*cryptography*

MDPI

*Article*

# Further Observations on SIMON and SPECK Block Cipher Families

**Seyed Mojtaba Dehnavi**

Faculty of Mathematical and Computer Sciences, Kharazmi University, Tehran 19678, Iran; dehnavism@ipm.ir

Received: 7 November 2018; Accepted: 18 December 2018; Published: 20 December 2018

**Abstract:** SIMON and SPECK families of block ciphers are well-known lightweight ciphers designed by the NSA. In this note, based on the previous investigations on SIMON, a closed formula for the squared correlations and differential probabilities of the mapping $\phi(x) = x \odot S^1(x)$ on $\mathbb{F}_2^n$ is given. From the aspects of linear and differential cryptanalysis, this mapping is equivalent to the core quadratic mapping of SIMON via rearrangement of coordinates and EA -equivalence. Based on the proposed explicit formula, a full description of DDT and LAT of $\phi$ is provided. In the case of SPECK, as the only nonlinear operation in this family of ciphers is addition mod $2^n$, after reformulating the formula for linear and differential probabilities of addition mod $2^n$, straightforward algorithms for finding the output masks with maximum squared correlation, given the input masks, as well as the output differences with maximum differential probability, given the input differences, are presented. By the aid of the tools given in this paper, the process of the search for linear and differential characteristics of SIMON and SPECK families of block ciphers could be sped up, and the complexity of linear and differential attacks against these ciphers could be reduced.

**Keywords:** SIMON; SPECK; DDT; LAT; pseudo-octal representation; gaps and blocks representation; modular addition mod $2^n$

## 1. Introduction

SIMON and SPECK are two families of block ciphers that were designed by the NSA [1]. These lightweight ciphers have widely attracted the attention of researchers [2–14]. In [2], some linear characteristics for the SIMON family of block ciphers were presented. The authors of [3] provided differential attacks of up to slightly more than half of the number of rounds for SIMON and SPECK families of block ciphers. A technique for the automatic search for differential trails in ARX ciphers was used to improve the previous attacks on SIMON and SPECK block cipher families in [4]. In [5], significantly improved differential attacks against all 10 variants of SPECK were presented. Two variants of the SIMON family of ciphers were investigated in [6], and a 14-round linear approximation for SIMON-32, as well as a 17-round linear approximation for SIMON-48 were presented. In [7], using quadratic constraints or constraints from H-representation of a specific convex hull, a method for constructing a mixed-integer (non)linear programming model for SIMON was provided. The authors of [8] studied the security of a version of SIMON, using some kind of truncated differentials, and an attack of up to 26 rounds was presented. In [9], improved linear attacks on all reduced versions of SIMON were presented with dynamic key guessing. The authors of [10] showed that overlooking linear hulls, formed by a single round, may lead to the wrong estimations of linear correlations. In [11], a partial linear mask table was used to speed up the search progress to attack reduced round SPECK. In [12], firstly, the properties of the linear approximation of the bitwise AND with dependent input bits were investigated, and then, using MILP, improved linear characteristics for several versions of SIMON were obtained. The authors of [13], reducing the sufficient bit conditions corresponding to the differential propagations, and avoiding the guess for some subkey bits or equivalent key bits involved in the conditions, extended differential attacks on SIMON by 2–4 more rounds. In [14], an algorithm to find a differential path in ARXstructures was proposed, and based on this, previous differential attacks on various versions of SPECK were improved. All of the mentioned papers investigated SIMON and/or SPECK from linear and/or differential aspects and examined the resistance of these ciphers against linear and differential cryptanalysis.

Some authors have studied the properties of the components of these ciphers from theoretical aspects [15–24]. In [15,16], linear and differential properties of SIMON-like ciphers were investigated, from the mathematical viewpoint, and an efficient formula for computing linear and differential probabilities of SIMON was presented. In [18], after a theoretical examination, the authors studied how rotational cryptanalysis is affected when constants are injected. In [17], after some mathematical investigations, the resistance of SIMON-like ciphers against differential cryptanalysis was analyzed, and upper bounds for the differential probabilities of differential characteristics for some certain instances were provided. In [19,20], upon some theoretical studies, upper bounds for differential probabilities and squared correlations for SIMON-like ciphers were provided, and provably optimal differential trails for various versions of SIMON were presented. In [21–24], linear properties of addition mod $2^n$ were investigated, from the mathematical viewpoint.

In this note, based on the previous studies, nonlinear components of SIMON and SPECK families of ciphers are examined. The method of the research of this paper is somewhat similar to [15–24]: we study the linear and differential properties of the components of SIMON and SPECK families of block ciphers, from the mathematical viewpoint.

The only nonlinear component of SIMON family of block ciphers is the quadratic mapping:

$$f : \mathbb{F}_2^n \to \mathbb{F}_2^n,$$

$$f(x) = S^1(x) \odot S^8(x) \oplus S^2(x),$$

for $n = 16, 24, 32, 48, 64$. The mapping $f$ is equivalent to $\phi$ below, through a permutation of coordinates and EA-equivalence:

$$\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n,$$

$$\phi(x) = x \odot S^1(x).$$

Based on the previous research on the linear and differential properties of SIMON [15,16,18–20], a simple explicit formula for differential probabilities and squared correlations of $\phi$ is given. Besides, a full description of DDT and LAT of $\phi$ is provided, in this paper.

The only nonlinear operation in the SPECK family of block ciphers is addition mod $2^n$, with $n = 16, 24, 32, 48, 64$. Based on the previous studies on the linear and differential properties of this operation [21–24], a closed formula for differential probabilities and squared correlations of modular addition mod $2^n$, along with straightforward algorithms for finding the output masks with the maximum squared correlation, given the input masks and the output differences with the maximum differential probability, given the input differences, are presented.

