL}_r(K_0)$ s. t. $F^T F = \beta Id$.
- Compute the action of F on A and on the sets of indexes of theta functions.
- Compute the theta null point of B from the theta point of level $(2\ell, 2)$.

For $x = 0$, we consider any index i and (j_1, j_2) the preimage of $(i, 0)$ by F

$$\theta_i^B(f(x))\theta_0^B(0) = \lambda_{ax}\lambda_{bx} \sum_{t \in G} \theta_{j_1}^A(ax + at)\theta_{j_2}^A(bx + bt), \qquad (2)$$

Computing a theta null point of the target B

- Compute the action of β on A by applying a Koizumi type formulas with $F \in \mathrm{GL}_r(K_0)$ s. t. $F^T F = \beta Id$.
- Compute the action of F on A and on the sets of indexes of theta functions.
- Compute the theta null point of B from the theta point of level $(2\ell, 2)$.

For $x = 0$, we consider any index i and (j_1, j_2) the preimage of $(i, 0)$ by F

$$\theta_i^B(f(x))\theta_0^B(0) = \lambda_{ax}\lambda_{bx}\sum_{t\in G}\theta_{j_1}^A(ax+at)\theta_{j_2}^A(bx+bt), \qquad (2)$$

Computing a theta null point of the target B

- Compute the action of β on A by applying a Koizumi type formulas with $F \in \mathrm{GL}_r(K_0)$ s. t. $F^T F = \beta Id$.
- Compute the action of F on A and on the sets of indexes of theta functions.
- Compute the theta null point of B from the theta point of level $(2\ell, 2)$.

For $x = 0$, we consider any index i and (j_1, j_2) the preimage of $(i, 0)$ by F

$$\theta_i^B(f(x))\theta_0^B(0) = \lambda_{ax}\lambda_{bx}\sum_{t\in G}\theta_{j_1}^A(ax+at)\theta_{j_2}^A(bx+bt), \qquad (2)$$

Computing a theta null point of the target B

- Compute the action of β on A by applying a Koizumi type formulas with $F \in \mathrm{GL}_r(K_0)$ s. t. $F^T F = \beta Id$.
- Compute the action of F on A and on the sets of indexes of theta functions.
- Compute the theta null point of B from the theta point of level $(2\ell, 2)$.

For $x = 0$, we consider any index i and (j_1, j_2) the preimage of $(i, 0)$ by F

$$\theta_i^B(f(x))\theta_0^B(0) = \lambda_{ax}\lambda_{bx}\sum_{t \in G}\theta_{j_1}^A(ax + at)\theta_{j_2}^A(bx + bt), \qquad (2)$$

Computing a theta null point of the target B

- Compute the action of β on A by applying a Koizumi type formulas with $F \in \mathrm{GL}_r(K_0)$ s. t. $F^T F = \beta Id$.
- Compute the action of F on A and on the sets of indexes of theta functions.
- Compute the theta null point of B from the theta point of level $(2\ell, 2)$.

For $x = 0$, we consider any index i and (j_1, j_2) the preimage of $(i, 0)$ by F

$$\theta_i^B(f(x))\theta_0^B(0) = \lambda_{ax}\lambda_{bx} \sum_{t \in G} \theta_{j_1}^A(ax + at)\theta_{j_2}^A(bx + bt), \qquad (2)$$

Computing the image of x on the target B

- Equation (2) depends on x, hence we cannot work with projective points.
- There is no canonical way of defining affine theta coordinates over $\mathbf{F}_p$.
- We need to choose the affine lifts in a compatible way, i.e., each product on the right hand side should have the same λ.
- The affine lifts should not depend on t.

Computing the image of x on the target B

- Equation (2) depends on x, hence we cannot work with projective points.
- There is no canonical way of defining affine theta coordinates over $\mathbf{F}_p$.
- We need to choose the affine lifts in a compatible way, i.e., each product on the right hand side should have the same λ.
- The affine lifts should not depend on t.

Computing the image of x on the target B

- Equation (2) depends on x, hence we cannot work with projective points.
- There is no canonical way of defining affine theta coordinates over $\mathbf{F}_p$.
- We need to choose the affine lifts in a compatible way, i.e., each product on the right hand side should have the same λ.
- The affine lifts should not depend on t.

Computing the image of x on the target B

- Equation (2) depends on x, hence we cannot work with projective points.
- There is no canonical way of defining affine theta coordinates over $\mathbf{F}_p$.
- We need to choose the affine lifts in a compatible way, i.e., each product on the right hand side should have the same λ.
- The affine lifts should not depend on t.

Computing the image of x on the target B

- Equation (2) depends on x, hence we cannot work with projective points.
- There is no canonical way of defining affine theta coordinates over $\mathbf{F}_p$.
- We need to choose the affine lifts in a compatible way, i.e., each product on the right hand side should have the same λ.
- The affine lifts should not depend on t.

