In H. Cohen, editor, *Algorithmic Number Theory: Second International Symposium, ANTS-II Talence, France, May 18–23, 1996 Proceedings*, volume 1122 of *Lecture Notes in Computer Science*, pages 197–212. Springer Berlin / Heidelberg, May 1996.

Computing isogenies in $\mathbb{F}_{2^n}$

Reynald LERCIER[1][2]

[1] Laboratoire d'Informatique de l'École Polytechnique (LIX),
Route de Saclay, 91128 Palaiseau cedex, France
Email: lercier@lix.polytechnique.fr
[2] CELAR/SSIG, Route de Laillé, F-35170 Bruz, France

Abstract. Contrary to what happens over prime fields of large characteristic, the main cost when counting the number of points of an elliptic curve E over $\mathbb{F}_{2^n}$ is the computation of isogenies of prime degree ℓ. The best method so far is due to Couveignes and needs asymptotically $O(\ell^3)$ field operations. We outline in this article some nice properties satisfied by these isogenies and show how we can get from them a new algorithm that seems to perform better in practice than Couveignes's though of the same complexity. On a representative problem, we gain a speed-up of 5 for the whole computation.

1 Introduction

Many number theoretic algorithms are based on elliptic curves, among which integer factorization [5] or primality testing [1]. More directly, counting the number of points on these curves is essential to design secure cryptographical public schemes [8].

Algorithms to compute the cardinality of elliptic curves defined over finite fields of large characteristic give now satisfying results with the works of Schoof, Elkies, Atkin, Couveignes-Morain, Müller, Dewaghe . . . ; a precise bibliography can be found for instance in [7]. In finite fields of characteristic two (used to implement cryptographical schemes in hardware), most of the ideas developed in the case of the large characteristic can be used except the necessary computation of isogenies between elliptic curves.

Couveignes developed in his thesis [4] an algorithm to overcome this difficulty which was implemented in [7]. It consists of working in the formal group defined by the elliptic curve. However, this algorithm requires computations with huge series and unlike the finite fields of large characteristic, computing isogenies still remains the main cost while counting the number of points.

We describe in this paper a new algorithm to compute isogenies in $\mathbb{F}_{2^n}$. Instead of working in the formal group, we work on the curve itself. It is based on identities satisfied by isogenies as, for instance, commutativity with multiplication by two. Its complexity is similar to Couveignes's algorithm but it is conceptually simpler and much more efficient in practice. For instance, while counting points on elliptic curves over $\mathbb{F}_{2^{300}}$, computing isogenies takes 80% of the time in [7] and only 1% by our method. Section 2 recalls basic facts on elliptic curves and section 3 describes nice properties satisfied by these isogenies. We explain in section 4 how this algorithm works and finally give accurate benchmarks of our C implementation in section 5.

2 Elliptic curves over fields of characteristic 2

As explained in [8], we consider elliptic curves defined over $\mathbb{F}_{2^n}$ by

$$E_a : y^2 + xy = x^3 + a,\ a \in \mathbb{F}^*_{2^n}. \tag{1}$$

The invariant of E_a is $j = 1/a$, its discriminant is a and its set of points noted $E_a(\mathbb{F}_{2^n})$, is the union of O_E with the set $\{(x, y) \in \mathbb{F}^2_{2^n}, y^2 + xy = x^3 + a\}$. The formulae of the addition law on E_a are:

- $\forall P = (x_P, y_P) \in E_a(\mathbb{F}_{2^n}),\ P + O_E = O_E + P = P,\ -P = (x_P, y_P + x_P)$;

- if $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $P \neq -Q$, then if $P = Q$, let $\lambda = x_P + y_P/x_P$ otherwise, let $\lambda = (y_Q + y_P)/(x_Q + x_P)$ and $R = P + Q = (x_{P+Q}, y_{P+Q})$ is obtained by

$$\begin{cases} x_{P+Q} = \lambda^2 + \lambda + x_P + x_Q, \\ y_{P+Q} = \lambda(x_P + x_{P+Q}) + x_{P+Q} + y_P. \end{cases}$$

We easily deduce from these equations the formulae of the multiplication by two,

$$[2]_a : \ P = (x, y) \mapsto 2P = \left(x^2 + \frac{a}{x^2}, \left(x + \frac{y}{x}\right)\left(x^2 + \frac{a}{x^2}\right) + \frac{a}{x^2}\right). \tag{2}$$

Since a point $P = (x, y)$ is equal to $-P = (x, y + x)$ if and only if $x = 0$, the only point of order two is $P_a = (0, \sqrt{a})$ (remember that in characteristic two, every element has a unique square root). We will be specially interested in the translation by P_a in section 3. The formulae are

$$T_{P_a} : P = (x, y) \mapsto P + P_a = \left(\frac{\sqrt{a}}{x}, \sqrt{a} + \frac{\sqrt{a}}{x} + \frac{a}{x^2} + \sqrt{a}\frac{y}{x^2}\right). \tag{3}$$

3 Isogenies

Once given general results about isogenies in section 3.1, we describe the isogenies we are interested in and give necessary conditions satisfied by this description in section 3.2.

In what follows, $\bar{\mathbb{F}}_{2^n}$ is the algebraic closure of $\mathbb{F}_{2^n}$.

3.1 Classical results

The results given here can be found in [11] or [2]. First of all, an isogeny $\mathcal{I}$ between two elliptic curves E_a and E_b is classically defined as a map of algebraic curves from E_a to E_b satisfying $\mathcal{I}(O_{E_a}) = O_{E_b}$. It turns out that isogenies are also map of algebraic groups or in other words, $\mathcal{I}$ is a morphism from $E_a(\mathbb{F}_{2^n})$ to $E_b(\mathbb{F}_{2^n})$.

For instance, the multiplication by m (noted $[m]_a$) is an isogeny. There exists a sequence of polynomials f_k (called division polynomials) of degree at most $\lfloor \frac{k^2}{2} \rfloor$ such that if $m > 2$, $P = (X, Y) \in E_a(\mathbb{F}_{2^n})$ and $mP \neq O_{E_a}$, then $mP = (X_{mP}, Y_{mP})$ is given by

$$\begin{cases} X_{mP} = X + \dfrac{f_{m-1}f_{m+1}}{f_m^2}, \\ Y_{mP} = X + Y + \dfrac{f_{m-1}f_{m+1}}{f_m^2} + \dfrac{f_{m-2}f_{m+1}^2}{X f_m^3} + (X^2 + Y)\dfrac{f_{m-1}f_{m+1}}{X f_m^2}. \end{cases} \tag{4}$$

Division polynomials can be computed easily by induction [8, pp. 102].

For our purposes, the degree of an isogeny $\mathcal{I}$ can be defined as follows.

