Classification of Genus-2 Hyperelliptic Curves over $\mathbb{F}_{5^m}$

Luis HERNÁNDEZ-ENCINAS

and

Jaime MUÑOZ-MASQUÉ

Dpto. Tratamiento de la Información y Codificación, Instituto de Física Aplicada, C.S.I.C.
C/ Serrano 144, 28006 Madrid, Spain
Emails: {luis, jaime}@iec.csic.es

ABSTRACT

The reduced equations for the hyperelliptic curves of genus 2 over finite fields of characteristic 5 are given, and the number of isomorphism classes of these curves are determined. These results have applications to hyperelliptic cryptosystems, *i.e.*, to cryptosystems based on hyperelliptic curves whose security relais on the discrete logarithm problem.

Keywords: Hyperelliptic curves, finite fields, public key cryptology, discrete logarithm problem, discriminant of hyperelliptic curves

1. INTRODUCTION

Over the years, several groups over finite fields have been proposed for using in discrete logarithm cryptosystems. The most important of these are the following:

1. The multiplicative group of a finite field of characteristic 2;
2. A proper subgroup of the multiplicative group of a finite field ([19]);
3. The group of units of $\mathbb{Z}_n$, n being a composite integer ([16]);
4. The group of points on an elliptic curve defined over a finite field ([10, 18]);
5. The Jacobian of a hyperelliptic curve defined over a finite field ([11]); and
6. The class group of an imaginary quadratic number field ([4]).

One of the more promising groups is the group of the rational points on an elliptic curve E defined over a finite field $\mathbb{F}$ of q elements. The addition of points can be performed using a few arithmetic operations in $\mathbb{F}$. Moreover, the order of the group is roughly equal to q, and if the largest prime factor of this order is r, the best algorithm known for the discrete logarithm problem in this group needs $O(\sqrt{r})$ steps; *i.e.*, the algorithm is *exponential*. Hence, one can use an elliptic curve over a finite field $\mathbb{F}$ of q elements, where $q \approx 2^{160}$, and get the same security as when a group $\mathbb{Z}_p^*$ is used with $p \approx 2^{1024}$.

More generally, one can use the Jacobian of any algebraic curve C (see [12, 7]) instead of the curve, as the curve is not a group, in general, whereas its Jacobian do it. It is know that Jacobian elements can be represented by a pair of polynomials over $\mathbb{F}$, of degree at most the genus of the curve C. These elements are called *reduced divisors*. Moreover there exists an efficient algorithm to add two divisor classes ([5]).

If C is a hyperelliptic curve of genus g defined over a finite field of q elements, $\mathbb{F}$, the order of its Jacobian, $\mathcal{J}(\mathbb{F})$, is roughly q^g. Note that if $g = 1$, then a hyperelliptic curve is an elliptic curve and its Jacobian is isomorphic to the curve itself. When g is large, there is a subexponential algorithm ([1]) for the discrete logarithm problem in $\mathcal{J}(\mathbb{F})$. Moreover, there exits an index-calculus algorithm ([6]) which is faster than the Pollard's rho method if the genus of the hyperelliptic curve is rather small, *i.e.*, greater or equal to 5.

If g is small (*e.g.*, $g = 2$), and r is the largest prime divisor of the order of the Jacobian of a hyperelliptic curve, the best algorithm known needs $O(\sqrt{r})$ steps, *i.e.*, the algorithm is *exponential*. Hence, one can use a hyperelliptic curve of genus 2 over a finite field of q elements, $\mathbb{F}$, where $q \approx 2^{80}$, and get the same security as when an elliptic curve group is used, where $q \approx 2^{160}$. A possible disadvantage of using curves of genus 2 instead of elliptic curves is that the group law may be more expensive, computationally speaking.

We should also mention that hyperelliptic curves have found applications in other areas as the following: primality proving ([2]), integer factorization ([13]), and error-correcting codes ([3]).

There are several cryptographical questions that need

to be answered about genus-2 hyperelliptic curves:

- To classify the isomorphism classes of genus-2 hyperelliptic curves.
- To give a "simple" canonical representation for each isomorphism class.

In ([8, 9]) we have obtained the canonical forms for hyperelliptic curves curves in characteristic $\neq 2, 5$. In the present communication, we analyze the case of the characteristic 5.

