Differential Cryptanalysis of Block Cipher Halka

Yasutaka Igarashi, Shun Nakazawa, and Toshinobu Kaneko

***Abstract*—Halka is a lightweight block cipher proposed by Sourav Das in 2014. The block length of Halka is 64 bits and its key length is 80 bits. Halka uses 8-bit S-box for nonlinear permutation and uses bit shuffle for the linear permutation. In the differential cryptanalysis by the designers, the number of active S-box at each round is estimated to be 2, and differential attack can be mounted up to 5 rounds of Halka. In this article, focusing on Halka that has bit shuffle and 1-bit difference of active S-box at each round, we derive the new maximum differential characteristic probability (DCP). By analyzing trellis diagram of differential trails, we newly find that the maximum DCP of Halka is 2^{60} for 10 rounds of single trail and $2^{62.58}$ for 13 rounds of multiple trail, which are the results that the designers would not report.**

***Index Terms*—Differential cryptanalysis, block cipher Halka, multiple trail, 1-bit difference.**

I. Introduction

Halka is a lightweight block cipher with SPN structure proposed by Sourav Das in 2014 [1]. It consists of non-linear processing using 8-bit S-box and linear processing using bitwise permutation. The data block length of Halka is 64 bits and its key length is 80 bits. Here we call S-box "active" if the input and/or output difference of S-box is a nonzero difference. The designers evaluated that the number of active S-box is 2 at each round and that differential trail used for attack is limited up to 5 rounds of Halka.

On the other hand, we call S-box "1-bit active" if the Hamming weight of input/output differences of S-box is 1. When S-box is 1-bit active, the number of active S-box at each round can be reduced to 1 because the 1-bit difference is not diffused by bitwise permutation. This leads to the increase of rounds we can attack on.

Therefore, in this paper, we investigate the differential probability (DP) that the input/output difference of S-box is 1bit active, and derive the maximum differential characteristic probability (DCP) of Halka.

II. Data Mixing Process in Halka

Fig. 1 shows 1 round of data mixing process in Halka. It consists of exclusive OR (XOR) with 64-bit round key K_i (i = 1, 2, 3, ... , 24), 8 parallel S-boxes (S layer), and bitwise permutation (P layer). Halka consists of 24 rounds of this process and XOR of K_{25} at the output of the final round. The round key is generated by the key generation process with secret key.

Manuscript received March 6, 2020; revised May 9, 2020.

Y. Igarashi and T. Kaneko are with the Department of Electrical Engineering, Tokyo University of Science, Noda, Chiba, 2788510 Japan (e-mail: yasutaka@rs.noda.tus.ac.jp).

S. Nakazawa was with the Department of electrical engineering, Tokyo University of Science, Noda, Chiba, 2788510 Japan.

Table I shows the 8-bit input/output data of S-box in Halka. The uppermost row represents the lower 4 bits of the input 8 bits in hexadecimal, and the leftmost column represents the upper 4 bits. The intersection of rows and columns corresponds to the output. Table II shows bitwise permutation (bit suffle) where X represents the Xth input bit of the P layer from the right and Y represents the Yth output bit from the right (X, Y = 0, 1, 2, . . . , 63). Because the process of key generator does not affect our analysis, we omit its description.

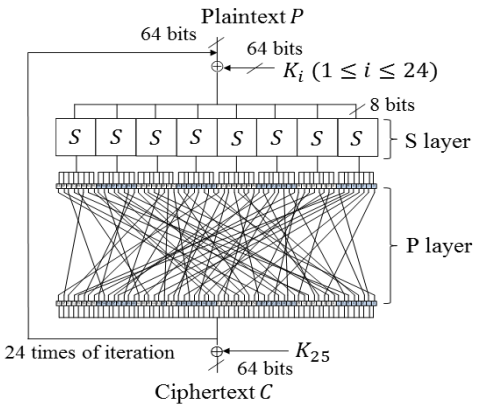

Fig. 1. One round of data mixing process in Halka.

TABLE I: 8-Bit Input/Output Data of S-box in Halka

Upper/ Lower	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

TABLE II: Bitwise Permutation (Bit Suffle) in Halka

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

III. Differential Probability and Differential Characteristic Probability

The differential attack is a cryptanalysis technique that can

doi: 10.18178/ijiee.2020.10.2.718

be performed when the distribution of difference in output is biased when we give the input some difference [2]-[7]. Here, the DP and the DCP are essential for the analysis of the differential trail used for the differential attack. We summarize DP and DCP in this section.