Theorem 1. *Let $\mathcal{I}$ be a non constant separable isogeny from E_a and E_b. Then*

1. *$\mathcal{I}\left(E_a(\bar{\mathbb{F}}_{2^n})\right) = E_b(\bar{\mathbb{F}}_{2^n})$.*
2. *For every S in $E_b(\bar{\mathbb{F}}_{2^n})$, we note $\mathcal{I}^{-1}(S)$ the set of points of $E_a(\bar{\mathbb{F}}_{2^n})$ whose image is S. The cardinal of $\mathcal{I}^{-1}(S)$ is finite and does not depend of S. We call it the degree of $\mathcal{I}$ and note it* $\deg(\mathcal{I})$*.*
3. *If m is a positive integer, $[m]_a$ is an isogeny of degree m^2.*
4. *There exists a unique isogeny $\hat{\mathcal{I}}$ from E_b to E_a such that $\hat{\mathcal{I}} \circ \mathcal{I} = [\deg(\mathcal{I})]_a$. Moreover* $\deg(\hat{\mathcal{I}}) = \deg(\mathcal{I})$*.*

Finally, it is easy to find an isogeny whose kernel is given using Vélu's formulae [12] adapted to the case of the characteristic 2.

Theorem 2. *Let F be a subgroup (of odd order) of an elliptic curve E_a. If $b = a + \sum_{(X_S, Y_S) \in F^*} Y_S + Y_S^2$, then there exists isogenies between E_a and E_b of kernel F. One of these isogenies is given by*

$$(X, Y) \mapsto \left(X + \sum_{S \in F^*} X_{P+S}, Y + \sum_{S \in F^*} Y_{P+S}\right). \tag{5}$$

3.2 Properties

The improvements of Schoof's original algorithm [9] to count the number of points on an elliptic curve can be seen as computing isogenies between this curve and other elliptic curves easily found by solving "modular equations" [10].

Theorem 3 shows examples of such isogenies.

Theorem 3. *Let ℓ be an odd integer and $d = (\ell-1)/2$. Let E_a be an elliptic curve defined over $\mathbb{F}_{2^n}$ such that isogenies of degree ℓ defined from it can be found. There exists a factor $Q(X)$ of degree d of $f_\ell(X)$ on E_a such that one of these isogenies sends (X,Y) to*

$$\left(\frac{XP^2(X)}{Q^2(X)}, (Y+X^2)\frac{P^2(X)}{Q^2(X)} + X^2 + \frac{X^2Q_1^2(X)}{Q^2(X)} \right.$$
$$\left. + X^3\left(\frac{Q_1^3(X)}{Q^3(X)} + \frac{Q_2(X)Q_1(X)+Q_3(X)Q(X)}{Q^2(X)}\right)\right), \quad (6)$$

where, if we let $Q(X) = E^2(X) + XO^2(X)$,

$$P(X) = Q(X) + O(X)E(X), \quad (7)$$

and $Q_1(X) = Q'(X) = O^2(X)$, $Q_2(X) = E'^2(X) + XO'^2(X)$, $Q_3(X) = Q_2'(X) = O'^2(X)$.

Proof. Since by hypothesis, there exists isogenies of degree ℓ from $E_a(\bar{\mathbb{F}}_{2^n})$ to an other curve $E_b(\bar{\mathbb{F}}_{2^n})$, we call $\mathcal{I}'$ one of these isogenies. The only point P_a of order two of $E_a(\bar{\mathbb{F}}_{2^n})$ is not in $\operatorname{Ker}(\mathcal{I}')$ because ℓ is odd and we can write that $\operatorname{Ker}(\mathcal{I}')$ is equal to $\{O_{E_a}\} \cup \mathfrak{S} \cup -\mathfrak{S}$ with $\mathfrak{S} \cap -\mathfrak{S} = O_{E_a}$. Therefore from theorem 2 and from the formulae of the addition law, an isogeny $\mathcal{I}$ of kernel $\operatorname{Ker}(\mathcal{I}')$ is given by

$$\mathcal{I}(X,Y) = \left(X\left(1 + \sum_{S\in\mathfrak{S}} \frac{X_S}{(X-X_S)^2}\right), \right.$$
$$\left. Y + \sum_{S\in\mathfrak{S}} X_S\left(\frac{Y+X^2}{(X-X_S)^2} + \frac{X^2}{(X-X_S)^3}\right)\right). \quad (8)$$

Let now $Q(X)$ be the polynomial $\prod_{S\in\mathfrak{S}}(X - X_S)$. It remains to check by a simple calculation that equations (8) and (6) are the same. Finally, from theorem 1, there exists an isogeny $\hat{\mathcal{I}}$ such that $\hat{\mathcal{I}} \circ \mathcal{I} = [\ell]_a$ and therefore $\operatorname{Ker}(\mathcal{I}) \subset \operatorname{Ker}([\ell]_a)$, which implies that $Q(X)$ divides $f_\ell(X)$.

□

On the other hand, isogenies must satisfy necessary conditions given in theorem 4.

Theorem 4. *Let E_a and E_b be two elliptic curves defined over $\mathbb{F}_{2^n}$, let ℓ be an odd integer and $d = (\ell-1)/2$. Let $\mathcal{I}$ be an isogeny of degree ℓ between E_a and E_b given by $(X,Y) \mapsto \left(\frac{G(X)}{Q^2(X)}, \frac{H(X)+YK(X)}{Q^3(X)}\right)$ where $(Q(X), G(X), H(X), K(X)) \in \mathbb{F}_{2^n}[X]^4$ with degrees at most d, ℓ, $3d$ and $2d$, then*

1. *$G(X) = XP^2(X)$ where $P(X)$ is a polynomial of degree d such that* $\gcd(P(X),Q(X)) = 1$ *and $X^dQ(\sqrt{a}/X) = \frac{\sqrt[8]{a}}{\sqrt[8]{b}}\left(\sqrt[4]{a}\right)^d P(X)$, or equivalently via $X \to \sqrt{a}/X$,*

$$X^dP(\sqrt{a}/X) = \frac{\sqrt[8]{b}}{\sqrt[8]{a}}\left(\sqrt[4]{a}\right)^d Q(X); \quad (9)$$

2. *$K(X) = P^2(X)Q(X)$;*
3. *$H(X) = XR(X)P(X) + \sqrt{b}Q^3(X) + \sqrt{a}P^2(X)Q(X)$ with $R(X) = X(PQ)'(X)$ or $R(X) = (XPQ)'(X)$.*

Proof. Since $[2](\mathcal{I}(P_a)) = \mathcal{I}([2](P_a)) = 0$ and P_b is the only point of order 2 in E_b, $\mathcal{I}(P_a) = P_b$. So

$$\forall S \in E_a,\ \mathcal{I}(S + P_a) = \mathcal{I}(S) + P_b. \tag{10}$$

With the formulas of the addition law between points of E_a, we obtain for $S = O_{E_a}$, $G(0)/Q^2(0) = 0$, and consequently X divides $G(X)$. Let $\varGamma(X) = G(X)/X$. For $S = (X, Y) \neq O_{E_a}$, equation (10) becomes

$$\begin{gathered}\left(\frac{\sqrt{a}\varGamma(\sqrt{a}/X)}{XQ^2(\sqrt{a}/X)}, \frac{H(\sqrt{a}/X) + \sqrt{a}(1 + 1/X + (Y + \sqrt{a})/X^2)K(\sqrt{a}/X)}{Q^3(\sqrt{a}/X)}\right)\\ =\\ \left(\frac{\sqrt{b}Q^2(X)}{X\varGamma(X)}, \sqrt{b} + \frac{\sqrt{b}Q^2(X)}{X\varGamma(X)} + \frac{\sqrt{b}Q^4(X)}{X^2\varGamma^2(X)}\left(\frac{H(X) + YK(X)}{Q^3(X)} + \sqrt{b}\right)\right).\end{gathered} \tag{11}$$

