超楕円曲線上の公開鍵暗号

情報セキュリティ大学院大学
松尾和人

2008年9月29日

♣ 離散対数問題の一般化 ♣

- **離散対数問題**
  - p: **素数**, $b, y \in \{1, \ldots, p-1\}$
  - $y \equiv b^x \bmod p$, $x \in \{0, \ldots, p-2\}$

$$\Downarrow$$

- **（有限体の乗法群上の）離散対数問題**
  - $b, y \in \mathbb{F}_p^*$
  - $y = b^x$, $x \in \{0, \ldots, \#\mathbb{F}_p^* - 1\}$

$$\Downarrow$$

- **離散対数問題**
  - G: **有限可換群**, $b, y \in G$
  - $y = xb = \underbrace{b + b + \cdots + b}_{x\text{個}}$,
    $x \in \{0, \ldots, \#G - 1\}$

♣ 楕円曲線暗号 ♣

- Square-root **法は一般に適用可**: $\sqrt{\#G}$
- **有限可換群**G**の中で指数計算法**
  が適用できないものはあるか？

$\Rightarrow$ **代数曲線から可換群を構成可能**

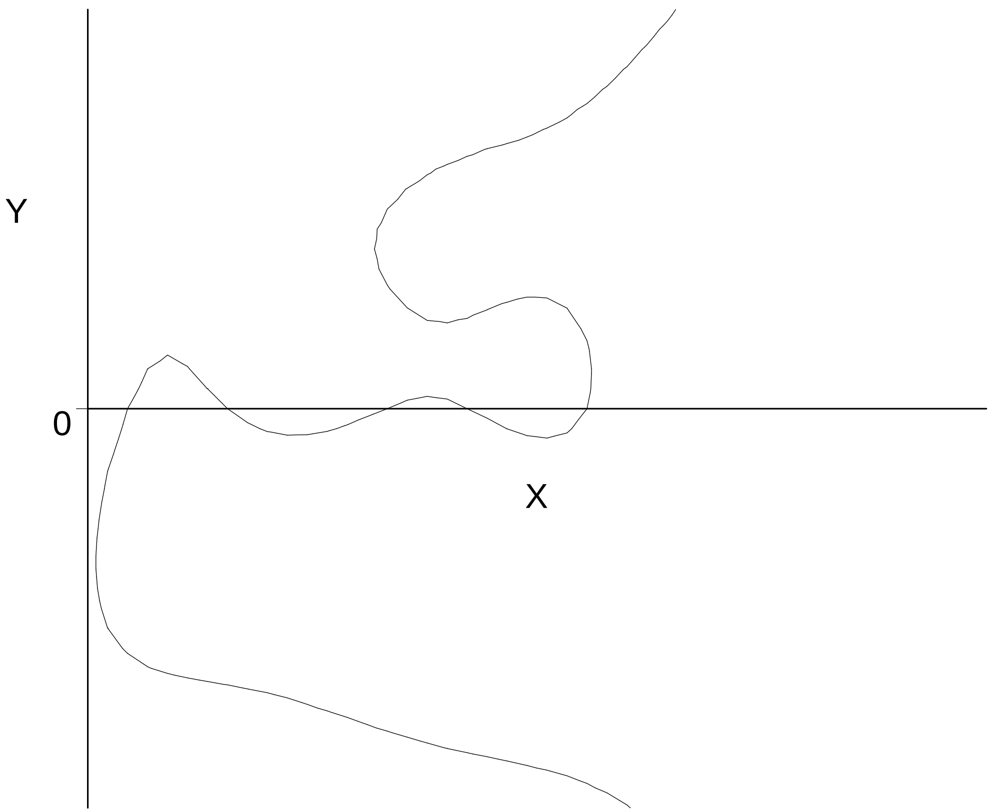
$\Rightarrow$ **楕円曲線暗号：**
有限体の乗法群上の
離散対数問題に基づく暗号アルゴリズムを
（有限体上の）楕円曲線の
群構造を利用して実現したもの

$\leftarrow$ **楕円曲線上の離散対数問題には**
指数計算法を適用できない

♣ 代数曲線の例 ♣

$$C : Y^4 + Y - XY^2 - X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X^2 + f_0 = 0,$$

