Designs, Codes and Cryptography manuscript No.
(will be inserted by the editor)

Proposing an MILP-based Method for the Experimental Verification of Difference-based Trails

Application to SPECK, SIMECK

Sadegh Sadeghi · Vincent Rijmen · Nasour Bagheri*

Received: date / Accepted: date

Abstract Searching for the right pairs of inputs in difference-based distinguishers is an important task for the experimental verification of the distinguishers in symmetric-key ciphers. In this paper, we develop an MILP-based approach to verify the possibility of difference-based distinguishers and extract the right pairs. We apply the proposed method to some published difference-based trails (Related-Key Differentials (RKD), Rotational-XOR (RX)) of block ciphers `SIMECK`, and `SPECK`. As a result, we show that some of the reported RX-trails of `SIMECK` and `SPECK` are incompatible, i.e. there are no right pairs that follow the expected propagation of the differences for the trail. Also, for compatible trails, the proposed approach can efficiently speed up the search process of finding the exact value of a weak key from the target weak key space. For example, in one of the reported 14-round RX trails of `SPECK`, the probability of a key pair to be a weak key is $2^{-94.91}$ when the whole key space is 2^{96}; our method can find a key pair for it in a comparatively short time. It is worth noting that it was impossible to find this key pair using a traditional search. As another result, we apply the proposed method to `SPECK` block cipher, to construct longer related-key differential trails of `SPECK` which we could reach 15, 16, 17, and 19 rounds for `SPECK32/64`, `SPECK48/96`, `SPECK64/128`, and `SPECK128/256`, respectively. It should be compared with the best previous results which are 12, 15, 15, and 20 rounds, respectively, that both attacks work

S. Sadeghi
imec-COSIC, KULeuven, Belgium.
Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran E-mail: s.sadeghi.khu@gmail.com

V. Rijmen
imec-COSIC, KULeuven, Belgium.
Department of Informatics, University of Bergen, Norway.
E-mail: vincent.rijmen@kuleuven.be

N. Bagheri (***Corresponding author**)
Electrical Engineering Department, Shahid Rajaee Teacher Training University (SRTTU), Tehran, Iran, E-mail: Nbagheri@sru.ac.ir

for a certain weak key class. It should be also considered as an improvement over the reported result of rotational-XOR cryptanalysis on SPECK.

Keywords Experimental verification · Differential-based distinguishers · Weak keys · Related key · MILP · SPECK · SIMECK

1 Introduction

Mixed Integer Linear Programming (MILP) was introduced in [38,49] to evaluate the security of a block cipher against differential and linear cryptanalysis. Mouha *et al.* [38] used MILP method to minimize the number of active S-boxes in a differential or linear trail. Later, Sun *et al.* in [46, 47] extended Mouha *et al.*'s work from byte-oriented ciphers to bit-oriented ciphers. Recently, MILP has been widely used for the cryptanalysis of block ciphers so that [13, 17, 39, 40, 42, 53] can be mentioned as some examples among others. Other automatic tools for the cryptanalysis of block ciphers are constraint programming see [18, 19, 45], SAT/SMT/CryptoSMT see [12, 21, 29, 35].

ARX-based ciphers are designed using only modular Addition, Rotation, and XOR. In particular, the only source of non-linearity in an ARX scheme is the modular addition. Algorithms built in this fashion are usually faster and smaller than S-Box-based algorithms in software, and have some inherent security against side-channel attacks as modular addition leaks less information than table look-ups. However, modular addition is not very attractive in designing hardware optimized algorithms due to its latency and "large" input and output size. Some examples of ARX ciphers are: the block ciphers SPECK [5], HIGHT [23], LEA [22], the stream cipher SALSA20 [6], and the SHA-3 finalists SKEIN [16] and BLAKE [4]. SPECK is a family of lightweight block ciphers that uses an ARX structure that was publicly released by the National Security Agency (NSA) in 2013 [5]. SPECK has been optimized for performance in software implementations. SPECK is evaluated by many cryptanalysis techniques [2, 10, 11, 14, 17, 24, 34, 43, 52].

The probability of differential trails (in differential [8] or rotational-XOR [3] cryptanalysis) is usually built by multiplying the probabilities of each non-linear operation, but this approach can lead to very misleading results in some ciphers. For example, in some ARX-based ciphers, the independence assumption does not hold since it is possible for an output of modular addition to be directly given as input to another modular addition. Therefore, in such cases, the probabilities of modular additions cannot be computed as the product of probabilities of the individual modular additions. It is important to note that in the case of ARX ciphers such differences were already described for some attacks. For example, Knudsen *et al.* in [28], treated this issue for the differential attack on RC2 block cipher. As another example, the authors of [26], investigated this issue for the rotational cryptanalysis on ARX structures. Several recent works have found trails that were incompatible when analyzing ARX hash functions [9, 30, 31, 37, 41, 48] and many others. Also, Elsheikh *et al.* in [15] recently studied this issue and proposed an MILP model to describe the differential propagation through the modular addition considering the dependency between the consecutive modular additions and utilized their approach to automate the search process for the differential trails for `Bel-T` cipher.

Recently, Liu *et al.* presented an MILP model for the automatic verification of differential characteristics in permutation-based primitives [33]. Their main idea is modeling the differential transitions and value transitions simultaneously for permutation-based primitives and then connecting the value transitions and differential transitions for non-linear operations used in primitives. They successfully applied their approach to reduced `Gimli` hash function [7]. To this end, in a part of their work, they described how they connected the value and differential transitions of AND and OR operations (the only non-linear operations used in `Gimli`). However, they did not explain how one can connect the value and differential transitions simultaneously for the other non-linear operations. Hence, our work has some advantages over [33]. In fact, our approach in this paper can be applied easily to any cipher structure with usual non-linear operations such as AND, OR, Addition modulo 2^n, S-boxes layers, and others. Also, as will be explained later, our approach can be efficiently used to verify the differential, related-key differential, and rotational-XOR trails of ciphers.

In this paper, for the first time, to the best of our knowledge, we present an MILP-based approach to experimentally verify whether a difference-based distinguisher includes any right pair. As for the applications, we apply our approach to the obtained differential trails of `SIMECK` and `SPECK` family of block ciphers. Also, the designers of `SPECK` family claim that `SPECK` is designed to have resistance against related-key attacks. Part of this paper, focuses on the automatic related-key differential cryptanalysis of a reduced `SPECK` block cipher to find distinguishers covering more rounds than those found previously. Moreover, the `SPECK` family of block ciphers is standardized by ISO in the RFID area of Sc31. Hence, analysis from various aspects is important.

1.1 Our Contribution

Our contribution in this paper is as follows:

- In this paper, we applied the MILP approach to identify incompatible differential trails of block ciphers. Moreover, to the best of our knowledge, for the first time we applied the MILP approach to efficiently speed up the search process of finding the exact value of a weak key from the target weak key space. As the applications, we apply our approach to verify the presented Rotational-XOR (RX) trails of SPECK and SIMECK family of block ciphers based on papers [34] and [36], respectively.
- We find some weak keys for 15 and 20-round RX-trails of `SIMECK32/64`, according to the tables 4 and 6 of [36]. Also, our approach returns this fact that the RX-trails for 27 and 35 rounds of `SIMECK48/96`, and `SIMECK64/128`, based on tables 7 and 8, respectively in [36], are incompatible.

- Our approach can find the weak keys for 12, 13, and 15-round RX-trail of SPECK48/96 based on tables 3 and 4 in [34]. Moreover, our approach shows that RX-trails for 11 and 12 rounds of SPECK32/64, and 14 rounds of SPECK48/96, according to tables 2 and 4 in [34], are incompatible trails.
- In addition, we explain how we can search compatible differential trails in block ciphers and apply it to search related-key differential trails of some variants of SPECK family. As a result, we present a search strategy for the searching of related-key differential trails of SPECK family. We also present several distinguishers for the reduced version of SPECK32/64, SPECK48/96, SPECK64/128, and SPECK128/256, in related-key mode. We consider our result for related-key differential as an improvement over Liu *et al.*'s work [34], but from differential view. For SPECK32/64, the longest distinguisher proposed in this paper covers 15 rounds of the cipher while the best previous related work, i.e., rotational-XOR differential trail, covers only 12-round [34] (of course we show that this 12-round is an invalid trail). In total, for this version of SPECK, we present distinguishers for 10 to 15 rounds which work for a certain weak key class. It is worth noting that the proposed distinguishers for 13 to 15 rounds are the new distinguishers for these rounds of SPECK32/64. For SPECK48/96, our longest distinguishers cover 16 rounds, while the best previous related work covers 15 rounds [34] and both work for a certain weak key class. We present the distinguishers for 13 to 17 rounds of SPECK64/128 so that the distinguishers for 16 and 17 rounds are the new distinguishers for these rounds of SPECK64/128, for a certain weak key class. Also, we present the distinguishers for 16 and 19 rounds of SPECK128/256.
- Moreover, for every obtained related-key differential of SPECK family, we use our MILP-based approach to test whether the key differential trails are valid. For each one, we report a weak key to verify it. Based on our experimental verification, our results are consistent with the theoretical predictions.

In this paper, the computations are performed on PC (Intel Core (TM)i-5, CPU 3.50 GHz, 8 Gig RAM, Windows 10 x64) and also on a server (36 Core, Intel(R) Xeon(R) CPU E5-2695, 2.10GHz) with the optimizer Gurobi [20].

1.2 Outline

The remainder of this paper is organized as follows. Section 2 provides the required preliminaries, including a brief description of SPECK and SIMECK block ciphers and as well as Rotational-XOR cryptanalysis. In Section 3, our MILP-based method in searching for the right pairs of difference-based trails is presented. In Section 4, some applications of our approach are given. We explain how we can search compatible differential trails in block ciphers and apply it to search related-key differential trails of some variants of SPECK family. Finally, the paper is concluded in Section 6.

2 Preliminaries

2.1 Notations

In this paper, we denote an n-bit vector by $x = (x_{n-1}, \cdots, x_1, x_0)$, where x_0 is the least significant bit. Also, the logical operation XOR, left circular rotation, right circular rotation, the concatenation of x and y, the modular addition of bit string x and y, and the bit-wise AND are referred to as $\oplus$, $\lll$, $\ggg$, $x\|y$, $x \boxplus y$, and &, respectively. Also, all input/output differentials (or values) are in hexadecimal form and we omit the `0x` symbol.

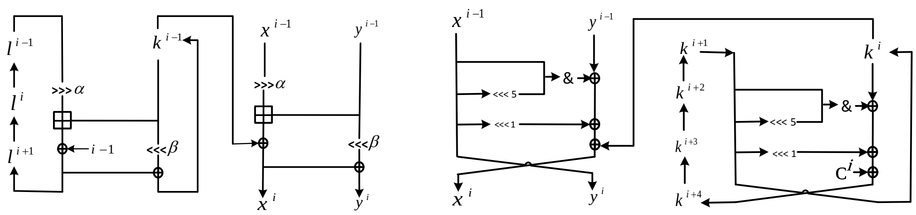
2.2 A brief description of SPECK

SPECK is a family of lightweight block ciphers designed by NSA in 2013 [5]. Generally, SPECKb/mn will denote SPECK with $b = 2n$ bit block size ($n \in \{16, 24, 32, 48, 64\}$) and mn bits key size ($m \in \{2, 3, 4\}$). The round function $F : \mathbb{F}_2^n \times \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ of SPECK takes as input a n bit sub-key k^{i-1} and a cipher state consisting of two n bit words (x^{i-1}, y^{i-1}) and produces the next round state (x^i, y^i) as follows:

$$x^i := \big((x^{i-1} \ggg \alpha) \boxplus y^{i-1}\big) \oplus k^{i-1}, \ \ y^i := \big(y^{i-1} \lll \beta\big) \oplus x^i$$

The value of rotation constant α and β are specified as: $\alpha = 7$, $\beta = 2$ for SPECK32/64 and $\alpha = 8$, $\beta = 3$ for all other variants. The SPECK key schedules algorithm uses the same round function to generate the round keys. Let $K = (l^{m-2}, \cdots, l^0, k^0)$ be a master key for SPECK$2n/mn$ where $l^i, k^0 \in \mathbb{F}_{2^n}$. The round key k^{i+1} is generated as $k^i = ((l^{i-1} \ggg \alpha) \boxplus k^i) \oplus c \oplus (k^{i-1} \lll \beta)$ for $l^{i+m-2} = ((l^{i-1} \ggg \alpha) \boxplus k^{i-1}) \oplus c$, with $c = i - 1$ the round number starting from 1.

A single round of SPECK with $m = 4$ is depicted in Figure 1a.



(a) One round of SPECK (for $m = 4$)

(b) One round of SIMECK

Fig. 1: Illustration of the SPECK and SIMECK ciphers

In this paper, we consider those members of SPECK family for which the parameter of m is 4, i.e., SPECK32/64, SPECK48/96, SPECK64/128, and SPECK128/256 that respectively include 22, 23, 27, and 34 rounds, to produce a ciphertext from a plaintext.

2.3 A short description of SIMECK

SIMECK is a family of block ciphers that was proposed at CHES 2015 [51]. For $n = 16, 24$, and 32, SIMECKb/k has a block size of $b = 2n$ and a key size of $k = 2b$. It is a classical Feistel network shown in Figure 1b where the function F is defined as $F(x^{i-1}) = x^{i-1} \& (x^{i-1} \lll 5)$. In the key schedule of SIMECK, the round keys $K^i \quad (i = 0, \cdots, r)$ are generated from a given master key (K^3, K^2, K^1, K^0) with the help of the feedback shift registers as follows:

$$K^{i+4} = K^i \oplus f_{c^i}(K^{i+1}) \oplus c^i, \quad i = 0, 1, \cdots, r-4, \tag{1}$$

where r for SIMECK32/64, SIMECK48/96, and SIMECK64/128 is 32, 36, and 44, respectively. Also, $c^i \in \{1_{n-2}01, 1_{n-2}00\}$ is predefined constants (1_{n-2} is a sequence of $n-2$ bit 1) and f_c^i is the SIMECK round function with c^i acting as the round key.

