数理解析研究所講究録
第1630巻 2009年 128-137

polycyclic groupの暗号への応用

大阪教育大学　亀川 良　(Ryoh Kamegawa)
大阪教育大学　藤井淳一　(Jun Ichi Fujii)

はじめに

近年急速に暗号の分野は変革をとげてきている。新しかった暗号もすぐに解き方が解明され陳腐化されていくのが実状である。したがって、常に新しい考えに基づく暗号が求められている。そこで我々はプレプリント [1] を読み、そこで提案されている polycyclic group（ここでは、**多巡回群**と呼ぶ）の暗号への全般的利用について研究することにした。以前に直積多巡回群を暗号化に応用したが、これは自明な例なのでもう少し一般的な多巡回群の構成法として半直積による拡大、さらに一般的な拡大として Schreier による群拡大を用いて暗号化を提案した。その際に、参考論文とは違った方法で鍵交換も暫定的に提案したいと思う。

1. 多巡回群

G を元となる群、$\{e\}$ をその単位元からなる群とし、G_{k-1} が G_k の正規部分群になっている次のような G の部分群の有限列があるとする：

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

これは、**subnormal sequence** と呼ばれることもあり、隣り合った群の商群 G_{k+1}/G_k は**因子群**と呼ばれる。**可解群**は各因子群が可換群、**多巡回群**は各因子群が巡回群となるような、subnormal sequence も持つことがそれぞれの定義である。**超可解群**は多巡回群であって、$G_k \lhd G$ となるような subnormal sequence を持つ場合で、この列は **normal sequence** と呼ばれる。**べき零群**は、因子群 G_{k+1}/G_k が対応する元の商群 G/G_k の中心に入っている normal sequence を持つ場合である。自明な例として巡回群の直積は多巡回群となる。

2. 群拡大

半直積 $A \rtimes X$ とは、集合として直積 $A \times X$ で、積 $(a,x)(b,y) = (a\theta_x(b), xy)$ (ただし、θ_x は、$\theta_{xy} = \theta_x \circ \theta_y$ となる X の A への作用) で定義できる群のことである。
$\theta_1 = \mathrm{id}_A$, $\theta_x^{-1} = \theta_{x^{-1}}$ が分かるので半直積も群となる。

さらに直積群同様、巡回群の半直積も多巡回群となる： ある半直積群 $G = X_1 \rtimes X_2 \rtimes \cdots \rtimes X_n$ について、$X_k (k = 1, 2, \cdots, n)$ が巡回群の場合、直積と同じように $X \cong X \rtimes \{e\}$ と見るとき、G が多巡回群であることが分かる。

2つの群 N、M が与えられたとき群 G を構成して N の埋め込み $\bar{N}$ が、G の正規部分群になって、商群が M になる G を N の M **による群拡大**という。しばしば、短完全系列

$$1 \to N \xrightarrow{\varphi} G \xrightarrow{\psi} M \to 1$$

によってあらわされる。この拡大は、以下の **Schreier 拡大**に限られることが示されている:

Schreier の定理. G が N の M による拡大であるための必要十分条件は、$\sigma, \tau \in M$ に対して N の自己同型 s_σ, s_τ が対応し、$\exists c_{\sigma,\tau} \in N$;

$$s_\sigma(s_\tau(a)) = c_{\sigma,\tau}(s_{\sigma\tau}(a))c_{\sigma,\tau}^{-1} \qquad (\forall a \in N) \tag{1}$$

$$c_{\sigma,\tau}c_{\sigma\tau,\rho} = s_\sigma(c_{\tau,\rho})c_{\sigma,\tau\rho} \tag{2}$$

このとき、$G = \{as_\sigma | a \in N, \sigma \in M\}$ とし、

$$as_\sigma bs_\tau \equiv (as_\sigma(b)c_{\sigma,\tau})s_{\sigma\tau} \tag{3}$$

としたとき、$\bar{N} = \{\bar{a} = ac_{1,1}^{-1}s_1 | a \in N\} \triangleleft G$ となり、$G/\bar{N} \cong M$ となる。
この場合の $\{s_\sigma, c_{\sigma,\tau}\}$ を M **による因子団**もしくは **2-cocycle** という。

(1) より、$\sigma = 1, \tau = 1$ とした時、$s_1(s_1(a)) = c_{1,1}s_1(a)c_{1,1}^{-1}$ となり、この時 $s_1(a) = x$ とすると、$s_1(x) = c_{1,1}xc_{1,1}^{-1}$ と表す事ができる。

