超楕円曲線上のHarley加算アルゴリズムと暗号系への応用

松尾 和人
中央大学

背景

1986: 楕円曲線暗号	Miller, Koblitz
1987: 加算アルゴリズム	Cantor
1989: 超楕円曲線暗号	Koblitz

代数曲線上の暗号系

$C/\mathbb{F}_q$: 代数曲線
$\mathcal{J}_C$: Cの Jacobi 多様体

$\mathcal{J}_C(\mathbb{F}_q)$ 上の離散対数問題:
$\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{J}_C(\mathbb{F}_q) \to m \in \mathbb{Z}$ s.t. $\mathcal{D}_1 = m\mathcal{D}_2$

離散対数問題ベースの暗号を構成可能

研究課題

1. 安全性の検討
   (a) 攻撃
   (b) 安全な曲線の構成

2. 高速化
   (a) 加算アルゴリズム
   (b) 整数倍算アルゴリズム

Cantorアルゴリズムの改良: Sakai-Sakurai-Ishizuka,
Paulus-Stein,
Nagao, ...

1999: Smart@Euro99

"On the Performance of Hyperelliptic Cryptosystems"

<u>主旨</u>

現在のところ,
超楕円曲線暗号は楕円曲線暗号と比較して
利点が認められない.

特に, 暗復号に楕円曲線暗号の数倍以上の時間を要する.

目次

Harleyアルゴリズム

2000: Gaudry-Harley@ANTS-IV

"Counting Points on Hyperelliptic Curves over Finite Fields"

`http://cristal.inria.fr/~harley/hyper/`

Cantor:

・超楕円関数体の整数環のイデアル類群に２次形式の高速composition, reductionアルゴリズムを適用

・Mumford representationの利用

Harley:

・種数を２に限定

・Divisorの詳細な分類

・楕円曲線のchord-tangent law的な加算

cf. 山本芳彦, 数論入門 2 (現代数学への入門)

・Mumford representationの利用

・多項式のCRTとNewton反復を適用

・Karatsuba乗算の適用

加算　: $2I + 27M$

２倍算 : $2I + 30M$

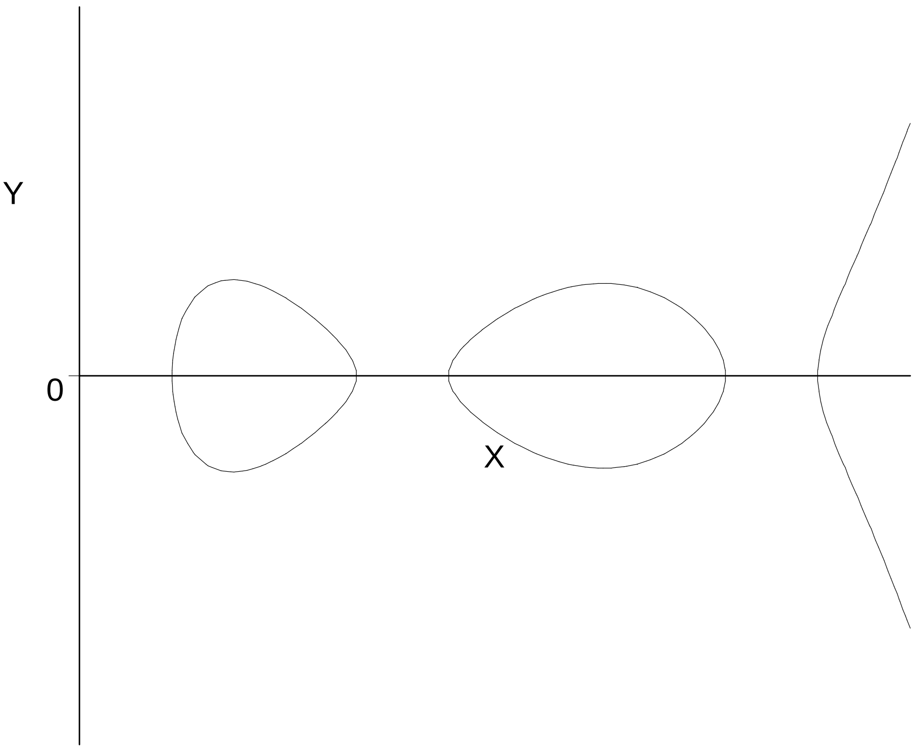
I: 定義体上の逆元計算時間, M: 定義体上の乗算計算時間

種数2の超楕円曲線

$\mathbb{F}_q$: 位数qの有限体

$p := \mathrm{char}\,\mathbb{F}_q \neq 2$

$$\begin{aligned} C/\mathbb{F}_q : & Y^2 = F(X), \\ & F(X) = X^5 + f_4 X^4 + \cdots + f_0, \\ & f_i \in \mathbb{F}_q, \mathrm{disc}\,(F) \neq 0 \end{aligned}$$



入出力

入力　: $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{J}_C(\mathbb{F}_q)$
出力　: $\mathcal{D}_3 = \mathcal{D}_1 + \mathcal{D}_2$

$P_\infty \in C$: 無限遠点
$P_{ij} = (P_{ijX}, P_{ijY}) \in C \backslash \{P_\infty\}$
$-P_{ij} := (P_{ijX}, -P_{ijY})$

Semi-reduced divisor:
$\mathcal{D}_i = \sum n_j P_{ij} - \sum n_j P_\infty$
$P_{ij} \neq -P_{ik \neq j}$

Reduced divisor:
Semi-reduced 且つ $\sum n_j \leq 2$ (genus)

入出力は reduced divisor

$$\begin{aligned} \mathcal{D}_i &= P_{i1} + P_{i2} - 2P_\infty, P_{i1} \neq -P_{i2} \\ \text{または} & \\ \mathcal{D}_i &= P_{i1} - P_\infty \\ \text{または} & \\ \mathcal{D}_i &= 0 \end{aligned}$$

概略フロー

入力 : $\mathcal{D}_1, \mathcal{D}_2 \in \mathcal{J}_C(\mathbb{F}_q)$
出力 : $\mathcal{D}_3 = \mathcal{D}_1 + \mathcal{D}_2$

1. Divisorの分類
   — メインフローで計算できないものを
   別フローに渡す

2. Composition
   — $\mathcal{D}_3$と同値で容易(?)に計算可能な
   semi-reduced divisor $\mathcal{D}$を計算

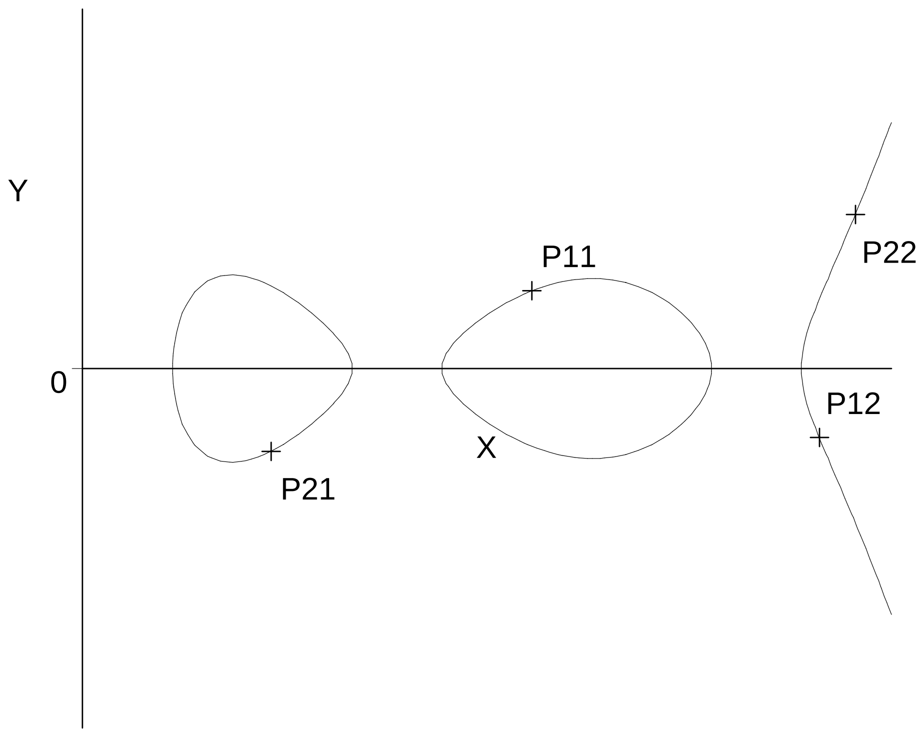
3. Reduction
   — $\mathcal{D} \mapsto \mathcal{D}_3$

