IEICE TRANSACTIONS

on Fundamentals of Electronics,
Communications
and Computer Sciences

DOI:10.1587/transfun.2024EAL2077

Publicized:2024/11/14

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3chome, Minato-ku, TOKYO, 105-0011 JAPAN

LETTER

Finding New Differential Characteristics on SPECK Family

Rikuto KURAHARA[†], *Nonmember*, Kosei SAKAMOTO[††], *and* Takanori ISOBE[†], *Members*

SUMMARY SPECK is a family of lightweight block ciphers. While Sun et al.'s evaluation of SPECK's differential characteristics was the most effective, it left room for further analysis over longer rounds. In this paper, we use a SAT-based search algorithm to analyze SPECK48, SPECK96, and SPECK128, presenting optimal differential characteristics up to 19, 15, and 11 rounds, respectively. We also explore the best characteristics up to 20 rounds for SPECK48, 18 rounds for SPECK96, and 20 rounds for SPECK128.

key words: *Symmetric-key Cipher, SPECK, Differential Characteristics, SAT solver.*

1. Introduction

SPECK [1] is a family of lightweight, software-optimized block ciphers developed by the National Security Agency (NSA). The cryptanalysis of SPECK has been extensively studied, particularly through solver-based approaches, which have yielded significant results. Song et al. evaluated the differential characteristics of SPECK using SMT models [2] and identified the best-known differential characteristics for a large number of rounds. In addition, Sun et al. explored optimal differential characteristics using a SAT solver [3]. While their approach successfully analyzed nearly the full number of rounds for SPECK32 and SPECK64, there remains potential for further evaluation of longer rounds in SPECK48, SPECK96, and SPECK128.

In this paper, we evaluate SPECK48, SPECK96, and SPECK128, which still present opportunities for improvement based on Sun's research. Our approach begins with an evaluation of each variant across the entire search space, aiming to discover optimal differential characteristics in more extended rounds compared to existing research. Subsequently, for rounds where finding the optimal differential characteristics becomes challenging, we focus on identifying differential characteristics with the highest possible probability. To facilitate this search, we implement a method to reduce the computational load by fixing the differential characteristics of the intermediate rounds, drawing on the evaluation method of Song et al. [2].

As a result, we provide optimal differential characteristics for longer rounds than previously reported. Specifically, we present new optimal differential characteristics for 19 rounds of SPECK48, 11-15 rounds of SPECK96, and 10-11 rounds of SPECK128. Furthermore, we explore the best differential characteristics up to 20 rounds for SPECK48, 18 rounds for SPECK96, and 20 rounds for SPECK128.

2. Preliminaries

In this section, we first describe differential characteristics. Then, we explain the security evaluation using the SAT solver.

2.1 Differential Cryptanalysis

The differential cryptanalysis proposed by Biham et al [4] is one of the most powerful cryptanalysis techniques to the symmetric-key cipher. When evaluating the security of a differential attack, we estimate the probability that the plaintext differences will reach the ciphertext differences. To estimate that probability, called *differential characteristic probability*, we often use *differential characteristics*, sequence of the internal differences in the cipher. Let $E(\cdot) = f_r(\cdot) \circ \cdot \cdot \circ f_1(\cdot)$ be the r-round block cipher, then differential characteristics are defined as follows:

Definition 1: (Differential Characteristics)
Differential characteristics are a sequence of differences over E defined as follows:

$$C = (c_0 \xrightarrow{f_1} c_1 \xrightarrow{f_2} \ldots \xrightarrow{f_r} c_r),$$

where $(c_0, c_1, \ldots, c_r)$ denotes the differences in the output of each round, and c_0, c_r denote the difference between plaintext and ciphertext respectively.

We can estimate the probability of differential characteristics as follows:

$$\Pr(C) = \prod_{i=1}^{r} \Pr(c_{i-1} \xrightarrow{f_i} c_i).$$

We often use *weight* to express the probability or differential characteristics for simplification. A weight is defined as follows:

Definition 2: (Weight)
A weight w is a negated value of the binary logarithm of the probability Pr defined as $w = -\log_2 P_r$

When we evaluate weight in stream ciphers, we consider weight related only to the first output key stream.

[†]The authors are with the Graduate School of Applied Informatics, University of Hyogo, Kobe-shi, 650-0047 Japan.
[††]The authors is with Mitsubishi Electric Corporation, Japan

2.2 Evaluation Using SAT Solver

Security evaluation using mathematical solvers is known as a promising method to evaluate the security of symmetric-key primitives. SAT is a problem of determining whether there is a true variable assignment in the boolean formula given by a binary variable. It is known that SAT solvers can efficiently solve such a problem. The recently proposed SAT solver accepts the boolean formula written in Conjunctive normal form (CNF), which is the conjunction ($\wedge$) of the disjunction ($\vee$) on boolean variables .

