Speeding up point multiplication on hyperelliptic curves with efficiently-computable endomorphisms.

Young-Ho Park[1]*, Sangtae Jeong[2], and Jongin Lim[3]

[1] Dept. of Information Security & System, Sejong Cyber Univ., Seoul, KOREA
youngho@cist.korea.ac.kr
[2] Dept. of Math., Seoul National Univ., Seoul, KOREA
stj@math.snu.ac.kr
[3] CIST, Korea Univ., Seoul, KOREA
jilim@korea.ac.kr

Abstract. As Koblitz curves were generalized to hyperelliptic Koblitz curves for faster point multiplication by Günter,*et al* [10], we extend the recent work of Gallant,*et al* [8] to hyperelliptic curves. So the extended method for speeding point multiplication applies to a much larger family of hyperelliptic curves over finite fields that have efficiently-computable endomorphisms. For this special family of curves, a speedup of up to 55 (59) % can be achieved over the best general methods for a 160-bit point multiplication in case of genus g =2 (3).

1 Introduction

The dominant cost operation in protocols based on the discrete logarithm problem on the Jacobians of hyperelliptic curves is point multiplication by an integer k, namely computing kD for a point D on the Jacobian. To speed up the main operation, a variety of techniques are now being in use by considering relevant objects involving curves and underlying base fields. Among other things, Koblitz [12] proposed the use of a certain family of elliptic curves, say Koblitz curves. These curves are ones defined over the binary field but considered over a suitably large extension field, with the advantage that point counting can be easily done with the help of the Frobenius endomorphism. Along this idea, Meier and Staffelbach [15], Müller [18], Smart [24], and Solinas [26, 27] have thoroughly investigated elliptic curves defined over small finite fields. In addition, the idea of Koblitz curves was generalized to hyperelliptic curves of genus 2 by Günter, Lange and Stein [10]. We also refer the reader to [14] for a detailed investigation on hyperelliptic Koblitz curves of small genus defined over small base fields.

Recently, another improvement on faster point multiplication was carried out by Gallant, Lambert, and Vanstone [8] whose method is applicable to a family

* This work was supported by Korea Research Foundation Grant(KRF-01–003-D00012) and the second author acknowledges the support of the Brain Korea 21

of elliptic curves having efficiently-computable endomorphisms. Their idea is to decompose an integer k modulo n into two components whose bit-lengths are half that of k. A precise analysis of their method showed that a speedup of up to 50% could be achieved over the best general methods for a 160-bit point multiplication.

The purpose of this paper is to extend the method of Gallant,*et al* [8] to the hyperelliptic setting. As is the case with elliptic curves, the extended method applies to a family of hyperellliptic curves having efficiently-computable endomorphisms since they also induce such endomorphisms on the Jacobians of the hyperellliptic curves. So what should be done here is to decompose an integer k modulo n into d components whose bit-lengths are $1/d$ that of n, where d is the degree of the characteristic polynomial of an efficiently-computable endomorphism on the Jacobian. Simultaneous multiple point multiplication then yields a significant speedup because of reduced bitlengths. A precise analysis shows that a speedup of up to 55 (59) % can be achieved over the best general methods for a 160-bit point multiplication when genus g =2 (3). The problem with this method is how efficiently a randomly chosen k can be decomposed into a sum of the required form. To resolve this problem we give two efficient algorithms for decomposing k. One method is a generalization of Gallant,*et al* [8]. The other is an extension of the method developed in [20].

The rest of the paper is organized as follows. In Section 2 we shall briefly summarize some basics on the Jacobians of hyperelliptic curves. In Section 3, we list up a collection of hyperellipic curves with efficient endomorphisms and provide the characteristic polynomials of such endomorphisms. Section 4 contains how to use such endomorphisms for decomposing k and there we apply known simultaneous exponentiation methods to the hyperelliptic curves and compare them. In Section 5 we generalize two decomposing methods to hyperelliptic curves. For security considerations, in Section 6, we touch on all known attacks to the DLP on hyperelliptic curves. The final Section contains our conclusions to the present work.

2 Preliminaries

2.1 Jacobians of hyperelliptic curves

We begin by introducing basic facts on the Jacobians of hyperelliptic curves over finite fields. Let $\mathbb{F}_q$ be a finite field of q elements and let $\overline{\mathbb{F}}_q$ denote its algebraic closure. A hyperelliptic curve of genus g over $\mathbb{F}_q$ is given by the Weierstrass equation of the form

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

where $h \in \mathbb{F}_q[x]$ is a polynomial of degree at most g and $f(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree $2g + 1$. Let $\mathbb{K}$ be an extension field of $\mathbb{F}_q$ in $\overline{\mathbb{F}}_q$. The set of $\mathbb{K}$-rational points on X consists of $\mathbb{K}$-solutions to the equation of X together with the point at infinity, denoted ∞.