加算概略

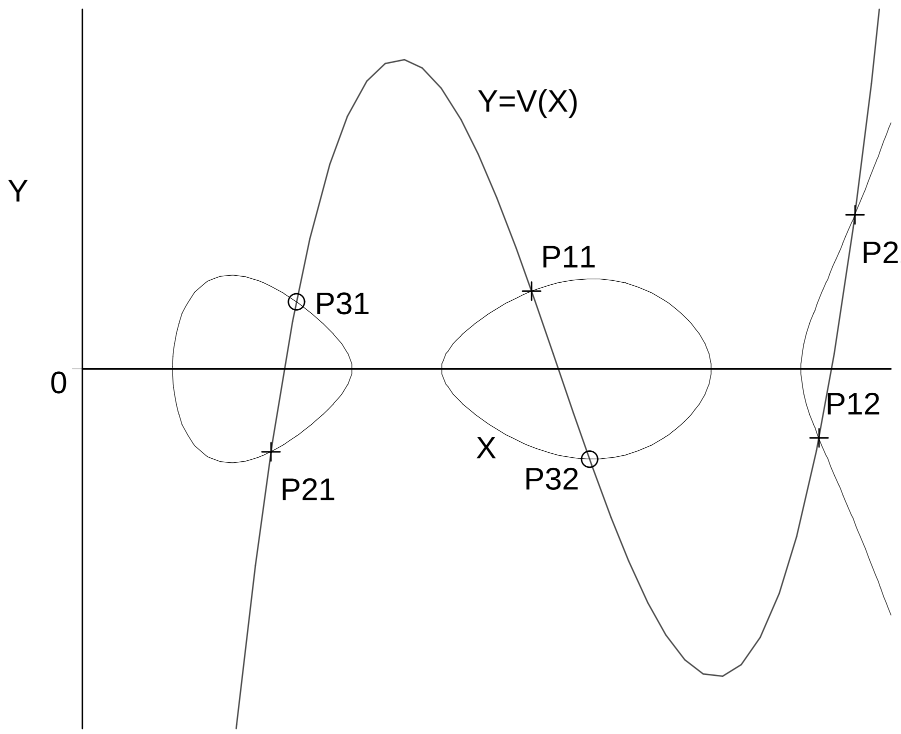
$\mathcal{D}_3 = \mathcal{D}_1 + \mathcal{D}_2$

$$\mathcal{D}_1 = P_{11} + P_{12} - 2P_\infty$$
$$\mathcal{D}_2 = P_{21} + P_{22} - 2P_\infty$$

$$\mathcal{D} = P_{11} + P_{12} + P_{21} + P_{22} - 4P_\infty$$



$$V \in \mathbb{F}_q[X] \text{ such that } \begin{aligned} V(P_{11X}) &= P_{11Y} \\ V(P_{12X}) &= P_{12Y} \\ V(P_{21X}) &= P_{21Y} \\ V(P_{22X}) &= P_{22Y} \end{aligned}$$

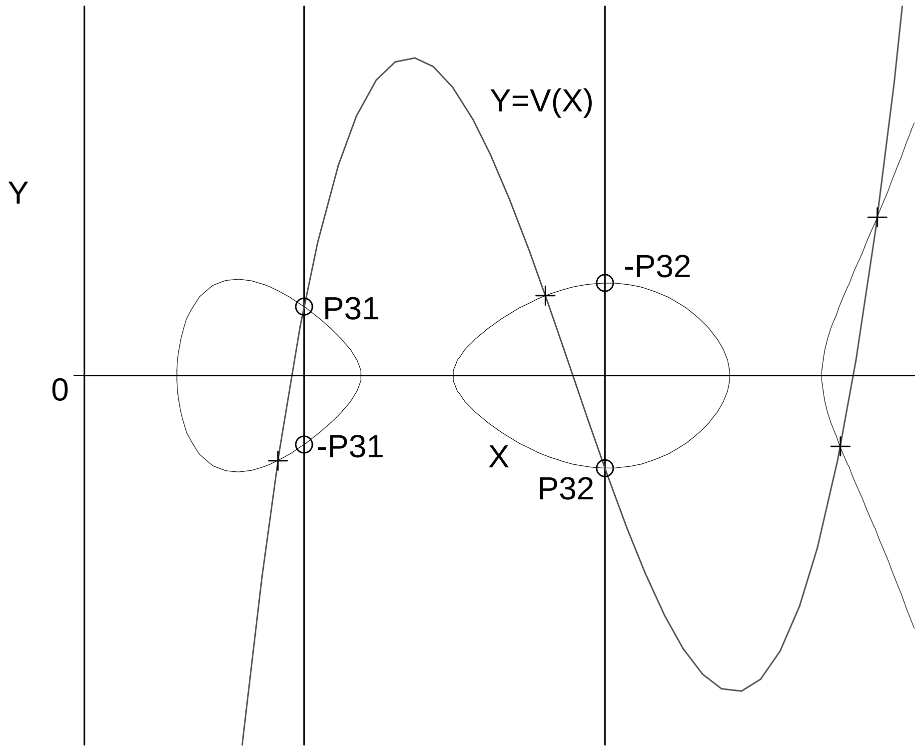


$$P_{11} + P_{12} + P_{21} + P_{22} + P_{31} + P_{32} - 6P_\infty = 0$$

$$\mathcal{D}_1 + \mathcal{D}_2 + P_{31} + P_{32} - 2P_\infty = 0$$

$$\mathcal{D}_3 = -(P_{31} + P_{32} - 2P_\infty)$$

$$\mathcal{D}_1 + \mathcal{D}_2 = \mathcal{D}_3$$



Mumford representation

$\mathcal{D} = (U, V)$,
$U, V \in \mathbb{F}_q[X], \deg V < \deg U$

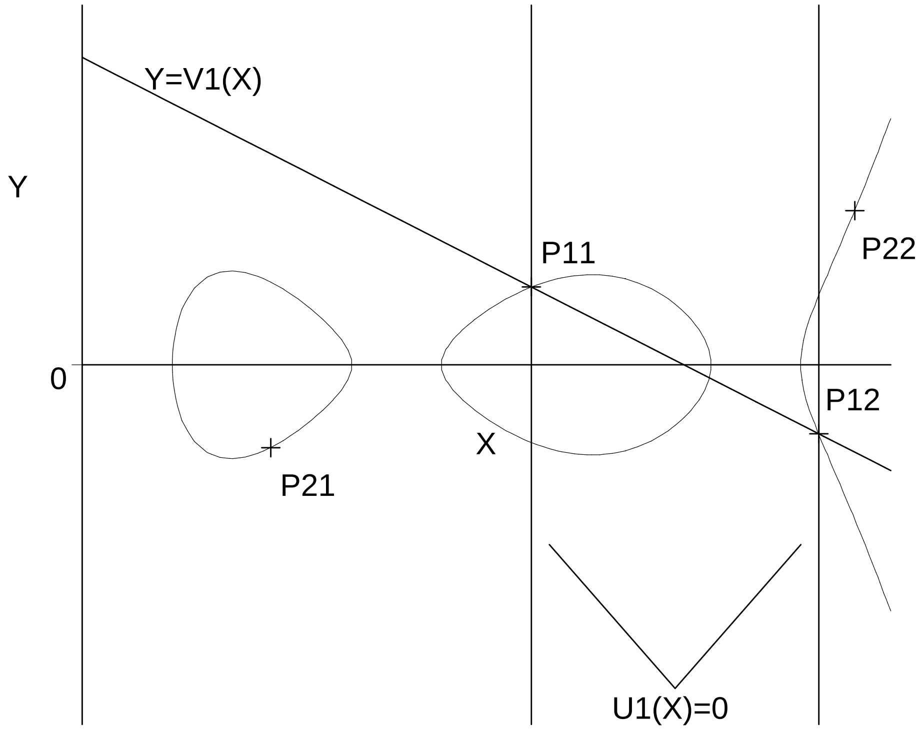
$$\mathcal{D}_1 = P_{11} + P_{12} - 2P_\infty = (U_1, V_1)$$

