Fast Scalar Multiplications on Hyperelliptic Curve Cryptosystems

Lin You
School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
mryoulin@gmail.com

Jiwen Zeng
Department of Mathematics, Xiamen University, Xiamen 361005, China
jwzeng@xmu.edu.cn

Keywords: Hyperelliptic Curve cryptosystems, scalar multiplications, Frobenious Endomorphism, Frobenious Expansion, Euclidean length

Received: August 14, 2008

Scalar multiplication is the key operation in hyperelliptic curve cryptosystem. By making use of Euclidean lengths of algebraic integral numbers in a related algebraic integer ring, we discuss the Frobenius expansions of algebraic numbers, theoretically and experimentally show that the multiplier in a scalar multiplication can be reduced and converted into a Frobenius expansion of length approximate to the field extension degree, and then propose an efficient scalar multiplication algorithm. Our method is an extension of the results given by Müller, Smart and Günther et al. If some (optimal) normal basis is employed, then, for some hyperelliptic curves over finite fields, our method will make the computations of scalar multiplications be lessened about fifty-five percent compared with the signed binary method.

Povzetek: Predstavljena je metoda pohitrenega skalarnega množenja.

1 Introduction

Elliptic curve cryptosystems (ECC) have now widely been studied and applied in e-commerce, e-government and other secure communications. The practical advantages of ECC is that it can be realized with much smaller parameters compared to the conventional discrete logarithms based cryptosystems or RSA but with the same levels of security. This advantage is especially important in the environments with limited processing power, storage space and bandwidth.

As a natural generalization of elliptic curve cryptosystems, the hyperelliptic curve cryptosystem (HECC) was first proposed by Koblitz (1; 2). In a hyperelliptic curve cryptosystem, the rational point group of an elliptic curve, is replaced by the Jacobian group of a hyperelliptic curve , and its security is based on the discrete logarithm on this Jacobian group, that is, based on the hyperelliptic curve discrete logarithm problems(HECDLP). Since the order of the Jacobian group can be constructed much large over a small base field in HECC, HECC has gotten much attention in cryptography, a lot of work has been done to study the group structures and operations on the Jacobian groups.

Let q be a power of some prime and $\mathbb{F}_q$ be the finite field of q elements. A hyperelliptic curve C of genus g over $\mathbb{F}_q$ is defined by the equation

$$v^2 + h(u)v = f(u), \tag{1}$$

where $h(u)$, $f(u) \in \mathbb{F}_q$ with $\deg_u(h) \leq g$ and $\deg_u(f) = 2g + 1$, and there is no solution $(u, v) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ which simultaneously satisfy the equation $v^2 + h(u)v = f(u)$ and the partial derivate equations $2v + h(u) = 0$ and $h'(u)v - f'(u) = 0$. If the characteristic of $\mathbb{F}_q$ is odd, then the curve (1) is isomorphic to a hyperelliptic curve with the corresponding $h(u)$ equal to 0.

A *divisor* D on C over $\mathbb{F}_q$ is defined as a finite formal sum of rational $\overline{\mathbb{F}}_q$-points $D = \sum m_i P_i$ on C with its *degree* defined as the integer $\sum m_i$. The Jacobian group $\mathbb{J}_C(\mathbb{F}_q)$ of the curve C over $\mathbb{F}_q$ is an Abelian group composed of reduced divisors on C. Every element or reduced divisor D in $\mathbb{J}_C(\mathbb{F}_q)$ can be uniquely expressed by a pair of polynomials $< a(u), b(u) >$ with the properties

$$\begin{cases} \deg_u b(u) < \deg_u a(u) \leq g \\ b(u)^2 + h(u)b(u) - f(u) = 0 \bmod a(u) \end{cases}, \tag{2}$$

where $a(u)$, $b(u) \in \mathbb{F}_q[u]$. Generally, $a(u)$ is a monic polynomial of degree g and $b(u)$ is a polynomial of degree $g - 1$ with a overwhelming probability. The zero element of $\mathbb{J}_C(\mathbb{F}_q)$ can be expressed as $< 1, 0 >$.

In practical hyperelliptic curve cryptosystems, the vital computation that dominates the whole running time is *scalar multiplication*, that is, the computation of the repeated divisor adding

$$\underbrace{D + D + \cdots + D}_{m}$$

for a given divisor $D \in \mathbb{J}(\mathbb{F}_{q^n})$ and a positive integer $m \geq 1$, which is denoted as mD.

Such as in the hyperelliptic curve Diffie-Hellman key exchange protocol(HECDH), suppose Alice and Bob wish to generate their shared secret key for their secure communication, then they do the followings:

- First they agree on a positive integer n and a hyperelliptic curve C over a finite field $\mathbb{F}_q$, and also a divisor $D \in \mathbb{J}(\mathbb{F}_{q^n})$.
- Alice randomly chooses an positive integer m_A that is smaller than $\sharp\mathbb{J}_C(\mathbb{F}_{q^n})$, and then compute the scalar multiplication $D_A = m_A D$ and send D_A to Bob.
- Bob similarly chooses an positive integer m_B, compute $D_B = m_B D$ and send D_B to Alice.
- Alice and Bob compute the scalar multiplications $D_{A,B} = m_A D_B$ and $D_{B,A} = m_B D_A$,respectively.
- Since $D_{A,B} = m_A D_B = m_A(m_B D) = (m_A m_B)D = (m_B m_A)D = D_{B,A}$, Alice and Bob get their shared secret key $D_{A,B}$.
- Using this shared secret key $D_{A,B}$ and some symmetric cryptographic algorithm of their choice, Alice and Bob can communicate securely.

As the above shown, each of Alice and Bob compute two scalar multiplications and the scalar multiplication is the unique operation that involved in HECDH. Also in the hyperelliptic curve digital signature algorithm(HECDSA), it takes three dominating scalar multiplications except for some simple field operations.

A natural algorithm to compute the scalar multiplication mD is (signed) binary method. In (6; 7), Müller and Smart employed Frobenius automorphism to compute point scalar multiplications on elliptic curves over small fields of characteristic even or odd, respectively. In (8), Günther et al employed Frobenius automorphism to compute scalar multiplications on two hyperelliptic curves of genus 2. Their ideas are based on the two facts: One is that, for a point or divisor D, computing $\phi(D)$ is much faster than doubling D, and the other is that every $\mathbb{Z}[\tau]$-integer can be represented as Frobenius expansion or τ-adic expansion of finite lengths, where τ is a root of $P(T)$. In this paper, we will extend their methods to compute scalar multiplications on hyperelliptic curves of general genus.

The remainder of this paper is organized as follows: In Section 2, we briefly describe the Frobenius endomorphism on Jacobian groups of hyperelliptic curves over finite fields and a lemma contributed to Weil's theorem((5)), and in this section, we also introduce the Euclidean length in the algebraic integral ring $\mathbb{Z}[\tau]$ with τ a root of some hyperelliptic curve's characteristic polynomial. In Section 3, we discuss the lengths of τ-adic expansions of algebraic integral numbers in $\mathbb{Z}[\tau]$ and obtain an upper bound for them. In Section 4, we study the cyclic τ-adic expansions and the optimization of the τ-expansions's lengths. The τ-expansion's length of any algebraic integral number is optimized in Section 5, An efficient scalar multiplication algorithm is proposed in Section 6, and the last section gives the conclusion.

2 Frobenius endomorphism over Jacobian groups of hyperelliptic curves

The Frobenius map ϕ of $\overline{\mathbb{F}}_q$ is defined as the map $x \longmapsto x^q$ for $x \in \overline{\mathbb{F}}_q$. Naturally, ϕ induces an endomorphism ϕ_J of $\mathbb{J}_C(\mathbb{F}_{q^n})$ as follows:

$$\begin{array}{ccc} \mathbb{J}_C(\mathbb{F}_{q^n}) & \xrightarrow{\phi_J} & \mathbb{J}_C(\mathbb{F}_{q^n}) \\ <\sum_{i=0}^{g} a_i x^i, \sum_{j=0}^{g-1} b_j x^j> & \xmapsto{\phi_J} & <\sum_{i=0}^{g} a_i^q x^i, \sum_{j=0}^{g-1} b_j^q x^j>, \end{array}$$

where $D =< a(u), b(u) >=< \sum_{i=0}^{g} a_i x^i, \sum_{j=0}^{g-1} b_j x^j >$ is a reduced divisor or an element of $\mathbb{J}_C(\mathbb{F}_{q^n})$ with $a_i, b_j \in \mathbb{F}_{q^n}$.

For convenience, ϕ_J is also denoted by ϕ.

Lemma 1((5)) *For any positive integer r, let M_r denote the number of rational points of the hyperelliptic curve C defined by Equation* (1) *over $\mathbb{F}_{q^r}$ and $\sharp\mathbb{J}_C(\mathbb{F}_{q^r})$ denotes the order of the Jacobian group $\mathbb{J}_C(\mathbb{F}_q)$. Then*

1. *The zeta-function $Z(t)$ has the expression*

$$Z(t) = \exp(\sum_{n=1}^{\infty} \frac{M_n}{n} t^n) = \frac{L(t)}{(1-t)(1-qt)},$$

where $L(t)$ is an integral coefficient polynomial of degree $2g$.

