종수 2의 초타원곡선에서의 구체적이고 효율적인 연산 방법[1)]

이은정, 최영주*

*포항공과대학교, 수학과

Explicit Formulae for operations in Jacobian of hyperelliptic curves

YoungJu. Choie, Eunjeong. Lee*

*Department of Mathematics, POSTECH

Abstract

We give explicit formulae for composition of genus two. The previous work described in [4] only contains the formulae for common cases. In this paper, we give formulae for all cases of two divisors as input. Furthermore, the formulae contains the form of rational functions such that related to the implementation of the Tate pairing.

I. Introduction

Since the algorithm for operations in divisor class group proposed by Cantor is performed for any hyperelliptic curves of arbitrary genus, implementation of the algorithm includes inefficient computation specially for genus 2 and 3 which is useful cryptographic purpose. Recently, explicit formulae of composition for the case of genus two, three and four have been given in [4], [5] and [6], respectively.

In this paper, we also give explicit formulae for composition of genus two. The previous work described in [4] only contains the formulae for common cases. we give explicit formulae for all cases of input divisors. Furthermore, the formulae give the form of rational functions related to the implementation of the Tate pairing explained in [2].

Sections II describes the definitions and properties about hyperelliptic curves. Section III and IV summarizes the addition law and doubling on the divisor class group. In the final section, concluding remark is given. Appendix A shows two tables.

II. Preliminary

In this section, we give the basic definitions and properties on hyperelliptic curves(See [3] for further details).

Let F_q be a finite field with q elements of characteristic p and $\overline{F_q}$ be the algebraic closure of F_q.

Definition 2.1. *A hyperelliptic curve H of genus 2 over F_q ($g \geq 1$) is an equation of the form*

1) This work was partially supported by University ITRC fund

$$H : y^2 + (h_2x^2 + h_1x + h_0)y = x^5 + \sum_{i=0}^{4} f_i x^i \quad (1)$$

where $h(x) = h_2x^2 + h_1x + h_0 \in F_q[x]$,

$F(x) = x^5 + \sum_{i=0}^{4} f_i x^i \in F_q[x]$ *and there are no singular solutions of (1).*

Now consider H as a set of rational points such as

$$H = \{(a,b) \in \bar{F}_q \times \bar{F}_q \mid b^2 + h(a)b = F(a)\} \cup \{O\}$$

where O is the point at infinity of H. Let K be a quadratic function field defined by (1). Let

$$\mathrm{Div}(K) = \{D \mid D = \sum_{P \in H} n_P P, n_P \in Z,$$
$$n_P = 0 \text{ for almost all points } P\}$$

where the formal sum $D = \sum_{P \in H} n_P P$ is called a *divisor*. If $n_P \geq 0$, D is called *effective*. The *support* of D is defined as

$$\mathrm{supp}(D) = \{P \mid D = \sum_{P \in H} n_P P, \text{ such that } n_P \neq 0\}$$

Consider a subgroup, called a group of zero divisors, for $\deg(D) = \sum_{P \in H} n_P$,

$$\mathrm{Div}_0(K) = \{D \mid D = \sum_{P \in H} n_P P, \deg(D) = 0\}$$

The greatest common divisors of D_1, D_2 of

$D_1 = \sum_{P \in H} m_P P, D_2 = \sum_{P \in H} n_P P$ is defined by

$$\mathrm{g.c.d}(D_1, D_2) = \sum_{P \in H} \min(m_P, n_P)P - \sum_{P \in H} \min(m_P, n_P)O$$

The set of principle divisors

$$P_H = \{(g) \mid (g) = \sum_{P \in H} v_P(g)P, g \in K\}$$

where v is a valuation map from K to Z, is a subgroup of $\mathrm{Div}_0(K)$. The quotient group

$$J_H = \mathrm{Div}_0(K)/P_H$$

is called the *divisor class group* which is the Jacobian of the curve H. It is well known that each divisor class, denote $\bar{D}$, can be uniquely represented via the *reduced divisor*.

Theorem 2.2. reduced divisor [3, 4]

Let K be the function field given by (1).

1. Each element, say $\bar{D}$, in the quotient group J_H has exactly one divisor of the following type

$$D = P_1 - O \text{ or } D = P_1 + P_2 - 2O, P_i \neq O$$

which is called the reduced divisor.