In this Section we only mention (reduced) representations of elements on the Jacobian of a hyperelliptic curve X. We recommend the reader to consult an appendix in [13] for more details on the Jacobians. Indeed, the Jacobian of X defined over $\mathbb{K}$, denoted $\mathbb{J}_X(\mathbb{K})$ is defined as the subgroup of $\mathbb{J}_X(\overline{\mathbb{F}})$ fixed by the Galois group $\mathrm{Aut}(\overline{\mathbb{F}}/\mathbb{K})$. It is well known by the Riemann-Roch theorem that every divisor D of degree 0 on X can be uniquely represented as an equivalence class in $\mathbb{J}_X(\mathbb{K})$ by a reduced divisor of the form $\sum m_i P_i - (\sum m_i)\mathcal{O}$ with $\sum m_i \leq g$. Thus, every element D of the Jacobian can be uniquely represented by a pair of polynomials $a, b \in \mathbb{K}[x]$ for which $deg(b) < deg(a) \leq g$, and $b(x)^2 + h(x)b(x) - f(x)$ is divisible by $a(x)$. Indeed, D is the equivalence class of the g.c.d. of the divisors of the functions $a(x)$ and $b(x) - y$. The element of $\mathbb{J}_X(\mathbb{K})$ will usually be abbreviated to $[a(x), b(x)] := \mathrm{div}(a, b)$.

As for addition in the Jacobian, it can be performed explicitly with Cantor's algorithm [4]. Here we do not go into details on the algorithms for composition and reduction but mention only the complexity of the generic operations in the Jacobian. Since operations in the Jacobian can be carried out using arithmetic in $\mathbb{K}[x]$, the generic addition needs $17g^2 + O(g)$ operations in $\mathbb{K}$ whereas doubling takes $16g^2 + O(g)$ field operations (see [28]). Another remark to complexity is that an inversion can be done for free, since the opposite of $D = [a(x), b(x)]$ is given by $-D = [(a(x), -h(x) - b(x)]$.

2.2 Counting group order of Jacobians

For cryptographic purposes, it is essentially necessary to know the group order of the Jacobian of a hyperelliptic curve in designing public schemes. Computing the group order of the Jacobian is believed to be a computationally hard task because it involves counting the number of rational points of a given hyperelliptic curve over an extension field of a base field of degree up to genus. However, it is rather easy to compute the group order of the Jacobians of hyperelliptic curves with extra properties such as complex multiplication. For example, Bulher and Koblitz [3] considered an especially simple family of hyperelliptic curves of genus g of the form $y^2 + y = x^{2g+1}$ defined over the field $\mathbb{F}_p$ of p elements such that $2g + 1$ is a prime < 9. They gave a procedure to determine the group order of the Jacobians of such curves by simply evaluating a Jacobi sum associated to a certain character. We mention here that these curves have efficiently-computable endomorphisms with which we can speed up point multiplication on the Jacobians(see Ex.5 in Section 3).

3 Hyperelliptic curves with efficient endomorphisms

In this Section we first collect a family of hyperelliptic curves of genus g over $\mathbb{F}_q$ that have efficiently-computable endomorphisms ϕ. They also induce efficient endomorphisms on the Jacobians and then we compute their characteristic polynomial. Since every element of the Jacobian $\mathbb{J}_X(\mathbb{F}_q)$ can be uniquely represented by a reduced divisor with at most g points, we can explicitly give induced endomorphisms, denoted ϕ also, on reduced divisors to see that they can be efficiently computed. For simplicity, we assume for once and all that $\phi(\infty) = \infty$ for any morphism ϕ involved and that ζ_m is a primitive mth root of unity in the prime field $\mathbb{F}_p$ of p elements.

Example 1.([14]) Let X_1 be a hyperelliptic curve over $\mathbb{F}_q$ given by (1). The q-th power map, called the Frobenius, $\Phi : X_1 \to X_1$ defined by $(x, y) \to (x^q, y^q)$ then induces an endomorphism on the Jacobian. We note that the Frobenius can be computed with no further costly arithmetic over $\mathbb{F}_{q^n}$ because for a given divisor D, computing $\Phi(D)$ is just reduced to cyclic shifting provided that an extension field $\mathbb{F}_{q^n}$ is represented with respect to a normal basis. Indeed, it is computed by at most $2g$ cyclic shiftings. The characteristic polynomial of the Frobenius 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 $S_i := N_i - (q^i + 1), 1 \leq i \leq g$ and $N_i = |X_1(\mathbb{F}_{q^i})|$.

