A New Classification of 4-bit Optimal S-boxes and its Application to PRESENT, RECTANGLE and SPONGENT

Wentao Zhang[1], Zhenzhen Bao[1], Vincent Rijmen[2], Meicheng Liu[1]

1.State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2.KU Leuven, Dept. of Electrical Engineering ESAT/COSIC and iMinds, Security Dept.
{*zhangwentao, baozhenzhen, liumeicheng*}*@iie.ac.cn*
{*vincent.rijmen*}*@esat.kuleuven.be*

Abstract. In this paper, we present a new classification of 4-bit optimal S-boxes. All optimal 4-bit S-boxes can be classified into 183 different categories, among which we specify 3 platinum categories. Under the design criteria of the PRESENT (or SPONGENT) S-box, there are 8064 different S-boxes up to adding constants before and after an S-box. The 8064 S-boxes belong to 3 different categories, we show that the S-box should be chosen from one out of the 3 categories or other categories for better resistance against linear cryptanalysis. Furthermore, we study in detail how the S-boxes in the 3 platinum categories influence the security of PRESENT, RECTANGLE and SPONGENT$_{88}$ against differential and linear cryptanalysis. Our results show that the S-box selection has a great influence on the security of the schemes. For block ciphers or hash functions with 4-bit S-boxes as confusion layers and bit permutations as diffusion layers, designers can extend the range of S-box selection to the 3 platinum categories and select their S-box very carefully. For PRESENT, RECTANGLE and SPONGENT$_{88}$ respectively, we get a set of potentially best/better S-box candidates from the 3 platinum categories. These potentially best/better S-boxes can be further investigated to see if they can be used to improve the security-performance tradeoff of the 3 cryptographic algorithms.

Key words: 4-bit S-box, classification, block cipher, hash function, differential cryptanalysis, linear cryptanalysis, PRESENT, RECTANGLE, SPONGENT

1 Introduction

S-boxes are widely used in modern block ciphers and hash functions. Substitution-Permutation (SP) and Feistel network are the most common structures. In these structures, S-boxes are usually the only non-linear part. Therefore, S-boxes have to be chosen carefully to optimize the security-performance tradeoff. The most common sizes of S-boxes are 8-bit and 4-bit. AES [15] uses an 8-bit S-box, which has influenced many subsequent ciphers; while Serpent [2] and NOEKEON [14] use 4-bit S-boxes. In the past few years, as the need for security in RFID and sensor networks is dramatically increasing, many lightweight constructions have been proposed. Since a 4-bit S-box is usually much more compact in hardware than an 8-bit S-box, many lightweight

block ciphers and hash functions use 4-bit S-boxes, such as LED [17], PHOTON [18], PRESENT [10], RECTANGLE [31] and SPONGENT [8].

For 4-bit S-boxes, the optimal values are known with respect to differential and linear cryptanalysis, an S-box attaining these optimal values is called an optimal S-box. In [21], Leander et al. classified all optimal 4-bit S-boxes into 16 affine equivalences; this result can be used to efficiently generate optimal S-boxes fulfilling additional criteria. However, for many constructions, the design criterion of being an optimal S-box is not enough, there are other important properties the designers should take into account. For example, the design criteria of the Serpent S-box require that a 1-bit input difference must cause an output difference of at least two bits.

Given an S-box S, let $CarD1_S$ denote the number of times that a 1-bit input difference causes a 1-bit output difference, and $CarL1_S$ the number of times that a 1-bit input selection pattern causes a 1-bit output selection pattern. We refer to Section 2.1 for a precise definition of $CarD1_S$ and $CarL1_S$. For the PRESENT S-box, $CarD1_S = 0$ and $CarL1_S = 8$. In [25], linear hulls were used to mount an attack on 25-round PRESENT. Later, a multidimensional linear attack on 26-round PRESENT was given in [12], which is the best shortcut attack on PRESENT so far. Both of the above attacks use the fact that the value of $CarL1_S$ of the PRESENT S-box is relatively high, i.e., $CarL1_S = 8$, which leads to a significant clustering of linear trails. For comparison, the value of $CarD1_S$ of the PRESENT S-box is zero, the best shortcut differential attack on PRESENT only reaches 18 rounds [29]. It can be seen that, with respect to security margin, there is a big gap between differential cryptanalysis and linear cryptanalysis on PRESENT. More recently, Blondeau and Nyberg [7] showed that there exists a chosen-plaintext truncated differential attack for any known-plaintext multidimensional linear attack, hence, they have successfully derived a truncated differential attack on 26-round PRESENT from the multidimensional linear attack on 26-round PRESENT [12]. From this result, we can learn that a block cipher had better have almost the same security margin against differential-like attacks and linear-like attacks. Now, the questions come up. Is there any optimal S-box satisfying $CarD1_S = 0$ and $CarL1_S = 0$? Is there a better S-box for PRESENT with respect to the security against differential and linear cryptanalysis? These questions are part of motivation of this paper.

SPONGENT is a family of lightweight hash functions based on PRESENT. The internal permutation of each variant uses SP-network with 4-bit S-boxes and a bit permutation. For the SPONGENT S-box, $CarD1_S = 0$ and $CarL1_S = 4$. RECTANGLE is designed with bit-slice technique. RECTANGLE also uses SP-network with 4-bit S-boxes and a bit permutation. For the RECTANGLE S-box, $CarD1_S = 2$ and $CarL1_S = 2$. Then, one may wonder if the security margin of PRESENT can be improved when replacing its S-box by the SPONGENT or RECTANGLE S-box. Moreover, is the S-box selection of SPONGENT and RECTANGLE optimal with respect to differential and linear cryptanalysis? In this paper, we will partly answer these questions.

1.1 Contributions

In Section 3 of this paper, we firstly prove that $CarL1_S \geq 2$ for any optimal S-box. Moreover, if $CarL1_S = 2$, then the S-box must be in 4 (out of 16) affine equivalent classes; if $CarL1_S = 3$, then the S-box must be in 8 (out of 16) affine equivalent classes.

We call the subset of optimal S-boxes with the same values of $CarD1_S$ and $CarL1_S$ a Num1-DL category. We show that all optimal 4-bit S-boxes can be classified into 183 different Num1-DL categories. Among all the 183 Num1-DL categories, there are 3 categories with the minimal value of $CarD1_S + CarL1_S$, we call the 3 categories platinum Num1-DL categories.

There are 4 measures to evaluate the security of a cipher against differential and linear cryptanalysis. In Section 4, we give a brief discussion on the 4 measures, and show why it is appropriate to use the heuristic measure for the study in this paper.

In Section 5, we consider PRESENT and 5 variants of SPONGENT. There are 8064 S-boxes (up to adding constants before and after an S-box, similarly hereinafter) satisfying the design criteria of the PRESENT (or SPONGENT) S-box. The 8064 S-boxes belong to 3 different categories. We show that, for each of the 6 fixed permutation layers, if the S-box comes from 2 out of the 3 categories, then there exists a linear trail with only one active S-box in each round. Hence, for SP-network schemes with the PRESENT or SPONGENT permutation layer, for better resistance against linear cryptanalysis, the S-box should be chosen from 1 out of the 3 categories or other categories.

