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

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

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

Abstract. The use of (hyper)elliptic 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 present several algorithms to obtain so-called *pairing-friendly* genus 2 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 demonstrate this method by constructing several interesting curves with ρ-values around 3. We found for each embedding degree $5 \leqslant k \leqslant 35$ a family of curves of ρ-value between 2.25 and 4.

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 [27] and Koblitz [23]. 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 [24] 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.

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 [30,26] runs in polynomial time in any characteristic (and in small characteristic, there are even faster algorithms based on the so-called p-adic method [28,26]). For genus 2 hyperelliptic curves, if the p-adic method gives efficient point counting algorithms, up to now, no efficient algorithms are known when the characteristic of the underlying finite field is large (though substantial progress has recently been made [18]).

Using basic properties on character sums, Furukawa, Kawazoe and Takahashi [12] 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 [29] 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 $\mathbb{F}_{q^4}$ and its zeta function over $\mathbb{F}_{q^4}$ is the square of the zeta function of the elliptic curve, which is 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 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.* [3,4]). Pairing-based cryptosystem 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 [9]. Unfortunately, there are very few results for constructing pairing-friendly hyperelliptic curves of genus $g \geq 2$ with small ρ-values [14,2].

Galbraith, Pujolas, Ritzenthaler and Smith [15] 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 [10] a general method that produces pairing-friendly (ordinary) genus 2 pairing-friendly hyperelliptic curves with $\rho \simeq 8$ for all embedding degrees k. Kawazoe and Takahashi [22] (see also [21]) 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 [11] 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 [22,21,11] produce Jacobian with $2 < \rho < 4$ only for embedding degrees divisible by 3 or 4.

Our contributions. Satoh's approach to compute the Jacobian order of a hyperelliptic curve of the form $Y^2 = X^5 + aX^3 + bX$ is not explicit. For each candidate, he has to check that the order is not weak for cryptographic use. In [19, § 4], Gaudry and Schost showed that the Jacobian 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 derived 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 (but intricate) polynomial root-finding techniques. This permits to generate efficiently a random hyperelliptic curve, in these two forms, suitable for cryptographic use. These curves enable various improvement to make scalar multiplication in the Jacobian efficient (*e.g.* the Gallant-Lambert-Vanstone algorithm [16], Takashima's algorithm [32] or Gaudry's algorithm [17]). 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 Jacobian.

The lack of explicitness in Satoh's algorithm does not permit the construction of pairing-friendly hyperelliptic curves in a way similar to is known for elliptic curves [7,6]. In particular, Freeman and Satoh were only able to construct such curves for restricted sets of parameters $a, b \in \mathbb{F}_p$ and embedding degrees divisible by 3 or 4. Using our closed formulas for the Jacobian order of hyperelliptic curves $Y^2 = X^5 + aX^3 + bX$ and $Y^2 = X^6 + aX^3 + b$ (with $a, b \in \mathbb{F}_q^*$), 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 [7] (see also [13, Algorithm IX.4]) of constructing individual ordinary pairing-friendly elliptic curves and the other is based on cyclotomic polynomials as originally proposed by Brezing and Weng [6] which generates families of curves while achieving better ρ-values. We adapt both constructions using the elliptic curve complex multiplication method (CM) [1,13] to compute the two elliptic curves to which the Jacobian is isogenous to.

Our approach not only contains the previous constructions by Kawazoe and Takahashi [22] and Freeman and Satoh [11] but also produces new families for ordinary genus 2 hyperelliptic curves. Explicit examples of cryptographically interesting curves are given: in particular we provide constructions using Cocks-Pinch-like method with $k = 7$ and $\rho \simeq 4$ which were not known before. Moreover, we present new complete polynomial families for each embedding degree between 5 and 35 and $2 < \rho < 4$.

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 [29].

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

Satoh showed in [29] that:

- if b is a fourth power then $J_{\mathcal{C}_5}$ splits into two isogenous elliptic curves E_1 and E_2 over $\mathbb{F}_q$;
- if b is a square but not a fourth power then $J_{\mathcal{C}_5}$ splits into $E_1 \times E_2$ defined over $\mathbb{F}_{q^2}$;
- if b is not a square then $\mathcal{C}_5$ splits into $E_1 \times E_2$ defined over $\mathbb{F}_{q^4}$.

The two elliptic curves are defined by

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

with $\gamma = \dfrac{2a-12\sqrt{b}}{a+2\sqrt{b}}$ and $\delta = \dfrac{a+2\sqrt{b}}{64\sqrt[4]{b}^3}$. Using the notation $c = a/\sqrt{b}$ from [11], we find

$$\gamma = \frac{2c-12}{c+2} \text{ and } j(E_1) = j(E_2) = 2^6\frac{(3c-10)^3}{(c+2)^2(c-2)}.$$

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 δ from their equations.

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

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 [30,26]. It remains to compute the Jacobian order from $\mathbb{F}_q[\sqrt[4]{b}]$ downto $\mathbb{F}_q$. We develop explicit formulas using the zeta function properties.

2.2 Computing explicit order using zeta function

Let $Z_{J_{\mathcal{C}_5}}$ denotes the zeta function of the Jacobian $J_{\mathcal{C}_5}$ which satisfies the following properties [29]:

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 $Z_{J_{\mathcal{C}}}(T, \mathbb{F}_{q^n})$ 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: $Z_{J_{\mathcal{C}}}(T, \mathbb{F}_{q^n}) = (T - z_{1,q}^n)(T - z_{2,q}^n)(T - z_{3,q}^n)(T - z_{4,q}^n)$.

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 t_{q^i} denotes the trace of $E_1(\mathbb{F}_{q^i})$ (for $i \in \mathbb{N}$).

With the previous analysis,

– 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 b is a square but not a fourth power, $Z_{J_{\mathcal{C}_5}}(T,\mathbb{F}_{q^2}) = Z_{E_1}(T,\mathbb{F}_{q^2})Z_{E_2}(T,\mathbb{F}_{q^2}) = (T^2 - t_{q^2}T + q^2)^2$ and we have to go down from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$;

– if b is not a square, $Z_{J_{\mathcal{C}_5}}(T,\mathbb{F}_{q^4}) = Z_{E_1}(T,\mathbb{F}_{q^4})Z_{E_2}(T,\mathbb{F}_{q^4}) = (T^2 - t_{q^4}T + q^4)^2$ and we have to recover the zeta function from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q$.

Let us denote

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

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 compute (a_q, b_q) in terms of (a_{q^2}, b_{q^2}) in the second case and (a_q, b_q) from (a_{q^4}, b_{q^4}) in the third case. We begin with

$$\begin{cases} a_{q^2} = z_{1,q}^2 + z_{2,q}^2 + z_{3,q}^2 + z_{4,q}^2 \\ \\ b_{q^2} = 2q^2 + (z_{1,q}^2 + z_{2,q}^2)(z_{3,q}^2 + z_{4,q}^2) \end{cases}$$

and clearly, $(a_q)^2 = a_{q^2} + 2b_q$. Then for b_{q^2} we compute $(b_q)^2$

$$\begin{aligned} (b_q)^2 &= 4q^2 + (z_{1,q} + z_{2,q})^2(z_{3,q} + z_{4,q})^2 + 4q(b_q - 2q) \\ &= 4qb_q - 4q^2 + \left(z_{1,q}^2 + z_{2,q}^2 + 2z_{1,q}z_{2,q}\right)\left(z_{3,q}^2 + z_{4,q}^2 + 2z_{3,q}z_{4,q}\right) \\ &= 4qb_q - 4q^2 + \left(z_{1,q}^2 + z_{2,q}^2 + 2q\right)\left(z_{3,q}^2 + z_{4,q}^2 + 2q\right) \\ &= 4qb_q - 4q^2 + (z_{1,q}^2 + z_{2,q}^2)(z_{3,q}^2 + z_{4,q}^2) + 2q\left(z_{1,q}^2 + z_{2,q}^2 + z_{3,q}^2 + z_{4,q}^2\right) + 4q^2 \\ &= 4qb_q + (b_{q^2} - 2q^2) + 2qa_{q^2} \end{aligned}$$

and obtain

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

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

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

Case 1: b is a square but not a fourth power. We have the following decomposition through isogenies:

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

[3] Satoh [29] used only Equation (1) which resulted in a more intricate polynomial system with degree 16 polynomial equations to solve.

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 $(a_{q^2}, b_{q^2}) = (2t_{q^2}, (t_{q^2})^2 + 2q^2)$ and it remains to solve

$$(a_q)^2 - 2b_q - 2t_{q^2} = 0 \tag{3}$$
$$(b_q)^2 - 4qb_q - 4qt_{q^2} - (t_{q^2})^2 = 0 \tag{4}$$

We easily solve equation (4) into $b_q \in \{4q + t_{q^2}, -t_{q^2}\}$ which gives from equation (3) that $a_q = \pm 2\sqrt{2q + t_{q^2}}$ if $b_q = 4q + t_{q^2}$ and $a_q = 0$ if $b_q = -t_{q^2}$. In the former case, since a_q must be an integer, $2q + t_{q^2}$ must be a square but this only happens if E_1 is actually defined over $\mathbb{F}_q$. In this case, $t_{q^2} = (t_q)^2 - 2q$ which gives $a_q = 2t_q$ and $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q + 1 - t_q)^2$. Therefore b is in fact a fourth power, which is a contradiction. The only solution of the system (3-4) is $(a_q, b_q) = (0, -t_{q^2})$ with $t_{q^2} = -t'_{q^2} = 2q - (t'_q)^2$ and

$$\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - t_{q^2} = (q-1)^2 + (t'_q)^2$$

with t'_q the trace of the elliptic curve $E'_1(\mathbb{F}_q)$.