Example 2. Let $p \equiv 1 \pmod 4$. Consider the hyperelliptic curve X_2 of genus g over the field $\mathbb{F}_p$ defined by

$$X_2 : y^2 = x^{2g+1} + a_{2g-1} x^{2g-1} + \cdots a_3 x^3 + a_1 x.$$

Then the morphism ϕ on X_2 defined by $P = (x, y) \mapsto \phi(P) := (-x, \zeta_4 y)$ induces an efficient endomorphism on the Jacobian. The characteristic polynomial of ϕ on the Jacobian is given by $P(t) = t^2 + 1$. The defining formulae for ϕ on the Jacobian are given by

$$\begin{aligned} \phi : [x^2 + a_1 x + a_0, b_1 x + b_0] &\mapsto [x^2 - a_1 x + a_0, -\zeta_4 b_1 x + \zeta_4 b_0] \\ [x + a_0, b_0] &\mapsto [x - a_0, \zeta_4 b_0] \\ 0 &\mapsto 0. \end{aligned}$$

We notice that ϕ can be easily computed using at most 2 field operations in $\mathbb{F}_p$, and the Jacobian has an automorphism of order 4, which follows from the composition of ϕ with the hyperelliptic involution.

Example 3. Let $p \equiv 1 \pmod 8$. Consider the hyperelliptic curve X_3 of genus 2 over the field $\mathbb{F}_p$ defined by

$$X_3 : y^2 = x^5 + ax.$$

Then the morphism ϕ on X_3 defined by $P = (x, y) \mapsto \phi(P) := (\zeta_8^2 x, \zeta_8 y)$ induces an efficient endomorphism. The characteristic polynomial of ϕ is given by $P(t) = t^4 + 1$.

The formulae for ϕ on the Jacobian are given by

$$\begin{aligned} \phi : [x^2 + a_1 x + a_0, b_1 x + b_0] &\mapsto [x^2 + \zeta_8^2 a_1 x + \zeta_8^4 a_0, \zeta_8^{-1} b_1 x + \zeta_8 b_0] \\ [x + a_0, b_0] &\mapsto [x + \zeta_8^2 a_0, \zeta_8 b_0] \\ 0 &\mapsto 0. \end{aligned}$$

It is easily seen that ϕ can be computed using at most 4 field operations in $\mathbb{F}_p$, and the Jacobian has an automorphism of order 8.

Example 4. Let $p \equiv 1 \pmod{12}$. Consider the hyperelliptic curve X_4 of genus 3 over the field $\mathbb{F}_p$ defined by

$$X_4 : y^2 = x^7 + ax.$$

Then the morphism ϕ on X_4 defined by $P = (x, y) \mapsto \phi(P) := (\zeta_{12}^2 x, \zeta_{12} y)$ induces an efficient endomorphism on the Jacobian as follows .

$$\begin{aligned}\phi : [x^3 + a_2x^2 + a_1x + a_0, b_2x^2 + b_1x + b_0] \mapsto& \\ &[x^3 + \zeta_{12}^2 a_2 x^2 + \zeta_{12}^4 a_1 x + \zeta_{12}^6 a_0, \zeta_{12}^{-3} b_2 x^2 + \zeta_{12}^{-1} b_1 x + \zeta_{12} b_0] \\ [x^2 + a_1x + a_0, b_1x + b_0] &\mapsto [x^2 + \zeta_{12}^2 a_1 x + \zeta_{12}^4 a_0, \zeta_{12}^{-1} b_1 x + \zeta_{12} b_0] \\ [x + a_0, b_0] &\mapsto [x + \zeta_{12}^2 a_0, \zeta_{12} b_0] \\ 0 &\mapsto 0.\end{aligned}$$

It is easily seen that ϕ can be obtained using at most 6 field operations in $\mathbb{F}_p$, and the Jacobian has an automorphism of order 12. The characteristic polynomial of ϕ is given by $P(t) = t^4 - t^2 + 1$.

Example 5.([5],[3]) Let $m = 2g + 1$ be an odd prime and let $p \equiv 1 \pmod{m}$. Consider the hyperelliptic curve X_5 of genus g over the field $\mathbb{F}_p$ defined by

$$X_5 : y^2 = x^m + a.$$

The morphism ϕ defined by $P = (x, y) \mapsto \phi(P) := (\zeta_m x, y)$ induces an efficient endomorphism on the Jaconbian. It is easily seen that ϕ can be obtained using at most $2g - 1$ field operations in $\mathbb{F}_p$, and the Jacobian has an automorphism of order $2m$. The defining morphism for the action by ζ_m on the Jacobian is left to the reader. The characteristic polynomial of ϕ is given by $P(t) = t^{2g} + t^{2g-1} + \cdots + t + 1$.