2.4 Rotational-XOR(RX) cryptanalysis

Rotational cryptanalysis is a generic attack targeting ARX structures [25,27]. RX-cryptanalysis is a recent technique as a related-key chosen plaintext attack to ARX structures proposed by Ashur and Liu in 2016 [3]. This attack was applied to the block cipher SPECK [34], SIMECK [36] and the hash function SipHash [50]. An RX-pair is defined as a rotational pair with rotational offset γ under translation a as $(x, (x \lll \gamma) \oplus a)$.

Definition 1 (RX-difference [3]) The RX-difference of x and $x' = (x \lll \gamma) \oplus a$ with rotational offset γ, and translation a is denoted by

$$\Delta_\gamma(x, x') = (x \lll \gamma) \oplus x'.$$

Furthermore, we will argue that RX difference of a pair (x, x') is $\Delta_\gamma(x, x')$ if $(x \lll \gamma) \oplus x' = \Delta_\gamma(x, x')$. It is clear that the rotation of an RX pair is an RX pair, the XOR of two RX pairs is also an RX pair. Also, the XOR of a constant c to each of the values in $(x, x') = (x, (x \lll \gamma) \oplus a)$ is the RX-pair $(z, z') = (x \oplus c, (x \lll \gamma) \oplus a \oplus c)$. Now, soppose that we denote the corresponding RX-difference in c by $\Delta^\gamma c$. Then the following condition should be satisfied.

$$\Delta_\gamma(x, x^{'}) \oplus \Delta^\gamma c = \Delta_\gamma(z, z^{'}).$$

Since $\Delta_\gamma(x, x^{'}) = a$ and $\Delta_\gamma(z, z^{'}) = a \oplus c \oplus (c \lll \gamma)$, therefore, the condition above gives us $\Delta^\gamma c = c \oplus (c \lll \gamma)$. Hence, by considering the corresponding RX-difference in c as $\Delta^\gamma c = c \oplus (c \lll \gamma)$, $\Delta_\gamma(x, x^{'})$ propagates to $\Delta_\gamma(z, z^{'})$ with propability 1.

For modular addition, in ([3], theorem 1) the authors showed how one can calculate the transition probability of RX pair through modular addition. In addition, the authors of [36] extended the idea of RX-cryptanalysis to AND-RX ciphers with applications to `SIMON` and `SIMECK`. We assume that $\gamma = 1$ throughout this paper.

3 MILP-based method to identify incompatible differential trails

In this section, we explore a simple approach based on the MILP method to verify whether the differential trails are compatible. Also, it must be noted that our method in this section can be very useful in most cases to find weak keys in related-key scenarios.

3.1 Our approach

To experimentally verify whether an RX or differential distinguisher includes any right pair, a common way is to use a simple method of guessing the keys and check the differences of the states. However, it is often infeasible because of the block size of the cipher and the probability of the distinguisher. In this section, we model an MILP-based method to determine whether there exist right pairs for the differential trails. To this end, suppose f is a function with variables $x_0, x_2, \cdots x_{n_v-1}$. In our approach, we built some linear inequalities to ensure that the following conditions are exactly established and added them to the MILP model.

$$f(x_0, x_2, \ldots, x_{n_v-1}) = y\,, \quad f(x'_0, x'_2, \ldots, x'_{n_v-1}) = y',$$

$$\Delta(x_0, x'_0) = X_0,\ \ \Delta(x_2, x'_2) = X_2, \ldots, \Delta(x_{n_v-1}, x'_{n_v-1}) = X_{n_v-1},$$

$$\Delta(y, y') = Y,$$

where the difference $\Delta(a, b)$ is defined as $a \oplus b$ and $\Delta_1(a, b)$ in case of differential and RX trails, respectively. In this paper, the function f is considered as the encryption function or key expansion function of a block cipher. It is obvious that for a given differential trail of a cipher, if its MILP model, as shown above is infeasible then the trail will be an incompatible trail; otherwise, the model returns the right pairs.

Each cipher is designed by combining several operations. The most important operations used in cryptographic algorithms are AND, modular addition, rotation, XOR operations. In the following section, we show that there is a set of linear inequalities which can exactly describe all valid values of these operators in the MILP model.

3.1.1 Modeling the XOR operation

For every XOR operation, with bit-level input values x_1, x_2, and bit-level output value y, the constraints are as follows[1]:

$$\begin{cases} x_1 + x_2 + y \leq 2, & x_1 + x_2 - y \geq 0, \\ x_1 + y - x_2 \geq 0, & x_2 + y - x_1 \geq 0. \end{cases} \tag{2}$$

3.1.2 Modeling the modular addition

In the following section, we present the basic definition of modular addition that will be used to model the modular addition.

Definition 2 (Addition modulo 2^n [32]) The carry, $\text{carry}(x, y) := c \in \{0,1\}^n, x, y \in \{0,1\}^n$, of addition $x + y$ is defined recursively as follows. First, $c_0 := 0$. Second, $c_{i+1} := (x_i \wedge y_i) \oplus (x_i \wedge c_i) \oplus (y_i \wedge c_i)$, for every $i \geq 0$. Equivalently, $c_{i+1} = 1 \Leftrightarrow x_i + y_i + c_i \geq 2$.

Property 1 (**[32]**) If $(x, y) \in \{0,1\}^n \times \{0,1\}^n$, then $x + y = x \oplus y \oplus carry(x, y)$.

Based on Definition 2 and Property 1, to model the modular addition ($z = x + y$) in the MILP model, we must consider the linear inequalities whose solution set is exactly satisfied in the following conditions.

$$\begin{array}{l} 1.\ c_0 = 0. \\ 2.\ c_{i+1} = 1 \Leftrightarrow x_i + y_i + c_i \geq 2,\ for\ \ i = 0, \cdots, n-2. \\ 3.\ z_i = x_i \oplus y_i \oplus c_i,\ \ for\ \ i = 0, \cdots, n-1. \end{array} \tag{3}$$

Therefore, it is enough to describe these conditions of the Equatione (3) as linear inequalities. The first condition is obvious. To model the second condition, we can consider the vector (x_i, y_i, c_i, c_{i+1}) as follows.

$$(x_i, y_i, c_i, c_{i+1}) \in \left\{ \begin{array}{cccc} (0,0,0,0) & (0,0,1,0) & (0,1,0,0) & (0,1,1,1) \\ (1,0,0,0) & (1,0,1,1) & (1,1,0,1) & (1,1,1,1) \end{array} \right\}.$$

Therefore, we consider the equations which prohibit the invalid (x_i, y_i, c_i, c_{i+1}). Hence, for $i = 0, \cdots, n-2$, we have

$$\begin{cases} x_i + y_i - c_{i+1} \geq 0, & x_i + c_i - c_{i+1} \geq 0, & y_i + c_i - c_{i+1} \geq 0, \\ y_i + c_i - c_{i+1} \leq 1, & x_i + c_i - c_{i+1} \leq 1, & x_i + y_i - c_{i+1} \leq 1, \end{cases}$$

To model the third condition, we can consider the following equations.

$$x_i + y_i + z_i + c_i - 2d_i = 0, \quad d_i = 0\ or\ 1\ or\ 2, \quad i = 0, \cdots, n-1.$$

Therefore, with these inequalities, we can model the exact values of modular addition operation to the MILP.

[1] XOR operation is a linear operation and can be modeled similar to the differential behavior of XOR based on [1].

3.1.3 Modeling the AND operation

For every AND operation with bit-level input values x_1, x_2. and bit-level output value y, the constraints are as follows:

$$x_1 - y \geqslant 0, \quad x_2 - y \geqslant 0, \quad x_1 + x_2 - y \leqslant 1.$$

4 Applications

In this section, we apply our method to verify RX trails for `SPECK` and `SIMECK` presented in [34] and [36], respectively.

4.1 Verifying the previous reported RX trails on `SIMECK`

The authors of [36] analyzed the propagation of RX-differences through AND-RX rounds and developed a formula for their expected probability. Also, they formulated an SMT model for searching RX-trails in `SIMON` and `SIMECK`. They found RX-distinguishers up to 20, 27, and 35 rounds with respective probabilities of 2^{-26},2^{-42}, and 2^{-54} for `SIMECK32/64`, `SIMECK48/94`, and `SIMECK64/128`, for a weak key class of size $2^{30}, 2^{44}$ and 2^{56} respectively. In most cases, these are the longest published distinguishers for the respective variants of `SIMECK`. The authours of [36] only presented the details of a 15 and 20-round RX trail in `SIMECK32/64`, a 27-round RX trail in `SIMECK48/96`, and a 35-round RX trail in `SIMECK64/128` (see [36], tables 4, 6, 7, and 8, respectively). Here we intend to find the right key pairs that satisfy the required RX-difference of the sub-keys in tables mentioned in [36].

The `SIMECK` key schedule algorithm is designed by combining AND, bit rotation, and XOR operations. Hence, we can model the `SIMECK` key schedule with the method described in Section 3 and then fix the RX-difference in sub-keys based on the mentioned RX trails. Our model returned the following result:

- For 15 and 20-round RX trails of `SIMECK32/64` ([36], tables 4, 6), our method found some weak keys (see Table 1).
- The RX trails in [36] for 27 and 35 rounds of `SIMECK48/96` and `SIMECK64/128`, respectively, are incompatible.

In the following lemma, we prove the incompatibility of RX trail related to 27 rounds of `SPECK48/96` in [36].

Lemma 1 *There are no right pair to satisfy the RX-difference of the sub-keys of 27 rounds of `SIMECK48/96` based on the table 7 in [36].*

Proof To find a contradiction in the RX-difference of sub-keys in this table 7 of [36], we only consider the rounds 2, 3, and 6 of the trail. These rounds are shown in Figure 2 in details. The red numbers show the RX-differences.

Table 1: Some master key values to satisfy the RX-differences in 15 and 20-round of `SIMECK32/64` based on tables 4 and 6 in [36].

	$(\Delta_1 k^3, \Delta_1 k^2, \Delta_1 k^1, \Delta_1 k^0) = (0001, 0004, 0008, 0014)$	
	(k^3, k^2, k^1, k^0)	(k'^3, k'^2, k'^1, k'^0)
15-round	(0166, DB05, 5662, C5B3) (82EF, D0A1, 454C, 1625) (B1C3, BB1F, 1443, D4E2) (B26B, 9338, 1504, F7BC) (916B, D43C, 1C04, E4BC) ⋮	(02CD, B60F, ACCC, 8B73) (05DE, A147, 8A90, 2C5E) (6386, 763B, 288E, A9D1) (64D6, 2675, 2A00, EF6D) (22D6, A87D, 3800, C96D) ⋮
	$(\Delta_1 k^3, \Delta_1 k^2, \Delta_1 k^1, \Delta_1 k^0) = (0002, 0001, 0000, 0004)$	
20-round	(5D08, 1D23, FAB7, B1BC) (5D0C, 1D2B, FBA7, 918E) (7D08, 7D23, 1AB7, 31A9) (6D08, 5D23, 7AB7, A1AD) (4D08, 3D23, 9AB7, 21B8) ⋮	(BA12, 3A47, F56F, 637D) (BA1A, 3A57, F74F, 2319) (FA12, FA47, 356E, 6356) (DA12, BA47, F56E, 435F) (9A12, 7A47, 356F, 4374) ⋮

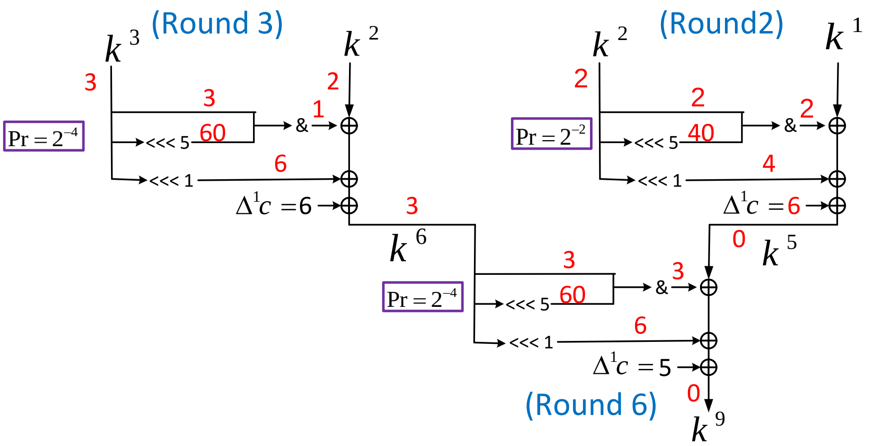


Fig. 2: Part of the 27-round RX-trail of sub-keys for `SIMECK48/96` based on table 7 in [36]

As can be seen in Figure 2, the AND operations in rounds 2, 3, and 6 satisfy the conditions of Lemma 1 in [36] and so they hold with probabilities of $2^{-2}, 2^{-4}$, and 2^{-4}, respectively. Assuming independency, the probability of the RX-difference of these three rounds should hold with a probability of 2^{-32}; however, we show that it is an incompatible trail. To this end, let $f(x) = x \& (x \lll 5)$ be the F-function of key schedule of `SIMECK`. Also, assume that $\Delta_1 \alpha$ and $\Delta_1 \beta$ respectively are RX-differences of the input and output of $f(x)$, such that the probability $\Delta_1 \alpha$ to $\Delta_1 \beta$ is non-zero. If we consider the input pairs of $f(x)$ as $(x, (x \lll 1) \oplus \Delta_1\alpha)$, then there is the following relation between $\Delta_1\alpha, \Delta_1\beta$, and x:

$$(f(x) \lll 1) \oplus f(x \lll 1 \oplus \Delta_1\alpha) = \Delta_1\beta.$$

By considering x as $x = (x_{23}, \cdots, x_1, x_0)$, the j-th bit of $\Delta_1\beta$ (i.e., $\Delta_1\beta_j$) is determined as follows.