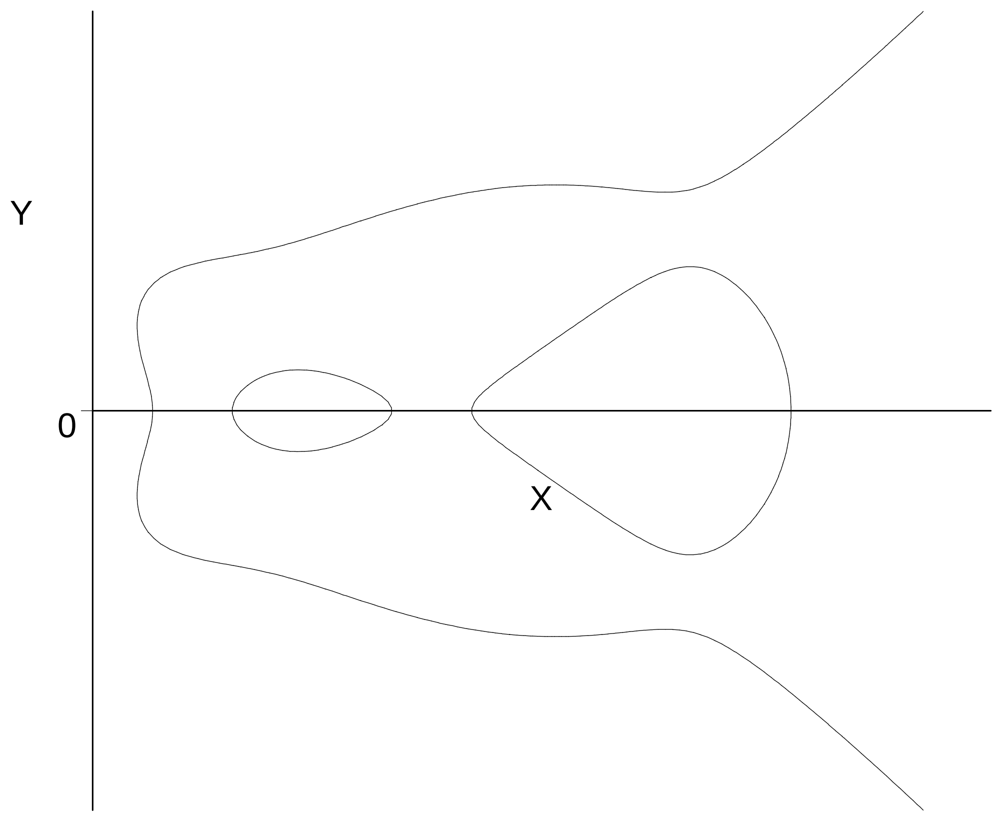
$$f_i \in \mathbb{F}_p$$



♣ 代数曲線の例 ♣

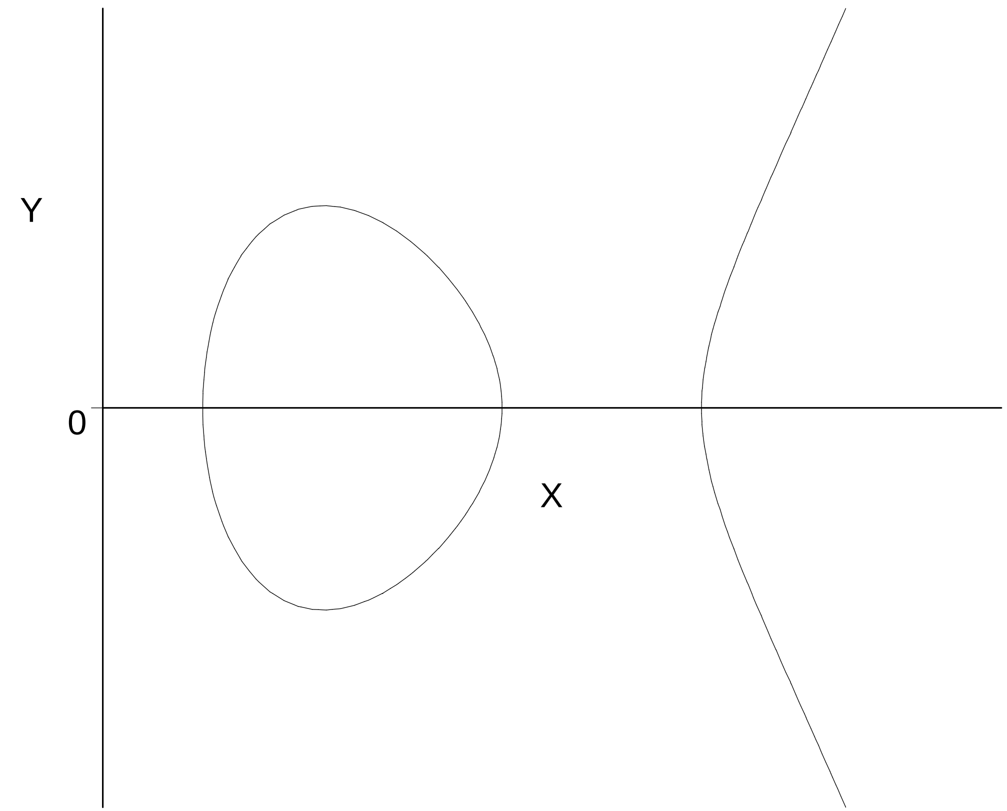
$$C : Y^4 - 1/2XY^2 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0 = 0,$$

