Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ON THE NUMBER OF ISOMORPHISM CLASSES OF JACOBI QUARTIC CURVES OVER A FINITE FIELD

[1]HONGFENG WU, [2]LI ZHU
[1]College of Sciences, North China University of Technology, Beijing 100144, China
[2]College of Sciences, North China University of Technology, Beijing 100144, China
E-mail: whfmath@gmail.com

ABSTRACT

Isomorphic elliptic curves are the same in the point of cryptographic view. Recent research activity has focused on counting distinct elliptic curves over finite field (up to isomorphism over the algebraic closure of the ground field or ground field) in various curves families. Jacobi quartic curve is an important curve family for elliptic curve cryptography. This paper presents explicit formulas for the number of isomorphism classes (up to isomorphism over ground field) of Jacobi quartic curves and generalized Jacobi quartic curves defined over finite fields. These results also can be used in the elliptic curve cryptography and classification problems.

Keywords: *Elliptic Curve, Jacobi Quartic Curve, Isomorphism Classes, Cryptography, Finite Field*

1. INTRODUCTION

Elliptic curves were independently introduced to cryptography in 1985 by Victor Miller [1] and Neal Koblitz [2]. Elliptic curve cryptography (ECC) is an efficient public key cryptosystem which rely on the difficulty of discrete logarithmic problem on elliptic curves. The one of advantages of ECC is that for suitably chosen curves there is no known subexponential algorithm like the number field sieve algorithm for integer factorization, to solve the elliptic curve discrete logarithm problem. Consequently, this leads to smaller key length in ECC to achieve the same level of security as in public key systems based on factorization and the discrete logarithm problem in finite fields. Hence elliptic curves are widely applied in many aspects of cryptography including elliptic curve based protocols, data encryption and digit signature. In particular, Weil pairing and Tate pairing on elliptic curves can be utilized in identity based encryption [3]. Further, elliptic curves can be applied in prime testing [4-5] and factoring integers [6].

Efficient elliptic curve arithmetic is crucial for ECC. The most expensive part is the computation of kP for an integer k and a point P on the curve. For an elliptic curves in Weierstrass form, the formulas of adding two distinct points and doubling a point are different, which makes ECC vulnerable to side channel analysis. One countermeasure protecting against these attacks is use a coordinate system that allows point additions and doublings to be performed with the same formulas. Namely, addition formulas are said to be unified if they also allow doubling of non-zero points, and complete if the allow addition of any pair of points, identical or not, zero or not. Hence it is preferable to find elliptic curves in other form with unified addition formula [7-12].

The Jacobi quartic curves is one of the most important curves in cryptography. Jacobi quartic curves, with equation $y^2 = x^4 + 2ax^2 + 1$, are unified [7-8] and have an addition formula costs 7M+3S [9-10]. Not all elliptic curves transform to the Jacobi quartic forms. Such curves were first proposed by Chudnovsky and Chudnovsky [8] in 1986. After that, Billet and Joye [7], Duquesne [9], Hisil et al. [13] gave more improvements for the arithmetic on Jacobi quartic curves.

In order to study the elliptic curves cryptosystem, we first need to answer how many curves there are up to isomorphism, because two isomorphic elliptic curves are the same in the point of cryptographic view. So it is natural to count the isomorphism classes of some kinds of elliptic curves. Recent research activity has focused on counting distinct elliptic curves over finite field (up to isomorphism over the algebraic closure of the ground field) in various families using explicit computation of the j-invariant, for example in the families of Doche-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Icart-Kohel and Edwards [14], Jacobi quartic curves [15]. We note that counting the number distinct elliptic curves over finite fields F_q, up to isomorphism over F_q, is a natural question which has cryptographic interests. This has been done for Weierstrass curves [16-17], Hessian curves [18] and 3-torstion curves [19], Legendre curves [20], Edwards and twisted Edwards curves [21], and Huff curves [12], et al. In this paper, we give the explicit formulas for the number of isomorphism classes of Jacobi quartic curves and generalized Jacobi quartic curves over a finite field, up to isomorphism over finite field F_q.

2. PRELIMINARIES

A curve means a projective variety of dimension one. There are several ways to define elliptic curves. In this paper, an irreducible curve is said to be an elliptic curve if it is birationally equivalent to a non-singular plane cubic curve.

