Four-Dimensional GLV via the Weil Restriction

Aurore Guillevic, Sorina Ionica

Four-Dimensional GLV via the Weil Restriction

Aurore Guillevic[1,2] and Sorina Ionica[1]

[1] Crypto Team – DI – École Normale Supérieure
45 rue d'Ulm – 75230 Paris Cedex 05 – France
[2] Laboratoire Chiffre – Thales Communications and Security
4 avenue des Louvresses – 92622 Gennevilliers Cedex – France
aurore.guillevic@ens.fr sorina.ionica@m4x.org

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 endomorphisms 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 operations used in curve-based cryptography. Various techniques were introduced to speed-up the scalar multiplication. Firstly there exist exponent-recoding techniques such as sliding window and Non-Adjacent-Form representation [7]. 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 [11] 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

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

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 [10] presented a 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 $\psi^2+1=0$ when restricted to points defined over $\mathbb{F}_{p^2}$. 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 $|k_i| < Cr^{1/4}$, $i = 1, \ldots, 4$. 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 [3] 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.

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 Φ satisfying $\Phi^2 \pm 2 = 0$ 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 Φ such that $\Phi^2 + 3 = 0$ 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 the endomorphisms on $E_{1,c}$ and $E_{2,c}$.

At last, we study genus 2 curves whose equations are $\mathcal{C}_1 : Y^2 = X^5 + aX^3 + bX$ and $\mathcal{C}_2 : Y^2 = X^6 + aX^3 + b$, with $a, b \in \mathbb{F}_p$. 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 [18] and Freeman and Satoh [9], 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 the $(2,2)$-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. In Section 2 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 3 and 4 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 5 explains how to obtain a four-dimensional GLV method on the Jacobians of $\mathcal{C}_1$ and $\mathcal{C}_2$. Finally, in Section 6, our operation count at the 128 bit security level is proof 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 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

$$\mathcal{C}_1(\mathbb{F}_p) : Y^2 = X^5 + aX^3 + bX, \text{ with } a, b \neq 0 \in \mathbb{F}_p \ . \tag{1}$$

It was shown [15,18,9, §2, §3, §4.1] that the Jacobian of $\mathcal{C}_1$ is isogenous to $E_{1,c} \times E_{1,c}$, where

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

with $c = a/\sqrt{b}$. We recall the formulae for the cover maps from $\mathcal{C}_1$ to $E_{1,c}$. The reader is referred to the proof of Prop. 4.1 in [9] for details of the computations.

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

where $i = \sqrt{-1} \in \mathbb{F}_p$ or $\mathbb{F}_{p^2}$. The $(2,2)$-isogeny is given by

$$\begin{array}{c} I : J_{\mathcal{C}_1} \to E_{1,c} \times E_{1,c} \\ P + Q - 2P_\infty \mapsto (\varphi_{1*}(P) + \varphi_{1*}(Q), \varphi_{2*}(P) + \varphi_{2*}(Q)) \end{array} \tag{4}$$

and its dual is

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

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 [14, 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 [8] and by Gaudry and Schost [12].

$$\mathcal{C}_2(\mathbb{F}_p) : Y^2 = X^6 + aX^3 + b \text{ with } a, b \neq 0 \in \mathbb{F}_p \ . \tag{5}$$

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

$$E_{2,c}(\mathbb{F}_p[\sqrt{b}]) : y^2 = (c+2)x^3 + (-3c+30)x^2 + (3c+30)x + (-c+2) \tag{6}$$
$$E_{2,-c}(\mathbb{F}_p[\sqrt{b}]) : y^2 = (-c+2)x^3 + (3c+30)x^2 + (-3c+30)x + (c+2), \tag{7}$$

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 [9, Prop. 4].

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

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

3 Four-dimensional GLV on $E_{1,c}$

In this section, we construct two endomorphisms which may be used to compute scalar multiplication on $E_{1,c}$ using a 4-dimensional GLV algorithm. We assume that $c \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $c^2 \in \mathbb{F}_p$.