$$U_1 = (X - P_{11X})(X - P_{12X})$$

$$V_1(P_{11X}) = P_{11Y}, V_1(P_{12X}) = P_{12Y}$$

$$F - V_1^2 \equiv 0 \bmod U_1$$

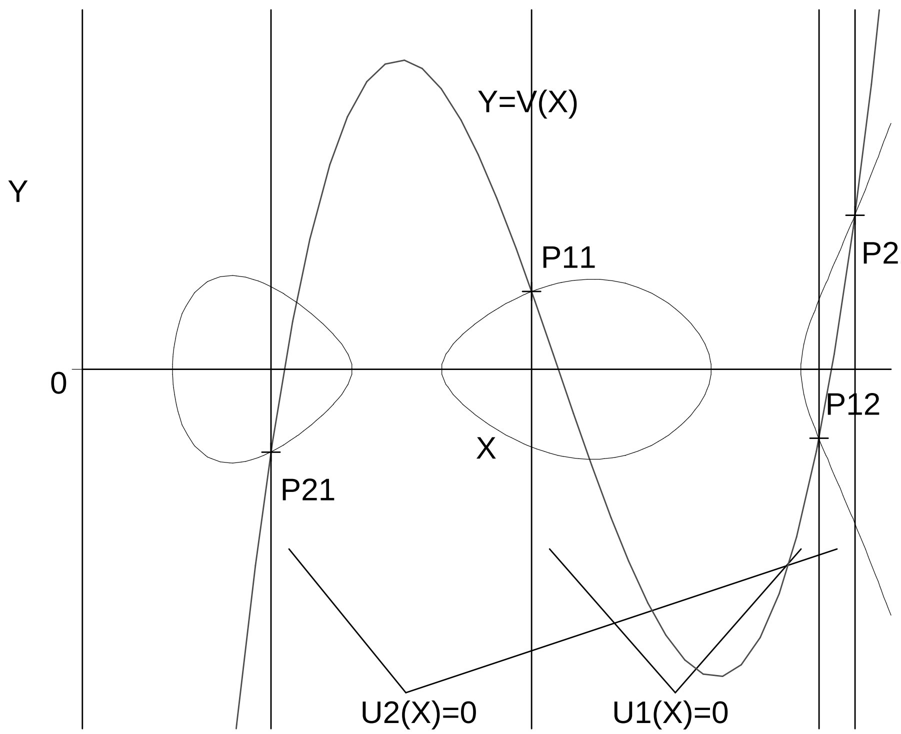
$F - V_2^2 \equiv 0 \bmod U_2,\ \mathcal{D}_2 = (U_2, V_2)$



Composition

$$\begin{aligned}\mathcal{D} &= P_{11} + P_{12} + P_{21} + P_{22} - 4P_\infty \\ &= (U, V) \\ U &= U_1 U_2\end{aligned}$$

$$F - V^2 \equiv 0 \bmod U = U_1 U_2$$



$$F - V_1^2 \equiv 0 \bmod U_1$$
$$F - V_2^2 \equiv 0 \bmod U_2$$

$$F - V^2 \equiv 0 \bmod U_1 U_2$$

中国人剰余定理によりVを求める.

$$V = SU_1 + V_1, S \in \mathbb{F}_q[X]$$

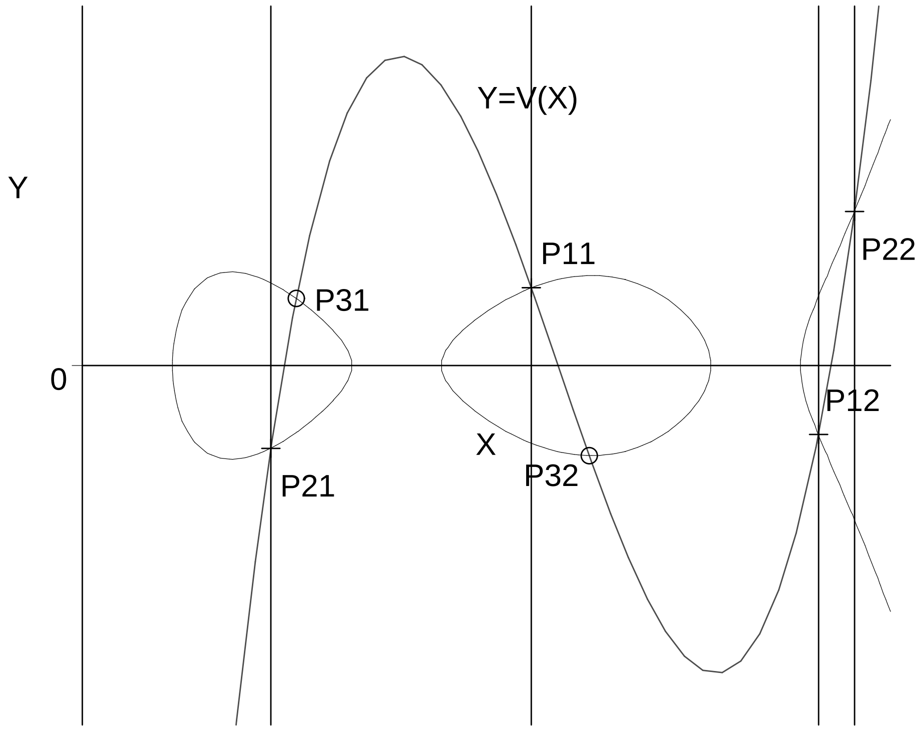
$$S \equiv (V_2 - V_1)U_1^{-1} \bmod U_2$$

Reduction

$$\mathcal{D}_3 = -(P_{31} + P_{32} - 2P\infty)$$
$$= (U_3, V_3)$$
$$\mathcal{D}_{3'} = P_{31} + P_{32} - 2P\infty$$
$$= (U_{3'}, V_{3'})$$

$$\mathcal{D}_3 = (U_3, V_3) = (U_{3'}, -V_{3'})$$

$$U_3 = (F - V^2)/U$$
$$V_3 \equiv -V \bmod U_3$$



2倍算

$\mathcal{D}_3 = 2\mathcal{D}_1$

$$U = U_1^2$$

$$F - V_1^2 \equiv 0 \bmod U_1$$

$$F - V^2 \equiv 0 \bmod U = U_1^2$$

Newton反復によりVを求める.

$$V = SU_1 + V_1, S \in \mathbb{F}_q[X]$$

$$S \equiv \frac{F - V_1^2}{U_1} V_1^{-1} \bmod U_1$$

例外の処理

加算

$\mathrm{res}(U_1, U_2) = 0$ のとき

$$\mathcal{D}_1 = P_{11} + P_{12} - 2P_\infty$$
$$\mathcal{D}_2 = P_{11} + P_{22} - 2P_\infty$$

$$\mathcal{D}_1 + \mathcal{D}_2 = 2(P_{11} - P_\infty) + (P_{12} - P_\infty) + (P_{22} - P_\infty)$$

2倍算

$\mathrm{res}(U_1, V_1) = 0$ のとき

$$\mathcal{D}_1 = P_{11} + P_{12} - 2P_\infty$$
$$2(P_{11} - P_\infty) = 0$$

$$2\mathcal{D}_1 = 2(P_{12} - P_\infty)$$

例

$$\mathcal{D}_1 = P_{11} + P_{12} - 2P_\infty$$
$$\mathrm{res}(U_1, V_1) = 0$$
$$2(P_{11} - P_\infty) = 0$$
$2(P_{12} - P_\infty) \neq 0$ のとき

$$U_1 := X^2 + u_{11}X + u_{10}$$
$$V_1 := v_{11}X + v_{10}$$

$$V_1(P_{11X}) = P_{11Y} = 0$$
$$\Rightarrow P_{11X} = -v_{10}v_{11}^{-1}$$

$$u_{11} = -(P_{11X} + P_{12X})$$
$$\Rightarrow P_{12X} = v_{10}v_{11}^{-1} - u_{11}$$

$$P_{12Y} = V_1(P_{12X})$$

$$\mathcal{D}_{1'} = (X - P_{12X}, P_{12Y})$$
$$2\mathcal{D}_1 = 2\mathcal{D}_{1'}$$