$$f_i \in \mathbb{F}_p$$



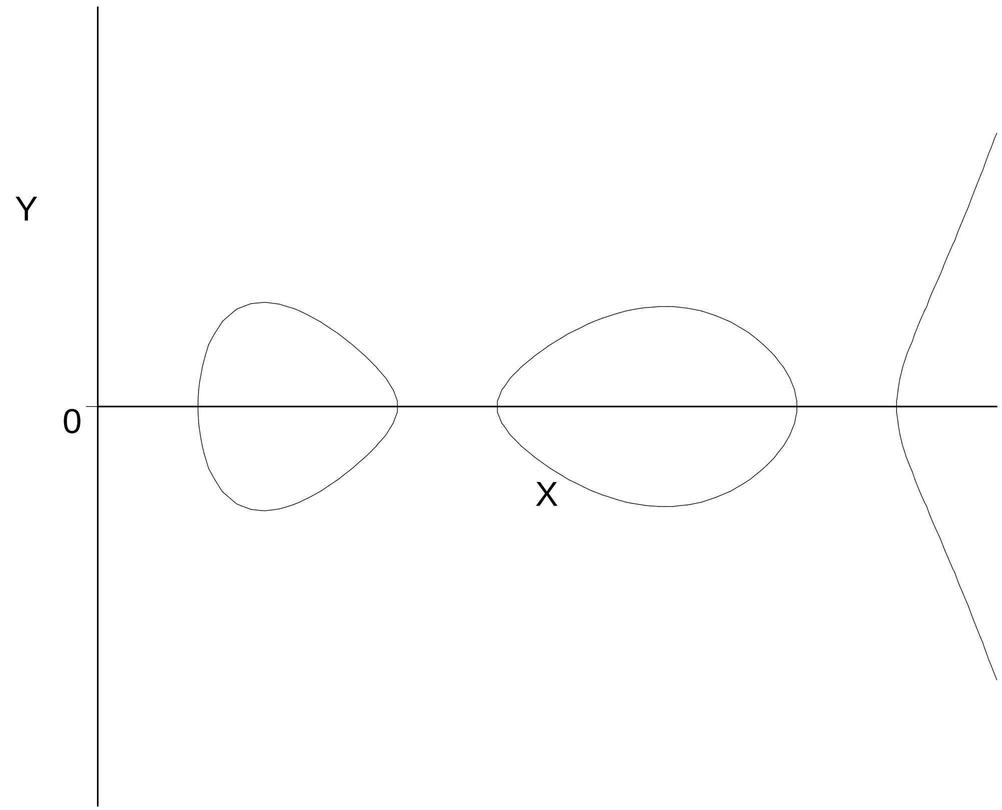
♣ 楕円曲線 ♣

$$E \; : \; Y^2 \; = \; X^3 + a_4 X + a_6, a_i \; \in \; \mathbb{F}_p$$



♣ 種数 g の超楕円曲線 ♣

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



♣ 超楕円曲線上の群構造 ♣

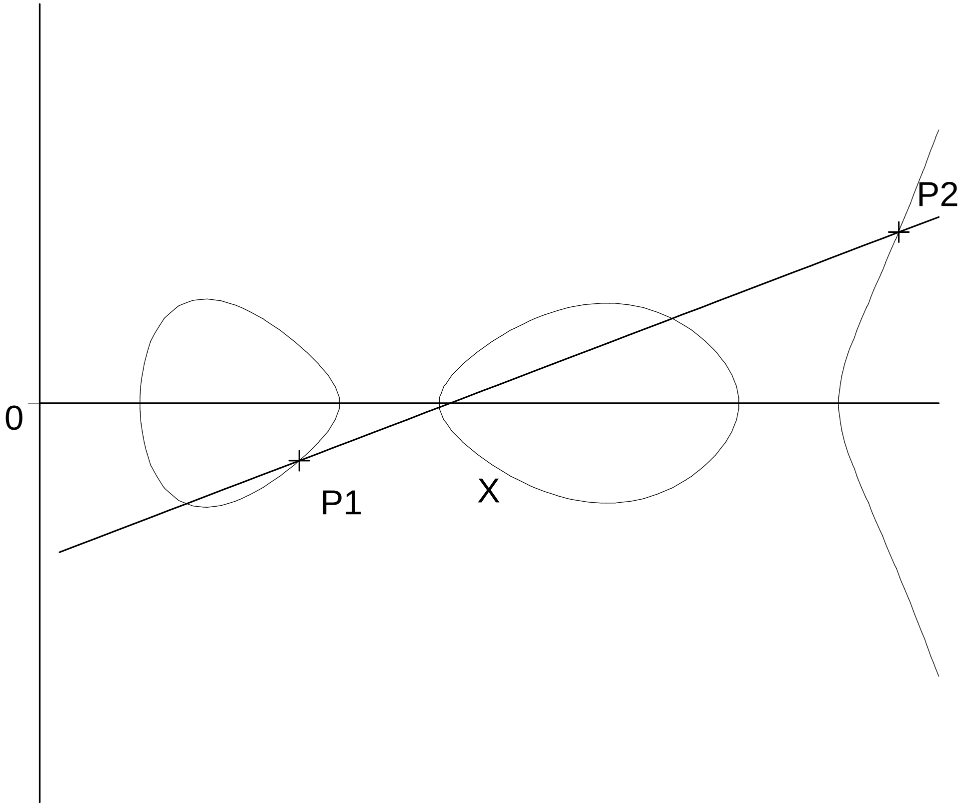
$$C : Y^2 = F(X)$$

$$\downarrow$$

$$C(\mathbb{F}_p) := \{P = (x, y) \in \mathbb{F}_p^2 \mid y^2 = F(x)\} \cup \{P_\infty\}$$

$$\downarrow$$

$C(\mathbb{F}_p)$ **は群構造を持たない**



♣ 超楕円曲線上の群構造 ♣

$$C : Y^2 = F(X)$$

$$\downarrow$$

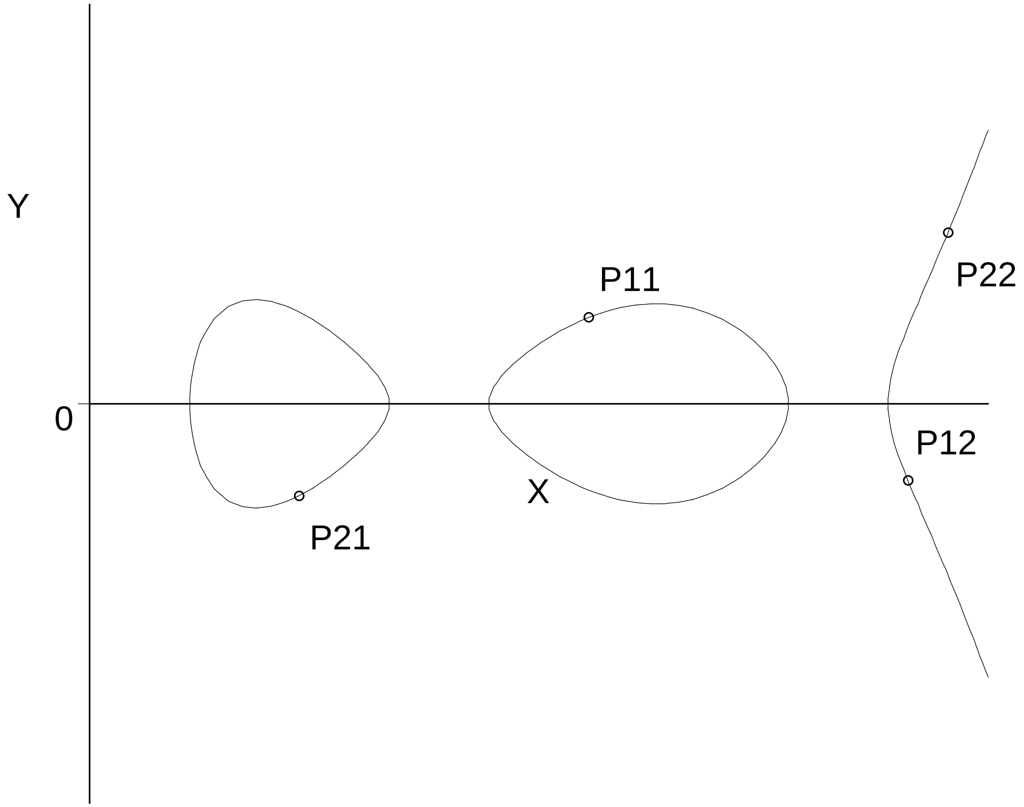
$$J_C(\mathbb{F}_p) := \left\{D = \{P_1, \ldots, P_n \in C(\overline{\mathbb{F}}_p) \setminus \{P_\infty\}\} \mid n \le g, D^p = D\right\}$$

