Speeding up Scalar Multiplication in Genus 2 Hyperelliptic Curves with Efficient Endomorphisms

Tae Jun Park, Mun-Kyu Lee, Kunsoo Park, and Kyo Il Chung

This paper proposes an efficient scalar multiplication algorithm for hyperelliptic curves, which is based on the idea that efficient endomorphisms can be used to speed up scalar multiplication. We first present a new Frobenius expansion method for special hyperelliptic curves that have Gallant-Lambert-Vanstone (GLV) endomorphisms. To compute *kD* for an integer *k* and a divisor *D*, we expand the integer *k* by the Frobenius endomorphism and the GLV endomorphism. We also present improved scalar multiplication algorithms that use the new expansion method. By our new expansion method, the number of divisor doublings in a scalar multiplication is reduced to a quarter, while the number of divisor additions is almost the same. Our experiments show that the overall throughputs of scalar multiplications are increased by 15.6 to 28.3 % over the previous algorithms when the algorithms are implemented over finite fields of odd characteristics.

Keywords: Hyperelliptic curve, scalar multiplication, Frobenius expansion.

Manuscript received Nov. 22, 2004; revised May 9, 2005.

This work was partially supported by Inha University Research Grant. The material in this work was in part presented at ICISC 2003 [1].

Tae Jun Park (phone: +82 42 860 1368, email: papswann@etri.re.kr), and Kyo Il Chung (email: kyoil@etri.re.kr) are with Information Security Research Division, ETRI, Daejeon, Korea.

Mun-Kyu Lee (email: mklee@inha.ac.kr) is with School of CSE, Inha University, Incheon, Korea.

Kunsoo Park (email: kpark@theory.snu.ac.kr) is with School of CSE, Seoul National University, Seoul, Korea.

I. Introduction

Since Diffie and Hellman introduced the idea of public key cryptography [2], various public key cryptosystems have been proposed, and they now have numerous applications in such areas as electronic banking, electronic commerce, network authentication, and so on. In particular, a recent remarkable growth in the market of mobile banking and mobile commerce has brought up the need of public key mechanisms optimized for resource-constrained devices. Hence, many standard bodies are adopting elliptic curve cryptography (ECC) in their public key cryptography standards, since ECC requires only a small amount of memory to store cryptographic keys. For example, 160-bit ECC is equivalent to 1024-bit RSA from the viewpoint of cryptanalysis.

On the other hand, hyperelliptic curve cryptography (HECC) has been introduced by Koblitz [3] as a generalization of ECC (an elliptic curve can be viewed as a genus 1 hyperelliptic curve). Although HECC is attractive to designers of resource-constrained systems since it requires smaller fields than ECC, it has been believed to be less practical than ECC due to its poor performance. However, recent implementations of HECC, for example [4], have achieved a performance comparable to that of ECC, making HECC a good alternative.

The most time consuming operation in HECC is a scalar multiplication by an integer k, that is, computing kD for a divisor D on the Jacobian of a curve. In this paper, we will present a method to speed up this operation.

We begin by examining existing methods. In elliptic curves, Koblitz [5] proposed curves that are defined over the binary field but whose coordinates are on suitably large extension fields, which are called Koblitz curves. The idea of elliptic Koblitz curves was improved by an extensive research [6]-[10], and was generalized to hyperelliptic curves by Günter, Lange, and Stein [11]. They investigated two special examples of genus 2 curves defined over a binary field using the Frobenius map. Lange [12] gave a detailed investigation on small genus hyperelliptic Koblitz curves defined over small fields using the Frobenius map. In Lange [12] and Choie and Lee [13], the Frobenius expansion method was generalized to the finite field of any characteristic.

Gallant, Lambert, and Vanstone [14] introduced a decomposition method (GLV) using special elliptic curves that have efficiently computable endomorphisms other than Frobenius maps. The idea of their method is to decompose an integer k into two components such that the size of each component is half that of k. Sica and others [15] improved the bound of these two components of the decomposition. And Park, Jeong, and Lim [16] extended the GLV method [14] to hyperelliptic curves that have efficiently computable endomorphisms in their own way.

In this paper, we propose a new Frobenius expansion method for hyperelliptic curves with efficiently computable endomorphisms. To compute kD for an integer k and a divisor D, we expand the integer k by the Frobenius endomorphism φ, that is, $k=\sum_{i=0}^{l} r_i\varphi^i$, where the coefficients r_i are of the form $r_{i0}+r_{i1}\rho+r_{i2}\rho^2+r_{i3}\rho^3$ or $r_{i0}+r_{i1}\gamma+r_{i2}\gamma^2+r_{i3}\gamma^3$ ($r_{ij}\in\mathbb{Z}$), and ρ and γ are efficiently computable endomorphisms used in [16]. Park, Lee, and Park [17] gave a similar Frobenius expansion method in elliptic curves.

Our method can be used to improve the known scalar multiplication algorithms for hyperelliptic curves that use the Frobenius expansion [12], [13]. While the methods of [12] and [13] focused on small characteristic fields, our method is applied to the fields of large characteristic, for example, optimal extension fields (OEFs). When our method is applied to known scalar multiplication algorithms, the number of divisor doublings in a scalar multiplication is reduced to a quarter, while the number of divisor additions remains almost the same. Our experiments show that the overall throughputs of scalar multiplications are increased by 15.6 to 28.3 % over the previous algorithms when the algorithms are implemented over $\mathbb{F}_{p^n}$, where p and n are prime.

II. Preliminaries

1. Basic Definitions

We first provide the basic definitions about the arithmetic of hyperelliptic curves [3], [18]. Let $\mathbb{F}_q$ be a finite field with q elements, and let $\overline{\mathbb{F}}_q$ be its algebraic closure. A nonsingular hyperelliptic curve C of genus g over $\mathbb{F}_q$ is defined by an equation of the form

$$C:\ y^2+h(x)y=f(x)\,, \qquad (1)$$

where $h(x),\ f(x)\in\mathbb{F}_q[x]$, f is monic, $\deg_x f=2g+1$, $\deg_x h\le g$, and there are no solutions $(x,y)\in\overline{\mathbb{F}}_q\times\overline{\mathbb{F}}_q$ that simultaneously satisfy (1) and the partial derivative equations $2y+h(x)=0$ and $h'(x)y-f'(x)=0$. Let K be an extension field of $\mathbb{F}_q$ in $\overline{\mathbb{F}}_q$. The set $C(K)$ of K-rational points on C consists of all points $(x,y)\in K\times K$ that satisfy (1), together with a point at infinity denoted by ∞. Let $P=(x,y)\ne\infty$ be a point on C. The opposite of P is the point $\widetilde{P}=(x,\ -y-h(x))$.

Unlike elliptic curves, there are no natural group laws on $C(K)$ for hyperelliptic curves of genus $g\ge 2$. Therefore, the group law is defined on the Jacobian of C over $\mathbb{F}_q$ as follows. A divisor is a formal sum $D=\sum_{P\in C} m_P P$, where $m_P\in\mathbb{Z}$ and $m_P=0$ for almost all $P\in C$. The degree of D is the integer $\sum_{P\in C} m_P$. The set of all divisors, denoted by $\mathbf{D}$, forms an additive group. The set of all divisors of degree 0, denoted by $\mathbf{D}^0$, is a subgroup of $\mathbf{D}$. The divisor of a rational function $f\in\overline{\mathbb{F}}_q(C)^*$ is defined by $div(f)=\sum_P ord_P(f)P$, where $ord_P(f)$ is the order of the vanishing of f at P. A divisor $D\in\mathbf{D}^0$ is called a principal divisor if $D=div(f)$ for some rational function $f\in\overline{\mathbb{F}}_q(C)^*$. The set of all principal divisors, denoted by $\mathbf{P}$, is a subgroup of $\mathbf{D}^0$.

