J. Appl. Math. & Informatics Vol. **30**(2012), No. 1 - 2, pp. 101 - 109
Website: http://www.kcam.biz

POINTS COUNTING ALGORITHM FOR ONE-DIMENSIONAL FAMILY OF GENUS 3 NONHYPERELLIPTIC CURVES OVER FINITE FIELDS

GYOYONG SOHN

Abstract. In this paper, we present an algorithm for computing the number of points on the Jacobian varieties of one-dimensional family of genus 3 nonhyperelliptic curves over finite fields. We also provide the explicit formula of the characteristic polynomial of the Frobenius endomorphism of the Jacobian of $C : y^3 = x^4 + a$ over a finite field $\mathbb{F}_p$ with $p \equiv 1 \pmod 3$ and $p \not\equiv 1 \pmod 4$. Moreover, we give some implementation results using Gaudry-Schost method. A 162-bit order is computed in 97 s on a Pentium IV 2.13 GHz computer using our algorithm.

AMS Mathematics Subject Classification : 14H45. 14G50. 94A60.
Key words and phrases : Counting points, Characteristic polynomial, Nonhyperelliptic curve.

1. Introduction

Elliptic curve cryptography was independently proposed by Koblitz [15] and Miller [16]. The elliptic curve cryptosystem is a public key cryptosystem based on the discrete logarithm problem in the group of points on a curve. Hyperelliptic curve cryptosystems were introduced by Koblitz [14] as a natural extension of Elliptic curve cryptography. Systems based on the discrete logarithm problem in Jacobians of superelliptic curves were introduced for constructing a public key cryptosystem [6]. In this study, we address these nonhyperelliptic curves of genus 3, which are called Picard curves.

In order to obtain cryptographically suitable curves, we must determine the number of rational points on the Jacobian. If the orders of Jacobians are sufficiently large prime numbers, then the corresponding cryptosystems are secure against various attacks. The order of the Jacobian of a curve over a finite field with q elements is roughly q^g, where g is the genus of the curve. More precisely, the elliptic curve cryptosystem needs a 160-bit field and for the hyperelliptic

Received September 15, 2011. Revised November 11, 2011. Accepted November 16, 2011.
© 2012 Korean SIGCAM and KSCAM.

curve cryptosystem of genus 2, we only need an 80-bit field. In genus 3 curves, we need a 54-bit field, and the order of a Jacobian group should have a large prime factor greater than approximately 2^{160} .

The problem of counting points on elliptic and hyperelliptic curves over finite fields has been studied by numerous researchers (e.g., [17, 10, 11, 13], and [8]). Schoof's algorithm [17] is a well-known method for counting points on elliptic curves over finite fields. There are several efficient counting points algorithms of Jacobian varieties of superelliptic curves [7], and there are known efficient algorithms to construct a special curve with its Jacobian group using complex multiplication [3]. Recently, Bauer, Teske, and Weng have proposed a related algorithm on a Picard curve in large characteristic [2] and have suggested improvements for using a small memory [1].

In this study, we provide an algorithm for computing the orders of Jacobians on one-dimensional family of genus 3 nonhyperelliptic curves over finite fields using the Gaudry-Schost algorithm. In particular, we use curves of the type $y^3 = x^4 + ax$ over finite prime fields with the characteristic $p > 3$. These curves are used in [5], but the resulting curves do not have a sufficient cryptographic size. By using the Gaudry-Schost method, we determine the order of the Jacobian of a curve defined over a 55-bit finite prime field, which is computed in 97 s on a Pentium IV 2.13 GHz computer and that has a 160-bit prime factor. We also provide the explicit formula of the characteristic polynomial of the Frobenius endomorphism of the Jacobian of genus 3 nonhyperelliptic curves defined by the equation $C : y^3 = x^4 + a$ over a finite field $\mathbb{F}_p$ with $p \equiv 1 \pmod 3$ and $p \not\equiv 1 \pmod 4$.

2. Basic Facts

Let p be a prime, $p \neq 2, 3$, and let $\mathbb{F}_q$ be a finite field of characteristic p with q elements. Let C be a Picard curve over $\mathbb{F}_q$ given by the equation

$$C \ : \ y^3 = f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

for all $a_i \in \mathbb{F}_q$. We denote the Jacobian variety of a Picard curve C by J_C. Then, $J_C(\mathbb{F}_q)$ is the group of $\mathbb{F}_q$-rational points on J_C.