Case 2: b is not a square. The decomposition into two isogenous elliptic curves is as follows:

$$\begin{array}{ccccc}
 & & E_1(\mathbb{F}_{q^8}) \times E_2(\mathbb{F}_{q^8}) & \overset{\text{isogeny}}{\longleftrightarrow} & E'_1(\mathbb{F}_{q^8}) \times E'_2(\mathbb{F}_{q^8}) \\
 & & \Big| & & \Big| \\
J_{\mathcal{C}_5}(\mathbb{F}_{q^4}) & \overset{\text{isogeny}}{\longleftrightarrow} & E_1(\mathbb{F}_{q^4}) \times E_2(\mathbb{F}_{q^4}) & & E'_1(\mathbb{F}_{q^4}) \times E'_2(\mathbb{F}_{q^4}) \\
 & & \text{whose trace is } t_{q^4} = -t'_{q^4} & & \text{of trace } t'_{q^4} = (t'_{q^2})^2 - 2q^2 \\
\Big| & & & & \Big| \\
J_{\mathcal{C}_5}(\mathbb{F}_{q^2}) & & & & E'_1(\mathbb{F}_{q^2}) \times E'_2(\mathbb{F}_{q^2}) \\
 & & & & \text{of trace } t'_{q^2} \\
\Big| & & & & \\
J_{\mathcal{C}_5}(\mathbb{F}_q) & & & &
\end{array}$$

Hence we start with

$$Z_{J_{\mathcal{C}_5}}(T, \mathbb{F}_{q^4}) = Z_{E_1}(T, \mathbb{F}_{q^4}) Z_{E_2}(T, \mathbb{F}_{q^4}) = (T^2 - t_{q^4}T + q^4)^2,$$

$$a_{q^4} = 2t_{q^4}$$

$$b_{q^4} = (t_{q^4})^2 + 2q^4$$

and the system

$$\begin{cases} (a_{q^2})^2 - 2b_{q^2} - 2t_{q^4} = 0 \\ (b_{q^2})^2 - 4q^2 b_{q^2} - 4q^2 t_{q^4} - (t_{q^4})^2 = 0 \end{cases}$$

We eliminate the solution $(a_{q^2}, b_{q^2}) = \left(\pm 2\sqrt{2q^2 + t_{q^4}}, 4q^2 + t_{q^4}\right)$ with an argument similar to the previous one. Since a_{q^2} must be an integer, if $b_{q^2} = 4q^2 + t_{q^4}$ then $2q^2 + t_{q^4}$ must be a square and $a_{q^2} = 2t_{q^2}$. In this case, E_1 is actually defined over $\mathbb{F}_{q^2}$ which contradicts that b is not a square. Thus we have $(a_{q^2}, b_{q^2}) = (0, -t_{q^4})$. The final polynomial system to solve is the following:

$$(a_q)^2 - 2b_q = 0 \tag{5}$$
$$(b_q)^2 - 4qb_q + 2q^2 + t_{q^4} = 0 \tag{6}$$

Equation (6) 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 (5) that $a_q = \pm\sqrt{2b_q}$. Thus $(a_q, b_q) = \left(\pm\sqrt{2\left(2q - t'_{q^2}\right)}, 2q - t'_{q^2}\right)$ or $(a_q, b_q) = \left(\pm\sqrt{2\left(2q + t'_{q^2}\right)}, 2q + t'_{q^2}\right)$ and either $4q + 2t'_{q^2}$ or $4q - 2t'_{q^2}$ is always a square. Let $n \in \mathbb{Z}$ be such that either $b_q = 2q + t'_{q^2} = 2n^2$ or $b_q = 2q - t'_{q^2} = 2n^2$. We have

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

The following theorem summarizes our results:

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 and let t'_{q^2} be the trace of $E_1'(\mathbb{F}_{q^2})$.*

1. *If b is a fourth power and $\sqrt{-1} \in \mathbb{F}_q$ then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q + 1 - t_q)^2$.*
2. *If b is a fourth power but $\sqrt{-1} \notin \mathbb{F}_q$ then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q + 1 - t_q)(q + 1 + t_q)$.*
3. *If b is a square but not a fourth power then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q-1)^2 + (t'_q)^2$.*
4. *If b is not a square, let $n \in \mathbb{Z}$ be such that either $2q + t'_{q^2} = 2n^2$ or $2q - t'_{q^2} = 2n^2$. Then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 + 1 - 2n(q+1) + 2n^2$.*

The first two cases of Theorem 1 are of no interest in cryptography. The last two cases provide ordinary Jacobian of hyperelliptic curves with explicit order.

Example 1. The numerical example in [29] takes $q = p = 509$ and $\mathcal{C}_5(\mathbb{F}_p) : Y^2 = X^5 + 3X^3 + 7X$ ($b = 7$ is not a square). The curve $E_1(\mathbb{F}_{p^4})$ has a trace $t_{q^4} = 126286$. We deduce that $t'_{q^2} = \pm\sqrt{2p^2 - t_{q^4}} = \pm 626$. As $2p + 626 = 2 \cdot 2 \cdot 3 \cdot 137$ is not 2 times a square, we try $2p - 626 = 2 \cdot 14^2 = 392$, so $n = \pm 14$ and $\#J_{\mathcal{C}_5}(\mathbb{F}_p) \in \{245194, 273754\}$. To finish, we have to exclude one of the two possibilities as in [29] by taking a random point P and test whether $[245194]P = \mathcal{O}$ or $[273754]P = \mathcal{O}$. We conclude that $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = 245194$.

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 [19,11]. 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 [11] 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

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

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

Freeman and Satoh remarked that both elliptic curves admit the same 3-torsion subgroup. With Vélu's formulas adapted to finite fields (e.g. [25, 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.

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

Our analysis gives us the following decompositions:

- If b is a square in $\mathbb{F}_q$ then $\mathcal{C}_6'$, E_c and E_{-c} are defined 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 $(a_q, b_q) = (0, -t_{q^2})$ 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 $\mathbb{F}_{q^2}$.

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.

3.2 Zeta function computation for $J_{\mathcal{C}_6}$

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 $\mathbb{F}_{q^3}$.

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

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 deduce that

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

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 factorizes into two polynomials with integer coefficients over $\mathbb{F}_{q^3}$ 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

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

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

$$z_{1,q}+z_{2,q}=\frac{1}{2}\left[-t_q\pm\sqrt{3(4q^2-t_q^2)}\right] \text{ and } (z_{3,q}+z_{4,q})=\frac{1}{2}\left[-t_q\pm\sqrt{3(4q^2-t_q^2)}\right] .$$

Moreover, $(z_{1,q}+z_{2,q})$ and $(z_{3,q}+z_{4,q})$ are complex conjugates as they are sum of two roots of the genus 2 zeta function. So 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) and

$$a_q=-t_q \text{ and } b_q=2q+\frac{1}{4}\left[t_q^2-3(4q-t_q^2)\right]=t_q^2-q$$

Finally we obtain that if b is a square but not a third power then

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

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

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

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.

Case 1: b is a square but not a third power. The Jacobian splits into the following isogenous elliptic curves:

$$\begin{array}{ccc} J_{\mathcal{C}_6}(\mathbb{F}_{q^3}) & \overset{\text{isogeny}}{\longleftrightarrow} & J_{\mathcal{C}_6'}(\mathbb{F}_{q^3}) \\ | & & | \\ J_{\mathcal{C}_6}(\mathbb{F}_q) & & J_{\mathcal{C}_6'}(\mathbb{F}_q) \overset{\text{isogeny}}{\longleftrightarrow} E_c(\mathbb{F}_q)\times E_{-c}(\mathbb{F}_q) \end{array}$$

Let t_{q^3} denotes the trace of the Frobenius endomorphism of $E_c(\mathbb{F}_{q^3})$ and t_q that of $E(\mathbb{F}_q)$. From zeta function properties for elliptic curves, we know that $t_{q^3}=(t_q)^3-3qt_q$. Moreover, $E_c(\mathbb{F}_q)$ is a subgroup of $E_c(\mathbb{F}_{q^3})$ and as a consequence its order $q+1-t_q$ divides that of $E_c(\mathbb{F}_{q^3})$. We find explicitly that

$$\#E_c(\mathbb{F}_{q^3})=(q+1-t_q)(q^2-q+1+(1+q+t_q)t_q) .$$

As $J_{\mathcal{C}_6}(\mathbb{F}_q)$ is a subgroup of $J_{\mathcal{C}_6}(\mathbb{F}_{q^3})$, $\#J_{\mathcal{C}_6}(\mathbb{F}_q)$ divides $\#J_{\mathcal{C}_6}(\mathbb{F}_{q^3})=(q+1-t_q)^2(q^2-q+1+(1+q+t_q)t_q)^2$ and we find (see computations 3.2 above):

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

Case 2: b is neither a square nor a third power. The decomposition is as follows:

$$\begin{array}{ccc} J_{\mathcal{C}_6}(\mathbb{F}_{q^6}) & \overset{\text{isogeny}}{\longleftrightarrow} & J_{\mathcal{C}_6'}(\mathbb{F}_{q^6}) \\ | & & | \\ J_{\mathcal{C}_6}(\mathbb{F}_{q^2}) & & J_{\mathcal{C}_6'}(\mathbb{F}_{q^2}) \overset{\text{isogeny}}{\longleftrightarrow} E_c(\mathbb{F}_{q^2})\times E_{-c}(\mathbb{F}_{q^2}) \\ | & & \\ J_{\mathcal{C}_6}(\mathbb{F}_q) & & \end{array}$$

We follow the same procedure as previously but over $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$. We have

$$\#J_{\mathcal{C}_6'}(\mathbb{F}_{q^2}) = \#E_c(\mathbb{F}_{q^2}) \cdot \#E_{-c}(\mathbb{F}_{q^2}) = (q^2 + 1 - t_{q^2})^2$$

and $\#J_{\mathcal{C}_6}(\mathbb{F}_{q^6}) = \#J_{\mathcal{C}_6'}(\mathbb{F}_{q^6}) = (q^2+1-t_{q^2})^2(q^4-q^2+1+(q^2+1+t_{q^2})t_{q^2})^2$. Using the zeta function computation (see 3.2 above), we find $\#J_{\mathcal{C}_6'}(\mathbb{F}_{q^2}) = q^4 - q^2 + 1 + (q^2 + 1 + t_{q^2})t_{q^2}$. We have here $(a_{q^2}, b_{q^2}) = (-t_{q^2}, (t_{q^2})^2 - q^2)$. We solve the equations (1) and (2) which give the system

$$\begin{cases} (a_q)^2 - 2b_q + t_{q^2} = 0 \\ (b_q)^2 - 4q(b_q) + 3q^2 + 2qt_{q^2} - (t_{q^2})^2 = 0 \end{cases}$$