In Section 6, we investigate how the S-boxes in the 3 platinum Num1-DL categories influence the security of PRESENT, RECTANGLE and SPONGENT against differential and linear cryptanalysis. We focus on 64- and 88-bit block length. Consider the following SP-network schemes. For 64-bit block length, the S-box is chosen from the 3 platinum Num1-DL categories, the diffusion layer is either the PRESENT permutation or the RECTANGLE permutation. Thus, there are 6 combinations. Similarly, for 88-bit block length, there are also 6 combinations. For each of these 12 combinations, we use the heuristic measure to evaluate which are the best possible S-box candidates. Our results show that the S-box selection has a significant influence on the security of the 3 primitives. For PRESENT, there are 336 potentially best S-boxes, which does not include the PRESENT S-box. For RECTANGLE, there are 128 potentially best S-boxes, which includes the RECTANGLE S-box. For SPONGENT_{88}, we present 4 potentially better S-boxes when considering differential cryptanalysis more important than linear cryptanalysis. We want to point out that these results do not mean any security weakness of PRESENT, RECTANGLE or SPONGENT. However, these results show that there are potentially better S-box selections for PRESENT and SPONGENT, which means, by choosing another S-box, it is possible to improve the hardware/software performance of PRESENT and SPONGENT with a fixed level of security margin. Since any platinum Num1-DL category is not always the best choice, we suggest that designers can extend the range of the S-box selection to the 3 platinum Num1-DL categories and select their S-box carefully, when designing a block cipher or a hash function using 4-bit S-boxes as confusion layer and a bit permutation as diffusion layer.

2 Preliminaries

2.1 Optimal S-box, Affine and PE Equivalence, m-resilient Boolean Function

Given an S-box mapping n bits to m bits $S : F_2^n \to F_2^m$, we call S an $n \times m$ S-box. In this paper, we only concentrate on 4×4 S-boxes.

Let S denote a 4×4 bijective S-box. Let $\triangle I, \triangle O \in F_2^4$, define $ND_S(\triangle I, \triangle O)$ as:

$$ND_S(\triangle I, \triangle O) = \sharp\{x \in F_2^4 | S(x) \oplus S(x \oplus \triangle I) = \triangle O\}.$$

Let $\Gamma I, \Gamma O \in F_2^4$, define the imbalance $Imb_S(\Gamma I, \Gamma O)$ as:

$$Imb_S(\Gamma I, \Gamma O) = |\sharp\{x \in F_2^4 | \Gamma I \cdot x = \Gamma O \cdot S(x)\} - 8|.$$

where "$\cdot$" denotes the inner product on F_2^4.

Define the differential-uniformity of S as:

$$Diff(S) = \max_{\triangle I \neq 0, \triangle O} ND_S(\triangle I, \triangle O)$$

Define the linearity of S as:

$$Lin(S) = \max_{\Gamma I, \Gamma O \neq 0} Imb_S(\Gamma I, \Gamma O)$$

For any bijective 4×4 S-box, $Diff(S) \geq 4$ and $Lin(S) \geq 4$ [21]. An S-box attaining these minima is called an optimal S-box.

Definition 1 ([21]). *Let S be a 4×4 S-box. S is called an **optimal S-box** if it satisfies the 3 conditions:*

1. *S is bijective, i.e., $S(x) \neq S(x')$ for any $x \neq x'$.*
2. *$Diff(S) = 4$.*
3. *$Lin(S) = 4$.*

Let $wt(x)$ denote the Hamming weight of a binary vector x. Define $SetD1_S$ [31] as:

$$SetD1_S = \{(\triangle I, \triangle O) \in F_2^4 \times F_2^4 | wt(\triangle I) = wt(\triangle O) = 1 \text{ and } ND_S(\triangle I, \triangle O) \neq 0\}.$$

Define $SetL1_S$ [31] as:

$$SetL1_S = \{(\Gamma I, \Gamma O) \in F_2^4 \times F_2^4 | wt(\Gamma I) = wt(\Gamma O) = 1 \text{ and } Imb_S(\Gamma I, \Gamma O) \neq 0\}.$$

Let $CarD1_S$ denote the cardinality of $SetD1_S$, and $CarL1_S$ the cardinality of $SetL1_S$.

Definition 2 ([21]). *Two S-boxes S and S' are called **affine equivalent** if there exist two invertible 4×4 matrices A, B over F_2, and constants $a, b \in F_2^4$ such that $S'(x) = B(S(A(x) \oplus a)) \oplus b$.*

Given an S-box S, the values of $Diff(S)$ and $Lin(S)$ both remain unchanged when applying an affine transformation in the domain or co-domain of S [11, 24].

Theorem 1 ([21]). *Let S and S' be two affine equivalent S-boxes. If S is an optimal S-box, then S' is an optimal S-box as well.*

According to Theorem 1, all optimal S-boxes can be divided into equivalence classes using affine equivalence relation. All 4×4 optimal S-boxes can be split into only 16 affine equivalence classes [21]. Let $\{G_i, 0 \leq i \leq 15\}$ denote the representatives for the 16 equivalence classes, we refer to [21] for the 16 representatives.

Table 1. ([21]) Number of $b \in F_2^4 \setminus \{0\}$ such that $deg(S_b) = 2,3$

S-box	G_0	G_1	G_2	G_3	G_4	G_5	G_6	G_7	G_8	G_9	G_{10}	G_{11}	G_{12}	G_{13}	G_{14}	G_{15}
$deg(S_b) = 2$	3	3	3	0	0	0	0	0	3	1	1	0	0	0	1	1
$deg(S_b) = 3$	12	12	12	15	15	15	15	15	12	14	14	15	15	15	14	14

Definition 3 ([21]). *Two S-boxes S and S' are called **permutation-then-XOR equivalent** if there exist two 4×4 permutation matrices P_0, P_1 over F_2, and constants $a, b \in F_2^4$ such that $S'(x) = P_1(S(P_0(x) \oplus a)) \oplus b$. The equivalence is called **PE equivalence**.*

Note that if two S-boxes are PE equivalent, then they must be affine equivalent.

Definition 4. *Let f be a Boolean function $f : F_2^n \to F_2$, define the Walsh Coefficient of f at a as:*

$$f^W(a) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus a \cdot x}.$$

An n-variable Boolean function f is balanced if its output in the truth table contains equal number of 0 and 1. f is balanced if and only if $f^W(0) = 0$.

Definition 5 ([30]). *A Boolean function f is m-resilient if and only if its Walsh Coefficient satisfy $f^W(a) = 0$ for any $0 \leq wt(a) \leq m$.*

For any $b \in F_2^4$, define the corresponding component Boolean function S_b of an S-box S as:

$$S_b : F_2^4 \to F_2,\ S_b(x) = b \cdot S(x).$$

Let $deg(f)$ denote the algebraic degree of the Boolean function f, the algebraic degree is invariant under affine equivalence. Table 1 [21] gives the number of $b \in F_2^4 \setminus \{0\}$ such that $deg(S_b) = 2,3$ for the 16 representative optimal S-boxes.

2.2 Differential Trail, Difference Propagation, Linear Trail and Linear Propagation

Differential cryptanalysis (DC) [5] and linear cryptanalysis (LC) [22] are among the most powerful techniques available for block ciphers. Let β be a Boolean transformation operating on n-bit vectors that is a sequence of r transformations:

$$\beta = \rho^{(r)} \circ \rho^{(r-1)} \circ \cdots \circ \rho^{(2)} \circ \rho^{(1)}.$$

In this paper, β refers to a key-alternating block cipher [15] or a permutation of a hash function, the round keys (or constants) are added to the state by means of an XOR. Thus, a difference is referred to as an XOR.