2. *Let*

$$P(T) = t^{2g} L(1/T) = \prod_{i=1}^{2g} (T - \tau_i),$$

then $|\tau_i| = \sqrt{q}$, and the roots come in complex conjugate pairs such that there exists an ordering with $\tau_{i+g} = \bar{\tau}_i$, and hence, $\tau_{i+g}\tau_i = q$.

3. *$P(T)$ is the characteristic polynomial of Frobenius endomorphism ϕ and $P(T)$ is an integral coefficient polynomial of the following form*

$$\begin{array}{l} P(T) = T^{2g} + a_1 T^{2g-1} + a_2 T^{2g-2} + \cdots + \\ + a_g T^g + q a_{g-1} T^{g-1} + \cdots + q^{g-1} a_1 T + q^g. \end{array} \quad (3)$$

4. *Let $a_0 = 1$, then for $1 \le i \le g$*

$$\begin{array}{rcl} i a_i & = & (M_i - q^i - 1)a_0 + (M_{i-1} - q^{i-1} - 1)a_1 \\ & & + \cdots + (M_1 - q - 1)a_{i-1} \end{array}.$$

5. *For any positive integer n,*

$$\sharp\mathbb{J}_C(\mathbb{F}_{q^n}) = \prod_{i=1}^{2g} (1 - \tau_i^n).$$

For cryptographic purposes, in order to resist all possible attacks on the HECDLP, such as Pollardąrs rho algorithm((3)) and Pohlig-Hellman algorithm((4) or their improved versions, it is most desirable that $\sharp\mathbb{J}_C(\mathbb{F}_{q^n})$ have a large prime integer factor, or to the best, $\sharp\mathbb{J}_C(\mathbb{F}_{q^n})$ is by itself a large prime or almost large prime. For the best possibility, the necessary condition is that $P(T)$ is irreducible. Hence, $P(T)$ is assured to be irreducible here.

3 Euclidean lengths in the algebraic integral ring $\mathbb{Z}[\tau]$

Let C be a hyperelliptic curve of genus g over $\mathbb{F}_q$ with the characteristic polynomial (3). Let τ be a root of $P(T)$. Then, since $P(T)$ is irreducible, every element ξ in $\mathbb{Z}[\tau]$ can be uniquely expressed as the form

$$x_0 + x_1\tau + \cdots + x_{2g-1}\tau^{2g-1}.$$

Let $\tau = \tau_1, \tau_2, \cdots, \tau_g$ be the g roots of $P(T)$ which are not conjugate each other. Then, we can define a positive number $N(\xi)$ corresponding to ξ as the following

$$N(\xi) = \sqrt{|\sum_{i=0}^{2g-1} x_i\tau_1^i|^2 + \cdots + |\sum_{i=0}^{2g-1} x_i\tau_g^i|^2},$$

where $|x|$ denotes the complex absolute value of x. $N(\xi)$ is often called the Euclidean length of ξ.

It is clear that $N(\xi\eta) \le N(\xi)N(\eta)$ and $N(\xi+\eta) \le N(\xi) + N(\eta)$ hold for any $\xi, \eta \in \mathbb{Z}[\tau]$. And $N(\xi)^2$ is a positive definite quadratic form in the variables $x_0, x_1, \cdots, x_{2g-1}$, with the coefficients being integer polynomials of $P(T)$'s coefficients $a_i (1 \le i \le g)$.

For $g = 1$ and $\xi = x_0 + x_1\tau$, we have

$$N(\xi)^2 = x_0^2 - a_1x_0x_1 + qx_1^2.$$

For $g = 2$ and $\xi = x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3$, we have

$$\begin{array}{ll} N(\xi)^2 & = 2x_0^2 - a_1x_0x_1 + (a_1^2 - 2a_2)x_0x_2 \\ & -(a_1^3 - 3(a_1a_2 - a_1q))x_0x_3 + 2qx_1^2 - a_1qx_1x_2 \\ & +(a_1^2 - 2a_2)qx_1x_3 + 2q^2x_2^2 - a_1q^2x_2x_3 + 2q^3x_3^2 \end{array}.$$

In general, let $S_i = \sum_{j=1}^{g}(\tau_j^i + \bar{\tau_j^i})$, $X = (x_0, x_1, \cdots, x_{2g-1})$, and let

$$A = \begin{pmatrix} g & S_1/2 & S_2/2 & \cdots & S_{2g-1}/2 \\ S_1/2 & qg & qS_1/2 & \cdots & qS_{2g-2}/2 \\ S_2/2 & qS_1/2 & q^2g & \cdots & q^2S_{2g-3}/2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ S_{2g-1}/2 & qS_{2g-2}/2 & q^2S_{2g-3}/2 & \cdots & q^{2g-1}g \end{pmatrix}$$

Then we can easily prove

$$N(\xi)^2 = XAX^T,$$

where S_i can be computed by the following Newton's formula:

$$S_i + a_1S_{i-1} + a_2S_{i-2} + \cdots + a_{i-1}S_1 + ia_i = 0$$

with $a_0 = 1$ and $a_j = a_{2g-j}q^{j-g}$ for $j > g$.

4 Convert m into τ-adic expansion

Similar to Lemma 1 in (6), we have

Lemma 2 (**Division With Remainder** in $\mathbb{Z}[\tau]$) *Let $m \in \mathbb{Z}[\tau]$, then there exists a unique pair of elements m' and r such that*

$$m = m'\tau + r \tag{4}$$

with $m' \in \mathbb{Z}[\tau]$, $r \in \{-\lceil q^g/2\rceil + 1, \cdots, \lfloor q^g/2\rfloor\}$.

Theorem 1 *Let $m \in \mathbb{Z}[\tau]$, then m can be uniquely represented as a τ-adic expansion*

$$m = \sum_{i=0}^{k-1} r_i\tau^i + m'\tau^k,\ r_i \in \{-\lceil q^g/2\rceil + 1, \cdots, \lfloor q^g/2\rfloor\}.$$

If $k \ge 2\log_q \frac{2(\sqrt{q}-1)N(m)}{\sqrt{g}}$, then $N(m') < \frac{q^g\sqrt{g}}{2(\sqrt{q}-1)}$.

Proof Iterate the Division With Remainder in $\mathbb{Z}[\tau]$ for $m_0 = m$, then we have

$$m_i = m_{i+1}\tau + r_i,\ r_i \in \{-\lceil q^g/2\rceil + 1, \cdots, \lfloor q^g/2\rfloor\}.$$

Hence,

$$m_0 = \sum_{i=0}^{j-1} r_i\tau^i + m_j\tau^j.$$

Apply triangle inequality for Euclidean length in $m_i = m_{i+1}\tau + r_i$, and we will get

$$N(m_j) < \frac{N(m_0)}{\sqrt{q}^j} + \frac{\sqrt{g}(\lfloor q^g/2\rfloor)}{\sqrt{q}-1}.$$

Hence, if $\frac{N(m_0)}{\sqrt{q}^j} \le \frac{\sqrt{g}}{2(\sqrt{q}-1)}$ or

$$j \ge 2\log_q \frac{2(\sqrt{q}-1)N(m_0)}{\sqrt{g}},$$

then

$$N(m_j) < \frac{\sqrt{g}(\lfloor q^g/2\rfloor + 1/2)}{\sqrt{q}-1} = \frac{q^g\sqrt{g}}{2(\sqrt{q}-1)}.$$

Hence, for $k = \lceil 2\log_q \frac{2(\sqrt{q}-1)N(m)}{\sqrt{g}}\rceil + 1$ and $m' = m_k$, we have $N(m') < \frac{q^g\sqrt{g}}{2(\sqrt{q}-1)}$. □

Lemma 3 $a_1 \le 2\lfloor 2\sqrt{q}\rfloor$. *And if $a_2 = 0$, then*

$$|a_1| < \sqrt{q}.$$

Proof $a_1 \le 2\lfloor 2\sqrt{q}\rfloor$ holds obviously since every root of $P(T)$ has the complex absolute value $\sqrt{q}$. If $a_2 = 0$, then $|a_1| < \sqrt{q}$ follows the facts $M_2 - q^2 - 1 + a_1^2 = 0$ and $M_2 > 1$.

Lemma 4 *If C is a hyperelliptic curve of genus 2 with the irreducible characteristic polynomial $P(T) = T^4 + a_1T^3 + a_2T^2 + a_1qT + q^2$, then $a_1^2 - 4a_2 + 8q$ is non-square and*

$$2|a_1|\sqrt{q} - 2q < a_2 < a_1^2/4 + 2q.$$

Proof If $a_1^2 - 4a_2 + 8q$ is square, then $P(T) = (T^2 + \frac{1}{2}(a_1 \pm \sqrt{a_1^2 - 4a_2 + 8q})T + q)(T^2 + \frac{1}{2}(a_1 \mp \sqrt{a_1^2 - 4a_2 + 8q})T + q)$, which contradicts our hypothesis that $P(T)$ is irreducible.

