Genus 2 Hyperelliptic Curve Families with Explicit Jacobian Order Evaluation and Pairing-Friendly Constructions

Aurore Guillevic[1,2] and Damien Vergnaud[1]

[1] Équipe crypto DI, École Normale Supérieure, C.N.R.S., I.N.R.I.A.
45, rue d'Ulm, 75230 Paris Cedex 05, France
aurore.guillevic@ens.fr damien.vergnaud@ens.fr
[2] Laboratoire Chiffre, Thales Communications & Security S.A.,
160 bd de Valmy BP 82, 92704 Colombes Cedex France

Abstract. The use of elliptic and hyperelliptic curves in cryptography relies on the ability to compute the Jacobian order of a given curve. Recently, Satoh proposed a probabilistic polynomial time algorithm to test whether the Jacobian – over a finite field $\mathbb{F}_q$ – of a hyperelliptic curve of the form $Y^2 = X^5 + aX^3 + bX$ (with $a, b \in \mathbb{F}_q^*$) has a large prime factor. His approach is to obtain candidates for the zeta function of the Jacobian over $\mathbb{F}_q^*$ from its zeta function over an extension field where the Jacobian splits. We extend and generalize Satoh's idea to provide *explicit* formulas for the zeta function of the Jacobian of genus 2 hyperelliptic curves of the form $Y^2 = X^5 + aX^3 + bX$ and $Y^2 = X^6 + aX^3 + b$ (with $a, b \in \mathbb{F}_q^*$). Our results are proved by elementary (but intricate) polynomial root-finding techniques. Hyperelliptic curves with small embedding degree and large prime-order subgroup are key ingredients for implementing pairing-based cryptographic systems. Using our closed formulas for the Jacobian order, we propose two algorithms which complement those of Freeman and Satoh to produce genus 2 pairing-friendly hyperelliptic curves. Our method relies on techniques initially proposed to produce pairing-friendly elliptic curves (namely, the Cocks-Pinch method and the Brezing-Weng method). We show that the previous security considerations about embedding degree are valid for an elliptic curve and can be lightened for a Jacobian. We demonstrate this method by constructing several interesting curves with ρ-values around 4 with a Cocks-Pinch-like method and around 3 with a Brezing-Weng-like method.

Keywords. Hyperelliptic Curves, Genus 2, Order Computation, Ordinary Curves, Pairing-Friendly Constructions, Cocks-Pinch Method, Brezing-Weng Method.

1 Introduction

In 1985, the idea of using the group of rational points on an elliptic curve over a finite field in public-key cryptography was introduced independently by Miller [33] and Koblitz [27]. The main advantage of using elliptic curves is efficiency since no sub-exponential algorithms are known for solving the discrete logarithm problem in these groups (and thus key sizes can remain small). In 1989, Koblitz [28] suggested using Jacobian of hyperelliptic curves in cryptography. Genus 1 hyperelliptic curves are elliptic curves; genus 2 and 3 hyperelliptic curves are more complicated but are an attractive replacement for elliptic curves in cryptography. They are as efficient as genus one curves for bandwidth but still have a slower group law.

As for any group used for the discrete logarithm problem, one needs the order of the group to contain a large prime factor. This raised the problem of finding hyperelliptic curves over a finite field whose Jacobian order is (almost) a prime. For elliptic curves over finite fields, the Schoof-Elkies-Atkin (SEA) algorithm [36,32] runs in polynomial time in any characteristic and in small characteristic, there are even faster algorithms based on the so-called p-adic method [34,32]. For genus 2 hyperelliptic curves, if the p-adic method gives efficient point counting algorithms in small

characteristic, up to now, no algorithms as efficient as SEA are known when the characteristic of the underlying finite field is large (though substantial progress has recently been made in [21] and [23]). Using basic properties on character sums, Furukawa, Kawazoe and Takahashi [15] gave an explicit closed formula for the order of Jacobians of very special curves of type $Y^2 = X^5 + bX$ where $b \in \mathbb{F}_q$. Satoh [35] considered an intermediate approach and showed that point counting on specific Jacobians of certain genus 2 curves can be performed much faster than point counting on Jacobians of generic curves. He gave an algorithm to test whether the order of the Jacobian of a given hyperelliptic curve in the form $Y^2 = X^5 + aX^3 + bX$ has a large prime factor. His method relies on the fact that the Jacobian of the curve is $\mathbb{F}_{q^4}$-isogenous to a square of an elliptic curve defined over $\mathbb{F}_{q^4}$, hence their respective zeta functions are the same over $\mathbb{F}_{q^4}$ and can be computed by the SEA algorithm. Satoh's method obtains candidates for the zeta function of the Jacobian over $\mathbb{F}_q$ from the zeta function over $\mathbb{F}_{q^4}$. The methodology can be formalized as an efficient probabilistic polynomial algorithm but is not explicit and gives 26 possible orders to test for the Jacobian.

In recent years, many useful cryptographic protocols have been proposed that make use of a bilinear map, or *pairing*, between two groups in which the discrete logarithm problem is hard (*e.g.* [4,5]). Pairing-based cryptosystems can be constructed by using the Weil or Tate pairing on abelian varieties over finite fields. These pairings take as input points on an abelian variety defined over the field $\mathbb{F}_q$ and produce as output elements of an extension field $\mathbb{F}_{q^k}$. The degree of this extension is known as the *embedding degree*. In cryptography, abelian varieties obtained as Jacobians of hyperelliptic curves are often used. Suitable hyperelliptic curves for pairing-based cryptography are called *pairing-friendly*. Such pairing-friendly curves are rare and thus require specific constructions.

For a pairing-based cryptosystem to be secure and practical, the group of rational points on the Jacobian should have a subgroup of large prime order r, and the embedding degree k should be large enough so that the discrete logarithm problem in $\mathbb{F}_{q^k}$ is difficult but small enough to make the pairing efficiently computable. The efficiency parameter in pairing-friendly constructions is the so-called ρ-*value*: for a Jacobian of hyperelliptic curve of genus g it is defined as $\rho = g \log q / \log r$. It measures the ratio of the bit-sizes of the order of the Jacobian and the subgroup order r. The problem of constructing pairing-friendly elliptic curves with small ρ-values has been studied extensively [12]. Unfortunately, there are very few results for constructing pairing-friendly hyperelliptic curves of genus $g \geq 2$ with small ρ-values [17,2]. Galbraith, Pujolas, Ritzenthaler and Smith [18] gave (supersingular) genus 2 pairing-friendly hyperelliptic curves with ρ-values close to 1 but only for embedding degrees $k \in \{4, 5, 6, 12\}$. Freeman, Stevenhagen and Streng presented in [13] a general method that produced pairing-friendly (ordinary) genus 2 pairing-friendly hyperelliptic curves with $\rho \simeq 8$ for all embedding degrees k. Kawazoe and Takahashi [26] (see also [25]) presented an algorithm which constructed hyperelliptic curves of the form $Y^2 = X^5 + bX$ (thanks to the closed formula for its Jacobian order). Following Satoh's approach, Freeman and Satoh [14] constructed pairing-friendly genus 2 hyperelliptic curves of the form $Y^2 = X^5 + aX^3 + bX$ and $Y^2 = X^6 + aX^3 + b$ (with $a, b \in \mathbb{F}_q^*$) by means of elliptic curves that become pairing-friendly over a finite extension of the underlying finite field. Constructions from [26,25,14] produce pairing-friendly Jacobians with $2.22 \leqslant \rho \leqslant 4$ only for embedding degrees divisible by 3 or 4.

Our contributions. Satoh's approach to compute the Jacobian order of a hyperelliptic curve $Y^2 = X^5 + aX^3 + bX$ is not explicit. For each candidate, he has to check that the order is not weak for cryptographic use. In [22, § 4], Gaudry and Schost showed that the Jacobians of hyperelliptic curves of the form $Y^2 = X^6 + aX^3 + b$ are also isogenous to a product of two elliptic curves over

an extension field. Satoh claimed that his method applies as well to this family but did not derive an algorithm for it.

Our first contribution is to extend and generalize Satoh's idea to provide *explicit* formulas for the zeta function of the Jacobian of genus 2 hyperelliptic curves of the form $Y^2 = X^5 + aX^3 + bX$ and $Y^2 = X^6 + aX^3 + b$ (with $a, b \in \mathbb{F}_q^*$). Our results are proved by elementary polynomial root-finding techniques. This permits to generate efficiently a random hyperelliptic curve, in one of these two forms, suitable for cryptographic use. These curves enable various improvements to make scalar multiplication in the Jacobian efficient (*e.g.* the Gallant-Lambert-Vanstone algorithm [19], Takashima's algorithm [38] or Gaudry's algorithm [20]). These large families of curves are still very specific but there is no evidence that they should be more vulnerable to discrete logarithm attacks than the absolutely simple Jacobians.

Two algorithms proposed in [14] to produce pairing-friendly genus 2 hyperelliptic curves are very general as they are still valid for arbitrary abelian varieties over any finite field. Assuming that the finite field is a prime field and the abelian variety is of the above form, we can consider any embedding degree. The security restrictions concerning the embedding degree (which must be a multiple of 3 or 4) made in [14] are unnecessary in this particular case. Satoh and Freeman exclude constructions which need an elliptic curve defined over a quadratic extension of a prime field (with j-invariant in $\mathbb{F}_{p^2}$), resulting in restricted sets of parameters $a, b \in \mathbb{F}_p$. Using our closed formulas for the Jacobian order, we use two approaches that construct pairing-friendly elliptic curves and adapt them to produce pairing-friendly genus 2 curves. The first one is based on the Cocks-Pinch method [9] (see also [16, Algorithm IX.4]) of constructing individual ordinary pairing-friendly elliptic curves. The other is based on cyclotomic polynomials as originally proposed by Brezing and Weng [7] which generates families of curves while achieving better ρ-values. We adapt both constructions using the elliptic curve complex multiplication method (CM) [1,16] to compute one of the two elliptic curves to which the Jacobian is isogenous to (even if the curve j-invariant is in $\mathbb{F}_{p^2}$ rather than in a prime field $\mathbb{F}_p$). In particular, this method can construct pairing-friendly elliptic curves over $\mathbb{F}_{p^2}$ but unfortunately with $\rho \simeq 4$.

Our approach contains the previous constructions by Kawazoe and Takahashi [26] and is in a sense a specialization of Freeman and Satoh [14]. It also produces new families for ordinary genus 2 hyperelliptic curves. Explicit examples of cryptographically interesting curves are given.

2 Explicit Computation of $J_{\mathcal{C}_5}$ Order

Throughout this paper, $p \geq 5$ denotes a prime number and q a power of p. In this section, we consider the genus 2 hyperelliptic curve defined over a finite field $\mathbb{F}_q$:

$$\mathcal{C}_5(\mathbb{F}_q) : Y^2 = X^5 + aX^3 + bX, \text{ with } a, b \neq 0 \in \mathbb{F}_q \ .$$

The Jacobian of the curve is denoted $J_{\mathcal{C}_5}$ and it splits into two isogenous elliptic curves in an extension over $\mathbb{F}_q$ of degree 1, 2 or 4 [35]. These two elliptic curves admit a quadratic twist which is half the time defined on a smaller extension. As the trace computation is then more efficient, we will also consider directly these quadratic twists, as in [14].

2.1 Splitting the Jacobian $J_{\mathcal{C}_5}$ into Two Isogenous Elliptic Curves

Satoh showed in [35] that the Jacobian splits into two elliptic curves defined by

$$\begin{aligned} E_1(\mathbb{F}_q[\sqrt[4]{b}]) : Y^2 &= \quad \delta(X-1)(X^2-\gamma X+1) \text{ and} \\ E_2(\mathbb{F}_q[\sqrt[4]{b}]) : Y^2 &= -\delta(X-1)(X^2-\gamma X+1) \end{aligned}$$

with $\gamma = (2a-12\sqrt{b})/(a+2\sqrt{b})$ and $\delta = (a+2\sqrt{b})/(64\sqrt[4]{b}^3)$. The isogeny between $J_{\mathcal{C}_5}$ and $E_1 \times E_2$ is defined over $\mathbb{F}_q[\sqrt[4]{b}]$. Using the notation $c = a/\sqrt{b}$ from [14], the curve parameters are

$$\gamma = \frac{2c-12}{c+2},\ \delta = \frac{c+2}{2^6\sqrt[4]{b}} \text{ and } j(E_1) = j(E_2) = 2^6\frac{(3c-10)^3}{(c+2)^2(c-2)}.$$

Since E_1 and E_2 are isogenous over $\mathbb{F}_q[\sqrt[4]{b}, \sqrt{-1}]$, they have the same order over this field. They also admit a 2-torsion point $P = (1,0)$ over $\mathbb{F}_q[\sqrt[4]{b}]$ (their order is therefore even). Let E_1' and E_2' denote the quadratic twists of E_1 and E_2 obtained by removing the term $1/(2^6\sqrt[4]{b})$ in δ. They are isogenous over $\mathbb{F}_q[\sqrt{b}, \sqrt{-1}]$.

$$\begin{array}{ccccc} & & (E_1\times E_2)(\mathbb{F}_q[\sqrt[8]{b}]) & \overset{\text{isomorphism}}{\longleftrightarrow} & (E_1'\times E_2')(\mathbb{F}_q[\sqrt[8]{b}]) \\ & & \vert & & \vert \\ J_{\mathcal{C}_5}(\mathbb{F}_q[\sqrt[4]{b}]) & \overset{\text{isogeny}}{\longleftrightarrow} & (E_1\times E_2)(\mathbb{F}_q[\sqrt[4]{b}]) & & (E_1'\times E_2')(\mathbb{F}_q[\sqrt[4]{b}]) \\ \vert & & & & \vert \\ J_{\mathcal{C}_5}(\mathbb{F}_q[\sqrt{b}]) & & & & (E_1'\times E_2')(\mathbb{F}_q[\sqrt{b}]) \\ \vert & & & & \\ J_{\mathcal{C}_5}(\mathbb{F}_q) & & & & \end{array}$$

The Jacobian $J_{\mathcal{C}_5}$ has *the same order* as the product $E_1 \times E_2$ over the extension field where the isogeny is defined. Computing the elliptic curve order is easy with the SEA algorithm [36,32] which computes the trace. As the computation is faster for the quadratic twist (which is defined over $\mathbb{F}_q[\sqrt{b}]$ instead of $\mathbb{F}_q[\sqrt[4]{b}]$, we will also consider the isogeny between $J_{\mathcal{C}_5}$ and $E_1' \times E_2'$.

$$\begin{aligned} E_1'(\mathbb{F}_q[\sqrt{b}]) : Y^2 &= \quad (c+2)(X-1)(X^2-\gamma X+1) \text{ and} \\ E_2'(\mathbb{F}_q[\sqrt{b}]) : Y^2 &= -(c+2)(X-1)(X^2-\gamma X+1)\,. \end{aligned}$$

It remains to compute the Jacobian order from $\#J_{\mathcal{C}_5}(\mathbb{F}_q[\sqrt[4]{b}])$ to $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$. We develop explicit formulas using the zeta function properties. Going down directly from $\#J_{\mathcal{C}_5}(\mathbb{F}_{q^4})$ to $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$ does not provide an explicit order. We compute step by step the explicit order, descending by quadratic extensions.