$$(x_{j-1}\&x_{j-6}) \oplus ((x_{j-6} \oplus \Delta_1\alpha_{j-5})\&(x_{j-1} \oplus \Delta_1\alpha_{j-1})) = \Delta_1\beta_j. \tag{4}$$

Now, in the second round by considering the sub-key k^2 as the input of $f(x)$ and for $j = 6$, we have

$$\left(k_5^2\&k_0^2\right) \oplus \left((k_0^2 \oplus \Delta_1\alpha_1)\&(k_5^2 \oplus \Delta_1\alpha_5)\right) = \Delta_1\beta_6,$$

since in the second round $\Delta_1\alpha = \Delta_1\beta =$ 000002, we have

$$\left(k_5^2\&k_0^2\right) \oplus \left((k_0^2 \oplus 1)\&k_5^2\right) = 0,$$

and this gives $k_5^2 = 0$. Now, in the third round by considering the sub-key k^3 as the input of $f(x)$, for $j = 6$, and due to the $\Delta_1\alpha =$ 000003 and $\Delta_1\beta =$ 000001 we have

$$\left(k_5^3\&k_0^3\right) \oplus \left((k_0^3 \oplus 1)\&k_5^3\right) = 0,$$

so we have $k_5^3 = 0$. Also, for $j = 5$,

$$\left(k_4^3\&k_{23}^3\right) \oplus \left((k_{23}^3 \oplus 1)\&k_4^3\right) = 0,$$

so this concludes

$$k_4^3 = 0. \tag{5}$$

In the sixth round, k^6 will be the input of $f(x)$ and also $\Delta_1\alpha = \Delta_1\beta =$ 000003, therefore, by considering $j = 6$ in Equation (4), we have

$$\left(k_5^6\&k_0^6\right) \oplus \left((k_0^6 \oplus 1)\&k_5^6\right) = 0,$$

so we have $k_5^6 = 0$. On the other hand according to the third round, we have

$$k_5^6 = \left((k_0^3\&k_5^3) \oplus k_4^3 \oplus k_5^2 \oplus c_5\right).$$

For the third round the constant $c =$ `fffffd` and so $c_5 = 1$. As was shown above, we have $k_5^2 = k_5^3 = k_5^6 = 0$ so the equation above concludes $k_4^3 = 1$. Hence, by considering the Equation 5, we reach a contradiction.

4.2 Verifying the previous reported RX trails on SPECK

In [34], the authors formulated a SAT/SMT model for RX cryptanalysis in the ARX primitives and applied it to the block cipher family SPECK. They obtained longer distinguishers than the ones previously published for the block cipher family SPECK working for a certain weak key class. They presented several distinguishers for SPECK32/64, SPECK48/96, SPECK64/128, SPECK96/144, and SPECK128/256. Note that the authors only presented the details of several trails and for other trails they only reported the probabilities. Hence, in this section, we just verified the trails that are presented in detail in [34]. We modeled the SPECK key schedule with the method described in Section 3 to verify the trails in [34]. Our MILP model returned the following result.

- Our model found the weak keys for 12, 13, and 15-round RX-difference of SPECK48/96 with respective probabilities of $2^{-26.75}, 2^{-31.98}$, and $2^{-43.81}$, for a weak key class of size $2^{43.51}, 2^{24.51}$, and $2^{1.09}$, respectively (for more details of these trails refer to tables 3 and 4 in [34]). Note that based on the authors' claim, for experimental verification of trails they injected key differences artificially and only tested the probability of the RX characteristics over the cipher part. The resultant weak key for these RX trails are listed in Table 2. Note that, [34] did not report the RX-differences for the master keys $(\Delta_1 l^2, \Delta_1 l^1, \Delta_1 l^0)$. Therefore, in our MLP model we did not fix the RX-differences of these master keys and let the MILP model choose any appropriate differences.

Table 2: Some master key values to satisfy the RX-differences in 12, 13, and 15-round of SPECK48/96 based on tables 3 and 4 in [34].

$(\Delta_1 l^2, \Delta_1 l^1, \Delta_1 l^0, \Delta_1 k^0)$ (l^2, l^1, l^0, k^0) (l'^2, l'^1, l'^0, k'^0)	12-round
	(003E00, 104F00, 0E0900, 000008)
	(CC2F12, 0BBC98, EB5E6F, 375180)
	(986025, 073630, D8B5DF, 6EA308)
	13-round
	(003F00, F1C000, 060900, 000008)
	(8FCFF8, 4070DA, 7DA7EF, CA1913)
	(1FA0F1, 7121B4, FD46DE, 94322F)
	15-round
	(001F00, 744000, 021800, 000008)
	(62C8CC, 253EA3, 14D708, 8D41E7)
	(C58E98, 3E3D46, 2BB610, 1A83C7)

- Our model did not find any weak keys for the following RX trails:
  - RX trails for 11 and 12 rounds of SPECK32/64 with respective probabilities of $2^{-22.15}$ and $2^{-25.57}$, for a weak key class of size $2^{18.68}$ and $2^{4.92}$, respectively (for more details of these trails refer to table 2 in [34]).
  - RX trails for 14 rounds of SPECK48/96 with respective probabilities of $2^{-37.40}$, for a weak key class of size $2^{0.34}$ (for more details of this trail refer to table 4 in [34]).

In the following lemma, we prove the incompatibility of RX trail related to 11 rounds of SPECK32/64 in [34]. In fact, the reason for this incompatibility is that the independence assumption in the key schedule algorithm of SPECK does not hold since an output of modular addition is given as input to another modular addition. A schematic view of this fact is depicted in Figure 3.

Lemma 2 *There are no right pairs to satisfy the RX-difference of the sub-keys of 11 rounds of SPECK32/64 based on the table 2 in [34].*

Proof Based on Equationes (3), the bit values of x, y, z ($z = x + y$), with the carry c, belong to the following set.

$$(x_j, y_j, z_j, c_j, c_{j+1}) \in \left\{ \begin{matrix} (0,0,0,0,0), (0,0,1,1,0), (0,1,1,0,0), (0,1,0,1,1) \\ (1,0,1,0,0), (1,0,0,1,1), (1,1,0,0,1), (1,1,1,1,1) \end{matrix} \right\} \quad (6)$$

We denote the two n-bit vectors representing RX-differences at the input of modular addition in the round i where $i = 5, 8$, as $\Delta_1 x^i = (\Delta_1 x^i_{n-1}, \cdots, \Delta_1 x^i_1, \Delta_1 x^i_0)$ and $\Delta_1 y^i = (\Delta_1 y^i_{n-1}, \cdots, \Delta_1 y^i_1, \Delta_1 y^i_0)$ and the n-bit vectors representing RX-difference for output of modular addition as $\Delta_1 z^i = (\Delta_1 z^i_{n-1}, \cdots, \Delta z^i_1, \Delta_1 z^i_0)$ and the n-bit vectors representing RX-difference for carry as $\Delta_1 c^i = (\Delta_1 c^i_{n-1}, \cdots, \Delta_1 c^i_1, \Delta_1 c^i_0)$. It should be noted that based on the third condition of Equation (3), the RX-difference of carry bit c^i can be obtained as $\Delta_1 c^i = \Delta_1 x^i \oplus \Delta_1 y^i \oplus \Delta_1 z^i$. Therefore, the input/output RX-differences and the carry RX-difference of modular additions for the 5-th and 8-th rounds based on Figure 3 can be written as binary notation as follows.

$$\begin{aligned} \Delta_1 x^5 &= 0000000000000000, \; \Delta_1 x^8 = 0000011000000000, \\ \Delta_1 y^5 &= 0000000000000000, \; \Delta_1 y^8 = 0000001000000101, \\ \Delta_1 z^5 &= 0000000000001111, \; \Delta_1 z^8 = 0000000000011100, \\ \Delta_1 c^5 &= 0000000000001111, \; \Delta_1 c^{14} = 0000010000011001. \end{aligned}$$

By considering the modular addition operation for the 11-th round, we have $(\Delta_1 x^5_0, \Delta_1 y^5_0, \Delta_1 z^5_0, \Delta_1 c^5_0, \Delta_1 c^5_1) = (0,0,1,1,1)$. It should be noted that the pair values that can have RX-difference $(0,0,1,1,1)$ must be selected from the Set (6). Therefore, according to the Set (6), the following pairs have the differential $(0,0,1,1,1)$.

$$\left\{(x^5_0, y^5_0, z^5_0, c^5_0, c^5_1)\right\} \in \left\{ \left\{ \begin{matrix} (0,1,1,0,0) \\ (0,1,0,1,1) \end{matrix} \right\}, \left\{ \begin{matrix} (1,0,1,0,0) \\ (1,0,0,1,1) \end{matrix} \right\} \right\}.$$

So, for each pair we get the condition

$$z^5_0 = \overline{c}^5_1, \quad (7)$$

where $\overline{c}$ is the bit-wise NOT of c. Now, in a similar way and by considering the RX-difference $(\Delta_1 x^5_1, \Delta_1 y^5_1, \Delta_1 z^5_1, \Delta_1 c^5_1, \Delta_1 c^5_2) = (0,0,1,1,1)$, for each possible pair we have

$$z^5_1 = \overline{c}^5_1, \quad (8)$$

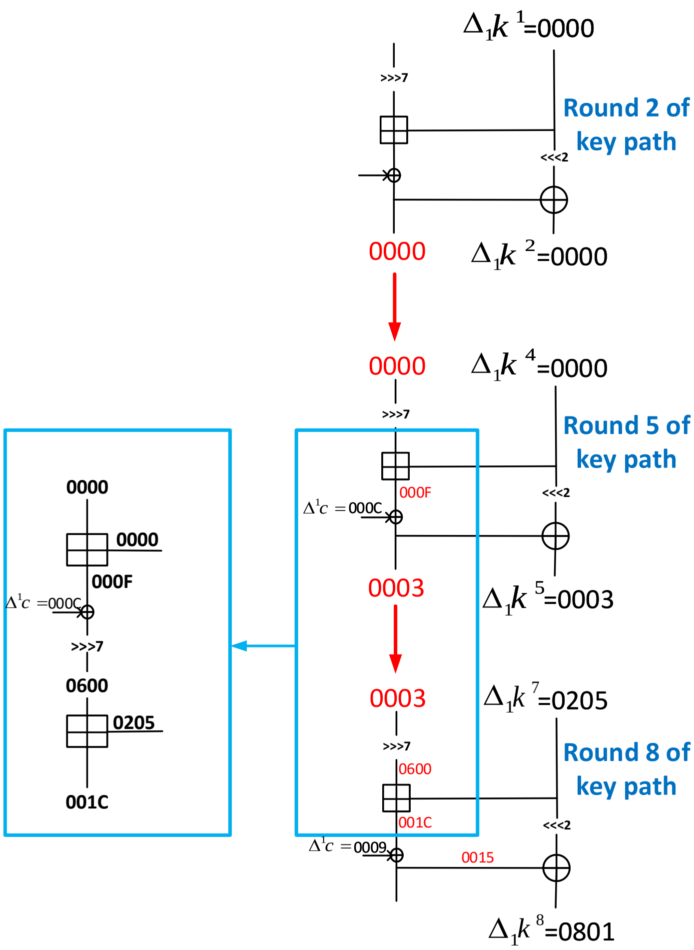


Fig. 3: Part of the 11-round RX-trail of sub-keys for SPECK32/64 based on Table 2 in [34].

By considering the Equation (7) and Equation (8), we have

$$z_0^5 = z_1^5. \tag{9}$$

Now, in the modular addition operation for the 8-th round, we have

$$(\Delta_1 x_9^8, \Delta_1 y_9^8, \Delta_1 z_9^8, \Delta_1 c_9^8, \Delta_1 c_{10}^8) = (1, 1, 0, 0, 1).$$

Thus, from Set (6) the following pairs will lead to the RX-difference $(1, 1, 0, 0, 1)$.

$$(x_9^8, y_9^8, z_9^8, c_9^8, c_{10}^8) \in \left\{ \left\{ \begin{matrix} (0,0,1,1,0) \\ (1,1,1,1,1) \end{matrix} \right\}, \left\{ \begin{matrix} (0,0,0,0,0) \\ (1,1,0,0,1) \end{matrix} \right\} \right\}.$$

Hence, for these pairs we can get the condition

$$x_9^8 = c_{10}^8. \tag{10}$$

Now, by considering the RX-difference $(\Delta_1 x_{10}^8, \Delta_1 y_{10}^8, \Delta_1 z_{10}^8, \Delta_1 c_{10}^8, \Delta_1 c_{11}^8) = (1,0,0,1,0)$ for the 10-th bit, the following pairs will lead to this differential.

$$(x_{10}^8, y_{10}^8, z_{10}^8, c_{10}^8, c_{11}^8) \in \left\{ \left\{ \begin{matrix} (0,0,1,1,0) \\ (1,0,1,0,0) \end{matrix} \right\}, \left\{ \begin{matrix} (0,1,0,1,1) \\ (1,1,0,0,1) \end{matrix} \right\} \right\}.$$

Therefore, we have the condition

$$x_{10}^8 = \overline{c}_{10}^8. \tag{11}$$

By combining the Equation (10) and Equation (11), we have

$$x_9^8 = \overline{x}_{10}^8. \tag{12}$$

Since $x^8 = (z^5 \oplus 0004) \ggg 7$ (see Figure 3), we have $z_0^5 = x_9^8$ and $z_1^5 = x_{10}^8$. Hence, by considering the Equation (9) and Equation (12), we reach a contradiction.