By the aid of the main contribution of the current paper, i.e., the full description of DDT and LAT of $\phi$, which in turn leads to the full determination of DDT and LAT of the core quadratic mapping of SIMON, as well as the straightforward algorithms for finding the optimum output differences, given the two input differences and the optimum output masks, given the two input masks for the operation of modular addition mod $2^n$, the process of finding good linear and differential characteristics for the lightweight ciphers SIMON and SPECK could be sped up, and the complexity of linear and differential attacks against these ciphers could be reduced.

Section 2 gives the preliminary notations and definitions. Section 3 is devoted to the examination of the linear and differential properties of SIMON. Section 4 discusses the linear and differential properties of SPECK, and Section 5 is the conclusion.

## 2. Preliminary Notations and Definitions

In the sequel $i$, $j$, $m$, $n$, $t$, $r$, and $s$ are natural numbers. The $n$-dimensional space over $\mathbb{F}_2$, the finite field with two elements, is denoted by $\mathbb{F}_2^n$. Left rotation by $t$ times on $x$ is denoted by $S^t(x)$. The operations of AND, OR, and XOR are denoted by $\odot$, $\vee$, and $\oplus$, respectively. The Hamming weight of a binary number or vector $x$ is represented by $\mathbf{w}(x)$ and the complement of $x$ by $\bar{x}$. The standard dot product in $\mathbb{F}_2^n$ is denoted by $\cdot$. The all one and the all zero vectors are represented by **1** and **0**, respectively.

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Define:

$$D_f(a,b) = |\{x \in \mathbb{F}_2^n : f(x) \oplus f(x \oplus a) = b\}|.$$

The matrix or table $[D_f(a,b)]$, $a, b \in \mathbb{F}_2^n$, is called the Difference Distribution Table (DDT) of $f$. The normalized DDT of $f$ is defined as:

$$\mathbb{D}_f = [\mathbb{D}_f(a,b)] = [D_f(a,b)/2^n].$$

Not that for every $a \in \mathbb{F}_2^n$, we have:

$$\sum_{x \in \mathbb{F}_2^n} \mathbb{D}_f(a,x) = 1.$$

If we have $\mathbb{D}_f(a,x) \neq 0$ for some $x \in \mathbb{F}_2^n$, then $x$ is called an admissible output difference for $a$ in this paper.

The Walsh coefficient of $f$ on $a$ and $b$ is defined as:

$$W_f(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot f(x)}.$$

The matrix or table $[W_f(a,b)]$, $a, b \in \mathbb{F}_2^n$, is called the Linear Approximation Table (LAT) of $f$. The normalized LAT of $f$ is defined as:

$$\mathbb{L}_f = [\mathbb{L}_f(a,b)] = [W_f^2(a,b)/2^{2n}].$$

Not that for every $b \in \mathbb{F}_2^n$, we have:

$$\sum_{x \in \mathbb{F}_2^n} \mathbb{L}_f(x,b) = 1.$$

If we have $\mathbb{L}_f(x,b) \neq 0$ for some $x \in \mathbb{F}_2^n$, then $x$ is called an admissible input mask for $b$, in the current paper.

Let $a = (a_{n-1}, \ldots, a_1, a_0) \in \mathbb{F}_2^n$. Put $\alpha = (\alpha_{n-1}, \ldots, \alpha_1, \alpha_0)$ with $\alpha_i = (a_i, a_{i-1}, a_{i-2})$, $0 \leq i < n$: the indices are calculated mod $n$. In this paper, this representation is called the pseudo-octal representation of $a$. It is obvious that every binary number $a$ has a unique pseudo-octal representation; but a sequence of octal symbols is not necessarily the pseudo-octal representation of a binary number. If a sequence of octal symbols is the pseudo-octal representation of a binary number, then it is called admissible in this paper. For an $\alpha$ to be admissible, the consecutive appearance of octal symbols should be as follows:

$$\{0,1\} \to \{0,4\}, \ \ \{2,3\} \to \{1,5\}, \ \ \{4,5\} \to \{2,6\}, \ \ \{6,7\} \to \{3,7\}. \tag{1}$$

For example, 110010 has the pseudo-octal representation 641253. This representation is used in Section 3.

Another representation for binary numbers that is used in Section 3, is as follows: any binary number could be represented by consecutive gaps and blocks. A gap is a series of zeroes, and a block is a series of ones. Any number, except the all one and all zero vectors, up to a rotation, consists of some $m$ many gaps and blocks $\mathbf{1}_{b_i}\mathbf{0}_{a_i}$, with $a_i, b_i \geq 1, 1 \leq i \leq m$. For example, the number 0011010110, rotated two times to the left, is of the form $\mathbf{1}_2\mathbf{0}_1\mathbf{1}_1\mathbf{0}_1\mathbf{1}_2\mathbf{0}_3$.

