Journal of the Faculty of Environmental Science and Technology,
Okayama University
Vol.12, No.1, pp.7-18, March 2007

The order of elliptic curves over finite fields of characteristic two using the Schoof algorithm

Keigo IMURA*, WANG XiaoDong* and Hirofumi ISHIKAWA*

(Received November 30, 2006)

The elliptic curve cryptosystem is a popular cryptosystem. Its safety depends on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). From the viewpoint of ECDLP, it is very interesting to determine the order of elliptic curves. We tabulate the order of elliptic curves on the finite field of characteristic two using the Schoof algorithm, which is an efficient algorithm to decide orders. The Schoof algorithm is carried out by $O(\log^8 q)$. Because the calculation of y^{q^2} occupies most of the time used to execute the Schoof algorithm, it is necessary to reduce the amount of y^{q^2} calculations.

***Key words**: elliptic curve, order, division polynomial, Schoof algorithm, finite field of characteristic two*

1. INTRODUCTION

This paper is intended to tabulate the order of elliptic curves on a large finite field of characteristic two.

The elliptic curve cryptosystem was invented in 1985 as a public key cryptosystem by Koblitz and Miller (Koblitz, 1987; Miller, 1986). The elliptic curve cryptosystem is a popular cryptosystem for the reasons that the key length of elliptic curve cryptosystem is shorter than that of the RSA cryptosystem and that the number of calculations for encoding and decoding of the elliptic curve cryptosystem is less than that in the RSA cryptosystems (Don & Alfred, 1999). The safety of the elliptic curve cryptosystem depends on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). It is difficult to solve the ECDLP if the order of an elliptic curve involves a large prime. Generally, an elliptic curve that is used in the cryptosystem is obtained using the following procedures. First, we randomly generate an elliptic curve; then, we verify whether its order involves a large prime. If not, we repeat these operations until we obtain a suitable elliptic curve. From the viewpoint of ECDLP, it is very interesting to determine the order of elliptic curves. The simplest method, counting up all points (x, y) over the elliptic curve, refers to the

* Department of Human Ecology, Graduate School of Environmental Science, Okayama University, 700-8530, Japan

number of solutions (y-coordinate) satisfying the elliptic curve equation for a given x-coordinate ($x \in F_q$). This method is carried out by $O(q^{1+\varepsilon})(\varepsilon > 0)$. Shanks (1969) proposed the Shanks-Mestre method based on the Baby-step Giant-step method and Hasse's theorem, which is performed using $O(q^{(1/4)+\varepsilon})$ for an elliptic curve over F_q. This method is more efficient than the simplest one for the elliptic curve on a field, the order of which is greater than 457 (Cohen, 1993). Schoof (1985) proposed a more efficient algorithm without calculation of actual points using division polynomials. The division polynomial that is easily obtained by recurrence gives the (x,y) coordinates of m-times point of an elliptic curve. The number of calculations in the Schoof algorithm decreases to $O(\log^8 q)$ (Schoof, 1995). The use of the field of characteristic two in the cryptosystem has the advantage of bit-string representation. From the viewpoint of the Schoof algorithm, the division polynomial of elliptic curves on the finite field of characteristic two can be represented by only one variable that is different from the finite field of characteristic greater than two.

2. Preparations

We use the n-degree algebraic extension field of characteristic two with 2^n elements. We denote the number of elements (2^n) by q. A non-singular elliptic curve E over F_q is given by the following equation.

$y^2+xy=x^3+ax^2+b$ or $y^2+cy=x^3+ax+b$ ($a, b, c \in F_q$)

We prepare several definitions and theorems that are used in the Schoof algorithm.

2.1. Definitions and theorems

2.1.1. Hasse's theorem

Definition 1 Frobenius trace

For an elliptic curve over F_q, the Frobenius trace t is defined as

$$\#E(F_q)=q-1+t \qquad (1)$$

Theorem 1 Hasse's theorem (Hasse, 1933)

The Frobenius trace (t) of an elliptic curve over F_q satisfies the inequality:

$$|t| \le 2\sqrt{q} \qquad (2)$$

Theorem 1 holds in all elliptic curves over any finite field. For an elliptic curve over the finite field F_q of characteristic two, the congruence formulae modulo 4 for the number of F_q-rational points are followed by the condition that there exist solutions of the quadratic equation in F_q. (Blake *et al.*, 1999)

Theorem 2 The number of points in $E(F_q)$

When E: $y^2+xy=x^3+ax^2+b$, $\#E(F_q)$ satisfies the congruence formulae.

$$\#E(F_q) \equiv \begin{cases} 0 \pmod 4 & \text{if } \mathrm{Tr}(a)=0 \\ 2 \pmod 4 & \text{if } \mathrm{Tr}(a)=1 \end{cases} \qquad (3)$$

Therein, Tr(a) denotes the trace of the coefficient (a) of E in F_q over F_2.

