IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 July 2023, accepted 27 August 2023, date of publication 4 September 2023, date of current version 20 September 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3311898*

RESEARCH ARTICLE

# Validity of Differential Characteristics of ARX Block Ciphers

**DONGYOUNG ROH, (Member, IEEE)**
The Affiliated Institute of ETRI, Daejeon 34044, South Korea
e-mail: dyroh@nsr.re.kr

This work was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korean Government (MSIT) (Development of Next-Generation Cryptosystem to Improve Security and Usability of National Information System) under Grant 2021-0-00046.

**ABSTRACT** In this paper, we examine the validity of the differential characteristics of ARX-based block ciphers. Recently, Peyrin et al. showed that some of the differential characteristics of block ciphers, SKINNY and GIFT, in the literature are not valid. However, their work is limited to SPN-based block ciphers. We find out that some of the differential characteristics of block ciphers, SIMON, SPECK, and CHAM, that appeared in the literature are not valid. Our work indicates that not only the differential characteristics of SPN-based block ciphers, but also the differential characteristics of ARX-based block ciphers may be invalid.

**INDEX TERMS** Block cipher, CHAM, differential characteristic, SIMON, SPECK, validity.

## I. INTRODUCTION

A differential characteristic is the most fundamental building block to mount a differential attack on a block cipher, one of the most powerful attacks on block ciphers. Therefore, when a new block cipher is developed, a lot of research is done to find differential characteristics of it. Most of the research looking for differential characteristics of block ciphers assumes independence between rounds (Markov assumption [1]). However, the rounds of a real block cipher are not independent at all. Actually, we already know that SPECK and CHAM are not Markov ciphers [2], [3]. Nevertheless, making Markov assumption even for a non-Markov cipher is still one of the best ways to find differential characteristics.

A differential characteristic of a block cipher is said to be valid (informally) when there exists a tuple of a plaintext pair, a ciphertext pair, and a key compliant with it. The existence of such a pair does not imply the success of a differential attack utilizing it. Because the existence of such a pair does not tell us the exact probability of it. On the other hand, the non-existence of such a pair does not imply the failure of a differential attack utilizing it. Because the non-existence of such a pair does not preclude the possibility of using it as a differential to mount a differential attack, rather than as a differential characteristic itself.

Nevertheless, it is not meaningless to check the validity of a differential characteristic. When calculating the success probability of a differential attack, one of the most important things is the probability of the differential used in the attack. If any of the underlying differential characteristics that form the differential are invalid, the probability of the differential may not be as expected, which means that the success probability of the attack may also not be as expected. Therefore, the validity of differential characteristics of a block cipher is closely related to the security of the block cipher.

Recently, Peyrin and Tan gave a framework and a corresponding tool to investigate the validity of differential characteristics [4]. They showed that many differential characteristics that appeared in the literature are invalid: they checked differential characteristics from eight articles (four each for both SKINNY and GIFT) and most of these published paths are impossible or working only for a very small proportion of the key space.

*Our Contributions:* Both SKINNY and GIFT are based on a design principle known as a substitution-permutation network (SPN). Another well-known design principle of block ciphers is an addition-rotation-XOR (ARX) structure. In this paper, we study the validity of differential characteristics that

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son.

**TABLE 1.** Invalid (related-key) differential characteristics.

| Cipher | Rounds | Prob. | (Key difference) / Input difference / Output difference | Ref. | Validity |
|---|---|---|---|---|---|
| **SPECK**-48/$k^{\dagger}$ | 10 | $2^{-41}$ | (480B01 094009)<br>(808524 84A805) | [5] | Invalid under the Markov assumption |
| **SPECK**-64/$k^{\dagger}$ | 13 | $2^{-55.9}$ | (10420040 40024000)<br>(20000524 20202C04) | [6] | Invalid under the Markov assumption |
| | 12 | $2^{-63}$ | (02080888 1A4A0848)<br>(80008004 84008020) | [7] | Invalid under the Markov assumption |
| **SPECK**-96/$k^{\dagger}$ | 13 | $2^{-89}$ | (A22A20200800 013223206808)<br>(80A0A0000088 8C81A02004C8) | [7] | Invalid under the Markov assumption |
| **SPECK**-128/$k^{\dagger}$ | 15 | $2^{-117.28}$ | (0640240804002440 6004400C20040004)<br>(888080A080820828 E88C81A4A0924B2C) | [6] | Invalid under the Markov assumption |
| | 14 | $2^{-112}$ | (144304280C010420 0006402400040024)<br>(0180208402886884 0080248012C96C80) | [5] | Invalid under the Markov assumption |
| **CHAM**-64/128$^{\dagger}$ | 39 | $2^{-63}$ | (0102 0280 0000 0400)<br>(0100 0281 0002 0000) | [8] | Invalid with independent round keys |
| | 44 | $2^{-73}$ | (4000 8040 00A0 0000)<br>(0001 8100 0001 0200) | [8] | Invalid with independent round keys |
| **CHAM**-128/128$^{\ddagger}$ | 47 | $2^{-120}$ | (00000000 00000000 24924925 24924925)<br>(00000000 00000000 00000000 FFFFFF25)<br>(FFFFF925 00000000 00000000 00000000) | [8] | Invalid |

†: Differential characteristic, ‡: Related-key differential characteristic

appeared in the literature of SIMON, SPECK, and CHAM, which are ARX-based block ciphers. We check differential characteristics from eleven articles (five for SIMON, eight for SPECK, and two for CHAM) and related-key differential characteristics from one article (one for CHAM). We find that some of them are invalid. In doing so, we define several forms of validity such as "valid differential characteristic," "valid differential characteristic with independent round keys," "valid differential characteristic under the Markov assumption," "valid differential," and "valid related-key differential characteristic," so that we can understand the nature of invalid (related-key) differential characteristics a little better. The invalid (related-key) differential characteristics that we have found are summarized in Table 1. In the last column of the table, the several forms of validity are used to describe the nature of the characteristics. The rigorous definitions of them will be given later.

Peyrin et al.'s framework does not apply well to ARX-based block ciphers, so we take a different approach. We set up a set of equations, which can check the validity of a differential characteristic, and convert it to a Boolean satisfiability problem. Then we use a SAT solver to see if the Boolean satisfiability problem is satisfiable or not.

Note that SIMON uses bitwise AND operations instead of additions. However, we can also check differential characteristics of it using our approach.

*Paper Organization:* The outline of the paper is as follows. We provide basic definitions and notations and brief descriptions of SIMON, SPECK, and CHAM in Section II. Several forms of validity of (related-key) differential characteristics are rigorously defined in Section III. Section IV shows whether each of the (related-key) differential characteristics of SIMON, SPECK, and CHAM in the literature is valid or not. Finally, Section V concludes the paper and presents some further studies.

## II. PRELIMINARIES

### A. BASIC DEFINITIONS AND NOTATIONS

#### 1) BOOLEAN SATISFIABILITY PROBLEM

The Boolean satisfiability problem involves determining whether a given Boolean formula can be satisfied by any interpretation. In simpler terms, it seeks to ascertain if the variables in the formula can be assigned the values TRUE or FALSE in a consistent manner that results in the formula evaluating to TRUE. If this is possible, the formula is said to be *satisfiable*. Conversely, if no such assignment exists, the formula is said to be *unsatisfiable*, indicating that the formula evaluates to FALSE for all potential variable assignments.

As you know, the Boolean satisfiability problem is classified as NP-complete, meaning that currently, only algorithms with exponential worst-case complexity are known for solving it. However, efficient and scalable algorithms are being constantly developed to solve it. Prominent examples include MiniSAT [9], ManySAT [10], and CryptoMiniSat [11]. Among these solvers, we utilize CryptoMiniSat due to its ability to perform multi-threaded operations and support for XOR clauses.