## 3. Linear and Differential Properties of SIMON

Linear and differential properties of the core quadratic mapping of the SIMON family of block ciphers were studied in [15–20]. The mapping:

$$\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n,$$

$$\phi(x) = x \to x \odot S^1(x),$$

is equivalent to the core quadratic mapping of SIMON, through a permutation of coordinates and EA-equivalence [15,16]. In this section, based on the previous examinations, the simple closed formula for differential probabilities and squared correlations of $\phi$ is given. Besides, a full description of DDT and LAT of $\phi$ is provided. Firstly, a theorem from [15,16] is recalled:

**Theorem 1.** *The differential probability of $\phi$ on $\alpha$ and $\beta$ is:*

$$\mathbb{D}_\phi(\alpha, \beta) = \begin{cases} 2^{1-n} & \alpha = \mathbf{1},\ \mathbf{w}(\beta) = 0 \mod 2, \\ 2^{-s} & \alpha \neq \mathbf{1}, \beta \odot \overline{varibits} = \mathbf{0}, (\beta \oplus S^1(\beta)) \odot doublebits = \mathbf{0}, \\ 0 & o.w. \end{cases}$$

*where:*

$$s = \mathbf{w}(varibits \oplus doublebits),$$

$$varibits = S^1(\alpha) \vee \alpha,$$

$$doublebits = \alpha \odot \overline{S^1(\alpha)} \odot S^2(\alpha).$$

**Theorem 2.** *Let $\alpha \neq \mathbf{0}, \mathbf{1}$ consist of gaps and blocks of the form $\mathbf{1}_{b_i}\mathbf{0}_{a_i}$, $1 \leq i \leq m$, according to the notations presented in Section 1. Then, for any admissible output difference $x \in \mathbb{F}_2^n$, we have:*

$$\mathbb{D}_\phi(\alpha, x) = 2^{-(\mathbf{w}(\alpha)+s)},$$

*where $s = |\{1 \leq i \leq m : a_i \neq 1\}|$; i.e., $s$ is the number of gaps of length greater than one.*

**Proof.** Firstly, note that $\mathbf{w}(\alpha) + s = \mathbf{w}(\alpha) + m - t$, where:

$$t = |\{1 \leq i \leq m : a_i = 1\}|.$$

According to Table 1 and (1), the theorem is proven via case-by-case analysis. The blocks of length one and the blocks of length greater than one should be treated separately. Furthermore, the gaps before and after this block should be analyzed separately, according to their lengths: again, the gaps of length one and the gaps of length greater than one should be verified separately. All the cases could also be examined by programming. For instance, consider the pattern $\star 101100 \star$ with the pseudo-octal representation $\star 5364 \star$. Either the pattern is of the form $\star 0101100 \star$ or $\star 25364 \star$ in pseudo-octal representation, in which the symbols 2, 3, 6, and 4 each add one to the absolute value of the exponent of differential probability, according to Table 1; or the leftmost block in the pattern is of length greater than one. For the sake of simplicity, suppose that the pattern is of the form $\star 01101100 \star$, which corresponds to $\star 365364 \star$, where 4, 6, 3, 6, and 3 each have a contribution of one. Therefore, for the presented pattern, the differential probability equals the weight, plus the number of blocks, minus the number of gaps of length one. □

In spite of the fact that the core mapping of SIMON does not inherit all the visual properties of $\phi$, but regarding the equivalence between the core quadratic mapping of SIMON and $\phi$, Theorem 5 in [19] and Lemma 2 in [17] are direct results of Theorem 2.

Before stating the next theorem, some notations are explained. In the following theorems, $\mathcal{A}_t$ denotes an arbitrary $t$-bit number, or equivalently, the set off all $t$-bit numbers, and $\mathcal{A}_t^{1/2}$ stands for the set of $t$-bit words with a half-rate. For example:

$$\mathcal{A}_1\mathcal{A}_2 = \{000, 001, 010, 011, 100, 101, 110, 111\},$$

$$\mathcal{A}_1^{1/2}\mathcal{A}_2 = \{000, 001, 110, 111\}.$$

**Table 1.** The pseudo-octal representation of the input (output) difference.

| $x$ | $\boldsymbol{Varibits}$ | $\boldsymbol{Doublebits}$ | $\boldsymbol{Varibits \oplus Doublebits}$ | $\boldsymbol{Adjacent\,Parity: \ x \oplus S^1(x)}$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 1 | 0 | 1 | 1 |
| 3 | 1 | 0 | 1 | 1 |
| 4 | 1 | 0 | 1 | 1 |
| 5 | 1 | 1 | 0 | 1 |
| 6 | 1 | 0 | 1 | 0 |
| 7 | 1 | 0 | 1 | 0 |

**Theorem 3.** *Let $\alpha \neq \mathbf{0}, \mathbf{1}$ consist of gaps and blocks of the form $\mathbf{1}_{b_i}\mathbf{0}_{a_i}$, $1 \leq i \leq m$. Then, all the admissible output differences for $\alpha$ could be represented by gaps and blocks of the following forms. Note that, rotating $\alpha$ by a suitable number, we could start from the first block:*

$$\begin{cases} \mathbf{0}_{a_{i+1}-1}\mathcal{A}_{b_i+1} & a_{i+1} \neq 1, \\ \mathbf{0}_{a_{i+2}-1}\mathcal{A}^{1/2}_{b_{i+1}+1}\mathcal{A}_{b_i+1} & a_{i+1} = 1, \end{cases}$$

**Proof.** Regarding Table 1, for $x$ to be admissible, $\alpha_i \rightarrow x_i$ (in which the symbols are in pseudo-octal representation) should follow the next patterns:

$$\{0, 1\} \rightarrow \{0, 1, 2, 3\},$$

$$\{5\} \rightarrow \{0, 1, 6, 7\},$$

$$\{2, 3, 4, 6, 7\} \rightarrow \{0, 1, 2, 3, 4, 5, 6, 7\}.$$

For example, for the symbol 5, only for 0, 1, 6, and 7, both:

$$\beta \odot \overline{\text{varibits}}, \ (\beta \oplus S^1(\beta)) \odot \text{doublebits},$$

