種数２の超楕円曲線を用いた高速暗号系について

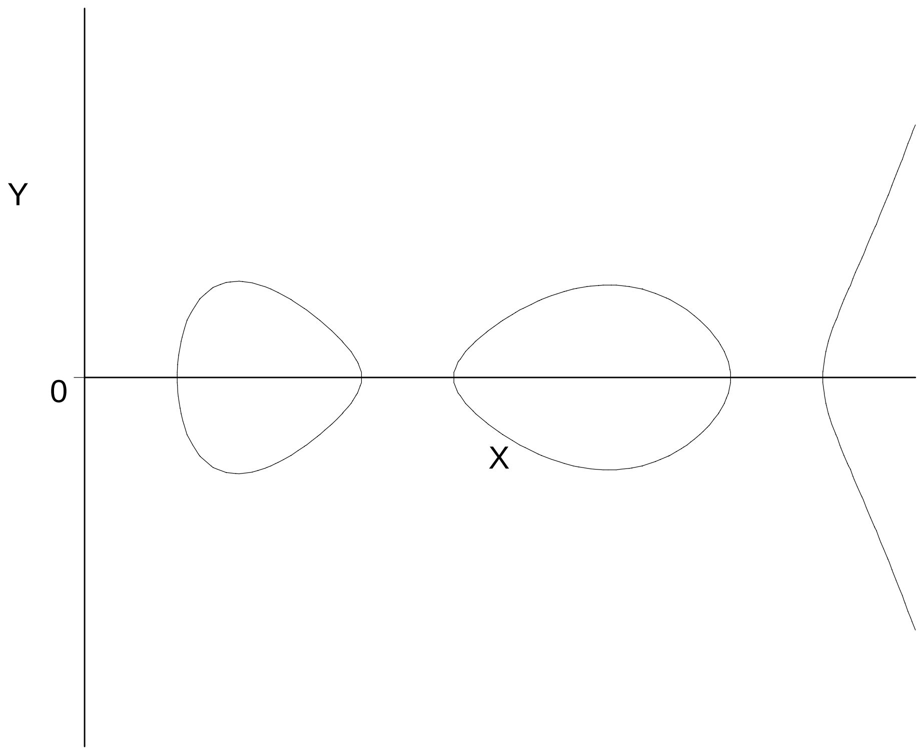
松尾 和人*　　趙 晋輝†

* 東洋通信機　　† 中央大学

種数2の超楕円曲線

char $\mathbb{F}_q \neq 2$

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



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

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"

主旨

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.

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の詳細な場合分け
・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