We find $b_q \in \{3q - t_{q^2}, q + t_{q^2}\}$. Hence $(a_q, b_q) = (\pm\sqrt{2q + t_{q^2}}, q + t_{q^2})$ or $(\pm\sqrt{3(2q - t_{q^2})}, 3q - t_{q^2})$. We eliminate the first solution which corresponds to the case where b is a square, the two elliptic curves E_c and E_{-c} are actually defined over $\mathbb{F}_q$ of trace t_q and $2q + t_{q^2} = (t_q)^2$ is a square. So $(a_q, b_q) = (\pm\sqrt{3(2q - t_{q^2})}, 3q - t_{q^2})$. 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

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

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 and $\sqrt{-3} \in \mathbb{F}_q$ then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q + 1 - t_q)^2$.*
2. *If b is a sixth power but $\sqrt{-3} \notin \mathbb{F}_q$ then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = (q + 1 - t_q)(q + 1 + t_q)$.*
3. *If b is a square but not a third power then $\#J_{\mathcal{C}_5}(\mathbb{F}_q) = q^2 - q + 1 + (1 + q + t_q)t_q$.*
4. *If b is a third power but not a square then $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2 + 1 - t_{q^2}$.*
5. *If b is neither a cube nor a square, let $n \in \mathbb{Z}$ be such that $2q - t_{q^2} = 3n^2$. Then $\#J_{\mathcal{C}_6}(\mathbb{F}_q) = q^2 + q + 1 + (q + 1 + n)3n$.*

Example 2. 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 $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2+1) = \mathbb{F}_p[i]$, $c = a/\sqrt{b} \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ 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 (few bits) cofactor h. The prime r must be of size twice the security level. 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. But in practice, a such efficient point counting algorithm does not exist for Jacobian, although improvements are in progress [18].

Here $r \sim q^2$ hence the size of q is a few bits more than the security level 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 a suitable elliptic curve.

4 Pairing-Friendly Constructions

We have several constraints for suitable constructions inherent to (hyper)elliptic curves:

1. The embedding degree must be small, of size the ratio between the size of p and the size of the RSA modulus in order to achieve the same security level 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 $6 \leqslant k \leqslant 60$. For a random elliptic curve, k is of size that of 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 $\Delta = t^2 - 4p = -D\gamma^2$ 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. An acceptable solution is $1 \leqslant \rho \leqslant 2$.

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 $\Delta = t^2 - 4p = -D\gamma^2$. The second useful formula is $D\gamma^2 = 4p - t^2 = 4hr - (t-2)^2$, hence $-D\gamma^2 \equiv (t-2)^2 \mod r$.

4.1 Cocks-Pinch Method

We first recall the method proposed by Cocks and Pinch in 2001 to construct pairing-friendly elliptic curves [7] (see also [13, Algorithm IX.4]):

1. Choose a square-free integer D of reasonable size and an embedding degree k to match the security level, knowing that $\rho = 2$.
2. Choose a prime r such that (i.e. take at random 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 $\gamma = (t-2)/\sqrt{-D}$ in $\mathbb{F}_r$.
4. Lift t and y from $\mathbb{F}_r$ to $\mathbb{Z}$ such that $p = \frac{1}{4}(t^2 + D\gamma^2)$ is prime.

We propose to adapt this method to the five Jacobian families of cryptographic interest presented above. First, we know explicitly the Jacobian order. As for 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 γ 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 Theorem 1 and Theorem 2. Let i be a primitive fourth root of unity an j be a primitive third root of unity in $\mathbb{F}_r$.

We consider the hyperelliptic curve model denoted $\mathcal{C}_5$ in Sec. 2.

$\mathcal{C}_5$ with b a square but not a fourth power. $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = p^2-2p+1+(t_p')^2$. Let $\Delta = (t_p')^2-4p = -D\gamma^2$. Hence

$$p = \frac{(t_p')^2 + D\gamma^2}{4} \ .$$

We search an expression for $t_p', \gamma \mod r$ in terms of p then lift t_p', γ from $\mathbb{F}_r$ into $\mathbb{Z}$ and find p. Note that $t_p' \in \mathbb{Z}$ must be even. $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = (p-1)^2 + (t_p')^2 = (p+1)^2 - D\gamma^2$. Because of $p \equiv \zeta_k \mod r$ and with $i = \pm\sqrt{-1} \in \mathbb{F}_r$,

$$t_p' \equiv i(\zeta_k - 1) \mod r \text{ and } \gamma \equiv \pm(\zeta_k + 1)/\sqrt{D} \mod r \ .$$

This gives the following variant of Cocks-Pinch method.

1. Choose a square-free integer D of reasonable size and an embedding degree k to match the security level, knowing that $\rho = 4$.
2. Choose a prime r of size twice the security level such that $i, \sqrt{D}, \zeta_k \in \mathbb{F}_r$.
3. Let $t_p' = i(\zeta_k - 1)$ and $\gamma \equiv \pm(\zeta_k + 1)/\sqrt{D} \in \mathbb{F}_r$.
4. Lift t_p' and γ from $\mathbb{F}_r$ to $\mathbb{Z}$ such that t_p' is even and $p = \frac{(t_p')^2+D\gamma^2}{4}$ is prime and verifies $p \equiv 1 \mod 4$.
5. Run the CM method to find the j-invariant of an elliptic curve $E_1'(\mathbb{F}_p)$ of trace t_p' and $\Delta = -D\gamma^2$.
6. Solve $j(E_1') = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}$ in $\mathbb{F}_p^*$ (this equation has no solution when t_p' is odd).
7. Choose $a, b \in \mathbb{F}_p$ such that a/c is not a square and $b = (a/c)^2$. The property $p \equiv 1 \mod 4$ is required otherwise b would be a square *and* a fourth power.
8. The Jacobian of the curve $\mathcal{C}_5 : Y^2 = X^5 + aX^3 + bX$ has a subgroup of order r and embedding degree k with respect to r.

Remark 1. In [11], the two authors note that the equation $j(E_1') = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}$ has no solution in $\mathbb{F}_p$ half the time. Indeed, the curves E_1 and E_2 have a non-trivial 2-torsion subgroup, hence when the trace is odd there is no solution. We always found a solution when the trace was chosen even.

Example 3. As a proof of concept, we construct a hyperelliptic curve with embedding degree $k = 7$ (which is not possible to achieve using Freeman-Satoh's method). Using [31] and `cm.cpp` compiled for Linux 64 bits, we picked $D = 12417$ at random and find the curve $\mathcal{C}_5(\mathbb{F}_p) : Y^2 = X^5 + aX^3 + bX$ with $a = 1$, $b = c^2$ and c is not a square in $\mathbb{F}_p$ whose Jacobian is suitable for pairing-based applications at 112 bits of security (its order r is of 219 bits). We achieve $\rho = 4.07$:

$c =$ `0x4930a06a481c83fcc496f5e275348e6451a9ac35af3cc3812bc4ac52`
`1f9f1d317d195a884b125a7ad076da1e2052110127e9b94c8db49c0`,
$r =$ `0x61570f6615aca5f4a0bb06c2583021c15a43814eb11ea9314366771d`,
$p =$ `0x3d7e62eear7d7c72ec306e7b6df3837873e46f16fda40f385969b976`
`b61b33dac1d38891061a2b9f7457563fe46d48d51ae5543a27861375`,
$t_p' =$ `0xf0c68c22caf4015873f9941e3b3769032093401a623c`,
$\gamma =$ `0x23fa65f148f2cba3797e5914ad17b8ac25418b5ea0b81670b46d132`,
$j_{E_1} =$ `0x17a793149158ec402527e6aa7d2598c1667ac20719fd08b2be00d8c7`
`7dfe4ce91d99817b4e2a17e2b1f0e8949c2f83459b7017af55b5687b`.

$\mathcal{C}_5$ with b not a square. $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = p^2+1+2n^2-2n(1+p) = (p-n)^2+(n-1)^2$ 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 $D\gamma^2 = 2p - n^2$ thus $\Delta = -D(2ny)^2$ 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 $\gamma^2 \equiv (2p-n^2)/D \mod r$ with $p \equiv \zeta_k \mod r$ and we find that

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

The trace will be even by construction as $t'_{p^2} = \pm(2p - 2n^2)$ and there is not any condition about p. To find the coefficients of the curve $\mathcal{C}_5(\mathbb{F}_p)$, do the following.

1. 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 $\Delta = -D\gamma^2$. The above cited program `cm.cpp` is not convenient for that.
2. Solve $j(E'_1) = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}$ in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$.
3. 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 $\mathbb{F}_p$).
4. 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.

Now we consider the hyperelliptic curve model denoted $\mathcal{C}_6$ in Sec. 3.

$\mathcal{C}_6$ with b a cube but not a square. $\#J_{\mathcal{C}_6}(\mathbb{F}_p) = p^2 + 1 - t_{p^2}$. This case is close to the elliptic curve case. Actually, this is the same construction as finding a pairing-friendly elliptic curve over a prime power field $\mathbb{F}_{p^2}$. But in practice the methods to find such pairing-friendly elliptic curves fail over $\mathbb{F}_{p^2}$. Indeed, the expression for p is $p^2 = \frac{1}{4}((t'_{p^2})^2 + D\gamma^2)$ 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. $\#J_{\mathcal{C}_6}(\mathbb{F}_p) = p^2 - p + 1 + (1+p)t_p + (t_p)^2$. The discriminant of the elliptic curve is $\Delta = (t_p)^2 - 4p = -D\gamma^2$. Once more

$$p = \frac{t_1^2 + Dy^2}{4} \ .$$

Solving $\#J_{\mathcal{C}_6}(\mathbb{F}_p) \equiv 0 \mod r$ we find with $j = \frac{-1+i\sqrt{3}}{2}$ that $t_p = j^2 p + j$ or $t_p = jp + j^2$. Thus let j be one of the two primitive third root of unity (the other one is then j^2).

$$t_p \equiv j\zeta_k + j^2 \mod r \text{ and } \gamma \equiv \pm(j\zeta_k - j^2)/\sqrt{-D} \mod r \ .$$

There is the Cocks-Pinch variant.