It is well-known that every elliptic curve E over a field K can be written as a Weierstrass equation $E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ with coefficients $a_1, a_2, a_3, a_4, a_6 \in K$. Two projective varieties V_1 and V_2 are isomorphic if there exist morphisms $\varphi: V_1 \to V_2$ and $\phi: V_2 \to V_1$, such that $\phi \circ \varphi$ and $\varphi \circ \phi$ are the identity maps. Two elliptic curves are said to be isomorphic if they are isomorphic as projective varieties. Assume that the characteristic of field is different from 2 and 3, Let $E_1: Y^2 = X^3 + a_2X^2 + a_4X + a_6$ and $E_2: Y^2 = X^3 + a_2'X^2 + a_4'X + a_6'$ be two elliptic curves defined over K. It is known that E_1 and E_2 are isomorphic over $\overline{K}$ if and only if $j(E_1) = j(E_2)$, where $\overline{K}$ is the algebraic closure of K. E_1 and E_2 are isomorphic over K if and only if there exist $u, r \in K$ and $u \neq 0$ such that the change of variables $(X, Y) \to (u^2X + r, u^3Y)$ maps the equation of E_1 to the equation of E_2 [23]. Hence, E_1 and E_2 are isomorphic over K if and only if there exist $u, r \in K$ and $u \neq 0$ such that

$$\begin{cases} u^2a_2' = a_2 + 3r, \\ u^4a_4' = a_4 + 2ra_2 + 3r^2, \\ u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3. \end{cases} \quad (1)$$

It is well known [17] that the number of elliptic curves which are F_q-isomorphic to a given curve $y^2 = x^3 + ax + b$ equals to

$$\begin{cases} \frac{q-1}{6}, & a = 0, q \equiv 1 \bmod 3 \\ \frac{q-1}{4}, & b = 0, q \equiv 1 \bmod 4 \\ \frac{q-1}{2}, & others. \end{cases} \quad (2)$$

For the remainder of the paper, we assume that the characteristic of F_q is greater than 3.

3. ENUMERATION JACOBI QUARTIC CURVES

Let $E_a: y^2 = x^4 + 2ax^2 + 1$ ($a^2 \neq 1$) be a Jacobi quartic curve defined over a finite field F_q with characteristic of F_q is greater than 3. Note that the j-invariant of E_a is $16(a^2+12)^3/(a^2-4)^2$. Recall the Legendre elliptic curve are of the form $y^2 = x(x-1)(x-\lambda)$. We have the following lemma:

Lemma 3.1. The curve $E_a: y^2 = x^4 + 2ax^2 + 1$ is birationally equivalent to the Legendre elliptic curve $L_{(1-a)/2}: v^2 = u(u-1)\left(u-(1-a)/2\right)$ via the change of variables $\phi(x, y) = (u, v)$, where $u = (x^2 - y + 1)/2, v = x(x^2 - y + a)/2$. The inverse change is $\psi(u, v) = (x, y)$ where $x = 2v/(2u + a - 1), y = x^2 - 2u + 1$.

Proof To prove E_a is isomorphic to Legendre curve $L_{(1-a)/2}: v^2 = u(u-1)\left(u-(1-a)/2\right)$, it is sufficient to prove $2v^2 = u(u-1)(2u-(1-a))$. Since $2u - (1-a) = x^2 - y + a$ and $64v^2 = 4x^2(2x^2 - 2y + 2a)^2$, it is sufficient to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

show that $x^2(x^2-y+a)=2u(u-1)$. The result then follows immediately from

$x^2(x^2-y+a)=x^4-x^2y+ax^2$ and

$4u(u-1)=(x^2-y+1)(x^2-y-1)$
$=2x^4-2x^2y+2ax^2$,

which complete the proof.

By the above theorem, the family of Jacobi quartic curves is the same as the family of Legendre curves in the sense of isomorphism. Hence, by the Theorem 6 of [20], we get the following theorem:

Theorem 3.2: Suppose F_q is the finite field with q elements and char(F_q) > 3. Let N_q be the number of F_q -isomorphism classes of Jacobi quartic curves $E_a: y^2=x^4+2ax^2+1$ defined over F_q with $a^2\neq 1$. Then

$$N_q=\begin{cases}\dfrac{7q+17}{24}, & if\ q\equiv 1 \bmod 24\\ \dfrac{7q+13}{24}, & if\ q\equiv 5 \bmod 24\\ \dfrac{q+2}{3}, & if\ q\equiv 7,19 \bmod 24\\ \dfrac{q-2}{3}, & if\ q\equiv 11,13 \bmod 24\\ \dfrac{7q+29}{24}, & if\ q\equiv 13 \bmod 24\\ \dfrac{7q+1}{24}, & if\ q\equiv 17 \bmod 24\end{cases}$$