A *differential trail* [15] Q over an iterative transformation consists of a sequence of $r+1$ difference patterns:

$$Q = (q^{(0)}, q^{(1)}, q^{(2)}, \cdots, q^{(r-1)}, q^{(r)}).$$

The probability of a differential step is defined as:

$$Prob(q^{(i-1)}, q^{(i)}) = 2^{-n} \times \sharp\{x \in F_2^n | \rho^{(i)}(x) \oplus \rho^{(i)}(x \oplus q^{(i-1)}) = q^{(i)}\}.$$

Assuming the independence of different steps, the probability of a differential trail Q can be approximated as:

$$Prob(Q) = \prod_i Prob(q^{(i-1)}, q^{(i)}).$$

A *difference propagation* [15] is composed of a set of differential trails, the probability of a difference propagation (a', b') is the sum of the probabilities of all r-round differential trails Q with initial difference a' and terminal difference b':

$$Prob(a', b') = \sum_{q^{(0)}=a', q^{(r)}=b'} Prob(Q) \tag{1}$$

The correlation $C(f,g)$ between two binary Boolean functions $f(a)$ and $g(a)$ is defined as:

$$C(f,g) = 2 \times Prob(f(a) = g(a)) - 1.$$

A *linear trail* [15] U over an iterative transformation consists of a sequence of $r+1$ selection patterns (also known as linear mask):

$$U = (u^{(0)}, u^{(1)}, u^{(2)}, \cdots, u^{(r-1)}, u^{(r)}).$$

The *correlation contribution* [15] of a linear trail is the product of the correlation of all its steps:

$$Cor(U) = \prod_i C(u^{(i)} \cdot \rho^{(i)}(a), u^{(i-1)} \cdot a). \tag{2}$$

A *linear propagation* is composed of a set of linear trails, the correlation of a linear propagation (u, w) is the sum of the correlation contributions of all r-round linear trails U with initial selection pattern w and final selection pattern u :

$$Cor(u, w) = \sum_{u^{(0)}=w, u^{(r)}=u} Cor(U). \tag{3}$$

The square of a correlation (contribution) is called correlation potential. The following theorem gives the expected value of the correlation potential $Cor(u, w)^2$ over all possible values of the expanded key.

Theorem 2 ([15]). *The average correlation potential between an input and an output selection pattern is the sum of the correlation potentials of all linear trails between the input and output selection patterns:*

$$E({Cor_t}^2) = \sum_i (Cor_i)^2 \tag{4}$$

where Cor_t is the overall correlation, and Cor_i the correlation contribution of a linear trail.

To attack a b-bit block cipher using DC, there must be a predictable difference propagation over all but a few rounds with a probability significantly larger than 2^{-b}. To attack a b-bit block cipher using LC, there must be a predictable linear propagation over all but a few rounds with a correlation potential significantly larger than 2^{-b}.

2.3 An Extension of RECTANGLE - RECTANGLE$_{88}$

Based on the design criteria of RECTANGLE, we present an extension of RECTANGLE to 88-bit block length, denoted as RECTANGLE$_{88}$. A 88-bit cipher state is pictured as a 4×22 rectangular array of bits. The *SubColumn* is 22 parallel applications of S-boxes to the 22 columns. The $ShiftRow$ step is defined as follows: row 0 is not rotated, row 1 is left rotated over 1 bit, row 2 is left rotated over 8 bits, row 3 is left rotated over 17 bits.

3 A New Classification of 4-bit S-boxes

The subset of 4×4 optimal S-boxes with the same values of $CarD1_S$ and $CarL1_S$ is called a category, the following is a formal definition.

Definition 6. *An (nd, nl)-**Num1-DL category** is defined as a subset of all 4×4 optimal S-boxes which satisfy $CarD1_S = nd$ and $CarL1_S = nl$. The category is also called a **Num1-DL category** for short.*

We are especially interested in those categories with low $CarD1_S$ and low $CarL1_S$. It can be easily seen that $0 \leq CarD1_S \leq 16$ and $0 \leq CarL1_S \leq 16$.

Theorem 3. *Let S denote an optimal S-box, then $CarL1_S \geq 2$. In other words, there does not exist an optimal S-box with $CarL1_S = 0$ or $CarL1_S = 1$.*

Proof: Let $x = (x_3, x_2, x_1, x_0)$ and $S(x) = (f_3(x), f_2(x), f_1(x), f_0(x))$, where x_i is the i-th bit of x, and $f_j(x)$ the j-th bit of $S(x)$. Since S is bijective, each Boolean function f_j $(0 \leq j \leq 3))$ is balanced.

Firstly, we show that there exist at least 2 Boolean functions f_{j_1} and f_{j_2} $(0 \leq j_1, j_2 \leq 3)$ with algebraic degree 3, equivalently speaking, there exist at most 2 Boolean functions with algebraic degree less than 3. Proof by contradiction. Assume that there exist 3 (or 4) out of the 4 Boolean functions f_j $(j = 0, 1, 2, 3)$ with algebraic degree less than 3. Then, for each of the 7 (or 15) non-zero linear combinations of these 3 (or 4) functions, the algebraic degree is also less than 3. However, according to Table 1, for any optimal S-box, there are at most 3 out of the 15 component functions with algebraic degree less than 3, which is a contradiction.

According to Siegenthaler's inequality [28], an n-variable Boolean function with degree $n-1$ is not 1-resilient. Particularly, if the degree of f_j is 3, then there exists $0 \leq i \leq 3$ such that $f_j(x) \oplus x_i$ is not balanced, which means that $(2^i, 2^j) \in SetL1_S$. Since there exist at least 2 functions f_{j_1} and f_{j_2} with algebraic degree 3, we can get that there are at least 2 elements in $SetL1_S$, i.e., $CarL1_S \geq 2$. □

Similar to the proof of Theorem 3, we can prove the following 2 theorems.

Theorem 4. *Let S denote an optimal S-box. If S is affine equivalent to G_9, G_{10}, G_{14} or G_{15}, then $CarL1_S \geq 3$.*

Theorem 5. *Let S denote an optimal S-box. If S is affine equivalent to $G_3, G_4, G_5, G_6, G_7, G_{11}, G_{12}$ or G_{13}, then $CarL1_S \geq 4$.*

According to Theorem 4 and 5, we can get the following corollary.

Corollary 1. *If $CarL1_S = 2$, then S is in the 4 affine equivalence classes corresponding to G_0, G_1, G_2 and G_8; if $CarL1_S = 3$, then S is in the 8 affine equivalence classes corresponding to $G_0, G_1, G_2, G_8, G_9, G_{10}, G_{14}$ and G_{15}.*

Corollary 1 indicates that we can restrict the search of S-boxes with $CarL1_S = 2$ (or $CarL1_S = 3$) within the 4 (or 8) affine equivalence classes. In the following, we present an efficient way which can experimentally classify all 4×4 optimal S-boxes into different categories.

The values of $CarD1_S$ and $CarL1_S$ are not generally invariant under the affine equivalence relation, but the two values are invariant under the PE equivalence relation.

