Suitable Curves for Genus-4 HCC over Prime Fields: Point Counting Formulae for Hyperelliptic Curves of type $y^2 = x^{2k+1} + ax$

Mitsuhiro Haneda[1], Mitsuru Kawazoe[2], and Tetsuya Takahashi[2]

[1] Sharp Corporation
[2] Department of Mathematics and Information Sciences,
College of Integrated Arts and Sciences,
Osaka Prefecture University,
1-1 Gakuen-cho Sakai Osaka 599-8531 Japan
{kawazoe, takahasi}@mi.cias.osakafu-u.ac.jp

Abstract. Computing the order of the Jacobian group of a hyperelliptic curve over a finite field is very important to construct a hyperelliptic curve cryptosystem (HCC), because to construct secure HCC, we need Jacobian groups of order in the form $l \cdot c$ where l is a prime greater than about 2^{160} and c is a very small integer. But even in the case of genus two, known algorithms to compute the order of a Jacobian group for a general curve need a very long running time over a large prime field. In the case of genus three, only a few examples of suitable curves for HCC are known. In the case of genus four, no example has been known over a large prime field. In this article, we give explicit formulae of the order of Jacobian groups for hyperelliptic curves over a finite prime field of type $y^2 = x^{2k+1} + ax$, which allows us to search suitable curves for HCC. By using these formulae, we can find many suitable curves for genus-4 HCC and show some examples.

1 Introduction

Let C be a hyperelliptic curve of genus g over $\mathbb{F}_q$, J_C the Jacobian variety of C and $J_C(\mathbb{F}_q)$ the Jacobian group of C which is the set of $\mathbb{F}_q$-rational points of J_C. Then $J_C(\mathbb{F}_q)$ is a finite abelian group and we can construct a public-key-cryptosystem by using DLP on it. This cryptosystem is called "hyperelliptic curve cryptosystem (HCC)". In particular, HCC obtained by using a hyperelliptic curve of genus g is called "genus-g HCC". It is said that $|J_C(\mathbb{F}_q)| = c \cdot l$ where l is a prime greater than about 2^{160} and c is a very small integer is suitable for HCC. We call a hyperelliptic curve "suitable for HCC"if its Jacobian group has such a suitable order. The advantage of HCC to an elliptic curve cryptosystem (ECC) is that we can construct a cryptosystem at the same security level as an elliptic one by using a smaller defining field. More precisely, we need a 160-bit field to construct a secure ECC, but for a genus-g HCC with $g \geq 2$, we only need about $(160/g)$-bit field. This comes from the fact that the order of the Jacobian group of a hyperelliptic curve defined over an N-bit field is about (Ng)-bit. The

merit of using higher genus HCC is its short operand size; less than 64-bit for genus ≥ 3. But due to Gaudry [9], it is recommended that the genus should be taken less than five to construct a secure HCC.

As in the case of ECC, to get a fast algorithm for adding points on the Jacobian group and to give an efficient way to produce a suitable curves for HCC are very important to construct HCC.

For the first problem, we already have many good results. See [12][16][17] for genus two, [15] for genus three and [21] for genus four.

For the second problem, we need to calculate the order of the Jacobian group. The most powerful way to solve this problem is to construct a fast point counting algorithm for any randomly given curve. However, for HCC over prime fields, there are few results in this direction even for the genus two case. In fact, a point counting algorithm for a hyperelliptic curve of genus two over 80-bit prime fields takes a very long time, e.g. a week for each curve (cf. [10]), at this moment. And this algorithm has not been generalized to the case of genus three or four.

There is a known algorithm to construct a curve with complex multiplication (CM) whose Jacobian group has a 160-bit prime factor. But this algorithm is efficient only for genus two at this moment. For genus three, only a few examples of suitable curves are constructed by this method [25]. For genus four, no example has been known over a large prime.

If the Jacobian of a curve is obtained as a reduction mod p of an abelian variety of CM type over $\mathbb{Q}$, the calculation of the order of the Jacobian group is much easier. It is based on a general theory of abelian varieties with CM. Let A be a simple abelian variety A over $\mathbb{F}_p$ with CM and assume that we know $\mathrm{End}(A)$. Since $\mathrm{End}(A)$ is an order in an imaginary quadratic extension of a totally real field whose degree is the dimension of A, the characteristic polynomial of the p-th power Frobenius endomorphism of A is in general the minimal polynomial of an element π in $\mathrm{End}(A)$ of norm p. Such an element is defined up to a root of unity. So once such an element is calculated, then the characteristic polynomial is almost determined (Only a small number of candidates!). The characteristic polynomial $\chi(t)$ gives $|A(\mathbb{F}_p)|$ by $|A(\mathbb{F}_p)| = \chi(1)$ and hence the problem is reduced to calculate $\pi \in \mathrm{End}(A)$ of norm p.