$$\downarrow$$

$J_C(\mathbb{F}_p)$ **は有限可換群**

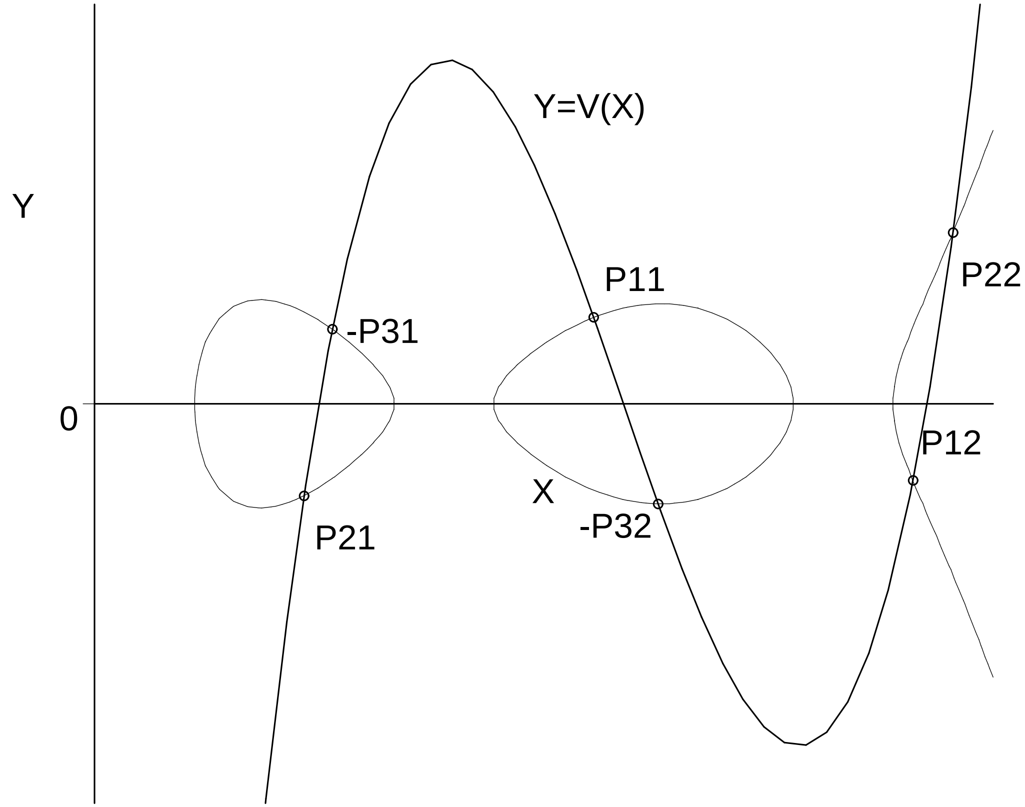
♣ 超楕円曲線上の加算 ($g=2$) ♣

$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$



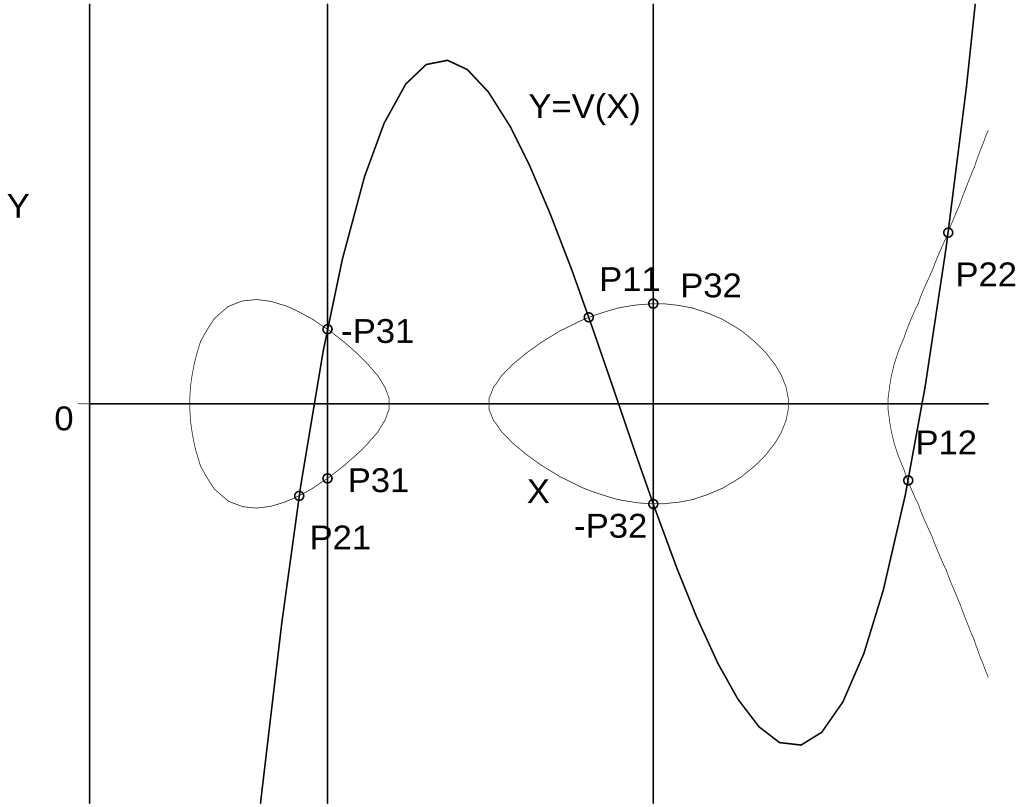
♣ 超楕円曲線上の加算 ($g=2$) ♣

$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$



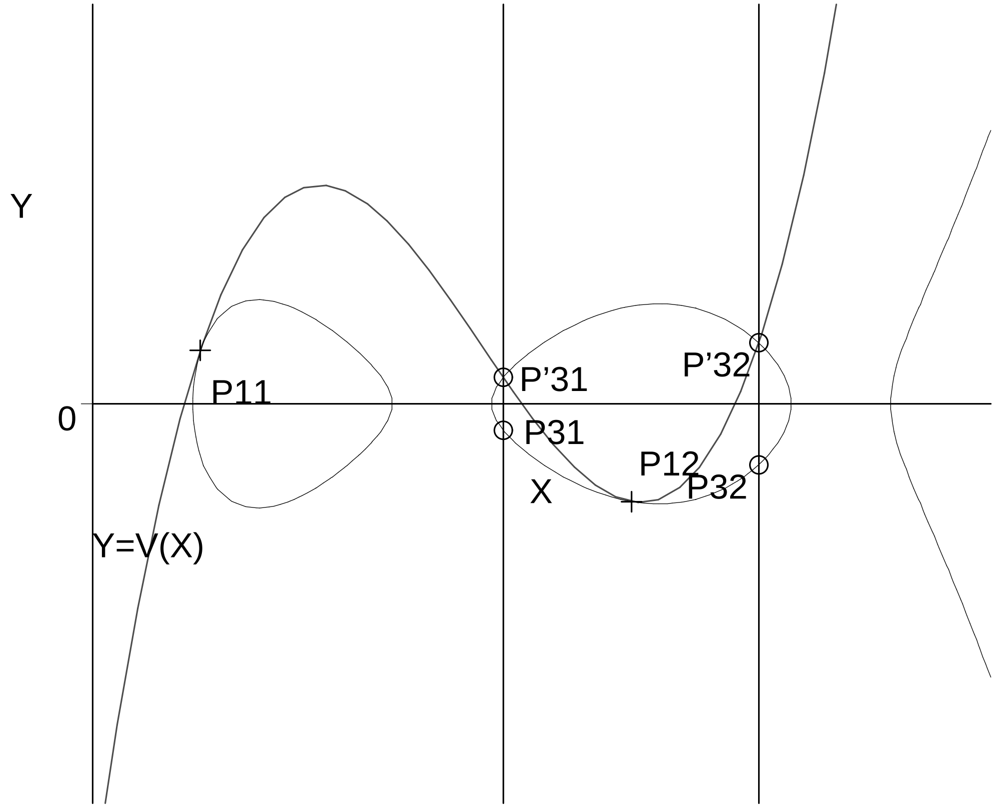
♣ 超楕円曲線上の加算 ($g = 2$) ♣

$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$



♣ 超楕円曲線上の２倍算 ($g = 2$) ♣

$$D_3 = D_1 + D_1,\ D_i = \{P_{i1}, P_{i2}\}$$