2. Put $P_i = (a_i, b_i, 1 \leq i \leq r)$ and let $u(x) = \prod_{i=1}^{r}(x - a_i)$, r=1 or 2. Then there exists unique polynomial $v(x) \in \bar{F}_q[x]$ satisfying $\deg(v) < \deg(u) \leq 2$, $b_i = v(a_i)$ and $u \mid (v^2 + hv - F)$. Then

$$D = \mathrm{g.c.d.}((u(x)), (v(x) - y)) .$$

We will denote a divisor class by $\bar{D}$ and let $\bar{D} = [u, v] = \mathrm{g.c.d.}((u), (v - y)) = D - \deg(D)O$ where $D = \overline{D_+} = P_1 - O$ or $P_1 + P_2 - 2O$ is the effective part of the reduced divisor.

The addition of divisor classes in J_H can be defined by the reduced divisors using Cantor's algorithm [1]. For two reduced divisors $\bar{D}_1, \bar{D}_2$, the algorithm proposed by Cantor (Algorithm 1) gives the third divisor $\bar{D}_3$ such that $\bar{D}_3 + (f) = \bar{D}_1 + \bar{D}_2$ for some rational function f.

Algorithm 1. Cantor's Algorithm [1]

Input: $\bar{D}_1 = [u_1, v_1]$, $\bar{D}_2 = [u_2, v_2]$

Output: $\bar{D}_3 = [u_3, v_3]$ where $\bar{D}_3 + (f) = \bar{D}_1 + \bar{D}_2$

Step 1. Compute e_1, e_2, e_3 such that
$d = \gcd(u_1, u_2, v_1 + v_2 + h) = e_1u_1 + e_1u_2 + e_3(v_1 + v_2 + h)$

Step 2. Compute $G(x) = u_1 u_2 / d^2$.

Step 3. Compute

$$l = \frac{e_1 u_1 v_2 + e_2 u_2 v_1 + e_3 (F + v_1 v_2)}{d} \bmod G$$

Step 4. Compute $u_3 = monic(\frac{F - l^2 - hl}{G})$

Step 5. Compute $v_3 = -l - h \bmod u_3$

Step 6. If $\deg(u_3) > 2$, then set

$$G \leftarrow u_3, l \leftarrow v_3$$

and goto the step 4.

III. Improved Formulae for Addition in J_H

Since Algorithm 1 is for hyperelliptic curves of arbitrary genus, an implementation of the algorithm may be inefficient for fixed genus, specially for genus 2 and 3 which is useful cryptographic purposes. Recently, for efficient computation, explicit formulae of composition for the case of genus two, three and four have been given in [4], [5] and [6], respectively.

In this section and next section, we also give explicit formulae for composition of genus two. The previous work described in [4] only contains the formulae for the most common cases. In this section, we discuss about the addition for all cases of input divisors $\bar{D}_1, \bar{D}_2$ (see Table 2 in Appendix A). Furthermore, Table 2 gives the form of rational functions such that $\bar{D}_3 + (f) \sim \bar{D}_1 + \bar{D}_2$ related to implementation of the Tate pairing [2].

Our improvements are summarized as follows.

1. We give explicit formulae for $\bar{D}_3$ with the rational function f.

2. We give an explicit formula for the case (4) in Table 2.

3. We rewrite the addition formulae in [4] to give explicit answer for $l(x)$ such that $f = \frac{y - l(x)}{u_3}$ in the case (3) and the case (6)(respectively, Algorithm 2 and Algorithm 4).

4. The addition procedure for the case (7) can be improved (Section III.4).

For H, defined as (1), let's denote reduced divisors by $\bar{D}_i = [u_i, v_i]$ for i=1,2,3, such that $\bar{D}_3 + (f) = \bar{D}_1 + \bar{D}_2$. We may assume $\deg(u_1) \le \deg(u_2) \le 2$ and $\deg(u_1) \neq 0$ since if $\deg(u_1)=0$, then $\bar{D}_1$ =identity in J_H. Denote $u_i(x) = x^2 + u_{i1}x + u_{i0}$ and $v_i = v_{i1}x + v_{i0}$ for $i = 1, 2, 3$ when $\deg(u_1) = 2$. Denote $u_1(x) = x + u_{10}$ and $v_1(x) = v_{10}$ when $\deg(u_1) = 1$. Furthermore, we assume $\bar{D}_1 \neq \bar{D}_2$, which is the duplication case(for this case, see Section IV).

The third divisor $\bar{D}_3$ and f are summarized as follows according to the cases of input divisors (See also Table 2 in Appendix A).

