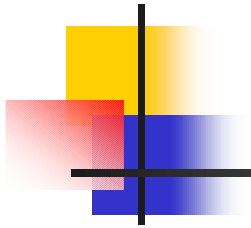
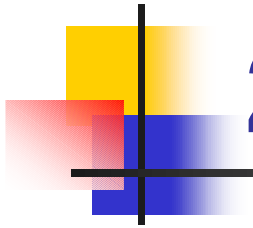
楕円曲線暗号
ーElliptic Curve Cryptosystemー

日本大学文理学部応用数学科
夜久研究室　府川由紀子



1. はじめに

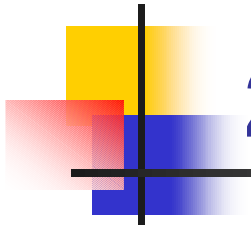
- 暗号技術は、2000年の歴史を持つ.
- 1970年代後半、 情報通信の発展により共通鍵暗号 ･公開鍵暗号が生み出される.
- 1990年半ば、インターネットの急速な普及により、情報セキュリティの重要性が強く望まれるようになる.



2 暗号

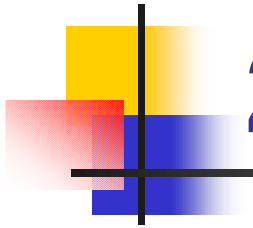
2.1 暗号方式

	共通鍵暗号方式	公開鍵暗号方式
代表方式,製品	DES,FEAL,MISTY	RSA,楕円曲線暗号
暗号鍵の関係	暗号鍵＝復号鍵	暗号鍵≠復号鍵
秘密鍵の配送	必要	不要
安全な認証	困難	容易
暗号化速度	速い	遅い
主要な用途	データの暗号化	電子捺印,鍵の配送



2.2 暗号の主な例

- DES
- RSA
- Merkle-Hellmanナップザック
- McElice
- ElGamal
- **楕円曲線暗号**(ECC)



