# PROJECTIVE GEOMETRY OF HESSIAN ELLIPTIC CURVES AND GENUS 2 TRIPLE COVERS OF CUBICS 

RÉMY OUDOMPHENG


#### Abstract

The existence of finite maps from hyperelliptic curves to elliptic curves has been studied for more than a century and their existence has been related to isogenies between a product of elliptic curves and their Jacobian surface Kuh88 Kan97.

Such finite covers, sometimes named gluing maps have recently appeared in cryptography in the context of genus 2 isogenies and more spectacularly, in the work of Castryck and Decru about the cryptanalysis of SIKE CD22. Computation methods include the use of algebraic theta functions CR15 LR or correspondences such as Richelot isogenies or degree 3 analogues BHLS15 BFT14 CD21 Kun22 Smi05.

This article aims at giving geometric meaning to the gluing morphism from a product of elliptic curves $E_{1} \times E_{2}$ to a genus 2 Jacobian when it is a degree $(3,3)$ isogeny. An explicit universal family and an algorithm were previously provided in BHLS15 and a similar special case was studied in Kuw11.

We provide an alternative construction of the universal family using concepts from classical algebraic and projective geometry. The family of genus 2 curves which are triple covers of 2 elliptic curves with a level 3 structure arises as a correspondence given by a polarity relation.

The construction does not provide closed formulas for the final curves equations and morphisms. However, an alternative algorithm based on the geometric construction is proposed for computation on finite fields. It relies only on elementary operations without requiring polynomial roots and computes the equation of the genus 2 curves and morphisms in all cases.


## 1. Introduction

The Hesse equations are a linear system of plane cubics defined by homogeneous equations in $\mathbb{P}^{2}$ :

$$
E_{t}: x^{3}+y^{3}+z^{3}=3 t x y z
$$

They are classically known to provide a model for the universal family of elliptic curves with a rational 3 -level structure (the modular curve $\mathcal{X}(3)$ ), with canonical sections for the 3 -torsion points at fixed coordinates $\left[1:-j^{k}: 0\right],\left[0: 1:-j^{k}\right]$, $\left[-j^{k}: 0: 1\right]$, where $j$ is a cubic root of unity and $k=1,2,3$.

The 9 torsion points are base points on this pencil and any other point in the plane belongs to a unique member $E_{\lambda}$ of the pencil. This identifies the total space of the Hesse pencil with the blow-up of $\mathbb{P}^{2}$ at these 9 base points, which is a well known elliptic surface.

The Hesse pencil has a large number of properties in projective geometry which can be found in AD09, Dol12, BM.

Using the traditional concepts of projective duality, we define a degree 3 correspondence between two members of the Hesse pencil which is invariant under diagonal action of $(\mathbb{Z} / 3 \mathbb{Z})^{2}$ acting by translation by order 3 points. The quotient of this correspondence is generically a smooth genus 2 curve.

Theorem 1. Let $E_{i}: x^{3}+y^{3}+z^{3}=3 t_{i} x y z(f o r i=1,2)$ be 2 smooth members of the Hesse pencil and $\Gamma$ be the isotropic subgroup of $E_{1}[3] \times E_{2}[3]$ consisting of elements $(x, \bar{x})$ which are conjugates for the map $j \mapsto j^{-1}$.

Then the quadratic equation $x_{1} x_{2}+y_{1} y_{2}+z_{1} z_{2}=0$ on $\mathbb{P}^{2} \times \mathbb{P}^{2}$ defines a divisor $\tilde{H}$ on $E_{1} \times E_{2}$ which descends to a principal polarisation on the abelian surface $E_{1} \times E_{2} / \Gamma$.

The quotient $H=\tilde{H} / \Gamma$ is a smooth genus 2 curve if and only if there is no degree 2 isogeny $\phi: E_{1} \rightarrow E_{2}$ such that $\phi(x)=\bar{x}$ for $x \in E_{1}[3]$.

A special case of genus 2 triple covering using a similar construction is presented by M. Kuwata in Kuw11.

Several special cases (singular covers, triple ramification) will also be illustrated by equivalent geometric properties.

Following this construction we describe a projection from $H$ to a rational nodal curve in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ allowing to compute explicit equations. Another way to obtain explicit equations was described in BHLS15.

Our results can be described as follows:
Theorem 2. The image of $H$ through the sequence of maps $\operatorname{Jac}(H) \simeq E_{1} \times E_{2} / \Gamma \rightarrow$ $E_{1} \times E_{2} \rightarrow \mathbb{P}^{1} \times \mathbb{P}^{1}$ defined by the dual isogeny and the quotient by hyperelliptic involutions maps $H$ to a rational curve $\bar{H}_{\iota}$ of degree $(3,3)$. The image of the 6 Weierstrass points of $H$ coincides with the 2 triples of Weierstrass points in $E_{1} \rightarrow \mathbb{P}^{1} \times\{\infty\}$ and $E_{2} \rightarrow\{\infty\} \times \mathbb{P}^{1}$.

It has generically 4 nodes whose coordinates are rational functions of $t_{1}$ and $t_{2}$ which are in canonical one-to-one correspondence with the 4 elements of $(\Gamma \backslash 0) / \pm 1$.

These 10 points determine uniquely the equation of $\bar{H}_{\iota}$.
The normalization of $\bar{H}_{\iota}$ contains 2 canonical rational points corresponding to the ramification points of $H \rightarrow E_{i}$. This determines an isomorphism $\mathbb{P}^{1} \rightarrow \bar{H}$ and an explicit hyperelliptic equation for $H$ with degree 3 morphisms to $E_{1}$ and $E_{2}$.

This construction can be closely related to geometric considerations from DL08. In particular the double points of $\bar{H}_{\iota}$ are related to effective divisors representing the kernel of the dual isogeny $H \rightarrow E_{1} \times E_{2}$.

Section 2 provides an overview of the construction of the family of genus 2 triple covers and explains relations with properties already known in the literature Kuh88, BHLS15. Section 3 examines the properties of these triple covers with more detail in order to derive equations and computational aspects in section 4 , including an alternate construction algorithm (section 4.7).

Many computations were assisted by Sagemath [SAGE and Singular DGPS22. The final implementation given in appendix uses Sagemath as software framework.

## 2. Projective geometry of Hesse cubics and polar conjugacy

In this section, the base field $\mathbb{k}$ has characteristic different from 2 and 3, and points will designate geometric points (with coefficients in an algebraic closure), and rational points will designate points with values in $\mathbb{k}$. Most computational aspects will target the specific case of finite fields but many formulas are also valid over $\mathbb{Q}\left(j, t_{1}, t_{2}\right)$ and can be applied in a broader context.

In this section we briefly recall the definition of the Hesse pencil of cubics and construct a universal family of common triple covers (with arithmetic genus 10) for pairs of elliptic curves. This family is invariant under the action of $(\mathbb{Z} / 3 \mathbb{Z})^{2}$ acting globally by universal projective transformations on all fibres, the action being equivalent to translation by 3 -torsion elements.
2.1. The Hesse pencil. The projective properties of the flex points of a plane cubic are beautifully explained in the expository article BM] and in Dol12. Following [Dol12] a flex point designates a point $P$ of a smooth plane curve where the tangent line $T_{P}$ intersects the curve at point $P$ with multiplicity 3 .

We are interested in the following theorem:
Theorem 2.1. Every plane cubic is projectively equivalent to a curve in Hesse normal form where $t^{3} \neq 1$.

$$
x^{3}+y^{3}+z^{3}=3 t x y z
$$

Moreover, if the cubic is defined over a field $\mathbb{k}$ and possesses 9 rational flex points, this projective equivalence can be realised over $\mathfrak{k}$.

A cubic defined by a Hesse equation has 9 flex points at coordinates $\left[0: 1: \zeta^{i}\right]$ (up to cyclic permutation) where $i \in\{0,1,2\}$ and $\zeta$ is a cubic root of unity.

Any flex point can be used as the origin of an elliptic curve structure where the group law is the secant law. The projection from a flex point defines a degree 2 map $E \rightarrow \mathbb{P}^{1}$ and the corresponding hyperelliptic involution.

The usual convention across this article will be to select point $O=[1:-1: 0]$ as the distinguished flex point, so that for any point $P=[x: y: z] \in E$ the point $\iota(P)=[y: x: z]$ also belongs to $E$ and $O, P, \iota(P)$ are collinear.

In particular, the involution associated to $O$ can be represented by the projective $\operatorname{map}[x: y: z] \mapsto[y: x: z]$. The corresponding 3 ramification points are the intersection of $E$ with the polar line of $O, \ell_{O}=\{x=y\}$.

This can be realized explicitly by using affine coordinates $u=z /(x+y+t z)$ and $v=(x-y) /(x+y+t z)$. The equation of $E_{t}$ in these coordinates is:

$$
3 v^{2}=4\left(t^{3}-1\right) u^{3}-9 t^{2} u^{2}+6 t u-1
$$

Throughout this article we assume that the equivalence between a Hessian equation and a level 3 structure is given by the choice of $[1:-1: 0]$ as the group law origin, and points $[0: 1:-1]$ and $[1:-j: 0]$ as the basis of the 3 -torsion subgroup.

This choice determines uniquely the projective transformation from an elliptic curve with a distinguished symplectic basis of the 3 -torsion subgroup (assumed to be defined over $\mathbb{k}$ ).
2.2. Properties of triple covers. Let $H$ be a genus 2 curve with 2 complementary elliptic degree 3 subcovers $H \rightarrow E_{1}$ and $H \rightarrow E_{2}$. Then $H$ defines a degree 3 correspondence between $E_{1}$ and $E_{2}$ and the associated morphism $E_{1} \rightarrow \operatorname{Sym}^{3} E_{2} \rightarrow$ $\mathrm{Jac} E_{2} \simeq E_{2}$ is the zero map Kuh88.

It is also known Mir85 that any triple cover can be defined as a subscheme of a $\mathbb{P}^{1}$-bundle Proj $E$ where $E$ is a rank 2 vector bundle on the base curve.

In the case of elliptic curves represented as plane cubics, the traditional definition of the group law implies that the image of a point of $E_{1}$ by the above correspondence must be a degree 3 divisor on $E_{2}$ equivalent to zero, so this divisor is defined by a line in $\mathbb{P}^{2}$ (a secant of $E_{2}$ ), which is a point in the dual projective plane $\left(\mathbb{P}^{2}\right)^{\vee}$. A natural candidate for the $\mathbb{P}^{1}$-bundle containing $H$ is thus a bundle of lines in $\mathbb{P}^{1}$ defined by a map $E_{1} \rightarrow\left(\mathbb{P}^{2}\right)^{\vee}$.

Moreover, since the map $H \rightarrow E_{2}$ has degree 3, we expect each point of $E_{2}$ to appear in 3 such lines, so the map $E_{1} \rightarrow\left(\mathbb{P}^{2}\right)^{\vee}$ would have degree 3 . Any such map is the composite of a group translation and a (linear) projective transformation, so
a natural candidate to realise the triple cover is a diagram:

where $\mathcal{L}$ is a bundle of lines (a $\mathbb{P}^{1}$-fibration over $E_{1}$ ) which is the pullback of the incidence variety $\mathcal{Q}=\{(\ell, P)$ such that $P \in \ell\} \subset\left(\mathbb{P}^{2}\right)^{\vee} \times \mathbb{P}^{2}$, seen as a tautological $\mathbb{P}^{1}$-bundle, by $E_{1} \rightarrow\left(\mathbb{P}^{2}\right)^{\vee}$.

Then $H$ could be viewed as the fiberwise intersection of $E_{1} \times E_{2}$ with $\mathcal{L}$ which is a degree 3 cover of $E_{1}$.

The hyperelliptic involution $\iota: H \rightarrow H$ defines a rational quotient $H_{\iota} \simeq \mathbb{P}^{1}$ and commutes with the projection maps as in diagram:


All vertical arrows in the diagram are quotients by the hyperelliptic involution ( $x$ coordinate). In particular, $H$ is stable under involution $\left(y_{1}, y_{2}\right) \rightarrow\left(-y_{1},-y_{2}\right)$.

In particular, the rational functions $u_{1}$ and $u_{2}$ have degree 3 , and the image of $H$ in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ through $\left(u_{1}, u_{2}\right)$ is a rational cubic of degree $(3,3)$.

We will need the following property proved in Kuh88.
Theorem 2.2. Let $\left\{C_{1}, \ldots, C_{6}\right\}$ be the 6 Weierstrass points of $H$. Then up to permutation, $\left\{C_{1}, C_{2}, C_{3}\right\}$ is the preimage of the zero point of $E_{1}$ and $\left\{C_{4}, C_{5}, C_{6}\right\}$ map to the 3 other Weierstrass points of $E_{1}$, and conversely for the projection $H \rightarrow E_{2}$.