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

We aim to compute a 2-isogeny on $E_{1,c}(\mathbb{F}_{p^2})$. First we reduce the equation (2) of $E_{1,c}$ to

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

through the change of variables $(x,y) \mapsto (3(c+2)x - (3c-10), (c+2)y)$. Note that we can write

$$E_{1,c}(\mathbb{F}_{p^2}) : y^2 = (x-12)(x^2 + 12x + 81c - 126). \tag{10}$$

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 [20,6,14] 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

$$E_{1,-c}(\mathbb{F}_{p^2}) : y^2 = x^3 + 27(-3c - 10)x + 108(14 + 9c) \tag{11}$$

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

$$\begin{aligned} \mathcal{I}_2 : E_{1,c}(\mathbb{F}_{p^2}) &\to E_{1,-c}(\mathbb{F}_{p^2}) \\ (x, y) &\mapsto \left(\tfrac{-x}{2} + \tfrac{162+81c}{-2(x-12)}, \tfrac{-y}{2\sqrt{-2}} \left(1 - \tfrac{162+81c}{(x-12)^2} \right) \right). \end{aligned} \tag{12}$$

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

$$\pi_p(c) = c^p = -c, \ \pi_p(j(E_{1,c})) = j(E_{1,-c}) \tag{13}$$

hence the curves $E_{1,c}$ and $E_{1,-c}$ 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, by composing $\pi_p \circ \mathcal{I}_2$, we obtain an efficiently computable endomorphism Φ_2 as follows:

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

If we compute formally[3] 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 $\sqrt{-2} \in \mathbb{F}_p$ or $\pi_{p^2} \circ [2]$ if $\sqrt{-2} \notin \mathbb{F}_p$. This difference occurs because a term $\sqrt{-2}\sqrt{-2}^p$ appears in the formula. If $p \equiv 1, 3 \mod 8$, $\sqrt{-2}^p = \sqrt{-2}$ and if $p \equiv 5, 7 \mod 8$, $\sqrt{-2}^p = -\sqrt{-2}$. Hence Φ_2 restricted to points defined over $\mathbb{F}_{p^2}$ verifies the equation

$$\Phi_2^2 \pm 2 = 0. \tag{14}$$

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 explicit method to compute such an endomorphism.

[3] e.g. Verification code with Maple can be found at the address `http://www.di.ens.fr/~ionica/VerificationMaple-Isogeny-2p-E1.maple`

Two-dimensional GLV. By using Id and Φ_2, we get a two-dimensional GLV algorithm on the curve $E_{1,c}$. Smith [19] constructs families of 2-dimensional GLV curves by reducing mod p $\mathbb{Q}$-curves defined over quadratic number fields. $\mathbb{Q}$-curves are curves without complex multiplication with isogenies towards all their Galois conjugates. Since we are interested into designing a fast higher dimensional algorithm, we will study curves with small complex multiplication discriminant. In this purpose, our curves are constructed using the complex multiplication method. For a discussion on the advantages of using dimension 2 curves, see [19].

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

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. $\sqrt{-D}$). Guillevic and Vergnaud [13, proof of Th. 1 (4.) §2.2] showed that $D = 2D'$, for some integer D'. Let t_{p^2} be the trace of $E_{1,c}(\mathbb{F}_{p^2})$. The equation of the complex multiplication is then

$$(t_{p^2})^2 - 4p^2 = -2D'\gamma^2, \tag{15}$$

for some $\gamma \in \mathbb{Z}$. 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.

Lemma 1. *There are integers m and n such that if $p \equiv 1, 3 \pmod 8$, then*

$$t_{p^2} + 2p = D^{'} m^2 \text{ and } t_{p^2} - 2p = -2n^2. \tag{16}$$

and if $p \equiv 5, 7 \pmod 8$, then

$$t_{p^2} + 2p = 2n^2 \text{ and } t_{p^2} - 2p = -D^{'} m^2. \tag{17}$$

Moreover, the characteristic equation of Φ_2 is

$$\Phi_2^2 - 2n\Phi_2 + 2p\mathrm{Id} = 0\ . \tag{18}$$

Proof. We have that $\mathrm{Tr}(\Phi_2^2) - \mathrm{Tr}^2(\Phi_2) + 2\deg(\Phi_2) = 0$. 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 $p \equiv 1, 3 \mod 8$, $\mathrm{Tr}(\Phi_2^2) = \mathrm{Tr}(\pi_{p^2} \circ [-2]) = -2t_{p^2}$ and we get $\mathrm{Tr}^2(\Phi_2) = -2t_{p^2} + 4p = -2(t_{p^2} - 2p)$. We may thus write $t_{p^2} - 2p = -2n^2$, for some integer n. If $p \equiv 5, 7 \mod 8$, $\mathrm{Tr}(\Phi_2^2) = \mathrm{Tr}(\pi_{p^2} \circ [2]) = 2t_{p^2}$ and we get $\mathrm{Tr}^2(\phi_2) = 2t_{p^2} + 4p = 2(t_{p^2} + 2p)$. Hence $t_{p^2} + 2p = 2n^2$ again. Using the complex multiplication equation (15), we have that there is an integer m such that $t_{p^2} + 2p = D'm^2$, if $p \equiv 1, 3 \pmod 8$ and $t_{p^2}^2 - 2p = -D'm^2$, if $p \equiv 5, 7 \pmod 8$. Using these notations, the characteristic equation of Φ_2 is