The *zeta function* $\zeta(t, C)$ of C can be written as

$$\zeta(t, C) = \frac{L(t, C)}{(1 - t)(1 - qt)},$$

where $L(t, C)$ is the *L-polynomial* of the curve. Let π_q be the Frobenius endomorphism of C and $\chi_C(t)$ the characteristic polynomial of π_q on the Tate module $T_l(J_C) \otimes \mathbb{Q}_l$. Then $\chi_{\pi_q,C}(t) = t^{2g}L(1/t, C)$. For simplicity, we write $\chi(t)$ instead of $\chi_{\pi_q,C}(t)$ if the reference to the curve is clear. Then, it is of the form

$$\chi(t) = t^6 - s_1t^5 + s_2t^4 - s_3t^3 + qs_2t^2 - q^2s_1t + q^3.$$

We obviously have $\sharp J_C(\mathbb{F}_q) = \chi(1)$. i.e.,

$$\sharp J_C(\mathbb{F}_q) = 1 + q^3 - s_1(1 + q^2) + s_2(1 + q) - s_3. \tag{1}$$

Let $M_r = (q^r + 1) - N_r$, where N_r is the number of $\mathbb{F}_{q^r}$-rational points on C for $r = 1, 2, 3$. Then, we have

$$s_1 = M_1,\ s_2 = \frac{1}{2}(M_1^2 - M_2), \tag{2}$$

$$s_3 = \frac{1}{3}\Big(M_3 - \frac{3}{2}M_2M_1 + \frac{1}{2}M_1^3\Big). \tag{3}$$

Thus, to compute the number of $\mathbb{F}_q$-rational points on J_C, we need only the values of three coefficients of the characteristic polynomial or, equivalently, the number of points $\sharp C(\mathbb{F}_{q^r})$ for $r = 1, 2, 3$.

The following is a well-known inequality, the Hasse-Weil bound, that bounds $\sharp J_C(\mathbb{F}_q)$:

$$\lceil(\sqrt{q} - 1)^{2g}\rceil \leq \sharp J_C(\mathbb{F}_q) \leq \lfloor(\sqrt{q} + 1)^{2g}\rfloor.$$

Then, we have

$$|s_1| \leq 6\sqrt{q},\ |s_2| \leq 15q,\ |s_3| \leq 20q\sqrt{q}. \tag{4}$$

3. The Hasse-Witt Matrix of C

In this section, we describe the Hasse-Witt matrix of Picard curve C. It is a useful tool to compute the modulo characteristic p of $\sharp J_C(\mathbb{F}_p)$. In our case, the Hasse-Witt matrix is defined as a 3×3 matrix, as in [12], and its entries are determined from the defined curve equation.

Theorem 3.1 ([12])**.** *Let $C : y^3 = f(x)$ with $\deg f = 4$ be the equation of a genus 3 Picard curve. Denote by $c_{i,j}$ the coefficient of x^i in the polynomial $f(x)^{p-1-\frac{j}{3}}$. Then the Hasse-Witt matrix is given by*

$$H = \begin{pmatrix} c_{p-1,p-1} & c_{2p-1,p-1} & c_{p-1,2p-1} \\ c_{p-2,p-1} & c_{2p-2,p-1} & c_{p-2,2p-1} \\ c_{p-1,p-2} & c_{2p-1,p-2} & c_{p-1,2p-2} \end{pmatrix}$$

Moreover, in [12], it has two forms corresponding to $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$. Further, it is used in the counting points procedure for cryptographically suitable curves.

In [18], Manin showed that this matrix is related to the characteristic polynomial of the Frobenius endomorphism modulo p. For a matrix $H = (a_{ij})$, let $H^{(p)}$ denote the elements raised to the power p, i.e., (a_{ij}^p). Then, we have the following theorem.

Theorem 3.2. *Let C be a curve of genus g defined over a finite field $\mathbb{F}_{p^n}$. Let H be the Hasse-Witt matrix of C and let $H_\pi = H \cdot H^p \cdot H^{p^2} \cdots H^{p^{n-1}}$. Let $\kappa(t)$ be the characteristic polynomial of the matrix H_π and $\chi(t)$ the characteristic polynomial of the Frobenius endomorphism of the Jacobian of C. Then,*

$$\chi(t) \equiv (-1)^g t^g \kappa(t)\ (mod\ p).$$

Proof. See [18]. $\square$

Note that this theorem provides a very efficient method to compute the characteristic polynomial of the Frobenius endomorphism and the group order of the Jacobian of C modulo p, when p is not too large.