2.2 Computing explicit order using zeta function

Let $Z_{J_{\mathcal{C}_5}}$ denote the zeta function of the Jacobian $J_{\mathcal{C}_5}$ which satisfies the following properties [35]:

1. $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_q) \in \mathbb{Z}[T]$ i.e. the zeta function is a polynomial with integer coefficients;
2. the degree of the zeta function polynomial is $\deg Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_q) = 2g = 4$;
3. the Jacobian order is related to the zeta function by $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = Z_{J_{\mathcal{C}_5}}(1, \mathbb{F}_q)$;
4. let $z_{1,q}, z_{2,q}, z_{3,q}, z_{4,q}$ be the four roots of $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_q)$ in $\mathbb{C}$. Up to index permutation, we have $z_{1,q}z_{2,q} = q$ and $z_{3,q}z_{4,q} = q$;

5. the roots of $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_{q^n})$ the zeta function of the Jacobian considered over a degree n extension $\mathbb{F}_{q^n}$ are those over $\mathbb{F}_q$ to the power n: $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_{q^n}) = (T - z_{1,q}^n)(T - z_{2,q}^n)(T - z_{3,q}^n)(T - z_{4,q}^n)$.

Satoh's method to compute the Jacobian order is derived from the fact that if $J_{\mathcal{C}_5}$ is isogenous over $\mathbb{F}_q$ to $E_1 \times E_2$, then $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_q) = Z_{E_1}(T, \mathbb{F}_q) \times Z_{E_2}(T, \mathbb{F}_q)$. We have $Z_{E_1}(T, \mathbb{F}_q) = T^2 - t_q T + q$ with t_q the trace of the Frobenius endomorphism and $\#E_1(\mathbb{F}_q) = q + 1 - t_q = Z_{E_1}(1, \mathbb{F}_q)$.

Let us denote $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_q) = T^4 - a_q T^3 + b_q T^2 - q a_q T + q^2$ with

$$\begin{aligned} a_q &= z_{1,q} + z_{2,q} + z_{3,q} + z_{4,q} \\ b_q &= z_{1,q}z_{2,q} + z_{1,q}z_{3,q} + z_{1,q}z_{4,q} + z_{2,q}z_{3,q} + z_{2,q}z_{4,q} + z_{3,q}z_{4,q} \\ &= 2q + (z_{1,q} + z_{2,q})(z_{3,q} + z_{4,q}) \ . \end{aligned}$$

Our goal is to find two simple formulas for computing (a_q, b_q) in terms of (a_{q^2}, b_{q^2}) and apply the two formulas recursively. A careful computation gives

$$a_{q^2} = (a_q)^2 - 2b_q \tag{1}$$

$$b_{q^2} = (b_q)^2 - 4qb_q + 2q^2 - 2qa_{q^2} \tag{2}$$

Knowing a_{q^2} and b_{q^2}, we can solve[3] equation (2) for b_q then recover a_q using (1).

We have to determine where the isogeny is defined in order to solve the corresponding system. In each case, two solutions are possible for b_q. One of them induces a square root in a_q that must be an integer because the two coefficients a_q and b_q are integers. This solution can be chosen if the isogeny is actually defined over $\mathbb{F}_{q^2}$ *and* $\mathbb{F}_q$ or if the elliptic curve has an additional property. In these two cases the Jacobian splits over $\mathbb{F}_{q^2}$ *and* over $\mathbb{F}_q$.

When the isogeny between $J_{\mathcal{C}_5}$ and $E_1 \times E_2$ is defined over $\mathbb{F}_{q^4}$ but not over a subfield of $\mathbb{F}_{q^4}$ and the trace t_{q^4} of the two elliptic curves is such that $2q^2 + t_{q^4}$ is not a square, we see an other simplification for the zeta function coefficients: they are not squares but of the form two times a square. After easy (but cumbersome) calculation and a difficult identification of the rare cases that do not correspond to the general solution, we obtain the following theorem:

Theorem 1. *Let $\mathcal{C}_5$ be a hyperelliptic curve defined over a finite field $\mathbb{F}_q$ by the equation $\mathcal{C}_5(\mathbb{F}_q)$: $Y^2 = X^5 + aX^3 + bX$ with $a, b \neq 0 \in \mathbb{F}_q$. Let E_1 and E_2 be the elliptic curves defined over $\mathbb{F}_q[\sqrt[4]{b}]$ and E_1', E_2' their quadratic twists defined over $\mathbb{F}_q[\sqrt{b}]$, isogenous over $\mathbb{F}_q[\sqrt{b}, \sqrt{-1}]$. Let t_q be the trace of $E_1(\mathbb{F}_q)$ if b is a fourth power, let t_q' be the trace of $E_1'(\mathbb{F}_q)$ if b is a square, let t_{q^2} be the trace of $E_1(\mathbb{F}_{q^2})$ if b is not a square in $\mathbb{F}_q$ and let t_{q^2}' be the trace of $E_1'(\mathbb{F}_{q^2})$ and t_{q^4} of $E_1(\mathbb{F}_{q^4})$ if b is neither a square nor a fourth power.*

1. *If b is a fourth power then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q+1-t_q)^2$ if $\sqrt{-1} \in \mathbb{F}_q$ and $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q+1-t_q)(q+1+t_q)$ if $\sqrt{-1} \notin \mathbb{F}_q$.*
2. *If b is a square but not a fourth power ($q \equiv 1 \mod 4$) and $t_{q^2} + 2q$ is not a square, then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q-1)^2 + (t_q')^2$.*
3. *If b is not a square and $\sqrt[4]{b} \in \mathbb{F}_{q^2}$ ($q \equiv 3 \mod 4$) and $t_{q^2} + 2q$ is not a square, then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - t_{q^2}$.*
4. *If b is not a square and $\sqrt[4]{b} \notin \mathbb{F}_{q^2}$ ($q \equiv 1 \mod 4$) and $t_{q^4} + 2q^2$ is not a square, then $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$ is equal to $q^2 + 1 - 2n(q+1) + 2n^2$ or $q^2 + 1 + 2n(q+1) + 2n^2$ where $n \in \mathbb{N}$ is such that $2q + t_{q^2}' = 2n^2$ if $q \equiv 5 \mod 8$ or $2q - t_{q^2}' = 2n^2$ if $q \equiv 1 \mod 8$.*

[3] Satoh [35] used only Equation (1) which resulted in a more intricate polynomial system with degree 16 polynomial equations to solve.

The case 1 of Th.1 is of no interest in cryptography as the Jacobian order factors trivially. In the cases 2 and 3, we may as well work directly with the elliptic curve $E_1(\mathbb{F}_{q^2})$ (of even order) since the arithmetic is not (yet) as efficient in genus two as in genus one. The case 4 provides ordinary Jacobians of hyperelliptic curves with explicit order and of cryptographic interest. The very special cases excluded in the theorem with $2q^2+t_{q^4}$ or $2q+t_{q^2}$ squares give a Jacobian either which splits over $\mathbb{F}_q$ or whose order is an elliptic curve order, as in case 3. They are detailed in the following remark.

Remark 1. With the same notations as in the previous theorem,

1. If b is a square but not a fourth power ($q \equiv 1 \mod 4$) and if $t_{q^2}+2q = y^2$ (with $y \in \mathbb{N}^*$), the Jacobian splits and its order is one of $(q+1-y)^2$, $(q+1+y)^2$ or $(q+1-y)(q+1+y) = (q-1)^2+(t_q^{'})^2$.
2. If b is not a square and $\sqrt[4]{b} \in \mathbb{F}_{q^2}$ ($q \equiv 3 \mod 4$) and if $t_{q^2}+2q = y^2$ (with $y \in \mathbb{N}^*$), the Jacobian splits and its order is one of $(q+1-y)^2$, $(q+1+y)^2$ or $(q+1-y)(q+1+y) = q^2+1-t_{q^2}$.
3. If b is not a square and $\sqrt[4]{b} \notin \mathbb{F}_{q^2}$ ($q \equiv 1 \mod 4$) and if $t_{q^4}+2q^2 = y^2$ (with $y \in \mathbb{N}^*$) then we decompose $-\Delta(E_1^{'}(\mathbb{F}_{q^2})) = -(t_{q^2}^{'})^2+4q^2 = t_{q^4}+2q^2 = y^2$ in the two factors $(2q+t_{q^2}^{'})(2q-t_{q^2}^{'})$. Let $2q+t_{q^2}^{'} = D_1y_1^2$ and $2q-t_{q^2}^{'} = D_2y_2^2$ with D_1, D_2 square-free integers.
   (a) if $D_1 \neq 2$ and $D_2 \neq 2$ then $\pm y+2q^2$ is not a square and $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$ is equal to q^2+1-y or q^2+1+y.
   (b) if $D_1 = D_2 = 2$ then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2+1-2n(q+1)+2n^2$ (case 4 of Th. 1) can happen with $n \in \{y_1, -y_1, y_2, -y_2\}$. In the same time, $y+2q^2 = (y_1+y_2)^2$ and $-y+2q^2 = (y_1-y_2)^2$ are squares hence $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$ can be $(q+1-s)^2$ with $s \in \{y_1+y_2, -y_1-y_2, y_1-y_2, -y_1+y_2\}$. The two last possibilities are q^2+1-y and q^2+1+y.

The cases 1, 2 and 3 in the remark 1 occur very rarely (*e.g.* the cases 1 and 3 appear only when the elliptic curves E_1 and E_2 have complex multiplication by $i = \sqrt{-1}$). Moreover, in 1, 2 and 3b of Rem. 1 the Jacobian order splits. In 3a, the Jacobian order is equal to the order of a quartic twist of $E_1(\mathbb{F}_{q^2})$.

In practice, when the Th. 1 or Rem. 1 present several order possibilities one can easily discriminate between them by checking whether the scalar multiplication of a random point by the possible orders gives the infinity point.

In the two following examples, we took at random a prime $p \equiv 1 \mod 4$ of 128 bits and started with $a = -3$ and $b = -2$ until b was not a square mod p. Then let $c = a/\sqrt{b}$, $E_1^{'}(\mathbb{F}_{p^2})$: $y^2 = (x-1)((c+2)x^2-(2c-12)x+(c+2))$ and $t_{p^2}^{'}$ its trace. We deduced the Jacobian order and factorized it. We repeated this process with subsequent b-values until the Jacobian order was almost prime.

Example 1. $p =$ `0x84c4f7a6b9aee8c6b46b34fa2a2bae69` $= 1 \mod 8$. The 17th test provided $b = -38$, $t_{p^2}^{'} =$ `0x702461acf6a929e295786868f846ab40` $= 0 \mod 2$, $b_p = 2p - t_{p^2}^{'} = 2n^2$ as expected with $n =$ `- 0x8c1fc81b9542ce23`. We found $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = 2^5r$ with r a 250-bit prime of cryptographic size close to the 128-bit security level:
$r =$ `0x226ddb780b2ded62d1d70138d9c7361794679a609fbe5ae85918c88f5b6ea7d`.

Example 2. $p =$ `0xb081d45d7d08109c2905dd6187f7cbbd` $= 5 \mod 8$. The 17th test provided $b = -41$, $t_{p^2}^{'} =$ `-0x11753eaa61f725ff118f63bb131c8b8f2` $= 0 \mod 2$, $b_p = 2p + t_{p^2}^{'} = 2n^2$ as

expected with $n = -$ `0x611e298cc019b06e`. We found $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = 2 \cdot 5 \cdot r$ with r a 252-bit prime of cryptographic size close to the 128-bit security level:
$r =$ `0xc2b7a2f39d49b6b579d4c15a8440315cd1ccc424df912e6748c949008ebd989`.

3 Explicit Computation of $J_{\mathcal{C}_6}$ Order

In this section, we consider the genus 2 hyperelliptic curves defined over a finite field $\mathbb{F}_q$:

$$\mathcal{C}_6(\mathbb{F}_q) : Y^2 = X^6 + aX^3 + b \text{ with } a, b \neq 0 \in \mathbb{F}_q \ .$$

The Jacobian of the curve is denoted $J_{\mathcal{C}_6}$ and it splits into two isogenous elliptic curves in an extension over $\mathbb{F}_q$ of degree 1, 2, 3 or 6 [22,14]. The computation of the zeta function of $J_{\mathcal{C}_6}$ over $\mathbb{F}_q$ is similar to those of $J_{\mathcal{C}_5}$ from the previous section but with more technical details.

3.1 Decomposition into two isogenous elliptic curves.

Freeman and Satoh showed in [14] that $J_{\mathcal{C}_6}$ is isogenous over $\mathbb{F}_q[\sqrt[6]{b}]$ to the Jacobian of another genus 2 hyperelliptic curve $\mathcal{C}_6'$ defined over $\mathbb{F}_q[\sqrt{b}]$. This Jacobian $J_{\mathcal{C}_6'}$ splits into two elliptic curves E_c and E_{-c} defined over $\mathbb{F}_q[\sqrt{b}]$ which are isogenous over $\mathbb{F}_q[\sqrt{b}, \sqrt{-3}]$. Let $c = a/\sqrt{b}$ and assume $c \neq \pm 2$. The two elliptic curves are defined (in a reduced form) by

$$\begin{aligned} E_c^{\text{red}}(\mathbb{F}_q[\sqrt{b}]) &: Y^2 = X^3 + 3(2c-5)X + c^2 - 14c + 22 \text{ and} \\ E_{-c}^{\text{red}}(\mathbb{F}_q[\sqrt{b}]) &: Y^2 = X^3 - 3(2c+5)X + c^2 + 14c + 22 \ . \end{aligned}$$

Freeman and Satoh remarked that both elliptic curves admit the same 3-torsion subgroup ([14, Proof of Prop. 4.2]). With Vélu's formulas adapted to finite fields (e.g. [31, p. 54]), we compute an isogeny from E_c into E_{-c} with kernel equal to this 3-torsion subgroup. Because of this isogeny, E_c and E_{-c} have the same order over $\mathbb{F}_q[\sqrt{b}, \sqrt{-3}]$ and moreover, this order is a multiple of 3.

$$\begin{array}{ccccc} J_{\mathcal{C}_6}(\mathbb{F}_q[\sqrt[6]{b}]) & \overset{\text{isogeny}}{\longleftrightarrow} & J_{\mathcal{C}_6'}(\mathbb{F}_q[\sqrt[6]{b}]) & & \\ \vert & & \vert & & \\ J_{\mathcal{C}_6}(\mathbb{F}_q[\sqrt{b}]) & & J_{\mathcal{C}_6'}(\mathbb{F}_q[\sqrt{b}]) & \overset{\text{isogeny}}{\longleftrightarrow} & (E_c \times E_{-c})(\mathbb{F}_q[\sqrt{b}]) \\ \vert & & & & \\ J_{\mathcal{C}_6}(\mathbb{F}_q) & & & & \end{array}$$

In the two cases where b is not a cube, we have to deduce $Z_{J_{\mathcal{C}_6}}(T, \mathbb{F}_q)$ from $Z_{J_{\mathcal{C}_6}}(T, \mathbb{F}_{q^3})$ or $Z_{J_{\mathcal{C}_6}}(T, \mathbb{F}_{q^2})$ from $Z_{J_{\mathcal{C}_6}}(T, \mathbb{F}_{q^6})$ which is equivalent. Note that we do not see explicitly the simplification in the formula if we descent from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^3}$ then to $\mathbb{F}_q$.