After simplification, the abscissae of equation (11) lead to $\sqrt{a}\,\varGamma(\sqrt{a}/X)\,\varGamma(X) = \sqrt{b}\,Q^2(\sqrt{a}/X)\,Q^2(X)$. The quantities $\tilde{\varGamma}(X) = X^{2d}\varGamma(\sqrt{a}/X)$ and
$\tilde{Q}(X) = X^d Q(\sqrt{a}/X)$ are in fact polynomials and the previous equation can be rewritten as

$$\sqrt{a}\,\tilde{\varGamma}(X)\,\varGamma(X) = \sqrt{b}\,\tilde{Q}^2(X)\,Q^2(X). \tag{12}$$

Since $\gcd(\varGamma(X), Q^2(X)) = 1$, $\varGamma(X)$ divides $\tilde{Q}^2(X)$. But $\varGamma(X)$ has the same degree as $\tilde{Q}^2(X)$, therefore there exists a constant $\gamma \in \mathbb{F}_{2^n}$ such that $\varGamma(X) = \gamma^2\tilde{Q}^2(X)$ (remember that every element in $\mathbb{F}_{2^n}$ is a square). So, $\varGamma(X)$ is a square. Let $P(X) = \sqrt{\varGamma(X)}$, then $P(X) = \gamma\tilde{Q}(X)$ or, equivalently $Q(X) = \frac{\sqrt{a}^d}{\gamma}\tilde{P}(X)$. Substituting these expressions in (12) gives $\gamma = (\sqrt[4]{a})^d\,\frac{\sqrt[8]{b}}{\sqrt[8]{a}}$, which proves relation (9).

Since $\forall S \in E_a,\ \mathcal{I}(-S) = -\mathcal{I}(S)$, we have $\frac{H(X)+(Y+X)K(X)}{Q^3(X)} = \frac{H(X)+YK(X)}{Q^3(X)} + X\frac{P^2(X)}{Q^2(X)}$, and consequently point 2 of the theorem is proved.

Moreover, from $\mathcal{I}(P_a) = P_b$, we obtain $H(0) = \sqrt{a}P^2(0)Q(0) + \sqrt{b}Q^3(0)$. Therefore, we can write $H(X) = \sqrt{a}P^2(X)Q(X) + \sqrt{b}Q^3(X) + XL(X)$ where $L(X)$ is a polynomial of degree at most $3d$. Furthermore, the ordinates of equation (11) lead to

$$\begin{aligned}&\frac{\sqrt{a}L(\sqrt{a}/X)}{XQ^3(\sqrt{a}/X)} + \left(\frac{\sqrt{a}}{X} + \frac{a}{X^2} + \frac{\sqrt{a}Y}{X^2}\right)\frac{P^2(\sqrt{a}/X)}{Q^2(\sqrt{a}/X)} =\\ &\qquad\qquad\frac{\sqrt{b}Q^2(X)}{XP^2(X)} + \frac{\sqrt{b}Q^4(X)}{X^2P^4(X)}\left(\frac{XL(X)}{Q^3(X)} + (Y + \sqrt{a})\frac{P^2(X)}{Q^2(X)}\right).\end{aligned} \tag{13}$$

Taking advantage of equation (9), this equation can be simplified as follows,

$$\sqrt{a}X^{3d}L(\sqrt{a}/X)P(X) = \sqrt{b}\left(\frac{\sqrt[8]{a}}{\sqrt[8]{b}}\right)^3\left(\sqrt[4]{a}\right)^{3d}Q(X)L(X). \tag{14}$$

Since $\gcd(P(X), Q(X)) = 1$, we deduce that $P(X)$ divides $L(X)$. The polynomial $R(X) = L(X)/P(X)$ has degree at most $2d$.

As for all $S \in E_a$, $\mathcal{I}(S) \in E_b$, we have

$$\begin{aligned}&\left(X\frac{R(X)P(X)}{Q^3(X)} + \sqrt{b} + (Y + \sqrt{a})\frac{P^2(X)}{Q^2(X)}\right)^2 + \left(\frac{XP^2(X)}{Q^2(X)}\right)^3 =\\ &\qquad\qquad\left(X\frac{R(X)P(X)}{Q^3(X)} + \sqrt{b} + (Y + \sqrt{a})\frac{P^2(X)}{Q^2(X)}\right)\frac{XP^2(X)}{Q^2(X)} + b.\end{aligned}$$

So,

$$\begin{aligned}&XR(X)\left(R(X) + P(X)Q(X)\right) =\\ &\qquad\qquad\left((X + \sqrt[4]{a})P(X)Q(X) + \sqrt[4]{b}Q^2(X) + XP^2(X)\right)^2.\end{aligned} \tag{15}$$

Let R_1 be a polynomial solution of equation (15) and $R_2(X) = R_1(X) + P(X)Q(X)$. Since the left hand side of (15) is $XR_1(X)R_2(X)$ and the right hand side is a square, X must divide $R_1(X)$ or $R_2(X)$. As $R_2(X)$ is a solution of equation (15) too, $R_1(X)$ and $R_2(X)$ play a symmetric part and we can assume that X divides $R_1(X)$.

Let us prove that $R_1(X)/X$ and $R_2(X)$ are both squares. We already know that $R_1(X)R_2(X)/X$ is a square. Let us assume now that an irreducible polynomial $\rho(X)$ divides both $R_1(X)/X$ and $R_2(X)$ ($\rho(X) \neq X$). The polynomial $\rho(X)$ divides $R_1(X) + R_2(X) = P(X)Q(X)$ and divides $P(X)$ or $Q(X)$ but not both since $\gcd(P(X), Q(X)) = 1$. Furthermore, $\rho(X)$ divides the square root of the right hand side of (15), that is to say it divides $(X + \sqrt[4]{a})P(X)Q(X) + \sqrt[4]{b}Q^2(X) + XP^2(X)$. Consequently, if we assume that $\rho(X)$ divides $P(X)$, $\rho(X)$ divides $Q(X)$ and we reach a contradiction. As we obtain the same conclusion if we assume at first that $\rho(X)$ divides $Q(X)$, we proved that $\gcd(R_1(X), R_2(X)) = 1$. Moreover, since $R_1(X)R_2(X)/X$ is a square, $R_1(X)/X$ and $R_2(X)$ are squares. Let $R_1(X) = XO^2(X)$ and $R_2(X) = E^2(X)$, then

$$XO^2(X) + E^2(X) = P(X)Q(X). \tag{16}$$

The derivation of (16) gives $R_1 = X(PQ)'$ and the derivation of (16) multiplied by X gives $R_2 = (XPQ)'$, which finally proves point 3 of the theorem.

□

According to theorem 3 or 4, it turns out that isogenies are completely determined by their polynomial $P(X)$ or equivalently by $Q(X)$.

Corollary 1. *With the notations of theorem 4, polynomials $P(X)$ and $Q(X)$ must satisfy*

$$X^d\widehat{Q}(X + \sqrt{a}/X) = Q(X)P(X), \tag{17}$$

and

$$\left(X + \sqrt[4]{a}\right) X^d\widehat{P}\left(X + \sqrt{a}/X\right) = XP^2(X) + \sqrt[4]{b}Q^2(X), \tag{18}$$

where $\widehat{P}(X) = \sqrt{P(X^2)}$ and $\widehat{Q}(X) = \sqrt{Q(X^2)}$ (polynomials whose coefficients are square roots of coefficients of $P(X)$ and $Q(X)$).