2.3 楕円曲線暗号

2.3.1 楕円曲線の方程式

体F上の楕円曲線E

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

$$a_i \in F \quad \text{——————} ①$$

$$Y^2 = X^3 + aX + b$$

$$a, b \in F, charF \neq 2,3 \quad \text{——————} ②$$

楕円曲線Eとは、

楕円曲線②を満たす点であり,
無限遠点O を含む点の集合

$$E(F_q) :=$$

$$\{(x,y) \mid x,y \in F_q, y^2 = x^3 + ax + b\} \cup \{O\}$$

③

2.3.2 楕円曲線加法則

(1) 2点 $A=(x_1,y_1), B=(x_2,y_2) \in E(F_q)$
$(A \neq O$ かつ $B \neq 0)$ に対して，

(a) $x_1 = x_2$ かつ $y_1 + y_2 = 0$ のとき，

$$A+B:=O$$

(b) それ以外のとき， $A+B:=(x_3,y_3)$

$$x_3 = \lambda^2 - x_1 - x_2$$

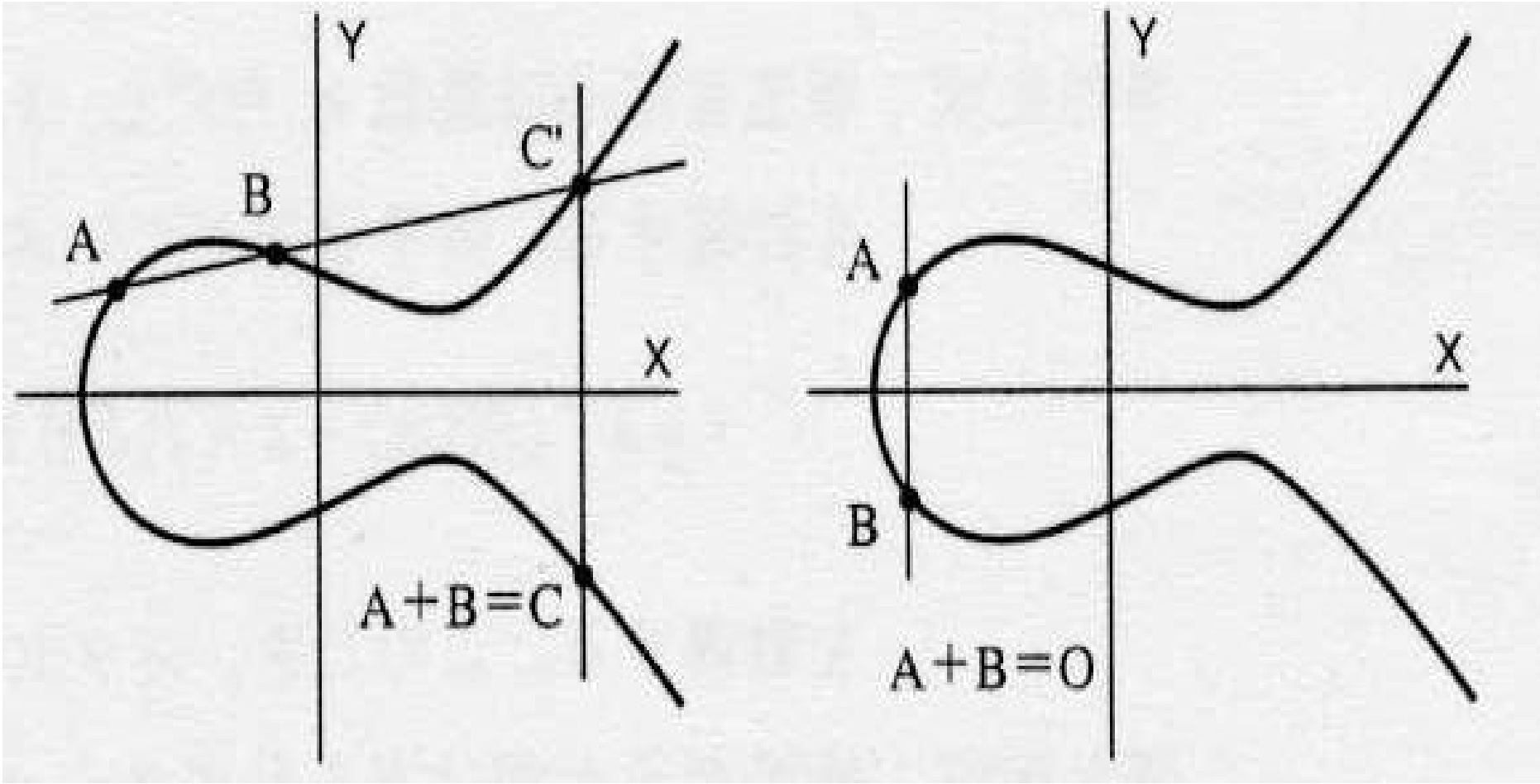
$$y_3 = -\lambda x_3 - \nu$$

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & (x_1 \neq x_2) \\ \frac{3{x_1}^2+a}{2y_1} & (x_1 = x_2) \end{cases}$$

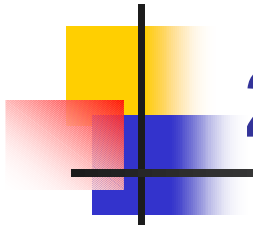
$$\nu = \begin{cases} \frac{y_1x_2-y_2x_1}{x_2-x_1} & (x_1 \neq x_2) \\ \frac{-{x_1}^3+ax_1+2b}{2y_1} & (x_1 = x_2) \end{cases}$$

(2) 任意の点 $A \in E(F_q)$ に対して，

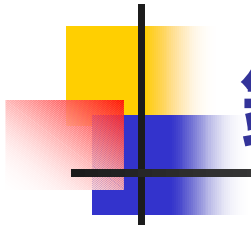
$$A+O = O+A = A$$



楕円曲線上の点の加法演算



2.3.3 構成



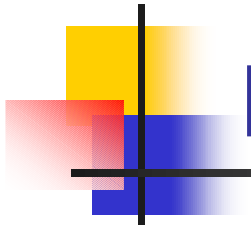
鍵生成

- 曲線EをFq上の楕円曲線.