#### 2) NOTATIONS

We will denote by $x\&y$ and $x \oplus y$ the bit-wise AND and the bit-wise exclusive OR (XOR) of bit strings $x$ and $y$, respectively. Let $x \boxplus y$ denote the addition of a $w$-bit word $x$ and a $w$-bit word $y$ modulo $2^w$, and let $x \lll i$ and $x \ggg i$ denote the rotation of a $w$-bit word $x$ to the left and right, respectively, by $i$ bits. Hexadeicmal values are written in a typewriter font.

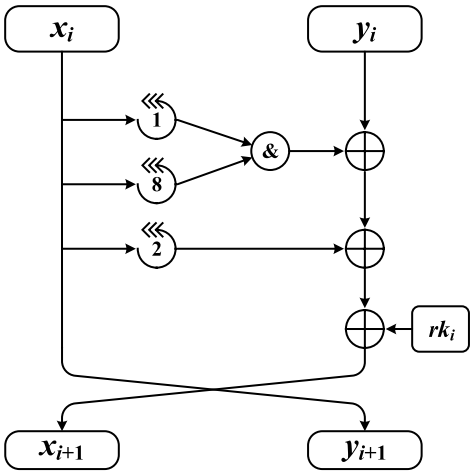


**FIGURE 1.** The round function of SIMON.

### B. THE BLOCK CIPHERS SIMON, SPECK, AND CHAM

In this subsection, we briefly review the block ciphers SIMON, SPECK, and CHAM.

#### 1) SIMON

By applying $r$ iterations of the key-dependent round function, SIMON-$n/k$ encrypts a plaintext of two $n/2$-bit words to a ciphertext of two $n/2$-bit words under a $k$-bit key. For a round key $rk \in \mathrm{GF}(2)^{n/2}$, the round function of SIMON is defined as follows.

$$f_{rk} : \mathrm{GF}(2)^{n/2} \times \mathrm{GF}(2)^{n/2} \longrightarrow \mathrm{GF}(2)^{n/2} \times \mathrm{GF}(2)^{n/2}$$
$$f_{rk}(x, y) = (y \oplus ((x \lll 1) \& (x \lll 8)) \oplus (x \lll 2) \oplus rk, x)$$

The SIMON key schedules generate round keys $rk_i$ for a given key $K = (rk_{m-1}, \cdots, rk_1, rk_0)$, where $rk_i \in \mathrm{GF}(2)^{n/2}$ and $m = 2k/n \in \{2, 3, 4\}$. The round keys are generated by

$$rk_{i+m} = \begin{cases} c \oplus (z_j)_i \oplus rk_i \oplus (rk_{i+1} \lll 3) \\ \quad \oplus (rk_{i+1} \lll 4), & \text{if } m = 2, \\ c \oplus (z_j)_i \oplus rk_i \oplus (rk_{i+2} \lll 3) \\ \quad \oplus (rk_{i+2} \lll 4), & \text{if } m = 3, \\ c \oplus (z_j)_i \oplus rk_i \oplus (rk_{i+3} \lll 3) \oplus rk_{i+1} \\ \quad \oplus (rk_{i+3} \lll 4) \oplus (rk_{i+1} \lll 1), & \text{if } m = 4, \end{cases}$$

for $0 \le i < r - m$, where $c = 2^{n/2} - 4 = \texttt{0xff} \cdots \texttt{fc}$ and $z_j$ $(0 \le j < 5)$ is a constant sequence. The value $rk_i$ is the $i$-th round key, for $0 \le i < r$.

The round function of SIMON is depicted in Fig. 1 and parameters of it are specified in Table 2.

#### 2) SPECK

By applying $r$ iterations of the key-dependent round function, SPECK-$n/k$ encrypts a plaintext of two $n/2$-bit words to a ciphertext of two $n/2$-bit words under a $k$-bit key. For a round key $rk \in \mathrm{GF}(2)^{n/2}$, the round function of SPECK is defined as follows.

$$f_{rk} : \mathrm{GF}(2)^{n/2} \times \mathrm{GF}(2)^{n/2} \longrightarrow \mathrm{GF}(2)^{n/2} \times \mathrm{GF}(2)^{n/2}$$
$$f_{rk}(x, y) = (((x \ggg \alpha) \boxplus y) \oplus rk, (y \lll \beta) \oplus ((x \ggg \alpha) \boxplus y) \oplus rk)$$

The SPECK key schedules generate round keys $rk_i$ for a given key $K = (l_{m-2}, \cdots, l_0, k_0)$, where $l_i, k_0 \in \mathrm{GF}(2)^{n/2}$ and $m = 2k/n \in \{2, 3, 4\}$. Sequences $rk_i$ and $l_i$ are defined by

$$rk_0 = k_0,$$
$$l_{i+m-1} = (rk_i \boxplus (l_i \ggg \alpha)) \oplus i, \text{ and}$$
$$rk_{i+1} = (rk_i \lll \beta) \oplus l_{i+m-1}.$$

The value $rk_i$ is the $i$-th round key, for $0 \le i < r$.

The round function of SPECK is depicted in Fig. 2 and parameters of it are specified in Table 3.

#### 3) CHAM

By applying $r$ iterations of the key-dependent round function, CHAM-$n/k$ encrypts a plaintext of four $n/4$-bit words to a ciphertext of four $n/4$-bit words under a $k$-bit key. For a round key $rk \in \mathrm{GF}(2)^{n/4}$, the $i$-th round function of CHAM is

**TABLE 2.** SIMON parameters.

| cipher | block size | key size | word size | key words | const seq | rounds |
|---|---|---|---|---|---|---|
| **SIMON**-32/64 | 32 | 64 | 16 | 4 | $z_0$ | 32 |
| **SIMON**-48/72 | 48 | 72 | 24 | 3 | $z_0$ | 36 |
| **SIMON**-48/96 | | 96 | | 4 | $z_1$ | 36 |
| **SIMON**-64/96 | 64 | 96 | 32 | 3 | $z_2$ | 42 |
| **SIMON**-64/128 | | 128 | | 4 | $z_3$ | 44 |
| **SIMON**-96/96 | 96 | 96 | 48 | 2 | $z_2$ | 52 |
| **SIMON**-96/144 | | 144 | | 3 | $z_3$ | 54 |
| **SIMON**-128/128 | 128 | 128 | 64 | 2 | $z_2$ | 68 |
| **SIMON**-128/192 | | 192 | | 3 | $z_3$ | 69 |
| **SIMON**-128/256 | | 256 | | 4 | $z_4$ | 72 |

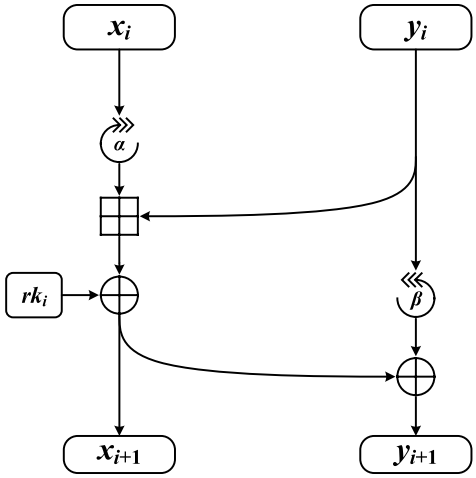


**FIGURE 2.** The round function of SPECK.

**TABLE 3.** SPECK parameters.

| cipher | block size | key size | word size | key words | rot $\alpha$ | rot $\beta$ | rounds |
|---|---|---|---|---|---|---|---|
| **SPECK**-32/64 | 32 | 64 | 16 | 4 | 7 | 2 | 32 |
| **SPECK**-48/72 | 48 | 72 | 24 | 3 | 8 | 3 | 36 |
| **SPECK**-48/96 | | 96 | | 4 | | | 36 |
| **SPECK**-64/96 | 64 | 96 | 32 | 3 | 8 | 3 | 42 |
| **SPECK**-64/144 | | 128 | | 4 | | | 44 |
| **SPECK**-96/96 | 96 | 96 | 48 | 2 | 8 | 3 | 52 |
| **SPECK**-96/144 | | 144 | | 3 | | | 54 |
| **SPECK**-128/128 | 128 | 128 | 64 | 2 | 8 | 3 | 68 |
| **SPECK**-128/192 | | 192 | | 3 | | | 69 |
| **SPECK**-128/256 | | 256 | | 4 | | | 72 |