1. Choose a square-free integer D of reasonable size and an embedding degree k to match the security level, knowing that $\rho = 4$.
2. Choose a prime r of size twice the security level such that a third root of unity j, $\sqrt{-D}$ and $\zeta_k \in \mathbb{F}_r$ that is $r \equiv 1 \mod 3$, $r \equiv 1 \mod k$ and $-D$ is a square in $\mathbb{F}_r$.
3. Let $t_p = j\zeta_k + j^2$ and $\gamma = \pm(j\zeta_k - j^2)/\sqrt{-D} \in \mathbb{F}_r$.

4. Lift t_p and γ from $\mathbb{F}_r$ to $\mathbb{Z}$ such that $p = \frac{1}{4}\left((t_p)^2 + D\gamma^2\right)$ is prime, $p \equiv 1 \mod 3$ and $p+1-t_p \equiv 0 \mod 3$.
5. Run the CM method to find the j-invariant of an elliptic curve $E_c(\mathbb{F}_p)$ of trace t_p and $\Delta = -D\gamma^2$.
6. Solve $j(E_c) = 2^8 3^3 \frac{(2c-5)^3}{(c-2)(c+2)^3}$ in $\mathbb{F}_p^*$ (this equation has no solution when $p+1 \pm t_p \not\equiv 0 \mod 3$).
7. Choose $a, b \in \mathbb{F}_p$ such that a/c is not a cube and $b = (a/c)^2$. Hence b is a square but not a cube.
8. The Jacobian of the curve $\mathcal{C}_6 : Y^2 = X^6 + aX^3 + b$ has a subgroup of order r and embedding degree k with respect to r.

Remark 2. 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 [11, § 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 finish to run the algorithm above. When $p \equiv 1 \mod 3$ and $t_p \equiv 1 \mod 3$, we can still construct the coefficients of $\mathcal{C}_6(\mathbb{F}_p)$. But at the end, we have to choose not $\mathcal{C}_6$ itself but its quadratic twist.

Example 4. We construct a hyperelliptic curve with embedding degree $k = 10$; we picked $D = 46478$ at random and find the curve $\mathcal{C}_6(\mathbb{F}_p) : Y^2 = X^6 + aX^6 + b$ with $a = 1$, $b = c^2$ and c is not a cube in $\mathbb{F}_p$ whose Jacobian is suitable for pairing-based applications at 128 bits of security (its order r is of 256 bits). We achieve $\rho = 4.1$:

$$
\begin{aligned}
c &= \texttt{0xa213648a9bee55ddc91046d1a82a20fab012fb72aad04c94200a1e311ed28212} \\
&\quad \texttt{8196b05372306d5276a158346b2064be8edf83c0dbd6788463326abe18e7be28ca4} \\
r &= \texttt{0xbfdf1060c31bd5d035574501de17ccf5470cce84b2f3cb8b6aae4bf4a519027b} \\
p &= \texttt{0x100cdaf542a76552561ba3e34b58bb5902cdb150afc01cf25e7ed5c72b6605da} \\
&\quad \texttt{fcd86c58a1d67c7ad1ac51d74b6adc33422b8376000ee4891380ee49f3e726afc0b9} \\
j &= \texttt{0x350356e16aa875e1ab51dd4206ee5375fd6a1f2bfedab7bbee9ffae13c53320d} \\
&\quad \texttt{08cd77d9e0f68dec49e1b97b33ba3249a93010374c2ab17a4aea3544313bcf76058}.
\end{aligned}
$$

$\mathcal{C}_6$ 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 verify $2p - t_{p^2} = 3n^2$. Let $2p + t_{p^2} (= 4p - 3n^2) = D\gamma^2$. Hence

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

Solving $p^2 + p + 1 - (p+1)3n + 3n^2 \equiv 0 \mod r$ gives $p = (1-j^2)n + j^2$ or $p = (1-j)n + j$ with j once more a primitive third root of unity. As $\gamma^2 = (4p - 3n^2)/D \mod r$ and with $p \equiv \zeta_k \mod r$ we find

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

The last version of the Cocks-Pinch method is as follows.

1. Choose a square-free integer D of reasonable size and an embedding degree k to match the security level, knowing that $\rho = 4$.
2. Choose a prime r of size twice the security level such that a third root of unity j, $\sqrt{D}$ and $\zeta_k \in \mathbb{F}_r$.
3. Let $n = (\zeta_k - j)/(1 - j)$ and $\gamma = \pm(j\zeta_k + j^2)/\sqrt{D} \in \mathbb{F}_r$.
4. Lift n and γ from $\mathbb{F}_r$ to $\mathbb{Z}$ such that $p = \frac{1}{4}\left(3n^2 + D\gamma^2\right)$ is prime and $p^2 + 1 - t_{p^2} \equiv 0 \mod 3$, that is $t_{p^2} = 2p - 3n^2 \equiv 2 \mod 3$, *i.e.* $p \equiv 1 \mod 3$.
5. 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 $\Delta = -D\gamma^2$.
6. Solve $j(E_c) = 2^8 3^3 \frac{(2c-5)^3}{(c-2)(c+2)^3}$ in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$.
7. 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. The Jacobian of the curve $\mathcal{C}_6 : Y^2 = X^6 + aX^3 + b$ has a subgroup of order r and embedding degree k with respect to r.

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 $5 \leqslant k \leqslant 35$. We ran a search (with Magma [5]) over different cyclotomic fields and with a change of basis as in [20] and [21]. We obtained complete families with $\rho \simeq 3$. An asterisk denotes a construction already mentioned in previous papers [22,11].

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

5 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. 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 better ρ-value using Weil restriction of order 8 or 12. It is worth noting that it is also possible to adapt the Dupont-Enge -Morain technique [8] to our setting but unfortunately it provides curves with $\rho \simeq 4$. It remains open to construct 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.

Table 1. Best ρ-values obtained for $5 \leqslant k \leqslant 35$.

k	ρ	Construction	D	r
5	3.5	$\mathcal{C}_5$, 2nd alg.	5	$\Phi_{20}(v)$
	3.5	$\mathcal{C}_6$, 1st alg.	15	$\Phi_{15}(v)$
6	3	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{12}(v)$
	3^*	$\mathcal{C}_6$, 1st alg.	7	$\Phi_{42}(v)$
9	2.67^*	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{36}(v)$
10	3	$\mathcal{C}_5$, 1st alg.	5	$\Phi_{20}(v)$
	3	$\mathcal{C}_5$, 2nd alg.	2,10	$\Phi_{40}(v)$
11	3.2	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{88}(v)$
12	3	$\mathcal{C}_5$, 1st alg.	3	$\Phi_{12}(v)$
13	3	$\mathcal{C}_6$, 1st alg.	3	$\Phi_{156}(v)$
14	3.33	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{56}(v)$
	3	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{84}(v)$
15	3.5	$\mathcal{C}_6$, 1st alg.	1,5	$\Phi_{60}(v)$
			2,6	$\Phi_{120}(v)$
			15	$\Phi_{15}(v)$
16	3.5	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{16}(v)$
18	3.33	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{72}(v)$
	3.33^*	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{36}(v)$
20	3.5	$\mathcal{C}_5$, 1st alg.	5	$\Phi_{20}(v)$
	3.5	$\mathcal{C}_5$, 2nd alg.	2,10	$\Phi_{40}(v)$
21	2.67^*	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{84}(v)$
	3	$\mathcal{C}_6$, 1st alg.	7	$\Phi_{21}(v)$
22	2.8	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{88}(v)$
	3	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{132}(v)$
24	3^*	$\mathcal{C}_5$, 1st alg.	2	$\Phi_{24}(v)$
25	3.2	$\mathcal{C}_5$, 1st alg.	5	$\Phi_{100}(v)$
26	2.33	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{104}(v)$
	2.5	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{156}(v)$
27	2.22^*	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{108}(v)$
28	3	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{56}(v)$
	3.33	$\mathcal{C}_6$, 2nd alg.	7	$\Phi_{84}(v)$
30	3.5	$\mathcal{C}_6$, 1st alg.	1,5	$\Phi_{60}(v)$
			15	$\Phi_{30}(v)$
32	3.312	$\mathcal{C}_5$, 1st alg.	5	$\Phi_{160}(v)$
	3.25	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{32}(v)$
33	2.8	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{132}(v)$
34	2.25	$\mathcal{C}_5$, 2nd alg.	2	$\Phi_{136}(v)$
	2.625	$\mathcal{C}_6$, 1st alg.	1	$\Phi_{204}(v)$
35	3	$\mathcal{C}_5$, 2nd alg.	10	$\Phi_{280}(v)$

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. D. Boneh & M. K. Franklin – "Identity-based encryption from the Weil pairing", *SIAM J. Comput.* **32** (2003), no. 3, p. 586–615.
4. D. Boneh, B. Lynn & H. Shacham – "Short signatures from the Weil pairing", *J. Cryptology* **17** (2004), no. 4, p. 297–319.
5. 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).
6. F. Brezing & A. Weng – "Elliptic curves suitable for pairing based cryptography", *Des. Codes Cryptography* **37** (2005), no. 1, p. 133–141.
7. C. Cocks & R. G. Pinch. – "ID-based cryptosystems based on the Weil pairing", 2001, Unpublished manuscript.
8. 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.
9. D. Freeman, M. Scott & E. Teske – "A taxonomy of pairing-friendly elliptic curves", *J. Cryptology* **23** (2010), no. 2, p. 224–280.
10. 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.
11. D. M. Freeman & T. Satoh – "Constructing pairing-friendly hyperelliptic curves using weil restriction", *J. Number Theory* **131** (2011), no. 5, p. 959–983.
12. 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.
13. 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.
14. 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.