Due to (9), we have $\lceil 2|a_1|\sqrt{q}-2q\rceil \le a_2 \le \lfloor a_1^2/4+2q\rfloor$, and it follows $2|a_1|\sqrt{q}-2q < a_2 < a_1^2/4+2q$. □

Theorem 2 *Let C be a hyperelliptic curve of genus g and its irreducible characteristic polynomial $P(T)$ have a root τ. Let $R=\{-\lceil q^g/2\rceil+1,\cdots,\lfloor q^g/2\rfloor\}$, and a τ-adic expansion means a τ-polynomial with the coefficients belong to R. Let $\xi\in\mathbb{Z}[\tau]$ with*

$$N(\xi) < \frac{q^g\sqrt{g}}{2(\sqrt{q}-1)}. \tag{5}$$

1. *If $g=2$, $a_1=a_2=0$, then for every positive integer m, m has a τ-adic expansion of length about $\frac{1}{2}\lfloor\log_q m\rfloor$. (But, in this case, the curves are supersingular and not suitable for cryptosystems).*
2. *If $g=2$, and only one of a_1 and a_2 equal to 0, then ξ has a τ-adic expansion of length at most 5.*
3. *If $g=2$, and none of a_1 and a_2 equals to 0, then ξ has a τ-adic expansion of length at most 8.*
4. *If $g\ge 3$, then ξ has a τ-adic expansion of length $l\le 2g+4$.*

Proof Suppose $\xi\in\mathbb{Z}[\tau]$ satisfying the inequality (5), then

$$N(\xi)^2 < \frac{gq^{2g}}{4(\sqrt{q}-1)^2}.$$

1. Since $q^2+\tau^4=0$ or $q^2=-\tau^4$, it obviously follows that m has a τ-adic expansion of length about $\frac{1}{2}\lfloor\log_q m\rfloor$.

2. Suppose $a_1=0$. Then $|a_2|<2q$, and it follows $4q^2-a_2^2\ge 4q-1$. Hence,

$$\begin{aligned}
&N(\xi)^2\\
&=2(x_0^2-a_2x_0x_2+qx_1^2-a_2qx_1x_3+q^2x_2^2+q^3x_3^2)\\
&=2((x_0-a_2/2x_2)^2+(q^2-a_2^2/4)x_2^2+q(x_1-a_2/2x_3)^2\\
&\quad +q(q^2-a_2^2/4)x_3^2)\\
&=2((1-\tfrac{a_2^2}{4q^2})x_0^2+q^2(x_2-\tfrac{a_2}{2q^2}x_0)^2+(q-\tfrac{a_2^2}{4q})x_1^2\\
&\quad +q^3(x_3-\tfrac{a_2}{2q^2}x_1)^2)\\
&<\tfrac{q^4}{2(\sqrt{q}-1)^2}
\end{aligned} \tag{6}$$

Thus,

$$\begin{cases}
|1-\frac{a_2^2}{4q^2}|^{1/2}|x_0| &< \frac{q^2}{2(\sqrt{q}-1)}\\
|1-\frac{a_2^2}{4q^2}|^{1/2}|x_1| &< \frac{q^2}{2(q-\sqrt{q})}\\
|q^2-a_2^2/4|^{1/2}|x_2| &< \frac{q^2}{2(\sqrt{q}-1)}\\
|q^2-a_2^2/4|^{1/2}|x_3| &< \frac{q^2}{2(q-\sqrt{q})}
\end{cases}, \tag{7}$$

and so,

$|x_0|<\frac{q^3}{(\sqrt{q}-1)\sqrt{4q-1}}$, $|x_1|<\frac{q^3}{(q-\sqrt{q})\sqrt{4q-1}}$,
$|x_2|<\frac{q^2}{(\sqrt{q}-1)\sqrt{4q-1}}$, $|x_3|<\frac{q^2}{(q-\sqrt{q})\sqrt{4q-1}}$.

a) If $q\ge 4$, then $|x_0|\le q^2$ and $|x_1|\le q^2/2$. Hence, if $x_0>q^2/2$(similar for $x_0<-q^2/2$), then from (6), we have $(2q^2x_2-a_2x_0)^2<q^6/(\sqrt{q}-1)^2-q^4(4q-1)/4$, and so $|x_2-a_2|\le|x_2-\frac{a_2}{2q^2}x_0|+|\frac{a_2}{2q^2}x_0-a_2|<\sqrt{4q^2-(4q-1)(\sqrt{q}-1)^2}/(4(\sqrt{q}-1))+3(2q-1)/4\le q^2/2$. Thus

$$\begin{aligned}
\xi&=x_0+x_1\tau+x_2\tau^2+x_3\tau^3\\
&=(x_0-q^2)+x_1\tau+(x_2-a_2)\tau^2+x_3\tau^3-\tau^4
\end{aligned}$$

is a τ-adic expansion of length at most 5 .

b) If $q\ge 4$ and $|x_0|\le q^2/2$, then ξ is itself a τ-adic expansion of length 4 .

c) If $q=2$, then $a_2=\pm 1$. Hence, from (7), we have $|x_0|\le 4$, $|x_1|\le 3$, $|x_2|\le 2$ and $|x_3|\le 1$. If $|x_0|\le 2$ and $|x_1|\le 2$, then ξ is itself a τ-adic expansion. If $|x_0|\le 2$ and $|x_1|=3$, then $\xi=x_0+(x_1\pm 4)\tau+x_2\tau^2+(x_3\pm 1)\tau^3-\tau^4$ is a τ-adic expansion of length $l\le 5$.

If $|x_0|=3$, then from (6), we have

$$\begin{aligned}
&9(1-1/16)+4(x_2\pm 3/8)^2+(2-1/8)x_1^2\\
&+8(x_3-1/8x_1)^2<\tfrac{2^4}{4(\sqrt{2}-1)^2},
\end{aligned} \tag{8}$$

which implies $|x_1|\le 2$. If $x_1=0$, then $\xi=(x_0\pm 4)+(x_2\pm a_2)\tau^2+x_3\tau^3\pm\tau^4$ (if $|x_2\pm a_2|\le 2$) or $\xi=(x_0\pm 4)+(x_2\pm a_2\pm 4)\tau^2+x_3\tau^3+(\pm 1\pm a_2)\tau^4\pm\tau^6$(if $|x_2\pm a_2|=3$) is a τ-adic expansion of length 5.

If $0<|x_1|\le 2$ and $x_3=0$, then ξ is itself a τ-adic expansion or $\xi=(x_0\pm 4)+x_1\tau+(x_2\pm a_2\pm 4)\tau^2+(\pm 1\pm a_2)\tau^4\pm\tau^6$ is a τ-adic expansion of length $l\le 5$.

If $0<|x_1|\le 2$ and $|x_3|=1$, then from the equation (8) we obtain $|x_2|\le 1$. Hence, $\xi=(x_0\pm 4)+x_1\tau+(x_2\pm a_2)\tau^2+x_3\tau^3\pm\tau^4$ is a τ-adic expansion of length $l\le 5$.

If $|x_0|=4$, then from (6), we have $|x_2|<\frac{\sqrt{2^6/(\sqrt{2}-1)^2-15\times 16}}{8}+4/8<2$, and so $|x_2\pm a_2|\le 2$. Hence, ξ is a τ-adic expansion of length $l\le 4$.

d) If $q=3$, then $|a_2|\le 3$. From (7), we have $|x_0|\le 7$, $|x_1|\le 4$, $|x_2|\le 2$ and $|x_3|\le 1$. If $|x_0|\le 4$, then ξ is itself a τ-adic expansion of length 4. If $|x_0|\ge 5$ and $|a_2|=3$, then from (6) we have $3x_0^2+(6x_2\pm x_0)^2+9x_1^2+3(6x_3\pm x_1)^2<3^4/(\sqrt{3}-1)^2$, which implies $x_1=0$ or $x_3=0$. Thus, $\xi=x_0+x_1\tau+x_2\tau^2+x_3\tau^3=(x_0-9)+x_1\tau+(x_2-a_2)\tau^2+x_3\tau^3-\tau^4$ or $\xi=(x_0-9)+x_1\tau+(x_2-a_2\pm 9)\tau^2+x_3\tau^3+(1\pm a_2)\tau^4\pm\tau^6$ is a τ-adic expansion of length $l\le 5$.

