代数曲線暗号とその安全性

松尾 和人 (IISEC)

2007年8月23日
（2007年8月24日修正）

本講演の主旨

- 何故、代数曲線暗号なのか？
- 何故、種数１が利用されているのか？

内容：

1. 有限体上の離散対数問題とその解法
2. 楕円曲線暗号
3. 超楕円曲線暗号
4. 超楕円曲線上の離散対数問題の解法

Diffie-Hellman鍵共有アルゴリズム (1976)

システム設定	
p: 素数, $b \in \mathbb{F}_p^*$ (s.t. $\langle b \rangle = \mathbb{F}_p^*$)	
鍵ペア生成	
A さん	
秘密鍵設定	$K_a \in \mathbb{Z}/(p-1)\mathbb{Z}$
公開鍵計算	$K'_a = b^{K_a}$
	公開鍵 K'_a を公開
B さん	
秘密鍵設定	$K_b \in \mathbb{Z}/(p-1)\mathbb{Z}$
公開鍵計算	$K'_b = b^{K_b}$
	公開鍵 K'_b を公開
共通鍵計算	
A さん	$K = K_b'^{K_a}$
B さん	$K = K_a'^{K_b}$
同一の鍵 K を共有できた	

離散対数問題

- $K'_a \mapsto K_a$
- Given: p: prime, $b \in \mathbb{F}_p^*$, $a \in \langle b \rangle$
  Find: $x \in \mathbb{Z}/(p-1)\mathbb{Z}$ s.t. $a = b^x$
  $\mathrm{Ind}_b a := x$
- **容易：** $(x, b) \mapsto a = b^x$
  - $x = (x_{k-1}x_{k-2}\cdots x_1 x_0)_2$,
    $a = \prod_{0 \le i < k} b^{2^{x_i}}$,
    $n = O(\log p)$
- **困難：** $(a, b) \mapsto x$

離散対数問題の難しさ

- **全数探索**
  - $O(p)$
- Square-root**法** (Pollard**の** rho**法**)
  - $O\left(\sqrt{l}\right)$
  - l**：**$p-1$**の最大素因子**
- **指数計算法** (Adleman, 1979)
  - $L_x(\alpha, \beta) :=$
    $\exp\left(\beta(\log x)^{\alpha}(\log\log x)^{1-\alpha}\right)$
  - $O(L_p(1/2, 2 + o(1)))$
  - $O(L_p(1/3, 1.903 + o(1)))$

Pollardのρ法（原型）の実際

Given: $p = 47, a = 40, b = 11$

Find: $\mathrm{Ind}_b a$ i.e. x s.t. $a \equiv b^x \bmod p$

	1	2	3	4	5	6
α	35	36	17	9	3	17
β	3	41	15	0	28	14
$a^\alpha b^\beta \bmod p$	27	43	24	29	<u>30</u>	15

7	8	9	10
16	37	38	39
7	17	25	8
40	6	13	<u>30</u>

$a^3 b^{28} \equiv a^{39} b^8 \bmod p$

$\Rightarrow$

$a \equiv b^{(8-28)/(3-39)} \bmod p$

$\Rightarrow$

$x \equiv \frac{8-28}{3-39} \equiv \frac{20}{36} \equiv 21 \bmod p-1$

指数計算法の実際

Given: $p = 47, a = 40, b = 11$

Find: $\mathrm{Ind}_b a$ i.e. x s.t. $a \equiv b^x \bmod p$

因子基底：$B = \{2, 3, 5, 7, 11, 13\}$

$\#B$**個の**relation**：**

$$\begin{pmatrix} 11^{42} \\ 11^{3} \\ 11^{29} \\ 11^{11} \\ 11^{31} \\ 11^{1} \end{pmatrix} = \begin{pmatrix} 2 \\ 15 \\ 10 \\ 39 \\ 35 \\ 11 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \times 5 \\ 2 \times 5 \\ 3 \times 13 \\ 5 \times 7 \\ 11 \end{pmatrix}$$

$$= \begin{pmatrix} 11^{\mathrm{Ind}_{11} 2} \\ 11^{\mathrm{Ind}_{11} 3} \times 11^{\mathrm{Ind}_{11} 5} \\ 11^{\mathrm{Ind}_{11} 2} \times 11^{\mathrm{Ind}_{11} 5} \\ 11^{\mathrm{Ind}_{11} 3} \times 11^{\mathrm{Ind}_{11} 13} \\ 11^{\mathrm{Ind}_{11} 5} \times 11^{\mathrm{Ind}_{11} 7} \\ 11^{\mathrm{Ind}_{11} 11} \end{pmatrix}$$

$$\begin{pmatrix} 42 \\ 3 \\ 29 \\ 11 \\ 31 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \mathrm{Ind}_{11}2 \\ \mathrm{Ind}_{11}3 \\ \mathrm{Ind}_{11}5 \\ \mathrm{Ind}_{11}7 \\ \mathrm{Ind}_{11}11 \\ \mathrm{Ind}_{11}13 \end{pmatrix}$$