15. 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.
16. 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.
17. P. Gaudry – "Fast genus 2 arithmetic based on theta functions", *J. Math. Crypt.* **1** (2007), no. 3, p. 243–265.
18. 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., Springer, 2011, To appear.
19. 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.
20. 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.
21. 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.
22. 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.
23. N. Koblitz – "Elliptic curve cryptosystems", *Math. Comp.* **48** (1987), no. 177, p. 203–209.
24. — , "Hyperelliptic cryptosystems", *J. Cryptology* **1** (1989), p. 139–150.
25. R. Lercier – "Algorithmique des courbes elliptiques dans les corps finis", Thèse, École Polytechnique, 1997.
26. 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.
27. 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.
28. 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.
29. — , "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.
30. R. Schoof – "Elliptic curves over finite fields and the computation of square roots mod p", *Math. Comput.* **44** (1998), p. 483–494.
31. M. Scott – "MIRACL library", 2011, Latest Version - V5.5.4 Last updated August 2011.
32. 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 Additional Examples

In this appendix, we provide additional examples of pairing-friendly $\mathcal{C}_5$ and $\mathcal{C}_6$ curve families with $2 < \rho < 4$.

A.1 With $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = (p-1)^2 + (t_p')^2$.

Example 5 ($k = 10, D = 5, \rho = 3$).

$$
\begin{aligned}
r &= \Phi_{20}(v) = v^8 - v^6 + v^4 - v^2 + 1 \\
t_p' &= -v^5 + v^3 \\
\gamma &= \tfrac{1}{5}\left(-3v^6 + v^4 + v^2 + 2\right) \\
p &= \tfrac{1}{20}\left(9v^{12} - v^{10} - 15v^8 - 5v^6 + 5v^4 + 4v^2 + 4\right) \\
v &\equiv 2, 8, 12, 18 \mod 20
\end{aligned}
$$

Example 6 ($k = 12, D = 3, \rho = 3$).

$$r = \Phi_{12}(v) = v^4 - v^2 + 1$$
$$t_p' = v^3 + v^2$$
$$\gamma = \tfrac{1}{3}\left(v^3 - v^2 - 2v + 2\right)$$
$$p = \tfrac{1}{3}\left(v^6 + v^5 + 2v^3 - 2v + 1\right)$$
$$v \equiv 1 \mod 12$$

Example 7 ($k = 20, D = 5, \rho = 3.5$).

$$r = \Phi_{20}(v) = v^8 - v^6 + v^4 - v^2 + 1$$
$$t_p' = -v^6 + -v^5$$
$$\gamma = \tfrac{1}{5}\left(2v^7 - 2v^6 - 2v^5 + 2v^4 - v + 1\right)$$
$$p = \tfrac{1}{20}\left(4v^{14} - 8v^{13} + v^{12} + 26v^{11} + v^{10} - 8v^9 + 8v^7 - 8v^5 + 4v^4 + v^2 - 2v + 1\right)$$
$$v \equiv 1, 3, 7, 11, 13, 17 \mod 20$$
$$r = \Phi_{20}(v) = v^8 - v^6 + v^4 - v^2 + 1$$
$$t_p' = v^6 - v^5$$
$$\gamma = \tfrac{1}{5}\left(-2v^7 - 2v^6 + 2v^5 + 2v^4 + v + 1\right)$$
$$p = \tfrac{1}{20}\left(4v^{14} + 8v^{13} + v^{12} - 26v^{11} + v^{10} + 8v^9 - 8v^7 + 8v^5 + 4v^4 + v^2 + 2v + 1\right)$$
$$v \equiv 3, 7, 9, 13, 17, 19 \mod 20$$

Example 8 ($k = 24, D = 2, \rho = 3$).

$$r = \Phi_{24}(v) = v^8 - v^4 + 1$$
$$t_p' = -v^6 + v^5$$
$$\gamma = \tfrac{1}{2}\left(v^5 + v^4 - v^3 - v^2 - v - 1\right)$$
$$p = \tfrac{1}{8}\left(2v^{12} - 4v^{11} + 3v^{10} + 2v^9 - v^8 - 4v^7 - 3v^6 - 2v^5 + v^4 + 4v^3 + 3v^2 + 2v + 1\right)$$
$$v \equiv 7 \mod 8$$
$$r = \Phi_{24}(v) = v^8 - v^4 + 1$$
$$t_p' = -v^6 - v^5$$
$$\gamma = \tfrac{1}{2}\left(v^5 - v^4 - v^3 + v^2 - v + 1\right)$$
$$p = \tfrac{1}{8}\left(2v^{12} + 4v^{11} + 3v^{10} - 2v^9 - v^8 + 4v^7 - 3v^6 + 2v^5 + v^4 - 4v^3 + 3v^2 - 2v + 1\right)$$
$$v \equiv 1 \mod 8$$

Example 9 ($k = 25, D = 5, \rho = 3.2$).

$$r = \Phi_{100}(v) = v^{40} - v^{30} + v^{20} - v^{10} + 1$$
$$t_p' = v^{27} + v^{25}$$
$$\gamma = \tfrac{1}{5}\left(2v^{32} - 2v^{30} - 2v^{22} + 2v^{20} - v^2 + 1\right)$$
$$p = \tfrac{1}{20}\left(4v^{64} - 8v^{62} + 4v^{60} - 3v^{54} + 26v^{52} - 3v^{50} + 4v^{44} - 8v^{42} + 4v^{40} - 4v^{34}\right.$$
$$\left. + 8v^{32} - 4v^{30} + 4v^{24} - 8v^{22} + 4v^{20} + v^4 - 2v^2 + 1\right)$$
$$v \equiv 1, 9, 11, 19 \mod 20$$

Example 10 ($k = 32, D = 5, \rho = 3.312$).

$$r = \Phi_{160}(v) = v^{64} - v^{48} + v^{32} - v^{16} + 1$$
$$t_p' = v^{45} + v^{40}$$
$$\gamma = \tfrac{1}{5}\left(2v^{53} - 2v^{48} - 2v^{37} + 2v^{32} - v^5 + 1\right)$$
$$p = \tfrac{1}{20}\left(4v^{106} - 8v^{101} + 4v^{96} - 3v^{90} + 26v^{85} - 3v^{80} + 4v^{74} - 8v^{69} + 4v^{64} - 4v^{58} + 8v^{53}\right.$$
$$\left. - 4v^{48} + 4v^{42} - 8v^{37} + 4v^{32} + v^{10} - 2v^5 + 1\right)$$
$$v \equiv 1, 11 \mod 20$$

$$
\begin{aligned}
r &= \Phi_{160}(v) = v^{64} - v^{48} + v^{32} - v^{16} + 1 \\
t_p' &= -v^{45} + v^{40} \\
\gamma &= \tfrac{1}{5}\left(-2v^{53} - 2v^{48} + 2v^{37} + 2v^{32} + v^5 + 1\right) \\
p &= \tfrac{1}{20}\left(4v^{106} + 8v^{101} + 4v^{96} - 3v^{90} - 26v^{85} - 3v^{80} + 4v^{74} + 8v^{69} + 4v^{64} - 4v^{58} - 8v^{53}\right. \\
&\quad \left. -4v^{48} + 4v^{42} + 8v^{37} + 4v^{32} + v^{10} + 2v^5 + 1\right) \\
v &\equiv 9, 19 \mod 20
\end{aligned}
$$

A.2 With $\#J_{\mathcal{C}_5}(\mathbb{F}_p) = p^2 + 1 - 2n(p + 1 - n)$.

Example 11 ($k = 5, D = 5, \rho = 3.5$).

$$
\begin{aligned}
r &= \Phi_{20}(v) = v^8 - v^6 + v^4 - v^2 + 1 \\
n &= \tfrac{1}{2}\left(-v^7 - v^5 - v^2 + 1\right) \\
\gamma &= \tfrac{1}{10}\left(-3v^7 + 2v^6 + v^5 - 4v^3 - v^2 + 2v + 1\right) \\
t_{p^2}' &= \tfrac{1}{5}\left(v^{14} - 3v^{13} - 3v^{12} + v^{11} + 5v^{10} - 5v^9 - 6v^8 + 6v^6 + 5v^5 - 5v^4 - 3v^3 + 3v^2 + v - 1\right) \\
p &= \tfrac{1}{20}\left(7v^{14} - 6v^{13} + 4v^{12} + 2v^{11} + 15v^{10} - 12v^8 + 12v^6 - 5v^4 - 6v^3 - 4v^2 + 2v + 3\right) \\
v &\equiv 3, 7, 13, 17 \mod 20 \\
r &= \Phi_{20}(v) = v^8 - v^6 + v^4 - v^2 + 1 \\
n &= \tfrac{1}{2}\left(v^7 + v^5 - v^2 + 1\right) \\
\gamma &= \tfrac{1}{10}\left(3v^7 + 2v^6 - v^5 + 4v^3 - v^2 - 2v + 1\right) \\
t_{p^2}' &= \tfrac{1}{5}\left(v^{14} + 3v^{13} - 3v^{12} - v^{11} + 5v^{10} + 5v^9 - 6v^8 + 6v^6 - 5v^5 - 5v^4 + 3v^3 + 3v^2 - v - 1\right) \\
p &= \tfrac{1}{20}\left(7v^{14} + 6v^{13} + 4v^{12} - 2v^{11} + 15v^{10} - 12v^8 + 12v^6 - 5v^4 + 6v^3 - 4v^2 - 2v + 3\right) \\
v &\equiv 3, 7, 13, 17 \mod 20
\end{aligned}
$$

Example 12 ($k = 10, D = 2, \rho = 3$).

$$
\begin{aligned}
r &= \Phi_{40}(v) = v^{16} - v^{12} + v^8 - v^4 + 1 \\
n &= \tfrac{1}{2}\left(v^{12} - v^{10} - v^2 + 1\right) \\
\gamma &= \tfrac{1}{2}\left(v^7 + v^5\right) \\
t_{p^2}' &= \tfrac{1}{4}\left(-v^{24} + 2v^{22} - v^{20} + 4v^{14} + 4v^{10} - v^4 + 2v^2 - 1\right) \\
p &= \tfrac{1}{8}\left(v^{24} - 2v^{22} + v^{20} + 8v^{12} + v^4 - 2v^2 + 1\right) \\
v &\equiv 1 \mod 2
\end{aligned}
$$

Example 13 ($k = 10, D = 10, \rho = 3$).