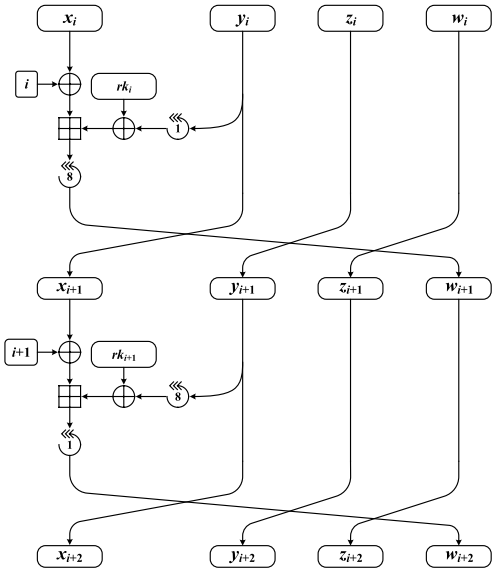


**FIGURE 3.** The round function of CHAM.

defined as follows.

$$
\begin{aligned}
f_{rk} &: \mathrm{GF}(2)^{n/4} \times \mathrm{GF}(2)^{n/4} \times \mathrm{GF}(2)^{n/4} \times \mathrm{GF}(2)^{n/4} \\
&\longrightarrow \mathrm{GF}(2)^{n/4} \times \mathrm{GF}(2)^{n/4} \times \mathrm{GF}(2)^{n/4} \times \mathrm{GF}(2)^{n/4} \\
& f_{rk}\,(x, y, z, w) \\
&= (y, z, w, ((x \oplus i) \boxplus ((y \lll \alpha_i) \oplus rk_i)) \lll \beta_i)\,,
\end{aligned}
$$

where $\alpha_i = 1$ and $\beta_i = 8$ when $i$ is even and $\alpha_i = 8$ and $\beta_i = 1$ when $i$ is odd. The **CHAM** key schedules generate round keys $rk_i$ for a given key of $4k/n$ $n$/4-bit words $K = (k_0, k_1, \cdots, k_{4k/n-1})$. The round keys are generated by

$$
rk_i = \begin{cases} k_j \oplus (k_j \lll 1) \oplus (k_j \lll 8)\,, & \text{if } 0 \le j < 4k/n, \\ k_{j\oplus 1} \oplus (k_{j\oplus 1} \lll 1) \oplus (k_{j\oplus 1} \lll 11)\,, & \text{otherwise,} \end{cases}
$$

where $j = i \mod 8k/n$. The value $rk_i$ is the $i$-th round key, for $0 \le i < r$.

The round function of **CHAM** is depicted in Fig. 3 and parameters of it are specified in Table 4.

**TABLE 4.** CHAM parameters.

| cipher | block size | key size | word size | rounds |
|---|---|---|---|---|
| **CHAM**-64/128 | 64 | 128 | 16 | 88 |
| **CHAM**-128/128 | 128 | 128 | 32 | 112 |
| **CHAM**-128/256 | 128 | 256 | 32 | 120 |

## III. VALIDITY OF A (RELATED-KEY) DIFFERENTIAL CHARACTERISTIC

In this section, we rigorously define the validity of a differential characteristic. In particular, we define several forms of validity, so that we can obtain a more comprehensive understanding of a differential characteristic.

Suppose that there is an $r$-round differential characteristic $(\Delta d_0, \Delta d_1, \cdots, \Delta d_r)$ of a block cipher. Here, $h_i$ denotes the key schedule function of the block cipher that takes a key as an input and outputs a sequence of round keys up to $(i-1)$-th round as an output and $g$ denotes the round key-dependent round function of the block cipher. We now give definitions of the several forms of validity of a differential characteristic. (For simplicity, we use a slightly different notation for round functions than the definitions of round functions in Section II-B. For **SIMON** and **SPECK**, $f_{rk}(x, y) = g(rk, x\|y)$ and for **CHAM**, $f_{rk}(x, y, z, w) = g(rk, x\|y\|z\|w)$.)

*Definition 1: We say that an $r$-round differential characteristic is valid up to $s$ rounds, where $s \le r$, if there is at least one tuple $(k, p_0, p_1, \cdots, p_s, q_0, q_1, \cdots, q_s)$ such that*

1) $h_s(k) = rk_0\| \cdots \|rk_{s-1}$,
2) $g\,(rk_i, p_i) = p_{i+1}$ *for* $0 \le i < s$,
3) $g\,(rk_i, q_i) = q_{i+1}$ *for* $0 \le i < s$, *and*
4) $p_i \oplus q_i = \Delta d_i$ *for* $0 \le i \le s$.

*In particular, we say that an $r$-round differential characteristic is valid if it is valid up to $r$ rounds.*

*Definition 2: We say that an $r$-round differential characteristic is valid with independent round keys up to $s$ rounds, where $s \le r$, if there is at least one tuple $(rk_0, rk_1, \cdots, rk_{s-1}, p_0, p_1, \cdots, p_s, q_0, q_1, \cdots, q_s)$ such that*

1) $g\,(rk_i, p_i) = p_{i+1}$ *for* $0 \le i < s$,
2) $g\,(rk_i, q_i) = q_{i+1}$ *for* $0 \le i < s$, *and*
3) $p_i \oplus q_i = \Delta d_i$ *for* $0 \le i \le s$.

*In particular, we say that an $r$-round differential characteristic is valid with independent round keys if it is valid with independent round keys up to $r$ rounds.*

*Definition 3: We say that an $r$-round differential characteristic is valid under the Markov assumption up to $s$ rounds, where $s \le r$, if there is at least one tuple $(rk_0, rk_1, \cdots, rk_{s-1}, p_0, p_1, \cdots, p_{2s-1}, q_0, q_1, \cdots, q_{2s-1})$ such that*

1) $g\,(rk_i, p_{2i}) = p_{2i+1}$ *for* $0 \le i < s$,
2) $g\,(rk_i, q_{2i}) = q_{2i+1}$ *for* $0 \le i < s$,
3) $p_{2i} \oplus q_{2i} = \Delta d_i$ *for* $0 \le i < s$, *and*
4) $p_{2i+1} \oplus q_{2i+1} = \Delta d_{i+1}$ *for* $0 \le i < s$.

*In particular, we say that an r-round differential characteristic is valid under the Markov assumption if it is valid under the Markov assumption up to r rounds.*

Note that the differential characteristics in the literature are supposed to be valid under the Markov assumption.

*Definition 4: We say that an r-round differential characteristic is a valid differential if there is at least one tuple* $(k, p_0, p_1, \cdots, p_r, q_0, q_1, \cdots, q_r)$ *such that*

1) $h_r(k) = rk_0 \| \cdots \| rk_{r-1}$,
2) $g(rk_i, p_i) = p_{i+1}$ *for* $0 \le i < r$,
3) $g(rk_i, q_i) = q_{i+1}$ *for* $0 \le i < r$, *and*
4) $p_i \oplus q_i = \Delta d_i$ *for* $i = 0$ *and* $r$.

The above properties have the following relations and implications.

- A valid differential characteristic is valid with independent round keys.
- A valid differential characteristic is valid under the Markov assumption.
- A valid differential characteristic is also a valid differential.
- A valid differential characteristic with independent round keys is valid under the Markov assumption.
- Suppose that a differential characteristic of a block cipher is invalid, but valid with independent round keys. Then the block cipher is not a Markov cipher. Furthermore, it means that dependencies in the round keys may make the differential characteristic invalid.
- Suppose that a differential characteristic of a block cipher is invalid and also invalid with independent round keys, but valid under the Markov assumption. Then the block cipher is not a Markov cipher. Furthermore, it means that dependencies in the plaintexts may make the differential characteristic invalid.
- Suppose that a differential characteristic of a block cipher is invalid, invalid with independent round keys, and invalid under the Markov assumption. This means there was an error in finding it.