2.2.1 The SAT model to Evaluate Optimal Differential Characteristics.

To explain the SAT models for each operation, we follow the explanation of Sun et al.'s work [3]. Since the rotation, which is the operation of ARX-based ciphers, involves just changes the position of the bit, it does not require SAT modeling. Therefore, we explain the models of an XOR and modular addition.

2.2.2 XOR.

Let α, β, and γ be boolean variables such that $\alpha \oplus \beta = \gamma$. The differential propagation over an XOR is expressed as follows:

$$\alpha \vee \beta \vee \overline{\gamma} = 1, \quad \alpha \vee \overline{\beta} \vee \gamma = 1,$$
$$\overline{\alpha} \vee \beta \vee \gamma = 1, \quad \overline{\alpha} \vee \overline{\beta} \vee \overline{\gamma} = 1.$$

2.2.3 Modular Addition.

Let $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{b-1})$, $\boldsymbol{\beta} = (\beta_0, \beta_1, \ldots, \beta_{b-1})$ and $\gamma = (\gamma_0, \gamma_1, \ldots, \gamma_{b-1})$ be boolean variables such that $\alpha + \beta = \gamma$, where b denotes word size of target variant. A b-bit modular addition is expressed as follows:

$$\begin{aligned}
&\alpha_i \vee \beta_i \vee \overline{\gamma_i} \vee \alpha_{i+1} \vee \beta_{i+1} \vee \gamma_{i+1} = 1,\\
&\alpha_i \vee \overline{\beta_i} \vee \gamma_i \vee \alpha_{i+1} \vee \beta_{i+1} \vee \gamma_{i+1} = 1,\\
&\overline{\alpha_i} \vee \beta_i \vee \gamma_i \vee \alpha_{i+1} \vee \beta_{i+1} \vee \gamma_{i+1} = 1,\\
&\overline{\alpha_i} \vee \overline{\beta_i} \vee \overline{\gamma_i} \vee \alpha_{i+1} \vee \beta_{i+1} \vee \gamma_{i+1} = 1,\\
&\alpha_i \vee \beta_i \vee \gamma_i \vee \overline{\alpha_{i+1}} \vee \overline{\beta_{i+1}} \vee \overline{\gamma_{i+1}} = 1,\\
&\alpha_i \vee \overline{\beta_i} \vee \overline{\gamma_i} \vee \overline{\alpha_{i+1}} \vee \overline{\beta_{i+1}} \vee \overline{\gamma_{i+1}} = 1,\\
&\overline{\alpha_i} \vee \beta_i \vee \overline{\gamma_i} \vee \overline{\alpha_{i+1}} \vee \overline{\beta_{i+1}} \vee \overline{\gamma_{i+1}} = 1,\\
&\overline{\alpha_i} \vee \overline{\beta_i} \vee \gamma_i \vee \overline{\alpha_{i+1}} \vee \overline{\beta_{i+1}} \vee \overline{\gamma_{i+1}} = 1,\\
&\alpha_{b-1} \oplus \beta_{b-1} \oplus \gamma_{b-1} = 0.
\end{aligned}$$

where $0 \leq i \leq b-1$. In addition, corresponding weight $\boldsymbol{w} = (w_0, w_1, \ldots, w_{b-1})$ over b-bit modular addition is determined for $0 \leq i \leq b-2$ as follows:

$$\overline{\alpha_{i+1}} \vee \gamma_{i+1} \vee w_i = 1, \quad \beta_{i+1} \vee \overline{\gamma_{i+1}} \vee w_i = 1,$$
$$\alpha_{i+1} \vee \overline{\beta_{i+1}} \vee w_i = 1, \quad \alpha_{i+1} \vee \beta_{i+1} \vee \gamma_{i+1} \vee \overline{w_i} = 1,$$
$$\overline{\alpha_{i+1}} \vee \overline{\beta_{i+1}} \vee \overline{\gamma_{i+1}} \vee \overline{w_i} = 1.$$

Table 1: Parameter of each variant of SPECK.