♣ Mumford表現 ♣

$$C : Y^2 = F(X),\ F(X) \in \mathbb{F}_p[X],$$
$$\deg F = 2g+1$$

$$D = \{P_1, \ldots, P_n \in C(\overline{\mathbb{F}}_p) \setminus \{P_\infty\}\},$$
$$n \le g, D^p = D, P_i = (x_i, y_i)$$

$$\Downarrow$$

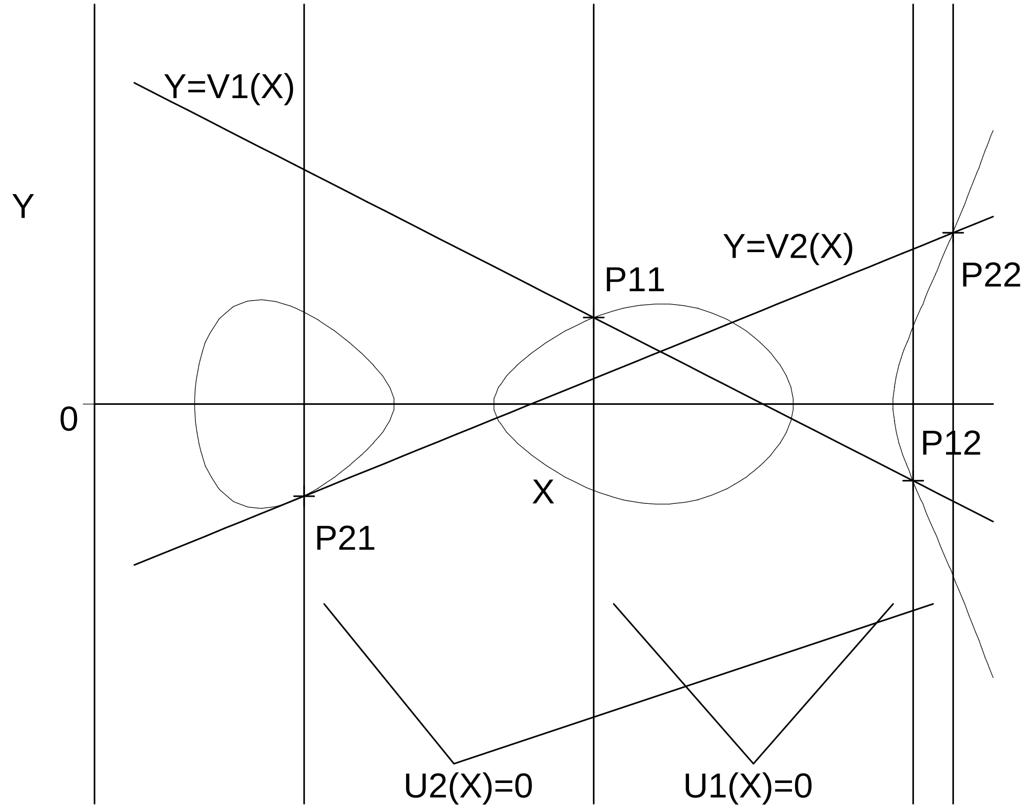
$$\begin{aligned} {}^{\exists 1}(U,V) \ \in \ & (\mathbb{F}_p[X])^2 \text{ s.t.} \\ & g \ge \deg U > \deg V, \\ & U = \prod_{1\le i\le n} (X - x_i), \\ & U \mid F - V^2, \\ & y_i = V(x_i). \end{aligned}$$