Eventually, we obtain the following theorem:

Theorem 2. *Let $\mathcal{C}_6$ be a hyperelliptic curve defined over a finite field $\mathbb{F}_q$ by the equation $\mathcal{C}_6(\mathbb{F}_q)$: $Y^2 = X^6 + aX^3 + b$ with $a, b \neq 0 \in \mathbb{F}_q$. Let E_c and E_{-c} be the elliptic curves defined over $\mathbb{F}_q[\sqrt{b}]$ isogenous over $\mathbb{F}_q[\sqrt{b}, \sqrt{-3}]$. Let t_{q^2} be the trace of $E_c(\mathbb{F}_{q^2})$ and let t_q be the trace of $E_c(\mathbb{F}_q)$ if it exists.*

1. *If b is a sixth power then $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = (q+1-t_q)^2$ if $\sqrt{-3} \in \mathbb{F}_q$ and $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = (q+1-t_q)(q+1+t_q)$ if $\sqrt{-3} \notin \mathbb{F}_q$.*

2. *If b is a square but not a third power and if $3(4q-(t_q)^2)$ is not a square then $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2-q+1+(1+q+t_q)t_q$.*
3. *If b is a third power but not a square and if $2q+t_{q^2}$ is not a square then $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2+1-t_{q^2}$.*
4. *If b is neither a cube nor a square and if $2q+t_{q^2}$ is not a square, then there exists $n \in \mathbb{N}$ such that $2q-t_{q^2} = 3n^2$ and $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2+q+1+(q+1+n)3n$ or $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2+q+1-(q+1-n)3n$.*

Once more, the first case is not interesting in cryptography as the Jacobian order splits. The third case provides nothing more than an elliptic curve defined over $\mathbb{F}_{q^2}$. Whenever the group law computation on $J_{\mathcal{C}_6}(\mathbb{F}_q)$ is not as efficient as a point addition on $E_c(\mathbb{F}_{q^2})$, it will be more appropriate to work with the elliptic curve. The case 2 might be interesting. The case 4 provides interesting genus 2 hyperelliptic curves.

Remark 2. With the same notations as in the previous theorem,

1. If b is a square but not a third power and if $4q-(t_q)^2 = 3y^2$ then $\#J_{\mathcal{C}_6}(\mathbb{F}_q)$ equals one of $(q+1+(t_q+3y)/2)(q+1+(t_q-3y)/2) = q^2-q+1+(1+q+t_q)t_q$, $(q+1+(t_q+3y)/2)^2$, $(q+1+(t_q-3y)/2)^2$.
2. If b is a third power but not a square and if $2q+t_{q^2} = y^2$ is a square then $\#J_{\mathcal{C}_6}(\mathbb{F}_q)$ equals one of $(q+1-y)^2$, $(q+1+y)^2$, $(q+1-y)(q+1+y) = q^2+1-t_{q^2}$.
3. If b is neither a cube nor a square,
   (a) if $2q+t_{q^2} = s^2$, $s \in \mathbb{N}$, and $3(2q-t_{q^2})$ is not a square then $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2-q+1-(1+q)s+s^2$ or $q^2-q+1+(1+q)s+s^2$.
   (b) if $2q+t_{q^2} = s^2$ and $2q-t_{q^2} = 3n^2$, $\#J_{\mathcal{C}_6}(\mathbb{F}_q)$ splits and equals one of $q^2+q+1+(q+1+n)3n$, $q^2+q+1-(q+1-n)3n$, $q^2-q+1-(q+1-s)s$, $q^2-q+1+(q+1+s)s$, $q^2+1-(-t_{q^2}+3y)/2)$, $q^2+1-(-t_{q^2}-3y)/2)$, $(q+1+\frac{s-3n}{2})^2$, $(q+1-\frac{s-3n}{2})^2$, $(q+1+\frac{s+3n}{2})^2$, $(q+1-\frac{s+3n}{2})^2$.

Example 3. We consider the 127-bit Mersenne prime $p = 2^{127}-1$ which allows efficient implementation of the modular arithmetic operations required in cryptography. Looking for a curve $\mathcal{C}_6$ over $\mathbb{F}_p$ with small parameters a and b and suitable for a cryptographic use, we found easily $\mathcal{C}_6(\mathbb{F}_p) : Y^2 = X^6-3X^3-92$ with $b = -92$ which is neither a square nor a cube. Let $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2+1) = \mathbb{F}_p[i]$, $c = a/\sqrt{b} \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $E_c(\mathbb{F}_{p^2}) : Y^2+X^3+3(2c-5)X+c^2-14c+22$. A few second computation gives us t_{p^2} =`0x6089c0341e5414a24bef1a1a93c54fd2` and $2p-t_{p^2} = 3n^2$ as expected with $n = \pm$ `0x74a69cde5282dbb6`. Hence $\#J_{\mathcal{C}_6}(\mathbb{F}_p) = p^2+p+1+3n(p+1)+3n^2$. Using few random points on the Jacobian, we find $n < 0$ and that $\#J_{\mathcal{C}_6}(\mathbb{F}_p)$ has a 250-bit prime factor:
$r =$ `0x25ed097b425ed0974c75619931ea7f1271757b237c3ff3c5c00a037e7906557` and provides a security level close to 128-bits.

Efficiency. For a cryptographic application, we need $\#J_{\mathcal{C}}(\mathbb{F}_q)$ be a large prime r times a small (*i.e.* few bits) cofactor h. The prime r must be of size twice the security level in bits. The common method consists in randomly generating the coefficients a and b of the hyperelliptic curve and computing the order until it is a large prime r times a small cofactor.

Here $r \sim q^2$ hence the size of q is a few bits more than the security level in bits instead of twice with an elliptic curve. To compute the Jacobian order, we have to run SEA algorithm once for an elliptic curve defined over $\mathbb{F}_q$ if b is a square or over $\mathbb{F}_{q^2}$ otherwise. If b is a square our method is much faster than generating a cryptographic elliptic curve and if b is not a square, our method is roughly as efficient as finding an elliptic curve suitable for cryptography.

4 Pairing-Friendly Constructions

We have several constraints for suitable pairing-friendly constructions inherent to elliptic curves:

1. The embedding degree k must be small, in order to achieve the same security level in bits in the elliptic curve r-torsion subgroup $E(\mathbb{F}_p)[r]$ and in the finite field extension $\mathbb{F}_{p^k}$. In practice, this means $6 \leqslant k \leqslant 60$. More precise recommendations are given in [12, Tab. 1]. For a random elliptic curve, we have usually $k \simeq r$ so this is a huge constraint.
2. The trace t of the curve must satisfy $|t| \leqslant 2\sqrt{p}$.
3. The determinant of the curve $\Delta = t^2 - 4p = -Dy^2$ must have a very small square-free part $D < 10^9$ in order to run the CM-method in reasonable time.
4. The size $\log r$ of the subgroup must be close to the optimal case, that is $\rho = g \log p / \log r \sim 1$ with g the genus of the curve. Quite generic methods for elliptic curves achieve $1 \leqslant \rho \leqslant 2$. We will try to find constructions for genus 2 curves with $2 \leqslant \rho \leqslant 4$.

The two methods use the same shortcuts in formulas. Let E an elliptic curve and let $\#E(\mathbb{F}_p) = p + 1 - t = hr$ with r a large prime and h the cofactor. Hence $p \equiv t - 1 \mod r$. Let $\Delta = t^2 - 4p = -Dy^2$. The second useful formula is $Dy^2 = 4p - t^2 = 4hr - (t-2)^2$, hence $-Dy^2 \equiv (t-2)^2 \mod r$.

4.1 Cocks-Pinch Method

We first recall the method proposed by Cocks and Pinch in 2001 to construct pairing-friendly elliptic curves [9] (see also [16, Algorithm IX.4]):

Algorithm 1: Cocks-Pinch method to find a pairing-friendly elliptic curve.

Input: Square-free integer D, size of r and embedding degree k to match the security level in bits, knowing that $\rho \approx 2$.
Output: Prime order r, prime number p, elliptic curve parameters $a, b \in \mathbb{F}_p$ such that $E(\mathbb{F}_p) : Y^2 = X^3 + aX + b$ has a subgroup of order r and embedding degree k with respect to r.

1 **repeat**
2 Pick at random a prime r of prescribed size until $-D$ is a square in the finite field $\mathbb{F}_r$ and $\mathbb{F}_r$ contains a primitive k-th root of unity ζ_k, that is $r \equiv 1 \mod k$.
3 As r divides $\Phi_k(p)$, we can rewrite it as $\Phi_k(p) \equiv 0 \mod r$. With properties of cyclotomic polynomials, we obtain $p \equiv \zeta_k \mod r$ with ζ_k a primitive k-th root of unity. Furthermore, $t \equiv 1 + p \mod r$ so this method chooses $t = 1 + \zeta_k$ in $\mathbb{F}_r$. Then $y = (t-2)/\sqrt{-D}$ in $\mathbb{F}_r$.
4 Lift t and y from $\mathbb{F}_r$ to $\mathbb{Z}$ and set $p = \frac{1}{4}(t^2 + Dy^2)$.
5 **until** *p is prime.*
6 **return** *r, p, $a, b \in \mathbb{F}_p$*

We propose to adapt this method to the Jacobian families of cryptographic interest presented above. See the size recommendations in [2, Tab. 3.1] depending on the security level in bits to choose accordingly the embedding degree. First, we know explicitly the Jacobian order. Just as in the case of elliptic curves, the definition of the embedding degree is equivalent to ask for $r \mid \#J_{\mathcal{C}}(\mathbb{F}_p)$ and $r \mid \Phi_k(p)$. We will use the property $p \equiv \zeta_k \mod r$ as well. The aim is to express the other parameters, namely the square part y and the trace of the elliptic curve isogenous to the Jacobian over some extension field, in terms of $\zeta_k \mod r$. We will use the same notations as previously, see Th.1 and Th.2. Let i be a primitive fourth root of unity an ω be a primitive third root of unity in $\mathbb{F}_r$.

Pairing-friendly Hyperelliptic curve $\mathcal{C}_5$

If b is not a square in $\mathbb{F}_p$ but $\sqrt{b}, \sqrt[4]{b} \in \mathbb{F}_{p^2}$ ($p \equiv 3 \mod 4$), then $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = \#E_1(\mathbb{F}_{p^2}) = p^2 + 1 - t_{p^2}$ (Th.1(3.)). A pairing-friendly Jacobian of this type has exactly the same order as the corresponding elliptic curve $E_1(\mathbb{F}_{p^2})$. Hence any pairing-friendly elliptic curve defined over a quadratic extension $\mathbb{F}_{p^2}$ (and of even order) will provide a pairing-friendly Jacobian of this type over the prime field $\mathbb{F}_p$, with the same order and the same ρ-value. Choosing the Jacobian instead of the elliptic curve will be appropriate only if the group law on the Jacobian over $\mathbb{F}_p$ is faster than the group law on the elliptic curve over $\mathbb{F}_{p^2}$. Note that the methods described in [12] are suitable for generating pairing-friendly elliptic curves over prime fields (in large characteristic), not over field extensions.

$\mathcal{C}_5$ with b a square but not a fourth power. This case is already almost solved in [14]. The Cocks-Pinch method adapted with $r \mid \#J_{\mathcal{C}_5}(\mathbb{F}_p) = (p-1)^2 + (t_p')^2$ instead of $r \mid p + 1 - t_p'$ produces indeed the same algorithm as [14, Alg. 5.5] followed by [14, Alg. 5.11] with $\pi = (t_p' - y\sqrt{-D})/2$, $d = 4$. We show that $d \mid k$ is unnecessary. It is completely hopeless to expect a prime power $q = \pi\overline{\pi} = p^n$ hence we assume that $q = p$ is prime.

Definition 1. *Embedding degree and embedding field[3, Def. 2.1 and 2.2] Let A be an abelian variety defined over $\mathbb{F}_q$, where $q = p^m$ for some prime p and integer m. Let $r \neq p$ be a prime dividing $\#A(\mathbb{F}_q)$. The* embedding degree *of A with respect to r is the smallest integer k such that r divides $q^k - 1$.*

The minimal embedding field *of A with respect to r is the smallest extension of $\mathbb{F}_p$ containing the rth roots of unity $\mu_r \subset \mathbb{F}_p$.*

Let k be the embedding degree of the Jacobian $J_{\mathcal{C}_5}(\mathbb{F}_p)$: $r \mid \#J_{\mathcal{C}_5}(\mathbb{F}_p)$, $r \mid \Phi_k(p)$. From the Jacobian point of view, there is no security problem induced by a difference between embedding degree and embedding field because $\mathbb{F}_p$ is a prime field. From elliptic curve side, the one-dimensional part of the r-torsion arises in $E_1'(\mathbb{F}_{p^4})$, not below. An elementary observation about elliptic curve orders shows that

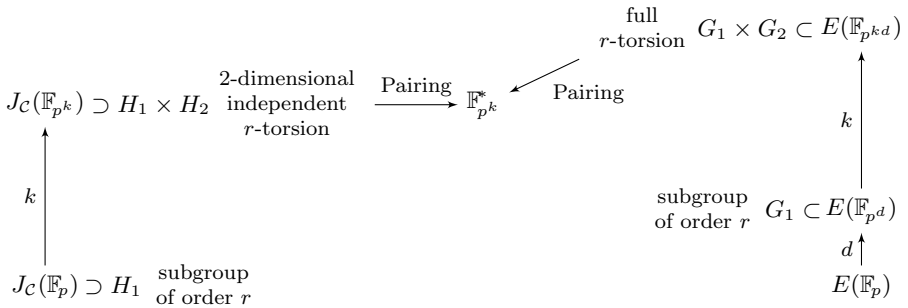
$$\begin{aligned}
\#E_1'(\mathbb{F}_p) &= p + 1 - t_p' \\
\#E_1'(\mathbb{F}_{p^2}) &= (p + 1 - t_p')(p + 1 + t_p') \\
\#E_1'(\mathbb{F}_{p^4}) &= (p + 1 - t_p')(p + 1 + t_p')((p+1)^2 + (t_p')^2)
\end{aligned}$$

and the last factor of $\#E_1'(\mathbb{F}_{p^4})$ is the Jacobian order. Hence $r \mid \#E_1'(\mathbb{F}_{p^4})$ but not underneath. The full r-torsion arises in $E_1'(\mathbb{F}_{p^{4k/\gcd(4,k)}})$ but the embedding field is $\mathbb{F}_{p^k}$. So the elliptic curve $E_1'(\mathbb{F}_{p^4})$ will not be suitable for a pairing implementation when $\gcd(k, 4) \in \{1, 2\}$ which does not matter because we are interested in Jacobians suitable for pairing, not elliptic curves. See Fig. 1.