$$
\begin{aligned}
r &= \Phi_{40}(v) = v^{16} - v^{12} + v^8 - v^4 + 1 \\
n &= \tfrac{1}{2}\left(v^{12} - v^{10} - v^2 + 1\right) \\
\gamma &= \tfrac{1}{10}\left(2v^{11} + 2v^9 - v^7 - v^5 + 2v^3 + 2v\right) \\
t_{p^2}' &= \tfrac{1}{20}\left(-5v^{24} + 18v^{22} + 11v^{20} - 16v^{16} + 20v^{14} + 16v^{12} + 20v^{10} - 16v^8 + 11v^4 + 18v^2 - 5\right) \\
p &= \tfrac{1}{40}\left(5v^{24} - 2v^{22} + 21v^{20} - 16v^{16} + 56v^{12} - 16v^8 + 21v^4 - 2v^2 + 5\right) \\
v &\equiv 3, 5, 7 \mod 10
\end{aligned}
$$

Example 14 ($k = 11, D = 2, \rho = 3.2$).

$$
\begin{aligned}
r &= \Phi_{88}(v) = v^{40} - v^{36} + v^{32} - v^{28} + v^{24} - v^{20} + v^{16} - v^{12} + v^8 - v^4 + 1 \\
n &= \tfrac{1}{2}\left(v^{32} - v^{22} - v^{10} + 1\right) \\
\gamma &= \tfrac{1}{2}\left(v^{21} + v^{11}\right) \\
t_{p^2}' &= \tfrac{1}{4}\left(-v^{64} + 2v^{54} - v^{44} + 4v^{42} + 4v^{22} - v^{20} + 2v^{10} - 1\right) \\
p &= \tfrac{1}{8}\left(v^{64} - 2v^{54} + v^{44} + 8v^{32} + v^{20} - 2v^{10} + 1\right) \\
v &\equiv 1 \mod 2
\end{aligned}
$$

Example 15 ($k = 14, D = 2, \rho = 3.33$).

$$
\begin{aligned}
r &= \Phi_{56}(v) = v^{24} - v^{20} + v^{16} - v^{12} + v^8 - v^4 + 1 \\
n &= \tfrac{1}{2}\left(v^{20} - v^{14} - v^6 + 1\right) \\
\gamma &= \tfrac{1}{2}\left(v^{13} + v^7\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(-v^{40} + 2v^{34} - v^{28} + 4v^{26} + 4v^{14} - v^{12} + 2v^6 - 1\right) \\
p &= \tfrac{1}{8}\left(v^{40} - 2v^{34} + v^{28} + 8v^{20} + v^{12} - 2v^6 + 1\right) \\
v &\equiv 1 \mod 2
\end{aligned}
$$

Example 16 ($k = 16, D = 2, \rho = 3.5$).

$$
\begin{aligned}
r &= \Phi_{16}(v) = v^8 + 1 \\
n &= \tfrac{1}{2}\left(-v^5 + v^4 - v + 1\right) \\
\gamma &= \tfrac{1}{2}\left(-v^7 - v^6\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(2v^{14} + 4v^{13} + 2v^{12} - v^{10} + 2v^9 - v^8 - 2v^6 + 4v^5 - 2v^4 - v^2 + 2v - 1\right) \\
p &= \tfrac{1}{8}\left(2v^{14} + 4v^{13} + 2v^{12} + v^{10} - 2v^9 + v^8 + 2v^6 - 4v^5 + 2v^4 + v^2 - 2v + 1\right) \\
v &\equiv 1, 5 \mod 8 \\
r &= \Phi_{16}(v) = v^8 + 1 \\
n &= \tfrac{1}{2}\left(v^5 + v^4 + v + 1\right) \\
\gamma &= \tfrac{1}{2}\left(v^7 - v^6\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(2v^{14} - 4v^{13} + 2v^{12} - v^{10} - 2v^9 - v^8 - 2v^6 - 4v^5 - 2v^4 - v^2 - 2v - 1\right) \\
p &= \tfrac{1}{8}\left(2v^{14} - 4v^{13} + 2v^{12} + v^{10} + 2v^9 + v^8 + 2v^6 + 4v^5 + 2v^4 + v^2 + 2v + 1\right) \\
v &\equiv 3 \mod 4
\end{aligned}
$$

Example 17 ($k = 18, D = 2, \rho = 3.33$).

$$
\begin{aligned}
r &= \Phi_{72}(v) = v^{24} - v^{12} + 1 \\
n &= \tfrac{1}{2}\left(v^{20} - v^{18} - v^2 + 1\right) \\
\gamma &= \tfrac{1}{2}\left(v^{11} + v^9\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(-v^{40} + 2v^{38} - v^{36} + 4v^{22} + 4v^{18} - v^4 + 2v^2 - 1\right) \\
p &= \tfrac{1}{8}\left(v^{40} - 2v^{38} + v^{36} + 8v^{20} + v^4 - 2v^2 + 1\right) \\
v &\equiv 1 \mod 2
\end{aligned}
$$

Example 18 ($k = 20, D = 2, \rho = 3.5$).

$$
\begin{aligned}
r &= \Phi_{40}(v) = v^{16} - v^{12} + v^8 - v^4 + 1 \\
n &= \tfrac{1}{2}\left(v^{14} - v^{10} - v^4 + 1\right) \\
\gamma &= \tfrac{1}{2}\left(v^9 + v^5\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(-v^{28} + 2v^{24} - v^{20} + 4v^{18} + 4v^{10} - v^8 + 2v^4 - 1\right) \\
p &= \tfrac{1}{8}\left(v^{28} - 2v^{24} + v^{20} + 8v^{14} + v^8 - 2v^4 + 1\right) \\
v &\equiv 1 \mod 2
\end{aligned}
$$

Example 19 ($k = 20, D = 10, \rho = 3.5$).

$$
\begin{aligned}
r &= \Phi_{40}(v) = v^{16} - v^{12} + v^8 - v^4 + 1 \\
n &= \tfrac{1}{2}\left(v^{14} - v^{10} - v^4 + 1\right) \\
\gamma &= \tfrac{1}{10}\left(2v^{13} + v^9 + 2v^5 + 2v\right) \\
t'_{p^2} &= \tfrac{1}{20}\left(-5v^{28} + 8v^{26} + 10v^{24} + 8v^{22} - 5v^{20} + 20v^{18} + 20v^{10} - 5v^8 + 8v^6 + 10v^4 + 8v^2 - 5\right) \\
p &= \tfrac{1}{40}\left(5v^{28} + 8v^{26} - 10v^{24} + 8v^{22} + 5v^{20} + 40v^{14} + 5v^8 + 8v^6 - 10v^4 + 8v^2 + 5\right) \\
v &\equiv 1 \mod 2
\end{aligned}
$$

Example 20 ($k = 22, D = 2, \rho = 2.8$).

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

Example 21 ($k = 26, D = 2, \rho = 2.33$).

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

Example 22 ($k = 28, D = 2, \rho = 3$).

$$
\begin{aligned}
r &= \Phi_{56}(v) = v^{24} - v^{20} + v^{16} - v^{12} + v^8 - v^4 + 1 \\
n &= \tfrac{1}{2}\left(v^{18} - v^{14} - v^4 + 1\right) \\
\gamma &= \tfrac{1}{2}\left(-v^{11} - v^7\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(-v^{36} + 2v^{32} - v^{28} + 4v^{22} + 4v^{14} - v^8 + 2v^4 - 1\right) \\
p &= \tfrac{1}{8}\left(v^{36} - 2v^{32} + v^{28} + 8v^{18} + v^8 - 2v^4 + 1\right) \\
v &\equiv 1, 3, 5, 7 \mod 8
\end{aligned}
$$

Example 23 ($k = 32, D = 2, \rho = 3.25$).

$$
\begin{aligned}
r &= \Phi_{32}(v) = v^{16} + 1 \\
n &= \tfrac{1}{2}\left(-v^9 + v^8 - v + 1\right) \\
\gamma &= \tfrac{1}{2}\left(-v^{13} - v^{12}\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(2v^{26} + 4v^{25} + 2v^{24} - v^{18} + 2v^{17} - v^{16} - 2v^{10} + 4v^9 - 2v^8 - v^2 + 2v - 1\right) \\
p &= \tfrac{1}{8}\left(2v^{26} + 4v^{25} + 2v^{24} + v^{18} - 2v^{17} + v^{16} + 2v^{10} - 4v^9 + 2v^8 + v^2 - 2v + 1\right) \\
v &\equiv 1, 5 \mod 8 \\
r &= \Phi_{32}(v) = v^{16} + 1 \\
n &= \tfrac{1}{2}\left(v^9 + v^8 + v + 1\right) \\
\gamma &= \tfrac{1}{2}\left(v^{13} - v^{12}\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(2v^{26} - 4v^{25} + 2v^{24} - v^{18} - 2v^{17} - v^{16} - 2v^{10} - 4v^9 - 2v^8 - v^2 - 2v - 1\right) \\
p &= \tfrac{1}{8}\left(2v^{26} - 4v^{25} + 2v^{24} + v^{18} + 2v^{17} + v^{16} + 2v^{10} + 4v^9 + 2v^8 + v^2 + 2v + 1\right) \\
v &\equiv 3, 7 \mod 8
\end{aligned}
$$

Example 24 ($k = 34, D = 2, \rho = 2.25$).

$$
\begin{aligned}
r &= \Phi_{136}(v) = v^{64} - v^{60} + v^{56} - v^{52} + v^{48} - v^{44} + v^{40} - v^{36} + v^{32} - v^{28} + v^{24} - v^{20} + v^{16} \\
&\quad - v^{12} + v^8 - v^4 + 1 \\
n &= \tfrac{1}{2}\left(v^{36} - v^{34} - v^2 + 1\right) \\
\gamma &= \tfrac{1}{2}\left(-v^{19} - v^{17}\right) \\
t'_{p^2} &= \tfrac{1}{4}\left(-v^{72} + 2v^{70} - v^{68} + 4v^{38} + 4v^{34} - v^4 + 2v^2 - 1\right) \\
p &= \tfrac{1}{8}\left(v^{72} - 2v^{70} + v^{68} + 8v^{36} + v^4 - 2v^2 + 1\right) \\
v &\equiv 1, 3, 5, 7 \mod 8
\end{aligned}
$$

Example 25 ($k = 35, D = 10, \rho = 3$).

$$r = \Phi_{280}(v) = v^{96} + v^{92} - v^{76} - v^{72} - v^{68} - v^{64} + v^{56} + v^{52} + v^{48} + v^{44} + v^{40} - v^{32} - v^{28} - v^{24} - v^{20} + v^4 + 1$$
$$n = \tfrac{1}{2}\left(v^{72} - v^{70} - v^2 + 1\right)$$
$$\gamma = \tfrac{1}{10}\left(-2v^{65} - 2v^{63} + v^{37} + v^{35} - 2v^9 - 2v^7\right)$$
$$t_{p^2}^{'} = \tfrac{1}{20}\left(-5v^{144} + 10v^{142} - 5v^{140} + 8v^{130} + 16v^{128} + 8v^{126} - 8v^{102} - 16v^{100} - 8v^{98} + 28v^{74} + 16v^{72} + 28v^{70} - 8v^{46} - 16v^{44} - 8v^{42} + 8v^{18} + 16v^{16} + 8v^{14} - 5v^4 + 10v^2 - 5\right)$$
$$p = \tfrac{1}{40}\left(5v^{144} - 10v^{142} + 5v^{140} + 8v^{130} + 16v^{128} + 8v^{126} - 8v^{102} - 16v^{100} - 8v^{98} + 8v^{74} + 56v^{72} + 8v^{70} - 8v^{46} - 16v^{44} - 8v^{42} + 8v^{18} + 16v^{16} + 8v^{14} + 5v^4 - 10v^2 + 5\right)$$
$$v \equiv 3, 5, 7 \mod 10$$

A.3 With $\#J_{\mathcal{C}_6}(\mathbb{F}_p) = p^2 - p + 1 + t_p(1 + p + t_p)$.