3. Suppose $a_2=0$. Then by Lemma 3, $|a_1|=1$ for $q=2,3$ and $|a_1|<\sqrt{q}$ for $q>3$. Since

$$\begin{aligned}
N(\xi)^2&=2x_0^2-a_1x_0x_1+a_1^2x_0x_2-(a_1^3+3a_1q)x_0x_3\\
&\quad +2qx_1^2-a_1qx_1x_2+a_1^2qx_1x_3+2q^2x_2^2\\
&\quad +2q^3x_3^2-a_1q^2x_2x_3\\
&=\tfrac{q^2(a_1^2+8q)}{a_1^2+4q}x_2^2+2q(x_1+\tfrac{a_1^2}{4}x_3-\tfrac{a_1}{4q}x_0-\tfrac{a_1}{4}x_2)^2\\
&\quad +\tfrac{q(16q^2-a_1^4)}{8}(x_3+\tfrac{-3a_1^3-12a_1q}{q(16q^2-a_1^4)}x_0-\tfrac{a_1}{4q+a_1^2}x_2)^2\\
&\quad +\tfrac{(a_1^2+8q)(a_1^2-q)}{q(a_1^2-4q)}x_0^2\\
&<\tfrac{q^4}{2(\sqrt{q}-1)^2}
\end{aligned}, \tag{9}$$

it follows that

$$\frac{(a_1^2-q)}{q(a_1^2-4q)}x_0^2+\frac{q^2}{a_1^2+4q}x_2^2<\frac{q^4}{2(\sqrt{q}-1)^2(8q+a_1^2)} \tag{10}$$

and

$$\begin{cases}
|x_0|<\frac{\sqrt{q}q^2\sqrt{1+\frac{3q}{q-a_1^2}}}{\sqrt{2}(\sqrt{q}-1)\sqrt{8q+a_1^2}} &< \frac{q^2\sqrt{1+\frac{3q}{2\sqrt{q}-1}}}{4(\sqrt{q}-1)}\\
|x_2|<\frac{q}{\sqrt{2}(\sqrt{q}-1)}\sqrt{1-\frac{4q}{8q+a_1^2}} &< \frac{\sqrt{5}q}{3\sqrt{2}(\sqrt{q}-1)}
\end{cases}. \tag{11}$$

Similarly, we will get

$$\begin{cases}
|x_1|<\frac{q^2}{\sqrt{2}(q-\sqrt{q})}\sqrt{1-\frac{4q}{8q+a_1^2}} &< \frac{\sqrt{5}q^2}{3\sqrt{2}(q-\sqrt{q})}\\
|x_3|<\frac{q}{\sqrt{2}(\sqrt{q}-1)\sqrt{8q+a_1^2}}\sqrt{1+\frac{3q}{q-a_1^2}} &< \frac{q\sqrt{1+\frac{3q}{2\sqrt{q}-1}}}{4(q-\sqrt{q})}
\end{cases}. \tag{12}$$

If $q\ge 4$ then $|x_i|\le q^2/2$ for $i=0,1,2,3$. Hence, ξ is a τ-adic expansion of length at most 4.

Let $q=3$, then from (9), (10),(11) and (12), we have $|x_0|\le 7$, $|x_1|\le 3$, $|x_2|\le 1$ and $|x_3|\le 1$. Without loss of generality,

suppose $a_1 = 1$ and $x_0 > 0$, then

$$\begin{aligned}\xi &= x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3 (\text{ if } |x_0| \le 4)\\ &= (x_0 - 9) + (x_1 - 3)\tau + x_2\tau^2 + (x_3 - 1)\tau^3 - \tau^4\\ &\quad (\text{ if } |x_0| > 4 \text{ and } |x_1 - 3| \le 4)\\ &= (x_0 - 9) + (x_1 - 3 + 9)\tau + (x_2 + 3)\tau^2 + (x_3 - 1)\tau^3 + \tau^5\\ &\quad (\text{ if } |x_0| > 4 \text{ and } x_1 - 3 < -4)\end{aligned}$$

is a τ-adic expansion of length at most 5.

Similar discussion will show that ξ can also be represented as a τ-adic expansion of length at most 5 for $q = 2$.

4. Suppose $a_1 \neq 0$ and $a_2 \neq 0$. Then for $\xi = x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3$, we have

$$\begin{aligned}&N(\xi)^2 =\\ &\quad 2q^3(x_3 - \tfrac{a_1}{4q}x_2 + \tfrac{a_1^2-2a_2}{4q^2}x_1 - \tfrac{a_1(a_1^2-3a_2+3q)}{4q^3}x_0)^2\\ &\quad + \tfrac{q(16q-a_1^2)}{8}(x_2 + \tfrac{a_1(a_1^2-2a_2-4q)}{q(16q-a_1^2)}x_1 + \tfrac{-a_1^4+3a_1^2a_2+qa_1^2-8qa_2}{q^2(16q-a_1^2)}x_0)^2\\ &\quad + \tfrac{-a_1^4+6a_1^2a_2-4qa_1^2-8a_2^2+32q^2}{16q-a_1^2}(x_1 -\\ &\qquad \tfrac{a_1(16q^2-14qa_1^2-2a_1^4+13a_1^2a_2-20a_2^2+32qa_2)}{2q(-a_1^4+6a_1^2a_2-4qa_1^2-8a_2^2+32q^2)}x_0)^2\\ &\quad + \tfrac{qa_1^4-\frac{1}{4}a_1^2a_2^2-5qa_1^2a_2+7q^2a_1^2+a_2^3+2qa_2^2-4q^2a_2-8q^3}{q^2(a_1^2-2a_2-4q)}x_0^2\\ &= 2q^2(x_2 - \tfrac{a_1}{4}x_3 + \tfrac{a_1^2-2a_2}{4q^2}x_0 - \tfrac{a_1}{4q}x_1)^2\\ &\quad + \tfrac{q^2(16q-a_1^2)}{8}(x_3 + \tfrac{-3a_1^3+10a_1a_2-12a_1q}{q^2(16q-a_1^2)}x_0 + \tfrac{3a_1^2-8a_2}{q(16q-a_1^2)}x_1)^2\\ &\quad + \tfrac{(4a_2-8q-a_1^2)(a_1^4-3a_1^2a_2+3a_1^2q-2a_2q-4q^2)}{q^2(16q-a_1^2)}(x_0 +\\ &\qquad \tfrac{a_1q(14a_1^2q+2a_1^4-32a_2q-13a_1^2a_2-16q^2+20a_2^2)}{2(4a_2-8q-a_1^2)(a_1^4-3a_1^2a_2+3qa_1^2-2qa_2-4q^2)}x_1)^2\\ &\quad + \tfrac{qa_1^4-\frac{1}{4}a_1^2a_2^2-5qa_1^2a_2+7q^2a_1^2+a_2^3+2qa_2^2-4q^2a_2-8q^3}{a_1^4-3a_1^2a_2+3a_1^2q-2a_2q-4q^2}x_1^2\\ &< \tfrac{q^4}{2(\sqrt{q}-1)^2}\end{aligned} \tag{13}$$

Let

$$\begin{cases} F = -qa_1^4 + \frac{1}{4}a_1^2a_2^2 + 5qa_1^2a_2 - 7q^2a_1^2 - a_2^3 - 2qa_2^2 \\ \qquad +4q^2a_2 + 8q^3 \\ G = -a_1^4 + 3a_1^2a_2 - 3a_1^2q + 2a_2q + 4q^2 \\ H = -a_1^2 + 2a_2 + 4q \end{cases}.$$

Since $|a_1| \le 2\lfloor 2\sqrt{q}\rfloor$ and $2|a_1|\sqrt{q} - 2q < a_2 < a_1^2/4 + 2q$, we have $F \ge 1$, $G > 0$ and $H > 0$. Hence from (13) we get $|x_0| < \frac{\sqrt{2}q^3}{2(\sqrt{q}-1)}\sqrt{H/F}$ and $|x_1| < \frac{\sqrt{2}q^2}{2(\sqrt{q}-1)}\sqrt{G/F}$. Similarly, we will get $|x_2| < \frac{\sqrt{2}q^2}{2(q-\sqrt{q})}\sqrt{G/F}$ and $|x_3| < \frac{\sqrt{2}q^2}{2(q-\sqrt{q})}\sqrt{H/F}$. That is,

$$\begin{cases} |x_0| < \frac{\sqrt{2}q^3}{2(\sqrt{q}-1)}\sqrt{H/F} \\ |x_1| < \frac{\sqrt{2}q^2}{2(\sqrt{q}-1)}\sqrt{G/F} \\ |x_2| < \frac{\sqrt{2}q^2}{2(q-\sqrt{q})}\sqrt{G/F} \\ |x_3| < \frac{\sqrt{2}q^2}{2(q-\sqrt{q})}\sqrt{H/F} \end{cases}. \tag{14}$$

If $a_2 = 2q + a_1^2/4$ or $a_1 = \pm(2q + a_2)/(2\sqrt{q})$, then $F = 0$, which contradicts $F \ge 1$. While, it is very likely that H/F or G/F takes maximal values at $a_2 = 2q + a_1^2/4 - \theta$ or $-2q + 2|a_1|\sqrt{q}+\delta$, where $\theta = 1$ or $1/4$, $\delta = 1$ or $\lceil 2|a_1|\sqrt{q}\rceil - 2|a_1|\sqrt{q}$.