本研究の目的

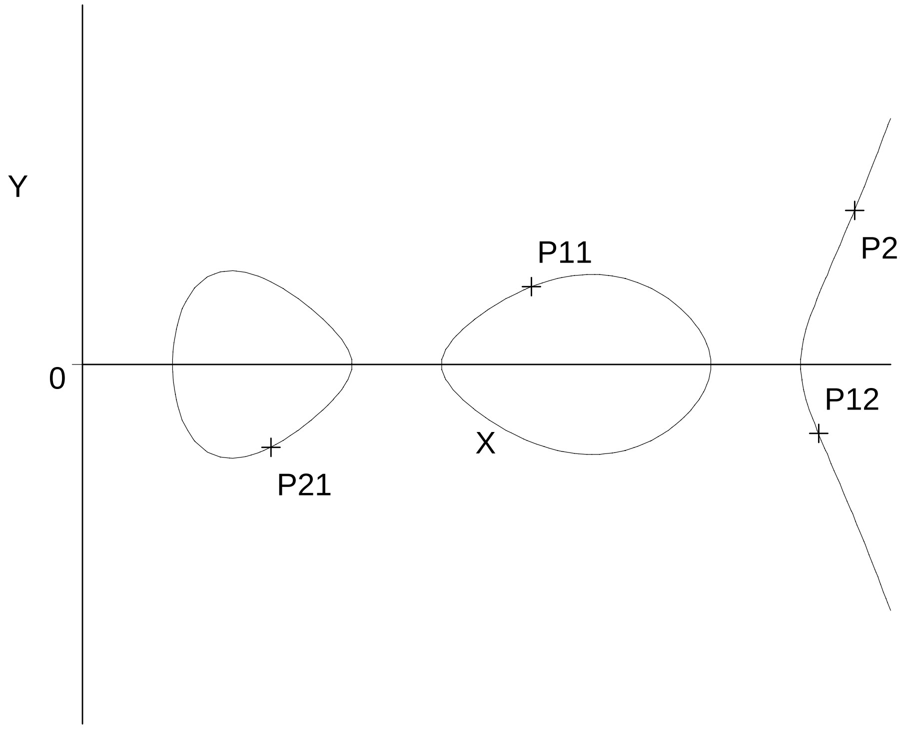
1. Harley アルゴリズムの改良

2. (改良)Harley アルゴリズムを用いた
   超楕円曲線暗号と，楕円曲線暗号の速度比較

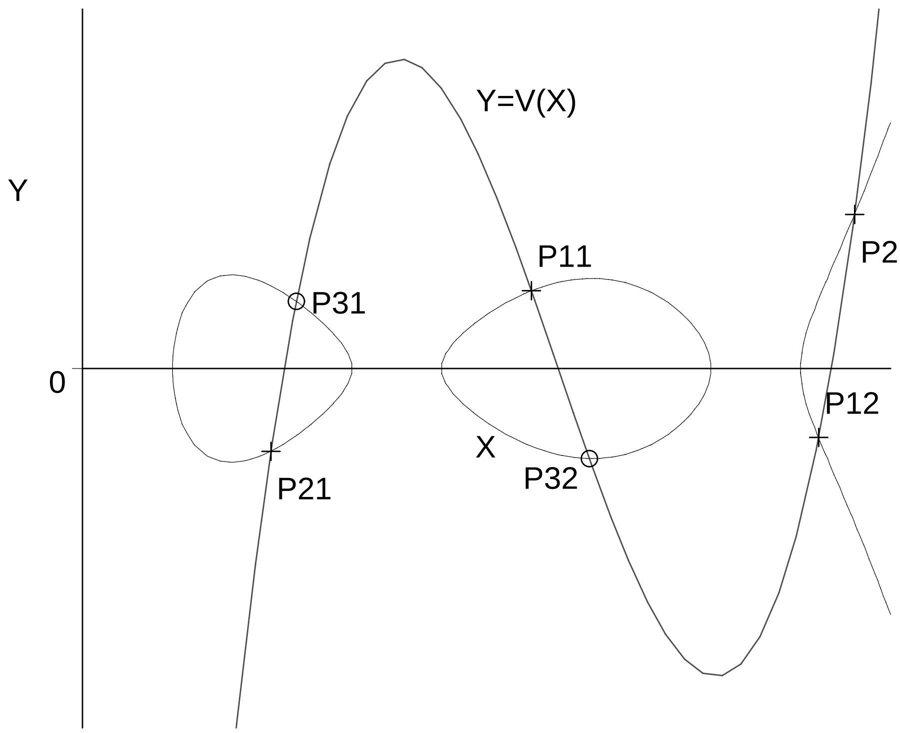
Harleyの加算

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

$\mathcal{D}_1 = P_{11} + P_{12} - 2P_\infty$
$\mathcal{D}_2 = P_{21} + P_{22} - 2P_\infty$
P_∞: 無限遠点



