Asian Journal of Mathematics and Computer Research

Volume 31, Issue 2, Page 80-86, 2024; Article no.AJOMCOR.12065
ISSN: 2395-4205 (P), ISSN: 2395-4213 (O)

Analysis of Isomorphism Classes of a Family of Elliptic Curves Over Finite Fields

Zhao Wei [a*]

[a] *College of Science, North China University of Technology, Beijing 100144, P. R. China.*

Author's contribution

The sole author designed, analyzed, interpreted and prepared the manuscript.

Article Information

DOI: 10.56557/AJOMCOR/2024/v31i28672

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://prh.ikprress.org/review-history/12065

Original Research Article

Received: 23/02/2024
Accepted: 26/04/2024
Published: 29/04/2024

Abstract

Doche et al. constructed a family of elliptic curves (DIK elliptic curves) and proposed more efficient tripling formulas leading to a fast scalar multiplication algorithm. In this paper we present a direct method to compute the number of $\bar{\mathbb{F}}_q$-isomorphism classes (isomorphism over $\bar{\mathbb{F}}_q$) and $\mathbb{F}_q$isomorphism classes of DIK family of elliptic curves defined over a finite field $\mathbb{F}_q$. We give the explicit formulae for the number of $\bar{\mathbb{F}}_q$-isomorphism and an estimate formulae for the number of isomorphism classes. These result can be used in the elliptic curve cryptosystems.

Keywords: Elliptic curves; isomorphism classes; cryptography.

1 Introduction

Elliptic curve cryptosystems were proposed by Miller (1986) and by Koblitz (1987) which relies on "the difficulty of elliptic curve discrete logarithmic problem". "The basic operation required to implement the system is point multiplication, that is the computation of kP for a large K and a point P on elliptic curves. To obtain

**Corresponding author: Email: mathcurve@163.com;*

faster operations, much effort has been done in representing the elliptic curves in special forms which provide faster addition, doubling and tripling in the last decades" [1]. In 2006, Doche, Icart and Kohel [2] introduced "the faster tripling in Weierstrass form curves $y^2 = x^3 + 3u(x+1)^2$". In 2008, study the general curves $y^2 = x^3 + 3a(x+t)^2$. Seeing for comparison analysis of computational cost for all kinds of curves. It is natural to count the isomorphism classes of these elliptic curves over a finite field $\mathbb{F}_q$ which has cryptographic applications. This has been done for Weierstrass curves [3,4], the numbers of distinct Edwards curves and their variants are presented in [5], Edwards curves [6], elliptic curves with rational 3-torsion [7], Legendre curves [8]. The isomorphism classes of different curve models were first studied in [5]. In [9], Farashahi and Hosseini give explicit formulas for" the number of distinct elliptic curves over a finite field, up to isomorphism, in two families of curves introduced by C. Doche, T. Icart and D.R. Kohel. But their papers use more mathematical theory, in our paper we take a more direct approach, which looks as if it is easier for people to understand".

In this paper we present a direct method to compute the number of $\bar{\mathbb{F}}_q$-isomorphism classes (isomorphism over $\bar{\mathbb{F}}_q$) and isomorphism classes of Doche-Icart-Kohel curves defined over a finite field $\mathbb{F}_q$. We give the explicit formulae for the number of $\bar{\mathbb{F}}_q$-isomorphism and an estimate formulae for the number of isomorphism classes. These result can be used in the elliptic curve cryptosystems.

The rest of this paper is organized as follows. In section 2 we give some basic notation about elliptic curves and isomorphism. In section 3 we counting $\bar{\mathbb{F}}_q$-isomorphism classes of Doche-Icart-Kohel curves defined over a finite field. And finally, we counting isomorphism classes of Doche-Icart-Kohel curves defined over a finite field. Throughout the paper, $\mathbb{F}_q$ denotes a finite field with characteristic > 3 and denote its algebraic closure by $\bar{\mathbb{F}}_q$.