Case (1). $\deg(u_1) = \deg(u_2) = 1, \gcd(u_1, u_2) = 1$

From the condition, we can let $D_1 = (a_1, b_1)$ and $D_2 = (a_2, b_2)$ with $a_1 \neq a_2$. Then $D_1 + D_2 - 2O$ is already a reduced divisor and thus $\bar{D}_3 + (1) = (a_1, b_1) + (a_2, b_2) - 2O = [u_3, v_3]$ where u_3, v_3 are given in Table 2.

Case (2). $\deg(u_1) = \deg(u_2) = 1, \gcd(u_1, u_2) \neq 1$

Since $u_1 = u_2$ and $D_1 \neq D_2$, we can let $D_1 = (a_1, b_1)$ and $D_2 = -D_1 = (a_1, -b_1 - h(a_1))$. Thus $\bar{D}_3 = (x - a_1) = \bar{D}_1 + \bar{D}_2$.

Case (3).

$\deg(u_1) = 1, \deg(u_2) = 2, \gcd(u_1, u_2) = 1$

This case is explained in Section III.1.

Case (4).

$\deg(u_1) = 1, \deg(u_2) = 2, \gcd(u_1, u_2) \neq 1$

$\gcd(u_1, u_2, v_1 + v_2 + h) = 1$

This case is explained in Section III.2.

Case (5).

$\deg(u_1) = 1, \deg(u_2) = 2, \gcd(u_1, u_2) = u_1$

$\gcd(u_1, u_2, v_1 + v_2 + h) = x - a_1 = u_1$

Since a_1 is a root of v_1+v_2+h, $\bar{D}_2$ has the form $\bar{D}_2=(a_1,-b_1-h)+(a_4,b_4)-2O$ where $a_1 \neq a_4$. Thus $\bar{D}_1+\bar{D}_2=(a_4,b_4)-O+(u_1)$ by Lemma 7 in [2].

Case (6) $\deg(u_1)=\deg(u_2)=2, \gcd(u_1,u_2)=1$

This case is explained in Section III.3.

Case (7) $\deg(u_1)=\deg(u_2)=2,$

$\gcd(u_1,u_2)=x-a_1, \gcd(u_1,u_2,v_1+v_2+h)=1$

This case is explained in Section III.4.

Case (8) $\deg(u_1)=\deg(u_2)=2,$

$\gcd(u_1,u_2)=\gcd(u_1,u_2,v_1+v_2+h)=x-a_1$

Let $\bar{D}_1=(a_1,b_1)+(a_2,b_2)-2O$. Since a_1 is a root of v_1+v_2+h, $\bar{D}_2$ is of the form $\bar{D}_2=(a_1,-b_1-h)+(a_4,b_4)-2O$, where $a_2 \neq a_4$. Thus $\bar{D}_3+(x-a_1)=(a_2,b_2)+(a_4,b_4)-2O$.

Case (9)

$\deg(u_1)=\deg(u_2)=2, u_1=u_2, v_1=-v_2$

This case is $\bar{D}_2=-\bar{D}_1$. Thus $\bar{D}_1+\bar{D}_2=(u_1)$

Case (10)

$\deg(u_1)=\deg(u_2)=2, u_1=u_2, v_1 \neq -v_2$

$v_1 \neq -v_2$ happens only

$\bar{D}_1=(a_1,b_1)+(a_2,b_2)-2O$ and

$\bar{D}_2=(a_1,b_1)+(a_2,-b_2-h)-2O$. Thus,

$\bar{D}_3+(x-a_2)=2(a_1,b_1)-2O$.

In the following subsections, we explain formulae for $\bar{D}_3$ and $l(x)$ in the case of $\gcd(u_1,u_2,v_1+v_2+h)=1$. We lists the number of field multiplications(M), squaring(S) and inversion(I) in F_q for each case, where the multiplication by the coefficients of h and F are not counted..

1. Addition in the case of $\deg(u_1)=1$, $\deg(u_2)=2$, $\gcd(u_1,u_2)=1$

From Lemma 7 in [2], we can let $l(x)=s_0u_2+v_2$. Since $0 \neq u_2(-u_{10}) \pmod{u_1}$ which can be checked by the computation of the resultant of u_1 and u_2, we get

$$s_0=(v_1-v_2)u_2^{-1} \pmod{u_1}$$
$$=(v_{10}+v_{21}u_{10}-v_{20})(u_{20}-(u_{21}-u_{10})u_{10})^{-1}$$

The formula for this case is described in Algorithm 2.

Algorithm 2. Divisor addition of the case (3)

Input: $\bar{D}_1=[u_1,v_1]$, $\bar{D}_2=[u_2,v_2]$

Output: $\bar{D}_3=[u_3,v_3]$ and $l(x)$.