Moreover we note that taking an even trace t_p' and a prime $p \equiv 1 \mod 4$ permits always to find valid parameters, namely a $c \in \mathbb{F}_p$ satisfying the j-invariant equation, hence coefficients $a, b \in \mathbb{F}_p$ of $\mathcal{C}_5$.

$\mathcal{C}_5$ with b not a square and $p \equiv 1 \mod 4$. In this case we have $\sqrt[4]{b} \notin \mathbb{F}_{p^2}$, $\sqrt[4]{b} \in \mathbb{F}_{p^4}$ and $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = p^2 + 1 + 2n^2 - 2n(1+p) = (p-n)^2 + (n-1)^2$ with $2p \pm t_{p^2}' = 2n^2$. The isogenous elliptic curve is defined over $\mathbb{F}_{p^2}$. We have $\Delta = (t_{p^2}')^2 - 4p^2 = (t_{p^2}' + 2p)(t_{p^2}' - 2p)$. With $2p - t_{p^2}' = 2n^2$ we obtain $2p + t_{p^2}' = 4p - 2n^2$ and find $\Delta = -4n^2(2p - n^2)$. With $2p + t_{p^2}' = 2n^2$ we obtain $2p - t_{p^2}' = 4p - 2n^2$ and find also $\Delta = -4n^2(2p - n^2)$. In both cases let $Dy^2 = 2p - n^2$ thus

Fig. 1. Difference between Jacobian and elliptic curve embedding degree



$\Delta = -D(2ny)^2$ and $p = (Dy^2 + n^2)/2$. The Jacobian order is a sum of two squares in p and n hence $n = (p+i)/(1+i) = (p+i)(1-i)/2 \mod r$. Furthermore $y^2 \equiv (2p - n^2)/D \mod r$ with $p \equiv \zeta_k \mod r$ and we find that

$n \equiv (\zeta_k + i)(1-i)/2 \mod r$ and $y \equiv \pm(\zeta_k - i)(1+i)/(2\sqrt{D}) \mod r$.

The trace will be even by construction as $t'_{p^2} = \pm(2p - 2n^2)$ and to find valid parameters, $p \equiv 1 \mod 4$ is required. To find the coefficients of the curve $\mathcal{C}_5(\mathbb{F}_p)$, do the following (Alg. 2).

Algorithm 2: Pairing-friendly Jacobian of type $J_{\mathcal{C}_5}$, Th.1(4.)

Input: Square-free integer D, size of r and embedding degree k to match the security level in bits, knowing that $\rho \approx 4$.

Output: Prime order r, prime number p, Jacobian parameters $a, b \in \mathbb{F}_p$ such that the Jacobian of the curve $\mathcal{C}_5(\mathbb{F}_p) : Y^2 = X^5 + aX^3 + bX$ has a subgroup of order r and embedding degree k with respect to r.

1 **repeat**
2 Choose a prime r of prescribed size with $i, \sqrt{D}, \zeta_k \in \mathbb{F}_r$.
3 Let $n = (\zeta_k + i)(1-i)/2$ and $y = \pm(\zeta_k - i)(1+i)/(2\sqrt{D}) \in \mathbb{F}_r$.
4 Lift n and y from $\mathbb{F}_r$ to $\mathbb{Z}$ and set $p = (n^2 + Dy^2)/2$.
5 **until** $p \equiv 1 \mod 4$ *and* p *is prime.*
6 Run the CM method to find the j-invariant of an elliptic curve $E'_1(\mathbb{F}_{p^2})$ of trace $\pm t'_{p^2}$ and $\Delta = -4D(ny)^2$.
7 Solve $j(E'_1) = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}$ in $\mathbb{F}_{p^2}$ and choose the solution satisfying $c^2 \in \mathbb{F}_p$.
8 Choose $a, b \in \mathbb{F}_p$ such that $a \neq 0$ and $b = (a/c)^2$ (b is a square in $\mathbb{F}_{p^2}$ but not in $\mathbb{F}_p$).
9 **return** r, p, $a, b \in \mathbb{F}_p$

We adapt the program `cm.cpp` of Miracl[4] [37] to compute the j-invariant of an elliptic curve defined over $\mathbb{F}_{p^2}$ (instead of $\mathbb{F}_p$). Indeed, it is not convenient for step 5 as it searches for an elliptic curve defined over a prime field. We isolate parts of the program which compute the Weber polynomial of a number field of discriminant D. Then we call the `factor` function but to find a factor mod p of degree 2 (instead of degree 1) of the Weber polynomial when $D \not\equiv 3 \mod 8$ and a factor of degree 6 (instead of degree 3) when $D \equiv 3 \mod 8$. The papers [30,29] contain efficient formulas to recover Hilbert polynomial roots in $\mathbb{F}_p$ from Weber polynomial roots in $\mathbb{F}_p$ or $\mathbb{F}_{p^3}$. We find in

[4] We learned very recently that the MIRACL library status has changed. This library is now a commercial product of Certivox [8]. The CM software [11] can be an even more efficient alternative to compute class polynomials.

$\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^6}$ a root of the factor of degree 2 or 6 of Weber polynomial and apply the corresponding transformation to get an element in $\mathbb{F}_{p^2}$. We obtain the j-invariant of (an isogenous curve to) the curve $E_1'(\mathbb{F}_{p^2})$. We solve $j(E_1') = 2^6\frac{(3c-10)^3}{(c-2)(c+2)^2}$ and find for various examples a solution $c \in \mathbb{F}_{p^2}$ satisfying $c^2 \in \mathbb{F}_p$. It comes from the appropriate restrictions $2p \pm t'_{p^2} = 2n^2$, $p \equiv 1 \mod 4$, n odd. Sometimes we have to choose a quadratic twist of $\mathcal{C}_5$, of the form $Y^2 = \nu(X^5 + aX^3 + bX)$ with $\nu \in \mathbb{F}_p$ non-square.

Example 4. $k = 6$, $D = 516505$, $\rho = 4.1$
$p =$`0x9d3e97371e27d006f11762f0d56b4fbf2caca7d606e92e8b6f35189723f46f57ed46e9650ce1cca1bd90dc393db35cc38970cb0abbe236bf2c4ac2f65f1b50afb135` (528 bits),
$r=$`0x679d8c817e0401203364615b9d34bdb3a0b89e70fa8d6807fa646e25140f25ad` (255 bits),
$n =$`0x28f34a88ab9271c2ea6d70f4a3dc758a025ad6e4ee51c16867763e8d940022de5`,
$y =$`-0x65110defe8f4669a158149675afaa23dba326d49ce841d7ef9855c7d8a65df95`,
$a = 1$, $b =$`0x85eb6f5b5594c1bca596a53066216ad79588cf39984314609bbd7a3a3022 41fc786703a19bc1ccb44fc9e09b9c17ac62fc38d6bf82851d3d8b753c79da7338ca56b0`,
$\mathcal{C}_5(\mathbb{F}_p) : Y^2 = 2(X^5 + aX^3 + bX)$.

Pairing-friendly Hyperelliptic curve $\mathcal{C}_6$

If b is a cube but not a square then $\#J_{\mathcal{C}_6}(\mathbb{F}_p) = p^2 + 1 - t_{p^2}$ (Th.2(3.)). This case is close to the elliptic curve case. Actually, this is the same construction as finding a pairing-friendly elliptic curve over a field $\mathbb{F}_{p^2}$. But in practice the methods to find such pairing-friendly elliptic curves over $\mathbb{F}_p$ fail over $\mathbb{F}_{p^2}$. Indeed, the expression for p is $p^2 = \frac{1}{4}((t'_{p^2})^2 + Dy^2)$ but this is hopeless to find a prime square. We did not find in the literature any such construction.

$\mathcal{C}_6$ with b a square but not a cube. This case is treated in [14, Alg. 5.5, Alg. 5.11] and corresponds to $d = 3$ and $\pi = (t_p - y\sqrt{-D})/2$. This is also a Cocks-Pinch-like method with $r \mid p^2 - p + 1 + (1 + p)t_p + (t_p)^2$ and $r \mid \Phi_k(p)$. As above for $\mathcal{C}_5$, the condition "$3 \mid k$" is not necessary since we consider the embedding degree of the Jacobian, not the elliptic curve.

We found that $p \equiv 1 \mod 3$ and $p + 1 \pm t_p \equiv 0 \mod 3$ are enough to find always valid parameters. Freeman and Satoh pointed out that the equation $j(E_c) = 2^8 3^3(2c-5)^3/((c-2)(c+2)^3)$ has a solution in $\mathbb{F}_p$ in only one third of the cases [14, § 6]. One can explain this phenomenon by simple arithmetic considerations.

The elliptic curve E_c has a 3-torsion point which means $p + 1 - t_p \equiv 0 \mod 3$, which happens one third of the cases when $p \equiv 1 \bmod 3$. Assuming that $p \equiv 1 \mod 3$, if $p+1+t_p \equiv 0 \mod 3$ then $E_c(\mathbb{F}_p)$ has not 3-torsion point but its quadratic twist has. These two elliptic curves have the same j-invariant and admit a 3-torsion subgroup over $\mathbb{F}_{p^2}$. In practice we verify that the equation has a solution when $p+1\pm t_p \equiv 0 \mod 3$. Combining the two conditions $p \equiv 1 \mod 3$ and $p+1\pm t_p \equiv 0 \mod 3$, the equation from $j(E_c)$ has indeed a solution one third of the time ($\frac{1}{2} \cdot \frac{2}{3}$). When $p \equiv 1 \mod 3$ and $t_p \equiv 2 \mod 3$, we can always find a solution in step 2 of [14, Alg. 5.11] and finish to run this algorithm. When $p \equiv 1 \mod 3$ and $t_p \equiv 1 \mod 3$, we can still find a solution in step 2 and construct the coefficients of $\mathcal{C}_6(\mathbb{F}_p)$ in step 3 of [14, Alg. 5.11]. But in step 6, we have to choose not $\mathcal{C}_6$ itself but its quadratic twist.

$\mathcal{C}_6$ *with b neither a square nor a cube.* $\#J_{\mathcal{C}_6}(\mathbb{F}_p) = p^2+p+1-(p+1)3n+3n^2$. Here the parameters satisfy $2p - t_{p^2} = 3n^2$. Let $2p + t_{p^2} (= 4p - 3n^2) = Dy^2$. Hence

$$p = \frac{1}{4}\left(3n^2 + Dy^2\right) \ .$$

Note that $3 \nmid D$ otherwise p would not be prime. Solving $p^2+p+1-(p+1)3n+3n^2 \equiv 0 \mod r$ gives $p = (1-\omega^2)n+\omega^2$ or $p = (1-\omega)n+\omega$ with ω a primitive third root of unity. As $y^2 = (4p-3n^2)/D \mod r$ and with $p \equiv \zeta_k \mod r$ we find

$$n \equiv (\zeta_k - \omega)/(1-\omega) \mod r \text{ and } y \equiv \pm(\omega\zeta_k + \omega^2)/\sqrt{D} \mod r \ .$$

The last version of the Cocks-Pinch method is presented in Alg. 3.

Algorithm 3: Pairing-friendly Jacobian of type $J_{\mathcal{C}_6}$, Th.2(4.)

Input: Square-free integer D, $3 \nmid D$, size of r and embedding degree k to match the security level in bits, knowing that $\rho \approx 4$.

Output: Prime order r, prime number p, Jacobian parameters $a, b \in \mathbb{F}_p$ such that the Jacobian of the curve $\mathcal{C}_6(\mathbb{F}_p) : Y^2 = X^6 + aX^3 + b$ has a subgroup of order r and embedding degree k with respect to r.

1 **repeat**
2 Choose a prime r of prescribed size such that a third root of unity ω, $\sqrt{D}$ and $\zeta_k \in \mathbb{F}_r$.
3 Let $n = (\zeta_k - \omega)/(1-\omega)$ and $y = \pm(\omega\zeta_k + \omega^2)/\sqrt{D} \in \mathbb{F}_r$.
4 Lift n and y from $\mathbb{F}_r$ to $\mathbb{Z}$ and set $p = (3n^2 + Dy^2)/4$.
5 **until** $p \equiv 1 \mod 3$ *and* p *is prime.*
6 Run the CM method to find the j-invariant of an elliptic curve $E_c(\mathbb{F}_{p^2})$ of trace t_{p^2} and $\Delta = -3D(ny)^2$. More precisely, run the CM method with $3D$. Find a degree 2 or 6 factor of the Weber polynomial $\mod p$, then apply the right transformation from [30,29] to obtain a root in $\mathbb{F}_{p^2}$ of the corresponding Hilbert polynomial.
7 Solve $j(E_c) = 2^8 3^3 \frac{(2c-5)^3}{(c-2)(c+2)^3}$ in $\mathbb{F}_{p^2}$ and choose a solution $c \in \mathbb{F}_{p^2}$ such that $c^2 \in \mathbb{F}_p$. Choose $a, b \in \mathbb{F}_p$ such that $(a/c)^2$ is not a cube and $b = (a/c)^2$. Hence b is neither a square nor a cube.
8 **return** r, p, $a, b \in \mathbb{F}_p$

4.2 Brezing-Weng Method

The method proposed by Brezing-Weng is to use a polynomial ring built with a cyclotomic polynomial instead of a finite prime field $\mathbb{F}_r$. The parameters will be polynomials modulo a cyclotomic polynomial instead of integers modulo a prime. But the choice of D is limited to few values. We tried with D square-free in the range 1 - 35 according to the embedding degree $5 \leqslant k \leqslant 36$. We ran a search (with Magma [6]) over different cyclotomic fields and with a change of basis as in [24] and [25]. We obtained complete families with $\rho \simeq 3$ and recover constructions already mentioned in previous papers [26,14] and new complete families for other embedding degrees:

Example 5 $(k = 22, D = 2, \rho = 2.8)$.

$$\begin{aligned}
r &= \Phi_{88}(x) = x^{40} - x^{36} + x^{32} - x^{28} + x^{24} - x^{20} + x^{16} - x^{12} + x^8 - x^4 + 1 \\
n &= \tfrac{1}{2}\left(x^{28} - x^{22} - x^6 + 1\right) \\
y &= \tfrac{1}{2}\left(x^{17} + x^{11}\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(-x^{56} + 2x^{50} - x^{44} + 4x^{34} + 4x^{22} - x^{12} + 2x^6 - 1\right) \\
p &= \tfrac{1}{8}\left(x^{56} - 2x^{50} + x^{44} + 8x^{28} + x^{12} - 2x^6 + 1\right) \\
x &\equiv 1 \mod 2
\end{aligned}$$

Example 6 ($k = 26, D = 2, \rho = 2.33$).

$$\begin{aligned} r &= \Phi_{104}(x) = x^{48} - x^{44} + x^{40} - x^{36} + x^{32} - x^{28} + x^{24} - x^{20} + x^{16} - x^{12} + x^8 - x^4 + 1 \\ n &= \tfrac{1}{2}\left(x^{28} - x^{26} - x^2 + 1\right) \\ y &= \tfrac{1}{2}\left(x^{15} + x^{13}\right) \\ t'_{p^2} &= \tfrac{1}{4}\left(-x^{56} + 2x^{54} - x^{52} + 4x^{30} + 4x^{26} - x^4 + 2x^2 - 1\right) \\ p &= \tfrac{1}{8}\left(x^{56} - 2x^{54} + x^{52} + 8x^{28} + x^4 - 2x^2 + 1\right) \\ x &\equiv 1 \mod 2 \end{aligned}$$

Some constructions ($k \in \{7, 17, 19, 23, 29, 31\}$) have a cyclotomic polynomial of too high degree for r. Hence there are very few possibilities for choosing a suitable integer x such that $p(x)$ and $r(x)$ are prime and of the desired size. Moreover the ρ-value is close to 4. It would be preferable to use the Cocks-Pinch-like method.