In this article, we study characteristic polynomials of curves defined by $y^2 = x^{2k+1} + ax$, $a \in \mathbb{F}_p$ and give explicit formulae giving the order of Jacobian groups of those curves. The Jacobian of such curve is obtained as a reduction mod p of an abelian variety of CM type over $\mathbb{Q}$. Our tactics for calculating the order of the Jacobi group of the curve $C : y^2 = x^{k+1} + ax$ is to calculate $|C(\mathbb{F}_{p^r})|$ for $r = 1, 2, \ldots, g$ directly. To do this, we prove Theorem 1; it reduces the calculation of $|C(\mathbb{F}_{p^r})|$ to Jacobi sums over $\mathbb{F}_p$. And as a result of it, we can determine the characteristic polynomial of the p-th power Frobenius endomorphism without ambiguity over unit elements. By using our formulae, we show that the case $k = 4$ produces suitable curves for genus-4 HCC when $p \equiv 1 \pmod{16}$ and give some examples of such curves. We can obtain explicit formulae for the case $k = 2$ and 3. But for the case $k = 3$, the genus three case, it is shown that the Jacobian splits over the base field and hence cannot produce suitable curves. So we omit

the formulae for that case. For the case $k = 2$, we should note that it was already appeared in [7] and many examples of suitable curves for HCC of genus two were found when $\left(\frac{a}{p}\right) = -1$ and $p \equiv 1 \pmod 8$. But in [7], the explicit formula was not given for the case $\left(\frac{a}{p}\right) = -1$ and $p \equiv 1 \pmod 8$. Our formula for that case gives a more efficient point counting algorithm.

In an analogous way, Buhler-Koblitz [2] obtained a point counting algorithm for a special curve of type $y^2 + y = x^n$ over a prime field $\mathbb{F}_p$ where n is an odd prime such that $p \equiv 1 \pmod n$. It produces suitable curves of genus two and three, but cannot produce suitable curves of genus four.

As far as we know, our examples are the first ones of suitable curves for genus-4 HCC over prime fields.

2 The characteristic polynomial and the order of the Jacobian group

Let p be an odd prime, $\mathbb{F}_q$ a finite field of order $q = p^r$ and C a hyperelliptic curve of genus g defined over $\mathbb{F}_q$. Then the defining equation of C is given as $y^2 = f(x)$ where $f(x)$ is a polynomial in $\mathbb{F}_q[x]$ of degree $2g + 1$.

Let J_C be the Jacobian variety of a hyperelliptic curve C. We denote the group of $\mathbb{F}_q$-rational points on J_C by $J_C(\mathbb{F}_q)$ and call it the Jacobian group of C. Let $\chi_q(t)$ be the characteristic polynomial of the q-th power Frobenius endomorphism of C. We call $\chi_q(t)$ for C the characteristic polynomial of C and denote it by $\chi(t)$ for the convenience. Then, it is well-known that the order $|J_C(\mathbb{F}_q)|$ is given by

$$|J_C(\mathbb{F}_q)| = \chi(1).$$

Due to Mumford [19], every point on $J_C(\mathbb{F}_q)$ can be represented by a pair $\langle u(x), v(x)\rangle$ where $u(x)$ and $v(x)$ are polynomials in $\mathbb{F}_q[x]$ with $\deg v(x) < \deg u(x) \leq g$ such that $u(x)$ divides $f(x) - v(x)^2$. The identity element of the addition law is represented by $\langle 1, 0\rangle$. By using this representation of points on $J_C(\mathbb{F}_q)$, we obtain an algorithm for adding two points on $J_C(\mathbb{F}_q)$. This algorithm was firstly given by Cantor [3] in general and has been improved for genus 2, 3 and 4 by many people [11][12][16][17][21].

In the following, for a generator g of $\mathbb{F}_p^\times$, we denote $\mathrm{Ind}_g\, a = k$ when $a = g^k$, $k = 0, 1, \ldots, p - 1$.

3 Jacobstahl sum and the key theorem

For two characters χ, ψ of $\mathbb{F}_{p^r}^\times$, the Jacobi sum $J_r(\chi, \psi)$ is defined by

$$J_r(\chi, \psi) = \sum_{t \in \mathbb{F}_{p^r}} \chi(t)\psi(1 - t).$$

For the convenience we use the following notation.

$$K_r(\chi) = \chi(4)J_r(\chi, \chi).$$

When $r = 1$, we drop the subscript J_r and K_r. For properties of Jacobi sums, see [1].

Let k be a positive integer and p a prime such that $p \equiv 1 \pmod{2k}$. Let χ_2 be a character of order 2 on a finite field $\mathbb{F}_{p^r}$. For an element a in $\mathbb{F}_p$,

$$\phi_{k,r}(a) := \sum_{x \in \mathbb{F}_{p^r}} \chi_2(x^{k+1} + ax)$$

is called a "Jacobstahl sum". It is easy to see that for a hyperelliptic curve defined by an equation $y^2 = x^{k+1} + ax$ over $\mathbb{F}_p$,

$$|C(\mathbb{F}_{p^r})| = p^r + 1 + \phi_{k,r}(a)$$

where $|C(\mathbb{F}_{p^r})|$ denotes the number of rational points of C over $\mathbb{F}_{p^r}$.

