Four-Dimensional GLV via the Weil Restriction

Aurore Guillevic and Sorina Ionica
Ecole Normale Supérieure, Thales

Abstract

The Gallant-Lambert-Vanstone (GLV) algorithm uses efficiently computable endomorphisms to accelerate the computation of scalar multiplication of points on an abelian variety. Freeman and Satoh proposed for cryptographic use two families of genus 2 curves defined over $\mathbb{F}_p$ which have the property that the corresponding Jacobians are $(2,2)$-isogenous over an extension field to a product of elliptic curves defined over $\mathbb{F}_{p^2}$. We exploit the relationship between the endomorphism rings of isogenous abelian varieties to exhibit efficiently computable endomorphism on both the genus 2 Jacobian and the elliptic curve. This leads to a four dimensional GLV method on Freeman and Satoh's Jacobians and on two new families of elliptic curves defined over $\mathbb{F}_{p^2}$.

Keywords: GLV method, elliptic curves, genus 2 curves, isogenies.

1 Introduction

The scalar multiplication of a point on a small dimension abelian variety is one of the most important primitives used in curve-based cryptography. Various techniques were introduced to speed-up the scalar multiplication. Firstly there exist recoding-exponent techniques such as sliding window and Non-Adjacent-Form representation. These techniques are valid for generic groups and improved for elliptic curves as the inversion (or negation in additive notation) is free.

Secondly, in 2001, Gallant, Lambert and Vanstone [GLV01] introduced a method which uses endomorphisms on the elliptic curve to decompose the scalar multiplication in a 2-dimensional multi-multiplication. Given an elliptic curve E over a finite field $\mathbb{F}_p$ with a fast endomorphism ϕ and a point P of large prime order r such that $\phi(P) = \lambda P$, the computation of $[k]P$ is decomposed as

$$kP = [k_1]P + [k_2]\phi(P),$$

with $k = k_1 + \lambda k_2 \pmod r$ such that $|k_1|, |k_2| \simeq \sqrt{r}$. Gallant et *al* provided examples of curves whose endomorphism ϕ is given by: complex-multiplication by $\sqrt{-1}$ (j-invariant $j = 1728$), $\frac{1+\sqrt{-3}}{2}$ ($j = 0$), $\sqrt{-2}$ ($j = 8000$) and $\frac{1+\sqrt{-7}}{2}$ ($j = -3375$). In 2009 Galbraith, Lin and Scott [GLS09] presented a very efficient method to construct an efficient endomorphism on elliptic curves E defined over $\mathbb{F}_{p^2}$ which are quadratic twists of elliptic curves defined over $\mathbb{F}_p$. In this case, a fast endomorphism ψ is obtained by carefully exploiting the Frobenius endomorphism. This endomorphism verifies the equation $\psi^2+1 = 0$ on $E(\mathbb{F}_{p^2})$. In 2012, Longa and Sica improved the GLS construction, by showing that a 4-dimensional decomposition of scalar multiplication is possible, on GLS curves allowing efficient complex multiplication ϕ. Let λ, μ denote the eigenvalues of the two endomorphisms ϕ, ψ. Then we can decompose the scalar k into $k = k_0 + k_1\lambda + k_2\mu + k_3\lambda\mu$ and compute

$$[k]P = [k_0]P + [k_1]\phi(P) + [k_2]\psi(P) + k_3\phi \circ \psi(P).$$

Moreover, Longa and Sica provided an efficient algorithm to compute decompositions of k such that $|k_i| < Cr^{1/4}$, $i = 1, \dots, 4$. Note that most curves presented in the literature have particular j-invariants. GLV curves have j-invariant 0, 1728, 8000, or -3375, while GLS curves have j-invariant in $\mathbb{F}_p$, even though they are defined over $\mathbb{F}_{p^2}$.

In 2013, Bos, Costello, Hisil and Lauter proposed in [BCHL13] a 4-dimensional GLV technique to speed-up scalar multiplication in genus 2. They considered the Buhler-Koblitz genus 2 curves $y^2 = x^5 + b$ and the Furukawa-Kawazoe-Takahashi curves $y^2 = x^5 + ax$. These two curves have a very efficient dimension-4 GLV technique available. On BK curves, they proposed 2-dimensional GLV on the corresponding Kummer surface.

In this paper we study GLV decompositions on two types of abelian varieties:

- Elliptic curves defined over $\mathbb{F}_{p^2}$, with j-invariant defined over $\mathbb{F}_{p^2}$.
- Jacobians of genus 2 curves defined over $\mathbb{F}_p$, which are isogenous over an extension field to a product of elliptic curves defined over $\mathbb{F}_{p^2}$.

First, we study a family of elliptic curves whose equation is of the form $E_{1,c}(\mathbb{F}_{p^2}) : y^2 = x^3 + 27(10 - 3c)x + 14 - 9c$ with $c \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, $c^2 \in \mathbb{F}_p$. These curves have an endomorphism ψ satisfying $\psi^2 \pm 2 = 0$ for points defined over $\mathbb{F}_{p^2}$. Nevertheless, the complex multiplication discriminant of the curve is not 2, but of the form $-D = -2D^{'}$. The second family is given by elliptic curves with equation of the form $E_{2,c}(\mathbb{F}_{p^2}) : y^2 = x^3 + 3(2c - 5)x + c^2 + 14c + 22$ with $c \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, $c^2 \in \mathbb{F}_p$. We show that these curves have an endomorphism ψ such that $\psi^2 + 3 = 0$ for points defined over $\mathbb{F}_{p^2}$. The complex multiplication discriminant of the curve $E_{2,c}$ is of the form $-D = -3D^{'}$. Our construction is a simple and efficient way to exploit the existence of a p-power Frobenius endomorphism on the Weil restriction of these curves. If the discriminant D is small, we propose a 4-dimensional GLV algorithm for the $E_{1,c}$ and $E_{2,c}$ families of curves. We use Velu's formulas to compute explicitly th endomorphisms on $E_{1,c}$ and $E_{2,c}$.

At last, we study genus 2 curves whose equations are $\mathcal{C}_1 : Y^2 + X^5 + aX^3 + bX$, $a, b \in \mathbb{F}_p$ and $\mathcal{C}_2 : Y^2 = X^6 + aX^3 + b$. The Jacobians of these curves split over an extension field in two isogenous elliptic curves. More precisely, the Jacobian of $\mathcal{C}_1$ is isogenous to $E_{1,c} \times E_{1,c}$ and the Jacobian of $\mathcal{C}_2$ is isogenous to $E_{2,c} \times E_{2,-c}$. These two Jacobians were proposed for use in cryptography by Satoh [Sat09] and Freeman and Satoh [FS11], who showed that they are isogenous over $\mathbb{F}_p$ to the Weil restriction of a curve of the form $E_{1,c}$ or $E_{2,c}$. This property is exploited to derive fast point counting algorithms and pairing-friendly constructions. We investigate efficient scalar multiplication via the GLV technique on Satoh and Freeman's Jacobians. We give explicit formulae for $(2, 2)$-isogeny between the product of elliptic curves and the Jacobian of the genus 2 curve. As a consequence, we derive a method to efficiently compute endomorphisms on the Jacobians of $\mathcal{C}_1$ and $\mathcal{C}_2$.

This paper is organized as follows. Section 2 briefly presents Vélu's formulae for computing isogenies on elliptic curves. In Section 3 we review the construction of $(2, 2)$-isogenies between Jacobians of $\mathcal{C}_1$ and $\mathcal{C}_2$ and products of elliptic curves. In Section 4 and 5 we give our construction of efficient endomorphisms on $E_{1,c}$ and $E_{2,c}$ and derive a four dimensional GLV algorithm on these curves. Section 6 explains how to obtain a four dimensional GLV method on the Jacobians of $\mathcal{C}_1$ and $\mathcal{C}_2$. Finally, in Section 7, we describe our implementation and conclude that both elliptic curves defined over $\mathbb{F}_{p^2}$ and Satoh and Freeman's Jacobians yield scalar multiplication algorithms competitive with those of Longa and Sica and Bos *et al.*

2 Vélu's formulas to compute isogenies

In this section we recall Vélu's formulas for computing isogenies and further improvements on these formulae found independently by Dewaghe [Dew95] and Kohel [Koh96]. For details, the reader is referred to Lercier's thesis. [Ler97, §4.1]. Let E_a be an elliptic curve defined over an algebraic closed field $\mathbb{K}$, and F a subgroup of the set of points of E_a. The isogeny from $E_a(\mathbb{K})$ into $E_b(\mathbb{K})$ of kernel F is given by

$$P \quad \mapsto \quad \begin{cases} \mathcal{O}_{E_b} & \text{if } P = \mathcal{O}_{E_a}, \\ \left(X + \sum_{Q \in F \setminus \mathcal{O}_{E_a}} X_{P+Q} - X_Q,\ Y + \sum_{Q \in F \setminus \mathcal{O}_{E_a}} Y_{P+Q} - Y_Q\right) & \text{if } P = (X, Y) \end{cases} \tag{1}$$

and the coefficients of E_b are also given by formulas. To simplify, assume that

$$E_a(\mathbb{K}) : y^2 = x^3 + a_4 x + a_6 \ . \tag{2}$$

There are more general formulas for elliptic curves that are not in a reduced Weierstrass form. Let R be the subset of F defined by $F \setminus E_a[2] = R \cup (-R)$, $R \cap (-R) = \emptyset$ and $S = F \cap E_a[2] - \{\mathcal{O}_{E_a}\}$. Now let for all point $Q(X_Q, Y_Q) \in F \setminus \{\mathcal{O}_{E_a}\}$,

$$\begin{array}{rclcrclcrcl} g_Q^x & = & 3X_Q^2 + a_4, & & t_Q & = & \begin{cases} g_Q^x & \text{if } Q \in S, \\ 2g_Q^x = 6X_Q^2 + 2a_4 & \text{otherwise,} \end{cases} & & t & = & \sum_{Q \in R \cup S} t_Q, \\ g_Q^y & = & -2Y_Q, & & u_Q & = & (g_Q^y)^2 = 4Y_Q^2 = 4X_Q^3 + 4a_4 X_Q + 4a_6, & & w & = & \sum_{Q \in R \cup S} u_Q + X_Q t_Q \ . \end{array} \tag{3}$$