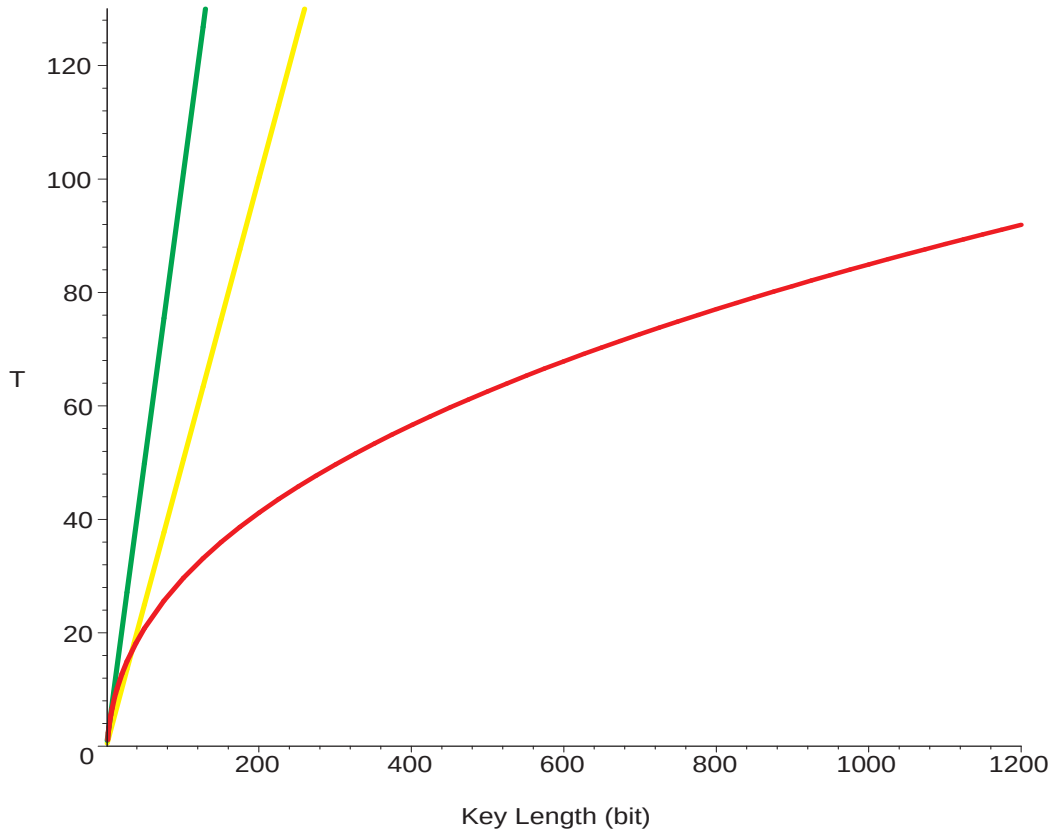
$$\begin{pmatrix} \mathrm{Ind}_{11}2 \\ \mathrm{Ind}_{11}3 \\ \mathrm{Ind}_{11}5 \\ \mathrm{Ind}_{11}7 \\ \mathrm{Ind}_{11}11 \\ \mathrm{Ind}_{11}13 \end{pmatrix} \equiv \begin{pmatrix} 42 \\ 16 \\ 33 \\ 44 \\ 1 \\ 41 \end{pmatrix} \mod p-1$$

$$\begin{aligned} 40 \times 11^{33} &\equiv 12 \\ &\equiv 2^2 \times 3 \mod p \end{aligned}$$

$\Rightarrow$

$$\begin{aligned} \mathrm{Ind}_{11}40 &\equiv 2\mathrm{Ind}_{11}2 + \mathrm{Ind}_{11}3 - 33 \\ &\equiv 2 \times 42 + 16 - 33 \\ &\equiv 21 \mod p-1 \end{aligned}$$

離散対数問題に必要な計算量



緑：全数探索

黄：Square-root法

赤：指数計算法的方法

安全な離散対数問題

- **離散対数問題の解読コスト**
  - p**のサイズに依存**
- 2^{80}**程度の手間はかけられない と考えられている**

$\Rightarrow$ 2^{80}**程度の手間が必要な**p**のサイズは？**

  - Square-root**法：**$\log_2 p \approx 160$
  - **指数計算法 ：**$\log_2 p \approx 1024$ (?)