The following properties of $\phi_{k,r}$ enables us to reduce the calculation of $\phi_{k,r}(a)$ to the case $p^r \equiv 1 \pmod{2k}$.

Lemma 1. *(1) For $d = (k, p^r - 1)$, $\phi_{k,r}(a) = \phi_{d,r}(a)$.*
(2) If $p^r - 1 \equiv k \pmod{2k}$, then $\phi_{k,r}(a) = 0$.

Then we have the following theorem. This is the key theorem in our results.

Theorem 1. *Let p be a prime such that $p \equiv 1 \pmod{2k}$ for some positive integer k. For $a \in \mathbb{F}_p$,*

$$\phi_{k,r}(a) = (-1)^{r-1}\hat{\chi}(-1)\hat{\chi}^{k+1}(a)\sum_{j=0}^{k-1}\hat{\chi}^{2j}(a)K(\chi^{2j+1})^r$$

where χ is a character of $\mathbb{F}_p^\times$ of order $2k$ and $\hat{\chi}$ is a character of $\mathbb{F}_{p^r}^\times$ of order $2k$.

Proof. We proceed as in the proof of Theorem 6.1.14 [1]. Since $\hat{\chi}^k = \chi_2$,

$$\begin{aligned}\phi_{k,r}(a) &= \sum_{x \in \mathbb{F}_{p^r}} \hat{\chi}^k(x)\hat{\chi}^k(x^k + a) \\ &= \sum_{x \in \mathbb{F}_{p^r}} \hat{\chi}(x^k)\hat{\chi}^k(x^k + a).\end{aligned}$$

By the equality

$$\sum_{j=0}^{k-1}\hat{\chi}^{2j}(x) = \begin{cases} 0 & \hat{\chi}^2(x) \neq 1 \\ k & \hat{\chi}^2(x) = 1 \end{cases}$$

and the fact each fiber of the map $x \mapsto x^k$ has k elements, we have

$$\phi_{k,r}(a) = \sum_{x \in \mathbb{F}_{p^r}} \hat{\chi}(x^k)\hat{\chi}^k(x + a)\sum_{j=0}^{k-1}\hat{\chi}^{2j}(x).$$

By the change of variable $x \to -x$ and $x \to -ax$,

$$\begin{aligned}\phi_{k,r}(a) &= \hat{\chi}(-1)\hat{\chi}^{1+k}(a) \sum_{x\in\mathbb{F}_{p^r}} \hat{\chi}(x)\hat{\chi}^k(1-x) \sum_{j=0}^{k-1} \hat{\chi}^{2j}(ax) \\ &= \hat{\chi}(-1)\hat{\chi}^{1+k}(a) \sum_{j=0}^{k-1} \hat{\chi}^{2j}(a) \sum_{x\in\mathbb{F}_{p^r}} \hat{\chi}^{2j+1}(x)\hat{\chi}^k(1-x) \\ &= \hat{\chi}(-1)\hat{\chi}^{1+k}(a) J_r(\hat{\chi}^{2j+1}, \hat{\chi}^k)\end{aligned}$$

where $J_r(\psi_1, \psi_2)$ is the Jacobi sum over $\mathbb{F}_{p^r}$ defined by

$$J_r(\psi_1, \psi_2) = \sum_{x\in\mathbb{F}_{p^r}} \psi_1(x)\psi_2(1-x).$$

Since

$$J_r(\hat{\chi}^{2j+1}, \hat{\chi}^k) = \hat{\chi}^{2j+1}(4) J_r(\hat{\chi}^{2j+1}, \hat{\chi}^{2j+1}) = K_r(\hat{\chi}^{2j+1}),$$

we get the formula

$$\phi_{k,r}(a) = \hat{\chi}(-1)\hat{\chi}^{1+k}(a) K_r(\hat{\chi}^{2j+1}).$$

It follows from the Hasse-Davenport relation that

$$K_r(\psi) = (-1)^{r-1} K_1(\psi)^r.$$

Hence our Theorem. □

Combining this theorem with the following fact, we get the formula of $\chi(t)$ for the curve $C : y^2 = x^{k+1} + ax$.

Theorem 2. *Let C be a hyperelliptic curve of genus g over $\mathbb{F}_p$. Assume $\chi(t)$ for C is decomposed as*

$$\chi(t) = \prod_{i=1}^{2g} (t - \alpha_i).$$

Then

$$|C(\mathbb{F}_{p^r})| = p^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

4 Explicit Formula for $y^2 = x^5 + ax$

Let p be an odd prime and C a hyperelliptic curve defined by an equation $y^2 = x^5 + ax$ over $\mathbb{F}_p$. In [7], the explicit formulae of the order of $J_C(\mathbb{F}_p)$ are given for all cases except for the only one case $p \equiv 1 \pmod 8$ with $\left(\frac{a}{p}\right) = -1$. Here we show the explicit formula for the remaining case.