A. Differential Probability

The difference ΔX between n-bit data X and n-bit data X^* is defined as

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

The differential probability $DP_S(\Delta X \to \Delta Y)$ that the output difference becomes ΔY with respect to the input difference ΔX of an arbitrary function $S(X)$ with n-bit I/O is defined as

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

where the symbol { } represents a set and the symbol # represents the number of element of the set. We need 2^n of computational complexity to derive *DPs* for one pattern of ΔX and one pattern of ΔY. Because ΔX and ΔY are n-bit difference, we need 2^{3n} of computational complexity to derive *DPs* for all patterns of ΔX and ΔY. It is known that the maximum DP of S-box in Halka is 2^{-6} [1].

B. Differential Characteristic Probability

Although it is an accurate to analyze the maximum DP of the entire block cipher function by using (2) and use the DP as a strength index against a differential attack, it is difficult to analyze due to the huge computational complexity when n is large, e.g. n=64, 128, or 256 corresponding to n-bit block cipher. As alternative to DP, we use DCP for strength index of differential attack.

The maximum DCP (DCP_{max}) of block cipher consisting of R-time iteration of an arbitrary round function F is given by

$$DCP_{\max} = \max_{\Delta X_0 \neq 0.\, \Delta X_1, \Delta X_2, \cdots, \Delta X_R} \prod_{i=1}^{R} DP_F(\Delta X_{i-1} \to \Delta X_i) \tag{3}$$

where $\Delta X_i = \Delta Y_{i-1}$ and ΔX_i is the input difference to the ith round of function F, which DP is represented by DP_F. The propagation of difference $\Delta X_0 \to \Delta X_1 \to \ldots \to \Delta X_R$ is called a differential trail. Usually we can find many kinds of trail from ΔX_0 to ΔX_R because ΔX_i (i=1, 2, ..., R-1) is not fixed to one kind of values, i.e. we can find many kinds of ΔX_i (i=1, 2, ..., R-1) even when ΔX_0 and ΔX_R are fixed values. We call these many kinds of differential trail multiple trail. The input difference to a block cipher is the XOR of one pair of plaintext. Assuming the block length of the target cipher to be N and input difference is fixed to one kind of value, the total number of pair of plaintext is 2^N. This leads to $DCP_{max} > 2^{-N}$ for feasible differential attack.

IV. Analysis of Differential Trail

In this section, we search for a differential trail where the number of active S-boxes in each round is 1, and attempt to find the higher DCP than the designers found.

First, we analyze the DP of S-box in Halka where S-box is 1-bit active. And then we analyze the maximum DCP of Halka by using DP of S-box and trellis diagram of differential trail.

A. Differential Probability of 1-Bit Active S-box

Table III shows DP of 1-bit active S-box we derived. The uppermost row represents the 1-bit output difference of S-box in hexadecimal, and the leftmost column represents the 1-bit input difference of input. The intersection of rows and columns corresponds to the numerator of right-hand side of (2) where denominator is 2^8. We can find that the maximum DP of 1-bit active S-box in Halka is $4/2^8=2^{-6}$ from Table III. I/O differences (0x8, 0x1), (0x4, 0x2), (0x2, 0x4), and (0x1, 0x8) give the maximum DP.

TABLE III: DP of 1-Bit Active S-box

I/O difference	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

B. Searching Multiple Differential Trail

A trellis diagram is used as a method for obtaining the difference path and the maximum difference characteristic probability. A differential path takes the input differential value of each round as a state, considers the transition cost from a round to the next round as the differential probability. We find the differential path with the maximum differential probability by analyzing the trellis diagram of differential path. We also analyze differential multipaths to obtain high probability of differential path.

When the input/output difference of an n-bit function are ΔX_0 and ΔX_R, the differential probability (DP_{mul}) as the sum of all the differential multipaths is given by

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

We calculate the sum of multipaths where the input/output difference of each round is 1-bit active, derive the maximum difference characteristic probability. Therefore, the value of ΔX_i is limited to 64 types. This focuses on only the path with a high differential probability and ignores the path with a low differential probability, thereby avoiding a computational difficulty. We calculate the product of the differential probability held in the previous state of the trellis diagram and the differential probability associated with the transition to the next state. The product obtained by summing up all the previous states is the differential probability of the next state. Therefore, the final state holds the multipath difference probability shown in equation (4).