4. The Characteristic Polynomial of C

Assume that C is a Picard curve over $\mathbb{F}_p$, where p is congruent to 2 modulo 3. $\chi(t)$ is of the form $t^6 + s_2t^4 + ps_2t^2 + p^3$ and splits over $\mathbb{Q}$. Now we consider the case of the $p \equiv 1 \pmod 3$. In this case, the automorphism group of C is generated by $\rho : (x, y) \to (x, \zeta_3 y)$, where ζ_3 is a primitive cubic root of unity in $\mathbb{F}_q$. It extends to the Jacobian of C. Therefore, $\mathbb{Z}[\zeta_3] \subseteq \mathrm{End}(J_C(\mathbb{F}_p))$. In particular, we treat curves of form $C : y^3 = x^4 + ax$ over finite fields defined for $p \equiv 4, 7 \pmod 9$.

Remark 4.1. Let $p \equiv 1 \pmod 3$ and C be a Picard curve over $\mathbb{F}_p$ of the form $y^3 = x^4 + ax$. If $a^{(p-1)/3} = 1$, then 27 divides $\sharp J_C(\mathbb{F}_p)$. Otherwise, 3 divides $\sharp J_C(\mathbb{F}_p)$.

Theorem 4.1 ([5]). *Let C be a Picard curve defined by the equation $y^3 = x^4+ax$ for $a \in \mathbb{F}_p$ over a finite field with $p \equiv 4, 7$ (mod 9). Then, the characteristic polynomial of the Frobenius endomorphism, $\chi(t)$, has the form*

$$\chi(t) = t^6 + c_2pt^4 - c_3pt^3 + c_2p^2t^2 + p^3,$$

where $c_2 = -3, 0, 3$ and c_3 is an integer satisfying $|c_3| \leq 2[\sqrt{p}] + 1$ and $c_3 \equiv 2$ (mod 3).

Proof. The Serre bounds are $|M_i| \leq [6\sqrt{p^i}]$ for $i = 1, 2, 3$ in (2) and (3). The coefficients of the Hasse-Witt matrix for the curve C has the following forms:

$$c_{p-2,p-1} = \binom{\frac{2p-2}{3}}{\frac{p-4}{9}} a^{\frac{5p-2}{9}} \text{ and } c_{i,j} = 0 \text{ otherwise} \qquad \text{if } p \equiv 4 \pmod 9,$$

$$c_{2p-1,p-1} = \binom{\frac{2p-2}{3}}{\frac{4p-1}{9}} a^{\frac{2p-5}{9}} \text{ and } c_{i,j} = 0 \text{ otherwise} \qquad \text{if } p \equiv 7 \pmod 9.$$

Therefore, the coefficients of $P(t)$ are

$$s_1 \equiv s_2 \equiv s_3 \equiv 0 \pmod p.$$

This is the Manin result. We trivially obtain $M_1 = 0$ in (2) for $p > 37$. Therefore, s_1 is zero.

Since $N_2 \equiv 2 \pmod 3$ and $2s_2 = M_1^2 - M_2 \equiv 0 \pmod{2p}$ in (2), we have $-M_2 = N_2 - (p^2 + 1) = 2c_2p$ for some integer $|c_2| \leq 6$. Now, we have

$$2 \equiv N_2 = (p^2 + 1) + 2c_2p \equiv 2 + 2c_2 \pmod 3.$$

Since $|(p^2 + 1) - N_2| \leq 6p$, we have $c_2 = -3, 0, 3$.

Finally, let $s_3 = c_3p$ for $c_3 \in \mathbb{Z}$. Since $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod 3$ from Remark 4.1, we have

$$\sharp J_C(\mathbb{F}_p) = p^3 + 1 + c_2p(1 + p) - c_3p$$

$$\equiv 2 - c_3 \equiv 0 \pmod 3.$$

Hence, $c_3 \equiv 2 \pmod 3$ and $M_3 = 3pc_3$ with $c_3 \le 2[\sqrt{p}] + 1$. □

Next, we consider the curve $C : y^3 = x^4 + a$ for $a \in \mathbb{F}_p$ over a finite field $\mathbb{F}_p$ and compute the explicit formula of the characteristic polynomial of C.

