SCIS 2010 The 2010 Symposium on Cryptography and Information Security
Takamatsu, Japan, Jan. 19-22, 2010
The Institute of Electronics, Information and Communication Engineers

共通鍵１２８ビットブロック暗号 HyRAL
The 128bit blockcipher HyRAL

平田 耕蔵*
Kouzou Hirata

あらまし 先に発表した共通鍵ブロック暗号ＨｙＲＡＬ[１]では、差分確率および線形確率において安全性を保証する上界値が得られなかった[２]。その為、安全性を確保すべく改良を行い再度発表するものである。今回の改良の主たるものは、ｓ－ｂｏｘと基本関数となる *f* 関数である。その他は、先に発表したものと設計概念は異なっていない。データ長１２８ビット、鍵長１２８ビット、１９２～２５６ビットをサポートしたもので、一般化Ｆｅｉｓｔｅｌ型構造を採ったものである。

キーワード ＨｙＲＡＬ、一般化Ｆｅｉｓｔｅｌ型、ｓ－ｂｏｘ、*f* 関数

1 記号の説明

１．１ データ構造

x（1bit）：1または0

x（8bit）：斜体小文字

x =（[上位]x_7、x_6、x_5、x_4、x_3、x_2、x_1、x_0[下位]）

X（32bit）： 斜体太字

X =（[上位]*x0*、*x1*、*x2*、*x3* [下位]）

X（128bit）：大文字太字

X =（[上位]*X0*、*X1*、*X2*、*X3* [下位]）

１．２ 演算

⊕：Ｘｏｒ

＋：算術加算

≫i：iビット右シフト

8bit データの乗算は、GF(2^8)の元を多項式表現し、法多項式x^8+x^4+x^3+x+1を使用。

多項式表現においては、0ビット目（最下位）をx^0の係数とする。

１．３ 関数名

G1、G2、F1、F2（128bit入力）

基本関数 f_i（32bit入力）

１．４ 鍵の表示

Rki（128bit）：ラウンド鍵（*i*=1～9）

IKi（128bit）： f_i 関数入力鍵（*i*=1～6）

KMi（128bit）：中間鍵（*i*=1～4）

OKi（128bit）：秘密鍵（*i*=1～2）

2 HyRAL の構造概要

２．１ HyRAL の全体構造

HyRAL の全体構造には鍵長 128bit の場合と、129～256bit が存在する。[図８と図９を参照]

４系列の一般化 Feistel 型で G1、G2、F1、F2 と４つの異なるアルゴリズムの関数を接続している。これまでの Feistel 型とは異なり拡大鍵を逆順に使用し同一のアルゴリズムで復号する方法ではなく、複合時には各々の逆関数を使用して復号する。

２．２ 基本関数（ f_i関数）

入力 32bit 出力 32bit のものであり入力のバイト転置により８種類ある。

f_i（ *i*= 1、2、3、4、5、6、7、8）

[詳細は節４を参照]

２．３ 拡大関数

基本関数（ f_i関数）を用いた G1、G2、F1、F2 の４種類の拡大関数がある。[詳細は節５を参照]

２．４ 鍵生成部

鍵処理モードでは OKi と定数 Li（*i*= 1、2、3）を G1、G2 関数に入力しその出力を KMi とする。

[詳細は節７を参照]

拡大鍵の割り当てでは KMi から拡大キーである RKi と IKi を生成する。[詳細は節８を参照]

*株式会社ﾛｰﾚﾙｲﾝﾃﾘｼﾞｪﾝﾄｼｽﾃﾑｽﾞ，東京都港区虎ノ門 1-1-10,
Laurel Intelligent Systems Co.,Ltd, 1-10 Toranomon 1-chome Minato-ku Tokyo, k-hirata2453@lbm.co.jp