- **将来は？(漸近計算量)：**
  - Square-root**法：**$\log_2 p$**の指数時間**
  - **指数計算法 ：**$\log_2 p$**の準指数時間**
- **何とかならないか？**
  - **離散対数問題の一般化**

離散対数問題の一般化 と代数曲線暗号

- **離散対数問題**
  - Given:
    G: **有限可換群**, $b \in G$, $a \in \langle b \rangle$
  - Find:
    $x \in \mathbb{Z}/\#G\mathbb{Z}$ s.t. $a = [x]b$

- Square-root**法は一般に適用可**:
  - $\sqrt{l}$, l**：**$\#G$**の最大素因子**

- **指数計算法が適用できない**G**はあるか？**

- **代数曲線暗号**
  - **有限体の乗法群上の離散対数問題 に基づく暗号アルゴリズムを （有限体上の）平面代数曲線上の 群構造を利用して実現したもの**

楕円曲線上の加算速度

$$E/\mathbb{F}_p : Y^2 = X^3 + a_4X + a_6$$

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$$

$$P_3 = (x_3, y_3) = P_1 + P_2$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + a_4}{2x_1} & \text{if } P_1 = P_2 \end{cases}$$

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

$\mathbb{F}_p$上の演算コスト:

$$ab:\ M = O((\log p)^2)$$

$$a + b,\ -a:\ O(\log p) \ll M$$

$$a^{-1} : I \approx 20M$$

加算： $I + 3M \approx 23M$

2倍算： $I + 4M \approx 24M$

楕円曲線暗号の速度

楕円曲線暗号の安全性

- $\#E(\mathbb{F}_p) = O(p)$
- Square-root**法のみ適用可**

  E**の適切な選択の下**:

  $O\left(\sqrt{\#E(\mathbb{F}_p)}\right) = O\left(\sqrt{p}\right)$

$\mathbb{F}_p^*$に対する指数計算法的方法と
$E(\mathbb{F}_p)$に対するsquare-root**法の計算量を**
考え合わせると

$\mathbb{F}_p^*$	$E(\mathbb{F}_p)$	Ratio
512	120?	4
1024	160?	6
2048	224?	9
3072	256?	12

現在では、
同一の安全性の下で、
楕円曲線暗号の方が高速

超楕円曲線暗号

$$C : Y^2 = F(X),$$
$$F(X) = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_0,$$
$$f_i \in \mathbb{F}_p$$

$$\mathcal{J}_C(\mathbb{F}_p) = \{D = \{P_1, \ldots, P_n \in$$
$$\cup_{1 \le k \le g} C(\mathbb{F}_{p^k}) \setminus \{P_\infty\}\} \mid 0 \le n \le g, D^p = D\}$$

$$\begin{aligned}\mathcal{J}_C(\mathbb{F}_p) \;=\; & \{(U, V) \in (\mathbb{F}_p[X])^2 \mid \\ & \mathsf{lc}(U) = 1, \\ & \deg V < \deg U \le g, \\ & U \mid F - V^2\}\end{aligned}$$

$$U = \prod_{1 \le i \le n} (X - x_i),\ y_i = V(x_i)$$

$$\#\mathcal{J}_C(\mathbb{F}_p) \approx p^g$$

因子類の加法公式

Input	Genus 2 HEC $C : Y^2 = F(X) = X^5 + f_3x^3 + f_2X^2 + f_1X + f_0$, Weight two coprime reduced divisors $D_1 = (U_1, V_1), D_2 = (U_2, V_2)$	
Output	A weight two reduced divisor $D_3 = (U_3, V_3) = D_1 + D_2$	