According to (10), if C is a curves with $a_2 = 2q + (a_1^2 - 1)/4$, then it may not be a hyperelliptic curve. Thus, we do not consider this case.

i) Let $a_2 = 2q + a_1^2/4 - 1$. Then, if $a_1 \neq \pm(4\sqrt{q} - 2)$, H/F and G/F are strictly increasing or decreasing with $a_1 > 0$ or $a_1 < 0$. Hence, if q is a square, then H/F and G/F reach their maximal values at $a_1 = \pm(4\sqrt{q} - 4)$, that is, $\frac{2(48q-56\sqrt{q}+128q^{3/2}-15)}{3(-160q+9+256q^2)}$ and $\frac{2(-1872q^2+8q^{3/2}+1152q^{5/2}+1353q-368\sqrt{q}-168)}{3(-160q+9+256q^2)}$, respectively. Thus, $H/F < \frac{3}{5}q^{-1/2}$ and $G/F < 3\sqrt{q}$. If q is non-square, without loss of generality, suppose $a_1 \ge 2$. Because both H/F and G/F are strictly increasing functions of a_1 except in a neighborhood of $a_1 = 4\sqrt{q} - 2$, they will reach their possible maximal values at $a_1 = 2(2\sqrt{q} - \varepsilon) - 2$ since $a_1 \le 2\lfloor 2\sqrt{q}\rfloor$ and a_1 is even, where $\varepsilon = 2\sqrt{q} - \lfloor 2\sqrt{q}\rfloor$. Replace a_1 and a_2 in H/F with $2(2\sqrt{q} - \varepsilon) - 2$ and $2q + a_1^2/4 - 1$, respectively. Then, since $\varepsilon = 2\sqrt{q} - \lfloor 2\sqrt{q}\rfloor > \frac{3}{2\lfloor 2\sqrt{q}\rfloor+1} > \frac{3}{5\sqrt{q}}$, we get

$$\begin{aligned}H/F &= \tfrac{-2(-4\sqrt{q}\varepsilon-4\sqrt{q}+\varepsilon^2+2\varepsilon+2)}{\varepsilon(4\varepsilon+\varepsilon^3+4\varepsilon^2-8\sqrt{q}\varepsilon^2-24\sqrt{q}\varepsilon-16\sqrt{q}+16q\varepsilon+32q)}\\ &\approx \tfrac{1}{4\sqrt{q}\varepsilon} < \tfrac{1}{4\sqrt{q}} \cdot \tfrac{5\sqrt{q}}{3} < \tfrac{5}{12}.\end{aligned}$$

Similarly, we have $G/F \approx \frac{9\sqrt{q}}{4\varepsilon} < \frac{9\sqrt{q}}{4} \cdot \frac{5\sqrt{q}}{3} < \frac{15q}{4}$.

ii) Let q be square and $a_2 = -2q + 2|a_1|\sqrt{q} + 1$. Without loss of generality, suppose $a_1 \ge 1$. Since $a_2 < a_1^2/4 + 2q$, it follows $a_1 \le 4\sqrt{q} - 3$. It is easy to show that H/F is strictly increasing for $1 \le a_1 \le 4\sqrt{q} - 3$. Hence, H/F will reach its maximal value at $a_1 = 4\sqrt{q} - 3$, and so, $H/F < \frac{4}{5}q^{-1/2}$. Similar discussion will induce $G/F < \frac{27}{5}q^{1/2}$.

iii) Let $a_2 = -2q + 2|a_1|\sqrt{q} + \delta$ with $\delta = \lceil 2|a_1|\sqrt{q}\rceil - 2|a_1|\sqrt{q}$ (q is non-square). Still suppose $a_1 \ge 1$. Then, $a_1 < 4\sqrt{q} - 2\sqrt{\delta}$. Let $a_1 = 4\sqrt{q} - 2 + \epsilon$, where $0 < \epsilon < 1$ such that a_1 is an integer, that is, $a_1 = \lceil 4\sqrt{q} - 2\rceil$. Replace a_1 and a_2 in H/F with $4\sqrt{q} - 2 + \epsilon$ and $-2q + 2a_1\sqrt{q} + \delta$, respectively. Then, since $\delta = \lceil 2a_1\sqrt{q}\rceil - 2a_1\sqrt{q} > \frac{1}{4\sqrt{q}}$, we have $H/F \approx -4q^{1/2}\frac{-8\sqrt{q}}{\delta 64q^{3/2}} = \frac{1}{2\delta\sqrt{q}} < 2$. Similar discussion will induce $G/F \approx \frac{9}{2}\sqrt{q}\delta^{-1} < 18q$.

From all the discussion above, we conclude that if $a_2 \neq 2q + (a_1^2 - 1)/4$, then

$$H/F < \begin{cases} \frac{4}{5}q^{-1/2} & \text{if } q \text{ is square} \\ 2 & \text{if } q \text{ is non-square} \end{cases},$$

and

$$G/F < \begin{cases} \frac{18}{5}q^{1/2} & \text{if } q \text{ is square} \\ 18q & \text{if } q \text{ is non-square.} \end{cases}.$$

Hence, if q is square, we have

$$\begin{cases} |x_0| < \frac{2}{\sqrt{5}}q^{9/4} \\ |x_1| < \frac{\sqrt{36}}{\sqrt{5}}q^{7/4} \\ |x_2| < \frac{\sqrt{36}}{\sqrt{5}}q^{5/4} \\ |x_3| < \frac{2}{\sqrt{5}}q^{3/4} \end{cases},$$

and if q is non-square, we have

$$\begin{cases} |x_0| < 2q^{5/2} \\ |x_1| < \sqrt{36}q^2 \\ |x_2| < \sqrt{36}q^{3/2} \\ |x_3| < 2q \end{cases}.$$

In the following discussions, without loss of generality, we assure $a_1 > 0$ and $x_0 > 0$. And, for the worst case, we also assume that all x_i is near to its upper bound. Then, if q is a square no less than 49 and $a_2 > 0$(similar discussion for $a_2 < 0$), we have

$$\begin{aligned}\xi &= x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3 + x_4\tau^4\\ &= (x_0 - d_0q^2) + (x_1 - d_0a_1q)\tau + (x_2 - d_0a_2)\tau^2\\ &\quad + (x_3 - d_0a_1)\tau^3 - d_0\tau^4\\ &= (x_0 - d_0q^2) + (x_1 - d_0a_1q + d_1q^2)\tau + (x_2 - d_0a_2\\ &\quad + d_1a_1q)\tau^2 + (x_3 - d_0a_1 + d_1a_2)\tau^3 + (-d_0 + d_1a_1)\tau^4\\ &\quad + d_1\tau^5\\ &= (x_0 - d_0q^2) + (x_1 - d_0a_1q + d_1q^2)\tau + (x_2 - d_0a_2\\ &\quad + d_1a_1q + d_2q^2)\tau^2 + (x_3 - d_0a_1 + d_1a_2 + d_2a_1q)\tau^3\\ &\quad + (-d_0 + d_1a_1 + d_0a_2)\tau^4 + (d_1 + d_2a_1)\tau^5 + d_2\tau^6,\end{aligned}$$

which implies that ξ is a τ-adic expansion of length at most 7, where d_0 is an integer close to $\frac{2}{\sqrt{5}}q^{1/4}$ such that $|x_0 - d_0q^2| \leq q^2/2$. $d_1 = 0, -1$ if $x_1 > 0$, or $d_1 = 1, 2$ if $x_1 < 0$. $d_2 = 0$ if $d_1 = 0, 1$, or $d_2 = 0, 1$ if $d_1 = -1$, or $d_2 = -1$ if $d_1 = 2$.

By almost the same discussions, we will show that ξ can be expressed as a τ-adic expansion of length at most 8 if q is a non-square no less than 37.

If q is a square smaller than 25 or a non-square smaller than 31, then ξ may go to a cyclic τ-adic expansion with the coefficients in R. But, we can easily show that if $a_2 \neq 2q + (a_1^2 - 1)/4$ and ξ does not go to a cyclic τ-adic expansion, then ξ will be a τ-adic expansions of length at most 8.

Our discussions and results above can be naturally generalized to the curves of genus $g \geq 3$, though it will be a bit more burdensome for high genus. In general, there exist fixed integers k_i and l_i non-related to q such that

$$|x_i| < \begin{cases} k_i q^{(5g-2i-1)/4} & \text{if } q \text{ is square} \\ l_i q^{(3g-i-1)/2} & \text{if } q \text{ is non-square} \end{cases} \quad (15)$$

hold for $i = 0, 1, \cdots, 2g-1$. And, every element $\xi \in \mathbb{Z}[\tau]$ can be represented as a τ-adic expansion of length at most $2g+4$ as long as the related characteristic polynomial $P(T)$ will not lead to cyclic τ-adic expansions. □

5 Cyclic τ-adic expansions in $\mathbb{Z}[\tau]$

Let $q = 9$. Then, $a_1 = M_1 - 9 - 1 \leq 9, 6a_1 - 18 < a_2 \leq a_1^2/4 + 18$. If $a_1 = 9$, then $a_2 = 37$ or 38, and hence, $P(T) = T^4 + 9T^3 + 37T^2 + 81T + 81$ or $P(T) = T^4 + 9T^3 + 38T^2 + 81T + 81$. We have

$$\begin{aligned} 81 &= -a_2\tau^2 + (a_2 - 9)\tau^3 + ((89 - a_2)\tau^4 + (a_2 - 8)\tau^5 \\ &\quad + 8\tau^6 + \tau^7) \\ &= -a_2\tau^2 + (a_2 - 9)\tau^3 + -(a_2 - 8)\tau^4 \\ &\quad - \tau((89 - a_2)\tau^4 + (a_2 - 8)\tau^5 + 8\tau^6 + \tau^7), \end{aligned}$$

which implies that 81 can only be expressed in a cyclic τ-adic expansion, that is, both $P(T) = T^4 + 9T^3 + 37T^2 + 81T + 81$ and $P(T) = T^4 + 9T^3 + 38T^2 + 81T + 81$ lead to cyclic τ-adic expansions.

