Efficient $(3,3)$-isogenies between fast Kummer surfaces

Maria Corte-Real Santos[1] Craig Costello[2] Benjamin Smith[3]

[1]University College London

[2]Microsoft Research, Redmond

[3]INRIA & Laboratoire d'Informatique de l'École polytechnique (LIX)

ANTS XVI 2024

A classical problem

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 5$.

Problem

Given an elliptic curve E defined over $\mathbb{F}_q$ and a finite subgroup G of $E(\mathbb{F}_q)$, compute the quotient isogeny

$$\varphi : E \longrightarrow E' := E/G.$$

This was solved by Vélu (1971) (when E is given by a Weierstrass equation).

A newer problem

Problem

Given the Jacobian $\mathcal{J}$ of a genus-2 curve C defined over $\mathbb{F}_q$ and a finite subgroup G of $\mathcal{J}$, compute the quotient isogeny

$$\varphi : \mathcal{J} \longrightarrow \mathcal{J}' := \mathcal{J}/G.$$

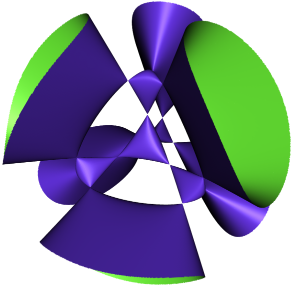
We want to find efficient algorithms to compute these isogenies where $G \subset \mathcal{J}[N]$ for N odd.

Our motivation comes from isogeny-based cryptography: low-degree isogenies in higher dimension gives high-degree isogenies in genus 1 (e.g., SQIsign2D).

Using the Kummer Surface

Let $\mathcal{J}$ be the Jacobian of a genus-2 hyperelliptic curve $\mathcal{C}$ defined over $\mathbb{F}_q$. $\mathcal{J}$ is an abelian surface with projective embedding in $\mathbb{P}^{15}$ $\rightsquigarrow$ not efficient!

Idea: follow Cassels–Flynn to replace $\mathcal{J}$ with the *Kummer surface*. The Kummer surface $\mathcal{K}$ of a Jacobian $\mathcal{J}$ is the quotient $\mathcal{J}/\{\pm 1\}$. It is the genus-2 analogue of the x-coordinate.



The surface $\mathcal{K}$ can be embedded as a quartic surface in $\mathbb{P}^3$.

It has 16 nodes (point singularities) given by the image of $\mathcal{J}[2]$ in $\mathcal{K}$.

Our Main Problem

Problem

Let N be an odd prime. Given a Kummer surface $\mathcal{K}$ defined over $\mathbb{F}_q$ and (the image of) a maximal N-Weil isotropic subgroup $G \subset \mathcal{K}$, compute the quotient isogeny

$$\varphi : \mathcal{K} \longrightarrow \mathcal{K}' := \mathcal{K}/G.$$

A subgroup $\widetilde{G} \subseteq \mathcal{J}[N]$ is a *maximal N-Weil isotropic subgroup* if $e_N(\widetilde{P}, \widetilde{Q}) = 1$ for all $\widetilde{P}, \widetilde{Q} \in \widetilde{G}$ and is not contained in any other isotropic subgroup.

Our Main Problem

Problem

Let N be an odd prime. Given a Kummer surface $\mathcal{K}$ defined over $\mathbb{F}_q$ and (the image of) a maximal N-Weil isotropic subgroup $G \subset \mathcal{K}$, compute the quotient isogeny

$$\varphi : \mathcal{K} \longrightarrow \mathcal{K}' := \mathcal{K}/G.$$

The quotient isogeny $\Phi : \mathcal{J} \to \mathcal{J}' := \mathcal{J}/\widetilde{G}$ descends to a morphism of Kummer surfaces $\varphi : \mathcal{K} \to \mathcal{K}'$, such that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{J} & \xrightarrow{\ \Phi\ } & \mathcal{J}' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ \mathcal{K} & \xrightarrow[\ \varphi\ ]{} & \mathcal{K}' \end{array}$$

Our Main Problem

Problem

Let N be an odd prime. Given a Kummer surface $\mathcal{K}$ defined over $\mathbb{F}_q$ and (the image of) a maximal N-Weil isotropic subgroup $G \subset \mathcal{K}$, compute the quotient isogeny

$$\varphi : \mathcal{K} \longrightarrow \mathcal{K}' := \mathcal{K}/G.$$

The quotient isogeny $\Phi : \mathcal{J} \to \mathcal{J}' := \mathcal{J}/\widetilde{G}$ descends to a morphism of Kummer surfaces $\varphi : \mathcal{K} \to \mathcal{K}'$. We set $G := \pi(\widetilde{G})$.