Then E_b is given by

$$E_b(\mathbb{K}) : y^2 = x^3 + b_4 x + b_6 \text{ with } b_4 = a_4 - 5t \text{ and } b_6 = a_6 - 7w \tag{4}$$

and the isogeny has degree $\#F$ and is given by

$$\begin{array}{rcl} \mathcal{I} : E_a(\mathbb{K}) & \to & E_b(\mathbb{K}) \\ P & \mapsto & \begin{cases} \mathcal{O}_{E_b} & \text{if } P = \mathcal{O}_{E_a}, \\ (X_{\mathcal{I}(P)}, Y_{\mathcal{I}(P)}) & \text{if } P = (X, Y) \end{cases} \end{array} \tag{5}$$

with

$$\begin{cases} X_{\mathcal{I}(P)} & = & X + \sum_{Q \in R \cup S} \left(\frac{t_Q}{X - X_Q} + \frac{u_Q}{(X - X_Q)^2} \right), \\ Y_{\mathcal{I}(P)} & = & Y + \sum_{Q \in R \cup S} \left(\frac{2u_Q Y}{(X - X_Q)^3} + \frac{t_Q (Y - Y_Q) - g_Q^x g_Q^y}{(X - X_Q)^2} \right) \end{cases} \tag{6}$$

3 Elliptic curves with a genus 2 cover

In this paper we will work with two examples of genus 2 curves whose Jacobians allow over an extension field a $(2,2)$-isogeny to a product of elliptic curves. We first study the genus 2 curve

$$\mathcal{C}_1(\mathbb{F}_p) : Y^2 = X^5 + aX^3 + bX, \text{ with } a, b \neq 0 \in \mathbb{F}_p \ . \tag{7}$$

It was shown [LM97, Sat09, FS11, §2, §3, §4.1] that the Jacobian of $\mathcal{C}_1$ is isogenous to $E_{1,c} \times E_{1,c}$, where

$$E_{1,c}(\mathbb{F}_p[\sqrt{b}]) : y^2 = (c+2)x^3 - (3c-10)x^2 + (3c-10)x - (c+2) \tag{8}$$

with $c = a/\sqrt{b}$. We recall the formulae for the cover maps from $\mathcal{C}_1$ to $E_{1,c}$ with the notation $i = \sqrt{-1} \in \mathbb{F}_p$ or $\mathbb{F}_{p^2}$. The reader is referred to the proof of Prop. 4.1 in [FS11] for details of the computations.

$$\begin{array}{rclcrcl} \varphi_1 : \mathcal{C}_1(\mathbb{F}_p) & \to & E_{1,c}(\mathbb{F}_p[\sqrt[8]{b}]) & \quad & \varphi_2 : \mathcal{C}_1(\mathbb{F}_q) & \to & E_{1,c}(\mathbb{F}_p[\sqrt[8]{b}]) \\ (x, y) & \mapsto & \left(\left(\frac{x + \sqrt[4]{b}}{x - \sqrt[4]{b}} \right)^2, \frac{8y \sqrt[8]{b}}{(x - \sqrt[4]{b})^3} \right) & & (x, y) & \mapsto & \left(\left(\frac{x - \sqrt[4]{b}}{x + \sqrt[4]{b}} \right)^2, \frac{8iy \sqrt[8]{b}}{(x + \sqrt[4]{b})^3} \right) \end{array} \tag{9}$$

The $(2,2)$-isogeny is given by

$$\begin{array}{rcl} I : J_{\mathcal{C}_1} & \to & E_{1,c} \times E_{1,c} \\ P + Q - 2P_\infty & \mapsto & (\varphi_{1*}(P) + \varphi_{1*}(Q), \varphi_{2*}(P) + \varphi_{2*}(Q)) \end{array} \tag{10}$$

and its dual is

$$\begin{array}{rcl} \hat{I} : E_{1,c} \times E_{1,c} & \rightarrow & J_{\mathcal{C}_1} \\ (S_1, S_2) & \mapsto & \varphi_1^*(S_1) + \varphi_2^*(S_2) - 4P_\infty \end{array}$$

with $\varphi_1^*(S_1) = \left(\frac{\sqrt{x_1}+1}{\sqrt{x_1}-1}\sqrt[4]{b}, \frac{y_1\sqrt[8]{b}^5}{(\sqrt{x_1}-1)^3}\right) + \left(\frac{-\sqrt{x_1}+1}{-\sqrt{x_1}-1}\sqrt[4]{b}, \frac{y_1\sqrt[8]{b}^5}{(-\sqrt{x_1}-1)^3}\right)$
and $\varphi_2^*(S_2) = \left(\frac{1+\sqrt{x_2}}{1-\sqrt{x_2}}\sqrt[4]{b}, \frac{-iy_2\sqrt[8]{b}^5}{(1-\sqrt{x_2})^3}\right) + \left(\frac{1-\sqrt{x_2}}{1+\sqrt{x_2}}\sqrt[4]{b}, \frac{-iy_2\sqrt[8]{b}^5}{(1+\sqrt{x_2})^3}\right)$.

Note that I and its dual are defined over an extension field of $\mathbb{F}_p$ of degree 1, 2, 4 or 8. One may easily check that $I \circ \hat{I} = [2]$ and $\hat{I} \circ I = [2]$. Since I splits multiplication by 2, an argument similar to [Koh96, Prop. 21] implies that $2\mathrm{End}(J_{\mathcal{C}_1}) \subseteq \mathrm{End}(E_{1,c} \times E_{1,c})$ and $2\mathrm{End}(E_{1,c} \times E_{1,c}) \subseteq \mathrm{End}(J_{\mathcal{C}_1})$. We will use these inclusions to exhibit efficiently computable endomorphisms on both $J_{\mathcal{C}_1}$ and $E_{1,c}$.

Secondly, we consider an analogous family of degree 6 curves. These curves were studied by Duursma and Kiyavash [DK05] and by Gaudry and Schost [GS01].

$$\mathcal{C}_2(\mathbb{F}_p) : Y^2 = X^6 + aX^3 + b \text{ with } a, b \neq 0 \in \mathbb{F}_p \tag{11}$$

The Jacobian of the curve is denoted $J_{\mathcal{C}_2}$ is isogenous to the product of elliptic curves $E_{2,c} \times E_{2,-c}$, where

$$E_{2,c}(\mathbb{F}_p[\sqrt{b}]) \; : \; y^2 = (c+2)x^3 + (-3c+30)x^2 + (3c+30)x + (-c+2) \text{ and} \tag{12}$$
$$E_{2,-c}(\mathbb{F}_p[\sqrt{b}]) \; : \; y^2 = (-c+2)x^3 + (3c+30)x^2 + (-3c+30)x + (c+2), \tag{13}$$

with $c = a/\sqrt{b}$. The construction of the isogeny is similar to the one for I. We recall the formulae for cover maps from $\mathcal{C}_2$ to $E_{2,c}$ and to $E_{2,-c}$. For detailed computations, the reader is referred to Freeman and Satoh [FS11, Prop. 4].

$$\begin{array}{rcl} \varphi_2 : \mathcal{C}_2(\mathbb{F}_p) & \rightarrow & E_{2,c} \times E_{2,-c}(\mathbb{F}_{p^6}) \\ (X, Y) & \mapsto & \left\{\left(\left(\frac{X+\sqrt[6]{b}}{X-\sqrt[6]{b}}\right)^2, \frac{8Y}{(X-\sqrt[6]{b})^3}\right), \left(\left(\frac{X-\sqrt[6]{b}}{X+\sqrt[6]{b}}\right)^2, \frac{8Y}{(X+\sqrt[6]{b})^3}\right)\right\} \end{array} \tag{14}$$

Note that the isogeny constructed using these cover maps is defined over an extension field of degree 1,2,3 or 6.

4 Four dimensional GLV on $E_{1,c}$

We assume that $c \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $c^2 \in \mathbb{F}_p$.