are 0. Since

$$\sum_{x \in \mathbb{F}_2^n} \mathbb{D}_\phi(\alpha, x) = 1,$$

and for any admissible $x \in \mathbb{F}_2^n$, we have $\mathbb{D}_\phi(\alpha, x) = 2^{-(\mathbf{w}(\alpha)+s)}$, so there are exactly $2^{\mathbf{w}(\alpha)+s}$ admissible output differences. Thus, it only suffices to show that all the presented output differences are admissible. Again, according to Table 1, it is straightforward to prove that every presented output difference is admissible: the case-by-case analysis or programming could be applied to prove the theorem. For instance, consider the input pattern $\star 001100 \star$ with pseudo-octal representation $\star 1364 \star$. The output admissible patterns could be of the following forms:

$$\star 00124 \star, \ \star 01240 \star, \ \star 01364 \star, \ \star 12400 \star, \ \star 12524 \star, \ \star 13640 \star, \ \star 13764 \star,$$

considering Table 1. Note that the number of these patterns is $8 = 2^{2+1}$. Therefore, the theorem is proven in this case. □

As an example, let $n = 8$ and $\alpha = 00101100$. Since $\mathbf{w}(\alpha) = 3$ and $\alpha$ has one gap of length greater than one, so for any admissible $x \in \mathbb{F}_2^8$, we have:

$$\mathbb{D}_\phi(\alpha, x) = 2^{-4},$$

by Theorem 2. Rotating $\alpha$ two times to the right gives 00001011. Now, by Theorem 3, the admissible output differences are of the form $\mathbf{0}_3\mathcal{A}_2^{1/2}\mathcal{A}_3$; i.e.,

00000000, 00000001, 00000010, 00000011, 00001100, 00001101, 00001110, 00001111,

00010000, 00010001, 00010010, 00010011, 00011100, 00011101, 00011110, 00011111.

The actual differences are the above numbers, rotated two times to the left.

**Theorem 4.** *Let $\beta \neq \mathbf{0}, \mathbf{1}$ consist of gaps and blocks of the form $\mathbf{1}_{b_i}\mathbf{0}_{a_i}$, $1 \leq i \leq m$. Then, for any admissible input mask $x \in \mathbb{F}_2^n$, we have:*

$$\mathbb{L}_\phi(x, \beta) = 2^{-(\mathbf{w}(\beta)+t)},$$

*where $t = |\{1 \leq i \leq m : b_i \mod 2 = 1|$; i.e., $t$ is the number of blocks of odd length. Furthermore, all the admissible input masks consist of gaps and blocks of the form:*

$$\begin{cases} \mathcal{A}_{b_i+1}\mathbf{0}_{a_i-1} & b_i \mod 2 = 1, \\ \mathcal{E}_{b_i+1}\mathbf{0}_{a_i-1} & b_i \mod 2 = 0, \end{cases}$$

*where $\mathcal{E}_{2t+1}$ denotes all the $(2t+1)$-bit patterns $(a_{2t}, \ldots, a_1, a_0)$ with:*

$$\bigoplus_{i=0}^{t} a_{2i} = 0.$$

**Proof.** The theorem could be proven either directly, using Theorem 5 in [15,16], or considering the comments in Appendix A (A.2) in [15]. In fact, $\mathbb{L}_\phi(x, \beta)$ is equal to:

$$2^{-\sum_{i=1}^{m} 2\lceil b_i/2 \rceil}.$$

Now, if $b_i$ is even, the contribution of this block in the absolute value of the exponent is only its length, and if $b_i$ is odd, the contribution is equal to its length, plus one. Therefore, the presented formula is correct. For the admissible input masks, note that similar to the case of differential probability, since we have $\mathbb{L}_\phi(x, \beta) = 2^{-(\mathbf{w}(\alpha)+t)}$, for any admissible $x \in \mathbb{F}_2^n$, and $\sum_{x \in \mathbb{F}_2^n} \mathbb{L}_\phi(x, \beta) = 1$, so there are exactly $2^{\mathbf{w}(\beta)+t}$ admissible input masks. Again, either by Theorem 5 in [15,16] or considering the comments of Appendix A (A.2) in [15], the admissibility of the presented input masks is proven. □

Regarding the equivalence between the core quadratic mapping of SIMON and $\phi$, Theorem 5 in [20] is a direct result of Theorem 4.

Let $n = 8$ and $\beta = 00101100$. Since $\mathbf{w}(\beta) = 3$ and $\beta$ has one block of odd length, so for any admissible $x \in \mathbb{F}_2^8$, we have:

$$\mathbb{L}_\phi(x, \beta) = 2^{-4},$$

by Theorem 4. Rotating $\beta$, two times to the left, gives 10110000. Now, by Theorem 4, the admissible output masks are of the form $\mathcal{A}_2\mathcal{E}_3\mathbf{0}_3$; i.e.,

$$00000000,\ 00101000,\ 00010000,\ 00111000,\ 01000000,\ 01101000,\ 01010000,\ 01111000,$$

$$10000000,\ 10101000,\ 10010000,\ 10111000,\ 11000000,\ 11101000,\ 11010000,\ 11111000.$$

The actual masks are the above numbers, rotated two times to the right.

**Remark 1.** *It is worth noting that, Theorems 3 and 4 characterize the set of all admissible input masks (output differences) for a given output mask (input difference) for the mapping $\phi$; this in turn culminates in complete determination of the corresponding input masks (output differences) for the core quadratic mapping of SIMON. Note that, using the previous methods and without the proposed characterization, given any input difference or output mask, we should search for desired admissible output differences or input masks and then verify whether they are admissible or not; but, with the aid of the provided characterization, we simply search within the set of all admissible masks or differences. Further, we could even save a table for the sparse masks or differences (the ones with a low Hamming weight) to speed the search process. This way, the complexity of finding optimal linear and differential characteristics could be reduced, significantly.*

Defining $\mathcal{N}_d(s)$ as the number of $\alpha \in \mathbb{F}_2^n$ such that $\mathbb{D}_\phi(\alpha, x) = 2^{-s}$ for any admissible $x \in \mathbb{F}_2^n$ and $\mathcal{N}_l(t)$ as the number of $\beta \in \mathbb{F}_2^n$ such that $\mathbb{L}_\phi(x, \beta) = 2^{2-2t}$ for any admissible $x \in \mathbb{F}_2^n$, we have the following propositions.