2.1.2. The definition of the Frobenius map over an elliptic curve

Definition 2 The Frobenius endomorphism map (Tate, 1974)

The Frobenius endomorphism map of $E(\overline{F}_q)$ is defined as

$$\varphi:\begin{cases}E(\overline{F}_q)\to E(\overline{F}_q)\\(x,y)\to(x^q,y^q).\\\mathcal{O}\to\mathcal{O}\end{cases}$$

The Frobenius endomorphism φ satisfies eq. (4) for any point P in $E(\overline{F}_q)$.

$$\varphi^2(\mathrm{P})-t\varphi(\mathrm{P})+q\mathrm{P}=\mathcal{O} \quad (4)$$

For a prime l, when P belongs to l-torsion group $E[l]$ of $E(\overline{F}_q)$, eq. (4) can be transformed to eq. (5):

$$\varphi^2(\mathrm{P})-\tau\varphi(\mathrm{P})+q_l\mathrm{P}=\mathcal{O} \quad (5)$$

$\tau\equiv t(\mathrm{mod}\ l)$ and $q_l\equiv q(\mathrm{mod}\ l)$.

2.1.3. Theorem of the supersingular curves

We limit ourselves to the equation $y^2+xy=x^3+ax^2+b$ as an elliptic curve in this paper because the elliptic curve $y^2+cy=x^3+ax+b$ is supersingular.

THEOREM 3

The necessary and sufficient condition that an elliptic curve (F_q) is supersingular is that the Frobenius trace (t) divides the characteristic (p) of F_q.

Consequently, the non-supersingular curve satisfies $t \not\equiv 0(\mathrm{mod}\ p)$, especially for the case $q=2^n$, $t\equiv 1$ mod 2.

2.1.4. Division polynomials

To calculate m-times point (mP) of the elliptic curve, the division polynomials were devised in the 19th century. Division polynomials can increase the efficiency of calculations of the m-times point over the elliptic curve.

DEFINITION 3 m-division polynomial of the elliptic curve over F_q (Cassels, 1966)

For the finite field of characteristic two, the division polynomial can be reduced to one variable polynomial $f_m(x)$ of x. The division polynomials are defined by the following recursive formulae.

$$\begin{aligned}f_0&=0\\f_1&=1\\f_2&=x\\f_3&=x^4+x^3+b\\f_4&=x^6+bx^2\\f_{2m+1}&=f_{m+2}f_m^3+f_{m-1}f_{m+1}^3 \quad (m\ge 2)\\f_{2m}&=(f_{m+2}f_{m-1}^2+f_{m-2}f_{m+1}^2)f_m/x \quad (m\ge 3)\end{aligned}$$

For $m\geqq 2$ and $\mathrm{P}=(x,y)\in E(\overline{F}_q)\setminus E[m]$ ($E[m]$ being the m-torsion group of $E(\overline{F}_q)$), mP is represented by eq. (6).

$$m\mathrm{P}=\left(x+\frac{f_{m-1}f_{m+1}}{f_m^2},x+y+\frac{(x^2+x+y)f_{m-1}f_mf_{m+1}+f_{m-2}f_{m+1}^2}{xf_m^3}\right) \quad (6)$$

2.2. Outline of the Schoof algorithm

The Schoof algorithm (Schoof, 1985) comprises two steps. First, the Frobenius trace mod l (τ) is computed for the prime l according to eq. (5). Secondly, the set of τ's for l is computed as $l\leqq l_{max}$ in inequality (7) because the absolute value of the Frobenius trace is limited to $4\sqrt{q}$ by Theorem 1.

$$\#l\max:=\prod_{\substack{l,\,prime\\2\le l\le l\max}}l>4\sqrt{q} \quad (7)$$

Next, the Frobenius trace (t) is determined according to the Chinese remainder theorem. In the first step of the calculation, $\varphi^2(\mathrm{P})+q_l\mathrm{P}=\tau\varphi(\mathrm{P})$, we use the division polynomial without determining an explicit point of the elliptic curve $E(\overline{F}_q)$. Value t, which is obtained using the Chinese remainder theorem, is the absolute value of the Frobenius trace. Therefore, we decide the sign of t following Theorem 2.

3. Material and Methods

3.1. Determination of finite field

There are two kind of bases over a finite field of characteristic two: a normal basis representation and a polynomial basis representation (ANSI X9.62, 1998). We adopt a polynomial basis in this paper because we can easily perform a multiplication operation on that basis. For the field F_q, as a reduction polynomial of degree n, which provides a polynomial basis of F_q, we choose a trinomial or pentanomial irreducible polynomial on F_2 following the method of Seroussi (1998).

3.2. Representation of an element in F_q

An element of F_q, which is represented by a polynomial of degree n-1 on F_2 can be expressed for computer calculations as an n-array of coefficients in its polynomial.

3.3. Calculations on F_q

Calculations such as multiplication, division, inversion and power are carried out on the basis of ANSI X9.62.