4. ENUMERATION FOR GENERALIZED JACOBI QUARTIC CURVES

In this section, we consider the generalized Jacobi quartic curve. The generalized Jacobi quartic curve is the curve form $E_{a,b}: y^2=x^4+ax^2+b$ with $(a^2-b)b\neq 0$ defined over F_q of characteristic >3. A Jacobi quartic curve is a special one of $E_{a,b}$ with $b=1$. The j-invariant of $E_{a,b}$ is $j=64(a^2+3b)^3/(b(a^2-b)^2)$. The following lemma can be proved by a direct computation similar as that in *Lemma 3.1*.

Lemma 4.1. The generalized Jacobi quartic curve $E_{a,b}: y^2=x^4+ax^2+b$ is birationally equivalent to the curve $W_{a,b}: v^2=u(u^2-4au+4a^2-4b)$ via the change of variables $u=2x^2-2y+2a$ and $v=4x(x^2-y+a)$.

Note that when a,b run over the finite field F_q, $-4a$ and $4a^2-4b$ run over the finite field, too. Hence, the family of generalized Jacobi quartic curves is the same as the family of elliptic curves with at least a 2-order point in the sense of isomorphism.

For the elliptic curve $E_{a,b}$, The j-invariant $j(E_{a,b})=0$ if and only if $a^2+3b=0$. Moreover, we have the following proposition. Since $E_{a,b}$ is birationally equivalent to the Weierstrass elliptic curve $W_{a,b}: y^2=x^3-4ax^2+(4a^2-4b)x$, and $W_{a,b}$ is isomorphic to the short form Weierstrass curve $S_{a,b}: y^2=x^3+(-8a-\frac{4a^2}{3})x+(\frac{16a^3}{27}-\frac{16ab}{3})$. It is clear that the j-invariant of $S_{a,b}$ is equal to 1728 if and only if $\frac{16a^3}{27}-\frac{16ab}{3}=0$, that is $a(a^2-9b)=0$. Thus $j(E_{a,b})=1728$ if and only if $a(a^2-9b)=0$.

Lemma 4.2. Let $E_{a,b}: y^2=x^4+ax^2+b$ be a generalized Jacobi quartic curves defined over a finite field F_q with $b(a^2-b)\neq 0$. Let N be the number of generalized Jacobi quartic curves form $E_{a,b}$ with $j\neq 0,1728$. If b is a square element, then $N=\begin{cases}(q-1)(q-7)/2, if\ q\equiv 1,7 \bmod 12,\\ (q-1)(q-5)/2, if\ q\equiv 5,11 \bmod 12,\end{cases}$

If b is a non-square element, then

$$N=\begin{cases}(q-1)^2/2, & if\ q\equiv 1,7 \bmod 12,\\ (q-1)(q-3)/2, & if\ q\equiv 5,11 \bmod 12.\end{cases}$$

Proof Assume first that b is a square in F_q. Then the equation $a^2-b=0$ has two roots in finite field. Hence the number of curves of the form $E_{a,b}$ over F_q is $(q-1)(q-2)/2$. Since $j(E_{a,b})=0$ if and ony if $a^2+3b=0$, and $a^2+3b=0$ has two roots

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in F_q when $q \equiv 1,7 \pmod{12}$, but it has no root when $q \equiv 5,11 \pmod{12}$. Hence, the number of curves of the form $E_{a,b}$ over F_q with $j=0$ is $2 \cdot \frac{q-1}{2} = q-1$ when $q \equiv 1,7 \pmod{12}$, and is 0 when $q \equiv 5,11 \pmod{12}$. If $j(E_{a,b}) = 1728$, then $a=0$ or $a^2 = 9b$. Thus the number of curves form $E_{a,b}$ with $j(E_{a,b}) = 1728$ is $\frac{q-1}{2} + \frac{q-1}{2} \cdot 2 = \frac{3(q-1)}{2}$. By subtraction, when $q \equiv 1,7 \pmod{12}$, we get that