Step 1. Compute $r=\mathrm{res}(u_1,u_2)$

$$r=u_{20}-(u_{21}-u_{10})u_{10}$$

Step 2. If $r=0$, then goto Algorithm 3(case (4)).

else compute $inv=r^{-1}$.

Step 3. Compute $l(x)=s_0u_2+v_2=s_0x^2+l_1x+l_0$

$$s_0=(v_{10}+v_{21}u_{10}-v_{20}) \cdot inv$$

$$l_1=s_0u_{21}+v_{21}, \quad l_0=s_0u_{20}+v_{20}.$$

Step 4. Compute $u_3=\mathrm{monic}\left(\frac{F-l^2-hl}{u_1u_2}\right)$

$$w_1=f_4-u_{21}, w_2=-u_{21}w_1+f_3-u_{20}+h_2l_1$$

$$w_3=-l_1-v_{21}-h_1+h_2u_{21}$$

$$u_{31}=w_1-s_0^2-u_{10}-h_2s_0,$$

$$u_{30}=w_2+s_0w_3-u_{10}u_{31}$$

Step 5. Compute $v_{31}x+v_{30}=-l-h \pmod{u_3}$

$$v_{31}=(s_0+h_2)u_{31}-l_1-h_1, v_{30}=(s_0+h_2)u_{30}-l_0-h_0$$

Cost : 10M, 1S, 1I

2. Addition in the case of $\deg(u_1)=1$, $\deg(u_2)=2$, $\gcd(u_1,u_2)=u_1$, $\gcd(u_1,u_2,v_1+v_2+h)=1$

The condition $\gcd(u_1,u_2)=u_1$ means that if we let $\bar{D}_1=(a_1,b_1)-O$, then the support of $\bar{D}_2$ has (a_1,b_1) or $-(a_1,b_1)=(a_1,-b_1-h(a_1))$. But from $\gcd(u_1,u_2,v_1+v_2+h)=1$ note that

$v_1(a_1)=v_2(a_1)+h(a_1)$ and $\bar{D}_2$ has the form $(a_1,b_1)+(a_2,b_2)-2O, a_1 \neq a_2$, or $2(a_1,b_1)-2O$.

From the fact $F-l^2-hl \equiv 0 \pmod{u_1u_2}$, we can compute $l(x)=s_0u_2+v_2$ directly. That is,

$$\frac{F-(s_0u_2+v_2)^2-h\cdot(s_0u_2+v_2)}{u_2} \equiv 0 \pmod{u_1}$$

$$\rightarrow \quad \frac{F-v_2^2-hv_2}{u_2}(-u_{10}) = 2s_0v_{10}$$

$$\rightarrow\ s_0=(2v_{10})^{-1}\frac{F-v_2^2-hv_2}{u_2}(-u_{10})$$

The formula for this case is described in the Algorithm 3.

Algorithm 3. Divisor addition of the case (4)

Input: $\bar{D}_1=[u_1,v_1]$, $\bar{D}_2=[u_2,v_2]$

Output: $\bar{D}_1=[u_3,v_3]$ and $l(x)$

Step 1. Check if $\gcd(u_1,u_2,v_1+v_2+h)=1$

If $(h_2u_{10}-v_{21}-h_1)u_{10}+v_{20}+v_{10}+h_0=0$, then goto the case (5) (see Table 2 in Appendix A)

Step 2. Compute $l(x)=s_0u_2+v_2=s_0x^2+l_1x+l_0$

$w_1=f_3-u_{20}-u_{21}(f_4-u_{21})+u_{10}^2$

$w_2=u_{21}(u_{20}+h_2v_{21})-v_{21}^2$

$w_3=-(u_{10}+u_{21})w_1+w_2+f_2+f_4(u_{10}^2-u_{21})-h_1v_{21}-h_2u_{10}$

$s_0=(2v_{10}+h_2u_{10}^2-h_1u_{10}+h_0)^{-1}\cdot w_3$

$l_1=s_0u_{21}+v_{21}$, $l_0=s_0u_{20}+v_{20}$

Step 3. Compute $u_3=\mathrm{monic}\left(\frac{F-l^2-hl}{u_1u_2}\right)$

$u_{31}=-s_0^2-u_{10}+f_4-u_{21}-h_2s_0$

$u_{30}=w_1+u_{10}(s_0^2-f_4+u_{21})-s_0(v_{21}+l_1+h_1-h_2u_{10})-h_2v_2s_1=0$ then goto Step 5'