3　s-box の生成

s-box は非線形層である GF(2^8)上の逆関数 $s = z^{-1}$(ただし $z^{-1}=0$)と線形関数であるアフィン変換式１とグレイコード変換式２の組み合わせで構成される。（図１、２）

s-box の最大線形及び最大差分確率は 2^{-6} である。

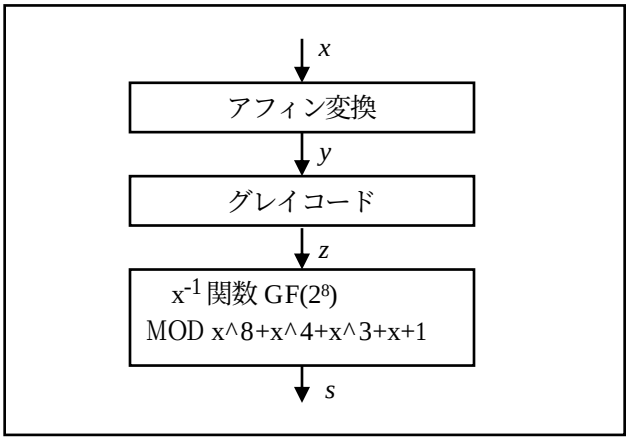

図１

アフィン変換 $y=(x+64) \bmod 256$

$$\begin{pmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

式１

グレイコード $z = y \oplus (y \gg 1)$

$$\begin{pmatrix} z_7 \\ z_6 \\ z_5 \\ z_4 \\ z_3 \\ z_2 \\ z_1 \\ z_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix}$$

式２

・入力 x の上位 4bit
・入力 x の下位 4bit

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	5e	d3	af	36	43	a6	49	33	93	3b	21	91	df	47	f4
1	b6	70	06	d0	81	82	fa	a1	10	b5	3c	ba	97	85	b7	79
2	ed	5c	ca	05	87	bf	24	4c	51	ec	17	61	22	f0	3e	18
3	a7	64	13	ab	e9	09	25	54	2d	31	69	f5	37	67	fe	1d
4	0b	28	a3	2f	e4	0f	d4	da	1b	fc	e6	ac	53	04	27	a9
5	94	8b	d5	c4	90	6b	f8	9d	c5	db	ea	e2	ae	63	07	7a
6	5b	23	34	38	03	8c	46	68	cd	1a	1c	41	7d	a0	9c	dd
7	08	4e	e3	d7	1e	b3	50	5d	c6	0e	ad	cf	d6	eb	0d	b1
8	fb	7c	c3	2e	65	48	b8	8f	ce	e7	62	d2	12	4a	c8	26
9	a5	8e	3d	76	86	57	bc	bd	11	75	71	78	1f	ef	e0	0c
A	de	6a	6d	32	84	72	8a	d8	f9	dc	9a	89	9f	88	14	2a
B	9b	9e	d9	95	b9	a4	02	f7	96	73	56	be	7f	80	7e	83
C	00	01	f6	8d	7b	d1	52	cb	b0	e1	c7	e5	29	c0	4f	e8
D	58	3f	cc	fd	ee	b2	40	ff	99	2b	5f	60	aa	4b	b4	74
E	2c	45	6c	92	66	42	39	f3	77	bb	19	59	20	6f	35	f2
F	c1	0a	15	98	a2	c2	44	30	55	4d	c9	a8	5a	f1	6e	3a

図２

4　基本関数(f_i関数)

f_i関数は、SP 構造の 32bit 入出力関数で、最大線形・差分確率が 2^{-6}の 8 ビット S-box を 4 並列で用い、P 層は 4 バイト入出力の MDS 行列とする。（図３）

ＡＥＳの様に、巡回型の MDS 行列と同一 s-box の並置の S 層を用いた場合、f_i関数の入力がバランスしている時、出力もバランスしている性質を持つ。

f_i 関数に供給される段鍵がバランスしている場合、32bit 変数 $X = (x_0, x_1, x_2, x_3)$ において、$x_0 = x_1 = x_2 = x_3$ が成り立つ時、X はバランスしていると呼ぶ。複数段の f_i関数縦接続においても入出力のバランス性が維持される。