Theorem 3. *Let p be a prime such that $p \equiv 1 \pmod 8$ and C a hyperelliptic curve defined by an equation $y^2 = x^5 + ax$ over $\mathbb{F}_p$. Put $f = (p-1)/8$. Write p as $p = c^2 + 2d^2$ where $c \equiv 1 \pmod 4$ and $2d \equiv -(a^f + a^{3f})c \pmod p$. Then the characteristic polynomial of p-th power Frobenius map for C is given by the following formula:*

$$\chi(t) = t^4 + (-1)^f 4dt^3 + 8d^2t^2 + (-1)^f 4dpt + p^2.$$

In particular,

$$|J_C(\mathbb{F}_p)| = 1 + (-1)^f 4d + 8d^2 + (-1)^f 4dp + p^2.$$

Proof. This follows from Theorem 1, Theorem 2 and the formula for $K(\chi)$. (See [1]). □

This formula provides us a faster algorithm to compute the order of the Jacobian than in [7].

Remark 1. All formulae for $\chi(t)$ in this paper are obtained in the same way. Since we have not enough space, we omit the proofs for those formulae.

5 Remark on $y^2 = x^7 + ax$

Unfortunately the Jacobian of a hyperelliptic curve of type $y^2 = x^7 + ax$ splits over $\mathbb{F}_p$ splits over $\mathbb{F}_p$, because for $k \equiv 0 \pmod 3$, one has a degree 3 covering from $y^2 = x^{2k+1} + ax$ to $Y^2 = X^{2k/3+1} + aX$, given by $(x, y) \mapsto (x^3, xy)$. Therefore the characteristic polynomial is reducible over $\mathbb{Z}$ and this curve is not suitable for HCC.

6 Explicit Formula for $y^2 = x^9 + ax$

Let p be an odd prime and C a hyperelliptic curve defined by an equation $y^2 = x^9 + ax$ over $\mathbb{F}_p$.

6.1 The case of $p \equiv 1 \pmod{16}$

Let p be a prime such that $p \equiv 1 \pmod{16}$. We fix a generator g of $\mathbb{F}_p^\times$. Put $f = (p-1)/16$ and $\alpha = g^{(p-1)/16}$. Then there exist integers x, u, v, w such that

$$\begin{aligned}
&p = x^2 + 2(u^2 + v^2 + w^2) \\
&x \equiv 1 \pmod 8 \\
&2xv = u^2 - 2uw - w^2 \\
&x + u(\alpha + \alpha^7) + v(\alpha^2 - \alpha^6) + w(\alpha^3 + \alpha^5) \equiv 0 \pmod p \\
&2v^2 - x^2 \equiv -(u^2 + 2uw - w^2)(\alpha^2 - \alpha^6) \pmod p.
\end{aligned} \tag{1}$$

It is known that the above x, u, v, w are uniquely determined.

Let $\chi(t) = t^8 - s_1t^7 + s_2t^6 - s_3t^5 + s_4t^4 - s_3pt^3 + s_2p^2t^2 - s_1p^3t + p^4$ be the characteristic polynomial of C. Then by using the above notation, we have the following theorems.

Theorem 4. *s_1, s_2, s_3 and s_4 are given by the following tables.*

$\mathrm{Ind}_g\, a \pmod{16}$	s_1
$1, 7$	$(-1)^f 8w$
$9, 15$	$(-1)^{f+1} 8w$
$3, 5$	$(-1)^{f+1} 8u$
$11, 13$	$(-1)^f 8u$
$2, 14$	$(-1)^{f+1} 8v$
$6, 10$	$(-1)^f 8v$
8	$(-1)^{f+1} 8x$
0	$(-1)^f 8x$
$4, 12$	0

$\mathrm{Ind}_g\, a \pmod{16}$	s_2
$1, 7, 9, 15$	$32w^2 + 16xv$
$3, 5, 11, 13$	$32u^2 - 16xv$
$2, 6, 10, 14$	$32v^2$
$0, 8$	$4p + 24x^2 - 16v^2$
$4, 12$	$-4p + 8x^2 + 16v^2$

$\mathrm{Ind}_g\, a \pmod{16}$	s_3
$1, 7$	$(-1)^{f+1} 8(pu - 4(u^3 + w^3 + u^2w - 3uw^2))$
$9, 15$	$(-1)^f 8(pu - 4(u^3 + w^3 + u^2w - 3uw^2))$
$3, 5$	$(-1)^{f+1} 8(pw + 4(u^3 - w^3 + 3u^2w + uw^2))$
$11, 13$	$(-1)^f 8(pw + 4(u^3 - w^3 + 3u^2w + uw^2))$
$2, 14$	$(-1)^{f+1}(8pv + 64v^3 - 32x^2v)$
$6, 10$	$(-1)^f(8pv + 64v^3 - 32x^2v)$
8	$(-1)^{f+1}(24px + 32x^3 - 64xv^2)$
0	$(-1)^f(24px + 32x^3 - 64xv^2)$
$4, 12$	0

