3-3　種数２の超楕円曲線に対するHarley加算アルゴリズムの一般型

3-3 A Generalized Harley Algorithm for Genus Two Hyperelliptic Curves

杉崎大樹　松尾和人　趙　晋輝　辻井重男
SUGIZAKI Hiroki, MATSUO Kazuto, CHAO Jinhui, and TSUJII Shigeo

要旨

最近、Harleyによって奇標数の有限体上の種数2の超楕円曲線に対する高速加算アルゴリズム（Harleyアルゴリズム）が提案され、また、著者らやLangeが独立に標数2の有限体上の種数2の超楕円曲線に対するHarleyアルゴリズムを示した。本論文では、定義体の標数に依存しない、種数2の超楕円曲線に対するHarleyアルゴリズムを示す。提案アルゴリズムによって、任意標数の有限体F_q上の種数2の超楕円曲線の因子類の加算をI+26M、2倍算をI+31Mのコストで実現可能である。ここで、I及びMは、F_q上の逆元計算及び乗算の演算コストを表す。

A fast addition algorithm for divisor classes of genus two hyperelliptic curves over finite fields of odd characteristics was proposed by Harley in 2000 and a lot of improvements of the algorithm has been proposed,besides extensions of the algorithm for the curves over finite fields of characteristic two have been proposed by the authors and Lange independently. However, any Harley algorithm over arbitrary characteristic fields have not been known until now. This paper shows a generalization of the Harley algorithm to genus two hyper elliptic curves over finite fields of arbitrary characteristics. The proposed algorithm takes I+26M,I+31M for an addition and a doubling respectively, where I and M denote the cost for an inversion and a multiplication over the definition field respectively.

[キーワード]
超楕円曲線暗号，超楕円曲線，加算アルゴリズム，Cantorアルゴリズム，Harleyアルゴリズム
Hyperelliptic curve cryptosystems, Hyperelliptic curves, Addition algorithm, Cantor algorithm, Harley algorithm

1　まえがき

インターネット等の不特定多数ディジタル通信を利用して電子商取引等を安全に行うためには、秘密通信、個人のプライバシーの保護、個人認証等の情報セキュリティ技術が不可欠である。中でも公開鍵暗号アルゴリズムは、このような安全な情報通信サービスを提供する基盤技術として必須のものであり、電子決済、電子政府、電子医療など、社会、生活全般にわたるインフラストラクチャの核となる技術である。

現在のところ最も優れた公開鍵暗号は楕円曲線暗号であるが、これに用いる楕円曲線自体は代数曲線の中の小さなクラスの一つに過ぎない。そこで、最近では、より効率的な公開鍵暗号の構成を目指して、より一般的な代数曲線のクラスである超楕円曲線上の離散対数問題を用いた暗号アルゴリズムの研究も盛んに行われるようになってきた。

楕円曲線や超楕円曲線上の離散対数問題に基づく暗号系の構成には高速群演算（加算）アルゴリズムが必要不可欠である。楕円曲線に対しては、多くの実用的なアルゴリズムが得られているが、超楕円曲線に対しては有効なアルゴリズ

ムが知られてこなかった。近年 Cantor[1]によって提案された超楕円曲線の因子類の高速な加算法(Cantor アルゴリズム)により超楕円曲線を用いた実用的な暗号系が構成可能となったものの、Cantor アルゴリズムを用いた超楕円曲線暗号は、楕円曲線暗号と比較し数倍以上低速であることが知られていた。