2 Elliptic Curve

A curve means a projective variety of dimension 1. An irreducible curve is said to be elliptic curve if it is birationally equivalent to a plane non-singular cubic curve.

We know every elliptic curve E/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 $a_1, a_2, a_3, a_4, a_6 \in K$. The discriminant $\triangle(E)$ and j-invariant are defined as

$$\triangle(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

And

$$j(E) = (b_2^2 - 24b_4)^3/\triangle(E),$$

where;

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2. \end{aligned}$$

Let $E_1/K: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ and $E_2/K: Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6'$ be two elliptic curves defined over K, we call them are isomorphism over $\bar{K}$ or $\bar{K}$-isomorphism if there is an isomorphism which is defined over $\bar{K}$. We call them are isomorphism over K or K-isomorphism if there is an isomorphism which is defined over K. It is well known that E_1 and E_2 are isomorphism over $\bar{K}$ if and only if $j(E_1) = j(E_2)$, where $\bar{K}$ is the algebraic closure of K. However, E_1 and E_2 are isomorphism over K if and only if there exists $u, r, s, t \in K$ and $u \neq 0$ such that the change of variables

$$(X, Y) \rightarrow (u^2X + r, u^3Y + u^2sX + t)$$

equation E_1 to equation E_2. The relationship of isomorphism is an equivalence relation. The above change of variables is said to be admissible change of variables. Therefore, E_1 and E_2 are isomorphism over K if and only if there exists $u, r, s, t \in K$ and $u \neq 0$ such that

$$\begin{aligned} ua_1' &= a_1 + 2s, \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\ u^3a_3' &= a_3 + ra_1 + 2t, \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned}$$

If $a_1 = a_3 = a_1' = a_3' = 0$, then E_1 and E_2 are isomorphism over K if and only if there exists $u, r, s, t \in K$ and $u \neq 0$ such that

$$\begin{aligned} u^2a_2' &= a_2 + 3r, \\ u^4a_4' &= a_4 + 2ra_2 + 3r^2, \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3. \end{aligned}$$

See [10,11,12] for more details.

For two elliptic curves E_1 and E_2 which are defined over finite field $\mathbb{F}_q$, if $j(E_1) = j(E_2)$, then we call them are $\bar{\mathbb{F}}_q$-isomorphism. Some formulae about counting the number of the isomorphism classes of general elliptic curves over a finite field can be found in literatures. In , R. Schoof present the number of isomorphism classes of elliptic curves over a finite field $\mathbb{F}_q$ is $2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right)$, where $\left(\frac{n}{q}\right)$ is Jacobi Symbol. In , A.J. Menezes present the number of isomorphism classes of elliptic curves forms $y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_q$ is $2q + 6, 2q + 2, 2q + 4, 2q$ for $q \equiv 1,5,7,11$ (mod 12) respectively. The following definition from [1].

Definition 1. A Doche-Icart-Kohel curves over a finite field $\mathrm{F_q}$ is defined by $\mathrm{E_a}$: $\mathrm{y^2 = x^3 + 3a(x + 1)^2}$ where $\mathrm{a \in F_q}$ with $\mathrm{a\left(a - \frac{9}{4}\right) \neq 0}$.

The Doche-Icart-Kohel curves is smooth elliptic curves for $a\left(a - \frac{9}{4}\right) \neq 0$. The j-invariant is $j(E_a) = \frac{2^{8}3^{3}a(a-2)^3}{4a-9}$. Following, we count the number of $\bar{\mathbb{F}}_q$-isomorphism classes and $\mathbb{F}_q$-isomorphism classes. In fact, we can generalise the above family of curves to a more general situation.

Definition 2. *A general Doche-Icart-Kohel curves $E_{a,t}$ over a finite field $\mathbb{F}_q$ is defined by $E_{a,t}$: $y^2 = x^3 + 3a(x + t)^2$ where $a, t \in \mathbb{F}_q$ and $ta(4a - 9t) \neq 0$.*

The j-invariant is $j(E_{a,t}) = \frac{2^{8}3^{3}a(a-2t)^3}{t^3(4a-9t)}$.