In particular, there exists an equation for $H: y^{2}=P(x) Q(x)$ where $P$ and $Q$ have degree 3 such that the $x$-coordinates of the projection maps have denominator $P$ and $Q$. This will be revisited with more detail in the next sections.
2.3. The canonical duality of the projective plane. In appropriate coordinates, the incidence variety

$$
\mathcal{Q}=\{(P, \ell) \text { such that } P \in \ell\} \subset \mathbb{P}^{2} \times\left(\mathbb{P}^{2}\right)^{\vee}
$$

can be defined by a bilinear equation $x_{1} x_{2}+y_{1} y_{2}+z_{1} z_{2}=0$. The quadratic form $x^{2}+y^{2}+z^{2}$ can be used to identify $\mathbb{P}^{2}$ with the dual plane and define a polarity relation where a point $P=[a: b: c]$ is associated to the line $\ell_{P}: a x+b y+c z=$ 0 . Throughout this article $\ell_{P}$ will always denote the polar line of $P$ w.r.t. that particular quadratic form.

For this duality relation, the polar of a flex point $P_{0}$ intersects Hesse cubics at the 3 Weierstrass points of the projection from pole $P_{0}$ (the polar line of $[1:-1: 0]$ is the line $\{x=y\}$ ), which conveniently coincides with the relation between Weierstrass points of $H, E_{1}, E_{2}$ described in Kuh88.

We therefore define the curve:

$$
\tilde{H}=\left\{x_{1} x_{2}+y_{1} y_{2}+z_{1} z_{2}=0\right\} \subset E_{1} \times E_{2}
$$

This is a genus 10 curve with a free action of the group $\Gamma=(\mathbb{Z} / 3 \mathbb{Z})^{2}$ acting by translation on both $E_{1}$ and $E_{2}$ via its generators:

$$
\begin{aligned}
& \gamma_{1}:\left(\left[x_{1}: y_{1}: z_{1}\right],\left[x_{2}: y_{2}: z_{2}\right]\right) \mapsto\left(\left[z_{1}: x_{1}: y_{1}\right],\left[z_{2}: x_{2}: y_{2}\right]\right) \\
& \gamma_{2}:\left(\left[x_{1}: y_{1}: z_{1}\right],\left[x_{2}: y_{2}: z_{2}\right]\right) \mapsto\left(\left[x_{1}: j y_{1}: j^{2} z_{1}\right],\left[x_{2}: j^{2} y_{2}: j z_{2}\right]\right)
\end{aligned}
$$



Figure 1. The polarity relation over $\mathbb{R}$, where $\left(P, Q_{i}\right) \in \tilde{H}$
The inverted roots of unity on the second factor are reminiscent of Kani's property: a genus 2 triple cover is determined by an anti-isometry over the 3 -torsion groups of $E_{1}$ and $E_{2}$.

The computation of genus can be done using the determination of ramification points (see below) and the Riemann-Hurwitz formula.

We will be interested in the quotient on this curve by $\Gamma$, which is a genus 2 curve.

### 2.4. Tangents and ramification.

Theorem 2.3. Let $\left(p_{1}, p_{2}\right)$ be a point of $\tilde{H}$. The differential of the map $\tilde{H} \rightarrow E_{i}$ can be identified with the linear equations of $\ell_{p_{2}}$ and $\ell_{p_{1}}$.

In particular, the projection to $E_{i}$ is ramified if and only if the polar line through $p_{i}$ is tangent to $E_{i}$.
Proof. This is a consequence of the equation of $\tilde{H}$. The differential of $x_{1} x_{2}+y_{1} y_{2}+$ $z_{1} z_{2}$ is $\left(x_{1}, y_{1}, z_{1}\right) \cdot d\left(x_{2}, y_{2}, z_{2}\right)+\left(x_{2}, y_{2}, z_{2}\right) \cdot d\left(x_{1}, y_{1}, z_{1}\right)$ where symbol $\cdot$ is the "dot product" corresponding to the standard bilinear form.

In particular, the projection to $E_{2}$ is ramified if and only if the tangent space of $E_{2}$ is orthogonal to $\left(x_{1}, y_{1}, z_{1}\right)$ for the standard bilinear form, which is the same equation as the polar line $\ell_{1}$.

This allows to determine the condition for the special triple covers in a geometric way (special in the sense of Sha04 refers to triple covers having a single triple ramification point).

Lemma 2.4. A triple cover is special (i.e. the map $H \rightarrow E_{1}$ has a triple ramification point) if and only if a Weierstrass point of $E_{1}$ is conjugate to a tangent through a flex point of $E_{2}$, which is defined by equation $t_{2}^{3}-3 t_{1} t_{2}+2=0$.

Proof. A triple ramification point can only happen if for some point $P \in E_{1}$ the polar line $\ell_{P}$ intersects $E_{2}$ with multiplicity 3 , meaning that it meets $E_{2}$ at a flex point. By $\Gamma$-invariance we can assume that this flex point is $[1:-1: 0]$.

The coordinates of the tangent line to that flex point in $E_{2}$ are $\left[x^{2}-t_{2} y z\right.$ : $\left.y^{2}-t_{2} z x: z^{2}-t_{2} x y\right]=\left[1: 1: t_{2}\right]$ which belongs to $E_{1}$ if and only if $t_{2}^{3}-3 t_{1} t_{2}+2=0$.

In this situation, since $\left[1: 1: t_{2}\right]$ lies on line $\{x=y\}$ it is a Weierstrass point of $E_{1}$.

The curve $E_{2}$ is known as the Cayleyan curve of $E_{1}$ and the construction of the genus 2 triple cover in that case can be found in Kuw11.
2.5. The singular case and isogenous elliptic curves. From Kani's theorem Kan97, the quotient $E_{1} \times E_{2} / \Gamma$ fails to be a genus 2 Jacobian if and only if the isomorphism $E_{1}[3] \simeq E_{2}[3]$ is induced by an isogeny of degree 2 .

A geometric construction of such isogenies is provided in Dol12, Section 3.2.2] and can be summarised by the following property (relating the Hessian curve and the Cayleyan curve of a given cubic):
Proposition 2.5. Let $E_{t}$ be a Hessian cubic curve, and let $\tau$ be an involution corresponding to translation by a 2-torsion point.

Then the set of lines $(P, \tau(P))$ is also a Hessian cubic curve $E_{u}$ in the dual projective plane, and the map $f: P \rightarrow(P, \tau(P)) \in\left(\mathbb{P}^{2}\right)^{\vee}$ is a degree 2 isogeny.

By definition, a line in the dual projective plane can be identified with its polar point in $\mathbb{P}^{2}$. So for every point $P \in E_{t}, P$ and $\tau(P)$ are conjugates to $f(P) \in E_{u}$.

If $\tilde{H}$ is the triple cover of $E_{t}$ and $E_{u}$ defined by the polarity relation, the latter property implies the existence of a section $E_{t} \rightarrow \tilde{H}$ by $P \mapsto(P, f(P))$, which would be impossible if $\tilde{H}$ was a smooth curve of genus $g>1$.

Proposition 2.6. Let $\phi: E_{\lambda} \rightarrow E_{\mu}$ be a degree 2 isogeny between curves in Hesse form, and let $\tilde{H}$ be the set of conjugate points in $E_{\lambda} \times E_{\mu}$ using the above construction.

Then $\tilde{H}$ is not irreducible and is the union of the graph of $\phi$ and the (translated) graph of the dual isogeny.

Proof. From the dual construction above, we can identify $\phi$ with the map $P \mapsto$ $\ell(P, P+\epsilon)$ where $\epsilon$ is the order 2 point in the kernel of $\phi$.

According to the secant group law, since $\phi(P)=\phi(P+\epsilon)=Q$, the polar line $\ell_{Q}$ goes through $P, P+\epsilon$ and $-2 P-\epsilon$.

This means that $\tilde{H}$ consists of pairs $(P, Q)=(P, \phi(P)),(P+\epsilon, Q)=(P+$ $\epsilon, \phi(P+\epsilon)$ ) (belonging to the graph of $\phi$ ) and $(-2 P-\epsilon, Q)=\left(-\phi^{*}(Q)-\epsilon, Q\right)$ (belonging to the translated graph of the dual isogeny $\phi^{*}$ ).

In particular, $\tilde{H}$ is the union of 2 irreducible components isomorphic to $E_{\lambda}$ and $E_{\mu}$.

These irreducible components meet when $Q=\phi\left(-\phi^{*}(Q)-\epsilon\right)=-2 Q$, that is, exactly along the graph of $\phi$ restricted to the 3 -torsion subgroup.

This decomposition corresponds to the classically known fact that a Theta divisor on a principally polarised abelian variety is reducible when the abelian variety decomposes as a product. The union of 2 elliptic curves intersecting at 9 points has arithmetic genus equal to 10 , which is the same as the smooth case.

## 3. Geometry of the genus 2 triple cover

This section establishes several properties that will be used for explicit computations in 4.

The action of group $\Gamma$ on $\mathbb{P}^{2}$ is generated by projective transformations:

$$
\begin{gathered}
{[x: y: z] \mapsto[y: z: x]} \\
{[x: y: z] \mapsto\left[x: \alpha y: \alpha^{2} z\right] \text { for } \alpha \in \mu_{3}}
\end{gathered}
$$

This action has no fixed point on each smooth member $E_{t}$ of the Hesse pencil.

Across this section we will use Halphen's coordinates defining a degree 9 rational map $\mathbb{P}^{2} \rightarrow \mathbb{P}^{2}$. This map is invariant under $\Gamma$ and acts on each element of the Hesse pencil as the isogeny [3] : $P \mapsto 3 P$, so the tripling map [3] realises a quotient $\mathbb{P}^{2} \rightarrow \mathbb{P}^{2} / \Gamma$.

The Halphen coordinates correspond to the fact that the formula for computing the triple of a point for the elliptic curve group law, choosing a given flex point as origin (we have chosen $[1:-1: 0]$ ) are independent of the parameter $t$ and defined by universal polynomials:

$$
\begin{aligned}
& X=x^{6} y^{3}+y^{6} z^{3}+z^{6} x^{3}-3 x^{3} y^{3} z^{3} \\
& Y=x^{3} y^{6}+y^{3} z^{6}+z^{3} x^{6}-3 x^{3} y^{3} z^{3} \\
& Z=x y z\left(x^{6}+y^{6}+z^{6}-x^{3} y^{3}-y^{3} z^{3}-z^{3} x^{3}\right)
\end{aligned}
$$

3.1. The genus 2 triple cover as a quotient correspondence. We have established that the polarity conjugacy relation defines a $\Gamma$-equivariant degree 3 correspondence between a pair of elliptic curves in Hesse normal form.

As a consequence the quotient $\tilde{H} \rightarrow H=\tilde{H} / \Gamma$ is an unramified map with genus $2\left(2 g_{H}-2=\left(2 g_{\tilde{H}}-2\right) / 9=2\right.$ and the following diagram commutes:


The projections from $H$ to $E_{i}$ have degree 3. By Riemann-Hurwitz formula, the map $H \rightarrow E_{i}$ has 2 ramification points which are exchanged by the hyperelliptic involution (or in the special case, a triple ramification point which is a Weierstrass point) Kuh88.

Theorem 3.1. The embedding

$$
H \simeq \tilde{H} / \Gamma \hookrightarrow\left(E_{1} \times E_{2}\right) / \Gamma
$$

is isomorphic to the embedding of $H$ as a Theta divisor in its Jacobian.
In particular $E_{1} \times E_{2} \rightarrow \mathrm{Jac} H$ is a $(3,3)$-isogeny with kernel

$$
\Gamma \simeq\left\{\left(T_{1}, T_{2}\right) \in E_{1}[3] \times E_{2}[3] \text { such that } T_{1}=T_{2} \text { in } \mathbb{P}^{2}\right\}
$$

It should be noted that whereas $\tilde{H}$ is embedded as a smooth curve in $E_{1} \times E_{2}$, the projection maps from $H$ to $E_{i}$ do not define a smooth embedding $H \subset E_{1} \times E_{2}$. The map $H \rightarrow E_{1} \times E_{2}$ factors through $\left(E_{1} \times E_{2}\right) / \Gamma \rightarrow E_{1} \times E_{2}$ and the final image of $H$ has singularities. The following sections will show that it generically has 8 double points, which is consistent with the fact that a bilinear pairing generates a polarity correspondence which is represented by a curve of arithmetic genus 10 .
3.2. The polarity relation on quotient $H$. Using the same properties as the first section, we can determine that the following property is true:

Proposition 3.2. The degree 3 correspondence $E_{1} \leftarrow H \rightarrow E_{2}$ defines a map $E_{1} \rightarrow\left(\mathbb{P}^{2}\right)^{\vee}$ which is induced by a projective transformation or equivalently by polarity via a bilinear pairing.

This bilinear pairing $b_{t_{1}, t_{2}}$ depends on the Hesse parameters $t_{1}$ and $t_{2}$ and is not always symmetric.

Equivalent, this means that the image of $H$ in $E_{1} \times E_{2}$ can be defined as the zero locus of a section of $\mathcal{O}(1,1)$.

