軽量型ブロック暗号 Halka の差分パス解析

中澤 俊*　　五十嵐 保隆*　　金子 敏信*

あらまし　Halka は 2014 年に Sourav Das によって提案された軽量型ブロック暗号である。データブロック長は 64bit、鍵長は 80bit である。非線形処理に 8bit S-box を使用し、線形処理に bit shuffle を持つ。提案者による差分パス解析では各段における active S-box 数は 2 個と見積もられており、差分攻撃に使用可能な差分パスは 5 段までとなっている。本稿では Halka が bit shuffle を持つことに着目し、各段の S-box の入出力差分が 1bit active となる最大差分特性確率を導出する。評価にはトレリス表現を用い、最大差分特性確率を与える差分パスを探索した。結果として、Halka の最大差分特性確率はシングルパスにおいて2^{-60}で 10 段まで差分攻撃に使用可能、マルチパスを考慮した場合では$2^{-62.58}$で 13 段まで差分攻撃に使用可能となり、提案者による評価を大きく上回る結果となった。

キーワード　Halka, ブロック暗号, bit shuffle, 1bit active, 差分攻撃

1　はじめに

Halka は 2014 年に Sourav Das によって提案された SPN 構造の軽量型ブロック暗号である[1]。演算要素として 8bit S-box を使用した非線形処理、ビット単位の線形処理、排他的論理和で構成されており、データブロック長は 64bit、鍵長 80bit である。今、ある関数（例えば S-box）に入力される差分またはある関数から出力される差分が非零であることを active と呼ぶこととすると、提案者による差分パス解析では active S-box 数が 1 段当たり 2 個と見積もられ、差分攻撃に使用可能な差分パスは 5 段までとなっている。その一方で、S-box の入力差分または出力差分を 2 進数シンボルと見たときに、そのハミング重みが 1 であるとき、差分は 1bit active であると呼ぶこととし、S-box の入出力差分が 1bit active となれば線形処理によって差分が拡散することはないので、1 段当たりの active S-box 数を 1 つにすることができ、攻撃可能な段数の増加が期待できる。そこで本稿では、S-box の入出力差分が 1bit active となる差分確率の調査をし、最大差分特性確率を与える差分パス解析を行う。

2　Halka のデータ撹拌部

図 1 に Halka のデータ撹拌部を示す。64bit の段鍵$K_i(i = 1,2,3,\cdots,24)$との排他的論理和、S 層と P 層からなる段関数を 24 回繰り返す（ただし最終段の最後に段鍵K_{25}と排他的論理和をする）。段鍵K_iは秘密鍵を元に鍵生成部で生成される。

＊　東京理科大学大学院理工学研究科電気工学専攻

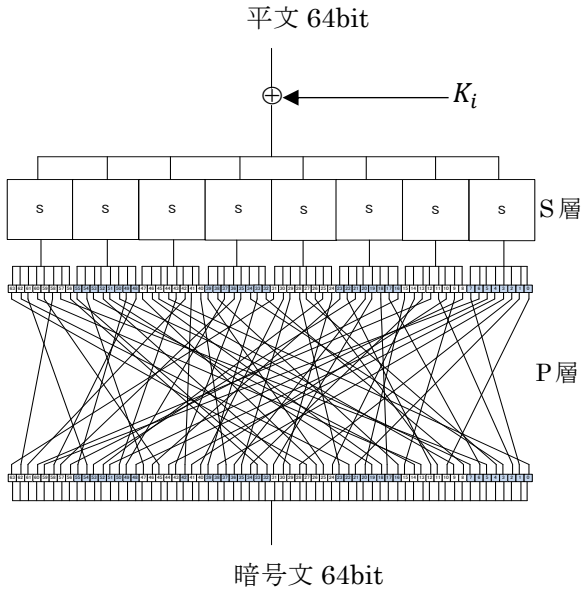

図 1　Hlaka のデータ攪拌部

1.1　段関数

Halka の S 層は 64bit の入力を 8 つの byte 列に分割し、それぞれに S-box を適用する。その後 P 層で bit shuffle を行う。S-box を表 1 に示す。最上位の行は入力 8bit 中の下位の 4bit を 16 進数で表し、左端の列が上位の 4bit を表している。行と列の交点が出力に対応している。表 2 は P 層の入力ビットを右からX番目、出力ビットを右からY番目$(X, Y = 0,1,2,\cdots,63)$としたときの bit shuffle の線形変換マッピングを表している。鍵生成部の構造は差分特性確率に影響しないため、本稿では説明を省く。