Proof. Using the fact that $\forall S \in E_a$, $\mathcal{I}([2](S)) = [2](\mathcal{I}(S))$, we get $\left(\frac{XP^2(X)}{Q^2(X)}\right) \circ \left(X^2 + \frac{a}{X^2}\right) = \left(X^2 + \frac{b}{X^2}\right) \circ \left(\frac{XP^2(X)}{Q^2(X)}\right)$. Taking the square root of this equation twice leads to

$$\left(X + \sqrt[4]{a}\right) \frac{X^d\widehat{P}\left(X + \sqrt{a}/X\right)}{X^d\widehat{Q}\left(X + \sqrt{a}/X\right)} = \frac{XP^2(X) + \sqrt[4]{b}Q^2(X)}{P(X)Q(X)}. \tag{19}$$

Since $\gcd(XP^2(X), Q^2(X)) = 1$, the right hand side of this equation is an irreducible fraction. So, numerators and denominators of both sides of equation (19) are equal, which finally proves (17) and (18).

□

From theorem 4 and corollary 1, we deduce the following relations.

Corollary 2. *Let $P(X) = \sum_{i=0}^{d} p_i^2 X^i$, $Q(X) = X^d + \sum_{i=0}^{d-1} q_i^2 X^i$, $\alpha = \sqrt[4]{a}$ and $\beta = \sqrt[4]{b}$. We have*

$$q_i = \frac{\sqrt[4]{\alpha}}{\sqrt[4]{\beta}} \sqrt{\alpha}^{d-2i} p_{d-i}, \ \forall i \in \{0, \dots, d\}, \tag{20}$$

and

$$p_0 = \sqrt[4]{\alpha^{2d} + \alpha^{2d-1}p_{d-1}}, \ p_d = 1, \ p_{d-1} = \alpha + \beta,$$
$$p_{d-2} = \begin{cases} p_{d-1}^4 + \alpha p_{d-1} + \alpha^2 & \textit{if } d \textit{ is odd,} \\ p_{d-1}^4 + \alpha p_{d-1} & \textit{if } d \textit{ is even.} \end{cases}$$

Proof. Equation (20) is a direct application of equation (9). The coefficient of X^{2d} in equation (17) is $p_d^2+p_d$, which yields $p_d = 1$. Then, the coefficient of X^{2d} in equation (18) is $p_{d-1}+\alpha+\beta$, which gives p_{d-1}. The coefficient of X^{2d-1} in equation (18) is $p_{d-2}+p_{d-1}^4+\alpha p_{d-1}+\alpha^2$ if d is odd, and $p_{d-2}+p_{d-1}^4+\alpha p_{d-1}$ if d is even, which yields p_{d-2}. Finally the coefficient of X in equation (18) which is $p_0^4+\alpha^{2d}+\alpha^{2d-1}p_{d-1}$ gives p_0.

□

What was done for two in corollary 1 can be done in the same way for the multiplication by any odd positive integer m.

Corollary 3. *With the notations of theorem 4, the polynomials $P(X)$ and $Q(X)$ must satisfy*

$$f_{m,a}^{\ell}(X)Q\left(\frac{h_{m,a}(X)}{f_{m,a}^2(X)}\right) = Q^{m^2}(X)f_{m,b}\left(X\frac{P^2(X)}{Q^2(X)}\right), \tag{21}$$

where m is any odd positive integer, $f_{m,a}$ (resp. $f_{m,b}$) is the m-division polynomial on E_a (resp. E_b) and $h_{m,a}(X) = Xf_{m,a}^2(X) + f_{m-1,a}(X)f_{m+1,a}(X)$.

4 Computing isogenies

We describe in this section how we take advantage of the previous results to explicitly compute the polynomials $P(X)$ or $Q(X)$. Precisely, we show in section 4.1 how we use equation (18) to compute them. Unfortunately the complexity of this method is too high, and we describe in section 4.2 how we speed it up using equation (17). Finally in section 4.3, we describe how we further improve this algorithm using equation (7) and equation (21).

4.1 Solving a linear system over $\mathbb{F}_{2^n}$

This first method is based on equation (18). With the notations of corollary 2, this equation yields

$$\boxed{\begin{aligned}\forall k = 0,\dots,\left\lfloor\frac{d-1}{2}\right\rfloor,\ p_k^4 =& \alpha^{2d-4k-1}\sum_{i=0}^{k} p_{d-2k-1+2i}\varepsilon_{d-2k-1+2i,i}\alpha^{2i}\\ &+\alpha^{2d-4k}\sum_{i=0}^{k} p_{d-2k+2i}\varepsilon_{d-2k+2i,i}\alpha^{2i},\end{aligned}} \tag{22}$$

$$\boxed{\begin{aligned}\forall k = 1,\dots,\left\lfloor\frac{d}{2}\right\rfloor,\ p_{d-k}^4 =& \alpha\sum_{i=0}^{k-1} p_{d+1-2k+2i}\varepsilon_{d+1-2k+2i,i}\alpha^{2i}\\ &+\sum_{i=0}^{k} p_{d-2k+2i}\varepsilon_{d-2k+2i,i}\alpha^{2i}.\end{aligned}} \tag{23}$$

where for all integers i, j such that $0 \le j \le i$, $\varepsilon_{i,j} = \frac{i!}{j!(i-j)!} \bmod 2$.

A first way to solve system (22, 23) is to write each p_i as a linear combination in a polynomial basis $1, T, T^2, \dots, T^{n-1}$ of $\mathbb{F}_{2^n}$, $p_i = p_{i,0} + p_{i,1}T + \dots + p_{i,n-1}T^{n-1}$ with $\forall j \in \{0,\dots,n-1\}$, $p_{i.j} \in \{0,1\}$. Rewriting the system (22, 23) with these notations gives us a linear system of $n(d-2)$ equations in $n(d-3)$ variables $p_{i,j}$, once substituted p_d, p_{d-1}, p_{d-2}, and p_0 as functions of α and β (corollary 2).

Unfortunately, such a method costs asymptotically $O(\ell^3n^3)$ elementary operations (or $O(\ell^3n)$ field operations) with classical algorithms. Furthermore, in practice the huge size of the matrix is a serious drawback. For instance, finding an isogeny of degree $\ell \simeq 500$, in $\mathbb{F}_{2^{1000}}$ (as what was done in [7] with Couveignes's algorithm) yields a matrix of size one gigabyte.

We suggest two improvements. Rather than solving system (22, 23) in $\mathbb{F}_2$, we first write $[p_1^{2^n}, \ldots, p_{d-3}^{2^n}]$ from $[p_1^{2^{n-2}}, \ldots, p_{d-3}^{2^{n-2}}]$, and then write in the same way $[p_1^{2^{n-2}}, \ldots, p_{d-3}^{2^{n-2}}]$ from $[p_2^{2^{n-4}}, \ldots, p_{d-3}^{2^{n-4}}]$. After $O(n)$ such iterations we finally get a linear equation for $[p_1, \ldots, p_{d-3}]$ because $p_j^{2^n} = p_j$ in $\mathbb{F}_{2^n}$. The main cost of solving this system in such a way is the computation of $O(n)$ (or may be $O(\log n)$ as suggested by F. Morain) product of matrices of size d, that is $O(\ell^3)$ multiplications in $\mathbb{F}_{2^n}$. So we finally need $O(\ell^3 n^3)$ operations (or maybe $O(\ell^3 n^2 \log n)$).