$$N = \frac{(q-1)(q-2)}{2} - (q-1) - \frac{3(q-1)}{2} = \frac{(q-1)(q-7)}{2},$$

and when $q \equiv 5,11 \pmod{12}$, we get

$$N = (q-1)(q-2)/2 - 0 - 3(q-1)/2 = (q-1)(q-5)/2 .$$

Secondly, assume that b is a non-square element Then the number of generalized Jacobi quartic curves form $E_{a,b}$ is $q(q-1)/2$. For this case, the number of curves of the form $E_{a,b}$ over F_q with $j=0$ is $q-1$ when $q \equiv 5,11 \pmod{12}$, and is 0 when $q \equiv 1,7 \pmod{12}$. And the number of curves form $E_{a,b}$ with $j(E_{a,b}) = 1728$ is $(q-1)/2$. By subtraction, when $q \equiv 1,7 \pmod{12}$, we get that $N = \frac{q(q-1)}{2} - \frac{(q-1)}{2} = \frac{(q-1)^2}{2}$, and when $q \equiv 5,11 \pmod{12}$, we get

$$N = q(q-1)/2 - (q-1) - (q-1)/2 = (q-1)(q-3)/2 .$$

This complete the proof of the lemma.

Let N_0 and N_{1728} be the number of generalized Jacobi quartic curves form $E_{a,b}$ with $j=0$ and $j=1728$. If b is a square element, then

$$N_0 = \begin{cases} q-1, & q \equiv 1,7 \bmod 12, \\ 0, & q \equiv 5,11 \bmod 12. \end{cases}$$

and $N_{1728} = 3(q-1)/2$. If b is a non-square element, then

$$N_0 = \begin{cases} 0, & q \equiv 1,7 \bmod 12, \\ q-1, & q \equiv 5,11 \bmod 12. \end{cases}$$

and $N_{1728} = (q-1)/2$.

By the Lemma 4.1, curve $E_{a,b} : y^2 = x^4 + ax^2 + b$ is birationally equivalent to the Weierstrass elliptic curve $W_{a,b} : v^2 = u(u^2 - 4au + 4a^2 - 4b)$. It is clear that $W_{a,b}$ has at least a 2-order point. Furthermore, if b is a square in F_q, then $W_{a,b}$ has three 2-order points $(0,0)$, $(2a + 2\sqrt{b}, 0)$ and $(2a - 2\sqrt{b}, 0)$.

Therefore, the generalized Jacobi quartic $E_{a,b}$ has three points of order 2 if and only if b is a square in F_q. The generalized Jacobi quartic $E_{a,b}$ has only a point of order 2 if and only if b is a non-square in F_q.

By the Lemma 4.1, the Weierstrass curve $W_{a,b}$ is isomorphic to the short Weierstrass elliptic curve $S_{a,b} : y^2 = x^3 - (8a + \frac{4a^2}{3})x + 16(\frac{a^3 - 9ab}{27})$. Every point of order 2 admits such a change, By the formula (2), we can get the number N of elliptic curves which are F_q-isomorphic to a given generalized Jacobi quartic curve $y^2 = x^4 + 2ax + b$ equals to

$$N_{ns} = \begin{cases} \frac{q-1}{6}, & \text{if } j = 0 \text{ and } q \equiv 1 \bmod 3, \\ \frac{q-1}{4}, & \text{if } j = 1728 \text{ and } q \equiv 1 \bmod 4, \\ \frac{q-1}{2}, & \text{others.} \end{cases}$$

when b is a non-square element in finite field F_q. If b is a square element in finite field F_q, then $E_{a,b}$ has three order 2 points, the number of elliptic curves which is F_q-isomorphic to $E_{a,b}$ equals to

$$N_s = \begin{cases} \frac{q-1}{2}, & \text{if } j = 0 \text{ and } q \equiv 1 \bmod 3, \\ \frac{3(q-1)}{4}, & \text{if } j = 1728 \text{ and } q \equiv 1 \bmod 4, \\ \frac{3(q-1)}{2}, & \text{others.} \end{cases}$$

By the argument of above and Lemma 4.2, for the generalized Jacobi quartic curve form the $E_{a,b}$ with b is a non-square element in finite field F_q, let N_{sq} be the number of F_q-isomorphism classes. Then if $q \equiv 1 \bmod 12$, we can get

Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$N_{nq} = 0 + \frac{(q-1)/2}{(q-1)/4} + \frac{(q-1)^2/2}{(q-1)/2} = q+1.$$