(2) より、$\tau = 1, \rho = 1$ とした時 $c_{\sigma,1}c_{\sigma,1} = s_\sigma(c_{1,1})c_{\sigma,1}$ となり、右から $c_{\sigma,1}^{-1}$ をかけると、$c_{\sigma,1} = s_\sigma(c_{1,1})$. また、$\tau = 1$ の時、$c_{\sigma,1}c_{\sigma,\rho} = s_\sigma(c_{1,\rho})c_{\sigma,\rho}$ となり、右から $c_{\sigma,\rho}^{-1}$ をかけると $c_{\sigma,1} = s_\sigma(c_{1,\rho})$. よって $s_\sigma(c_{1,1}) = c_{\sigma,1} = s_\sigma(c_{1,\rho})$ となることが分かり、$s_\sigma(c_{1,1}) = s_\sigma(c_{1,\rho})$ がいえる。ゆえに、$c_{1,1} = c_{1,\rho}$.

2つの因子団 $(s_\sigma, c_{\sigma,\tau}), (t_\sigma, d_{\sigma,\tau})$ に対して、

$$\forall \sigma \in M, \exists n_\sigma \in N \ s.t. \ t_\sigma(n) = s_\sigma(n_\sigma n n_\sigma^{-1}), d_{\sigma,\tau} = n_\sigma(s_\sigma(n_\tau))c_{\sigma,\tau}n_{\sigma\tau}^{-1}$$

となるときに、この因子団あるいはこれに対応する群の拡大は**分裂**するという。

定理. 分裂条件は、$1 = n_\sigma(n_\sigma(n_\tau))c_{\sigma,\tau}n_{\sigma\tau}^{-1}$、つまり $n_\sigma s_\sigma(n_\tau)c_{\sigma,\tau} = n_{\sigma\tau}$ であり、群の準同型の短完全系列 $1 \xrightarrow{\psi_1} N \xrightarrow{\psi_2} G \xrightarrow{\psi_3} M \xrightarrow{\psi_4} 1$ において、$\psi_3 \circ \psi_3' = \mathrm{id}_M$ となる準同型 $\psi_3' : M \to G$ が存在する事と同値である。このとき、G は半直積である：$G = \psi_2(N) \rtimes \psi_3'(M)$.

3. 基礎群とアルファベット

正方形をそれ自身の上に重ねる合同変換のなす群を**4次の2面体群**といい、D_4で表す。その元は、以下のAを単位元として、B, C, Dは90度ずつの回転E, F, G, Hは直線の折り返しである。ここで、ξ、ηは2つの対角線のことを表している。

$D_4 = \{A, B, C, D, E, F, G, H\}$
A = 正四角形の中心Oのまわりの0°の回転。
B = Oのまわりの90°の回転。
C = Oのまわりの180°の回転。
D = Oのまわりの270°の回転。
E = OYを軸とする折り返し。
F = OXを軸とする折り返し。
G = 直線ξに関する折り返し。
H = 直線ηに関する折り返し。

2面体群D_4の群表は以下のようになる。

	A	B	C	D	E	F	G	H
A	A	B	C	D	E	F	G	H
B	B	C	D	A	H	G	E	F
C	C	D	A	B	F	E	H	G
D	D	A	B	C	G	H	F	E
E	E	G	F	H	A	C	B	D
F	F	H	E	G	C	A	D	B
G	G	F	H	E	D	B	A	C
H	H	E	G	F	B	D	C	A

$$\{A\} \lhd \{A, C\} \lhd \{A, B, C, D\} \lhd D_4$$

このように回転部分はsubnormal sequenceということは明らかであり、因子群が位数2の巡回群であることがわかるのでD_4自身も多巡回群になる。
D_4のS_2によるSchreier拡大Gを考える：

$$1 \to D_4 \to G \to S_2 \to 1 \qquad (exact)$$

この時、$s_1(n) = c_{1,1} n c_{1,1}^{-1}$となることは前に示したので$c_{1,1} = F$とした時$s_1(n) = FnF^{-1}$となる。この拡大への埋め込み同型は$\varphi : X \mapsto Xc_{1,1}^{-1}s_1 = XF^{-1}s_1, \quad X \in D_4$となる。この埋め込みによって$As_1$、$Bs_1$と順に並ぶように$F$をあらかじめかけて$XF$とすることで順序づけられ、このとき単位元がずれることになる。この拡大の埋め込み部分の積表は以下のようになり、単位元はFs_1となる。これはD_4を埋め込んだ部分である。