As $G \cong (\mathbb{Z}/N\mathbb{Z})^2$, i.e., $G = \langle R, S \rangle$ with $e_N(\widetilde{R}, \widetilde{S}) = 1$, we call φ an (N, N)-isogeny.

Our result is to give a new efficient method for $N = 3$ (and more generally odd prime N).

Previous Literature

	Construct invariant homogeneous forms	**Theta structures of level 2**	**Multiradical formulae**
$\mathbf{N = 2}$	Cassels–Flynn (1996)	Dartois–Maino–Pope–Robert (2023)	Castryk–Decru (2021)
$\mathbf{N = 3}$	Bruin–Flynn–Testa (2014), revisited by Flynn–Ti (2019) and Decru–Kunzweiler (2023)		Castryk–Decru (2021)
$\mathbf{N = 4}$	Nicholls (2018)		
$\mathbf{N = 5}$	Flynn (2015)		Castryk–Decru (2021)
General odd $\mathbf{N \neq p}$		Lubicz–Robert (2012, 2015, 2022), Cosset–Robert (2015)	

Fast Kummer Surfaces

Following Gaudry (2007), we use the *fast Kummer surface* model.

The Fast Kummer Surface

Let X_1, X_2, X_3, X_4 be coordinates on $\mathbb{P}^3$. The equation defining the fast Kummer surface $\mathcal{K}$ is

$$\mathcal{K} : X_1^4 + X_2^4 + X_3^4 + X_4^4 - 2E \cdot X_1X_2X_3X_4 - F \cdot (X_1^2X_4^2 + X_2^2X_3^2) - G \cdot (X_1^2X_3^2 + X_2^2X_4^2) - H \cdot (X_1^2X_2^2 + X_3^2X_4^2) = 0,$$

where E, F, G, H are rational functions in the *fundamental theta constants* $a, b, c, d \in \overline{\mathbb{F}}_p$.

The identity element $\mathcal{K}$ is $\mathcal{O}_{\mathcal{K}} = (a : b : c : d)$.

General method for computing (N, N)-isogenies

Fix odd $N \neq p$. Let $\mathcal{K}[N]$ be the image of $\mathcal{J}[N]$ in $\mathcal{K}$. Fix $R, S \in \mathcal{K}[N]$ generating the kernel of an (N, N)-isogeny $\varphi : \mathcal{K} \to \mathcal{K}/\langle R, S\rangle$.

Step 1: Find homogeneous functions of degree N that are invariant under translation-by-R. These forms generate a space X_R. Repeat for S.

Invariant Forms

Let $P = (X_1 : X_2 : X_3 : X_4)$ and $R \in \mathcal{K}[N]$. For $I = (i_1, \ldots, i_N) \in \{1, 2, 3, 4\}^N$, compute homogeneous forms of degree N defined by

$$F_{R,N}(I) = \sum_{\tau \in \mathrm{C}_N} X_{i_{\tau(1)}} \prod_{k=1}^{(N-1)/2} B_{i_{\tau(2k)}, i_{\tau(2k+1)}}(P, [k]R),$$

where C_N is the cyclic group of order N and $B_{i,j}$ are the biquadratic forms associated to $\mathcal{K}$.

General method for computing (N, N)-isogenies

Fix odd $N \neq p$. Let $\mathcal{K}[N]$ be the image of $\mathcal{J}[N]$ in $\mathcal{K}$. Fix $R, S \in \mathcal{K}[N]$ generating the kernel of an (N, N)-isogeny $\varphi : \mathcal{K} \to \mathcal{K}/\langle R, S \rangle$.

Step 1: Find homogeneous functions of degree N that are invariant under translation-by-R. These forms generate a space X_R. Repeat for S.

Example: $N = 3$

Let $R_{i,j} = B_{i,j}(P, R)$

1. $F_{R,3}(1,1,1) = X_1 R_{1,1}$
2. $F_{R,3}(1,2,3) = X_1 R_{2,3} + X_2 R_{1,3} + X_3 R_{1,2}$

General method for computing (N, N)-isogenies

Fix odd $N \neq p$. Let $\mathcal{K}[N]$ be the image of $\mathcal{J}[N]$ in $\mathcal{K}$. Fix $R, S \in \mathcal{K}[N]$ generating the kernel of an (N, N)-isogeny $\varphi : \mathcal{K} \to \mathcal{K}/\langle R, S \rangle$.