If $q \equiv 5 \bmod 12$, then

$$N_{nq} = \frac{(q-1)}{(q-1)/2} + \frac{(q-1)/2}{(q-1)/4} + \frac{(q-1)(q-3)/2}{(q-1)/2}$$
$$= q+1.$$

If $q \equiv 7 \bmod 12$, then

$$N_{nq} = 0 + \frac{(q-1)/2}{(q-1)/2} + \frac{(q-1)^2/2}{(q-1)/2} = q.$$

If $q \equiv 11 \bmod 12$, then

$$N_{nq} = \frac{(q-1)}{(q-1)/2} + \frac{(q-1)/2}{(q-1)/2} + \frac{(q-1)(q-3)/2}{(q-1)/2} = q.$$

Therefore, we can get the following theorem:

Theorem 4.3: Suppose F_q is the finite field with q elements and char(F_q) > 3. Let N_{nq} be the number of F_q -isomorphism classes of Jacobi quartic curves $E_{a,b} : y^2 = x^4 + 2ax^2 + b$ defined over F_q with b is a non-square element in finite field and $b(a^2 - b) \neq 0$. Then

$$N_{nq} = \begin{cases} q+1, & if\ q \equiv 1,5 \bmod 12, \\ q, & if\ q \equiv 7,11 \bmod 12. \end{cases}$$

Similarly, if b is a square element in finite field F_q, let N_{sq} be the number of F_q -isomorphism classes. Then if $q \equiv 1 \bmod 12$, we can get

$$N_{sq} = \frac{q-1}{(q-1)/2} + \frac{3(q-1)/2}{3(q-1)/4} + \frac{(q-1)(q-7)/2}{3(q-1)/2}.$$
$$= \frac{q+5}{3}$$

If $q \equiv 5 \bmod 12$, then

$$N_{sq} = 0 + \frac{3(q-1)/2}{3(q-1)/4} + \frac{(q-1)(q-5)/2}{3(q-1)/2}$$
$$= \frac{q+1}{3}$$

If $q \equiv 7 \bmod 12$, then

$$N_{sq} = \frac{q-1}{(q-1)/2} + \frac{3(q-1)/2}{3(q-1)/2} + \frac{(q-1)(q-7)/2}{3(q-1)/2}$$
$$= \frac{q+2}{3}$$

If $q \equiv 11 \bmod 12$, then

$$N_{sq} = 0 + \frac{3(q-1)/2}{3(q-1)/2} + \frac{(q-1)(q-5)/2}{3(q-1)/2}$$
$$= \frac{q-2}{3}$$

Therefore, we can get the following theorem:

Theorem 4.4: Suppose F_q is the finite field with q elements and char(F_q) > 3. Let N_{nq} be the number of F_q -isomorphism classes of Jacobi quartic curves $E_{a,b} : y^2 = x^4 + 2ax^2 + b$ defined over F_q with b is a square element in finite field and $b(a^2 - b) \neq 0$. Then

$$N_{sq} = \begin{cases} \frac{q+5}{3}, & if\ q \equiv 1 \bmod 12, \\ \frac{q+1}{3}, & if\ q \equiv 5 \bmod 12, \\ \frac{q+2}{3}, & if\ q \equiv 7 \bmod 12, \\ \frac{q-2}{3}, & if\ q \equiv 11 \bmod 12. \end{cases}$$

Summing up the numbers in Theorems 4.3 and 4.4, we get the number of isomorphism classes of generalized Jacobi quartic curves in the following theorem.

Theorem 4.5: Suppose F_q is the finite field with q elements and char(F_q) > 3. Let N_q be the number of F_q -isomorphism classes of Jacobi quartic curves $E_{a,b} : y^2 = x^4 + 2ax^2 + b$ defined over F_q with $b(a^2 - b) \neq 0$. Then

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$N_q = \begin{cases} \dfrac{4q+8}{3}, & if\ q \equiv 1 \bmod 12, \\ \dfrac{4q+4}{3}, & if\ q \equiv 5 \bmod 12, \\ \dfrac{4q+2}{3}, & if\ q \equiv 7 \bmod 12, \\ \dfrac{4q-2}{3}, & if\ q \equiv 11 \bmod 12. \end{cases}$$

5. CONCLUSIONS

In this work we answered a question posed in [14]. That is, we presented the explicit formulas for the number of F_q isomorphism classes of Jacobi quartic curves and generalized Jacobi quartic curves over a finite field F_q. A natural and related question is to find a formula for the number of distinct isogeny classes for a given family of elliptic curves. It is an open problem to find explicit formulas for most families of curves, such as twisted Edwards curves and Huff's curves, etc.