$$\Downarrow$$

$$J_C(\mathbb{F}_p) := \Big\{D = (U,V) \in \mathbb{F}_p[X]^2 \mid U\text{: monic} \quad g \ge \deg U > \deg V, U \mid F - V^2\Big\}$$

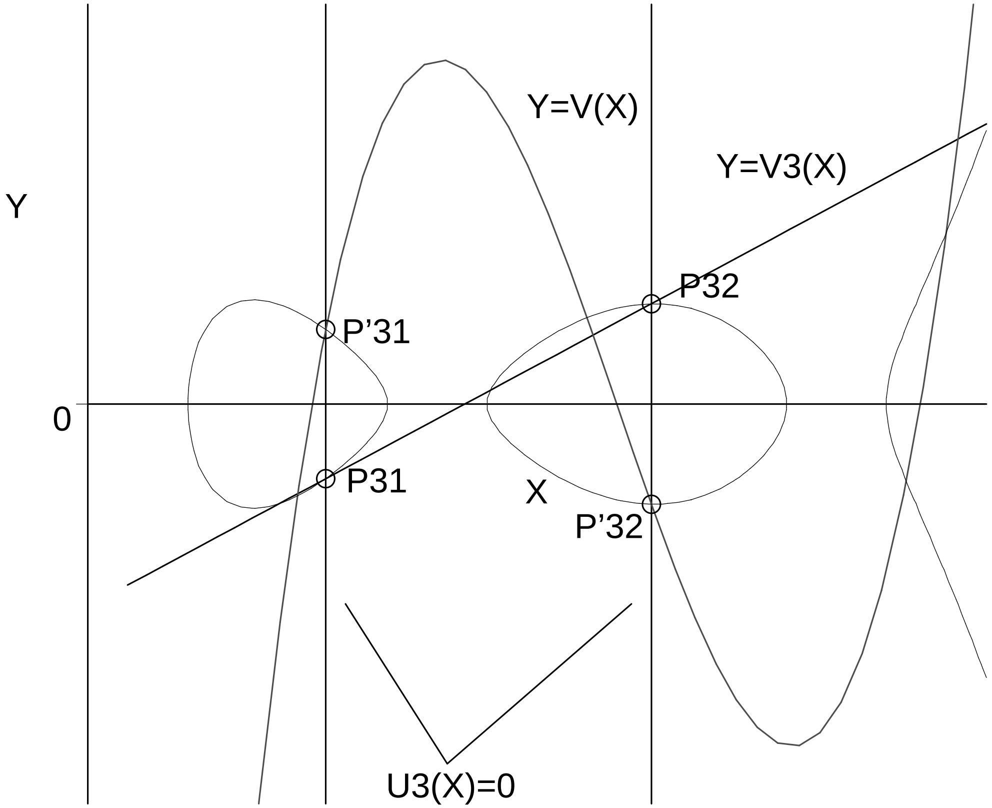
♣ 超楕円曲線上の加算 ($g=2$) ♣

$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$

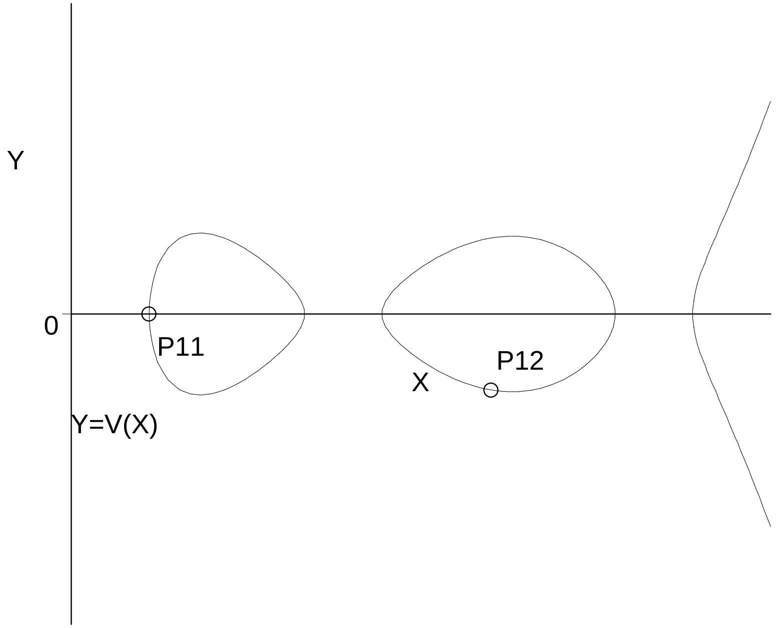


♣ 超楕円曲線上の加法公式 ($g = 2$) ♣

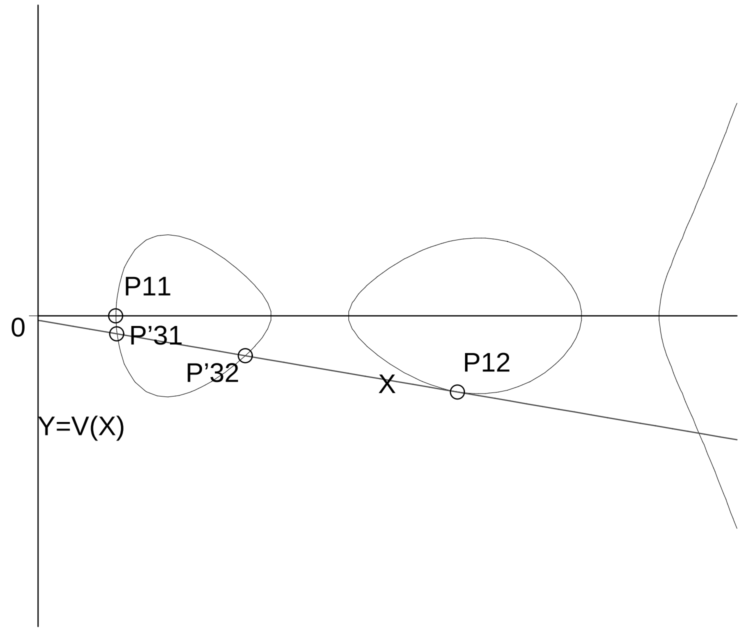
$$D_3 = D_1 + D_2,\ D_i = \{P_{i1}, P_{i2}\}$$



♣ 特殊ケース ♣



↓



♣ Cantor アルゴリズム ♣

アルゴリズム 1 半被約因子の加算

入力: 超楕円曲線 C: $Y^2 = F$，半被約因子 $D_1 = (U_1, V_1)$，$D_2 = (U_2, V_2)$

出力: 半被約因子 $D = (U, V) = D_1 + D_2$

1: $d = \gcd(U_1, U_2, V_1 + V_2) = S_1U_1 + S_2U_2 + S_3(V_1 + V_2)$ を満足する d，S_2，S_3 を Euclid の互除法により求める

2: $U = \dfrac{U_1U_2}{d^2}$ を求める

3: $1 = \gcd(d, U) = T_1d + T_2U$ を満足する T_1 を Euclid の互除法により求める

4: $V \equiv T_1(S_1U_1V_2 + S_2U_2V_1 + S_3(V_1V_2 + F)) \pmod{U}$, $\deg V < \deg U$ を満足する V を求める

アルゴリズム 2 被約因子への還元

入力: 種数 g の超楕円曲線 C: $Y^2 = F$，半被約因子 $D = (U, V)$

出力: 被約因子 $D_r = (U_r, V_r) \sim D$