3 Counting $\bar{\mathbb{F}}_q$-isomorphism Classes

Let E_a and E_b are two Doche-Icart-Kohel curves defined over $\mathbb{F}_q$, then E_a and E_b are isomorphism over $\bar{\mathbb{F}}_q$ if and only if there exists $u, r \in \bar{\mathbb{F}}_q$ and $u \neq 0$ such that

$$\begin{cases} 3u^2b = 3a + 3r, \\ 6u^4b = 6a + 6ar + 3r^2, \\ 3u^6b = 3a + 6ar + 3ar^2 + r^3. \end{cases} \quad \text{or} \quad \begin{cases} u^2b = a + r, \\ 2u^4b = 2a + 2ar + r^2, \\ 3u^6b = 3a + 6ar + 3ar^2 + r^3. \end{cases}$$

Because $ub \neq 0$, thus $(a + r)(r^2 + 2ar + 2a)(3a + 6ar + 3ar^2 + r^3) \neq 0$. Therefore,

$$\begin{cases} 2u^2 &= \dfrac{r^2+2ar+2a}{a+r}, \\ \dfrac{3u^2}{2} &= \dfrac{r^3+3ar^2+6ar+3a}{r^2+2ar+2a}. \end{cases}$$

Therefore,

$r(r^3+4ar^2+12ar+12a)=0.$
If $r=0$ then $u^2b=u^4b=u^6b$ therefore $u^2=1$ and $b=a$.
If $r^3+4ar^2+12ar+12a=0$ and $a+r=0$, then $r=-a$ and $a(a-2)=0$.
If $r^3+4ar^2+12ar+12a=0$ and $r^2+2ar+2a=0$, then $r(r^2+2ar+2a)+2ar^2+10ar+12a=0$, therefore $r^2+5r+6=0$ for $a\neq 0$. Thus $r=-2$ or $r=-3$.
If $r^3+4ar^2+12ar+12a=0$ and $r^3+3ar^2+6ar+3a=0$, then $ar^2+6ar+9a=0$, therefore $r^2+6r+9=0$, thus $r=-3$.
Assume $r^3+4ar^2+12ar+12a=0$ and $r\neq -2,-3,-a$, then

$$b=\frac{a+r}{u^2}=\frac{2(r^2+2ar+a^2)}{r^2+2ar+2a},$$

if $b=a$, then $(a-2)r^2+(2a^2-4a)r=0$, that is $r(a-2)(r+2a)=0$, thus $r=0$ or $r=-2a$ if $a\neq 2$. Moreover, $b=\frac{2(r^2+2ar+a^2)}{r^2+2ar+2a}=2\left(1+\frac{a^2-2a}{r^2+2ar+2a}\right)$, Therefore, from above argument, we have

Lemma 3. *Two Doche-Icart-Kohel curves E_a and E_b($b\neq a$) defined over $\mathbb{F}_q$ are $\bar{\mathbb{F}}_q$-isomorphism if and only if there exists $r\in\bar{\mathbb{F}}_q$ and $r\neq 0,-2,-3,-a,-2a$ such that $r^3+4ar+12ar+12a=0$ and $r^2+2ar\in\mathbb{F}_q$.*

Let $f(a)=\frac{4a-9}{4a}$ with $a\in\mathbb{F}_q,\ a\neq 0,\frac{9}{4}$ then we have the following lemma:

Lemma 4. *Let x_1,x_2,x_3 are the roots of $x^3-f(a)=0$ in $\bar{\mathbb{F}}_q$, then $r_i=\frac{3}{x_i-1}, i=1,2,3$ are the roots of $r^3+4ar^2+12ar+12a=0$ in $\bar{\mathbb{F}}_q$.*

Proof 1. Since

$$\left[\left(\frac{3}{x_i-1}\right)^3+4a\left(\frac{3}{x_i-1}\right)^2+12a\left(\frac{3}{x_i-1}\right)+12a\right](x_i-1)^3$$

$$\begin{aligned}
&= 27+36a(x_i-1)+36a(x_i-1)^2+12a(x_i-1)^3 \\
&= 12ax_i^3-12a+27 \\
&= 12a\frac{4a-9}{4a}-12a+27 \\
&= 12a-27-12a+27=0
\end{aligned}$$