Now suppose that there is an $r$-round related-key differential characteristic $(\Delta k, (\Delta d_0, \Delta d_1, \cdots, \Delta d_r))$ of a block cipher. Again, $h_i$ and $g$ denote the key schedule function and the round key-dependent round function of the block cipher, respectively, as earlier. We now give a definition of the validity of a related-key differential characteristic.

*Definition 5: We say that an r-round related-key differential characteristic is valid up to s rounds, where* $s \le r$, *if there is at least one tuple* $\left(k_p, k_q, p_0, p_1, \cdots, p_s, q_0, q_1, \cdots, q_s\right)$ *such that*

1) $h_s(k_p) = rk_{p,0} \| \cdots \| rk_{p,s-1}$,
2) $h_s(k_q) = rk_{q,0} \| \cdots \| rk_{q,s-1}$,
3) $g\left(rk_{p,i}, p_i\right) = p_{i+1}$ *for* $0 \le i < s$,
4) $g\left(rk_{q,i}, q_i\right) = q_{i+1}$ *for* $0 \le i < s$,
5) $k_p \oplus k_q = \Delta k$, *and*
6) $p_i \oplus q_i = \Delta d_i$ *for* $0 \le i \le s$.

*In particular, we say that an r-round related-key differential characteristic is valid if it is valid up to r rounds.*

**TABLE 5. Part of the differential characteristic #1 of SPECK-48/k.**

| $r$ | $\Delta L$ | $\Delta R$ | $\log_2 p$ |
|---|---|---|---|
| 0 | 480B01 | 094009 | |
| 1 | 081082 | 42084A | $-8$ |

## IV. VALIDITY OF DIFFERENTIAL CHARACTERISTICS OF SIMON, SPECK, AND CHAM

In this section, we examine the validity of the differential characteristics of SIMON, SPECK, and CHAM that appeared in the literature. For CHAM, we also check the validity of the related-key differential characteristics. Furthermore, we give maximum probability of a differential characteristic of CHAM-64/128 by round and an optimal 38-round differential characteristic with probability greater than $2^{-64}$ that is valid.

As mentioned earlier, we utilize a SAT solver, CryptoMiniSAT, to obtain the results. We first set up a set of equations as shown in Section III to find out whether the given differential characteristic is valid or not. Then we convert the set of equations to a Boolean satisfiability problem in the conjunctive normal form so that it can be taken as input to the SAT solver. Finally, we can see whether the differential characteristic is valid or invalid based on the result of the SAT solver (satisfiable or unsatisfiable).

Meanings of the symbols in the last column of the tables that show the validity of the (related-key) differential characteristics are as follows.

- ◯: The given (related-key) differential characteristic is valid.
- × (Up to $i$ rounds): The given (related-key) differential characteristic is not valid. And it is valid up to $i$ rounds, not $i + 1$ rounds.
- ? (Up to $i$ rounds): We do not know whether the given (related-key) differential characteristic is valid or not. However, we do know that it is valid up to $i$ rounds.

### A. SIMON

This subsection shows whether the differential characteristics of SIMON in [5], [12], [13], [14], and [15] are valid or not.

We find that the four differential characteristics of SIMON-32/64, the five differential characteristics of SIMON-48/72, the five differential characteristics of SIMON-48/96, the four differential characteristics of SIMON-64/96, and the four differential characteristics of SIMON-64/128 are all valid (Table 13 in Appendix).

And we only find that each of the four differential characteristics of SIMON-96/96, the four differential characteristics of SIMON-96/144, the two differential characteristics of SIMON-128/128, the two differential characteristics of SIMON-128/192, and the two differential characteristics of SIMON-128/256 is valid up to a certain number of rounds (Table 14 in Appendix). This means that we do not know whether each of them is valid or not. However, we do find that all of them are valid with independent round keys.

**TABLE 6.** Part of the invalid differential characteristic #1 of SPECK-64/*k*.

| $r$ | $\Delta L$ | $\Delta R$ | $\log_2 p$ |
|---|---|---|---|
| 3 | 00000000 | 00000080 | |
| 4 | 40000000 | 40000000 | $-1$ |

**TABLE 7.** Part of the invalid differential characteristic #6 of SPECK-64/*k*.

| $r$ | $\Delta L$ | $\Delta R$ | $\log_2 p$ |
|---|---|---|---|
| 1 | 92480040 | 40184200 | |
| 2 | 008A0A00 | 0481A021 | $-8$ |

**TABLE 8.** Part of the invalid differential characteristic #3 of SPECK-96/*k*.

| $r$ | $\Delta L$ | $\Delta R$ | $\log_2 p$ |
|---|---|---|---|
| 6 | 800000000000 | 000000000000 | |
| 7 | 800000000000 | 008000000000 | $-1$ |

**TABLE 9.** Part of the invalid differential characteristic #1 of SPECK-128/*k*.

| $r$ | $\Delta L$ | $\Delta R$ | $\log_2 p$ |
|---|---|---|---|
| 1 | 2002002828000020 | 2020004928200003 | |
| 2 | 0000900900480001 | 0100001003084008 | $-12.66$ |

**TABLE 10.** Part of the invalid differential characteristic #2 of SPECK-128/*k*.

| $r$ | $\Delta L$ | $\Delta R$ | $\log_2 p$ |
|---|---|---|---|
| 1 | 2012032028080120 | 2020020028280000 | |
| 2 | 0000100318400801 | 0100000249000800 | $-13$ |

### B. SPECK

This subsection shows whether the differential characteristics of SPECK in [5], [6], [7], [14], [16], [17], [18], and [19] are valid or not.

Note that the authors of [7] did not give the differences of the last rounds of their differential characteristics. Therefore, the differential characteristics we experimented are one-round shorter than those they claimed.

We find that all of the twelve differential characteristics of SPECK-32/64 are valid (Table 15 in Appendix).

Out of the nine differential characteristics of SPECK-48/72 and SPECK-48/96, we find that one, #1, is invalid and the others are valid (Table 16 in Appendix).

Now let's see why the differential characteristic #1 is invalid. Suppose that $((\Delta L_0, \Delta R_0), (\Delta L_1, \Delta R_1), \cdots, (\Delta L_r, \Delta R_r))$ be an $r$-round differential characteristic of SPECK. For all $0 \leq i < r$, $\Delta R_{i+1}$ should be equal to $(\Delta R_i \lll \beta) \oplus \Delta L_{i+1}$ for it to be valid. However, for the differential characteristic #1, $\Delta R_1 \neq (\Delta R_0 \lll 3) \oplus \Delta L_1$ as you can see from Table 5. Therefore, it is definitely invalid for both SPECK-48/72 and SPECK-48/96. This means that it is neither valid with independent round keys nor valid under the Markov assumption for both SPECK-48/72 and SPECK-48/96.

We have tested the validity of eighteen differential characteristics of SPECK-64/96 and SPECK-64/128 (Table 17 in Appendix). We find that three, #2, #3, and #5, are valid.

On the other hand, we find that two, #1 and #6, are invalid for both SPECK-64/96 and SPECK-64/128. As you can see from Tables 6 and 7, $\Delta R_4 \neq (\Delta R_3 \lll 3) \oplus \Delta L_4$ for #1 and $\Delta R_2 \neq (\Delta R_1 \lll 3) \oplus \Delta L_2$ for #6. This means that they are neither valid with independent round keys nor valid under the Markov assumption for both SPECK-64/96 and SPECK-64/128.

And we only find that each of the other thirteen differential characteristics is valid up to a certain number of rounds for both SPECK-64/96 and SPECK-64/128. This means that we do not know whether each of them is valid or not. However, we do find that all of them are valid with independent round keys for both SPECK-64/96 and SPECK-64/128.