Step 1: Find homogeneous functions of degree N that are invariant under translation-by-R. These forms generate a space X_R. Repeat for S.

Step 2: Compute the intersection $X_{R,S} := X_R \cap X_S$. Then, $\dim X_{R,S} = 4$ with basis $\psi_1, \ldots, \psi_4$. The morphism

$$\psi = (\psi_1 : \psi_2 : \psi_3 : \psi_4) : \mathcal{K} \to \widetilde{\mathcal{K}}$$

has kernel $\langle R, S \rangle$, but $\tilde{\mathcal{K}}$ is *not* a fast Kummer surface.

Step 3: Find a linear transformation $\mathbf{M} : \widetilde{\mathcal{K}} \to \mathcal{K}'$, where $\mathcal{K}'$ is a fast Kummer surface. Then $\varphi = \mathbf{M} \circ \psi$. To find $\mathbf{M}$, we observe: for $T \in \mathcal{K}[2]$

$$\sigma_{(\varphi(T))}((\varphi_1 : \varphi_2 : \varphi_3 : \varphi_4)) = \varphi(\sigma_T(X_1 : X_2 : X_3 : X_4)).$$

The case $N = 3$

We now focus on $N = 3$. Run steps 1 and 2.

The morphism ψ is of the form

$$\begin{aligned}
\psi_1 &:= X_1(a_1X_1^2 + a_2X_2^2 + a_3X_2^2 + a_4X_4^2) + a_5X_2X_3X_4 \\
\psi_2 &:= X_2(b_1X_1^2 + b_2X_2^2 + b_3X_3^2 + b_4X_4^2) + b_5X_1X_3X_4 \\
\psi_3 &:= X_3(c_1X_1^2 + c_2X_2^2 + c_3X_3^2 + c_4X_4^2) + c_5X_1X_2X_4 \\
\psi_4 &:= X_4(d_1X_1^2 + d_2X_2^2 + d_3X_3^2 + d_4X_4^2) + d_5X_1X_2X_3
\end{aligned}$$

for some $a_i, b_i, c_i, d_i \in \mathbb{F}_q[\mathcal{O}_\mathcal{K}, R, S]$.

The case $N = 3$

We now focus on $N = 3$. Run steps 1 and 2. Apply the linear map (a scaling in this case).

The isogeny φ is of the form

$$\begin{aligned}
\varphi_1 &:= X_1(a_1X_1^2 + a_2X_2^2 + a_3X_2^2 + a_4X_4^2) + a_5X_2X_3X_4 \\
\varphi_2 &:= X_2(a_2X_1^2 + a_1X_2^2 + a_4X_3^2 + a_3X_4^2) + a_5X_1X_3X_4 \\
\varphi_3 &:= X_3(a_3X_1^2 + a_4X_2^2 + a_1X_3^2 + a_2X_4^2) + a_5X_1X_2X_4 \\
\varphi_4 &:= X_4(a_4X_1^2 + a_3X_2^2 + a_2X_3^2 + a_1X_4^2) + a_5X_1X_2X_3
\end{aligned}$$

for some $a_i \in \mathbb{F}_q[\mathcal{O}_\mathcal{K}, R, S]$.

The cost of computing $(3,3)$-isogenies

Precomputation: to compute the $(3,3)$-isogeny, we precompute *tripling constants*. This requires $12\mathtt{M}$, $4\mathtt{S}$ and $6\mathtt{a}$.

Computing Image of Isogeny: Given tripling constants, compute coefficients $a_1, \ldots, a_5$ defining the isogeny and then the image constants $(a' : b' : c' : d')$. Requires $102\mathtt{M}$, $8\mathtt{S}$ and $113\mathtt{a}$.

Pushing points through the isogeny: Given tripling constants and the coefficients $a_1, \ldots, a_5$, compute the image of the point under the isogeny. This requires $26\mathtt{M}$, $4\mathtt{S}$ and $16\mathtt{a}$.

We implement and optimise these algorithms in the code accompanying our paper.

Benchmarks

We compare our algorithms for computing $(3^k, 3^k)$-isogenies to those due to Castryk–Decru and Decru–Kunzweiler. We ran the algorithms in `Magma` and average over 100 random inputs for each prime size ($\log_2(p) = 128, 256$).

	k	Time taken (ms)
Castryk–Decru (2021)	225	1.51
	462	4.81
Decru–Kunzweiler (2023)	240	5.99
	477	18.29
This work	225	0.18
	462	0.53

We also give a implementation of our algorithms in SageMath/Python which returns the precise cost.