2. REDUCED EQUATIONS OF HYPERELLIPTIC CURVES

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of q elements, and $\mathbb{F} \subset \mathbb{K} = \mathbb{F}_{q^m}$ be a field extension. We recall ([14, 2.22]) that the trace of an element $\alpha \in \mathbb{K}$ over $\mathbb{F}$ is defined by

$$\mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}}.$$

Set $\mathbb{F}^* = \mathbb{F} - \{0\}$ and we denote the algebraic closure of $\mathbb{F}$ by $\overline{\mathbb{F}}$. For each positive integer k, we set $\mathbb{F}^{(k)} = \{\alpha^k : \alpha \in \mathbb{F}\}$.
As we are interested in hyperelliptic curves of genus 2 in characteristic 5, throught this paper we assume that $\mathbb{F}$ is a finite field of characteristic 5, so that $\#\mathbb{F} = 5^m$. Moreover, we write $\mathrm{Tr}(\alpha)$ instead of $\mathrm{Tr}_{\mathbb{F}_5}^{\mathbb{F}_{5^m}}(\alpha)$.
In this section we will study the Weierstrass equation defining a hyperelliptic curve of genus 2 and several properties of this kind of curves.

Definition and equations

As is well known (*e.g.*, see [12]), a *hyperelliptic curve C of genus g* over a finite field $\mathbb{F}$ is a projective non-singular irreducible curve of genus g defined over $\mathbb{F}$ for which there exists a map $C \to \mathbb{P}^1$ of degree two, where $\mathbb{P}^1$ is the 1-dimensional projective space over $\overline{\mathbb{F}}$. Every hyperelliptic curve C of genus g ($g \geq 1$) defined over $\mathbb{F}$ can be given by a *Weierstrass equation*

$$H\colon v^2 + h(u)\, v = f(u), \tag{1}$$

where $h(u) \in \mathbb{F}[u]$ is a polynomial of degree at most g, and $f(u) \in \mathbb{F}[u]$ is a monic polynomial of degree $2g+1$. In the particular case for which $g = 2$, we have

$$\begin{aligned} h(u) &= a_1u^2 + a_3u + a_5, \\ f(u) &= u^5 + a_2u^4 + a_4u^3 + a_6u^2 + a_8u + a_{10}, \end{aligned} \tag{2}$$

with all $a_i \in \mathbb{F}$. It is easily checked that C has a unique point O at infinity, and this point is the only singular point of the curve, and the curve is tangent to the infinity line at this point. The set of $\mathbb{K}$-*rational points* on C, $C(\mathbb{K})$, is the set of all points $P = (x, y) \in \mathbb{K} \times \mathbb{K}$ that satisfy the Eq. (1) of the curve H.

Examples

We can see several examples of hyperelliptic curves. First, we consider a hyperelliptic curve of genus 2 over the real numbers $\mathbb{R}$. In this case the genus of the curve can be identify with its number of holes.

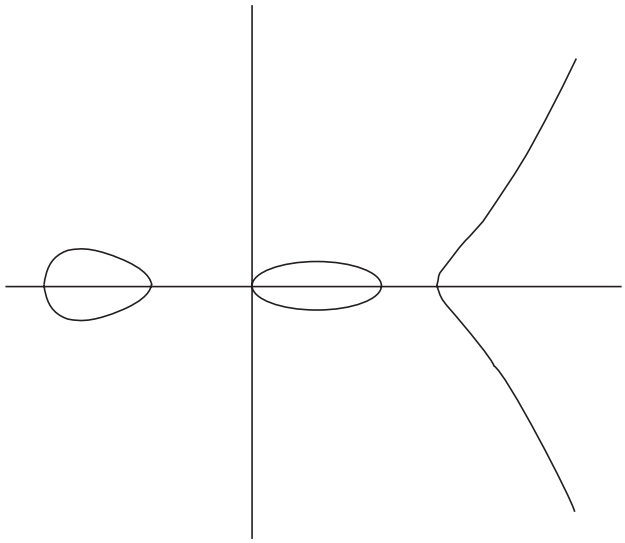

Figure 1. Hyperelliptic curve over $\mathbb{R}$

The graphic representation of a hyperelliptic curve if genus 2 over $\mathbb{R}$ is showed in Figure 1.