**Proposition 1.** *Let $n > 4$. We have:*

$$\mathcal{N}_d(1) = 0,\ \mathcal{N}_d(2) = n,\ \mathcal{N}_d(3) = 2n,\ \mathcal{N}_d(n-1) = 2n.$$

**Proof.** The least absolute value for the exponent is two, which corresponds to $n$ numbers of Hamming weight one. There are $n$ numbers with only one block of length two, whose absolute value for the exponent equals three, and $n$ numbers with only one pattern of 101, whose absolute value for the exponent is also equal to three. The $n$ numbers with weight $n-2$ have the absolute value for the exponent equal to $n$, as well as the $n$ numbers with weight $n-1$. □

The proof of the next preposition is straightforward.

**Proposition 2.** *Let $n > 4$. We have*

$$\mathcal{N}_l(1) = 0,\ \mathcal{N}_l(2) = 2n.$$

$$\mathcal{N}_l(r) = 0,\ r > \frac{n+2}{2}.$$

Table 2 presents $\mathcal{N}_l$ and $\mathcal{N}_d$ for $n = 16$.

**Remark 2.** *On the one hand, the discussions of this section, combined with other techniques and using suitable data structures, could improve linear and differential attacks on the SIMON family of block ciphers, as stated in Remark 1. On the other hand, these studies show why this family of ciphers is resistant to (classical?) linear and differential cryptanalysis: in fact, regarding Table 2, we see that the number of input differences and output masks with large differential probability or large squared correlation is small, compared to $2^n$.*

**Table 2.** Values of $\mathcal{N}_l$ and $\mathcal{N}_d$ for $n = 16$.

| **r** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
|---|---|---|---|---|---|---|---|---|
| $\mathcal{N}_d(r)$ | 0 | 16 | 32 | 152 | 432 | 1216 | 2960 | 6318 |
| $\mathcal{N}_l(r)$ | 0 | 32 | 416 | 2816 | 10,560 | 21,504 | 21,504 | 8192 |
| **r** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | |
| $\mathcal{N}_d(r)$ | 411,472 | 16,320 | 15,344 | 8344 | 2496 | 400 | 32 | |
| $\mathcal{N}_l(r)$ | 510 | 0 | 0 | 0 | 0 | 0 | 0 | |

## 4. Linear and Differential Properties of SPECK

In this section, based on the previous studies on linear and differential properties of the operation of addition mod $2^n$, the explicit formula for differential probabilities and linear biases of modular addition mod $2^n$, along with straightforward algorithms for finding the output masks with maximum squared correlation, given the input masks and the output differences with the maximum differential probability, given the input differences, are presented.

Let $a = (a_{n-1}, \ldots, a_1, a_0)$, $b = (b_{n-1}, \ldots, b_1, b_0)$, and $c = (c_{n-1}, \ldots, c_1, c_0)$ be the two input masks and the output mask for the operation of addition mod $2^n$, respectively. We wish to find $|\mathcal{P}(a \cdot x \oplus b \cdot y = c \cdot z) - \frac{1}{2}|$, where $z = x + y \mod 2^n$. Put:

$$\gamma_i = 4c_{n-i-1} + 2b_{n-i-1} + a_{n-i-1}, \ 0 \leq i < n.$$

The sequence $\gamma_i$ could be represented as a series of blocks $\mathcal{B}_i$, $1 \leq i \leq m$, for some $m$, where each $\mathcal{B}_i$ is an e-block (a block of symbols 3, 5, and 6), an o-block (a block of symbols 1, 2, and 4), a 0-block, or a 7-block. The number of symbols in a block $\mathcal{B}$ is denoted by $|\mathcal{B}|$, in the current paper. The following theorem, whose proof is illustrated in Figure 1, is proven in [24]. Start from the START state and traverse the diagram in Figure 1. If we are in State 0 and we see a symbol in $\{1,2,3,4,5,6\}$, then the correlation is zero. Otherwise, the absolute exponent for the bias is the number of times we see $w = w + 1$. Note that if this bias equals $2^{-t}$, then the squared correlation is equal to $2^{2-2t}$.

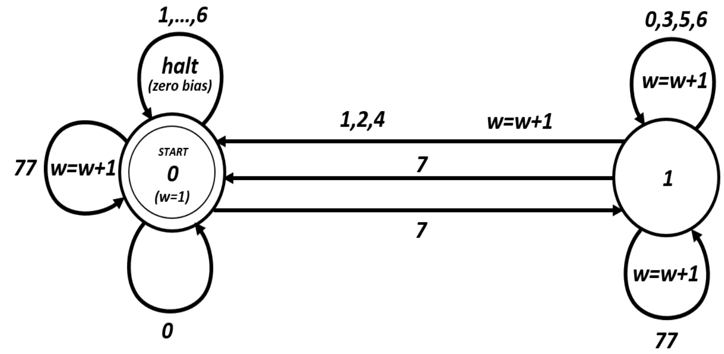

**Figure 1.** Linear biases of modular addition mod $2^n$.

**Theorem 5.** *With the notations as above, we have:*

$$|\mathcal{P}(a \cdot x \oplus b \cdot y = c \cdot z) - \frac{1}{2}| = \begin{cases} 2^s & \rho = 1, \\ \\ 0 & \rho = 0, \end{cases}$$