Embeddings of an elliptic curve in a projective plane can differ by translations by an elliptic curve element and by projective transformations.

Here the fact that the zero element is mapped to the secant through the 3 associated Weierstrass points (which have a zero sum) is in favour of looking for a purely projective transform.

We prove this proposition by constructively building the matrix. The coefficients can be obtained through formal computation (see section 4.3). They were determined by interpolating rational functions through numerical simulations (over finite fields) and checking that the composite equation $b_{t_{1}, t_{2}}\left(3 P_{1}, 3 P_{2}\right)=0$ on $E_{1} \times E_{2}$ (a bilinear combination of Halphen coordinates) belongs to the ideal defining $\tilde{H}$.

To avoid confusion when referring to the polarity relation defined by bilinear form $b_{t_{1}, t_{2}}$ the notation $\ell_{P}^{1}$ will be used (and $\ell_{Q}^{2}$ for the polar line w.r.t. bilinear form $\left.b_{t_{2}, t_{1}}\right)$.
3.3. Projection to $\mathbb{P}^{1} \times \mathbb{P}^{1}$. Since 2-torsion points are sent to themselves by the tripling map [3], in the quotient representation the distinguished origin $[1:-1: 0$ ] is still conjugate to the line $\{x=y\}$ through the 3 Weierstrass points of either $E_{1}$ or $E_{2}$, even when considering the parametre-dependent bilinear relation $b_{t_{1}, t_{2}}$.

Since the tangent line at origin has dual coordinates $[1: 1: t]$, we can define the projection from the origin with formula $z /(x+y+z t)$, which is invariant by the involution $[x: y: z] \mapsto[y: x: z]$ and maps $E_{i}$ to $\mathbb{P}^{1}$ (the origin is mapped to the infinity point).

The 2 projections to $\mathbb{P}^{1}$ define a rational (hence regular) map from $H$ to $\mathbb{P}^{1} \times \mathbb{P}^{1}$ via $E_{1} \times E_{2}$. The 2 triples of Weierstrass points of $E_{1}$ and $E_{2}$ are mapped to the 2 lines at infinity in $\mathbb{P}^{1} \times \mathbb{P}^{1}$.

Since this projection realises the quotient by the hyperelliptic involution of $H$, we expect the image of $H$ to be a rational curve. Additionally, the "horizontal" and "vertical" pencils of lines lift to pencils of lines through the origin $P_{0}=[1:-1: 0]$ in $\mathbb{P}^{2}$. Each such line generically meets $E_{1}$ (or $E_{2}$ ) in 2 points outside $P_{0}$, thus defines 6 points in $H$ ( 3 pairs of points exchanged by the hyperelliptic involution). This implies that the image of $H$ in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ is expected to have degree $(3,3)$.

A degree $(3,3)$ in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ has generic genus $4\left(2 g_{a}-2=C \cdot\left(C+K_{\mathbb{P}^{1} \times \mathbb{P}^{1}}\right)=\right.$ $(3,3) \cdot(1,1)=6)$. Since the image of $H$ is a rational curve, we expect it to have 4 singular points, corresponding to generically 8 singular points in $E_{1} \times E_{2}$.

Each point of $\mathbb{P}^{1} \times \mathbb{P}^{1}$ defines a birational map to $\mathbb{P}^{2}$ by blowing up that point and contracting the horizontal and vertical lines through it $\left(L^{2}=(L+E)^{2}-2 L \cdot E-E^{2}=\right.$ -1 ). Choosing the point at infinity $(\infty, \infty)$ recovers the birational map $\mathbb{P}^{1} \times \mathbb{P}^{1} \rightarrow \mathbb{P}^{2}$ which coincides with the identity map on the open set corresponding to the affine plane $\mathbb{A}^{2}$.

Thus if the 4 singular points are in general position, a standard quadratic transformation centered at one of these points, followed by a quadratic transformation based on the triangle formed by the 3 other points, will resolve all singularities and establish a birational map from $H_{\iota}$ to a conic (we will see that the scenario of a triple point is also possible). This process is detailed in section 4.7 .

The singular case. When $\tilde{H}$ becomes reducible as the union of the graph of a 2-isogeny $\phi: E_{1} \rightarrow E_{2}$ and its dual (see section 2.5) the graph of $\phi$ has degrees $(1,2)$ with respect to the projections, and the graph of $\phi^{*}$ has degree $(2,1)$. These graphs are invariant by action of $\Gamma$ so the final image of $\tilde{H}$ in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ is a union of conics of degrees $(1,2)$ and $(2,1)$ intersecting in 4 points. This can be detected in the implementation by obtaining a degree 2 instead of 6 in the rational parameterisation.
3.4. Twisted dual curves and double points. A specific situation arises when $\tilde{H}$ contains pairs $(P, Q)$ and $\left(P, Q^{\prime}\right)$ such that $3 Q=3 Q^{\prime}$ (meaning that $Q$ and $Q^{\prime}$
differ by a 3 -torsion element). In that case, the corresponding points of $H$ map to the same pair $(3 P, 3 Q)$ in $E_{1} \times E_{2}$.

In other words, while $\ell_{P}$ is a secant of $E_{2}$, the line $\ell_{3 P}^{1}$ is tangent to $E_{2}$ at $3 Q$. By $\Gamma$ invariance, we observe that if $\tilde{H}$ contains $(P, Q)$ and $(P, Q+T)$, it also contains $(P-T, Q)$ thus the polar line $\ell_{3 Q}^{2}$ is tangent to $E_{1}$ at point $3 P$.

Lemma 3.3. The locus of lines $(Q, Q+T)$ defines a singular sextic $E_{2}^{T}$ in the dual projective plane. When identified to a sextic in $\mathbb{P}^{2}$ via the $x^{2}+y^{2}+z^{2}$ duality, it intersects $E_{1}$ in 18 points forming $2 \Gamma$-orbits exchanged by the canonical involution.

Explicit equations for these twisted dual curves will be given in the last section. Since $E_{2}^{T}$ and $E_{2}^{-T}$ have the same definition, we can define 4 such twisted duals.

Since pairs $(P, Q)$ and $(P, Q+T)$ are not in the same orbit for the action of $\Gamma$, they do not define the same point of $H$, even though they map to the same point $(3 P, 3 Q) \in E_{1} \times E_{2}$.

It results that each twisted dual curve defines a double point of the image of $H$ in $\mathbb{P}^{1} \times \mathbb{P}^{1}$. The coordinates of these double points are given by rational functions of $t_{1}$ and $t_{2}$ and are computed in section 4.

The case of triple points. Under adequate conditions, it may happen that a line $\ell_{P}$ contains $Q, Q+T_{1}$ and $Q+T_{2}$ where $T_{2}$ and $T_{1}$ are linearly independent (the case $T_{2}=-T_{1}$ implies that $Q$ is a 3 -torsion point, which has already been studied). In this situation $Q$ is necessarily a 9 -torsion point.

This means that $P$ belongs to the 3 twisted duals $E_{2}^{T_{1}}, E_{2}^{T_{2}}$ and $E_{2}^{T_{1}-T_{2}}$, and any point belonging to 2 twisted duals automatically belongs to the third one.

Similarly, the points $(P, Q),\left(P, Q+T_{1}\right),\left(P, Q+T_{2}\right)$ do not define the samme $\Gamma$-orbit and are 3 different points of $H$ mapping to the same point $(3 P, 3 Q)$ in $E_{1} \times E_{2}$. This situation defines a triple point in the image of $H$ in $E_{1} \times E_{2}$.

This triple point will also be visible in the image in $\mathbb{P}^{1} \times \mathbb{P}^{1}$.
3.5. A family of genus 2 coverings. Since the Hesse pencil is isomorphic to the universal family of elliptic curves with a 3-level structure, the family:

where $\mathcal{Q}$ is the quadric defined by the polarity relation and the downward arrow are quotients under the action of $\Gamma$, and $S(3)$ is the blow-up of $\mathbb{P}^{2}$ along the 9 base points of the Hesse pencil, define a universal family of triple coverings of elliptic curves by a genus 2 curve (for any pair of elliptic curve with a choice of symplectic 3 -torsion basis, the genus 2 triple cover is known to be unique up to isomorphism).

Over the open locus of $\mathbb{P}^{1} \times \mathbb{P}^{1}$ corresponding to pairs of smooth elliptic curves $\left(t \neq \infty\right.$ and $\left.t^{3} \neq 1\right)$, each fibre is either a smooth genus 2 curve, or a stable curve isomorphic to the two elliptic curves joined by the origin $E_{1} \sqcup E_{2}$.

Further properties of this family as an actual scheme-theoretic moduli space (in particular as representing a sheaf in an appropriate topology) are not in scope of this work.

In particular, the existence of this family does not imply that it is globally isomorphic to a family of hyperelliptic curves defined by equations $y^{2}=H(x)$, even if it is true pointwise.

## 4. Computing explicit Equations of the Triple cover

A base field of definition $\mathbb{k}$ is fixed for these computation, in order to distinguish cases where the geometric situation (over $\overline{\mathbb{k}}$ ) can differ from the base field situation.

Most explicit equations in this section were obtained using software SageMath SAGE and Singular DGPS22 by writing equations on $\tilde{H}$ and descending to the quotient in Halphen coordinates $[X: Y: Z]$ by variable elimination.

In this section we will often have to determine point coordinates in Weierstrass form $U=Z /(X+Y+t Z)$ by finding a linear relation between $X+Y$ and $t Z$. When performing variable elimination via Grőbner basis computation the following invariant polynomials (with fewer terms) turn out to be very useful:

$$
\begin{aligned}
A & =x y z \\
B & =x^{6} y^{3}+y^{6} z^{3}+z^{6} x^{3} \\
C & =x^{3} y^{6}+y^{3} z^{6}+z^{3} x^{6} \\
X & =B-3 A^{3} \\
Y & =C-3 A^{3} \\
t Z & =9\left(t^{3}-1\right) A^{3}-(B+C) \text { if }[x: y: z] \in E_{t}
\end{aligned}
$$

The usual procedure is then to perform a change of variables from $(x, y, z)$ to $(A, B, C)$ and obtain a linear relation between $A^{3}$ and $B+C$. An additional intermediate step can use $\left(x y z, x^{2} y+y^{2} z+z^{2} x, x y^{2}+y z^{2}+z x^{2}\right)$ if necessary.
4.1. Coordinates of the pair of ramification points. A projection $\tilde{H} \rightarrow E_{1}$ is ramified over a point $p$ iff the polar line (with respect to the standard bilinear form) $\ell_{p}$ is tangent to $E_{2}$ (see section 2.4). The set of ramification points is invariant under the hyperelliptic involution and the action of $\Gamma$, and can be expressed as the intersection of $E_{1}$ and the dual variety $E_{2}^{\vee}$ which is the locus of tangent lines to $E_{2}$, viewed in $\left(\mathbb{P}^{2}\right)^{\vee} \simeq \mathbb{P}^{2}$. The birational map $[x: y: z] \mapsto\left[x^{2}-t y z: y^{2}-t z x: z^{2}-t x y\right]$ associates a point of $E_{t}$ to its tangent and maps $E_{t} \rightarrow E_{t}^{\vee}$.

The dual curve can be represented by a (singular) plane sextic and its equation can be found in AD09 or Dol12, Section 3.2.3]:

$$
\begin{aligned}
& E_{1}: x^{3}+y^{3}+z^{3}=3 t_{1} x y z \\
& E_{2}: x^{3}+y^{3}+z^{3}=3 t_{2} x y z \\
& E_{2}^{\vee}: x^{6}+y^{6}+z^{6}+\left(4 t_{2}^{3}-2\right)\left(x^{3} y^{3}+y^{3} z^{3}+z^{3} x^{3}\right) \\
& -6 t_{2}^{2} x y z\left(x^{3}+y^{3}+z^{3}\right)+\left(12 t_{2}-3 t_{2}^{4}\right) x^{2} y^{2} z^{2}=0
\end{aligned}
$$

Using intermediate coordinates as above, a computer-assisted computation finds a low-degree member of the ideal of $E_{1} \cap E_{2}^{\vee}$ :

$$
A^{3}\left(144 t_{1} t_{2}^{4}+216 t_{1}^{2} t_{2}^{2}-27 t_{1}^{3}-96 t_{2}^{3}-72 t_{1} t_{2}+12\right)+\left(4-32 t_{2}^{3}\right)(B+C)=0
$$

to obtain a linear equation in the quotient plane:

$$
\begin{aligned}
& \tau=t_{2}^{4}+6 t_{1} t_{2}^{2}+t_{1}^{2}-4 t_{2} \\
& (X+Y)\left(4 t_{1}^{2} t_{2}^{3}-\tau\right)=Z\left(\tau t_{1}-4 t_{1}^{3}+4-4 t_{2}^{3}\right)
\end{aligned}
$$

for the ramification of $H \rightarrow E_{1}$.
This is enough to determine the first coordinate (in Weierstrass form) for the image of ramification point of $H \rightarrow E_{1}$ in $E_{1} / \iota$ as $u_{1}=Z /\left(X+Y+t_{1} Z\right)$.