The quotient group $\mathbf{J}=\mathbf{D}^0/\mathbf{P}$ is called the Jacobian of curve C. The Jacobian is an abelian variety whose dimension is the genus of curve C [19]. By the Riemann-Roch theorem, every divisor $D\in\mathbf{D}^0$ can be uniquely represented as an equivalence class in $\mathbf{J}$ by a reduced divisor of the form $\sum m_i P_i-\sum m_i\infty$ with $\sum m_i\le g$. Due to Mumford [20], a reduced divisor can be represented by a pair of polynomials $u(x)$ and $v(x)\in\mathbb{F}_q[x]$ for which $\deg_x v<\deg_x u\le g$, and $v(x)^2+h(x)v(x)-f(x)$ is divisible by $u(x)$. Divisor D is the equivalence class of the GCD of the divisors of functions $u(x)$ and $v(x)-y$, denoted by $div(u, v)$.

The addition algorithms in the Jacobian were presented by Koblitz [3], and are a generalization of the earlier algorithms of Cantor [21]. Using explicit formulae in affine coordinates, one addition in a genus 2 hyperelliptic curve needs one inversion, three squarings, and 22 multiplications [22].

The scalar multiplication by an integer k is defined by $kD=\overbrace{D+D+\cdots+D}^{k}$.

The discrete logarithm problem in the Jacobian is the problem of determining $k\in\mathbb{Z}$ given two divisor classes D_1 and D_2, such that $D_2=kD_1$ if such k exists.

2. Hyperelliptic Curves with Efficient Endomorphisms

Park, Jeong, and Lim [16] collected the following hyperelliptic curves over $\mathbb{F}_q$, which have efficiently computable endomorphisms.

Example 1. Let X be a hyperelliptic curve of genus g over $\mathbb{F}_q$ given by (1). The q-th power map, called the Frobenius map,

$$\varphi : X \to X$$
$$(x, y) \to (x^q, y^q),$$

induces an endomorphism on the Jacobian. The characteristic polynomial of the Frobenius map φ is given by

$$P(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g,$$

where $a_0=1$, and $i a_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1}$ for $S_i = N_i - (q^i + 1)$, $1 \le i \le g$ and $N_i = \left| X(\mathbb{F}_{q^i}) \right|$.

Example 2. [23], [24] Let $p \equiv 1 \bmod 5$ be prime. Consider the hyperelliptic curve X_1 of genus 2 over the field $\mathbb{F}_p$ defined by

$$X_1: y^2 = x^5 + a. \tag{2}$$

The endomorphism ρ defined by $(x, y) \mapsto (\zeta_5 x, y)$ induces an efficient endomorphism on the Jacobian, where ζ_5 is a 5th root of unity. The characteristic polynomial of ρ is given by

$$P(t) = t^4 + t^3 + t^2 + t + 1.$$

The formulae for ρ on the Jacobian are given by

$$[x^2 + a_1 x + a_0,\, b_1 x + b_0] \mapsto [x^2 + \zeta_5 a_1 x + \zeta_5 a_0,\, \zeta_5^{-1} b_1 x + b_0]$$
$$[x + a_0,\, b_0] \mapsto [x + \zeta_5 a_0,\, b_0]$$
$$0 \mapsto 0.$$

Example 3. [16] Let $p \equiv 1 \bmod 8$ be prime. Consider the hyperelliptic curve X_2 of genus 2 over the field $\mathbb{F}_p$ defined by

$$X_2 : y^2 = x^5 + ax. \tag{3}$$

Then, γ on X_2 defined by $(x, y) \mapsto (\zeta_8^2 x, \zeta_8 y)$ induces an efficient endomorphism, where ζ_8 is an 8th root of unity. The characteristic polynomial of γ is given by $P(t) = t^4 + 1$. The formulae for γ on the Jacobian are given by

$$[x^2 + a_1 x + a_0, b_1 x + b_0] \mapsto [x^2 + \zeta_8^2 a_1 x + \zeta_8^4 a_0, \zeta_8^{-1} b_1 x + \zeta_8 b_0]$$
$$[x + a_0,\, b_0] \mapsto [x + \zeta_8^2 a_0,\, \zeta_8 b_0]$$
$$0 \mapsto 0.$$

3. Lattices and Endomorphism Rings

In this section, we introduce isomorphic properties between lattices and endomorphism rings of (hyper) elliptic curves. By 2- and 4-dimensional lattices in the complex plane $\mathbb{C}$, we shall mean subgroups which are free of dimension 2 and 4 over $\mathbb{Z}$, respectively. If $\{w_1, w_2\}$ is a basis of 2-dimensional lattice L over $\mathbb{Z}$, then we write $L = [w_1, w_2]$. The fundamental parallelogram for $L = [w_1, w_2]$ is the set consisting of all points $t_1 w_1 + t_2 w_2$, where $0 \le t_i \le 1$.

Similarly, if $\{w_1, w_2, w_3, w_4\}$ is a basis of 4-dimensional lattice L over $\mathbb{Z}$, then we write $L = [w_1, w_2, w_3, w_4]$. The fundamental parallelogram for $L = [w_1, w_2, w_3, w_4]$ is the set consisting of all points $t_1 w_1 + t_2 w_2 + t_3 w_3 + t_4 w_4$, where $0 \le t_i \le 1$.

For a nonsupersingular elliptic curve E, its endomorphism ring $End(E)$ has a complex multiplication [25], and the structure of that ring is $\mathbb{Z}[w] = \{a + bw \mid a, b \in \mathbb{Z}\}$ [26], where w is the smallest norm in $End(E)$. We can consider $\mathbb{Z}[w]$ as the lattice $L=[1, w]$.

We introduce an important property of an endomorphism ring of Jacobian. According to Tate [27], the characteristic polynomial of the Frobenius map φ has no double roots if and only if $End(X) \otimes \mathbb{Q} \cong \mathbb{Q}(\varphi)$ and $[End(X) \otimes \mathbb{Q} : \mathbb{Q}] = 2g$. Thus, the endomorphism ring of a hyperelliptic curve with genus 2 is 4-dimensional if the characteristic polynomial of the Frobenius map φ has no double roots.

Lemma 1. If the characteristic polynomial of Frobenius map φ for X_1 in Example 2 has no double roots, then $\varphi \in \mathbb{Z}[\rho]$ and $End(X_1)$ contain the isomorphic image

$$\mathbb{Z}[\rho] = \{a + b\rho + c\rho^2 + d\rho^3 \mid a, b, c, d \in \mathbb{Z}\} \text{ of}$$
$$\mathbb{Z}[\zeta_5] = \{a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 \mid a, b, c, d \in \mathbb{Z}\}.$$

Proof. By J. Tate [27], $End(X_1)$ is 4-dimensional. We will show that $End(X_1)$ contains a 4-dimensional lattice. Let $\mathbb{Q}(\zeta_5) = \{u_0 + u_1\zeta_5 + u_2\zeta_5^2 + u_3\zeta_5^3 \mid u_i \in \mathbb{Q}\}$. It is well known that the set of all algebraic integers in $\mathbb{Q}(\zeta_5)$ is $\mathbb{Z}[\zeta_5] = \{c_0 + c_1\zeta_5 + c_2\zeta_5^2 + c_3\zeta_5^3 \mid c_i \in \mathbb{Z}\}$ [28].