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

Theorem 1. *Let $E_{1,c}$ be an elliptic curve given by equation* (10)*, defined over $\mathbb{F}_{p^2}$. 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*

$$\Phi_{D'}^2 - D^{'} m \; \Phi_{D'} + D^{'} p \; \mathrm{Id} = 0 \; . \tag{19}$$

Proof. Since $D = 2D'$, we have that Φ_D is the composition of a horizontal isogeny of degree 2 with a horizontal[4] isogeny of degree D'. We denote by $\mathcal{I}_2 : E_{1,c} \to E_{1,-c}$ the isogeny given by equation (12). 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 $\Phi_D = \mathcal{I}_{D'} \circ \mathcal{I}_2$, 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

$$\Phi_{D'} \circ \Phi_2 = \Phi_D \circ \pi_{p^2}.$$

Hence, by using equation (18), we obtain that $\Phi_{D'}$ seen as algebraic integer in $\mathbb{Z}[\sqrt{-D}]$ is $\frac{-D'm \pm n\sqrt{-2D'}}{2}$. Hence we have $\Phi_{D'}^2 - D^{'} m \; \Phi_{D'} + D^{'} p \; \mathrm{Id} = 0$.

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 $\mathbb{F}_{p^2}$.

Four-dimensional GLV algorithm. Assume that $E_{1,c}$ is such that $\#E_{1,c}(\mathbb{F}_{p^2})$ is divisible by a large prime 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 $[k]P$ 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 [16].

Eigenvalue computation. From equation (14), we deduce that the eigenvalue of Φ_2 is $p\sqrt{-2}$ if $p \equiv 1.3 \mod 8$ and $p\sqrt{2}$ if $p \equiv 5, 7 \mod 8$. We explain how to compute this eigenvalue mod $\#E_{1,c}(\mathbb{F}_{p^2})$. We will use the formulas (16) and (1).

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

If $p \equiv 1, 3 \mod 8$, we obtain

$$\begin{aligned} \#E_{1,c}(\mathbb{F}_{p^2}) &= (p+1)^2 - D^{'}m^2 && \rightarrow \quad \sqrt{D'} \equiv (p+1)/m \\ &= (p-1)^2 + 2n^2 && \rightarrow \quad \sqrt{-2} \equiv (p-1)/n, \\ &= (1 - t_{p^2}/2)^2 + 2D^{'}(nm/2)^2 && \rightarrow \sqrt{-2D'} \equiv (2 - t_{p^2})/(nm)\ . \end{aligned}$$

If $p \equiv 5, 7 \mod 8$, we obtain

$$\begin{aligned} \#E_{1,c}(\mathbb{F}_{p^2}) &= (p-1)^2 + D^{'}m^2 && \rightarrow \quad \sqrt{-D'} \equiv (p-1)/m \\ &= (p+1)^2 - 2n^2 && \rightarrow \quad \sqrt{2} \equiv (p+1)/n, \\ &= (1 - t_{p^2}/2)^2 + 2D^{'}(nm/2)^2 && \rightarrow \sqrt{-2D'} \equiv (2 - t_{p^2})/(nm)\ . \end{aligned}$$

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 $p \equiv 1, 3 \mod 8$ or $p\sqrt{2} \equiv p(p+1)/n \mod \#E_{1,c}(\mathbb{F}_{p^2})$ if $p \equiv 5, 7 \mod 8$.

The eigenvalue of $\Phi_{D'}$ on $E_{1,c}(\mathbb{F}_{p^2})$ is $p\sqrt{D'} \equiv p(p+1)/m \mod \#E_{1,c}(\mathbb{F}_{p^2})$ if $p \equiv 1, 3 \mod 8$ or $p\sqrt{-D'} \equiv p(p-1)/m \mod \#E_{1,c}(\mathbb{F}_{p^2})$ if $p \equiv 5, 7 \mod 8$.