Now, if we consider the hyperelliptic curve, C, of genus 2 given by the equation

$$H\colon v^2 + uv = u^5 + 2u^4 + 3u^3 + 6u^2 + u + 5$$

over the finite field $\mathbb{F}_{11}$, this curve only has a singular point at the infinity and its $\mathbb{F}_{11}$-rational points, $C(\mathbb{F}_{11})$, are

$$\{(0,4),(0,7),(3,9),(3,10),(4,9),\\ (8,4),(8,10),(9,3),(9,10),(10,6)\}$$

A different example could be the hyperelliptic curve of genus 2 defined, over $\mathbb{F}_{5^2} = \mathbb{F}_5[x]/(x^2 + x + 1)$, by the equation

$$H\colon v^2 = u^5 + u^2 + 1.$$

Here, if α is a primitive root of $x^2 + x + 1$ in $\mathbb{F}_{5^2}$, then the finite points in $C(\mathbb{F}_{5^2})$, that is, the set of

$\mathbb{F}_{5^2}$-rational points on C is

$$\{(0,2),(0,3),(1,1+2\alpha),(1,4+3\alpha),(2,3+\alpha),$$
$$(2,2+4\alpha),(3,1+2\alpha),(3,4+3\alpha),(4,2),(4,3),$$
$$(1+\alpha,2),(1+\alpha,3),(2+\alpha,3+2\alpha),(2+\alpha,2+3\alpha),$$
$$(2\alpha,1+\alpha),(2\alpha,4+4\alpha),(4+2\alpha,0),(2+3\alpha,0),$$
$$(3+3\alpha,\alpha),(3+3\alpha,4\alpha),(4\alpha,2),(4\alpha,3),$$
$$(1+4\alpha,4+2\alpha),(1+4\alpha,1+3\alpha)\}.$$

Reduced equations for hyperelliptic curves

Two hyperelliptic curves of genus g are said to be *isomorphic* over $\mathbb{F}$ if they are isomorphic as projective varieties over $\mathbb{F}$. In general, two projective varieties V_1, V_2 over $\mathbb{F}$ are isomorphic over $\mathbb{F}$ if there exist morphisms $\phi : V_1 \longrightarrow V_2$, $\psi : V_2 \longrightarrow V_1$ (ϕ , ψ defined over $\mathbb{F}$), such that $\psi\circ\phi$ and $\phi\circ\psi$ are the identity maps on V_1, V_2 respectively (*cf.* [20]). If C_1, C_2 are isomorphic over $\mathbb{F}$, then their $\mathbb{F}$-Jacobians $\mathcal{J}_{C_1}(\mathbb{F})$ and $\mathcal{J}_{C_2}(\mathbb{F})$ are also isomorphic (as abelian groups) ([21]). Thus, a classification of the isomorphism classes of genus-2 hyperelliptic curves over $\mathbb{F}$ is relevant to hyperelliptic curve cryptology because the $\mathbb{F}$-Jacobians of these curves are used as the finite groups in discrete logarithm cryptographic schemes. Note, however, that if C_1, C_2 are such that $\mathcal{J}_{C_1}(\mathbb{F})$ and $\mathcal{J}_{C_2}(\mathbb{F})$ are isomorphic (as abelian groups), then this does not imply that C_1 and C_2 are isomorphic (as projective varieties) over $\mathbb{F}$.

The Eq. (1) defining a hyperelliptic curve C of genus 2 is unique up to a change of coordinates of the form ([15, Proposition 1.2])

$$(u,v) \mapsto \left(\alpha^2 u + \beta, \alpha^5 v + \alpha^4\gamma u^2 + \alpha^2\delta u + \epsilon\right), \quad (3)$$

where $\alpha \in \mathbb{F}^*$, and $\beta, \gamma, \delta, \epsilon \in \mathbb{F}$. By carrying out the change of coordinates of Eq. (3) in Eq. (1), and computing the values for the new coefficients $\overline{a}_i$, corresponding to the formulas in Eq. (2), we obtain