4.1 First Endomorphism on $E_{1,c}$ with Vélu's formulas

We aim to compute a 2-isogeny on $E_{1,c}(\mathbb{F}_{p^2})$. Note that we can write

$$E_{1,c}(\mathbb{F}_{p^2}) : y^2 = (x-12)(x^2 + 12x + 81c - 126). \tag{15}$$

Hence there always exists a 2-torsion point $P_2 = (12, 0)$ on $E_{1,c}(\mathbb{F}_{p^2})$. We apply Velu's formulas to compute the isogeny whose kernel is generated by P_2. We obtain an isogeny from $E_{1,c}$ into $E_b : y^2 = x^3 + b_4x + b_6$ with $b_4 = -2^2 \cdot 27(3c+10)$, $b_6 = -2^2 \cdot 108(14+9c)$. We observe that E_b is isomorphic to the curve whose equation is

$$E_{1,-c}(\mathbb{F}_{p^2}) : y^2 = x^3 + 27(-3c-10)x + 108(14+9c) \tag{16}$$

through $(x_b, y_b) \mapsto (x_b/(-2), y_b/(-2\sqrt{-2}))$. Note that $\sqrt{-2} \in \mathbb{F}_{p^2}$ and thus this isomorphism is defined over $\mathbb{F}_{p^2}$. We define the isogeny

$$\begin{array}{rcl} \mathcal{I}_2 : E_{1,c}(\mathbb{F}_{p^2}) & \to & E_{1,-c}(\mathbb{F}_{p^2}) \\ (x,y) & \mapsto & \left(\frac{-x}{2} + \frac{162+81c}{-2(x-12)}, \frac{-y}{2\sqrt{-2}}\left(1 - \frac{162+81c}{(x-12)^2}\right)\right) = \left(\frac{x^2-12x+162+81c}{-2(x-12)}, y\frac{x^2-24x-18-81c}{-2\sqrt{-2}(x-12)^2}\right) \end{array} \tag{17}$$

We show that we can use this isogeny to get an efficiently computable endomorphism on $E_{1,c}$. Observe that since $c \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $c^2 \in \mathbb{F}_p$, we have that

$$\pi_p(c) = c^p = -c, \ \pi_p(j(E_{1,c})) = j(E_{1,-c}) \tag{18}$$

hence the curves $E_{1,c}$ and $E_{1,-c}$ (16) are *isogenous* over $\mathbb{F}_{p^2}$ via the Frobenius map π_p. They are not isomorphic, because they do not have the same j-invariant.

To sum up, we obtain an efficiently computable endomorphism Φ_2 by composing $\pi_p \circ \mathcal{I}_2$

$$\begin{array}{rcl} \Phi_2 : E_{1,c}(\mathbb{F}_{p^2}) & \to & E_{1,c}(\mathbb{F}_{p^2}) \\ (x,y) & \mapsto & \left(\dfrac{-x^p}{2} - \dfrac{162-81c}{2(x^p-12)}, \dfrac{-y^p}{2\sqrt{-2}^p}\left(1 - \dfrac{162-81c}{(x^p-12)^2}\right)\right) \\ & & = \left(\dfrac{x^{2p} - 12x^p + 162 - 81c}{-2(x^p-12)}, y^p\dfrac{x^{2p} - 24x^p - 18 + 81c}{-2\sqrt{-2}^p(x^p-12)^2}\right) \end{array} \tag{19}$$

If we compute formally[1] Φ_2^2 then we obtain exactly the formulas to compute $\pi_{p^2} \circ [-2]$ on $E_{1,c}(\mathbb{F}_{p^2})$ if $\sqrt{-2} \in \mathbb{F}_p$, $\pi_{p^2} \circ [2]$ if $\sqrt{-2} \notin \mathbb{F}_p$. This difference occurs because a term $\sqrt{-2}\sqrt{-2}^p$ appears in the formula. If $p \equiv 1, 7 \mod 8$, $\sqrt{-2}^p = \sqrt{-2}$ and if $p \equiv 3, 5 \mod 8$, $\sqrt{-2}^p = -\sqrt{-2}$. Hence Φ_2 restricted to $E_{1,c}(\mathbb{F}_{p^2})$ verifies the equation

$$\Phi_2^2 \pm 2 = 0.$$

We note that the above construction does not come as a surprise. Since $2\mathrm{End}(J_{\mathcal{C}_1}) \subseteq \mathrm{End}(E_{1,c} \times E_{1,c})$ and since the Jacobian $J_{\mathcal{C}_1}$ is equipped with a p-power Frobenius endomorphism, we deduce that there are endomorphisms with inseparability degree p on the elliptic curve $E_{1,c}$. Our construction is simply an efficient method to compute such an endomorphism.

4.2 Efficient complex multiplication on $E_{1,c}(\mathbb{F}_{p^2})$

In the remainder of this paper, we assume that the curve $E_{1,c}$ is defined over $\mathbb{F}_{p^2}$, with $p \equiv 1 \pmod 4$. We suppose that the complex multiplication discriminant D of the curve $E_{1,c}$ is small. A natural way to obtain an efficiently computable endomorphism is to take Φ_D the generator for the endomorphism ring (i.e. $\sqrt{-D}$). Let t_{p^2} be the trace of $E_{1,c}(\mathbb{F}_{p^2})$. The equation of the complex multiplication is then

$$(t_{p^2})^2 - 4p^2 = -D\gamma^2.$$

Guillevic and Vergnaud [GV12, proof of Th. 1 (4.) §2.2] showed that if $p \equiv 1 \mod 8$, one may write

$$t_{p^2} + 2p = D^{'}y^2 \text{ and } t_{p^2} - 2p = -2n^2. \tag{20}$$

Similarly, if $p \equiv 5 \mod 8$ then

$$t_{p^2} + 2p = 2n^2 \text{ and } t_{p^2} - 2p = -D^{'}y^2. \tag{21}$$

This implies, in particular, that we have $D = 2D'$. We prove that there is an endomorphism on $E_{1,c}$ whose degree of separability is D'. In order to do that, we will need to compute first the general equation of Φ_2.

[1] e.g. with Maple, verification code can be provided on demand

Lemma 1. *The characteristic equation of Φ_2 is*

$$\Phi_2^2 - Tr(\Phi_2)\phi_2 + \deg(\Phi_2)Id = 0 \ . \tag{22}$$

Proof. Hence $\mathrm{Tr}(\Phi_2^2) - \mathrm{Tr}^2(\Phi_2) + 2\deg(\Phi_2) = 0$. We know that $\deg(\Phi_2) = 2p$ because $\Phi_2 = \pi_p \circ \mathcal{I}_2$ and $\deg(\pi_p) = p, \deg(\mathcal{I}_2) = 2$, so $\mathrm{Tr}^2(\Phi_2) = \mathrm{Tr}(\Phi_2^2) + 4p$. Now, if $p \equiv 1 \mod 8$, $\mathrm{Tr}(\Phi_2^2) = \mathrm{Tr}(\pi_{p^2} \circ [-2]) = -2t_{p^2}$ thus we get $\mathrm{Tr}^2(\Phi_2) = -2t_{p^2} + 4p = -2(t_{p^2} - 2p) = 2(2n^2)$ hence $\mathrm{Tr}(\Phi_2) = 2n$. If $p \equiv 5 \mod 8$, $\mathrm{Tr}(\Phi_2^2) = \mathrm{Tr}(\pi_{p^2} \circ [2]) = 2t_{p^2}$ thus we get $\mathrm{Tr}^2(\phi_2) = 2t_{p^2} + 4p = 2(t_{p^2} + 2p) = 2(2n^2)$ hence $\mathrm{Tr}(\Phi_2) = 2n$ again. We get that the characteristic equation is

$$\Phi_2^2 - 2n \ \Phi_2 + 2p \ Id = 0 \ . \tag{23}$$

□

Theorem 1. *Let $E_{1,c}$ be an elliptic curve given by equation* (15)*, defined over $\mathbb{F}_{p^2}$ with $p \equiv 1 \pmod 4$. Let $-D$ be the complex multiplication discriminant and consider D' such that $D = 2D'$. There is an endomorphism $\Phi_{D'}$ of $E_{1,c}$ with degree of separability D'. The characteristic equation of this endomorphism is*

$$\Phi_{D'}^2 - D^{'}y \ \Phi_{D'} + D^{'}p \ Id = 0 \ . \tag{24}$$

Proof. Since $D = 2D'$, we have that Φ_D is the composition of a horizontal isogeny of degree 2 with a horizontal[2] isogeny of degree D'. We denote by $\mathcal{I}_2 : E_{1,c} \to E_{1,-c}$ the isogeny given by equation (17). Note that $\mathcal{I}_2$ is a horizontal isogeny of degree 2. Indeed, since $\pi_p : E_{1,-c} \to E_{1,c}$, it follows that $(\mathrm{End}(E_{1,c}))_2 \simeq (\mathrm{End}(E_{1,-c}))_2$. Since $2|D$, there is a unique horizontal isogeny of degree 2 starting from $E_{1,c}$. Hence the complex multiplication endomorphism on $E_{1,-c}$ is $\Phi'_D = \mathcal{I}_2 \circ \mathcal{I}_{D'}$, with $\mathcal{I}_{D'} : E_{1,-c} \to E_{1,c}$ a horizontal isogeny of degree D'. We define $\Phi_{D'} = \mathcal{I}_{D'} \circ \pi'_p$, with $\pi'_p : E_{1,c} \to E_{1,-c}$. To compute the characteristic polynomial of $\Phi_{D'}$, we observe that

$$\Phi_{D'} \circ \Phi_2 = \Phi_D$$

Hence, by using equation (24), we obtain that $\Phi_{D'}$ seen as algebraic integer in $\mathbb{Z}[\sqrt{D}]$ is $\frac{-2D'y \pm n\sqrt{2D'}}{2}$. Hence we have $\phi_{D'}^2 - D^{'}y \ \phi_{D'} + D^{'}p \ Id = 0$. □

The endomorphism $\Phi_{D'}$ constructed in Theorem 1 is thus computed as the composition of a horizontal isogeny with the p-power of the Frobenius. Since computing the p-power Frobenius for extension fields of degree 2 costs one negation, we conclude that $\phi_{D'}$ may be computed with Vélu's formulae with half the operations needed to compute Φ_D over $\mathbb{F}_{p^2}$.