3.3 Curve construction and examples

We construct curves $E_{1,c}$ with good cryptographic properties (i.e. a large prime divides the number of points of $E_{1,c}$ over $\mathbb{F}_{p^2}$) by using the complex multiplication algorithm. More precisely, we look for prime numbers p such that the complex multiplication equation

$$4p = 2n^2 + D'm^2$$

is verified. Once p is found, we compute the roots of the Hilbert polynomial in $\mathbb{F}_{p^2}$ to get the j-invariant of the curve $j(E_{1,c})$. We finally get the value of c by solving $j(E_{1,c}) = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}$ in $\mathbb{F}_{p^2}$ and choosing a solution satisfying $c^2 \in \mathbb{F}_p$.

We note that for a bunch of discriminants (such as $-20, -24, -36$ etc.), Hilbert polynomial precomputation may be avoided by using parameterizations computed by Quer [17]:

$$C_t : y^2 = x^3 - 6(5 + 3\sqrt{t})x + 8(7 + 9\sqrt{t}), \tag{20}$$

for some $t \in \mathbb{Q}$. For instance $t = \frac{5}{4}$ for $D = -20$, $t = \frac{8}{9}$ for $D = -24$ etc. Once p is found, one may directly reduce mod p the curve given by equation 20. Curves given by equation (20) are $\mathbb{Q}$-curves and for these discriminants, we obtain the same curves as in [19].

Complex multiplication algorithms may not be avoided in certain cryptographic frames, such as pairing-friendly constructions. One advantage of the construction is that one has the liberty to choose the value r of the large prime number dividing the curve group order. This helps in preventing certain attacks, such as Cheon's attack [4] on the q-DH assumption. On the negative side, we cannot construct curves with fixed p (such as the attractive $2^{127} - 1$).

Using Magma, we computed an example with $p \equiv 5 \mod 8$, $D = 40$, $D^{'} = 20$.

Example 1. We first search 63-bit numbers n, m such that $p = (2n^2 + 20m^2)/4$ 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 a few seconds, we find the following parameters.

n = 0x55d23edfa6a1f7e4
m = 0x549906b3eca27851
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 $E_{b,5} : y_b^2 = x_b^3 - 25 \cdot 27(3c + 10)x_b + 125 \cdot 108(9c + 14)$. The curve E_b is isomorphic to $E_{1,-c}$ over $\mathbb{F}_{p^2}$ through $i_{\sqrt{5}} : (x_b, y_b) \mapsto (x_b/5, y_b/(5\sqrt{5}))$. The above function outputs also the desired isogeny with coefficients in $\mathbb{F}_{p^2}$:

$$
\begin{aligned}
\mathcal{I}_5 : \\
E_{1,c}(\mathbb{F}_{p^2}) &\to E_{b,5}(\mathbb{F}_{p^2}) \\
(x, y) &\mapsto \Bigg(x + \frac{2\cdot 3^3\left(\frac{3}{5}(13c+40)x+4(27c+28)\right)}{x^2+\frac{27}{2}cx-\frac{81}{10}c+162} \\
&\quad + \frac{-2^3\cdot 3^4((9c+16)x^2+\frac{2}{5}11(27c+64)x+\frac{2}{5}3^3(53c+80)}{(x^2+\frac{27}{2}cx-\frac{81}{10}c+162)^2}, \\
&\quad y\left(1 + \frac{-2^4\cdot 3^4((9c+16)x^3+\frac{3}{5}11(27c+64)x^2+\frac{2}{5}3^4(53c+80)x+\frac{2}{5^2}3^2(4419c+13360))}{(x^2+\frac{27}{2}cx-\frac{81}{10}c+162)^3}\right. \\
&\quad \left. + \frac{2\cdot 3^3\left(\frac{3}{5}(13c+40)x^2+2^3(27c+28)x+2\frac{3}{5}(369c+1768)\right)}{(x^2+\frac{27}{2}cx-\frac{81}{10}c+162)^2}\right)\Bigg)
\end{aligned}
\tag{21}
$$

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 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. (6) in the reduced form:

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

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 (8) 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 $(x, y) \mapsto \big(x/(-3), y/(-3\sqrt{-3})\big)$. We define the isogeny

$$\begin{array}{l} \mathcal{I}_3 : E_{2,c} \to E_{2,-c} \\ \quad (x, y) \mapsto \left(\frac{-1}{3} \left(x + \frac{12(c+2)}{x-3} + \frac{4(c+2)^2}{(x-3)^2} \right), \frac{-y}{3\sqrt{-3}} \left(1 - \frac{12(c+2)}{(x-3)^2} - \frac{8(c+2)^2}{(x-3)^3} \right) \right). \end{array}$$

