群と暗号系

澤田　秀樹

山形大学大学院理工学研究科

sawada@sci.kj.yamagata-u.ac.jp

October, 1999

はじめに

本講演では組立関数が全単射となるような暗号系について, その組立関数が生成する群と暗号系との関係の代数的な特徴について考察する。

1　暗号系の定義

定義 1.1 $\mathcal{M}$ と $\mathcal{C}$ を長さ有限な記号列よりなる有限集合とする。このとき次の 5 つの集合 $\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$ の組を暗号系 (cryptosystem) とよび $\mathcal{S}$ で表す。すなわち

$$\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}),$$

(i) 平文 (plaintext) の集合, $\mathcal{M}$
(ii) 暗文 (ciphertext) の集合, $\mathcal{C}$
(iii) 鍵 (key) の集合, $\mathcal{K}$
(iv) 組立関数 (enciphering transformation) の集合, $\mathcal{E} = \{E_K \mid K \in \mathcal{K}\}$,

$$E_K : \mathcal{M} \longrightarrow \mathcal{C},\ \text{ただし}\ K \in \mathcal{K}$$

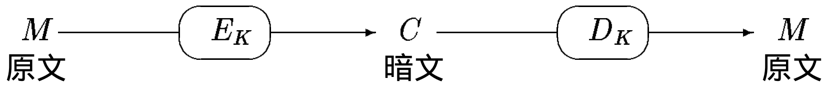
(v) 翻訳関数 (deciphering transformation) の集合 $\mathcal{D} = \{D_K \mid K \in \mathcal{K}\}$,

$$D_K : \mathcal{C} \longrightarrow \mathcal{M},\ \text{ただし}\ K \in \mathcal{K}$$

である。この 2 つの有限集合が互いに等しい数の元を含むときは, $\mathcal{M} = \mathcal{C}$ と仮定することが多い。 E_K $(K \in \mathcal{K})$ は $\mathcal{M}$ から $\mathcal{C}$ への写像, D_K は $\mathcal{C}$ から $\mathcal{M}$ への写像で,

$$D_K(E_K(M)) = M \quad (\forall M \in \mathcal{M})$$

となっている。 このとき E_K は単射, D_K は全射となる。



上の定義において特に $|\mathcal{M}| = |\mathcal{C}|$ ならば E_K $(K \in \mathcal{K})$ は $\mathcal{M}$ から $\mathcal{C}$ への全単射となり, D_K はその逆写像となる。

定義 **1.2** 暗号系 $\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ において $\mathcal{M} = \mathcal{C}$ であるとき集合 $\mathcal{M}$ の自分自身への全単射全体が作る群 $P(\mathcal{M})$ の部分群 G で $\mathcal{E}$ で生成されるもの, すなわち

$$G = \langle \mathcal{E} \rangle$$

を暗号系 $\mathcal{S}$ の群とよぶ。

この群 G は $\mathcal{M}$ に自然に作用している。

$$\begin{array}{rcl} G \times \mathcal{M} & \longrightarrow & \mathcal{M} \\ (g, m) & \longmapsto & g(m) \end{array}$$

2 RSA 暗号の群

RSA 暗号を定義しよう。$p \neq q$ を二つの大きな素数, φ を Euler 関数とする。$L = \varphi(pq) = (p-1)(q-1)$, F_p と F_q をそれぞれ標数 p, q の素体とする。

$$A = \mathsf{Z}/pq\mathsf{Z} \text{ すなわち}$$

$$A \cong \{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a \in F_p,\ b \in F_q \}$$

とする (Chinese Reminder Theorem)。$\mathcal{M}(=\mathcal{C})$ を A の乗法群 すなわち

$$\mathcal{M} \cong \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a \in {F_p}^*,\ b \in {F_q}^*\},$$

