ISOMORPHISM CLASSES OF HYPERELLIPTIC CURVES OF GENUS 3 OVER FINITE FIELDS

EUNKYUNG JEONG
DEPARTMENT OF MATHEMATICS
POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY
POHANG, 790–784, KOREA
EMAIL:EKJEONG@POSTECH.AC.KR

Abstract. We give the number of the isomorphism classes of hyperelliptic curves of genus 3 defined over finite fields $\mathbb{F}_{p^n}$, $p \neq 2, 7$. These results have applications to cryptography.

Keywords cryptography, hyperelliptic curves, finite fields, isomorphism classes.

1. Introduction

Since elliptic curve cryptosystems were proposed in 1985 by V. Miller [16] and by N. Koblitz [10] independently, as a good source of public key cryptosystem with a small key length, there has been a lot of research in this direction. The advantages using elliptic curve cryptosystem were the greater flexibility in choosing the group over a given field and especially the absence of subexponential time algorithms to break the system if an elliptic curve is suitably chosen.

In 1989, Koblitz generalized the concept of elliptic curve cryptosystems to hyperelliptic curves of higher genus [11]. Using the Jacobian of a hyperelliptic curve defined over a finite field instead of a finite field or an elliptic curve, we can further reduce the key size while maintaining the same level of security. One can use a hyperelliptic curve of genus 2 over a finite field $\mathbb{F}_q$, where $q \approx 2^{80}$, and achieve the same level of security as when an elliptic curve group $E(\mathbb{F}_q)$ is used, where $q \approx 2^{160}$ or a group $\mathbb{F}_q^*$ is used with $q \approx 2^{1024}$.

1991 *Mathematics Subject Classification.*
This work was partially supported by MSRC.

To select suitable hyperelliptic curves, we need some security requirements. Let H be a hyperelliptic curve over the field $\mathbb{F}_q$ of genus g such that the order of the Jacobian $J_H(\mathbb{F}_q)$ is $N = c \cdot \ell$, where ℓ is a large prime. At first, ℓ should be greater than 2^{160} to protect against Pollard-rho and Baby-Step/Giant-Step attacks. And if $q = 2^r$, then r should be a prime to prevent Weil descent attack on $J_H(\mathbb{F}_q)$. To protect against the Tate-pairing attack, the smallest $s \geq 1$ such that $q^s \equiv 1 \pmod{p}$ should be greater than 20[8]. At last, the genus g must be smaller than 5 to protect against the attack by Gaudry[9]. So we consider the only hyperelliptic curves of genus $2, 3$ or 4.

It may be useful to classify the isomorphism classes of hyperelliptic curves of genus 2 and 3 over finite fields, in order to know how many essentially different choices of curves are. And this classification is used to produce nonisomorphic hyperelliptic curves, which may be useful for a cryptographic purpose. In [7] the number of isomorphism classes of hypereilliptic curves of genus 2 over F_q with characteristic different from 2 or 5 were studied. Later the bound of number of isomorphism classes of the hyperelliptic curves of genus 2 over F_{2^n} was derived in [5] and the exact number and the representatives of each isomorphism classes are determined[4].

In this paper we count the number of isomorphism classes of hyperelliptic curves of genus 3 over a finite field with characteristic different from 2,7.
This paper is organized as follows; In section 2 we give necessary definitions. In section 3 we give the number of isomorphism classes of hyperelliptic curves of genus 3 over finite fields.

2. **Hyperelliptic curves**

In this section, we recall the basic definitions and theories. We follow notations given in [13].

A hyperelliptic curve over a field $\mathbb{F}$ of genus g is a nonsingular projective curve C over $\mathbb{F}$ of genus g for which there exists a map $C \longrightarrow \mathbb{P}^1(\mathbb{F})$ of degree two.

A divisor on the curve C is a finite formal sum of points of the curve. For a divisor D, let $L(D)$ denote a vector space of rational functions f over C which satisfy $(f) + D \geq 0$ and $l(D) = dim L(D)$. For $C \in H_g$, $P \in C$ is called a

Weierstrass point of C if $l(2P) > 1$. When $g = 1$, every point is a Weierstrass point. However, when $g > 1$, there are at least $2g + 2$ Weierstrass points (see [3], page 43). As in [13], we assume that $C \in H_g$ has an Weierstrass point. In this paper, we consider a pointed hyperelliptic curve the pair (C, P). Thus, when $g = 1, (C, P)$ being hyperelliptic means that C is an elliptic curve with origin P. We denote the set of all hyperelliptic curves (C, P) over $\mathbb{F}$ of genus g by H_g.