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

$$\begin{array}{l} \Phi_3 : \\ E_{2,c}(\mathbb{F}_{p^2}) \to E_{2,c}(\mathbb{F}_{p^2}) \\ \quad (x, y) \mapsto \left(\frac{-1}{3} \left(x^p + \frac{12(2-c)}{x^p-3} + \frac{4(2-c)^2}{(x^p-3)^2} \right), \frac{y^p}{-3\sqrt{-3}^p} \left(1 - \frac{12(2-c)}{(x^p-3)^2} - \frac{8(2-c)^2}{(x^p-3)^3} \right) \right). \end{array}$$

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 if $p \equiv 1 \mod 3$, then $\left(\frac{-3}{p}\right) = 1$, $\sqrt{-3}\sqrt{-3}^p = -3$ and $\Phi_3^2 = \pi_{p^2} \circ [-3]$. Similarly, if $p \equiv 2 \mod 3$, then $\Phi_3^2 = \pi_{p^2} \circ [3]$. We conclude that for points defined over $\mathbb{F}_{p^2}$, we have

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

Guillevic and Vergnaud [13, Theorem 2] showed that the complex multiplication discriminant is of the form $3D'$. With the same arguments as for $E_{1,c}$, we deduce that there are integers m and n such that if $p \equiv 1 \pmod 3$, then

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

and if $p \equiv 2 \pmod 3$, then

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

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 (22), 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*

$$\Phi_{D'}^2 - D' m \ \Phi_{D'} + D' p \ \mathrm{Id} = 0 \ . \tag{23}$$

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 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 [10]. We reproduce the computation for the Jacobian of $\mathcal{C}_1$.

Theorem 3. *Let $\mathcal{C}_1 : y^2 = x^5 + ax^3 + b$ be 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 (4) 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 $\Phi^2 - 2D^{'}m\ \Phi + 4D^{'}p\ \mathrm{Id} = 0$.*

Proof. 1. Note that $\mathrm{End}(J_{\mathcal{C}_1})$ is commutative, and Φ is defined over $\mathbb{F}_p$ (see [2, Prop. III.1.3]). Hence, for $\mathcal{D} \in J_{\mathcal{C}_1}(\mathbb{F}_p)$, we have that $\pi(\Phi(\mathcal{D})) = \Phi(\pi(\mathcal{D})) = \Phi(\mathcal{D})$. Since there is only one subgroup of order r in $J_{\mathcal{C}_1}(\mathbb{F}_p)$, we obtain that $\Phi(\mathcal{D}) = \lambda\mathcal{D}$.

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

$$\Phi^2 = \hat{I}(\Phi_{D'} \times \Phi_{D'})I\hat{I}(\Phi_{D'} \times \Phi_{D'})I = 2\hat{I}(\Phi_{D'}^2, \Phi_{D'}^2)I. \tag{24}$$

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

$$\Phi_{D'}^2 - D^{'}m\ \Phi_{D'} + D^{'}p\ \mathrm{Id} = 0, \tag{25}$$

we have

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

Using equation (24), we conclude that $\Phi^2 - 2D^{'}m\ \Phi + 4D^{'}p\ \mathrm{Id} = 0$.

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

We show first how to compute stately 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 give the formulas to compute $S_1(x_{3,1},y_{3,1})=\varphi_{1*}(P_1)+\varphi_{1*}(P_2)$.

$$x_{3,1}=\tfrac{\lambda_1^2}{c+2}-(x_{1,1}+x_{2,1})+\tfrac{3c-10}{c+2} \text{ with}$$

$$\lambda_1=\tfrac{2}{\sqrt[8]{b}}\tfrac{\left[(v_0u_1-v_1u_0)u_1-v_0u_0\right]+\left[3(v_0u_1-v_1u_0)\right]\sqrt[4]{b}+\left[3v_0\right]\sqrt{b}+\left[v_1\right]\sqrt[4]{b}^3}{\left[u_0^2-b\right]+\left[u_0u_1\right]\sqrt[4]{b}+\left[-u_1\right]\sqrt{b}}.$$

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

$$x_{1,1}+x_{2,1}=2\tfrac{\left(\left[u_0^2+b\right]+\left[u_1^2-6u_0\right]\sqrt{b}\right)\left(\left[u_0^2+b\right]+\left[-2u_0\right]\sqrt{b}\right)}{\left(\left[u_0^2-b\right]+\left[u_0u_1\right]\sqrt[4]{b}+\left[-u_1\right]\sqrt{b}\right)^2}$$

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

$$\begin{aligned}x_{3,1}&=\tfrac{\Lambda_1^2}{\sqrt[4]{b}(c+2)}-(x_{1,1}+x_{2,1})+\tfrac{3c-10}{c+2}\\&=\tfrac{\sqrt[4]{b}\Lambda_1^2}{(a+2\sqrt{b})}-(x_{1,1}+x_{2,1})+\tfrac{3a-10\sqrt{b}}{a+2\sqrt{b}}.\end{aligned}$$

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 $\mathbb{F}_{p^2}$.