Step	Procedure	Cost
1	Compute the resultant r of U_1 and U_2. $z_1 \leftarrow u_{21} - u_{11}$; $z_2 \leftarrow u_{21}z_1$; $z_3 \leftarrow z_2 + u_{10} - u_{20}$; $r \leftarrow u_{10}(z_3 - u_{20}) + u_{20}(u_{20} - u_{11}z_1)$;	$4M$
2	If $r = 0$ then call the sub procedure.	—
3	Compute $I_1 \equiv 1/U_1 \bmod U_2$. $w_0 \leftarrow r^{-1}$; $i_{11} \leftarrow w_1z_1$; $i_{10} \leftarrow w_1z_3$;	$I + 2M$
4	Compute $S \equiv (V_2 - V_1)I_1 \bmod U_2$. (Karatsuba) $w_1 \leftarrow v_{20} - v_{10}$; $w_2 \leftarrow v_{21} - v_{11}$; $w_3 \leftarrow i_{10}w_1$; $w_4 \leftarrow i_{11}w_2$; $s_1 \leftarrow (i_{10} + i_{11})(w_1 + w_2) - w_3 - w_4(1 + u_{21})$; $s_0 \leftarrow w_3 - u_{20}w_4$;	$5M$
5	If $s_1 = 0$ then call the sub procedure.	—
6	Compute $U_3 = s_1^{-2}((S^2U_1 + 2SV_1)/U_2 - (F - V_1^2)/(U_1U_2))$. $w_1 \leftarrow s_1^{-1}$; $u_{30} \leftarrow w_1(w_1(s_0^2 + u_{11} + u_{21}) + 2(v_{11} - s_0w_2)) + z_2 + u_{10} - u_{20}$; $u_{31} \leftarrow w_1(2s_0 - w_1) - w_2$; $u_{32} \leftarrow 1$;	$I + 5M$
7	Compute $V_3 \equiv -(SU_1 + V_1) \bmod U_3$.(Karatsuba) $w_1 \leftarrow u_{30} - u_{10}$; $w_2 \leftarrow u_{31} - u_{11}$; $w_3 \leftarrow s_1w_2$; $w_4 \leftarrow s_0w_1$; $w_5 \leftarrow (s_1 + s_0)(w_1 + w_2) - w_3 - w_4$ $v_{30} \leftarrow w_4 - w_3u_{30} - v_{10}$; $v_{31} \leftarrow w_5 - w_3u_{31} - v_{11}$;	$5M$
Total		$2I + 21M$

In.	Genus 3 HEC $C : Y^2 = F(X) = X^7 + f_5X^5 + f_4X^4 + f_3x^3 + f_2X^2 + f_1X + f_0$, Reduced divisors $\mathcal{D}_1 = (U_1, V_1)$, $\mathcal{D}_2 = (U_2, V_2)$, where $U_1 = X^3 + u_{12}X^2 + u_{11}X + u_{10}$, $V_1 = v_{12}X^2 + v_{11}X + v_{10}$, $U_2 = X^3 + u_{22}x^2 + u_{21}X + u_{20}$, and $V_2 = v_{22}X^2 + v_{21}X + v_{20}$	
Out.	Reduced divisor $\mathcal{D}_O = (U_O, V_O) = \mathcal{D}_1 + \mathcal{D}_2$, where $U_O = X^3 + u_{O2}X^2 + u_{O1}X + u_{O0}$, and $V_O = v_{O2}X^2 + v_{O1}X + v_{O0}$	