The endomorphism $\rho \in End(X_1)$ can be considered as ζ_5 since $\rho^5 = I$. Thus, the ring $\mathbb{Z}[\rho]$ is isomorphic to the ring $\mathbb{Z}[\zeta_5]$ by $\rho \mapsto \zeta_5$. Since φ satisfies the characteristic polynomial $f(t) = t^4 + a_1 t^3 + a_2 t^2 + a_1 p t + p^2$, φ is represented by an algebraic integer, that is, $\varphi \in \mathbb{Z}[\rho]$.

It is obvious that $\mathbb{Z}[\rho]$ is a subring of $End(X_1)$. □

Lemma 2. If the characteristic polynomial of Frobenius map φ for X_2 in Example 3 has no double roots, then $\varphi \in \mathbb{Z}[\gamma]$ and $End(X_2)$ contain the isomorphic image

$$\mathbb{Z}[\gamma] = \{a + b\gamma + c\gamma^2 + d\gamma^3 \mid a, b, c, d \in \mathbb{Z}\} \text{ of}$$
$$\mathbb{Z}[\zeta_8] = \{a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3 \mid a, b, c, d \in \mathbb{Z}\}.$$

Proof. Similar to Lemma 1. □

Ring $\mathbb{Z}[\zeta_5]$ is the 4-dimensional lattice $L=[1, \zeta_5, \zeta_5^2, \zeta_5^3]$; its fundamental parallelogram has 16 points, 32 edges, 24 faces, and 8 cubes as shown in Fig. 1. Similarly, $\mathbb{Z}[\zeta_8]$ is the 4-dimensional

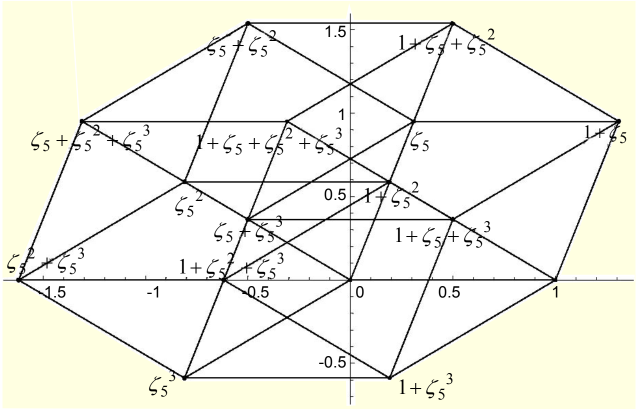


Fig. 1. Fundamental parallelogram of $\mathbb{Z}[\zeta_5]$.

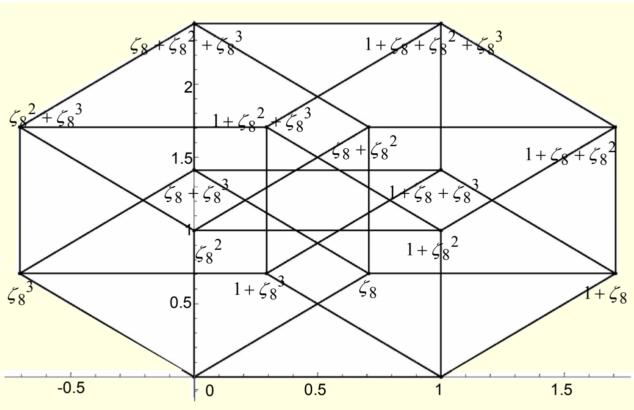


Fig. 2. Fundamental parallelogram of $\mathbb{Z}[\zeta_8]$.

lattice $L=[1,\zeta_8,\zeta_8^2,\zeta_8^3]$ as shown in Fig. 2.

In [12], the norms of vectors in 4-dimensional lattices are defined as follows. In $\mathbb{Z}[\zeta_5]$, for $z=a+b\zeta_5+c\zeta_5^2+d\zeta_5^3$,

$$\begin{aligned}N(z)^2 &= 2a^2+2b^2+2c^2+2d^2\\ &\quad -ab-ac-bc-bd-cd-da.\end{aligned} \tag{4}$$

In $\mathbb{Z}[\zeta_8]$ for $z=a+b\zeta_8+c\zeta_8^2+d\zeta_8^3$,

$$N(z)^2=2a^2+2b^2+2c^2+2d^2. \tag{5}$$

III. New Frobenius Method for Hyperelliptic Curves

1. Fifth Roots of Unity

In this section, we show that when $p\equiv 1$ mod 5, the coefficients of a Frobenius expansion can be represented using the efficient endomorphism ρ that is considered as the 5th root of unity $\zeta_5=\frac{-1+\sqrt{5}}{4}+i\frac{\sqrt{5+\sqrt{5}}}{2\sqrt{2}}$. We begin by proving the following division method.

Lemma 3. Let $p\equiv 1$ mod 5 and $s\in\mathbb{Z}[\rho]$. There exist $r,t\in\mathbb{Z}[\rho]$ such that $s=t\varphi+r$ and $N(r)\le\sqrt{10p}/2$.

Proof. By Lemma 1, φ can be written as $a+b\rho+c\rho^2+d\rho^3$ for $a,b,c,d\in\mathbb{Z}$. Note that $N(\varphi)=\sqrt{2p}$. Let $s=s_0+s_1\rho+s_2\rho^2+s_3\rho^3$ for $s_i\in\mathbb{Z}$. Then, there exists a quotient

$$x=x_0+x_1\rho+x_2\rho^2+x_3\rho^3\,(x_i\in\mathbb{Q})$$

such that $s=\varphi\cdot x$.

If we represent s as (s_0, s_1, s_2, s_3), we get

$$\begin{pmatrix}s_0\\ s_1\\ s_2\\ s_3\end{pmatrix}=A\begin{pmatrix}x_0\\ x_1\\ x_2\\ x_3\end{pmatrix},$$

where $A=\begin{pmatrix}a & -d & -c+d & -b+c\\ b & a-d & -c & -b+d\\ c & b-d & a-c & -b\\ d & c-d & b-c & a-b\end{pmatrix}$.

To find a quotient in $\mathbb{Z}[\rho]$, set $t=(\lfloor x_0\rceil, \lfloor x_1\rceil, \lfloor x_2\rceil, \lfloor x_3\rceil)$, where $\lfloor z\rceil$ means the nearest integer to z. Then, put

$$r=s-t\varphi=\begin{pmatrix}s_0\\ s_1\\ s_2\\ s_3\end{pmatrix}-A\begin{pmatrix}\lfloor x_0\rceil\\ \lfloor x_1\rceil\\ \lfloor x_2\rceil\\ \lfloor x_3\rceil\end{pmatrix}.$$

The largest norm between points in the fundamental parallelogram in $\mathbb{Z}[\rho]$ is $\sqrt{10}$. Thus, the largest norm between points in the fundamental parallelogram in $\varphi\mathbb{Z}[\rho]$ is less than or equal to $\sqrt{10p}$ since $N(\varphi\cdot x)=\sqrt{p}N(x)$ [12], as shown in Fig. 3. Thus, any lattice point of $\mathbb{Z}[\rho]$ has its nearest point of $\varphi\mathbb{Z}[\rho]$ with the distance less than or equal to $\sqrt{10p}/2$. □

The following theorem shows that the expansion using our division method given in Lemma 3 is not periodic, and its length is finite.