The lemma follows. 0□

Let $\beta^3=\frac{4a-9}{4a}$, if $\frac{3}{\beta-1}=-3$, then $\frac{4a-9}{4a}=0$ and $a=\frac{9}{4}$.
If $\frac{3}{\beta-1}=-2$, then $\beta=\frac{-1}{2}$ and $a=2$.
If $\frac{3}{\beta-1}=-a$, then $\beta=\frac{a-3}{a}$, $\frac{(a-3)^3}{a^3}=\frac{4a-9}{4a}$, thus $a^2-4a+4=0$ and $a=2$.
If $\frac{3}{\beta-1}=-2a$, then $\beta=\frac{2a-3}{2a}$, $\frac{(2a-3)^3}{8a^3}=\frac{4a-9}{4a}$, thus $2a^2-6a+3=0$. Therefore, in $\bar{\mathbb{F}}_q$, $a=\frac{3-\sqrt{3}}{2}$ or $a=\frac{3+\sqrt{3}}{2}$.
If $2a^2-6a+3=0$ is solvable in $\mathbb{F}_q$, then 3 is a square in $\mathbb{F}_q$, then $q\equiv 1,11 \pmod{12}$.

Now, we present and prove the theorem:

Theorem 5. *Let N_q be the number of $\bar{\mathbb{F}}_q$-isomorphism classes of Doche-Icart-Kohel curves which defined over a finite field $\mathbb{F}_q$ of characteristic > 3, then we have*

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

Proof 2. For $r^3 + 4ar + 12ar + 12a = 0$, the discriminant is $\triangle = -48a^2(4a-9)^2$, since $a \neq 0, \frac{9}{4}$ thus $\triangle \neq 0$ and $r^3 + 4ar + 12ar + 12a = 0$ has 3 diffident roots r_1, r_2, r_3 in $\bar{\mathbb{F}}_q$.

Since $b = \frac{2(r^2+2ar+a^2)}{r^2+2ar+2a} = 2\left(1 + \frac{a^2-2a}{r^2+2ar+2a}\right)$, assume $r_1^2 + 2ar_1 + 2a = r_2^2 + 2ar_2 + 2a$ in $\bar{\mathbb{F}}_q$, then $(r_1 - r_2)(r_1 + r_2 + 2a) = 0$, then $r_1 + r_2 = -2a$. For $r_1 + r_2 + r_3 = -4a$, then $r_3 = -2a$. Thus, we must have $r^3 + 4ar^2 + 12ar + 12a = (r + 2a)(r^2 + 2ar + y)$, where $y = 6$ and a satisfy $2a^2 - 6a + 3 = 0$.

Assume $q \equiv 5(\bmod 12)$, then $q \equiv 2 \ (\bmod 3)$, therefore for every element in $\mathbb{F}_q$ has just one cubic root in $\mathbb{F}_q$. Therefore, $x^3 - \frac{4a-9}{4a} = 0$ is solvable and has just one root in $\mathbb{F}_q$ and two roots in some quadratic extensions of $\mathbb{F}_q$. Thus, $r^3 + 4ar + 12ar + 12a = 0$ has just one root in $\mathbb{F}_q$ and two other roots r_2, r_3 are in some quadratic extensions of $\mathbb{F}_q$. We claim $r_2^2 + 2ar_2 \notin \mathbb{F}_q$ and $r_3^2 + 2ar_3 \notin \mathbb{F}_q$. For if $r_2^2 + 2ar_2 \in \mathbb{F}_q$, then the minimal polynomial of r_2 over $\mathbb{F}_q$ has the form $x^2 + 2ax + d$ for some $d \in \mathbb{F}_q$. Therefore, $r^3 + 4ar + 12ar + 12a = (r + e)(r^2 + 2ar + d)$ for some $e \in \mathbb{F}_q$. Thus, $e = 2a$ and $2a^2 - 6a + 3 = 0$, but this occur just at $q \equiv 1{,}11 \ (\bmod 12)$. Moreover, $\frac{2(r_2^2+2ar_2+a^2)}{r_2^2+2ar_2+2a} = \frac{3-\sqrt{3}}{2}$ or $\frac{2(r_2^2+2ar_2+a^2)}{r_2^2+2ar_2+2a} = \frac{3+\sqrt{3}}{2}$ when $q \equiv 1{,}11 \ (\bmod 12)$ and $a = \frac{3-\sqrt{3}}{2}$ or $\frac{3-\sqrt{3}}{2}$.

