FAST ADDITION ON NON-HYPERELLIPTIC GENUS 3 CURVES

STÉPHANE FLON, ROGER OYONO, CHRISTOPHE RITZENTHALER

Stéphane Flon, Université de Lille 1,
UFR de mathématiques, Cité scientifique, F-59655 Villeneuve d'Ascq, France
email: Stephane.Flon@math.univ-lille1.fr

Roger Oyono, Institut für Experimentelle Mathematik,
Universität Essen, Ellernstr. 29, D-45326 Essen, Germany
email: oyono@exp-math.uni-essen.de

Christophe Ritzenthaler, Leiden University,
Mathematical Institute, P.O. Box 9512
2300 RA Leiden, The Netherlands
email: ritzenth@math.jussieu.fr

Abstract. We present a fast addition algorithm in the Jacobian of a genus 3 non-hyperelliptic curve over a field of any characteristic. When the curve has a rational flex and $\mathrm{char}(k) > 5$, the computational cost for addition is $148M + 15SQ + 2I$ and $165M + 20SQ + 2I$ for doubling. An appendix focuses on the computation of flexes in all characteristics. For large odd q, we also show that the set of rational points of a non-hyperelliptic curve of genus 3 can not be an arc.

Introduction

Thanks to the papers [2, 7, 12, 8, 25] of Gaudry, Enge and others, the only curves considered to be suitable for cryptographic purposes have genus $1, 2$ or 3. As a prerequisite to create a discrete logarithm framework in the Jacobian of such a curve, its group law should be efficiently computable. Many papers were already devoted to this problem [18, 13, 19, 17, 23]. As far as the authors know, the only incomplete case was that of genus 3 non-hyperelliptic curves (there existed fast algorithms for Picard curves and $C_{3,4}$ curves already, see [9, 3, 5, 6]). Thanks to the algorithm given in this paper for the addition in the Jacobian of a genus 3 non-hyperelliptic curve, and the preceding ones on hyperelliptic curves, everyone can now create an efficient cryptographic system based on any presumably suitable algebraic curve.

The paper begins with a discussion on the general framework where our algorithm applies (see also the Appendix). In the second part, we describe it geometrically. In the next part, which is the core of the paper, we write down an algebraic version of the algorithm. Lastly, we present two applications,

Date: May 18, 2004.

Key words and phrases. Jacobians, non-hyperelliptic curves, algebraic curves cryptography, discrete logarithm problem.

The third author acknowledges the financial support provided through the European Community's Human Potential Programme under contract HPRN-CT-2000-00114, GTEM.

related to point counting: one to make AGM algorithm complete, and the other one on simple factors of dimension 3 of Jacobians of modular curves.

1. General framework for the algorithm

Let C be a non-singular curve of genus g over a field k. Let D^∞ be an effective k-rational divisor of degree g. A consequence of Riemann-Roch theorem is the following representation of divisors :

Fact (Representation of divisors)**.** *Let D be a degree 0 divisor of C over k (i.e. an element of $Div_k^0(C)$). Then there exists an effective divisor E over k of degree g such that $E - D^\infty \sim D$. Generically, the divisor E is unique.*

We now restrict ourselves to the case where C is a genus 3 non-hyperelliptic curve. Thanks to the canonical embedding, we may assume that C is a smooth plane quartic (this is example 5.2.1 of [14]). We denote by x, y, z (or sometimes x_1, x_2, x_3) the chosen coordinates in $\mathbb{P}^2$.

We denote by $(*)$ the following condition : *There is a rational line l^∞ which crosses C in four (not necessarily distinct, but with multiplicity then) k-points $P_1^\infty, P_2^\infty, P_3^\infty, P_4^\infty$.*

In the following, we will choose D^∞ to be the divisor $P_1^\infty + P_2^\infty + P_3^\infty$. This special case will allow us to find a geometric description of the group law on the Jacobian of C (see the theorem in the next section). Moreover, k will denote a finite field $\mathbb{F}_q$ (with $q = p^n$ for a certain prime p).

Recall that for a quartic, there are 5 possibilities for the intersection divisor $(l^\infty \cdot C) = P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty$:

(1) The four points are pairwise distinct. This is the generic position.
(2) $P_1^\infty = P_2^\infty$, then l^∞ is tangent to C at P_1^∞.
(3) $P_1^\infty = P_2^\infty = P_4^\infty$. The point P_1^∞ is then called a *flex*. As a linear intersection also represents the canonical divisor, these points are exactly the ones where a regular differential has a zero of order 3. They are thus the Weierstrass points of C.
(4) $P_1^\infty = P_2^\infty$ and $P_3^\infty = P_4^\infty$. The line l^∞ is called a *bitangent* of the curve C. It is well known (see for example [20]) that if $\mathrm{char}(k) \neq 2$ then C has exactly 28 bitangents. If $\mathrm{char}(k) = 2$, then C has respectively $7, 4, 2$, or 1 bitangents, according to the 2-rank of its Jacobian (resp. $3, 2, 1, 0$).
(5) $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$. The point P_1^∞ is called a *hyperflex*. Generically, such a hyperflex does not exist (*i.e.* the set of quartics with at least one hyperflex is of codimension 1 in the space of quartics).