$$\begin{aligned}
\alpha\overline{a}_1 =& a_1 + 2\gamma \quad (4)\\
\alpha^3\overline{a}_3 =& a_3 + 2\beta a_1 + 2\delta\\
\alpha^5\overline{a}_5 =& a_5 + \beta a_3 + \beta^2 a_1 + 2\varepsilon\\
\alpha^2\overline{a}_2 =& a_2 + 4\gamma a_1 + 4\gamma^2\\
\alpha^4\overline{a}_4 =& a_4 + 4\gamma a_3 + 4\beta a_2 + (3\beta\gamma + 4\delta)a_1 + 3\gamma\delta\\
\alpha^6\overline{a}_6 =& a_6 + 4\gamma a_5 + 3\beta a_4 + 4\left(\beta\gamma + \delta\right)a_3 + \beta^2 a_2\\
&+ (3\beta\delta + 4\beta^2\gamma + 4\varepsilon)a_1 + 4\delta^2 + 3\gamma\epsilon\\
\alpha^8\overline{a}_8 =& a_8 + 2\beta a_6 + 4\delta a_5 + 3\beta^2 a_4 + 4\left(\beta\delta + \varepsilon\right)a_3\\
&+ 4\beta^3 a_2 + (4\beta^2\delta + 3\beta\varepsilon)a_1 + 3\delta\epsilon\\
\alpha^{10}\overline{a}_{10} =& a_{10} + \beta a_8 + \beta^2 a_6 + 4\varepsilon a_5 + \beta^3 a_4 + 4\beta\varepsilon a_3\\
&+ \beta^4 a_2 + 4\beta^2\varepsilon a_1 + \beta^5 + 4\varepsilon^2.
\end{aligned}$$

By using the formulas in Eq. (4) it is readily checked that every hyperelliptic curve of genus 2 can be represented by the Eq. (1) such that $h(u) = 0$; that is,

$$v^2 = u^5 + a_2u^4 + a_4u^3 + a_6u^2 + a_8u + a_{10}. \quad (5)$$

Moreover, as a simple computations shows, the only admissible changes of variables of Eq. (3) transforming the Eq. (5) into another of the same form, are

$$(u,v) \mapsto \left(\alpha^2 u + \beta, \alpha^5 v\right), \quad \alpha \in \mathbb{F}^*, \beta \in \mathbb{F}, \quad (6)$$

that is, $\gamma, \delta, \varepsilon$ should vanish. Hence, the formulas in Eq. (4) yield

$$\begin{aligned}
\alpha^2\overline{a}_2 &= a_2 \quad (7)\\
\alpha^4\overline{a}_4 &= a_4 + 4\beta a_2 \quad (8)\\
\alpha^6\overline{a}_6 &= a_6 + 3\beta a_4 + \beta^2 a_2 \quad (9)\\
\alpha^8\overline{a}_8 &= a_8 + 2\beta a_6 + 3\beta^2 a_4 + 4\beta^3 a_2 \quad (10)\\
\alpha^{10}\overline{a}_{10} &= a_{10} + \beta a_8 + \beta^2 a_6 + \beta^3 a_4 + \beta^4 a_2 + \beta^5 \quad (11)
\end{aligned}$$

Now, we will distinguish several cases:

(i) If $a_2 \neq 0$, taking $\beta = a_4/a_2$ in Eq. (8) we obtain $\overline{a}_4 = 0$. Hence, the Eq. (5) is reduced to

$$H_1 \colon v^2 = u^5 + \overline{a}_2u^4 + \overline{a}_6u^2 + \overline{a}_8u + \overline{a}_{10},$$

by means of the change of variables

$$(u,v) \mapsto \left(\alpha^2 u + \frac{a_4}{a_2}, \alpha^5 v\right).$$

(ii) If $a_2 = 0$ and $a_4 \neq 0$, by taking $\beta = a_6/(2a_4)$ in Eq. (9) we have $\overline{a}_6 = 0$. Hence, the Eq. (5) is reduced to

$$H_2 \colon v^2 = u^5 + \overline{a}_4u^3 + \overline{a}_8u + \overline{a}_{10},$$

by means of the change of variables

$$(u,v) \mapsto \left(\alpha^2 u + \frac{a_6}{2a_4}, \alpha^5 v\right).$$

(iii) If $a_2 = a_4 = 0$ and $a_6 \neq 0$, by taking $\beta = a_8/(3a_6)$ in Eq. (10) we obtain $\overline{a}_8 = 0$. Then, the Eq. (5) is reduced to

$$H_3 \colon v^2 = u^5 + \overline{a}_6u^2 + \overline{a}_{10},$$

by means of the change of variables

$$(u,v) \mapsto \left(\alpha^2 u + \frac{a_8}{3a_6}, \alpha^5 v\right).$$

(iv) Finally, if $a_2 = a_4 = a_6 = 0$ and $a_8 \neq 0$, then the Eq. (5) is reduced to

$$H_4 \colon v^2 = u^5 + \overline{a}_8u + \overline{a}_{10}.$$

In summary, we have proved that every hyperelliptic curve of genus 2 admits a reduced equation of the following four types:

$$H_1\colon v^2 = u^5 + a_2u^4 + a_6u^2 + a_8u + a_{10}, a_2 \neq 0 \quad (12)$$

$$H_2\colon v^2 = u^5 + a_4u^3 + a_8u + a_{10}, a_4 \neq 0 \quad (13)$$

$$H_3\colon v^2 = u^5 + a_6u^2 + a_{10}, a_6 \neq 0 \quad (14)$$

$$H_4\colon v^2 = u^5 + a_8u + a_{10}, a_8 \neq 0 \quad (15)$$

3. NUMBER OF HYPERELLIPTIC CURVES

Next, we compute the automorphism group of each non-singular hyperelliptic curve of genus 2. To do this, we first define the discriminant of a hyperelliptic curve.