To obtain the exact location of the ramification points of $H \rightarrow E_{1}$ (projected to $\mathbb{P}^{1} \times \mathbb{P}^{1}$ ) we need to identify the second coordinate (in $E_{2} / \iota$ ). This amounts to compute the preimage of $E_{1} \cap E_{2}^{\vee}$ via the map $E_{2} \rightarrow E_{2}^{\vee}$ described earlier, followed
by variable elimination to compute the image through Halphen coordinates. We obtain the following equation in $E_{2}$ :

$$
\left(X_{2}+Y_{2}\right)\left(t_{2}^{3}-t_{1} t_{2}\right)+Z_{2}\left(2 t_{1} t_{2}^{2}-2 t_{2}\right)=0
$$

Exchanging $t_{1}$ and $t_{2}$ gives explicit coordinates for the image of the ramification locus of $H \rightarrow E_{2}$ in $\mathbb{P}^{1} \times \mathbb{P}^{1}$.
4.2. Coordinates of double points. The double points of the rational sextic in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ are the images of the intersection of $E_{1}$ with the twisted duals of $E_{2}$ defined in section 3.4.

For $\gamma \in \Gamma / \pm 1$ the twisted dual $E_{2}^{\gamma}$ is the curve in the dual projective plane whose points are lines $(P, P+\gamma)$ for $P \in E_{2}$. By symmetry, $E_{2}^{\gamma}=E_{2}^{-\gamma}$.

It is especially easy to understand $E_{2}^{\gamma_{0}}$ where the group element $\gamma_{0}$ acts through $[x: y: z] \mapsto\left[x: j y: j^{2} z\right]$. In that case, the line $\left(P, \gamma_{0}(P)\right)$ has coordinates $\left[\left(j^{2}-j\right) y z:\left(1-j^{2}\right) z x:\left(j-j^{2}\right) x y\right]$ so the locus of such lines is the same as the image of $E_{2}$ by the standard quadratic transformation $[y z: z x: x y]$ based on an inflection triangle (3 lines going through 9 flex points). There are four such triangles.

The equations of the twisted duals can be computed by variable elimination or by applying quadratic transformations:

$$
\begin{array}{ll}
E_{2}^{\gamma_{0}}: & (x y)^{3}+(y z)^{3}+(z x)^{3}-3 t\left(x^{2} y^{2} z^{2}\right)=0 \\
E_{2}^{\gamma_{1}}: & x^{6}+y^{6}+z^{6}+(3 j t-1)\left(x^{3} y^{3}+y^{3} z^{3}+z^{3} x^{3}\right) \\
& -3 j(j t+1)\left(x^{4} y z+y 4 z x+z^{4} y x\right)+(3 j x y z)^{2}=0 \\
E_{2}^{\gamma_{2}}: & x^{6}+y^{6}+z^{6}+\left(3 j^{2} t-1\right)\left(x^{3} y^{3}+y^{3} z^{3}+z^{3} x^{3}\right) \\
& -3 j^{2}\left(j^{2} t+1\right)\left(x^{4} y z+y^{4} z x+z 4 y x\right)+\left(3 j^{2} x y z\right)^{2}=0 \\
E_{2}^{\gamma_{3}}: & x^{6}+y^{6}+z^{6}+(3 t-1)\left(x^{3} y^{3}+y^{3} z^{3}+z^{3} x^{3}\right) \\
& -3(t+1)\left(x^{4} y z+y^{4} z x+z^{4} y x\right)+(3 x y z)^{2}=0
\end{array}
$$

where $\gamma_{0}:[x: y: z] \mapsto\left[x: j y: j^{2} z\right], \gamma_{1}:[x: y: z] \mapsto\left[z: j x: j^{2} y\right], \gamma_{2}:[x: y: z] \mapsto$ $\left[z: j^{2} x: j y\right], \gamma_{3}:[x: y: z] \mapsto[z: x: y]$.

The pairs of special points above double points are located on lines:

$$
\begin{aligned}
& L_{0}:(x+y)\left(t_{1}^{2}-t_{2}\right)-z\left(t_{1} t_{2}-1\right)=0 \\
& L_{1}:(x+y)\left(j t_{1} t_{2}-j\right)+z\left(t 1^{2}-j^{2} t_{1} t_{2}-t_{2}+j^{2}\right)=0 \\
& L_{2}:(x+y)\left(j^{2} t_{1} t_{2}-j^{2}\right)+z\left(t_{1}^{2}-j t_{1} t_{2}-t_{2}+j\right)=0 \\
& L_{3}:(x+y)\left(t_{1} t_{2}-1\right)+z\left(t_{1}^{2}-t_{1} t_{2}-t_{2}+1\right)=0
\end{aligned}
$$

This defines the first coordinate of double points in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ as an element of the base field $\mathbb{k}$. Exchanging $t_{1}$ and $t_{2}$ and replacing $j$ by $j^{2}$ provides the second coordinate of these double points.

Note that although these double points are themselves rational, it is not true in general that the tangent lines to their branches (or equivalently, their preimages in the normalized curve) are also rational.
4.3. Determination of the polar transformation. The polynomial coefficients of the polarity relation defining $H$ as a correspondence in $E_{1} \times E_{2}$ were determined by numerical simulations using the following process:
(1) choose a base field with large enough characteristic (e.g. $\mathbb{F}_{65537}$ );
(2) generate random Hesse equation parametres;
(3) for each $\left(t_{1}, t_{2}\right)$ determine orthogonal pairs $P \in E_{1}$ and its polar line $\ell_{P}$ intersecting $E_{2}$ at 3 rational points, and their image via the [3] tripling morphism;
(4) once 4 projectively independent pairs $\left(3 P, \ell_{3 P}\right)$ are obtained, compute the unique transformation matrix $M\left(t_{1}, t_{2}\right)$ realising this polarity relation.
It turns out that the coefficients of $M$ have degree $\leq 4$ in each variable $t_{1}$ and $t_{2}$ so the system can be overdetermined by generating enough relations.

Once candidate polynomials are found, it can be further confirmed by running the same process on a larger field (for example $\mathbb{F}_{2^{32}-5}$ ) and verifying the result formally by checking that the resulting equation $b_{t_{1}, t_{2}}\left(3 P_{1}, 3 P_{2}\right)=0$ lifts to a function on $\mathbb{P}^{2} \times \mathbb{P}^{2}$ belonging to the ideal of $\tilde{H}$ (generated by the equations of $E_{1}, E_{2}$ and the standard bilinear form). The final verification can be done on field $\mathbb{Q}\left(t_{1}, t_{2}\right)$.

The transformation matrix (which is the matrix of bilinear form $b_{t_{1}, t_{2}}$ ) can be computed explicitly:

$$
\begin{aligned}
& M=\left(\begin{array}{lll}
m_{00} & m_{01} & m_{02} \\
m_{01} & m_{00} & m_{02} \\
m_{20} & m_{20} & m_{22}
\end{array}\right) \\
& m_{00}=3 t_{1}^{3} t_{2}^{3}-3 t_{1}^{2} t_{2}^{2}-2 t_{1}^{3}-2 t_{2}^{3}+3 t_{1} t_{2}+1 \\
& m_{01}=t_{1}^{3}+t_{2}^{3}-3 t_{1}^{2} t_{2}^{2}+3 t_{1} t_{2}-2 \\
& m_{02}=t_{1}^{4}-3 t_{1}^{3} t_{2}^{2}+3 t_{1}^{2} t_{2}+t_{1} t_{2}^{3}-2 t_{1} \\
& m_{20}=t_{2}^{4}-3 t_{1}^{2} t_{2}^{3}+3 t_{1} t_{2}^{2}+t_{1}^{3} t_{2}-2 t_{2} \\
& m_{22}=t_{1}^{4} t_{2}+t_{1} t_{2}^{4}+3 t_{1}^{2} t_{2}^{2}-3 t_{1}^{3}-3 t_{2}^{3}-2 t_{1} t_{2}+3 \\
& \operatorname{det} M=\left(t_{1}^{3}-1\right)^{2}\left(t_{2}^{3}-1\right)^{2}\left(t_{1} t_{2}-1\right) \\
& \times\left(t_{1}+t_{2}+1\right)\left(t_{1}+j^{2} t_{2}+j\right)\left(t_{1}+j t_{2}+j^{2}\right) \text { where } j^{3}=1
\end{aligned}
$$

The coefficients were obtained by running numerical computations on a small finite field, interpolating using rational functions of lowest degree, with a final formal verification over $\mathbb{Z}[j]$.

When applying the projective transformations turning $E_{1}$ and $E_{2}$ in Weierstrass form, the bilinear relation is even simpler, because the point at infinity must be dual to the line $\{v=0\}$, giving another equation of $H$.

Theorem 4.1. Let $\left(u_{1}, v_{1}\right)$ and $\left(u_{2}, v_{2}\right)$ be affine coordinates such that:

$$
\begin{aligned}
& E_{1}: 3 v_{1}^{2}=4\left(t_{1}^{3}-1\right) u_{1}^{3}-9 t_{1}^{2} u_{1}^{2}+6 t_{1} u_{1}-1 \\
& E_{2}: 3 v_{2}^{2}=4\left(t_{2}^{3}-1\right) u_{2}^{3}-9 t_{2}^{2} u_{2}^{2}+6 t_{2} u_{2}-1
\end{aligned}
$$

and define $T=\left(t_{1}^{3}-1\right)\left(t_{2}^{3}-1\right)$.
Then the polarity relation defining $H$ can be expressed as the polynomial:

$$
3 T\left(u_{1} u_{2}\left(t_{1} t_{2}+2\right)-t_{1} u_{1}-t_{2} u_{2}+v_{1} v_{2}\right)+T+2\left(t_{1} t_{2}-1\right)^{3}=0
$$

in particular $v_{1} v_{2}$ is a regular function of $u_{1}, u_{2}, t_{1}$ and $t_{2}$.
Proof. The coordinates $\left(u_{i}, v_{i}\right)$ can be deduced from projective coordinates $\left[z_{i}\right.$ : $\left.x_{i}-y_{i}: x_{i}+y_{i}+t_{i} z_{i}\right]$ so the bilinear relation in these new coordinates is given by matrix:
$\frac{1}{4}\left(\begin{array}{ccc}-t_{2} & -t_{2} & 2 \\ 1 & -1 & 0 \\ 1 & 1 & 0\end{array}\right) \cdot M \cdot\left(\begin{array}{ccc}-t_{1} & 1 & 1 \\ -t_{1} & -1 & 1 \\ 2 & 0 & 0\end{array}\right)=\frac{1}{2}\left(\begin{array}{ccc}3\left(t_{1} t_{2}+2\right) T & 0 & -3 t_{2} T \\ 0 & 3 T & 0 \\ -3 t_{1} T & 0 & T+2\left(t_{1} t_{2}-1\right)^{3}\end{array}\right)$
4.4. Equation of the rational sextic. The image $H_{\iota}$ of $H$ in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ can be determined by variable elimination, but the previous properties provide enough constraints to determine entirely its equation.
Lemma 4.2. Let $\left[u_{1}: u_{1}^{\prime}\right],\left[u_{2}: u_{2}^{\prime}\right]$ be projective coordinates so that $u_{1} / u_{1}^{\prime}=$ $z_{1} /\left(x_{1}+y_{1}+t_{1} z_{1}\right)$ and $u_{2} / u_{2}^{\prime}=z_{2} /\left(x_{2}+y_{2}+t_{2} z_{2}\right)$ are affine coordinates for $E_{1} / \iota$ and $E_{2} / \iota$.

Then the specialisation of $H_{\iota}$ to $u_{1}^{\prime}=0$ is the cubic polynomial for the normalised $y^{2}=P_{2}(x)$ equation of $E_{2}$, and the specialisation of $H_{\iota}$ to $u_{2}^{\prime}=0$ is the cubic polynomial for the normalised equation of $E_{1}\left(y^{2}=P_{1}(x)\right)$.
Proof. This follows directly from the fact that $H$ contains the pairs $\left(O_{1}, W_{2, i}\right)$ and $\left(W_{1, i}, O_{2}\right)$ for $i=1,2,3$.

The conventions chosen earlier imply that the basis of the 3-torsion is sent to coordinates $1 /(t-1)$ and 0 respectively (the other 3 -torsion points will have coordinates $j /(j t-1)$ and $\left.j^{2} /\left(j^{2} t-1\right)\right)$ which defines uniquely the normalised equation of $E_{i}$.