5 More Pairing-Friendly constructions with $D = 1, 2, 3$

We observed that when $D = 1$, the obtained genus 2 hyperelliptic curve of the form $\mathcal{C}_5(\mathbb{F}_p)$ with b a square splits actually into two non-isogenous elliptic curves over $\mathbb{F}_p$. We observed the same decomposition for genus 2 hyperelliptic curve of the form $\mathcal{C}_6$ obtained with $D = 3$ and b a square but not a cube. A theoretical explanation can be found in [14, Proposition 3.10]. From Rem. 1 1 we get the explicit decomposition. We give here a practical point of view from explicit zeta function computation. Let $E_1(\mathbb{F}_q)$ be an elliptic curve defined over a finite field $\mathbb{F}_q$ of trace t_q an satisfying $(t_q)^2 - 4q = -y^2$, *i.e.* $D = 1$. The zeta function of E_1 is $Z_{E_1}(T, \mathbb{F}_q) = T^2 - t_q T + q = (T - \frac{t_q + iy}{2})(T - \frac{t_q - iy}{2})$ with $i \in \mathbb{C}$ such that $i^2 = -1$. We will use the notation $\alpha = \frac{t_q + iy}{2}$. With the formula given in [14, Proposition 3.4] we find that the zeta function of the order 4 Weil restriction of $E_1(\mathbb{F}_q)$ is

$$Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_q) = (T - i\alpha)(T + i\alpha)(T - i\overline{\alpha})(T + i\overline{\alpha}) = (T^2 - yT + q)(T^2 + yT + q) \ .$$

Note that $q + 1 - y$ and $q + 1 + y$ are the orders of the two quartic twists of $E_1(\mathbb{F}_q)$. Hence the obtained Jacobian always splits into the two quartic twists of $E_1(\mathbb{F}_q)$.

For $J_{\mathcal{C}_6}(\mathbb{F}_q)$ and $D = 3$ when b is a square but not a cube, a similar computation explains the matter. Here E_c is an elliptic curve defined over $\mathbb{F}_q$ of trace t_q and such that $(t_q)^2 - 4q = -3y^2$. Let us denote $\alpha = \frac{t_q + i\sqrt{3}y}{2}$ one of the two roots of its zeta function. The zeta function of the order 3 Weil restriction of $E_c(\mathbb{F}_q)$ is

$$Z_{J_{\mathcal{C}_6}}(T, \mathbb{F}_q) = \left(T^2 + \tfrac{t+3y}{2}T + q\right)\left(T^2 + \tfrac{t-3y}{2}T + q\right) \ .$$

We recognize the two cubic twists of $E_c(\mathbb{F}_q)$. This confirm the results found in Rem 2 1. Trying with an order 6 Weil restriction, we find

$$Z_{J_{\mathcal{C}_6}}(T, \mathbb{F}_q) = \left(T^2 - \tfrac{t-3y}{2}T + q\right)\left(T^2 - \tfrac{t+3y}{2}T + q\right) \ .$$

Hence the Jacobian splits into the two sextic twists of $E_c(\mathbb{F}_q)$. We recognize a case described in Rem. 2 3b. Freeman and Satoh suggested to construct an order 8 Weil restriction when $D = 1, 2$ and an order 12 Weil restriction when $D = 3$. For $k = 32, 64, 88$ and $D = 2$ this order 8 Weil restriction corresponds to families previously found by Kawazoe and Takahashi.

5.1 Order-8 Weil restriction when D = 1

Let $E(\mathbb{F}_p)$ an elliptic curve defined over a prime field $\mathbb{F}_p$, of trace t_p and satisfying $(t_p)^2 - 4p = -y^2$ (that is, $D = 1$). The two roots of its zeta function over $\mathbb{C}$ are $\alpha = (t_p + iy)/2$ and $\overline{\alpha}$. Let ζ_8 denotes an eighth root of unity. The zeta function of the order 8 Weil restriction of $E(\mathbb{F}_p)$ is

$$\begin{aligned} Z(T, \mathbb{F}_p) &= \big((T - \zeta_8\alpha)(T - \zeta_8^7\overline{\alpha})(T - \zeta_8^5\alpha)(T - \zeta_8^3\overline{\alpha})\big)\big((T - \zeta_8^3\alpha)(T - \zeta_8^5\overline{\alpha})(T - \zeta_8^7\alpha)(T - \zeta_8\overline{\alpha})\big) \\ &= (T^4 + tyT^2 + p^2)(T^4 - tyT^2 + p^2) \end{aligned}$$

We see this zeta function factors as two degree 4 zeta functions, that is into two genus 2 hyperelliptic curve zeta functions. So we start from an elliptic curve $E(\mathbb{F}_p)$ as above, with $(t_p)^2 - 4p = -y^2$ and search for suitable p, t, y such that there exists a genus 2 hyperelliptic curve of order $\#J_{\mathcal{C}}(\mathbb{F}_p) = p^2 + 1 \pm ty$ suitable for pairing-based cryptography.

To apply one of the two previous methods (Cocks-Pinch or Brezing-Weng), we have to find an expression of t and y in terms of p modulo r.

$$t = \zeta_8 + \zeta_8^7\zeta_k \text{ and } y = -\zeta_8^7 - \zeta_8\zeta_k \mod r \ .$$

To finish, $p = (t^2 + y^2)/4$.

Example 7 ($k = 8, D = 1, \rho = 3.0$).
$r = x^4 + 2x^2 + 4x + 2$
$t = x$
$y = \frac{1}{3}(-x^3 + 2x^2 - 3x + 2)$
$p = \frac{1}{36}(x^6 - 4x^5 + 10x^4 - 16x^3 + 26x^2 - 12x + 4)$
$x \equiv 4 \mod 6$

5.2 Order-8 Weil restriction when D = 2

Let $E(\mathbb{F}_p)$ an elliptic curve defined over a prime field $\mathbb{F}_p$, of trace t_p and satisfying $(t_p)^2 - 4p = -2y^2$ (that is, $D = 2$). The two roots of its zeta function over $\mathbb{C}$ are $\alpha = (t_p + i\sqrt{2}y)/2$ and $\overline{\alpha}$. Let ζ_8 denotes an eighth root of unity. The zeta function of the order 8 Weil restriction of $E(\mathbb{F}_p)$ is

$$\begin{aligned} Z(T, \mathbb{F}_p) &= \big((T - \zeta_8\alpha)(T - \zeta_8^7\overline{\alpha})(T - \zeta_8^3\alpha)(T - \zeta_8^5\overline{\alpha})\big)\big((T - \zeta_8^5\alpha)(T - \zeta_8^3\overline{\alpha})(T - \zeta_8^7\alpha)(T - \zeta_8\overline{\alpha})\big) \\ &= (T^4 - 2yT^3 + 2y^2T^2 - 2ypT + p^2)(T^4 + 2yT^3 + 2y^2T^2 + 2ypT + p^2) \end{aligned}$$

and $\#J_{\mathcal{C}}(\mathbb{F}_p) = p^2 + 1 - 2yp + 2y^2 - 2y = (p - y)^2 + (y - 1)^2$. We recognize the order of $J_{\mathcal{C}_5}(\mathbb{F}_p)$ when the considered isogeny is defined over $\mathbb{F}_{p^4}$ (and with n and y swapped). Hence it is the construction detailed above in Alg. 2 with $D = 2$.

5.3 Order-12 Weil restriction when D = 3

Let $E(\mathbb{F}_p)$ an elliptic curve defined over a prime field $\mathbb{F}_p$, of trace t_p and satisfying $(t_p)^2 - 4p = -3y^2$ (i.e. $D = 3$). The two roots of its zeta function over $\mathbb{C}$ are $\alpha = (t_p + i\sqrt{3}y)/2$ and $\overline{\alpha}$. Let ζ_{12} denotes a twelfth root of unity. The zeta function of the order 12 Weil restriction of $E(\mathbb{F}_p)$ is

$$\begin{aligned} Z(T, \mathbb{F}_p) &= \big((T - \zeta_{12}\alpha)(T - \zeta_{12}^{11}\overline{\alpha})(T - \zeta_{12}^7\alpha)(T - \zeta_{12}^5\overline{\alpha})\big)\big((T - \zeta_{12}^5\alpha)(T - \zeta_{12}^7\overline{\alpha})(T - \zeta_{12}^{11}\alpha)(T - \zeta_{12}\overline{\alpha})\big) \\ &= \left(T^4 - \left(-p + t_p\tfrac{t_p+3y}{2}\right)T^2 + p^2\right)\left(T^4 - \left(-p + t_p\tfrac{t_p-3y}{2}\right)T^2 + p^2\right) \end{aligned}$$

which can be interpreted as the zeta functions of two Jacobians of hyperelliptic curves defined over $\mathbb{F}_p$ of order $p^2+p+1-t_p(t_p \pm 3y)/2$. For further simplifications, we can also write $\#J_{\mathcal{C}}(\mathbb{F}_p) = (p-1)^2 + ((t_p-3y)/2)^2 = (p+1)^2 - 3((t_p+y)/2)^2$.

To apply the Cocks-Pinch or Brezing-Weng method, we use

$$t_p \equiv -\omega(\omega p-1)/i \mod r,\ y \equiv -\omega(\omega p+1)/\sqrt{3} \mod r$$

with ω a third root of unity and i a fourth root of unity. We found new families with $\rho = 3$ (with Brezing-Weng method). It would be interesting to know if these quite special curves provide more features such as compression due to twists of higher degree.

6 Conclusion

We provided *explicit* formulas for the zeta function of the Jacobian of genus 2 hyperelliptic curves of the form $Y^2 = X^5 + aX^3 + bX$ and $Y^2 = X^6 + aX^3 + b$ (with $a, b \in \mathbb{F}_q^*$). We also presented several algorithms to obtain pairing-friendly hyperelliptic families. The constructions require to run the CM method to find a j-invariant in $\mathbb{F}_{p^2}$. We explained the differences with a j-invariant in $\mathbb{F}_p$ and gave references to fill the gap. There are some special issues for $D = 1, 3$: a ρ-value of 2 can be achieved but the Jacobian is unfortunately not simple. However, it is possible to construct suitable curves with $D = 1$ and $D = 3$ that achieve ρ-value around 3 using Weil restriction of order 8 or 12. It is worth noting that it is also possible to adapt the Dupont-Enge-Morain technique [10] to our setting but unfortunately it provides curves with $\rho \simeq 4$. It remains open to construct pairing-friendly hyperelliptic curves with $1 \leqslant \rho < 2$.

Acknowledgments

This work was supported in part by the French ANR-09-VERS-016 BEST Project and by the Commission of the European Communities through the ICT program under contract ICT-2007-216676 ECRYPT II. Aurore Guillevic is grateful to Olivier Orcière for his help in early computations and hints on how to run the CM method. We would thank the reviewers of the Pairing Conference for their precise proofreading and their constructive and thorough remarks.

References

1. A. O. L. Atkin & F. Morain – "Elliptic curves and primality proving", *Math. Comput.* **61** (1993), p. 29–68.
2. J. Balakrishnan, J. Belding, S. Chisholm, K. Eisenträger, K. Stange & E. Teske – "Pairings on hyperelliptic curves", in *WIN - Women in Numbers: Research Directions in Number Theory*, Fields Institute Communications, vol. 60, Amer. Math. Soc., Providence, RI, 2011, p. 87–120.
3. N. Benger, M. Charlemagne & D. M. Freeman – "On the security of pairing-friendly abelian varieties over non-prime fields", in *Pairing-Based Cryptography - Pairing 2009* (H. Shacham & B. Waters, eds.), Lect Notes Comput. Sci., vol. 5671, Springer, 2009, p. 52–65.
4. D. Boneh & M. K. Franklin – "Identity-based encryption from the Weil pairing", *SIAM J. Comput.* **32** (2003), no. 3, p. 586–615.
5. D. Boneh, B. Lynn & H. Shacham – "Short signatures from the Weil pairing", *J. Cryptology* **17** (2004), no. 4, p. 297–319.
6. W. Bosma, J. Cannon & C. Playoust – "The Magma algebra system. I. The user language", *J. Symbolic Comput.* **24** (1997), no. 3-4, p. 235–265, Computational algebra and number theory (London, 1993).
7. F. Brezing & A. Weng – "Elliptic curves suitable for pairing based cryptography", *Des. Codes Cryptography* **37** (2005), no. 1, p. 133–141.