5 Searching compatible differential trails in block ciphers

The two following steps can help us to search the compatible differential trails in the block ciphers.

1 Build an MILP-based model for searching a (related-key) differential trail or a SMT-based model for a RX trail (targeting ARX/AND structures) to obtain a satisfactory differential trail[2].
2 Check if there exists a right pair of messages/keys based on the method mentioned in Section 3.

It is worth noting that if there exist no right pairs, the differential trail found above is an incompatible differential trail[3].

5.1 Application on SPECK family of block ciphers

In the following section, we search the compatible related-key differential trails of `SPECK` family of block ciphers.

[2] The papers [34,36,46,47] can help to model the difference behavior of the ciphers based on MILP and SMT methods. However, this step can also be performed with other automated solvers.

[3] In this case, we can check the alternative solutions in step 1. For example, by using *"PoolSearchMode"* function in the optimizer Gurobi solver [20].

5.1.1 Searching the related-key differential trails of SPECK family of block ciphers

In this section, first, thanks to the MILP method, we present several distinguishers for the reduced version of `SPECK32/64`, `SPECK48/96`, `SPECK64/128`, and `SPECK128/256`, in related-key mode. Then, we apply the method described in Section 3 to find the incompatible trails. Our result in this section should be considered as an improvement over Liu *et al.*'s work [34], but from differential view. Both works analyze SPECK-family in weak key models but Liu *et al.* presented RX trails while we intend to present differential trails. However, as can be seen in the following section, we obtain significantly better results, in terms of weak key(s), class-size, or the number of rounds of the distinguishers.

5.1.2 Attack models

Let Q_D be the encryption datapath and Q_K be the key expansion datapath of SPECK block cipher and $\Pr(Q_D)$ and $\Pr(Q_K)$ show probability over the data path and the key expansion datapath, respectively. In this paper, inspired by the rotational-XOR analysis [34], we also consider 3 models of weak key attacks. In these models, an adversary can obtain data encrypted under two different keys with a known relation, for plaintexts that are chosen by the adversary. Attack models considered in this paper are as follows where $b = 2n$, and mn denote the length of the block size and the length of the key, respectively.

1. Finding a good related-key differential trail of the cipher such that $\Pr(Q_D) \times \Pr(Q_K) > 2^{-b}$.
2. Finding a good related-key differential trail of the cipher with probability $\Pr(Q_D) > 2^{-b}$ such that $\Pr(Q_D) \times \Pr(Q_K) > 2^{-mn}$. This case of attacks is in a weak key class and the results are marked with † in the results tables.
3. Finding a good related-key differential trail of the cipher with probability $\Pr(Q_D) > 2^{-b}$ over the data part, and the key expansion part with probability $\Pr(Q_K) > 2^{-mn}$ (i.e., ensuring that at least one weak key exists). This case of attack can only be used in the open-key model, i.e., in addition to being in the weak key class and knowing the differential of the two related-keys; the adversary also knows the key values. These results are marked with ‡ in the results tables.

5.1.3 MILP-based differential trail search for SPECK family block cipher

In order to model the differential behavior of `SPECK` block cipher with the linear constraints expression in the MILP, it is sufficient to express XOR, bitwise rotation, and modular addition. Both XOR and bit rotation are linear operations and can be modeled similar to the ones in Section 3.

MILP model for modular addition

Definition 3 (The differential of addition modulo 2^n [32]) We define the differential of addition modulo 2^n as a triplet of two input and one output differences, denoted as $(\alpha, \beta \mapsto \gamma)$, where $(\alpha, \beta, \gamma) \in \{0,1\}^n$. The differential probability of addition (DP^+) is defined as follows:

$$DP^+(\alpha, \beta \mapsto \gamma) := 2^{-2n}.\#\{x, y : (x+y) \oplus ((x \oplus \alpha) + (y \oplus \beta)) = \gamma\}.$$

In order to characterize the feasible differential trails for the modular addition and their corresponding probabilities, Lipmaa and Moriai in [32] proposed two theorems as follows.

Theorem 1 *The necessary and sufficient condition for the differential $(\alpha, \beta \to \gamma)$ to have a probability > 0 is the following two conditions.*

1. $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$,
2. *if* $\alpha_{i-1} = \beta_{i-1} = \gamma_{i-1}$, *then* $\alpha_{i-1} = \beta_{i-1} = \gamma_{i-1} = \alpha_i \oplus \beta_i \oplus \gamma_i$, $i = 1, \cdots, n-1$.

Theorem 2 *When the differential $(\alpha, \beta \to \gamma)$ has a probability > 0, the probability is*

$$2^{-\sum_{i=0}^{n-2} \sim eq(\alpha_i, \beta_i, \gamma_i)}$$

where

$$eq(\alpha_i, \beta_i, \gamma_i) = eq_i = \begin{cases} 1 & \alpha_i = \beta_i = \gamma_i \\ 0 & o.w \end{cases} \tag{13}$$

Based on these theorems, Fu *et al.* proposed an MILP modeling method for modular addition operation in [17]. The first feasibility condition $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$, in Theorem 1 can be represented in MILP model as Inequalities (2). To describe the second conditions of Theorem 1 and also the definition of eq_i in the MILP model, Fu *et al.* considered the vectors $(\alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}, \alpha_i, \beta_i, \gamma_i, \sim eq_{i-1})$ (for $i = 1, \cdots, n-1$) such that it is satisfied in the conditions. For example, the differential patterns $(0,0,0,1,0,1,0)$ and $(1,0,0,0,0,1,1)$ are possible patterns and the differential pattern $(0,0,0,1,0,0,0)$ is an impossible pattern as $\alpha_{i-1} = \beta_{i-1} = \gamma_{i-1} \neq \alpha_i \oplus \beta_i \oplus \gamma_i$. Hence, 56 vectors were generated in each bit in total. Fu *et al.* used the "*inequality generator()*" function in the *sage. geometry. polyhedron* class of SAGE [44] and the greedy algorithm in [46] to get 13 linear inequalities satisfying all these 56 possible transitions. Then, given Theorem 2, it is sufficient to set the objective function as sum of $\sim eq_{i-1}$'s for $i = 1, \cdots, n-1$.

Hence, for n-bit words of the modular addition, the total number of the constraints contains $13(n-1)+4$ linear inequalities.

5.1.4 Searching for differential trails of `SPECK`

In this paper, we use the MILP model for related-key differential (RKD) cryptanalysis of reduced `SPECK` block cipher. Hence, first, we explain our strategy for searching the RKD trails and then present the searching result of `SPECK`.

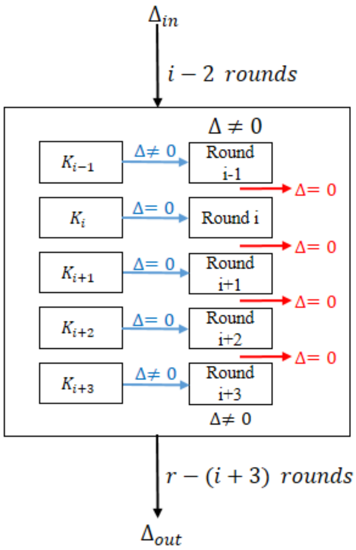


Fig. 4: Our strategy for searching the differential trails of SPECK.

Our searching strategy

We will give the details on how to search for the differential trails for SPECK. Based on the structure of the key schedule of SPECK, the maximum number of consecutive rounds of sub-keys that there are no differentials is 3 rounds. Based on the observation from our identified differential trail for the small number of rounds, we found that the differential probability is better when these 3 consecutive rounds of sub-keys lead to four consecutive rounds with zero input differential in the encryption datapath of SPECK. The details of this strategy are shown in Figure 4. In this figure, we do not have any differentials in the input of i-th round to $(i+3)$-th round, such that i can be 2 to $r-3$ for r-round of SPECK.

The only non-linear operation in the SPECK round function is the modular addition, and the only key-dependent operation is the sub-key addition. Given that the sub-key addition happens after the modular addition, i.e., the cipher operation is completely predictable until this first sub-key addition, we can ignore the modular addition in the first round of the distinguishers.

5.1.5 Search results

In this section, we apply the technique described above in order to find a good differential trail of the reduced-round variants of SPECK.

Differential Trails of SPECK32/64

Table 3 shows the RKD trail covering up to 15 rounds found by our model. To the best of our knowledge, the best published distinguisher trail so far has covered 12 rounds of SPECK32/64 with a probability of $2^{-25.57}$ for a weak key class of size $2^{4.92}$ [34]. Based on Table 3, our 13-round trail has a much better probability of $2^{-23.85}$ for a weak key class of size 2^{41}. Tables 9 to 14 in the Appendix A.1, show the differential trails covering 10 to 15 rounds found by our program.

Table 3: The comparison of our related-key differentials (RKD) with rotational-XOR (RX) result of [34] for SPECK32/64. Entries marked with † can be used in weak key model and entries marked with ‡ can only be used in the open-key model (see Section 5.1.2 for more details of these marks).

Ver.	Rounds	Data Prob. trail	Data Prob. differential (♯ trails)	Data Key Prob. (Key class size)	Method	Ref.
32/64	10 †	$2^{-19.15}$	-	$2^{-35.9}$ ($2^{28.10}$)	RX	[34]
	11 ‡	$2^{-22.15}$	-	$2^{-45.32}$ ($2^{18.68}$)		
	12 ‡	$2^{-25.57}$	-	$2^{-59.08}$ ($2^{4.92}$)		
	10	2^{-13}	$2^{-12.95}$(3)	2^{-7} (2^{57})	RKD	Our
	11	2^{-17}	$2^{-16.85}$(15)	2^{-14} (2^{50})		
	12 †	2^{-24}	$2^{-23.79}$(90)	2^{-13} (2^{51})		
	13 †	2^{-24}	$2^{-23.85}$(27)	2^{-23} (2^{41})		
	14†	2^{-30}	$2^{-29.17}$($\geq$ 180)*	2^{-29} (2^{35})		
	15‡	2^{-32}	$2^{-31.73}$($\geq$ 100)	2^{-62} (2^{2})		

∗: The ($\geq a$) means we can have more than a trails for this differential but at least a trails are enough to have the mentioned differential. For example, for 14 rounds, the program finds 2181 trails, while only 180 trails affect the increase of the probability of differential and other trails do not have more effect on the probability of differential.

Note that the authors of [34] wrote that *" We extended our search to 13-round trails and found that none exists, suggesting that a 12-round RX-trail is the longest possible one."* So, our result shows that the related-key differential is more powerful against SPECK32/64, compared to the rotational-XOR.

Differential Trails of SPECK48/96

We found RKD trails covering up to 16 rounds for SPECK48/96. Table 4 shows the summary of searching result and also a comparison of our results with [34] for SPECK48/96. The trails for 11 to 16 rounds are shown in Tables 15 to 20 in the Appendix A.2.

Differential Trails of SPECK64/128

For SPECK64/128, we successfully extended a distinguisher up to 17 rounds with a probability of $2^{-60.81}$ for a weak key class of size 2^{78}. Our results for

Table 4: The comparison of our related-key differentials (RKD) with rotational-XOR (RX) result of [34] for SPECK48/96. Entries marked with † can be used in weak key model and entries marked with ‡ can only be used in the open-key model (see Section 5.1.2 for more details of these marks).

Ver.	Rounds	Data Prob.		Data Key Prob. (Key class size)	Method	Ref.
		trail	differential (♯ trails)			
48/96	11 †	$2^{-24.15}$	-	$2^{-70.32}$ ($2^{25.68}$)	RX	[34]
	11 ‡	$2^{-23.15}$	-	$2^{-81.07}$ ($2^{14.93}$)		
	12 †	$2^{-26.57}$	-	$2^{-68.5}$ ($2^{27.5}$)		
	12 †	$2^{-26.57}$	-	$2^{-52.49}$ ($2^{43.51}$)		
	13 ‡	$2^{-31.98}$	-	$2^{-71.49}$ ($2^{24.51}$)		
	14 ‡	$2^{-37.40}$	-	$2^{-95.66}$ ($2^{0.34}$)		
	15 ‡	$2^{-43.81}$	-	$2^{-94.91}$ ($2^{1.09}$)		
	11	2^{-17}	$2^{-16.95}$(3)	2^{-13} (2^{83})	RKD	Our
	12	2^{-21}	$2^{-20.90}$(20)	2^{-23} (2^{73})		
	13 †	2^{-33}	$2^{-32.69}$(≥ 50)	2^{-18} (2^{78})		
	14 †	2^{-43}	$2^{-42.38}$(≥ 200)	2^{-25} (2^{71})		
	15†	2^{-46}	$2^{-45.63}$(≥ 100)	2^{-43} (2^{53})		
	16‡	2^{-47}	$2^{-46.61}$(≥ 100)	2^{-94} (2^{2})		

13 to 17 rounds of SPECK64/128 are shown in Table 5. Tables 21 to 25 in the Appendix A.3, show the RKD trail for these 13 to 17 rounds of SPECK64/128.

Table 5: The comparison of our related-key differentials (RKD) with rotational-XOR (RX) result of [34] for SPECK64/128. Entries marked with † can be used in weak key model and entries marked with ‡ can only be used in the open-key model (see Section 5.1.2 for more details of these marks).