The efficiency of the algebraic version of the algorithm will depend on the choice of l^∞ (see section 3). We now look for situations where the condition $(*)$ is fulfilled:

Proposition 1. *The condition $(*)$ is fulfilled in the following cases:*

Condition on p	*Condition on* n	*Condition on* q	*Condition on* $\lvert C(k)\rvert$
$p > 2$		$q \geq 10^6$	
$p > 2$		$q > 8$	$\lvert C(k)\rvert \geq q - \sqrt{q}/4 + 7/4$
$p = 2$	$n > 3$	$q > 8$	$\lvert C(k)\rvert \geq q + 3$

In particular for large odd q, there is always four collinear points on a non-singular quartic.

Proof. Suppose that condition $(*)$ fails. Then no three points in $\mathcal{K} = C(k)$ are collinear, and the set $C(k)$ is called a $|C(k)|$-*arc*. Following [15], this implies that $|C(k)| \leq q+2$ if $p=2$ (from which the last row of the table follows), and that $|C(k)| \leq q+1$ if p is odd. Moreover, if p is odd, one can give an explicit bound $m'(2,q)$, such that every r-arc with $r > m'(2,q)$ is a subset of the rational points of a conic (see [15, Tab 1.3]). Thus, if $|C(k)| \geq \max(9, m'(2,q)+1)$, the quartic through these points has to properly contain a conic, but this contradicts its irreducibility. The second row of the table in the proposition immediately follows from this remark and from [15, Tab 1.3]. We now deal with the first row, for which we do not want a condition on the curve. We may suppose that $|C(k)| \leq m'(2,q)$. As $q \geq 10^6$, one has

$$(3q+5)/4 < |C(k)| \leq m'(2,q)$$

(the first inequality is obtained from Hasse-Weil formula, and is already true for $q > 24^2$).

We will use the results of [26], for which we refere for both notations and propositions. It is classical to associate to the arc $\mathcal{K}$ a plane curve $\mathcal{E}$ in the dual plane, which is the enveloppe of the 1-secants of $\mathcal{K}$ (the rational lines which cut $\mathcal{K}$ in one point). As the condition $(*)$ fails, every tangent of C at a point of $\mathcal{K}$ is a 1-secant. By Bézout theorem, the dual curve C^* is an irreducible component of $\mathcal{E}$. Let P_0 be a point of $C(k)$. As the condition $(*)$ fails, P_0 is neither on a bitangent nor a flex. Let l_0 be the tangent of C at P_0. By the properties of the dual curve, the point $l_0^* \in C^*$ is a non-singular rational point. Moreover, by [26, Th. 5.2.(3)], $i(\mathcal{E}, P_0^*; l_0^*) = 2 = i(C^*, P_0^*; l_0^*)$ so C^* is not a multiple component of $\mathcal{E}$. Moreover, the point l_0^* is a *special point* and C^* is an *irreducible enveloppe associated to* l_0^*. Using the notations of [26, Sec. 5.2], we deduce that $\nu_4 \leq 2\deg(C^*)$ (where ν_4 is the 4th positive $\mathbb{F}_q$-Frobenius order of a certain linear series), and thus $\nu_4 \leq 24$ (the degree of the dual of a degree n non-singular curve is equal to $n(n-1)$). We now apply [26, Prop. 5.11]:

$$|C(k)| \leq \min\left(q - \frac{1}{4}\nu_4 + \frac{7}{4}, \frac{28+4\nu_4}{29+4\nu_4}q + \frac{32+2\nu_4}{29+4\nu_4}\right).$$

For $q \geq 10^6$, $|C(k)| < q+1-6\sqrt{q}$ which is absurd. □

Remark 1. The given bounds may be improved, especially in the case $p=2$ (see [15] ; note that (the dimension one part of) a hyperoval is a parametric curve). It is possible that one may extend the preceding argument to characteristic 2.

2. Geometric description of the algorithm

From now on, we assume that condition $(*)$ is fulfilled.

We recall that we then choose $D^\infty = P_1^\infty + P_2^\infty + P_3^\infty$. For an element D in $\mathrm{Div}_k^0(C)$, let D^+ be an effective divisor (generically unique) such that $D^+ - D^\infty \sim D$. By abuse of language we say that a curve C' *goes through* nP if $i(C, C'; P) = n$, where $i(C, C'; P)$ denotes the intersection multiplicity of C and C' at P.

Theorem. *Let $D_1, D_2 \in Div_k^0(C)$. Then $D_1 + D_2$ is equivalent to a divisor $D = D^+ - D^\infty$, where the points in the support of D^+ are given by the following algorithm:*

(1) *Take the unique cubic E which goes (with multiplicity) through the support of D_1^+, D_2^+ and $P_1^\infty, P_2^\infty, P_4^\infty$. This cubic also crosses C in the residual effective divisor D_3.*
(2) *Take the unique conic Q which goes through the support of D_3 and P_1^∞, P_2^∞. This conic also crosses C in the residual effective divisor D^+.*

Proof. C being canonically embedded, $(E \cdot C) \sim 3K$, where $(E \cdot C)$ denotes the intersection divisor of E with C, and where K is the canonical divisor of C. Therefore we have