Block size	Word size	α	β	rounds
32	16	7	2	22
48	24	8	3	22 or 23
64	32	8	3	26 or 27
96	48	8	3	28 or 29
128	64	8	3	32 or 33 or 34

2.2.4 Objective Function.

We set the objective function to identify the weigh of differential characteristics. Let $\boldsymbol{w} = (w_0, w_1, \ldots, w_{n-1})$ be a set of weights in a primitive. It is enough to give the following objective function to identify the total weight in a primitive:

$$\sum_{i=0}^{n-1} w_i \leq k.$$

We call a objective function *Boolean cardinality constraints* and can efficiently implement it by `kmtotalizer` [5].

3. Our Target

3.1 Specifications of SPECK

In this section, we introduce the specification of SPECK [1]. SPECK is a lightweight block cipher with ARX structure proposed by the National Security Agency (NSA). SPECK has variants with 5 message block sizes of 32/48/64/96/128 bits. For example, the 32-bit variant is expressed as SPECK32.

The Table. 1 shows the size of the parameters in each variant, and the Fig. 1 shows the flow in which ciphertext CT is generated from plaintxst PT through N rounds. Where, the $>>>\alpha$, $<<<\beta$, $\boxplus$ in the Fig. 1 mean α rotate on the right, β rotate on the left, and modular addition, respectively. Also, k_i $(1 \leq i \leq N)$ indicates the round key generated by the key schedule. In this paper, we do not elaborate on the key schedule, because it is not related with the evaluation of ours.

PT is divided into PT_1 and $PT2$, and $BT^r_{1,2}$, which is the middle block of the r round, where r for $1 \leq r \leq N$, are calculated by the following formula.

$$\begin{aligned}
BT^r_1 &= (BT^{r-1}_1 >>> \alpha) \boxplus BT^{r-1}_2,\\
BT^r_2 &= (BT^{r-1}_2 <<< \beta) \oplus ((BT^{r-1}_1 >>> \alpha) \boxplus BT^{r-1}_2),
\end{aligned}$$

where, BT^0 and BT^N denote plaintext and ciphertext respectively.

3.2 Existing Results

Differential analysis of SPECK has been extensively studied

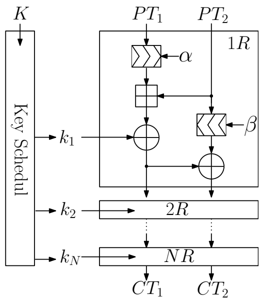

Fig. 1: Outlook of SPECK

in exisitng research. Notably, the combination of the SAT solver and Matsui's algorithm implemented by Sun et al. [3] provide significant results compared to other methods.

They discovered optimal differential characteristics in a large number of rounds for all variants. While their approach successfully analyzed nearly the full number of rounds for SPECK32 and SPECK64, there remains potential for further evaluation of longer rounds in SPECK48, SPECK96, and SPECK128.

Additionally, although not optimal, the analysis using SMT by Song [2] identified the best-known differential characteristics for long rounds. In their evaluation of long rounds, they fix the differences in intermediate rounds and reduce the computational burden by dividing the problem into two parts.

4. Efficient Search for Differential Characteristics

In this paper, we evaluate the SPECK48, SPECK96 and SPECK128, which still has room for improvement for existing research. In order to conduct an efficient search for a larger numner of rounds, we utilize a automatic search method using the SAT solver proposed by Sun et al [3]. SAT modeling is built by the method shown in Sect. 2.

Our approach begins by evaluating each variant across the entire search space to find optimal differential characteristics over extended rounds. For rounds where this is difficult, we focus on identifying characteristics with the highest probability. To reduce computational load, we fix the differential characteristics of intermediate rounds, following the method of Song et al. [2]. The search in each variant follows three steps

Step 1: (Search for the Optimal Differential Characteristic)
In this step, we aim to discover optimal differential characteristics that cannot be further improved, conducting the search for as many rounds as feasible within the available computation time.

Step 2: (Search for the Best Differential Characteristic)
In this step, we begin with the round that did not yield optimal results in step 1 and explore the best possible differential characteristics for each round.

Step 3: (Limitation of Search Space)
In this step, by fixing the intermediate differential path, the search space is reduced, which makes it easier to discover the best differential characteristics. The differential characteristics that are fixed corresponds to the segment where the Hamming weight is expected to be lower. This approach is inspired by the search method proposed by Song [2], as discussed in Sect. 3.

We confirm that the optimal differential characteristics associated with the increase in rounds exhibit a partial, regular transition. To select an intermediate round to fix, this regularity can be used to predict where the Hamming weight will decrease.

5. Results

Tables 2, 3, and 4 present the results of the existing evaluations alongside our evaluation results. The numerical values in each table primarily represent the weight of the differential characteristics. Additionally, the entries highlighted in bold indicate the differential characteristics that were identified under the conditions of step 3.