Theorem 6. *Let S and S' be two PE equivalent S-boxes, then $CarD1_S = CarD1_{S'}$ and $CarL1_S = CarL1_{S'}$.*

Every 4×4 optimal S-box can be written as $B(G_i(A(x) \oplus a)) \oplus b$, where G_i ($0 \leq i \leq 15$) is the representative S-box, A and B are two invertible 4×4 matrices over F_2, a and b are two constants over F_2^4. The number of 4×4 invertible matrices is $\prod_{i=0}^{3}(2^4 - 2^i) = 20160$. At the first sight, up to adding constants, we need to consider $16 \times 20160 \times 20160 \approx 2^{32.6}$ S-boxes. However, this number can be decreased greatly.

Lemma 1. *Let M denote a 4×4 matrix over F_2:*

$$M = \begin{pmatrix} a_{03} & a_{02} & a_{01} & a_{00} \\ a_{13} & a_{12} & a_{11} & a_{10} \\ a_{23} & a_{22} & a_{21} & a_{20} \\ a_{33} & a_{32} & a_{31} & a_{30} \end{pmatrix}$$

where $a_{ij} \in F_2$, $0 \leq i, j \leq 3$. Let $r_i = a_{i3}||a_{i2}||a_{i1}||a_{i0}$ denote the nibble consisting of the 4 bits in the i-th row, a_{i0} is the least significant bit. There are 840 matrices satisfying the following 2 conditions:

1. *invertible.*
2. *$r_0 < r_1 < r_2 < r_3$.*

we call such a matrix a row-increasing matrix.

Proof: Given a 4×4 invertible matrix, there are 24 different matrices obtained by permuting the 4 rows. Among the 24 matrices, only one matrix satisfies $r_0 < r_1 < r_2 < r_3$. Hence there are $20160/24 = 840$ invertible row-increasing matrices. □

According to Lemma 1, every 4×4 optimal S-box is PE equivalent to an S-box with the form $M_1(G_i(M_0^T(x)))$, $0 \leq i \leq 15$, M_0 and M_1 are two row-increasing matrices. Hence, up to PE equivalence, we only need to consider $16 \times 840 \times 840 = 11289600 \approx 2^{23.43}$ S-boxes. By exhaustively checking all the 11289600 S-boxes, we have the following result.

Result 1 *All optimal* 4×4 *S-boxes can be split into 183 different Num1-DL categories. Table 2 gives the details, the symbol "✓" at position* (i,j) *means that there exist optimal S-boxes satisfying* $CarD1_S = i$ *and* $CarL1_S = j$*. From Table 2, the following facts are of interest:*

1. *No Num1-DL category satisfies that* $CarL1_S = 0$ *or* $CarL1_S = 1$.

2. *The minimal possible value for* $CarD1_S$ *is 0. When* $CarD1_S = 0$*, the minimal possible value for* $CarL1_S$ *is 4, i.e., the* $(0,4)$*-Num1-DL category.*

3. *The minimal possible value for* $CarL1_S$ *is 2. When* $CarL1_S = 2$*, the minimal possible value for* $CarD1_S$ *is 2, i.e., the* $(2,2)$*-Num1-DL category.*

Note that the first fact in Result 1 is in accordance with Theorem 3. For each Num1-DL category satisfying $CarD1_S + CarL1_S \leq 8$, by checking all the S-boxes (out of 11289600 S-boxes) in this category, we get the following result.

Result 2 *There are 24 Num1-DL categories satisfying* $CarD1_S + CarL1_S \leq 8$*. Table 3 gives the number of PE classes for each of the 24 Num1-DL categories. Moreover, we have the following facts:*

1. *Consider the sum of the values in row 0, there are 20 PE classes satisfying* $CarD1_S = 0$.

2. *Restricting* $CarD1_S + CarL1_S \leq 4$*, there are 3 Num1-DL categories:* $(0,4)$*-,* $(1,3)$*-,* $(2,2)$*-Num1-DL category. We call these 3 categories* ***platinum Num1-DL categories****. Table 4 lists representative S-boxes for each PE class in each of the 3 platinum Num1-DL categories.*

Generally, the S-boxes in a Num1-DL category belong to many affine equivalence classes. For example, (0,8)-Num1-DL category includes 8 PE classes, and the 8 PE classes belong to 5 affine equivalence classes. In Result 2, the first fact is in accordance

Table 2. 183 Num1-DL Categories: marked by ✓

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0					✓	✓	✓	✓	✓								
1				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
2			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
3			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
4			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
7				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
10					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
11					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
12							✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
13								✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
14										✓	✓	✓	✓	✓	✓	✓	✓
15															✓	✓	
16																	

Notes: the leftmost column denotes the 17 possible values of $CarD1_S$
the uppermost row denotes the 17 possible values of $CarL1_S$

Table 3. Number of PE Classes in the 24 Num1-DL Categories satisfying $CarD1_S + CarL1_S \leq 8$

	0	1	2	3	4	5	6	7	8
0					2	2	6	2	8
1				4	26	50	112	113	–
2			4	54	155	290	648	–	–
3			10	116	593	1445	–	–	–
4			9	168	1141	–	–	–	–
5			5	146	–	–	–	–	–

Notes: the leftmost column denotes the possible values of $CarD1_S$
the uppermost row denotes the possible values of $CarL1_S$
"–" denotes the class does not satisfy $CarD1_S + CarL1_S \leq 8$

Table 4. Representative S-boxes for the 3 platinum Num1-DL categories

$(0,4)$-Num1-DL category	0, 11, 12, 5, 6, 1, 9, 10, 3, 14, 15, 8, 13, 4, 2, 7
	0, 12, 13, 10, 5, 11, 14, 7, 15, 6, 2, 1, 3, 8, 9, 4
$(1,3)$-Num1-DL category	0, 12, 9, 7 ,6, 1, 15, 2, 3, 11, 4, 14, 13, 8, 10, 5
	0, 12, 9, 7, 15, 2, 6, 1, 3, 11, 4, 14, 10, 5, 13, 8
	0, 11, 8, 5, 15, 12, 3, 6, 14, 4, 7, 9, 2, 1, 13, 10
	0, 13, 4, 11, 7, 14, 9, 2, 6, 10, 3, 5, 8, 1, 15, 12
$(2,2)$-Num1-DL category	0, 13, 8, 2, 14, 11, 7, 5, 15, 6, 3, 12, 4, 1, 9, 10
	0, 11, 14, 1, 10, 7, 13, 4, 6, 12, 9, 15, 5, 8, 3, 2
	0, 11, 6, 9, 12, 5, 3, 14, 13, 7, 8, 4, 2, 10, 15, 1
	0, 14, 9, 5, 15, 8, 10, 7, 3, 11, 6, 12, 4, 1, 13, 2

Note: In each row, the first integer represents the image of 0, the second the image of 1, and so on.

with Fact 4 in [21]. For the $(2,2)$-Num1-DL category, the 4 representative S-boxes are respectively PE equivalent to the 4 representative S-boxes given in [31].

4 Measures for Evaluating the Security against DC and LC

Kanda et al. [19] classified 4 measures to evaluate the security of a cipher against DC and LC as follows:

1. Precise measure: The maximum probability of difference propagations, and the maximum average correlation potential of linear propagations.
2. Theoretical measure: The upper bound of the maximum probability of difference propagations, and the upper bound of the maximum average correlation potential of linear propagations.
3. Heuristic measure: The maximum probability of differential trails, and the maximum correlation potential of linear trails.
4. Practical measure: The upper bound of the maximum probability of differential trails, and the upper bound of the maximum correlation potential of linear trails.