Step 4. Compute $v_{31}x+v_{30}=-l-h \pmod{u_3}$

$v_{31}=(s_0+h_2)u_{31}-l_1-h_1$, $v_{30}=(s_0+h_2)u_{30}-l_0-h_0$

Cost : 11M, 3S, 1I

3. Addition in the case of $\deg(u_1)=\deg(u_2)=2$, $\gcd(u_1,u_2)=1$

This is the most common case in divisor composition. To optimize the computation, the needed subexpressions have been listed in [4]. We rewrite the expressions to give the formula for $l(x)$ of Lemma 7 in [2]. From $l \equiv v_1 \pmod{u_1} \equiv v_2 \pmod{u_2}$, $s(x)$ for $l(x)=su_2+v_2$ can be computed by

$$s(x)=s_1x+s_0=(v_1-v_2)\cdot u_2^{-1} \pmod{u_1}$$
$$=(v_1-v_2)\cdot r^{-1}\cdot((u_{11}-u_{21})x+u_{11}\cdot(u_{11}-u_{21})+u_{20}-u_{10} \pmod{u_1}$$

where r is the resultant of u_1 and u_2.

With the help of tricks in the section 4.2.1 of [4], we can get an efficient formular for l, u_3, v_3 (see Algorithm 4 for more details).

Algorithm 4. Divisor addition of the case (6)

Input: $\bar{D}_1=[u_1,v_1]$, $\bar{D}_2=[u_2,v_2]$

Output: $\bar{D}_1=[u_3,v_3]$ and $l(x)$.

Step 1. Compute $r=\mathrm{res}(u_1,u_2)$

$z_1=u_{11}-u_{21}, z_2=u_{20}-u_{10}, z_3=u_{11}z_1$

$r=z_2(z_3+z_2)+z_1^2u_{10}$

Step 2. If $r=0$, then goto Algorithm 5(case (7))

Step 3. Compute almost inverse of $u_2 \bmod u_1$

$inv_1=z_1, inv_0=z_3+z_2$

Step 4. Compute $s0=rs \equiv (v_1-v_2)inv \pmod{u_1}$

$w_0=v_{10}-v_{20}, w_1=v_{11}-v_{21}$,

$w_2=inv_0w_0, w_3=inv_1w_1$

$s_10=z_1w_0+z_2w_1, s_00=w_2-u_{10}w_3$

Step 5. Compute $s=s_1x+s_0$ and s_1^{-1}

$w_1=(rs_10)^{-1}, w_2=s_10w_1, w_3=r^2w_1\ (=s_1^{-1})$,

$s_1=s_10w_2, s_0=s_00w_2$

Step 6. Compute $l(x) = s_1x^3 + l_2x^2 + l_1x + l_0$

$l_2 = s_1u_{21} + s_0, l_0 = s_0u_{20} + v_{20}$

$l_1 = (s_1 + s_0)(u_{21} + u_{20}) - s_1u_{21} - s_0u_{20} + v_{21}$

Step 7. Compute $u_3 = \text{monic}(\frac{F - l^2 - hl}{u_1u_2})$

$s_00 = w_3s_0, u_{31} = s_00 - z_1 - w_3^2 + h_2w_3$

$u_{30} = s_0C \cdot (s_00 - 2u_{11}) + z_3 - u_{10} - u_{20} +$
$w_3 \cdot (2l_1 + h_1 - h_2(u_{11} + u_{21})) -$
$w_3 \cdot (f_4 - u_{21} - u_{11} - h_2l_2))$