Gallant-Lambert Vanstone algorithm on $E_{1,c}$

Assume that $E_{1,c}$ is such that $\#E_{1,c}(\mathbb{F}_{p^2})$ is divisible by a large number of cryptographic size. Let $\Psi = \Phi_{D'}$ and $\Phi = \Phi_2$. We observe Φ and Ψ viewed as algebraic integers generate disjoint quadratic extensions of $\mathbb{Q}$. Consequently, one may use $1, \Phi, \Psi, \Phi\Psi$ to compute the scalar multiple kP of a point $P \in E_{1,c}(\mathbb{F}_{p^2})$ using a four dimensional GLV algorithm. We do not give here the details of the algorithm which computes decompositions

$$k = k_1 + k_2\lambda + k_3\mu + k_4\lambda\mu,$$

with λ and μ the eigenvalues of Φ and Ψ and $|k_i| < Cr^{1/4}$. Such an algorithm is obtained by working over $\mathbb{Z}[\Phi, \Psi]$, using a similar analysis to the one proposed by Longa and Sica [LS13].

[2] An isogeny $I : E \to E'$ of degree ℓ is called horizontal if $(\mathrm{End}(E))_\ell \simeq (\mathrm{End}(E'))_\ell$

Eigenvalue computation

We deduce that the eigenvalue of ϕ_2 is $p\sqrt{-2}$ if $p \equiv 1 \mod 8$ and $p\sqrt{2}$ if $p \equiv 5 \mod 8$. We can explicitly compute this eigenvalue mod $\#E_{1,c}(\mathbb{F}_{p^2})$. We will use the formulas (20) and (4.2).

If $p \equiv 1 \mod 8$, we obtain

$$\begin{array}{rclcrcl} \#E_{1,c}(\mathbb{F}_{p^2}) & = & (p+1)^2 - D_1 y^2 & \rightarrow & \sqrt{D_1} & \equiv & (p+1)/y \mod \#E_{1,c}(\mathbb{F}_{p^2}), \\ & = & (p-1)^2 + 2n^2 & \rightarrow & \sqrt{-2} & \equiv & (p-1)/n, \\ & = & (1 - t_{p^2}/2)^2 + 2D_1(ny/2)^2 & \rightarrow & \sqrt{-2D_1} & \equiv & (2 - t_{p^2})/(ny) \ . \end{array}$$

If $p \equiv 5 \mod 8$, we obtain

$$\begin{array}{rclcrcl} \#E_{1,c}(\mathbb{F}_{p^2}) & = & (p-1)^2 + D_1 y^2 & \rightarrow & \sqrt{-D_1} & \equiv & (p-1)/y \mod \#E_{1,c}(\mathbb{F}_{p^2}), \\ & = & (p+1)^2 - 2n^2 & \rightarrow & \sqrt{2} & \equiv & (p+1)/n, \\ & = & (1 - t_{p^2}/2)^2 + 2D_1(ny/2)^2 & \rightarrow & \sqrt{-2D_1} & \equiv & (2 - t_{p^2})/(ny) \ . \end{array}$$

The eigenvalue of ϕ_2 on $E_{1,c}(\mathbb{F}_{p^2})$ is $p\sqrt{-2} \equiv p(p-1)/n \mod \#E_{1,c}(\mathbb{F}_{p^2})$ if $p \equiv 1 \mod 8$ or $p\sqrt{2} \equiv p(p+1)/n \mod \#E_{1,c}(\mathbb{F}_{p^2})$ if $p \equiv 5 \mod 8$.

The eigenvalue of $\phi_{D'}$ on $E_{1,c}(\mathbb{F}_{p^2})$ is $p\sqrt{D'} \equiv p(p+1)/y \mod \#E_{1,c}(\mathbb{F}_{p^2})$ if $p \equiv 1 \mod 8$ or $p\sqrt{-D'} \equiv p(p-1)/y \mod \#E_{1,c}(\mathbb{F}_{p^2})$ if $p \equiv 5 \mod 8$.

4.3 Example for $D' = 5$

By equations (20) and (4.2), we have that

$$4p = 2n^2 + D'y^2.$$

Using Magma, we computed an example with $p \equiv 5 \mod 8$, $D^{'} = 5$. For completeness, we list in Tab. 1 the necessary congruence conditions we used in order to obtain $p \equiv 1, 5 \mod 8$.

n	y	D_1	p	$\#E_{c,1}(\mathbb{F}_{p^2})$
$0 \mod 4$	$2 \mod 4$	$1 \mod 8$	$1 \mod 8$	$0 \mod 16$
$0 \mod 4$	$2 \mod 4$	$5 \mod 8$	$5 \mod 8$	$4 \mod 16$
$2 \mod 4$	$2 \mod 4$	$3 \mod 8$	$5 \mod 8$	$12 \mod 16$
$2 \mod 4$	$2 \mod 4$	$7 \mod 8$	$1 \mod 8$	$8 \mod 16$
$1 \mod 8$	$1, 7 \mod 8$	$2 \mod 32$	$1 \mod 8$	$2 \mod 16$
$1 \mod 8$	$3, 5 \mod 8$	$18 \mod 32$	$1 \mod 8$	$2 \mod 16$
$5 \mod 8$	$1, 7 \mod 8$	$18 \mod 32$	$1 \mod 8$	$2 \mod 16$
$5 \mod 8$	$3, 5 \mod 8$	$2 \mod 32$	$1 \mod 8$	$2 \mod 16$

Table 1: Parameter values mod 8 in order to get $p \equiv 1, 5 \mod 8$

Example 1. *We first search 63-bit numbers n, y such that $4 \mid n$, $y \equiv 2 \mod 4$, $p = (2n^2+5y^2)/4$ is prime and $\#E_{1,c}(\mathbb{F}_{p^2})$ is almost prime. We can expect an order of the form $4r$, with r prime. In few seconds, we find the following parameters. n = 0x55d23edfa6a1f7e4*
y = 0xa9320d67d944f0a2
t_{p^2} = - 0xfaca844b264dfaa353355300f9ce9d3a
p = 0x9a2a8c914e2d05c3f2616cade9b911ad
r = 0x1735ce0c4fbac46c2245c3ce9d8da0244f9059ae9ae4784d6b2f65b29c444309
c^2 = 0x40b634aec52905949ea0fe36099cb21a
with r, p prime and $\#E_{1,c}(\mathbb{F}_{p^2}) = 4r$.

We use Vélu's formulas to compute a degree-5 isogeny from $E_{1,c}$ into $E_{b,5}$. We find a 5-torsion point $P_5(X_5, Y_5)$ on $E_{1,c}(\mathbb{F}_{p^8})$. The function `IsogenyFromKernel` in Magma evaluated at $(E_{1,c}(\mathbb{F}_{p^8}), (X - X_{P_5})(X - X_{2P_5}))$ outputs a curve $E_{b,5}$ with $b_{5,4} = -25 \cdot 27(3c+10) = 5^2 a_{4,-c}$ and $b_{5,6} = 125 \cdot 108(9c+14) = 5^3 a_{6,-c}$. Hence $E_{b,5}$ and $E_{1,-c}$ are *isomorphic* over $\mathbb{F}_{p^2}$ through $i_{\sqrt{5}} : (x_{b,5}, y_{b,5}) \mapsto (x_{b,5}/5, y_{b,5}/(5\sqrt{5}))$. The above function outputs also the desired isogeny with coefficients in $\mathbb{F}_{p^2}$:

$$\begin{array}{rcl} \mathcal{I}_5 : E_{1,c}(\mathbb{F}_{p^2}) & \to & E_{b,5}(\mathbb{F}_{p^2}) \\ (x,y) & \mapsto & \left(x + \dfrac{2 \cdot 3^3 \left(\frac{3}{5}(13c+40)x + 4(27c+28)\right)}{x^2 + \frac{27}{2}cx - \frac{81}{10}c + 162} \right. \\ & & \\ & & + \dfrac{-2^3 \cdot 3^4((9c+16)x^2 + \frac{2}{5}11(27c+64)x + \frac{2}{5}3^3(53c+80)}{(x^2 + \frac{27}{2}cx - \frac{81}{10}c + 162)^2}, \\ & & \\ & & y \left(1 + \dfrac{-2^4 \cdot 3^4((9c+16)x^3 + \frac{3}{5}11(27c+64)x^2 + \frac{2}{5}3^4(53c+80)x + \frac{2}{5^2}3^2(4419c+13360))}{(x^2 + \frac{27}{2}cx - \frac{81}{10}c + 162)^3} \right. \\ & & \\ & & \left.\left. + \dfrac{2 \cdot 3^3 \left(\frac{3}{5}(13c+40)x^2 + 2^3(27c+28)x + 2\frac{3}{5}(369c+1768)\right)}{(x^2 + \frac{27}{2}cx - \frac{81}{10}c + 162)^2} \right) \right) \end{array} \tag{25}$$

We finally obtain a second computable endomorphism on $E_{1,c}$ in this example by composing $\pi_p \circ i_{\sqrt{5}} \circ \mathcal{I}_5$.