Two curves in H_g are said to be isomorphic over $\mathbb{F}$ if they are isomorphic as projective varieties over $\mathbb{F}$. The relation of isomorphism over $\mathbb{F}$ is an equivalence relation on H_g.

It is known that if $(C_1, P), (C_2, P) \in H_g$ are isomorphic over $\mathbb{F}$, then their jacobian $J_{C_1}(\mathbb{F})$ and $J_{C_2}(\mathbb{F})$ are isomorphic [17]. But note that the converse is not true.

Next, we consider the notion of Weierstrass equation;

Definition 2.1. *A Weierstrass equation E over $\mathbb{F}$ of genus g is*

$$E/\mathbb{F} : y^2 + h(x)y = f(x),$$

where $h, f \in \mathbb{F}[x]$, $deg(h) \leq g$, $deg(f) = 2g + 1$, f is monic, and there are no singular points; a singular point on $E(x, y) = y^2 + h(x)y - f(x)$ is a solution $(x, y) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}}$ which satisfies $E(x, y), E_x(x, y)$ and $E_y(x, y)$. We denote the set of all Weierstrass equations of genus g over $\mathbb{F}$ by W_g.

The following proposition corresponds a Weierstrss equation to hyperelliptic pair (C, P).

Proposition 2.2. [13] *Let (C, P) be hyperelliptic over $\mathbb{F}$ with genus g. Then there exist nonconstant functions $x, y \in \mathbb{F}(C)$ with $x \in L(2P), y \in L((2g + 1)P)$, which satisfy a Weierstrass equation of genus g over $\mathbb{F}$. Moreover, such an equation is unique up to a change of coordinates of the form*

$$(x, y) \longrightarrow (\alpha^2 x + \beta, \alpha^{2g+1} y + t) \tag{2.1}$$

where $\alpha, \beta \in \mathbb{F}$ with $\alpha \neq 0$ and $t \in \mathbb{F}[x]$ with $deg(t) \leq g$.

Furthermore, a Weierstrass equation E arises from some (C, P) if and only if E has no singular points, and in this case the set of such E form an equivalence class of Weierstrass equations related by the transformations (2.1).

So, we can say that there is a 1-1 correspondence between isomorphism classes of curves in H_g and equivalence classes of Weierstrass equations in W_g, where $E, \bar{E} \in W_g$ are said to be equivalent over $\mathbb{F}$ if there exist such that the change of coordinates transforms (2.1) equation E to equation $\bar{E}$. Thus, it is enough to count the number of equivalence classes in W_g in order to count the number of isomorphism classes in H_g. In the remainder we call $E \in W_g$ a hyperelliptic curve and let isomorphism denote a change of coordinates of the above type.

3. **Isomorphism classes of hyperelliptic curves of genus** 3

In this section, we count the number of isomorphism classes of genus 3 hyperelliptic curves over $\mathbb{F}_q, q = p^n, p \neq 2, 7$ and list all the representatives of each isomorphism class. In this section, we let $q = p^n$.

Let H be a hyperelliptic curve of genus 3 defined over $\mathbb{F}_q$ given by a Weierstrass equation;

$$H : y^2 + h(x)y = f(x),$$

where $h(x)$ is a polynomial of degree ≤ 3, and $f(x)$ is a monic polynomial of degree $7, i.e.,$

$$h(x) = a_1x^3 + a_3x^2 + a_5x + a_7,$$

$$f(x) = x^7 + a_2x^6 + a_4x^5 + a_6x^4 + a_8x^3 + a_{10}x^2 + a_{12}x + a_{14},$$

with $a_i \in \mathbb{F}_q$.

The equation (3.1) defining a hyperelliptic curves H of genus 3 is unique up to a change of coordinates of the form

$$(x, y) \mapsto (\alpha^2 x + \beta, \alpha^7 y + t(x)), \tag{3.1}$$

where $\alpha \in \mathbb{F}_q^*$ and $t(x) \in \mathbb{F}_q[x]$ with $\deg t \leq 3$ (see [13]).