Step 8. Compute $v_{31}x + v_{30} = -l - h \pmod{u_3}$

$w_1 = u_{31}s_1, w_2 = l_2 + h_2 - w_1, w_3 = u_{30}w_2$

$v_{31} = (u_{31} + u_{30})(w_2 + s_1) - w_3 - w_1 - l_1 - h_1,$

$v_{30} = w_3 - l_0 - h_0$

Cost: 23M, 3S, 1I

Step 5'. Compute $l(x) = s_0x^2 + l_1x + l_0$

$inv = r^{-1}, s_0 = s_00inv,$

$l_1 = s_0u_{21} + v_{21}, l_0 = s_0u_{20} + v_{20}$

Step 6'. Compute $u_3 = \text{monic}(\frac{F - l^2 - hl}{u_1u_2})$

$u_{30} = f_4 - u_{21} - u_{11} - s_0^2 - h_2s_0$

Step 4. Compute $v_{31}x + v_{30} = -l - h \pmod{u_3}$

$v_{30} = u_{30}(l_1 + h_1 - u_{30}(s_0 + h_2)) - l_0 - h_0$

Cost: 13M, 3S, 1I

4. Addition in the case of $\deg(u_1)=\deg(u_2)=2$, $\gcd(u_1,u_2)=x-a_1$, $\gcd(u_1,u_2,v_1+v_2+h)=1$

As the case (4), we can check whether $\gcd(u_1, u_2, v_1 + v_2 + h) = 1$ by checking $v_1(a_1) = v_2(a_1)$. This case occur when the support of $\bar{D}_1$ and the support of $\bar{D}_2$ contains simultaneously (a_1, b_1). If we let $\bar{D}_1 = (a_1, b_1) + (a_2, b_2) - 2O$, then $\bar{D}_2$ has the form of $\bar{D}_2 = (a_1, b_1) + (a_4, b_4) - 2O, a_1 \neq a_4$ or $\bar{D}_2 = 2(a_1, b_1) - 2O$.

If we apply the algorithm in the section 4.1 of [4], $\bar{D}_3$ is computed by the following steps;

Step 1. Compute $\bar{D}0 = 2((a_1, b_1) - O)$

Step 2. Compute $\bar{D}00 = ((a_2, b_2) - O) + \bar{D}0$

Step 3. Compute $\bar{D}_3 = ((a_4, b_4) - O) + \bar{D}00.$

The step 2 and step 3 are the case (3) or (4) according to the form of $\bar{D}_2$. This requires an additional check to determine which case should be applied. We reorder the intermediate additions to remove one additional check.

Algorithm 5. Divisor addition of the case (7)

Input: $\bar{D}_1 = [u_1, v_1]$, $\bar{D}_2 = [u_2, v_2]$

Output: $\bar{D}_3 = [u_3, v_3]$ and $f(x)$ such that

$$\bar{D}_3 + (f) = \bar{D}_1 + \bar{D}_2.$$

Step 1. Check if $\gcd(u_1, u_2, v_1 + v_2 + h) = 1$

$z_1 = u_{11} - u_{21}, z_2 = u_{20} - u_{10}, a_1 = z_2z_1^{-1}$

$b_1 = v_{11}a_1 + v_{10}, b_3 = (h_2a_1 + h_1 + v_{21})a_1 + v_{20} + h_0$

if $b_1 = -b_3$ then goto the case (8)(see Table 2)

Step 2. Case of $\bar{D}_2 = 2(a_1, b_1) - 2O$

if $2a_1 = -u_{21}$, compute $a_2 = -u_{11} - a_1$ and set

$$\bar{D}_10 \leftarrow \bar{D}_2, \bar{D}_20 \leftarrow (a_1, b_1) - O,$$

$$\bar{D}_30 \leftarrow (a_2, v_{11}a_2 + v_{10}) - O$$

Step 3. Case of $\bar{D}_2 = (a_1, b_1) + (a_4, b_4) - 2O$

else compute $a_4 = -u_{21} - a_1$ and set

$$\bar{D}_10 \leftarrow \bar{D}_1, \bar{D}_20 \leftarrow (a_1, b_1) - O,$$

$$\bar{D}_30 \leftarrow (a_4, v_{21}a_4 + v_{20}) - O$$

Step 4. Compute $\bar{D}_3 + (f) = (\bar{D}_10 + \bar{D}_20) + \bar{D}_30$

Compute $\bar{D}_40 + (f_1) = \bar{D}_20 + \bar{D}_10$ using

Algorithm 3.

Compute $\bar{D}_3 + (f_2) = \bar{D}_3 0 + \bar{D}_4 0$ using Algorithm 4 and $f = f_1 f_2$.

IV Explicit formulae for Double in J_H

Let $\bar{D} = [u, v]$ and $\bar{D}0 = [u0, v0] = 2\bar{D} - (f)$.

Table 1 in Appendix A describes a formula for $\bar{D}0 = [u0, v0]$ and f for all cases. Doubling for the most common case, $\gcd(u, 2v+h) = 1$, is explained in Algorithm 6.

Algorithm 6. Doubling for the most case.

Input: $\bar{D} = [u, v]$, $u = x^2 + u_1 x + u_0$, $v = v_1 x + v_0$

Output: $\bar{D}0 = [u0, v0]$ and $l(x)$.