バランスしている段鍵の発生確率は、無視できるという理由で、この性質を考慮する必要は無いのかもしれないが、未知の攻撃法に結びつく可能性も考え、HyRAL では、非巡回型の MDS 行列を用いることにする。但し、関数に入力される直前に転置を行い、転置の仕方が８通りあるので、転置種類毎に *T1*～*T8* と表記しておく。

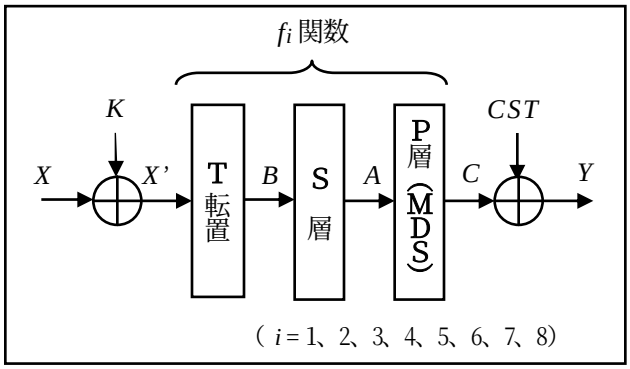

図３

図３において各々の 32bit 変数は、8bit 変数では式３から式１０で表され、Ｓ層では B が３節で述べた s-box にて A に変換される。（式７）
また CST は定数。（式９）

$X = (x_0、x_1、x_2、x_3)$……式３
$K = (k_0、k_1、k_2、k_3)$……式４
$X' = (x_0'、x_1'、x_2'、x_3') = X \oplus K$……式５
$B = (b_0、b_1、b_2、b_3)$……式６
$A = (a_0、a_1、a_2、a_3)$
$=(s\text{-}box(b_0)、s\text{-}box(b_1)、s\text{-}box(b_2)、s\text{-}box(b_3))$
……式７
$C = (c_0、c_1、c_2、c_3)$……式８
$CST = (0x11、0x22、0x44、0x88)$……式９
$Y = (y_0、y1、y_2、y_3) = C \oplus CST$…式１０

バイト転置 $B=Ti$

$T1$：$B=(x'_0、x'_1、x'_2、x'_3)$
$T2$：$B=(x'_1、x'_2、x'_3、x'_0)$
$T3$：$B=(x'_2、x'_3、x'_0、x'_1)$
$T4$：$B=(x'_3、x'_0、x'_1、x'_2)$
$T5$：$B=(x'_3、x'_2、x'_1、x'_0)$
$T6$：$B=(x'_2、x'_1、x'_0、x'_3)$
$T7$：$B=(x'_1、x'_0、x'_3、x'_2)$
$T8$：$B=(x'_0、x'_3、x'_2、x'_1)$

Ｐ層（ＭＤＳ）、要素の計算は GF(2^8)

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 3 & 3 & 2 & 1 \\ 1 & 2 & 2 & 2 \\ 7 & 3 & 1 & 2 \\ 7 & 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

式１１

5　拡大関数 G1、G2、F1、F2

G1 および G2 関数を図４、５に示す。各ラウンドで f_i 関数を１回使用する。
F1 および F2 関数を図６、７に示す。各ラウンドで、f_i 関数を２回使用する。
復号時に使用される、これらの関数の逆関数は、図の下端を入力として計算する。図４を例に説明すれば、$X0$、$X1$、$X2$ から $f4$ 関数入力を計算し、その出力を求めて１ラウンド遡る。