Divisorの分類

1. 加算/2倍算 の場合分け:
   $U_1 = U_2, V_1 = V_2$

2. U_1, U_2の次数

3. 共通因子による場合分け:
   Resultant

4. (Composition)

5. 結果の次数による場合分け:
   S の次数

6. (Reduction)

Stp.	Procedure	Cost
1	Compute the resultant r of U_1 and U_2.	$5M$
	$w_1 \leftarrow u_{11}u_{21}$; $w_2 \leftarrow u_{10} + u_{21}^2 - u_{20} - w_1$;	
	$r \leftarrow u_{10}(w_2 - u_{20}) + u_{20}(u_{11}^2 + u_{20} - w_1)$;	
2	If $r = 0$ then $\mathcal{D}_1$ and $\mathcal{D}_2$ have a linear factor in common, and call the exclusive procedure.	—
3	Compute $I_1 = i_{11}X + i_{10} \equiv U_1^{-1} \bmod U_2$.	$I + 2M$
	$w_1 \leftarrow r^{-1}$; $I_1 \leftarrow (w_1(u_{21} - u_{11}))X + w_1w_2$;	
4	Compute $S = s_1X + s_0 \equiv (V_2 - V_1)I_1 \bmod U_2$. (Karatsuba)	$5M$
	$w_1 \leftarrow v_{20} - v_{10}$; $w_2 \leftarrow v_{21} - v_{11}$; $w_3 \leftarrow i_{10}w_1$;	
	$w_4 \leftarrow i_{11}w_2$;	
	$w_5 \leftarrow (i_{10} + i_{11})(w_1 + w_2) - w_3 - w_4$;	
	$S \leftarrow (w_5 - u_{21}w_4)X - u_{20}w_4 + w_3$;	
5	If $s_1 = 0$ then $\mathcal{D}_3$ should be weight one, and call the exclusive procedure.	—
6	Compute the coefficient k_2 of X^2 in $K = (F - V_1^2)/U_1$.	—
	$k_2 \leftarrow f_4 - u_{11}$;	
7	Compute $T_1 = s_1X^3 + t_{12}X^2 + t_{11}X + t_{10} = SU_1$. (Karatsuba)	$3M$
	$w_1 \leftarrow s_1u_{11}$; $t_{10} \leftarrow s_0u_{10}$;	
	$t_{11} \leftarrow (s_0 + s_1)(u_{10} + u_{11}) - w_1 - t_{10}$;	
	$t_{12} \leftarrow w_1 + s_0$;	
8	Compute $U_3 = (S(T_1 + 2V_1) - K)/U_2$. (Karatsuba)	$7M$
	$u_{32} \leftarrow s_1^2$;	
	$w_1 \leftarrow s_1(s_0 + t_{12}) - 1$;	
	$w_2 \leftarrow s_1(t_{11} + 2v_{11}) + s_0t_{12} - k_2$;	
	$u_{31} \leftarrow w_1 - u_{21}u_{32}$; $u_{30} \leftarrow w_2 - u_{20}u_{32} - u_{21}u_{31}$;	
9	Make U_3 monic	$I + 2M$
	$w_1 \leftarrow u_{32}^{-1}$; $u_{30} \leftarrow u_{30}w_1$; $u_{31} \leftarrow u_{31}w_1$; $u_{32} \leftarrow 1$;	
10	Compute $V_3 \equiv -(T_1 + V_1) \bmod U_3$. (Karatsuba)	$3M$
	$w_1 \leftarrow t_{11} + v_{11}$; $w_2 \leftarrow t_{10} + v_{10}$;	
	$w_3 \leftarrow s_1u_{31}$; $w_4 \leftarrow t_{12} - w_3$; $w_5 \leftarrow w_4u_{30}$;	
	$w_6 \leftarrow (u_{30} + u_{31})(s_1 + w_4) - w_3 - w_5$;	
	$v_{31} \leftarrow w_6 - w_1$; $v_{30} \leftarrow w_5 - w_2$;	
	Total	$2I + 27M$

Harleyアルゴリズムの効果

	加算	２倍算
Cantor	$3I+70M$	$3I+76M$
Nagao	$I+56M$	$I+66M$
Harley	$2I+27M$	$2I+30M$

加算:
入力 $\mathcal{D}_1=(U_1,V_1),\mathcal{D}_2=(U_2,V_2)$ に対し,
$\deg U_1=\deg U_2=2$,
$\mathrm{res}(U_1,U_2)\neq 0$
２倍算:
入力 $\mathcal{D}_1=(U_1,V_1)$ に対し,
$\deg U_1=2$,
$\mathrm{res}(U_1,V_1)\neq 0$
のとき

上記以外の場合が起こる確率: $O(1/q)$
$\Rightarrow$
暗号への応用では上記以外は無視できる

Harleyアルゴリズムの改良

改良の方針

1. 詳細計算のチューニング

2. 曲線の定義方程式の制限

3. 逆元計算の削減

   (a) Montgomery multiple inversion

   (b) Mumford representationの拡張

詳細計算のチューニング

・Resultantの計算

$5M \Rightarrow 4M$

・U_3の計算

8	Compute $U_3 = (S(T_1 + 2V_1) - K)/U_2$. (Karatsuba)
	$u_{32} \leftarrow s_1^2$;
	$w_1 \leftarrow s_1(s_0 + t_{12}) - 1$;
	$w_2 \leftarrow s_1(t_{11} + 2v_{11}) + s_0 t_{12} - k_2$;
	$u_{31} \leftarrow w_1 - u_{21}u_{32}$; $u_{30} \leftarrow w_2 - u_{20}u_{32} - u_{21}u_{31}$;
9	Make U_3 monic
	$w_1 \leftarrow u_{32}^{-1}$; $u_{30} \leftarrow u_{30}w_1$; $u_{31} \leftarrow u_{31}w_1$; $u_{32} \leftarrow 1$;

$$U_3 = X^2 + (w_1(2s_0 - w_1) - w_2)X + w_1(w_1(s_0^2 + u_{11} + u_{21} - f_4) + 2(v_{11} - s_0 w_2)) + u_{21}w_2 + u_{10} - u_{22},$$

where $w_1 = s_1^{-1}$ and $w_2 = u_{21} - u_{11}$.