Proposition 3.1. *Every hyperellitic curve of genus 3 over $\mathbb{F}_q$ can be represented by an equation of the form*

$$y^2 = x^7 + a_4x^5 + a_6x^4 + a_8x^3 + a_{10}x^2 + a_{12}x + a_{14}.$$

If $H, \bar{H}$ be isomorphic curves of genus 3 defined over $\mathbb{F}_q$ given by the following equations

$$H : y^2 = x^7 + a_4x^5 + a_6x^4 + a_8x^3 + a_{10}x^2 + a_{12}x + a_{14},$$

$$\bar{H}: y^2 = x^7 + \bar{a_4}x^5 + \bar{a_6}x^4 + \bar{a_8}x^3 + \bar{a_{10}}x^2 + \bar{a_{12}}x + \bar{a_{14}},$$

then only admissible change of variables (3.2) *transforming* H *into* $\bar{H}$ *is*

$$(x, y) \mapsto (\alpha^2 x, \alpha^7 y), \quad \alpha \in \mathbb{F}_q^*.$$

This gives the following relations;

$$(3.2) \qquad \begin{cases} \alpha^4 \bar{a_4} = a_4 \\ \alpha^6 \bar{a_6} = a_6 \\ \alpha^8 \bar{a_8} = a_8 \\ \alpha^{10} \bar{a_{10}} = a_{10} \\ \alpha^{12} \bar{a_{12}} = a_{12} \\ \alpha^{14} \bar{a_{14}} = a_{14}. \end{cases}$$

(Proof) Letting $t(x) = -\frac{1}{2}h(x)$ and $\beta = -\frac{1}{7}a_2 - \frac{1}{28}a_1^2$, we obtain $\bar{a_i} = 0, i = 1, 2, 3, 5, 7$. If $a_i = \bar{a_i}, i = 1, 2, 3, 5, 7$, then $\beta = t(x) = 0$. □

3.1. **The number of singular equations.**

The Weierstrass equation $y^2 = f(x)$ over $\mathbb{F}_q$ is singular if and only if $f(x)$ has a multiple root in $\bar{\mathbb{F}}_q$. We denote $\Delta(f)$ is a discriminant of the polynomial $f(x)$.

Theorem 3.2. *Let*

$$\mathcal{V} = \{f(x) \in \mathbb{F}_q[x] | f(x) = x^7 + a_4x^5 + a_6x^4 + a_8x^3 + a_{10}x^2 + a_{12}x + a_{14}, \Delta(f) = 0\}.$$

Then $|\mathcal{V}| = q^5$.

(Proof) Suppose $f(x) \in \mathcal{V}$.
Then we have one of the following three factorizations of $f(x) \in \mathbb{F}_q[x]$;

$A = \{f(x) \mid \quad f(x) = (x - \alpha)^2(x^5 + 2\alpha x^4 + \beta x^3 + \gamma x^2 + \delta x + \epsilon),$
$\alpha, \beta, \gamma, \delta, \epsilon \in \mathbb{F}_q\}$

$B = \{f(x) \mid \quad f(x) = (x^2 + \alpha x + \beta)^2(x^3 - 2\alpha x^2 + \gamma x + \delta),$
$\alpha, \beta, \gamma, \delta \in \mathbb{F}_q, x^2 + \alpha x + \beta$ is irreducible over $\mathbb{F}_q[x]\}$

$C = \{f(x) | \quad f(x) = (x^3 + \alpha x^2 + \beta x + \gamma)^2(x - 2\alpha), \alpha, \beta, \gamma \in \mathbb{F}_q,$
$x^3 + \alpha x^2 + \beta x + \gamma$ is irreducible over $\mathbb{F}_q[x]\}$

Define a map

$$\varphi : \mathbb{F}_q^5 \longrightarrow \mathcal{V},$$

$$\varphi(\alpha,\beta,\gamma,\delta,\epsilon) = (x-\alpha)^2(x^5+2\alpha x^4+\beta x^3+\gamma x^2+\delta x+\epsilon).$$

Suppose $\alpha \neq \bar{\alpha}$ and $\varphi(\alpha,\beta,\gamma,\delta,\epsilon) = \varphi(\bar{\alpha},\bar{\beta},\bar{\gamma},\bar{\delta},\bar{\epsilon})$. That is $f(x) = \bar{f}(x)$, where

$$f(x) = (x-\alpha)^2(x^5+2\alpha x^4+\beta x^3+\gamma x^2+\delta x+\epsilon)$$

and

$$\bar{f}(x) = (x-\bar{\alpha})^2(x^5+2\bar{\alpha} x^4+\bar{\beta} x^3+\bar{\gamma} x^2+\bar{\delta} x+\bar{\epsilon}).$$