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + D_3 \sim 3K.$$

Similarly, $(Q \cdot C) \sim 2K$ so

$$D_3 + P_1^\infty + P_2^\infty + D_e \sim 2K$$

and $(l^\infty \cdot C) = P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty \sim K$. Combining these three relations, we obtain

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + D_3 \sim D_3 + P_1^\infty + P_2^\infty + D_e + P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty$$

so

$$D_1^+ + D_2^+ \sim D_e + D^\infty.$$

Now we subtract $2D^\infty$ on both sides :

$$D_1 + D_2 \sim D_e - D^\infty \sim D$$

So $D_e = D^+$. □

3. Algebraic description

In this section, we give an algebraic transcription of the algorithm. It depends slightly on the line l^∞. In fact, the fastest algorithm is the one for the hyperflex case, and then that of the flex case. We first look for simple representations of the curve and its divisors: we may suppose (after a k-linear transformation) that P_1^∞ is a point at infinity (*i.e.* such that its z-coordinate is 0), and that l^∞ is the line $z = 0$. Let $f(x, y) = 0$ be an affine equation of C. We now come to the representation, called *Mumford representation*, of a divisor $D \in \mathrm{Div}_k^0(C)$ by a couple (u, v) of polynomials. It is unique under the following generic assumptions on D, which define a *typical divisor*:

(1) The three points in the support of D^+ are non-collinear. In this case D^+ is unique: in fact if $P_1 + P_2 + P_3 + (f) = Q_1 + Q_2 + Q_3$ then $f \in \mathcal{L}(P_1 + P_2 + P_3)$ and f has to be constant by Riemann-Roch theorem.
(2) There is no point at infinity in the support of D^+. Let $P_i = (x_i : y_i : 1)$ $(i = 1, 2, 3)$ be the three points in the support of D^+ and $u = \prod(x - x_i)$. Since D^+ is a rational divisor, $u \in k[x]$.

(3) The $(x_i)_{i=1,2,3}$ are distinct. In this case, there exists a unique polynomial $v \in k[x]$ of degree 2 such that $y_i = v(x_i)$ for $i = 1, 2, 3$ (it is just the interpolation polynomial).

Conversely, given a couple (u, v) such that

- $u, v \in k[x]$,
- $u = \prod(x - x_i)$ is monic of degree 3 and with simple roots,
- $\deg(v) = 2$,
- $u | f(x, v(x))$,

then $P_1 + P_2 + P_3 - D^\infty$ is a rational typical divisor of C (where, for $i \in \{1, 2, 3\}$, we have $P_i = (x_i : v(x_i) : 1)$).

At last, it is obvious that the addition of two typical divisors is generically a typical divisor. As we had cryptographic applications in mind, we implemented our algorithm only in that case.

3.1. **The tangent case.**

After a linear transformation, we may suppose that l^∞ is tangent at $P_1^\infty = (0 : 1 : 0)$ and goes through $P_4^\infty = (1 : 0 : 0)$. An equation for C is then of the form

$$y^3 + h_1 y^2 + h_2 y = f_4,$$

where $h_1, h_2, f_4 \in \mathbb{F}_q[x]$ and $\deg(h_1) \leq 2, \deg(h_2) \leq 3, \deg(f_4) \leq 4$. If $\deg(f_4) = 4$, we can assume in addition that f_4 is monic.
We then have

Lemma 1. *The cubic E from the theorem is generically of the form*

$$y^2 + s \cdot y + t,$$

where s and t are polynomials in x, with $\deg(s) \leq 2$ *and* $\deg(t) \leq 2$.
The conic Q is of the form

$$y - v,$$

where $v \in \mathbb{F}_q[x]$ and $\deg(v) = 2$.

This gives the following algorithm, which is a slight adaptation of the one for Picard curves [9]:

Algorithm 1 Algorithm for Addition.

```
INPUT: $D_1 = (u_1, v_1)$ and $D_2 = (u_2, v_2)$
OUTPUT: $D_1 + D_2 = (u_{D_1+D_2}, v_{D_1+D_2})$

1.  Computation of the cubic $E$
    Addition
        compute the inverse $t_1$ of $v_1 - v_2$ modulo $u_2$
        compute the remainder $r$ of $(u_1 - u_2)t_1$ by $u_2$
        solve the linear equations given by the following conditions
            $\begin{cases} \deg_x(-v_1(v_1 + s) + u_1\delta_1) = 2 & \text{(2 eq.)} \\ v_1 + v_2 + s \equiv r\delta_1 \quad [u_2] & \text{(3 eq.)} \end{cases}$
        where $s, \delta_1 \in k[x]$ with $\deg(s) = 2$ and $\deg(\delta_1) = 1$. Then
            $E = (y - v_1)(y + v_1 + s) + u_1\delta_1$
    Doubling
        compute $\omega_1 = (v_1^3 + v_1^2 h_1 + v_1 h_2 - f_4)/u_1$
        compute the inverse $t_1$ of $\omega_1$ modulo $u_1$
        compute the remainder $r$ of $(3v_1^2 + 2v_1 h_1 + h_2)t_1$ by $u_1$
        solve the linear equations given by the following conditions
            $\begin{cases} \deg_x(-v_1(v_1+s) + u_1\delta_1) = 2 & \text{(2 eq.)} \\ 2v_1 + s \equiv r\delta_1 \quad [u_1] & \text{(3 eq.)} \end{cases}$
        where $s, \delta_1 \in k[x]$ with $\deg(s) = 2$ and $\deg(\delta_1) = 1$. Then
            $E = (y - v_1)(y + v_1 + s) + u_1\delta_1$
2.  Computation of the conic $Q$
    compute $u' := Res^*(E, C, y)/(u_1 u_2)$
    compute the inverse $\alpha_1$ of $t - s^2 - h_2 + sh_1$ modulo $u'$
    compute the remainder $v'$ of $\alpha_1(st - th_1 - f_4)$ by $u'$
3.  Computation of $D_1 + D_2$
    $v_{D_1+D_2} := v'$
    $u_{D_1+D_2} := ((v^3 + v^2 h_1 + v h_2 - f_4)/(u'))^*$
    $D_1 + D_2 = (u_{D_1+D_2}, v_{D_1+D_2})$
```