Remark 4.2. Let C be a Picard curve defined by an equation $y^3 = x^4 + a$, $a \in \mathbb{F}_p$ over finite field $\mathbb{F}_p$ with $p \equiv 1 \pmod 3$ and $\left(\frac{-1}{p}\right) = -1$. Then we have

(1) if $a^{(p-1)/2} = -1$, then 9 divides $\sharp J_C(\mathbb{F}_p)$,
(2) if $a^{(p-1)/2} = 1$, then 3 divides $\sharp J_C(\mathbb{F}_p)$.

Theorem 4.2. *Let $C : y^3 = x^4 + a$ be a Picard curve over a finite field $\mathbb{F}_p$ with $p \equiv 1$ (mod 3) and $p \not\equiv 1$ (mod 4). Then the characteristic polynomial of the Frobenius endomorphism, $\chi(t)$, has the form*

$$\chi(t) = t^6 - c_1 t^5 + c_2 p t^4 - c_3 p t^3 + c_2 p^2 t^2 - c_1 p^2 t + p^3$$

where $c_2 \in \mathbb{Z}$ satisfying $c_2 \equiv 2$ (mod 3) with $|c_2| \le 15$, and for $c_2, c_3 \in \mathbb{Z}$,

$$\begin{aligned} &c_1 \equiv 1 \ (mod\ 3) \ \textit{and} \ c_3 \equiv 2 \ (mod\ 3) && \textit{if}\ a^{(p-1)/2} = 1, \\ &c_1 \equiv 2 \ (mod\ 3) \ \textit{and} \ c_3 \equiv 1 \ (mod\ 3) && \textit{if}\ a^{(p-1)/2} = -1, \end{aligned}$$

where $|c_1| \le 6\sqrt{p}$ and $|c_3| \le 20\sqrt{p}$.

Proof. If $p \equiv 1 \pmod 3$ and $p \not\equiv 1 \pmod 4$, then the coefficients of the Hasse-Witt matrix H for the curve C are equal to

$$c_{2p-2,p-1} = \binom{\frac{2p-2}{3}}{\frac{p-1}{2}} a^{\frac{p-1}{6}} \text{ and } c_{i,j} = 0 \text{ otherwise.}$$

From the Theorem 3.2, the coefficients of $P(t)$ are

$$s_1 \equiv c_{2p-2,p-1} \pmod p, \ \ s_2 \equiv s_3 \equiv 0 \pmod p.$$

We prove the case of $a^{(p-1)/2} = 1$. Since there exists a primitive cubic root of unity $\mathbb{F}_p$ and $f(x)$ splits into two factors of degree 2, we have $N_1 \equiv 1 \pmod 3$. Then we get $s_1 \equiv 1 \pmod 3$ with $|s_1| \le 6\sqrt{p}$.

Since $N_2 \equiv 2 \pmod 3$ and $2s_2 = M_1^2 - M_2 \equiv 0 \pmod{2p}$ in (2), we have $M_1^2 - M_2 = 2c_2 p$ for some integer $|c_2| \le 15$. Then we have

$$1 \equiv M_1^2 - (p^2 + 1) + N_2 = 2c_2 p \equiv 2c_2 \pmod p.$$

Thus, we get $c_2 \equiv 2 \pmod 3$ with $|c_2| \le 15$.

Finally, let $s_3 = c_3 p$ for $c_3 \in \mathbb{Z}$. Since $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod 3$ from Remark 4.2, we have

$$\begin{aligned} \sharp J_C(\mathbb{F}_p) &= 1 + p^3 - c_1(1 + p^2) + c_2 p(1 + p) - c_3 p \\ &\equiv 1 - c_3 \pmod 3 \end{aligned}$$

Hence, $c_3 \equiv 1 \pmod 3$ with $|c_3| \le 20\sqrt{p}$.

For the case of $a^{(p-1)/2} = -1$, $f(x)$ splits a factor of degree 2 and two factors of degree 1. So we have $s_1 \equiv 2 \pmod 3$. By equation (2) and Remark 4.2, we can show this case in the same way. $\square$

Example 4.3. Consider the curve $C : y^3 = x^4 + 123421$ over $\mathbb{F}_p$ with $p = 161375359$. Then we have that the coefficients of the characteristic polynomial of C are $c_1 = 20873$, $c_2 = 2$, and $c_3 = 20873$. Hence $\sharp J_C(\mathbb{F}_p) = 42019946240671021/80629367$.