とする。ただし ${F_p}^* = F_p \setminus \{0\}$。さらに

$$B = \mathsf{Z}/L\mathsf{Z}$$

ととし, $\mathcal{K}$ を B の乗法群とする

$$\mathcal{K} = \{e_i + L\mathsf{Z} \mid i \in I\}$$

ただし $\{e_i \mid i \in I\}$ は $0 < e_i < L$ かつ $\gcd(e_i, L) = 1$ を満足する自然数の集合である。

$$\mathcal{M} = \{m + pq\mathsf{Z} \mid (m, pq) = 1\}$$

で $\mathcal{M}$ の位数は L であるから

$$\overline{m}^L = 1 \ \ \forall \overline{m} \in \mathcal{M}$$

となる。ただし $\overline{m} = m + pq\mathsf{Z}$。公開鍵 E_i 秘密鍵 D_i $(i \in I)$ の組は

$$e_i d_i \equiv 1 \ \ (mod\ L)$$

を満足する自然数を d_i としたとき,

$$\begin{array}{rcl} E_i : \mathcal{M} & \longrightarrow & \mathcal{C} \\ \overline{m} & \longmapsto & \overline{m}^{e_i}, \end{array}$$

$$\begin{array}{rcl} D_i : \mathcal{C} & \longrightarrow & \mathcal{M} \\ \overline{c} & \longmapsto & \overline{c}^{d_i} \end{array}$$

で与えられる。 ただし $\overline{c} = c + pq\mathsf{Z}$。

ある整数 t が存在して

$$e_i d_i = 1 + tL$$

となることよりただちに

$$\overline{m}^{e_i d_i} = \overline{m}^{1+tL} = \overline{m} \cdot (\overline{m}^L)^t = \overline{m} \ \ (\overline{m} \in \mathcal{M})$$

すなわち, 任意の $\overline{m} \in \mathcal{M}$ と $\overline{c} \in \mathcal{C}$ に対して

$$D_i(E_i(\overline{m})) = D_i(\overline{m}^{e_i}) = (\overline{m}^{e_i})^{d_i} = \overline{m}^{e_i d_i} = \overline{m}$$

かつ

$$E_i(D_i(\overline{c})) = E_i(\overline{c}^{d_i}) = (\overline{c}^{d_i})^{e_i} = \overline{c}^{e_i d_i} = \overline{c}$$

となることが確かめられる。このようにして RSA 暗号系 $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_i\}, \{D_i\})$ が定義できる。

定義 2.1 (RSA 暗号系) ([15]) 大きな素数 $p \neq q$ に対して $\mathcal{M}$, E_i, D_i 等を上のようにとる。このとき $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_i\}, \{D_i\})$ を (p,q) 型 *RSA* 暗号系という。

$\mathcal{K}$ は B の乗法群で $\mathcal{M}$ へはその自己同型として作用している。

$$\begin{array}{rcl} \mathcal{K} \times \mathcal{M} & \longrightarrow & \mathcal{M} \\ (e_i + L\mathsf{Z}, \overline{m}) & \longmapsto & \overline{m}^{e_i} \end{array}$$

ただし $\overline{m} = m + pq\mathsf{Z}$ とする。以下の補題から $\mathcal{K}$ と $\mathcal{M}$ の構造がわかる。

補題 2.2 $m, n (\geq 2)$ を任意の自然数とし ℓ をそれらの最小公倍数とする。このとき準同型

$$\begin{array}{rcl} f : (\mathsf{Z}/mn\mathsf{Z})^\times & \longrightarrow & (\mathsf{Z}/m\mathsf{Z})^\times \times (\mathsf{Z}/n\mathsf{Z})^\times \\ x + mn\mathsf{Z} & \longmapsto & (x + m\mathsf{Z},\ x + n\mathsf{Z}) \end{array}$$

の核は

$$\ker f = \{x \in (\mathsf{Z}/mn\mathsf{Z})^\times \mid x \equiv 1 \pmod{\ell}\}$$

となりさらに

(i) $|\ker f| = \gcd(m,n)$,

(ii) f が全単射になる必要十分条件は $\gcd(m,n) = 1$ または $\gcd(m,n) = 2$ であることがわかる。

この補題から (p,q) 型 RSA 暗号系の平文の集合 $\mathcal{M}$ と鍵の集合 $\mathcal{K}$ 上では以下のような同型 f, 準同型 ρ が定義されることがわかる。

$$\begin{array}{rcl} f : \mathcal{M} = (\mathsf{Z}/pq\mathsf{Z})^{\times} & \cong & (\mathsf{Z}/p\mathsf{Z})^{\times} \times (\mathsf{Z}/q\mathsf{Z})^{\times} \\ m + pq\mathsf{Z} & \longmapsto & (m + p\mathsf{Z},\ m + q\mathsf{Z}) \end{array}$$