2000 年に Harley[2][3]により Cantor アルゴリズムとは異なる手法を用いた種数 2 の超楕円曲線上の高速加算法(Harley アルゴリズム)が提案された。Harley アルゴリズムは、Cantor アルゴリズムと異なり、奇標数の定義体上の種数 2 の超楕円曲線に限定したアルゴリズムである。また、Cantor アルゴリズム同様、入出力因子類の表現に Mumford 表現を利用しているが、Cantor アルゴリズムにおける多項式の 2 次型式計算の代わりに、楕円曲線における chord-tangent law 的な手法を用いて加算を行うものである。さらに計算過程において中国人剰余定理、Newton 反復を用いて計算を行うほか、多項式乗算に Karatsuba 乗算を利用し、Cantor アルゴリズムと比較し高速なアルゴリズムを得ている。その結果、Harley アルゴリズムを用いた超楕円曲線暗号が楕円曲線暗号と理論上同等の速度を達成し得ることが示され[4]、その後、Harley アルゴリズムに関し多くの研究がなされてきた[1]。特に[8][9]は、Harley アルゴリズムの標数 2 の定義体上の超楕円曲線に対する拡張アルゴリズムを示した。このように、これまで Harley アルゴリズムの研究は、定義体が奇標数のときと標数 2 のときのそれぞれについて個別に行われてきた。しかし、標数に依存しない有限体上の超楕円曲線に対する統一的アルゴリズムを示すことは、研究の更なる発展を目指し、加算アルゴリズムに関する理解を深め上で重要な課題である。また、数式処理ソフトウェアへの実装等で現実的に有用であると考えられる。

そこで、本論文では定義体の標数に依存しない Harley アルゴリズムを示す。提案アルゴリズムによって、任意標数の有限体 F_q 上の種数 2 の超楕円曲線の因子類の加算を $I+26M$、2 倍算を $I+31M$ のコストで実現可能である。ここで、I 及び M は、F_q 上の逆元計算及び乗算の演算コストを表す。

1 Harley アルゴリズムに関する最新の研究動向については[5]－[7]などを参照されたい。

2 準備

2.1 超楕円曲線

F_q を q 個の元からなる有限体とする。F_q 上の種数 2 の超楕円曲線 C を下式で定義する。

$$\begin{aligned} C \ : \ & Y^2+H(X)Y=F(X), \\ & H(X)=X^2+h_1X+h_0, \\ & F(X)=X^5+f_4X^4+\cdots+f_1X+f_0. \end{aligned} \tag{1}$$

条件

$$(x,y)\in\overline{\mathbf{F}}_q{}^2 \text{ such that } y^2+H(x)y+F(x)=0$$

を満足する組 $(x,\ y)$ と唯一の無限遠点 P_∞ とを併せて C 上の点と呼ぶ。曲線 C 上の点 $P=(x,\ y)\neq P_\infty$ に対し $(x,\ -y-H(x))$ もまた C 上の点である。ここではこの点を $-P$ と書く。また、$-P_\infty=P_\infty$ とする。$P=-P$ を満足する P を分岐点と呼ぶ。P_∞ 以外の分岐点 $P=(x,\ y)$ に対して、

$$2y+H(x)=0 \tag{2}$$

が成り立つ。また、C 上の分岐点は(2)を満足する C 上の点 $(x,\ y)$ と P_∞ で尽くされる。

2.2 超楕円曲線上の因子と Jacobi 多様体

C 上の因子 D を以下の C 上の点 P_i の整係数の有限形式和で定義する。

$$D=\sum_{P_i\in C} n_iP_i,\ n_i\in\mathbf{Z}. \tag{3}$$

C の因子全体 $\mathbf{D}$ は明らかに可換群をなす。

式(3)で与えられた因子 D の次数を

$$\deg D=\sum_i n_i$$

と定義する。次数 0 の因子全体の集合 $\mathbf{D}^0$ は $\mathbf{D}$ の部分群をなす。

C の有理関数 f の因子 (f) を

$$(f)=\sum m_{P_i}P_i-\sum m_{Q_j}Q_j$$

で定義する。ただし、P_i は C 上 f の重複度 m_{P_i} の零点、Q_j は重複度 m_{Q_j} の極である。f の因子 (f) を主因子という。主因子全体の集合を $\mathbf{D}^l$ で