Fig. 2 shows an example of a multiple differential path. The numbers in the figure represent the appearance frequencies shown in Table III. As shown in Fig. 2, when a difference is input to the 0th bit of the first round, there are a total of 4 different differential paths in which the difference is output to the 21st bit of the third round. The differential probability of this differential multipath is given by

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

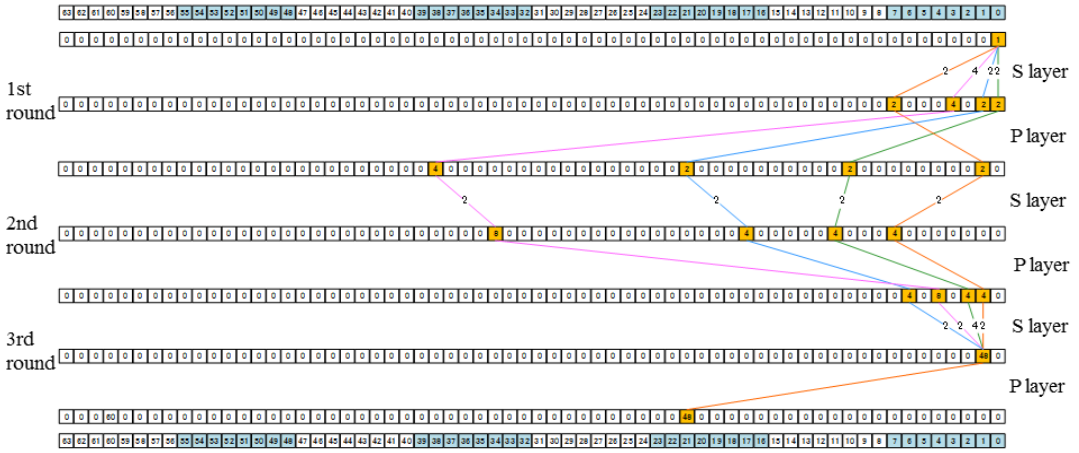

Fig. 2. Example of multiple trail from the first round to the third round.

V. Analytical Rusult of Differential Path

First, without using the algorithm shown in Section IV.B, we found a single differential path where the number of active S-boxes in each round is 1 by a heuristic method as shown in Fig. 3. When the differential probability is maximized, there are two types of input difference: input to the 42nd bit and input to the 17th bit from the least significant bit. When the difference is input to the 42nd bit, the difference is output to the 41st bit of the S layer with the maximum difference probability 2^{-6}. Subsequently, the difference is transposed to the 42nd bit of the P layer by bit shuffle. This differential path can be repeated in any number of rounds connected in series. Therefore, the maximum differential characteristic probability over 10 rounds becomes 2^{-60}. The same applies when a difference is input to the 17th bit.

Table IV shows the results of computer analysis of the search algorithm shown in Section IV.*B*. When the multipath difference probability is maximum, the difference is input to the 33rd bit, and the difference is output to the 42nd bit of the 13th round. The differential probability of this 13-round multipath is $2^{-62.58}$, which multiple differential path is shown in Fig. 4. This differential path is 8-round longer than the path designers found. Table V summarizes the maximum differential probability of Halka for 5, 10, and 13 rounds.

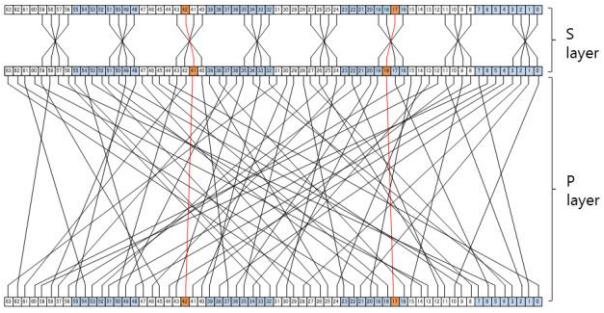

Fig. 3. Single differential trail in 1round of Halka with the maximum differential probability, which can be iterated in every round.