We have tested the validity of six differential characteristics of SPECK-96/96 and SPECK-96/144 (Table 18 in Appendix). We find that one, #2, is valid.

On the other hand, we find one, #3, is invalid for both SPECK-96/96 and SPECK-96/144. As you can see from Table 8, $\Delta R_7 \neq (\Delta R_6 \lll 3) \oplus \Delta L_7$. This means that it is neither valid with independent round keys nor valid under the Markov assumption for both SPECK-96/96 and SPECK-96/144.

And we only find that each of the other four differential characteristics is valid up to a certain number of rounds for both SPECK-96/96 and SPECK-96/144. This means that we do not know whether each of them is valid or not. However, we do find that all of them are valid with independent round keys for both SPECK-96/96 and SPECK-96/144.

We have tested the validity of six differential characteristics of SPECK-128/128, SPECK-128/192, and SPECK-128/256 (Table 19 in Appendix). We find that one, #4, is valid.

On the other hand, we find two, #1 and #2, are invalid for all of SPECK-128/128, SPECK-128/192, and SPECK-128/256. As you can see from Tables 9 and 10, $\Delta R_2 \neq (\Delta R_1 \lll 3) \oplus \Delta L_1$ for both #1 and #2. This means that they are neither valid with independent round keys nor valid under the Markov assumption for all of SPECK-128/128, SPECK-128/192, and SPECK-128/256.

And we only find that each of the other nine differential characteristics is valid up to a certain number of rounds for all of SPECK-128/128, SPECK-128/192, and SPECK-128/256. This means that we do not know whether each of them is valid or not. However, we do find that all of them are valid with independent round keys for all of SPECK-128/128, SPECK-128/192, and SPECK-128/256.

### C. CHAM

In this subsection, we check the differential characteristics and the related-key differential characteristics of CHAM from [8] and [18].

We have reviewed the validity of three differential characteristics of CHAM-64/128 (Table 20 in Appendix). We find that one, #3, is valid and the other two, #1 and

**TABLE 11.** Maximum probability of a differential characteristic of CHAM-64/128 by round.

| Rounds | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| [8] | 1 | 1 | 1 | 1 | $2^{-1}$ | $2^{-1}$ | $2^{-2}$ | $2^{-3}$ | $2^{-4}$ | $2^{-5}$ |
| This paper | 1 | 1 | 1 | 1 | $2^{-1}$ | $2^{-1}$ | $2^{-2}$ | $2^{-3}$ | $2^{-4}$ | $2^{-5}$ |
| Rounds | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| [8] | $2^{-6}$ | $2^{-7}$ | $2^{-8}$ | $2^{-9}$ | $2^{-11}$ | $2^{-14}$ | $2^{-15}$ | $2^{-16}$ | $2^{-19}$ | $2^{-21}$ |
| This paper | $2^{-6}$ | $2^{-7}$ | $2^{-8}$ | $2^{-9}$ | $2^{-11}$ | $2^{-14}$ | $2^{-15}$ | $2^{-16}$ | $2^{-19}$ | $2^{-21}$ |
| Rounds | 21 | 22 | 23 | 24 | 25 | $26^{\dagger}$ | 27 | $28^{\dagger}$ | $29^{\dagger}$ | $30^{\dagger}$ |
| [8] | $2^{-23}$ | $2^{-25}$ | $2^{-28}$ | $2^{-30}$ | $2^{-32}$ | $2^{-34}$ | $2^{-38}$ | $2^{-39}$ | $2^{-41}$ | $2^{-43}$ |
| This paper | $2^{-23}$ | $2^{-25}$ | $2^{-28}$ | $2^{-30}$ | $2^{-32}$ | $2^{-35}$ | $2^{-38}$ | $2^{-40}$ | $2^{-42}$ | $2^{-46}$ |
| Rounds | $31^{\dagger}$ | $32^{\dagger}$ | $33^{\dagger}$ | $34^{\dagger}$ | $35^{\dagger}$ | $36^{\dagger}$ | $37^{\dagger}$ | $38^{\dagger}$ | $39^{\dagger}$ | 40 |
| [8] | $2^{-46}$ | $2^{-48}$ | $2^{-49}$ | $2^{-51}$ | $2^{-55}$ | $2^{-56}$ | $2^{-58}$ | $2^{-60}$ | $2^{-63}$ | $< 2^{-64}$ |
| This paper | $2^{-49}$ | $2^{-50}$ | $2^{-51}$ | $2^{-53}$ | $2^{-56}$ | $2^{-58}$ | $2^{-59}$ | $2^{-61}$ | $< 2^{-64}$ | |

**TABLE 12.** Optimal 38-round differential characteristic with probability $2^{-61}$ of CHAM-64/128.

| Round | Difference | Prob. | Round | Difference | Prob. | Round | Difference | Prob. |
|---|---|---|---|---|---|---|---|---|
| 0 | 0020 0010 1020 2800 | | 13 | 0001 8100 4001 0200 | $2^{-1}$ | 26 | 0004 0002 0000 0000 | $2^{-1}$ |
| 1 | 0010 1020 2800 0000 | $2^{-1}$ | 14 | 8100 4001 0200 0100 | $2^{-2}$ | 27 | 0002 0000 0000 0000 | $2^{-1}$ |
| 2 | 1020 2800 0000 4000 | $2^{-2}$ | 15 | 4001 0200 0100 0201 | $2^{-2}$ | 28 | 0000 0000 0000 0004 | $2^{-1}$ |
| 3 | 2800 0000 4000 2040 | $2^{-3}$ | 16 | 0200 0100 0201 8003 | $2^{-3}$ | 29 | 0000 0000 0004 0000 | $2^{-0}$ |
| 4 | 0000 4000 2040 5000 | $2^{-2}$ | 17 | 0100 0201 8003 0000 | $2^{-1}$ | 30 | 0000 0004 0000 0000 | $2^{-0}$ |
| 5 | 4000 2040 5000 0080 | $2^{-0}$ | 18 | 0201 8003 0000 0004 | $2^{-2}$ | 31 | 0004 0000 0000 0800 | $2^{-1}$ |
| 6 | 2040 5000 0080 0040 | $2^{-2}$ | 19 | 8003 0000 0004 0402 | $2^{-4}$ | 32 | 0000 0000 0800 0008 | $2^{-1}$ |
| 7 | 5000 0080 0040 4080 | $2^{-2}$ | 20 | 0000 0004 0402 0007 | $2^{-2}$ | 33 | 0000 0800 0008 0000 | $2^{-0}$ |
| 8 | 0080 0040 4080 A000 | $2^{-2}$ | 21 | 0004 0402 0007 0800 | $2^{-1}$ | 34 | 0800 0008 0000 0010 | $2^{-1}$ |
| 9 | 0040 4080 A000 0000 | $2^{-1}$ | 22 | 0402 0007 0800 0400 | $2^{-2}$ | 35 | 0008 0000 0010 1008 | $2^{-2}$ |
| 10 | 4080 A000 0000 0001 | $2^{-1}$ | 23 | 0007 0800 0400 0004 | $2^{-4}$ | 36 | 0000 0010 1008 0010 | $2^{-1}$ |
| 11 | A000 0000 0001 8100 | $2^{-3}$ | 24 | 0800 0400 0004 0002 | $2^{-4}$ | 37 | 0010 1008 0010 2000 | $2^{-1}$ |
| 12 | 0000 0001 8100 4001 | $2^{-1}$ | 25 | 0400 0004 0002 0000 | $2^{-1}$ | 38 | 1008 0010 2000 1000 | $2^{-2}$ |

**TABLE 13.** Validity of the differential characteristics of SIMON-32/64, SIMON-48/72, SIMON-48/96, SIMON-64/96, and SIMON-64/128.