表す。$\mathbf{D}^1$は$\mathbf{D}^0$の部分群となることが知られている。

CのJacobi多様体を$\mathbf{J}_C$を下式で定義する。

$$\mathbf{J}_C = \mathbf{D}^0/\mathbf{D}^1.$$

$\mathbf{J}_C$の因子類でq乗Frobenius写像により固定される因子類の集合を$\mathbf{J}_C(\mathbf{F}_q)$と書く。$\mathbf{J}_C(\mathbf{F}_q)$は有限可換群であり、離散対数問題が定義可能なため、その上で暗号系が構成可能である。この暗号系を超楕円曲線暗号という。高速な超楕円曲線暗号の構成には$\mathbf{J}_C(\mathbf{F}_q)$の因子類の高速加算アルゴリズムが必要である。そこで、本論文では$\mathbf{J}_C(\mathbf{F}_q)$の因子類の加算を考える。

2.3 因子類とその表現

$D_1, D_2 \in \mathbf{D}^0$に対して、$D_1 - D_2 \in \mathbf{D}^1$であるとき$D_1$と$D_2$が線形同値であるといい、$D_1 \sim D_2$と書く。

$\mathbf{J}_C$の任意の因子類を以下の形式の因子で表現可能である。

$$D = \sum_i m_i P_i - \left(\sum_i m_i\right) P_\infty,\ m_i \geq 0.$$

ただし、$i \neq j$に対し$P_i \neq -P_j$とする。

式(4)の形式の因子を半被約因子(semi-reduced divisor)と呼び、特に$\sum_i m_i \leq g$を満足する半被約因子を被約因子(reduced divisor)と呼ぶ。被約因子により$\mathbf{J}_C$の因子類を一意に表現可能である。

多項式$U, V \in \overline{\mathbf{F}}_q[X]$を用いて(4)の形式で与えられた半被約因子$D$を

$$D = (U, V) \tag{5}$$

と表現可能である。ここで$P_i = (x_i, y_i)$としたとき、

$$U = \prod (X - x_i)^{m_i} \tag{6}$$

であり、Vは

$$\begin{aligned} F - HV - V^2 &\equiv 0 \bmod U, \\ \deg V &< \deg U, \\ y_i &= V(x_i) \end{aligned} \tag{7}$$

を満足する唯一の多項式である。この半被約因子の表現をMumford表現と呼ぶ。

$D=(U, V)$に対し、$U, V \in \mathbf{F}_q[X]$と$\mathrm{D} \in \mathbf{J}_C(\mathbf{F}_q)$は同値である。したがって、以降では$U, V \in \mathbf{F}_q[X]$とする。

$\mathbf{J}_C(\mathbf{F}_q)$の因子類$D$がMumford表現によって表されると、その逆元$-D$が容易に決定される。すなわち、$\deg U=2$の$D=(U, V)$に対し、

$$-D = (U, U - V - H) \tag{8}$$

であり、特に分岐点P_r, P'_rに対して$D=P_r+P'_r-2P_\infty$のとき、

$$-D = D$$

となる。また、$\deg U=1$の$D=(X+u_0, v_0)$に対し、

$$-D = (X + u_0, -v_0 - H(u_0))$$

である。

3 Harleyアルゴリズムの一般化

本節では、(1)で与えられた$\mathbf{F}_q$上の種数2の超楕円曲線に対するHarleyアルゴリズムを提案する。提案アルゴリズムは、奇標数の定義体上のHarleyアルゴリズムと同様、加算と2倍算に異なる手順を用い、入出力には被約因子を用いる。

本節の構成は、まず**3.1**で入力因子の分類について述べ、**3.2**で加算アルゴリズムの詳細を、**3.3**で2倍算アルゴリズムの詳細を述べる。

以下では、英小文字で$\mathbf{F}_q$の元、英大文字で$\mathbf{F}_q$上のXの多項式を表す。

3.1 入力因子の分類

ここでは、提案アルゴリズムの加算及び2倍算の入力因子の条件とその分類の方法を示す。

被約因子$D_1=(U_1, V_1)$, $D_2=(U_2, V_2)$の加算$D_3=(U_3, V_3)=D_1+D_2$では、暗号利用可能な十分に大きなサイズ(例えば80bit)の$\mathbf{F}_q$に対し、ほとんどの場合

$$\begin{aligned} &\deg U_1 = \deg U_2 = \deg U_3 = 2, \\ &\gcd(U_1, U_2) = 1 \end{aligned}$$