Then

$$f(x) = \bar{f}(x) = (x-\alpha)^2(x-\bar{\alpha})^2(x^3+2(\alpha+\bar{\alpha})x^2+\beta' x+\gamma')$$

for some $\beta',\gamma' \in \mathbb{F}_q$ and the above polynomial determined the non-ordered pairs $(\alpha,\bar{\alpha})$ such that $\alpha \neq \bar{\alpha}$ and $\beta',\gamma' \in \mathbb{F}_q$. Also if $\alpha,\bar{\alpha},\bar{\bar{\alpha}}$ are distinct and $\varphi(\alpha,\beta,\gamma,\delta,\epsilon) = \varphi(\bar{\alpha},\bar{\beta},\bar{\gamma},\bar{\delta},\bar{\epsilon}) = \varphi(\bar{\bar{\alpha}},\bar{\bar{\beta}},\bar{\bar{\gamma}},\bar{\bar{\delta}},\bar{\bar{\epsilon}})$, then

$$f(x) = \bar{f}(x) = \bar{\bar{f}}(x) = (x-\alpha)^2(x-\bar{\alpha})^2(x-\bar{\bar{\alpha}})^2(x+2(\alpha+\bar{\alpha}+\bar{\bar{\alpha}}))$$

and the above polynomial determined the non-ordered tuples $(\alpha,\bar{\alpha},\bar{\bar{\alpha}})$ such that $\alpha,\bar{\alpha},\bar{\bar{\alpha}}$ are pairwise distinct. So we have

$$|A| = q^5 - q^3(q-1)/2 + q(q-1)(q-2)/6.$$

We note that there are $\frac{1}{d}(q^d-q)$ many monic irreducible polynomial of degree d over $\mathbb{F}_q$ (see [12]), so we get

$$|B| = q^3(q-1)/2, \quad |C| = q^2(q-1)/3.$$

If $f(x) \in A \cap B$, then

$$f(x) = (x-\alpha)^2(x^2+\beta x+\gamma)^2(x+2\alpha-2\beta),$$

where $\alpha,\beta,\gamma \in \mathbb{F}_q$ and $x^2+\beta x+\gamma$ is irreducible. Therefore $|A\cap B| = \frac{1}{2}q^2(q-1)$. Since $B\cap C = C\cap A = \phi$, we get

$$\mathcal{V} = |A|+|B|+|C|-|A\cap B| = q^5.$$

$\square$

3.2. The number of isomorphism classes .

Let $\mathcal{H}$ be the set of hyperelliptic curves $H : y^2 = f(x)$ where $f(x) \in \mathbb{F}_q[x]$ is of the following form;

$$f(x) = x^7 + a_2x^6 + a_4x^5 + a_6x^4 + a_8x^3 + a_{10}x^2 + a_{12}x + a_{14}.$$

Let $\mathcal{H}_i, 1 \le i \le 5$ be the subsets in $\mathcal{H}$ defined as follows;

$$\begin{aligned}
\mathcal{H}_1 = &\ \{H \in \mathcal{H} | a_4 = a_6 = a_8 = a_{10} = a_{12} = 0, a_{14} \neq 0\} \\
\mathcal{H}_2 = &\ \{H \in \mathcal{H} | a_4 = a_6 = a_8 = a_{10} = a_{14} = 0, a_{12} \neq 0\} \\
\mathcal{H}_3 = &\ \{H \in \mathcal{H} | a_4 = a_8 = a_{10} = a_{14} = 0, a_6 \neq 0, a_{12} \neq 0\} \\
\mathcal{H}_4 = &\ \{H \in \mathcal{H} | a_6 = a_{10} = a_{14} = 0, a_4 \neq 0 \text{ or } a_8 \neq 0\} \\
\mathcal{H}_5 = &\ \mathcal{H} \backslash (\mathcal{H}_1 \cup \mathcal{H}_2 \cup \mathcal{H}_3 \cup \mathcal{H}_4).
\end{aligned}$$

Then $\mathcal{H}$ is the disjoint union of sets $\cup_{i=1}^5 \mathcal{H}_i$. We have $|\mathcal{H}_i|$ for each $1 \le i \le 5$ as the following lemma;

Lemma 3.3. $|\mathcal{H}_1| = |\mathcal{H}_2| = q - 1$, $|\mathcal{H}_3| = (q-1)(q-2)$, $|\mathcal{H}_4| = q(q-1)^2$, $|\mathcal{H}_5| = q^2(q-1)^2(q^2+q+1)$.