For a polynomial g, we used the notation g^* to symbolize the quotient of g by its leading coefficient.

One may wonder about the special choice of the divisor D^∞. It was chosen so that the conic Q be of the form $y - v$. It thus gives directly the second part of the Mumford representation of the final divisor. Other choices imply using an auxiliary conic to find the representation.

We stress the fact that algorithm 1 is valid for any base field (*e.g.* characteristic 0 fields).

Comments. *To make the algorithm of the theorem more efficient, we used the following optimisations:*

1. *In order to reduce the number of field inversions, we used Montgomery's trick to compute simultaneous inversions. For the same reason, we computed almost inverses (using Bézout matrix), rather than inverses.*
2. *We used either Karatsuba or Toom-Cook (in case $p \neq 2, 3, 5$) trick to multiply two polynomials, and we computed only the coefficients we needed in the algorithm. For instance, as we only need to known the quotient of the resultant of ω and C by $u_1 u_2$, the degree ≤ 5 part of this resultant is irrelevant.*

3.2. **The flex case.** This case is the most interesting. Indeed, we will see that it seems to happen quite often. Moreover the expressions involved in the algorithm are very similar to those in the Picard curves [9] case, and decrease the number of operations.

Unfortunately, we don't know how to compute the probability for a quartic to have at least a rational flex. But we can have a guess on that number, coming from heuristic remarks from one side, and relying on numerical evidences from the other side. Here we suppose that $\mathrm{char}(k) > 3$.

Conjectural fact. *The probability that a smooth quartic has at least one rational flex is asymptotically, when q tends to ∞, equals to $1 - e^{-1} + \alpha$, with $|\alpha| \leq 10^{-25}$.*

Let $C : f = 0$ be the curve and $H : h = 0$ its Hessian (see Appendix). The curve H is of degree 6 and the $(C \cdot H)$ are the 24 flexes with multiplicities. Generically when $q >> 0$ we may suppose that no two flexes have the same abssicae. Then there is a rational flex if and only if the polynomial $\mathrm{Res}(f, h, y)$ has a root in k. If we suppose that these polynomials are uniformly distributed among the classes of splitting of polynomials of degree 24, then one only has to compute the probability that a polynomial of degree 24 has at least one linear factor in $\mathbb{F}_q$. Let $(\alpha_i)_{i \in \{1,\cdots,q\}}$ be an enumeration of $\mathbb{F}_q$.

Let S be the set of all monic polynomials of degree n and S_i the subset of S of polynomials having one or more factors of the form $x - \alpha_i, i = 1, \cdots, q$. Then $|S| = q^n$ and $|S_i| = q^{n-1}$. With the principle of inclusion and exclusion the number $N(n, q)$ of monic polynomials of degree n with one or more linear factors is equal to

$$N(n,q) = \sum_{i=1}^{n} \binom{q}{i} q^{n-i} (-1)^{i-1} \qquad \text{if } n < q,$$

and

$$N(n,q) = \sum_{i=1}^{q} \binom{q}{i} q^{n-i} (-1)^{i-1} \qquad \text{if } n \geq q.$$

After straightforward computations, one computes that the probability $P(n, q)$ that a monic polynomial of degree n has at least a linear factor in $\mathbb{F}_q$ is

$$P(n,q) = 1 - \left(1 - \frac{1}{q}\right)^q - \alpha_n(q), \qquad \text{where} \qquad \lim_{\substack{n \geq q \\ q \to \infty}} \alpha_n(q) = 0.$$

Already for $n = 24$ and $q \geq 2^{10}$ we have $|\alpha_n(q)| \leq 0.62 \cdot 10^{-25}$.