が成り立つ。そこで、まずこの条件を満足するか否かで入力因子を分類する。実際には、まずU_1とU_2の次数により入力因子の分類を行い、次にU_1とU_2の判別式を計算し

$$\mathrm{res}(U_1, U_2) \neq 0 \Leftrightarrow \gcd(U_1, U_2) = 1 \qquad (9)$$

により分類する。**3.2** では、入出力因子が上記条件を満足する場合の計算手順を示す。

被約因子 $D_1=(U_1,\ V_1)$ の 2 倍算 $D_2=(U_2,\ V_2)=2D_1$ では、暗号利用可能な十分に大きなサイズの $\mathbf{F}_q$ に対し、ほとんどの場合

$$\deg U_1 = \deg U_2 = 2,$$
$$\gcd(U_1, 2V_1 + H) = 1$$

が成り立つ。そこで、加算と同様に、まずこの条件を満足するか否かで入力因子を分類する。実際も加算と同様に、まず U_1の次数により入力因子の分類を行い、次に U_1と $2V_1+H$ の判別式を計算し

$$\mathrm{res}(U_1, 2V_1 + H) \neq 0 \Leftrightarrow \gcd(U_1, 2V_1 + H) = 1 \qquad (10)$$

により分類する。**3.3** では、入出力因子が上記条件を満足する場合の計算手順を示す。

加算、2 倍算の入力因子が上記の条件を満足しない場合には、**3.2**、**3.3** で示す計算手順を適用することができない。これらの場合には、更に詳細な分類を行い、それぞれについて個別の計算手順を用意する必要がある。実際には、加算の分類手順は[3]と同一となり、2 倍算の分類手順は[8]と同一となる。また、計算手順は、加算は[3]、2 倍算は[8]に示された手順を **3.2**、**3.3** に従って変更することで容易に得られる。

3.2 加算アルゴリズム

ここでは、$\deg U_1=\deg U_2=2$ かつ $\gcd(U_1, U_2)=1$ を満足する被約因子 $D_1=(U_1,\ V_1)$と $D_2=(U_2,\ V_2)$ の加算 $D_3=D_1+D_2=(U_3,\ V_3)$ の計算手順を示す。

奇標数の定義体上の Harley アルゴリズムと同様、標数を限定しない $\mathbf{F}_q$ 上の種数 2 の超楕円曲線に対する Harley アルゴリズムも合成部と還元部からなる。

まず、合成部で D_1と D_2 を合成する。具体的には、$-D_3$ と線形同値かつ

$$U = U_1 U_2$$

である半被約因子 $D=(U,\ V)$ を計算する。V は

$$V \equiv V_1 \bmod U_1,$$
$$V \equiv V_2 \bmod U_2$$

から、中国人剰余定理を用いて

$$V = SU_1 + V_1,$$
$$S \equiv (V_2 - V_1)U_1^{-1} \bmod U_2,\ \deg S \leq 1 \qquad (11)$$

と計算される。

次に、還元部では、まず D'_3〜D である被約因子 $D'_3=(U'_3,\ V'_3)$ を計算する。U'_3は C と V の(重複を含んだ)6 個の交点のうち Uの根となっていない 2 点の X 座標を根とする 2 次多項式である。具体的には、[4][10]に示された手順を用いて、

$$U'_3 = s_1^{-2}\frac{F - HV - V^2}{U} \qquad (12)$$

と計算される(暗号利用可能な十分に大きなサイズの $\mathbf{F}_q$ に対し $s_1=0$ となることはまれであるが、この場合には別のアルゴリズムが必要となる。これは[8]に示された手順の簡単な修正で得られるので、ここでは省略する。この場合出力因子 $D_3=(U_3,\ V_3)$ は $\deg U_3=1$ を満足する。)。