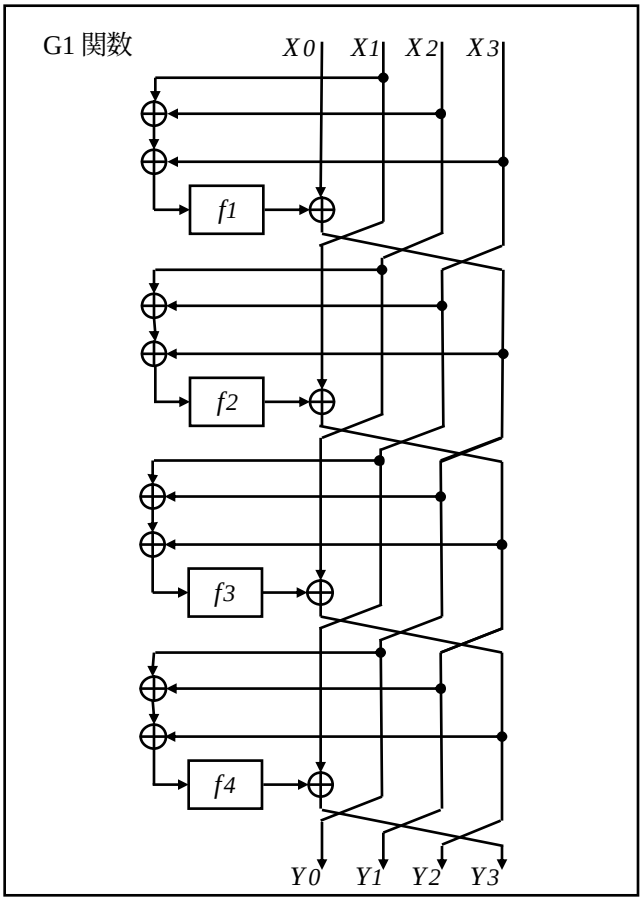

図４

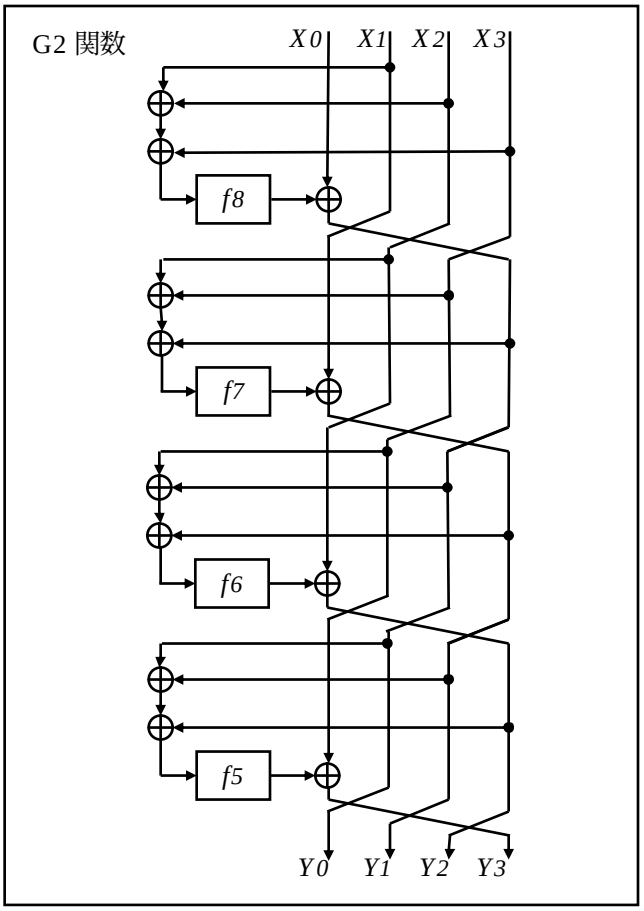

図５

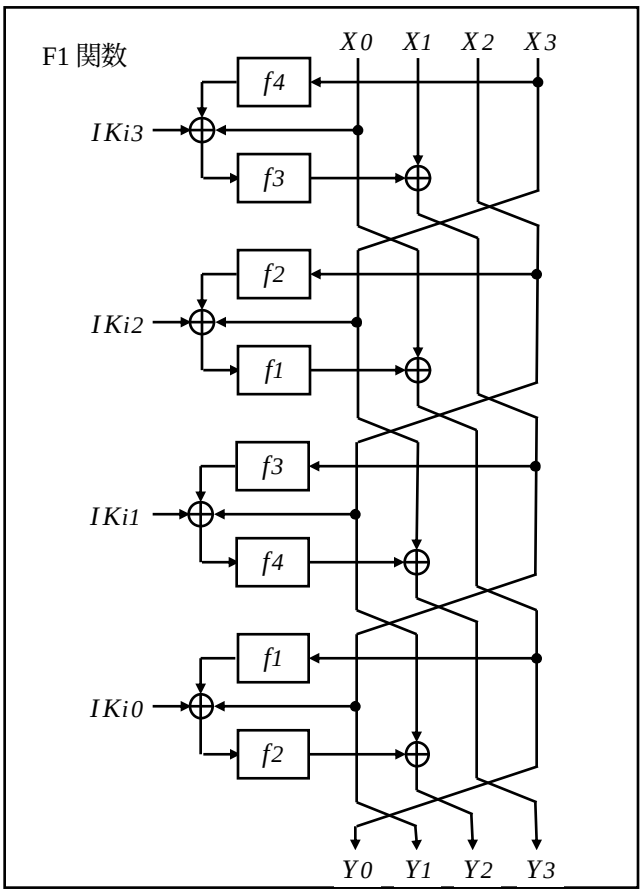

図6

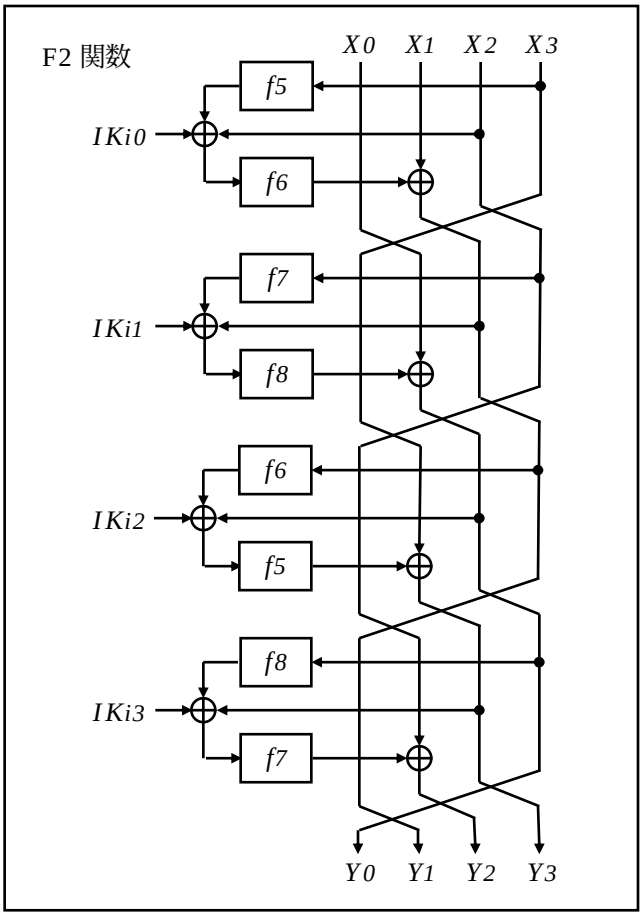

図7

6 HyRAL の全体構造

HyRAL の鍵長 128bit の場合は図８にて示し、129、256bit の場合は図９にて示す。

鍵長 128bit の場合は、ラウンド鍵 RK1～RK6 の６種類と f_i 関数入力鍵 IK1～ IK4 の４種類を使用する。

鍵長 129、256bit の場合は、ラウンド鍵 RK1～RK9 の９種類と f_i 関数入力鍵 IK1～ IK6 の６種類を使用する。

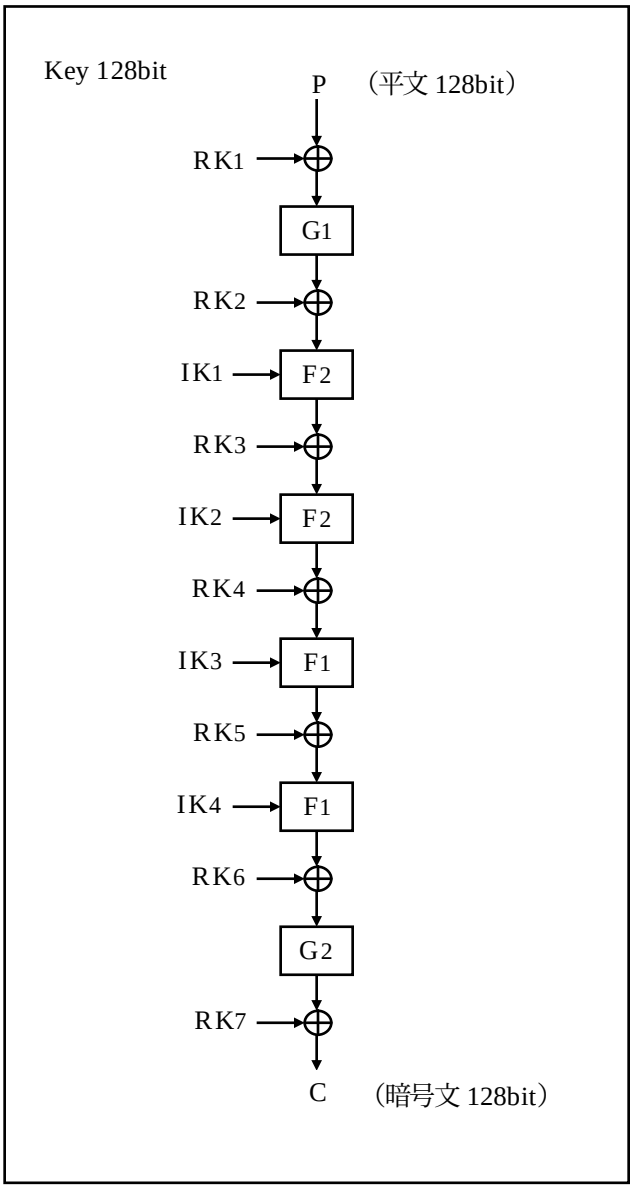

図8