表 1　Halka の S-box

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

表 2　線形変換マッピング

X	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
Y	10	21	28	38	44	48	59	1	51	15	41	2	60	34	24	20	56	6	17	31	36	53	12	46	30	52	11	4	23	35	40	63
X	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Y	8	39	3	43	57	49	16	25	37	42	61	50	0	9	18	26	58	55	7	19	29	14	47	32	33	5	62	45	13	54	22	27

3　差分確率と差分特性確率

差分攻撃とは、入力を変化させたとき、出力の変化の分布に偏りがある場合に行うことができる暗号解読手法である。ここでは、差分攻撃で用いる差分パスの解析のために必要となる差分確率と差分特性確率についてまとめる。

3.1　差分確率

2 つのn bits データXとX^*の差分ΔXは式(1)で定義される[2]。

$$X \oplus X^* = \Delta X \tag{1}$$

関数$S(X)$の入力差分ΔXに対し、出力差分がΔYとなる確率$DP_s(\Delta X \to \Delta Y)$は式(2)で定義される。

$$DP_s(\Delta X \to \Delta Y) = \frac{\#\{X \in (0,1)^n \mid S(X) \oplus S(X \oplus \Delta X) = \Delta Y\}}{2^n} \tag{2}$$

ここで、$\#\{X \in (0,1)^n \mid S(X) \oplus S(X \oplus \Delta X) = \Delta Y\}$ は2^n通りのすべての入力対$(X, X^*) = (X, X \oplus \Delta X)$ に対し、S-box の出力差分がΔYとなる出現頻度を表す。Halka の S-box の最大差分確率は2^{-6}であることが知られている[1]。

3.2　最大差分特性確率

式(2)を用いてブロック暗号全体の最大差分確率を計算し、差分攻撃に対する強度指標とすることが正確な評価となるが、計算量の問題で困難である。そのため一般的には最大差分特性確率を強度指標とする。段関数FをR回繰り返す暗号系の最大差分特性確率DCP_{max}はi段目の入力差分をΔX_i、出力差分をΔY_iとしたとき$\Delta X_i = \Delta Y_{i-1}$となる差分確率$DP_F(\Delta X_R, \Delta Y_R)$に対し、各確

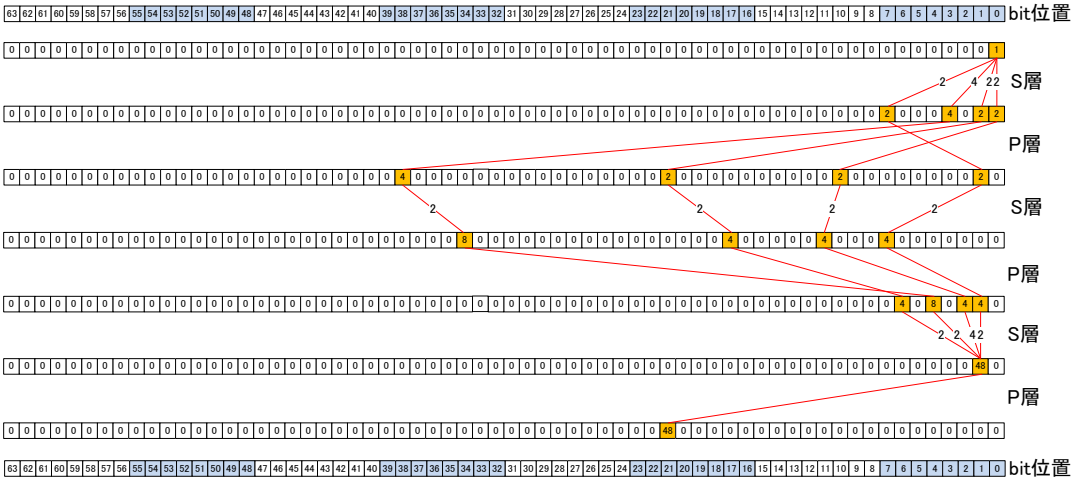

図 2　マルチパスの一例

率の積の最大値として式(3)で定義される。

$$DCP_{max} = \max_{\Delta X_0 \neq 0, \Delta X_1, \cdots, \Delta X_R} \prod_{i=1}^{R} DP_F(\Delta X_{i-1} \rightarrow \Delta X_i) \qquad (3)$$