In addition to that, the first coordinate of double points has been computed earlier, so a linear relation $(x+y) \lambda+z \mu=0$ gives $u_{1}=\lambda /\left(t_{1} \lambda-\mu\right)$ :

$$
\begin{aligned}
& u_{1}\left(D_{0}\right)=\frac{t_{1}^{2}-t_{2}}{t_{1}^{3}-1} \\
& u_{1}\left(D_{1}\right)=\frac{j t_{1} t_{2}-j}{j t_{1}\left(t_{1} t_{2}-1\right)-\left(t_{1}^{2}-j^{2} t_{1} t_{2}-t_{2}+j^{2}\right)} \\
& u_{1}\left(D_{2}\right)=\frac{j^{2}\left(t_{1} t_{2}-1\right)}{j^{2} t_{1}\left(t_{1} t_{2}-1\right)-\left(t_{1}^{2}-j t_{1} t_{2}-t_{2}+j\right)} \\
& u_{1}\left(D_{3}\right)=\frac{t_{1} t_{2}-1}{t_{1}\left(t_{1} t_{2}-1\right)-\left(t_{1}^{2}-t_{1} t_{2}-t_{2}+1\right)}
\end{aligned}
$$

The coordinate $u_{2}$ is obtained by exchanging $t_{1}$ and $t_{2}$ in formulas.
These rational functions can be rewritten to show that they are fully regular on the whole parameter space $t_{1}, t_{2} \in \mathbb{A}^{1} \backslash \mu_{3}$ :

$$
\begin{aligned}
& u_{1}\left(D_{0}\right)=\frac{t_{1}^{2}-t_{2}}{t_{1}^{3}-1} \\
& u_{1}\left(D_{1}\right)=\frac{t_{1} t_{2}-1}{\left(t_{1}-j^{2}\right)\left(t_{1}-1\right)\left(t_{2}-j^{2}\right)} \\
& u_{1}\left(D_{2}\right)=\frac{t_{1} t_{2}-1}{\left(t_{1}-1\right)\left(t_{1}-j\right)\left(t_{2}-j\right)} \\
& u_{1}\left(D_{3}\right)=\frac{t_{1} t_{2}-1}{\left(t_{1}-j\right)\left(t_{1}-j^{2}\right)\left(t_{2}-1\right)}
\end{aligned}
$$

Theorem 4.3. The equation of $H_{\iota}$ can be normalised as

$$
\begin{aligned}
u_{1}^{3} u_{2}^{3} & +u_{2}^{3}\left(A_{1} u_{1}^{2} u_{1}^{\prime}+B_{1} u_{1} u_{1}^{\prime 2}+C_{1} u_{1}^{\prime 3}\right) \\
& +u_{1}^{3}\left(A_{2} u_{2}^{2} u_{2}^{\prime}+B_{2} u_{2} u_{2}^{\prime 2}+C_{2} u_{2}^{\prime 3}\right) \\
& +u_{1}^{\prime} u_{2}^{\prime} F\left(u_{1}, u_{1}^{\prime}, u_{2}, u_{2}^{\prime}\right)
\end{aligned}
$$

where $F$ is a homogeneous polynomial of degree (2, 2) and $P_{i}=c_{i}\left(X^{3}+A_{i} X^{2}+\right.$ $\left.B_{i} X+C_{i}\right)$. The nine coefficients of $F$ are entirely determined by the constraint of having double points $\left(D_{i}\right)_{i=0,1,2,3}$, or a triple point $D_{0}$ and a double point $D_{1}$.

Each double point defines 3 constraints by the vanishing of the equation polynomial and its first order derivatives. A triple point defines 6 constraints, with the additional vanishing of second order derivatives.
4.5. Rational parameters for the rational sextic. The quotient of $H$ by the hyperelliptic involution $\left(H_{\iota}\right)$ defines a correspondence between the $u$ coordinates of $E_{1}$ and $E_{2}$, represented by Weierstrass equations by the choice of the origin point.

As described earlier, its singularities can be resolved by a sequence of linear transformations and quadratic birational transformations to a plane conic, which is parameterised by rational functions by projection from any rational point. This is where the ramification locus of $H \rightarrow E_{i}$ can be used.

Proposition 4.4. The ramification locus of morphism $H \rightarrow E_{1}$ (resp. $H \rightarrow E_{2}$ ) defines a rational point of $H_{\iota}$. Its coordinates in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ are:

$$
\begin{aligned}
& u_{1}=\frac{4 t_{1}^{2} t_{2}^{3}-t_{1}^{2}-t_{2}^{4}-6 t_{1} t_{2}^{2}+4 t_{2}}{4\left(t_{1}^{3}-1\right)\left(t_{2}^{3}-1\right)} \\
& u_{2}=\frac{t_{2}^{2}-t_{1}}{t_{2}^{3}-3 t_{1} t_{2}+2}
\end{aligned}
$$

Proof. Following the computation done in section 4.1, the pair of conjugate ramification points of the map $H \rightarrow E_{1}$ satisfies a linear relation between $x+y$ and $z$, allowing to compute the coordinate in Weierstrass form $u_{1}\left(R_{1}\right)=z /\left(x+y+t_{1} z\right)$.

$$
\begin{aligned}
& \tau=t_{2}^{4}+6 t_{1} t_{2}^{2}+t_{1}^{2}-4 t_{2} \\
& (X+Y)\left(4 t_{1}^{2} t_{2}^{3}-\tau\right)=Z\left(\tau t_{1}-4 t_{1}^{3}+4-4 t_{2}^{3}\right) \\
& \left(X+Y+t_{1} Z\right)\left(4 t_{1}^{2} t_{2}^{3}-\tau\right)=Z\left(4 t_{1}^{3} t_{2}^{3}-4 t_{1}^{3}+4-4 t_{2}^{3}\right)
\end{aligned}
$$

Since $H_{\iota}$ is defined by a degree (3,3) equation $S\left(u_{1}, u_{2}\right)$ in $\mathbb{P}^{1}$ the fact that $S\left(u_{1}\left(R_{1}\right), u_{2}\right)$ is a degree 3 polynomial in variable $u_{2}$ with a multiple root $u_{2}\left(R_{1}\right)$ implies that this root is rational because $S\left(u_{1}\left(R_{1}\right), u_{2}\right)$ must be divisible by the square of the minimal polynomial of $u_{2}\left(R_{1}\right)$.

We actually know explicitly the second coordinate using formulas from 4.1;

$$
\begin{aligned}
& \left(X_{2}+Y_{2}\right)\left(t_{2}^{3}-t_{1} t_{2}\right)+Z_{2}\left(2 t_{1} t_{2}^{2}-2 t_{2}\right)=0 \\
& \left(X_{2}+Y_{2}+t_{2} Z_{2}\right)\left(t_{2}^{3}-t_{1} t_{2}\right)=Z_{2}\left(2 t_{2}-2 t_{1} t_{2}^{2}+t_{2}^{4}-t_{1} t_{2}^{2}\right)
\end{aligned}
$$

Note that the case $u_{2}=\infty$ is possible, corresponding to the special case where $H \rightarrow E_{1}$ has a triple ramification point. It was shown already in lemma 2.4 that this happens when $t_{2}^{3}-t_{1} t_{2}+2=0$.

In the triple point case, the first quadratic transformation can resolve the triple point and leave only one node: the result is then a nodal plane cubic, which readily admits a rational parameterisation.

In the singular case, the sextic equation defines a reducible curve which is a union of conics and this calculation will return rational functions of degree 1 and 2.
4.6. Hyperelliptic equation of $H$. The previous calculations allow to fully determine equations for the morphisms $H / \iota \rightarrow E_{i} / \iota$ between rational curves (the $x$ coordinates) but the lift to a double cover is possibly only defined up to a quadratic twist. This apparent indeterminacy will be resolved by the existence of a square root of $P_{1}\left(u_{1}\right) P_{2}\left(u_{2}\right)$ in the coordinate ring of $H \rightarrow E_{1} \times E_{2}$, where $E_{i}$ has equation $v_{i}^{2}=P_{i}\left(u_{i}\right)$.
Lemma 4.5. There exists a point $\left(u_{1}, u_{2}\right)$ on rational curve $\bar{H}_{\iota} \subset \mathbb{P}^{1} \times \mathbb{P}^{1}$ such that $P_{1}\left(u_{1}\right) P_{2}\left(u_{2}\right) \neq 0$.

Proof. The rationality of ramification points obtained in the previous section shows that there is a birational morphism $\mathbb{P}_{\mathfrak{k}}^{1} \rightarrow \bar{H}_{\iota}$ and since the curve is defined by a degree $(3,3)$ equation in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ there are at most 18 rational points such that $P_{1}\left(u_{1}\right) P_{2}\left(u_{2}\right)=0$. The lemma is thus true for any field containing more than 18 elements.

Since we assumed that $\mathbb{k}$ has characteristic more than 3 and contains a cubic root of unity, the remaining cases are $\mathbb{F}_{7}$ and $\mathbb{F}_{13}$. In that case it is impossible for either $P_{i}$ to have 3 rational roots, as it would mean that $E_{i}$ has both rational 2 -torsion and 3 -torsion thus at least 36 rational points exceeding the Hasse-Weil bound. So there are at most 6 rational points such that $P_{1}\left(u_{1}\right) P_{2}\left(u_{2}\right)=0$, proving the lemma.

Assuming the same conventions as before, we have determined explicit rational functions of degree 3 :

$$
T \mapsto\left(\frac{\mathrm{NX}_{1}(T)}{\mathrm{DX}_{1}(T)}, \frac{\mathrm{NX}_{2}(T)}{\mathrm{DX}_{2}(T)}\right) \in H_{\iota} \subset \mathbb{P}^{1} \times \mathbb{P}^{1}
$$

realising a birational map from $\mathbb{P}^{1}$ to $H_{\iota}$. Using the previous lemma, using an appropriate change of rational parameter we can assume that $T=\infty$ defines a point $\left(u_{1, \infty}, u_{2, \infty}\right)$ such that $P_{1}\left(u_{1, \infty}\right) P_{2}\left(u_{2, \infty}\right) \neq 0$.

Since the Weierstrass points of $E_{1}$ and $E_{2}$ lie on the two lines at infinity, $\mathrm{NX}_{2} / \mathrm{DX}_{2}$ maps the roots of $\mathrm{DX}_{1}$ to the coordinates of the Weierstrass points of $E_{2}$, and conversely. These 6 points of $H_{\iota}$ are known to be the Weierstrass points of $H$ Kuh88. Additionally, neither $u_{1, \infty}$ nor $u_{2, \infty}$ are at infinity. This implies that $\mathrm{DX}_{1}$ and $\mathrm{DX}_{2}$ have degree 3 and we can arrange for them to be monic polynomials.

Following equations given in Kuh88, BHLS15, we are looking for an equation $y_{H}^{2}=\alpha \mathrm{DX}_{1}\left(x_{H}\right) \mathrm{DX}_{2}\left(x_{H}\right)$ for some scalar constant $\alpha$ where $x_{H}$ is identified with the rational parameter $T$.

Lemma 4.6. The polynomial $P_{1}\left(\mathrm{NX}_{1} / \mathrm{DX}_{1}\right) \mathrm{DX}_{1}^{3}$ is a multiple of $\mathrm{DX}_{2}$ and the quotient by $\mathrm{DX}_{2}$ admits a square root as a polynomial $R_{1}$ up to a multiplicative constant.

Proof. Through the rational parametrisation $\mathbb{P}^{1} \rightarrow H_{\iota}$ we can geometrically interpret the corresponding divisors.

The polynomial $\mathrm{DX}_{2}$ defines a divisor which is the intersection with line at infinity $\mathbb{P}^{1} \times\{\infty\}$, corresponding to Weierstrass points of $E_{1}$.

The zeros of $P_{1}\left(\mathrm{NX}_{1} / \mathrm{DX}_{1}\right)$ correspond to the $T$-coordinates of Weierstrass points of $E_{1}$, so $P_{1}\left(\mathrm{NX}_{1} / \mathrm{DX}_{1}\right) \mathrm{DX}_{1}^{3}$ is a degree 9 effective divisor on $\mathbb{P}^{1}$ containing $\operatorname{div} \mathrm{DX}_{2}$.

The complement consists of 3 pairs of points which are the other preimages of the Weierstrass points of $E_{1}$ in $H_{\iota}$, and since they are exchanged by the action of $\iota$, they map to a point of multiplicity $2\left(H_{\iota}\right.$ is tangent to the line $\left.\left\{x=x\left(W_{1, i}\right)\right\}\right)$, implying that this divisor has a square root.

Note that since

$$
\left(x^{3}+a x^{2}+b x+c\right)^{2}=x^{6}+2 a x^{5}+\left(2 b+a^{2}\right) x^{4}+(2 c+2 a b) x^{3}+\ldots
$$

the square root of a monic degree 6 polynomial can be computed using only elementary field operations.

Denote by $\alpha_{i}$ the nonzero field elements $P_{i}\left(u_{i, \infty}\right)$. Then there exists a unique monic polynomial $R_{1}$ such that $P_{1}\left(\mathrm{NX}_{1} / \mathrm{DX}_{1}\right) \mathrm{DX}_{1}^{3}=\alpha_{1} \mathrm{DX}_{2} R_{1}^{2}$.