4.4 Example for $D' = 2$

Assume that curve is defined over $\mathbb{F}_{p^2}$, with $p \equiv 1 \mod 8$. Our construction gives two endomorphisms Φ_2, Φ_{-2} such that $\Phi_2^2 - 2 = 0$, $\Phi_{-2}^2 + 2 = 0$. The discriminant of the curve is $D = -4$. The curve is of the form $E_\alpha(\mathbb{F}_{p^2}) : y^2 = x^3 + \alpha x$ with $\alpha \in \mathbb{F}_{p^2}$. A 2-torsion point is $P_2(0,0)$. Vélu's formulas applied to this point give us an isogeny $(x,y) \mapsto (x + \frac{\alpha}{x}, y - y\frac{\alpha}{x^2})$ into $E_b : y^2 = x^3 - 4\alpha x$. The j-invariant of this curve is 1728 hence the curves are *isomorphic*. Applying $(x_b, y_b) \mapsto (x_b/(2i), y_b/(2i)(1+i))$ (as $(1+i)^4 = -4$) to go back in E_α does not give us the endomorphism we are looking for, this gives us $[1 + \sqrt{-1}]$ actually. We use the same trick as previously. If $\alpha \in \mathbb{F}_{p^2}$ is such that $\pi_p(\alpha) = \alpha^p = -\alpha$ (this is the case for example if $\alpha = \sqrt{a}$ with $a \in \mathbb{F}_p$ a non-square) then $(x_b, y_b) \mapsto (x_b^p/(-2), y_b^p/(-2\sqrt{-2})$ gives us the endomorphism Φ_2 and $(x_b, y_b) \mapsto (x_b^p/2, y_b^p/2\sqrt{2})$ gives us Φ_{-2}. Note that $\sqrt{-1}, \sqrt{2}, \sqrt{-2} \in \mathbb{F}_p$ since $p \equiv 1 \mod 8$. We obtain

$$\begin{array}{rcl} \Phi_2 : E_\alpha(\mathbb{F}_{p^2}) & \to & E_\alpha(\mathbb{F}_{p^2}) \\ (x,y) & \mapsto & \begin{cases} \mathcal{O} & \text{if } (x,y) = (0,0), \\ \left(\frac{(x^p)^2+\alpha}{2x^p}, \frac{y^p}{2\sqrt{2}} \left(1 - \frac{\alpha}{(x^p)^2}\right)\right) & \text{otherwise,} \end{cases} \\ \Phi_{-2} : E_\alpha(\mathbb{F}_{p^2}) & \to & E_\alpha(\mathbb{F}_{p^2}) \\ (x,y) & \mapsto & \begin{cases} \mathcal{O} & \text{if } (x,y) = (0,0), \\ \left(\frac{(x^p)^2+\alpha}{-2x^p}, \frac{y^p}{-2\sqrt{-2}} \left(1 - \frac{\alpha}{(x^p)^2}\right)\right) & \text{otherwise.} \end{cases} \end{array} \tag{26}$$

Since the j-invariant $j = 1728 \in \mathbb{F}_p$, we observe that the curve E_α is a GLS curve and is treated in [LS13, App. B]. The 4 dimensional GLV algorithm of Longa and Sica on this curve uses an endomorphism Ψ such that $\Psi^4 + 1 = 0$. With our method we obtain two distinct endomorphisms but these three ones Ψ, Φ_2, Φ_{-2} are linearly dependant on the subgroup $E(\mathbb{F}_{p^2}) \setminus E[2]$. Indeed $\Phi_2 \circ \Psi^2 = \Phi_{-2}$ (and the 2-torsion points are sent to $\mathcal{O}$).

In this case the corresponding Jacobian splits into two isogenous elliptic curves over $\mathbb{F}_p$, namely the two quartic twists defined over $\mathbb{F}_p$ of $E_{1,c}$.

5 Four dimensional GLV on $E_{2,c}(\mathbb{F}_{p^2})$

The construction of two efficiently computable endomorphisms on $E_{2,c}$, with degree of inseparability p, is similar to the one we gave for $E_{1,c}$.

We consider the elliptic curve given by eq. (12) in the reduced form:

$$E_{2,c}(\mathbb{F}_{p^2}) : y^2 = x^3 + 3(2c-5)x + c^2 - 14c + 22 \ . \tag{27}$$

We assume that $c \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, $c^2 \in \mathbb{F}_p$, c is not a cube in $\mathbb{F}_{p^2}$. In this case the isogeny (14) between $J_{\mathcal{C}_2}$ and $E_{2,c} \times E_{2,-c}$ is defined over $\mathbb{F}_{p^6}$. The 3-torsion subgroup $E_{2,c}(\mathbb{F}_{p^2})[3]$ contains the order 3 subgroup $\{\mathcal{O}, (3, c+2), (3, -c-2)\}$. We compute an isogeny whose kernel is this 3-torsion subgroup. With Vélu's formulas we obtain the curve $E_b : y^2 = x^3 - 27(2c+5)x - 27(c^2+14c+22)$. The curve E_b is isomorphic to $E_{2,-c} : (\mathbb{F}_{p^2}) : y^2 = x^3 - 3(2c+5)x + c^2 + 14c + 22$, via the isomorphism $(x, y) \mapsto (x/(-3), y/(-3\sqrt{-3})$. We define the isogeny

$$\begin{array}{rcl} \mathcal{I}_3 : E_{2,c} & \rightarrow & E_{2,-c} \\ (x,y) & \mapsto & \left(\frac{-1}{3} \left(x + \frac{12(c+2)}{x-3} + \frac{4(c+2)^2}{(x-3)^2} \right), \frac{-y}{3\sqrt{-3}} \left(1 - \frac{12(c+2)}{(x-3)^2} - \frac{8(c+2)^2}{(x-3)^3} \right) \right) \end{array} \tag{28}$$

Finally, we observe that $\pi_p(c) = -c$ and $\pi_p(j(E_{2,c})) = j(E_{2,-c})$. This implies that $E_{2,c}$ and $E_{2,-c}$ are isogenous through the Frobenius map π_p. We obtain the isogeny $\Phi_3 = \mathcal{I}_3 \circ \pi_p$ which is given by the following formula

$$\begin{array}{rcl} \Phi_3 : E_{2,c}(\mathbb{F}_{p^2}) & \rightarrow & E_{2,c}(\mathbb{F}_{p^2}) \\ (x,y) & \mapsto & \left(\frac{-1}{3} \left(x^p + \frac{12(2-c)}{x^p-3} + \frac{4(2-c)^2}{(x^p-3)^2} \right), \frac{y^p}{-3\sqrt{-3}^p} \left(1 - \frac{12(2-c)}{(x^p-3)^2} - \frac{8(2-c)^2}{(x^p-3)^3} \right) \right) \end{array} \tag{29}$$

We compute formally Φ_3^2 and obtain $\Phi_3^2 = \pi_{p^2} \circ [\pm 3]$. There is a term $\sqrt{-3}\sqrt{-3}^p$ in the y side of Φ_3^2. We observe that as $p \equiv 1 \mod 3$ here, $\left(\frac{-3}{p}\right) = 1$ and $\sqrt{-3}\sqrt{-3}^p = -3$ so $\Phi_3^2 = \pi_{p^2} \circ [-3]$. We conclude that for points in $E_{2,c}(\mathbb{F}_{p^2})$, we have

$$\Phi_3^2 + 3 = 0 \ .$$

Guillevic and Vergnaud [GV12, Theorem 2] showed that there are integers n and y such that $2q + t_{p^2} = D'y^2$ and such that $2q - t_{p^2} = 3n^2$. This implies that the complex multiplication discriminant is of the form $3D'$. As a consequence, we have the following theorem, whose proof is similar to the proof of 1.

Theorem 2. *Let $E_{2,c}$ be an elliptic curve given by equation (27), defined over $\mathbb{F}_{p^2}$. Let $-D$ be the complex multiplication discriminant and consider D' such that $D = 3D'$. There is an endomorphism $\Phi_{D'}$ of $E_{2,c}$ with degree of separability D'. The characteristic equation of this endomorphism is*

$$\Phi_{D'}^2 - D^{'} y \ \Phi_{D'} + D^{'} p \ Id = 0 \ . \tag{30}$$

We have thus proven that $\Phi = \Phi_3$ and $\Psi = \Phi_{D'}$, viewed as algebraic integers, generate different quadratic extensions of $\mathbb{Q}$. As a consequence, we obtain a four dimensional GLV algorithm on $E_{2,c}$.

5.0.1 Eigenvalues

To compute the eigenvalues of $\phi_{D'}$ and ϕ_3, we write $p = \frac{3n^2 + D^{'} y^2}{4}$, $t_{p^2} = \frac{D^{'} y^2 - 3n^2}{2}$. We obtain

$$\begin{array}{rclcrcl} \#E_{2,c}(\mathbb{F}_{p^2}) & = & (p-1)^2 - D^{'} y^2 & \rightarrow & \sqrt{D'} & \equiv & (p-1)/y \mod \#E_{2,c}(\mathbb{F}_{p^2}), \\ & = & (p+1)^2 + 3n^2 & \rightarrow & \sqrt{-3} & \equiv & (p+1)/n, \\ & = & (t_{p^2}/2 - 1)^2 + 3D^{'} (ny/2)^2 & \rightarrow & \sqrt{-3D'} & \equiv & (t_{p^2} - 2)/ny \ . \end{array}$$

The eigenvalue of ϕ_3, mod $\#E_{2,c}(\mathbb{F}_{p^2})$ is $p(p+1)/n$ and the eigenvalue of $\phi_{D'}$, mod $\#E_{2,c}(\mathbb{F}_{p^2})$ is $p(p-1)/y$.