Example 26 ($k = 5, D = 15, \rho = 3.5$).

$$r = \Phi_{15}(v) = v^8 - v^7 + v^5 - v^4 + v^3 - v + 1$$
$$t_p = v^5 + v^4 \equiv 2 \mod 3$$
$$\gamma = \tfrac{1}{15}\left(-2v^7 + 2v^6 - v^5 + 3v^4 - 4v^2 + 4v - 2\right)$$
$$p = \tfrac{1}{15}\left(v^{14} - 2v^{13} + 2v^{12} - 4v^{11} + 7v^{10} + 10v^9 - 2v^8 + 8v^7 - 10v^6 + 7v^5 + v^4 - 8v^3 + 8v^2 - 4v + 1\right)$$
$$v \equiv 1 \mod 15$$

Example 27 ($k = 6, D = 1, \rho = 3$).

$$r = \Phi_{12}(v) = v^4 - v^2 + 1$$
$$t_p = v^2 - 2 \equiv 2 \mod 3$$
$$\gamma = -v^3 + v$$
$$p = \tfrac{1}{4}\left(v^6 - v^4 - 3v^2 + 4\right)$$
$$v \equiv 0, 4, 8 \mod 12$$

Example 28 ($k = 6, D = 7, \rho = 3$).

$$r = \Phi_{42}(v) = v^{12} + v^{11} - v^9 - v^8 + v^6 - v^4 - v^3 + v + 1$$
$$t_p = v^7 - 2 \equiv 1 \mod 3$$
$$\gamma = \tfrac{1}{7}\left(2v^9 - v^7 + 2v^4 - 2v^2 - 2v\right)$$
$$p = \tfrac{1}{7}\left(v^{18} - v^{16} + 2v^{14} + 2v^{13} - 3v^{11} - 2v^{10} + v^9 + 2v^8 - 7v^7 - 2v^6 - 2v^5 + v^4 + 2v^3 + v^2 + 7\right)$$
$$v \equiv 0, 3, 12 \mod 21$$

Example 29 ($k = 9, D = 1, \rho = 2.67$).

$$r = \Phi_{36}(v) = v^{12} - v^6 + 1$$
$$t_p = -v^8 + v^6 + v^2 - 1 \equiv 2 \mod 3$$
$$\gamma = v^5 + v^3$$
$$p = \tfrac{1}{4}\left(v^{16} - 2v^{14} + v^{12} - v^{10} + 6v^8 - v^6 + v^4 - 2v^2 + 1\right)$$
$$v \equiv 3 \mod 6$$

Example 30 ($k = 13, D = 1, \rho = 3$).

$$r = \Phi_{156}(v) = v^{48} + v^{46} - v^{42} - v^{40} + v^{36} + v^{34} - v^{30} - v^{28} + v^{24} - v^{20} - v^{18} + v^{14} + v^{12} - v^8 - v^6 + v^2 + 1$$
$$t_p = -v^{36} + v^{26} + v^{10} - 1 \equiv 2 \mod 3$$
$$\gamma = v^{23} + v^{13}$$
$$p = \tfrac{1}{4}\left(v^{72} - 2v^{62} + v^{52} - v^{46} + 6v^{36} - v^{26} + v^{20} - 2v^{10} + 1\right)$$
$$v \equiv 3, 9 \mod 12$$

Example 31 ($k=14, D=1, \rho=3$).

$$r = \Phi_{84}(v) = v^{24}+v^{22}-v^{18}-v^{16}+v^{12}-v^8-v^6+v^2+1$$
$$t_p = -v^{18}+v^{14}+v^4-1 \equiv 2 \mod 3$$
$$\gamma = -v^{11}-v^7$$
$$p = \tfrac{1}{4}\left(v^{36}-2v^{32}+v^{28}-v^{22}+6v^{18}-v^{14}+v^8-2v^4+1\right)$$
$$v \equiv 3 \mod 6$$

Example 32 ($k=15, D=1, \rho=3.5$).

$$r = \Phi_{60}(v) = v^{16}+v^{14}-v^{10}-v^8-v^6+v^4+1$$
$$t_p = -v^{14}-v^{12}+v^{10}+v^6+v^4-2 \equiv 1 \mod 3$$
$$\gamma = -v^5-v^3$$
$$p = \tfrac{1}{4}\left(v^{28}+2v^{26}-v^{24}-2v^{22}-v^{20}-4v^{18}+6v^{14}+5v^{12}-v^{10}+3v^8-3v^6-4v^4+4\right)$$
$$v \equiv 0, 6 \mod 12$$

Example 33 ($k=15, D=2, \rho=3.5$).

$$r = \Phi_{120}(v) = v^{32}+v^{28}-v^{20}-v^{16}-v^{12}+v^4+1$$
$$t_p = -v^{28}-v^{24}+v^{20}+v^{12}+v^8-2 \equiv 2 \mod 3$$
$$\gamma = \tfrac{1}{2}\left(-v^{25}+v^{23}-v^{21}+v^{19}-v^{11}-v^7-v^3\right)$$
$$p = \tfrac{1}{8}\left(2v^{56}+4v^{52}+v^{50}-4v^{48}+3v^{46}-8v^{44}+3v^{42}-4v^{40}+v^{38}-6v^{36}-2v^{34}\right.$$
$$\left.+4v^{32}-4v^{30}+16v^{28}-4v^{26}+12v^{24}-v^{22}-4v^{20}+2v^{18}+2v^{16}+3v^{14}-8v^{12}\right.$$
$$\left.+2v^{10}-8v^8+v^6+8\right)$$
$$v \equiv 2, 4 \mod 6$$

Example 34 ($k=15, D=5, \rho=3.5$).

$$r = \Phi_{60}(v)$$
$$t_p = -v^{14}-v^{12}+v^{10}+v^6+v^4-2 \equiv 1 \mod 3$$
$$\gamma = \tfrac{1}{5}\left(2v^{13}-2v^9-2v^7-v^5-v^3\right)$$
$$p = \tfrac{1}{20}\left(5v^{28}+14v^{26}-5v^{24}-18v^{22}-13v^{20}-20v^{18}+4v^{16}+38v^{14}+33v^{12}-5v^{10}\right.$$
$$\left.+7v^8-19v^6-20v^4+20\right)$$
$$v \equiv 0, 30 \mod 60$$

Example 35 ($k=15, D=6, \rho=3.5$).

$$r = \Phi_{120}(v)$$
$$t_p = -v^{28}-v^{24}+v^{20}+v^{12}+v^8-2 \equiv 1 \mod 3$$
$$\gamma = \tfrac{1}{6}\left(v^{25}-v^{23}+v^{21}-v^{19}-2v^{15}-v^{11}+v^7-2v^5+v^3-2v\right)$$
$$p = \tfrac{1}{24}\left(6v^{56}+12v^{52}+v^{50}-8v^{48}+3v^{46}-16v^{44}+3v^{42}-12v^{40}+5v^{38}-30v^{36}+6v^{34}+44v^{28}\right.$$
$$\left.-8v^{26}+40v^{24}-9v^{22}-6v^{18}+18v^{16}-v^{14}-24v^{12}+6v^{10}-32v^8+9v^6-4v^4+4v^2+24\right)$$
$$v \equiv 0, 6, 12, 18 \mod 24$$

Example 36 ($k=15, D=15, \rho=3.5$).

$$r = \Phi_{15}(v) = v^8-v^7+v^5-v^4+v^3-v+1$$
$$t_p = -v^7+v^5-v^2 \equiv 2 \mod 3$$
$$\gamma = \tfrac{1}{15}\left(-5v^7+2v^6+3v^5-2v^4+4v^3-3v^2+2v+4\right)$$
$$p = \tfrac{1}{15}\left(10v^{14}-5v^{13}-14v^{12}+8v^{11}-6v^{10}+16v^9-v^8-24v^7+14v^6-2v^5+6v^4\right.$$
$$\left.+5v^3-5v^2+4v+4\right)$$
$$v \equiv 11 \mod 15$$

$$r = \Phi_{15}(v) = v^8 - v^7 + v^5 - v^4 + v^3 - v + 1$$
$$t_p = v^7 + v^4 - v^3 + v - 1 \equiv 2 \mod 3$$
$$\gamma = \tfrac{1}{15}\left(-3v^7 - 2v^6 - 2v^5 + v^4 + v^3 - 2v^2 + 3v - 3\right)$$
$$p = \tfrac{1}{15}\left(6v^{14} + 3v^{13} + 4v^{12} + 8v^{11} - 9v^{10} + v^9 + 8v^8 - 11v^7 + 3v^6 + 11v^5 - 14v^4 + 3v^3 + 9v^2 - 12v + 6\right)$$
$$v \equiv 9 \mod 15$$