Computing $\sqrt[4]{b}\Lambda_1^2$ is done by shifting to the right coefficients and 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 $S_2(x_{3,2}, y_{3,2})$ is free of cost. We notice that

$$\varphi_1(X_j, Y_j) = \varphi_2(-X_j, iY_j)$$

with i such that $i^2 = -1$ and $j \in \{1, 2\}$. Rewriting this equation in terms of divisors, we derive that

$$S_2(x_{3,2}, y_{3,2}) = \varphi_{1*}([-u_1, u_0, -iv_1, iv_0]) \ .$$

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

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

and

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

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 $\mathbb{F}_{p^2}$.

5.2 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.

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

Then we go back to $J_{\mathcal{C}_1}$. We compute the divisor of these two points (with $\pm\sqrt{x_{3,1}}$) on $J_{\mathcal{C}_1}$ and get

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

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

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

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

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

Hence $\varphi_2^*(x_{3,2}, y_{3,2}) = \pi_{p^2}(\varphi_1^*(x_{3,1}, y_{3,1}))$.
Finally, we have

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

and, with similar 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 A and show that most multiplications are performed over $\mathbb{F}_{p^2}$. We have followed computations for a multiplication in Mumford coordinates provided in [5].

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 $\mathbb{F}_{p^2}$.

6 Complexity analysis and comparison to GLS-GLV curves

We explain that our construction is valid for GLS curves with discriminants -3 and -4. These curves are particularly interesting for cryptography, because their simple equation forms result into simple and efficient point additions. A four-dimensional GLV algorithm on these curves was proposed by Longa and Sica [16]. Although the endomorphisms we construct do not allow to derive a higher dimension algorithm, they offer an alternative to Longa and Sica's construction.

The case $D = -4$. We consider a curve with CM discriminant $D = -4$, defined over $\mathbb{F}_{p^2}$, with $p \equiv 1 \mod 8$. Assume that 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 $P_2(0, 0)$. Using Vélu's formulas, we get the isogeny with kernel generated by P_2, whose equation is

$$(x, y) \mapsto \left(x + \frac{\alpha}{x}, y - y\frac{\alpha}{x^2}\right) .$$

This isogeny sends points on E_α on the curve $E_b : y^2 = x^3 - 4\alpha x$. 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 by composing with $(x_b, y_b) \mapsto \left(x_b^p/(-2), y_b^p/(-2\sqrt{-2})\right)$, we get an endomorphism Φ_2. Note that $\sqrt{-1} \in \mathbb{F}_p$ since $p \equiv 1 \mod 8$. We obtain

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

We obtained an endomorphism Φ_2 such that $\Phi_2^2 - 2 = 0$, when restricted to points defined over $\mathbb{F}_{p^2}$. The complex multiplication endomorphism Φ on E_α is $(x, y) \to (-x, iy)$ and verifies the equation $\Phi^2 + 1 = 0$. 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 the three ones Ψ, Φ_2, Φ are not "independent" on the subgroup $E(\mathbb{F}_{p^2}) \setminus E[2]$. Indeed, we have $\Phi_2 + \Phi\Phi_2 = 2\Psi$.

Note that 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 $E_{1,c}$.

The case $D = -3$. We consider the curve E_β whose Weierstrass equation is

$$y^2 = x^3 + \beta, \tag{26}$$

where $\beta^2 \in \mathbb{F}_p$. Our construction yields the following efficiently computable endomorphism

$$\Phi_3(x, y) = \left(\frac{1}{3}\left(x^p + \frac{4\beta^p}{x^{2p}}\right), \frac{y^p}{\sqrt{3}}\left(1 + \frac{8\beta^p}{x^{3p}}\right)\right).$$

When restricted to points defined over $\mathbb{F}_{p^2}$, this endomorphism verifies the equation $\Phi_3^2 - 3 = 0$, while the complex multiplication endomorphism Φ has characteristic equation $\Phi^2 + \Phi + 1 = 0$. Longa and Sica's algorithm uses the complex multiplication Φ and an endomorphism Ψ verifying $\Psi^2 + 1 = 0$ for points defined over $\mathbb{F}_{p^2}$. We observe that $2\Phi_3\Psi - 1 = 2\Phi$.