6 Four dimensional GLV on $J_{\mathcal{C}_1}$ and $J_{\mathcal{C}_2}$

The first endomorphism Ψ on $J_{\mathcal{C}_1}$ is induced by the curve automorphism $(x, y) \to (-x, iy)$, with i a square root of -1. The characteristic polynomial is $X^2 + 1 = 1$. On $J_{\mathcal{C}_2}$ we consider Ψ the endomorphism induced by the curve automorphism $(x, y) \to (\zeta_3 x, y)$. Its characteristic equation is $X^2 + X + 1$. The second endomorphism is constructed as $\Phi = \hat{I}(\Phi_{D'}, \Phi_{D'})I$, where $\Phi_{D'}$ is the elliptic curve endomorphism constructed in Theorem 1. In order to compute the characteristic equation for Φ, we follow the lines of the proof of Theorem 1 in [GLS09]. We reproduce the computation for the Jacobian of $\mathcal{C}_1$.

Theorem 3. *Let $\mathcal{C}_1 : y^2 = x^5 + ax^3 + b$ a hyperelliptic curve defined over $\mathbb{F}_p$ with ordinary Jacobian and let r a prime number such that $r || J_{\mathcal{C}_1}(\mathbb{F}_p)$. Let $I : J_{\mathcal{C}_1} \to E_{1,c} \times E_{1,c}$ the $(2, 2)$-isogeny defined by equation (10) and assume I is defined over an extension field of degree $k > 1$. We define $\Phi = \hat{I}(\Phi_{D'} \times \Phi_{D'})I$. where $\Phi_{D'}$ is the endomorphism defined in Theorem 1. Then*

1. *For $P \in J_{\mathcal{C}_1}[r](\mathbb{F}_p)$, we have $\Phi(P) = \lambda P$, with $\lambda \in \mathbb{Z}$.*
2. *The characteristic equation of Φ is $\Phi^2 - 2D^{'}y\ \Phi + 4D^{'}p\ Id = 0$.*

Proof. 1. Note that $\mathrm{End}(J_{\mathcal{C}_1})$ is commutative, and Φ is defined over $\mathbb{F}_p$ (see [Bis11, Prop. III.1.3]). Hence, for $D \in J_{\mathcal{C}_1}(\mathbb{F}_p)$, we have that $\pi(\Phi(D)) = \Phi(\pi(D)) = \Phi(D)$. Since there is only one subgroup of order r in $J_{\mathcal{C}_1}(\mathbb{F}_p)$, we obtain that $\Phi(D) = \lambda D$.

2. Since $\hat{I}I = [2]$ then

$$\Phi^2 = \hat{I}(\phi_{D'} \times \phi_{D'})I\hat{I}(\Phi_{D'} \times \Phi_{D'})I = 2\hat{I}(\Phi^2_{D'}, \Phi^2_{D'})I. \tag{31}$$

Since $\Phi_{D'}$ verifies the equation

$$\Phi^2_{D'} - D^{'}y\ \Phi_{D'} + D^{'}p\ Id = 0, \tag{32}$$

we have

$$[2]\hat{I}((\Phi^2_{D'}, \Phi^2_{D'}) - D^{'}y\ (\Phi_{D'}, \Phi_{D'}) + D^{'}p\ (Id, Id))I = O_{J_{\mathcal{C}_1}}$$

Using equation (31), we conclude that $\Phi^2 - 2D^{'}y\ \Phi + 4D^{'}p\ Id = 0$.

□

6.1 Computing I on $J_{\mathcal{C}_1}(\mathbb{F}_p)$.

We show first how to compute explicitly the $(2, 2)$-isogeny on $J_{\mathcal{C}_1}(\mathbb{F}_p)$ with only a small number of operations over extension fields of $\mathbb{F}_p$.

Let $\mathcal{D}$ be a divisor in $J_{\mathcal{C}_1}(\mathbb{F}_p)$ given by its Mumford coordinates

$$\mathcal{D} = [U, V] = [T^2 + u_1T + u_0, v_1T + v_0],\ u_0, u_1, v_0, v_1 \in \mathbb{F}_p\ .$$

It corresponds to two points $P_1(X_1, Y_1), P_2(X_2, Y_2) \in \mathcal{C}_1(\mathbb{F}_p)$ or $\mathcal{C}_1(\mathbb{F}_{p^2})$. We have

$$u_1 = -(X_1 + X_2), u_0 = X_1X_2, v_1 = \frac{Y_2 - Y_1}{X_2 - X_1}, v_0 = \frac{X_1Y_2 - X_2Y_1}{X_1 - X_2}.$$

Explicit formula to compute $\varphi_{1*}(P_1)+\varphi_{1*}(P_2)$. Let $\varphi_{1*}(P_1) = (x_{1,1}, y_{1,1})$ and $\varphi_{1*}(P_2) = (x_{2,1}, y_{2,1})$ In the following we explicit the formulas to compute $(x_{3,1}, y_{3,1})$.

$$\begin{aligned}
x_{3,1} &= \frac{\lambda_1^2}{c+2} - (x_{1,1} + x_{2,1}) + \frac{3c-10}{c+2} \text{ with} \\
\lambda_1 &= \frac{2}{\sqrt[8]{b}} \frac{(v_0u_1 - v_1u_0)(u_1 + 3\sqrt[4]{b}) - v_0u_0 + 3\sqrt{b}v_0 + \sqrt[4]{b}^3 v_1}{(u_0 - \sqrt{b})(u_0 + \sqrt[4]{b}u_1 + \sqrt{b})}, \\
\lambda_1 &= \frac{2}{\sqrt[8]{b}} \frac{\big[(v_0u_1 - v_1u_0)u_1 - v_0u_0\big] + \big[3(v_0u_1 - v_1u_0)\big]\sqrt[4]{b} + \big[3v_0\big]\sqrt{b} + \big[v_1\big]\sqrt[4]{b}^3}{\big[u_0^2 - b\big] + \big[u_0u_1\big]\sqrt[4]{b} + \big[-u_1\big]\sqrt{b}},
\end{aligned}$$

We denote $\lambda_1 = \Lambda_1/\sqrt[8]{b}$. The computation of the numerator of Λ_1 costs $4M_p$ and the denominator costs $S_p{+}M_p$. We will use the Jacobian coordinates for S_1: $x_{3,1} = X_{3,1}/Z_{3,1}^2$, $y_{3,1} = Y_{3,1}/Z_{3,1}^3$ to avoid inversion in $\mathbb{F}_{p^4}$. We continue with

$$\begin{aligned}
x_{1,1} + x_{2,1} &= 2\frac{\big[u_0^2 + b\big] + \big[u_1^2 - 6u_0\big]\sqrt{b}}{(u_0 + \sqrt[4]{b}u_1 + \sqrt{b})^2} = 2\frac{\big(\big[u_0^2 + b\big] + \big[u_1^2 - 6u_0\big]\sqrt{b}\big)\big(u_0 - \sqrt{b}\big)^2}{(u_0 + \sqrt[4]{b}u_1 + \sqrt{b})^2(u_0 - \sqrt{b})^2} \\
&= 2\frac{\big(\big[u_0^2 + b\big] + \big[u_1^2 - 6u_0\big]\sqrt{b}\big)\big(\big[u_0^2 + b\big] + \big[-2u_0\big]\sqrt{b}\big)}{\big(\big[u_0^2 - b\big] + \big[u_0u_1\big]\sqrt[4]{b} + \big[-u_1\big]\sqrt{b}\big)^2}
\end{aligned}$$

As u_0^2 was already computed in Λ_1, this costs one square (u_1^2) and a multiplication in $\mathbb{F}_{p^2}$, hence $S_p + M_{p^2}$. The denominator is the same as the one of Λ_1^2, that is, Z_3^2.

Then

$$x_{3,1} = \frac{\Lambda_1^2}{\sqrt[4]{b}(c+2)} - (x_{1,1} + x_{2,1}) + \frac{3c-10}{c+2} = \frac{\sqrt[4]{b}\Lambda_1^2}{(a + 2\sqrt{b})} - (x_{1,1} + x_{2,1}) + \frac{3a - 10\sqrt{b}}{a + 2\sqrt{b}}$$

To avoid tedious computations, it is preferable to precompute both $1/(a + 2\sqrt{b})$ and $(3a - 10\sqrt{b})/(a + 2\sqrt{b})$ with one inversion in $\mathbb{F}_{p^2}$ and one multiplication in $\mathbb{F}_{p^2}$.

$\sqrt[4]{b}\Lambda_1^2$ is a shift to the right of the coefficients thus costs one multiplication by b as $\Lambda_1^2 \in \mathbb{F}_{p^4}$. Then $\sqrt[4]{b}\Lambda_1^2 \cdot (a + 2\sqrt{b})^{-1}$ costs $2M_{p^2}$. Finally we need to compute $\frac{3a-10\sqrt{b}}{a+2\sqrt{b}} \cdot Z_3^2$ which costs $S_{p^4} + 2M_{p^2}$. The total cost of $X_{3,1}$, $Z_{3,1}$ and $Z_{3,1}^2$ is $6M_p + 2S_p + 5M_{p^2} + S_{p^4}$.