ここで途中段の伝播状態$\Delta X_0 \rightarrow \Delta X_1 \rightarrow \cdots \Delta X_R$を差分パスという。また、2 段目以降の入力差分がある特定のΔX_i以外でも最終段の出力差分がΔX_Rとなる場合がありΔX_0からΔX_Rに至るパスは通常、複数通り存在する。これら複数通りのパスをマルチパスという。差分は 2 つの平文組の排他的論理和なので攻撃対象とする暗号のブロック長をNとしたとき2^N以上の差分は用意できない。そのため差分攻撃に使用可能な差分パスの範囲は$DCP_{max} > 2^{-N}$となる場合である。

4　差分パスの解析方法

差分パスにおいて、0 ではない差分が入力される S-box の数を active S-box 数と呼ぶ。本節では各段の active S-box 数が 1 個となる差分パスの探索を行い、最大差分特性確率の向上を試みる。そこで、まず S-box の入出力差分が 1bit active となる差分確率を求め、その結果を元にトレリス表現を用いてデータ撹拌部全体の差分パスの最大差分特性確率を導出する。

4.1　S-box の入出力差分が 1bit active となる差分確率の解析

式(2)を用いて S-box に 1bit active の入力差分を入れたときに 1bit active となる出力差分の出現頻度を調査すると、結果として表 3 が得られた。表 3 の 10 進数表記は式(2)の右辺の分数の分子を表している。分母は2^8である。Halka の S-box の最大差分確率は$2^{-6} = \frac{4}{2^8}$なので、入出力差分が最大差分確率で 1bit active となる組が 4 組存在することが分かる。

表 3　S-box の入出力差分が 1bit active となる差分の出現頻度

出力差分＼入力差分	0x1	0x2	0x4	0x8	0x10	0x20	0x40	0x80
0x1	2	2	2	4	0	0	0	2
0x2	2	2	4	2	2	2	2	2
0x4	2	4	2	2	0	0	2	2
0x8	4	2	2	0	0	2	2	2
0x10	0	2	0	0	0	2	0	0
0x20	0	2	0	2	2	2	0	0
0x40	0	2	2	2	0	0	2	2
0x80	2	2	2	2	0	0	2	0

4.2　マルチ差分パス探索アルゴリズム

差分パス及び最大差分特性確率を求める手法としてトレリス表現を用いる。各段の入力差分値を状態とし、ある段から次の段への遷移コストを差分確率と考え、トレリス線図を描くことで繋がる差分パスを求め、その中から最大差分特性確率を与える差分パスを探索する。また、すべての入力差分に対して取り得るマルチパスの総和を計算し、

最大差分特性確率の向上を試みる。$n$bit ブロック暗号に入力差分ΔX_0を入力したとき最終段の出力差分がΔX_Rとなる全てのマルチパスの総和による差分特性確率は式(4)で表される。

$$DCP = \sum_{\Delta X_1=0}^{2^n-1} \sum_{\Delta X_2=0}^{2^n-1} \cdots \sum_{\Delta X_{R-1}=0}^{2^n-1} \prod_{i=1}^{R} DP_F(\Delta X_{i-1} \to \Delta X_i) \quad (4)$$

本稿では各段の入出力差分が 1bit active となるマルチパスの総和を計算し、最大差分特性確率を導出する。従って、ΔX_iの値は実際には 64 種類に制限されている。これは差分確率の高いパスのみに焦点を絞り、差分確率の低いパスを無視することにより、計算困難な状況を回避している。トレリス線図の前状態が保持している差分特性確率と次状態への遷移に伴う差分確率の積を計算し、これを全ての前状態について総和をとったものが次状態の差分特性確率となる。従って最終状態は式(4)に示すマルチパスの差分特性確率を保持している。トレリス表現したマルチパスの一例を図 2 に示す。図中の数字は表 3 に示された出現頻度を表している。図 2 より、1 段目の 0 ビット目に差分を入力したとき、3 段目の 21 ビット目に差分が出力される差分パスは計 4 通りあり、その差分特性確率は式(5)となる。