$\mathrm{Ind}_g\, a \pmod{16}$	s_4
$1, 7, 9, 15$	$32u^4 + 32w^4 + 64u^2w^2 - 64puw + 128u^3w - 128uw^3$
$3, 5, 11, 13$	$32u^4 + 32w^4 + 64u^2w^2 + 64puw + 128u^3w - 128uw^3$
$2, 6, 10, 14$	$2p^2 + 16x^4 + 64v^4 - 16px^2 - 64x^2v^2 + 32pv^2$
$0, 8$	$6p^2 + 16x^4 + 64v^4 + 48px^2 - 64x^2v^2 - 32pv^2$
$4, 12$	$6p^2 + 16x^4 + 64v^4 - 16px^2 - 64x^2v^2 - 32pv^2$

Corollary 1. *If a is octic, the characteristic polynomial of C is given by*

$$\chi(t) = \left(t^4 - s_1t^3/2 + (s_2/2 - s_1^2/8)t^2 - s_1pt/2 + p^2\right)^2.$$

In particular, if a is octic, it is not suitable for HCC.

We look at the case when a is not octic. Since $\left(\frac{-1}{p}\right) = 1$, if a is square, then there is an element $b \in \mathbb{F}_p$ such that $b^2 = -a$. Then $x^9 + ax$ factors into $x(x^4 + b)(x^4 - b)$ and we have that $|J_C(\mathbb{F}_p)|$ is divided by at least 4. Moreover if a is quartic, $|J_C(\mathbb{F}_p)|$ is divided by at least 16.

If a is not square, it is possible to obtain a Jacobian group whose order is in the form $2l$ where l is prime.

6.2 The case of $p \equiv 7 \pmod{16}$

Let p be a prime such that $p \equiv 7 \pmod{16}$. Then there exist integers x, u, v, w such that

$$\begin{aligned} &p = x^2 + 2(u^2 + v^2 + w^2) \\ &x \equiv 1 \pmod 8 \\ &2xv = u^2 - 2uw - w^2, \\ &u \equiv v \equiv w \equiv 1 \pmod 2. \end{aligned} \tag{2}$$

Let $\chi(t) = t^8 - s_1 t^7 + s_2 t^6 - s_3 t^5 + s_4 t^4 - s_3 p t^3 + s_2 p^2 t^2 - s_1 p^3 t + p^4$ be the characteristic polynomial of C. Then, for a fixed generator g of $\mathbb{F}_p^\times$, we have the following theorem.

Theorem 5. *The characteristic polynomial of C is determined by the following formula.*

1. $s_1 = s_3 = 0$,
2. $s_2 = (-1)^{\mathrm{Ind}_g\, a}(4p - 8x^2 - 16v^2)$,
3. $s_4 = 6p^2 + 16x^4 + 64v^4 - 16px^2 - 64x^2v^2 - 32pv^2$.

Remark 2. There is some ambiguity with respect to u, w and the sign of v. But it does not affect to determine the characteristic polynomial of C.

Corollary 2. *If a is square, the characteristic polynomial of C is given by*

$$\begin{aligned} \chi(t) = &(t^4 + 4xt^3 + (2p + 4x^2 - 8v^2)t^2 + 4xpt + p^2) \\ &\times (t^4 - 4xt^3 + (2p + 4x^2 - 8v^2)t^2 - 4xpt + p^2). \end{aligned}$$

In particular, if a is square, it is not suitable for HCC.

We look at the case when a is not square. From Theorem 5, we have that $|J_C(\mathbb{F}_p)|$ is divided by at least 2^7.

6.3 The case of $p \not\equiv 1, 7 \pmod{16}$

Theorem 6. *If $p \equiv 3, 11 \pmod{16}$, then the characteristic polynomial of C is given by $\chi(t) = (t^4 + (-1)^{\mathrm{Ind}_g\, a} p^2)^2$.*

Theorem 7. *Assume that* $p \equiv 5, 13 \pmod{16}$. *Then the characteristic polynomial of* C *is given by the following formula.*

1. *If* $\mathrm{Ind}_g\, a \not\equiv 0 \pmod 2$, *then* $\chi(t) = t^8 + p^4$,
2. *if* $\mathrm{Ind}_g\, a \equiv 0 \pmod 4$, *then* $\chi(t) = (t^4 + p^2)^2$,
3. *if* $\mathrm{Ind}_g\, a \equiv 2 \pmod 4$, *then* $\chi(t) = (t^2 - p)^2(t^2 + p)^2$.