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

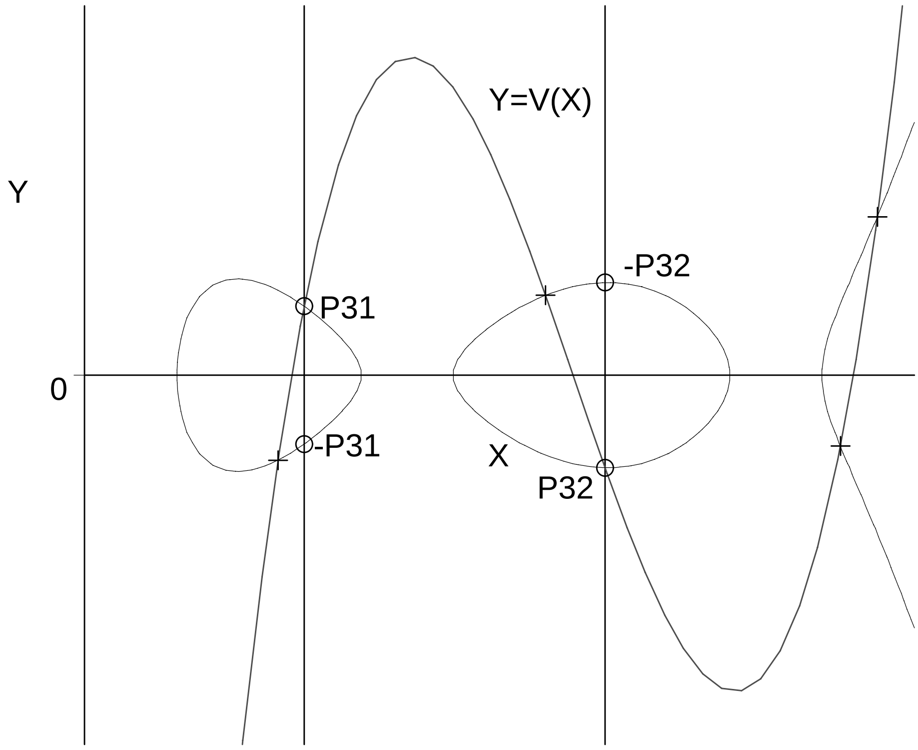


$$P_{11} + P_{12} + P_{21} + P_{22} + P_{31} + P_{32} - 6P_\infty = 0$$

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

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

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



Mumford representation

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

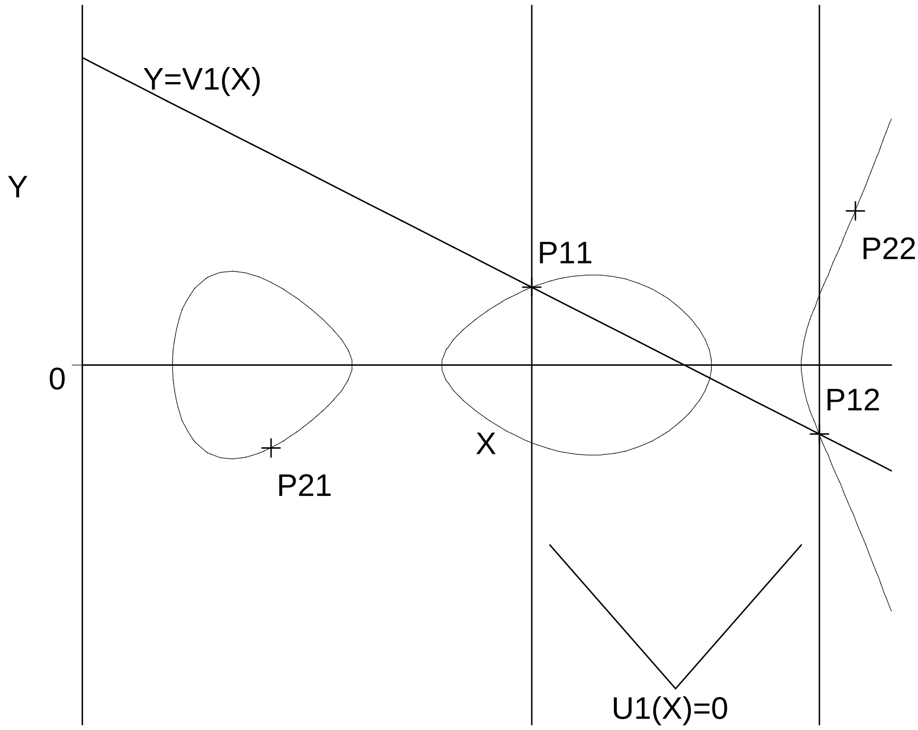
$$\mathcal{D}_1 = P_{11} + P_{12} - 2P_\infty = (U_1, V_1)$$