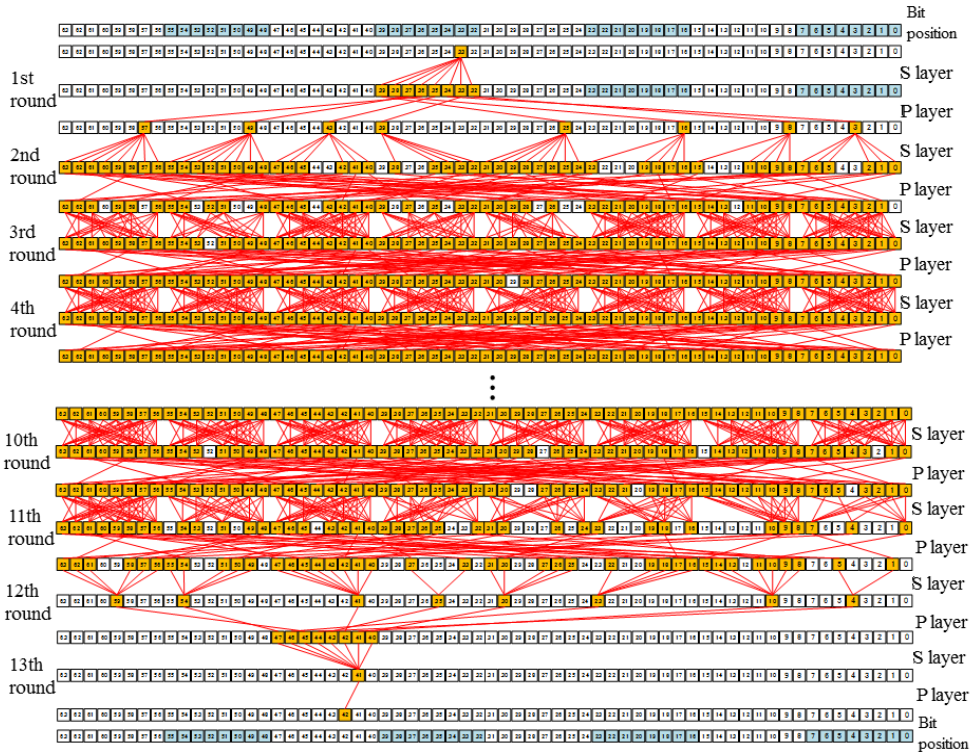

Fig. 4. Multiple differential trail with the maximum differential probability from the first round to the 13th round of Halka.

TABLE IV: DCP OF 13-ROUND HALKA WITH MULTIPLE DIFFERENTIAL TRAIL

position of 1-bit input difference	position of 1-bit output difference	DP ($\log_2$)	position of 1-bit input difference	position of 1-bit output difference	DP ($\log_2$)
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

TABLE V: MAXIMUM DCP OF HALKA FOR 5, 10, AND 13 ROUNDS

	5 rounds	10 rounds	13 rounds
Designers' estimation	2^{-60}	2^{-120}	2^{-156}
Single trail	2^{-30}	2^{-60}	2^{-78}
Multiple trail	$2^{-26.56}$	$2^{-49.07}$	$2^{-62.58}$

VI. CONCLUSION

We have focused on the fact that the I/O differences of S-box of Halka is effective with 1bit active, and analyzed differential trails where the number of active S-boxes in each round is 1. We also analyzed multiple differential trail by using the trellis diagram, and derived the maximum differential characteristic probability of Halka.

As a result, the single trail can be used for differential attacks up to 10 rounds, and the number of attackable rounds was successfully increased. In addition, by considering multiple trail, the differential characteristic probability over 13 rounds was $2^{-62.58}$, and the number of attackable rounds could be further increased by 3 more rounds. In the evaluation by the designers, it was possible to use it for differential attacks up to 5 rounds, so our results are more efficient than the designers' evaluation.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Yasutaka Igarashi conducted the research. Shun Nakazawa analyzed the data. Yasutaka Igarashi and Toshinobu Kaneko wrote the paper. All authors had approved the final version.

REFERENCES

[1] S. Das. (March 2014). Halka: A lightweight, software friendly block cipher using ultra-lightweight 8-bit S-box. Cryptology ePrint Archive: Report 2014/110 [Online]. Available: https://eprint.iacr.org/2014/110

[2] T. Kaneko. (May 2013). Cryptanalysis on common key ciphers. *IEICE Fundamentals Review*. [Online]. 7(1). pp. 14-29. Available: https://www.jstage.jst.go.jp/article/essfr/7/1/7_14/_pdf

[3] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, New York: Springer-Verlag, 1993.

[4] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, issue 1, pp. 3-72, January, 1991.

[5] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," *Advances in Cryptology - CRYPTO'92, Lecture Notes in Computer Science*, vol. 740, pp. 487-496, Springer, Berlin, Heidelberg.

[6] H. M. Heys and S. E. Tavares, "Substitution-permutation networks resistant to differential and linear cryptanalysis," *Journal of Cryptology*, vol. 9, no. 1, pp. 1-19, March 1996.

[7] F. Abazari and B. Sadeghiyan, "Cryptanalysis with ternary difference: Applied to block cipher present," *International Journal of Information and Electronics Engineering*, vol. 2, no. 3, pp. 441-445, 2012.

Yasutaka Igarashi received the B.E., M.E., and Ph.D. degrees in information and computer sciences from Saitama University, Japan from 2002-2005. He is currently a junior associate professor of Tokyo University of Science. His research is involved with the cryptanalysis of symmetric key cryptography.

Dr. Igarashi is a member of IEICE.

Shun Nakazawa received the B.E. and M.E. degrees in electrical engineering from Tokyo University of Science, Japan, from 2017 to 2019. His research was involved with the cryptanalysis of symmetric key cryptography.

Toshinobu Kaneko received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo from 1971 to 1976, respectively. He is currently an honorary professor of Tokyo University of Science. He has been engaged in coding theory and information security. Prof. Kaneko is a member of CRYPTREC and served as a chairman of Symmetric-Key Cryptography subcommittee in 2001--2003. Prof. Kaneko is a member of IEICE, IEEJ, IPSJ, and IEEE.