8. Certivox – "MIRACL Crypto SDK", 2012, http://certivox.com/index.php/solutions/miracl-crypto-sdk/.
9. C. Cocks & R. G. Pinch. – "ID-based cryptosystems based on the Weil pairing", 2001, Unpublished manuscript.
10. R. Dupont, A. Enge & F. Morain – "Building curves with arbitrary small mov degree over finite prime fields", *J. Cryptology* **18** (2005), no. 2, p. 79–89.
11. A. Enge – "CM Software", February 2012, http://www.multiprecision.org/index.php?prog=cm.
12. D. Freeman, M. Scott & E. Teske – "A taxonomy of pairing-friendly elliptic curves", *J. Cryptology* **23** (2010), no. 2, p. 224–280.
13. D. Freeman, P. Stevenhagen & M. Streng – "Abelian varieties with prescribed embedding degree", in *Algorithmic Number Theory* - ANTS *VIII* (A. J. van der Poorten & A. Stein, eds.), Lect Notes Comput. Sci., vol. 5011, Springer, 2008, p. 60–73.
14. D. M. Freeman & T. Satoh – "Constructing pairing-friendly hyperelliptic curves using weil restriction", *J. Number Theory* **131** (2011), no. 5, p. 959–983.
15. E. Furukawa, M. Kawazoe & T. Takahashi – "Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields", in *Selected Areas in Cryptography, 10th International Workshop, SAC 2003* (M. Matsui & R. J. Zuccherato, eds.), Lect Notes Comput. Sci., vol. 3006, Springer, 2003, p. 26–41.
16. S. D. Galbraith – "Pairings", in *Advances in Elliptic Curve Cryptography* (I. F. Blake, G. Seroussi & N. P. Smart, eds.), London Mathematical Society Lecture Note Series, vol. 317, Cambridge Univ. Press, 2004.
17. S. D. Galbraith, F. Hess & F. Vercauteren – "Hyperelliptic pairings", in *Pairing-Based Cryptography* - Pairing *2007* (T. Takagi, T. Okamoto, E. Okamoto & T. Okamoto, eds.), Lect Notes Comput. Sci., vol. 4575, Springer, 2007, p. 108–131.
18. S. D. Galbraith, J. Pujolas, C. Ritzenthaler & B. Smith – "Distortion maps for supersingular genus two curves", *J. Math. Crypt.* **3** (2009), no. 1, p. 1–18.
19. R. P. Gallant, R. J. Lambert & S. A. Vanstone – "Faster point multiplication on elliptic curves with efficient endomorphisms", in *Advances in Cryptology* - Crypto *2001* (J. Kilian, ed.), Lect Notes Comput. Sci., vol. 2139, Springer, 2001, p. 190–200.
20. P. Gaudry – "Fast genus 2 arithmetic based on theta functions", *J. Math. Crypt.* **1** (2007), no. 3, p. 243–265.
21. P. Gaudry, D. Kohel & B. Smith – "Counting points on genus 2 curves with real multiplication", in *Advances in Cryptology* – Asiacrypt *2011* (D. H. Lee & H. Wang, eds.), Lect Notes Comput. Sci., vol. 7073, Springer, 2011, p. 504–519.
22. P. Gaudry & É. Schost – "On the invariants of the quotients of the jacobian of a curve of genus 2", in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 2001* (S. Boztas & I. Shparlinski, eds.), Lect Notes Comput. Sci., vol. 2227, Springer, 2001, p. 373–386.
23. — , "Genus 2 point counting over prime fields", *J. Symb. Comput.* **47** (2012), no. 4, p. 368–400.
24. E. Kachisa, E. Schaefer & M. Scott – "Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field", in *Pairing-Based Cryptography* – Pairing *2008* (S. Galbraith & K. Paterson, eds.), Lect. Notes Comput. Sci., vol. 5209, Springer, 2008, p. 126–135.
25. E. J. Kachisa – "Generating more Kawazoe-Takahashi genus 2 pairing-friendly hyperelliptic curves", in *Pairing-Based Cryptography* - Pairing *2010* (M. Joye, A. Miyaji & A. Otsuka, eds.), Lect Notes Comput. Sci., vol. 6487, Springer, 2010, p. 312–326.
26. M. Kawazoe & T. Takahashi – "Pairing-friendly hyperelliptic curves with ordinary jacobians of type $y^2 = x^5 + ax$", in *Pairing-Based Cryptography* - Pairing *2008* (S. D. Galbraith & K. G. Paterson, eds.), Lect Notes Comput. Sci., vol. 5209, Springer, 2008, p. 164–177.
27. N. Koblitz – "Elliptic curve cryptosystems", *Math. Comp.* **48** (1987), no. 177, p. 203–209.
28. — , "Hyperelliptic cryptosystems", *J. Cryptology* **1** (1989), p. 139–150.
29. E. Konstantinou, A. Kontogeorgis, Y. Stamatiou & C. Zaroliagis – "On the efficient generation of prime-order elliptic curves", *J. Cryptology* **23** (2010), p. 477–503.
30. E. Konstantinou, Y. Stamatiou & C. Zaroliagis – "Efficient generation of secure elliptic curves", *International Journal of Information Security* **6** (2007), p. 47–63.
31. R. Lercier – "Algorithmique des courbes elliptiques dans les corps finis", Thèse, École Polytechnique, 1997.
32. R. Lercier, D. Lubicz & F. Vercauteren – "Point counting on elliptic and hyperelliptic curves", in *Handbook of Elliptic and Hyperelliptic Curve Cryptography* (R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen & F. Vercauteren, eds.), Discrete Mathematics and its Applications., vol. 34, CRC Press, Boca Raton, FL, 2005, p. 239–263.
33. V. Miller – "Use of elliptic curves in cryptography", in *Advances in Cryptology* - Crypto *'85* (H. Williams, ed.), Lect Notes Comput. Sci., vol. 218, Springer, 1986, p. 417–426.

34. T. Satoh – "On p-adic point counting algorithms for elliptic curves over finite fields", in *Algorithmic Number Theory* - ANTS-V (C. Fieker & D. R. Kohel, eds.), Lect Notes Comput. Sci., vol. 2369, Springer, 2002, p. 43–66.
35. — , "Generating genus two hyperelliptic curves over large characteristic finite fields", in *Advances in Cryptology* – Eurocrypt *2009* (A. Joux, ed.), Lect Notes Comput. Sci., vol. 5479, Springer, 2009.
36. R. Schoof – "Elliptic curves over finite fields and the computation of square roots mod p", *Math. Comput.* **44** (1998), p. 483–494.
37. M. Scott – "MIRACL library", August 2011, `www.shamus.ie`.
38. K. Takashima – "A new type of fast endomorphisms on jacobians of hyperelliptic curves and their cryptographic application", *IEICE Transactions* **89-A** (2006), no. 1, p. 124–133.

A Details of the proof of Theorem 1 and Theorem 2

A.1 Proof of Theorem 1

Let us recall that the Jacobian $J_{\mathcal{C}_5}$ has *the same order* as the product $E_1 \times E_2$ over the extension field where the isogeny is defined.

- if the isogeny is defined over $\mathbb{F}_q$, i.e. if b is a fourth power, $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_q) = Z_{E_1}(T, \mathbb{F}_q) Z_{E_2}(T, \mathbb{F}_q)$ and
  (i) $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = \#E_1(\mathbb{F}_q)\#E_2(\mathbb{F}_q) = (q + 1 - t_q)^2$ if -1 is a square in $\mathbb{F}_q$,
  (ii) $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = \#E_1(\mathbb{F}_q)\#E_2(\mathbb{F}_q) = (q + 1 - t_q)(q + 1 + t_q)$ otherwise;
- if the isogeny is defined over $\mathbb{F}_{q^2}$, i.e. if b is a square but not a fourth power (hence $q \equiv 1 \mod 4$), or if b is not a square and $q \equiv 3 \mod 4$, then E_1 and E_2 are defined over $\mathbb{F}_{q^2}$, of trace t_{q^2} and $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_{q^2}) = Z_{E_1}(T, \mathbb{F}_{q^2}) Z_{E_2}(T, \mathbb{F}_{q^2}) = (T^2 - t_{q^2} T + q^2)^2$ and we have to go down from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$;
- if the isogeny is defined over $\mathbb{F}_{q^4}$, i.e. if b is not a square and $q \equiv 1 \mod 4$, $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_{q^4}) = Z_{E_1}(T, \mathbb{F}_{q^4}) Z_{E_2}(T, \mathbb{F}_{q^4}) = (T^2 - t_{q^4} T + q^4)^2$ with t_{q^4} the trace of E_1 and E_2 over $\mathbb{F}_{q^4}$. We have to recover the zeta function from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q$.

The isogeny is defined over $\mathbb{F}_{q^2}$. We have the following decomposition through isogenies:

$$\begin{array}{ccccc}
 & & (E_1 \times E_2)(\mathbb{F}_{q^4}) & \overset{\text{isomorphism}}{\longleftrightarrow} & (E_1' \times E_2')(\mathbb{F}_{q^4}) \\
 & & \Big| & & \Big| \\
J_{\mathcal{C}_5}(\mathbb{F}_{q^2}) & \overset{\text{isogeny}}{\longleftrightarrow} & (E_1 \times E_2)(\mathbb{F}_{q^2}) & & (E_1' \times E_2')(\mathbb{F}_{q^2}) \\
 & & \text{whose trace is } t_{q^2} = -t'_{q^2} & & \text{of trace } t'_{q^2} = (t'_q)^2 - 2q \\
\Big| & & & & \Big| \\
J_{\mathcal{C}_5}(\mathbb{F}_q) & & & & (E_1' \times E_2')(\mathbb{F}_q) \\
 & & & & \text{of trace } \pm t'_q
\end{array}$$

If b is a square but not a fourth power, the coefficient δ of the curves E_1 and E_2 is in $\mathbb{F}_{q^2}$. The parameter $\sqrt{b}$ is in $\mathbb{F}_q$ hence a corresponding quadratic twist for the two elliptic curves is available and defined over $\mathbb{F}_q$. If b is not a square, a quadratic extension $\mathbb{F}_{q^2}$ contains $\sqrt{b}$ which is a square in $\mathbb{F}_{q^2}$ if $q \equiv 3 \mod 4$ (hence $\sqrt[4]{b} \in \mathbb{F}_{q^2}$). Otherwise the lowest extension containing $\sqrt[4]{b}$ is $\mathbb{F}_{q^4}$ and the isogeny is defined over $\mathbb{F}_{q^4}$.

We have $Z_{E_1}(T, \mathbb{F}_{q^2}) = Z_{E_2}(T, \mathbb{F}_{q^2}) = T^2 - t_{q^2} T + q^2$ and for the Jacobian $J_{\mathcal{C}_5}$, its zeta function is $Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_{q^2}) = T^4 - a_{q^2} T^3 + b_{q^2} T^2 - q^2 a_{q^2} T + q^4 = (T^2 - t_{q^2} T + q^2)^2$. Hence $(a_{q^2}, b_{q^2}) = (2t_{q^2}, (t_{q^2})^2 + 2q^2)$. We easily solve equations (2-1) into $(a_q, b_q) = (\pm 2\sqrt{2q + t_{q^2}}, 4q + t_{q^2})$ or $(a_q, b_q) = (0, -t_{q^2})$.

In the former case, since a_q must be an integer, $2q + t_{q^2}$ must be a square. If E_1 is actually defined over $\mathbb{F}_q$ (and so does the isogeny), $2q + t_{q^2} = (t_q)^2$. If E_1 is not defined over $\mathbb{F}_q$, neither is the isogeny and $2q + t_{q^2}$ is rarely a square. Assuming that $2q + t_{q^2}$ is not a square, the unique possibility is $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - t_{q^2}$. If $\sqrt{b} \in \mathbb{F}_q$, a quadratic twist E_1' of E_1 defined over $\mathbb{F}_q$ exists with $t_{q^2} = -t'_{q^2} = 2q - (t'_q)^2$. We can simplify the trace computation to t'_q, the trace of the elliptic curve $E_1'(\mathbb{F}_q)$. $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q - 1)^2 + (t'_q)^2$.

Special case. If $2q + t_{q^2}$ is still a square, let $2q + t_{q^2} = y^2$ with $y \in \mathbb{N}$. There are three possibilities for the Jacobian order: $(q+1-y)^2$, $(q+1+y)^2$ or $(q+1-y)(q+1+y) = q^2+1-t_{q^2}$ ('*normal*' case) and the Jacobian is not simple (its zeta function factors in the same way). If $q \equiv 1 \mod 4$, $\sqrt{b} \in \mathbb{F}_q$ and a quadratic twist $E_1^{'}$ is defined over $\mathbb{F}_q$ (we remove $b^{1/4}$ from the equation of E_1). Hence $\Delta(E_1(\mathbb{F}_{q^2})) = (t_{q^2})^2 - 4q^2 = -(y \cdot t_q^{'})^2$ and the curve has $D = 1$ (i.e. Complex Multiplication by $i = \sqrt{-1}$). Moreover $E_1(\mathbb{F}_{q^2})$ is isogenous to a curve $\mathring{E}_1(\mathbb{F}_{q^2})$ with j-invariant 0. The Jacobian is isogenous over $\mathbb{F}_q$ to two quartic twists of $E_1^{'}$ and $E_2^{'}$.

$$
\begin{array}{ccccc}
 & & (E_1 \times E_2)(\mathbb{F}_{q^4}) & \overset{\text{isomorphism}}{\longleftrightarrow} & (E_1^{'} \times E_2^{'})(\mathbb{F}_{q^4}) \\
 & & \Big| & & \Big| \\
J_{\mathcal{C}_5}(\mathbb{F}_{q^2}) & \overset{\text{isogeny}}{\longleftrightarrow} (\mathring{E}_1 \times \mathring{E}_2)(\mathbb{F}_{q^2}) & \overset{\text{isogeny}}{\longleftrightarrow} (E_1 \times E_2)(\mathbb{F}_{q^2}) & & (E_1^{'} \times E_2^{'})(\mathbb{F}_{q^2}) \\
 & & \text{whose trace is} & & \text{of trace } t_{q^2}^{'} = (t_q^{'})^2 - 2q \\
\Big| & \Big| & t_{q^2} = -t_{q^2}^{'} & & \Big| \\
J_{\mathcal{C}_5}(\mathbb{F}_q) & \overset{\text{isogeny}}{\longleftrightarrow} (\mathring{E}_1 \times \mathring{E}_2)(\mathbb{F}_q) & & & (E_1^{'} \times E_2^{'})(\mathbb{F}_q) \\
 & & & & \text{of trace } \pm t_q^{'}
\end{array}
$$

The isogeny is defined over $\mathbb{F}_{q^4}$. The decomposition into two isogenous elliptic curves is as follows:

$$
\begin{array}{ccccc}
 & & (E_1 \times E_2)(\mathbb{F}_{q^8}) & \overset{\text{isomorphism}}{\longleftrightarrow} & (E_1^{'} \times E_2^{'})(\mathbb{F}_{q^8}) \\
 & & \Big| & & \Big| \\
J_{\mathcal{C}_5}(\mathbb{F}_{q^4}) & \overset{\text{isogeny}}{\longleftrightarrow} & (E_1 \times E_2)(\mathbb{F}_{q^4}) & & (E_1^{'} \times E_2^{'})(\mathbb{F}_{q^4}) \\
 & & \text{whose trace is } t_{q^4} = -t_{q^4}^{'} & & \text{of trace } t_{q^4}^{'} = (t_{q^2}^{'})^2 - 2q^2 \\
\Big| & & & & \Big| \\
J_{\mathcal{C}_5}(\mathbb{F}_{q^2}) & & & & (E_1^{'} \times E_2^{'})(\mathbb{F}_{q^2}) \\
\Big| & & & & \text{of trace } t_{q^2}^{'} \\
J_{\mathcal{C}_5}(\mathbb{F}_q) & & & &
\end{array}
$$

We proceed in two steps. First we find the coefficients of the zeta function over $\mathbb{F}_{q^2}$. There is also a special case: if $2q^2 + t_{q^4}$ is a square there are three other possibilities, see below. If $2q^2 + t_{q^4}$ is not a square we obtain $(a_{q^2}, b_{q^2}) = (0, -t_{q^4}) = (0, (t_{q^2}^{'})^2 - 2q^2)$. The final polynomial system to solve is the following:

$$(a_q)^2 - 2b_q = 0 \tag{3}$$

$$(b_q)^2 - 4qb_q + 2q^2 + t_{q^4} = 0 \tag{4}$$

Equation (4) gives $b_q = 2q \pm \sqrt{2q^2 - t_{q^4}}$. The elliptic curve E_1 admits a twisted elliptic curve $E_1^{'}$ defined over $\mathbb{F}_{q^2}$ and of opposite trace over $\mathbb{F}_{q^4}$, $t_{q^4} = -t_{q^4}^{'} = -(t_{q^2}^{'})^2 + 2q^2$. Hence $b_q \in \{2q - t_{q^2}^{'}, 2q + t_{q^2}^{'}\}$ and we obtain through equation (3) that $a_q = \pm\sqrt{2b_q}$. Thus $(a_q, b_q) = \left(\pm\sqrt{2(2q - t_{q^2}^{'})}, 2q - t_{q^2}^{'}\right)$ or $(a_q, b_q) = \left(\pm\sqrt{2(2q + t_{q^2}^{'})}, 2q + t_{q^2}^{'}\right)$ and either $2(2q + t_{q^2}^{'})$ or $2(2q - 2t_{q^2}^{'})$ is always a square. More precisely, when $q \equiv 1 \mod 8$ we observe that $2q - t_{q^2}^{'} = 2n^2$ and when $q \equiv 5 \mod 8$, $2q + t_{q^2}^{'} = 2n^2$. Let $n \in \mathbb{N}$ be such that either $b_q = 2q + t_{q^2}^{'} = 2n^2$ or $b_q = 2q - t_{q^2}^{'} = 2n^2$. We have

$$\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - 2n(1+q) + 2n^2 \text{ or } \#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 + 2n(1+q) + 2n^2 \ .$$

Special case. We now consider the special case of $2q^2+t_{q^4}=y^2$ being a square. This implies because of the quadratic twist and $t_{q^4}-2q^2=-(t'_{q^2})^2$ that the curve E_1 has $D=1$ ($\Delta(E_1)=-(y\cdot t'_{q^2})^2$). When solving the first system to get (a_{q^2},b_{q^2}), these two additional possibilities have to be checked: $(a_{q^2}=\pm 2y, b_{q^2}=2q^2+y^2)$ and $\#J_{\mathcal{C}_5}(\mathbb{F}_{q^2})=(q^2+1\mp y)^2$. The Jacobian zeta function splits in two parts. This means that the Jacobian is isogenous over $\mathbb{F}_{q^2}$ to two elliptic curves, namely the quartic twists of $E'_1(\mathbb{F}_{q^2})$ and $E'_2(\mathbb{F}_{q^2})$.