*where:*

$$s = \sum_{\mathcal{B}_i \in \mathbb{E} \cup \mathbb{O}} |\mathcal{B}_i| + \sum_{\mathcal{B}_i \in \mathbf{1}} \lfloor \frac{|\mathcal{B}_i|}{2} \rfloor + \sum_{\mathcal{B}_i \in \mathbf{0}} \rho_i |\mathcal{B}_i|,$$

*and* $\rho_1 = 0$, *and for* $1 < i \leq m$,

$$\rho_i = |\{j : 0 \leq j < i, \mathcal{B}_j \in \mathbb{O}\}| + |\{j : 0 \leq j < i, \mathcal{B}_j \in \mathbf{1}, |\mathcal{B}_j| = 1 \mod 2\}| \mod 2.$$

*Here,* $\mathbb{E}$ *stands for the set of all e-blocks,* $\mathbb{O}$ *stands for the set of all o-blocks,* $\mathbf{1}$ *denotes the set of all 7-blocks, and* $\mathbf{0}$ *represents the set of all 0-blocks.*

We have $\rho = 0$ if and only if there exists $1 \leq i \leq m$ such that $\rho_i = 0$ and $\mathcal{B}_i \in \mathbb{E} \cup \mathbb{O}$, and $\rho = 1$, otherwise. Note that, in any case, the absolute value for the exponent of any nonzero linear bias is greater than or equal to $\sum_{\mathcal{B}_i \in \mathbb{E} \cup \mathbb{O}} |\mathcal{B}_i| + \sum_{\mathcal{B}_i \in \mathbf{1}} \lfloor \frac{|\mathcal{B}_i|}{2} \rfloor$.

Suppose that $a = (a_{n-1}, \ldots, a_1, a_0)$, and $b = (b_{n-1}, \ldots, b_1, b_0)$, are the two input masks. Put:

$$\gamma_i = 2b_{n-i-1} + a_{n-i-1},\ 0 \leq i < n.$$

Clearly, $\gamma_i$ consists of 0-blocks, 3-blocks, and $\{1, 2\}$-blocks, i.e., blocks of Symbols 1 and 2. Now, regarding the diagram in Figure 1, we have the following straightforward algorithm for finding output masks with maximum correlation:

"Firstly, put $c_i = 0$ for every symbol in every 0-block, and $c_i = 1$, otherwise. Therefore, we have 0-blocks, 7-blocks, and e-blocks. Now, starting from the first block, for each series of consecutive 0-blocks and 7-blocks, put $c_i = 0$ for the last symbol in each 7-block of odd length, to make it of even length. For the last 7-block in this series of blocks, if it is of even length, make it of odd length by setting $c_i = 0$, for the last symbol in this 7-block. For each e-block, make the last symbol an o-block of length one by setting $c_i = 0$ for its corresponding symbol. Note that, if the first block which is always a 7-block is of length one, it could not be rendered an even block; so, if there is a series of 0-blocks and 7-blocks after this 7-block, then the first appearing 7-block should be made of odd length."

As an example, Let $n = 16$,

$$a = (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1),$$

$$b = (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1).$$

Then, an optimum output mask is $c = (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$.

Let $a = (a_{n-1}, \ldots, a_1, a_0)$, $b = (b_{n-1}, \ldots, b_1, b_0)$, and $c = (c_{n-1}, \ldots, c_1, c_0)$ be the two input differences and the output difference, respectively. We want to find:

$$\mathcal{P}((x + y) \oplus ((x \oplus a) + (y \oplus b)) = c).$$

Here, + stands for addition mod $2^n$. Put:

$$\gamma_i = 4c_{n-1-i} + 2b_{n-i-1} + a_{n-i-1},\ 0 \leq i < n.$$

The sequence $\gamma_i$ could be represented as a series of blocks $\mathcal{B}_i$, $1 \leq i \leq m$, for some $m$, where each $\mathcal{B}_i$ is an e-block, an o-block, a 0-block, or a 7-block. The next theorem is proven considering Figure 2. This picture is due to [18].

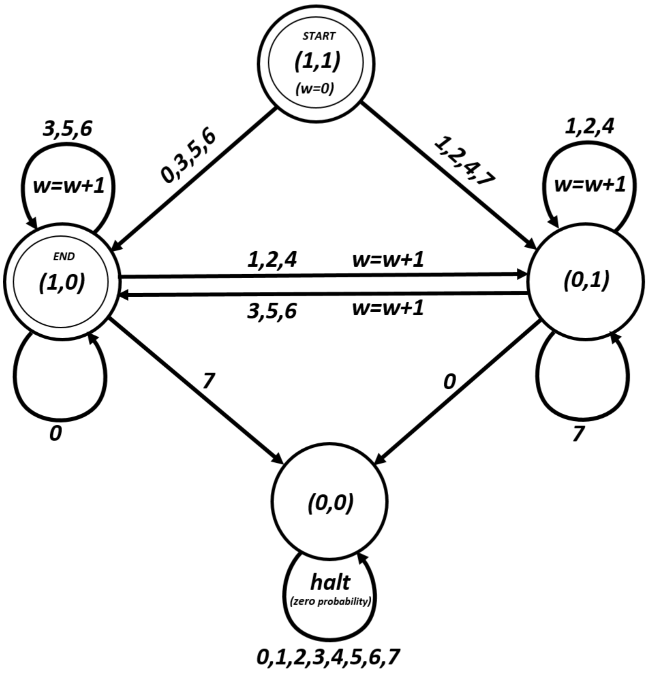

**Figure 2.** Differential probabilities of modular addition mod $2^n$.

**Theorem 6.** *With the notations as before, we have:*

$$\mathcal{P}((x+y)\oplus((x\oplus a)+(y\oplus b))=c)=\begin{cases}2^t & \alpha=1,\\ \\ 0 & \alpha=0,\end{cases}$$