Remark 4.3. Since $s_1 \leq 6\sqrt{p}$, if $p > 37$, then s_1 is uniquely determined by $c_{2p-2,p-1}$ in Hasse-Witt matrix. Moreover, if s_1 is determined, then there are only at most ten possibilities for the value of s_2.

If $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$, then the Hasse-Witt matrix of C has the three elements $c_{p-1,p-1}$, $c_{2p-2,p-1}$ and $c_{p-1,2p-2}$. Then we can obtain the three coefficients of the characteristic polynomial $\chi(t)$ for modulo p by Theorem 3.2.

5. Implementation details

5.1. Gaudry-Schost algorithm. Now, we show how to determine the order of the Jacobian of a Picard curve using the Gaudry-Schost algorithm [9]. Gaudry and Schost give a low-memory algorithm of Matsuo, Chao, Tsujii for genus 2 hyperelliptic curves.

We denote by L_i (U_i) the lower (upper) bound of s_i for $i = 1, 2, 3$ in (4). According to Theorem 3.2, we denote that for $i = 1, 2, 3$

$$s_i = s_i' + t_i p \tag{5}$$

with $s_i', t_i \in \mathbb{Z}$ $(0 \leq s_i' < p)$. Then each t_i is bounded by

$$\lceil L_i/p \rceil \leq t_i \leq \lfloor U_i/p \rfloor.$$

We substitute (5) into (1) and denote $M = 1 + p^3 - s_1'(1+p^2) + s_2'(1+p) - s_3'$. Then, the order of the Jacobian obeys the equation

$$\sharp J_C(\mathbb{F}_p) = M - t_1 p(1+p^2) + t_2 p(1+p) - t_3 p.$$

Let D be a random divisor of $J_C(\mathbb{F}_p)$. Since $\chi(1) \cdot D = 0$, we have

$$M \cdot D + (-t_1 p(1+p^2) + t_2 p(1+p) - t_3 p) \cdot D = 0.$$

We should determine the values (t_1, t_2, t_3) in order to get $\sharp J_C(\mathbb{F}_p)$. Assume that a prime $p > 37$. From Remark 4.3, there are several choices for t_2 and still many more for t_3. Let $M' = M - t_1 p(1+p^2)$.

Define the tame set

$$T = \{(n_2(1+p) - n_3)p \cdot D | \lceil L_2/p \rceil \leq n_2 \leq \lfloor U_2/p \rfloor, \lceil L_3/p \rceil \leq n_3 \leq \lfloor U_3/p \rfloor\},$$

and the wild set

$$W = \{M' \cdot D + (n_2(1+p) - n_3)p \cdot D | \lceil L_2/p \rceil \leq n_2 \leq \lfloor U_2/p \rfloor, \lceil L_3/p \rceil \leq n_3 \leq \lfloor U_3/p \rfloor\}.$$

We run a large number of pseudorandom walks. A tame walk and wild walk are sequences of divisors in tame set T and wild set W, respectively. Each walk proceeds until a distinguished point is hit. This distinguished point is then stored in an easily searched structure, together with the corresponding 2-tuple of (n_2, n_3). The algorithm require the computation of $O(N)$ point multiples, where N is the number of search space. i.e., $N \approx \sqrt{2^2 U_2 U_3 / p^2}$.

By Theorem 4.2, there are $400\sqrt{p}/3$ choices for candidates (c_1, c_2, c_3). Hence expected running time of our algorithm is $O(11.547p^{1/4})$. By Theorem 4.1, the expected running time is $O(p^{\frac{1}{4}})$.

The following techniques speed up the algorithm during its implementation: Flon and Oyono provided suggestions for the efficient arithmetic on Jacobians of Picard curves over finite fields [4]. Using this method, the addition operation in a Jacobian can be computed by performing 144 multiplications and 2 inversions and squaring 12 times. The Doubling can be obtained as 158 multiplications, 2 inversions and squaring 16 times. Moreover, we can easily make an inversion algorithm on the Jacobian of a Picard curve over a finite field. In our algorithm, the precomputation of p and the addition of a divisor pN times are needed, and a double-and-add method is used for these operations. As the same divisors are repeatedly computed, we store them at first and subsequently execute the comparison test. In comparison part, two divisors are identical and therefore, their conics are the same. Hence we can then avoid the computation for the inversion of a divisor.