Ver.	Rounds	Data Prob.		Data Key Prob. (Key class size)	Method	Ref.
		trail	differential (♯ trails)			
64/128	13 ‡	$2^{-37.98}$	-	$2^{-106.08}$($2^{21.92}$)	RX	[34]
	13	2^{-36}	$2^{-35.67}$(≥ 150))	2^{-18} (2^{110})	RKD	Our
	14 †	2^{-37}	$2^{-36.81}$(≥ 50))	2^{-51} (2^{77})		
	15 †	2^{-45}	$2^{-44.81}$(≥ 30)	2^{-60} (2^{68})		
	16 †	2^{-60}	$2^{-58.81}$(≥ 200)	2^{-43} (2^{85})		
	17 †	2^{-62}	$2^{-60.81}$(≥ 200)	2^{-50} (2^{78})		

Differential Trails of SPECK128/256

We present the distinguishers for 16 and 19 rounds of SPECK128/256 as shown in Table 6. Also, Tables 26 and 27 in the Appendix A.4, show the RKD trail for these 16 and 19 rounds of SPECK128/256.

Table 6: The comparison of our related-key differentials (RKD) with rotational-XOR (RX) result of [34] for SPECK128/256. Entries marked with † can be used in weak key model and entries marked with ‡ can only be used in the open-key model (see Section 5.1.2 for more details of these marks).

Ver.	Rounds	Data Prob.		Data Key Prob. (Key class size)	Method	Ref.
		trail	differential (♯ trails)			
128/256	13	$2^{-31.98}$	-	$2^{-73.49}(2^{182.51})$	RX	[34]
	16 19†	2^{-76} 2^{-111}	$2^{-75.19}(\geq 100)$ $2^{-109.75}(\geq 250)$	2^{-45} (2^{211}) $2^{-79}(2^{177})$	RKD	Our

5.1.6 Experimental verification

Here we intend to measure the accuracy of our estimates for the probabilities, and therefore, we first try to identify a weak key and then encrypt 2^{32} (for case of SPECK32/64) plaintexts, and measure the probability such that the differential feature is met.

We modeled the SPECK key schedule with the method described in Section 3 and fixed the key input differentials based on Tables 9 to 14 for rounds 10 to 15 of SPECK32/64, respectively. The time of solving the model to find the first weak key is shown in the third column of Table 7. Also in this table, the number of pairs that is satisfied in the encryption datapath are listed in the fifth column. This table shows that the results matched the theoretical predictions. For all versions of SPECK mentioned above, we tested whether the key differential trail is followed. For each version, we reported a weak key (see Tables 9 to 27 in Appendix A)

5.1.7 Incompatible trails

It must be noted that the method mentioned in Section 3 can be very useful in most cases to find a weak key. For example, our MILP model to find the related-key trails can find a 14-round related-key trail with the input differential (1805, 1281), the output differential (DA52, 25AD), and the key input differential (0201, 4080, 1891, 4A25) with the data probability of 2^{-26} and key probability of 2^{-63} (key class size of 2^{1}). In this case, our model, after 150 seconds shows that there are no keys which can satisfy the differentials of round keys. Note that without using our MILP method, we had to run the SPECK key schedule algorithm for 2^{64} times to know it. As a few other examples, in Table 8, we listed some of the differential trails for which there are not any key values to reach the differentials of round-keys. In fact, the independency assumption between the two continuous modular addition of the key schedule algorithm of SPECK is not enough to ensure the validity of the some of the differential trails. As an example, in the following lemma, we show that the modular additions used in the key schedule algorithm of SPECK are not independent. To show this, we consider one of the differential trails shown in

Table 7: The number of pairs for rounds 10 to 15 of SPECK32/64 with a weak key. In this table, we show the values of two input keys as: $K = (l_2, l_1, l_0, k_0)$, $K' = (l'_2, l'_1, l'_0, k'_0)$ and the differential of them as $\Delta K = (\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0)$.

Rounds	Tested weak key	Time	♯ right pairs expected	♯ right pairs obtained
10	$K = (\texttt{10CD}, \texttt{31BF}, \texttt{A172}, \texttt{E11F})$ $K' = (\texttt{38CD}, \texttt{33BF}, \texttt{A1F2}, \texttt{E11E})$ $\Delta K = (\texttt{2800}, \texttt{0200}, \texttt{0080}, \texttt{0001})$	≤ 1 Sec.	$2^{19.05}$	$524729 \backsimeq 2^{19}$
11	$K = (\texttt{8D43}, \texttt{1D53}, \texttt{ED28}, \texttt{C242})$ $K' = (\texttt{8F43}, \texttt{1DD3}, \texttt{ED59}, \texttt{8842})$ $\Delta K = (\texttt{0200}, \texttt{0080}, \texttt{0071}, \texttt{4A00})$	≤ 1 Sec.	$2^{15.15}$	$32922 \backsimeq 2^{15}$
12	$K = (\texttt{89C6}, \texttt{B836}, \texttt{00B4}, \texttt{B223})$ $K' = (\texttt{8946}, \texttt{B867}, \texttt{00BC}, \texttt{A023})$ $\Delta K = (\texttt{0080}, \texttt{0051}, \texttt{0008}, \texttt{1200})$	≤ 1 Sec.	$2^{8.21}$	$287 \backsimeq 2^{8.16}$
13	$K = (\texttt{0502}, \texttt{DB48}, \texttt{E36E}, \texttt{75EC})$ $K' = (\texttt{4502}, \texttt{C3C8}, \texttt{E76E}, \texttt{75E5})$ $\Delta K = (\texttt{4000}, \texttt{1880}, \texttt{0400}, \texttt{0009})$	141 Sec.	$2^{8.15}$	$246 \backsimeq 2^{7.95}$
14	$K = (\texttt{96D6}, \texttt{C06E}, \texttt{877E}, \texttt{8860})$ $K' = (\texttt{8256}, \texttt{C4AE}, \texttt{8656}, \texttt{9862})$ $\Delta K = (\texttt{8256}, \texttt{C4AE}, \texttt{8656}, \texttt{9862})$	75 Sec.	$2^{2.83}$	$8 = 2^3$
15	$K = (\texttt{7A1F}, \texttt{D850}, \texttt{C89F}, \texttt{B35A})$ $K' = (\texttt{3A1F}, \texttt{CDD0}, \texttt{CC9F}, \texttt{B353})$ $\Delta K = (\texttt{4000}, \texttt{1580}, \texttt{0400}, \texttt{0009})$	2420 Sec.	$2^{0.27}$	$3 \backsimeq 2^{1.58}$

Table 8: The list of some of the related-key differential trails of SPECK for which there are not any key values to satisfy the differential of key rounds.

Ver.	# rounds	$\Pr(Q_K)$	$\Pr(Q_D)$	Ref.
32/64	14	2^{-36}	2^{-27}	Table 28
48/96	16	2^{-69}	2^{-47}	Table 29
64/128	16	2^{-41}	2^{-57}	Table 30
128/256	21	2^{-94}	2^{-122}	Table 31

Table 8 shows that the cause of the invalidity of that trail is the dependence of the modular additions.

Lemma 3 *There are no right pair to satisfy the RK-difference of the sub-keys of 16 rounds of SPECK48/96 as shown in Table 29.*

Proof The proof is almost the same with proof of Lemma 2 and its detrails are presented in Appendix C.

6 Conclusion and future works

Thanks to the MILP method, in this study, we presented an efficient method to verify differential trails and also search for the right pairs. We applied our approach to the the previously known RX trails of SIMECK and SPECK family of block ciphers to verify their corectness. In addition, we presented related-key differential distinguishers on different variants of the SPECK block cipher and obtained longer distinguishers compared to the ones previously published. For each variant of the SPECK family of block ciphers, we presented several distinguishers. The longest distinguishers for SPECK32/64, SPECK48/96, SPECK64/128, and SPECK128/256, cover 15, 16, 17, and 19 rounds, respectively, which are working on a certain weak key class. In addition, we showed that the transitional probability over two consecutive modular addition operations in the key schedule structure of SPECK is not independent and our approach in this paper could find this case of the trails.

To the best of our knowledge, the current method for searching RX trails is based on SAT/SMT solvers and thus proposing an MILP-based method to find the RX trails can be considered as a future work. Also, based on our result, some previously reported RX trails of SPECK and SIMECK were incompatible, for instance, 11 and 12 rounds of SPECK32/64, 27 and 35 rounds of SIMECK48/96 and SIMECK64/128, respectively, therefore, finding compatible RX trails or prove nonexistence of them can be considered as another future work. In addition, in our analysis to find a good differential distinguisher for SPECK family, we noticed that most of the obtained trails are incompatible (especially in case of SPECK128/256). Thus, considering a direct approach to find a compatible differential trail may help improve the results (e.g., inspired by [15, 33]). As another work, considering our search to find a weak key in this paper may help find a collision in hash functions at a reasonable time. Besides, the results of this paper could be used to verify many differential trails which have been already considered as theoretical trails and we were not sure whether there could be any pair of inputs following that trail (as we did this for recent results on SPECK and SIMECK, in this article).

References

1. A. Abdelkhalek, Y. Sasaki, Y. Todo, M. Tolba, and A. M. Youssef. Milp modeling for (large) s-boxes to optimize probability of differential characteristics. *IACR Transactions on Symmetric Cryptology*, 2017(4):99–129, 2017.
2. F. Abed, E. List, S. Lucks, and J. Wenzel. Differential cryptanalysis of round-reduced Simon and Speck. In *International Workshop on Fast Software Encryption*, pages 525–545. Springer, 2014.
3. T. Ashur and Y. Liu. Rotational cryptanalysis in the presence of constants. *IACR Transactions on Symmetric Cryptology*, pages 57–70, 2016.
4. J.-P. Aumasson, L. Henzen, W. Meier, and R. C.-W. Phan. Sha-3 proposal blake. *Submission to NIST*, 92, 2008.
5. R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers. The SIMON and SPECK lightweight block ciphers. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2015.
6. D. J. Bernstein. The Salsa20 family of stream ciphers. In *New stream cipher designs*, pages 84–97. Springer, 2008.
7. D. J. Bernstein, S. Kölbl, S. Lucks, P. M. C. Massolino, F. Mendel, K. Nawaz, T. Schneider, P. Schwabe, F.-X. Standaert, Y. Todo, et al. Gimli: a cross-platform permutation. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 299–320. Springer, 2017.
8. E. Biham and A. Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.

9. A. Biryukov, M. Lamberger, F. Mendel, and I. Nikolić. Second-order differential collisions for reduced sha-256. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 270–287. Springer, 2011.
10. A. Biryukov, A. Roy, and V. Velichkov. Differential analysis of block ciphers SIMON and SPECK. In *International Workshop on Fast Software Encryption*, pages 546–570. Springer, 2014.
11. A. Biryukov and V. Velichkov. Automatic search for differential trails in ARX ciphers. In *Cryptographers' Track at the RSA Conference*, pages 227–250. Springer, 2014.
12. N. T. Courtois and G. V. Bard. Algebraic cryptanalysis of the data encryption standard. In *IMA International Conference on Cryptography and Coding*, pages 152–169. Springer, 2007.
13. T. Cui, K. Jia, K. Fu, S. Chen, and M. Wang. New Automatic Search Tool for Impossible Differentials and Zero-Correlation Linear Approximations. *IACR Cryptology ePrint Archive*, 2016:689, 2016.
14. I. Dinur. Improved differential cryptanalysis of round-reduced speck. In *International Workshop on Selected Areas in Cryptography*, pages 147–164. Springer, 2014.
15. M. ElSheikh, A. Abdelkhalek, and A. M. Youssef. On MILP-Based Automatic Search for Differential Trails Through Modular Additions with Application to Bel-T. In *Progress in Cryptology-AFRICACRYPT 2019 - 11th International Conference on Cryptology in Africa, Rabat, Morocco, July 9-11, 2019, Proceedings*, pages 273–296, 2019.
16. N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, and J. Walker. The Skein hash function family. *Submission to NIST (round 3)*, 7(7.5):3, 2010.
17. K. Fu, M. Wang, Y. Guo, S. Sun, and L. Hu. MILP-based automatic search algorithms for differential and linear trails for speck. In *International Conference on Fast Software Encryption*, pages 268–288. Springer, 2016.
18. D. Gérault, P. Lafourcade, M. Minier, and C. Solnon. Computing aes related-key differential characteristics with constraint programming. *Artificial Intelligence*, page 103183, 2019.
19. D. Gerault, M. Minier, and C. Solnon. Constraint programming models for chosen key differential cryptanalysis. In *International Conference on Principles and Practice of Constraint Programming*, pages 584–601. Springer, 2016.
20. L. Gurobi Optimization. Gurobi optimizer reference manual, 2019.
21. H. Hadipour, S. Sadeghi, M. M. Niknam, L. Song, and N. Bagheri. Comprehensive security analysis of craft. *IACR Transactions on Symmetric Cryptology*, pages 290–317, 2019.
22. D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K. H. Ryu, and D.-G. Lee. LEA: A 128-bit block cipher for fast encryption on common processors. In *International Workshop on Information Security Applications*, pages 3–27. Springer, 2013.
23. D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, et al. HIGHT: A new block cipher suitable for low-resource device. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 46–59. Springer, 2006.
24. M. Huang and L. Wang. Automatic tool for searching for differential characteristics in arx ciphers and applications. In *International Conference on Cryptology in India*, pages 115–138. Springer, 2019.
25. D. Khovratovich and I. Nikolić. Rotational cryptanalysis of ARX. In *International Workshop on Fast Software Encryption*, pages 333–346. Springer, 2010.
26. D. Khovratovich, I. Nikolić, J. Pieprzyk, P. Sokołowski, and R. Steinfeld. Rotational cryptanalysis of ARX revisited. In *International Workshop on Fast Software Encryption*, pages 519–536. Springer, 2015.
27. D. Khovratovich, I. Nikolić, J. Pieprzyk, P. Sokołowski, and R. Steinfeld. Rotational cryptanalysis of ARX revisited. In *International Workshop on Fast Software Encryption*, pages 519–536. Springer, 2015.
28. L. R. Knudsen, V. Rijmen, R. L. Rivest, and M. J. Robshaw. On the design and security of RC2. In *International Workshop on Fast Software Encryption*, pages 206–221. Springer, 1998.
29. S. Kölbl. Cryptosmt: An easy to use tool for cryptanalysis of symmetric primitives (2015).