*where:*

$$t=\sum_{\mathcal{B}_i\in\mathbb{E}\cup\mathbb{O}}|\mathcal{B}_i|,$$

*and $\alpha=0$ if and only if there exists an $0\le i<m$, such that $\mathcal{B}_i\in\mathbf{1}\cup\mathbb{O}$ and $\mathcal{B}_{i+1}\in\mathbf{1}$, or $\mathcal{B}_i\in\mathbf{1}\cup\mathbb{E}$ and $\mathcal{B}_{i+1}\in\mathbf{0}$, or when $\mathcal{B}_m\in\mathbb{O}\cup\mathbf{1}$; and $\alpha=1$, otherwise.*

The correctness of the following algorithm is justified considering Figure 2: note that the differential probability is zero if we end at states (1,0) or (0,0). The absolute value for the exponent is equal to the number of times we see $w=w+1$.

Suppose that $a=(a_{n-1},\dots,a_1,a_0)$ and $b=(b_{n-1},\dots,b_1,b_0)$ are the two input differences. Put:

$$\gamma_i=2b_{n-i-1}+a_{n-i-1},\ 0\le i<n.$$

Obviously, $\gamma_i$ consists of 0-blocks, 3-blocks, and $\{1,2\}$-blocks. Now, regarding the diagram in Figure 2, we have the following straightforward algorithm for finding output differences with maximum differential probability:

"If $\mathcal{B}_t$ is a 0-block and $\mathcal{B}_{t+1}$ is a $\{1,2\}$-block, for some $t$, then make this $\{1,2\}$-block an e-block, by setting $c_i=1$ for all the symbols in this block. If $\mathcal{B}_t$ is a 0-block and $\mathcal{B}_{t+1}$ is a 3-block, then make an o-block of length one, by setting $c_i=0$ for the last symbol in this 0-block. If $\mathcal{B}_t$ is a 3-block and $\mathcal{B}_{t+1}$ is a $\{1,2\}$-block, then make this $\{1,2\}$-block an o-block by setting $c_i=0$ for all the symbols in this block. If $\mathcal{B}_t$ is a 3-block and $\mathcal{B}_{t+1}$ is a 0-block, then make an e-block of length one, by setting $c_i=1$ for the last symbol in this 3-block. If $\mathcal{B}_t$ is an o-block and $\mathcal{B}_{t+1}$ is a 0-block, then make an e-block of length one by setting $c_i=1$ for the last symbol in this o-block. If $\mathcal{B}_t$ is an e-block and $\mathcal{B}_{t+1}$ is a 3-block, then make an o-block of length one by setting $c_i=0$ for the last symbol in this 0-block. Finally, if the last block is an o-block or a 3-block, make an e-block of length one by setting $c_i = 1$ for the last symbol in the o-block or setting $c_i = 0$ for the last symbol in the 3-block."

As an example, Let $n = 16$,

$$a = (1,1,1,1,1,0,0,0,0,0,1,1,0,0,0,0),$$

$$b = (0,0,1,0,0,0,0,0,1,1,1,0,0,0,0,0).$$

Then, an optimum output difference is $c = (1,1,1,0,1,0,0,0,1,0,1,0,0,0,0,0)$.

**Remark 3.** *Similar to the case of SIMON, the presented algorithms characterize optimum output masks (output differences) for given input masks (input differences) for the operation of addition mod* $2^n$*. Without the proposed algorithms, given any input differences or masks, we should search for desired admissible output differences or masks; but, with the aid of the proposed algorithms, we simply search within the set of optimum masks or differences. In the case of sparse masks or differences (the ones with a low Hamming weight), even a table could be saved to speed the search process. This way, the complexity of finding linear and differential characteristics could be reduced, significantly.*

**Remark 4.** *On the one hand, the studies of this section, combined with other methods and using suitable data structures, could reduce the complexity of linear and differential attacks on the SPECK family of block ciphers and speed up the search for finding the optimal differences or masks. On the other hand, they somehow show why this family of ciphers is resistant to (classic?) linear and differential cryptanalysis: Theorems 5 and 6 show that, whatever the two input masks and differences are, the absolute value in the exponent of nonzero differential probabilities and squared correlations could not be smaller than some lower bounds.*

## 5. Conclusions

SIMON and SPECK families of block ciphers are well-known lightweight ciphers, which have widely attracted the attention of researchers. In this note, based on the previous studies on SIMON, an explicit formula for the linear and differential probabilities of this family of ciphers is proposed. In the case of SPECK, as the only nonlinear operation in this family of ciphers is addition mod $2^n$, after reformulating the formula for squared correlations and differential probabilities of addition mod $2^n$, straightforward algorithms for finding the output masks with maximum squared correlation, given the input masks, as well as the output differences with the maximum differential probability, given the input differences, are presented.

The studies of the current paper, combined with other methods and using suitable data structures, could improve linear and differential cryptanalysis on the SIMON and SPECK families of block ciphers, as stated in Remarks 1 and 3. Besides, the investigations of this paper somehow show why these families of ciphers are resistant to classic linear and differential cryptanalysis.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The author declares no conflict of interest.