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

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

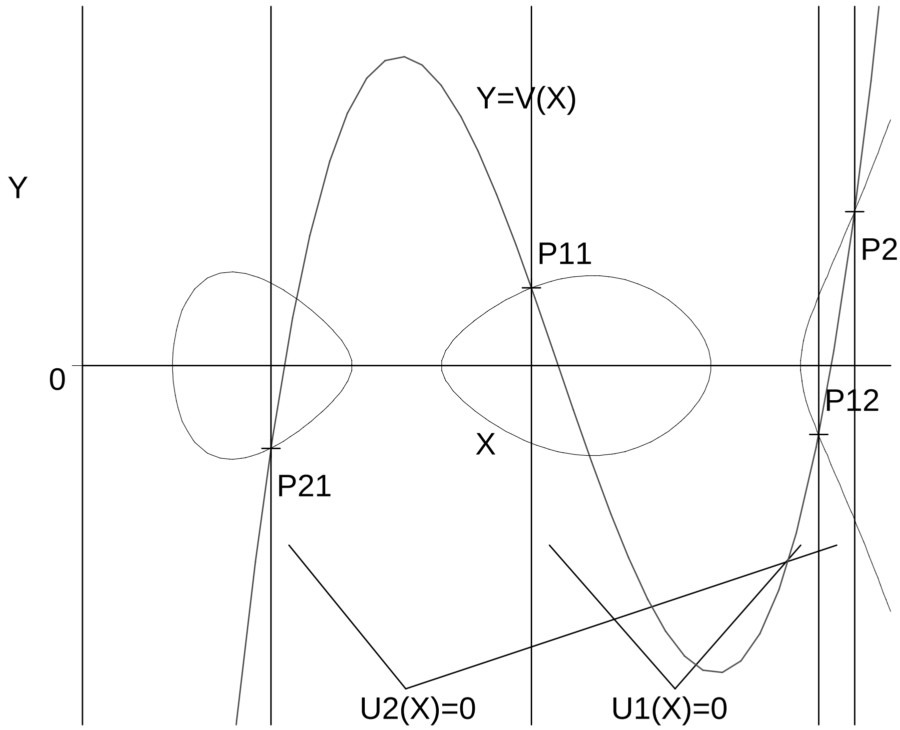
$$F - V_1^2 \equiv 0 \bmod U_1$$

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



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

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



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

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

中国人剰余定理により V を求める.

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

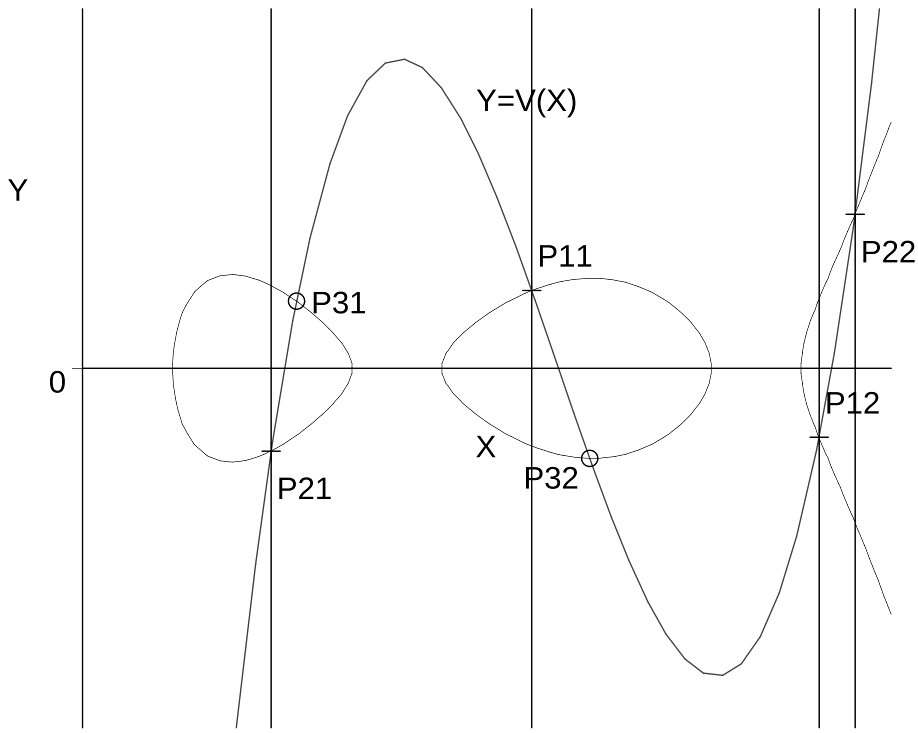
$$S \equiv (V_2 - V_1)U_1^{-1} \bmod U_2$$