3.4. Determination of elliptic curves

A nonsingular and non-supersingular elliptic curve, $y^2+xy=x^3+ax^2+b$, satisfies the conditions as

$$\mathrm{Tr}(a)=1 \text{ or } a=0,\ b\in \mathrm{F}_q^* \qquad (8)$$

The two curves, which have the same constant term b and x^2-coefficient (a) 0 and $\mathrm{Tr}(a)=1$, are called twist curves. The sum of the orders of the twist curves becomes the constant $2q+2$.

$$\#E_{0,b}(F_q)+\#E_{\mathrm{Tr}(a)=1,b}(F_q)=2q+2 \qquad (9)$$

Therefore, the x^2-coefficient a is limited to 0 in this paper.

3.5. Division polynomials

3.5.1. Record of division polynomials

Division polynomials are recorded in files A and B to save memory. We classify coefficients of division polynomials into 0 and 1 and others, e.g. the type of coefficients. For all necessary division polynomials, the type of coefficients and the location of the figure in file B for other type coefficients are recorded in a two-dimensional array file A, although an exact figure of other type coefficients is recorded in a one-dimensional array file B.

3.5.2. Calculation of division polynomials

The flow chart of the calculation from f_0 to f_{lmax} is shown in Fig. 1.

3.6. Execution of the Schoof alogrithm

3.6.1. Definition of the data structure for F_q-polynomials

We introduce two data structures. A polynomial of x over F_q is represented by structure α, whereas a polynomial $r(x,y)$ of two variables (x,y) with a linear form for variable y, that is, a set of two polynomials of x, $(p(x), q(x))$, $r(x, y)=p(x)+q(x)y$, is represented by structure β.

3.6.2. Calculation of F_q-polynomials

In the process for the decision of τ for the fixed prime l, all the polynomial calculations are carried out under modulo f_l (f_l being the l-th division polynomial).

Here, $r(x,y)$ is reduced to the linear form of y by replacement of a high y-term with a linear form of y through the equation of the elliptic curve when a two-variable polynomial $r(x,y)$ with two or more y-degree appears in the calculation.