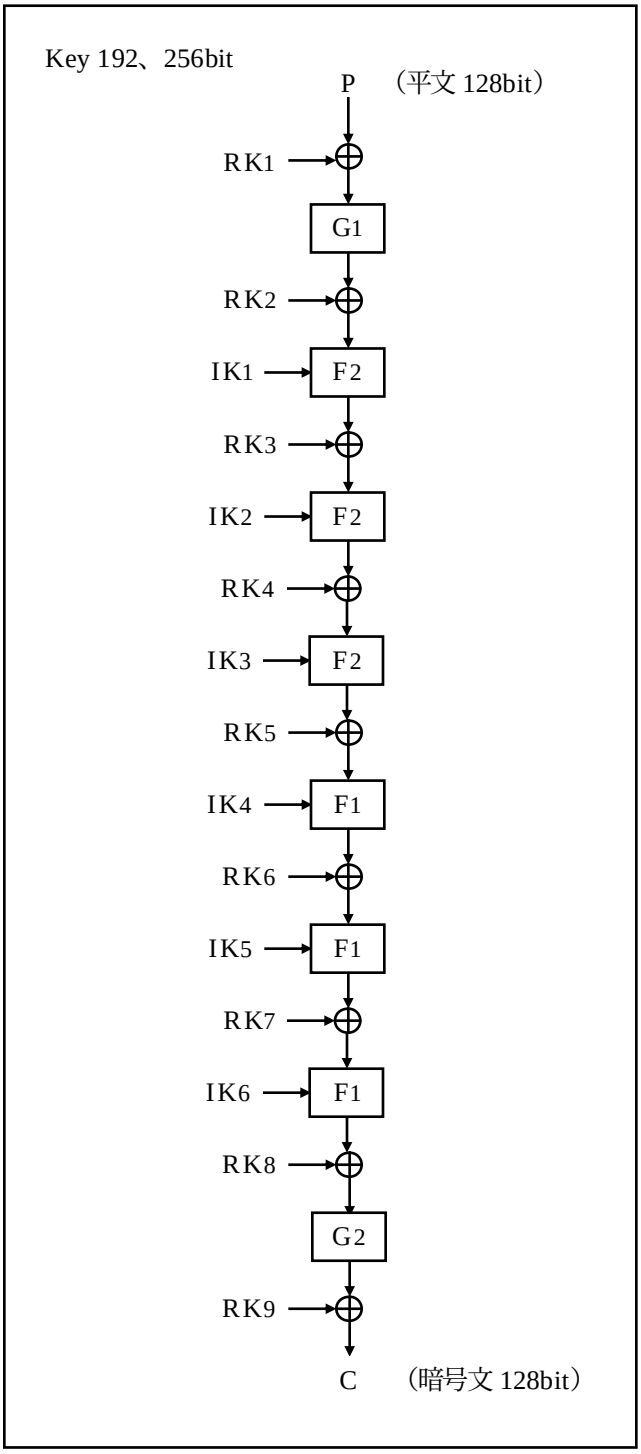

図９

7　鍵処理モード

G1 、G2 関数を使用して、秘密鍵 OK から中間鍵 KMi(Key material)を作成し、それを元に、暗号化変換の各ラウンドにおいて使用する拡大鍵(RKi、IKi)を生成する。秘密鍵長が 128 bit 時と、192bit および 256 bit 時では、異なる鍵処理モードを使う。前者を Single Key Mode,後者を Double Key Mode と呼ぶ。

①Single Key Mode(秘密鍵“ OK ”128bit)

Y1 = G1(L1 ⊕ 0x00)…… 式１２
Y2 = G2(L1 ⊕ Y1)…… 式１３
Y3 = G1(OK ⊕ Y2) …… 式１４
KM1= Y4 = G2(OK ⊕ Y3) …… 式１５
KM3= Y5 = G1(OK ⊕ Y4) …… 式１６
KM2= Y6 = G2(OK ⊕ Y5) …… 式１７
KM4= Y7 = G1(OK ⊕ Y6) …… 式１８