Computing $y_{3,1}$ is quite complicated because we deal with divisors so we do not have directly the coefficients of the two points. We use this trick:

$$\begin{aligned}
y_{3,1} &= \lambda_1(x_{1,1} - x_{3,1}) - y_{1,1} \\
y_{3,1} &= \lambda_1(x_{2,1} - x_{3,1}) - y_{2,1} \\
2y_{3,1} &= \lambda_1(x_{1,1} + x_{2,1} - 2x_{3,1}) - (y_{1,1} + y_{2,1})
\end{aligned}$$

Since $x_{1,1}+x_{2,1}$ was already computed for $x_{3,1}$, getting $(x_{1,1}+x_{2,1}-2x_{3,1})$ costs only additions. We multiply the numerators of λ_1 and $(x_{1,1} + x_{2,1} - 2x_{3,1})$ which costs $1M_{p^4}$. The denominator is $Z_{3,1}^3$ and as $Z_{3,1}^2$ is already computed, this costs $1M_{p^4}$. The numerator of $(y_{1,1}+y_{2,1})$ contains products of u_0, u_1, v_0, v_1 previously computed and its denominator is simply Z_3^3. The total cost of $y_{3,1}$ is then $2M_{p^4}$. Finally, computing $(x_{3,1}, y_{3,1})$ costs

$$6M_p + 2S_p + 5M_{p^2} + S_{p^4} + 2M_{p^4} \ .$$

Now we show that computing $(x_{3,2}, y_{3,2})$ is free of cost. We notice that

$$\varphi_1(X_i, Y_i) = \varphi_2(-X_i, iY_i).$$

Rewriting this equation in terms of divisors, we derive that

$$S_2 = \varphi_{1*}([-u_1, u_0, -iv_1, iv_0]) \ .$$

We can simply compute S_2 with φ_{1*}:

$$\begin{array}{rcl} x_{3,2} & = & x_{3,1}([-u_1, u_0, -iv_1, iv_0]) \text{ with} \\ \lambda_2 & = & \lambda_1([-u_1, u_0, -iv_1, iv_0]) = \frac{2i}{\sqrt[8]{b}} \frac{(v_0u_1 - v_1u_0)(u_1 - 3\sqrt[4]{b}) - v_0u_0 + 3\sqrt{b}v_0 - \sqrt[4]{b}^3 v_1}{(u_0 - \sqrt{b})(u_0 - \sqrt[4]{b}u_1 + \sqrt{b})} = \pi_{p^2}(\lambda_1) \end{array}$$

and

$$(x_{1,1} + x_{2,1})([-u_1, u_0, -iv_1, iv_0]) = 2\frac{u_0^2 + \sqrt{b}u_1^2 - 6\sqrt{b}u_0 + b}{(u_0 - \sqrt[4]{b}u_1 + \sqrt{b})^2} = \pi_{p^2}(x_{1,1} + x_{2,1}) \ .$$

We deduce that $x_{3,2} = \pi_{p^2}(x_{3,1}),\ y_{3,2} = \pi_{p^2}(y_{3,1})$ and

$$\varphi_{2*}(\mathcal{D}) = \varphi_{2*}(P_1) + \varphi_{2*}(P_2) = \pi_{p^2}(\varphi_{1*}(P_1) + \varphi_{1*}(P_2)) \ .$$

Computing $(x_{3,2}, y_{3,2})$ costs two Frobenius π_{p^2} which are performed with four negations on $\mathbb{F}_{p^2}$.

6.2 Computing endomorphisms on $E_{1,c}$

Here we apply the endomorphism $\phi_{D'}$ on $S_1(x_{3,1}, y_{3,1})$. As $\phi_{D'}$ is defined over $\mathbb{F}_{p^2}$, it commutes with π_{p^2} hence $\phi_{D'}(x_{3,2}) = \pi_{p^2}(\phi_{D'}(x_{3,1}))$ is free. Unfortunately S_1 has coefficients in $\mathbb{F}_{p^4}$ hence we need to perform some multiplications in $\mathbb{F}_{p^4}$. More precisely, $y_{3,1}$ is of the form $\sqrt[8]{b}y'_{3,1}$ with $y'_{3,1} \in \mathbb{F}_{p^4}$. As the endomorphism is of the form $\phi_{D'}(x, y) = (\phi_{D',x}(x), y\phi_{D',y}(x))$ the $\sqrt[8]{b}y'_{3,1}$ term is not involved in the endomorphism computation.

6.3 Computing $\hat{I}$ on $J_{\mathcal{C}_1}(\mathbb{F}_p)$.

Then we go back to $J_{\mathcal{C}_1}$. In $J_{\mathcal{C}''_1}$ we have $\varphi_1^*(S_1) = (\sqrt{x_{3,1}}, y_{3,1}) + (-\sqrt{x_{3,1}}, y_{3,1}) - 2P_\infty$. We compute the divisor of these two points (with $\pm\sqrt{x_{3,1}}$) on $J_{\mathcal{C}_1}$ and get

$$\varphi_1^*(x_{3,1}, y_{3,1}) = T^2 - 2\sqrt[4]{b}\frac{x_{3,1}+1}{x_{3,1}-1}T + \sqrt{b}, \frac{\sqrt[8]{b}^3\, y_{3,1}}{2(x_{3,1}-1)}\left(\frac{x_{3,1}+3}{x_{3,1}-1}T - \sqrt[4]{b}\right)$$

If $(x_{3,1}, y_{3,1})$ is in Jacobian coordinates $(X_{3,1}, Y_{3,1}, Z_{3,1})$ then we compute $\frac{x_{3,1}+1}{x_{3,1}-1} = \frac{X_{3,1}+Z_{3,1}^2}{X_{3,1}-Z_{3,1}^2}$.

A similar computation gives

$$\varphi_2^*(x_{3,2}, y_{3,2}) = T^2 + 2\sqrt[4]{b}\frac{x_{3,2}+1}{x_{3,2}-1}T + \sqrt{b}, \frac{i\sqrt[8]{b}^3\, y_{3,2}}{2(x_{3,2}-1)}\left(\frac{x_{3,2}+3}{x_{3,2}-1}T + \sqrt[4]{b}\right) \ .$$

Since $x_{3,2} = \pi_{p^2}(x_{3,1})$ and $y_{3,2} = \pi_{p^2}(y_{3,1})$, we have

$$\varphi_2^*(x_{3,2}, y_{3,2}) = T^2 + 2\sqrt[4]{b}\frac{\pi_{p^2}(x_{3,1})+1}{\pi_{p^2}(x_{3,1})-1}T + \sqrt{b}, \frac{i\sqrt[8]{b}^3\, \pi_{p^2}(y_{3,1})}{2(\pi_{p^2}(x_{3,1})-1)}\left(\frac{\pi_{p^2}(x_{3,1})+3}{\pi_{p^2}(x_{3,1})-1}T + \sqrt[4]{b}\right) \ .$$

$$\varphi_2^*(x_{3,2}, y_{3,2}) = \pi_{p^2}(\varphi_1^*(x_{3,1}, y_{3,1}))$$

Finally,

$$\varphi_2^*(\varphi_{2*}(P_1) + \varphi_{2*}(P_2)) = \pi_{p^2}(\varphi_1^*((\varphi_{1*}(P_1) + \varphi_{1*}(P_2)))) \ .$$

and with the same arguments,

$$\varphi_2^*(\phi_{D'}(\varphi_{2*}(P_1)+\varphi_{2*}(P_2))) = \pi_{p^2}(\varphi_1^*(\phi_{D'}((\varphi_{1*}(P_1)+\varphi_{1*}(P_2))))) \ .$$

The computation of the sum $\varphi_1^*(\phi_{D'}(\varphi_{1*}(\mathcal{D}))) + \pi_{p^2} \circ \varphi_1^*(\phi_{D'}(\varphi_{1*}(\mathcal{D})))$ involves terms in $\mathbb{F}_{p^4}$ but thanks to its special form, we need to perform the operations in $\mathbb{F}_{p^2}$ only. We give the table of computations in Appendix **??** and show that most multiplications are performed over $\mathbb{F}_{p^2}$. We have followed computations for a multiplication in Mumford coordinates provided in [CL11].

We conclude that applying $\varphi_{1*}(P_1) + \varphi_{1*}(P_2)$ costs roughly as much as an addition on $J_{\mathcal{C}_1}$ over $\mathbb{F}_p$, $\varphi_{2*}(P_1) + \varphi_{2*}(P_2)$ is cost free. Computing $\phi_{D'}$ depends on the size of D' and costs few multiplications over $\mathbb{F}_{p^4}$. Finally adding $\varphi_1^* + \varphi_2^*$ costs roughly an addition of divisors over $\mathbb{F}_{p^2}$.

7 Implementation Results

We implemented both the GLV method and our four dimensional GLV on the curve $E_{1,c}/\mathbb{F}_{p^2}$ given in Example 1. We have realized a similar implementation on the a curve with discriminant -3 proposed in [LS13].

Example 2. *Let $p_1 = 2^{127} - 58309$ and $\mathbb{F}_{p_1^2} = \mathbb{F}_{p_1}[i]/(i^2+1)$. The curve $E_1/\mathbb{F}_{p_1^2}$ with Weierstrass equation $y^2 = x^3 + 9u$, where $u = i + 1$ has $\#E_1(\mathbb{F}_{p_1}) = r$, with r a 254-bit prime number. This curve has the following efficiently computable endomorphisms*

$$\Phi(x,y) = (\xi x, y) \text{ and } \Psi(x,y) = (u^{(1-p)/3}x^p, u^{(1-p)/2}y^p),$$

where $\xi^3 = 1 \bmod p_1$. These endomorphisms have equations $\Phi^2 + \Phi + 1 = 0$ and $\Psi^2 + 1 = 0$.