| Cipher | No | Rounds | Prob. | Input difference / Output difference | Ref. | Validity |
|---|---|---|---|---|---|---|
| **SIMON**-32/64 | 1 | 13 | $2^{-36}$ | (0000 0040)/(4000 0000) | [5] | ◯ |
| | 2 | 12 | $2^{-34}$ | (0400 1900)/(1500 0500) | [14] | ◯ |
| | 3 | 13 | $2^{-36}$ | (0000 0040)/(4000 0000) | [14] | ◯ |
| | 4 | 11 | $2^{-30}$ | (0001 4404)/(0444 1010) | [15] | ◯ |
| **SIMON**-48/72 / -48/96 | 5 | 15 | $2^{-46}$ | (008000 022200)/(002200 000800) | [13] | ◯ / ◯ |
| | 6 | 16 | $2^{-50}$ | (800000 220082)/(800000 220000) | [12] | ◯ / ◯ |
| | 7 | 15 | $2^{-50}$ | (010100 044040)/(444040 100000) | [5] | ◯ / ◯ |
| | 8 | 15 | $2^{-48}$ | (200020 080088)/(080888 000200) | [14] | ◯ / ◯ |
| | 9 | 15 | $2^{-46}$ | (000001 400004)/(400044 000010) | [15] | ◯ / ◯ |
| **SIMON**-64/96 / -64/128 | 10 | 21 | $2^{-70}$ | (00080000 00222000)/(00002000 00000000) | [12] | ◯ / ◯ |
| | 11 | 21 | $2^{-80}$ | (00000100 00000440)/(00000440 00000100) | [5] | ◯ / ◯ |
| | 12 | 21 | $2^{-72}$ | (04000000 11000000)/(11000000 04000000) | [14] | ◯ / ◯ |
| | 13 | 19 | $2^{-64}$ | (00000000 00000001)/(00000011 00000004) | [15] | ◯ / ◯ |

#2, are invalid. We also find that the two invalid differential characteristics are invalid with independent round keys. They are valid with independent round keys only up to 21 and 30 rounds, respectively. However, they are both valid under the Markov assumption. This tells us that **CHAM** is not a Markov cipher. Unfortunately, we do not know why the two differential characteristics, #1 and #2, are invalid. Note that it was already shown that #1 is invalid and #3 is valid [3].

We have tested the validity of three differential characteristics of **CHAM**-128/128 and **CHAM**-128/256. We only find that each of them is valid up to a certain number of rounds for both **CHAM**-128/128 and **CHAM**-128/256 (Table 21 in Appendix). Again, this means that we do not know whether each of them is valid or not. However, we do find that all of them are valid with independent round keys for both **CHAM**-128/128 and **CHAM**-128/256.

The designers of **CHAM** also gave a related-key differential characteristic for each of **CHAM**-64/128, **CHAM**-128/128, and **CHAM**-128/256 [8]. Therefore, we have also checked the validity of the related-key differential characteristics of **CHAM**.

**TABLE 14.** Validity of the differential characteristics of SIMON-96/96, SIMON-96/144, SIMON-128/128, SIMON-128/192, and SIMON-128/256.

| Cipher | No | Rounds | Prob. | Input difference / Output difference | Ref. | Validity |
|---|---|---|---|---|---|---|
| **SIMON**-96/96 | 1 | 30 | $2^{-106}$ | (000000100000 000000444040) | [5] | ? (Up to 18 rounds) |
| | | | | (000000010100 000000004440) | | ? (Up to 18 rounds) |
| **SIMON**-96/144 | 2 | 28 | $2^{-96}$ | (000000000001 440000000004) | [15] | ? (Up to 25 rounds) |
| | | | | (000000000100 040000000044) | | ? (Up to 25 rounds) |
| **SIMON**-128/128 | 3 | 41 | $2^{-144}$ | (0000000000001000 0000000000004440) | [5] | ? (Up to 26 rounds) |
| | | | | (0000000000004440 0000000000001000) | | ? (Up to 24 rounds) |
| **SIMON**-128/192 | | | | | | ? (Up to 24 rounds) |
| **SIMON**-128/256 | 4 | 37 | $2^{-128}$ | (0000000000000001 4000000000000004) | [15] | ? (Up to 26 rounds) |
| | | | | (4000000000000004 0000000000000001) | | ? (Up to 26 rounds) |
| | | | | | | ? (Up to 26 rounds) |

**TABLE 15.** Validity of the differential characteristics of SPECK-32/64.

| No | Rounds | Prob. | Input / output differences | Ref. | Validity |
|---|---|---|---|---|---|
| 1 | 9 | $2^{-31}$ | (0A60 4205)/(81A8 D30B) | [5] | ◯ |
| 2 | 9 | $2^{-30}$ | (8054 A900)/(0040 0542) | [14] | ◯ |
| 3 | 9 | $2^{-30}$ | (0211 0A04)/(1001 5001) | [16] | ◯ |
| 4 | 10 | $2^{-35}$ | (2040 0040)/(0800 A840) | [17] | ◯ |
| 5 | 7 | $2^{-30}$ | (0014 0800)/(D440 85E9) | [7] | ◯ |
| 6 | 8 | $2^{-31}$ | (14AC 5209)/(850A 9520) | [7] | ◯ |
| 7 | 9 | $2^{-30}$ | (8054 A900)/(0040 0542) | [18] | ◯ |
| 8 | 9 | $2^{-30}$ | (7458 B0F8)/(802A D4A8) | [19] | ◯ |
| 9 | 9 | $2^{-30}$ | (7C58 B0F8)/(802A D4A8) | [19] | ◯ |
| 10 | 9 | $2^{-30}$ | (1488 1008)/(802A D4A8) | [19] | ◯ |
| 11 | 9 | $2^{-30}$ | (7448 B0F8)/(802A D4A8) | [19] | ◯ |
| 12 | 9 | $2^{-30}$ | (7C48 B0F8)/(802A D4A8) | [19] | ◯ |

**TABLE 16.** Validity of the differential characteristics of SPECK-48/$k$.

| No | Rounds | Prob. | Input / output differences | Ref. | Validity **SPECK**-48/72 / **SPECK**-48/96 |
|---|---|---|---|---|---|
| 1 | 10 | $2^{-41}$ | (480B01 094009)/(808524 84A805) | [5] | × (Up to 0 rounds) / × (Up to 0 rounds) |
| 2 | 11 | $2^{-47}$ | (202040 082921)/(808424 84A905) | [14] | ◯ / ◯ |
| 3 | 11 | $2^{-46}$ | (504200 004240)/(202001 202000) | [17] | ◯ / ◯ |
| 4 | 9 | $2^{-47}$ | (100082 120000)/(919020 B91080) | [7] | ◯ / ◯ |
| 5 | 10 | $2^{-43}$ | (020888 5A4208)/(248085 0584A8) | [7] | ◯ / ◯ |
| 6 | 11 | $2^{-45}$ | (080048 080800)/(808400 848000) | [18] | ◯ / ◯ |
| 7 | 11 | $2^{-45}$ | (001202 020002)/(210020 200021) | [16], [19] | ◯ / ◯ |
| 8 | 11 | $2^{-45}$ | (080048 080800)/(808400 848000) | [19] | ◯ / ◯ |
| 9 | 11 | $2^{-45}$ | (0800C8 080800)/(808400 848000) | [19] | ◯ / ◯ |

We find that the related-key differential characteristic of **CHAM**-64/128 is valid and the related-key differential characteristic of **CHAM**-128/128 is invalid (it's valid up to only 7 rounds). However, we do not know whether the related-key differential characteristic of **CHAM**-128/256 is valid or not. We only find that it is valid up to 40 rounds (Table 22 in Appendix).

The designers of **CHAM** also gave the maximum probability of a differential characteristic by round. However, it is found that there were no valid differential characteristics of **CHAM**-64/128 with the probabilities they gave for several rounds (with † marks in Table 11). This means that for these rounds, the maximum probability of a differential characteristic is smaller than they presented. In particular, we can conclude that there are no valid differential characteristics with probability greater than $2^{-64}$ and that the maximum length of a valid differential characteristic with probability greater than $2^{-64}$ is 38 rounds. We also find an optimal 38-round differential characteristic with probability $2^{-61}$ (Table 12). Note that unfortunately, we do not use the Markov assumption to check the validity of the differential characteristic, but we still use it to calculate the probability of the differential characteristic. This means that the maximum probability per round that we find may not be the exact probability.