For many modern ciphers, such as AES and Serpent, it is almost computationally infeasible to perform an evaluation using the precise measure or the theoretical measure. For ciphers with good diffusion, such as Serpent [2], the heuristic measure is only effective for a small number of rounds. On the other hand, many ciphers evaluated with the practical measure are practically secure against DC and LC, such as AES and NOEKEON, hence the practical measure is the most common measure.

However, compared with the practical measure, the heuristic measure is more accurate. If the heuristic measure is feasible for a cipher, then both the cryptanalysts and designers can have a better understanding on the security of the cipher against DC and LC. Particularly, for PRESENT, RECTANGLE and SPONGENT, the heuristic measure is feasible, we will discuss this problem in Section 6.2.

Consider the following SP-network schemes. Fix the permutation layer of PRESENT, RECTANGLE or SPONGENT, the S-box can have many different choices. Then, for each scheme, we wonder which S-boxes are the best with respect to DC and LC? In this paper, we mainly concentrate on S-boxes in the 3 platinum Num1-DL categories. In Section 5 and Section 6, we adopt the heuristic measure for the study. One may say that, for such schemes, the clustering of differential/linear trails must not be neglected [6, 12, 25, 29, 31], hence it needs to use the precise (or the theoretical) measure. However, we think that it is still appropriate to use the heuristic measure for the study. The following gives the reasons.

The total number of schemes investigated in this paper is 4368 (see Table 5), it needs an extremely huge computational effort to evaluate the clustering of differential/linear trails for all the schemes investigated in this paper.

Let rD_p denote the highest number of rounds of an exploitable differential distinguisher by using the precise measure, and rL_p the highest number of rounds of an exploitable linear distinguisher by using the precise measure, define $r_p \equiv \max\{rD_p, rL_p\}$. For a fixed permutation, among all the S-box candidates, the smaller the value of r_p, the better the scheme, because schemes with the minimal r_p need the least number of rounds to resist against DC and LC. Let rD_h denote the highest number of rounds of an exploitable differential distinguisher by using the heuristic measure, and rL_h the highest number of rounds of an exploitable linear distinguisher by using the heuristic measure, define $r_h \equiv \max\{rD_h, rL_h\}$. Based on equations (1) and (4), we have $rD_p \geq rD_h$ and $rL_p \geq rL_h$, thus $r_p \geq r_h$. The smaller the value of $rD_p - rD_h$ ($rL_p - rL_h$), the less the clustering of differential (linear) trails. Based on the known results on PRESENT, RECTANGLE and SPONGENT [1, 6, 12, 25, 29, 31], the difference $rD_p - rD_h$ (or $rL_p - rL_h$) between the two measures are as follows: For PRESENT against DC, the difference is $16 - 14 = 2$; for PRESENT against LC, the difference is $24 - 16 = 8$. For RECTANGLE against DC, the difference is $14 - 14 = 0$; for RECTANGLE against LC, the difference is $14 - 13 = 1$. For SPONGENT$_{88}$ against LC, the difference is $23 - 22 = 1$. Based on the above results, we expect that there exist S-boxes with a small value of both $rD_p - rD_h$ and $rL_p - rL_h$ for each fixed permutation layer. For such schemes, if r_h reaches the minimal, we expect that it is very likely that r_p also reaches the minimal. Hence, it is reasonable to make the following assumption:

Assumption 1 *For each fixed permutation layer, consider the SP-network schemes investigated in this paper. Among those with a minimal value of r_h, there exist some schemes satisfying $rD_p - rD_h \leq 2$ and $rL_p - rL_h \leq 2$.*

By using the heuristic measure, for each combination of a fixed permutation layer and a platinum Num1-DL category, we can discard a large proportion of the S-box candidates and concentrate only on S-boxes with the minimal value of r_h (we will present the results in Section 6). We emphasize that this is the first step. For such cipher designs,

designers must take differential/linear clustering into consideration. Ideally, designers can make a further selection from the schemes with the minimal value of r_h by selecting an S-box which has the minimal value of $r_p - r_h$. Note that the minimal value of $r_p - r_h$ is not more than 2 under Assumption 1.

5 A Relation of the S-box Selection, the Value of $CarL1_S$ and the Security of PRESENT and SPONGENT

The block length of PRESENT is 64 bits. For SPONGENT [8], the block length of the internal permutation has 5 choices: 88, 136, 176, 240 and 272 bits [1], which are denoted as SPONGENT$_b$ respectively, b is the block length. In this section, we focus on these 6 block lengths.

The design criteria of the PRESENT S-box are as follows:

1. Optimal.
2. $CarD1_S = 0$.
3. For $\Gamma I, \Gamma O \in F_2^4$ such that $wt(\Gamma I) = wt(\Gamma O) = 1$ it holds that $Imb_S(\Gamma I, \Gamma O) = 2$.
4. No fixed point, i.e., $S(x) \neq x$ for any $x \in F_2^4$.

There are 20 PE classes satisfying criteria 1 and 2. Among the 20 PE classes, 14 PE classes satisfy criterion 3. Up to adding constants before and after an S-box, which does not change any of the design criteria 1-3 of the PRESENT S-box and moreover does not change the probability of the best differential trail and the correlation potential of the best linear trail , there are $14 \times 4! \times 4! = 8064$ S-boxes. The 8064 S-boxes belong to 3 different categories. Fix the permutation of PRESENT (or the permutation layer of the SPONGENT internal permutation), we wonder which are the best choices among the 8064 S-boxes.

For the schemes investigated in this section, if the best r-round linear trail has only one active S-box in each round, then its correlation potential is 2^{-4r+4}. Thus, when $r = \frac{b}{4}$, the correlation potential of such a linear trail is 2^{-b+4}, which means there exists a $\frac{b}{4}$-round exploitable linear distinguisher. For $b = 64$ and $b = 88$, our experiments show that there exist some S-boxes such that the correlation potential of the best $\frac{b}{4}$-round linear trail is less than or equal to 2^{-b} (see Table 7 and Table 9).

Based on the above discussion, we decide to discard the S-boxes which can result in a linear trail with only one active S-box in each round. Note that a r-round iterative linear trail can be used to construct a r'-round linear trail for any $r' \geq r$. Algorithm 1 is designed to detect if an S-box can result in a r-round iterative linear trail with only one active S-box in each round, note that such a linear trail is connected by the elements in $SetL1_S$. We only check up to 25 rounds for practical reasons (nevertheless, we point out that it can not exclude the possibility that more S-boxes may be discarded if more rounds are checked). Let e_i denote the vector with a single one at position i (counting from zero). Since all of the round input/output selection patterns belong to the set $\{e_i\}$, for simplicity, we use In (Out) to denote the subscript of the input (output) selection pattern of the S-box layer. By running Algorithm 1, we get the following result.

[1] The block length of the internal permutation of SPONGENT is extended to 11 different choices in [9]. We do not consider the other 6 choices in this paper.

Algorithm 1

INPUT:

b: the block length S: an S-box candidate $Perm_b$: the b-bit permutation layer of the block cipher or the hash function

OUTPUT:

Check if the S-box can result in a linear trail with only one active S-box in each round. If yes, $flag$=1; else $flag$=0.