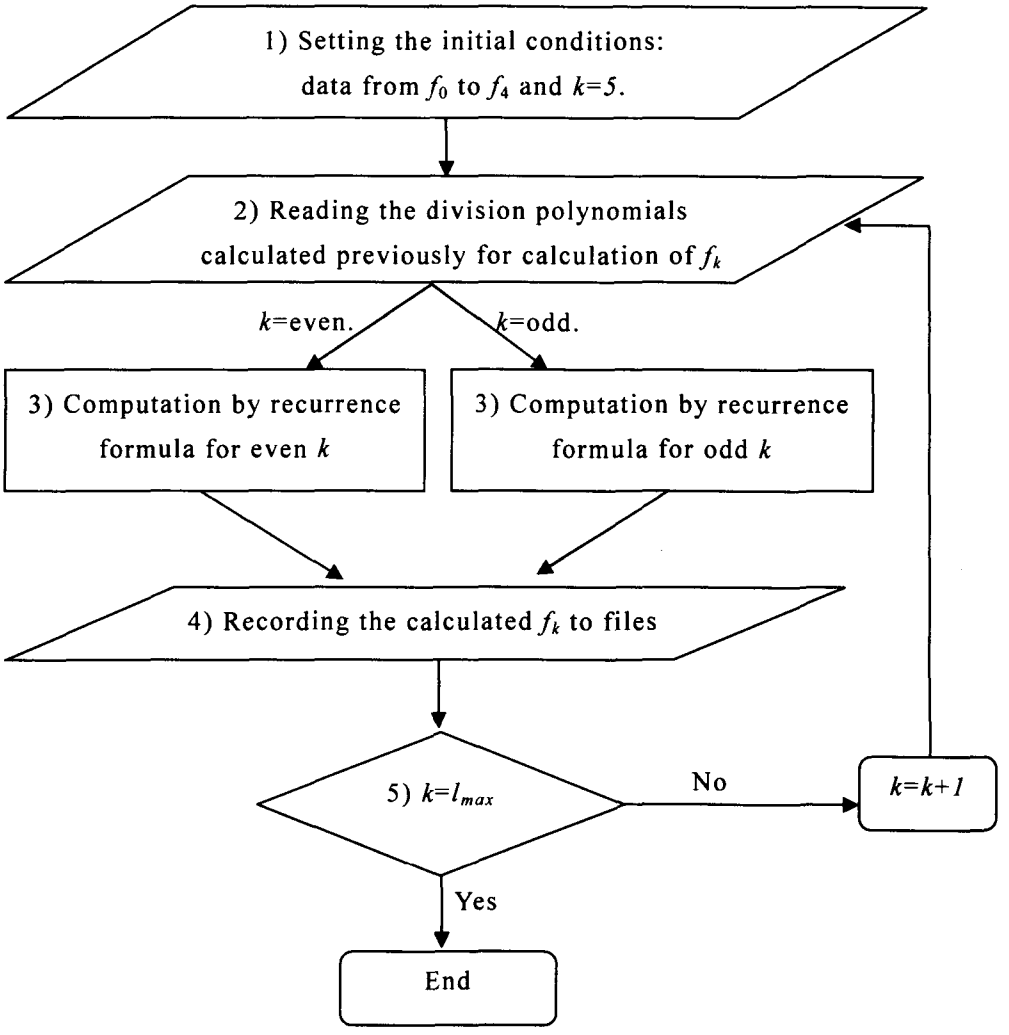

Fig. 1 Flow chart of the calculations for division polynomials

3.6.3. Calculation of y^q and y^{q^2}

It is necessary to express the principal terms y^q and y^{q^2} in the Schoof algorithm in the form of structure β. Under the equation of the elliptic curve, the explicit formula of y^q is given as the following.

$$y^\beta = y^{q^2} = \left(\sum_{i=0}^{n+1} x^i\right) y + \left\{ (x^3)^{\frac{q^2-1}{2}} + \sum_{i=0}^{n-2} \left(\sum_{j=i+1}^{n+1} x^j\right) (x^3)^i \right\} + \left\{ b^{\frac{q^2-1}{2}} + \sum_{i=0}^{n-2} \left(\sum_{j=i+1}^{n+1} x^j\right) b^i \right\} \quad (10)$$

Moreover, y^{q^2} can be expressed by the form of structure β by replacing n with $2n$ in (10).

3.6.4. Procedures of the Schoof algorithm

For a fixed prime l, we search τ (0,⋯, (l-1)/2), which satisfies

$$\left[\varphi^2(\mathrm{P}) + q_l \mathrm{P}\right]_X = \left[\pm \tau\varphi(\mathrm{P})\right]_X \quad (\tau=0,\cdots, (l-1)/2)$$

on account of the correspondence between x-coordinates of $+\tau\varphi$(P) and $-\tau\varphi$(P).

(1) The case in which $\varphi^2(\mathrm{P}) = \pm q_l \mathrm{P}$

The equation $\varphi^2(\mathrm{P}) = -q_l \mathrm{P}$ leads to $\tau \equiv 0 \pmod{l}$. On the other hand, the equation $\varphi^2(\mathrm{P}) = q_l \mathrm{P}$ leads to $\varphi^2(\mathrm{P}) = \pm\omega \mathrm{P}$, where ω represents a square root of q_l in F_q, which indicates that $\tau = \pm 2\omega$.

(2) The case in which $\varphi^2(\mathrm{P}) \neq \pm q_l \mathrm{P}$ ($\tau \neq 0$)

For this case, we verify the equation: $\varphi^2(\mathrm{P}) + q_l \mathrm{P} = \pm\tau\varphi(\mathrm{P})$ for τ ($1 \leqq \tau \leqq (l-1)/2$). As the

x-coordinate of both the left-hand and right-hand side of the equation, $\varphi^2(\mathrm{P})+q_l\mathrm{P}$ and $\pm\tau\varphi(\mathrm{P})$ are expressed as fractions. The equation is transformed into a β–type structure by multiplying the common denominator form of structure α-type polynomials. We then transform it into the y-linear form of $p(x)+q(x)y=0$ or $y=p(x)/q(x)$. When we substitute $p(x)/q(x)$ for y in the elliptic curve equation, we can obtain the polynomial $h(x)$ of x satisfying

$$h(x)=p^2(x)+xp(x)q(x)+q^2(x)x^3+q^2(x)b=0.$$

If $\mathrm{P}\in E[l]$ satisfies $\varphi^2(\mathrm{P})+q_l\mathrm{P}=\pm\tau\varphi(\mathrm{P})$, $\gcd(h(x), f_l)\neq 1$. Thereafter, we determine the sign of τ through y-coodinate in $\varphi^2(\mathrm{P})+q_l\mathrm{P}=\tau\varphi(\mathrm{P})$ in the same manner. We can obtain $\tau\equiv t \pmod{l}$ or $-\tau\equiv t \pmod{l}$ by satisfying the equation or not satisfying it.

When we find $\tau\equiv t \pmod{l}$ for all primes l ($l\leqq l_{max}$), t can be determined using the Chinese remainder theorem, which leads to determination of the order of the elliptic curve using Hasse's theorem.