Theorem 1. Let $p\equiv 1$ mod 5 and $s\in\mathbb{Z}[\rho]$. Then, we can write

$$s=\sum_{i=0}^{l} r_i\varphi^i, \tag{6}$$

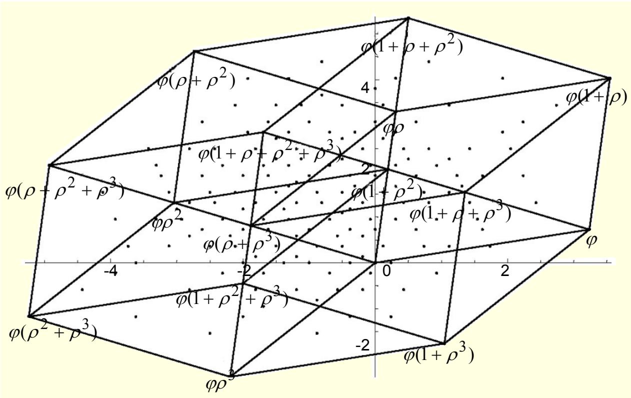


Fig. 3. Lattice points of $\mathbb{Z}[\rho]$ in the fundamental parallelogram of lattice $\varphi\mathbb{Z}[\rho]$.

where $r_i \in \mathbb{Z}[\rho]$, $N(r_i) \le \sqrt{10p}/2$, and $l \le \lceil 2\log_p N(s) \rceil$.

Proof. Let $s_0 = s$. By Lemma 3, $s_0 = s_1\varphi + r_0$. Recursively, $s_j = s_{j+1}\varphi + r_j$. Then,

$$\begin{aligned} s &= s_0 \\ &= s_1\varphi + r_0 \\ &= (s_2\varphi + r_1)\varphi + r_0 = s_2\varphi^2 + r_1\varphi + r_0 \\ &= (\sum_{i=0}^{j} r_i\varphi^i) + s_{j+1}\varphi^{j+1}, \end{aligned} \tag{7}$$

with $N(r_i) \le \sqrt{10p}/2$ for $0 \le i \le j$. Using the triangular inequality, we get

$$\begin{aligned} N(s_{j+1}) &\le \frac{N(s_j) + N(r_j)}{\sqrt{p}} \\ &\le \frac{N(s_j) + \sqrt{10p}/2}{\sqrt{p}} = \frac{N(s_j)}{\sqrt{p}} + \frac{\sqrt{10}}{2} \\ &\le \frac{N(s_{j-1})}{\sqrt{p}^2} + \frac{\sqrt{10}}{2}\left(1 + \frac{1}{\sqrt{p}}\right) \\ &\le \frac{N(s_0)}{\sqrt{p}^{j+1}} + \frac{\sqrt{10}}{2}\sum_{i=0}^{j}\left(\frac{1}{\sqrt{p}}\right)^i \\ &\le \frac{N(s_0)}{\sqrt{p}^{j+1}} + \frac{\sqrt{10}}{2}\sum_{i=0}^{j}\frac{\sqrt{p}}{\sqrt{p}-1}. \end{aligned} \tag{8}$$

Now, if $j \ge \lceil 2\log_p N(s_0) \rceil - 1$, then

$$\frac{N(s_0)}{\sqrt{p}^{j+1}} \le 1. \tag{9}$$

We see

$$1 + \frac{\sqrt{10}}{2} \cdot \frac{\sqrt{p}}{\sqrt{p}-1} < \frac{\sqrt{10p}}{2} \tag{10}$$

since $p \equiv 1 \bmod 5$ is prime, that is, $p \ge 11$. By (8), (9) and (10), we get $N(s_{j+1}) < \sqrt{10p}/2$. Setting $s_{j+1} = r_{j+1}$ in (7), we get the expansion (6) with l at most $\lceil 2\log_p N(s) \rceil$. □

For example, consider $p = 11$ and the curve $X_1 : y^2 = x^5 + 1$. Its Frobenius endomorphism can be written as $\varphi = -1 - 2\rho - 2\rho^2 - 4\rho^3$. The number of lattice points of $\mathbb{Z}[\rho]$ in the fundamental parallelogram of $\varphi\mathbb{Z}[\rho]$ is 176. But the actual number of possible remainders r in Lemma 3 is $11^2 = 121$. We can expand 37 as follows:

$$\begin{aligned} 37 = (1 - \rho - \rho^2)\varphi^3 + (\rho + 3\rho^2 + \rho^3)\varphi^2 \\ + (2 + \rho + \rho^2 + \rho^3)\varphi - 2 - \rho + \rho^2. \end{aligned}$$

2. Eighth Roots of Unity

In this section, we show that when $p \equiv 1 \bmod 8$, the coefficients of a Frobenius expansion can be represented using an efficient endomorphism γ that is considered as the 8th root of unity $\zeta_8 = \frac{1+i}{\sqrt{2}}$.

Lemma 4. Let $p \equiv 1 \bmod 8$ and $s \in \mathbb{Z}[\gamma]$. There exist $r, t \in \mathbb{Z}[\gamma]$ such that $s = t\varphi + r$ and $N(r) \le \sqrt{2p}$.

Proof. By Lemma 2, φ can be written as $a + b\gamma + c\gamma^2 + d\gamma^3$ for $a, b, c, d \in \mathbb{Z}$. Let $s = s_0 + s_1\gamma + s_2\gamma^2 + s_3\gamma^3$ for $s_i \in \mathbb{Z}$. Then, there exists a quotient

$$x = x_0 + x_1\gamma + x_2\gamma^2 + x_3\gamma^3 (x_i \in \mathbb{Q}),$$

where $s = \varphi \cdot x$. If we represent s as (s_0, s_1, s_2, s_3), we get

$$\begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix} = B \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ where } B = \begin{pmatrix} a & -d & -c & -b \\ b & a & -d & -c \\ c & b & a & -d \\ d & c & b & a \end{pmatrix}.$$

To find a quotient in $\mathbb{Z}[\gamma]$, set $t = (\lfloor x_0 \rceil, \lfloor x_1 \rceil, \lfloor x_2 \rceil, \lfloor x_3 \rceil)$.

Then, put

$$r = s - t\varphi = \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix} - B \begin{pmatrix} \lfloor x_0 \rceil \\ \lfloor x_1 \rceil \\ \lfloor x_2 \rceil \\ \lfloor x_3 \rceil \end{pmatrix}.$$

The proof of $N(r) = \sqrt{2p}$ is similar to that of Lemma 3, as can be seen in Fig. 4. □

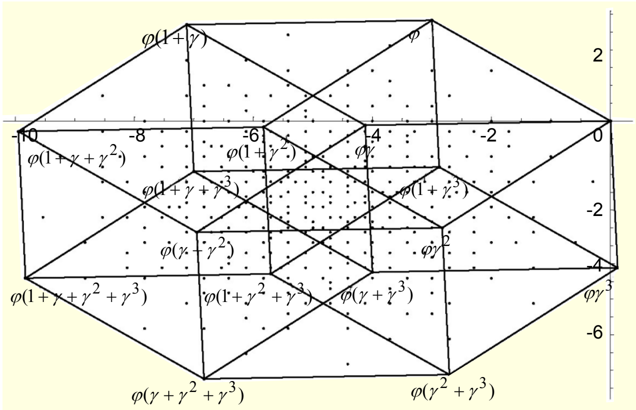


Fig. 4. Lattice points of $\mathbb{Z}[\gamma]$ in the fundamental parallelogram of lattice $\varphi\mathbb{Z}[\gamma]$.

Theorem 2 shows that the expansion using our division method given in Lemma 4 is not periodic, and its length is finite.