What is happening over the ground field $\mathbb{F}_q$? They are at most 10 possibilities for $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$ and this order splits in two parts in each case. Writing $t_{q^4}+2q^2=y^2$, we decompose it into $-(t'_{q^2})^2+4q^2=(2q-t'_{q^2})(2q+t'_{q^2})$. Let $2q-t'_{q^2}=D_1(y_1)^2$ and $2q+t'_{q^2}=D_2(y_2)^2$ with D_1 and D_2 square-free and D_1D_2 a square. Hence $D_1=D_2$. As $q\equiv 1 \mod 4$ and $t'_{q^2}\equiv 0 \mod 2$, we obtain that

1. $D_1(y_1)^2\equiv D_2(y_2)^2\equiv 0 \mod 4$ if $t'_{q^2}\equiv 2 \mod 4$;
2. $D_1(y_1)^2\equiv D_2(y_2)^2\equiv 2 \mod 4$ if $t'_{q^2}\equiv 0 \mod 4$.

Moreover, $q=(D_1y_1^2+D_2y_2^2)/4$ is a prime power, char >2, $t'_{q^2}\neq 0$. We obtain that if q is prime then y_1 and y_2 are coprime and $D_1=D_2=2$ if $t'_{q^2}\equiv 0 \mod 4$ or $D_1=D_2=1$ and $\gcd(y_1^2,y_2^2)=4$ if $t'_{q^2}\equiv 2 \mod 4$. We reformulate it as $\gcd(y_1,y_2)=1$ and

1. $D_1=D_2=2$ if $t'_{q^2}\equiv 0 \mod 4$ (and $q=(y_1^2+y_2^2)/2$);
2. $D_1=D_2=4$ if $t'_{q^2}\equiv 2 \mod 4$ (and $q=y_1^2+y_2^2$).

If q is a prime power, let $p=\mathrm{char}(q)$. $\gcd(y_1,y_2)$ is 1 or a power of p and

1. if $t'_{q^2}\equiv 0 \mod 4$ then $D_1=D_2=2$ and $q=(y_1^2+y_2^2)/2$ or $D_1=D_2=2p$ and $q=p(y_1^2+y_2^2)/2$;
2. if $t'_{q^2}\equiv 2 \mod 4$ then $D_1=D_2=4$ and $q=y_1^2+y_2^2$ or $D_1=D_2=4p$ and $q=p(y_1^2+y_2^2)$.

Does $q^2+1\pm y$ splits ? In other words, are $y+2q$ and $-y+2q$ squares ?

1. if $D_1=D_2=2$ then $q=(y_1^2+y_2^2)/2$, $y=2y_1y_2$ and a possible choice for $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$ is $q^2+1-n(q+1-n)$ with $n\in\{\pm y_1,\pm y_2\}$. More precisely, the Jacobian order has always two factors:
   (i) $n=y_1$, $\#J_{\mathcal{C}_5}(\mathbb{F}_q)=(q+1-y_1+y_2)(q+1-y_1-y_2)$;
   (ii) $n=-y_1$, $\#J_{\mathcal{C}_5}(\mathbb{F}_q)=(q+1+y_1+y_2)(q+1+y_1-y_2)$;
   (iii) $n=y_2$, $\#J_{\mathcal{C}_5}(\mathbb{F}_q)=(q+1+y_1-y_2)(q+1-y_1-y_2)$;
   (iv) $n=-y_2$, $\#J_{\mathcal{C}_5}(\mathbb{F}_q)=(q+1+y_1+y_2)(q+1-y_1+y_2)$.
   $y+2q=2y_1y_2+y_1^2+y_2^2=(y_1+y_2)^2$ and $-y+2q=(y_1-y_2)^2$. The others choices for $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$ are $\{(q+1-y_1+y_2)(q+1+y_1-y_2)=q^2+1+y,(q+1+y_1+y_2)(q+1-y_1-y_2)=q^2+1-y,(q+1-y_1+y_2)^2,(q+1+y_1-y_2)^2,(q+1+y_1+y_2)^2,(q+1-y_1-y_2)^2\}$.
2. Otherwise ($D_1\neq 2, D_2\neq 2$), the two numbers $y+2q$ and $-y+2q$ are not squares. The two choices for $\#J_{\mathcal{C}_5}(\mathbb{F}_q)$ are q^2+1+y and q^2+1-y.

All possibilities are summarized in Tab. 1.

A.2 Proof of Theorem 2

A first observation gives these simplifications. For the notations, see 3.1.

– If b is a square in $\mathbb{F}_q$ then $\mathcal{C}'_6$, E_c and E_{-c} are defined over $\mathbb{F}_q$.

Conditions			$\#J_{\mathcal{C}_5}(\mathbb{F}_q)$
b is a 4th power in $\mathbb{F}_q$		-1 is a square in $\mathbb{F}_q$	$(q+1-t_q)^2$
		-1 is not a square in $\mathbb{F}_q$	$(q+1-t_q)(q+1+t_q)$
b is a square but not a 4th power in $\mathbb{F}_q$ $q \equiv 1 \bmod 4$		$t_{q^2}+2q$ is not a square	$(q-1)^2+(t_q^{'})^2$
		$t_{q^2}+2q=y^2$ is a square	$(q+1-y)^2$, $(q+1+y)^2$ or $(q+1-y)(q+1+y)=(q-1)^2+(t_q^{'})^2$
b is not a square in $\mathbb{F}_q$ and $q \equiv 3 \bmod 4$		$t_{q^2}+2q$ is not a square	$q^2+1-t_{q^2}$
		$t_{q^2}+2q=y^2$ is a square	$(q+1-y)^2$, $(q+1+y)^2$ or $(q+1-y)(q+1+y)=q^2+1-t_{q^2}$
b is not a square in $\mathbb{F}_q$ and $q \equiv 1 \bmod 4$	$t_{q^4}+2q^2$ is not a square	let $n \in \mathbb{N}$ s.t. $2q+t_{q^2}^{'}=2n^2$ if $q \equiv 5 \bmod 8$ or $2q-t_{q^2}^{'}=2n^2$ if $q \equiv 1 \bmod 8$	$q^2+1-2n(q+1)+2n^2$ or $q^2+1+2n(q+1)+2n^2$
	$t_{q^4}+2q^2$ is a square, $=y^2$. Write $y^2=-(t_{q^2}^{'})^2+4q^2=(2q+t_{q^2}^{'})(2q-t_{q^2}^{'})=D_1y_1^2D_2y_2^2$	$D_1 \neq 2$ and $D_2 \neq 2$	q^2+1-y or q^2+1+y.
		$D_1=D_2=2$	$(q+1-y_1+y_2)(q+1-y_1-y_2)$ (i.e. $n=y_1$), $(q+1+y_1+y_2)(q+1+y_1-y_2)$ (i.e. $n=-y_1$), $(q+1+y_1-y_2)(q+1-y_1-y_2)$ (i.e. $n=y_2$), $(q+1+y_1+y_2)(q+1-y_1+y_2)$ (i.e. $n=-y_2$), $(q+1+y_1+y_2)(q+1-y_1-y_2)=q^2+1-y$, $(q+1-y_1+y_2)(q+1+y_1-y_2)=q^2+1+y$, $(q+1-y_1+y_2)^2$, $(q+1+y_1-y_2)^2$, $(q+1+y_1+y_2)^2$, $(q+1-y_1-y_2)^2$.

Table 1. Possible Jacobian orders for the curve $\mathcal{C}_5$ over $\mathbb{F}_q$.

(i) If b is a cube in $\mathbb{F}_q$ then $J_{\mathcal{C}_6}(\mathbb{F}_q)$, $J_{\mathcal{C}_6'}(\mathbb{F}_q)$, $E_c(\mathbb{F}_q) \times E_{-c}(\mathbb{F}_q)$ are all three isogenous over $\mathbb{F}_q$. If $q \equiv 1 \mod 3$ then -3 is a square in $\mathbb{F}_q$. $E_c(\mathbb{F}_q)$ and $E_{-c}(\mathbb{F}_q)$ are isogenous and have the same trace t_q, and we have $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = (q+1-t_q)^2$. Otherwise, -3 is not a square and E_c and E_{-c} are isogenous over $\mathbb{F}_{q^2}$ but of opposite trace $t_q, -t_q$ over $\mathbb{F}_q$ and $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = (q+1-t_q)(q+1+t_q)$.

(ii) If b is not a cube in $\mathbb{F}_q$, $J_{\mathcal{C}_6}$ and $J_{\mathcal{C}_6'}$ are isogenous over $\mathbb{F}_{q^3}$. But as b is not a cube, $q \equiv 1 \mod 3$, hence -3 is a square in $\mathbb{F}_q$. E_c and E_{-c} are isogenous over $\mathbb{F}_q$, with the same trace t_q and $\#J_{\mathcal{C}_6'}(\mathbb{F}_q) = \#E_c(\mathbb{F}_q)\#E_{-c}(\mathbb{F}_q) = (q+1-t_q)^2$. We have to compute $\#J_{\mathcal{C}_6}(\mathbb{F}_q)$ from $\#J_{\mathcal{C}_6'}(\mathbb{F}_q)$ through $\#J_{\mathcal{C}_6}(\mathbb{F}_{q^3}) = \#J_{\mathcal{C}_6'}(\mathbb{F}_{q^3})$.

– If b is not a square in $\mathbb{F}_q$, the abelian varieties $J_{\mathcal{C}_6'}, E_c, E_{-c}$ are defined over $\mathbb{F}_{q^2}$. In this case $-3 \in \mathbb{F}_q$ is a square in $\mathbb{F}_{q^2}$ and the two elliptic curves $E_c(\mathbb{F}_{q^2})$ and $E_{-c}(\mathbb{F}_{q^2})$ are isogenous with the same trace t_{q^2}. The Jacobian $J_{\mathcal{C}_6'}$ and $E_c \times E_{-c}$ are isogenous over $\mathbb{F}_{q^2}$.

(i) If b is a cube, $J_{\mathcal{C}_6}(\mathbb{F}_{q^2})$ is isogenous to $J_{\mathcal{C}_6'}(\mathbb{F}_{q^2})$. Solving equations (2) and (1) with $(a_{q^2}, b_{q^2}) = (2t_{q^2}, (t_{q^2})^2 + 2q^2)$ we find $(a_q, b_q) = (0, -t_{q^2})$ (if $t_{q^2}+2q$ is not a square) and $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2+1-t_{q^2}$.

(ii) If b is not a cube, $J_{\mathcal{C}_6}$ and $J_{\mathcal{C}_6'}$ are isogenous over $\mathbb{F}_{q^6}$ and $J_{\mathcal{C}_6'}$ is isogenous to $E_c \times E_{-c}$ over $\mathbb{F}_{q^2}$.

The isogeny is defined over $\mathbb{F}_{q^3}$. With the same assumptions about zeta functions as in Section 2, we denote by a_{q^3} and b_{q^3} the zeta function coefficients of $J_{\mathcal{C}_6}$ over $\mathbb{F}_{q^3}$. We have

$$a_{q^3} = z_{1,q}^3 + z_{2,q}^3 + z_{3,q}^3 + z_{4,q}^3 \text{ and } b_{q^3} = 2q^3 + (z_{1,q}^3 + z_{2,q}^3)(z_{3,q}^3 + z_{4,q}^3)$$

We note that $z_{1,q}^3 + z_{2,q}^3 = (z_{1,q} + z_{2,q})^3 - 3q(z_{1,q} + z_{2,q})$ and $z_{3,q}^3 + z_{4,q}^3 = (z_{3,q} + z_{4,q})^3 - 3q(z_{3,q} + z_{4,q})$. We have

$$\begin{aligned}
a_{q^3} &= (z_{1,q}^3 + z_{2,q}^3) + (z_{3,q}^3 + z_{4,q}^3) \\
&= (z_{1,q} + z_{2,q})^3 + (z_{3,q} + z_{4,q})^3 - 3q(z_{1,q} + z_{2,q}) - 3q(z_{3,q} + z_{4,q}) \\
&= (z_{1,q} + z_{2,q})^3 + (z_{3,q} + z_{4,q})^3 - 3qa_q \\
&= (z_{1,q} + z_{2,q})^3 + (z_{3,q} + z_{4,q})^3 - 3qa_q \\
&\quad +3\left[(z_{1,q} + z_{2,q}) + (z_{3,q} + z_{4,q})\right]\left[(z_{1,q} + z_{2,q})(z_{3,q} + z_{4,q})\right] - 3a_q(b_q - 2q) \\
&= (z_{1,q} + z_{2,q} + z_{3,q} + z_{4,q})^3 - 3a_q(b_q - 2q + q) \\
&= (a_q)^3 - 3a_q(b_q - q)
\end{aligned}$$

and

$$\begin{aligned}
b_{q^3} &= 2q^3 + \left[(z_{1,q} + z_{2,q})^3 - 3q(z_{1,q} + z_{2,q})\right]\left[(z_{3,q} + z_{4,q})^3 - 3q(z_{3,q} + z_{4,q})\right] \\
&= 2q^3 + \left[(z_{1,q} + z_{2,q})(z_{3,q} + z_{4,q})\right]^3 + 9q^2(z_{1,q} + z_{2,q})(z_{3,q} + z_{4,q}) \\
&\quad -3q(z_{1,q} + z_{2,q})(z_{3,q} + z_{4,q})^3 - 3q(z_{1,q} + z_{2,q})^3(z_{3,q} + z_{4,q}) \\
&= 2q^3 + (b_q - 2q)^3 + 9q^2(b_q - 2q) - 3q(b_q - 2q)\left[(z_{3,q} + z_{4,q})^2 + (z_{1,q} + z_{2,q})^2\right] \\
&= 2q^3 + (b_q - 2q)^3 + 9q^2(b_q - 2q) - 3q(b_q - 2q)(a_{q^2} + 4q) \\
&= 2q^3 + (b_q - 2q)^3 + 9q^2(b_q - 2q) - 3q(b_q - 2q)((a_q)^2 - 2b_q + 4q) \\
&= (b_q)^3 - 3q^2b_q - 3q(a_q)^2b_q + 6q^2(a_q)^2
\end{aligned}$$

which gives the following system to solve

$$\begin{cases} a_{q^3} = (a_q)^3 - 3a_q(b_q - q) \\ b_{q^3} = (b_q)^3 - 3q^2(b_q) - 3q(a_q)^2(b_q) + 6q^2(a_q)^2 \end{cases}$$