Theorem 8. *Assume that* $p \equiv 9 \pmod{16}$. *Then the characteristic polynomial of* C *is given by the following formula.*

1. *If* $\mathrm{Ind}_g\, a \not\equiv 0 \pmod 2$, *then* $\chi(t) = t^8 + p^4$,
2. *if* $\mathrm{Ind}_g\, a \equiv 2 \pmod 4$, *then* $\chi(t) = (t^4 + p^2)^2$,
3. *if* $\mathrm{Ind}_g\, a \equiv 4 \pmod 8$, *then* $\chi(t) = (t^2 - p)^4$,
4. *if* $\mathrm{Ind}_g\, a \equiv 0 \pmod 8$, *then* $\chi(t) = (t^2 + p)^4$.

Theorem 9. *If* $p \equiv 15 \pmod{16}$, *then the characteristic polynomial of* C *is given by* $\chi(t) = (t^2 + p)^4$.

In particular, for $p \not\equiv 1, 7 \pmod{16}$, C is a supersingular curve which is not recommended to use for HCC.

6.4 Which parameter is suitable for HCC?

From the above results, all the cases which can produce suitable curves for HCC are the followings:

1. $p \equiv 1 \pmod{16}$ with a not square,
2. $p \equiv 1 \pmod{16}$ with a square but not quartic,
3. $p \equiv 1 \pmod{16}$ with a quartic but not octic,
4. $p \equiv 7 \pmod{16}$ with a not square.

In each case, the best possible order is in the form (1) $2l$, (2) $4l$, (3) $2^4 l$ and (4) $2^7 l$ where l is prime.

Now we consider splitting of the Jacobian over extension fields. Let $\chi(t)$ be the characteristic polynomial of a hyperelliptic curve C over $\mathbb{F}_p$. In the following, we denote by $\chi_{p^r}(t)$ the characteristic polynomial of the p^r-th power Frobenius endomorphism of C as a curve over $\mathbb{F}_{p^r}$.

Proposition 1. *Let* $\chi(t) = t^8 - s_1 t^7 + s_2 t^6 - s_3 t^5 + s_4 t^4 - s_3 p t^3 + s_2 p^2 t^2 - s_1 p^3 t + p^4$ *be the characteristic polynomial of a hyperelliptic curve* C *of genus four over* $\mathbb{F}_p$. *If* $\chi(t)$ *is irreducible over* $\mathbb{Q}$, *then*

1. $\chi_{p^2}(t)$ *is a product of two polynomials of degree four if and only if* $s_1 = s_3 = 0$,
2. $\chi_{p^4}(t)$ *is a product of four polynomials of degree two if and only if* $\chi_{p^2}(t)$ *is a product of two polynomials of degree four.*

Proof. Let γ be a root of $\chi(t)$. We have only to show that if $[\mathbb{Q}(\gamma^2) : \mathbb{Q}] = 4$, $s_1 = s_3 = 0$. Since $\gamma\bar{\gamma} = p$, we can show $(\gamma^2 + \bar{\gamma}^2)^2 \in \mathbb{Q}$ under the assumption $[\mathbb{Q}(\gamma^2) : \mathbb{Q}] = 4$. This implies $s_1 = s_3 = 0$. □

By Proposition 1 and Theorem 4, we have that in the case $p \equiv 1 \pmod{16}$ with a not square, $\chi_{p^2}(t)$ is irreducible and therefore its DLP cannot be reduced to DLP of HCC of genus two over $\mathbb{F}_{p^2}$ nor of ECC over $\mathbb{F}_{p^4}$.

7 Examples of suitable curves for genus-4 HCC

In this section, we describe how to search suitable curves for genus-4 HCC of type $y^2 = x^9 + ax$ and show the result of search. Based on the argument in 6.4, we only treat the case of $p \equiv 1 \pmod{16}$.

7.1 LLL algorithm

Let p be a prime such that $p \equiv 1 \pmod{16}$. We describe the algorithm to determine $|J_C(\mathbb{F}_p)|$. For a given p, if we obtain x, u, v and w in (1), we can determine the order of $J_C(\mathbb{F}_p)$ and check its suitability. So the main part of the algorithm is determining x, u, v, w in (1). To determine x, u, v, w, we use the LLL algorithm.

Let α_i, $i = 1, 2, \ldots, 7$ be positive integers such that $0 \leq \alpha_i < p$ and $\alpha_i \equiv g^{(p-1)i/16} \pmod{p}$. Let $\zeta \in \mathbb{C}$ be a primitive 16th root of unity and P a prime ideal over (p) in the integer ring $\mathcal{O}_K$ of $K = \mathbb{Q}(\zeta + \zeta^7)$. A $\mathbb{Z}$-basis $\{b_0, b_1, b_2, b_3\}$ of P is given by

$$\begin{aligned} b_0 &= p, \\ b_1 &= \zeta + \zeta^7 - \alpha_1 - \alpha_7, \\ b_2 &= \zeta^2 - \zeta^6 - \alpha_2 + \alpha_6, \\ b_3 &= \zeta^3 + \zeta^5 - \alpha_3 - \alpha_5. \end{aligned} \tag{3}$$