	$\varphi(F) = As_1$	$\varphi(G) = Bs_1$	$\varphi(E) = Cs_1$	$\varphi(H) = Ds_1$	$\varphi(C) = Es_1$	$\varphi(A) = Fs_1$	$\varphi(B) = Gs_1$	$\varphi(D) = Hs_1$
$\varphi(F) = As_1$	Fs_1	Hs_1	Es_1	Gs_1	Cs_1	As_1	Ds_1	Bs_1
$\varphi(G) = Bs_1$	Gs_1	Fs_1	Hs_1	Es_1	Ds_1	Bs_1	As_1	Cs_1
$\varphi(E) = Cs_1$	Es_1	Gs_1	Fs_1	Hs_1	As_1	Cs_1	Bs_1	Ds_1
$\varphi(H) = Ds_1$	Hs_1	Es_1	Gs_1	Fs_1	Bs_1	Ds_1	Cs_1	As_1
$\varphi(C) = Es_1$	Cs_1	Ds_1	As_1	Bs_1	Fs_1	Es_1	Hs_1	Gs_1
$\varphi(A) = Fs_1$	As_1	Bs_1	Cs_1	Ds_1	Es_1	Fs_1	Gs_1	Hs_1
$\varphi(B) = Gs_1$	Bs_1	Cs_1	Ds_1	As_1	Hs_1	Gs_1	Es_1	Fs_1
$\varphi(D) = Hs_1$	Ds_1	As_1	Bs_1	Cs_1	Gs_1	Hs_1	Fs_1	Es_1

他の拡大部分を見るために$s_2(m) = BmB^{-1}$とおくと、$c_{1,2} = F$、$c_{2,1} = E$、$c_{2,2} = E$は自動的にこのようになる。下の表はD_4をS_2で拡大した積表である。

	As_1	Bs_1	Cs_1	Ds_1	Es_1	Fs_1	Gs_1	Hs_1	As_2	Bs_2	Cs_2	Ds_2	Es_2	Fs_2	Gs_2	Hs_2
As_1	Fs_1	Hs_1	Es_1	Gs_1	Cs_1	As_1	Ds_1	Bs_1	Fs_2	Hs_2	Es_2	Gs_2	Cs_2	As_2	Ds_2	Bs_2
Bs_1	Gs_1	Fs_1	Hs_1	Es_1	Ds_1	Bs_1	As_1	Cs_1	Gs_2	Fs_2	Hs_2	Es_2	Ds_2	Bs_2	As_2	Cs_2
Cs_1	Es_1	Gs_1	Fs_1	Hs_1	As_1	Cs_1	Bs_1	Ds_1	Es_2	Gs_2	Fs_2	Hs_2	As_2	Cs_2	Bs_2	Ds_2
Ds_1	Hs_1	Es_1	Gs_1	Fs_1	Bs_1	Ds_1	Cs_1	As_1	Hs_2	Es_2	Gs_2	Fs_2	Bs_2	Ds_2	Cs_2	As_2
Es_1	Cs_1	Ds_1	As_1	Bs_1	Fs_1	Es_1	Hs_1	Gs_1	Cs_2	Ds_2	As_2	Bs_2	Fs_2	Es_2	Hs_2	Gs_2
Fs_1	As_1	Bs_1	Cs_1	Ds_1	Es_1	Fs_1	Gs_1	Hs_1	As_2	Bs_2	Cs_2	Ds_2	Es_2	Fs_2	Gs_2	Hs_2
Gs_1	Bs_1	Cs_1	Ds_1	As_1	Hs_1	Gs_1	Es_1	Fs_1	Bs_2	Cs_2	Ds_2	As_2	Hs_2	Gs_2	Es_2	Fs_2
Hs_1	Ds_1	As_1	Bs_1	Cs_1	Gs_1	Hs_1	Fs_1	Es_1	Ds_2	As_2	Bs_2	Cs_2	Gs_2	Hs_2	Fs_2	Es_2
As_2	Es_2	Hs_2	Fs_2	Gs_2	Cs_2	As_2	Bs_2	Ds_2	Es_1	Hs_1	Fs_1	Gs_1	Cs_1	As_1	Bs_1	Ds_1
Bs_2	Hs_2	Fs_2	Gs_2	Es_2	Ds_2	Bs_2	Cs_2	As_2	Hs_1	Fs_1	Gs_1	Es_1	Ds_1	Bs_1	Cs_1	As_1
Cs_2	Fs_2	Gs_2	Es_2	Hs_2	As_2	Cs_2	Ds_2	Bs_2	Fs_1	Gs_1	Es_1	Hs_1	As_1	Cs_1	Ds_1	Bs_1
Ds_2	Gs_2	Es_2	Hs_2	Fs_2	Bs_2	Ds_2	As_2	Cs_2	Gs_1	Es_1	Hs_1	Fs_1	Bs_1	Ds_1	As_1	Cs_1
Es_2	As_2	Ds_2	Cs_2	Bs_2	Fs_2	Es_2	Gs_2	Hs_2	As_1	Ds_1	Cs_1	Bs_1	Fs_1	Es_1	Gs_1	Hs_1
Fs_2	Cs_2	Bs_2	As_2	Ds_2	Es_2	Fs_2	Hs_2	Gs_2	Cs_1	Bs_1	As_1	Ds_1	Es_1	Fs_1	Hs_1	Gs_1
Gs_2	Ds_2	Cs_2	Bs_2	As_2	Hs_2	Gs_2	Fs_2	Es_2	Ds_1	Cs_1	Bs_1	As_1	Hs_1	Gs_1	Fs_1	Es_1
Hs_2	Bs_2	As_2	Ds_2	Cs_2	Gs_2	Hs_2	Es_2	Fs_2	Bs_1	As_1	Ds_1	Cs_1	Gs_1	Hs_1	Es_1	Fs_1