## References

1. Beaulieu, R.; Shors, D.; Smith, J.; Treatman-Clark, S.; Weeks, B.; Wingers, L. The SIMON and SPECK Families of Lightweight Block Ciphers. *IACR Cryptol. ePrint Arch.* **2013**, *2013*, 404.
2. Alizadeh, J.; AlKhzaimi, H.; Aref, M.R.; Bagheri, N.; Gauravaram, P.; Kumar, A.; Lauridsen, M.M.; Sanadhya, S.K. Cryptanalysis of SIMON Variants with Connections. In Proceedings of the International Workshop on Radio Frequency Identification: Security and Privacy Issues, Graz, Austria, 9–11 July 2013; pp. 90–107.
3. Abed, F.; List, E.; Lucks, S.; Wenzel, J. Differential Cryptanalysis of Round-Reduced Simon and Speck. In Proceedings of the International Conference on Fast Software Encryption, London, UK, 3–5 March 2014; pp. 525–545.

4. Biryukov, A.; Roy, A.; Velichkov, V. Differential Analysis of Block Ciphers SIMON and SPECK. In Proceedings of the International Conference on Fast Software Encryption, London, UK, 3–5 March 2014; pp. 546–570.
5. Dinur, I. Improved Differential Cryptanalysis of Round-Reduced Speck. In Proceedings of the International Workshop on Selected Areas in Cryptography, Montreal, QC, Canada, 14–15 August 2014; pp. 147–164.
6. Abdelraheem, M.A.; Alizadeh, J.; AlKhzaimi, H.A.; Aref, M.R.; Bagheri, N.; Gauravaram, P. Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48. In Proceedings of the International Conference in Cryptology in India, Bangalore, India, 6–9 December 2015; pp. 153–179.
7. Sun, S.; Hu, L.; Wang, M.; Wang, P.; Qiao, K.; Ma, X.; Shi, D.; Song, L.; Fu, K. Constructing Mixed-integer Programming Models whose Feasible Region is Exactly the Set of All Valid Differential Characteristics of SIMON. *IACR Cryptol. ePrint Arch.* **2015**, *2015*, 122.
8. Mourouzis, T.; Song, G.; Courtois, N.; Christofi, M. Advanced Differential Cryptanalysis of Reduced-Round SIMON64/128 Using Large-Round Statistical Distinguishers. *IACR Cryptol. ePrint Arch.* **2015**, *2015*, 481.
9. Chen, H.; Wang, X. Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-Guessing Techniques. In Proceedings of the International Conference on Fast Software Encryption, Bochum, Germany, 20–23 March 2016; pp. 428–449.
10. Ashur, T.; Rijmen, V. On Linear Hulls and Trails in Simon. *IACR Cryptol. ePrint Arch.* **2016**, *2016*, 88.
11. Liu, Y.; Fu, K.; Wang, W.; Sun, L.; Wang, M. Linear cryptanalysis of reduced-round SPECK. *Inf. Process. Lett.* **2016**, *116*, 259–266. [CrossRef]
12. Shi, D.; Hu, L.; Sun, S.; Song, L.; Qiao, K.; Ma, X. Improved linear (hull) cryptanalysis of round-reduced versions of SIMON. *Sci. China Inf. Sci.* **2017**, *60*, 1–3. [CrossRef]
13. Wang, N.; Wang, X.; Jia, K.; Zhao, J. Differential attacks on reduced SIMON versions with dynamic key-guessing techniques. *Sci. China Inf. Sci.* **2018**, *61*, 1–3. [CrossRef]
14. Dwivedi, A.D.; Morawiecki, P. Differential cryptanalysis in ARX ciphers, Application to SPECK. *IACR Cryptol. ePrint Arch.* **2018**, *2018*, 899.
15. Kölbl, S.; Leander, G.; Tiessen, T. Observations on the SIMON block cipher family. *IACR Cryptol. ePrint Arch.* **2015**, *2015*, 145.
16. Kölbl, S.; Leander, G.; Tiessen, T. Observations on the SIMON block cipher family. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015; pp. 161–185.
17. Beierle, C. Pen and Paper Arguments for SIMON and SIMON-like Designs. In Proceedings of the International Conference on Security and Cryptography for Networks, Amalfi, Italy, 31 August–2 September 2016; pp. 431–446.
18. Ashur, T.; Liu, Y. On Rotational Cryptanalysis in the Presence of Constants. *IACR Trans. Symmetric Cryptol.* **2016**, *2016*, 57–70.
19. Liu, Z.; Li, Y.; Wang, M. Optimal Differential Trails in SIMON-like Ciphers. *IACR Trans. Symmetric Cryptol.* **2017**, *2017*, 358–379.
20. Liu, Z.; Li, Y.; Wang, M. The Security of SIMON-like Ciphers Against Linear Cryptanalysis. *IACR Cryptol. ePrint Arch.* **2017**, *2017*, 576.
21. Wallén, J. Linear Approximations of Addition Modulo $2^n$. In Proceedings of the International Conference on Fast Software Encryption, Lund, Sweden, 24–26 February 2003; pp. 261–273.
22. Nyberg, K.; Wallén, J. Improved Linear Distinguishers for SNOW 2. In Proceedings of the International Conference on Fast Software Encryption, Graz, Austria, 15–17 March 2006; pp. 144–162.
23. Schulte-Geers, E. On CCZ-equivalence of addition mod $2^n$. *Des. Codes Cryptogr.* **2013**, *66*, 111–127. [CrossRef]
24. Dehnavi, S.M.; Rishakani, A.M.; Shamsabad, M.R.M. A More Explicit Formula for Linear Probabilities of Modular Addition Modulo a Power of Two. *IACR Cryptol. ePrint Arch.* **2015**, *2015*, 26.