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

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

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

フロー

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. 加算

5. 結果の次数による場合分け:
   S の次数

6. Reduction

改良

フローはオリジナルのまま
詳細計算のチューニングを行った

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 $I_1 = i_{11}X + i_{10} \equiv U_1^{-1} \bmod U_2$.	$I + 2M$
	$w_1 \leftarrow r^{-1}$; $I_1 \leftarrow (w_1(u_{21} - u_{11}))X + w_1 w_2$;	
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	$2I + 27M$

・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 $w_2 = u_{21} - u_{11}$.

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

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) $w_1 \leftarrow v_{20} - v_{10}$; $w_2 \leftarrow v_{21} - v_{11}$; $w_3 \leftarrow i_{10}w_1$; $w_4 \leftarrow i_{11}w_2$; $w_5 \leftarrow (i_{10} + i_{11})(w_1 + w_2) - w_3 - w_4$; $S \leftarrow (w_5 - u_{21}w_4)X - u_{20}w_4 + w_3$;	$5M$
5	If $s_1 = 0$ then $\mathcal{D}_3$ should be weight one, and call the exclusive procedure.	—
6	Compute $U_3 = s_1^{-2}((SU_1 + V_1)^2 - F)/(U_1U_2)$. $w_1 \leftarrow s_1^{-1}$; $w_2 \leftarrow u_{21} - u_{11}$; $u_{30} \leftarrow w_1(w_1(s_0^2 + u_{11} + u_{21} - f_4)$ $+2(v_{11} - s_0w_2))+$ $u_{21}w_2 + u_{10} - u_{20}$; $u_{31} \leftarrow w_1(2s_0 - w_1) - w_2$; $u_{32} \leftarrow 1$;	$I + 6M$
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		$2I + 23M$

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 $T_1 \equiv (F - V_1^2)/U_1 \bmod U_1$. $w_2 \leftarrow u_{11} - f_4$; $w_3 \leftarrow 2u_{10}$; $t_{10} \leftarrow u_{11}(2w_3 - u_{11}w_2 - f_3)$ $\quad -f_4w_3 + f_2 - w_1$; $t_{11} \leftarrow u_{11}(2w_2 + u_{11}) + f_3 - w_3$	$4M$
5	Compute $S \equiv I_1T_1 \bmod U_1$. (Karatsuba) $w_1 \leftarrow i_{10}t_{10}$; $w_2 \leftarrow i_{11}t_{11}$; $w_3 \leftarrow (i_{10} + i_{11})(t_{10} + t_{11}) - w_1 - w_2$; $S \leftarrow (w_3 - u_{11}w_2)X - u_{10}w_2 + w_1$;	$5M$
6	If $s_1 = 0$ then $\mathcal{D}_2$ should be weight one, and call the exclusive procedure.	—
7	Compute $U_2 = s_1^{-2}((SU_1 + V_1)^2 - F)/U_1^2$. $w_1 \leftarrow s_1^{-1}$; $u_{20} \leftarrow w_1(w_1(s_0^2 + 2u_{11} - f_4) + 2v_{11})$; $u_{21} \leftarrow w_1(2s_0 - w_1)$; $u_{22} \leftarrow 1$;	$I + 4M$
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		$2I + 25M$