$$\begin{array}{rcl} \rho : \mathcal{K} = (\mathsf{Z}/(p-1)(q-1)\mathsf{Z})^{\times} & \to & (\mathsf{Z}/(p-1)\mathsf{Z})^{\times} \times (\mathsf{Z}/(q-1)\mathsf{Z})^{\times} \\ e_i + (p-1)(q-1)\mathsf{Z} & \mapsto & (e_i + (p-1)\mathsf{Z},\ e_i + (q-1)\mathsf{Z}) \end{array}$$

このことから前回報告された結果は次のようにまとめることができる ([16])。

定理 2.3 $(\mathcal{M},\mathcal{C},\mathcal{K},\{E_i\},\{D_i\})$ を (p,q) 型 *RSA* 暗号系とし, f,ρ を上で定義された準同型とする。$\overline{m} \in \mathcal{M}$, $\overline{e}_i \in \mathcal{K}$ とすれば

(i)

$$f(\overline{m}^{e_i}) = f(\overline{m})^{\rho(\overline{e}_i)}$$

となる。ただし $f(\overline{m})^{\rho(\overline{e}_i)} = (m^{e_i} + p\mathsf{Z},\ m^{e_i} + q\mathsf{Z})$。

(ii) ρ は $\mathcal{K}$ から $\rho(\mathcal{K})$ への $d_0 - 1$ 対応となる。ただし $d_0 = \gcd(p-1, q-1)$。

$\rho(\mathcal{K})$ が RSA 暗号の群となっている。

3 ブロック暗号の群

定義 3.1 (ブロック暗号) 暗号系 $\mathcal{S} = (\mathcal{M},\ \mathcal{C},\ \mathcal{K},\ \mathcal{E},\ \mathcal{D})$ において $\mathcal{M}$ が有限体 F 上の有限次元ベクトル空間で $\mathcal{M} = \mathcal{C}$ であるとき $\mathcal{S}$ をブロック暗号とよぶ。

$\mathcal{S}$ をブロック暗号とし $U = \mathcal{E} \cup \mathcal{D}$ と置こう。定義より U は空でない $P(\mathcal{M})$ の部分集合で

$$U^{-1} \subset U$$

であることから $U = U^{-1}$ であることがわかる。さらに非常に一般的な条件として U は以下のような性質を持つことが望ましいとされている ([17] の 12.3 章)。

(i) U は多くの元を持ち, かつ, それぞれの位数も大きい。しかし

(ii) U は群構造を持たない, すなわち

$$UU \not\subset U$$

となり, さらに

(iii) 条件

$$UUU \not\subset U$$

も満足する。

さらにこのような U を構成できたとしても暗号を実用化するには

任意の $\pi \in U$ について

$$\pi(\mathbf{x}) = \mathbf{y} \quad \forall \mathbf{x} \in \mathcal{M}$$

の計算は容易でも π^{-1} を見つけるのは難しい。

ような $\pi \in U$ を計算するアルゴリズムを見つける必要がある。これは例えば非常に大きな鍵の空間 $\mathcal{K}$ から U への「一方向関数」を与えることにより実現できる。では対称群 $P(\mathcal{M})$ の部分集合 U が条件

$$\begin{aligned} UU &\not\subset U \\ UUU &\not\subset U \end{aligned}$$

を満たすことの意味を考えてみよう。

補題 3.2 G を群, H をその部分群とし自明でない両側剰余類を HgH $(g \notin H)$ とすれば

$$\begin{aligned} (gHgH) \cap gH &= \emptyset \\ (HgHg) \cap Hg &= \emptyset \end{aligned}$$

となる。

[証明] $HgH \cap H = \emptyset$ より明らか。

(証明終)

補題 3.3 G を群, H をその部分群とする。自明でない両側剰余類 HgH が条件 $gHg \cap H = \emptyset$ を満足するならば

$$\begin{aligned}(gHgHgH) \cap gH &= \emptyset \\ (HgHgHg) \cap Hg &= \emptyset\end{aligned}$$