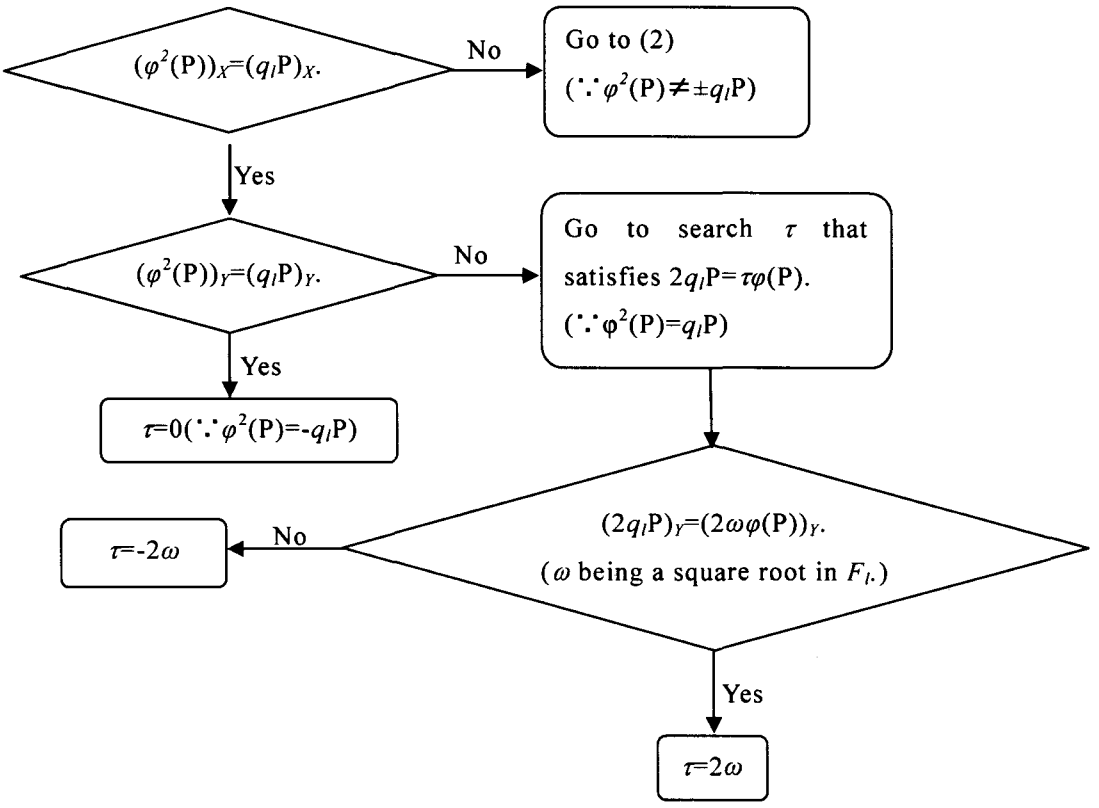

Fig. 2 Flow chart for the case $\varphi^2(\mathrm{P})=\pm q_l\mathrm{P}$

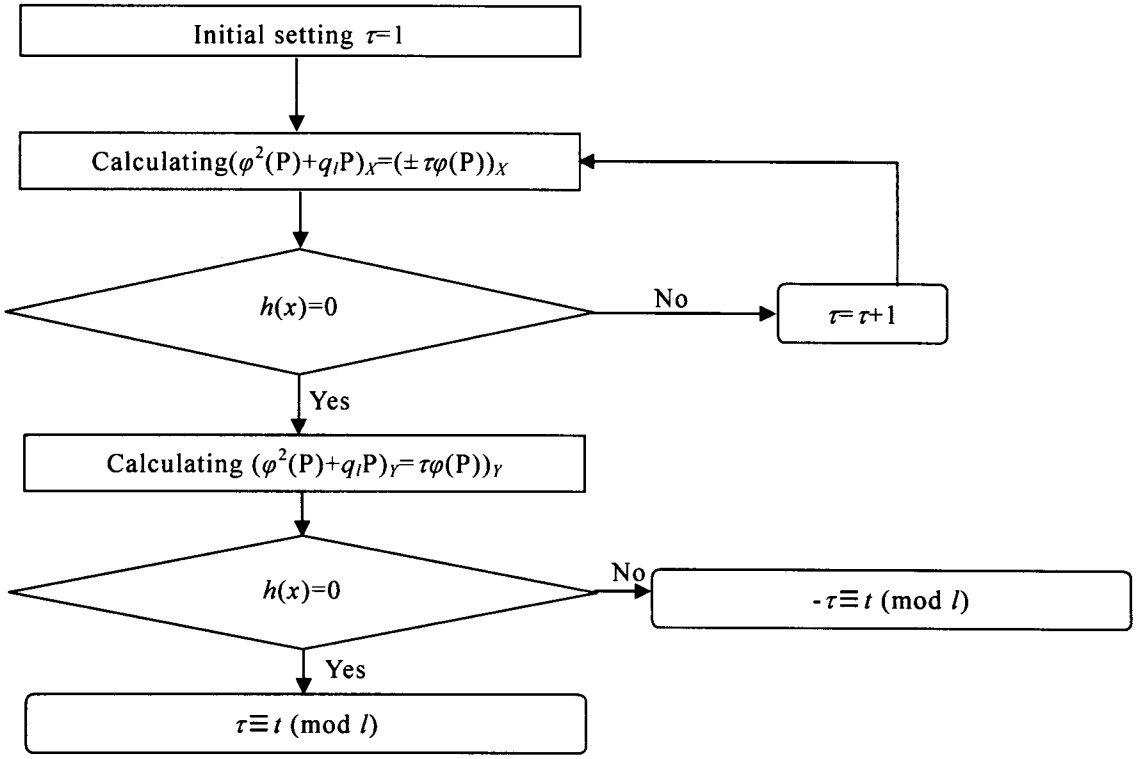

Fig. 3 Flowchart for the case in which $\varphi^2(P)\neq\pm q_l(P)$

4. Result

We calculated the order of elliptic curves with the constant terms b=1, ⋯ , $F_{(16)}$ over $F_{2^{30}}, F_{2^{40}}, F_{2^{50}}, F_{2^{60}}$ and $F_{2^{80}}$ (Table 1). The distribution of the Frobenius trace for 2^{12} constant terms (b=1, ⋯, $1000_{(16)}$) over $F_{2^{17}}$ is shown in Fig. 4. We tabulated the orders and the residues modulo l (l=2, ⋯, 43) of the Frobenius trace over $F_{2^{100}}$ (Table 2). The irreducible polynomial on F_2 used in the results is shown in Table 3.

5. Discussion

The utilization of division polynomials provides the key to the Schoof algorithm for a search of the Frobenius trace without the determination of l-torsion point in $E(\overline{F}_q)$. Consequently, we obtain the Frobenius trace t mod l deterministically (Schoof, 1985). The calculation of y^{q^2} occupies most of the computation time in the Schoof algorithm. For example, in the elliptic curve over $F_{2^{24}}$, we spend 178 s computing y^{q^2}, whereas we spent about 290 s for the entire computation of the Frobenius trace modulo l. The y^{q^2}-calculation requires about 60% in the calculation of the Schoof algorithm irrespective of the difference of the search path. Therefore, it is important to reduce of y^{q^2}-calculation. Most computation time in y^{2^m} is spent in the second term of the left hand side in (10):

$$\sum_{i=0}^{m-2}(\eta(x))^{2^i}\left(x^{\sum_{j=i+1}^{m-1}2^j}\right), \qquad (11)$$

where $\eta(x)$ stands for x^3+b, the right hand side the equation of the elliptic curve. We introduce the reserve calculation to reduce the amount of the calculation in (11). First, for the division d ($1<d$