$I + 9M \Rightarrow I + 6M$

2001/7 電子情報通信学会 ISEC研究会,
2001/8 暗号とそれを支える代数曲線理論ワークショップ

では、

加算: $2I + 23M$
2倍算: $2I + 25M$

と報告したが、
加算に重複処理があることが判明

実際には

加算: $2I + 22M$
2倍算: $2I + 25M$

で計算可能

加算

Input	Weight two coprime reduced divisors $\mathcal{D}_1 = (U_1, V_1)$ and $\mathcal{D}_2 = (U_2, V_2)$	
Output	A weight two reduced divisor $\mathcal{D}_3 = (U_3, V_3)$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and U_2. $w_1 \leftarrow u_{21} - u_{11};\ w_2 \leftarrow u_{21}w_1 + u_{10} - u_{20};$ $r \leftarrow u_{10}(w_2 - u_{20}) + u_{20}(u_{20} - u_{11}w_1);$	$4M$
2	If $r = 0$ then $\mathcal{D}_1$ and $\mathcal{D}_2$ have a linear factor in common, and call the exclusive procedure.	—
3	Compute $I_1 \equiv U_1^{-1} \bmod U_2$. $w_3 \leftarrow r^{-1};\ \ I_1 \leftarrow w_1w_3X + w_2w_3;$	$I + 2M$
4	Compute S. (Karatsuba) $w_3 \leftarrow v_{20} - v_{10};\ \ w_4 \leftarrow v_{21} - v_{11};$ $w_5 \leftarrow i_{10}w_3;\ \ w_6 \leftarrow i_{11}w_4;$ $w_7 \leftarrow (i_{10} + i_{11})(w_3 + w_4) - w_5 - w_6;$ $S \leftarrow (w_7 - u_{21}w_6)X - u_{20}w_6 + w_5;$	$5M$
5	If $s_1 = 0$ then $\mathcal{D}_3$ should be weight one, and call the exclusive procedure.	—
6	Compute $U_3 = s_1^{-2}((SU_1 + V_1)^2 - F)/(U_1U_2)$. $w_3 \leftarrow s_1^{-1};$ $u_{30} \leftarrow w_3(w_3(s_0^2 + u_{11} + u_{21} - f_4)$ $+2(v_{11} - s_0w_1)) + w_2;$ $u_{31} \leftarrow w_3(2s_0 - w_3) - w_1;\ \ u_{32} \leftarrow 1;$	$I + 5M$
7	Compute $V_3 \equiv -(SU_1 + V_1) \bmod U_3$. $w_1 \leftarrow u_{30} - u_{10};\ w_2 \leftarrow u_{11} - u_{31};$ $v_{30} \leftarrow s_1u_{30}w_2 + s_0w_1 - v_{10};$ $v_{31} \leftarrow s_1(u_{31}w_2 + w_1) - s_0w_2 - v_{11};$	$6M$
Total		$2I + 22M$

2倍算

Input	A weight two reduced divisor $\mathcal{D}_1 = (U_1, V_1)$ without ramification points	
Output	A weight two reduced divisor $\mathcal{D}_2 = (U_2, V_2) = 2\mathcal{D}_1$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and V_1. $w_1 \leftarrow v_{11}^2;\quad w_2 \leftarrow u_{11}v_{11};$ $r \leftarrow u_{10}w_1 + v_{10}(v_{10} - w_2);$	$4M$
2	If $r = 0$ then $\mathcal{D}_1$ is with a ramification point, and call the exclusive procedure.	—
3	Compute $I_1 \equiv (2V_1)^{-1} \bmod U_1$. $w_3 \leftarrow (2r)^{-1};$ $I_1 \leftarrow -v_{11}w_3X + (v_{10} - w_2)w_3;$	$I + 2M$
4	Compute $T_1 \equiv (F - V_1^2)/U_1 \bmod U_1$. $w_2 \leftarrow u_{11} - f_4;\quad w_3 \leftarrow 2u_{10};$ $t_{10} \leftarrow u_{11}(2w_3 - u_{11}w_2 - f_3)$ $\qquad -f_4w_3 + f_2 - w_1;$ $t_{11} \leftarrow u_{11}(2w_2 + u_{11}) + f_3 - w_3$	$4M$
5	Compute $S \equiv I_1T_1 \bmod U_1$. (Karatsuba) $w_1 \leftarrow i_{10}t_{10};\quad w_2 \leftarrow i_{11}t_{11};$ $w_3 \leftarrow (i_{10} + i_{11})(t_{10} + t_{11}) - w_1 - w_2;$ $S \leftarrow (w_3 - u_{11}w_2)X - u_{10}w_2 + w_1;$	$5M$
6	If $s_1 = 0$ then $\mathcal{D}_2$ should be weight one, and call the exclusive procedure.	—
7	Compute $U_2 = s_1^{-2}((SU_1 + V_1)^2 - F)/U_1^2$. $w_1 \leftarrow s_1^{-1};$ $u_{20} \leftarrow w_1(w_1(s_0^2 + 2u_{11} - f_4) + 2v_{11});$ $u_{21} \leftarrow w_1(2s_0 - w_1);\quad u_{22} \leftarrow 1;$	$I + 4M$
8	Compute $V_2 \equiv -(SU_1 + V_1) \bmod U_2$. $w_1 \leftarrow u_{11} - u_{21};$ $v_{20} \leftarrow u_{20}(s_1w_1 + s_0) - s_0u_{10} - v_{10};$ $v_{21} \leftarrow s_1(u_{21}w_1 + u_{20} - u_{10}) - s_0w_1 - v_{11};$	$6M$
Total		$2I + 25M$

曲線の定義方程式の制限

$p \neq 5$のとき

$$(X, Y) \mapsto \left(X + \frac{f_4}{5}, Y\right)$$

により

$$\begin{aligned} C/\mathbb{F}_q :& Y^2 = F(X), \\ & F(X) = X^5 + f_3X^3 + \cdots + f_0 \end{aligned}$$

とできる.

暗号への応用を考慮すると，この定義で十分
※楕円曲線暗号ではより強い制限を与えて
　高速化を計る事も多い

$f_4 = 0 \Rightarrow$ 2倍算に必要な乗算を2回削減可能
$\Rightarrow$ 2倍算: $2M + 23M$

加算

Input	Weight two coprime reduced divisors $\mathcal{D}_1 = (U_1, V_1)$ and $\mathcal{D}_2 = (U_2, V_2)$	
Output	A weight two reduced divisor $\mathcal{D}_3 = (U_3, V_3)$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and U_2. $w_1 \leftarrow u_{21} - u_{11};\ w_2 \leftarrow u_{21}w_1 + u_{10} - u_{20};$ $r \leftarrow u_{10}(w_2 - u_{20}) + u_{20}(u_{20} - u_{11}w_1);$	$4M$
2	If $r = 0$ then $\mathcal{D}_1$ and $\mathcal{D}_2$ have a linear factor in common, and call the exclusive procedure.	—
3	Compute $I_1 \equiv U_1^{-1} \bmod U_2$. $w_3 \leftarrow r^{-1};\ \ I_1 \leftarrow w_1w_3X + w_2w_3;$	$I + 2M$
4	Compute S. (Karatsuba) $w_3 \leftarrow v_{20} - v_{10};\ \ w_4 \leftarrow v_{21} - v_{11};$ $w_5 \leftarrow i_{10}w_3;\ \ w_6 \leftarrow i_{11}w_4;$ $w_7 \leftarrow (i_{10} + i_{11})(w_3 + w_4) - w_5 - w_6;$ $S \leftarrow (w_7 - u_{21}w_6)X - u_{20}w_6 + w_5;$	$5M$
5	If $s_1 = 0$ then $\mathcal{D}_3$ should be weight one, and call the exclusive procedure.	—
6	Compute $U_3 = s_1^{-2}((SU_1 + V_1)^2 - F)/(U_1U_2)$. $w_3 \leftarrow s_1^{-1};$ $u_{30} \leftarrow w_3(w_3(s_0^2 + u_{11} + u_{21})$ $+2(v_{11} - s_0w_1)) + w_2;$ $u_{31} \leftarrow w_3(2s_0 - w_3) - w_1;\ \ u_{32} \leftarrow 1;$	$I + 5M$
7	Compute $V_3 \equiv -(SU_1 + V_1) \bmod U_3$. $w_1 \leftarrow u_{30} - u_{10};\ w_2 \leftarrow u_{11} - u_{31};$ $v_{30} \leftarrow s_1u_{30}w_2 + s_0w_1 - v_{10};$ $v_{31} \leftarrow s_1(u_{31}w_2 + w_1) - s_0w_2 - v_{11};$	$6M$
Total		$2I + 22M$