5.2. Computational results. We implement our algorithm in C++ using Shoup's NTL library on a Pentium 2.13 GHz computer with less than 2 GB memory. The NTL helps performing the arithmetic of finite fields and polynomials using a FFT algorithm.

Example 5.1. Let $p = 18987816139962349$ be a 55-bit prime and let curve C over $\mathbb{F}_p$ be defined by

$$C \; : \; y^3 = x^4 + 12339674275x.$$

We compute the group order of the Jacobian:

$$\begin{aligned} &6845813339217962025886182834432914559053454455811 \\ &= 3 \cdot 2281937779739320675295394278144304853017818151937 \end{aligned}$$

The number of the Jacobian is of 162 bits and its quasiprime factor is of 160 bits. The total time is 97 s.

The results of our study show that our algorithm considers a lager number of bits as compared the group size in [5].

6. Conclusions

In this study, using the Gaudry-Schost method, we have presented an algorithm for computing the orders of Jacobians of genus 3 nonhyerelliptic curves defined by $y^3 = x^4 + ax$ over a finite field, $\mathbb{F}_p$, with $p \equiv 4$ or 7 modulo 9. The complexity of the algorithm is $O(p^{\frac{1}{4}})$. Moreover, we obtained some implementation results by considering a feasible cryptographic size using our algorithm. We also provide the explicit formula of the characteristic polynomial of the Frobenius endomorphism of the Jacobian of genus 3 nonhyperelliptic curves $C : y^3 = x^4 + a$ over $\mathbb{F}_p$ with $p \equiv 1 \pmod 3$ and $p \not\equiv 1 \pmod 4$.

References

1. A. Weng, *A low-memory algorithm for point counting on Picard curves*, Designs, Codes and Cryptography **38** (2006), 383–393.
2. M. Bauer, E. Teske and A. Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), 1983–2005.
3. K. Koike and A. Weng, *Construction of CM Picard curves*, Math. Comp. **74** (2005), 499–518.
4. S. Flon and R. Oyono, *Fast arithmetic on Jacobians of Picard curves*, LNCS 2947 (2004), Springer-Verlag, 55–68.
5. J. E-Sarlabous, J. P. Cherdieu, E. R-Barreiro and R.-P. Holzapfel, *The emergence of Picard Jacobians in cryptography*, Fourth Italian-Latin American Conference on Applied and Industrial Mathematics (2001), 266–275.
6. P. Gaudry and S. M. Paulus, and N. Smart, *Arithmetic on superelliptic curves*, Math. Comp. **71** (231) (2002), 393–405.
7. P. Gaudry and N. Gürel, *An extension of Kedlaya's point counting algorithm to superelliptic curves*, Advances in Cryptology-ASIACRYPT 2001, LNCS 2248 (2001), Springer-Verlag, 480–494.
8. P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, ANTS-IV, W. Bosma ed., LNCS 1838 (2000), Springer-Verlag, 297–312.
9. P. Gaudry and E. Schost, *A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm*, Proceedings of Algorithm Number Theory Symposium-ANTS VI, LNCS 3076, Springer-Verlag, 208–222.
10. I. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Math. Soc. Lecture Note Series **265** (1999).
11. T. Satoh, *The canonical lift of an ordinary elliptic curve over a prime field and its point counting*, Journal of the Ramanujan Mathematical Society **15** (2000), 247–270.
12. J. Estrada Sarlabous, On the Jacobian varieties of Picard curves defined over fields of characteristic $p > 0$, Math. Nachr. **152** (1991), 392–340.
13. K. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society **16** (2001), 323–338.
14. N. Koblitz, *Hyperelliptic curve cryptosystems*, J. Cryptology **1** (1989), 139–150.
15. N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209.
16. V. Miller, *Uses of elliptic curves in cryptography*, Advances in Cryptology: Crypto'85, LNCS 218 (1986), Spinger-Verlag, 417–426.
17. R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494.
18. Yu. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, AMS Trans. Ser. 2 **45** (1965), 245–264.

Gyoyong Sohn received the Ph.D degree in mathematics from Kyungpook National University in 2008. He has been a Post-doctoral course in School of Electrical Engineering and Computer Science at Kyungpook National University since 2010. His research interests include computational algebraic geometry and cryptography.

School of Electrical Engineering and Computer Science, Kyungpook National University, Deagu, Korea
e-mail: gyongsohn@gmail.com