We give in Table 6 the operation count of a computation of one scalar multiplication using two-dimensional and four-dimensional GLV on E and E_β given by equation (26). We denote by m, s and by M, S the cost of multiplication and squaring over $\mathbb{F}_p$ and over $\mathbb{F}_{p^2}$, 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 $S \sim 3s$. Additions in $\mathbb{F}_p$ are not completely negligible compared to multiplications, but we do not count additions here. We counted operations by using formulæ from Bernstein and Lange's database [1] for addition and doubling in projective coordinates. On the curve

$E_{1,c}$ addition costs $12M + 2S$, while doubling costs $5S + 6M + 1c$. For E_β , 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 formulæ given by Costello and Lauter [5] in projective coordinates. An addition costs $43M + 4S$ and a doubling costs $30M + 9S$.

Table 1. Total cost of scalar multiplication at a 128-bit security level.

Curve	Method	Operation count	Global estimation
$E_{1,c}$	4-GLV, 16 pts.	$1168M + 440S$	$4797m$
E_β	4-GLV, 16 pts.	$976M + 440S$	$4248m$
$E_{1,c}$	2-GLV, 4 pts.	$2048M + 832S$	$8640m$
E_β	2-GLV, 4 pts.	$1664M + 832S$	$7488m$
$J_{\mathcal{C}_1}$	4-GLV, 16 pts.	$4500m + 816s$	$5316m$
$J_{\mathcal{C}_1}$	2-GLV, 4 pts.	$7968m + 1536s$	$9504m$
FKT [3]	4-GLV, 16 pts.	$4500m + 816s$	$5316m$
Kummer [3]	–	$3328m + 2304s$	$5632m$

The practical gain of the 4-dimensional GLV on $E_{1,c}$, when compared to the 2-dimensional GLV method, is of 44%. Curves with discriminant -3, defined over $\mathbb{F}_{p^2}$, which belong both to the family of curves we propose and to the one proposed by Longa and Sica, offer a 12% speed-up, thanks to their efficient arithmetic.

7 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 complexity estimates 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.

8 Acknowledgements

We are grateful to Damien Vergnaud and Léo Ducas for many helpful discussions on the GLV algorithm and lattice reduction. We thank the anonymous reviewers

of the Asiacrypt conference for their remarks. This work was supported in part by the French ANR-09-VERS-016 BEST Project.

References

1. Bernstein, D., Lange, T.: Explicit-Formulas Database, http://www.hyperelliptic.org/EFD/
2. Bisson, G.: Endomorphism rings in cryptography. PhD thesis, Institut National Polytechnique de Lorraine (2011)
3. Bos, J., Costello, C., Hisil, H., Lauter, K.: Fast cryptography in genus 2. In: Johansson, T., Nguyen, P. (eds.) Advances in Cryptology – EUROCRYPT 2013. LNCS, vol. 7881, pp. 194–210. Springer (2013)
4. Cheon, J.: Security analysis of the strong Diffie-Hellman problem. In: Vaudenay, S. (ed.) Eurocrypt 2006. LNCS, vol. 4004, pp. 1–11. Springer (2006)
5. Costello, C., Lauter, K.: Group Law Computations on Jacobians of Hyperelliptic Curves. In: Miri, A., Vaudenay, S. (eds.) Selected Areas in Cryptography. LNCS, vol. 7118, pp. 92–117. Springer (2011)
6. Dewaghe, L.: Un corollaire aux formules de Vélu. Draft (1995)
7. Doche, C.: Exponentiation, Chapter 9. In: Handbook of elliptic and hyperelliptic curve cryptography. pp. 145–168. Chapman and Hall/CRC, Taylor and Francis Group (2006)
8. Duursma, I., Kiyavash, N.: The vector decomposition problem for elliptic and hyperelliptic curves. Journal of the Ramanujan Mathematical Society 20(1), 59–76 (2005)
9. Freeman, D.M., Satoh, T.: Constructing pairing-friendly hyperelliptic curves using Weil restriction. Journal of Number Theory 131(5), 959–983 (2011)
10. Galbraith, S., Lin, X., Scott, M.: Endomorphisms for faster elliptic curve cryptography on a large class of curves. In: Joux, A. (ed.) Advances in Cryptology – Eurocrypt 2009. LNCS, vol. 5479. Springer (2009)
11. Gallant, R., Lambert, R., Vanstone, S.: Faster point multiplication on elliptic curves with efficient endomorphisms. In: Kilian, J. (ed.) CRYPTO. LNCS, vol. 2139, pp. 190–200. Springer (2001)
12. Gaudry, P., Schost, É.: On the invariants of the quotients of the jacobian of a curve of genus 2. In: Boztas, S., Shparlinski, I. (eds.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 2001. LNCS, vol. 2227, pp. 373–386. Springer (2001)
13. Guillevic, A., Vergnaud, D.: Genus 2 Hyperelliptic Curve Families with Explicit Jacobian Order Evaluation and Pairing-Friendly Constructions. In: Abdalla, M., Lange, T. (eds.) Pairing-Based Cryptography-Pairing 2012. LNCS, vol. 7708, pp. 234–253. Springer (2013)
14. Kohel, D.: Endomorphism rings of elliptic curves over finite fields. Ph.D. thesis, University of California at Berkeley (1996)
15. Leprévost, F., Morain, F.: Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. Journal of Number Theory 64, 165–182 (1997), `http://www.lix.polytechnique.fr/Labo/Francois.Morain/Articles/LIX-RR-94-07-revetement.ps.gz`
16. Longa, P., Sica, F.: Four dimensional Gallant-Lambert-Vanstone scalar multiplication. Journal of Cryptology pp. 1–36 (2013)