$<m/2$) that is sufficiently large, but adequate to support computer memory, the interval $[0,m]$ is divided into $d+1$ interval $[0, m_1-1]$, $[m_1, 2m_1-1]$, $\cdots$,$[dm_1, m]$, where m_1 stands for $\lfloor \frac{m}{d} \rfloor$. Secondly, we compute d couples of $\left(x^{2^{m_1 \cdot i}}, \eta(x)^{2^{m_1 \cdot i}}\right)$ $(0 \leqq i \leqq d)$ and save them. Finally, we calculate each term $x^{2^{m_1 \cdot i+j}}$ $\left(\text{or } \left(\eta(x)^{2^{m_1 \cdot i+j}}\right)\right)$ in $[m_1 \cdot i, m_1 \cdot (i-1)]$ on the basis of the saved term $x^{2^{m_1 \cdot i}}$ $\left(\text{or } \left(\eta(x)^{2^{m_1 \cdot i}}\right)\right)$.

Next, we evaluate the calculation amounts in (11). We respectively denote the number of calculations in square, product and division as S, P and M. The number of calculations in (11) without reserve calculations is counted as

$$m(m+1)S+2mP+(m+1)^2M \qquad (12)$$

whereas that with the reserve calculation is reduced to

$$((m-2)m_1)S+(m-2)P+(m-2)(m_1+1)M \qquad (13)$$

Because P is nearly M and S is negligible, the formulae (12) and (13) are simplified as the following.

$$m(m+1)S+2mP+(m+1)^2M \approx (m^2+4m+1)P \quad (14)$$

$$((m-2)m_1)S+(m-2)P+(m-2)(m_1+1)M \approx (m-2)(m_1+2)P \quad (15)$$

The experimental calculation-time in eq. (11) for $d=5$ is shown in Table 4. For $d=5$, the number of calculations in (11) can be reduced to about 60% because of the improvement. For $l=23$ and $d=5$, y^{q^2} -calculation over $F_{2^{60}}$ with and without reserve calculation spent 2,787 seconds and 11,434 seconds. The ratio of the time in y^{q^2}-calculation with the reserve calculation with 5-division points to the time without it was estimated as 0.24, while as the ratio of the number was shown as 0.21 in Table 4. Therefore, the actual time in the refinement method was reduced according to the reduction in the number of calculation. The execution time of the determination of the Frobenius trace using a Pentium4 processor and 512 MB computer memory is shown in Table 5, with the Schoof algorithm programmed by C++ based on Visual Studio™ software (Microsoft Corp.)