ACKNOWLEDGEMENS

This work was supported by National Natural Science Foundation of China (No. 11101002) and Beijing Natural Science Foundation (No. 1132009).

REFRENCES:

[1] V. S. Miller, "Uses of Elliptic Curves in Cryptography", *Proceedings of Advances in cryptology (CRYPTO '85)*, Vol. 218 of Lecture Notes in Computer Science, Springer-Verlag, 1985, pp. 417-426.

[2] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, Vol. 48, No. 177, 1987, pp. 203-209.

[3] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil pairing", *SIAM J. of Computing*, Vol. 32, No. 3, 2003, pp. 586-615.

[4] A. O. L. Atkin and F. Morain, "Elliptic curves and primality proving", *Math. Comp.*, Vol. 61, No. 203,1993, pp. 29- 68.

[5] S. Goldwasser and J. Kilian, "Primality testing using elliptic curves", *J. ACM*, Vol.46, No. 4, 1999, pp. 450-472.

[6] H. W. Lenstra Jr., "Factoring integers with elliptic curves", *Annals of Mathematics*, Vol. 126 1987, pp. 649-673.

[7] O. Billet and M. Joye, "The Jacobi model of an elliptic curve and side-channel analysis", *Proceedings AAECC 2003*, Vol. 2643 of Lecture Notes in Computer Science, Springer-Verlag, 2003, pp. 34-42.

[8] D.V. Chudnovsky and D.V. Chudnovsky, "Sequences of numbers generated by addition in formal groups and new primality and factorization tests", *Advances in Applied Mathematics 7*, 1986, pp. 385-434.

[9] S. Duquesne, "Improving the arithmetic of elliptic curves in the Jacobi model", *Information Processing Letters*, Vol. 104, No. 3, 2007, pp. 101-105.

[10] D. J. Bernstein and T. Lange, "Faster addition and doubling on elliptic curves", *Proceedings of Advances in Cryptology-ASIACRYPT 2007*, Springer-Verlag, 2007, 29-50.

[11] D. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, "Twisted Edwards Curves", *Proceedings of Cryptology–AFRICACRYPT 2008*, Springer-Verlag, 2008, pp. 389–405.

[12] H. Wu and R. Feng, "Elliptic curves in Huff's model"， *Wuhan University Journal of Natural Sciences*， Vol. 17, NO. 6, 2012, pp. 473-480.

[13] H. Hisil, G.Carter and E. Dawson, "New formulae for efficient elliptic curve arithmetic", *Proceedings INDOCRYPT 2007*, Springer-Verlag, 2007, pp. 138-151.

[14] R.Farashahi and I. Shparlinski, "On the number of distinct elliptic curves in some families", *Des. Codes Cryptogr*, Vol. 54, 2010, pp. 83—99.

[15] H. Wu, R. Feng, "Isomorphism Classes of Jacobi Quartic Curve over Finite Fields", *Proceedings of Information Technology Convergence, Secure and Trust Computing, and Data Management*, 2012, pp. 145-153.

[16] R. Schoof., "Nonsigular plane cubic curves over finite field", *J. Combine, Theory Ser. A*, Vol. 46, 1987, pp. 183-211.

[17] A.J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

[18] R. Farashahi, M. Joye, "Efficient Arithmetic on Hessian Curves", *Proceedings of International Conference on Practice and Theory in Public Key Cryptography 2010*, Springer-Verlag, 2010, pp. 243-260.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[19] D. Moody H. Wu, “Families of elliptic curves with rational 3-torsion”, *Journal of Mathematical Cryptology*, Vol. 5, No 3-4, January 2012, pp. 225–246.

[20] H. Wu and R. Feng, “On the isomorphism classes of Legendre elliptic curves over finite fields”, *Sci. China Math.*, Vol. 54, No. 9, 2011, pp. 1885-1890.

[21] R. Farashahi, D. Moody and H. Wu. “Isomorphism classes of Edwards and twisted Edwards curves over finite fields”, *Finite Fields and Their Applications*, Vol. 18, No. 3, 2012, pp. 597-612.

[22] Silverman J.H.. The Arithmetic of Elliptic Curves, Springer, New York,1986.