Step	Procedure	Cost
1	[Compute the resultant r of U_1 and U_2] $t_0 = u_{10} - u_{20}$; $t_1 = u_{11} - u_{21}$; $t_2 = u_{12} - u_{22}$; $t_3 = t_1 - u_{22}t_2$; $t_4 = t_0 - u_{21}t_2$; $t_5 = t_4 - u_{22}t_3$; $t_6 = u_{20}t_2 + u_{21}t_3$; $t_7 = t_4t_5 + t_3t_6$; $t_8 = -(t_2t_6 + t_1t_5)$; $t_9 = t_1t_3 - t_2t_4$; $r = u_{20}(t_3t_9 + t_2t_8) - t_0t_7$;	$15M$
2	[If $r = 0$ then call the Cantor algorithm]	–
3	[Compute the pseudo-inverse $I = i_2x^2 + i_1x + i_0 \equiv r/U_1 \bmod U_2$] $i_2 = t_9$; $i_1 = t_8$; $i_0 = t_7$;	–
4	[Compute $S' = s'_2x^2 + s'_1x + s'_0 = rS \equiv (V_2 - V_1)I \bmod U_2$ (Karatsuba, Toom)] $t_1 = v_{10} - v_{20}$; $t_2 = v_{11} - v_{21}$; $t_3 = v_{12} - v_{22}$; $t_4 = t_2i_1$; $t_5 = t_1i_0$; $t_6 = t_3i_2$; $t_8 = u_{22}t_6$; $t_8 = t_4 + t_6 + t_7 - (t_2 + t_3)(i_1 + i_2)$; $t_9 = u_{20} + u_{22}$; $t_{10} = (t_9 + u_{21})(t_8 - t_6)$; $t_9 = (t_9 - u_{21})(t_8 + t_6)$; $s'_0 = -(u_{20}t_8 + t_5)$; $s'_2 = t_6 - (s'_0 + t_4 + (t_1 + t_3)(i_0 + i_2) + (t_{10} + t_9)/2)$; $s'_1 = t_4 + t_5 + (t_9 - t_{10})/2 - (t_7 + (t_1 + t_2)(i_0 + i_1))$;	$10M$
5	[If $s'_2 = 0$ then call the Cantor algorithm]	–
6	[Compute S, w and $w_i = 1/w$ s.t. $wS = S'/r$ and S is monic] $t_1 = (rs'_2)^{-1}$; $t_2 = rt_1$; $w = t_1{s'_2}^2$; $w_i = rt_2$; $s_0 = t_2s'_0$; $s_1 = t_2s'_1$;	$I + 7M$
7	[Compute $Z = X^5 + z_4X^4 + z_3X^3 + z_2X^2 + z_1X + z_0 = SU_1$] $t_6 = s_0 + s_1$; $t_1 = u_{10} + u_{12}$; $t_2 = t_6(t_1 + u_{11})$; $t_3 = (t_1 - u_{11})(s_0 - s_1)$; $t_4 = u_{12}s_1$; $z_0 = u_{10}s_0$; $z_1 = (t_2 - t_3)/2 - t_4$; $z_2 = (t_2 + t_3)/2 - z_0 + u_{10}$; $z_3 = u_{11} + s_0 + t_4$; $z_4 = u_{12} + s_1$;	$4M$
8	[Compute $U_t = X^4 + u_{t3}X^3 + u_{t2}X^2 + u_{t1}X + u_{t0} = (S(Z + 2w_iV_1) - w_i^2((F - V_1^2)/U_1))$] $t_1 = s_0z_3$; $u_{t3} = z_4 + s_1 - u_{22}$; $t_5 = s_1z_4 - u_{22}u_{t3}$; $u_{t2} = z_3 + s_0 + t_5 - u_{21}$; $t_3 = u_{21}u_{t2}$; $t_4 = t_1 - t_3$; $t_2 = (u_{22} + u_{21})(u_{t3} + u_{t2})$; $u_{t2} = z_3 + s_0 + t_5 - u_{21}$; $u_{t1} = z_2 + t_6(z_4 + z_3) + w_i(2v_{12} - w_i) - (t_5 + t_2 + t_4 + u_{20})$; $u_{t0} = z_1 + t_4 + s_1z_2 + w_i(2(v_{11} + s_1v_{12}) + w_iu_{12}) - (u_{22}u_{t1} + u_{20}u_{t3})$;	$13M$
9	[Compute $V_t = v_{t2}X^2 + v_{t1}X + v_{t0} \equiv wZ + V_1 \bmod U_t$] $t_1 = u_{t3} - z_4$; $v_{t0} = w(t_1u_{t0} + z_0) + v_{10}$; $v_{t1} = w(t_1u_{t1} + z_1 - u_{t0}) + v_{11}$; $v_{t2} = w(t_1u_{t2} + z_2 - u_{t1}) + v_{12}$; $v_{t3} = w(t_1u_{t3} + z_3 - u_{t2})$	$8M$
10	[Compute $U_O = X^3 + u_{O2}X^2 + u_{O1}X + u_{O0} = (F - V_t^2)/U_t$] $t_1 = 2v_{t3}$; $u_{O2} = -(u_{t3} + v_{t3}^2)$; $u_{O1} = f_5 - (u_{t2} + u_{O2}u_{t3} + t_1v_{t2})$; $u_{O0} = f_4 - (u_{t1} + v_{t2}^2 + u_{O2}u_{t2} + u_{O1}u_{t3} + t_1v_{t1})$;	$7M$
11	[Compute $V_O = v_{O2}x^2 + v_{O1}x + v_{O0} \equiv -V_t \bmod U_O$] $v_{O2} = v_{t2} - u_{O2}v_{t3}$; $v_{O1} = v_{t1} - u_{O1}v_{t3}$; $v_{O0} = v_{t0} - u_{O0}v_{t3}$;	$3M$
Total		$I + 67M$

超楕円暗号の速度

- **超楕円暗号の安全性**
  - Square-root**法のみ適用可** (?)
    C**の適切な選択の下**:
    $O\left(\sqrt{\#\mathcal{J}_C(\mathbb{F}_p)}\right) = O(\sqrt{p^g})$
- **解読に**2^{80}**程度の手間がかかる**$p \approx 2^{160/g}$
  - $g = 1$**:** $p \approx 2^{160}$
  - $g = 2$**:** $p \approx 2^{80}$
  - $g = 3$**:** $p \approx 2^{54}$
- **群演算一回あたりのコスト**
  - $g = 1$**:** $I_{160} + 3M_{160} = 23M_{160}$
  - $g = 2$**:** $I_{80} + 25M_{80} = 45M_{80}$
  - $g = 3$**:** $I_{54} + 67M_{54} = 87M_{54}$

$\Rightarrow 23M_{160} > 45M_{80} > 87M_{54}$ (?)