As_1からHs_1までを0から7までの数値に対応させ、As_2からHs_2までを8から15までの数値に対応させると積表は以下のようになる。これを**基礎群**と呼び、$\mathbb{F}$と表すことにする。

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	5	7	4	6	2	0	3	1	13	15	12	14	10	8	11	9
1	6	5	7	4	3	1	0	2	14	13	15	12	11	9	8	10
2	4	6	5	7	0	2	1	3	12	14	13	15	8	10	9	11
3	7	4	6	5	1	3	2	0	15	12	14	13	9	11	10	8
4	2	3	0	1	5	4	7	6	10	11	8	9	13	12	15	14
5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
6	1	2	3	0	7	6	4	5	9	10	11	8	15	14	12	13
7	3	0	1	2	6	7	5	4	11	8	9	10	14	15	13	12
8	12	15	13	14	10	8	9	11	4	7	5	6	2	0	1	3
9	15	13	14	12	11	9	10	8	7	5	6	4	3	1	2	0
10	13	14	12	15	8	10	11	9	5	6	4	7	0	2	3	1
11	14	12	15	13	9	11	8	10	6	4	7	5	1	3	0	2
12	8	11	10	9	13	12	14	15	0	3	2	1	5	4	6	7
13	10	9	8	11	12	13	15	14	2	1	0	3	4	5	7	6
14	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
15	9	8	11	10	14	15	12	13	1	0	3	2	6	7	4	5

aとbの群としての積を表したい時は$\langle a\rangle\langle b\rangle$と表すことにする。

今回の polycyclic group

$$G[N] = \mathbb{F} \rtimes \overbrace{S_2 \rtimes S_2 \rtimes \cdots \rtimes S_2}^{N-4} \qquad (\mathbb{F}:\text{基礎群})$$

基礎群 $\mathbb{F}$ と S_2 の半直積により拡大していく。

$$ns_{k_1} \cdots s_{k_n} \in \mathbb{F} \rtimes S_2 \rtimes S_2 \rtimes \cdots \rtimes S_2$$

半直積群の $s_1(X) = X, s_2(X) = YXY^{-1}$ と表す事ができ、$s_2(X) = \langle 6\rangle X\langle 6^{-1}\rangle = \langle 6\rangle X\langle 7\rangle$ はこのように常におくことにする。そして、アルファベットは 2^N 個ある。

$G[N]$ の積表は常に 4 ブロックの自己相似形をしており、左上から右上へは 2^N の和であり、左上から右下へは群の積であり、右下から左下へもやはり 2^N の和で計算することができる。この性質からアルファベットの群の積計算は再帰的に定義できる。

半直積 $\mathbb{F} \rtimes S_2$

以下は、基礎群 $\mathbb{F}$ を半直積 1 つ拡大した例である。(2^5)