This allows to define a map:

$$
\left(x_{H}, y_{H}\right) \mapsto\left(\frac{\mathrm{NX}_{1}\left(x_{H}\right)}{\mathrm{DX}_{1}\left(x_{H}\right)}, y_{H} \kappa_{1} \frac{R_{1}\left(x_{H}\right)}{\mathrm{DX}_{1}\left(x_{H}\right)^{2}}\right)
$$

satisfying the relation:

$$
\left(y_{H} \kappa_{1} \frac{R_{1}\left(x_{H}\right)}{\mathrm{DX}_{1}\left(x_{H}\right)^{2}}\right)^{2}=\alpha \mathrm{DX}_{1}\left(x_{H}\right) \mathrm{DX}_{2}\left(x_{H}\right) \frac{\kappa_{1}^{2} R_{1}\left(x_{H}\right)^{2}}{\mathrm{DX}_{1}\left(x_{H}\right)^{4}}=\left(\alpha \kappa_{1}^{2} / \alpha_{1}\right) P_{1}\left(\frac{\mathrm{NX}_{1}\left(x_{H}\right)}{\mathrm{DX}_{1}\left(x_{H}\right)}\right)
$$

meaning that this is a well-defined map $H \rightarrow E_{1}$ when $\alpha \kappa_{1}^{2}=\alpha_{1}$.
To define the second projection, another constant $\kappa_{2}$ is needed, and must satisfy the equation $\alpha \kappa_{2}^{2}=\alpha_{2}$. A solution to these constraints can be given by $\alpha=\alpha_{1}$, $\kappa_{1}=1$ and $\kappa_{2}=\sqrt{\alpha_{1} \alpha_{2}} / \alpha_{1}$ for some choice of a square root of $\alpha_{1} \alpha_{2}$.

This square root can be determined using the final equation of 4.3, showing that for any point $\left(e_{1}, e_{2}\right) \in \bar{H} \subset E_{1} \times E_{2}$ with coordinates $\left(u_{1}, v_{1}\right),\left(u_{2}, v_{2}\right)$ in Weierstrass form, the following identity holds:

$$
v_{1} v_{2}=t_{1} u_{1}+t_{2} u_{2}-u_{1} u_{2}\left(t_{1} t_{2}+2\right)-\frac{1}{3}-\frac{2\left(t_{1} t_{2}-1\right)^{3}}{3\left(t_{1}^{3}-1\right)\left(t_{2}^{3}-1\right)}
$$

Moreover, $v_{1}^{2} v_{2}^{2}=P_{1}\left(u_{1}\right) P_{2}\left(u_{2}\right)$, so using any point above $\left(u_{1, \infty}, u_{2, \infty}\right) \in \mathbb{P}^{1} \times \mathbb{P}^{1}$, the above polynomial function of $u_{1, \infty}$ and $u_{2, \infty}$ is a well-defined square root of $\alpha_{1} \alpha_{2}$.

As a consequence, we can define the following final equations:

$$
\begin{aligned}
& H: y^{2}=\alpha_{1} \mathrm{DX}_{1}(x) \mathrm{DX}_{2}(x) \\
& H \rightarrow E_{1}:(x, y) \mapsto\left(\frac{\mathrm{NX}_{1}(x)}{\mathrm{DX}_{1}(x)}, y \frac{R_{1}(x)}{\mathrm{DX}_{1}(x)^{2}}\right) \\
& H \rightarrow E_{2}:(x, y) \mapsto\left(\frac{\mathrm{NX}_{2}(x)}{\mathrm{DX}_{2}(x)}, \frac{\alpha_{2}}{\sqrt{\alpha_{1} \alpha_{2}}} y \frac{R_{2}(x)}{\mathrm{DX}_{2}(x)^{2}}\right)
\end{aligned}
$$

4.7. An algorithm to compute the triple cover from elliptic curves with level structure. In the above calculations, we can observe that if the input elliptic curves are given in Weierstrass form, the formulas depend on the Hesse pencil parameters $t_{1}$ and $t_{2}$ but the actual triple cover can be given in hyperelliptic form using solely the parameterisation of the sextic in $\mathbb{P}^{1} \times \mathbb{P}^{1}$. The sextic is entirely determined by the location of the double points and computations can be done without referring to the Hessian equations.

The algorithm can be summarised with the following steps:
(1) Compute Hesse pencil parameters from input data.
(2) Compute singularities of $H_{\iota} \subset \mathbb{P}^{1} \times \mathbb{P}^{1}$ using explicit formulas.
(3) Compute the sextic model of $H_{\iota}$ from an overdetermined linear system.
(4) Compute a resolution of singularities as a chain of 2 quadratic transformations and deduce a rational parameterisation.
(5) Deduce full projection maps from the $x$-coordinate projections.

The algorithm only involves basic field operations (addition, subtraction, multiplication, division). All operations are well defined on fields $\mathbb{F}_{q}\left(j, t_{1}, t_{2}\right)$ or $\mathbb{Q}\left(j, t_{1}, t_{2}\right)$. Since no square root or polynomial root is involved, this method is expected to have lower asymptotic complexity than the one described in BHLS15.

The operations are described as pseudocode here but a complete SageMath implementation is given as appendix.

Step 1. Compute Hesse parameter and associated Weierstrass form. We mentioned earlier that in normalised Weierstrass form, the basis of 3-torsion must be sent to $u\left(T_{1}\right)=-1 /(1-t)$ and $u\left(T_{2}\right)=0$. Using the same conventions, $T_{1}+T_{2}$ has coordinates $[0: 1:-j]$ in Hesse form and abscissa $u\left(T_{1}+T_{2}\right)=-j /(1-j t)$ in projection from the origin.

In particular the quantity:

$$
\frac{x\left(T_{1}+T_{2}\right)-x\left(T_{2}\right)}{x\left(T_{1}+T_{2}\right)-x\left(T_{1}\right)}=\frac{1-t}{j+2}
$$

is invariant by affine transformations.
Compute the affine transformation mapping $1 /(1-t)$ and 1 to $u\left(T_{1}\right)$ and $u\left(T_{2}\right)$, and returns the transformed equation $y^{2}=P^{\prime}(x)$.

Normalize $y$ to obtain the Weierstrass form of Hessian curve $y^{2}=p_{3} x^{3}+p_{2} x^{2}+$ $p_{1} x+p_{0}$ where $p_{1}+p_{2}=1$. This is done by ensuring that $y\left(T_{1}\right)=-1 /(1-t)$.
function CurveParams(E: $\left.y^{2}=P(x), T_{1} \in E[3], T_{2} \in E[3], j \in \mu_{3}\right)$
Assert WeilPairing $\left(T_{1}, T_{2}\right)=\mathrm{j}$
$x_{1}, x_{2}, x_{12} \leftarrow x\left(T_{1}\right), x\left(T_{2}\right), x\left(T_{1}+T_{2}\right)$
$t \leftarrow-(j+2)\left(x_{12}-x_{2}\right) /\left(x_{12}-x_{1}\right)$
$a \leftarrow\left(x_{2}-x_{1}\right)(1 / t-1)$
$b \leftarrow x_{2}-a$
$c \leftarrow(t-1) y\left(T_{1}\right)$
$P^{\prime} \leftarrow P(a x+b) / c^{2}$
Assert $3 t^{3} P^{\prime}=4\left(1-t^{3}\right) x^{3}+3\left(t^{3}-4\right) x^{2}+12 x-4$
return $t,(x, y) \mapsto(a x+b, c y), P^{\prime}$
end function
Step 2. Compute singularities coordinates. The singularities of the image of $H$ in $\mathbb{P}^{1} \times \mathbb{P}^{1}$ are entirely known by explicit formulas given above. They are 8 rational functions of total degree 3 in $t_{1}$ and $t_{2}$.

If there is a triple point, 2 of these double points will be equal.
function DoubleCoords $\left(j \in \mu_{3}, t_{1}, t_{2}\right)$
$u_{0} \leftarrow\left(t_{1}^{2}-t_{2}\right) /\left(t_{1}^{3}-1\right)$
$u_{1} \leftarrow\left(t_{1} t_{2}-1\right) /\left(t_{1}-1\right)\left(t_{1}-j^{2}\right)\left(t_{2}-j^{2}\right)$
$u_{2} \leftarrow\left(t_{1} t_{2}-1\right) /\left(t_{1}-j\right)\left(t_{1}-1\right)\left(t_{2}-j\right)$
$u_{3} \leftarrow\left(t_{1} t_{2}-1\right) /\left(t_{1}-j^{2}\right)\left(t_{1}-j\right)\left(t_{2}-1\right)$
return $u_{0}, u_{1}, u_{2}, u_{3}$
end function
function DoublePoints $\left(j \in \mu_{3}, t_{1}, t_{2}\right)$
$u_{0}, u_{1}, u_{2}, u_{3} \leftarrow \operatorname{DoubleCoords}\left(j, t_{1}, t_{2}\right)$
$v_{0}, v_{1}, v_{2}, v_{3} \leftarrow \operatorname{DoubleCoords}\left(j^{2}, t_{2}, t_{1}\right)$
if any $\left(u_{i}, v_{i}\right)=\left(u_{j}, v_{j}\right)$ for $i \neq j$ then
return triple point, double point
else
return $\left(u_{i}, v_{i}\right)$ for $i=0,1,2,3$
end if
end function
Step 3. Compute a sextic equation for $H_{\iota}$. The normalised Weierstrass polynomials and the coordinates of the 4 double points provide $3 \times 4+6=18$ constraints on the 16 coefficients of polynomials of degree $(3,3)$.

If there is a triple point, the 3 second order derivatives give a total of $6+3 \times 2+3=$ 15 constraints only.

This is an overdetermined linear system: a matrix kernel computation provides the equation in the general case. In the case of a triple point, the matrix is square.

```
function RationalSextic \(\left(P_{1}, P_{2}\right.\), Nodes \(=N_{0}, \ldots, N_{3}\) or \(N_{0}\) (triple), \(N_{1}\) )
    \(a_{3} x^{3}+a_{2} x^{2}+a_{1} x+a_{0} \leftarrow P_{1}(x)\)
    \(b_{3} x^{3}+b_{2} x^{2}+b_{1} x+b_{0} \leftarrow P_{2}(x)\)
    \(B(u, v) \leftarrow a_{3} b_{3} u^{3} v^{3}+b_{3} v^{3}\left(a_{2} u^{2}+a_{1} u+a_{0}\right)+a_{3} u^{3}\left(b_{2} v^{2}+b_{1} v+b_{0}\right)\)
```

```
    \(M \leftarrow \operatorname{Matrix}(9,12)\)
    \(V \leftarrow \operatorname{VEctor}(12)\)
    for \(k \leftarrow 0 \ldots\) len(Nodes) -1 do
        for \((i, j) \leftarrow(0,0) \ldots(2,2)\) do
            \(m(u, v) \leftarrow u^{i} v^{j}\)
            \(M[3 i+j][3 k] \leftarrow m\left(N_{k}\right)\)
            \(M[3 i+j][3 k+1] \leftarrow \partial m / \partial u\left(N_{k}\right)\)
            \(M[3 i+j][3 k+2] \leftarrow \partial m / \partial v\left(N_{k}\right)\)
    end for
    \(V[3 k] \leftarrow-B\left(N_{k}\right)\)
    \(V[3 k+1] \leftarrow-\partial B / \partial u\left(N_{k}\right)\)
    \(V[3 k+2] \leftarrow-\partial B / \partial v\left(N_{k}\right)\)
    end for
    if \(N_{0}\) is a triple point then
        \(M[6][3 k] \leftarrow \partial m / \partial u^{2}\left(N_{0}\right)\)
        \(M[7][3 k+1] \leftarrow \partial m / \partial v^{2}\left(N_{0}\right)\)
        \(M[8][3 k+2] \leftarrow \partial m / \partial u \partial v\left(N_{0}\right)\)
        \(V[6] \leftarrow-\partial B / \partial u^{2}\left(N_{k}\right)\)
        \(V[7] \leftarrow-\partial B / \partial v^{2}\left(N_{0}\right)\)
        \(V[8] \leftarrow-\partial B / \partial u \partial v\left(N_{0}\right)\)
    end if
    \(Q \leftarrow \operatorname{Solve}(\mathrm{MQ}=\mathrm{V})\)
    return \(B+\sum Q[3 i+j] u^{i} v^{j}\)
end function
```

Step 4. Compute a rational parameterisation. The first quadratic transformation uses the base triangle formed by the $x$ and $y$ axes through one of the singular points (and the line at infinity), if the source is assumed to be compactified as $\mathbb{P}^{2}$. If the source is viewed as $\mathbb{P}^{1} \times \mathbb{P}^{1}$ the operation consists in blowing up the singular point and contracting the $x$ and $y$ lines through that point.

The second quadratic transformation has base triangle the remaining 3 singular points.

The image of the curves through these transformations is a conic which is easily rationally parameterised. This gives the two degree 3 rational functions $N_{1} / D_{1}$ and $N_{2} / D_{2}$ defining the projections from $H_{\iota}$ to $E_{i, \iota}$.