Another solution takes advantage of the shape of system (22, 23). We notice that we easily get p_{d-3} as a function of p_1 by setting $k = 2$ in equation (22) and once substituted it in the other equations, p_{d-3} as a function of p_1 by setting $k = 1$ in equation (23). Then by induction, we easily get p_{d-2i-1} as a function of $p_1, \ldots, p_i$ by setting $k = i$ in equation (22) and once substituted it in the remaining equations, p_{d-2i-2} as a function of $p_1, \ldots, p_i$ by setting $k = i + 1$ in equation (23). We iterate this process until $i = d - 2i - 1$ or $i = d - 2i - 2$. So, at the end of this process, we express $p_{d-3}, \ldots, p_{i+1}$ as a function of $p_i, \ldots, p_1$ where $i \simeq d/3$. Furthermore, the $i+1$ remaining equations (22, 23) for $k \geq i$, are polynomials whose monomials are p_i raised to the power 2^j. So these equations still are linear equations when considered over $\mathbb{F}_2$ and we can use the method given at first with a matrix whose size is divided by 3.

4.2 Solving a non linear system over $\mathbb{F}_2$

The information obtained with equation (17) enables us to replace a linear system with unknowns in $\mathbb{F}_{2^n}$ by a non linear system with unknowns in $\mathbb{F}_2$. Equation (17) leads to the following $d+1$ equations,

$$\boxed{\forall k = 0, \ldots, d,\ \sqrt[4]{\alpha} \sum_{i=0}^{k} p_i^2 p_{d-k+i}^2 \alpha^{2i} = \sqrt[4]{\beta}\sqrt{\alpha}^{d+2k} \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} p_{k-2i} \varepsilon_{d-k+2i,i}.} \tag{24}$$

From equation (24), each p_i is solution of an equation of degree 2. Consequently, $p_i = a_i + \pi_i b_i$, where $b_i \in \mathbb{F}_{2^n}$, a_i depends on $p_1, \ldots, p_{i-1}$ and $\pi_i \in \mathbb{F}_2$. So combined with the ideas expressed at the end of section 4.1, each p_k for $k = 0..d$ can be written as a multivariate polynomial in binary variables π_i. This is an important simplification in relation to the computations we did in the last section. Furthermore, p_i satisfies an equation of degree 2 whose coefficients are linked by a "compatibility" relation; this has the surprising effect of keeping the number of these variables π_i almost stationary when ℓ increases.

The following algorithm is based on these two facts. Once the initialization done (step 1), it consists of two phases. The first phase is a loop in which we compute each p_k for $k = 1, \ldots, d-3$ as a a function of binary variables π_i. In fact, for K from 0 to $d/3$, we get p_K with equation (24) as a function of the binary variables $\pi_0, \ldots, \pi_{K-1}$ (step 2) and then we extract p_{d-2K+1} (step 3) and p_{d-2K} (step 4) also as functions of $\pi_0, \ldots, \pi_{K-1}$. In the second phase (step 5), we solve the equations satisfied by the binary variables π_i and finally get the p_k's.

Algorithm:

1. Initialization: $K = 1$, $K_1 = 0$, $K_2 = 1$ and p_0, p_{d-2}, p_{d-1}, p_d are initialized as in corollary 2.

<u>Phase 1</u>: 2. At the beginning of this step, we already have $p_0, \ldots p_{K-1}$ and $p_{d-2K+2}, \ldots, p_d$ known as functions of the binary variables $\pi_0, \ldots, \pi_{K-2}$. We rewrite equation (24) for $k = K$ as

$$p_K^2 + b_K p_K + c_K = 0 \tag{25}$$

where $c_K = \left(\sum_{i=0}^{K-1} p_i^2 p_{d-K+i}^2 \alpha^{2i} + \sqrt[4]{\beta}\sqrt{\alpha}^{d+2K} \sum_{i=1}^{\lfloor \frac{K}{2} \rfloor} p_{K-2i}\varepsilon_{d-K+2i,i} \right)$ $/ \left(\alpha^{2K} \sqrt[4]{\alpha}\right)$ and $b_K = \sqrt[4]{\beta}\sqrt{\alpha}^{d+2K} / (\alpha^{2K} \sqrt[4]{\alpha})$. So, c_K is a multivariate polynomial in the unknowns $\pi_0, \ldots, \pi_{K-2}$.
Let $c_K/b_K^2 = \sum_{(\mu_0,\ldots,\mu_{K-2}) \in \{0,1\}^{K-1}} C_\mu \pi_0^{\mu_0} \ldots \pi_{K-2}^{\mu_{K-2}}$. Equation (25) has a solution if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(c_K/b_K^2) = 0$, that is to say,

$$\sum_{\substack{(\mu_0,\ldots,\mu_{K-2}) \in \{0,1\}^{K-1} \\ \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(C_\mu)=1}} \pi_0^{\mu_0} \ldots \pi_{K-2}^{\mu_{K-2}} = 0. \tag{26}$$

The left hand side of equation (26) can be

(a) 1: Then E_a and E_b are not isogenous and we return FAIL.

(b) 0: We set $p_K = b_K \pi_{K-1} + b_K \sum_{(\mu_0,\ldots,\mu_{K-2})\in\{0,1\}^{K-1}} P_\mu \pi_0^{\mu_0} \ldots \pi_{K-2}^{\mu_{K-2}}$ where $\pi_{K-1} \in \mathbb{F}_2$ and P_μ is any solution of $X^2 + X + C_\mu = 0$ (we easily check that this formula gives us the two solutions of equation (25)).

(c) a multivariate polynomial with coefficients in $\mathbb{F}_2$: We get a monomial from equation (26) as a function of the others and substitute it in c_K/b_K^2 to obtain p_K as in step 2b. Whenever it is possible, we choose for this monomial a single variable π_k (this is always the case in practice) and substitute it in $p_0, \ldots p_{K-1}$ and $p_{d-2K+2}, \ldots, p_d$ in order to decrease the number of binary variables to handle.

Finally, we increment K. If $K > d - 2K + 1$ then we go to step 5.

3. We set $K_1 = K$ and we extract p_{d-2K+1} as a function of $\pi_0, \ldots, \pi_{K-2}$ from equation (22) for $k = K_1$. If $K > d - 2K$ then we go to step 5.
4. We set $K_2 = K - 1$ and we extract p_{d-2K} as a function of $\pi_0, \ldots, \pi_{K-2}$ from equation (23) for $k = K_2$. Then we return to step 2 if $K \neq d - 2K$.