As shown in Tables 2, 3, and 4, we identify the optimal differential characteristics up to 19 rounds in SPECK48, up to 15 rounds in SPECK96, and up to 11 rounds in SPECK128. Furthermore, in the search for the best differential characteristics, we discover differential characteristics for all rounds up to 20, 18, and 20 rounds, respectively.

Our contributions are summarized below.

- In the search for optimal differential characteristics (step 1), we find new optimal differential characteristics of 19 rounds of SPECK48, 11-15 rounds of SPECK96, and 10-11 rounds of SPECK128.
- In the search for the best differential characteristics (step 2 and 3), we discover differential characteristics in several rounds each variant. Specifically, differential characteristics in 20 round of SPECK48, 16-18 round in SPECK96, and 12-20 rounds in SPECK128 are identified.

6. Conclusion

In this paper, we utilized a SAT-based search algorithm to analyze SPECK48, SPECK96, and SPECK128, presenting optimal differential characteristics up to 19, 15, and 11 rounds, respectively. We also explored the best characteristics up to 20 rounds for SPECK48, 18 rounds for SPECK96, and 20 rounds for SPECK128.

References

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK families of lightweight block ciphers." Cryptology ePrint Archive, Paper 2013/404, 2013.

[2] L. Song, Z. Huang, and Q. Yang, "Automatic differential analysis of arx block ciphers with application to speck and lea," Information Security and Privacy, ed. J.K. Liu and R. Steinfeld, Cham, pp.379–394, Springer International Publishing, 2016.

Table 2: Differential characteristic probability on SPECK48 where each result is given in weight.

optimal	1R	2R	3R	4R	5R	6R	7R	8R	9R	10R	Ref
-	-	-	-	-	-	-	-	-	-	-	[2]
✓	0	1	3	6	10	14	19	26	33	40	[3]
✓	0	1	3	6	10	14	19	26	33	40	Our
-	-	-	-	-	-	-	-	-	-	-	Our
optimal	11R	12R	13R	14R	15R	16R	17R	18R	19R	20R	Ref
-	46	-	-	-	-	-	-	-	-	-	[2]
✓	45	49	54	58	63	68	75	82	-	-	[3]
✓	45	49	54	58	63	68	75	82	89	-	Our
-	-	-	-	-	-	-	-	-	-	**107**	Our

Table 3: Differential characteristic probability on SPECK96 where each result is given in weight.

optimal	1R	2R	3R	4R	5R	6R	7R	8R	9R	10R	Ref
-	-	-	-	-	-	-	-	-	-	-	[2]
✓	0	1	3	6	10	15	21	30	39	49	[3]
✓	0	1	3	6	10	15	21	30	39	49	Our
-	-	-	-	-	-	-	-	-	-	-	Our
optimal	11R	12R	13R	14R	15R	16R	17R	18R	-	-	Ref
-	-	-	-	-	-	-	96	-	-	-	[2]
✓	-	-	-	-	-	-	-	-	-	-	[3]
✓	58	62	66	72	78	-	-	-	-	-	Our
-	-	-	-	-	-	87	**96**	**110**	-	-	Our

Table 4: Differential characteristic probability on SPECK128 where each result is given in weight.

optimal	1R	2R	3R	4R	5R	6R	7R	8R	9R	10R	Ref
-	-	-	-	-	-	-	-	-	-	-	[2]
✓	0	1	3	6	10	15	21	30	39	-	[3]
✓	0	1	3	6	10	15	21	30	39	49	Our
-	-	-	-	-	-	-	-	-	-	-	Our
optimal	11R	12R	13R	14R	15R	16R	17R	18R	19R	20R	Ref
-	-	-	-	-	-	-	-	113	-	128	[2]
✓	-	-	-	-	-	-	-	-	-	-	[3]
✓	58	-	-	-	-	-	-	-	-	-	Our
-	-	66	73	**81**	**87**	**96**	**104**	**113**	**119**	**128**	Our

[3] L. Sun, W. Wang, and M. Wang, "Accelerating the Search of Differential and Linear Characteristics with the SAT Method," IACR Transactions on Symmetric Cryptology, vol.2021, no.1, p.269–315, Mar. 2021.

[4] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Journal of CRYPTOLOGY, vol.4, no.1, pp.3–72, 1991.

[5] R. Martins, S. Joshi, V.M. Manquinho, and I. Lynce, "Incremental Cardinality Constraints for MaxSAT," CoRR, vol.abs/1408.4628, 2014.