Theorem 2. Let $p \equiv 1 \bmod 8$ and $s \in \mathbb{Z}[\gamma]$. Then, we can write

$$s = \sum_{i=0}^{l} r_i \varphi^i, \tag{11}$$

where $r_i \in \mathbb{Z}[\gamma]$. $N(r_i) \le \sqrt{2p}$, and $l \le \lceil 2\log_p N(s) \rceil$.

Proof. Let $s_0 = s$. By Lemma 4, $s_0 = s_1\varphi + r_0$. Recursively, $s_j = s_{j+1}\varphi + r_j$. Then,

$$s = s_0 = \sum_{i=0}^{j} r_i \varphi^i + s_{j+1}\varphi^{j+1}, \tag{12}$$

with $N(r_i) \le \sqrt{2p}$ for $0 \le i \le j$. Using the triangular inequality, we get

$$N(s_{j+1}) \le \frac{N(s_0)}{\sqrt{p}^{\,j+1}} + \sqrt{2}\sum_{i=0}^{j} \frac{\sqrt{p}}{\sqrt{p}-1}. \tag{13}$$

Now, if $j \ge \lceil 2\log_p N(s_0) \rceil - 1$, then

$$\frac{N(s_0)}{\sqrt{p}^{\,j+1}} \le 1. \tag{14}$$

We see

$$1 + \sqrt{2} \cdot \frac{\sqrt{p}}{\sqrt{p}-1} < \sqrt{2p}, \tag{15}$$

since $p \equiv 1 \bmod 8$ is prime, that is, $p \ge 17$. By (13), (14) and (15), we get $N(s_{j+1}) < \sqrt{2p}$. Setting $s_{j+1} = r_{j+1}$ in (12), we get the expansion (11) with l at most $\lceil 2\log_p N(s) \rceil$. □

For example, consider $p = 17$ and the curve $X_2 : y^2 = x^5 + 2x$. Its Frobenius endomorphism can be written as $\varphi = -2\gamma - 3\gamma^2 + 2\gamma^3$. The number of lattice points of $\mathbb{Z}[\gamma]$ in the fundamental parallelogram of $\varphi\mathbb{Z}[\gamma]$ is 368. But the actual number of possible remainders r in Lemma 4 is $17^2 = 289$. We can expand 37 as follows:

$$37 = (2 + 2\gamma)\varphi^2 + (1 + 2\gamma + 2\gamma^3)\varphi + 2 + 2\gamma.$$

IV. Scalar Multiplication Algorithms

In this section, we present practical algorithms that perform scalar multiplication in hyperelliptic curves with genus 2 using our new expansion method. First, we explain a well-known algorithm that uses the Frobenius map over $\mathbb{F}_{p^n}$, that is, the hyperelliptic curve version of the Kobayashi-Morita-Kobayashi-Hoshino algorithm [29], [30], which we call hereafter algorithm KMKH. Then, we show how these algorithms can be adapted to use our new expansion method.

The following algorithm is the hyperelliptic curve version of algorithm KMKH, and it consists of three steps. The first step is the Frobenius expansion step of m, which uses Lange's expansion algorithm [12]. In the second step, the length of the expansion is reduced to n using $\varphi^n(D) = D$,[1)] and k is expanded to $k = \sum_{i=0}^{n-1} r_i \varphi^i$. The third step is a simultaneous scalar multiplication $r_0 D_0 + r_1 D_1 + \cdots + r_{n-1} D_{n-1}$ for $D_i = \varphi^i(D)$.[2)]

From now on, subscripts are used to denote array indices, and superscripts with parentheses are used to denote bit positions,

1) Note that it is possible to first reduce m modulo $(\varphi^n - 1)/(\varphi - 1)$ and then apply the first step, which produces an expansion with smaller coefficients [31], [32]. In [12], this approach is taken. However, we don't use this approach since it does not seem to bring a significant speed-up that can justify the additional complexity. It reduces the number of bits in each coefficient at most by two, but its implementation is more complicated than the above implementation of Step 2, i.e., simple integer additions.

2) For curves with very small characteristic, the cardinality of the set of possible r_i's is very small. Then, the third step can be implemented with no doublings: $\varphi(\cdots\varphi(\varphi(r_{n-1}D) + r_{n-2}D) + \cdots + r_1 D) + r_0 D$, where $D, 2D, 3D, \ldots, rD$ are precomputed for $r = \max(|r_i|)$. Note that our new expansion method is not applied to this case.

where the least significant bit is regarded as the 0th bit.

Algorithm 1.

Input: integer m, divisor D
Output: divisor $Q = mD$

Step 1: Frobenius expansion of m [12].

$i \leftarrow 0,\ c_0 \leftarrow m,\ c_1 \leftarrow 0,\ c_2 \leftarrow 0,\ c_3 \leftarrow 0.$

while ($c_0 \neq 0$ or $c_1 \neq 0$ or $c_2 \neq 0$ or $c_3 \neq 0$) do

$d \leftarrow \lfloor c_0 / p^2 \rceil,\quad u_i \leftarrow c_0 - dp^2,\quad c_0 \leftarrow c_1 - a_1 dp,$
$c_1 \leftarrow c_2 - a_2 d,\quad c_2 \leftarrow c_3 - a_1 d,\quad c_3 \leftarrow -d,$

where a_1, a_2 are from the characteristic polynomial

$\varphi^4 + a_1\varphi^3 + a_2\varphi^2 + pa_1\varphi + p^2.$
$i \leftarrow i+1.$

od.

Step 2: Optimization of the Frobenius expansion using $\varphi^n(D) = D$ [29], [30].

$r_i \leftarrow u_i + u_{i+n} + u_{i+2n} + u_{i+3n} + u_{i+4n}$ for $0 \le i < n.$ [3)]

Step 3: Scalar multiplication.

$D_i \leftarrow \varphi^i(D)$ for $0 \le i < n.$
$Q \leftarrow \infty.$

for $j \leftarrow \max_{i=0}^{n-1} \lceil \log_2 |r_i| \rceil - 1$ to 0 do

$Q \leftarrow 2Q.$
for $i = 0$ to $n - 1$ do

if ($r_i > 0$ and $r_i^{(j)} = 1$) then $Q \leftarrow Q + D_i$.

else if ($r_i < 0$ and $(-r_i)^{(j)} = 1$) then $Q \leftarrow Q - D_i$.

od.

od.

The above algorithm can be modified to use the endomorphism ρ as well as the Frobenius map as follows.

Algorithm 2

Input: integer m, divisor D
Output: divisor $Q = mD$

Step 1: Frobenius expansion of m

$i \leftarrow 0, s_0 \leftarrow m, s_1 \leftarrow 0, s_2 \leftarrow 0, s_3 \leftarrow 0.$
while ($s_0 \neq 0$ or $s_1 \neq 0$ or $s_2 \neq 0$ or $s_3 \neq 0$) do

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \leftarrow A^{-1} \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix}, \begin{pmatrix} u_{i,0} \\ u_{i,1} \\ u_{i,2} \\ u_{i,3} \end{pmatrix} \leftarrow \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix} - A \begin{pmatrix} \lfloor x_0 \rceil \\ \lfloor x_1 \rceil \\ \lfloor x_2 \rceil \\ \lfloor x_3 \rceil \end{pmatrix}, \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix} \leftarrow \begin{pmatrix} \lfloor x_0 \rceil \\ \lfloor x_1 \rceil \\ \lfloor x_2 \rceil \\ \lfloor x_3 \rceil \end{pmatrix}$$

$i \leftarrow i+1.$

od.