(Proof)

(1) Let $f(x) = x^7 + a_{14}$. Then the Weierstrass equation $y^2 = f(x)$ is nonsingular if and only if $a_{14} \neq 0$. So we have $|\mathcal{H}_1| = q - 1$.

(2) Let $f(x) = x^7 + a_{12}x$. Also the equation $y^2 = f(x)$ is nonsingular if and only if $a_{12} \neq 0$ and we get the desired result.

(3) Let $f(x) = x^7 + a_6x^4 + a_{12}x, a_6 \neq 0$ and $a_{12} \neq 0$. Then

$$\Delta(f) = 3^6 a_{12}^4 (a_6^2 - 4a_{12})^3.$$

Therefore the equation $y^2 = f(x)$ is singular if and only if $a_{12} = a_6^2/4$ and we obtain $|\mathcal{H}_3| = (q-1)^2 - (q-1) = (q-1)(q-2)$.

(4) Let $f(x) = x^7 + a_4x^5 + a_8x^3 + a_{12}x, a_4 \neq 0$ or $a_8 \neq 0$.
If $a_{12} = 0$, then $f(x)$ has a multiple root zero. Suppose $a_{12} \neq 0$.
If $f(x)$ can be factorized as

$$f(x) = (x-\alpha)^2(x^5 + 2\alpha x^4 + \beta x^3 + \gamma x^2 + \delta x + \epsilon), \alpha, \beta, \gamma, \delta, \epsilon \in \mathbb{F}_q,$$

then

$$\alpha \neq 0,\ \beta \neq \alpha^2,\ \gamma = 2\alpha\beta - 2\alpha^3,\ \delta = \alpha^2\beta - \alpha^4,$$

and

$$f(x) = x(x-\alpha)^2(x+\alpha)^2(x^2+\beta-\alpha^2).$$

There are $(q-1)^2/2$ many polynomials which have the above form. If $f(x)$ can be factorized as

$$f(x) = (x^2+\alpha x+\beta)^2(x^3-2\alpha x^2+\gamma x+\delta), \alpha, \beta, \gamma, \delta \in \mathbb{F}_q,$$

where $x^2+\alpha x+\beta$ is irreducible over $\mathbb{F}_q[x]$, then

$$\alpha = \delta = 0, \gamma \neq 0, \sqrt{\beta} \notin \mathbb{F}_q^*.$$

Also there are $(q-1)^2/2$ many polynomials which have the above form. One can check $f(x)$ cannot be factorized as

$$(x^3+\alpha x^2+\beta x+\gamma)^2(x-2\alpha), \alpha, \beta, \gamma \in \mathbb{F}_q$$

where $x^3+\alpha x^2+\beta x+\gamma$ is irreducible over $\mathbb{F}_q[x]$. Therefore we get

$$|\mathcal{H}_4| = (q-1)(q^2-1)-(q-1)^2 = q(q-1)^2.$$

(5) We have $|\mathcal{H}| = q^6-q^5$ from Theorem 3.2. So we obtain

$$|\mathcal{H}_5| = |\mathcal{H}| - \sum_{i=1}^{4}|\mathcal{H}_i| = q^2(q-1)^2(q^2+q+1).$$

□

Theorem 3.4. *The number of isomorphism classes of hyperelliptic curves of genus 3 over $\mathbb{F}_q, q = p^n, p \neq 2, 7$ is $2q^5 + r(q)$, where $r(q)$ is given in the following table;*

$r(q)$	$q \equiv 1 \pmod{12}$	$q \equiv 5 \pmod{12}$	$q \equiv 7 \pmod{12}$	$q \equiv 11 \pmod{12}$
$q \equiv 1 \pmod 7$	$2q^2+2q+14$	$2q^2-2q+14$	$4q+8$	12
$q \not\equiv 1 \pmod 7$	$2q^2+2q+2$	$2q^2-2q+2$	$4q-4$	0

(Proof)

Let A be the group of transforms of the form $(x, y) \to (\alpha^2 x, \alpha^7 y)$. Let A_i be the group of automorphisms of an arbitrary curve in each of the classes $\mathcal{H}_i$, with $i = 1, 2, 3, 4, 5$. From (3.2), we get the follows;