This system is not linear and the two equations are not independent. Nevertheless we can obtain a more precise system to solve. Indeed, as the Jacobian splits into two isogenous elliptic curves over $\mathbb{F}_{q^3}$ (assuming b is a square but not a cube in a first case), its zeta function over $\mathbb{F}_{q^3}$ splits into two polynomials with integer coefficients and we can find independently the two roots of each factor. More precisely, $Z_{J_{\mathcal{C}_6}}(T, \mathbb{F}_{q^3}) = Z_{E_c}(T, \mathbb{F}_{q^3}) Z_{E_{-c}}(T, \mathbb{F}_{q^3})$ which results in

$$(T^2 - (z_{1,q}^3 + z_{2,q}^3)T + q^3)(T^2 - (z_{3,q}^3 + z_{4,q}^3)T + q^3) = (T^2 - t_{q^3}T + q^3)^2 \ .$$

With a last simplification using the fact $t_{q^3} = (t_q)^3 - 3qt_q$, we obtain an easy system to solve

$$\begin{cases} z_{1,q}^3 + z_{2,q}^3 = (z_{1,q} + z_{2,q})^3 - 3q(z_{1,q} + z_{2,q}) = (t_q)^3 - 3qt_q \\ z_{3,q}^3 + z_{4,q}^3 = (z_{3,q} + z_{4,q})^3 - 3q(z_{3,q} + z_{4,q}) = (t_q)^3 - 3qt_q \end{cases}$$

It is important here to note that the two elliptic curves are isogenous, hence of same trace t_q. An obvious solution is $z_{1,q} + z_{2,q} = z_{3,q} + z_{4,q} = t_q$ which corresponds to the case where b is a cube and $J_{\mathcal{C}_6}$ is isogenous to $E_c \times E_{-c}$ over $\mathbb{F}_q$. The two other solutions are

$$z_{1,q} + z_{2,q} = \left(-t_q \pm \sqrt{3(4q - (t_q)^2)}\right)/2, \ z_{3,q} + z_{4,q} = \left(-t_q \pm \sqrt{3(4q - (t_q)^2)}\right)/2 \ .$$

If $3(4q-(t_q)^2)$ is not a square, we have no choice concerning the signs (the two above square roots which are irrational must eliminate themselves when computing a_q and b_q), we must choose $z_{1,q}+z_{2,q}$ as the conjugate of $z_{3,q}+z_{4,q}$. This results in

$$a_q = -t_q \text{ and } b_q = 2q + \big((t_q)^2 - 3(4q-(t_q)^2)\big)/4 = (t_q)^2 - q$$

Finally we obtain that if b is a square but not a third power (and $3(4q-(t_q)^2)$ is not a square) then

$$\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2 - q + 1 + (1+q+t_q)t_q \ .$$

Note that

$$\begin{aligned}\#E_c(\mathbb{F}_q) &= q+1-t_q\\ \#E_c(\mathbb{F}_{q^3}) &= q^3+1-((t_q)^3-3qt_q) = (q+1-t_q)(q^2-q+1+t_q(q+1+t_q))\\ &= \#E_c(\mathbb{F}_q)\#J_{\mathcal{C}_6}(\mathbb{F}_q).\end{aligned}$$

Special case. If $3(4q-(t_q)^2)$ is a square, we face a special curve with $4q-(t_q)^2 = 3y^2$. More precisely, this curve is *isogenous* to a curve with j-invariant equals to 0. This curve admits two cubic twists of order (over $\mathbb{F}_q$) $q+1+(t_q+3y)/2$ and $q+1+(t_q-3y)/2$. Six possibilities can occur for the Jacobian order but we don't consider $z_{1,q}+z_{2,q}=t_q$ or $z_{3,q}+z_{4,q}=t_q$ as it corresponds to the isogeny between $J_{\mathcal{C}_6}$ and $E_c \times E_{-c}$ defined over $\mathbb{F}_q$.

$$z_{1,q}+z_{2,q},\ z_{3,q}+z_{4,q} \in \{(-t_q+3y)/2,\ (-t_q-3y)/2\} \ .$$

In each case, the Jacobian splits as the two above values are integers. The Jacobian zeta function splits into two degree 2 polynomials $(T^2-(z_{1,q}+z_{2,q})T+q)(T^2-(z_{3,q}+z_{4,q})T+q)$.

$\#J_{\mathcal{C}_6}(\mathbb{F}_q)$ is one of $(q+1+(t_q+3y)/2)^2$, $(q+1+(t_q-3y)/2)^2$, $(q+1+(t_q+3y)/2)(q+1+(t_q-3y)/2) = q^2-q+1+(1+q+t_q)t_q$ ('*normal*' case). When solving $j(E_c)=0$ we obtain $c=5/2$. To construct a toy example, we take $a=1, b=(2/5)^2$. Let $p=313,\ a=1,\ b=213,\ c=159$ and $\mathcal{C}(\mathbb{F}_p): y^2 = x^6+ax^3+b$. $j(E_c)=0, j(E_{-c})=67$ and their trace is $t_p=35$. It satisfies $(t_p)^2-4p = -3\cdot 3^2$. We obtain that $\#J_{\mathcal{C}_6}(\mathbb{F}_p) = 327\cdot 336 = (p+1+(t_p-3y)/2)(p+1+(t_p+3y)/2)$. It would be interesting to find explicitly the isogeny.

The isogeny is defined over $\mathbb{F}_{q^6}$. To generalize to the case where b is neither a square nor a cube, we just have to consider q^2, z_{i,q^2} and t_{q^2} instead of q, $z_{i,q}$ and t_q. With the same arguments we find with $3(4q^2-(t_{q^2})^2)$ not a square

$$\#J_{\mathcal{C}_6}(\mathbb{F}_{q^2}) = q^4 - q^2 + 1 + (1+q^2+t_{q^2})t_{q^2} \ .$$

The descent from $\#J_{\mathcal{C}_6}(\mathbb{F}_{q^2})$ to $\#J_{\mathcal{C}_6}(\mathbb{F}_q)$ was already treated in 2.2. We have here $(a_{q^2}, b_{q^2}) = (-t_{q^2}, (t_{q^2})^2 - q^2)$. We solve the equations (2-1) into $(a_q, b_q) = (\pm\sqrt{2q+t_{q^2}}, q+t_{q^2})$ or $(\pm\sqrt{3(2q-t_{q^2})}, 3q-t_{q^2})$. We assumed at the preceding step that $3(4q^2-(t_{q^2})^2)$ is not a square. The expression $2q+t_{q^2}$ is a square if E_c is actually defined over $\mathbb{F}_q$ (i.e. $2q+t_{q^2}=(t_q)^2$) or if E_c is a very special curve, with $2q+t_{q^2}=s^2$ a square. For this choice, $(a_q,b_q)=(\pm s, s^2-q)$ and $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2-q+1\pm(1+q)s+s^2$. We can't have $2q+t_{q^2}$ and $3(2q-t_{q^2})$ both squares as we assumed that $3(4q^2-(t_{q^2})^2)$ is not a square. If $2q+t_{q^2}$ is not a square, the right solution is $(a_q,b_q) = (\pm\sqrt{3(2q-t_{q^2})}, 3q-t_{q^2})$. Once more, a_q must be an integer. Let $n\in\mathbb{Z}$ be such that $2q-t_{q^2}=3n^2$. We conclude that

$$\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2+q+1+3n^2+3n(q+1) \ .$$

Special case. When $3(4q^2 - (t_{q^2})^2) = 9y^2$ is a square, we have

$$z_{1,q^2} + z_{2,q^2};\ z_{3,q^2} + z_{4,q^2} \in \{t_{q^2}, (-t_{q^2} + 3y)/2, (-t_{q^2} - 3y)/2\}.$$

These three values correspond to the traces of three elliptic curves that are cubic twists of each other. One of them is $E_c(\mathbb{F}_{q^2})$. As the isogeny is defined over $\mathbb{F}_{q^6}$ but not $\mathbb{F}_{q^2}$, we eliminate the cases $z_{1,q^2} + z_{2,q^2} = t_{q^2}$ and $z_{1,q^2} + z_{2,q^2} = t_{q^2}$. This value t_{q^2} is for the cubic twist $J_{\mathcal{C}_6'}(\mathbb{F}_{q^2})$. Indeed because of the isogeny between $J_{\mathcal{C}_6'}(\mathbb{F}_{q^2})$ and $(E_c \times E_{-c})(\mathbb{F}_{q^2})$, the zeta function for this Jacobian is $Z_{J_{\mathcal{C}_6'}}(T, \mathbb{F}_{q^2}) = (T^2 - t_{q^2}T + q^2)^2$. We obtain the following possibilities for (a_{q^2}, b_{q^2}):

case	$z_{1,q^2} + z_{2,q^2}$	$z_{3,q^2} + z_{4,q^2}$	a_{q^2}	b_{q^2}
1	$(-t_{q^2} + 3y)/2$	$(-t_{q^2} - 3y)/2$	$-t_{q^2}$	$(t_{q^2})^2 - q^2$
2	$(-t_{q^2} + 3y)/2$	$(-t_{q^2} + 3y)/2$	$-t_{q^2} + 3y$	$(-t_{q^2} + 3y)^2/4 + 2q^2$
3	$(-t_{q^2} - 3y)/2$	$(-t_{q^2} - 3y)/2$	$-t_{q^2} - 3y$	$(-t_{q^2} - 3y)^2/4 + 2q^2$

The first one corresponds to the '*normal*' case, we obtain $\#J_{\mathcal{C}_6}(\mathbb{F}_{q^2}) = q^4 - q^2 + 1 + (1 + q^2 + t_{q^2})t_{q^2}$ and moreover it factors. The two possibilities for $J_{\mathcal{C}_6}(\mathbb{F}_q)$ are

1. $(a_q, b_q) = (\pm\sqrt{3(2q - t_{q^2})}, 3q - t_{q^2})$
2. $(a_q, b_q) = (\pm\sqrt{2q + t_{q^2}}, q + t_{q^2})$

hence $3(2q - t_{q^2})$ or $2q + t_{q^2}$ must be a square. As $3(-(t_{q^2})^2 + 4q^2)$ is a square, the two last values are both squares (or both not squares). If $3(2q - t_{q^2}) = n^2$ and $2q + t_{q^2} = s^2$, these two orders must be checked both :

1. $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2 - q + 1 \pm s(q + 1) + s^2$
2. $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2 + q + 1 + 3n(q + 1) + 3n^2$.

The other cases are more special and we don't see how to construct such an example. We can say that for each case, the Jacobian splits in two elliptic curves. We recognize two cubic twists and two sextic twists. Let denote $\Delta(E_c(\mathbb{F}_{q^2})) = t_{q^2}^2 - 4q^2 = (t_{q^2} - 2q)(t_{q^2} + 2q)$ and decompose it in $t_{q^2} - 2q = -D_1 y_1^2$ and $t_{q^2} + 2q = D_2 y_2^2$ with D_1, D_2 square-free.

All possibilities are summarized in Tab. 2.

Conditions		$\#J_{\mathcal{C}_5}(\mathbb{F}_q)$
b is a 6th power in $\mathbb{F}_q$	-3 is a square in $\mathbb{F}_q$	$(q+1-t_q)^2$
	-3 is not a square in $\mathbb{F}_q$	$(q+1-t_q)(q+1+t_q)$
b is a square but not a cube in $\mathbb{F}_q$	$3(4q-(t_q)^2)$ is not a square	$q^2-q+1+(1+q+t_q)t_q$
	$4q-(t_q)^2=3y^2$	$(q+1+(t_q+3y)/2)^2$, $(q+1+(t_q-3y)/2)^2$ or $(q+1+\frac{t_q+3y}{2})(q+1+\frac{t_q-3y}{2})=q^2-q+1+(1+q+t_q)t_q$
b is a cube but not a square in $\mathbb{F}_q$	$t_{q^2}+2q$ is not a square	$q^2+1-t_{q^2}$
	$t_{q^2}+2q$ is a square, $=y^2$	$(q+1-y)^2$, $(q+1+y)^2$ or $(q+1-y)(q+1+y)=q^2+1-t_{q^2}$
b is neither a square nor a cube in $\mathbb{F}_q$. Write $-t_{q^2}^2+4q^2=(2q-t_{q^2})(2q+t_{q^2})$ and $2q-t_{q^2}=D_1n^2$, $2q+t_{q^2}=D_2s^2$.	$D_2\neq 1$, $D_1=3$ i.e. $2q-t_{q^2}=3n^2$	$q^2+q+1-3n(q+1)+3n^2$ or $q^2+q+1+3n(q+1)+3n^2$
	$D_1\neq 3$, $D_2=1$ i.e. $2q+t_{q^2}=s^2$	$q^2-q+1-(1+q)s+s^2$ or $q^2-q+1+(1+q)s+s^2$.
	$D_1=3, D_2=1$ i.e. $2q-t_{q^2}=3n^2$ and $2q+t_{q^2}=s^2$	$(q+1-\frac{s-3n}{2})(q+1-\frac{s+3n}{2})=q^2-q+1+(1+q)s+s^2$, $(q+1+\frac{s+3n}{2})(q+1+\frac{s-3n}{2})=q^2-q+1-(1+q)s+s^2$, $(q+1+\frac{s-3n}{2})(q+1-\frac{s+3n}{2})=q^2+q+1-3n(q+1)+3n^2$, $(q+1+\frac{s+3n}{2})(q+1-\frac{s-3n}{2})=q^2+q+1+3n(q+1)+3n^2$, $(q+1+\frac{s+3n}{2})(q+1-\frac{s+3n}{2})=q^2+1-\frac{-t_{q^2}+3y}{2}$, $(q+1-\frac{s-3n}{2})(q+1+\frac{s-3n}{2})=q^2+1-\frac{-t_{q^2}-3y}{2}$, $(q+1+\frac{s-3n}{2})^2$, $(q+1-\frac{s-3n}{2})^2$, $(q+1+\frac{s+3n}{2})^2$, $(q+1-\frac{s+3n}{2})^2$.

Table 2. Possible Jacobian orders for the curve $\mathcal{C}_6$ over $\mathbb{F}_q$.