## V. CONCLUSION

In this work, we showed that some of the (related-key) differential characteristics of **SIMON**, **SPECK**, and **CHAM** that appeared in the literature are not invalid. To better understand the nature of (related-key) differential characteristics,

**TABLE 17.** Validity of the differential characteristics of SPECK-64/$k$.

| No | Rounds | Prob. | Input / output differences | Ref. | Validity<br>**SPECK**-64/96 / **SPECK**-64/128 |
|---|---|---|---|---|---|
| 1 | 13 | $2^{-55.9}$ | (10420040 40024000)/(20000524 20202C04) | [6] | × (Up to 3 rounds) / × (Up to 3 rounds) |
| 2 | 13 | $2^{-59}$ | (49200020 20082100)/(20000524 20202C04) | [5] | ◯ / ◯ |
| 3 | 14 | $2^{-60}$ | (00000009 01000000)/(00040024 04200D01) | [14] | ◯ / ◯ |
| 4 | 15 | $2^{-62}$ | (04092400 20040104)/(808080A0 A08481A4) | [16], [17] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 5 | 11 | $2^{-63}$ | (00000000 08000000)/(A0A00800 81A0680C) | [7] | ◯ / ◯ |
| 6 | 12 | $2^{-63}$ | (02080888 1A4A0848)/(80008004 84008020) | [7] | × (Up to 1 round) / × (Up to 1 round) |
| 7 | 15 | $2^{-62}$ | (40004092 10420040)/(0A080808 1A4A0848) | [18] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 8 | 15 | $2^{-62}$ | (92400040 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 9 | 15 | $2^{-62}$ | (924000C0 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 10 | 15 | $2^{-63}$ | (96400040 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 11 | 15 | $2^{-63}$ | (B2400040 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 12 | 15 | $2^{-63}$ | (B24000C0 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 13 | 15 | $2^{-63}$ | (92440040 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 14 | 15 | $2^{-63}$ | (924400C0 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 15 | 15 | $2^{-63}$ | (92C000C0 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 16 | 15 | $2^{-63}$ | (964000C0 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 17 | 15 | $2^{-63}$ | (92C00040 40104200)/(080A0808 481A4A08) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 18 | 15 | $2^{-63}$ | (09240004 04010420)/(8080A080 8481A4A0) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |

**TABLE 18.** Validity of the differential characteristics of SPECK-96/$k$.

| No | Rounds | Prob. | Input / output differences | Ref. | Validity<br>**SPECK**-96/96 / **SPECK**-96/144 |
|---|---|---|---|---|---|
| 1 | 13 | $2^{-84}$ | (2A20200800A2 322320680801)/(01008004C804 0C0180228C60) | [5] | ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 2 | 10 | $2^{-92}$ | (000000000080 000000000000)/(C00481364920 80608C811463) | [7] | ◯ / ◯ |
| 3 | 13 | $2^{-89}$ | (A22A20200800 013223206808)/(80A0A0000088 8C81A02004C8) | [7] | × (Up to 6 rounds) / × (Up to 6 rounds) |
| 4 | 16 | $2^{-87}$ | (010420040000 000024000400)/(800400008124 842004008801) | [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 5 | 16 | $2^{-87}$ | (240004000009 010420040000)/(800400008124 842004008801) | [16], [19] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |
| 6 | 17 | $2^{-96}$ | (240004000009 010420040000)/(A0A000008880 81A02004C88C) | [17] | ? (Up to 14 rounds) / ? (Up to 14 rounds) |

**TABLE 19.** Validity of the differential characteristics of SPECK-128/$k$.

| No | Rounds | Prob. | Input difference<br>Output difference | Ref. | Validity<br>**SPECK**-128/128 / **SPECK**-128/192 / **SPECK**-128/256 |
|---|---|---|---|---|---|
| 1 | 15 | $2^{-117.28}$ | (0640240804002440 6004400C20040004)<br>(888080A080820828 E88C81A4A0924B2C) | [6] | × (Up to 1 round) / × (Up to 1 round) / × (Up to 1 round) |
| 2 | 14 | $2^{-112}$ | (144304280C010420 0006402400040024)<br>(0180208402886884 0080248012C96C80) | [5] | × (Up to 1 round) / × (Up to 1 round) / × (Up to 1 round) |
| 3 | 20 | $2^{-128}$ | (0124000400000000 0801042004000000)<br>(8004000080000124 8420040080000801) | [17] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 4 | 11 | $2^{-125}$ | (0000000000000060 0000000000000000)<br>(8808020008280082 80c81a0201682804) | [7] | ◯ / ◯ / ◯ |
| 5 | 15 | $2^{-127}$ | (0096492440040124 0420144304600c01)<br>(04810080048000c8 608c018020840288) | [7] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 6 | 19 | $2^{-120}$ | (0124000400000010 0801042004000000)<br>(8080808000000020 A084808000000124) | [19] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 7 | 19 | $2^{-119}$ | (0124000400000000 0801042004000000)<br>(8080808000000020 A084808000000124) | [16]<br>[19] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 8 | 19 | $2^{-120}$ | (0324000400000000 0801042004000000)<br>(8080808000000020 A084808000000124) | [19] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 9 | 19 | $2^{-120}$ | (0124000C00000000 0801042004000000)<br>(8080808000000020 A084808000000124) | [19] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 10 | 19 | $2^{-120}$ | (0124400400000000 0801042004000000)<br>(8080808000000020 A084808000000124) | [19] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 11 | 19 | $2^{-120}$ | (012C000400000000 0801042004000000)<br>(8080808000000020 A084808000000124) | [19] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |
| 12 | 19 | $2^{-120}$ | (0164000400000000 0801042004000000)<br>(8080808000000020 A084808000000124) | [19] | ? (Up to 11 rounds) / ? (Up to 11 rounds) / ? (Up to 11 rounds) |

we defined several definitions of validity and classified them according to these definitions.

Whereas there has been research on the validity of differential characteristics of SPN-based block ciphers, this

**TABLE 20.** Validity of the differential characteristics of CHAM-64/128.

| No | Rounds | Prob. | Input / output differences | Ref. | Validity |
|---|---|---|---|---|---|
| 1 | 39 | $2^{-63}$ | (0102 0280 0000 0400) / (0100 0281 0002 0000) | [8] | × (Up to 20 rounds) |
| 2 | 44 | $2^{-73}$ | (4000 8040 00A0 0000) / (0001 8100 0001 0200) | [8] | × (Up to 29 rounds) |
| 3 | 39 | $2^{-64}$ | (0020 0010 1020 2800) / (0010 2000 1000 2810) | [18] | ○ |

**TABLE 21.** Validity of the differential characteristics of CHAM-128/*k*.

| No | Rounds | Prob. | Input difference / Output difference | Ref. | Validity **CHAM**-128/128 / **CHAM**-128/256 |
|---|---|---|---|---|---|
| 1 | 62 | $2^{-126}$ | (08000000 04000000 000C0800 00020008) / (04000002 00040001 00000800 00000400) | [8] | ? (Up to 40 rounds) / ? (Up to 40 rounds) |
| 2 | 67 | $2^{-138}$ | (0001000C 08000000 04000000 000C0800) / (08000004 00180002 00000000 00000010) | [8] | ? (Up to 44 rounds) / ? (Up to 40 rounds) |
| 3 | 64 | $2^{-130}$ | (80000000 40000000 00408000 00200080) / (00008000 00004000 80000040 00800020) | [18] | ? (Up to 40 rounds) / ? (Up to 40 rounds) |