The *discriminant* of a polynomial $f(x) \in \mathbb{F}[x]$ is denoted by $\Delta(f)$, *i.e.*, $\Delta(f) = \text{Resultant}(f, f')$, where f' is the derivative of f. It is know ([15, Theorem 1.7]) that a hyperelliptic curve C defined by an Weierstrass equation like Eq. (1) has not singular affine points, *i.e.*, its discriminant $\Delta(C)$ does not vanish. In our case, if the hyperelliptic curve is of genus 2 and it is defined over a field of characteristic 5, the curve C is always given by a reduced equation likes Eq. (5), hence $h = 0$ and we have $\Delta(C) = \Delta(f)$, where f is as in Eq. (2).

Now, we compute the automorphism group of each non-singular hyperelliptic curve of genus 2. To this end, we first compute the discriminant of each class of curves H_1–H_4. We have

$$\begin{aligned}
\Delta_1 = \Delta(H_1) &= 4a_{10}a_2^3a_8^3 + a_8^5 + 3a_2a_8^4a_6 + 3a_2^4a_8^4 \\
&\quad + 4a_6^2a_2^2a_8^3 + 4a_6^3a_2^2a_8a_{10} + 4a_6a_2^4a_{10}a_8^2 + 2a_6^2a_2^4a_{10}^2 \\
&\quad + a_6^4a_2^3a_{10} + a_6^3a_2^3a_8^2 + a_2^5a_{10}^3 + 3a_6^4a_8^2 + 3a_6^5a_{10} \\
\Delta_2 = \Delta(H_2) &= 2a_8^4a_4^2 + a_4^4a_8^3 + 3a_4^5a_{10}^2 + a_8^5 \\
\Delta_3 = \Delta(H_3) &= 3a_6^5a_{10} \\
\Delta_4 = \Delta(H_4) &= a_8^5
\end{aligned}$$

To determine the automorphism group of each class of curve given in Eq. (12)–(15), we consider the following cases:

(a) Making the change of variables of Eq. (6) in the Eq. (12) of H_1, and imposing that the transformed curve coincides with H_1, from the Eq. (7)–(11), we obtain $\beta = 0$ and $\alpha^2 = 1$. Therefore, the automorphism group for each curve of type H_1 is

$$(u, v) \mapsto (u, \alpha v), \quad \alpha^2 = 1.$$

(b) Analogously, for the Eq. (13) of H_2, we have $\beta = 0$, and if $a_{10} = 0$, then $\alpha^4 = 1$; if $a_{10} \neq 0$, then $\alpha^4 = \alpha^{10} = 1$, hence $\alpha^2 = 1$. Consequently, the automorphism group of the curves of type H_2 is

$$\begin{cases} (u, v) \mapsto (u, \alpha v), & \alpha^4 = 1 \quad \text{if } a_{10} = 0 \\ (u, v) \mapsto (u, \alpha v), & \alpha^2 = 1 \quad \text{if } a_{10} \neq 0. \end{cases}$$

(c) In this case, Eq. (14), a_{10} cannot vanish as the curve is assumed to be non-singular, and we obtain $\beta = 0$ and $\alpha^6 = \alpha^{10} = 1$, hence $\alpha^4 = 1$ and finally, $\alpha^2 = 1$. Therefore, the automorphism group of the curves of type H_3 is

$$(u, v) \mapsto (u, \alpha v), \quad \alpha^2 = 1.$$

(d) For the curves H_4 of Eq. (15), we obtain

$$\begin{aligned}
\alpha^8 a_8 &= a_8 \\
\alpha^{10} a_{10} &= a_{10} + \beta a_8 + \beta^5.
\end{aligned}$$

Hence $\alpha^8 = 1$, and substituting it into the second equation above, we obtain

$$\beta^5 + a_8\beta = a_{10}(\alpha^2 - 1). \quad (16)$$

We distinguish several cases:

(d.1) If $-a_8 \notin (\mathbb{F}^*)^{(4)}$, then the map $x \mapsto x^5 + a_8x$ is bijective; hence the Eq. (16) has a unique solution, say β_α, and the automorphism group is

$$(u, v) \mapsto \left(\alpha^2 u + \beta_\alpha, \alpha^5 v\right), \quad \alpha^8 = 1.$$

(d.2) If $-a_8 \in (\mathbb{F}^*)^{(4)}$, then there exists $\beta_0 \in \mathbb{F}^*$ such that $\beta_0^4 = -a_8$, and letting $\bar{\beta} = \beta/\beta_0$, the Eq. (16) becomes

$$\bar{\beta}^5 - \bar{\beta} = \frac{a_{10}(\alpha^2 - 1)}{\beta_0^5}. \quad (17)$$

Hence, according to ([17, Theorem 3.5]), we have: If $\text{Tr}(a_{10}(\alpha^2 - 1)/\beta_0^5) \neq 0$, the equation (17) has no solution. If $\text{Tr}(a_{10}(\alpha^2 - 1)/\beta_0^5) = 0$, the equation (17) has five distinct solutions: If $\bar{\beta}_\alpha$ is one of them, the other solutions are $\bar{\beta}_\alpha \pm 1$, $\bar{\beta}_\alpha \pm 2$. Then, we have the following subcases:

(d.2.1) If m is even, then the solutions to $\alpha^8 = 1$ are $\{\pm 1, \pm 2, \pm\sqrt{2} \pm 2\sqrt{2}\}$, and we have:
If $\text{Tr}(a_{10}/\beta_0^5) = 0$, then the automorphism group is

$$(u, v) \mapsto \left(\alpha^2 u + \beta, \alpha^5 v\right),$$

where $\alpha^8 = 1$, $\beta \in \{\beta_0\bar{\beta}_\alpha, \beta_0(\bar{\beta}_\alpha \pm 1), \beta_0(\bar{\beta}_\alpha \pm 2)\}$.
If $\text{Tr}(a_{10}/\beta_0^5) \neq 0$, then the automorphism group is

$$(u, v) \mapsto (u + \beta, \alpha v), \quad \alpha^2 = 1, \ \beta \in \{0, \beta_0\bar{\beta} : \bar{\beta}^4 = 1\}.$$

(d.2.2) If m is odd, then the only solutions to the equation $\alpha^8 = 1$ are $\{\pm 1, \pm 2\}$, and we have:

If $\mathrm{Tr}(a_{10}/\beta_0^5)=0$, then the automorphism group is

$$(u,v)\mapsto \left(\alpha^2 u+\beta,\alpha v\right),$$

where $\alpha^4=1,\ \beta\in\{\beta_0\bar{\beta}_\alpha,\beta_0(\bar{\beta}_\alpha\pm 1),\beta_0(\bar{\beta}_\alpha\pm 2)\}$.
If $\mathrm{Tr}(a_{10}/\beta_0^5)\neq 0$, then the automorphism group is

$$(u,v)\mapsto (u+\beta,\alpha v),\quad \alpha^2=1,\ \beta\in\{0,\beta_0\bar{\beta}:\bar{\beta}^4=1\}.$$

Let us compute the number of singular reduced equations. If we consider the sets

$$\begin{aligned}
W_1&=\left\{(a_2,a_6,a_8,a_{10})\in\mathbb{F}^4 : a_2\neq 0,\Delta_1=0\right\}\\
W_{21}&=\left\{(a_4,a_8,0)\in\mathbb{F}^3 : a_4\neq 0,\Delta_2=0\right\}\\
W_{22}&=\left\{(a_4,a_8,a_{10})\in\mathbb{F}^3 : a_4\neq 0,a_{10}\neq 0,\Delta_2=0\right\},
\end{aligned}$$

then, we have

$$\begin{aligned}
|W_1|&=q^2(q-1)\\
|W_{21}|&=q-1,\qquad |W_{22}|=q-1.
\end{aligned}$$