となる。

[証明] $gHg \cap H = \emptyset \Leftrightarrow HgHgH \cap H = \emptyset$ より明らか。

(証明終)

定理 3.4 G を群, H をその部分群とする。

(i) G における H の自明でない左剰余類 gH において

$$(gHgH) \cap Hg^{-1} = \emptyset$$

となるならば, 集合 $U = gH \cup Hg^{-1}$ は条件 $U = U^{-1}$ かつ

$$(UU) \cap U = \emptyset$$

を満足する。

(ii) HgH を G における H の自明でない両側剰余類とする。このとき $gHg \cap H = \emptyset$ ならば, 集合 $V = gH$, $V' = Hg$ では以下の条件が成り立つ。

$$\begin{aligned}(VVV) \cap V &= \emptyset \\ (V'V'V') \cap V' &= \emptyset\end{aligned}$$

[証明] (i) $U = U^{-1}$ であることは明らか。一方

$$\begin{aligned}UU &= (gH \cup Hg^{-1})(gH \cup Hg^{-1}) \\ &= gHgH \cup gHg^{-1} \cup H \cup Hg^{-1}Hg^{-1}\end{aligned}$$

であるから

$$(UU) \cap U = (gHgH \cap U) \cup (gHg^{-1} \cap U) \cup (H \cap U) \cup (Hg^{-1}Hg^{-1} \cap U)$$

となる。仮定より $g \notin H$ であるから $(gHgH) \cap gH = \emptyset$,
$(Hg^{-1}Hg^{-1}) \cap Hg^{-1} = \emptyset$ となりさらに $(gHgH) \cap Hg^{-1} = \emptyset$ であるから

$$\begin{aligned}
(gHgH) \cap U &= (gHgH) \cap (gH \cup Hg^{-1}) = \emptyset, \\
(gHg^{-1}) \cap U &= (gHg^{-1}) \cap (gH \cup Hg^{-1}) = \emptyset, \\
H \cap U &= H \cap (gH \cup Hg^{-1}) = \emptyset, \\
(Hg^{-1}Hg^{-1}) \cap U &= (Hg^{-1}Hg^{-1}) \cap (gH \cup Hg^{-1}) = \emptyset,
\end{aligned}$$

となり $(UU) \cap U = \emptyset$ であることがわかる。
(ii) 上の補題より明らか。

(証明終)

系 3.5 G を群, N をその正規部分群とし, $\overline{G}$ を G の N による剰余群とする。このとき $\overline{G}$ の元 gN $(g \in G)$ に対して $\mathrm{ord}(gN) > 3$ ならば

(i) 集合 $U = gN \cup g^{-1}N$ は条件 $U = U^{-1}$ かつ

$$(UU) \cap U = \emptyset$$

を満足する。

(ii) 集合 $V = gN$ では条件

$$\underbrace{(VV \cdots V)}_{\mathrm{ord}(gN)} \cap V = \emptyset$$

が成り立つ。

[証明] (i) $\mathrm{ord}(gN) > 3$ より上の定理の条件

$$(gNgN) \cap Ng^{-1} = \emptyset$$

が成り立つ。故に $(UU) \cap U = \emptyset$ となる。
(ii) $\mathrm{ord}(gN)$ の定義より明らか。

(証明終)

4 実例

ブロック暗号を $\mathcal{S} = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ とする。すなわち $\mathcal{M}$ は有限体 F 上の有限次元ベクトル空間で $\mathcal{M} = \mathcal{C}$ が成り立っている。GAP 4.1 ([10]) を使って U および V の実例を示す。