The Schoof algorithm has been improved by Elkies (1998) and Schoof (1995), to produce the so-called Schoof-Elkies-Atkin algorithm.

Table 1. Orders of the elliptic curves

b	Finite Fields			
	$F_{2^{30}}$	$F_{2^{40}}$	$F_{2^{50}}$	$F_{2^{60}}$
01	10737 51912	109 95110 07596	1 12589 98591 90680	1152 92150 25611 51248
02	10737 00864	109 95123 43724	1 12589 99032 95340	1152 92150 50017 83296
03	10737 15048	109 95129 85496	1 12589 98852 17196	1152 92150 55450 12752
04	10737 00864	109 95120 88936	1 12589 99032 95340	1152 92150 50017 83296
05	10737 15048	109 95098 35596	1 12589 98852 17196	1152 92150 58450 12752
06	10737 17760	109 95109 76644	1 12589 99237 48440	1152 92150 41237 20704
07	10737 11400	109 95120 80328	1 12589 99282 64512	1152 92150 34747 76592
08	10737 75872	109 95120 53140	1 12589 98701 60984	1152 92150 36724 09600
09	10737 29832	109 95112 30880	1 12589 99411 97632	1152 92150 45773 13936
0A	10737 10848	109 95118 65520	1 12589 99281 73164	1152 92150 63360 53760
0B	10737 16008	109 95114 77564	1 12589 99260 96812	1152 92150 53923 73520
0C	10737 00864	109 95128 32276	1 12589 99115 82700	1152 92150 57695 77472
0D	10737 15048	109 95124 75464	1 12589 99195 27084	1152 92150 56279 20784
0E	10737 73056	109 95101 51600	1 12589 99534 57792	1152 92150 47049 61152
0F	10736 95080	109 95112 16356	1 12589 99096 31768	1152 92150 26268 57232

Table 1. (continued)

b	Finite Fields
	$F_{2^{80}}$
01	12089 25819 61285 88503 22624
02	12089 25819 61627 76289 88780
03	12089 25819 61564 04045 90068
04	12089 25819 61627 76289 88780
05	12089 25819 61564 04045 90068
06	12089 25819 61634 62876 39000
07	12089 25819 61614 31188 38440
08	12089 25819 61306 73205 00312
09	12089 25819 61502 57616 02600
0A	12089 25819 61428 90833 97484
0B	12089 25819 61583 32578 67252
0C	12089 25819 61318 23321 06220
0D	12089 25819 61499 69255 59924
0E	12089 25819 61656 83605 49760
0F	12089 25819 61371 65584 33344

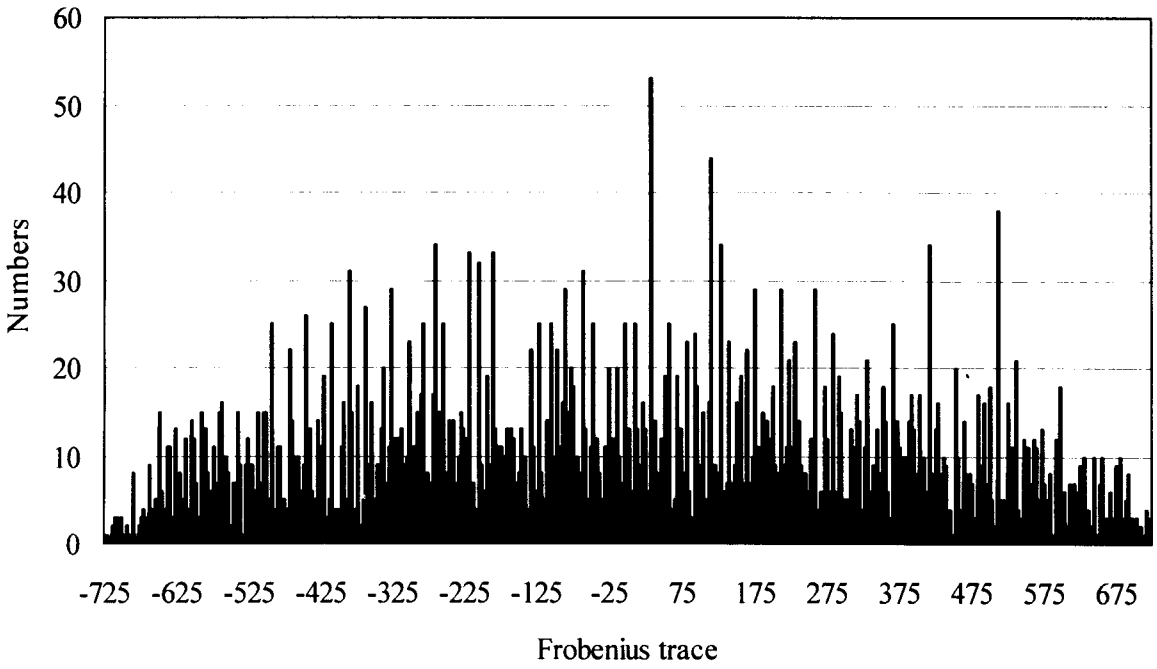

Fig. 4 Histogram of the distribution of the Frobenius traces for elliptic curves over $F_{2^{17}}$. The abscissas and ordinates respectively indicate the Frobenius traces and the number of curves.