2倍算

Input	A weight two reduced divisor $\mathcal{D}_1 = (U_1, V_1)$ without ramification points	
Output	A weight two reduced divisor $\mathcal{D}_2 = (U_2, V_2) = 2\mathcal{D}_1$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and V_1. $w_1 \leftarrow v_{11}^2$; $w_2 \leftarrow u_{11}v_{11}$; $r \leftarrow u_{10}w_1 + v_{10}(v_{10} - w_2)$;	$4M$
2	If $r = 0$ then $\mathcal{D}_1$ is with a ramification point, and call the exclusive procedure.	—
3	Compute $I_1 \equiv (2V_1)^{-1} \bmod U_1$. $w_3 \leftarrow (2r)^{-1}$; $I_1 \leftarrow -v_{11}w_3X + (v_{10} - w_2)w_3$;	$I + 2M$
4	Compute $T_1 \equiv (F - V_1^2)/U_1 \bmod U_1$. $w_2 \leftarrow u_{11}^2$; $w_3 \leftarrow w_2 + f_3$; $w_4 \leftarrow 2u_{10}$; $t_{10} \leftarrow u_{11}(2w_4 - w_3) + f_2 - w_1$; $t_{11} \leftarrow 2w_2 + w_3 - w_4$	$2M$
5	Compute $S \equiv I_1T_1 \bmod U_1$. (Karatsuba) $w_1 \leftarrow i_{10}t_{10}$; $w_2 \leftarrow i_{11}t_{11}$; $w_3 \leftarrow (i_{10} + i_{11})(t_{10} + t_{11}) - w_1 - w_2$; $S \leftarrow (w_3 - u_{11}w_2)X - u_{10}w_2 + w_1$;	$5M$
6	If $s_1 = 0$ then $\mathcal{D}_2$ should be weight one, and call the exclusive procedure.	—
7	Compute $U_2 = s_1^{-2}((SU_1 + V_1)^2 - F)/U_1^2$. $w_1 \leftarrow s_1^{-1}$; $u_{20} \leftarrow w_1(w_1(s_0^2 + 2u_{11}) + 2v_{11})$; $u_{21} \leftarrow w_1(2s_0 - w_1)$; $u_{22} \leftarrow 1$;	$I + 4M$
8	Compute $V_2 \equiv -(SU_1 + V_1) \bmod U_2$. $w_1 \leftarrow u_{11} - u_{21}$; $v_{20} \leftarrow u_{20}(s_1w_1 + s_0) - s_0u_{10} - v_{10}$; $v_{21} \leftarrow s_1(u_{21}w_1 + u_{20} - u_{10}) - s_0w_1 - v_{11}$;	$6M$
Total		$2I + 23M$

逆元計算の削減

有限体上の演算において
乗算処理と比較し
逆元計算処理にはより多くの時間を必要とする

実装により異なるが
$I > 4M$
と考える事は妥当なことと思われる
※ $I \approx 2M$ という実装も存在する

乗算回数が多少増えても,
逆元計算回数が減れば高速になる

1. Montgomery multiple inversion
   — 逆元計算1回

2. Mumford representationの拡張
   — 逆元計算0回

Montgomery multiple inversionの利用

Montgomery multiple inversion

$a_i \in \mathbb{F}_q^*$,
$(a_1, \ldots, a_n) \mapsto (a_1^{-1}, \ldots, a_n^{-1})$

通常: nI
Montgomery: $I + (3n-3)M$

独立な2元の逆元は $I + 3M$ で計算可能
詳細はCohen's text book

いまは,

$(r, s' = rs) \mapsto (r^{-1}, s^{-1})$

$$\begin{array}{lll} 1 & w_1 & \leftarrow (rs')^{-1} \\ 2 & r^{-1} & \leftarrow w_1 s' \\ 3 & w_2 & \leftarrow r^2 \\ 4 & s^{-1} & \leftarrow w_1 w_2 \end{array}$$

$\underline{2I \to I + 4M}$

加算

Input	Weight two reduced divisors $\mathcal{D}_1 = (U_1, V_1)$ and $\mathcal{D}_2 = (U_2, V_2)$	
Output	A weight two reduced divisor $\mathcal{D}_3 = (U_3, V_3)$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and U_2. $w_1 \leftarrow u_{21} - u_{11}$; $w_2 \leftarrow u_{21}w_1 + u_{10} - u_{20}$; $r \leftarrow u_{10}(w_2 - u_{20}) + u_{20}(u_{20} - u_{11}w_1)$;	$4M$
2	If $r = 0$ then $\mathcal{D}_1$ and $\mathcal{D}_2$ have a linear factor in common, and call the exclusive procedure.	—
3	Compute $I_1 \equiv rU_1^{-1} \bmod U_2$. $I_1 \leftarrow w_1X + w_2$;	—
4	Compute S. (Karatsuba) $w_3 \leftarrow v_{20} - v_{10}$; $w_4 \leftarrow v_{21} - v_{11}$; $w_5 \leftarrow i_{10}w_3$; $w_6 \leftarrow i_{11}w_4$; $w_7 \leftarrow (i_{10} + i_{11})(w_3 + w_4) - w_5 - w_6$; $S \leftarrow (w_7 - u_{21}w_6)X - u_{20}w_6 + w_5$;	$5M$
5	If $s_1 = 0$ then $\mathcal{D}_3$ should be weight one, and call the exclusive procedure.	—
6	Collect S $w_3 \leftarrow (rs_1)^{-1}$; $w_4 \leftarrow s_1w_3$; $w_3 \leftarrow r^2w_3$; $s_0 \leftarrow s_0w_4$; $s_1 \leftarrow s_1w_4$;	$I + 6M$
7	Compute $U_3 = s_1^{-2}((SU_1 + V_1)^2 - F)/(U_1U_2)$. $u_{30} \leftarrow w_3(w_3(s_0^2 + u_{11} + u_{21}) +2(v_{11} - s_0w_1)) + w_2$; $u_{31} \leftarrow w_3(2s_0 - w_3) - w_1$; $u_{32} \leftarrow 1$;	$5M$
8	Compute $V_3 \equiv -(SU_1 + V_1) \bmod U_3$. $w_1 \leftarrow u_{30} - u_{10}$; $w_2 \leftarrow u_{11} - u_{31}$; $v_{30} \leftarrow s_1u_{30}w_2 + s_0w_1 - v_{10}$; $v_{31} \leftarrow s_1(u_{31}w_2 + w_1) - s_0w_2 - v_{11}$;	$6M$
Total		$I + 26M$

2倍算

Input	A weight two divisor $\mathcal{D}_1 = (U_1, V_1)$ without ramification points	
Output	A weight two reduced divisor $\mathcal{D}_2 = (U_2, V_2) = 2\mathcal{D}_1$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and V_1.	$4M$
	$w_1 \leftarrow v_{11}^2$; $w_2 \leftarrow u_{11}v_{11}$;	
	$r \leftarrow u_{10}w_1 + v_{10}(v_{10} - w_2)$;	
2	If $r = 0$ then	
	$\mathcal{D}_1$ is with a ramification point,	
	and call the exclusive procedure.	—
3	Compute $I_1 \equiv rV_1^{-1} \bmod U_1$.	—
	$I_1 \leftarrow -v_{11}X + v_{10} - w_2$;	
4	Compute $T_1 \equiv (F - V_1^2)/U_1 \bmod U_1$.	$2M$
	$w_2 \leftarrow u_{11}^2$; $w_3 \leftarrow w_2 + f_3$; $w_4 \leftarrow 2u_{10}$;	
	$t_{10} \leftarrow u_{11}(2w_4 - w_3) + f_2 - w_1$;	
	$t_{11} \leftarrow 2w_2 + w_3 - w_4$;	
5	Compute $S \equiv I_1T_1 \bmod U_1$. (Karatsuba)	$5M$
	$w_1 \leftarrow i_{10}t_{10}$; $w_2 \leftarrow i_{11}t_{11}$;	
	$w_3 \leftarrow (i_{10} + i_{11})(t_{10} + t_{11}) - w_1 - w_2$;	
	$S \leftarrow (w_3 - u_{11}w_2)X - u_{10}w_2 + w_1$;	
6	If $s_1 = 0$ then $\mathcal{D}_2$ should be weight one,	
	and call the exclusive procedure.	—
7	Collect S	$I + 6M$
	$w_1 \leftarrow (2rs_1)^{-1}$; $w_2 \leftarrow s_1w_1$; $w_1 \leftarrow 4r^2w_1$;	
	$s_0 \leftarrow s_0w_2$; $s_1 \leftarrow s_1w_2$;	
8	Compute $U_2 = s_1^{-2}((SU_1 + V_1)^2 - F)/U_1^2$.	$4M$
	$u_{20} \leftarrow w_1(w_1(s_0^2 + 2u_{11}) + 2v_{11})$;	
	$u_{21} \leftarrow w_1(2s_0 - w_1)$; $u_{22} \leftarrow 1$;	
9	Compute $V_2 \equiv -(SU_1 + V_1) \bmod U_2$.	$6M$
	$w_1 \leftarrow u_{11} - u_{21}$;	
	$v_{20} \leftarrow u_{20}(s_1w_1 + s_0) - s_0u_{10} - v_{10}$;	
	$v_{21} \leftarrow s_1(u_{21}w_1 + u_{20} - u_{10}) - s_0w_1 - v_{11}$;	
Total		$I + 27M$