4 Using an efficient endomorphism and simultaneous multi-exponentiation

4.1 Using an efficient endomorphism

Let X be a hyperelliptic curve over $\mathbb{F}_q$ having an efficiently-computable endomorphism ϕ on the Jacobian, $\mathbb{J}_X(\mathbb{F}_q)$. Let $D = [a(x), b(x)] \in \mathbb{J}_X(\mathbb{F}_q)$ be a reduced divisor of a large prime order n. The endomorphism ϕ acts as a multiplication map by λ on the subgroup $< D >$ of $\mathbb{J}_X(\mathbb{F}_q)$ where λ is a root of the characteristic polynomial $P(t)$ of ϕ modulo n. In what follows, let d denote the degree of the characteristic polynomial $P(t)$.

The problem we consider now is that of computing kD for k selected randomly from the range $[1, n - 1]$. Suppose that one can write

$$k = k_0 + k_1\lambda + \cdots + k_{d-1}\lambda^{d-1} \pmod{n}, \tag{2}$$

where $k_i \approx n^{1/d}$. Then we compute

$$\begin{aligned} kD &= (k_0 + k_1\lambda + \cdots + k_{d-1}\lambda^{d-1})D \\ &= k_0D + k_1\lambda D + \cdots + k_{d-1}\lambda^{d-1}D \\ &= k_0D + k_1\phi(D) + \cdots + k_{d-1}\phi^{d-1}(D). \end{aligned} \tag{3}$$

Since $\phi(D)$ can be easily computed and the bitlengths of components are approximately $\frac{1}{d}$ that of k, various known methods for simultaneous multiple exponentiation can be applied to (3) to yield faster point multiplication. Thus we might expect to achieve a significant speedup because a great number of point doublings are eliminated at the expense of a few addition on the Jacobian.

4.2 Analysis on simultaneous multi-exponentiation

When simultaneous multi-exponentiation methods apply to hyperelliptic settings we here focus on determining the best method by comparing running times taken by these methods. In fact, seeking the optimal one involves various factors such as bitlengths of components, the number of decomposed components and absolute memory constrains.

There are two conventional methods for simultaneous multi-exponentiation: simultaneous 2^w-ary method and simultaneous sliding window method. Recently, Möller [17] presented a method, called wNAF-based interleaving method (for short, wNAF-IM), which is applicable to groups where inverting elements is easy (e.g. elliptic curves, hyperelliptic curves). It is analyzed there that his method usually wins over the conventional methods. One reason for this is that a speedup for simultaneous multi-exponentiation is affected by storage requirements, which are given by the formula concerning the expected number of generic operations in the precomputation stage. By the formula in Table 1 below, the expected number of generic operations by the wNAF-IM is linear in the number d of decomposed components but that by other methods is more or less exponential in d, so the wNAF-IM could be preferably chosen in practical implementations of point multiplication on the Jaconians of hyperelliptic curves.

We now give a precise analysis of speedup by comparing the expected number of doublings and additions taken by the three methods above. The comparison procedure we consider here consists of two stages, the precomputation and the evaluation. Since addition on the Jacobian takes $17g^2 + O(g)$ operations in $\mathbb{F}_p$ and doubling costs $16g^2 + O(g)$ operations, we may assume that one addition takes the same cost as one doubling because for security reasons, the genus g involved is relatively small, e.g. 2 or 3(see Section 6 for security). In Table 1 we list the expected number of generic operations by three methods. Let b be the longest bitlength of components k_i and let w be the window size.

We compare the best algorithm to compute a single multiplication kD with that to compute a multi-exponentiation (3). In case of a single multiplication ($d = 1$), the NAF sliding window method [2] is known as one with best performance in general. The expected number of additions taken by this method with window size w is estimated at $b + \frac{b+1}{w+\nu(w)} + \frac{2^w-(-1)^w}{3} - 2$ where $\nu(w) = 4/3 - (-1)^w/(3 \cdot 2^{w-2})$.

In Table 2 below we give the minimum of the expected numbers of additions taken by all four methods(including a single point multiplication) for given k and d. Table 2 provides some indication of the relative benefits of simultaneous methods applied to our decomposition (3) to a single multiplication kD as in

Table 1. Expected number of generic operations by three methods for $\sum_{i=0}^{d-1} k_i D_i$ with multipliers up to b bits.