30. G. Leurent. Analysis of differential attacks in arx constructions. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 226–243. Springer, 2012.
31. G. Leurent and A. Roy. Boomerang attacks on hash function using auxiliary differentials. In *Cryptographers' Track at the RSA Conference*, pages 215–230. Springer, 2012.
32. H. Lipmaa and S. Moriai. Efficient algorithms for computing differential properties of addition. In *International Workshop on Fast Software Encryption*, pages 336–350. Springer, 2001.
33. F. Liu, T. Isobe, and W. Meier. Automatic verification of differential characteristics: Application to reduced gimli. IACR-CRYPTO-2020, 2020. `https://eprint.iacr.org/2020/591`.
34. Y. Liu, G. De Witte, A. Ranea, and T. Ashur. Rotational-XOR cryptanalysis of reduced-round SPECK. *IACR Transactions on Symmetric Cryptology*, pages 24–36, 2017.
35. Y. Liu, Q. Wang, and V. Rijmen. Automatic search of linear trails in arx with applications to speck and chaskey. In *International Conference on Applied Cryptography and Network Security*, pages 485–499. Springer, 2016.
36. J. Lu, Y. Liu, T. Ashur, B. Sun, and C. Li. Rotational-xor cryptanalysis of simon-like block ciphers. *Information Security and Privacy-2020th Australasian Conference, ACIS*, 2020.
37. F. Mendel, T. Nad, and M. Schläffer. Finding sha-2 characteristics: searching through a minefield of contradictions. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 288–307. Springer, 2011.
38. N. Mouha, Q. Wang, D. Gu, and B. Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *International Conference on Information Security and Cryptology*, pages 57–76. Springer, 2011.
39. S. Sadeghi and N. Bagheri. Security analysis of SIMECK block cipher against related-key impossible differential. *Information Processing Letters*, 147:14–21, 2019.
40. S. Sadeghi, T. Mohammadi, and N. Bagheri. Cryptanalysis of Reduced round SKINNY Block Cipher. *IACR Trans. Symmetric Cryptol.*, 2018(3):124–162, 2018.
41. Y. Sasaki. Boomerang distinguishers on md4-family: First practical results on full 5-pass haval. In *International Workshop on Selected Areas in Cryptography*, pages 1–18. Springer, 2011.
42. Y. Sasaki and Y. Todo. New impossible differential search tool from design and cryptanalysis aspects. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 185–215. Springer, 2017.
43. L. Song, Z. Huang, and Q. Yang. Automatic differential analysis of ARX block ciphers with application to SPECK and LEA. In *Australasian Conference on Information Security and Privacy*, pages 379–394. Springer, 2016.
44. W. Stein et al. Sage: Open source mathematical software. *7 December 2009*, 2008.
45. S. Sun, D. Gerault, P. Lafourcade, Q. Yang, Y. Todo, K. Qiao, and L. Hu. Analysis of aes, skinny, and others with constraint programming. *IACR transactions on symmetric cryptology*, pages 281–306, 2017.
46. 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. *Cryptology ePrint Archive, Report*, 747:2014, 2014.
47. 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 *International Conference on the Theory and Application of Cryptology and Information Security*, pages 158–178. Springer, 2014.
48. G. Wang, N. Keller, and O. Dunkelman. The delicate issues of addition with respect to xor differences. In *International Workshop on Selected Areas in Cryptography*, pages 212–231. Springer, 2007.
49. S. Wu and M. Wang. Security evaluation against differential cryptanalysis for block cipher structures. *IACR Cryptology ePrint Archive*, 2011:551, 2011.
50. W. Xin, Y. Liu, B. Sun, and C. Li. Improved cryptanalysis on siphash. In *International Conference on Cryptology and Network Security*, pages 61–79. Springer, 2019.

51. G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong. The simeck family of lightweight block ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 307–329. Springer, 2015.
52. Y. Yao, B. Zhang, and W. Wu. Automatic search for linear trails of the SPECK family. In *International Conference on Information Security*, pages 158–176. Springer, 2015.
53. C. Zhou, W. Zhang, T. Ding, and Z. Xiang. Improving the milp-based security evaluation algorithm against differential/linear cryptanalysis using a divide-and-conquer approach. *IACR Transactions on Symmetric Cryptology*, pages 438–469, 2019.

A RKD trails of SPECK variants

A.1 RKD trails of SPECK32/64

Tables 9 to 14.

Table 9: 10-round related-key differential trail in SPECK32/64 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (2800, 0200, 0080, 0001)$.

Round	Differential in Key	$\log_2 \Pr$	Differential in Data	$\log_2 \Pr$
0	0001		0204||0005	
1	0004	-1	0205||0200	
2	0010	-1	0800||0000	-3
3	0000	-2	0000||0000	-1
4	0000	0	0000||0000	0
5	0000	0	0000||0000	0
6	8000	0	0000||0000	0
7	8002	0	8000||8000	0
8	8008	-1	0102||0100	-1
9	812A	-2	850A||810A	-3
10			152A||1100	-5
	$\log_2(\Pr(Q_K))$:	-7	$\log_2(\Pr(Q_D))$:	-13

A pair of weak keys:
$K = (10CD, 31BF, A172, E11F)$
$K' = (38CD, 33BF, A1F2, E11E)$

A.2 RKD trails of SPECK48/96

Tables 15 to 20.

A.3 RKD trails of SPECK64/128

Tables 21 to 25.

A.4 RKD trails of SPECK128/256

Tables 26 to 27.

Table 10: 11-round related-key differential trail in SPECK32/64 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{0200}, \texttt{0080}, \texttt{0071}, \texttt{4A00})$.

Round	Differential in Key	$\log_2 \Pr$	Differential in Data	$\log_2 \Pr$
0	4A00		4B21||C121	
1	0008	-4	0121||C000	
2	0004	-1	0203||0200	-3
3	0010	-1	0800||0000	-4
4	0000	-2	0000||0000	-1
5	0000	0	0000||0000	0
6	0000	0	0000||0000	0
7	8000	0	0000||0000	0
8	8002	0	8000||8000	0
9	8008	-1	0102||0100	-1
10	812A	-2	850A||810A	-3
11			152A||1100	-5
	$\log_2(\Pr(Q_K))$:	-11	$\log_2(\Pr(Q_D))$:	-17

A pair of weak keys:
$K = (\texttt{8D43}, \texttt{1D53}, \texttt{ED28}, \texttt{C242})$
$K' = (\texttt{8F43}, \texttt{1DD3}, \texttt{ED59}, \texttt{8842})$

Table 11: 12-round related-key differential trail in SPECK32/64 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{0080}, \texttt{0051}, \texttt{0008}, \texttt{1200})$.

Round	Differential in Key	$\log_2 \Pr$	Differential in Data	$\log_2 \Pr$
0	1200		16E4||144C	
1	4A00	-2	04E4||10A8	
2	0008	-4	02A1||4001	-7
3	0004	-1	0205||0200	-4
4	0010	-1	0800||0000	-3
5	0000	-2	0000||0000	-1
6	0000	0	0000||0000	0
7	0000	0	0000||0000	0
8	8000	0	0000||0000	0
9	8002	0	8000||8000	0
10	8008	-1	0102||0100	-1
11	812A	-2	850A||810A	-3
12			152A||1100	-5
	$\log_2(\Pr(Q_K))$:	-13	$\log_2(\Pr(Q_D))$:	-24

A pair of weak keys:
$K = (\texttt{89C6}, \texttt{B836}, \texttt{00B4}, \texttt{B223})$
$K' = (\texttt{8946}, \texttt{B867}, \texttt{00BC}, \texttt{A023})$

B Some of incompability RKD trails of SPECK variants

Tables 28 to 31.

C Manual verification of one of the incompatible RKD trails

Lemma 4 *There are no right pair to satisfy the RK-difference of the sub-keys of 16 rounds of SPECK48/96 as shown in Table 29.*

Table 12: 13-round related-key differential trail in SPECK32/64 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (4000, 1880, 0400, 0009)$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	0009		560B||020A	
1	0025	-2	5602||5408	
2	0080	-4	5081||00A0	-7
3	0200	-1	0281||0001	-4
4	0800	-1	0004||0000	-3
5	0000	-2	0000||0000	-1
6	0000	0	0000||0000	0
7	0000	0	0000||0000	0
8	0040	-1	0000||0000	0
9	01C0	-2	0040||0040	0
10	0140	-5	8100||8000	-2
11	8440	-2	8042||8040	-2
12	1543	-3	8100||8002	-3
13			9443||9449	-2
	$\log_2(\Pr(Q_K))$:	-23	$\log_2(\Pr(Q_D))$:	-24

A pair of weak keys:
$K = (0502, DB48, E36E, 75EC)$
$K' = (4502, C3C8, E76E, 75E5)$

Table 13: 14-round related-key differential trail in SPECK32/64 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (1480, 04C0, 0128, 1002)$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	1002		1418||A418	
1	8008	-3	041A||A002	
2	0023	-2	5402||D408	-6
3	0080	-5	5083||00A0	-6
4	0200	-2	0281||0001	-5
5	0800	-1	0004||0000	-3
6	0000	-3	0000||0000	-1
7	0000	0	0000||0000	0
8	0000	0	0000||0000	0
9	0040	-1	0000||0000	0
10	01C0	-2	0040||0040	0
11	0140	-5	8100||8000	-2
12	8440	-2	8042||8040	-2
13	1543	-3	8100||8002	-3
14			9443||9449	-2
	$\log_2(\Pr(Q_K))$:	-29	$\log_2(\Pr(Q_D))$:	-30

A pair of weak keys:
$K = (96D6, C06E, 877E, 8860)$
$K' = (8256, C4AE, 8656, 9862)$

Proof To find a contradiction in the key expansion datapath of the key differences of the trails in Table 29, we fixed the input differential of sub-keys in all 16 rounds. Our MILP model gives us an infeasible solution. This means that there are not any key values to satisfy the differential of round keys for 16 rounds of SPECK48/96 based on Table 29. After that, we tried to find the key values for fewer rounds by removing some last rounds. When we removed the fourteenth round, the MILP model found two key values whose differential was

Table 14: 15-round related-key differential trail in SPECK32/64 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{4000}, \texttt{1580}, \texttt{0400}, \texttt{0009})$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	0009			
1	0023	-4	543E‖D408	
2	0080	-5	5083‖00A0	-6
3	0200	-1	0281‖0001	-5
4	0800	-3	0004‖0000	-3
5	0000	-3	0000‖0000	-1
6	0000	0	0000‖0000	0
7	0000	0	0000‖0000	0
8	0040	-1	0000‖0000	0
9	01C0	-2	0040‖0040	0
10	0140	-5	8100‖8000	-2
11	8440	-2	8042‖8040	-2
12	6AFD	-15	8100‖8002	-3
13	C01E	-12	EBFD‖EBF7	-2
14	4753	-9	2FC0‖801F	-5
15			476D‖4713	-3
	$\log_2\big(\Pr(Q_K)\big)$:	-62	$\log_2\big(\Pr(Q_D)\big)$:	-32

A pair of weak keys:
$K = (\texttt{7A1F}, \texttt{D850}, \texttt{C89F}, \texttt{B35A})$
$K' = (\texttt{3A1F}, \texttt{CDD0}, \texttt{CC9F}, \texttt{B353})$

Table 15: 11-round related-key differential trail in SPECK48/96 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{020000}, \texttt{004000}, \texttt{000882}, \texttt{120008})$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	120008		12504A‖405040	
1	000040	-3	005042‖400002	
2	000200	-1	020012‖020000	-5
3	001000	-1	100000‖000000	-3
4	000000	-2	000000‖000000	-1
5	000000	0	000000‖000000	0
6	000000	0	000000‖000000	0
7	000080	-1	000000‖000000	0
8	000480	-1	000080‖000080	0
9	002080	-2	800400‖800000	-1
10	812480	-2	80A084‖80A080	-2
11			VV8504A0‖8000A4	-5
	$\log_2\big(\Pr(Q_K)\big)$:	-13	$\log_2\big(\Pr(Q_D)\big)$:	-17

A pair of weak keys:
$K = (\texttt{426E81}, \texttt{01E2A0}, \texttt{23AD82}, \texttt{401C62})$
$K' = (\texttt{406E81}, \texttt{01A2A0}, \texttt{23A500}, \texttt{521C6A})$

the differential of the key rounds for 14 rounds of SPECK48/96. So, the fourteenth round of key expansion datapath can be effective in finding a contradiction. Note that the left input differential of round 14 is the same as the left output differential of round 11 (see Figure 5).