Note that the standard quadratic transformation $(x, y, z) \mapsto(x y, y z, z x)$ does not involve any operation on coefficients and can be computed only on each monomial.

A rational point on the final conic is given by the ramification point computed explicitly earlier. The ramification point may coincide with a double point of the sextic, but since its tangent direction is known, it defines non ambiguously a rational point on the conic. As shown earlier, the resulting parameterisation may be unsuitable if the point at parameter $T=\infty$ satisfies $P_{1}\left(u_{1}\right) P_{2}\left(u_{2}\right)=0$. It is possible to avoid such a situation using at most 19 evaluations of the rational functions and polynomials $P_{i}$.

If there is a triple point, after the first quadratic transformation the curve will already be a rational nodal cubic instead of a 3 -nodal quartic, and it can be readily parameterised using the double point node as the origin.

The successive transformations are:

- $S$ : the original sextic;
- $S_{1}$ : a translation of $S$ so that $N_{0}$ is the affine plane origin;
- $Q$ : the image by a standard quadratic transformation;
- $Q_{T}$ : a projective transformation of $Q$ moving $N_{1}, N_{2}, N_{3}$ to [1:0:0], [0 : $1: 0],[0: 0: 1] ;$
- C: a smoooth conic obtained from $Q_{T}$ by the standard quadratic transformation;
- $C_{T}$ : a translated conic so that a chosen rational point is the origin.
function RamificationPoint $\left(t_{1}, t_{2} \in \mathbb{k}\right)$
$u_{n} \leftarrow 4 t_{1}^{2} t_{2}^{3}-t_{1}^{2}-t_{2}^{4}-6 t_{1} t_{2}^{2}+4 t_{2}$
$u_{d} \leftarrow 4\left(t_{1}^{3}-1\right)\left(t_{2}^{3}-1\right)$
$v \leftarrow\left(t_{2}^{2}-t_{1}\right) /\left(t_{2}^{3}-3 t_{1} t_{2}+2\right)$
return $u_{n} / u_{d}, v$
end function
function RationalParams(Sextic, Nodes $=N_{0}, N_{1}, N_{2}, N_{3}$ or $N_{0}($ triple $\left.), N_{1}\right)$ $S(x, y, z) \leftarrow$ Homogenize(Sextic)
$x_{0}, y_{0} \leftarrow N_{0}$
$S_{1}(x, y, z) \leftarrow S\left(x_{0} z+x, y_{0} z+y, z\right) \quad$ Translate $N_{0}$ to point $(0,0)$
$Q(x, y, z) \leftarrow S_{1}(y z, z x, x y) \quad \triangleright$ Apply quadratic transform
$Q \leftarrow Q / x^{3} y^{3} z^{2} \quad \triangleright$ Remove exceptional lines
if $N_{0}$ is a triple point then
$Q \leftarrow Q / z \quad \triangleright Q$ is a cubic with node $N_{1}$
$a x^{2}+b x y+c y^{2}+k x^{3}+l x^{2} y+m x y^{2}+n y^{3} \leftarrow C\left(x_{P_{C}}+x, y_{P_{C}}+y, 1\right)$
$x_{Q}(T) \leftarrow-\left(a+b T+c T^{2}\right) /\left(k+l T+m T^{2}+n T^{3}\right)$
$y_{Q}(T) \leftarrow T x_{Q}(T)$
$\left(x_{Q}(T), y_{Q}(T)\right) \leftarrow\left(x_{P_{Q}}+x_{Q}(T), y_{P_{Q}}+y_{Q}(T)\right)$
$x_{Q}(T), y_{Q}(T), z_{Q}(T) \leftarrow$ Homogenize $\left(x_{Q}(T), y_{Q}(T)\right)$
else
$M \leftarrow \operatorname{MatRIX}\left((x, y, z) \mapsto x N_{1}+y N_{2}+z N_{3}\right)$
$Q_{T}(x, y, z) \leftarrow Q(M(x, y, z)) \quad$ Move $N_{i}$ to basis vectors
$C(x, y, z) \leftarrow Q_{T}(y z, z x, x y) / x^{2} y^{2} z^{2} \quad \triangleright C$ is a conic
$P_{C} \leftarrow(S \rightarrow C)$ (RamificationPoint $\left.\left(t_{1}, t_{2}\right)\right)$
$a x^{2}+b x y+c y^{2}+d x+e y \leftarrow C\left(x_{P_{C}}+x, y_{P_{C}}+y, 1\right)=0$
$x_{C}(T) \leftarrow-(d+e T) /\left(a+b T+c T^{2}\right)$
$y_{C}(T) \leftarrow T x_{C}(T)$
$\left(x_{C}(T), y_{C}(T)\right) \leftarrow\left(x_{P_{C}}+x_{C}(T), y_{P_{C}}+y_{C}(T)\right) \triangleright$ Then clear denominator
$x_{C}(T), y_{C}(T), z_{C}(T) \leftarrow$ Homogenize $\left(x_{C}(T), y_{C}(T)\right)$
$\left(x_{Q_{T}}, y_{Q_{T}}, z_{Q_{T}}\right) \leftarrow\left(y_{C} z_{C}, z_{C} x_{C}, x_{C} y_{C}\right)$
$\left(x_{Q}, y_{Q}, z_{Q}\right) \leftarrow M^{-1}\left(x_{Q_{T}}, y_{Q_{T}}, z_{Q_{T}}\right)$
end if
$\left(x_{S_{1}}, y_{S_{1}}, z_{S_{1}}\right) \leftarrow\left(y_{Q} z_{Q}, z_{Q} x_{Q}, x_{Q} y_{Q}\right)$
$U_{1} \leftarrow x_{0}+x_{S_{1}} / z_{S_{1}}$
$U_{2} \leftarrow y_{0}+y_{S_{1}} / z_{S_{1}}$
if $P_{1}\left(U_{1}(T=\infty)\right) P_{2}\left(U_{2}(T=\infty)\right)=0$ then
Find $a \in 1 \ldots 20$ such that $P_{1}\left(U_{1}(a)\right) P_{2}\left(U_{2}(a)\right) \neq 0$
Substitute $T$ with $a+1 / T$
end if
return $U_{1}, U_{2}$
end function

Step 5. Compute final morphisms. Using the rational functions above, and following computations done in the previous section, we can define the main function of the algorithm.

```
function TripleCover ((E 
    j}\leftarrow\operatorname{WeilPairing}(T\mp@subsup{T}{11}{},\mp@subsup{T}{12}{}
    t},\mp@subsup{f}{1}{},\mp@subsup{P}{1}{}\leftarrow\operatorname{CurveParams}(\mp@subsup{E}{1}{},\mp@subsup{T}{11}{},\mp@subsup{T}{12}{},j
    t},\mp@subsup{f}{2}{},\mp@subsup{P}{2}{}\leftarrow\mathrm{ CurveParams ( }\mp@subsup{E}{2}{},\mp@subsup{T}{21}{},\mp@subsup{T}{22}{},j
```

```
    Nodes \(\leftarrow \operatorname{DoublePoints}\left(j, t_{1}, t_{2}\right)\)
    \(S \leftarrow\) RationalSextic \(\left(P_{1}, P_{2}\right.\), Nodes \()\)
    \(\mathrm{NX}_{1} / \mathrm{DX}_{1}, \mathrm{NX}_{2} / \mathrm{DX}_{2} \leftarrow\) RationalParams( S , Nodes)
    \(u_{1} \leftarrow \mathrm{NX}_{1}(\infty) / \mathrm{DX}_{1}(\infty)\)
    \(u_{2} \leftarrow \mathrm{NX}_{2}(\infty) / \mathrm{DX}_{2}(\infty)\)
    \(a_{1}, a_{2} \leftarrow P_{1}\left(u_{1}\right), P_{2}\left(u_{2}\right)\)
    \(R_{1} \leftarrow \sqrt{P_{1}\left(\mathrm{NX}_{1} / \mathrm{DX}_{1}\right) \mathrm{DX}_{1}^{3} /\left(a_{1} \mathrm{DX}_{2}\right)} \triangleright\) Square root of a monic polynomial
    \(R_{2} \leftarrow \sqrt{P_{2}\left(\mathrm{NX}_{2} / \mathrm{DX}_{2}\right) \mathrm{DX}_{2}^{3} /\left(a_{2} \mathrm{DX}_{1}\right)} \triangleright\) Square root of a monic polynomial
    \(a \leftarrow t_{1} u_{1}+t_{2} u_{2}-u_{1} u_{2}\left(t_{1} t_{2}+2\right)-1 / 3-2\left(t_{1} t_{2}-1\right)^{3} /\left(t_{1}^{3}-1\right)\left(t_{2}^{3}-1\right)\)
    \(H \leftarrow a_{1} \mathrm{DX}_{1} \mathrm{DX}_{2}\)
    \(p_{1} \leftarrow \operatorname{map}(x, y) \mapsto\left(f_{1}\left(\mathrm{NX}_{1}(x) / \mathrm{DX}_{1}(x)\right), y R_{1}(x) / \mathrm{DX}_{1}(x)^{2}\right)\)
    \(p_{2} \leftarrow \operatorname{map}(x, y) \mapsto\left(f_{2}\left(\mathrm{NX}_{2}(x) / \mathrm{DX}_{2}(x)\right),\left(a_{2} / a\right) y R_{2}(x) / \mathrm{DX}_{2}(x)^{2}\right)\)
    return \(\mathrm{H}, p_{1}, p_{2}\)
end function
```


## Appendix: Sagemath implementation

The implementation was tested on the whole parameter space for $\mathbb{F}_{q}$ where $q$ $\bmod 6=1$ and $q \leq 200$. It returns either the equation of a hyperelliptic curve and 2 morphisms to the input elliptic curves, or an error if the triple cover is found to be singular.
Step 1: compute Hesse pencil parameter

```
def curve_params(E, j, T1, T2):
    xT1 = T1[0]
    xT2 = T2[0]
    xT12 = (T1 + T2)[0]
    t = (-j-2) * (xT12-xT2) / (xT12-xT1) + 1
    a = (xT1 - xT2) * (t - 1)
    b = xT2
    a1, a2, a3, a4, a6 = E.a_invariants()
    assert a1 == 0 and a3 == 0
    x = E.base_field()["x"].gen()
    P = (a*x+b)**3 + a2* (a*x+b)**2 + a4* (a*x+b) + a6
    return t, P, a, b
```

Step 2: compute singularities coordinates

```
def double_coords(j, t1, t2):
    j2 = j*j
    d0 = (t1**2 - t2) / (t1**3 - 1)
    num = t1*t2 - 1
    den1 = (t1-1)*(t1-j2)*(t2-j2)
    den2 = (t1-1)*(t1-j)*(t2-j)
    den3 = (t2-1)*(t1-j)*(t1-j2)
    return d0, num / den1, num / den2, num / den3
def double_points(j, t1, t2):
    XD0, XD1, XD2, XD3 = double_coords(j, t1, t2)
    YD0, YD1, YD2, YD3 = double_coords(j**2, t2, t1)
    nodes = [(XD0, YD0), (XD1, YD1), (XD2, YD2), (XD3, YD3)]
    if nodes[0] == nodes[1]:
        return [nodes[0]] + [n for n in nodes if n != nodes[0]]
    if nodes[2] == nodes[3]:
        return [nodes[2]] + [n for n in nodes if n != nodes[2]]
```

Step 3: equation of the plane rational sextic

```
def rational_sextic(P1, P2, nodes):
    assert P1[3] == 1 and P2[3] == 1
    K = P1.base_ring()
    R = K["u", "v"]
    u, v = R.gens()
    # Information from lines at infinity
    S_inf = u**3*V**3 \
        +(v**3 * (u**2*P1[2] + u*P1[1] + P1[0])) \
        + (u**3 * (v**2*P2[2] + v*P2[1] + P2[0]))
    dS_du = derivative(S_inf, u)
    dS_dv = derivative(S_inf, v)
    rows = []
    vals = []
    degrees = [(i, j) for i in range(3) for j in range(3)]
    for xN, yN in nodes:
        rows.append([xN**i * yN**j for i, j in degrees])
        vals.append(-K(S_inf(u=xN, v=yN)))
        rows.append([i*xN**(i-1)*yN**j if i > 0 else 0 for i, j in degrees])
        vals.append(-K(dS_du(u=xN, v=yN)))
        rows.append([j*xN**i*yN**(j-1) if j > 0 else 0 for i, j in degrees])
        vals.append(-K(dS_dv(u=xN, v=yN)))
    if len(nodes) == 2: # triple point
        dS_du2 = derivative(dS_du, u)
        dS_duv = derivative(dS_du, v)
        dS_dv2 = derivative(dS_dv, v)
        xN, yN = nodes[O]
        vals.append(-K(dS_du2(u=xN, v=yN)))
        rows.append([2 * yN**j if i == 2 else 0 for i, j in degrees])
        vals.append(-K(dS_dv2(u=xN, v=yN)))
        rows.append([2 * xN**i if j == 2 else O for i, j in degrees])
        vals.append(-K(dS_duv(u=xN, v=yN)))
        rows.append([0, 0, 0, 0, 1, 2*yN, 0, 2*xN, 4*xN*yN])
    M = Matrix(K, rows)
    coef = M.solve_right(vector(K, vals))
    S_rest = sum(c * u**i * v**j for c, (i, j) in zip(coef, degrees))
    return S_inf + S_rest
```