Step 2: Optimization of the Frobenius expansion using $\varphi^n(D) = D$.

$r_{i,j} \leftarrow u_{i,j} + u_{i+n,j} + u_{i+2n,j} + u_{i+3n,j} + u_{i+4n,j}$
for $0 \le i < n,\ 0 \le j \le 3.$ [4)]

Step 3: Scalar multiplication

$D_i \leftarrow \varphi^i(D)$ for $0 \le i < n.$
$Q \leftarrow \infty.$
for $k \leftarrow \max_{i,j} \lceil \log_2 |r_{ij}| \rceil - 1$ to 0 do

$Q \leftarrow 2Q.$
for $i = 0$ to $n - 1$ do

for $j = 0$ to 3 do

if ($r_{ij} > 0$ and $r_{ij}^{(k)} = 1$) then $Q \leftarrow Q + \rho^j(D_i)$.
else if ($r_{ij} < 0$ and $(-r_{ij})^{(k)} = 1$)
then $Q \leftarrow Q - \rho^j(D_i)$.

od.

od.

od.

Note that this algorithm can be modified easily to a version that uses endomorphism γ instead of ρ: we only have to change matrix A into B in Step 1, and change ρ into γ in Step 3.

Table 1. Comparison of the number of divisor operations.

	Algorithm 1	Algorithm 2
Expansion length (after optimization)	n	n
Number of coefficients	n	$4n$
Number of bits in each coefficient	$\max_i \lceil \log_2 \lvert r_i \rvert \rceil$ $\approx 2\log_2 p$	$\max_{i,j} \lceil \log_2 \lvert r_{ij} \rvert \rceil$ $\approx (\log_2 p)/2$
Average number of divisor additions[a)]	$\approx n\log_2 p$	$\approx n\log_2 p$
Number of divisor doublings	$\approx 2\log_2 p$	$\approx (\log_2 p)/2$
Number of Frobenius maps	n-1	n-1
Number of ρ or γ maps[b)]	0	$3n$

a) (the total number of bits) / 2
b) The costs for these operations are negligible.

3) According to Lemma 8.2 in [12], the expansion length can be slightly greater than $4n$.

4) According to Theorem 1, the expansion length can be slightly greater than $4n$.

Now, we compare the number of divisor operations in Algorithm 2 with that of Algorithm 1, as shown in Table 1. Note that in Algorithm 2, the number of coefficients is quadrupled, but the size of each coefficient is reduced to a fourth root order. Hence, the number of divisor additions is approximately the same. However, the number of divisor doublings is reduced to a quarter, which is the main improvement of our algorithm. Although Algorithm 2 needs $3n$ computations of ρ or γ maps, the required time for these operations is negligible. Finally, we remark that the required memory to store the expansion coefficients (r_i or r_{ij}) and divisors D_i is approximately the same for the two algorithms.

V. Performance Analysis

In this section, we compare the performance of the scalar multiplication algorithms described in the previous section. For the underlying fields, we consider only finite fields $\mathbb{F}_{p^n}$ that have irreducible binomials $f(x) = x^n - \omega$ as their field polynomials. The fields and curves that we have implemented are shown in Table 2. We can calculate the orders of some Jacobian groups and the characteristic polynomials of the Frobenius maps φ with the help of the program made by Lange [33], which uses MAGMA [34].

Table 3 shows the timings for scalar multiplications on a 2.66 GHz Pentium 4 CPU with 512 MB RAM using Visual C++ 6.0 compiler. For reference, we have also shown the results for the non-adjacent form scalar multiplication algorithm. As shown in Table 3, our method improves the throughput by 15.6 to 28.3 %. According to our experiments, the time required for an expansion is equivalent to only a few divisor additions.

We remark that our comparison could be done on more optimized versions of Algorithms 1 and 2, that is, we could use non-adjacent forms for each coefficient r_i or r_{ij}, a Joint Sparse Form [35], and an on-line precomputation method such as Lim and Hwang's algorithm [36]. Note that in these cases the gains are expected to be greater than those of Table 3, since these optimizations reduce only the number of divisor additions while leaving the number of doublings unchanged (that is, the portions of doublings in the overall computations become greater). However, our method does not seem to give much improvement in the divisor-known-in-advance case, since one can reduce the required number of on-line doublings by pre-computing some of the doublings in the off-line pre-computation stage.

Table 2. Implemented fields and curves.

curve	p	n	Irreducible binomial	Curve equation	Order (bits)	Endo-morphism
1	1021	17	$f(x)=x^{17}-2$	$y^2=x^5+2$	267	ρ
2	8191	13	$f(x)=x^{13}-2$	$y^2=x^5+1$	268	ρ
3	8161	17	$f(x)=x^{17}-2$	$y^2=x^5+1$	416	ρ
4	457	19	$f(x)=x^{19}-2$	$y^2=x^5+5x$	318	γ
5	761	19	$f(x)=x^{19}-2$	$y^2=x^5+2x$	336	γ

Table 3. Timings for scalar multiplications (ms).

curve	NAF	Algorithm 1	Algorithm 2	Gain[a)]
1	382.81	127.19	109.06	16.6%
2	250.00	86.40	67.35	28.3%
3	722.34	194.38	168.12	15.6%
4	543.91	149.37	120.63	23.8%
5	575.79	157.96	130.79	20.8%

a) Throughput increase of Algorithm 2 over Algorithm 1

VI. Conclusions

We have presented efficient scalar multiplication algorithms using a new Frobenius expansion method for special hyperelliptic curves with GLV endomorphisms. By replacing some divisor doublings with other efficiently computable maps, our method improves the speed of scalar multiplication by 15.6 to 28.3 %, when the algorithms are implemented over $\mathbb{F}_{p^n}$, where p and n are prime.

Note that there exist many curves with GLV endomorphisms that are suitable for cryptographic use, that is, curves that have a large prime factor in their group orders. Some example curves are given in Appendix A.

Finally, we make a short remark about the security of using extension fields $\mathbb{F}_{p^n}$ for HECC, where p and n are prime. For ECC, the security implications of the Weil-descent [37] on these types of curves are not yet clear [38]. Similarly, there is no known attack that significantly reduces the time required to compute hyperelliptic curve discrete logarithms on these curves.

Appendix A. Some Suitable Curves

There exist many curves that are suitable for cryptographic use, that is, those that have a large prime factor in their Jacobian group orders. We give some of them here.