$$\frac{2^3 + 2^4 + 2^4 + 2^3}{(2^8)^3} = 2^{-18.46} \quad (5)$$

5　差分パスの解析結果

はじめに、節 4.2 に示したアルゴリズムを用いずに、発見的手法により、各段における active S-box 数が 1 個で繋がる差分のシングルパスを見つけることができた。差分特性確率が最大となる差分パスを与える入力差分は、最下位ビットから 42 ビット目に入力する場合と 17 ビット目に入力する場合の 2 つである。42 ビット目に差分を入力する場合、最大差分確率2^{-6}で S 層の 41 ビット目に差分が出力され、その後 bit shuffle によって P 層の 42 ビット目に差分が転置される。この差分パスは何段でも直列に接続して繰り返すことができるため、10 段に渡る最大差分特性確率が2^{-60}となった。17 ビット目に差分を入力した場合も同様である。また、探索アルゴリズムを適用した計算機による解析の結果を表 4 に示す。探索した範囲内で最大差分特性確率を与えるマルチパスは 33 ビット目に差分を入力したとき、13 段の 42 ビット目に差分が出力されるパスである。このマルチパスの 13 段に渡る差分特性確率は$2^{-62.58}$となり、提案者による評価を 8 段上る特性が得られた。最大差分特性確率を与えるシングルパス及びマルチパスを図 3、図 4 に示し、5,10,13 段構成における提案者評価との比較を表 5 にまとめる。

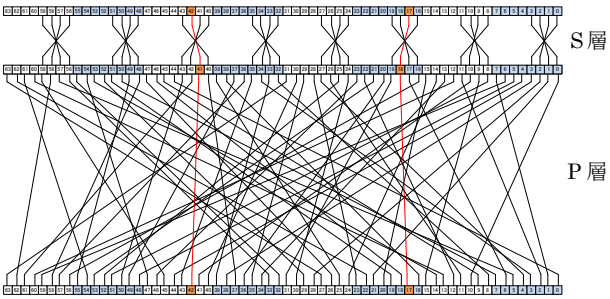

図 3　最良のシングルパス

表 5　5,10,13 段構成における最大差分特性確率

	5 段	10 段	13 段
提案者評価	2^{-60}	2^{-120}	2^{-156}
シングルパス	2^{-30}	2^{-60}	2^{-78}
マルチパス	$2^{-26.56}$	$2^{-49.07}$	$2^{-62.58}$

6　まとめ

本稿では、軽量型ブロック暗号 Halka の S-box の入出力差分が 1bit active で繋がることを利用し、各段の active S-box 数が 1 個となる差分パス解析を行った。また、マルチパスを考慮した解析では、トレリス表現を用いて各段の active S-box 数が 1 個となる差分パスを探索し、最大差分特性確率を導出した。その結果、シングルパスでは 10 段まで

差分攻撃に使用可能となり、攻撃可能な段数の増加に成功した。また、マルチパスを考慮することで 13 段に渡る差分特性確率が$2^{-62.58}$と攻撃可能な段数をさらに 3 段増加することができた。提案者による評価では 5 段まで差分攻撃に使用可能となっているので、提案者評価を大きく上回る結果となった。

参考文献

[1] Sourav Das, ”Halka: A Lightweight, software Friendly Block Cipher Using Ultra-lightweight 8-bit S-box”, https://eprint.iacr.org/2014/110.pdf

[2] 金子敏信, “共通鍵暗号の安全性評価”, https://www.jstage.jst.go.jp/article/essfr/7/1/7_14/_pdf

表 4　13 段に渡るマルチパスを考慮した差分特性確率

入力データブロックのbit位置	出力データブロックのbit位置	差分確率(log_2)	入力データブロックのbit位置	出力データブロックのbit位置	差分確率(log_2)
0	42	-63.625848	32	42	-63.19287
1	42	-63.114335	33	42	-62.58193
2	42	-63.426513	34	42	-63.06462
3	42	-63.243589	35	42	-63.01103
4	42	-65.427117	36	42	-64.77664
5	42	-64.426802	37	42	-63.69273
6	42	-63.869233	38	42	-63.50442
7	42	-63.921658	39	42	-63.5832
8	42	-63.416784	40	42	-63.47423
9	42	-62.881873	41	42	-62.9011
10	42	-63.297583	42	42	-63.23258
11	42	-63.183297	43	42	-63.22558
12	42	-64.797138	44	42	-64.54136
13	42	-64.152219	45	42	-63.7236
14	42	-63.867945	46	42	-63.76045
15	42	-63.586431	47	42	-63.74402
16	42	-63.62959	48	42	-63.40877
17	42	-63.149647	49	42	-63.03225
18	42	-63.478651	50	42	-63.2704
19	42	-63.426874	51	42	-63.2658
20	42	-65.588062	52	42	-65.3311
21	42	-64.761655	53	42	-64.35756
22	42	-64.030214	54	42	-63.76474
23	42	-63.955094	55	42	-63.80503
24	42	-64.179155	56	42	-63.43835
25	42	-63.05874	57	42	-63.01909
26	42	-63.806863	58	42	-63.35219
27	42	-63.395508	59	42	-63.07191
28	42	-65.242914	60	42	-65.55299
29	42	-6457458	61	42	-64.48344
30	42	-64.134337	62	42	-64.05767
31	42	-64.207475	63	42	-63.77959