Computing the image of x via f on the target B

- $a, b \in K_0$ can be expressed in terms of Frobenius π over $\mathbf{F}_{p^k}$, for k the extension degree s.t. the theta null point is over $\mathbf{F}_{p^k}$.
- Fix embeddings $\mathrm{End}_{\mathbf{Q}} \to K \to \mathbf{C}$.
- $\sqrt{D}$ can be written as a degree 3 polynomial in complex root π of
$$X^4 - s_1X^3 + (s_2 + 2q)X^2 - qs_1X + q^2,$$
where $q = p^k$, for some k,$s_1^2 - 4s_2 > 0$, $s_2 + 4q > 2|s_1|\sqrt{q}$, $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 4q$.
- When computing the action of F on ℓ torsion points, computations modulo $\ell \Rightarrow$ the matrix elements are polynomials in $\mathbf{Z}/\ell\mathbf{Z}[X]$.
- When computing the action of F on 4 torsion points, the matrix has elements modulo 4.

Computing the image of x via f on the target B

- $a, b \in K_0$ can be expressed in terms of Frobenius π over $\mathbf{F}_{p^k}$, for k the extension degree s.t. the theta null point is over $\mathbf{F}_{p^k}$.
- Fix embeddings $\mathrm{End}_{\mathbf{Q}} \to K \to \mathbf{C}$.
- $\sqrt{D}$ can be written as a degree 3 polynomial in complex root π of
$$X^4 - s_1X^3 + (s_2 + 2q)X^2 - qs_1X + q^2,$$
where $q = p^k$, for some k,$s_1^2 - 4s_2 > 0$, $s_2 + 4q > 2|s_1|\sqrt{q}$, $|s_1| \le 4\sqrt{q}$ and $|s_2| \le 4q$.
- When computing the action of F on ℓ torsion points, computations modulo $\ell \Rightarrow$ the matrix elements are polynomials in $\mathbf{Z}/\ell\mathbf{Z}[X]$.
- When computing the action of F on 4 torsion points, the matrix has elements modulo 4.

Computing the image of x via f on the target B

- $a, b \in K_0$ can be expressed in terms of Frobenius π over $\mathbf{F}_{p^k}$, for k the extension degree s.t. the theta null point is over $\mathbf{F}_{p^k}$.
- Fix embeddings $\mathrm{End}_{\mathbf{Q}} \to K \to \mathbf{C}$.
- $\sqrt{D}$ can be written as a degree 3 polynomial in complex root π of
$$X^4 - s_1X^3 + (s_2 + 2q)X^2 - qs_1X + q^2,$$
where $q = p^k$, for some k,$s_1^2 - 4s_2 > 0$, $s_2 + 4q > 2|s_1|\sqrt{q}$, $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 4q$.
- When computing the action of F on ℓ torsion points, computations modulo $\ell \Rightarrow$ the matrix elements are polynomials in $\mathbf{Z}/\ell\mathbf{Z}[X]$.
- When computing the action of F on 4 torsion points, the matrix has elements modulo 4.

Computing the image of x via f on the target B

- $a, b \in K_0$ can be expressed in terms of Frobenius π over $\mathbf{F}_{p^k}$, for k the extension degree s.t. the theta null point is over $\mathbf{F}_{p^k}$.
- Fix embeddings $\mathrm{End}_{\mathbf{Q}} \to K \to \mathbf{C}$.
- $\sqrt{D}$ can be written as a degree 3 polynomial in complex root π of

$$X^4 - s_1 X^3 + (s_2 + 2q)X^2 - q s_1 X + q^2,$$

where $q = p^k$, for some k, $s_1^2 - 4s_2 > 0$, $s_2 + 4q > 2|s_1|\sqrt{q}$, $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 4q$.
- When computing the action of F on ℓ torsion points, computations modulo $\ell \Rightarrow$ the matrix elements are polynomials in $\mathbf{Z}/\ell\mathbf{Z}[X]$.
- When computing the action of F on 4 torsion points, the matrix has elements modulo 4.

Computing the image of x via f on the target B

- $a, b \in K_0$ can be expressed in terms of Frobenius π over $\mathbf{F}_{p^k}$, for k the extension degree s.t. the theta null point is over $\mathbf{F}_{p^k}$.
- Fix embeddings $\mathrm{End}_{\mathbf{Q}} \to K \to \mathbf{C}$.
- $\sqrt{D}$ can be written as a degree 3 polynomial in complex root π of
$$X^4 - s_1X^3 + (s_2 + 2q)X^2 - qs_1X + q^2,$$
where $q = p^k$, for some k,$s_1^2 - 4s_2 > 0$, $s_2 + 4q > 2|s_1|\sqrt{q}$, $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 4q$.
- When computing the action of F on ℓ torsion points, computations modulo $\ell \Rightarrow$ the matrix elements are polynomials in $\mathbf{Z}/\ell\mathbf{Z}[X]$.
- When computing the action of F on 4 torsion points, the matrix has elements modulo 4.