5	7	4	6	2	0	3	1	13	15	12	14	10	8	11	9	21	23	20	22	18	16	19	17	29	31	28	30	26	24	27	25
6	5	7	4	3	1	0	2	14	13	15	12	11	9	8	10	22	21	23	20	19	17	16	18	30	29	31	28	27	25	24	26
4	6	5	7	0	2	1	3	12	14	13	15	8	10	9	11	20	22	21	23	16	18	17	19	28	30	29	31	24	26	25	27
7	4	6	5	1	3	2	0	15	12	14	13	9	11	10	8	23	20	22	21	17	19	18	16	31	28	30	29	25	27	26	24
2	3	0	1	5	4	7	6	10	11	8	9	13	12	15	14	18	19	16	17	21	20	23	22	26	27	24	25	29	28	31	30
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	2	3	0	7	6	4	5	9	10	11	8	15	14	12	13	17	18	19	16	23	22	20	21	25	26	27	24	31	30	28	29
3	0	1	2	6	7	5	4	11	8	9	10	14	15	13	12	19	16	17	18	22	23	21	20	27	24	25	26	30	31	29	28
12	15	13	14	10	8	9	11	4	7	5	6	2	0	1	3	28	31	29	30	26	24	25	27	20	23	21	22	18	16	17	19
15	13	14	12	11	9	10	8	7	5	6	4	3	1	2	0	31	29	30	28	27	25	26	24	23	21	22	20	19	17	18	16
13	14	12	15	8	10	11	9	5	6	4	7	0	2	3	1	29	30	28	31	24	26	27	25	21	22	20	23	16	18	19	17
14	12	15	13	9	11	8	10	6	4	7	5	1	3	0	2	30	28	31	29	25	27	24	26	22	20	23	21	17	19	16	18
8	11	10	9	13	12	14	15	0	3	2	1	5	4	6	7	24	27	26	25	29	28	30	31	16	19	18	17	21	20	22	23
10	9	8	11	12	13	15	14	2	1	0	3	4	5	7	6	26	25	24	27	28	29	31	30	18	17	16	19	20	21	23	22
11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4	27	26	25	24	31	30	29	28	19	18	17	16	23	22	21	20
9	8	11	10	14	15	12	13	1	0	3	2	6	7	4	5	25	24	27	26	30	31	28	29	17	16	19	18	22	23	20	21
20	22	21	23	18	16	19	17	29	31	28	30	24	26	25	27	4	6	5	7	2	0	3	1	13	15	12	14	8	10	9	11
23	20	22	21	19	17	16	18	30	29	31	28	25	27	26	24	7	4	6	5	3	1	0	2	14	13	15	12	9	11	10	8
21	23	20	22	16	18	17	19	28	30	29	31	26	24	27	25	5	7	4	6	0	2	1	3	12	14	13	15	10	8	11	9
22	21	23	20	17	19	18	16	31	28	30	29	27	25	24	26	6	5	7	4	1	3	2	0	15	12	14	13	11	9	8	10
16	17	18	19	21	20	23	22	26	27	24	25	28	29	30	31	0	1	2	3	5	4	7	6	10	11	8	9	12	13	14	15
18	19	16	17	20	21	22	23	24	25	26	27	29	28	31	30	2	3	0	1	4	5	6	7	8	9	10	11	13	12	15	14
19	16	17	18	23	22	20	21	25	26	27	24	30	31	29	28	3	0	1	2	7	6	4	5	9	10	11	8	14	15	13	12
17	18	19	16	22	23	21	20	27	24	25	26	31	30	28	29	1	2	3	0	6	7	5	4	11	8	9	10	15	14	12	13
29	30	28	31	26	24	25	27	20	23	21	22	16	18	19	17	13	14	12	15	10	8	9	11	4	7	5	6	0	2	3	1
30	28	31	29	27	25	26	24	23	21	22	20	17	19	16	18	14	12	15	13	11	9	10	8	7	5	6	4	1	3	0	2
28	31	29	30	24	26	27	25	21	22	20	23	18	16	17	19	12	15	13	14	8	10	11	9	5	6	4	7	2	0	1	3
31	29	30	28	25	27	24	26	22	20	23	21	19	17	18	16	15	13	14	12	9	11	8	10	6	4	7	5	3	1	2	0
26	25	24	27	29	28	30	31	16	19	18	17	20	21	23	22	10	9	8	11	13	12	14	15	0	3	2	1	4	5	7	6
24	27	26	25	28	29	31	30	18	17	16	19	21	20	22	23	8	11	10	9	12	13	15	14	2	1	0	3	5	4	6	7
25	24	27	26	31	30	29	28	19	18	17	16	22	23	20	21	9	8	11	10	15	14	13	12	3	2	1	0	6	7	4	5
27	26	25	24	30	31	28	29	17	16	19	18	23	22	21	20	11	10	9	8	14	15	12	13	1	0	3	2	7	6	5	4

よって、$\mathbb{F} \rtimes S_2$ において、$\mathbb{F}$ を基本とした時に、右にスライドされたものは基礎群 $\mathbb{F}$ の各々と 16 の和で表されている。右下にスライドされたものは群の積 $(X_1\langle 6\rangle X_2\langle 7\rangle$ の計算方法) で求められる。それを左にスライドさせるには +16 すれば $(X_1\langle 6\rangle X_2\langle 7\rangle + 16)$ 求められる。同様に $\mathbb{F} \rtimes S_2 \cdots$ も同様に行っていくことで求められる。この時、正規部分群の有限列

$$\varphi(\{A\}) = \{\tilde{F}\} \lhd \varphi(\{A,C\}) = \{\tilde{F},\tilde{E}\} \lhd \varphi(\{A,B,C,D\}) = \{\tilde{F},\tilde{G},\tilde{E},\tilde{H}\} \lhd \varphi(D_4)$$
$$\lhd \mathbb{F} \lhd \mathbb{F} \rtimes S_2 \lhd \mathbb{F} \rtimes S_2 \rtimes S_2 \lhd \cdots \lhd \mathbb{F} \rtimes S_2 \rtimes S_2 \rtimes \cdots \rtimes S_2 = G[N]$$