Table 2-1. Frobenius traces of the elliptic curve on $F_{2^{100}}$

b	Trace	$t \bmod l$												
		3	5	7	11	13	17	19	23	29	31	37	41	43
01	2 07515 30866 27109	1	1	1	2	6	5	7	22	14	8	35	33	19
02	- 64983 49082 86975	2	0	2	7	5	12	3	21	7	30	11	24	40
03	52578 54784 32113	2	3	4	9	3	3	12	13	11	27	2	34	4
04	- 64983 49082 86975	2	0	2	7	5	12	3	21	7	30	11	24	40
05	52578 54784 32113	2	3	4	9	3	3	12	13	11	27	2	34	4
B665 9568D 6A779 2B862 915FD	- 1088 95900 25219	2	3	6	10	7	16	13	18	27	28	26	21	42

Table 2-2. Orders of the elliptic curves

b	Finite Field $F_{2^{100}}$
01	1 26765 06002 28231 47664 97898 32484
02	1 26765 06002 28228 75166 17949 18400
03	1 26765 06002 28229 92728 21816 37488
04	1 26765 06002 28228 75166 17949 18400
05	1 26765 06002 28229 92728 21816 37488
B665 9568D 6A779 2B862 915FD	1 26765 06002 28229 39060 71131 80156

Table 3. The irreducible polynomials on F_2

n	Irreducible polynomial
17	$x^{17}+x^3+1$
30	$x^{30}+x+1$
40	$x^{40}+x^{39}+x^{38}+x^5+1$
50	$x^{50}+x^{49}+x^{48}+x^4+1$
60	$x^{60}+x+1$
80	$x^{80}+x^{79}+x^{78}+x^{26}+1$
100	$x^{100}+x^{15}+1$

Table 4. Comparison of numbers of the calculation with and without reserve calculation

n	Number of calculations in $y^{2^{2n}}$ without reserve calculation (A)	Number of calculations in $y^{2^{2n}}$ with reserve calculation (B)	(B)/(A)
10	141	32	0.196
20	481	108	0.227
30	1021	224	0.227
40	1761	380	0.216
50	2701	576	0.213
60	3841	812	0.211
70	5181	1088	0.210
80	6721	1404	0.209
90	8461	1760	0.208
100	10401	2156	0.207

Table 5. Computation time in the Schoof algorithm

q	Time for search the Frobenius trace
2^{17}	4.6 seconds
2^{40}	6.8 minutes
2^{60}	1.6 hours
2^{80}	14.5 hours
2^{100}	52.2 hours

References

Blake, IF, Seroussi, G, Smart, NP, Ellipticcurves in cryptography, The University of Cambridge Press Syndicate, Cambridge, 1999

Cassels, JWS, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.*, **41**, 193-291, 1966

Cohen, H, A course in computational algebraic number theory, GTM 138, Springer-Verlag, Berlin, 1993

Don, J, Alfred, M, Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA), National Institute of Standards and Technology, U. S. Department of Commerce, 1998

Elkies, ND, Elliptic and modular curves over finite fields and related computational issues, AUSCRTPT92, In: Advances in Cryptology, Ohta, K and Pei, D (eds.), Springer-Verlag, Berlin, 21-76, 1998

Koblitz, N, A course in number theory and cryptography, Springer-Verlag, Berlin, 1994

Lang, S and Trotter, H, Frobenius distributions in GL2-Extensions, LN Math, 504, Springer-Verlag, Berlin, 1976

Lay, G-J and Zimmer, HG, Constructing elliptic curves with given group order over large finite fields, LNCS 877, 250-263, 1994

Miller, V, Use of elliptic curves in cryptography, CRYPTO 85, In: Advances in cryptology, Williams, HC (eds.), Springer-Verlag, Berlin, 417-426, 1986

Schoof, R, Elliptic curves over finite fields and the computation of squqre roots mod p, *Math. Comp.*, **44**, 483-494, 1985

Schoof, R, Counting points on elliptic curves over finite fields, *J. Theorie Nombres Bordeaux*, **7**, 219-254, 1995

Seroussi, G, Table of low-weight binary irreducible polynomials, Hewlett-Packard Technical Report, HPL-98-135, 1998

Shanks, D, Class number, a theory of factorization, and genera, Proceedings Symposium in Pure Maths, 20, AMS, 415-440, 1969

Silverman, JH, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, Berlin, 1986

Tate, J, The arithmetic of elliptic curves, *Inventiones Mathematicae*, **23**, 179-206, 1974