If $a_1 = 8$, then $31 \leq a_2 \leq 33$. If $a_2 = 32, 33$, then ξ has a τ-adic expansion of length at most 8. If $a_2 = 31$, then we can only get a cyclic τ-adic expansion for $\xi = 81$. Thus, for the curves with the characteristic polynomial $P(T) = T^4 \pm 8T^3 + 31T^2 \pm 72T + 81$, we can not get a finite τ-adic expansion for 81 with the coefficients in $\{-\lceil q^2/2 \rceil + 1, \cdots, \lfloor q^2/2 \rfloor\}$. But if we add ± 41 to the coefficient set, then 81 will have a τ-adic expansion of length five.

Theorem 3 *Let C is a hyperelliptic curve of genus g over $\mathbb{F}_q$ and*

$$P(T) = T^{2g} + a_1T^{2g-1} + \cdots + a_gT^g + \cdots + a_1q^{g-1}T + q^g$$

be its characteristic polynomial with a root τ. If there exists $\xi \in \mathbb{Z}[\tau]$ such that ξ can only be expressed in a cyclic τ-adic expansion, then we call that $P(T)$ leads to cyclic τ-adic expansions.

Let $\tilde{C}$ be a quadratic twist of the hyperelliptic curve C and its characteristic polynomial $\tilde{P}(T)$ as

$$T^{2g} - a_1T^{2g-1} + \cdots + (-1)^g a_gT^g + \cdots - a_1q^{g-1}T + q^g$$

with a root of $\tilde{\tau}$. Then,

1) $P(T)$ leads to cyclic τ-adic expansions if and only if the following inequality (16) *holds.*

$$\sharp\mathbb{J}_C(\mathbb{F}_q) \leq \lfloor q^g/2 \rfloor \quad \text{or} \quad \sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q) \leq \lfloor q^g/2 \rfloor. \quad (16)$$

2) There exists an element $\xi \in \mathbb{Z}[\tau]$ which has only a cyclic τ-adic expansion if and only if there exists an element $\tilde{\xi} \in \mathbb{Z}[\tilde{\tau}]$ which has only a cyclic $\tilde{\tau}$-adic expansion, that is, $P(T)$ leads to cyclic τ-adic expansions if and only if $\tilde{P}(T)$ leads to cyclic $\tilde{\tau}$-expansion.

Proof 1). Suppose ξ can only be expressed as a cyclic τ-adic expansion and

$$\begin{aligned} \xi &= x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3 \\ &= r_0 \pm \tau(x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3), \\ &\quad x_0 > \lfloor q^2/2 \rfloor, |r_0| \leq \lfloor q^2/2 \rfloor. \end{aligned}$$

Let $x_0 - r_0 = dq^2$, then $x_0 = \pm(x_1 - da_1q)$, $x_1 = \pm(x_2 - da_2)$, $x_2 = \pm(x_3 - da_1)$ and $x_3 = \mp d$. and hence, $x_0 = -d - da_1 - da_2 - da_1q = d(q^2 - \sharp\mathbb{J}_C(\mathbb{F}_q))$ when $x_3 = -d$, or $x_0 = -d + da_1 - da_2 + da_1q = d(q^2 - \sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q))$ when $x_3 = d$.

It follows $r_0 = -d\,\sharp\mathbb{J}_C(\mathbb{F}_q)$ and $d\,\sharp\mathbb{J}_C(\mathbb{F}_q) \leq \lfloor q^2/2 \rfloor$, or $r_0 = -d\,\sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q)$ and $d\,\sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q) \leq \lfloor q^2/2 \rfloor$. Hence

$$\sharp\mathbb{J}_C(\mathbb{F}_q) = |r_0|/d \leq \lfloor q^2/2 \rfloor$$

or

$$\sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q) = |r_0|/d \leq \lfloor q^2/2 \rfloor.$$

Suppose ξ can be expressed as the following cyclic τ-adic expansion and

$$\begin{aligned} \xi &= x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3 \\ &= r_0 + r_1\tau + \tau^2(x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3), \\ &\quad x_0 > \lfloor q^2/2 \rfloor, |r_i| \leq \lfloor q^2/2 \rfloor, i = 0, 1. \end{aligned}$$

Let $x_0 - r_0 = dq^2$ and $x_1 - da_1q - r_1 = eq^2$, then we have $x_0 = x_2 - da_2 - ea_1q$, $x_1 = x_3 - da_1 - ea_2$, $x_2 = -d - ea_1$ and $x_3 = -e$.

Thus, $x_0 = dq^2 + r_0 = -d - ea_1 - da_2 - ea_1q$ and $x_1 = da_1q + eq^2 + r_1 = -e - da_1 - ea_2$, which implies

$$r_0 + r_1 = -(d + e)\,\sharp\mathbb{J}_C(\mathbb{F}_q). \quad (17)$$

Hence, if $|d + e| \geq 2$, then

$$\sharp\mathbb{J}_C(\mathbb{F}_q) \leq (|r_0| + |r_1|)/|d + e| \leq \lfloor q^2/2 \rfloor.$$

If $d + e = 0$, then $r_0 = -d\,\sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q)$, and so,

$$\sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q) \leq |r_0|/d \leq \lfloor q^2/2 \rfloor/d \leq \lfloor q^2/2 \rfloor.$$

If $d + e = \pm 1$, then for $\tilde{\xi} = x_0 - x_1\tilde{\tau} + x_2\tilde{\tau}^2 - x_3\tilde{\tau}^3$, we have

$$\tilde{\xi} = r_0 - r_1\tilde{\tau} + \tilde{\tau}^2(x_0 - x_1\tilde{\tau} + x_2\tilde{\tau}^2 - x_3\tilde{\tau}^3).$$

It follows

$$r_0 - r_1 = (-2d + 1)\,\sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q). \quad (18)$$

From the equations (17) and (18) we deduce that

$$\sharp\mathbb{J}_C(\mathbb{F}_q) \leq \lfloor q^2/2 \rfloor \quad \text{or} \quad \sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q) \leq \lfloor q^2/2 \rfloor. \quad (19)$$

Similarly, we can easily show that Inequality (19) also holds if ξ has a longer period expression.

On the other hand, we suppose $\sharp\mathbb{J}_C(\mathbb{F}_q) \leq \lfloor q^2/2 \rfloor$(similar discussion for $\sharp\mathbb{J}_{\tilde{C}}(\mathbb{F}_q) \leq \lfloor q^2/2 \rfloor$), and let

$$\begin{cases} x_0 &= a_1q + a_2 + a_1 + 1 \\ x_1 &= a_2 + a_1 + 1 \\ x_2 &= a_1 + 1 \\ x_3 &= 1 \end{cases}$$

Then, we have

$$\begin{aligned}\xi &= x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3 \\ &= \sharp\mathbb{J}_C(\mathbb{F}_q) + \tau(x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3)\end{aligned}$$

is a cyclic τ-adic expansion.

2). Suppose

$$\begin{aligned}\xi &= x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3 \\ &= r_0 + \tau(x_0 + x_1\tau + x_2\tau^2 + x_3\tau^3) \\ &\text{(with } x_0 > \lfloor q^2/2\rfloor, |r_0| \le \lfloor q^2/2\rfloor)\end{aligned}$$

is a cyclic τ-adic expansion, then

$$\begin{aligned}\tilde{\xi} &= x_0 - x_1\tilde{\tau} + x_2\tilde{\tau}^2 - x_3\tilde{\tau}^3 \\ &= r_0 - \tilde{\tau}(x_0 - x_1\tilde{\tau} + x_2\tilde{\tau}^2 - x_3\tilde{\tau}^3)\end{aligned}$$

is is a cyclic $\tilde{\tau}$-adic expansion.

Similar discussions will show that Theorem 3 still holds for the hyperelliptic curve of genus $g > 2$. □

For example, The curves with $P(T) = T^4 \pm 9T^3 + 38T^2 \pm 81T + 81$, $P(T) = T^4 - 5T^3 + 15T^2 - 25T + 25$ or $P(T) = T^6 - 7T^5 + 21T^4 - 49T^3 + 147T^2 - 343T + 343$ will lead to cyclic τ-adic expansions. For $q = g = 2$, only the non-supersingular curves with $P(T) = T^4 \pm 2T^3 + 2T^2 \pm 4T + 4$ lead to cyclic τ-adic expansions. For $q = 3$ and $g = 2$, only the non-supersingular curves with $P(T) = T^4 \pm 2T^3 + 2T^2 \pm 6T + 9$ or $T^4 \pm T^3 - 2T^2 \pm 3T + 9$ or $T^4 \pm 3T^3 + 5T^2 \pm 9T + 9$ will lead to cyclic τ-adic expansions.

Based on Hasse-Weil Theorem, that is, $(\sqrt{q} - 1)^{2g} \le \sharp\mathbb{J}_C(\mathbb{F}_q) \le (\sqrt{q}+1)^{2g}$, if q is an integer such that $(\sqrt{q}-1)^{2g} \ge q^g/2$, then, the corresponding hyperelliptic curves will not lead to cyclic expansion. For $g = 2$, 3 and 4, we have $q \ge 37$, 83 and 139, respectively.