Step 4: compute a rational parameterisation of the sextic

```
def ramif1_coords(S, t1, t2):
    numx = 4*t1**2*t2**3 - t1**2 - t2**4 - 6*t1*t2**2 + 4*t2
    denx = 4*(t1**3-1)*(t2**3-1)
    deny = t2**3 - 3*t1*t2 + 2
    x = numx / denx
    return (x, (t2**2 - t1)/deny if deny != 0 else None)
def rational_params(S, nodes, ramif):
    K = S.base_ring()
    R = K["x", "y", "z"]
    x, y, z = R.gens()
    if ramif in nodes:
        nodes = [ramif] + [n for n in nodes if n != ramif]
```

```
x0, y0 = nodes[0]
S = S(x, y).homogenize(var=z)
S1 = S(x + x0*z, y + y0*z, z)
Q = div_monom(S1(y*z, z*x, x*y), x**3 * y**3 * z**2)
T = K["T"].gen() # Uniformizer
if len(nodes) == 2: # triple point
    Q = div_monom(Q, z) # nodal cubic
    x1, y1 = nodes[1]
    qx1, qy1, qz1 = (y1-y0, x1-x0, (x1-x0)*(y1-y0))
    QT = Q(qx1 * z + x, qy1 * z + y, qz1 * z)
    num = QT[2,0,1] + QT[1,1,1]*T + QT[0,2,1]*T**2
    den = QT[3,0,0] + QT[2,1,0]*T + QT[1,2,0]*T**2 + QT[0,3,0]*T**3
    xQT, yQT, zQT = -num, -num*T, den
    x_Q, y_Q, z_Q = qx1 * zQT + xQT, qy1 * zQT + yQT, qz1 * zQT
else:
    (x1, y1), (x2, y2), (x3, y3) = nodes[1:4]
    M = Matrix(K, [
        [y1-y0, x1-x0, (x1-x0)*(y1-y0)],
        [y2-y0, x2-x0, (x2-x0)*(y2-y0)],
        [y3-y0, x3-x0, (x3-x0)*(y3-y0)],
        ]).transpose()
        u, v, w = M * vector([x, y, z])
        QT = Q(u, v, w)
        C = div_monom(QT(y*z, z*x, y*x), (x*y*z) ** 2)
        assert C.total_degree() == 2
        if ramif == (x0, y0):
        rat = (1, 0, 0) # vertical tangent
        elif ramif[1] is None:
        rat = (1/(ramif[0]-x0), 0, 1) # at infinity
    else:
        rat = (1/(ramif[0]-x0), 1/(ramif[1]-y0), 1)
    rat = M.inverse() * vector(rat)
    rat = (rat[2]/rat[0], rat[2]/rat[1])
    CT = C(rat[0]*z + x, rat[1]*z + y, z)
    # CT: ax^2+bxy+cy^2+dx+ey=0
    num = CT[1,0,1] + CT[0,1,1]*T
    den = CT[2,0,0] + CT[1,1,0]*T + CT[0,2,0]*T**2
    x_CT, y_CT, z_CT = -num, -T*num, den
    x_C, y_C, z_C = x_CT+rat[0]*z_CT, y_CT+rat[1]*z_CT, z_CT
    x_QT, y_QT, z_QT = y_C*z_C, z_C*x_C, x_C*y_C
    x_Q, y_Q, z_Q = M*vector([x_QT, y_QT, z_QT])
    for a in range(20):
        if a == 0:
            if z_Q.degree() == 4:
                    xQinf, yQinf = x_Q[4]/z_Q[4], y_Q[4]/z_Q[4]
                    if Q(xQinf, 0, 1) != 0 and Q(0, yQinf, 1) != 0:
                    break
        else:
            a = K(a)
            if z_Q(a) != 0:
                        xQa, yQa = x_Q(a) / z_Q(a), y_Q(a) / z_Q(a)
                        if Q(xQa, 0, 1) != 0 and Q(0, yQa, 1) != 0:
                    x_Q = x_Q(a + 1/T)
                    y_Q = y_Q (a + 1/T)
```

```
                    z_Q = z_Q (a + 1/T)
break
    x_S1, y_S1, z_S1 = y_Q*z_Q, z_Q*x_Q, x_Q*y_Q
    X = x0 + x_S1 / z_S1
    Y = y0 + y_S1 / z_S1
    return X, Y
def div_monom(f, q):
    R = f.parent()
    res = 0
    for c, m in zip(f.coefficients(), f.monomials()):
        assert R.monomial_divides(q, m)
        res += c * R.monomial_quotient(m, q)
    return res
```


## Step 5: compute final equations

```
def triple_cover(E1, T11, T12, E2, T21, T22):
    K = E1.base_field()
    j = T11.weil_pairing(T12, 3)
    assert j == T21.weil_pairing(T22, 3)
    t1, P1, a1, b1, c1 = curve_params(E1, j, T11, T12)
    t2, P2, a2, b2, c2 = curve_params(E2, j, T21, T22)
    nodes = double_points(j, t1, t2)
    S = rational_sextic(P1.monic(), P2.monic(), nodes)
    ramif = ramif1_coords(S, t1, t2)
    X1, X2 = rational_params(S, nodes, ramif)
    NumX1, DenX1 = X1.numerator(), X1.denominator()
    NumX2, DenX2 = X2.numerator(), X2.denominator()
    if max(pol.degree() for pol in [NumX1, DenX1, NumX2, DenX2]) <= 2:
        return "H\sqcupis
    Z1 = (P1(NumX1 / DenX1) * DenX1**3).numerator() // DenX2
    aZ1 = Z1.lc()
    Y1 = Z1.monic().sqrt()
    Z2 = (P2(NumX2 / DenX2) * DenX2**3).numerator() // DenX1
    aZ2 = Z2.lc()
    Y2 = Z2.monic().sqrt()
    u1 = NumX1[3] / DenX1[3]
    u2 = NumX2[3] / DenX2[3]
    T = (t1**3-1)*(t2**3-1)
    aZ12 = t1*u1+t2*u2-u1*u2*(t1*t2+2) - (1 + 2*(t1*t2-1)**3/T)/K(3)
    assert aZ12**2 == aZ1*aZ2
    def f1(x, y):
        return (a1*NumX1(x)/DenX1(x)+b1, c1*Y1(x)/DenX1(x)**2 * y)
    def f2(x, y):
        return (a2*NumX2(x)/DenX2(x)+b2, c2*Y2(x)/DenX2(x)**2 * y * aZ2 / aZ12)
    H = aZ1*DenX1*DenX2
    return H, f1, f2
```


## Sample program and output

```
from sage.all import GF, EllipticCurve
K = GF(4099)
R = K["x", "y"]
x, y = R.gens()
E1 = EllipticCurve(K, [-961, -1125])
T11, T12 = E1.abelian_group().torsion_subgroup(3).gens()
```

```
E2 = EllipticCurve(K, [1044, 354])
T21, T22 = E2.abelian_group().torsion_subgroup(3).gens()
H, f1, f2 = triple_cover(
    E1, T11.element(), T12.element(),
    E2, T21.element(), T22.element())
print("H:", H)
# shows 2641*T^6+3151*T^5+2443*T^4+1911*T^3+3286*T^2+3446*T+3655
print("H->E1:", f1(x, y))
# shows
# (880*x^3 + 671*x^2 - 1915*x - 231)/(x^3 - 765*x^2 + 1818*x + 731)
# y*(x^3 - 1219*x^2 - 1118*x + 1170)/( (x^3 - 765*x^2 + 1818*x + 731)^2
print("H->E2:", f2(x, y))
# shows
# (1625*x^3 - 496*x^2 - 172*x - 983)/(x^3 - 432*x^2 + 380*x + 149)
# y*(1937*x^3-1580*x^2-245*x-1525)/(405*(x^3 - 432*x^2 + 380*x + 149)^2)
```


## References

[AD09] Michela Artebani and Igor V. Dolgachev, The Hesse pencil of plane cubic curves, Enseign. Math. 55 (2009), no. 3, 235-273, DOI 10.4171/LEM/55-3-3, available at https://ems.press/journals/lem/articles/12146
[BFT14] Nils Bruin, Victor E. Flynn, and Damiano Testa, Descent via (3,3)-isogeny on Jacobians of genus 2 curves, Acta Arithmetica 165 (2014), no. 3, 201-223, DOI 10.4064/aa165-3-1, available at https://arxiv.org/abs/1401.0580
[BHLS15] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, Genus-2 curves and Jacobians with a given number of points, LMS Journal of Computation and Mathematics 18 (2015), no. 1, 170-197, DOI 10.1112/s1461157014000461, available at https://arxiv.org/abs/1403.6911
[BM] Araceli Bonifant and John Milnor, On Real and Complex Cubic Curves, available at https://arxiv.org/abs/1603.09018
[CD21] Wouter Castryck and Thomas Decru, Multiradical isogenies, Cryptology ePrint Archive 2021/1133 (2021), available at https://eprint.iacr.org/2021/1133
[CD22] Wouter Castryck and Thomas Decru, An efficient key recovery attack on SIDH (preliminary version), Cryptology ePrint Archive 2022/975 (2022), available at https: //eprint.iacr.org/2022/975
[Dol12] Igor V. Dolgachev, Classical Algebraic Geometry: a modern view, Cambridge University Press, 2012.
[DL08] I. Dolgachev and D. Lehavi, On isogenous principally polarized abelian surfaces, Curves and abelian varieties, Contemp. Math. 465 (2008), 51-69.
[CR15] Romain Cosset and Damien Robert, Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves, Math. Comp. 84 (2015), 1953-1975, DOI 10.1090/S0025-5718-2014-02899-8, available at https://hal.archives-ouvertes.fr/hal-00578991/ file/niveau.pdf
[LR] David Lubicz and Damien Robert, Arithmetic on Abelian and Kummer Varieties, available at https://www.normalesup.org/~robert/pro/publications/ articles/arithmetic.pdf
[Gau07] Pierrick Gaudry, Fast genus 2 arithmetic based on Theta functions, Journal of Mathematical Cryptology 1 (2007), no. 3, 243-265, DOI doi:10.1515/JMC.2007.012, available at https://doi.org/10.1515/JMC. 2007.012
[Kan97] Ernst Kani, The number of curves of genus 2 with elliptic differentials, J. reine angew. Math 485 (1997), 93-121, available at https://mast.queensu.ca/~kani/ papers/numgenl.pdf
[Kuh88] Robert M. Kuhn, Curves of Genus 2 with Split Jacobian, Transactions of the American Mathematical Society 307 (1988), no. 1, 41-49, available at https://doi.org/10. 1090/S0002-9947-1988-0936803-3
[Kun22] Sabrina Kunzweiler, Efficient Computation of $\left(2^{n}, 2^{n}\right)$-Isogenies, Cryptology ePrint Archive, Paper 2022/990 (2022), available at https://eprint.iacr.org/2022/990
[Kuw11] Masato Kuwata, Constructing families of elliptic curves with prescribed mod 3 representation via Hessian and Cayleyan curves (2011), available at https://arxiv.org/ abs/1112.6317.
[Mir85] Rick Miranda, Triple Covers in Algebraic Geometry, American Journal of Mathematics 107 (1985), no. 5, 1123-1158, DOI 10.2307/2374349.
[MW12] Dustin Moody and Hongfeng Wu, Families of elliptic curves with rational 3-torsion, Journal of Mathematical Cryptology 5 (2012), no. 3-4, 225-246, DOI doi:10.1515/jmc-2011-0013, available at https://doi.org/10.1515/jmc-2011-0013
[SAGE] The Sage Developers, Sagemath, the Sage Mathematics Software System (Version 9.6), 2022. https://www. sagemath.org.
[Sha04] Tony Shaska, Genus 2 fields with degree 3 elliptic subfields, Forum Math. 16 (2004), no. 2, 263-280, available at https://arxiv.org/abs/math/0109155
[DGPS22] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SinGULAR 4-3-0 - A computer algebra system for polynomial computations, 2022. http: //www.singular.uni-kl.de
[Smi05] Benjamin Smith, Explicit Endormorphisms and Correspondences (PhD dissertation) (2005), available at http://iml.univ-mrs.fr/~kohel/phd/thesis_smith.pdf
[Roh05] Jan Christian Rohde, Short equations for the genus 2 covers of degree 3 of an elliptic curve (2005), available at https://arxiv.org/abs/math/0503412
Email address: remyoudompheng@gmail.com