が存在し、各商群が巡回群であるから $\mathbb{F} \rtimes S_2 \rtimes \cdots \rtimes S_2$ は多巡回群である。

4. 暗号化

(1) N ビットアルファベット化 (8 ビットから N ビットへ)

今回行う暗号化は基礎群と S_2 の半直積を使う。それを一般的に $G[N] = F \rtimes S_2 \rtimes S_2 \cdots \rtimes S_2$ とおき、$G[N]$ を基本とした暗号化について考える。$G[N]$ は、N ビットの数値で表すことができるものである。ある文字列をアスキー/シフト JIS キャラクターコードに変換したとき、これは 8 ビットまでを表すので、まずは N ビットで表さなければならない。
そこで、L を N と 8 の最小公倍数とおいた時、p を合体した数値とすると

$$p = \sum_{i=1}^{L/8} 256^{L/8-1} \times a_i \tag{4}$$

という式で表すことができる。$256^{L/8-1}$は 単位を計算している部分で、$\sum_{i=1}^{L/8} a_i$ はアルファベットの各桁を足し合わせている部分である。
以下演算//は商とすると、数値 p は

$$[A_0 = p//2^N//\cdots//2^N \bmod 2^N, \cdots, A_{L/N-1} = p//2^N \bmod 2^N, A_{L/N} = p \bmod 2^N] \tag{5}$$

という式で N ビットアルファベットにすることができる。

(2) 暗号化

暗号化の基本は 4.1 で得られたアルファベットと共通秘密鍵の積により実現でき、2^N 拡大の積表を用いて計算している。さらに暗号を強度にするため、積表で得られた数値ともう一つの共通秘密鍵の和を取ることにした。$\tilde{z_n}$ を求めたい暗号とし、4.1 で得られたアルファベットを $Z = [z_1, z_2, \cdots]$ とした時、これを暗号化するには、z_k と共通秘密鍵 v_1, v_2 を用いて、

$$\tilde{z_n} = (\langle z_n \rangle \langle v_1 \rangle + v_2) \bmod 2^N$$

という計算を施す。復号化は

$$z_n = \langle (\tilde{z_n} - t_2) \bmod 2^N \rangle \langle t_1 \rangle^{-1}$$

である。

(3) 8 ビットアルファベット化 (N ビットから 8 ビットへ)

暗号化された数値は N ビットで表されているので、Base64 変換するにはひとまず 8 ビットに直さなければならない。まず、N ビット で表された数値を L/N 個ず

つ合体させる計算方法は、

$$q = \sum_{i=1}^{L/N} (2^N)^{L/N-1} \times d_i \tag{6}$$

となる。合体した数値を $[Q_0, Q_1, \cdots]$ とする。次に、この合体した数値8ビットで表現するため $L/8$ 個に分解する計算方法は、

$$[B_0 = Q_i /\!/ 256 /\!/ \cdots /\!/ 256 \bmod 256, \cdots, B_{L/N-1} = Q_i /\!/ 256 \bmod 256, B_{L/N} = Q_i \bmod 256] \tag{7}$$

となる。

(4) Base64 の方式で文章化

最後に暗号文を可視化するために、Base64 の方式を用いる。

(5) 鍵交換

今回の鍵交換を暫定的に次のようにした。N はお互い分かっているものとし、a_1 は Alice の一つの秘密鍵であり、a_2 はもう一つの秘密鍵で、r はランダムな数とする。そこから Alice の Bob だけに対しての個人公開鍵はこのような計算をすることにする。

$$r \times (2^N)^2 + a_1 \times 2^N + a_2 \tag{8}$$

Bob は自分で b_1,b_2 の鍵を決めておく。Alice の個人公開鍵を Bob に渡した時、Bob は以下の計算で Alice の2つの秘密鍵を得ることができる。

$$a_1 = A/2^N \bmod 2^N, \quad a_2 = A \bmod 2^N \tag{9}$$

共通秘密鍵 t_1, t_2 は以下のように群の計算をすることにし、この時積の順番は名前のアルファベット順に決めた。

$$t_1 = \langle a_1 \rangle \langle b_1 \rangle, \quad t_2 = \langle a_2 \rangle \langle b_2 \rangle \tag{10}$$