Phase2: 5. At this step, each p_i, $i = 0, \ldots, d$, is a multivariate polynomial in at most $K - 1$ binary variables, $\pi_0, \ldots, \pi_{K-2}$. Furthermore, we have $K = (d+2)/3$ (resp. $(d+1)/3$, $d/3$), $K_1 = (d-1)/3$ (resp. $(d+1)/3$, $d/3$) and $K_2 = (d-4)/3$ (resp. $(d-5)/3$, $d/3 - 1$) according to $d \bmod 3$. So, in any case, it remains $d - 1 - K_1 - K_2 = K$ equations obtained from (22) and (23).

We substitute the p_i's in these K equations. It is then easy to get a variable π_{K-2} as a fraction of $\pi_0, \ldots, \pi_{K-3}$ from one of these equations, to substitute it in the K other equations and iterate until π_0. If the last two equations do not give the same value for π_0, E_a and E_b are not isogenous and we return FAIL. Otherwise we only have to go back to get step by step $\pi_1, \ldots, \pi_{K-2}$ and $p_1, \ldots, p_{d-3}$.

Example: In $\mathbb{F}_{2^{10}} \simeq \mathbb{F}_2[T]/(T^{10}+T^3+1)$ with the notation $\overline{\tau_0 + \tau_1 2 + \ldots + \tau_9 2^9} = \tau_0 + \tau_1 T + \ldots + \tau_9 T^9$, we are going to show how we can compute an isogeny of degree $\ell = 37$ between $E_{\overline{6}}$ and $E_{\overline{272}}$. Here, $d = 18$, $\alpha = \overline{794}$ and $\beta = \overline{6}$.

First we get at step 1 of the algorithm $p_0 = \overline{153}$, $p_{16} = \overline{334}$, $p_{17} = \overline{796}$, $p_{18} = \overline{1}$. Then the first phase of the algorithm consists of these 5 iterations:

K	1	2	3	4	5
b_K	$\overline{253}$	$\overline{212}$	$\overline{536}$	$\overline{575}$	$\overline{470}$
c_K	$\overline{151}$	$\overline{590}\pi_0 + \overline{451}$	$\overline{847} + \overline{58}\pi_0 + \overline{453}\pi_1$	$\overline{374} + \overline{574}\pi_0 + \overline{804}\pi_1 + \overline{387}\pi_2$	$\overline{669} + \overline{353}\pi_0 + \overline{141}\pi_1 + \overline{492}\pi_0\pi_1 + \overline{487}\pi_2 + \overline{418}\pi_3$
p_K	$\overline{253}\pi_0 + \overline{581}$	$\overline{212}\pi_2 + \overline{609}\pi_1 + \overline{444}$	$\overline{536}\pi_2 + \overline{182}\pi_1 + \overline{412}\pi_0 + \overline{329}$	$\overline{575}\pi_3 + \overline{77}\pi_2 + \overline{24}\pi_1 + \overline{574}\pi_0 + \overline{94}$	$\overline{470}\pi_4 + \overline{741}\pi_3 + \overline{86}\pi_2 + \overline{849}\pi_0\pi_1 + \overline{656}\pi_1 + \overline{449}\pi_0 + \overline{724}$
p_{d-2K-1}	$\overline{6}\pi_0 + \overline{364}$	$\overline{6}\pi_1 + \overline{529}\pi_0 + \overline{121}$	$\overline{6}\pi_2 + \overline{529}\pi_1 + \overline{268}\pi_0 + \overline{611}$	$\overline{6}\pi_3 + \overline{529}\pi_2 + \overline{570}\pi_1 + \overline{822}\pi_0 + \overline{853}$	$\overline{6}\pi_4 + 529\pi_3 + \overline{566}\pi_2 + \overline{521}\pi_0\pi_1 + \overline{187}\pi_1 + \overline{23}\pi_0 + \overline{434}$
p_{d-2K-2}	$\overline{590}\pi_0 + \overline{451}$	$\overline{590}\pi_1 + \overline{811}\pi_0 + \overline{391}$	$\overline{590}\pi_2 + \overline{571}\pi_1 + \overline{802}\pi_0 + \overline{450}$	$\overline{590}\pi_3 + \overline{571}\pi_2 + \overline{320}\pi_1 + \overline{53}\pi_0 + \overline{575}$	$\overline{590}\pi_4 + \overline{571}\pi_3 + \overline{197}\pi_2 + \overline{514}\pi_0\pi_1 + \overline{647}\pi_1 + \overline{23}\pi_0 + \overline{240}$

In the second phase (step 5), equation (22) for $k = 7, 8$ and equation (23) for $k = 6, 7, 8, 9$ yield

$$\overline{331} + \overline{615}\pi_0 + \overline{438}\pi_1 + \overline{436}\pi_2 + \overline{331}\pi_3 = 0 \tag{27}$$

$$\overline{168} + \overline{125}\pi_0 + \overline{867}\pi_1 + \overline{384}\pi_0\pi_1 + \overline{350}\pi_2 + \overline{795}\pi_3 + \overline{947}\pi_4 = 0 \tag{28}$$

$$\overline{444} + \overline{399}\pi_0 + \overline{238}\pi_1 + \overline{849}\pi_0\pi_1 + \overline{523}\pi_2 + \overline{991}\pi_3 + \overline{611}\pi_4 = 0 \tag{29}$$

$$\overline{611} + \overline{217}\pi_0 + \overline{245}\pi_1 + \overline{654}\pi_0\pi_1 + \overline{268}\pi_2 + \overline{522}\pi_3 + \overline{105}\pi_4 = 0 \tag{30}$$

$$\overline{214} + \overline{574}\pi_0 + \overline{666}\pi_1 + \overline{848}\pi_0\pi_1 + \overline{255}\pi_2 + \overline{2}\pi_3 + \overline{212}\pi_4 = 0 \tag{31}$$

$$\overline{127} + \overline{163}\pi_0 + \overline{111}\pi_1 + \overline{394}\pi_0\pi_1 + \overline{704}\pi_2 + \overline{851}\pi_3 + \overline{812}\pi_4 = 0 \tag{32}$$

With equation (29), we obtain $\pi_4 = \overline{843} + \overline{935}\pi_0 + \overline{255}\pi_1 + \overline{256}\pi_0\pi_1 + \overline{470}\pi_2 + \overline{842}\pi_3$. Once substituted π_4, equation (28) yields $\pi_3 = \overline{1} + \overline{876}\pi_0 + \overline{103}\pi_1 + \overline{796}\pi_2$. Then π_4 and π_3 substituted in equation (27) yields $\pi_2 = \overline{979}\pi_0 + \overline{144}\pi_1 + \overline{194}\pi_0\pi_1$. Afterwards, π_4, π_3 and π_2 substituted in equation (30) yields $\pi_1 = \pi_0/(\overline{176} + \overline{795}\pi_0)$ and once substituted π_4, π_3, π_2 and π_1 , equation (31) gives $\pi_0 = 0$, and we only have to check that equation (32) is trivial, which is the case. Therefore, $\pi_1 = 0$, $\pi_2 = 0$, $\pi_3 = 1$, $\pi_4 = 1$, and

$$\begin{aligned} P(X) = & X^{18} + \overline{514}\, X^{17} + \overline{560}\, X^{16} + \overline{573}\, X^{15} + \overline{753}\, X^{14} + \overline{364}\, X^{13} + \overline{709}\, X^{12} + \\ & \overline{314}\, X^{11} + \overline{752}\, X^{10} + \overline{627}\, X^{9} + \overline{300}\, X^{8} + \overline{986}\, X^{7} + \overline{129}\, X^{6} + \overline{744}\, X^{5} + \\ & \overline{318}\, X^{4} + \overline{549}\, X^{3} + \overline{905}\, X^{2} + \overline{295}\, X + \overline{465}. \end{aligned}$$

Remark: When E_a and E_b are isogenous of degree ℓ, most of the time there are only two isogenies from E_a and E_b defined over $\mathbb{F}_{2^n}$ (an isogeny and its opposite) and in this case, the algorithm always produced only one solution in our experiments. If by chance, the system of equations had several solutions, we would have to compute all of them and test if each solution is an isogeny or not. When there are more than two isogenies from E_a to E_b, these systems have several solutions. When E_a and E_b are not isogenous, these systems have in practice no solution and this fact can be detected quickly because at step 2, equation (26) is most of the time false (typically $1 = 0$) for a small index K.