1: $D_r = D$

2: **while** $\deg U_r > g$ **do**

3: $\quad \widehat{U}_r = \dfrac{F - V_r^2}{sU_r}$, $s \in \bar{K}$ は $\dfrac{F - V_r^2}{U_r}$ の最高次係数

4: $\quad \widehat{V}_r \equiv -V_r \pmod{\widehat{U}_r}$，$\deg \widehat{V}_r < \deg \widehat{U}_r$

5: $\quad U_r = \widehat{U}_r$，$V_r = \widehat{V}_r$

♣ Cantor アルゴリズム (1987) ♣

- **任意種数に適用可能**
- **加算・２倍算に同一アルゴリズムで対応可**
- **特殊ケースを含む一般アルゴリズム**
- **整係数２次形式の合成・還元のアナロジー**
- **「アルゴリズム１」→「アルゴリズム２」の順に用いる**

このアルゴリズムを用いた超楕円曲線暗号は
（十分実用的だが）
楕円曲線暗号より遅い

♣ Harleyアルゴリズム（2000）♣

- **種数固定**
- **加算・2倍算に個別アルゴリズム**
- **（最頻ケースに対するアルゴリズム）**
- **多項式演算のチューニング**
  - Euclid **の互除法**
    - ∗ **終結式**
    - ∗ **中国の剰余定理・**Newton **法**
  - Karatsuba **乗算・（除算）**
  - （Montgomery **の同時逆元計算）**
  - **係数演算への書き下し**

このアルゴリズムを用いた場合
楕円曲線上と同程度の加算速度を達成可能

♣ Harleyアルゴリズム ♣

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 $S' = s_2'x^2 + s_1'x + s_0' = rS \equiv (V_2 - V_1)I \bmod U_2$ (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		$I + 67M$