Computing the image of x via f on the target B

- $a, b \in K_0$ can be expressed in terms of Frobenius π over $\mathbf{F}_{p^k}$, for k the extension degree s.t. the theta null point is over $\mathbf{F}_{p^k}$.
- Fix embeddings $\mathrm{End}_{\mathbf{Q}} \to K \to \mathbf{C}$.
- $\sqrt{D}$ can be written as a degree 3 polynomial in complex root π of
$$X^4 - s_1X^3 + (s_2 + 2q)X^2 - qs_1X + q^2,$$
where $q = p^k$, for some k, $s_1^2 - 4s_2 > 0$, $s_2 + 4q > 2|s_1|\sqrt{q}$, $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 4q$.
- When computing the action of F on ℓ torsion points, computations modulo $\ell \Rightarrow$ the matrix elements are polynomials in $\mathbf{Z}/\ell\mathbf{Z}[X]$.
- When computing the action of F on 4 torsion points, the matrix has elements modulo 4.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P + Q$, we need $P, Q, P - Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x + t)$ if we have all combinations of two points. They depend on
  - x: normal addition, arbitrary factor
  - t : $\lambda_t^{\ell} = \alpha_t$, for some known α_t
  - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P + Q$, we need $P, Q, P - Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x + t)$ if we have all combinations of two points. They depend on
  - x: normal addition, arbitrary factor
  - t : $\lambda_t^\ell = \alpha_t$, for some known α_t
  - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P + Q$, we need $P, Q, P - Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x + t)$ if we have all combinations of two points. They depend on
  - x: normal addition, arbitrary factor
  - t : $\lambda_t^\ell = \alpha_t$, for some known α_t
  - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P + Q$, we need $P, Q, P - Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x + t)$ if we have all combinations of two points. They depend on
  - x: normal addition, arbitrary factor
  - t : $\lambda_t^\ell = \alpha_t$, for some known α_t
  - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P + Q$, we need $P, Q, P - Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x + t)$ if we have all combinations of two points. They depend on
  - x: normal addition, arbitrary factor
  - t : $\lambda_t^\ell = \alpha_t$, for some known α_t
  - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P + Q$, we need $P, Q, P - Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x + t)$ if we have all combinations of two points. They depend on
  - x: normal addition, arbitrary factor
  - t : $\lambda_t^\ell = \alpha_t$, for some known α_t
  - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P+Q$, we need $P, Q, P-Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x+t)$ if we have all combinations of two points. They depend on
  - x: normal addition, arbitrary factor
  - t : $\lambda_t^\ell = \alpha_t$, for some known α_t
  - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P + Q$, we need $P, Q, P - Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x + t)$ if we have all combinations of two points. They depend on
    - x: normal addition, arbitrary factor
    - t : $\lambda_t^{\ell} = \alpha_t$, for some known α_t
    - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the image of x via f on the target B

- Let $a := \sum_{k=0}^{3} a_k \pi^k$, with $a_k \in \mathbf{Z}/m\mathbf{Z}$.
- **When working with affine coordinates, we need to keep track of the projective factors after each operation.**
- To compute $P + Q$, we need $P, Q, P - Q$ (pseudo-addition).
- $s \cdot P, \pi P$ are easy to compute.
- We can compute $a(x + t)$ if we have all combinations of two points. They depend on
  - x: normal addition, arbitrary factor
  - t : $\lambda_t^{\ell} = \alpha_t$, for some known α_t
  - x and t : find $t' \in G$ s.t. x and t' have the same coefficient.

Computing the equation of the target curve

We deduce a Rosenhain form of the target hyperelliptic curve of the form $y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$ by using the theta constants of level $(2,2)$:

$$\lambda = \frac{\theta_0^2\theta_8^2}{\theta_4^2\theta_{12}^2}, \quad \mu = \frac{\theta_8^2\theta_2^2}{\theta_{12}^2\theta_6^2}, \quad \nu = \frac{\theta_2^2\theta_0^2}{\theta_6^2\theta_4^2}.$$

In case the hyperelliptic curve is over an extension field, we apply Mestre's algorithm.

Algorithm complexity Polynomial in ℓ and further, in $\log p$.