今は Alice から Bob への一方向についてのみ述べたが，逆に Bob も同じ方式で Alice に公開鍵を送ることで同様に同じ秘密鍵を共有できる。

5. 具体例

$N = 6$ の時、$G[6] = F \rtimes S_2 \rtimes S_2$ となる。まず鍵交換について説明する。Alice の2つの秘密鍵を $a_1 = 20$,$a_2 = 32$ とし，ランダムな数を仮に $r = 7682905$ としておく。(8) より Alice の個人公開鍵を計算すると、$A = 31469180192$ となる。Bob は自分で $b_1 = 42, b_2 = 47$ の鍵を決めておく。Alice の個人公開鍵を Bob に渡した時、Bob は (9) より $a_1 = 20$,$a_2 = 32$ を得る事ができる。そして、共通秘密鍵は (10) より $t_1 = \langle 20 \rangle \langle 32 \rangle = 56$、$t_2 = \langle 42 \rangle \langle 47 \rangle = 11$ となる。

例として、平文「red 絨毯」をアスキー/シフト JIS キャラクターコードで数値に変換すると、[114, 101, 100, 227, 79, 159, 126] となる。

Lは8と6との最小公倍数なので$L = 24$となる。$L/8 = 3$であることから3つの数値を一つにまとめていく。この8ビットで表現された数値は7個しかないので3の倍数、つまり9個にしなければならない。よって、ダミーとして0を2ついれる([114, 101, 100, 227, 79, 159, 126, 0, 0])。(4)より、数値を合体させていくと、

$$\begin{array}{ccc} [114,101,100] & [227,79,159] & [126,0,0] \\ \downarrow & \downarrow & \downarrow \\ 7497060 & 14897055 & 8257536 \end{array}$$

となる。この合体した数値[7497060,14897055, 8257536]を(5)の方法で分解すると、

$$\begin{array}{ccc} 7497060 & 14897055 & 8257536 \\ \downarrow & \downarrow & \downarrow \\ [28,38,21,36] & [56,52,62,31] & [31,32,0,0] \end{array}$$

となる。これで、8ビットで表現された[114, 101, 100, 227, 79, 159, 126]を6ビットで表現された[28, 38, 21, 36, 56, 52, 62, 31, 31, 32, 0, 0]に変換することができた。

何らかの形で伝達された2つの共通秘密鍵t_1, t_2を用いて暗号化するが今回は$t_1 = 56, t_2 = 11$とすることに決めた。このアルファベットの数値列
[28, 38, 21, 36, 56, 52, 62, 31, 31, 32, 0, 0]を暗号化すると
[43, 36, 51, 37, 15, 21, 14, 44, 44, 40, 8, 8]になる。

それを6ビットで表現された[43, 36, 51, 37, 15, 21, 14, 44, 44, 40, 8, 8]を8ビットに変換する。(6)より、数値を合体させていくと、

$$\begin{array}{ccc} [43,36,51,37] & [15,21,14,44] & [44,40,8,8] \\ \downarrow & \downarrow & \downarrow \\ 11422949 & 4019116 & 11698696 \end{array}$$

となる。この合体した数値[11422949, 4019116, 11698696]を(7)の方法で分解すると、

$$\begin{array}{ccc} 11422949 & 4019116 & 11698696 \\ \downarrow & \downarrow & \downarrow \\ [174,76,229] & [61,83,172] & [178,130,8] \end{array}$$

となる。これで6ビットで表現された[43, 36, 51, 37, 15, 21, 14, 44, 44, 40, 8, 8]を8ビットで表現された[174, 76, 229, 61, 83, 172, 178, 130, 8]に変換することができた。
これをBase64の方式で文章化するとrkzlPVOssoIIとなる。

6. シミュレーションプログラムでの群計算

このプログラムはrubyで作成したものである。特徴的な部分として基礎群$\mathbb{F}$を作成するための関数の定義をあげておく。

< プログラム解説 >

A,B,C,D,E,F,G,Hは3.1で示したD_4の元であり、このプログラムでは行列表現にしている。関数suuはA,B,C,D,E,F,G,Hを$0,1,2,3,4,5,6,7$の数値に変換するものである。T[0][0],T[0][1],T[1][0],T[1][1]はそれぞれ$c_{1,1}, c_{1,2}, c_{2,1}, c_{2,2}$に対応している。「^」はビット演算子といい、xx ^ yyはxxとyyの2進数の各桁の排他的論理和である。yy=0の時、基礎群の上部を計算しており、yy=1の時は下部を計算しており、それを戻り値としている。

```
def kake0(v,w) #基礎群Fの積
  yy=v/8; y=D4[v%8]
  xx=w/8; x=D4[w%8]
  if yy==0 then (suu(y*F*x*F*T[0][(xx^yy)^1])+(xx^yy)*8)
  else (suu(y*B*x*D*T[1][(xx^yy)^1])+(xx^yy)*8) end
end
```