At step 5 of the algorithm, the K equations obtained from (22) and (23) lead in fact to nK equations between the binary unknowns π_i once rewritten in a polynomial basis $1,\ldots,\ T^{n-1}$ of $\mathbb{F}_{2^n}$. Firstly, that means this system is very constrained, secondly, we can use this to speed up the computations. For instance, in the previous example, the equation $\pi_1(\overline{176}+\overline{795}\pi_0) = \pi_0$ leads to $\pi_1\pi_0T^9 + \pi_1\pi_0T^8 + \pi_1T^7 + \pi_1T^5 + \pi_1(\pi_0+1)T^4 + \pi_1\pi_0T^3 + \pi_1\pi_0T + \pi_1\pi_0 + \pi_0 = 0$ and we immediately find $\pi_0 = 0$ and $\pi_1 = 0$.

Complexity: The complexity of this algorithm is hard to estimate. As sketched at the beginning of this section, the number of variables remains more or less the same during the computation because of equation (26). For $K > 10$, each time we write p_K as a function of a new binary variable π_{K-1}, we observed we are able to get π_k $(k < K-1)$ as a polynomial function of the other π_i's except a logarithmic number of times. Therefore, asymptotically, we assume that the number of variables π_i grows heuristically as $O(\log \ell)$.

With this hypothesis, the maximal number of terms in the multivariate polynomials computed in this algorithm is at most $O(2^{\log(\ell)}) = O(\ell)$ and so we estimate that the cost of this algorithm is probably at most $O(\ell^3)$ multiplications in $\mathbb{F}_{2^n}$.

With regard to the storage, we have to write in phase 1 each p_K as a multivariate polynomial of $O(\log \ell)$ binary variables, that is to say a storage of at most $O(\ell^2)$ elements of $\mathbb{F}_{2^n}$. In phase 2, we have to write $d/3$ equations as a function of $O(\log \ell)$ binary variables, which yields a storage of at most $O(\ell^2)$ too.

4.3 Practical improvements

The improvements described here are based on equation (7) and on equation (4). They are practical in the sense that they probably do not change the asymptotic complexity of the algorithm described in section 4.2, but decrease in practice its computation time.

Vélu's equation. Equation (7) enables us to decrease the number of binary variables π_i needed in the algorithm by half. This equation leads to the following $d+1$ equations,

$$\boxed{\begin{aligned}&\alpha^{2k-d}\sqrt{\alpha\beta}p_k^2+\alpha p_{d-k}^2=\\&\qquad\qquad\begin{cases}\displaystyle\sum_{i=0}^{k} p_{d-2i-1}p_{d-2k+2i}, & \text{if } k=0,\ldots,\left\lfloor\dfrac{d-1}{2}\right\rfloor,\\ \displaystyle\sum_{i=0}^{d/2-1} p_{d-2i-1}p_{2i}, & \text{if } d \text{ is even and } k=\dfrac{d}{2},\\ \displaystyle\sum_{i=k-\lfloor\frac{d}{2}\rfloor}^{\lfloor\frac{d-1}{2}\rfloor} p_{d-2i-1}p_{d-2k+2i}, & \text{if } k=\left\lfloor\dfrac{d+3}{2}\right\rfloor,\ldots,d.\end{cases}\end{aligned}} \tag{33}$$

Using this equation is straightforward. At step 2 of the algorithm when $K=1 \bmod 2$ ($K\geq 3$), we replace the computation of p_K with equation (24) by the computation of p_K with equation (33) for $k=K$. In this way we directly get p_K as a function of p_1, …, p_{K-1} and we do not have to introduce a new binary variable π_K. So, we are able to express p_0, …, p_d as functions of at most $d/6$ binary variables instead of at most $d/3$. Unfortunately, in this case, equation (26) becomes useful later in practice ($K\leq 22$, which is twice larger than initially) and so for a "large" degree ℓ ($\ell>200$), the number of variables π_i to handle is more or less the same as above.

Multiplication by three. Our last improvement is a heuristic improvement based on equation (21) with $m=3$. It enables us to express a variable π_i as a function of π_0,… π_{i-1} much earlier than with equation (26). This system is

$$\boxed{\begin{aligned}&\sideset{}{'}\sum_{\substack{k\\0,\lceil\frac{i-4-d}{8}\rceil}}^{\lfloor\frac{i-4}{8}\rfloor,d} p_k^8q_{i-4-8k}+\beta^2\sideset{}{'}\sum_{\substack{k\\0,\lceil\frac{i-d}{8}\rceil}}^{\lfloor\frac{i}{8}\rfloor,d} q_k^8q_{i-8k}=\\&\qquad\sideset{}{'}\sum_{\substack{j\\0,i-d}}^{8d+4,i} q_{i-j}T_{i,j}+\sideset{}{'}\sum_{\substack{j\\0,\lceil\frac{i-3-d}{2}\rceil}}^{\lfloor\frac{i-3}{2}\rfloor,4d} q_{i-2j-3}\sideset{}{'}\sum_{\substack{k\\0,j-d}}^{j,3d} q_{j-k}^2\sideset{}{'}\sum_{\substack{l\\0,\lceil\frac{k-d}{2}\rceil}}^{d,\lfloor\frac{k}{2}\rfloor} p_l^4p_{k-2l}^2.\end{aligned}} \tag{34}$$

where $i=4,..,9d$, $T_{i,j}$ is a constant which depends on α and $\sideset{}{'}\sum_{\substack{j\\k,l}}^{m,n}$ must be read as $\sum_{j=\max(k,l)}^{\min(m,n)}$.

From this expression, we deduce that at step 2 of the algorithm, we can compute this equation for $i\leq 2K$. So, we obtain new relations between the binary variables π_i. In practice, we observed that it is enough before computing p_K at step 2 of the algorithm to compute equation (34) for $i=2K-1$ when $K=1 \bmod 2$, the other equations giving no new information. In this case, for K large enough, we can write one variable π_i as a function of the others. In practice, this phenomenon happens already for $K=11$. So, at the expense of an additional computation, the number of binary variables we have to handle is asymptotically smaller compared to the original algorithm.

5 Results

We implemented in C the algorithm described in section 4.2 (called `MULTBY2`) and its improvements described in section 4.3 (called `VELU`) and 4.3 (called `MULTBY3`). We did not implement the methods of section 4.1 because we estimate that the resources (space and time) they need are too high. Furthermore, we compare these algorithms with the implementation of Couveignes's ideas [4] as done in [7], which we call COUVEIGNES. Notice that the multivariate polynomials we have to manipulate in this case are sparse, so we implemented them as lists.