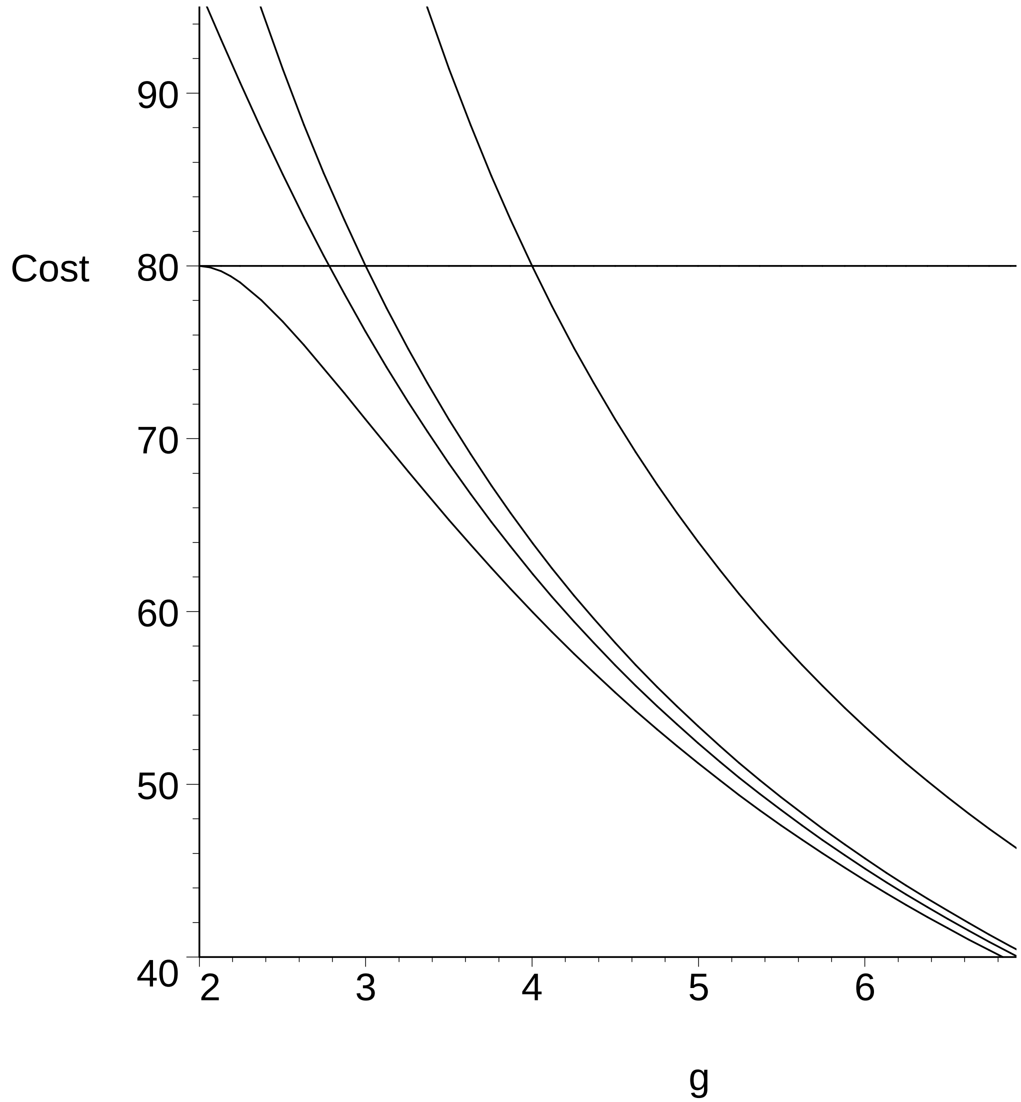
♣ 研究課題 ♣

- 実装
  - 整数倍算
    - 効率的な写像の利用
    - 効率化可能な曲線の利用
- 構成
  - 定義体の標数が小さい場合は解決済
  - その他の場合は部分的に解決
- 攻撃
- ペアリング暗号

♣ 超楕円曲線暗号の安全性 ♣

指数計算法が効果を持つ
$(C(\mathbb{F}_p) \subset J_C(\mathbb{F}_p)$ をFBとして用いる)

- 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

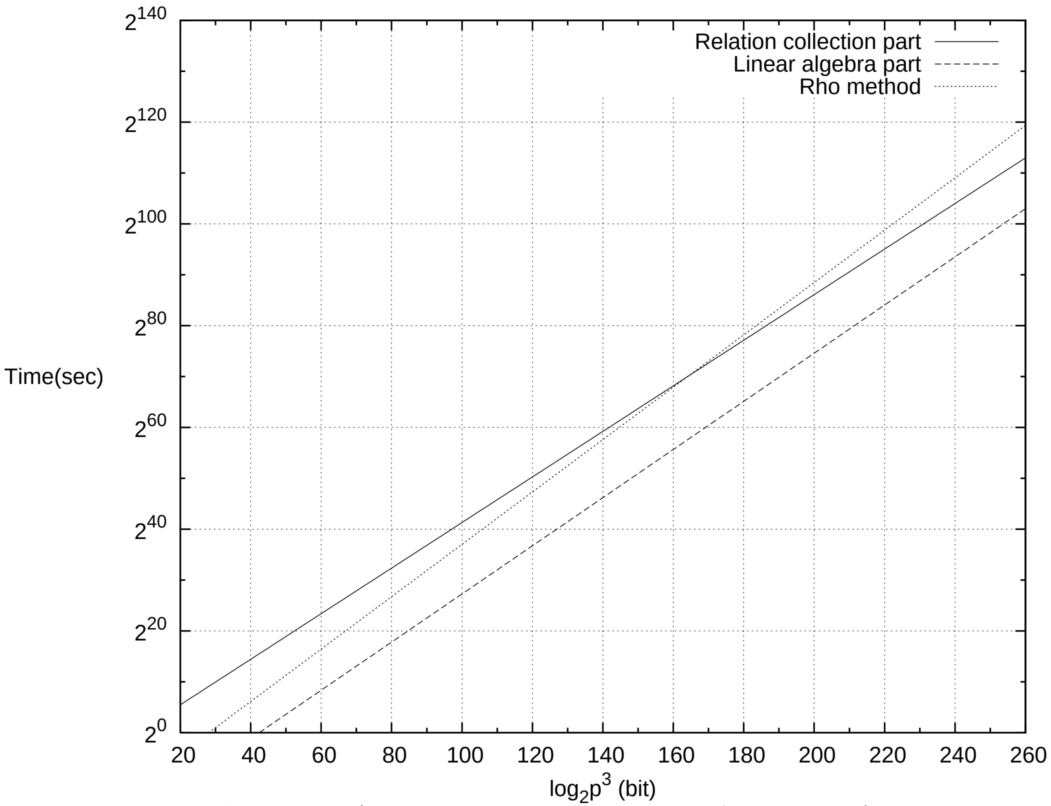


♣ 楕円曲線暗号の安全性 ♣

超楕円曲線暗号に対する攻撃法を

拡大体上の

楕円曲線暗号に対し適用可能



山外他（JANT，2008年３月）