1. Set $flag$=0. Declare $Init$ as a global variable.
2. Calculate $CarL1_S$ and the $CarL1_S$ pairs $\{(\Gamma I, \Gamma O)\}$ of the set $SetL1_S$.
3. for $\frac{b}{4}$ S-box indexes of $i \in \{0, 1, \cdots, \frac{b}{4}-1\}$ do
   for $CarL1_S$ pairs $(\Gamma I, \Gamma O) \in SetL1_S$ do
   $\{Init = In = i \times 4 + log_2^{\Gamma I}$; $Out = i \times 4 + log_2^{\Gamma O}$;
   if ($Perm_b[Out] = Init$), then $\{flag$=1; return $flag$ and exit the program$\}$; // a 1-round iterative weak linear trail is found.
   else call ***Function loop(2)***; $\}$
4. Return $flag$ and exit the program;

Function loop(r)

$\{$for all pairs $(\Gamma I^*, \Gamma O^*) \in SetL1_S$ satisfying $(Perm_b[Out] \bmod 4 = \Gamma I^*)$ do
$\{In = Perm_b[Out]$; $Out = \lfloor \frac{In}{4} \rfloor \times 4 + log_2^{\Gamma O^*}$;
if ($Perm_b[Out] = Init$), then $\{flag = 1$; return $flag$ and exit the program$\}$; // a r-round iterative weak linear trail is found.
else if (r < 25), call loop(r+1); $\}$ $\}$

Table 5. Number of the Remaining S-boxes using Algorithm 1 for the 6 Block Lengths

block length (bits)	64	88	136	176	240	272
number of remaining S-boxes	96	112	32	48	64	0

Result 3 *For each of the 6 block lengths, fix the corresponding permutation layer, when combining with the 8064 S-boxes, there are 8064 SP-network schemes. Discard the S-boxes which can result in a linear trail with only one active S-box in each round using Algorithm 1, we have the following facts:*

1. *Table 5 gives the number of the remaining S-boxes, which shows that more than* 98.6 *percent of the 8064 S-boxes are discarded for each block length.*

2. *For 64-, 88-, 136-, 176- and 240-bit block length, all of the remaining S-boxes belong to the* $(0,4)$*-Num1-DL category; for 272-bit block length, there is no S-box left.*

For each of the 6 block lengths, among the 8064 S-boxes, every S-box in $(0,6)$-Num1-DL and $(0,8)$-Num1-DL categories can result in a linear trail with only one active S-box in each round. For 272-bit block length, fix the permutation layer of SPONGENT$_{272}$, for each of the 8064 S-box candidates, there exists a linear trail with only one active S-box in each round. Hence, we get a new design criterion for the S-box of PRESENT-like or SPOGNENT-like schemes.

Design Criterion 1 *For 64-bit (88-, 136-, 176- and 240-bit respectively) block length, fix the permutation layer of PRESENT (the corresponding SPONGENT variant). For better resistance against LC, besides the 4 design criteria for the S-box, designers should add* $CarL1_S = 4$ *as a new design criterion.*

For 272-bit block length, fix the permutation layer of SPONGENT$_{272}$*. For better resistance against LC, designers should change their design criteria* $CarD1_S = 0$ *and choose an S-box with* $CarD1_S \neq 0$*.*

6 An Investigation of the S-box Selection of PRESENT, RECTANGLE and SPONGENT

Due to the huge computational effort required to run the experiments, we only focus on 64- and 88-bit block lengths in this section. Consider the following SP-network schemes. For 64-bit block length, the S-box is chosen from the 3 platinum Num1-DL categories, the diffusion layer is either the PRESENT or RECTANGLE permutation. Thus, there are 6 combinations. Similarly, for 88-bit block length, there are also 6 combinations. Hence, 12 combinations in total. In Section 6.3, we consider both DC and LC for the security of the 12 combinations using the heuristic measure. Since DC is more important than LC for hash functions, in Section 6.4, we only consider DC for the 12 combinations.

Definition 7. *Let b denote the block length. For a b-bit block cipher (or permutation of a hash function), let $Prob_r$ denote the probability of the best r-round differential trail, and Cor_r the correlation of the best r-round linear trail. Define r_{min} as*

$$r_{min} = \min_r \{Prob_r \leq 2^{-b} \text{ and } {Cor_r}^2 \leq 2^{-b}\}.$$

In this section, we use the values of r_{min}, $Prob_{r_{min}}$ and $Cor_{r_{min}}$ for a comparative study. Generally speaking, the smaller the value of r_{min}, the better the scheme against DC and LC. For schemes with the same value of r_{min}, the smaller the value of $Prob_{r_{min}}$ (or $Cor_{r_{min}}$), the better the scheme against DC (or LC).

6.1 Influence of S-box Selection and Differential/Linear Trails with One Active S-box per Round

According to Table 4, up to adding constants before and after an S-box, there are $1152, 2304$ and 2304 S-boxes in the $(0,4)$-Num1-DL category, the $(1,3)$-Num1-DL category and the $(2,2)$-Num1-DL category respectively. By checking all the 10 platinum representative S-boxes, we get the following result. For any of the investigated schemes, if a r-round linear trail has only one active S-box in each round, then its correlation potential is 2^{-4r+4}; if a r-round differential trail has only one active S-box in each round, then its differential probability is between 2^{-3r} and 2^{-3r+2}.

For each of the 12 combinations, we firstly discard the S-boxes which can result in a differential/linear trail with only one active S-box in each round. For schemes using the PRESENT or SPONGENT$_{88}$ permutation layer, we use Algorithm 1 to perform the filtering, note that Algorithm 1 can be modified a little for the differential case. For schemes using the RECTANGLE or RECTANGLE$_{88}$ permutation, we extend the idea of Algorithm 2 in [31] to perform the filtering, the number of remaining S-boxes only depends on properties of the S-boxes and not on the block length. Table 6 presents our experimental results of the number of remaining S-boxes for the 12 combinations.

In [27], 4 PE classes are specified as "golden" S-boxes. For each of the 4 PE classes, $CarD1_S = 0$ and $CarL1_S = 8$. Fix the RECTANGLE permutation, when combining with these golden S-boxes, we get 2304 SP-network schemes. For each of the 2304 schemes, there exists a linear trail with only one active S-box in each round. Thus, together with Result 3, we get that all of the golden S-boxes are not good choices for the 3 primitives.

Table 6. Number of the Remaining S-boxes for the 12 Combinations

	PRESENT Perm.	SPONGENT_{88} Perm.	RECTANGLE_{64} Perm. /RECTANGLE_{88} Perm.
(0,4)-Num1-DL	96	112	96
(1,3)-Num1-DL	384	592	384
(2,2)-Num1-DL	528	640	528

6.2 Search Algorithm for the Best Differential/Linear Trail

Matsui proposed a branch-and-bound search algorithm [23] for determining the best differential/linear trail of DES-like cryptosystems in 1994. Ohta et al. [26] improved Matsui's algorithm by introducing the concept of search pattern to reduce unnecessary search candidates before the search, and applied their algorithm on DES and FEAL. Aoki et al. [3] further improved Ohta's search algorithm by discarding more unnecessary search patterns, and applied their algorithm on FEAL. Based on these 3 previous work, we have written a program for the search of the best differential/linear trails for PRESENT, RECTANGLE and the internal permutation of SPONGENT respectively.

6.3 Experimental Results

In the following, we present our experimental results by running Algorithm 2. The experiments have been performed using 4 computers: 3 with Intel Core i7 (or i5) CPU, and 1 with Intel Xeon E7-2820 (16 cores) CPU. It took us about 4 weeks to do all the experiments.