	Precomputation stage	Evaluation stage
Simultaneous 2^w-ary method	$2^{dw} - 1 - d$	$\lfloor \frac{b-1}{w} \rfloor w + b(1 - \frac{1}{2^{dw}})/w$
Simultaneous sliding window method	$2^{dw} - 2^{d(w-1)} - d$ $(w = 1)$ $2^{dw} - 2^{d(w-1)}$ $(w > 1)$	$b - 1 + b/(w + \frac{1}{2^d-1})$
wNAF-based interleaving method	0 $(w = 1)$ $d2^{w-1}$ $(w > 1)$	$b + d\frac{b}{w+2}$

elliptic curves [8]. As shown in Table 2, the contribution to running times depends on the bitlength b of k and on the degree d of the characteristic polynomial $P(t)$ of ϕ. It also shows that the wNAF-IM turns out to be the best algorithm except for two cases where $d = 1$, denoted $(*)$ below. In those cases the NAF sliding window method is the best among the methods.

Table 2. Expected number of additions to compute $\sum_{i=0}^{d-1} k_i \phi^i(D)$ where k_i is b bits

$d = 1, b = 160$	$d = 2, b = 80$	$d = 4, b = 40$	$d = 6, b = 27$
193.7 $(*w = 4)$	120 $(w = 3)$	88 $(w = 2)$	79.5 $(w = 2)$
$d = 1, b = 256$	$d = 2, b = 128$	$d = 4, b = 64$	$d = 6, b = 43$
305.3 $(*w = 5)$	186.7 $(w = 4)$	131.2 $(w = 3)$	118.6 $(w = 3)$
$d = 1, b = 512$	$d = 2, b = 256$	$d = 4, b = 128$	$d = 6, b = 86$
601.1 $(w = 5)$	357.3 $(w = 4)$	245.3 $(w = 4)$	213.2 $(w = 3)$

Table 3. The ratio of the running times of the exended method to the conventional method.

d	ratio	Examples
2	0.62	Ex.2
4	0.45	Ex.1 (g=2), Ex.3 (g=2), Ex.5 (g=2)
6	0.41	Ex.1 (g=3), Ex.5 (g=3)

Table 3 contains the ratios of running times of the extended Gallant's method to the conventional method for a 160-bit single point multiplication. It also shows that the extended method improves multiplication reasonably compared to the conventional method. For example, when $d = 6$ and $b = 27$, the extended method improves a running time up to 59 % compared with the best general methods when $d = 1$ and $b = 160$.

5 Decomposition of an integer k

We are now in a position to decompose an integer k into a sum of the form given by (2). To this end, we briefly describe a generalization of Gallant, *et al.*'s method to the hyperelliptic setting.

5.1 A general method of Gallant *et al.*'s

We retain notation of Section 4.1. An extended method of Gallant *et al.*'s is composed of two steps. Consider the homomorphism

$$f : \prod_{i=0}^{d-1} \mathbb{Z} \to \mathbb{Z}_n, \qquad \prod_{i=0}^{d-1} a_i \mapsto \sum_{i=0}^{d-1} a_i\lambda^i \pmod{n}.$$

Firstly, we find d linearly independent short vectors $v_j \in \prod_{i=0}^{d-1}\mathbb{Z}$ such that $f(v_j) = 0$ for $0 \le j \le d-1$. As a stage of precomputations this process can be done by the LLL algorithm, independently of k.

Secondly, one needs to find a vector in $\mathbb{Z}v_0 + \cdots + \mathbb{Z}v_{d-1}$ that is close to $(k, 0, \cdots, 0)$ using linear algebra. Then $(k_0, \cdots, k_{d-1})$ is determined by the equation:

$$(k_0, \cdots, k_{d-1}) = (k, 0, \cdots, 0) - (\lfloor b_0 \rceil v_0 + \cdots + \lfloor b_{d-1} \rceil v_{d-1}),$$

where $(k, 0, 0, \cdots, 0) = b_0 v_0 + \cdots + b_{d-1} v_{d-1}$ is represented as an element in $\prod_{i=0}^{d-1}\mathbb{Q}$ and $\lfloor b \rceil$ denotes the nearest integer to b. Finally, we obtain a short vector $v = (k_0, \cdots, k_{d-1})$ such that $f(v) = f((k, 0, \cdots, 0)) - f((\lfloor b_0 \rceil v_0 + \cdots + \lfloor b_{d-1} \rceil v_{d-1})) = k$ and then we have (2) as desired.

The following Lemma shows that the vector v is indeed short.

Lemma 1. *The vector* $v = (k, 0, \cdots, 0) - (\lfloor b_0 \rceil v_0 + \cdots + \lfloor b_{d-1} \rceil v_{d-1})$ *constructed as above has norm at most* $\frac{d}{2}\max\{\|v_0\|, \cdots, \|v_{d-1}\|\}$.

Proof. The statement is a generalization of Lemma 1 (d=2) in [8], so the proof proceeds in a similar way.

5.2 Another method using a division

We are now describing an alternate method for decomposing k using a division in the ring $\mathbb{Z}[\phi]$ generated by an efficiently-computable endomorphism ϕ.