超楕円曲線上の離散対数問題に対する指数計算法

- Adleman-DeMarrais-Huang (1991)
  - **因子基底：素数** $< s \rightarrow \deg U < s$
  - **計算量**: $O(L_{p^{2g+1}}(1/2, c < 2.181))$,
    $\log p < (2g+1)^{0.98}$, $g \rightarrow \infty$
  - **改良の計算量**: $O(L_{p^g}(1/2, *))$,
    $p^g \rightarrow \infty$
    Enge, Gaudry-Enge

  $\Rightarrow$ **種数の大きな曲線は暗号利用不可**
- Gaudry (1997)
  - **因子基底：**$\deg U = 1$ i.e. $C(\mathbb{F}_p)$
  - **計算量**: $O(p^2)$
  - **改良の計算量**: $O(p^{2-2/g})$
    Gaudry-Harley, Thériault, Nagao,
    Gaudry-Thomé-Thériault-Diem

Gaudryの指数計算法（簡易版）

$p = 7$

$$C/\mathbb{F}_p : Y^2 = X^{13} + 5X^{12} + 4X^{11} + 6X^9 + 2X^8 + 6X^7 + 5X^4 + 5X^3 + X^2 + 2X + 6$$

$\#\mathcal{J}_C(\mathbb{F}_p) = 208697$: 18 bit **素数**

$$D_a = (X^6+2X^5+4X^4+X^3+5X^2+3,\ 4X^5+5X^3+2X^2+5X+4)$$

$$D_b = (X^5+6X^3+3X^2+1,\ 3X^4+X^3+4X^2+X+3)$$

Find $\mathrm{Ind}_{D_b} D_a$ s.t. $D_a = [\mathrm{Ind}_{D_b} D_a] D_b$.

$C(\mathbb{F}_p) = \{P_\infty, (1,1), (1,6), (2,1), (2,6), (4,1), (4,6)(5,3), (5,4), (6,3), (6,4)\}$

$\#C(\mathbb{F}_p) = 11$

因子基底：

$B = \{(1,1), (2,1), (4,1), (5,3), (6,3)\}$

$[9343]D_b = ($
$X^5+6X^4+6X^3+5X^2+6X+4,$
$X^4+X^3+X^2+4X+6)$

$X^5+6X^4+6X^3+5X^2+6X+4 = (X-1)^2(X-4)^2(X-5)$

$$X^4+X^3+X^2+4X+6\ |_{X=1} = 6$$

$$X^4+X^3+X^2+4X+6\ |_{X=4} = 1$$

$$X^4+X^3+X^2+4X+6\ |_{X=5} = 3$$

$\Rightarrow$

$[9343]D_b = -[2](1,1) + [2](4,1) + (5,3)$

$$\begin{pmatrix} [9343]D_b \\ [120243]D_b \\ [121571]D_b \\ [120688]D_b \\ [151649]D_b \end{pmatrix} =$$

$$\begin{pmatrix} -2 & 0 & 2 & 1 & 0 \\ 0 & -2 & 1 & 1 & -2 \\ -1 & 0 & 2 & -1 & -1 \\ 2 & 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} (1,1) \\ (2,1) \\ (4,1) \\ (5,3) \\ (6,3) \end{pmatrix}$$

$$\begin{pmatrix} \mathsf{Ind}_{D_b}(1,1) \\ \mathsf{Ind}_{D_b}(2,1) \\ \mathsf{Ind}_{D_b}(4,1) \\ \mathsf{Ind}_{D_b}(5,3) \\ \mathsf{Ind}_{D_b}(6,3) \end{pmatrix} \equiv \begin{pmatrix} 85159 \\ 114347 \\ 182999 \\ 22360 \\ 136908 \end{pmatrix}$$

$$\mathsf{mod}\ \#\mathcal{J}_C(\mathbb{F}_p)$$

$$D_a + [105454]D_b =$$
$$(1,1) + [2](2,1) + (4,1) - (6,3)$$

$$\begin{aligned} \mathsf{Ind}_{D_b} D_a &\equiv \mathsf{Ind}_{D_b}(1,1) + 2\mathsf{Ind}_{D_b}(2,1) \\ &\quad + \mathsf{Ind}_{D_b}(4,1) - \mathsf{Ind}_{D_b}(6,3) \\ &\quad - 105454 \\ &\equiv 85159 + 2 \times 114347 \\ &\quad + 182999 - 136908 \\ &\quad - 105454 \\ &\equiv 45793 \bmod \#\mathcal{J}_C(\mathbb{F}_p) \end{aligned}$$