For this basis, any entry of the Gram matrix with respect to an inner product $\langle u, v \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(u\bar{v})$ is an integer. Put $c_1 = -\alpha_1 - \alpha_7$, $c_2 = -\alpha_2 + \alpha_6$, $c_3 = -\alpha_3 - \alpha_5$. Then each entry of the Gram matrix is given as follows.

$$\begin{aligned} \langle b_0, b_0 \rangle &= 4p^2, \\ \langle b_0, b_i \rangle &= 4pc_i \quad (1 \leq i \leq 3), \\ \langle b_i, b_j \rangle &= 4c_ic_j \quad (1 \leq i \neq j \leq 3), \\ \langle b_i, b_i \rangle &= 8 + 4c_i^2 \quad (1 \leq i \leq 3). \end{aligned}$$

Then the LLL algorithm for the Gram matrix works and we can determine x, u, v and w in (1) by using the following algorithm. (For the details on the LLL algorithm, see [4] for example.)

[3] This algorithm does not always give β with $N_{K/\mathbb{Q}}(\beta) = p$ theoretically. But the vector produced by this algorithm had norm p in all experiments we tried.

Algorithm[3]

Input	p: a prime ($p \equiv 1 \pmod{16}$)
Output	x, u, v, w satisfying (1)
	(Step 1-5: Finding $\beta \in \mathcal{O}_K$, $N_{K/\mathbb{Q}}(\beta) = p$.)
Step 1	$g \leftarrow$ a generator of $\mathbb{F}_p^\times$.
Step 2	$\mathbf{b} = (b_0, b_1, b_2, b_3) \leftarrow$ a $\mathbb{Z}$-basis (3) of $\mathcal{O}_K$.
Step 3	$G \leftarrow$ the Gram matrix for $\mathbf{b}$.
Step 4	$H = (h_{ij}) \leftarrow$ a transformation matrix obtained by the LLL algorithm for G.
Step 5	$\beta \leftarrow \sum_{i=0}^{3} b_i h_{0i}$
Step 6	Determine x, u, v, w by $\beta\tau(\beta) = x + u(\zeta + \zeta^7) + v(\zeta^2 - \zeta^6) + w(\zeta^3 + \zeta^5)$ and (1) where τ is an automorphism of $\mathbb{Q}(\zeta + \zeta^7)$ given by $\zeta \mapsto \zeta^3$.
Step 7	Return x, u, v, w.

This algorithm can be easily implemented and we can compute $|J_C(\mathbb{F}_p)|$ of C defined by $y^2 = x^9 + ax$ in a very short time.

7.2 Examples of suitable curves

We can obtain many suitable curves for HCC by varying p and a.

Table 1: Search results

search range $(r,\ s)$ for $r < p < s$	the number of primes[4] s.t. $\lvert J_C(\mathbb{F}_p)\rvert = 2\cdot$(prime)	time [sec]
$(2^{41}, 2^{41} + 10^4)$	12	2.824
$(2^{41}, 2^{41} + 10^5)$	79	26.548
$(2^{41}, 2^{41} + 10^6)$	714	267.054

Here we show some examples of suitable curves for HCC obtained by our algorithm.

[4] Here we count the number of primes p such that $|J_C(\mathbb{F}_p)| = 2\cdot$(prime) for at least one a.

Table 2: Examples of suitable curves for genus-4 HCC

$y^2 = x^9 + 29x$, $p = 1759218504481$(41-bit)	
s_1	4722688
s_2	14617568463136
s_3	29894897984637227312
s_4	46358542553945186095112704
$\lvert J_C(\mathbb{F}_p)\rvert$	2·47890346203766534635408594897978552632194970470 89(162-bit)
Time	0.01[sec]

$y^2 = x^9 + 1953125x$, $p = 2199023315233$(41-bit)	
s_1	5185024
s_2	13708576868352
s_3	26252697890967218048
s_4	42229265708937781717303296
$\lvert J_C(\mathbb{F}_p)\rvert$	2·11691986799636433497742258013292719544703684675777(163-bit)
Time	0.01[sec]

All computation were done on a system with Pentium 4 1.6GHz.

7.3 Notes on security

All examples in Table 2 are not weak against Frey-Rück attack[6]. To see this, one can easily check that a large prime factor of $|J_C(\mathbb{F}_p)|$ does not divide $p^r - 1$, $r = 1, 2, \ldots, 4^3\lfloor \log^2 p \rfloor$.

From the result of Duursma, Gaudry and Morain [5], an automorphism of large order can be exploited to accelerate the Pollard's rho algorithm. If there is an automorphism of order m, we can get a speed up of $\sqrt{m}$. The order of any automorphism of $y^2 = x^9 + ax$ is at most 16. So the Pollard's rho algorithm for these curves can be improved only by a factor 4.