Table A1. Curves $y^2 = x^5 + a$ over $\mathbb{F}_{p^n}$.

p	a	n	$\lvert J \rvert$, the characteristic polynomial of the Frobenius map φ
211	4	13	2699876120698661907132756440968534354370062556956720944119105=5·11·521·941·14561·1560131·44075934928 67288 828467654997293793808617561, $t^4 + 31t^3 + 661t^2 + 6541t + 44521$
241	1	13	855939575352177085753553884272196501269375032093742737849420000=2^4·5^3·31·911·151542009020958373597527 33335 791871769225151943871370031, $t^4 + 16t^3 + 46t^2 + 3856t + 58081$
		17	9740459558691879278071642854399637401600408915273205698543499104018100222627820000=2^4·5^3·31·104891·23 8886041·626987321804777160720652188364657947099117050861939624179149131, $t^4 + 16t^3 + 46t^2 + 3856t + 58081$
	3	17	974045955869187927826338276197753342825169792078312871639095777211324211562093555=3^4·5·151·15927494 98600585279742193240450908908225279686171715921247806029288405218808 1, $t^4 + 11t^3 + 411t^2 + 2651t + 58081$
	5	17	974045955869187927838499773361318117484598828710900025003171798786323692389965155=5·101·131·1472369 368708620554513641861327667020610080611761620474647678631677611204580 1, $t^4 + 31t^3 + 571t^2 + 7471t + 58081$
251	1	13	24632968898266569396334775840228868226763912536309976772078200 0=2^4·5^3·31·397305949972041441876367352 2617559391413534280049996253561, $t^4 - 4t^3 + 6t^2 - 1004t + 63001$
431	11	17	37344546120679654500221875248094525827091387790116094372231088237993081526466535707046045 5=5·31·129 1·18662475260827892606492529046297956486390338967100319518368400708624512893963936786 71, $t^4 + 31t^3 + 951t^2 +13361t + 185761$
461	1	13	180394818929264587117378003830123797642134798067264562395640055868288 0=2^8·5·151·13820431·67532924343 373538490235421589217933993135777748200040619 1, $t^4 - 44t^3 + 1086t^2 - 20284t + 212521$
		17	36798614146968034215916617651406680065751354554157038726702751039827919533392440703379340 80=2^8·5·15 1·19039018081005812404758183801431436292296851487043169871017565728387789493684002847361, $t^4 - 44t^3 + 1086t^2 -20284t + 212521$
	2	13	180394818929264585980344020255131605075933092699440110511128218747908 1=131·221261·622368915662017 15 20703 245331560230363013067352202030012882379 1, $t^4 + 19t^3 - 39t^2 +8759t + 212521$
491	1	13	929220527332812008803546715139252665209977988024125571965245550578168 0=2^4·5·3511·330824739152952153 5 18779092544592945460687121911181134991898871 61, $t^4 + 76t^3 + 2406t^2 +37316t + 241081$
	7	17	31388512296654191827836489891634642465288469320272196732182775697565323967887270074386525041=11·31· 691·1332104531944192055707291905209189048354777992720490798417134235205271121706705402701 11, $t^4 - 11t^3 - 39t^2 - 5401t + 241081$
1021	1	11	15796698381639088763419129027203363791060660927960855577428876556 80=2^8·5·11^2·71·143652317665644722 34 2232505558172831588477957746122900941291, $t^4 - 44t^3 + 2206t^2 - 44924t + 1042441$
		13	1716600735466713513867139209916276849110527017403516911968872038175647606964480=2^8·5·11·71·131·76599 91·17112313805035012518046734588191789769864668535065725464083457 41, $t^4 - 44t^3 + 2206t^2 - 44924t + 1042441$
	2	17	2027100267499919411876102556983999683464074391446837995143876575842817166714496694350681328472760 7 04661=1051^2·1361·153511·60898931·144232291576573027994268529227194603960061840880228761605835395961 4 37394493939561, $t^4 + 59t^3 + 1861t^2 + 60239t + 1042441$
8161	1	17	998331666963524465775619840537484502618680616111340149609440504955394624886636186111650422038985 69 13302097293234645111931345157792000=2^8·5^3·11·191·14849055017901065947400342701949733796684326155868 3 387316968185530014669337017519352637199851110437192142094437688081745766081, $t^4 + 76t^3 + 9766t^2 +620236t$ $+ 66601921$
	3	17	998331666963524465775619840537483059623144909200114034340295754612293311174425558807849781071347 29 660669833169282344136911614150753 05=3^4·5·31·41·131·56611·449311·58204303962263840504517043908487692 03 87705388081869445799396587689415451772421780635755342954316200604172434259986 1, $t^4 + 101t^3 + 6621t^2 +$ $824261t + 66601921$
8191	1	13	558161753386567530356642481079515447179005866471293322697709119203021228802032517449931472502568 20 2000=2^4·5^3·71·491·1171·9491·1941941·37092434480076333343013764866950699296342581291819214596488512 514 7273033693786541, $t^4 + 316t^3 + 40846t^2 + 2588356t + 67092481$

Table A2. Curves $y^2 = x^5 + ax$ over $\mathbb{F}_{p^n}$.

p	a	n	$\lvert J \rvert$, the characteristic polynomial of the Frobenius map φ
233	3	13	35583932904202122404699549210191429703958828849165564347732194=2·28097·633233670929318475365689383389533218919436752129507854001, $t^4 + 8t^3 + 32t^2 + 1864t + 54289$
		17	309101643971325034558249053383976545806788006378631831042669370159458854231108994=2·137·28097·571479889·7025704005056055050795698628104176460612, $t^4 + 8t^3 + 32t^2 + 1864t + 54289$
257	9	17	8664154603710852581745538101767290958726499060721225994384649715431091073714140036=2^2·17^2·977·7671385290497048536535416749394632745823932330027683426760694693726550695153, $t^4 + 386t^2 + 66049$
449	3	19	61004371637573399777978803270713287432992308363094379613429808026076282051691525900576739728874380914=2·99017·6308153·2265185929·21558330468296002917728602672815324504328883422912391492046751440047846150296433, $t^4 - 8t^3 + 32t^2 - 3592t + 201601$
457	5	19	119348125597239127352211185778361698907124541391518889953109292373390999394891781742150413639790344594=2·193·601·514462621008332948333999404181121700909212372261769632448118819124391124442387824015890672884529, $t^4 + 48t^3 + 1152t^2 + 21936t + 208849$
761	2	19	31089730491797053629629165686526223258322292694627170645161548718533794460473210096035833024410924136341147236=2^2·17·457·8537·117188923026787372088742832044880615221782289931614791737313775305785054987875986885295547086928474153, $t^4 + 1394t^2 + 579121$
1009	2	17	1356124780944559314025630631296625520698058750965191768750651784920544226702593056477931528006566908390=2·3·5·13·2609·10099·43793·123863·24329674687898572760228883675033427981944247396716903575491532948618622175312516429, $t^4 - 574t^2 + 1018081$

References

[1] T. Park, M. Lee, and K. Park, "Efficient Scalar Multiplication in Hyperelliptic Curves Using a New Frobenius Expansion," *Information Security and Cryptology-ICISC 2003*, vol. 2971 of LNCS, 2003, pp. 152-165.

[2] W. Diffie and M.E. Hellman, "New Directions in Cryptography," *IEEE Trans. on Information Theory*, vol. IT-22, no. 6, 1976, pp. 644-654.

[3] N. Koblitz, "Hyperelliptic Cryptosystems," *J. of Cryptology*, vol. 1, no. 3, 1989, pp. 139-150.

[4] R.M. Avanzi, "Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementations," *Cryptographic Hardware and Embedded Systems-CHES 2004*, vol. 3156 of LNCS, 2004, pp. 148-162.

[5] N. Koblitz, "CM-Curves with Good Cryptographic Properties," *Advances in Cryptology-CRYPTO 91*, vol. 576 of LNCS, 1991, pp. 279-287.

[6] W. Meier and O. Staffelbach, "Efficient Multiplication on Certain Non-Supersingular Elliptic Curves," *Advances in Cryptology-CRYPTO 92*, vol. 740 of LNCS, 1992, pp. 333-344.

[7] V. Müller, "Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two," *J. of Cryptology*, vol. 11, 1998, pp. 219-234.

[8] J.H. Cheon, S. Park, C. Park and S.G. Hahn, "Scalar Multiplication on Elliptic Curves by Frobenius Expansions," *ETRI J.*, vol. 21, no. 1, Mar. 1999, pp. 27-38.

[9] N.P. Smart, "Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic," *J. of Cryptology*, vol. 12, 1999, pp. 141-151.