Remark 2. Computations realised with a bench of 10^6 non-singular quartics over $\mathbb{F}_{1009^2}$ and over $\mathbb{F}_{2^{17}+29}$ give the right percentage. In characteristics 2 and 3 the computation of flexes is a bit harder since $H(f) \equiv 0$. We refere to the appendix for a good replacement for the polynomial $H(f)$. Though the heuristic approach seems to extend also in these cases.

p	n	*Probabilities*
2	17	$632074/10^6 = 0.632074$
3	11	$632344/10^6 = 0.632344$
1009	2	$631358/10^6 = 0.631358$
$2^{17} + 29$	1	$632921/10^6 = 0.632921$

As in the tangent case, we can assume (after a linear transformation) that $l = l^\infty$ is tangent at the flex $P_1^\infty = (0 : 1 : 0)$, such that the curve is of the form

$$y^3 + h_1y^2 + h_2y = f_4,$$

where $h_1, h_2, f_4 \in \mathbb{F}_q[x]$ and $\deg(h_1) \leq 1, \deg(h_2) \leq 3, \deg(f_4) \leq 4$.
In the same way as for the Lemma 1 we obtain

Lemma 2. *The cubic E is generically of the form*

$$y^2 + s \cdot y + t,$$

where s and t are polynomials in x, with $\deg(s) \leq 1$ and $\deg(t) \leq 3$.
The conic Q is of the form

$$y - v,$$

where $v \in \mathbb{F}_q[x]$ and $\deg(v) = 2$.

The only difference with Algorithm 1 is that s and δ_1 have now degree 1. Computations are thus a lot easier: the linear system in step 1 consists only of 4 equations, and consequently, the resultant $\operatorname{res}(\omega, C, y)$ is easier to compute.

Furthermore, if $\operatorname{char}(k) \neq 3$, we can also assume (thanks to Tschirnhaus transformation) that C is of the following form:

$$y^3 + h_2y = f_4,$$

with h_2 and f_4 as above. If in addition $\operatorname{char}(k) \neq 2$, then we can assume that f_4 has no x^3 term. Using this form, computations of steps 2 and 3 will be much faster (both for addition and doubling). Moreover, step 1 will be slightly faster for doubling. In that case, an addition requires $148M + 15SQ + 2I$ and a doubling $165M + 20SQ + 2I$. The interested reader can find a program in MAGMA at the following webpage:

`http://www.exp-math.uni-essen.de/~oyono`

Remark 3. As explained in [4], one can try to use -2-adic expansion rather than usual 2-adic expansion, in order to save time for scalar multiplication. But this is only worthwile if the computation of $-(D_1 + D_2)$ is easier than that of $D_1 + D_2$. This only happens in the theorem if $P_1^\infty = P_2^\infty = P_4^\infty$. In that case (and only in that case), this leads to a saving of at least 10% for the computation of scalar multiples mD, assuming a ratio of 10 : 1 for inversions and 2 : 3 for squarings, in relation to multiplications.

3.3. **The hyperflex case.**

The algorithm is a special case of the version for flex. We recall that a generic non-singular quartic has no hyperflex. Still, if it has one, this point is automatically rational.

Proposition 2. *A non-singular plane quartic C with a hyperflex P is k-isomorphic to a $C_{3,4}$-curve of genus 3.*

Proof. By a linear rational transformation, we may suppose that P is the point $(0 : 1 : 0)$ and that the tangent in this point is the line at infinity. Therefore the equation of C is of the form

$$y^3 + h_1y^2 + h_2y = f_4$$

where h_i is a degree i polynomial and f_4 is a degree 4 monic polynomial. □

In case $\mathrm{char}(k) \neq 3$, we can assume that $h_1 = 0$ (and that f_4 has no x^3 term if in addition $\mathrm{char}(k) \neq 2$). Addition then requires $131M + 14SQ + 2I$ and a doubling requires $148M + 19SQ + 2I$. We refer to [9] for explicit formulae in the case of Picard curves. Note that thanks to the new remarks made in this paper, we can reduce the cost for addition in the case of Picard curves to $116M + 14SQ + 2I$ and to $133M + 19SQ + 2I$ for doubling.

Remark 4. Since there is only one point at infinity, there is an isomorphism between $\mathrm{Jac}(C)(k)$ and the Ideal Class group of $k[x, y]/f(x, y)$.

Remark 5. One may like to characterize Picard curves among $C_{3,4}$. It appears that Picard curves are exactly the $C_{3,4}$-curves with one hyperflex P^∞ and 4 distinct flexes $(P_i)_{i=1,\cdots,4}$ whose tangents are all concurrent at P^∞. To prove that, it is enough to see that the four flexes are collinear : indeed, since $P^\infty + 3P_i \sim K \sim 4P^\infty$, it follows $P_1 + P_2 + P_3 + P_4 \sim 4P^\infty$, so $(P_i)_{i=1,\cdots,4}$ are collinear. We take this line as the $y = 0$ line. The equation is then of the form $y^3 = f_4(x)$, with f_4 a monic polynomial in x of degree 4.

4. Two applications

We give here two applications of our algorithm, based on the fact that computing fastly in the Jacobian is of course linked to point counting.

4.1. **AGM-method.**

In [24], a quasi-quadratic time algorithm for point counting on a genus 3 ordinary non-hyperelliptic curve $\tilde{C}$ over $k = \mathbb{F}_{2^n}$ is described. The algorithm ended with a sign problem for the Frobenius polynomial $\chi_{\tilde{C}}(\pm X)$. Determinating this sign can be done by answering to the following question: $\chi_{\tilde{C}}(1) \cdot D \overset{?}{\sim} 0$ where D is a generic degree 0 k-divisor. The curve $\tilde{C}$ is given by an equation of the form $Q^2 = xyz(x+y+z)$ where Q is a conic. In particular the seven bitangents β_i are $x, y, z, x+y, x+z, y+z, x+y+z$, and are thus rational. If we assume that at least one of the intersections $(\beta_i \cdot Q)$ consists of two k-points then we can apply Algorithm 3.1.