②Double Key Mode

(秘密鍵“ OK1 ”“ OK2 ”128bit)

Z1 = G1(L2 ⊕ 0x00) …… 式１９
Z2 = G2(L2 ⊕ Z1) …… 式２０
Z3 = G1(OK1 ⊕ Z2) …… 式２１
Z4 = G2(OK1 ⊕ Z3)…… 式２２
Z5 = G1(OK1 ⊕ Z4) …… 式２３
Z6 = G2(OK1 ⊕ Z5)…… 式２４
Z7 = G1(OK1 ⊕ Z6) …… 式２５
W1 = G1(L-3 ⊕ 0x00) …… 式２６
W2 = G2(L-3 ⊕ W1)…… 式２７
W3 = G1(OK2 ⊕ W2) …… 式２８
W4 = G2(OK2 ⊕ W3)…… 式２９
W5 = G1(OK2 ⊕ W4) …… 式３０
W6 = G2(OK2 ⊕ W5)…… 式３１
W7 = G1(OK2 ⊕ W6) …… 式３２
KM1 = Z4 ⊕ W4 ……式３３
KM2 = Z6 ⊕ W6 ……式３４
KM3 = Z5 ⊕ W5 ……式３５
KM4 = Z7 ⊕ W7……式３６

ここで、L1、L2、L3 は LABEL と呼ぶ定数であり、以下の値をとる。

L1 = (48 59 52 41 4C 40 40 40 00 00 00 00 00 00 00 12)
L2= (48 59 52 41 4C 40 40 40 00 00 00 00 00 00 00 22)
L3 = (48 59 52 41 4C 40 40 40 00 00 00 00 00 00 00 32)

LABEL が定数であり式１３、式２０、式２７は事前計算可能である。結果を示せば、

Y2 = (62 8c cd a0 3b 15 65 c1 3b ad 2d 4f b8 80 6a c5)
Z2 = (f9 25 1a 23 65 cd 3c 2e 80 66 cb bb fe 31 6b 7b)
W2=(5d e2 86 25 65 6b 71 ff 9f fb 1e 12 ee f1 27 f5)