V'_3は U'_3に対して(7)を満足する唯一の多項式である。具体的には、

$$V'_3 \equiv V \bmod U'_3$$

と(11)から

$$V'_3 = S(U'_3 - U_1) - s_1(u'_{31} - u_{11})U'_3 + V_1$$

と計算される。

そして最後に、(8)より加算の出力因子

$$D_3 = (U_3, V_3) = (U'_3, U'_3 - V'_3 - H)$$

を得る。

詳細計算では、[4][8][10]に従い、定義体上の演算の最適化を行った。具体的には、(11)を計算せず(12)に代入し、そこで得た多項式の係数を効率的にまとめて演算数の削減を行った。また、Karatsuba 乗算を用いることにより定義体上の乗算を削減した。さらに、[8][10]と同様に Montgomery 同時逆元計算を用いた。これにより、アルゴリズム中で計算される 2 回の逆元演算を 4 回の乗算と 1 回の逆元計算に変換し、逆元計算回数を削減した。

結果として、$D_3=D_1+D_2$ を $I+26M$ の演算コストで計算可能なアルゴリズムを得た。

ここで述べた加算アルゴリズムの詳細及び各 step の計算コストを表1に示す。

3.3 2倍算アルゴリズム

ここでは、$\deg U_1=2$ かつ $\gcd(U_1, 2V_1+H)=1$ を満足する被約因子 $D_1=(U_1, V_1)$ の2倍算 $D_2=(U_2, V_2)=2D_1$ の計算手順を示す。

2倍算アルゴリズムも加算アルゴリズムと同様に合成部と還元部からなる。

まず、合成部で $-D_2$ と同値かつ

$$U = U_1^2$$

である半被約因子 $D=(U, V)$ を計算する。V は

$$V \equiv V_1 \bmod U_1$$

から、Newton 反復を用いて

$$\begin{aligned} V &= SU_1 + V_1, \\ S &\equiv \frac{F - HV_1 - V_1^2}{U_1}(2V_1 + H)^{-1} \bmod U_2,\ \deg S \le 1 \end{aligned}$$

と計算される。

次に還元部では、加算と同一の手順により、D から出力因子 $D_2=(U_2, V_2)$ を

$$\begin{aligned} U_2 &= s_1^{-2}\frac{F - HV - V^2}{U}, \\ V_2 &= U_2(h_2 - s_1(u_{21} - u_{11})) - S(U_2 - U_1) - V_1 - H \end{aligned}$$

と得る。

実際の計算過程でも加算と同様[4][8][10]で示された方法を用いて定義体上の演算の削減を行った。

結果として、$D_2=2D_1$ を $I+31M$ の演算コストで計算可能なアルゴリズムを得た。

ここで述べた2倍算アルゴリズムの詳細及び各 step の計算コストを表2に示す。

4 むすび

本論文では、研究の更なる発展を目指し、超楕円曲線上の加算アルゴリズムに関する理解を深める目的で、標数に依存しない有限体 $\mathbf{F}_q$ 上の超楕円曲線に対し Harley アルゴリズムを拡張した。提案アルゴリズムは $\mathbf{F}_q$ 上の種数2の超楕円曲線の因子類の加算を $I+26M$ のコスト、2倍算を $I+31M$ のコストで実現可能であり、数式処理ソフトウェア上等への実装に十分な効率を持つ。