We denote the two n-bit vectors representing differentials at the input of modular addition in the round i where $i = 11, 14$, as $\Delta x^i = (\Delta x^i_{n-1}, \cdots, \Delta x^i_1, \Delta x^i_0)$ and $\Delta y^i = (\Delta y^i_{n-1}, \cdots, \Delta y^i_1, \Delta y^i_0)$ and the n-bit output differential as $\Delta z^i = (\Delta z^i_{n-1}, \cdots, \Delta z^i_1, \Delta z^i_0)$

Table 16: 12-round related-key differential trail in SPECK48/96 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (020000, 004000, 000882, 120008)$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	120008		12504A||405040	
1	000040	-3	005042||400002	
2	000200	-1	020012||020000	-5
3	001000	-1	100000||000000	-3
4	000000	-2	000000||000000	-1
5	000000	0	000000||000000	0
6	000000	0	000000||000000	0
7	000080	-1	000000||000000	0
8	000780	-3	000080||000080	0
9	000080	-7	800400||800000	-3
10	800480	-1	808084||808080	-2
11	002085	-4	840480||800084	-3
12			00A405||00A021	-4
	$\log_2\big(\Pr(Q_K)\big)$:	-23	$\log_2\big(\Pr(Q_D)\big)$:	-21

A pair of weak keys:
$K = (3BC6A8, 4B6ED8, EBC297, C8A20E)$
$K' = (39C6A8, 4B2ED8, EBCA15, DAA206)$

Table 17: 13-round related-key differential trail in SPECK48/96 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (000200, 0000C0, 820008, 081200)$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	081200		4A12D0||4040D0	
1	400000	-4	4200D0||024000	
2	000002	-1	120200||000200	-5
3	000010	-1	001000||000000	-3
4	000000	-2	000000||000000	-1
5	000000	0	000000||000000	0
6	000000	0	000000||000000	0
7	800000	0	000000||000000	0
8	800004	0	800000||008000	0
9	800020	-1	008004||008000	-1
10	808124	-2	8480A0||8080A0	-3
11	840800	-4	A08504||A48000	-5
12	A0C804	-3	242885||002880	-7
13			25CCAC||2488AC	-8
	$\log_2\big(\Pr(Q_K)\big)$:	-18	$\log_2\big(\Pr(Q_D)\big)$:	-33

A pair of weak keys:
$K = (34AF36, 1AA373, C48D92, 2B0794)$
$K' = (34AD36, 1AA3B3, 468D9A, 231594)$

and the n-bit vectors representing carry differential as $\Delta c^i = (\Delta c^i_{n-1}, \cdots, \Delta c^i_1, \Delta c^i_0)$. It should be noted that based on the third condition of Inequality (3), the differential of carry bit c^i can be obtained as $\Delta c^i = \Delta x^i \oplus \Delta y^i \oplus \Delta z^i$. Therefore, the input/output differentials and the carry differentials of modular additions for the 11-th and 14-th rounds based on

Table 18: 14-round related-key differential trail in SPECK48/96 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (020000, 004010, 248801, 102088)$.

Round	Differential in Key	$\log_2 \Pr$	Differential in Data	$\log_2 \Pr$
0	102088		10625A||5042C2	
1	900040	-6	0042D2||500010	
2	000204	-2	120012||920090	-6
3	001024	-2	841449||141010	-8
4	008000	-4	A08400||000480	-9
5	040000	-1	002404||000004	-5
6	200000	-1	000020||000000	-3
7	000000	-2	000000||000000	-1
8	000000	0	000000||000000	0
9	000000	0	000000||000000	0
10	010000	-1	000000||000000	0
11	090000	-1	010000||010000	0
12	410000	-2	080100||000100	-2
13	490102	-3	410901||410101	-3
14			09410A||014900	-6
	$\log_2(\Pr(Q_K))$:	-25	$\log_2(\Pr(Q_D))$:	-43

A pair of weak keys:
$K = (\mathtt{A45E80}, \mathtt{E09F24}, \mathtt{F047C1}, \mathtt{4608BA})$
$K' = (\mathtt{A65E80}, \mathtt{E0DF34}, \mathtt{D4CFC0}, \mathtt{562832})$

Figure 5, can be written as binary notation as follows.

$$\begin{aligned} \Delta x^{11} &= 100000000000000000000000, \ \Delta x^{14} = 100000000000011111101100, \\ \Delta y^{11} &= 100000010010010010000000, \ \Delta y^{14} = 001000111001000110000100, \\ \Delta z^{11} &= 000001111110110010000000, \ \Delta z^{14} = 100111001000110000100000, \\ \Delta c^{11} &= 000001101100100000000000, \ \Delta c^{14} = 001111110001101001001000. \end{aligned}$$

As can be seen in Figure 5, the modular addition operations in rounds 11 and 14 satisfy the conditions of Theorem 1 and they hold with probabilities of 2^{-9} and 2^{-17}, respectively. Assuming independency, the differential probability of these two rounds should hold with probability of 2^{-26}; however, we show that it is an incompatibility differential. To this end, by considering the modular addition operation for the 11-th round, we have $(\Delta x^{11}_{13}, \Delta y^{11}_{13}, \Delta z^{11}_{13}, \Delta c^{11}_{13}, \Delta c^{11}_{14}) = (0, 1, 1, 0, 1)$. It should be noted that the values that can have this differential must be selected from the set (6). According to the set (6), the following pairs have the differential $(\Delta x^{11}_{13}, \Delta y^{11}_{13}, \Delta z^{11}_{13}, \Delta c^{11}_{13}, \Delta c^{11}_{14}) = (0, 1, 1, 0, 1)$.

$$\{(x^{11}_{13}, y^{11}_{13}, z^{11}_{13}, c^{11}_{13}, c^{11}_{14})\} \in \left\{ \left\{ \begin{matrix} (0,0,1,1,0) \\ (0,1,0,1,1) \end{matrix} \right\}, \left\{ \begin{matrix} (1,0,1,0,0) \\ (1,1,0,0,1) \end{matrix} \right\} \right\}.$$

So, for each pair we get the condition

$$z^{11}_{13} = \bar{c}^{11}_{14}, \tag{14}$$

where $\bar{c}$ is the bit-wise NOT of c. Now, by considering the differential $(\Delta x^{11}_{14}, \Delta y^{11}_{14}, \Delta z^{11}_{14}, \Delta c^{11}_{14}, \Delta c^{11}_{15}) = (0, 0, 1, 1, 1)$, for the 14-th bit, the following pairs can reach to this differential.

$$(x^{11}_{14}, y^{11}_{14}, z^{11}_{14}, c^{11}_{14}, c^{11}_{15}) \in \left\{ \left\{ \begin{matrix} (0,1,1,0,0) \\ (0,1,0,1,1) \end{matrix} \right\}, \left\{ \begin{matrix} (1,0,1,0,0) \\ (1,0,0,1,1) \end{matrix} \right\} \right\}.$$

So, these pairs conclude the condition

$$z^{11}_{14} = \bar{c}^{11}_{14}. \tag{15}$$

Table 19: 15-round related-key differential trail in SPECK48/96 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (000010, 000002, 441000, 004090)$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	004090		825092‖820202	
1	020000	-4	821002‖001200	
2	100000	-1	009010‖000010	-5
3	800000	-1	000080‖000000	-3
4	000000	-1	000000‖000000	0
5	000000	0	000000‖000000	0
6	000000	0	000000‖000000	0
7	040000	-1	000000‖000000	0
8	1C0000	-4	040000‖040000	0
9	040000	-5	200400‖000400	-5
10	240400	-2	042404‖040404	-3
11	042001	-6	240420‖042400	-4
12	240409	-7	202005‖010005	-5
13	042044	-6	20242C‖282404	-6
14	250664	-5	002464‖410445	-7
15			C00245‖C8206F	-8
	$\log_2\left(\Pr(Q_K)\right)$:	-43	$\log_2\left(\Pr(Q_D)\right)$:	-46

A pair of weak keys:
$K = (0C8E5B, 240ABD, 8BFBE8, 73CFA3)$
$K' = (0C8E4B, 240ABF, CFEBE8, 738F33)$

By combining the equations (14) and (8), we have

$$z_{13}^{11} = z_{14}^{11}. \tag{16}$$

Now, in the modular addition operation for 14-th round, we have $(\Delta x_5^{14}, \Delta y_5^{14}, \Delta z_5^{14}, \Delta c_5^{14}, \Delta c_6^{14}) = (1, 0, 1, 0, 1)$. Thus, the following pairs will lead to the differential $(1, 0, 1, 0, 1)$.

$$(x_5^{14}, y_5^{14}, z_5^{14}, c_5^{14}, c_6^{14}) \in \left\{ \left\{ \begin{matrix} (0,0,1,1,0) \\ (1,0,0,1,1) \end{matrix} \right\}, \left\{ \begin{matrix} (0,1,1,0,0) \\ (1,1,0,0,1) \end{matrix} \right\} \right\}.$$

Hence, for these pairs, we can get the condition

$$x_5^{14} = c_6^{14}. \tag{17}$$

Now, by considering the differential $(\Delta x_6^{14}, \Delta y_6^{14}, \Delta z_6^{14}, \Delta c_6^{14}, \Delta c_7^{14}) = (1, 0, 0, 1, 0)$ for the 6-th bit, the following pairs will lead to this differential.

$$(x_6^{14}, y_6^{14}, z_6^{14}, c_6^{14}, c_7^{14}) \in \left\{ \left\{ \begin{matrix} (0,0,1,1,0) \\ (1,0,1,0,0) \end{matrix} \right\}, \left\{ \begin{matrix} (0,1,0,1,1) \\ (1,1,0,0,1) \end{matrix} \right\} \right\}.$$

Therefore, we have the condition

$$x_6^{14} = \overline{c}_6^{14}. \tag{18}$$

By combining the equations (17) and (18), we have

$$x_5^{14} = \overline{x}_6^{14}. \tag{19}$$

Since $x^{14} = (z^{11} \ggg 8)$ (see Figure 5), we have $z_{13}^{11} = x_5^{14}$ and $z_{14}^{11} = x_6^{14}$. Hence, by considering the equations (16) and (19), we reach a contradiction.

Table 20: 16-round related-key differential trail in SPECK48/96 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{000010}, \texttt{000020}, \texttt{00441000}, \texttt{004090})$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	004090		825092‖820202	
1	020000	-4	821002‖001200	
2	100000	-1	009010‖000010	-5
3	800000	-1	000080‖000000	-3
4	000000	-1	000000‖000000	0
5	000000	0	000000‖000000	0
6	000000	0	000000‖000000	0
7	040000	-1	000000‖000000	0
8	1C0000	-4	040000‖040000	0
9	040000	-5	200400‖000400	-5
10	240400	-2	042404‖040404	-3
11	042001	-6	240420‖042400	-4
12	1A1C77	-19	202005‖010005	-5
13	DA03C7	-15	183C54‖103C7C	-8
14	FFFEC1	-21	FE1FFF‖7FFC1F	-8
15	83C4D4	-14	8000FF‖7FE004	-3
16			FC24D0‖0324F3	-3
	$\log_2\big(\Pr(Q_K)\big)$:	-94	$\log_2\big(\Pr(Q_D)\big)$:	-47

A pair of weak keys:
$K = (\texttt{E768B7}, \texttt{64197F}, \texttt{A32B17}, \texttt{E346B7})$
$K' = (\texttt{E768A7}, \texttt{64197D}, \texttt{E73B17}, \texttt{E30627})$

Table 21: 13-round related-key differential trail in SPECK64/128 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{00000200}, \texttt{00000040}, \texttt{00820008}, \texttt{08001200})$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	08001200		18421240‖10404040	
1	40000000	-4	10420040‖00024000	
2	00000002	-1	00120200‖00000200	-5
3	00000010	-1	00001000‖00000000	-3
4	00000000	-2	00000000‖00000000	-1
5	00000000	0	00000000‖00000000	0
6	00000000	0	00000000‖00000000	0
7	80000000	0	00000000‖00000000	0
8	80000004	0	80000000‖80000000	0
9	80000020	-1	00800004‖00800000	-1
10	80800124	-2	84808020‖80808020	-3
11	84000800	-4	20840184‖24800080	-6
12	A0804804	-3	24A08481‖00A08080	-9
13			20046800‖25006C00	-8
	$\log_2\big(\Pr(Q_K)\big)$:	-18	$\log_2\big(\Pr(Q_D)\big)$:	-36

A pair of weak keys:
$K = (\texttt{10477738}, \texttt{AA9DC904}, \texttt{8E451208}, \texttt{7556C2C3})$
$K' = (\texttt{10477538}, \texttt{AA9DC944}, \texttt{8EC71200}, \texttt{7D56D0C3})$

Table 22: 14-round related-key differential trail in SPECK64/128 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (00000002, 40000000, 08008200, 00080012)$.

Round	Differential in Key	$\log_2 \Pr$	Differential in Data	$\log_2 \Pr$
0	00080012		40184212||40104040	
1	00400000	-4	40104200||00000240	
2	02000000	-1	00001202||00000002	-5
3	10000000	-1	00000010||00000000	-3
4	00000000	-1	00000000||00000000	-1
5	00000000	0	00000000||00000000	0
6	00000000	0	00000000||00000000	0
7	00800000	-1	00000000||00000000	0
8	07800000	-3	00800000||00800000	0
9	00800000	-7	04008000||00008000	-4
10	03808000	-5	00848080||00808080	-3
11	00840000	-9	84008400||80048000	-7
12	05A08000	-7	80048084||80208080	-5
13	10A50080	-12	01000400||00040004	-6
14			10A00080||108000A0	-3
	$\log_2(\Pr(Q_K))$:	-51	$\log_2(\Pr(Q_D))$:	-37

A pair of weak keys:
$K = $ (BE466B7E, F02B57A6, 6F474116, 3E245A23)
$K' = $ (BE466B7C, B02B57A6, 6747C316, 3E2C5A31)

Table 23: 15-round related-key differential trail in SPECK64/128 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (00000002, 40000000, 08008200, 00080012)$.