Example 1. *Here is an illustration of the algorithm: let $\tilde{C}$ over $k = \mathbb{F}_q$, $q = 2^N$ with $N = 100$, be defined by*

$$(\omega x^2 + (\omega^3+1)y^2 + \omega^2 z^2 + \omega^4 xy + (\omega^3+\omega^2)xz + \omega^6 yz)^2 - xyz(x+y+z) = 0,$$

where the generator ω of k is a root of $(X^{101} - 1)/(X - 1)$.

Thanks to the AGM-algorithm, we recover the Frobenius polynomial up to a sign in 2 minutes

$$\begin{aligned}\chi_{\tilde{C}}(\pm X) = X^6 &+ 377276036264709 \cdot X^5 + 3455351061169045838894227937403 \cdot X^4 \\ &+ 92979302197227669130776666646461687227769187 1 \cdot X^3 \\ &+ 3455351061169045838894227937403 \cdot 2^{100} \cdot X^2 \\ &+ 377276036264709 \cdot 2^{200} \cdot X + 2^{300}.\end{aligned}$$

We can now use the algorithm presented in this paper to prove that the present $\chi_{\tilde{C}}$ has the accurate sign. The computation lasts about 4 seconds.

Remark 6. On the same computer, if one uses rather MAGMA general algorithms, it takes more than 2 minutes to determine the sign.

4.2. **3-dimensional factors of** $J^{new}(X_0(N))$**.** Let f be a new form of $X_0(N)$. Following a construction due to Shimura, one may associate to this new form a factor of $J_0(N)$ (the Jacobian of $X_0(N)$), denoted A_f. If $\dim A_f \leq 3$, it is easy to determine whether it is the Jacobian of a curve C_f or not (see for example [11] or [10]). In particular, if $\dim A_f = 3$, and if the curve C_f is non-hyperelliptic, an equation of C_f seems to be often given by linear relations in $S_2(f)^{\otimes 4}$. These computations carry out a first part towards a cryptosystem based on such curves: indeed, thanks to the Eichler-Shimura relation, fast computation of Hecke operators T_p leads to a fast determination of $|A_f \otimes \mathbb{F}_p|$. If the current algorithms fail to reach cryptographic size, new techniques allow us to hope for a breakthrough.

Example 2. *We consider the curve* $X_0(203)$*. There is only one simple factor of dimension* 3*. We find one quartic relation between the associated cusp forms :*

$$C : y^4-(x+3z)y^3+y^2(x^2-3xz+6z^2)+y(4xz^2-3z^3)-x^3z+3x^2z^2-4xz^3+2z^4=0$$

We choose $p = 25033$*. We denote* $\tilde{C} = C \otimes \mathbb{F}_p$ *and* $\tilde{C_f} = C_f \otimes \mathbb{F}_p$*. The computation of the characteristic polynomial of* T_p *leads to* $|\tilde{C_f}(\mathbb{F}_p)| =$ 15692826275509*, which is prime.*
The curve $\tilde{C}$ *has a rational flex. After a linear transformation, and by denoting new coordinates still by* x, y, z*, we have*

$$\begin{aligned} \tilde{C} \quad : \quad & y^3z+y^2(5057xz+22616z^2)+y(6567x^3+18877x^2z+162xz^2+14333z^3) \\ = \quad & 8673x^4+24517x^3z+20295x^2z^2+17815xz^3+3799z^4 \end{aligned}$$

Choosing a random rational divisor, and computing its order, we may check that this curve has the correct cardinality in 0.14 *seconds.*

Remark 7. Our p is far from the cryptographic size. It is basically due to the use of MAGMA. Current algorithms reach 10^9.

Remark 8. For a 'general quartic' over $\mathbb{Q}$, the density of primes p such that the reduction of the quartic modulo p has a rational flex is approximately 0.63. A proof of this result may be find in [22].

5. Conclusion

In the first two rows of the following table we summarize the amount of computation of our algorithm for a given quartic of the form $y^3 + h_2y = f_4$.

Operation		hyperelliptic of genus 3	$C_{3,4}$			generic quartic
			Picard	$\deg(h_2) = 1$	$\deg(h_2) = 2$	$\deg(h_2) = 3$
Our Methods	Add		2I+130M	2I+138M	2I+145M	2I+163M
	Dbl		2I+152M	2I+160M	2I+167M	2I+185M
Previous Work	Add	I+70M [13]	2I+140M [6]	2I+147M [6]	2I+150M [6]	
	Dbl	I+71M [13]	2I+164M [6]	2I+171M [6]	2I+174M [6]	

Remark 9. Our first intention was to develop an algorithm for DLP based cryptosystems, and hence to efficiently perform scalar multiplication. It should be noted that, for that matter, and on the contrary to that of [6], our algorithm benefits from the -2-adic expansion [4], which speeds up the algorithm up to 10%.