Let $\mathcal{H}_i$, $i=1,\dots,4$, be the set of equations of the form (12)-(15) satisfying $\Delta_i\neq 0$, respectively. We set $\mathcal{H}_2=\mathcal{H}_2^1\cup\mathcal{H}_2^2$ and

$$\mathcal{H}_4=\mathcal{H}_4^1\cup\mathcal{H}_4^2\cup\mathcal{H}_4^3\cup\mathcal{H}_4^4\cup\mathcal{H}_4^5\cup\mathcal{H}_4^6$$

where

$$\begin{aligned}
\mathcal{H}_2^1&=\{H_2\in\mathcal{H}_2 : a_{10}=0\}\\
\mathcal{H}_2^2&=\{H_2\in\mathcal{H}_2 : a_{10}\neq 0\}\\
\mathcal{H}_4^1&=\{H_4\in\mathcal{H}_4 : -a_8\notin(\mathbb{F}^*)^{(4)}, m\text{ even}\}\\
\mathcal{H}_4^2&=\{H_4\in\mathcal{H}_4 : -a_8\notin(\mathbb{F}^*)^{(4)}, m\text{ odd}\}\\
\mathcal{H}_4^3&=\{H_4\in\mathcal{H}_4 : -a_8\in(\mathbb{F}^*)^{(4)}, \mathrm{Tr}\left(a_{10}/\beta_0^5\right)=0, m\text{ even}\}\\
\mathcal{H}_4^4&=\{H_4\in\mathcal{H}_4 : -a_8\in(\mathbb{F}^*)^{(4)}, \mathrm{Tr}\left(a_{10}/\beta_0^5\right)\neq 0, m\text{ even}\}\\
\mathcal{H}_4^5&=\{H_4\in\mathcal{H}_4 : -a_8\in(\mathbb{F}^*)^{(4)}, \mathrm{Tr}\left(a_{10}/\beta_0^5\right)=0, m\text{ odd}\}\\
\mathcal{H}_4^6&=\{H_4\in\mathcal{H}_4 : -a_8\in(\mathbb{F}^*)^{(4)}, \mathrm{Tr}\left(a_{10}/\beta_0^5\right)\neq 0, m\text{ odd}\}.
\end{aligned}$$

We denote by G_i the group of changes of the form (6) transforming $\mathcal{H}_i$ into itself; that is,

$$\begin{aligned}
G_1=G_2=G_3&=\{(u,v)\mapsto(\alpha^2u,\alpha^5v):\alpha\in\mathbb{F}^*\}\\
G_4&=\{(u,v)\mapsto(\alpha^2u+\beta,\alpha^5v):\alpha\in\mathbb{F}^*\}
\end{aligned}$$

Moreover, we denote by I_i^j the group of automorphisms of an arbitrary curve in each of the classes $\mathcal{H}_i^j$, defined above. Then we have

$$\begin{aligned}
&|G_1|=|G_2|=|G_3|=q-1\\
&|G_4|=q(q-1)\\
&|I_1|=2\\
&|I_2^1|=4,\quad |I_2^2|=2\\
&|I_3|=2\\
&|I_4^1|=8,\quad |I_4^2|=4\\
&|I_4^3|=40,\quad |I_4^4|=10,\quad |I_4^5|=20,\quad |I_4^6|=10.
\end{aligned}$$

Then we have

$$\begin{aligned}
|\mathcal{H}_1/G_1|&=\frac{|\mathcal{H}_1|}{(G_1:I_1)}=2q^2(q-1)\\
|\mathcal{H}_2^1/G_2|&=\frac{|\mathcal{H}_2^1|}{(G_2:I_2^1)}=4(q-2)\\
|\mathcal{H}_2^2/G_2|&=\frac{|\mathcal{H}_2^2|}{(G_2:I_2^2)}=2(q-1)(q-2)\\
|\mathcal{H}_3/G_3|&=\frac{|\mathcal{H}_3|}{(G_3:I_3)}=2(q-1)\\
|\mathcal{H}_4^1/G_4|&=\frac{|\mathcal{H}_4^1|}{(G_4:I_4^1)}=6\\
|\mathcal{H}_4^2/G_4|&=\frac{|\mathcal{H}_4^2|}{(G_4:I_4^2)}=3\\
|\mathcal{H}_4^3/G_4|&=\frac{|\mathcal{H}_4^3|}{(G_4:I_4^3)}=2\\
|\mathcal{H}_4^4/G_4|&=\frac{|\mathcal{H}_4^4|}{(G_4:I_4^4)}=2\\
|\mathcal{H}_4^5/G_4|&=\frac{|\mathcal{H}_4^5|}{(G_4:I_4^5)}=1\\
|\mathcal{H}_4^6/G_4|&=\frac{|\mathcal{H}_4^6|}{(G_4:I_4^6)}=2
\end{aligned}$$