Let us consider the map

$$g : \mathbb{Z}[\phi] \to \prod_{i=0}^{d-1}\mathbb{Z}, \qquad \sum_{i=0}^{d-1} a_i\phi^i \mapsto \prod_{i=0}^{d-1} a_i.$$

Then $f \circ g(\sum_{i=0}^{d-1} a_i\phi^i) = \sum_{i=0}^{d-1} a_i\lambda^i \pmod{n}$.

Firstly, we need to find $\alpha \in \mathbb{Z}[\phi]$ with short components such that $f \circ g(\alpha) = 0$. More precisely, we find a short vector $v \in \prod_{i=0}^{d-1} \mathbb{Z}$ such that $f(v) = 0$. (Note that in the Gallant's method one has to find d such short vectors which are linearly independent but here only one such vector.) Then we can obtain $\alpha = g^{-1}(v)$. Secondly, viewing an integer k as an element in $\mathbb{Z}[\phi]$ we divide k by α using Algorithm below and write

$$k = \beta\alpha + \rho$$

with $\beta, \rho \in \mathbb{Z}[\phi]$. Since $f \circ g(\alpha) = 0$ and $\alpha D = O$ for $D \in \mathbb{J}_X(\mathbb{F}_q)$, we compute

$$kD = (\beta\alpha + \rho)D = \beta\alpha D + \rho D = \rho D.$$

Writing $\rho = \sum_{i=0}^{d-1} k_i \phi^i \in \mathbb{Z}[\phi]$, the preceding equation alternately gives an desired decomposition of an integer k as in Eqn.(3). This decomposition makes use of the division process in the ring $\mathbb{Z}[\phi]$, so we now describe an efficient and practical algorithm to compute a remainder ρ of a given integer k divided by α. Let $\alpha = \sum_{i=0}^{d-1} a_i \phi^i \in \mathbb{Z}[\phi]$ with its minimal polynomial $g(t)$. Write $g(t) = t \cdot h(t) + N$ for some $h(t) \in \mathbb{Z}[t]$. It is then easy to see that $N = -\alpha h(\alpha)$ and $-h(\alpha) \in \mathbb{Z}[\phi]$. Put $\widehat{\alpha} = -h(\alpha) \in \mathbb{Z}[\phi]$.

Algorithm (Divide k by $\alpha = \sum_{i=0}^{d-1} a_i \phi^i$)

```
 Input:  $k \approx n$.
Output:  $\rho = \sum_{i=0}^{d-1} k_i \phi^i$.

     1)  Precompute $\widehat{\alpha} = N/\alpha$ in $\mathbb{Z}[\phi]$ and put $\widehat{\alpha} = \sum_{i=0}^{d-1} b_i \phi^i$.
     2)  $x_i = k \cdot b_i$  (for $i = 0,, d-1$).
     3)  $y_i = \lfloor \frac{x_i}{N} \rceil$  (for $i = 0,, d-1$).
     4)  $\rho = k - \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} a_i y_j \phi^{i+j}$.
Return:  $\rho = \sum_{i=0}^{d-1} k_i \phi^i$.
```

Proof. Assume that $k = \beta\alpha + \rho$ for some $\beta, \rho \in \mathbb{Z}[\phi]$. Then we have $k/\alpha = \beta + \rho/\alpha$. Since $k\widehat{\alpha}/\alpha\widehat{\alpha} = k\widehat{\alpha}/N$, we have

$$k/\alpha = \sum_{i=0}^{d-1} (kb_i/N)\phi^i.$$

Putting $\beta = \sum_{i=0}^{d-1} \lfloor kb_i/N \rfloor \phi^i$ gives $\rho = k - \alpha\beta$. □

Giving explicit upper bounds for components of a remainder ρ depends on the characteristic polynomial of ϕ and so it is complicated to obtain good upper bounds in general. But, for a fixed ϕ one can give explicit upper bounds for components by analyzing the above algorithm further.

Now we compare two decomposition methods. For this we apply both methods to the hyperelliptic curves in Section 3. Our implementation results show that two decompositions of an integer $k \in [1, n]$ turn out to be identically same and the bitlengths of components are approximately $1/d$ that of n. More precisely, for each curve in Section 3 (Ex.2 - 5), we select 100 random primes n of size 160-bits and for each n we carried out decompositions of 10^5 random integers $k \in [1, n]$ by two methods and see that two decompositions coincide. But it is expected that two decompositions might not be the same, as in elliptic curves [20]. As for the bitlengths of components, in Table 4 we compute the maximum of ratios of A to B where A denotes the maximum of the absolute value of decomposed components and B denotes $n^{1/d}$. These maxima tell us that the bitlengths of components are approximately $1/d$ that of n because they are < 2, which implies that A and B are within one bit.