Remark 10. In addition, in the case of Picard curves, we can use the fast automorphism σ of order 3 to speed up scalar multiplication. All in all, those two tricks approximately halve the complexity of scalar multiplication. Consequently, the gap between the efficiency of DLP-Cryptosystems based on hyperelliptic curves of genus 3 and those based on Picard curves can be deemed negligible.

6. Appendix

We now show how to compute the flexes of an algebraic curve over any field using algebraic methods. An article of Abhyankar [1] gives another formula when the characteristic is different from 2.

Definition 1. *Let k be an algebraically closed field of characteristic $p \geq 0$. Let $f \in k[x_1, x_2, x_3]$ be a homogeneous polynomial of degree n. We denote by f_i the derivative of f with respect to x_i. We call the* Hessian matrix *of f the matrix $(f_{ij})_{i,j}$ and we call its determinant $H(f)$ the* Hessian *of f.*

Lemma 3. *Let $g \in GL_3(k)$ be a linear transformation. Then $H(f \circ g^{-1}) = (\det g)^2 H(f) \circ g^{-1}$.*

Proof. Apply the chain rule. □

Lemma 4. $x_1^2 H(f) = \begin{vmatrix} n(n-1)f & (n-1)f_2 & (n-1)f_3 \\ (n-1)f_2 & f_{22} & f_{23} \\ (n-1)f_3 & f_{23} & f_{33} \end{vmatrix}$

Proof. Apply twice the Euler's formula $x_1 f_1 + x_2 f_2 + x_3 f_3 = (\deg f) f$. See for example [21]. □

Definition 2. *Let C be a plane curve, and P a non-singular point of C. The point P is a* flex *if the intersection multiplicity at P of the tangent at P with the curve is greater than or equal to* 3.

If $f = 0$ is an equation of C of degree $n \geq 3$, then there exists a linear transformation g which sends a non-singular point $P = (p_1 : p_2 : p_3)$ on $(1 : 0 : 0)$ and its tangent to the line $x_2 = 0$. Then in affine coordinates

$$f \circ g^{-1} = x_2 + r x_2^2 + s x_2 x_3 + t x_3^2 + R(x_2, x_3)$$

and R has only terms of degree greater or equal to 3. Then P is a flex if and only if $r = 0$.

Proposition 3. *Suppose that char(k) does not divide $2(n-1)$. Then P is a flex if and only if $H(f)(P) = 0$.*

Proof. Suppose that the x_1-coordinate of P is not 0 (otherwise you do the same proof with an other coordinate). We have

$$(x_1^2 H(f) \circ g^{-1})(g(P)) = (\det g)^{-2} (x_1^2 H(f \circ g^{-1}))(g(P))$$

by Lemma 3 and because the $x_i x_j$ $(i, j \neq 1)$ terms in $(x_1^2) \circ g^{-1}$ are 0 at $g(P) = (1 : 0 : 0)$. Then by Lemma 4 and the form of $f \circ g^{-1}$

$$(x_1^2 H(f))(P) = -(\det g)^{-2} 2(n-1)^2 r.$$

So $H(f)(P) = 0$ if and only if $r = 0$ (i.e P is a flex).

□

Now we want to deal with the cases where $\mathrm{char}(k)$ may divide $2(n-1)$. Let k be an algebraically closed field of characteristic $p > 0$. We denote K a complete local field of characteristic 0, $\mathcal{O}$ its ring of integers, $\mathcal{M}$ its maximal ideal such that $\mathcal{O}/\mathcal{M} \simeq k$ ($\mathcal{O}$ may be the ring of Witt vectors of k).

Proposition 4. *Let $\tilde{f} \in k[x_1, x_2, x_3]$ be an homogeneous polynomial of degree n. Let $\tilde{C} = V(\tilde{f})$ and $C/\mathcal{O}$ be a model of $\tilde{C}$ given by a polynomial $f \in \mathcal{O}[x_1, x_2, x_3]$. We denote G the polynomial*

$$G = \frac{x_1^2 H(f) - n(n-1) f (f_{22} f_{33} - f_{23}^2)}{2(n-1)^2}.$$

Then G is in $\mathcal{O}[x_1, x_2, x_3]$. We call $\tilde{G}$ its reduction modulo $\mathcal{M}$.
Let $\tilde{P} = (\tilde{p}_1 : \tilde{p}_2 : \tilde{p}_3) \in \tilde{C}$ be a non-singular point such that $\tilde{p}_1 \neq 0$. The point $\tilde{P}$ is a flex if and only if $\tilde{G}(\tilde{P}) = 0$.