Mumford representationの拡張

Harleyアルゴリズムの入出力divisor $\mathcal{D}_i$:

$$\begin{aligned}
\mathcal{D}_i &= (U_i, V_i),\\
U_i &= X^2 + u_{i1}X + u_{i0},\\
V_i &= v_{i1}X + v_{i0}
\end{aligned}$$

$\Rightarrow$
出力のU_iをモニックにするために，
逆元計算は不可避

$\Rightarrow$
逆元計算を消去するためには，
Mumford representationの拡張が必要

U_i, V_i に任意の $a \in \mathbb{F}_q^*$ を乗じた,

$$\begin{aligned} U_i' &= aU_i & &= aX^2 + au_{i1}X + au_{i0}, \\ V_i' &= aV_i & &= av_{i1}X + av_{i0} \end{aligned}$$

を用いた表現

$$\mathcal{D}_i = (U_i', V_i') \ (= (U_i, V_i))$$

を許す
(Modified Mumford Representation)

※ $(U_i, V_i) = (U_i'/u_{i2}', V_i'/u_{i2}')$

入力 divisor も MMR なので,
計算手順は全面的な書き換えが必要であった

加算: $54M$
2倍算: $53M$

改良の変遷

		加算	2倍算
2000/7	[1]	$2I + 30M$	$2I + 30M^{\ddagger}$
2000	[2]	$2I + 27M$	$2I + 30M^{\ddagger}$
2001/7	[3]	$2I + 23M^{\dagger}$	$2I + 25M^{\ddagger}$
2001/8	[4]	$I + 27M^{\dagger}$	$I + 27M$
2002/1	[5]	$I + 26M$	$I + 27M$
		$54M$	$53M$
2002/1	[6]	$2I + 21M$	$2I + 25M^{\ddagger}$
		$I + 25M$	$I + 29M^{\ddagger}$

[1]Gaudry-Harley, ANTS IV, [2]Harley, Homepage

[3]M-Chao-Tsujii, ISEC

[4]M, 暗号とそれを支える代数曲線理論ワークショップ (アナウンスのみ)

[5]Miyamoto-Doi-M-Chao-Tsujii, SCIS

[6]Takahashi, SCIS

†: 本来 $-M$

‡: $f_4 = 0 \Rightarrow -2M$

高橋さんのアイディア

U_3 : モニック化 $\Rightarrow S$: モニック化

楕円曲線暗号との比較

比較対象:

EC　IEEE P1363方式(Jacobian Projective)
加算: $16M$, 2倍算: $10M$
Affine
加算: $I+3M$, 2倍算: $I+4M$

HEC 加算: $54M$, 2倍算: $53M$
加算: $I+25M$, 2倍算: $I+27M$
加算: $2I+21M$, 2倍算: $2I+23M$

安全性$\approx \#E(\mathbb{F}_q), \#\mathcal{J}_C(\mathbb{F}_q)$

$(q^{1/2}-1)^{2g} \le \#\mathcal{J}_C(\mathbb{F}_q) \le (q^{1/2}+1)^{2g}$
$\Rightarrow$
$\#E(\mathbb{F}_q) \approx q$
$\#\mathcal{J}_C(\mathbb{F}_q) \approx q^2$

$N \approx \#E(\mathbb{F}_{q_E}) \Rightarrow q_E \approx N$
$N \approx \#\mathcal{J}_C(\mathbb{F}_{q_H}) \Rightarrow q_H \approx \sqrt{N} \Rightarrow q_H \approx \sqrt{q_E}$

定義体上の乗算コスト
$M \approx (\log q)^2$ (classical mulitiplication)

$M_E : \mathbb{F}_{q_E}$上の乗算コスト
$M_H : \mathbb{F}_{q_H}$上の乗算コスト
$\Rightarrow M_E \approx 4M_H$

整数倍算時間比

暗復号処理時間の殆んどは整数倍算処理

	加算	２倍算
EC1	$16M_E = 64M_H$	$10M_E = 40M_H$
EC2	$I_E + 3M_E = 4I_H + 12M_H$	$I_E + 4M_E = 4I_H + 16M_H$
HEC1	$54M_H$	$53M_H$
HEC2	$I_H + 25M_H$	$I_H + 27M_H$
HEC3	$2I_H + 21M_H$	$2I_H + 23M_H$

整数倍算中に
加算と２倍算が等頻度で現れるとすると

I_H/M_H	EC1	EC2	HEC1	HEC2	HEC3
2	2.4	$\underline{1}$	2.4	1.3	1.2
4	1.7	$\underline{1}$	1.8	$\underline{1}$	$\underline{1}$
6	1.6	1.2	1.7	$\underline{1}$	1.1
8	1.5	1.4	1.6	$\underline{1}$	1.1
10	1.4	1.5	1.5	$\underline{1}$	1.2
12	1.4	1.6	1.4	$\underline{1}$	1.2
14	1.3	1.8	1.3	$\underline{1}$	1.3
16	1.2	1.9	1.3	$\underline{1}$	1.3
18	1.2	2.0	1.2	$\underline{1}$	1.3
20	1.1	2.0	1.2	$\underline{1}$	1.3
22	1.08	2.1	1.1	$\underline{1}$	1.4
24	1.04	2.2	1.07	$\underline{1}$	1.4
26	$\underline{1}$	2.3	1.03	$\underline{1}$	1.4
28	$\underline{1}$	2.4	1.03	1.04	1.5
30	$\underline{1}$	2.6	1.03	1.07	1.6

加算の頻度が2倍算の頻度の1/2とすると

I_H/M_H	EC1	EC2	HEC1	HEC2	HEC3
2	2.1	$\underline{1}$	2.4	1.3	1.2
4	1.6	1.01	1.8	$\underline{1}$	$\underline{1}$
6	1.5	1.2	1.6	$\underline{1}$	1.06
8	1.4	1.4	1.6	$\underline{1}$	1.1
10	1.3	1.5	1.5	$\underline{1}$	1.2
12	1.3	1.6	1.4	$\underline{1}$	1.2
14	1.2	1.8	1.3	$\underline{1}$	1.2
16	1.1	1.9	1.3	$\underline{1}$	1.3
18	1.1	2.0	1.2	$\underline{1}$	1.3
20	1.03	2.0	1.2	$\underline{1}$	1.3
22	$\underline{1}$	2.1	1.1	1.01	1.4
24	$\underline{1}$	2.3	1.1	1.04	1.5
26	$\underline{1}$	2.5	1.1	1.09	1.5
28	$\underline{1}$	2.6	1.1	1.1	1.6
30	$\underline{1}$	2.8	1.1	1.2	1.7

実装による比較

超楕円曲線 : 加算 $2I+23M$ 版と $I+26M$ 版
楕円曲線 : P1363

整数倍算 : sliding window (幅4)
逆元演算 : Kobayashi et al. @Euro99

$\mathbb{F}_{q_H} = \mathbb{F}_p(\alpha)$: 93–bit OEF
$\mathbb{F}_{q_E} = \mathbb{F}_p(\beta)$: 186–bit OEF

$p = 2^{31} - 1$
$\alpha^3 - 5 = 0$
$\beta^6 - 5 = 0$

$\#\mathcal{J}_C(\mathbb{F}_{q_H}) \approx \#E(\mathbb{F}_{q_E}) \approx 2^{186}$

整数倍算は186bit乱数倍

使用言語　：C++
コンパイラ：gnu g++−2.95.2

	加算	２倍算	整数倍算
EC	11.6μs.	6.58μs.	1.76ms.
$2I+23M$ 版	8.32μs.	8.74μs.	1.98ms.
$I+26M$ 版	7.22μs.	7.50μs.	1.69ms.

on Pentium III 866MHz

$M_E \approx 3.8 M_H$
$I_H \approx 6.4 M_H$
$\Rightarrow$
超楕円曲線の演算は理論値より遅い
$\Rightarrow$
実装について検討する必要がある.