Computing the equation of the target curve

We deduce a Rosenhain form of the target hyperelliptic curve of the form $y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$ by using the theta constants of level $(2,2)$:

$$\lambda = \frac{\theta_0^2\theta_8^2}{\theta_4^2\theta_{12}^2}, \quad \mu = \frac{\theta_8^2\theta_2^2}{\theta_{12}^2\theta_6^2}, \quad \nu = \frac{\theta_2^2\theta_0^2}{\theta_6^2\theta_4^2}.$$

In case the hyperelliptic curve is over an extension field, we apply Mestre's algorithm.

Algorithm complexity Polynomial in ℓ and further, in $\log p$.

Random Self-Reducibility of Discrete Logarithms - genus 1

- Using vertical isogenies, reduce the problem to two curves on the top layer $\mathcal{O}_K$
- Via complex multiplication theory, the curves on the top layer (after liftings to characteristic zero) correspond to $\mathbf{C}/\mathfrak{a}$ where $\in \mathrm{Cl}(\mathcal{O}_K)$
- Get a Cayley graph whose vertices are the curves in the top layer (in bijection with $\mathrm{Pic}(\mathcal{O}_K)$) and whose edges correspond to prime ideals of small norm of $\mathcal{O}_K$
- **Conclusion:** via random walks, discrete log is, with some probability, comparatively hard on all curves in an isogeny class (Jao–Miller–Venkatesan'05)

Goal: what can we say about curves of genus 2?

Random Self-Reducibility of Discrete Logarithms - genus 1

- Using vertical isogenies, reduce the problem to two curves on the top layer $\mathcal{O}_K$
- Via complex multiplication theory, the curves on the top layer (after liftings to characteristic zero) correspond to $\mathbf{C}/\mathfrak{a}$ where $\in \mathrm{Cl}(\mathcal{O}_K)$
- Get a Cayley graph whose vertices are the curves in the top layer (in bijection with $\mathrm{Pic}(\mathcal{O}_K)$ and whose edges correspond to prime ideals of small norm of $\mathcal{O}_K$
- **Conclusion:** via random walks, discrete log is, with some probability, comparatively hard on all curves in an isogeny class (Jao–Miller–Venkatesan'05)

Goal: what can we say about curves of genus 2?

Random Self-Reducibility of Discrete Logarithms - genus 1

- Using vertical isogenies, reduce the problem to two curves on the top layer $\mathcal{O}_K$
- Via complex multiplication theory, the curves on the top layer (after liftings to characteristic zero) correspond to $\mathbf{C}/\mathfrak{a}$ where $\in \mathrm{Cl}(\mathcal{O}_K)$
- Get a Cayley graph whose vertices are the curves in the top layer (in bijection with $\mathrm{Pic}(\mathcal{O}_K)$) and whose edges correspond to prime ideals of small norm of $\mathcal{O}_K$
- **Conclusion:** via random walks, discrete log is, with some probability, comparatively hard on all curves in an isogeny class (Jao–Miller–Venkatesan'05)

Goal: what can we say about curves of genus 2?

Random Self-Reducibility of Discrete Logarithms - genus 1

- Using vertical isogenies, reduce the problem to two curves on the top layer $\mathcal{O}_K$
- Via complex multiplication theory, the curves on the top layer (after liftings to characteristic zero) correspond to $\mathbf{C}/\mathfrak{a}$ where $\in \mathrm{Cl}(\mathcal{O}_K)$
- Get a Cayley graph whose vertices are the curves in the top layer (in bijection with $\mathrm{Pic}(\mathcal{O}_K)$) and whose edges correspond to prime ideals of small norm of $\mathcal{O}_K$
- **Conclusion:** via random walks, discrete log is, with some probability, comparatively hard on all curves in an isogeny class (Jao–Miller–Venkatesan'05)

Goal: what can we say about curves of genus 2?

Isogeny Graph and the random-self reducibility of DLP

Application: DLP on A can be reduced in polynomial time to the DLP on B.

Claim: Under GRH, the DLP in genus 2 is random-self reducible: Given a fixed order $\mathcal{O}$ in K, given any algorithm Alg that solves the DL on some 1/(polynomial in $\log p$) percentage of Jacobians of e.r. $\mathcal{O}$, one can solve probabilistically the DL on any Jacobian of e.r. $\mathcal{O}$ in polynomial in $\log p$ expected queries to Alg with random inputs.

Isogeny Graph and the random-self reducibility of DLP

Application: DLP on A can be reduced in polynomial time to the DLP on B.

Claim: Under GRH, the DLP in genus 2 is random-self reducible: Given a fixed order $\mathcal{O}$ in K, given any algorithm Alg that solves the DL on some $1/(\text{polynomial in } \log p)$ percentage of Jacobians of e.r. $\mathcal{O}$, one can solve probabilistically the DL on any Jacobian of e.r. $\mathcal{O}$ in polynomial in $\log p$ expected queries to Alg with random inputs.

Thank you.