実例 1 ブロック暗号 $\mathcal{S}$ において F を標数 2 の素体とし, $\mathcal{M} = F^4$ とする。このとき $|\mathcal{M}| = 16$, $|S_{16}| = 20922789888000$ である。

```
gap> g:=SymmetricGroup(16);
Sym( [ 1 .. 16 ] )
gap> Size(g);
20922789888000
gap> m1:=( 1, 3)( 5,16,14,15, 11, 8)( 6,10);
( 1, 3)( 5,16,14,15,11, 8)( 6,10)
gap> m2:=( 1, 8, 5,11,16, 3, 6,12,15,10, 9,14);
( 1, 8, 5,11,16, 3, 6,12,15,10, 9,14)
gap> m:=Subgroup(g,[m1,m2]);
Group([ ( 1, 3)( 5,16,14,15,11, 8)( 6,10),
  ( 1, 8, 5,11,16, 3, 6,12,15,10, 9,14) ])
gap> Size(m);
479001600
gap> n:=Normalizer(g,m);
Group([ ( 1, 3)( 5, 8,14, 9,15,16)( 6,12),
  ( 1, 5, 8,16,14, 3, 6,11,15,12,10, 9), ( 4, 7),
                                  ( 4,13), ( 2, 4,13) ])
gap> Size(n);
11496038400
gap> q:=FactorGroup(n,m);
<pc group of size 24 with 4 generators>
gap> nat:=NaturalHomomorphismByNormalSubgroup(n,m);
Pcgs([(4,7), (4,13,7), (2,4)(7,13), (2,13)(4, 7)]) ->
[ f1, f2, f3, f4 ]
gap> n1:=(1,9,3,11)(2,4,13)(5,6,10,15,8,12)(14,16);
( 1, 9, 3,11)( 2, 4,13)( 5, 6,10,15, 8,12)(14,16)
gap> Image(nat,n1);
f2^2*f3
gap> Order(Image(nat,n1));
3
```

```
gap> n2:=(1,10,15,8,9,11,6,16)(2,7,4,13)(3,14,12,5);
( 1,10,15, 8, 9,11, 6,16)( 2, 7, 4,13)( 3,14,12, 5)
gap> Image(nat,n2);
f1*f2*f3*f4
gap> Order(Image(nat,n2));
4
gap>
```

系 3.5 において $G = \mathtt{n}$, $N = \mathtt{m}$, $\overline{G} = \mathtt{q}$, $g = \mathtt{n2}$ とおけばよい。すなわち

$$\begin{aligned} U &= gN \cup g^{-1}N = \mathtt{n2}\,\mathtt{m} \cup \mathtt{n2}^{-1}\mathtt{m} \\ V &= gN = \mathtt{n2}\,\mathtt{m} \end{aligned}$$

となる。ただし $[\mathtt{s16} : \mathtt{m}] = 43680$ である。

References

[1] 池野信一, 小山謙二, 現代暗号理論 (第 5 版). 電子情報通信学会 1995

[2] 太田和夫, 黒澤馨, 渡辺治, 情報セキュリティの科学. 講談社ブルーバックス 1995

[3] 岡本栄司, 暗号理論入門. 共立出版 1993

[4] 岡本龍明, 太田和夫 編, 暗号 · ゼロ知識証明 · 数論. 共立出版 1995

[5] 岡本龍明, 山本博資, 現代暗号. 産業図書 1997

[6] 加藤正隆, 基礎暗号学 I,II. サイエンス社 1989

[7] 近藤武, 基礎数学 群論 I. 岩波書店 1987

[8] 澤田秀樹, 暗号理論と代数学, 海文堂 1997

[9] 和田秀男, コンピュータと素因子分解. 遊星社 1987

[10] GAP, Groups, Algorithms and Programming 4.1. *School of Mathematical and Computational Sciences, University of St Andrews, Scotland, 1999*

[11] K.W.Campbell and M.J.Wierner, DES is not a group, *Advances in Cryptology-CRYPTO '92 Proceedings,* Springer-Verlag (1992) pp.512-520.

[12] D.E.R.Denning, Cryptography and data security. *Addison-Wesley 1983*

[13] N.Koblitz, A course in number theory and cryptography, 2nd edition. *Springer-Verlag, 1994*

[14] W.Patterson, Mathematical cryptology for computer scientists and mathematicians.*Rowman & Littlefield 1987*

[15] R.L.Rivest, A.Shamir and L.Adleman, A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, Vol.21, No.2 (Feb. 1978) 120-126*

[16] H.Sawada and T.Abe, Groups and RSA cryptosystems, *to aapear in CRYPTOLOGIA.*

[17] B.Schneier, Applied cryptography, 2nd edition. *John Wiley & Sons, Inc. 1996*

[18] D.R.Stinson, Cryptography, theory and practice. *CRC Press, Inc. 1995*

本研究は平成 11 年度科学研究費補助金萌芽的研究「暗号系に現れる群構造について」の一部である。