If the curve C with $P(T)$ leads to cyclic expansion, then by Theorem 3, $P(1) \le \lfloor q^g/2\rfloor$ or $P(-1) \le \lfloor q^g/2\rfloor$, hence we can add $\pm(P(1) - q^g)$ or $\pm(P(-1) - q^g)$ to the coefficient set to make the expansion finite. For example, if the coefficient set is $\{0, \pm1, \cdots, \pm39, \pm40\} \bigcup \{\pm51\}$, then for the hyperelliptic curves with $P(T) = T^4 \pm 9T^3 + 38T^2 \pm 81T + 81$, all τ-adic expansions are finite.

6 Optimizing the length of the τ-expansion

Let $\beta = b_0 + b_1\tau + \cdots + b_{2g-1}\tau^{2g-1} \in \mathbb{Z}[\tau]$, then since $P(T)$ is irreducible, $P(T)$ and $B(T) = b_0 + b_1T + \cdots + b_{2g-1}T^{2g-1}$ are coprime. Hence, there exist polynomials $U(T), V(T) \in \mathbb{Z}[T]$ such that

$$U(T)B(T) + V(T)P(T) = 1.$$

Replace T with τ, we have $\beta^{-1} = U(\tau) \in \mathbb{Z}[\tau]$. That is, we can use the extended Euclidean algorithm to compute the inverse of any element of $\mathbb{Z}[\tau]$.

For any divisor $D \in \mathbb{J}(\mathbb{F}_{q^n})$, we have $\phi^n(D) = D$. Furthermore, by Lemma 1, we have

$$\sharp\mathbb{J}(\mathbb{F}_{q^n}) = \prod_{i=1}^{2g}(1 - \tau_i^n) = \prod_{i=1}^{2g}(1 - \tau_i)\prod_{i=1}^{2g}(\sum_{j=0}^{n-1}\tau_i^j).$$

If for some $D \in \mathbb{J}(\mathbb{F}_{q^n})$, $\phi(D) = D$, that is, $(1 - \tau)D =< 1, 0 >$, then $\prod_{i=1}^{2g}(1 - \tau_i)D =< 1, 0 >$, that is, $\sharp\mathbb{J}(\mathbb{F}_q)D =< 1, 0 >$. For practical cryptosystems, the divisor D should be chosen to be of large order. Hence, $\sharp\mathbb{J}(\mathbb{F}_q)D =< 1, 0 >$ generally does not hold. Thus, for a large multiplier m, we can obtain the divisor multiplication mD by computing $\bar{m}D$ with $\bar{m} = m \bmod (\tau^n - 1)$ or $m \bmod (\frac{\tau^n-1}{\tau-1})$.

Similar to Theorem 3.1 in (8), we have the following Lemma 5.

Lemma 5 *For any positive integers n and m, there exists $\bar{m} \in \mathbb{Z}[\tau]$, such that*

1. $\bar{m} = m \bmod (\tau^n - 1)$,
2. $N(\bar{m}) \le \frac{\sqrt{g}(q^g-1)(\sqrt{q}^n+1)}{2(\sqrt{q}-1)}$.

We can prove this lemma by letting $s = m/(\tau^n - 1) = \sum_{i=0}^{2g-1} s_i\tau^i \in \mathbb{Q}[\tau]$, $r = \sum_{i=0}^{2g-1} \lfloor s_i + 1/2\rfloor\tau^i$ and $\bar{m} = m - r(\tau^n - 1)$.

By letting $\alpha = m(\tau - 1)/(\tau^n - 1) = \sum_{i=0}^{2g-1} \alpha_i\tau^i \in \mathbb{Q}[\tau]$, $\gamma = \sum_{i=0}^{2g-1} \lfloor \alpha_i + 1/2\rfloor\tau^i \in \mathbb{Z}[\tau]$ and $\bar{m} = m - \gamma(\tau^n - 1)/(\tau - 1)$, we can prove the following Lemma 6.

Lemma 6 *For any positive integers n and m, there exists $\bar{m} \in \mathbb{Z}[\tau]$, such that*

1. $\bar{m} = m \bmod ((\tau^n - 1)/(\tau - 1))$,
2. $N(\bar{m}) \le \frac{\sqrt{g}(q^g-1)(\sqrt{q}^n-1)}{2(\sqrt{q}-1)^2}$.

Thus, by Theorem 1, Theorem 2, Lemma 5 and Lemma 6, we obtain the following Theorem 4.

Theorem 4 *Let C be a hyperelliptic curve of genus g over $\mathbb{F}_q$, and let τ be a root of C's irreducible characteristic polynomial $P(T)$. If C does not lead to cyclic τ-adic expansions, then for a large positive integer m, m is congruent, modulo $\tau^n - 1$ or $(\tau^n - 1)/(\tau - 1)$, to a τ-adic expansion of length at most $n+4g+5$ or $n+4g+4$, respectively. If C leads to cyclic τ-adic expansions, then this conclusion still holds if $P(-1) - q^g$ or $P(1) - q^g$ is added to the coefficient set.*

7 An efficient scalar multiplication algorithm

According to the above discussion, we can obtain an efficient scalar multiplication algorithm. This algorithm is composed of the four steps: pre-computing, reducing the multiplier, converting the reduced multiplier into Frobenius expansion and computing scalar multiplications.

Let $a_0 = 1$, $P[i] = a_iq^{g-i}$ and $P[g + i] = a_{g-i}$ for $i = 1, \ldots, g$.

Algorithm 1 Compute scalar multiplication by τ-adic Expansion

Input: a large positive integer multiplier m and a divisor $D \in \mathbb{J}(\mathbb{F}_{q^n})$.

Output: mD.

I) **Pre-computing**:

1. For $0 < r \le \lfloor q^g/2\rfloor$, compute rD by (signed) binary method and store it as D_r.
2. For $-\lceil q^g/2\rceil + 1 \le r < 0$, set

$$rD :=< x((-r)D), -y((-r)D) - h(u) >$$

and store it as D_r, where $x((-r)D)$ and $y((-r)D)$ denote the first polynomial and the second polynomial of the divisor $(-r)D$, respectively.

II) **Computing** $m \bmod (\tau^n - 1)$:

1. Find integers $s[i]$ such that

$$s = \sum_{i=0}^{2g-1} s[i]\tau^i = \tau^n - 1 :$$

1) Initialize $s[i] := -P[i]$ for $0 \le i \le 2g-1$.
2) For k from 1 to $n - 2g$, do
   (a) $\Delta := s[2g-1]$.
   (b) For i from 1 to $2g-1$, set $s[i] := s[i-1] - P[i]\Delta$, and $s[0] := -P[0]\Delta$.
3) Set $s[0] := s[0] - 1$.
4) Set $s := \sum_{i=0}^{2g-1} s[i]\tau^i$.

2. Applying Extended Euclidean Algorithm, there exist t, $u \in \mathbb{Z}[\tau]$ with $\deg_\tau t \le 2q-1$, such that

$$t \cdot s + u \cdot P(\tau) = 1.$$

3. For $t := \sum_{i=0}^{2g-1} t_i\tau^i$, set

$$\alpha := \sum_{i=0}^{2g-1} \lfloor m \cdot t_i + 1/2 \rfloor \tau^i.$$

4. Set $\bar{m} := m - s\alpha \bmod P(\tau)$.

III) **Supposing** $\bar{m} = \sum_{i=0}^{2g-1} \bar{m}_i\tau^i$ **and converting** $\bar{m}$ **into a** τ**-adic expansion**:

1. $j := 0$; $k := 0$.
2. If $\bar{m} \neq 0$, then do
   (a) Select $r_j \in \{-\lceil q^g/2 \rceil + 1, \ldots, -1, 0, 1, \ldots, \lfloor q^g/2 \rfloor\}$ such that $q^g | (\bar{m}_0 - r_j)$.
   (b) Set $d := (\bar{m}_0 - r_j)/q^g$.
   (c) Set $\bar{m} := \sum_{i=0}^{2g-2} (\bar{m}_{i+1} - P[i+1]d)\tau^i - d\tau^{2g-1}$.
   (d) Set $j := j + 1$ and $k := k + 1$, and go back.

IV) **Computing** $\bar{m}D$:

1. Initialize $B := D_{r_{k-1}}$.
2. For i from $k-2$ downto 0 do
   (a) Set $B := \phi(B)$.
   (b) Set $B := B + D_{r_i}$.

V) Output B as mD.

Since the multiplier m can also be reduced by modulo $(\tau^n - 1)/(\tau - 1)$, Steps 1 in Step II) can be replaced by the following steps:

Step II*) **Computing** $m \bmod (\tau^n - 1)/(\tau - 1)$:

1. Find integers $s[i]$ such that $s = \sum_{i=0}^{2g-1} s[i]\tau^i = (\tau^n - 1)/(\tau - 1)$:
   1) Initialize $0 \le i \le 2g-1$, set $s[i] := 1 - P[i]$ and $t[i] := -P[i]$;
   2) For k from 1 to $n - 2g - 1$ do
      (a) Set $\Delta := t[2g-1]$ and $t[0] := -P[0]\Delta$;
      (b) For i from 1 to $2g-1$, set $t[i] := t[i-1] - P[i]\Delta$ and $s[i] := s[i] + t[i]$;
   3) Set $s := \sum_{i=0}^{2g-1} s[i]\tau^i$;

Note that if $P(1) \le \lfloor q^g/2 \rfloor$ or $P(-1) \le \lfloor q^g/2 \rfloor$, then add $P(1) - q^g$ or $P(-1) - q^g$ to the coefficient set. Take $P(1) < q^g/2$ for example, we only make some minor modifications in Algorithm 1 as follows:

First, add the computation of $\pm(q^g - P(1))D$ in the precomputation step; Second, change the step (a)-(b) in Step III) as follows:

(a*) If $|\bar{m}_0| \le \lfloor q^g/2 \rfloor$ or $\bar{m}_0 = P(1) - q^g$, then set $r_j := \bar{m}_0$, otherwise, go to the next step:

(b*) Select $r_j \in \{P(1) - q^g, -\lceil q^g/2 \rceil + 1, \cdots, -1, 0, 1, \cdots, \lfloor q^g/2 \rfloor\}$ such that $q^g | (\bar{m}_0 - r_j)$.