Round	Differential in Key	$\log_2 \Pr$	Differential in Data	$\log_2 \Pr$
0	00080012		40184212||40104040	
1	00400000	-4	40104200||00000240	
2	02000000	-1	00001202||00000002	-5
3	10000000	-1	00000010||00000000	-3
4	00000000	-1	00000000||00000000	-1
5	00000000	0	00000000||00000000	0
6	00000000	0	00000000||00000000	0
7	00800000	-1	00000000||00000000	0
8	07800000	-3	00800000||00800000	0
9	00800000	-7	04008000||00008000	-4
10	038080000	-5	00848080||00808080	-3
11	00840000	-9	84008400||80048000	-7
12	05A08000	-7	80048084||80208080	-5
13	10A50080	-12	01000400||00040004	-6
14	95908480	-9	10A00080||108000A0	-3
15			04002420||800002120	-8
	$\log_2(\Pr(Q_K))$:	-60	$\log_2(\Pr(Q_D))$:	-45

A pair of weak keys:
$K = $ (BE466B7E, F02B57A6, 6F474116, 3E245A23)
$K' = $ (BE466B7C, B02B57A6, 6747C316, 3E2C5A31)

Table 24: 16-round related-key differential trail in SPECK64/128 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{00000200}, \texttt{00000040}, \texttt{00820008}, \texttt{08001200})$.

Round	Differential in Key	$\log_2 \Pr$	Differential in Data	$\log_2 \Pr$
0	08001200		18421240||10404040	
1	40000000	-4	10420040||00024000	
2	00000002	-1	00120200||00000200	-5
3	00000010	-1	00001000||00000000	-3
4	00000000	-2	00000000||00000000	-1
5	00000000	0	00000000||00000000	0
6	00000000	0	00000000||00000000	0
7	80000000	0	00000000||00000000	0
8	80000004	0	80000000||80000000	0
9	80000020	-1	00800004||00800000	-1
10	80800124	-2	84808020||80808020	-3
11	84000800	-4	20840184||24800080	-6
12	A0804804	-3	24A08C81||00A08880	-8
13	84020821	-6	21046000||24002400	-10
14	8092592C	-8	A0232801||80220800	-8
15	84808078	-11	01104004||00000000	-11
16			80819038||80819038	-4
	$\log_2(\Pr(Q_K))$:	-43	$\log_2(\Pr(Q_D))$:	-60

A pair of weak keys:
$K = (\texttt{7009EF82}, \texttt{01B2A171}, \texttt{C4E14153}, \texttt{2A5CEE20})$
$K' = (\texttt{7009ED82}, \texttt{01B2A131}, \texttt{C463415B}, \texttt{225CFC20})$

Table 25: 17-round related-key differential trail in SPECK64/128 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{00000200}, \texttt{00000040}, \texttt{00820008}, \texttt{08001200})$.

Round	Differential in Key	$\log_2 \Pr$	Differential in Data	$\log_2 \Pr$
0	08001200		18421240||10404040	
1	40000000	-4	10420040||00024000	
2	00000002	-1	00120200||00000200	-5
3	00000010	-1	00001000||00000000	-3
4	00000000	-2	00000000||00000000	-1
5	00000000	0	00000000||00000000	0
6	00000000	0	00000000||00000000	0
7	80000000	0	00000000||00000000	0
8	80000004	0	80000000||80000000	0
9	80000020	-1	00800004||00800000	-1
10	80800124	-2	84808020||80808020	-3
11	84000800	-4	20840184||24800080	-6
12	A0804804	-3	24A08C81||00A08880	-8
13	84020821	-6	21046000||24002400	-10
14	8092592C	-8	A0232801||80220800	-8
15	84811040	-12	01104004||000000000	-11
16	A409920C	-6	80800000||80800000	-4
17			2409120C||20091208	-2
	$\log_2(\Pr(Q_K))$:	-50	$\log_2(\Pr(Q_D))$:	-62

In this case, after limiting the time for two weeks of running the MILP model, we could not find a weak key, while based on our test for each of the two consecutive rounds there are not any independed modular addition.

Table 26: 16-round related-key differential trail in SPECK128/256 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0)$ = (0200000000000000, 0040000000000010, 0008000001248000, 1000080000002080).

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	1000080000002080		50402c02c0442012‖40002426c0944082	
1	9000400000000000	-6	40402402C0440092‖0040000400D04010	
2	0002000000000004	-2	0200002002100410‖0000000004920490	-13
3	0010000000000024	-2	0200002002100410‖0000000004920490	-14
4	0080000000000000	-4	8000000000208400‖000000000000480	-10
5	0400000000000000	-1	0000000000002404‖0000000000000004	-5
6	2000000000000000	-1	0000000000000020‖0000000000000000	-3
7	0000000000000000	-2	0000000000000000‖0000000000000000	-1
8	0000000000000000	0	0000000000000000‖0000000000000000	0
9	0000000000000000	0	0000000000000000‖0000000000000000	0
10	0100000000000000	-1	0000000000000000‖0000000000000000	0
11	0F00000000000000	-3	0100000000000000‖0100000000000000	0
12	0100000000000000	-7	0801000000000000‖0001000000000000	-4
13	0901000000000000	-2	0109010000000000‖0000000000000000	-3
14	4108000000000000	-5	0801080100000000‖0009000100000000	-5
15	C947000000000002	-9	4109010901000000‖4141010101000000	-6
16			0841080008010002‖0249000800010000	-12
	$\log_2(\Pr(Q_K))$:	-45	$\log_2(\Pr(Q_D))$:	-76

A pair of weak keys:
K = (535876A8F21D9DE0, 3CCC449DCEECCBFE, A0BAEDD3FAF2F38F, 6032F128F67FD07E)
K' = (515876A8F21D9DE0, 3C8C449DCEECCBEE, A0B2EDD3FBD6738F, 7032F928F67FF0FE)

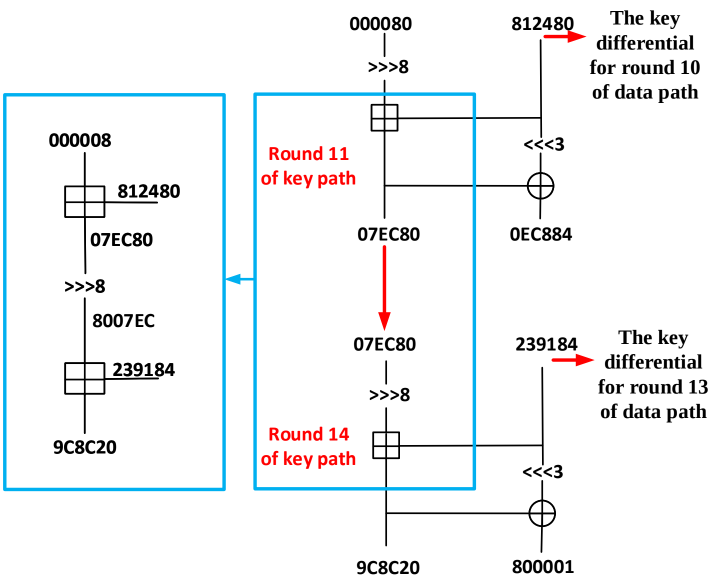


Fig. 5: Part of the 16-round incompatible differential trail of SPECK48/96 based on Table 29.

Table 27: 19-round related-key differential trail in SPECK128/256 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{0200000000000000}, \texttt{0040000000000010}, \texttt{0008000001248000}, \texttt{1000080000002080})$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	1000080000002080		50402C02C0442012||40002406C0944082	
1	9000400000000000	-6	40402402C0440092||0040000400D04010	
2	0002000000000004	-2	0200002002100410||0000000004920490	-13
3	0010000000000024	-2	0200002002100410||0000000004920490	-14
4	0080000000000000	-4	8000000000208400||000000000000480	-10
5	0400000000000000	-1	0000000000002404||0000000000000004	-5
6	2000000000000000	-1	0000000000000020||0000000000000000	-3
7	0000000000000000	-2	0000000000000000||0000000000000000	-1
8	0000000000000000	0	0000000000000000||0000000000000000	0
9	0000000000000000	0	0000000000000000||0000000000000000	0
10	0100000000000000	-1	0000000000000000||0000000000000000	0
11	0F00000000000000	-3	0100000000000000||0100000000000000	0
12	0100000000000000	-7	0801000000000000||0001000000000000	-4
13	0901000000000000	-2	0109010000000000||0000000000000000	-3
14	4108000000000000	-5	0801080100000000||0009000100000000	-5
15	C947000000000002	-9	4109010901000000||4141010101000000	-6
16	03F8010000000010	-11	0841080008010002||0249000800010000	-12
17	0001090000000090	-13	0249400000090110||1001404000010110	-14
18	0148400000000410	-10	0002000000010881||8008020000090001	-12
19			0040400000090509||0000500000410505	-9
	$\log_2\left(\Pr(Q_K)\right)$:	-79	$\log_2\left(\Pr(Q_D)\right)$:	-111

A pair of weak keys:
$K = (\texttt{A86999C9C3C38FDA}, \texttt{800A91FA534F6705}, \texttt{843997FC7C0B7F01}, \texttt{CE6525B90E522DB6})$
$K' = (\texttt{AA6999C9C3C38FDA}, \texttt{804A91FA534F6715}, \texttt{843197FC7D2FFF01}, \texttt{DE652DB90E520D36})$

Table 28: An incompatible differential trail for 14 rounds of SPECK32/64 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (\texttt{0001}, \texttt{4000}, \texttt{0880}, \texttt{0025})$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	0025		50A4||5021	
1	0080	-4	5081||00A0	
2	0200	-1	0281||0001	-4
3	0800	-1	0004||0000	-3
4	0000	-2	0000||0000	-1
5	0000	0	0000||0000	0
6	0000	0	0000||0000	0
7	0040	-1	0000||0000	0
8	0140	-1	0040||0040	0
9	0240	-4	8100||8000	-1
10	87C0	-5	8142||8140	-3
11	0042	-7	8002||8500	-5
12	8140	-4	8042||9440	-2
13	0557	-6	9000||C102	-4
14			C575||C17E	-4
	$\log_2\left(\Pr(Q_K)\right)$:	-36	$\log_2\left(\Pr(Q_D)\right)$:	-27

Table 29: An incompatible differential trail for 16 rounds of SPECK48/96 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0) = (020000, 004000, 000882, 120008)$.

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	120008		12504A‖405040	
1	000040	-3	005040‖400002	
2	000200	-1	020012‖020000	-5
3	001000	-1	100000‖000000	-3
4	000000	-2	000000‖000000	-1
5	000000	0	000000‖000000	0
6	000000	0	000000‖000000	0
7	000080	-1	000000‖000000	0
8	000480	-1	000080‖000080	0
9	002080	-2	800400‖800000	-1
10	812480	-2	80A084‖80A080	-2
11	0EC884	-9	84C4A0‖81C0A4	-6
12	840CA0	-11	2E03A4‖200680	-11
13	239184	-11	002421‖001020	-9
14	800001	-17	008180‖000080	-6
15	00F245	-8	000000‖000400	-2
16			00F645‖00D645	-1
	$\log_2\left(\Pr(Q_K)\right)$:	-69	$\log_2\left(\Pr(Q_D)\right)$:	-47

Table 30: An incompatible differential trail for 16 rounds of SPECK64/128 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0)$=(00208002, 40000000, 08000200, 00080012).

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	00080012		82888292‖90C09080	
1	00400080	-3	82808280‖12401200	
2	02000480	-2	92829202‖00820202	-10
3	10000000	-4	04108010‖00009000	-11
4	80000000	-1	00048080‖00000800	-5
5	00000004	0	00000400‖00000000	-2
6	00000000	-2	00000000‖00000000	-1
7	00000000	0	00000000‖00000000	0
8	00000000	0	00000000‖00000000	0
9	20000000	-1	00000000‖00000000	0
10	E0000001	-2	20000000‖20000000	0
11	20000000	-6	00200001‖00200000	-3
12	20200001	-2	21202000‖20202000	-3
13	21000008	-5	00210021‖01200020	-5
14	20200049	-7	01202128‖08202028	-6
15	21002200	-6	00010040‖41000100	-8
16			A0002200‖A8002A02	-3
	$\log_2\left(\Pr(Q_K)\right)$:	-41	$\log_2\left(\Pr(Q_D)\right)$:	-57

Table 31: An incompatible differential trail for 21 rounds of SPECK128/256 with $(\Delta l_2, \Delta l_1, \Delta l_0, \Delta k_0)$= (00500040000005A4, 0008000800000034, 4001400100010400, 0240014001000024).

Round	Differential in Key	$\log_2$ Pr	Differential in Data	$\log_2$ Pr
0	0240014001000024		1248414801001224‖100A000800001202	
1	1000080008000000	-9	1008400800001200‖0002400000000002	
2	A400500040000000	-6	1012404000000010‖1000404000000000	-8
3	2002000200000000	-8	8410020000000000‖0412000000000000	-8
4	001C001000000000	-6	2C90100000000000‖0C00100000000000	-8
5	0000008000000000	-7	0400800000000000‖6400000000000000	-9
6	0700040000000000	-4	E404000000000000‖C404000000000003	-5
7	0000200000000000	-8	C06000000000001F‖E040000000000001	-14
8	0001000000000000	-3	030000000000000F‖0100000000000000	-15
9	0008000000000000	-3	0800000000000000‖0000000000000000	-6
10	0000000000000000	-4	0000000000000000‖0000000000000000	-1
11	0000000000000000	0	0000000000000000‖0000000000000000	0
12	0000000000000000	0	0000000000000000‖0000000000000000	0
13	0000400000000000	-1	0000000000000000‖0000000000000000	0
14	0003C00000000000	-3	0000400000000000‖0000400000000000	0
15	0000400000000000	-7	0002004000000000‖0000004000000000	-4
16	0002404000000000	-2	0000424040000000‖0000404040000000	-3
17	0010420000000000	-5	0002004200400000‖0000024000400000	-5
18	0092404000000000	-7	0010424042404000‖0010504040404000	-6
19	0400420040000000	-6	0082004200020040‖0000824002000040	-10
20	2402504240000000	-5	4400424000000240‖4404504010000040	-8
21			2042004010000042‖0060824090000240	-12
	$\log_2\left(\Pr(Q_K)\right)$:	-94	$\log_2\left(\Pr(Q_D)\right)$:	-122