Table 4. Numerical experiments for decomposition

Examples	Characteristic polynomial of ϕ	Maxum of ratios of A to B
Ex. 2	$P(t) = t^2 + 1$	0.704
Ex. 3	$P(t) = t^4 + 1$	1.082
Ex. 4	$P(t) = t^4 - t^2 + 1$	1.247
Ex. 5 (g=2)	$P(t) = (t^5 - 1)/(t - 1)$	1.477
Ex. 5 (g=3)	$P(t) = (t^7 - 1)/(t - 1)$	1.682

6 Security Considerations

We described a method for speeding up point multiplication, which is applicable to hyperelliptic curves with efficiently-computable endomorphisms. Such endomorphisms could be also helpful to obtain a speedup for attacks to the discrete log problems on the Jacobians [9]. In this Section we shall touch on various attacks to public-key cryptosystems based on the DLP on the Jacobians of hyperelliptic curves. Most attacks are hyperelliptic variants extending those to elliptic curves and standard finite fields. Adleman, DeMarris and Hwang [1] came up with the first-published algorithm for computing DLP, which runs in subexponential time. This algorithm applies to hyperelliptic curves over finite fields whose genus is sufficiently large relative to the size of the underlying fields. Later, Enge [6] improved their algorithm and precisely evaluated the running time. Moreover Müller, Stein and Thiel [19] extends the results to real quadratic congruence function fields of large genus.

When selecting hyperelliptic curves $X/\mathbb{F}_q$ of small genus < 4, one has to avoid curves for which special attacks are known such as the Pohlig-Hellman and the Pollard rho method. For this reason, hyperelliptic curves are believed to be ”cryptographically good” provided that the group order of the Jacobians is divisible by a large prime number $\approx$ 160-bit.

The hyperelliptic curves we have considered have a small number of automorphisms as in a family of hyperelliptic Koblitz curves. In applying the Pollard's

ρ method, Duursma, Gaudry, and Morain [5] employed an equivalence relation on points of the Jacobian via automorphisms and could speed up the attack by a factor of $\sqrt{2l}$, where l is the order of an automorphism. Gaudry [9] also gave a variant of existing index-calculus methods like [1] to achieve a more speed-up of a factor of l^2. Indeed, this method is faster than the Pollard ρ for genus > 4, and its complexity $O(q^2)$ depends on the cardinality of the base field. So the public schemes based on our curves are still intractable to this attack since these curves are hyperelliptic ones of genus 2 or 3 defined over large prime fields.

We now mention other known attacks using special features on groups. Rück [21] extended an attack on anomalous curves to hyperelliptic curves. His method works for the groups whose order is divisible by a power of p, where p is the characteristic of the base field. On the other hand, anomalous curves are investigated by Semaev [23], Smart[25], and Satoh and Araki [22].

There is the Frey-Rück attack using Tate pairing [7]. It is an extension of an attack using the Weil pairing on elliptic curves. In fact, these attacks are applied to curves over $\mathbb{F}_q$ of which group order divides $q^k - 1$ for some $k \leq 20$.

The Weil descent attack on elliptic curves has a hyperelliptic variant. To avoid this attack one must choose curves defined over extension fields of prime degree for odd characteristic and of degree $\neq 2^l - 1$ for even characteristic. For a detailed analysis on the Weil descent we refer to [11], [16].

Finally we conclude that our hyperellipic curves of small genus < 4 are intractable to all known attacks even if efficient endomorphisms may result in speedy attacks by a factor, which depends upon the number of automorphisms groups on the Jacobians as shown by Gaudry [9].

7 Conclusion

Motivated by the work of [8], we presented an extended method for accelerating point multiplication on a family of hyperelliptic curves having efficiently-computable endomorphisms. One of advantages of this method is that it improves a running time by 55 (59) % compared with the best general ordinary methods for a 160-bit point multiplication when applied to such curves of g =2 (3). Another advantage is that there is a wide range of possibility of selecting hyperelliptic curves of genus $g \leq 3$ over large prime fields rather than elliptic curves. Also we presented two algorithms for decomposing a multiplier k so that the extended method can be applicable to such curves. Computer implementations of two algorithms showed that the bitlengths of decomposition components are roughly equal to $1/d$ -bit of an integer k.

References

1. L. Adleman, J.DeMarrais, M-D. Hwang, *"A Subexponential algorithms for Discrete Logarithms over the Rational Subgroups of the Jacobians of Large Genus Hyperelliptic Curves over Finite fields",* ANTS-I, LNCS **77** (Springer) 1994, 28-40.