We implement Step II)-III) in Algorithm 1 in Maple for five hyperelliptic curves and get the Table 1. Table 1 lists five hyperelliptic curves and the bits of the orders of their corresponding Jacobian groups, the average lengths and densities of the τ-adic expansions of the multipliers approximate to the Jacobian group orders, and the average lengths (1)-(2) and densities (1)-(2) of the τ-adic expansions of the multipliers after reduced by modulo $(\tau^n - 1)/(\tau - 1)$ or $(\tau^n - 1)$, respectively. The density means the ratio of the number of the non-zero coefficients to the length in a τ-adic expansion.

The corresponding characteristic polynomials of the five hyperelliptic curves in Table 1 are $T^4 + 2T^3 + 3T^2 + 4T + 4$, $T^4 - 2T^3 + 2T^2 - 6T + 9$, $T^6 + 2T^4 - 2T^3 + 4T^2 + 8$, $T^4 - 4T^3 + 11T^2 - 20T + 25$, and $T^6 + 2T^5 + 4T^4 + 14T^3 + 20T^2 + 50T + 125$, respectively.

Table 1 shows that, when the multipliers are reduced by modulo $(\tau^n - 1)/(\tau - 1)$ or $\tau^n - 1$, the average lengths of the τ-adic expansions are between $n - 2$ and $n + g$, or between $n + 1$ and $n + g + 1$, respectively. It also shows that, if the multipliers are not reduced, then the average length of τ-adic expansions is about q^g times of the extension degree of the field. While their average densities are almost the same whether the multipliers are reduced or not.

Suppose the multiplier $m \sim q^{gn}$(near to the Jacobian order). Then, to compute mD, the binary method needs on average $\frac{ng}{3} \log_2 q$ divisor additions and $ng \log_2 q$ divisor doublings. While according to our experiments, Algorithm 1 needs on average $n + \frac{g}{2}$ divisor additions and $g \log_2 q - 1$ divisor doublings, plus about $n + \frac{g}{2}$ divisor evaluations of Frobenius endomorphism. If we implement Algorithm 1 in some *normal basis*, then the Frobenius evaluation cost can be considered free. Hence, according to Theorem 14 in (11), Algorithm 1 will cost about 55% less than the signed binary method for the curves listed in Table 1. It follows that our algorithm will greatly speed up the implementation of hyperelliptic curve cryptosystems since the divisor scalar multiplication is the most time-consuming operation.

8 Conclusion

In this paper, we have applied Frobenius endomorphism and Euclidean length to reduce the multipliers in divisor scalar multiplications by modulo $\tau^n - 1$ or $(\tau^n - 1)/(\tau - 1)$, and show that the upper bound of the lengths of the reduced multipliers' τ-adic expansions is $n + 4g + 5$. In addition, our experiment results show that the lengths of the multipliers' τ-adic expansions

Hyperelliptic curves	q	n	bits of orders	average length	average density	reduced average length(1)	reduced average density(1)	reduced average length(2)	reduced average density(2)
$v^2+(u^2+u+1)v=u^5+u^4+u^3+u$	2	61	122	242.125	0.749	62.000	0.761	62.833	0.756
		67	134	264.250	0.738	64.667	0.732	68.000	0.733
		73	146	291.000	0.758	70.500	0.756	73.000	0.752
		89	178	355.000	0.736	87.833	0.784	87.500	0.760
		113	226	451.000	0.741	110.667	0.768	112.333	0.712
$v^2=u^5+u^4-u^3+u^2-u+2$	3	61	194	244.000	0.832	61.833	0.865	62.000	0.869
		67	213	267.500	0.828	67.667	0.872	68.167	0.905
		97	308	386.833	0.844	97.667	0.887	99.500	0.901
		103	327	412.333	0.826	104.500	0.890	105.333	0.889
		113	359	452.000	0.824	112.667	0.873	114.667	0.903
$v^2+v=u^7+u^6+u^5$	2	29	87	168.400	0.828	30.333	0.890	29.667	0.832
		37	111	210.000	0.861	37.667	0.858	38.333	0.878
		43	129	254.000	0.867	42.833	0.883	45.500	0.865
		59	177	352.000	0.845	60.500	0.859	59.833	0.847
		67	201	398.000	0.865	67.167	0.868	70.000	0.877
$v^2=u^5+u^4+2u^3+u^2+u+2$	5	61	284	246.000	0.906	62.167	0.949	64.000	0.958
		67	312	270.000	0.916	68.667	0.973	70.500	0.962
		71	330	285.600	0.936	72.167	0.972	74.167	0.951
		79	367	318.000	0.936	81.167	0.955	81.667	0.943
		83	386	334.000	0.930	84.500	0.955	85.167	0.967
$v^2=u^7+u^5+u^3+u-1$	5	29	203	174.000	0.986	31.667	0.984	33.500	0.985
		31	216	186.000	0.985	33.667	0.980	34.833	0.990
		37	258	222.000	0.998	40.833	0.988	40.333	0.979
		43	300	258.000	0.979	44.167	0.985	47.333	0.986
		53	370	318.000	0.991	55.167	0.988	57.667	0.991

Figure 1: Average Lengths and Densities of τ-adic Expansions

are actually between $n-2$ and $n+g+1$. While Günther et al(8) did experimentally show that the two hyperelliptic curves $v^2+uv=u^5+\alpha u^2+1$ ($\alpha=0,1$) have some τ-adic expansions of length about $n+\frac{4}{3}$ (which are near to our experimental result, but they did not give a theoretical proof.

In practical hyperelliptic curve cryptosystems, since the parameters q, g, n and the basic divisor D are relatively fixed, we can pre-compute $\phi^i(r_jD)$ for $1\leq i\leq n+4g+4$ and $-\lfloor q^g/2\rfloor+1\leq j\leq\lfloor q^g/2\rfloor$ and then store the results as a table. If we employ this table, then our algorithm only needs at most $n+4g+4$ divisor additions, which is approximately one third computation expense that the binary method does. In addition, based on the Proposition 3.4 in (12), the elliptic curve rational point group $E_C(\mathbb{F}_{q^n})$ is isomorphic to the Jacobian group $\mathbb{J}_C(\mathbb{F}_{q^n})$ under their group law definitions when the curve C's genus $g=1$, hence, our Algorithm 1 is also applicable to the scalar multiplication computations on $E_C(\mathbb{F}_{q^n})$.

Acknowledgement

This research is supported by the National Science Foundation of China (No.60763009), the science and technology Key Project of the Ministry of Education of China(No.207089), and Zhejiang Natural Science Foundation of Outstanding Youth Team Project(No.R1090138).

References

[1] N. Koblitz(1989). A Family of Jacobians suitable for discrete log cryptosystems, Advances in Cryptology-Crypto'88, LNCS 403, Springer-Verlag, pp.94-99.

[2] N. Koblitz(1989). Hyperelliptic cryptosystems, Journal of Cryptology, No.1, pp.139-150.

[3] J. Pollard(1978). Monte Carlo methods for index computation mod p, Mathematics of Computation, No.32, pp. 918ÍC924.

[4] S. C. Pohlig, M. E. Hellman(1978). An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. IEEE Trans. Information Theory, IT-24(1), pp.106ÍC110.

[5] A. Weil(1949). Number of solutions of equations in finite fields. Bull. AMS. 55, pp.497-508.

[6] V. Müller(1998). Fast multiplication on Elliptic Curve over Small fields of Characteristic Two. Journal of Cryptology. 11, pp. 219-234.

[7] N. P. Smart(1999). Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic. Journal of Cryptology. 12, pp.141-151.

[8] Ch. Günther, T. Lange and A.Stein(2001). Speeding Up the Arithmetic on Koblotz Curves of Genus Two. LNCS 2012,pp. 106-117.

[9] K. Matsuo, J.Chao, S.Tsujii(2002). An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields. LNCS. 2369, pp. 461-474.

[10] D. Maisner, E. Nart(2002). Abelian surfaces over finite fields as Jacobians. Experimental Mathematics. 11, pp. 321-337.

[11] A. Enge(2001). The Extended Euclidean Algorithm on Polynomials. and the Com-putational Efficiency of Hyper-elliptic Cryptosystems,Design, Codes and Cryptography. 23(1), pp.53-74.

[12] J. H. Silverman(1986). The Arithmetic of Elliptic Curves, Spriger-Verlag, pp.66-67.