Example 37 ($k = 18, D = 1, \rho = 3.33$).

$$r = \Phi_{36}(v) = v^{12} - v^6 + 1$$
$$t_p = -v^{10} + v^6 + v^4 - 1 \equiv 2 \mod 3$$
$$\gamma = v^7 + v^3$$
$$p = \tfrac{1}{4}\left(v^{20} - 2v^{16} - v^{14} + v^{12} + 6v^{10} + v^8 - v^6 - 2v^4 + 1\right)$$
$$v \equiv 3 \mod 6$$

Example 38 ($k = 21, D = 1, \rho = 2.67$).

$$r = \Phi_{84}(v) = v^{24} + v^{22} - v^{18} - v^{16} + v^{12} - v^8 - v^6 + v^2 + 1$$
$$t_p = -v^{16} + v^{14} + v^2 - 1 \equiv 2 \mod 3$$
$$\gamma = -v^9 - v^7$$
$$p = \tfrac{1}{4}\left(v^{32} - 2v^{30} + v^{28} - v^{18} + 6v^{16} - v^{14} + v^4 - 2v^2 + 1\right)$$
$$v \equiv 3 \mod 6$$

Example 39 ($k = 21, D = 7, \rho = 3$).

$$r = \Phi_{21}(v) = v^{12} - v^{11} + v^9 - v^8 + v^6 - v^4 + v^3 - v + 1$$
$$t_p = v^7 + v^6 \equiv 2 \mod 3$$
$$\gamma = \tfrac{1}{7}\left(2v^9 - 2v^8 - v^7 + v^6 - 2v^4 + 2v^3 + 2v^2 - 4v + 2\right)$$
$$p = \tfrac{1}{7}\left(v^{18} - 2v^{17} + 2v^{15} + v^{14} + v^{13} + 6v^{12} + v^{11} - 8v^{10} + 6v^9 + 2v^8 - 5v^7 + 6v^5 - 5v^4 - 2v^3 + 6v^2 - 4v + 1\right)$$
$$v \equiv 1, 4, 16 \mod 21$$

Example 40 ($k = 22, D = 1, \rho = 3$).

$$r = \Phi_{132}(v) = v^{40} + v^{38} - v^{34} - v^{32} + v^{28} + v^{26} - v^{22} - v^{20} - v^{18} + v^{14} + v^{12} - v^8 - v^6 + v^2 + 1$$
$$t_p = -v^{30} + v^{22} + v^8 - 1 \equiv 2 \mod 3$$
$$\gamma = -v^{19} - v^{11}$$
$$p = \tfrac{1}{4}\left(v^{60} - 2v^{52} + v^{44} - v^{38} + 6v^{30} - v^{22} + v^{16} - 2v^8 + 1\right)$$
$$v \equiv 3 \mod 6$$

Example 41 ($k = 26, D = 1, \rho = 2.5$).

$$r = \Phi_{156}(v) = v^{48} + v^{46} - v^{42} - v^{40} + v^{36} + v^{34} - v^{30} - v^{28} + v^{24} - v^{20} - v^{18} + v^{14} + v^{12} - v^8 - v^6 + v^2 + 1$$
$$t_p = -v^{30} + v^{26} + v^4 - 1 \equiv 2 \mod 3$$
$$\gamma = v^{17} + v^{13}$$
$$p = \tfrac{1}{4}\left(v^{60} - 2v^{56} + v^{52} - v^{34} + 6v^{30} - v^{26} + v^8 - 2v^4 + 1\right)$$
$$v \equiv 3 \mod 6$$

Example 42 ($k = 27, D = 1, \rho = 2.22$).

$$r = \Phi_{108}(v) = v^{36} - v^{18} + 1$$
$$t_p = -v^{20} + v^{18} + v^2 - 1 \equiv 2 \mod 3$$
$$\gamma = v^{11} + v^9$$
$$p = \tfrac{1}{4}\left(v^{40} - 2v^{38} + v^{36} - v^{22} + 6v^{20} - v^{18} + v^4 - 2v^2 + 1\right)$$
$$v \equiv 3 \mod 6$$

Example 43 ($k=30, D=1, \rho=3.5$).

$$
\begin{aligned}
r &= \Phi_{60}(v)\\
t_p &= -v^{14}+2v^{10}+v^8-v^2-2 \equiv 2 \mod 3\\
\gamma &= v^{11}-v^5\\
p &= \tfrac{1}{4}\left(v^{28}-4v^{24}-v^{22}+4v^{20}+4v^{18}+v^{16}+4v^{14}-4v^{12}-9v^{10}-4v^8+v^4+4v^2+4\right)\\
v &\equiv 2,4 \mod 6\\
r &= \Phi_{60}(v)\\
t_p &= -v^{14}+v^{10}+v^4-1 \equiv 2 \mod 3\\
\gamma &= -v^9-v^5\\
p &= \tfrac{1}{4}\left(v^{28}-2v^{24}+v^{20}-v^{18}+6v^{14}-v^{10}+v^8-2v^4+1\right)\\
v &\equiv 3 \mod 6
\end{aligned}
$$

Example 44 ($k=30, D=5, \rho=3.5$).

$$
\begin{aligned}
r &= \Phi_{60}(v)\\
t_p &= -v^{14}+2v^{10}+v^8-v^2-2\\
\gamma &= \tfrac{1}{5}\left(2v^{13}-v^{11}+v^5-2v^3\right) \equiv 2 \mod 3\\
p &= \tfrac{1}{20}\left(5v^{28}+4v^{26}-24v^{24}-9v^{22}+20v^{20}+24v^{18}+5v^{16}+24v^{14}-20v^{12}-49v^{10}\right.\\
&\quad \left.-24v^8+4v^6+5v^4+20v^2+20\right)\\
v &\equiv 4,10,14,16,20,26 \mod 30
\end{aligned}
$$

Example 45 ($k=30, D=15, \rho=3.5$).

$$
\begin{aligned}
r &= \Phi_{30}(v) = v^8+v^7-v^5-v^4-v^3+v+1\\
t_p &= v^5-v^4-1 \equiv 2 \mod 3\\
\gamma &= \tfrac{1}{15}\left(-4v^7-2v^6+v^5+v^4+2v^3+6v^2-1\right)\\
p &= \tfrac{1}{15}\left(4v^{14}+4v^{13}-v^{12}-3v^{11}-v^{10}-21v^9-v^8+6v^7+5v^6-2v^5+16v^4-v^3-3v^2+4\right)\\
v &\equiv 4,13 \mod 15\\
r &= \Phi_{30}(v) = v^8+v^7-v^5-v^4-v^3+v+1\\
t_p &= v^5+v^3-1 \equiv 2 \mod 3\\
\gamma &= \tfrac{1}{15}\left(-2v^7+2v^6+3v^5+3v^3+4v^2-4v-3\right)\\
p &= \tfrac{1}{15}\left(v^{14}-2v^{13}-2v^{12}+3v^{11}+3v^{10}-v^9+20v^8+5v^7-3v^6-6v^5-2v^4-20v^3-2v^2+6v+6\right)\\
v &\equiv 3,13 \mod 15
\end{aligned}
$$

Example 46 ($k=33, D=1, \rho=2.8$).

$$
\begin{aligned}
r &= \Phi_{132}(v) = v^{40}+v^{38}-v^{34}-v^{32}+v^{28}+v^{26}-v^{22}-v^{20}-v^{18}+v^{14}+v^{12}-v^8-v^6+v^2+1\\
t_p &= -v^{28}+v^{22}+v^6-1 \equiv 2 \mod 3\\
\gamma &= -v^{17}-v^{11}\\
p &= \tfrac{1}{4}\left(v^{56}-2v^{50}+v^{44}-v^{34}+6v^{28}-v^{22}+v^{12}-2v^6+1\right)\\
v &\equiv 3,9 \mod 12
\end{aligned}
$$

Example 47 ($k=34, D=1, \rho=2.625$).

$$
\begin{aligned}
r &= \Phi_{204}(v) = v^{64}+v^{62}-v^{58}-v^{56}+v^{52}+v^{50}-v^{46}-v^{44}+v^{40}+v^{38}-v^{34}-v^{32}-v^{30}\\
&\quad +v^{26}+v^{24}-v^{20}-v^{18}+v^{14}+v^{12}-v^8-v^6+v^2+1\\
t_p &= -v^{42}+v^{34}+v^8-1 \equiv \mod 3\\
\gamma &= v^{25}+v^{17}\\
p &= \tfrac{1}{4}\left(v^{84}-2v^{76}+v^{68}-v^{50}+6v^{42}-v^{34}+v^{16}-2v^8+1\right)\\
v &\equiv 3,9 \mod 12
\end{aligned}
$$

A.4 With $\#J_{\mathcal{C}_6}(\mathbb{F}_p) = p^2 + p + 1 - 3n(p + 1 - n)$.

Example 48 ($k = 28, D = 7, \rho = 3.33$).

$$
\begin{aligned}
r &= \Phi_{84}(v) = v^{24} + v^{22} - v^{18} - v^{16} + v^{12} - v^8 - v^6 + v^2 + 1 \\
n &= \tfrac{1}{3}\left(v^{15} + v^{14} + v + 1\right) \\
\gamma &= \tfrac{1}{7}\left(2v^{20} - 2v^{19} + 2v^{18} - 2v^{17} - 2v^{14} + 2v^{13} + v^8 - v^7 - 2v^4 + 2v^3\right) \\
p &= \tfrac{1}{84}\left(12v^{40} - 24v^{39} + 36v^{38} - 48v^{37} + 36v^{36} - 24v^{35} - 12v^{34} + 48v^{33} - 48v^{32} + 48v^{31} - 17v^{30}\right. \\
&\quad +14v^{29} + 31v^{28} - 48v^{27} + 36v^{26} - 24v^{25} - 12v^{24} + 48v^{23} - 60v^{22} + 72v^{21} - 36v^{20} + 24v^{18} \\
&\quad \left. -48v^{17} + 41v^{16} + 22v^{15} + 17v^{14} - 12v^{12} + 24v^{11} - 12v^{10} + 12v^8 - 24v^7 + 12v^6 + 7v^2 + 14v + 7\right) \\
v &\equiv 35, 71 \mod 84
\end{aligned}
$$