Therefore, for $q \equiv 5 \ (\bmod 12)$, $N_q = \frac{q-2-1}{2} + 1 = \frac{q-1}{2}$. Similarly, for $q \equiv 11 \ (\bmod 12)$, because $r = -2a$ will lead to $b = a$, therefore $N_q = \frac{q-2-1-2}{2} + \frac{2}{2} + 1 = \frac{q-1}{2}$.

If $q \equiv 1 \ (\bmod 3)$ and $a \in \mathbb{F}_q$ not is a cube, then all the roots of $x^3 - \frac{4a-9}{4a} = 0$ in $\bar{\mathbb{F}}_q$ are in some cubic extensions of $\mathbb{F}_q$. Thus the roots of $r^3 + 4ar + 12ar + 12a = 0$ are all in this cubic extensions of $\mathbb{F}_q$ and no roots in $\mathbb{F}_q$. Therefore, for these a and r, $r^2 + 2ar + 2a$ not in $\mathbb{F}_q$. Assume $q \equiv 1{,}7 \ (\bmod 12)$, then $q \equiv 1 \ (\bmod 3)$. Therefore, have $\frac{q-1}{3}$ elements there exists cubit root, and have 3 diffident cubic roots. Hence, for $q \equiv 7 \ (\bmod 12)$, $N_q = \frac{\frac{q-1}{3}-2}{4} + \left((q-2) - \left(\frac{q-1}{3} - 2\right)\right) = \frac{3q-1}{4}$. For $q \equiv 1 \ (\bmod 12)$, $N_q = \frac{\frac{q-1}{3}-2-2}{4} + \frac{2}{2} + \left((q-2) - \left(\frac{q-1}{3} - 2\right)\right) = \frac{3q+1}{4}$.

Thus the proof is completed. □

4 Counting $\mathbb{F}_q$-isomorphism Classes

Let E_a and E_b are two Doche-Icart-Kohel curves defined over $\mathbb{F}_q$, then E_a and E_b are isomorphism over $\mathbb{F}_q$ if and only if there exists $u, r \in \mathbb{F}_q$ and $u \neq 0$ such that

$$\begin{cases} u^2 b &= a + r, \\ 2u^4 b &= 2a + 2ar + r^2, \\ 3u^6 b &= 3a + 6ar + 3ar^2 + r^3. \end{cases}$$

From the argument of section 2, we only to consider that u^2 is or isn't a square element in $\mathbb{F}_q$ when u^2 be represented by a and r, where $r = \frac{3}{\sqrt[3]{\frac{4a-9}{4a}}-1}$ is the root of $r^3 + 4ar^2 + 12ar + 12a = 0$. For

$$\begin{aligned} \frac{3u^2}{2} &= \frac{r^3 + 3ar^2 + 6ar + 3a}{r^2 + 2ar + 2a} = -a\frac{r^2 + 6r + 9}{r^2 + 2ar + 2a} \\ &= -a\frac{(r+3)^2}{r^2 + 2ar + 2a}, \end{aligned}$$

We only to see $\frac{-2a}{3(r^2+2ar+2a)}$ is or isn't a square element in $\mathbb{F}_q$. For $\frac{-2a}{r^2+2ar+2a} = \frac{-2a}{3\left(r^2 - \frac{r^3+4ar^2}{6}\right)} = \frac{4a}{r^2(4a+r-6)}$, it is only to see $a(4a + r - 6) = 4a^2 + ar - 6a$ is or isn't a square element in $\mathbb{F}_q$.