Proof. First we prove that G is in $\mathcal{O}[x_1, x_2, x_3]$. By Lemma 4,

$$x_1^2 H(f) - n(n-1) f (f_{22} f_{33} - f_{23}^2) = (n-1)^2 (2 f_2 f_3 f_{23} - f_2^2 f_{33} - f_3^2 f_{22}).$$

So $2(n-1)^2$ divides $x_1^2 H(f) - n(n-1) f (f_{22} f_{33} - f_{23}^2)$.
Let $\tilde{P}$ be a non-singular point of $\tilde{C}$ such that $\tilde{p}_1 \neq 0$. Since $\tilde{P}$ is non-singular, it exists $P \in C(\mathcal{O})$ lifting $\tilde{P}$ and $p_1 \notin \mathcal{M}$. Let $g \in \mathrm{GL}_3(\mathcal{O})$ a linear transformation that sends P on $(1 : 0 : 0)$ with tangent $x_2 = 0$. The reduction of this point is a flex if and only if the corresponding r is in $\mathcal{M}$. Now $G(P) = ur$ with $u \in \mathcal{O}^*$ by the computations of Proposition 3. So $\tilde{P}$ is a flex if and only if $\tilde{G}(\tilde{P}) = 0$. □

Remark 11. Strange things may appear when the characteristic divides $n-1$. A curve such that all points are flexes is called a *funny curve*. Homma proved in [16] that a funny quartic is isomorphic to the Klein quartic.

References

[1] S. Abhyankar. Remark on Hessians and flexes. *Nieuw Arch. Wisk.*, 11:110–117, 1963.

[2] L. M. Adleman, J. DeMarrais, and M-D. Huang. A subexponential algorithm for discrete logarithms in the rational subgroup of the Jacobian of a hyperelliptic curve over a finite field. In *Algorithmic Number Theory Symposium - 1994*, volume 877 of *LNCS*, pages 28–40. Springer, 1994.

[3] S. Arita. An Addition Algorithm in Jacobian of $C_{3,4}$ Curve. In *Information Security and Privacy, ACISP 2003*, volume 2727 of *LNCS*, pages 93–105. Springer, 2003.

[4] R. M. Avanzi, G. Frey, T. Lange, and R. Oyono. On using expansions to the base of −2. To appear in *Inter. J. of. Comp. Math.*, 81(4):403–406, 2004.

[5] A. Basiri, A. Enge, J-C. Faugère, and N. Gürel. The arithmetic of Jacobian groups of superelliptic cubics. Technical report, INRIA, 2002.

[6] A. Basiri, A. Enge, J-C. Faugère, and N. Gürel. Implementing the Arithmetic of $C_{3,4}$ Curves. *To appear* in Algorithmic Number Theory Symposium - ANTS-VI, 2004.

[7] M. Bauer. A subexponential algorithm for solving the discrete logarithm problem in the Jacobian of high genus hyperelliptic curves over arbitrary finite fields. preprint, 1998.

[8] A. Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Mathematics of Computation*, 71(238):729–742, 2002.

[9] S. Flon and R. Oyono. Fast arithmetic on Jacobians of Picard curves. In *Public Key Cryptography - PKC 2004*, volume 2947 of *LNCS*, pages 55–68. Springer, 2004.

[10] G. Frey and M. Müller. Arithmetic of modular curves and applications. In *Algorithmic Algebra and Number Theory*, pages 11–48. Ed. Matzat et al., Springer-Verlag, Berlin, 1999.

[11] S. D. Galbraith. *Equations for modular curves.* PhD thesis, Oxford, 1996.

[12] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology - Eurocrypt'2000*, volume 1807 of *LNCS*, pages 19–34. Springer, 2000.

[13] M. Gonda, K. Matsuo, K. Aoki, J. Chao, and S. Tsujii. Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementations. In *SCIS 2004*, 2004.

[14] R. Hartshorne. *Algebraic geometry*, volume 52. Springer-Verlag, GTM, 1977.

[15] J.W.P Hirschfeld, G. Korchmáros, and L. Storme. Arcs and caps in projective spaces. Available on `http://cage.ugent.be/~fdc/intensivecourse/james.ps`.

[16] M. Homma. Funny plane curves in characteristic $p > 0$. *Comm. Algebra*, 15:1469–1501, 1987.

[17] J. Kuroki, M. Gonda, K. Matsuo, J. Chao, and S. Tsujii. Fast genus three hyperelliptic curve cryptosystems. In *SCIS 2002*, 2002.

[18] T. Lange. Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae. In *Cryptology ePrint archive*, Report 2002/121, 2002. http://eprint.iacr.org/.

[19] K. Matsuo, J. Chao, and S. Tsujii. Fast genus two hyperelliptic curve cryptosystems. Technical report, IEICE, 2001. ISEC2001-31.

[20] E. Nart and C. Ritzenthaler. Non hyperelliptic curves of genus three over finite fields of characteristic two. submitted, see arXiv, math.NT/0312366, 2003.

[21] G. Orzech and M. Orzech. *Plane algebraic curves*, volume 61. Pure and Applied Math., New-York, 1981.

[22] R. Oyono. *Arithmetik algebraischer Kurven von Geschlecht 3.* PhD thesis, Essen, to appear.

[23] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar. Hyperelliptic curves cryptosystems: closing the performance gap to elliptic curves. In *Cryptographic Hardware and Embedded Systems - CHES 2003*, volume 2779 of *LNCS*, pages 351–365. Springer, 2003.

[24] C. Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. *To appear* in Algorithmic Number Theory Symposium - ANTS-VI, 2004.

[25] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In *Asiacrypt 2003*, LNCS, pages 75–92. Springer, 2003.

[26] F. Torres. The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs. Available on `http://arxiv.org/abs/math.AG/0011091`, 2000.