8　拡大鍵の割り当て

各ラウンドの拡大鍵 RKi、IKi は、中間鍵 KMi を利用して以下のように求める。各々の拡大鍵は KMi の二

つを合成(Xor)して割り当てるが、KMi を 32bit 単位で区切った４つのブロックを入れ替えて Xor をとる。

各中間鍵 KMi ブロックの種類には下記の６種類があり、式３７～式４２で示す。

KMiⅠ=(KMi_0、KMi_1、KMi_2、KMi_3) ･式３７
KMiⅡ=(KMi_1、KMi_2、KMi_3、KMi_0) ･式３８
KMiⅢ=(KMi_2、KMi_3、KMi_0、KMi_1) ･式３９
KMiⅣ=(KMi_3、KMi_0、KMi_1、KMi_2) ･式３０
KMiⅤ=(KMi_3、KMi_2、KMi_1、KMi_0) ･式４１
KMiⅥ=(KMi_0、KMi_3、KMi_2、KMi_1) ･式４２

①Single Key Mode
RK1 =KM3Ⅴ⊕KM4Ⅰ ･･･ 式４３
RK3 =KM3Ⅰ⊕KM4Ⅲ･･･ 式４４
RK2 =KM1Ⅵ⊕KM2Ⅱ ･･･ 式４５
RK4 =KM1Ⅰ⊕KM4Ⅴ ･･･ 式４６
RK5 =KM1Ⅰ⊕KM2Ⅲ･･･ 式４７
RK6 =KM3Ⅵ⊕KM4Ⅱ･･･ 式４８
RK7 =KM1Ⅴ⊕KM2Ⅰ････ 式４９
IK1 =KM1Ⅱ⊕KM4Ⅵ････ 式４０
IK4 =KM1Ⅲ⊕KM4Ⅰ････ 式５１
IK2 =KM3Ⅳ⊕KM4Ⅳ･･･ 式５２
IK3 =KM1Ⅳ⊕KM2Ⅳ ･･･ 式５３

②Double Key Mode
RK1 =KM3Ⅴ⊕KM4Ⅰ ･･･式５４
RK2 =KM1Ⅵ⊕KM2Ⅱ ･･･式５５
RK3 =KM3Ⅰ⊕KM4Ⅲ･･･式５６
RK4 =KM3Ⅳ⊕KM4Ⅳ･･･式５７
RK5 =KM1Ⅰ⊕KM4Ⅴ････式５８
RK6 =KM1Ⅳ⊕KM2Ⅳ ･･･式５９
RK7 =KM1Ⅰ⊕KM2Ⅲ ･･･式５０
RK8 =KM3Ⅵ⊕KM4Ⅱ ･･･式６１
RK9 =KM1Ⅴ⊕KM2Ⅰ ･･･式６２
IK1 =KM1Ⅱ⊕KM4Ⅵ････式６３
IK2 =KM2Ⅴ⊕KM3Ⅰ ･･･式６４
IK3 =KM2Ⅵ⊕KM3Ⅱ ･･･式６５
IK4 =KM2Ⅰ⊕KM3Ⅲ･･･式６６
IK5 =KM2Ⅳ⊕KM3Ⅳ･･･式６７
IK6 =KM1Ⅲ⊕KM4Ⅰ････式６８

9 安全性について

今回の改良により、8bit トランケーションによる最大線形確率および最大差分確率の上界は、次のように向上し、安全性を示すことが出来た。

Single Key Mode (秘密鍵 128bit)でそれぞれ 2^{-228}、2^{-222}、Double Key Mode (秘密鍵 192bit および 256 bit)でそれぞれ 2^{-318}、2^{-342}である。

今後他の攻撃に対する耐性についても評価していく予定である。

謝辞

今回の改良に当たっては有力な助言を頂きました東京理科大学　金子敏信教授　五十嵐保隆助教および金子研究室の諸兄に感謝致します。

参考文献

[1]平田耕蔵、共通鍵暗号 HyRAL16、信学技報　ISEC 2006-76（2006-09）P29
[2] 五十嵐保隆・金子敏信・福林直人、共通鍵ブロック暗号 HyRAL の線形攻撃耐性評価、信学技報　ISEC 2006-157 （2007-03）P99