17. Quer, J.: Fields of definition of $\mathbb{Q}$-curves. Journal de Théorie des Nombres de Bordeaux 13(1), 275–285 (2001)
18. Satoh, T.: Generating genus two hyperelliptic curves over large characteristic finite fields. In: Joux, A. (ed.) Advances in Cryptology – EUROCRYPT 2009. LNCS, vol. 5479. Springer (2009)
19. Smith, B.: Families of fast elliptic curves from $\mathbb{Q}$-curves. In: Sako, K., Sarkar, P. (eds.) Asiacrypt. LNCS, vol. To appear. Springer (2013), `http://eprint.iacr.org/2013/312`
20. Vélu, J.: Isogenies entre courbes elliptiques. Comptes Rendus De l'Académie Des Sciences Paris, Série I-Mathèmatique, Série A. 273, 238–241 (1971)

A Appendix 1

Following [5], we explain here the step addition of two divisors in the isogeny computation in Section 5.3. We denote by m_n and s_n the cost of multiplication and squaring, respectively, in an extension field $\mathbb{F}_{p^n}$.

$\sigma_1 = u_1 + \pi_{p^2}(u_1)$, $\Delta_0 = v_0 - \pi_{p^2}(v_0)$, $\Delta_1 = v_1 - \pi_{p^2}(v_1)$, $U_1 = u_1^2$ $(1m_4)$
$M_1 = u_1^2 - \pi_{p^2}(u_1^2)$,$M_2 = \sqrt{b}(\pi_{p^2}(u_1) - u_1)$, $M_3 = u_1 - \pi_{p^2}(u_1)$;
$l_2 = 2(M_2 \cdot \Delta_1 + \Delta_0 \cdot M_1)$; $l_3 = \Delta_0 \cdot M_3$; $d = -2M_2 \cdot M_3$; $(4m_2)$
$A = 1/(d \cdot l3)$; $B = d \cdot A$; $C = d \cdot B$; $D = l_2 \cdot B$; $(3m_2{+}1m_4)$
$E = l_3^2 \cdot A$; $CC = C^2$; $u_1'' = 2 \cdot D - CC - \sigma_1$ $(1m_2{+}2s_2)$
$u_0'' = D^2 + C \cdot (v_1 + \pi_{p^2}(v_1)) - ((u_1'' - CC) \cdot \sigma_1 + (U_1 + \pi_{p^2}(U_1)))/2$ $(2m_2{+}1s_4)$
$U_0'' = \pi_{p^2}(u_1) \cdot u_0''$; $v_1'' = D \cdot (u_1 - u_1'') + u_1^{2''} - u_0'' - U_1$; $(2m_4{+}1s_1)$
$v_0'' = D \cdot (u_0 - u_0'') + U_0''$;$v_1'' = -(E \cdot v_1'' + v_1)$; $v_0'' = -(E \cdot v_0'' + v_0)$; $(3m_4)$