**TABLE 22.** Validity of the related-key differential characteristics of CHAM in [8].

| Cipher | No | Rounds | Prob. | Key difference / Input difference / Output difference | Validity |
|---|---|---|---|---|---|
| **CHAM**-64/128 | 1 | 47 | $2^{-57}$ | (0000 0000 3251 A938 0000 0000 100F A463) / (0000 0000 0000 83E0) / (F8C3 0000 0000 0000) | ○ |
| **CHAM**-128/128 | 2 | 47 | $2^{-120}$ | (00000000 00000000 24924925 24924925) / (00000000 00000000 00000000 FFFFFF25) / (FFFFF925 00000000 00000000 00000000) | × (Up to 7 rounds) |
| **CHAM**-128/256 | 3 | 47 | $2^{-121}$ | (00000000 00000000 5BEE1236 00800000 00000000 00000000 B5DC246C 6AB848D9) / (00000000 00000000 00000000 81100000) / (3EC7091F 00000000 00000000 00000000) | ? (Up to 40 rounds) |

paper focused on the validity of differential characteristics of ARX-based block ciphers. So we took a slightly different approach. We constructed a set of equations, which can verify the validity of a (related-key) differential characteristic, and converted it to a Boolean satisfiability problem. Then we used a SAT solver to see if the Boolean satisfiability problem is satisfiable or not.

Invalidity of a differential characteristic does not mean that it can not be used for a differential attack, because a differential attack uses a differential and not a differential characteristic. However, it does mean that some of the differential characteristics that make up the differential are invalid, so the probability of the differential will be smaller than expected. Therefore, this affects the probability of success of the differential attack using the differential, and in some cases, the attack may not be feasible.

In order to better understand the properties of differential characteristics of ARX-based block ciphers, we anticipate that the following further studies are necessary:

- finding a way to check the validity of the (related-key) differential characteristics more efficiently,
- finding theoretical backgrounds on the validity of (related-key) differential characteristics,
- calculating an exact probability of a (related-key) differential characteristic,
- calculating an exact probability of a (related-key) differential, and
- studying whether the approach in this paper can be leveraged for the characteristics used in other attacks such as linear cryptanalysis, rotational-XOR cryptanalysis, truncated differential cryptanalysis, etc.

## APPENDIX
## DETAILED RESULTS

In this appendix, we present tables describing detailed results on the validity of the (related-key) differential characteristics.

## REFERENCES


[1] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Proc. Adv. Cryptology-EUROCRYPT Workshop Theory Appl. Cryptograph. Techn.* Brighton, U.K.: Springer, Apr. 1991, pp. 17–38.

[2] A. Biryukov, V. Velichkov, and Y. L. Corre, "Automatic search for the best trails in ARX: Application to block cipher SPECK," in *Proc. Fast Softw. Encryption, 23rd Int. Conf.* Bochum, Germany: Springer, Mar. 2016, pp. 289–310.

[3] Z. Xu, Y. Li, L. Jiao, M. Wang, and W. Meier, "Do NOT misuse the Markov cipher assumption—Automatic search for differential and impossible differential characteristics in ARX ciphers," Cryptol. ePrint Arch., Paper 2022/135, 2022. [Online]. Available: https://eprint.iacr.org/2022/135

[4] T. Peyrin and Q. Q. Tan, "Mind your path: On (key) dependencies in differential characteristics," *IACR Trans. Symmetric Cryptol.*, vol. 2022, no. 4, pp. 179–207, 2022.
[5] F. Abed, E. List, S. Lucks, and J. Wenzel, "Differential cryptanalysis of round-reduced SIMON and SPECK," in *Proc. Fast Softw. Encryption, 21st Int. Workshop* London, U.K.: Springer5, 2015, pp. 525–554.
[6] F. Abed, E. List, S. Lucks, and J. Wenzel, "Cryptanalysis of the SPECK family of block ciphers," Cryptol. ePrint Arch., Paper 2013/568, 2013. [Online]. Available: https://eprint.iacr.org/2013/568
[7] A. D. Dwivedi and P. Morawiecki, "Differential cryptanalysis of round-reduced SPECK," Cryptol. ePrint Arch., Paper 2018/899, 2018. [Online]. Available: https://eprint.iacr.org/2018/899
[8] D. Roh, B. Koo, Y. Jung, I. W. Jeong, D.-G. Lee, D. Kwon, and W.-H. Kim, "Revised version of block cipher CHAM," in *Proc. Inf. Secur. Cryptol. 22nd Int. Conf.* Seoul, South Korea: Springer, Dec. 2020, pp. 1–19.
[9] N. Eén and N. Sörensson, "An extensible SAT-solver," in *Proc. Int. Conf. Theory Appl. Satisfiability Test.* Cham, Switzerland: Springer, 2003, pp. 502–518.
[10] Y. Hamadi, S. Jabbour, and L. Sais, "ManySAT: A parallel SAT solver," *J. Satisfiability, Boolean Model. Comput.*, vol. 6, no. 4, pp. 245–262, 2010.
[11] M. Soos, K. Nohl, and C. Castelluccia, "Extending SAT solvers to cryptographic problems," in *Proc. Int. Conf. Theory Appl. Satisfiability Test.* Cham, Switzerland: Springer, 2009, pp. 244–257.
[12] S. Sun, L. Hu, M. Wang, P. Wang, K. Qiao, X. Ma, D. Shi, L. Song, and K. Fu, "Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties," Cryptol. ePrint Arch., Paper 2014/747, 2014. [Online]. Available: https://eprint.iacr.org/2014/747
[13] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers," in *Proc. Adv. Cryptology–ASIACRYPT 20th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Kaoshiung, Taiwan: Springer, Dec. 2014, pp. 158–178.
[14] A. Biryukov, A. Roy, and V. Velichkov, "Differential analysis of block ciphers SIMON and SPECK," in *Proc. Fast Softw. Encryption, 21st Int. Workshop*. London, U.K.: Springer, Mar. 2015, pp. 546–570.
[15] Z. Liu, Y. Li, and M. Wang, "Optimal differential trails in SIMON-like ciphers," *IACR Trans. Symmetric Cryptol.*, vol. 2017, no. 1, pp. 358–379, Mar. 2017. [Online]. Available: https://tosc.iacr.org/index.php/ToSC/article/view/598, doi: 10.13154/tosc.v2017.i1.358-379.
[16] K. Fu, M. Wang, Y. Guo, S. Sun, and L. Hu, "MILP-based automatic search algorithms for differential and linear trails for SPECK," in *Proc. Fast Softw. Encryption, 23rd Int. Conf.* Bochum, Germany: Springer, Mar. 2016, pp. 268–288.
[17] L. Song, Z. Huang, and Q. Yang, "Automatic differential analysis of ARX block ciphers with application to SPECK and LEA," in *Proc. Inf. Secur. Privacy, 21st Australas. Conf.* Melbourne, VIC, Australia: Springer, Jul. 2016, pp. 379–394.
[18] M. Huang and L. Wang, "Automatic tool for searching for differential characteristics in ARX ciphers and applications," in *Proc. 20th Int. Conf. Cryptol.* India, Hyderabad: Springer, Dec. 2019, pp. 115–138.
[19] Z. Feng, Y. Luo, C. Wang, Q. Yang, Z. Liu, and L. Song, "Improved differential cryptanalysis on SPECK using plaintext structures," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Springer, 2023, pp. 3–24.

**DONGYOUNG ROH** (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in mathematics from the Korea Institute of Science and Technology, Daejeon, South Korea, in 2011.

From 2011 to 2012, he was a Researcher with the National Institute for Mathematical Sciences. Since 2012, he has been a Principal Researcher with the Affiliated Institute of ETRI. He is the author of more than ten articles and holds two patents. His research interests include designing and analyzing cryptographic algorithms, relations between discrete logarithm related problems.

Dr. Roh was a recipient of the Mid-Career Professional in Global Achievement Awards by $(ISC)^2$ in 2020. He is an editor of three ISO/IEC standards.