Let $r = \frac{3}{\sqrt[3]{\frac{4a-9}{4a}}-1} = \frac{3}{\rho-1}$, then $a(4a + r - 6) = \frac{9}{4(1-\rho^3)} \cdot \left(\frac{9}{1-\rho^3} - \frac{3}{1-\rho} - 6\right) = \frac{9}{4(1-\rho^3)^2} \cdot (6\rho^3 - 3\rho^2 - 3\rho)$. Therefore, it is only to see $3(2\rho^3 - \rho^2 - \rho)$ is or isn't a square element in $\mathbb{F}_q$. Summarising the above discussion, we can obtain the following theorem.

Theorem 7. *Let N_q be the number of $\mathbb{F}_q$-isomorphism classes of Doche-Icart-Kohel curves which defined over a finite field $\mathbb{F}_q$ of characteristic > 3, then we have* $N_q \leq \begin{cases} \frac{11q-23}{12}, & \text{if } q \equiv 1 \pmod{12}, \\ q-2, & \text{if } q \equiv 5 \pmod{12}, \\ \frac{11q-17}{4}, & \text{if } q \equiv 7 \pmod{12}, \\ q-3, & \text{if } q \equiv 11 \pmod{12}. \end{cases}$

5 Conclusion

In this paper we present a direct method to compute the number of $\bar{\mathbb{F}}_q$-isomorphism classes and $\mathbb{F}_q$-isomorphism classes of DIK family of elliptic curves defined over a finite field $\mathbb{F}_q$. We give the explicit formulae for the number of $\bar{\mathbb{F}}_q$-isomorphism and an estimate formulae for the number of isomorphism classes. In the future, we hope to be able to give exact formulas for the number of $\mathbb{F}_q$-isomorphism classes.

Competing Interests

Author has declared that no competing interests exist.

References

[1] Daniel J. Bernstein and Tanja Lange, Analysis and optimization of elliptic-curve single-scalar multiplication. Contemp. Math., Amer. Math. Soc., See also Cryptology ePrint Archive, Report 2007/455. 2008;461:1-20.

[2] Doche C, Icart T, Koh el DR. Efficient scalar miltiplication by isogeny decompositions, PKC 2006, LNCS 3958, 191-206, Spriger-Verlag; 2006.

[3] Menezes AJ. Elliptic curve public key cryptosystems, kluwer academic publishers; 1993.

[4] Schoof R. Nonsigular plane cubic curves over finite field, J. Combine, Theory Ser. A. 1987;46:183-211.

[5] Farashahi RR, Shparlinski IE. On the number of distinct elliptic curves in some families, Des. Codes Cryptogr. 2010;54(1):83–99.

[6] Farashahi RR, Moody D, Hongfeng Wu. Isomorphism classes of Edwards and twisted Edwards curves over finite fields, Finite Fields Appl. 2012;18(3):597–612.

[7] Moody D, Wu H. Families of elliptic curves with rational 3-torsion, J. Math. Cryptol. 2012;5(3–4):225–246.

[8] Wu H, Feng R. On the isomorphism classes of Legendre elliptic curves over finite fields. Sci. China Math. 2011;54(9):1885–1890.

[9] Farashahi RR, Hosseini M. Isomorphism classes of Doche–Icart–Kohel curves over finite fields, Finite Fields and Their Applications. 2016;39:111-129.

[10] Avanzi R, Cohen H, Doche C, Frey G, Lange T, Nguyen K, Vercauteren F. Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC Press; 2005.

[11] Silverman JH. The arithmetic of elliptic curves, GTM 106, Springer-Verlag, Berlin; 1986.

[12] Washington LC. Elliptic curves: Number Theory and Cryptography, CRC Press; 2008.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
https://prh.ikprress.org/review-history/12065