Harleyアルゴリズムの種数3の超楕円曲線への適用

種数3の超楕円曲線

$\mathbb{F}_q$: 位数qの有限体
$p :=$ char $\mathbb{F}_q \neq 2, 7$

$$
\begin{aligned}
C/\mathbb{F}_q : & Y^2 = F(X), \\
& F(X) = X^7 + f_5 X^5 + \cdots + f_0, \\
& f_i \in \mathbb{F}_q, \mathrm{disc}\,(F) \neq 0
\end{aligned}
$$

暗号応用での利点

位数size $\approx$ 種数 $\times$ 定義体size

定義体サイズ: 64bit $\Rightarrow$ 位数サイズ: 192bit

位数size$\geq$160bit $\Rightarrow$ 安全な暗号系を構成可能

64bit CPU 上で多倍長演算を用いること無く
安全な暗号系を構成可能

種数2の場合との相違点

1. Divisorの分類

2. Composition

3. Reduction

Divisorの分類

Reduced divisor

$$
\begin{aligned}
\mathcal{D}_i &= P_{i1} + P_{i2} + P_{i3} - 3P_\infty \\
\text{または} & \\
\mathcal{D}_i &= P_{i1} + P_{i2} - 2P_\infty \\
\text{または} & \\
\mathcal{D}_i &= P_{i1} - P_\infty \\
\text{または} & \\
\mathcal{D}_i &= 0
\end{aligned}
$$

$\Rightarrow$ 場合分けが爆発的に増える: コードサイズの増加
分類処理計算も複雑: 処理時間の増加
$\Rightarrow$ Cantorアルゴリズムを併用する

分類フロー

加算

入力: $\mathcal{D}_1 = (U_1, V_1), \mathcal{D}_2 = (U_2, V_2)$

1. $\deg U_1 = \deg U_2 = 3$ and $\mathrm{res}(U_1, U_2) \neq 0$
   $\Rightarrow$ Harleyアルゴリズム

2. そうでないならば
   $\Rightarrow$ Cantorアルゴリズム: 確率 $O(1/q)$

2倍算

入力: $\mathcal{D}_1 = (U_1, V_1)$

1. $\deg U_1 = 3$ and $\mathrm{res}(U_1, V_1) \neq 0$
   $\Rightarrow$ Harleyアルゴリズム

2. そうでないならば
   $\Rightarrow$ Cantorアルゴリズム: 確率 $O(1/q)$

Composition

基本的には種数２と同じ

$\deg U, \deg V$ が種数２と違う

	$\deg U$	$\deg V$
genus 2	4	3
genus 3	6	5

$\Rightarrow$ 有限体上の演算数は増える

Reduction

２回の reduction が必要

	$\deg U$	$\deg V$	$F - V^2$ の根
Composition	6	5	10 個
First reduction	4	3	7 個
Second reduction	3	2	

加算: $I + 81M$

Input	Weight three coprime reduced divisors $\mathcal{D}_1 = (U_1, V_1)$ and $\mathcal{D}_2 = (U_2, V_2)$	
Output	A weight three reduced divisor $\mathcal{D}_3 = (U_3, V_3) = \mathcal{D}_1 + \mathcal{D}_2$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and U_2.	$18M$
2	If $r = 0$ then call Cantor algorithm.	—
3	Compute $I_1 = i_{12}X^2 + i_{11}X + i_{10} \equiv r/U_1 \bmod U_2$.	$3M$
4	Compute $rS = rs_2X^2 + rs_1X + rs_0 \equiv (V_2 - V_1)I_1 \bmod U_2$. (Karatsuba)	$11M$
5	If $rs_2 = 0$ then call the exclusive procedure.	—
6	Compute $S = s_2X^2 + s_1X + s_0$ $= r^{-1}(rs_2X^2 + rs_1X + rs_0)$.	$I + 7M$
7	Compute $U_t = s_2^{-2}((S^2U_1 + 2SV_1)/U_2 - (F - V_1^2)/(U_1U_2))$.	$19M$
8	Compute $V_t = -(SU_1 + V_1) \bmod U_t$. (Karatsuba)	$12M$
9	Compute $U_3 = (F - V_t^2)/U_t$.	$8M$
10	Compute $V_3 = -V_t \bmod U_3$. (Karatsuba)	$3M$
Total		$I + 81M$

2倍算: $I + 74M$

Input	A weight three reduced divisor $\mathcal{D}_1 = (U_1, V_1)$ without ramification points	
Output	A weight three reduced divisor $\mathcal{D}_2 = (U_2, V_2) = 2\mathcal{D}_1$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and V_1.	$15M$
2	If $r = 0$ then call Cantor algorithm.	—
3	Compute $I_1 = i_{12}X^2 + i_{11}X + i_{10} \equiv r/V_1 \bmod U_1$.	$3M$
4	Compute $T_1 = t_{12}X^2 + t_{11}X + t_{10} \equiv (F - V_1^2)/U_1 \bmod U_1$.	$7M$
5	Compute $2rS = 2rs_2X^2 + 2rs_1X + 2rs_0 \equiv I_1T_1 \bmod U_1$. (Karatsuba)	$11M$
6	If $2rs_2 = 0$ then call the exclusive procedure.	—
7	Compute $S = s_2X^2 + s_1X + s_0$ $= (2r)^{-1}(2rs_2X^2 + 2rs_1X + 2rs_0)$.	$I + 7M$
8	Compute $U_t = s_2^{-2}(((SU_1 + V_1)^2 - F)/U_1^2)$.	$9M$
9	Compute $V_t = -(SU_1 + V_1) \bmod U_t$. (Karatsuba)	$12M$
10	Compute $U_2 = (F - V_t^2)/U_t$.	$7M$
11	Compute $V_2 = -V_t \bmod U_2$. (Karatsuba)	$3M$
Total		$I + 74M$

実装結果

定義体: $\mathbb{F}_p, p = 2^{61} - 1$

整数倍算は186bit乱数倍, sliding window (幅4)

使用言語　：C++ (1行だけinline assembler使用)
コンパイラ：Compaq C++

加算	2倍算	整数倍算
4.27 μs.	4.09 μs.	932 μs.

on Alpha 21264 667MHz

Harleyアルゴリズムの標数2の有限体上の超楕円曲線への適用 (g=2)

種数2の超楕円曲線$/\mathbb{F}_{2^n}$

$\mathbb{F}_q$: 位数qの有限体, $\mathrm{char}\,\mathbb{F}_q = 2$

$$\begin{aligned} C/\mathbb{F}_q :& Y^2 + H(X)Y = F(X), \\ & F(X) = X^5 + f_3X^3 + f_1X + f_0, \\ & H(X) = X^2 + h_1X + h_0, \\ & f_i, h_i \in \mathbb{F}_q, \end{aligned}$$

$$\{(x,y) \in \bar{\mathbb{F}}_q^2 \mid y^2 + H(x)y + F(x) = H(x) = H'(x)y + F'(x) = 0\} \\ = \phi$$

$\deg H = 2 \Leftrightarrow \mathcal{J}_C$: ordinary

$p \neq 2$の場合との相違点

	$p \neq 2$	$p = 2$
分岐点	$P_Y = 0$	$H(P_X) = 0$
Mumford	$U \mid F - V^2$	$U \mid F + HV + V^2$
$-\mathcal{D}$	$(U, -V)$	$(U, U + V + H)$
2倍算		
$\exists \mathcal{J}_C[2](\mathbb{F}_q)$	res(U, V)	res(H, V)
S	$\frac{F - V_1^2}{U_1} V_1^{-1}$ mod U_1	$\frac{F + HV_1 + V_1^2}{U_1} H^{-1}$ mod U_2

結果

加算: $I + 26M$(暫定)
2倍算: $I + 28M$(暫定)