表1 加算アルゴリズム

Input	A genus 2 hyperelliptic curve $C: Y^2+H(X)Y=F(X)$, Reduced divisors $D_1=(U_1,V_1)$ and $D_2=(U_2,V_2)$ such that $\gcd(U_1,U_2)=1$ and $\deg U_1=\deg U_2=2$	
Output	The reduced divisor $D_3=(U_3,V_3)=D_1+D_2$ such that $\deg D_3=2$	
Step	**Procedure**	**Cost**
1	Compute the resultant r of U_1 and U_2. $w_4 \leftarrow u_{10}-u_{20}$; $i_1 \leftarrow u_{11}-u_{21}$; $i_0 \leftarrow u_{21}i_1-w_4$; $r \leftarrow u_{20}i_1^2-w_4i_0$;	$4M$
2	If $r=0$ then call the other procedure.	—
3	Compute $I=i_1X+i_0 \equiv r(U_1)^{-1} \bmod U_2$.	—
4	Compute $T=t_1X+t_0 \equiv I(V_2-V_1) \bmod U_2$. $w_0 \leftarrow v_{20}-v_{10}$; $w_1 \leftarrow v_{21}-v_{11}$; $t_2 \leftarrow w_1i_1$; $t_0 \leftarrow w_0i_0$; $t_1 \leftarrow (w_0+w_1)(i_1+i_0)-t_0-t_2(u_{21}+1)$; $t_0 \leftarrow t_0-t_2u_{20}$;	$5M$
5	If $t_1=0$ then call the other procedure.	—
6	Compute $S=s_1X+s_0$. $w_0 \leftarrow (rt_1)^{-1}$; $w_1 \leftarrow w_0r$; $w_2 \leftarrow w_0t_1$; $w_3 \leftarrow w_1r$; $s_1 \leftarrow w_2t_1$; $s_0 \leftarrow w_2t_0$;	$I+6M$
7	Compute $U_3=X^2+u_{31}X+u_{30}=s_1^{-2}((SU_1+V_1)^2+H(SU_1+V_1)-F)/(U_1U_2)$. $w_0 \leftarrow w_3^2$; $w_1 \leftarrow s_0w_3$; $u_{31} \leftarrow i_1-w_0+2w_1+w_3$; $u_{30} \leftarrow (s_0^2+s_0+u_{11}+u_{21}-f_4)w_0-(u_{21}-2v_{11}-h_1)w_3$ $+(2w_1-u_{21})i_1+w_4$	$6M$
8	Compute $V_3=v_{31}X+v_{30}$. $w_1 \leftarrow u_{11}-u_{31}$; $w_0 \leftarrow u_{10}-u_{30}$; $w_2 \leftarrow s_1w_1$; $w_3 \leftarrow s_0w_0$; $w_4 \leftarrow (s_1+s_0)(w_1+w_0)-w_2-w_3$; $v_{31} \leftarrow u_{31}(h_2+w_2)-w_4-v_{11}-h_1$; $v_{30} \leftarrow u_{30}(h_2+w_2)-w_3-v_{10}-h_0$;	$5M$
Total		$I+26M$

表2 2倍算アルゴリズム

Input	A genus 2 hyperelliptic curve $C : Y^2 + H(X)Y = F(X)$, A reduced divisor $D_1 = (U_1, V_1)$ such that $\gcd(U_1, 2V_1 + H) = 1$ and $\deg U_1 = 2$	
Output	The reduced divisor $D_2 = (U_2, V_2) = 2D_1$ such that $\deg U_2 = 2$	
Step	Procedure	Cost
1	Compute the resultant r of U_1 and $2V_1 + H$. $w_0 \leftarrow 2v_{10} + h_0$; $w_1 \leftarrow 2v_{11} + h_1$; $i_1 \leftarrow u_{11} - w_1$; $i_0 \leftarrow u_{11}i_1 - u_{10} + w_0$; $r \leftarrow i_0 w_0 + u_{10}(u_{10} - w_0 - i_1 w_1)$	$4M$
2	If $r = 0$ then call the other procedure.	—
3	Compute $I = i_1 X + i_0 \equiv r(2V_1 + H)^{-1} \bmod U_1$.	—
4	Compute $T = t_1 X + t_0 \equiv I(F - HV_1 - V_1^2)/U_1 \bmod U_1$. $w_0 \leftarrow v_{11}(h_1 + v_{11})$; $w_1 \leftarrow 2u_{10}f_4$; $w_2 \leftarrow u_{11}(6u_{10} + 2v_{11} - 2f_3 + u_{11}(3f_4 - 4u_{11})) + f_2 - v_{10} - w_0 - w_1$; $w_3 \leftarrow u_{11}(3u_{11} - 2f_4) - v_{11} - 2u_{10} + f_3$; $t_1 \leftarrow i_1 w_2 + i_0 w_3$; $w_2 \leftarrow u_{10}w_3$; $w_3 \leftarrow f_2 - w_0 - w_1 - v_{10} + u_{11}(v_{11} - f_3 + 4u_{10} + u_{11}(f_4 - u_{11}))$; $t_0 \leftarrow i_0 w_3 - i_1 w_2$;	$12M$
5	If $t_1 = 0$ then call the other procedure.	—
6	Compute $S = s_1 X + s_0$. $w_0 \leftarrow (rt_1)^{-1}$; $w_1 \leftarrow w_0 r$; $w_2 \leftarrow w_0 t_1$; $w_3 \leftarrow w_1 r$; $s_1 \leftarrow w_2 t_1$; $s_0 \leftarrow w_2 t_0$;	$I + 6M$
7	Compute $U_2 = X^2 + u_{21}X + u_{20} = s_1^{-2}((SU_1 + V_1)^2 + H(SU_1 + V_1) - F)/U_1^2$. $u_{21} \leftarrow w_3(2s_0 + 1 - w_3)$; $u_{20} \leftarrow w_3(w_3(2u_{11} - f_4 + s_0(s_0 + 1)) - u_{11} + 2v_{11} + h_1)$;	$4M$
8	Compute $V_2 = v_{21}X + v_{20}$. $w_1 \leftarrow u_{11} - u_{21}$; $w_0 \leftarrow u_{10} - u_{20}$; $w_2 \leftarrow s_1 w_1$; $w_3 \leftarrow s_0 w_0$; $w_4 \leftarrow (s_1 + s_0)(w_1 + w_0) - w_2 - w_3$; $v_{21} \leftarrow u_{21}(1 + w_2) - w_4 - v_{11} - h_1$; $v_{20} \leftarrow u_{20}(1 + w_2) - w_3 - v_{10} - h_0$;	$5M$
Total		$I + 31M$