As we saw in 6.4, J_C in Table 2 cannot split over $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^4}$. So they cannot reduced to genus-2 HCC of about 80-bit and ECC of about 160-bit.

References

1. B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, Canadian Mathematical Society Series of Monographs and Advanced Texts **21**, A Wiley-Interscience Publication, 1998,
2. J. Buhler and N. Koblitz, *Lattice Basis Reduction, Jacobi Sums and Hyperelliptic Cryptosystems*, Bull. Austral. Math. Soc. **58** (1998), pp. 147–154,
3. D. G. Cantor, *Computing in the Jacobian of hyperelliptic curve*, Math. Comp. **48** (1987), pp. 95–101,
4. H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics **138**, Springer, 1996,
5. I. Duursma, P. Gaudry and F. Morain, *Speeding up the Discrete Log Computation on Curves with Automorphisms*, Advances in Cryptology – ASIA CRYPT '99, Springer-Verlag LNCS 1716, 1999, pp. 103–121,

6. G. Frey and H.-G. Rück, *A Remark Concerning m-divisibility and the Discrete Logarithm in the Divisor Class Group of Curves*, Math. Comp. **62**, No.206 (1994) pp. 865–874,
7. E. Furukawa, M. Kawazoe and T. Takahashi, *Counting Points for Hyperelliptic Curves of type $y^2 = x^5 + ax$ over Finite Prime Fields*, Selected Areas in Cryptography(SAC2003), Springer LNCS, 3004.
8. S. G. Galbraith, *Supersingular Curves in Cryptography*, Advances in Cryptology – ASIACRYPT 2001, Springer-Verlag LNCS 2248, 2001, pp. 495–513,
9. P. Gaudry, *An algorithm for solving the discrete logarithm problem on hyperelliptic curves*, EUROCRYPT 2000, Springer LNCS 1807, 2000, pp. 19–34,
10. P. Gaudry and E. Schost, *Construction of Secure Random Curves of Genus 2 over Prime Fields*, EUROCRYPT 2004, Springer LNCS 3027, 2004, pp. 239–256,
11. P. Gaudry and R. Harley, *Counting Points on Hyperelliptic Curves over Finite Fields*, ANTS-IV, Springer LNCS 1838, 2000, pp. 297–312.
12. R. Harley, *Fast Arithmetic on Genus Two Curves*, http://cristal.inria.fr/~harley/hyper/, 2000,
13. R. H. Hudson and K. S. Williams, *Binomial Coefficients and Jacobi Sums*, Trans. Amer. Math. Soc. **281** (1984), pp. 431–505,
14. N. Koblitz, Algebraic Aspects of Cryptography, Algorithms and Computation in Mathematics Vol. 3, Springer-Verlag, 1998,
15. J. Kuroki, M. Gonda, K. Matsuo, J. Chao and S. Tsujii, *Fast Genus Three Hyperelliptic Curve Cryptosystems*, In The 2002 Symposium on Cryptography and Information Security, Japan – SCIS 2002, Jan.29–Feb.1 2002,
16. T. Lange, *Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae*, Cryptology ePrint Archive, Report 2002/121, 2002, http://eprint.iacr.org/,
17. K. Matsuo, J. Chao and S. Tsujii, *Fast Genus Two Hyperelliptic Curve Cryptosystem*, ISEC2001-31, IEICE, 2001,
18. K. Matsuo, J. Chao and S. Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, ANTS-V, Springer-Verlag LNCS 2369, 2002, pp. 461–474,
19. D. Mumford, Tata Lectures on Theta II, Progress in Mathematics **43**, Birkhäuser, 1984,
20. K. Nagao, *Improving Group Law Algorithms for Jacobians of Hyperelliptic Curves*, In W. Bosma ed., ANTS IV, Springer-Verlag LNCS 1838, pp. 439–448,
21. J. Pelzl, T. Wollinger and C. Paar, *Low Cost Security: Explicit Formulae for Genus 4 Hyperelliptic Curves*, Selected Areas in Cryptography (SAC2003), Springer-Verlag LNCS, to appear,
22. K. Rubin and A. Silverberg, *Supersingular abelian varieties in cryptology*, in Advances in Cryptology – Crypto 2002, Lecture Notes in Computer Science 2442 (2002), Springer, pp. 336-353;
23. M. Takahashi, *Improving Harley Algorithms for Jacobians of Genus 2 Hyperelliptic Curves*, In SCIS, IEICE Japan, 2002, (in Japanese),
24. K. Takashima, *Efficient Construction of Hyperelliptic Curve Cryptosystems of Genus 2 by using Complex Multiplication*, Trans. Japan Soc. Indust. Appl. Math. **12**(4), 2002, pp. 269–279, (in Japanese),
25. A. Weng, *Hyperelliptic CM-curves of genus 3*, Journal of the Ramanujan Mathematical Society **16**, No. 4, 2001, pp.339-372.