[10] D.H. Lee, S. Chee, S.C. Hwang and J.-C. Ryou, "Improved Scalar Multiplication on Elliptic Curves Defined over $F_{2^{mn}}$," *ETRI J.*, vol. 26, no. 3, June 2004, pp. 241-251.

[11] C. Günter, T. Lange, and A. Stein, "Speeding up the Arithmetic on Koblitz Curves of Genus 2," *Selected Areas in Cryptography-SAC 2001*, vol. 2012 of LNCS, 2001, pp. 106-117.

[12] T. Lange, "Koblitz Curve Cryptosystems," *Finite Fields and their Applications*, vol. 11, 2005, pp. 200-229. More details can be found in T. Lange, *Efficient Arithmetic on Hyperelliptic Koblitz Curves*, doctorial dissertation, University of Essen, 2001.

[13] Y. Choie and J. Lee, "Speeding up the Scalar Multiplication in the Jacobians of cHyperelliptic Curves Using Frobenius Map," *Progress in Cryptology-INDOCRYPT 2002*, vol. 2551 of LNCS, 2002, pp. 285-295.

[14] R. Gallant, R. Lambert, and S. Vanstone, "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms," *Advances in Cryptology-CRYPTO 2001*, vol. 2139 of LNCS, 2001, pp. 190-200.

[15] F. Sica, M. Ciet, and J.-J. Quisquater, "Analysis of the Gallant-Lambert-Vanstone Method Based on Efficient Endomorphisms:

Elliptic and Hyperelliptic Curves," *Selected Areas in Cryptography-SAC 2002,* vol. 2595 of LNCS, 2003, pp. 21-36.

[16] Y. Park, S. Jeong, and J. Lim, "Speeding up Point Multiplication on Hyperelliptic Curves with Efficient-Computable Endomorphisms," *Advances in Cryptology-EUROCRYPT 2002*, vol. 2332 of LNCS, 2002, pp. 197-208.

[17] T. Park, M. Lee, and K. Park, "New Frobenius Expansions for Elliptic Curves with Efficient Endomorphisms," *Information Security and Cryptology-ICISC 2002*, vol. 2587 of LNCS, 2002, pp. 264-282.

[18] A.J. Menezes, Y.H. Wu, and R.J. Zuccherato, "An Elementary Introduction to Hyperelliptic Curves," Technical Report CORR 96-19, University of Waterloo, 1996.

[19] R. Hartshone, *Algebraic Geometry*, Springer-Verlag, 1977.

[20] D. Mumford, *Tata Lectures on Theta I*, Birkhäuser, 1983.

[21] D. Cantor, "Computing in the Jacobian of a Hyperelliptic Curve," *Mathematics of Computation*, vol. 48, 1987, pp. 95-101.

[22] T. Lange, "Formulae for Arithmetic on Genus 2 Hyperelliptic Curves," To appear in AAECC.

[23] J. Buhler and N. Koblitz, "Lattice Basis Reduction, Jacobi Sums and Hyperelliptic Cryptosystems," Bull. Austral. Math. Soc. vol. 58, 1998, pp. 147-154.

[24] L. Duursma, P. Gaudry, and F. Morain, "Speeding up the Discrete Log Computation on Curves with Automorphisms," *Advances in Cryptology -ASIACRYPT 99*, vol. 1716 of LNCS, 1999, pp. 103-121.

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

[26] T. Park, M. Lee, E. Kim, and K. Park, "A General Expansion Method Using Efficient Endomorphisms," *Information Security and Cryptology-ICISC 2003*, vol. 2971 of LNCS, 2003, pp. 264-282.

[27] J. Tate, "Endomorphisms of Abelian Varieties over Finite Fields," *Invent. Math*., vol. 2, 1966, pp. 134-144.

[28] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 3rd edition, Oxford University Press, 1954.

[29] T. Kobayashi, H. Morita, K. Kobayashi, and F. Hoshino, "Fast Elliptic Curve Algorithm Combining Frobenius Map and Table Reference to Adapt to Higher Characteristic," *Advances in Cryptology-EUROCRYPT 99*, vol. 1592 of LNCS, 1999, pp. 176-189.

[30] T. Kobayashi, "Base-φ Method for Elliptic Curves over OEF," *IEICE Trans. Fundamentals*, vol. E83-A, 2000, pp. 679-686.

[31] J. Solinas, "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves," *Advances in Cryptology-CRYPTO 97*, vol. 1294 of LNCS, 1997, pp. 357-371.

[32] J. Solinas, "Efficient Arithmetic on Koblitz Curves," *Designs, Codes and Cryptography*, vol. 19, 2000, pp. 195-249.

[33] T. Lange, "FrobSelf," Available at http://www.itsc.ruhr-uni-bochum.de/tanja/KoblitzC.html\#progs.

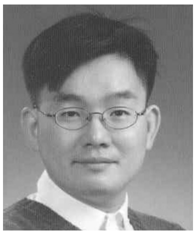
[34] MAGMA Group, "MAGMA V2.10 -The Magma Computational Algebra System," http://magma.maths.usyd.edu.au/magma/.

[35] J. Solinas, "Low-Weight Binary Representations for Pairs of Integers," Technical Report CORR 2001-41, University of Waterloo, 2001.

[36] C. Lim and H. Hwang, "Speeding up Elliptic Scalar Multiplication with Precomputation," *Information Security and Cryptology-ICISC 99*, vol. 1787 of LNCS, 1999, pp. 102-119.

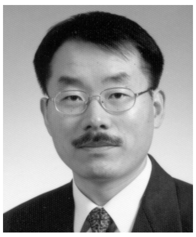
[37] P. Gaudry, F. Hess, and N. Smart, "Constructive and Destructive Facets of Weil Descent on Elliptic Curves," *J. of Cryptology,* vol. 15, 2002, pp. 19-46.

[38] H. Baier, "Elliptic Curves of Prime Order over Optimal Extension Fields for Use in Cryptography," *Progress in Cryptology-INDOCRYPT 2001*, vol. 2247 of LNCS, 2001, pp. 99-107.



Tae Jun Park received the BS degree in mathematics from Korea University in 1993 and the MS and PhD degrees in mathematics from Seoul National University in 1995 and 2001. He joined ETRI in 2004 and has worked as a Senior Engineer in the Cryptography Research Team. His research interests are in elliptic/hyperelliptic curve cryptosystems, cryptographic protocols and Privacy Enhancing Technologies (PETs).

Mun-Kyu Lee received the BS and MS degrees in computer engineering from Seoul National University in 1996 and 1998, and the PhD in electrical engineering and computer science from Seoul National University in 2003. From 2003 to 2005, he was a Senior Engineer at ETRI. He is currently with School of Computer Science and Engineering at Inha University. His research interests are in information security and theory of computation.



Kunsoo Park received the BS and MS degrees in computer engineering from Seoul National University in 1983 and 1985, and the PhD in computer science from Columbia University in 1991. From 1991 to 1993 he was a lecturer at King's College, University of London. He is currently a Professor in the School of Computer Science and Engineering at Seoul National University. His research interests include the design and analysis of algorithms, bioinformatics, and cryptography.

Kyo Il Chung received the BS, MS, and PhD degrees in electronic engineering from Hanyang University in 1981, 1983, and 1997. He joined ETRI in 1982 and has been involved with COMSEC systems. Currently, he is a Principal Member of Engineering Staff and his role is Director of Information Security Infrastructure Research Group. His research interests are in IC cards, RFID, biometrics, and information warfare.