参考文献

1 D. G. Cantor, "Computing in the Jacobian of hyperelliptic curve", Math. Comp., Vol.48, No.177, pp.95-101, 1987.

2 P. Gaudry and R. Harley, "Counting points on hyperelliptic curves over finite fields", In W.Bosma, editor, ANTS-IV, No.1838, in Lecture Notes in Computer Science, pp.313-332, Springer-Verlag, 2000.

3 R. Harley. adding. text, doubling. c. http://cristal.inria.fr/~harley/hyper/, 2000.

4 K. Matsuo, J. Chao, and S. Tsujii, "Fast genus two hyperelliptic curve cryptosystems", Technical Report, ISEC2001-31, IEICE, Japan, 2001.

5 松尾和人，有田正剛，趙晋輝，“代数曲線暗号”，日本応用数理学会論文誌，Vol.13，No.2，pp.231-243，2003.

6 松尾和人，有田正剛，趙晋輝，“代数曲線上の公開鍵暗号”，情報処理，Vol.45，No.11，pp.1114-1116，2004.

7 M. Gonda, K. Matsuo, K. Aoki, J. Chao, and S. Tsujii, "Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementation", IEICE Trans., Vol.E88-A, No.1, pp.89-96, 2005.

8 H. Sugizaki, K. Matsuo, J. Chao, and S. Tsujii, "An extension of Harley addition algorithm for hyperelliptic curves over finite fields of characteristic two", Technical Report, ISEC2002-9, IEICE, Japan, 2002.

9 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/

10 宮本洋輔，土井洋，松尾和人，趙晋輝，辻井重男，“種数２の超楕円曲線上の因子類群の高速演算法に関する

考察", In Proc. of SCIS2002, pp.497-502, 2002.

11 H. Sugizaki, K. Matsuo, J. Chao, and S. Tsujii, "A generalized Harley algorithm for genus two hyperelliptic curves", In Proc. of SCIS2003, pp.917-921, 2003.

杉崎大樹（すぎざきひろき）
中央大学大学院理工学研究科情報工学専攻
超楕円曲線暗号

松尾和人（まつおかずと）
情報セキュリティ大学院大学教授、中央大学研究開発機構教授　博士（工学）
代数曲線暗号及び計算機暗号理論

趙　晋輝（CHAO Jinhui）
中央大学大学院理工学研究科情報工学科教授　工学博士
楕円・超楕円曲線暗号

辻井重男（つじいしげお）
情報セキュリティ大学院大学学長、中央大学研究開発機構教授　工学博士
情報セキュリティ、暗号理論