For each combination, let N denote the number of the remaining S-boxes (see Table 6), the permutation layer is fixed, thus we have N SP-network schemes. Here are some notations:

- R_m: the minimal value of r_{min} among the N schemes
- Num_{R_m}: the number of schemes that the corresponding r_{min} reach the minimum value R_m
- num: the number of schemes with the values $Prob_{R_m}$ and $Cor^2_{R_m}$ in the same row

Tables 7-10 summarize our experimental results for each fixed permutation. The result in Table 8 is in accordance with that in [31]. From Table 7-10, we get the following results:

1. With the PRESENT permutation layer, the values of R_m are the same for the 3 combinations. There are 336 S-boxes (up to adding constants before and after an S-box, similarly hereinafter) such that the value of r_{min} reach the minimum $R_m = 16$.
2. With the RECTANGLE permutation layer, the (1,3)- and (2,2)-Num1-DL categories are better. There are 128 S-boxes such that the value of r_{min} reach the minimum $R_m = 15$. Note that RECTANGLE uses one of these 128 S-boxes.
3. With the SPONGENT_{88} permutation layer, the (1,3)- and (2,2)-Num1-DL categories are better. For the (1,3)-Num1-DL category, $R_m = 19$; for the (2,2)-Num1-DL category, $R_m \leq 19$.

Table 7. Experimental Results With the PRESENT Permutation

category	R_m	Num_{R_m}	$Prob_{R_m}$	$Cor^2_{R_m}$	num
$(0,4)$-Num1-DL	16	96	2^{-64}	2^{-64}	96
$(1,3)$-Num1-DL	16	192	2^{-70}	2^{-64}	96
			2^{-64}	2^{-64}	96
$(2,2)$-Num1-DL	16	48	2^{-68}	2^{-64}	48

Table 8. Experimental Results With the RECTANGLE Permutation

category	R_m	Num_{R_m}	$Prob_{R_m}$	$Cor^2_{R_m}$	num
$(0,4)$-Num1-DL	16	16	2^{-64}	2^{-80}	16
$(1,3)$-Num1-DL	15	64	2^{-74}	2^{-66}	16
			2^{-71}	2^{-66}	16
			2^{-65}	2^{-66}	16
			2^{-65}	2^{-64}	16
$(2,2)$-Num1-DL	15	64	2^{-73}	2^{-64}	8
			2^{-72}	2^{-64}	8
			2^{-69}	2^{-64}	16
			2^{-67}	2^{-66}	8
			2^{-66}	2^{-74}	4
			2^{-66}	2^{-72}	8
			2^{-66}	2^{-70}	4
			2^{-66}	2^{-66}	8

Table 9. Experimental Results With the SPONGENT$_{88}$ Permutation Layer

category	R_m	Num_{R_m}	$Prob_{R_m}$	$Cor^2_{R_m}$	num
$(0,4)$-Num1-DL	21	8	2^{-118}	2^{-88}	4
			2^{-117}	2^{-88}	4
$(1,3)$-Num1-DL*	19	?	$\leq 2^{-91}$	2^{-90}	?
$(2,2)$-Num1-DL*	≤ 19	?	$\leq 2^{-88}$	2^{-90}	?

Table 10. Experimental Results With the RECTANGLE$_{88}$ Permutation

category	R_m	Num_{R_m}	$Prob_{R_m}$	$Cor^2_{R_m}$	num
$(0,4)$-Num1-DL	22	96	2^{-88}	2^{-118}	84
			2^{-88}	2^{-116}	8
			2^{-88}	2^{-114}	4
$(1,3)$-Num1-DL	18	56	2^{-93}	2^{-92}	8
			2^{-93}	2^{-88}	10
			2^{-92}	2^{-88}	2
			2^{-91}	2^{-92}	4
			2^{-91}	2^{-90}	2
			2^{-90}	2^{-88}	2
			2^{-88}	2^{-92}	8
			2^{-88}	2^{-90}	6
			2^{-88}	2^{-88}	14
$(2,2)$-Num1-DL	17	1	2^{-88}	2^{-88}	1

4. With the RECTANGLE$_{88}$ permutation layer, the (2,2)-Num1-DL category is the best. There is only one S-box such that the value of r_{min} reach the minimum $R_m = 17$.

Table 11. Results for the 12 Combinations when only Considering DC

Permutation Layer	category	R_m^D	$Prob_{R_m^D}$
PRESENT	(0,4)-Num1-DL	16	2^{-64}
Permutation	(1,3)-Num1-DL	15	2^{-64}
	(2,2)-Num1-DL	16	2^{-68}
RECTANGLE	(0,4)-Num1-DL	16	2^{-64}
Permutation	(1,3)-Num1-DL	14	2^{-69}
	(2,2)-Num1-DL	14	2^{-68}
SPONGENT_{88}	(0,4)-Num1-DL	17	2^{-94}
Permutation Layer	(1,3)-Num1-DL*	≤ 18	$\leq 2^{-89}$
	(2,2)-Num1-DL*	≤ 19	$\leq 2^{-88}$
RECTANGLE_{88}	(0,4)-Num1-DL	22	2^{-88}
Permutation	(1,3)-Num1-DL	18	2^{-93}
	(2,2)-Num1-DL	17	2^{-88}

In Table 9, for the two combinations marked with "*", we have not finished the experiments for all of the corresponding S-boxes. However, we derived the value of R_m for one combination and a good estimate of R_m for the other, which are enough for us to derive the above results.

6.4 For Hash Functions - When DC is More Important than LC

According to the state-of-art security analysis on hash functions, DC is more important than LC. On the other hand, the permutation (or the compression function) of a hash function is normally required to be pseudo-random, which includes the requirement that there is no effective linear distinguisher. Therefore, we decide to consider the following question: For each of the 12 combinations, when only considering DC for the remaining S-boxes obtained in Section 6.1 (see Table 6), what results can we get? At first thought, the (0,4)-Num1-DL category should be the best choice, however, we will show that it is not always the case.

For each scheme, define $r_{min}^D = \min_r\{Prob_r \leq 2^{-b}\}$. For each combination, let R_m^D denote the minimal value of r_{min}^D among the N schemes. Table 11 summarizes our experimental results, and we get the following results:

1. With the PRESENT permutation, the (1,3)-Num1-DL category is the best. The minimal value of r_{min}^D is $R_m^D = 15$.
2. With the RECTANGLE permutation, the (1,3)- and (2,2)-Num1-DL categories are better. The minimal value of r_{min}^D is $R_m^D = 14$.
3. With the SPONGENT_{88} permutation layer, it seems that the (0,4)-Num1-DL category is the best and the minimal value of r_{min}^D is $R_m^D = 17$.
4. With the RECTANGLE_{88} permutation, the (2,2)-Num1-DL category is the best. The minimal value of r_{min}^D is $R_m^D = 17$.

Potentially Better S-boxes for SPONGENT_{88} For SPONGENT_{88}, there exists a 17-round differential trail with probability 2^{-86} [4], which is better than the one given by its designers in [9, Table 4]. Moreover, there exists a 22-round linear trail with correlation potential 2^{-84} for SPONGENT_{88} (only one active S-box in each of the 22 rounds).