以下のプログラムは基礎群$\mathbb{F}$とS_2との半直積をとっていったものの積表の関数である。再帰関数になっていることが分かるので、$\mathbb{F} \rtimes S_2 \rtimes \cdots \rtimes S_2$も計算できる。

< プログラム解説 >

関数haniは2^Nから$2^{N+1}-1$までの数値を2^Nに変換する再帰的関数である。(ただし、$N > 4$, 0から31までの数値は$16(=2^4)$に変換する。) y <16かつx <16の時は基礎群計算のkake0を呼び出している。y<hani(x)の時は、積表の右上の部分を計算している。x<hani(y)の時は積表の左下を計算している。それ以外の時は積表の右下を計算している。

```
def kake(y,x) #半直積拡大の積
  if (y <16)and(x <16)
      kake0(y,x)
      elsif(y<hani(x))
        kake(y,(x%hani(x)))+hani(x)
      elsif(x<hani(y))
        kake(kake(kake((y%hani(y)),6),x),7)+hani(y)
      else
        kake(kake(kake(y%hani(y),6),(x%hani(x))),7)
  end
end
```

おわりに

今回我々が取り扱ったpolycyclic groupは日本ではあまり知られていないようで、岩波の数学辞典にさえ載っていなかった。polycyclic groupを多巡回群としたが、この訳も正確ではないかもしれない。逆に、Schreier拡大について正確に述べた代数学の日本語テキストは見当たらなかったが、数学辞典には正確に記されていたことを付記しておく。このあたり、この概念を環に拡張した接合積や拡大の議論が作用素環論の分野で常識化していることとは対照的である。

今回の暗号化はSchreier拡大を1度だけしか使わず後は半直積をとっていったので、群計算が再帰的に定義されて簡単になった反面、元は変化せずに拡大していくので、暗号の強度的にはまだまだかもしれない。今後、Schreier拡大による単位元の移動を利用して、より強固な暗号化をめざし、さらに量子暗号など他の手法と組み合わせれば、さらに強度が高くなると考えられるので今後の課題にしておきたいと思う。

また、今回鍵交換を暫定的に決めたが、もう少し鍵交換についても強固な方式を考えていきたい。他の方式として、[1]にconjugate（内部自己同形）をうまく利用した**Arithmetica鍵交換**という方式が提案されている。SとTをGの有限生成部分群とし、2つの生成元をそれぞれ$\{s_1,\cdots s_n\}$,$\{t_1,\cdots t_n\}$として、二つの情報はあらかじめ共有しているものとする。ここでは共役x^yは$y^{-1}xy$を意味することにする。今、AliceとBobの2人が1つの鍵を共有したいとする。群Gとその部分群S,Tやこれらの生成元は公開された情報とする。このとき$k_j,\ell_j\in\mathbb{N}$, $a,b\in G$とし、

Aliceは、生成元での秘密の要素$a=s_{i_1}^{k_1}\cdots s_{i_n}^{k_n}\in S$を選び、$t_1^a,\cdots,t_n^a$を公開

Bobは、生成元での秘密の要素$b=t_{i_1}^{\ell_1}\cdots t_{i_n}^{\ell_n}\in T$を選び、$s_1^b,\cdots,s_n^b$を公開

すれば、k_jは単なる指数なので$(t^a)^{k_j}=(t^{k_j})^a$となり、

$$[a,b]=(b^{-1})^ab=((t_{i_1}^{\ell_1}\cdots t_{i_n}^{\ell_n})^a)^{-1}b=_{(*)}((t_{i_1}^a)^{\ell_1}\cdots(t_{i_n}^a)^{\ell_n})^{-1}b \qquad \text{Bob側}$$

$$=a^{-1}a^b=a^{-1}((s_{i_1}^{k_1}\cdots s_{i_n}^{k_n}))^b=a^{-1}(s_{i_1}^b)^{a_1}\cdots(s_{i_l}^b)^{a_l} \qquad \text{Alice側}$$

で、公開情報と秘密鍵で共通秘密鍵をそれぞれ得る事ができる。今後それも考慮して、さらに新しい方式を取り入れていきたいと考えている。

参考文献

[1] Bettina Eick ,Delaram Kahrobaei ; Polycyclic groups: A new platform for cryptology? http://turnbull.dcs.st-and.ac.uk/circa/Preprints/bedk-2004-PGNPC.pdf

[2] 彌永 昌吉 , 彌永 健一: 代数学 (岩波全書 285),1976.