We use Shoup's NTL library implementation of modular arithmetic, and our own implementation of degree 2 extension fields $\mathbb{F}_p[X]/(X^2 + \alpha)$, with α a very small constant (i.e. 1,2,3). Our purpose was to compare the performance of generic algorithms on the families of curves we propose. Further optimizations are of course possible: using sliding windows or wNAF for the scalar multiplication, choosing p a generalized Mersenne prime number in order to get a fast modular reduction algorithm. The computation of scalar decompositions is done by performing once and for all a BKZ-reduced basis of the matrix corresponding to proper values of endomorphisms. For that, we used the BKZ routine available in NTL. In practice, the decomposition stage performs well, all mini-scalars k_i in the decomposition of a 256 bit integer k have bit length at most 64.

We give in Table 7 the operation count of a computation of one scalar multiplication using two dimensional and four dimensional GLV on E and E_1. We denote by m, s and by M, S the cost of multiplication and squaring over $\mathbb{F}_{p^2}$ and over $\mathbb{F}_p$, respectively. We denote by c the cost of multiplication by a constant in $\mathbb{F}_{p^2}$. In order to give global estimates, we will assume that $M \sim S$ and that $m \sim 3M$ and $s \sim 3S$. As $\log p = 128$ and we run our benchmarks on a 64-bit processor, this estimation is rough. Additions in $\mathbb{F}_p$ are not completely negligible compared to multiplications. We used formulae from Lange's database [Lan] to implement addition and squaring in projective coordinates. On the curve $E_{1,c}$ addition costs $12m + 2s$, while squaring costs $5s + 6m + 1c$. For E' , addition costs $12m + 2s$, while doubling is $3m + 5s + 1c$. Note that by using Montgomery's simultaneous inversion method, we could also obtain all points in the look up table in affine coordinates and use mixed additions for the addition step of the scalar multiplication algorithm. This variant adds one inversion and $3(n-1)$ multiplications, where n is the length of the look-up table. We believe this is interesting for implementations of cryptographic applications which need to perform several scalar multiplications. For genus 2 arithmetic on curves of the form $y^2 = x^5 + ax^3 + bx$, we used formulae given by Costello and Lauter [CL11] in projective coordinates. An addition costs $43m + 4s$ and doubling costs $30m + 9s$.

Table 2: Total cost of scalar multiplication at 128 bit security level

Curve	Method	Operation count	Global estimation
$E_{1,c}$	4-GLV	$1168m + 440s$	$4797M$
E_1 [LS13]	4-GLV	$976m + 440s$	$4248M$
$E_{1,c}$	2-GLV	$2048m + 832s$	$8640M$
E_1	2-GLV	$1664m + 832s$	$7488M$
$J_{\mathcal{C}_1}$	4-GLV	$4500M + 816S$	$5316M$
$J_{\mathcal{C}_1}$	2-GLV	$7968M + 1536S$	$9504M$
FKT [BCHL13]	4-GLV	$4500M + 816S$	$5316M$
Kummer [BCHL13]	2-GLV	$2176M$+$1152S$	$3328M$

Our tests were run on a 2.67 GHz Intel Core i5-750 processor, with four cores. Our benchmarks in Table 7 show that practical results follow closely theoretical estimates. The practical gain of the 4 dimensional GLV on $E_{1,c}$, when compared to the 2 dimensional GLV implementation, is of 47%. Curves with discriminant -3, defined over $\mathbb{F}_{p_1^2}$, which belong both to the family of curves we propose and to the one proposed by Longa and Sica, offer a 15% speed-up, thanks to their efficient arithmetic. The difference between theory and practice between elliptic curves defined $\mathbb{F}_{p^2}$ and Jacobians defined over $\mathbb{F}_p$ comes from from the fact that we did not count the extra cost of additions over $\mathbb{F}_p$ performed for a Karatsuba multiplication. We do not dispose of an implementation on the arithmetic of Kummer surfaces and we were not able to compare ourselves to all current proposals of genus 2 Jacobians with efficient scalar multiplication arithmetic. Our aim is not to break records, but simply to improve the state of the art on families of abelian varieties allowing efficient implementation of 4 dimensional GLV. It would be also interesting to see whether the $J_{\mathcal{C}_1}$ and $J_{\mathcal{C}_2}$ families yield any interesting cryptographic examples of Kummer surfaces defined over $\mathbb{F}_p$ with efficient scalar multiplication.

Table 3: Benchmarks for scalar multiplication at 128 security level

Curve	Method	Time in ms.
$E_{1,c}$	4-GLV, 16 pts.	2.202
E_1	4-GLV, 16 pts.	1.882
$E_{1,c}$	2-GLV, 4pts.	4.070
$J_{\mathcal{C}_1}$	4-GLV, 4 pts.	1.831

8 Conclusion

We have studied two families of elliptic curves defined over $\mathbb{F}_{p^2}$ which have the property that the Weil restriction is isogenous over $\mathbb{F}_p$ to the Jacobian of a genus 2 curve. We have proposed a four dimensional GLV algorithm on these families of elliptic curves and on the corresponding Jacobians of genus 2 curves. Our benchmarks show that these abelian varieties offer efficient scalar multiplication, competitive to GLV algorithms on other families in the literature, having two efficiently computable and independent endomorphisms.

References

[BCHL13] JoppeW. Bos, Craig Costello, Huseyin Hisil, and Kristin Lauter. Fast cryptography in genus 2. In Thomas Johansson and PhongQ. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 194–210. Springer Berlin Heidelberg, 2013.

[Bis11] Gaetan Bisson. Endomorphism rings in cryptography, 2011.

[CL11] Craig Costello and Kristin Lauter. Group law computations on jacobians of hyperelliptic curves. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography*, volume 7118 of *LNCS*, pages 92–117. Springer, 2011.

[Dew95] L. Dewaghe. Un corollaire aux formules de Vélu. Draft, 1995.

[DK05] Ivan Duursma and N. Kiyavash. The vector decomposition problem for elliptic and hyperelliptic curves. *Journal of the Ramanujan Mathematical Society*, 20(1):59–76, 2005.

[FS11] David Mandell Freeman and Takakazu Satoh. Constructing pairing-friendly hyperelliptic curves using Weil restriction. *J. Number Theory*, 131(5):959–983, 2011.

[GLS09] Steven Galbraith, Xibin Lin, and Michael Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. In Antoine Joux, editor, *Advances in Cryptology –* EUROCRYPT *2009*, volume 5479 of *Lect Notes Comput. Sci.* Springer, 2009.

[GLV01] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In Joe Kilian, editor, *CRYPTO*, volume 2139 of *LNCS*, pages 190–200. Springer, 2001.

[GS01] Pierrick Gaudry and Éric Schost. On the invariants of the quotients of the jacobian of a curve of genus 2. In Serdar Boztas and Igor Shparlinski, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 2001*, volume 2227 of *Lect Notes Comput. Sci.*, pages 373–386. Springer, 2001.

[GV12] Aurore Guillevic and Damien Vergnaud. Genus 2 hyperelliptic curve families with explicit jacobian order evaluation and pairing-friendly constructions. In *Pairing*, pages 234–253, 2012.

[Koh96] David Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California at Berkeley, 1996.

[Lan] Tanja Lange. Explicit-formulas database. http://www.hyperelliptic.org/EFD/.

[Ler97] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis.* PhD thesis, École Polytechnique, 1997.

[LM97] F. Leprévost and F. Morain. Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. *J. Number Theory*, 64:165–182, 1997.

[LS13] Patrick Longa and Francesco Sica. Four dimensional gallant-lambert-vanstone scalar multiplication. *Journal of Cryptology*, pages 1–36, 2013.

[Sat09] Takakazu Satoh. Generating genus two hyperelliptic curves over large characteristic finite fields. In Antoine Joux, editor, *Advances in Cryptology –* EUROCRYPT *2009*, volume 5479 of *Lect Notes Comput. Sci.* Springer, 2009.

A Appendix 1

In this section we denote by m_n and s_2 the cost of multiplication and of a squaring, respectively, in an extension field $\mathbb{F}_{p^n}$.

$\sigma_1 = u_1 + \pi_{p^2}(u_1)$, $\Delta_0 = v_0 - \pi_{p^2}(v_0)$, $\Delta_1 = v_1 - \pi_{p^2}(v_1)$, $U_1 = u_1^2$ $(1m_4)$
$M_1 = u_1^2 - \pi_{p^2}(u_1^2)$,$M_2 = \sqrt{b}(\pi_{p^2}(u_1) - u_1)$
$M_3 = u_1 - \pi_{p^2}(u_1)$, $l_2 = t_1 - t_2$; $l_3 = \Delta_0 * M_3$; $d = M_1 * M_2 - 2M_2 * (M_1 + M_3)$; $(3m_2)$
$A = 1/(d * l3)$; $B = d * A$; $C = d * B$; $D = l_2 * B$; $(4m_2)$
$E = l_3^2 * A$; $CC = C^2$; $u_1'' = 2 * D - CC - \sigma_1$ $(2m_2$+$1s_2)$
$u_0'' = D^2 + C * (v_1 + \pi_{p^2}(v_1)) - ((u_1'' - CC) * \sigma_1 + (U_1 + \pi_{p^2}(U_1)))/2$ $(2m_2)$
$U_0'' = u_1' * u_0''$; $v_1'' = D * (u_1 - u_1'') + u_1^{2''} - u_0'' - u_1^2$; $(2m_4)$
$v_0'' = D * (u_0 - u_0'') + U_0''$;$v_1'' = -(E * v_1'' + v_1)$; $v_0'' = -(E * v_0'' + v_0)$; $(3m_2)$