Table 12. 4 Potentially Better S-boxes for SPONGENT$_{88}$

0, 6, 12, 1, 5, 9, 11, 14, 3, 13, 15, 8, 10, 7, 4, 2
0, 6, 5, 8, 10, 13, 15, 1, 12, 9, 11, 7, 3, 14, 4, 2
0, 3, 5, 12, 10, 13, 15, 2, 6, 9, 11, 7, 1, 14, 8, 4
0, 12, 10, 5, 3, 15, 13, 2, 6, 11, 9, 14, 8, 1, 7, 4

With the permutation layer of SPONGENT$_{88}$, we found 4 S-boxes in the (0,4)-Num1-DL category such that the probability of the best 17-round differential trail is 2^{-94} and the correlation potential of the best 21-round linear trail is 2^{-88} for each of the 4 schemes. It can be seen that the 4 S-boxes are potentially better than the SPONGENT$_{88}$ S-box with respect to the security against both DC and LC. The 4 S-boxes are listed in Table 12, which can be used for further investigation.

6.5 A New Design Criterion

For SP-network schemes with the SPONGENT$_{88}$ permutation layer, when considering both DC and LC, based on the results in Section 5 and Table 9, it can be deduced that an S-box with $CarD1_S = 0$ is not an optimal choice, while $(1,3)$- and $(2,2)$- Num1-DL categories are better choices. On the other hand, when considering DC more important than LC, it seems that $(0,4)$-Num1-DL category is the best choice. For SP-network schemes with RECTANGLE-like permutations, based on the results in Tables 7-11, it seems that the $(2,2)$-Num1-DL category is always an optimal choice. We have the following design criterion.

Design Criterion 2 *For block ciphers (or hash functions) using* 4×4 *S-boxes as confusion layers and bit permutations as diffusion layers, designers can extend the range of the S-box selection to the 3 platinum Num1-DL categories and select their S-box carefully.*

7 Discussion

Based on our experimental results, there are 336 potentially best S-boxes for PRESENT, 128 potentially best S-boxes for RECTANGLE, and 4 potentially better S-boxes for SPONGENT$_{88}$. To judge if a potentially best (better) S-box is a real best (better) S-box, it needs to investigate the clustering of differential/linear trails. In this respect, the approach used in [1] is of interest, we leave it for further study. The NOEKEON S-box belongs to the $(7,6)$-Num1-DL category. Serpent uses 8 S-boxes, among them, 3 S-boxes belong to the $(0,6)$-Num1-DL category, and the other 5 S-boxes belong to the $(0,8)$-Num1-DL category. It is also interesting to investigate the influence of the 3 platinum Num1-DL categories on the security of NOEKEON and Serpent against DC and LC.

Acknowledgments

We would like to thank anonymous referees for their helpful comments of SAC'2014 and FSE'2015. We also thank Andrey Bogdanov for his helpful discussions which help

us to improve the quality of this paper. The main work in this paper was performed while Wentao Zhang was a visitor at KU Leuven. The research presented in this paper is supported by the National Natural Science Foundation of China (No.61379138), the Research Fund KU Leuven (OT/13/071), and the "Strategic Priority Research Program" of the Chinese Academy of Sciences (No.XDA06010701).

References

1. Abdelraheem, M.A.: Estimating the Probabilities of Low-Weight Differential and Linear Approximations on PRESENT-Like Ciphers. In: Kwon T., Lee M.-K., and Kwon D. (eds.): ICISC 2012, LNCS, vol. 7839, pp. 368–382, Springer, Heidelberg (2013)
2. Anderson, R., Biham, E., Knudsen, L.R.: Serpent: A Proposal for the Advanced Encryption Standard. NIST AES proposal (1998)
3. Aoki, K., Kobayashi, K., Moriai, S.: Best Differential Characteristic Search of FEAL. In: Biham, E. (ed.) Fast Software Encryption, LNCS, vol. 1267, pp. 41–53. Springer, Heidelberg (1997)
4. Bao, Z., Zhang, W., Lin, D.: Speeding up the Search Algorithm for the Best Differential and Best Linear Trails, to appear in Inscrypt'2014.
5. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology 4(1), 3–72 (1991)
6. Blondeau, C., Gerard, B.: Multiple Differential Cryptanalysis: Theory and Practice. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 35–54. Springer, Heidelberg (2011)
7. Blondeau, C., Nyberg, K.: Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. In Nguyen, P.Q., Oswald., E. (eds.): EUROCRYPT 2014. LNCS, vol. 8441, pp.165–182. Springer (2014)
8. Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., and Verbauwhede, I.: SPONGENT: A Lightweight Hash Function. In: Preneel., B., Takagi., T. (eds.), CHES 2011, LNCS, vol. 6917, pp. 312–325. Springer (2011)
9. Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., and Verbauwhede, I.: SPONGENT: The Design Space of Lightweight Cryptographic Hashing. IEEE Transactions on Computers 62(10), 2013.
10. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
11. Carlet, C., Charpin, P., Zinoviev, V.: Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems. Des. Codes Cryptography 15(2), 125–156 (1998)
12. Cho, J.: Linear Cryptanalysis of Reduced-Round PRESENT. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 302–317. Springer, Heidelberg (2010)
13. Collard, B., Standaert, F.X.: A Statistical Saturation Attack against the Block Cipher PRESENT. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 195–210. Springer, Heidelberg (2009)
14. Daemen, J., Peeters, M., Van Assche, G., Rijmen, V.: Nessie Proposal: the Block Cipher Noekeon, Nessie submission (2000), http://gro.noekeon.org/
15. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, Heidelberg (2002)
16. De Cannière, C.: Analysis and Design of Symmetric Encryption Algorithms, Doctoral Dissertaion, KULeuven (2007)

17. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
18. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer (2011)
19. Kanda, M., Takashima, Y., Matsumoto, T., Aoki, K., and Ohta, K.: A Strategy for Constructing Fast Round Functions with Practical Security against Differential and Linear Cryptanalysis, In: Howard M. Heys, Carlisle M. Adams (eds.) SAC 1999. LNCS, vol. 1556, pp. 264–279. Springer, Heidelberg (2000)
20. Leander, G.: On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 303–322. Springer, Heidelberg (2011)
21. Leander, G., Poschmann, A.: On the Classification of 4 bit S-boxes. In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 159–176. Springer, Heidelberg (2007)
22. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
23. Matsui, M.: On Correlation between the Order of S-Boxes and the Strength of DES. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 366–375. Springer, Heidelberg (1995)
24. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T.(ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994)
25. Ohkuma, K.: Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 249–265. Springer, Heidelberg (2009)
26. Ohta, K., Moriai, S., Aoki, K.: Improving the Search Algorithm for the Best Linear Expression. In: Coppersmith, D. (ed.) CRYPTO 1995, LNCS, vol. 963, pp. 157–170. Springer, Heidelberg (1995)
27. Saarinen, M.-J.O.: Cryptographic Analysis of All 4×4-Bit S-Boxes. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 118–133. Springer, Heidelberg (2012)
28. Siegenthaler, T.: Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Transactions on Information Theory 30(5), 776–776 (1984)
29. Wang, M., Sun, Y., Tischhauser, E., Preneel, B.: A Model for Structure Attacks, with Applications to PRESENT and Serpent. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 49–68. Springer, Heidelberg (2012)
30. Xiao, G.Z., Massey., J.L.: A spectral characterization of correlation-immune combining functions. IEEE Transactions on Information Theory 34(3):569-571 (1988)
31. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: RECTANGLE: A Bitslice Ultra-Lightweight Block Cipher Suitable for Multiple Platforms. Cryptology ePrint Archive: Report 2014/084, http://eprint.iacr.org/2014/084