計算量評価

$$\begin{pmatrix} [9343]D_b \\ [120243]D_b \\ [121571]D_b \\ [120688]D_b \\ [151649]D_b \end{pmatrix} = \begin{pmatrix} \cdots \\ \cdots \\ \vdots \\ \cdots \end{pmatrix} \begin{pmatrix} (1,1) \\ (2,1) \\ (4,1) \\ (5,3) \\ (6,3) \end{pmatrix}$$

- $\#B = O(p)$
- **一行を得るために必要な試行回数**
  - g **次モニック多項式の数**: $O(p^g)$
  - 1 **次式の積に分解する**
    g **次モニック多項式の数**: $O(p^g/g!)$

  $\Rightarrow O(g!)$
- Jacobian **上の加算**: $O(g^2(\log p)^2)$
- **多項式の因数分解**: $O(g^3(\log p)^3)$

$\Rightarrow O(g!g^3p(\log p)^3)$

Gaudry の指数計算の計算量

疎行列の線形代数:

$O(gp^2(\log \#\mathcal{J}_C(\mathbb{F}_p))^2) = O(g^3p^2(\log p)^2)$

トータル：

$O(g!g^3p(\log p)^3) + O(g^3p^2(\log p)^2)$

小種数曲線に対しては $\tilde{O}(p^2)$ **と考えられる**

一方、種数 g **の曲線に対する** rho **法の計算量：**

$\tilde{O}(\sqrt{\#\mathcal{J}_C(\mathbb{F}_p)}) = \tilde{O}(p^{g/2})$

$\therefore$ **種数が** 4 **を越える曲線に対して、**
rho **より速くなる可能性有**

アルゴリズムの最適化

発想 (Gaudry-Harley)：

行列作成と線形代数の計算量のバランスをとる

$\Rightarrow$

因子基底をより小さく取る

$\#B = O(p^r),\ 0 < r < 1$ **とする**

$\tilde{O}(p) + \tilde{O}(p^2) \rightarrow$

$\tilde{O}\left(\frac{p^g}{p^{rg}} p^r\right) + \tilde{O}\left(p^{2r}\right) = \tilde{O}\left(p^{g+(1-g)r} + p^{2r}\right)$

$r = \frac{g}{g+1} \Rightarrow$

$\tilde{O}\left(p^{g+(1-g)r} + p^{2r}\right) = \tilde{O}\left(p^{2g/(g+1)}\right)$

種数が3**を越える曲線に対して、**
rho**より速くなる可能性有**

Large primesの利用

計算量最適化の結果利用しなくなった
リレーションの再利用：

$B = \{(1,1),(2,1),(4,1)\}$

$B_L = \{(5,3),(6,3)\}$

$$\begin{pmatrix} [9343]D_b \\ [120243]D_b \\ [121571]D_b \\ [120688]D_b \\ [151649]D_b \end{pmatrix} = \begin{pmatrix} -2 & 0 & 2 & 1 & 0 \\ 0 & -2 & 1 & 1 & -2 \\ -1 & 0 & 2 & -1 & -1 \\ 2 & 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} (1,1) \\ (2,1) \\ (4,1) \\ (5,3) \\ (6,3) \end{pmatrix}$$

計算量を最適化するとこれらは利用できなくなる。しかし、実際には

$$[2 \times 9343 - 120688]D_a = [-6](1,1) + [-1](2,1) + [4](4,1)$$

が得られる (Thériault, single large prime)