速度

	P_1	$2P_1$	$P_1 + P_2$
P_1	$I + 5M$	$I + 11M$	$2I + 17M$
$-P_1$	0	$3M$	$3M$
P_2	$I + 3M$	$I + 10M$	$2I + 17M$
$2P_1$	$I + 11M$	$2I + 25M$	$4I + 34M$
$P_1 + P_2$	$2I + 17M$	$4I + 34M$	$2I + 25M$
$-P_1 + P_2$	$3M$	$2I + 13M$	$2I + 7M$
$P_1 + P_3$	$2I + 17M$	$4I + 34M$	$4I + 34M$
$-P_1 + P_3$	$3M$	$2I + 13M$	$2I + 13M$
$P_3 + P_4$	$I + 10M$	$2I + 23M$	$2I + 23M$

		改良前	改良後
加算	通常	$2I + 27M$	$2I + 23M$
	最悪	$(6I + 47M)$	$4I + 34M$
２倍算	通常	$2I + 30M$	$2I + 25M$
	最悪	$2I + 30M$	$2I + 25M$

Worst case

$\mathcal{D}_1 + \mathcal{D}_2$
$\mathcal{D}_1 = P_1 + P_2 - 2P_\infty,$
$\mathcal{D}_2 = P_1 + P_3 - 2P_\infty,$
$P_2 \neq P_3,$
P_1 : ramification pointでは無い

$$
\begin{aligned}
P_1 \in C(\mathbb{F}_{q^2}) \Rightarrow & P_2 = P_3 = P_1^\sigma \in C(\mathbb{F}_{q^2}) \\
& \quad \sigma : (x, y) \mapsto (x^q, y^q) \\
\Rightarrow & P_1 \in C(\mathbb{F}_q) \\
\Rightarrow & P_2, P_3 \in C(\mathbb{F}_q)
\end{aligned}
$$

$\therefore \#(\mathcal{D}_1, \mathcal{D}_2) = O(q^3)$

加算の組合せ: $O(q^4)$

Worst caseの起こる確率: $O(1/q)$

加算: $2I + 23M$

2倍算: $2I + 25M$

楕円曲線暗号との比較

比較対象: IEEE P1363方式(Jacobian Projective)
加算: $16M$, 2倍算: $10M$

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

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

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

定義体上の乗算コスト
$M \approx 2(\log q)^2$ (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
$\Rightarrow M_E \approx 4M_H$

	P1363	Harley改
加算	$16M_E = 64M_H$	$2I_H + 23M_H$
2倍算	$10M_E = 40M_H$	$2I_H + 25M_H$

整数倍算において
加算と2倍算が同数出現すると仮定すれば,

$$I_H < 14M_H \qquad (*)$$

のとき, 超楕円曲線のほうが楕円曲線より高速

通常, $(*)$は満たされる.

実装

超楕円曲線 : Harley改
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

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

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

使用言語　：C++
コンパイラ：gnu g++−2.95.2

	Genus two HEC	EC
加算	8.32μs.	11.6μs.
２倍算	8.74μs.	6.58μs.
整数倍算	1.98ms.	1.76ms.

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２割程度遅くなってしまった.
$\Rightarrow$
実装について検討する必要がある.

まとめ

- Harley アルゴリズムの改良を行った.
- 種数２の超楕円曲線暗号が
  楕円曲線暗号と同等の性能を持つことを示した.

- 超楕円曲線暗号の実装については一層の検討が必要

現状と今後

$g=2$

	A	D	
char $\mathbb{F}_q \neq 2$	$I+27M$	$I+27M$	(with 土井)
$= 2$	?	?	(with 杉崎)

$g=3$

	A	D	
char $\mathbb{F}_q \neq 2$	?	$2I+74M$	(with 黒木)