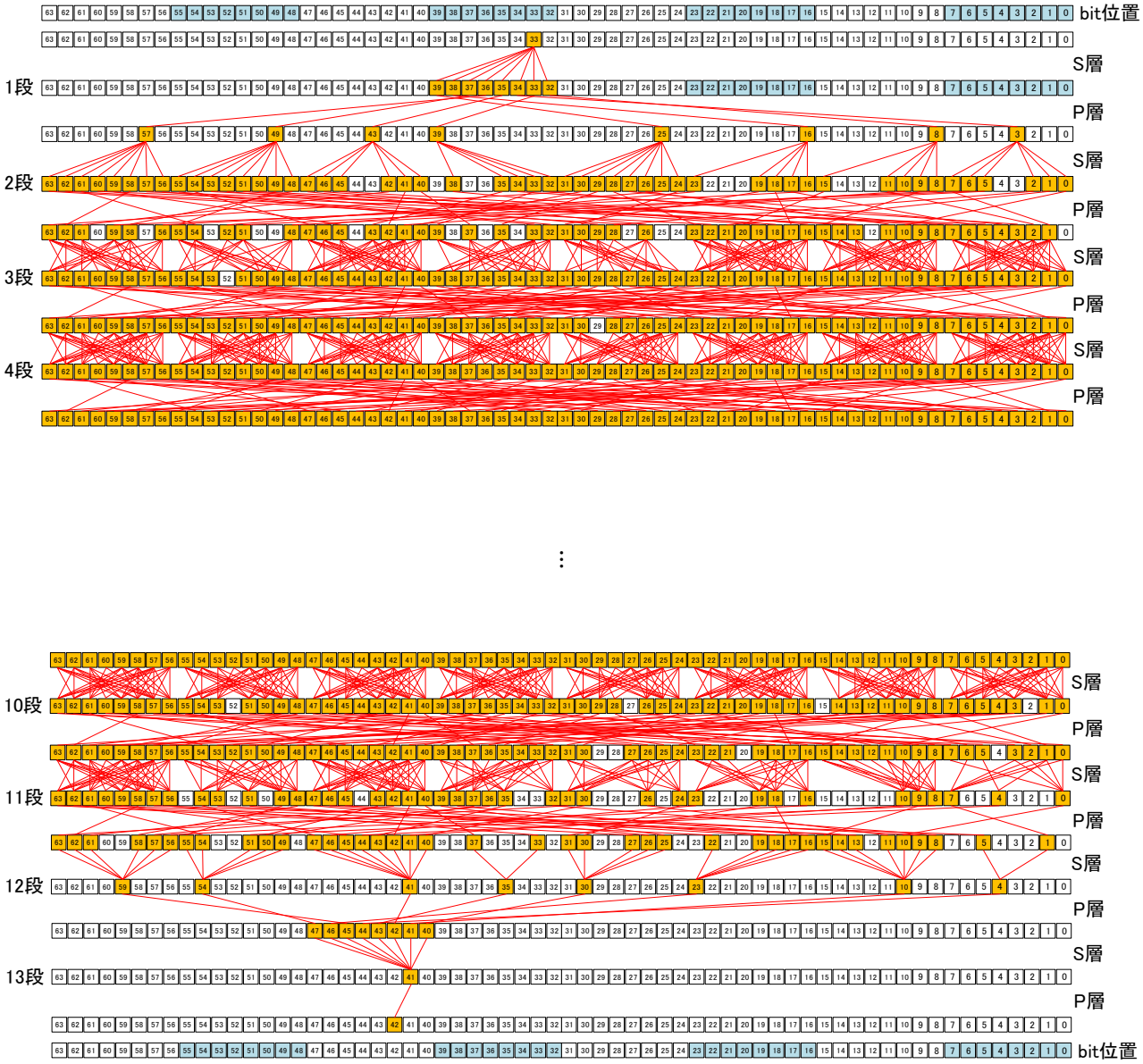

図 4　探索した範囲内で最大差分特性確率を与えるマルチパス

赤線と橙色の 1bit データはそれぞれ 1bit active を表す。省略した 4 段目から 10 段目の間はブロック長 64bit の全ての bit 位置が 1bit active となっている。