We measured the time needed to compute isogenies of prime degrees between ℓ such that $3 < \ell < 500$ in $\mathbb{F}_{2^{10}} \simeq \mathbb{F}_2[T]/(T^{10} + T^3 + 1)$ on a DEC Alpha workstation and the number of binary variables π at the beginning of step 5. The results are given in figure 1 and 2.

As in [6], we did benchmarks to count points of the elliptic curve $E_{\overline{91128}}$ defined over $\mathbb{F}_{2^{300}} \simeq \mathbb{F}_2[T]/(T^{300} + T^5 + 1)$. Time to compute isogenies is now completely negligible as shown in the following table.

	COUVEIGNES	MULTBY2	VELU	MULTBY3
Isogenies (s)	22974	146	59	71
Total (s)	30221	6103	6074	6079

6 Conclusion

We outlined in this paper nice properties of isogenies of degree ℓ in $\mathbb{F}_{2^n}$, and we showed how to take advantage of these properties to compute them efficiently. In practice, the algorithm we described is, as far as we know, the best method to solve this problem. Time needed to compute isogenies while counting the number of points of an elliptic curve is now negligible whereas it used to be the major cost. Moreover, the storage needed is much smaller than what was necessary before.

In finite fields of small characteristic greater than 2, it remains to be seen if we can (or not) adapt these ideas, and possibly to compare them with a new algorithm of Couveignes [3]. Lastly, as noticed in [7], the break even point between methods to compute isogenies in large characteristic and methods for small characteristic is not clear. This will be the subject of further research.

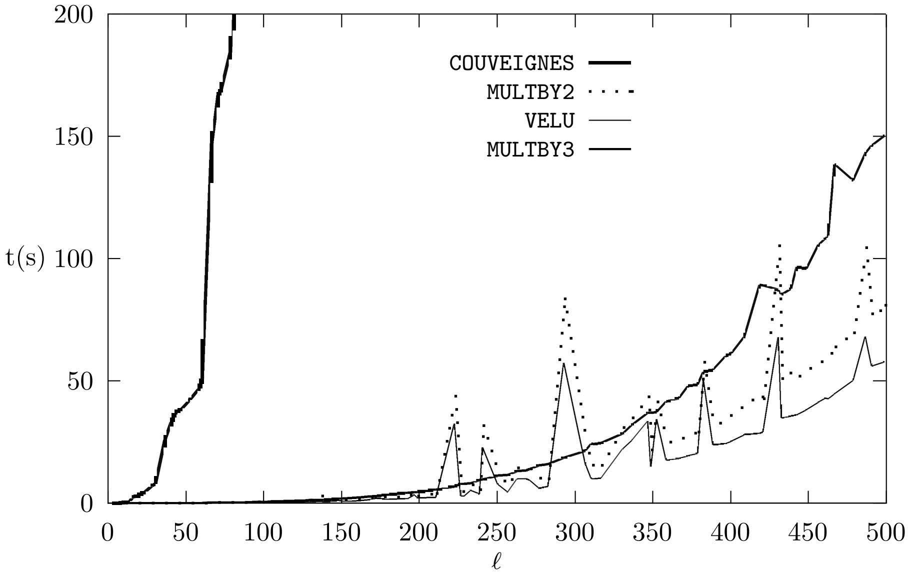

Fig. 1. Time needed to compute isogenies of degree ℓ in $\mathbb{F}_{2^{10}}$

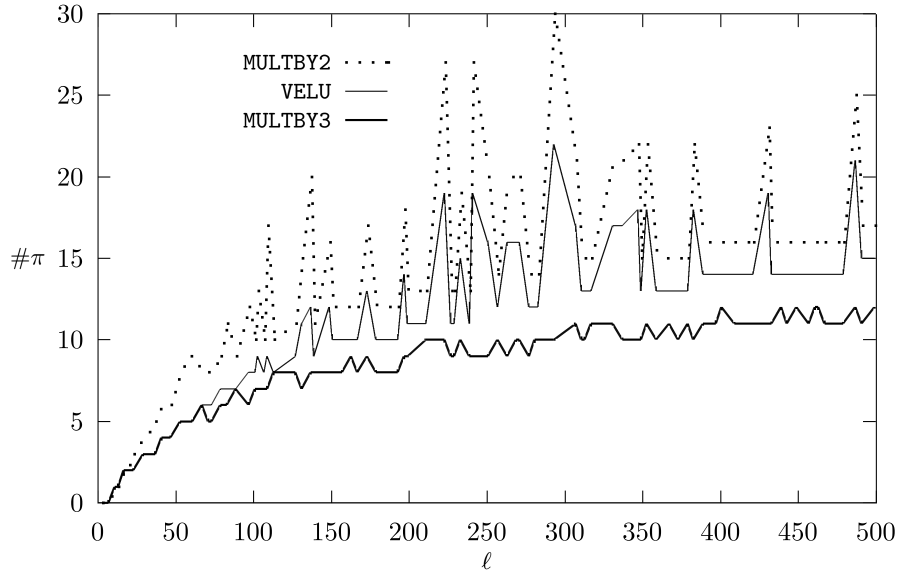

Fig. 2. Number of binary variables needed to compute isogenies of degree ℓ in $\mathbb{F}_{2^{10}}$

Acknowledgments: The author wants to express its gratitude to F. Morain. His deep knowledge of isogenies in finite fields of large characteristic was an invaluable help. Moreover, he pointed out the importance of Vélu's formulae and read carefully the drafts of this paper. Thanks a lot to J.-M. Couveignes for its careful reading of first versions of this paper and to have outlined the central role played by points of order 2 in elliptic curves over $\mathbb{F}_{2^n}$. Many thanks to J.-M. Steyaert too for his advice to solve the systems described in the second part of this paper.

References

[1] A. O. L. Atkin and François Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, July 1993.

[2] Henri Cohen. *A course in algorithmic algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, 1993.

[3] J. M. Couveignes. Computing l-isogenies with the p-torsion. In H. Cohen, editor, *ANTS-II*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 59–65. Springer-Verlag, 1996.

[4] Jean-Marc Couveignes. *Quelques calculs en théorie des nombres*. Thèse, Université de Bordeaux I, July 1994.

[5] Hendrik W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Math.*, 126:649–673, 1987.

[6] R. Lercier and F. Morain. Counting the number of points on elliptic curves over finite fields: strategies and performances. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, number 921 in Lecture Notes in Comput. Sci., pages 79–94, 1995. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

[7] R. Lercier and F. Morain. Counting the number of points on elliptic curves over F_{p^n} using Couveignes's algorithm. Rapport de Recherche LIX/RR/95/09, Laboratoire d'Informatique de l'École polytechnique (LIX), 1995. Available at `http://lix.polytechnique.fr/~morain/Articles`.

[8] Alfred J. Menezes. *Elliptic curve public key cryptosystems*. Kluwer Academic Publishers, 1993.

[9] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.

[10] René Schoof. Counting points on elliptic curves over finite fields. To appear in Proc. Journées Arithmétiques 93, January 1995.

[11] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.

[12] J. Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971. Série A.