↓

- aを楕円曲線上の点.
- ランダムな整数aを選ぶ.
- b＝a・a を楕円曲線E上で, 計算.

秘密鍵　：a　　**公開鍵　:**(E , a , b)



暗号化

乱数kを生成,平文$M = (x_1 \in Z_p, x_2 \in Z_p)$

↓

$y_0 = k \cdot \mathrm{a}$

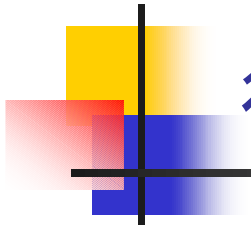
$(c_1, c_2) = k \cdot \mathrm{b}$

$y_1 = c_1 x_1 \bmod p$

$y_2 = c_2 x_2 \bmod p$

↓

暗号文 (y_0, y_1, y_2)

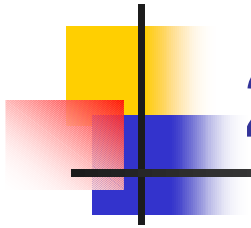


復号化

$$(c_1, c_2) = a \cdot y_0$$

$$\downarrow$$

平文　$M = (y_1 c_1^{-1} \bmod p,\ y_2 c_2^{-1} \bmod p)$

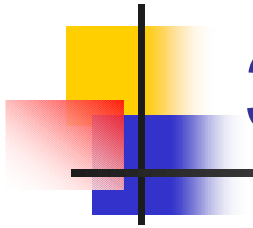


2.3.4 離散対数問題

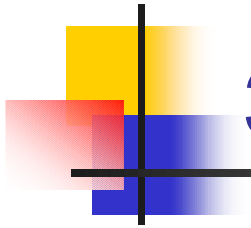
有限体F_q(q:素数,r:自然数,$q = p^r$) 上の楕円曲線E、$g, y \in E(F_q)$に対して、

$$\mathbf{y = x\,g = g + g + \cdots + g}$$

なるxが存在するなら、そのxを求める問題



3　準指数アルゴリズム



3.1　準備

- K　　標数が2でない体
- $f \in K(x)$　奇数次数の既約な多項式
- D　　divisor
- $div(f)$　$f \in K(C)$に対する　fの$divisor$
- $\deg(D)$　Dの次数
- $\tilde{D}$　　Dに対して、線形同型なdivisor
- $S = \log_q L_{q^n}[1/2, a]$, $S' = \log_q L_{q^n}[1/2, b]$

$N \in \mathbb{Z}_{>0}$, $s, c \in R$ (ここで, $0 \leq s \leq 1$) に対して,
$N \to \infty$ のとき,