Step 1. Compute $v \equiv h + 2v \pmod{u} = v_1 x + v_0$

$v_1 = h_1 + 2v_1 - h_2 u_1$, $v_0 = h_0 + 2v_0 - h_2 u_0$

Step 2. Compute $r = \mathrm{res}(u, v)$

$w_0 = v_1^2$, $w_1 = u_1^2$, $w_2 = v_1^2$, $w_3 = u_1 v_1$

$r = u_0 w_2 + v_0 (v_0 - w_3)$

If r=0, goto the case (4)(see Table 1)

Step 3. Compute $inv0 = r(2v)^{-1} \pmod{u}$

$inv_1 0 = -v_1$, $inv_0 0 = v_0 - w_3$

Step 4. Compute $k_1 0 = \dfrac{F - v^2 - hv}{u} \pmod{u}$

$k_1 0 = 2(w_1 - f_4 u_1) + w_3 - w_4 - v_1 h_2$

$k_0 0 = u_1 (2w_4 - w_3 + f_4 u_1 + h_2 v_1) + f_2 - w_0 - 2f_4 u_0 - v_1 h_1 - v_0 h_2$

Step 5. Compute $s0 = k0 \cdot inv0 \pmod{u}$

$w_0 = k_0 0 inv_0 0$, $w_1 = k_1 0 inv_1 0$

$s_1 0 = v_{10} k_1 0 - v_{11} k_0 0$, $s_0 0 = w_0 - u_0 w_1$

If $s_1 0 = 0$ then goto step 6′.

Step 6. Compute $s = s_1 x + s_0$ and s_1^{-1}

$w_1 = (rs_1 0)^{-1}$, $w_2 = s_1 0 w_1$, $w_3 = r^2 w_1 (= s_1^{-1})$,

$s_1 = s_1 0 w_2$, $s_0 = s_0 0 w_2$

Step 7. Compute $l(x) = s_1 x^3 + l_2 x^2 + l_1 x + l_0$

$l_2 = s_1 u_1 + s_0$, $l_0 = s_0 u_0 + v_0$

$l_1 = (s_1 + s_0)(u_1 + u_0) - s_1 u_1 - s_0 u_0 + v_1$

Step 8. Compute

$$x^2 + u_1 0 x + u_0 0 = \mathrm{monic}\left(\frac{F - l^2 - hl}{u^2}\right)$$

$u_0 0 = w_3 \cdot (2v_1 + h_1 - h_2 u_1 + w_3 \cdot (2u_1 - f_4 + h_2 s_0 + s_0^2)$

$u_1 0 = w_3 \cdot (2s_0 + h_2 - w_3)$

Step 9. Compute $v_1 0 x + v_0 0 = -l - h \pmod{u0}$

$w_1 = u_{31} s_1$, $w_2 = l_2 + h_2 - w_1$, $w_3 = u_{30} w_2$

$v_{31} = (u_{31} + u_{30})(w_2 + s_1) - w_3 - w_1 - l_1 - h_1$,

$v_{30} = w_3 - l_0 - h_0$

Cost: 23M, 5S, 1I

Step 6′. Compute $l(x) = s_0 x^2 + l_1 x + l_0$

$inv = r^{-1}$, $s_0 = s_0 0 inv$,

$l_1 = s_0 u_1 + v_1$, $l_0 = s_0 u_0 + v_0$

Step 7′. Compute $u0 = \mathrm{monic}\left(\dfrac{F - l^2 - hl}{u^2}\right)$

$u_0 0 = f_4 - 2u_1 - s_0^2 - h_2 s_0$

Step 4. Compute $v_0 0 = -l - h \pmod{u0}$

$v_0 0 = u_0 0 (l_1 + h_1 - u_0 0 (s_0 + h_2)) - l_0 - h_0$

Cost: 14M, 4S, 1I

V. Conclusion

We give explicit formulae for composition of genus two. The previous work described in [4] only contains the formulae for the most common cases. In this paper, we give explicit formulae for all cases according to input divisors. Furthermore, the formulae includes the

form of rational functions related to the implementation of the Tate pairing.

Reference

[1] D. Cantor, "Computing in the Jacobian of a Hyperelliptic Curves", *Math. Comp*, vol. 48, no.177, pp.95-101, 1987.

[2] Y. Choie and E. Lee, "Implementation of Tate Pairing of hyperelliptic curves of genus 2", appear in Proceeding of *ICISC 2003*.

[3] N. Koblitz, "Algebraic aspects of cryptography", *Springer-Verlag*, 1998.

[4] T. Lange, "Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae", Cryptology eprint Archives, http://eprint.iacr.org, Number 2002/121, 2002.

[5] J. Pelzl, T. Wollinger, J. Guajardo and C. Paar, "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves", Cryptology eprint Archives http://eprint.iacr.org, Number 2003/026, 2003.