さらに、

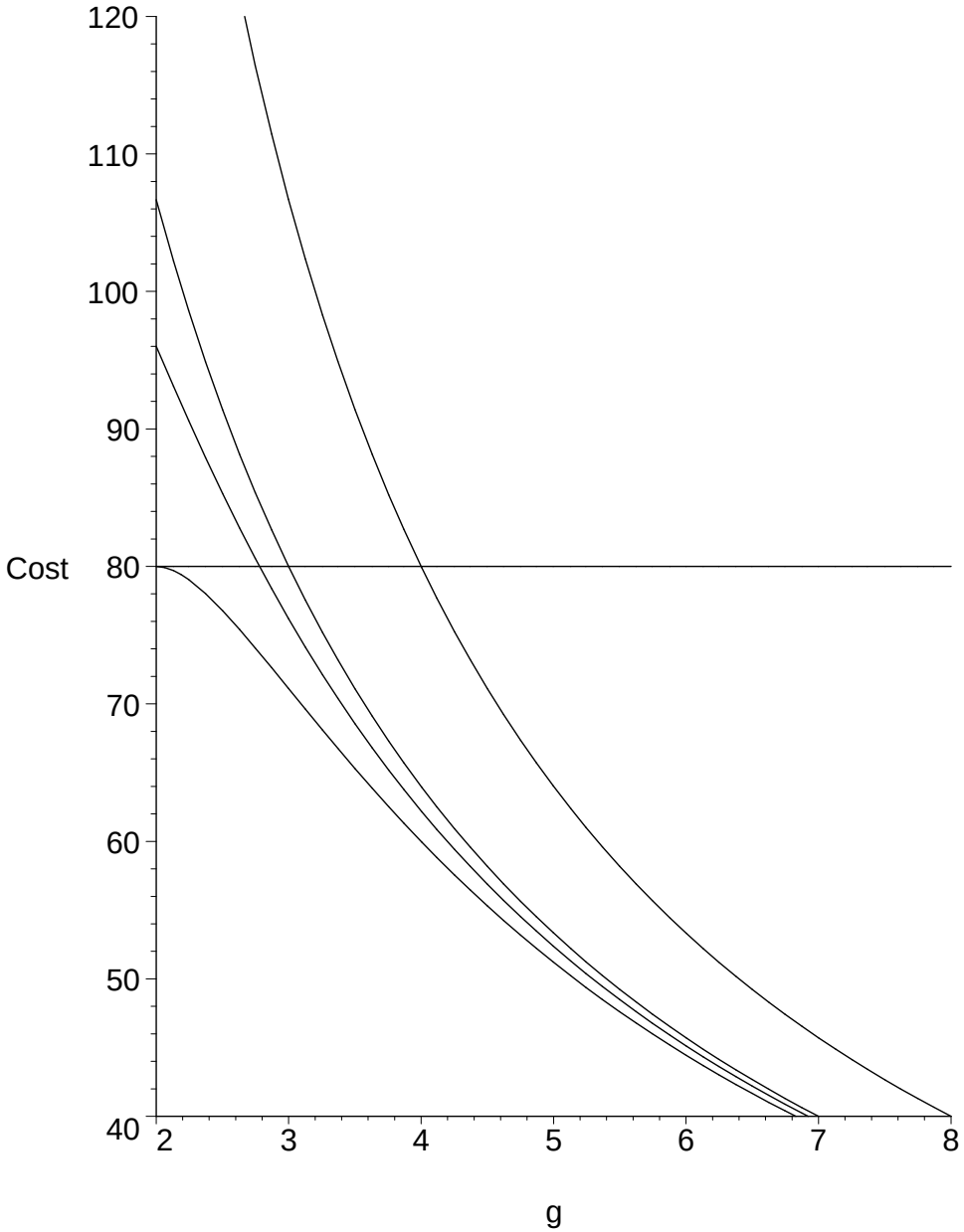
$$[121571 + 151649]D_a = [3](4,1) + [-3](5,3)$$

等が得られる

(Nagao and GTTD, double large prime)

超楕円暗号の安全性

- **準指数時間計算量ではなく指数時間計算量**
- g **により効果が異なる**



その他の結果

- Non-hyper (degree d plane curves)
  - Diem **のアルゴリズム**
    - $\tilde{O}\left(p^{2-2/(d-2)}\right)$
  - **準指数時間アルゴリズム**
    - $O\left(L_{p^g}(1/3, *)\right)$
      (Enge-Gaudry, Diem)
- $C/\mathbb{F}_{p^n}$
  - Weil descent attack
    - **種数のより大きな曲線** $/\mathbb{F}_p$
      上で指数計算法を適用
  - Generalized Weil descent attack
    - $\tilde{O}\left(p^{2-1/(ng)}\right)$?
      (Semaev, Gaudry, Nagao)

研究課題

- **高速化**
- **安全な曲線の構成**
- **攻撃**
- **暗号プロトコル** (Pairing**ベース暗号**)