$A_1 = \{\alpha \in \mathbb{F}_q^* | \ \alpha^{14} = 1\}, A_2 = \{\alpha \in \mathbb{F}_q^* | \ \alpha^{12} = 1\}$,
$A_3 = \{\alpha \in \mathbb{F}_q^* | \ \alpha^{6} = 1\}, A_4 = \{\alpha \in \mathbb{F}_q^* | \ \alpha^{4} = 1\}$,
$A_5 = \{\alpha \in \mathbb{F}_q^* | \ \alpha^{2} = 1\}$.
And we have

$$|A_1| = \begin{cases} 14 & if \ \ q \equiv 1 \pmod 7 \\ 2 & if \ \ q \not\equiv 1 \pmod 7 \end{cases}$$

$$|A_2| = \begin{cases} 12 & if \ \ q \equiv 1 \pmod{12} \\ 6 & if \ \ q \not\equiv 1 \pmod{12}, q \equiv 1 \pmod 3 \\ 4 & if \ \ q \not\equiv 1 \pmod{12}, q \equiv 1 \pmod 4 \\ 2 & if \ \ q \not\equiv 1 \pmod 3, q \not\equiv 1 \pmod 4 \end{cases}$$

$$|A_3| = \begin{cases} 6 & if \ \ q \equiv 1 \pmod 3 \\ 2 & if \ \ q \not\equiv 1 \pmod 3 \end{cases}$$

$$|A_4| = \begin{cases} 4 & if \ \ q \equiv 1 \pmod 4 \\ 2 & if \ \ q \not\equiv 1 \pmod 4 \end{cases}$$

$|A_5| = 2$.

$$|\mathcal{H}/A| = \sum_{i=1}^{5} |\mathcal{H}_i/A|$$

$$= |A_1| + |A_2| + |A_3|(q-2) + |A_4| \ q(q-1) + 2q^5 - 2q^2.$$

Then we get the desired result. □

References

[1] L. M. Adleman, *A subexponential algorithm for the discrete logarithm problem with applications to cryptography* , Proc. 20th IEEE Found. Comp. Sci. Symp., 55-60, 1979.

[2] L. Adleman, J. Demarrais and M.Huang, A *subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians fo large genus hyperelliptic curves over finite fields*, Algorithmic Number Theory, LNCS 877(1994), 28-40, Springer-Verlag, Berlin.

[3] E. Arabello, et al., *Geometry of algebraic curves*, Grundlehren Math. Wiss. 267, Springer-Verlag, New York, 1985.

[4] Y. Choie and E. Jeong, *The exact number of isomorphism classes of hyperelliptic curves of genus 2 over* $\mathbb{F}_{2^n}$, submitted (2003).

[5] Y. Choie and D. Yun, *Isomosrphism classes of hyperelliptic curves of genus 2 over* F_q ACISP'02,pp.190-202 (2002) LNCS, Springer Verlag.

[6] L. H. Encinas and J. M. Masqué, *Isomorphism classes of hyperelliptic curves of genus 2 in characteristic 5*, www.cacr.math.waterloo.ca/ technical reports COOR 2002-07.

[7] L.H. Encinas, A.J. Menezes, and J.M. Masqué, *Isomorphism classes of genus-2 hyperelliptic curves over finite fields* , Applicable Algebra in Engineering, Communication and Computing, Volume 13 Issue 1 (2002) pp 57-65.

[8] G.Frey and H.-G. Rúck, *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves*, Math. Comp., 62, 865-874, 1994.

[9] P. Gaudry, *A variant of the Adleman-DeMarrais-Huang algorithm and its application to small genera* , In Advances in Cryptology, EUROCRYPT 2000, Springer-Verlag LNCS 1807, 19-34, 2000.

[10] N. Koblitz, *Elliptic curve cryptosystems*, Math. of Comp. vol 48, 203-209, 1987.

[11] N. Koblitz, *Hyperelliptic cryptosystems*, J. Crypto., 1,139-150, 203-209, 1989.

[12] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Math. and its application, Vol. 20, Cambridge University Press, 1984.

[13] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. 342, 2, 729-752, 1994.

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

[15] A. Menezes and N. Koblitz, *Elliptic curve public key cryptosystems* , Kluwer Academic Publishers, 1993.

[16] V. Miller, *Uses of elliptic curves in cryptography* , Advances in cryptology - Crypto '85, LNCS 218, 417-426, 1986.

[17] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.