[6] J. Pelzl, T. Wollinger and C. Paar, "Low Cost Secyrity: Explicit Formulae for Genus 4 Hyperelliptic Curves Cryptology" eprint Archives http://eprint.iacr.org, Number 2003/097, 2003.

Appendix A. Tables

Tab;e 1. Doubling in divisor class group ($\bar{D}0 + (f) = 2\bar{D}$)

$\bar{D} = [u, v]$	$\gcd(u, 2v+h)$	$\bar{D}0 = [u0\ v0]$	f
$u = x + u_0$	1	$v_1 0 = \frac{F0(-u_0) - v_0 h0(-u_0)}{2v_0 + h(-u_0)}$ $u_1 0 = 2u_0,\ u_0 0 = u_0^2$ $v_0 0 = v_0 + u_0 v_1 0$	1
	u	identity	u
$u = x^2 + u_1 x + u_0$	1(i.e. $\mathrm{res}(u, 2v+h) \neq 0$)	See Algorithm 6 (section IV)	$\frac{y - l}{u0}$
	$x - a_1$	$a_2 = -u_1 + v_0 v_1^{-1}$ $b_2 = v_0 + v_1 x_2$ $\bar{D}0 = 2\ ((a_2, b_2) - O)$	$x - a_1$
	u	identity	u

Tab;e 2. Addition in divisor class group (assume $\bar{D}_1 \neq \bar{D}_2$)

$\bar{D}_{1+}, u_1, u_2$	case#	$\bar{D}_{2+}$	$\gcd(u_1, u_2)$ / $\gcd(u_1, u_2, v_1+v_2+h)$	$\bar{D}_3 = [u_3, v_3]$	f
(a_1, b_1) $x+u_{10}$ $x+u_{20}$	(1)	(a_2, b_2)	1(i.e. $u_1 \neq u_2$) / 1	$u_3 = u_1 u_2$ $v_3 = \frac{v_{20}-v_{10}}{u_{10}-u_{20}}(x+u_{10})+v_{10}$	1
	(2)	$(a_1, -b_1-h(a_1))$	$u_1 = u_2$ / $u_1 = u_2$	identity	u_1
(a_1, b_1) $x+u_{10}$ $x^2+u_{21}x+u_{20}$	(3)	$(a_3, b_3)+(a_4, b_4)$	1(i.e. $\mathrm{res}(u_1, u_2) \neq 0$) / 1	See Algorithm 2 (section III.1)	$\frac{y-l}{u_3}$
	(4)	$(a_1, b_1)+(a_4, b_4)$	$u_1 = x-a_1$ / 1	See Algorithm 3 (section III.2)	$\frac{y-l}{u_3}$
	(5)	$(a_1, -b_1-h(a_1))$ $+(a_4, b_4)$	$u_1 = x-a_1$ / $u_1 = x-a_1$	$u_3 = x+u_{21}-u_{10}$ $v_3 = v_{21} \cdot (u_{10}-u_{21})+v_{20}$	u_1
$(a_1, b_1)+(a_2, b_2)$ $x^2+u_{11}x+u_{10}$ $x^2+u_{21}x+u_{20}$	(6)	$(a_3, b_3)+(a_4, b_4)$	1(i.e. $\mathrm{res}(u_1, u_2) \neq 0$) / 1	See Algorithm 4 (section III.3)	$\frac{y-l}{u_3}$
	(7)	$(a_1, b_1)+(a_4, b_4)$	$u_1 = x-a_1$ / 1	See Algorithm 5 (section III.4)	$\frac{y-l}{u_3}$
	(8)	$(a_1, -b_1-h(a_1))$ $+(a_4, b_4)$	$x-a_1$ / $x-a_1$	$w = (u_{11}-u_{21})^{-1}$, $a_1 = (u_{20}-u_{10})w$ $u_{31} = u_{11}+u_{21}+2a_1$ $u_{30} = (u_{11}+a_1)(u_{21}+a_1)$ $b_2 = v_{11}(-u_{11}-a_1)+v_{10}$ $b_4 = v_{21}(-u_{21}-a_1)+v_{20}$ $v_{31} = (b_2-b_4)w$ $v_{30} = b_2+v_{31}(u_1+a_1)$	$x-a_1$
	(9)	$(a_1, -b_1-h(a_1))$ $+(a_2, -b_2-h(a_2))$	u_1 / u_1	identity	u_1
	(10)	$(a_1, -b_1-h(a_1))$ $+(a_2, b_2)$	u_1 / $x-a_1$	$\bar{D}_3 = 2((a_1, b_1)-O)$	$x-a_1$