Hence,

$$\begin{aligned}
|\mathcal{H}_1/G_1|&=2q^2(q-1)\\
|\mathcal{H}_2/G_2|&=2(q+1)(q-2)\\
|\mathcal{H}_3/G_3|&=2(q-1)\\
|\mathcal{H}_4/G_4|&=\begin{cases}10, & m\,\text{even}\\ 6, & m\,\text{odd}\end{cases}
\end{aligned}$$

and then,

$$\text{Isomorphism classes }=\begin{cases}2q^3+4, & m\,\text{even}\\ 2q^3, & m\,\text{odd}.\end{cases}$$

4. CONCLUSIONS

In this paper we have studied hyperelliptic curves of genus 2 defined over a finite field of characteristic 5 in relation to their applications to hyperelliptic cryptosystems. In this way, first we have proved that there only exit four classes of reduced equations for these curves. Moreover, we have stablished that the number of isomorphism classes of this kind of curves is around q^3. Hence, it is verified the hypotesis that if $\mathbb{F}$ is a finite field of order q, there are $\Theta(q^{2g-1})$ isomorphism classes of hyperelliptic curves of genus $g=2$ over $\mathbb{F}$.

Acknowledgement. Supported by CICYT (Spain) under grant TIC2001-0586.

5. REFERENCES

[1] L. Adleman, J. DeMarrais and M. Huang, "A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields", Algorithmic Number Theory, LNCS 877, 1994, pp. 28–40.

[2] L. Adleman and M. Huang, Primality testing and Abelian varieties over finite fields, Berlin: LNM 1512, Springer-Verlag, 1992.

[3] D. Le Brigand, "Decoding of codes on hyperelliptic curves", Proceedings of EUROCODE'90, LNCS 514, 1991, pp. 126–134.

[4] J. Buchmann and H. Williams, "A key-exchange system based on imaginary quadratic fields", J. Cryptology 1, 1988, pp. 107–118.

[5] D. Cantor, "Computing in the Jacobian of a hyperelliptic curve", Math. Comp. 48, 1987, pp. 95–101.

[6] P. Gaudry, "An algorithm for solving the discrete log problem on hyperelliptic curves", Proceedings of EUROCRYPT'2000, LNCS 1807, 2000, pp. 19–34.

[7] R. Hartshorne, Algebraic Geometry, New York: Springer Verlag, 1977.

[8] L. Hernández Encinas, Alfred J. Menezes, and J. Muñoz Masqué, "Isomorphism classes of genus-2 hyperelliptic curves over finite fields", Appl. Algebra Engrg. Comm. Comput. (to appear).

[9] L. Hernández Encinas and J. Muñoz Masqué, The number of hyperelliptic curves over a finite field. Recent results", Proceedings of SCI'2001, Vol. VII, 2001, pp. 505–510.

[10] N. Koblitz, "Elliptic curve cryptosystems", Math. Comput. 48, 1987, pp. 203–209.

[11] — , "Hyperelliptic cryptosystems", J. Cryptology 1, 1989, pp. 139-150.

[12] —, Algebraic aspects of cryptography, Berlin: ACM 3, Springer-Verlag, 1998.

[13] H. W. Lenstra, J. Pila, and C. Pomerance, "A hyperelliptic smoothness test, I", R. Soc. Philos. Trans. Ser. A 345, 1993, pp. 397–408.

[14] R. Lidl and H. Niederreiter, Introduction to finite fields and ther applications, Cambridge: Cambridge University Press, 1994.

[15] P. Lockhart, "On the discriminant of a hyperelliptic curve", Trans. Amer. Math. Soc. 342, 2, 1994, pp. 729–752.

[16] K. McCurley, "A key distribution system equivalent to factoring", J. Cryptology 1, 1988, pp. 95–105.

[17] A. Menezes (ed.), I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, Applications of finite fields, Boston: Kluwer Academic Publishers, 1993.

[18] V. Miller, "Uses of elliptic curves in cryptography", Proceedings of CRYPTO'85, LNCS 218, 1986, pp. 417–426.

[19] C. Schnorr, "Efficient signature generation by smart cards", J. Cryptology 4, 1991, pp. 161–174.

[20] J. Silverman, The arithmetic of elliptic curves, New York: Springer-Verlag, 1986.

[21] —, Advanced topics in the arithmetic of elliptic curves, New York: Springer-Verlag, 1994.