2. I. Blake, G. Seroussi, N. Smart: ‘Elliptic Curves in Cryptography’, London Mathematical Society Lecture Note Series. 265, Cambridge University Press, 1999.
3. J. Buhler, N. Koblitz, *”Lattice Basis Reduction, Jacobi Sums and Hyperelliptic Cryptoststems”,* Bull. Austral. Math. Soc., **57**, 147-154.
4. D. Cantor, *”Computing in the Jacobian of A Hyperelliptic curve”,* Mathematics of Computation, **48**(1987), 95-101.
5. I. Duursma, P. Gaudry, F. Morain, *”Speeding up the discrete log computation on curves with automorphisms”,* Advances in Cryptology, Asiacrypt’99 LNCS **1716** (Springer), 1999, 103-121.
6. A. Enge, *”Computing discrete logarithms in high-genus hyperelliptic Jacobian in provably subexponential time”,* University of Waterloo Technical Report CORR99-04, 2000.
7. G. Frey, H.-G. Rück, *”A Reamrk concerning m-Divisibility and the Discrete logarithm Problems in the Divisor Class Group of Curves”,* Mathematics of Computation **62**, 1994, 865-874.
8. R. Gallant, R. Lambert, S. Vanstone, *”Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms”,* Advances in Cryptology-Crypto 2001, LNCS **2139** (Springer), 2001, 190-200.
9. P. Gaudry, *”An algorithm for solving the discrete log problems on hyperelliptic curves”,* Advances in Cryptology, Eurocrypt’2000, LNCS **1807** (Springer), 2000, 19-34.
10. C. Günter, T. Lange, A. Stein, *”Speeding up the Arithmetic on Koblitz Curves of Genus Two”,* SAC 2000, LNCS **2012** (Springer), 2001, 106-117.
11. P. Gaudry, F. Hess, N.P. Smart,*”Constructive and destructive facets of Weil Decent on elliptic curve”,* Preprint (2000)
12. N. Koblitz, *”CM-curves with good cryptographic properties,”* Advances in Cryptology-Crypto’91, 1992, 279-287.
13. N. Koblitz, ’Algebraic Aspects of Cryptography’, Algorithms and Computations in Mathematics, **3**, Springer-Verlag, 1998.
14. T. Lange,’Efficient Arithmetic on Hyperelliptic Koblitz Curves’, Ph.D. Thesis, University of Essen, 2001
15. W. Meier, O. Staffelbach, *”Efficient multiplication on certain non-supersingular elliptic curves”*, Advances in Cryptology-Crypto’92, 1992, 333-344.
16. A. Menezes , M. Qu , *”Analysis of the Weil Descent Attack of Gaudry, Hess, and Smart”,* TCT-RSA 2001, LNCS **2020** (Springer) 2001, 308-318.
17. B. Möller,*”Algorithms for multi-exponentiation”*, SAC 2001, 179-194.
18. V. Müller,*”Fast multiplication in elliptic curves over small fields of characteristic two”*, Journal of Cryptology, **11**, 1998, 219-234.
19. V. Müller, A. Stein, C. Thiel,*”Computing Discrete Logarithms in Real Quadratic Congruence Function Fields of Large Genus”,* Mathematics of Computations **68**, 1999, 807-822.
20. Y.-H. Park, S. Jeong, C. Kim, J. Lim,*”An alternate decomposition of an integer for faster point multiplication on certain elliptic curves”,* to appear PKC2002.
21. R.G. Ruck,*”On the discrete logarithm in the divisor class group of curves”,* Mathematics of Computations, **68**, 1999, 805-806.
22. T. Satoh, K. Araki,*”Fermat quotients and the polynomial time discrete log algotithm for anamalous elliptic curves”,* Commentari Math. Univ. St. Pauli, **47**, 1998, 81-92.

23. I.A. Semaev,*"Evaluation of Discrete logathrims in a group of p-torsion points of an elliptic curves in characteristic p"*, Mathematics of Computations, **67**, 1998, 353-356.

24. N. Smart,*"Elliptic curve cryptosystems over small fields of odd characteristic"*, Journal of Cryptology, No 2 **12**, 1999, 141-145.

25. N. Smart, *"The Disrete Logarithm Problem on Elliptic Curves of Trace One"*, Journal of Cryptology, No 3 **12**, 1999, 193-196.

26. J. Solinas,*"An improved algorithm for arithmetic on a family of elliptic curves,"* Advances in Cryptology-Crypto '97, 1997, 357-371.

27. J. Solinas, *"Efficient arithmetic on Koblitz curves "*, Design , Codes and Cryptography, **19**, 2000, 195-249.

28. A. Stein, *"Sharp Upper Bounds for Arithmetics in Hyperelliptic Function Fields"*, Techn. Report. CORR 99-23, University of Waterloo (1999), 68 pages.