$$L_N[s;c] = \exp((c + o(1))(\log N)^s(\log\log N)^{1-s})$$

3.3 アルゴリズム

(1). g, f, a_a, b_a, a_b, b_b をとり、

$$D_a = div(a_a, y - b_a), D_b = div(a_b, y - b_b)$$

(2).S,S'をとり、Gの配列をおく。

$$G = g_1, g_2, \cdots g_w、\ w = \#(G)$$

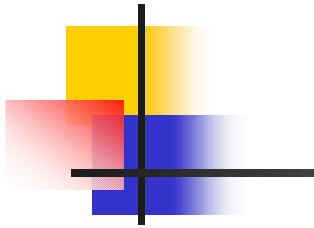
(3).Gの配列に対して、

$y^2 - f \bmod g_i$**の解をとり、**

それをy_i**とし、**$div(g_i, y_i) = D_{p_i}$**とおく**

(4). D_a**に対して、**$\tilde{D}_a = \sum_{i=1}^{m} q_i D_{Q_i}$**とおく**

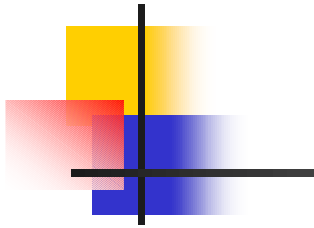
$\tilde{D}_b$**も同様**



(5). $i = 1, \cdots, w$に対して、

$D_{Q_i} = div(u_i, v_i)$とし、以下を繰り返す。

(a). $A \in K[x], B = -Av_i \bmod u_i$ なる互いに placeなBを見つける。



(b). $(B^2 - A^2 f)/u_i$がG上でなめらか。

↓ →(a).へ

$$(B^2 - A^2 f)/u_i = \prod_{j=1}^{w} g_j^{e_j}$$

↓

$j = 1, \cdots, w$に対して、 $Ay_j + B \equiv 0 \bmod g_j$

↓ ↓

$p_{ij} = -e_j$ $p_{ij} = e_j$

(6). (5). と同様

(7). $\sum_{i=1}^{m} q_i p_i \to p_{\mathrm{a}}$

$\sum_{i=1}^{m'} r_i p_i \to p_{\mathrm{b}}$ とおく

(8).(a).

(i). $A, B \in K[x]$より、 $g = A^2 f - B^2$とする

(ii). $g = \prod_{i=1}^{w} g_i^{\,e_i}$ならば、

$i = 1, \cdots, w$に対して $Ay_i + B \equiv 0 \bmod g_i$

↓ ↓

$e_{i'} = e_i$ $e_{i'} = -e_i$

ベクトル $(e_{1'}, e_{2'}, \cdots, e_{w'}) = \mathrm{g}_j$

(b). 行列$\mathrm{M}=(\mathrm{m}_{\mathrm{jk}})$のランクが w以下

→(8).(a).へ

(c). $\mathrm{P},\mathrm{D}=(\mathrm{d}_{\mathrm{i}}),\mathrm{Q},$

$\mathrm{Z}_{\mathrm{x}_1}\oplus\mathrm{Z}_{\mathrm{x}_2}\oplus\cdots\oplus\mathrm{Z}_{\mathrm{x}_w}$ なる$x_1,\cdots,x_w$

ここで、$d_i\geq(g^{1/2}+1)^{2g}$ →(8).(a).へ

(d). $p_{\mathrm{a}} P^{-1} = (t_1, \cdots, t_w)$

$p_{\mathrm{b}} P^{-1} = (s_1, \cdots, s_w)$

(e). $rt_j = s_j \bmod d_j \ (j = 1, \cdots, w)$ **なる** $r \in Z_{\geq 0}$

が見つかるか　　→(8).(a).へ

↓

求める r **が存在**

3.4 アルゴリズムについて

(1). ----------

(2).平方加群の多項式の計算 多項式時間）

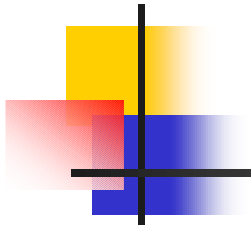
(3).平方根加群g_iの計算 （〃）

(4). ----------

(5).(a). $L_{q^n}[1/2,1/(2a)]$

(6). (5).と同様

(7). ----------



(8).(a).• $B^2 - A^2$ f**がなめらか**

• A, B**が**g**を形成できるか**

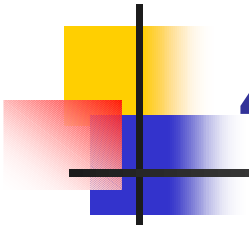
おおよそ $L_{q^n}[1/2, 1/(2a)]$

(b).(c).(d).行列計算により、 $L_{q^n}[1/2, ka]$

(e). - - - - - - - - - - - -

$$L_{q^n}[1/2, 1/(2a)],\ L_{q^n}[1/2, ka]$$

$$L_{q^n}[1/2, (k+1)/\sqrt{2k}]$$



4. 終わりに

- 楕円離散対数問題を準指数時間で解く確実なアルゴリズムが見つかっていないため，暗号解読に膨大な時間を強いられる.
- 体を固定したときに，その上に楕円曲線が豊富に存在するため，安全である.