BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **16**, No 4
Sofia • 2016 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2016-0063

On a Linear Cryptanalysis of a Family of Modified DES Ciphers with Even Weight S-Boxes

Yuri Borissov, Peter Boyvalenkov, Robert Tsenkov

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria
Emails: *youri@math.bas.bg peter@math.bas.bg r_cenkov@yahoo.com*

Abstract**:** *We investigate the effect of inserting extra linearity in the Data Encryption Standard* (*DES*) *through appropriate nonsingular linear encodings of the output of the individual S-boxes. More specifically, we examine the general situation when the output of each S-box of the DES is precoded separately into a properly constructed copy of the inherent even-weight code of length 4. The study is focused on finding multi-round linear characteristics for thus modified DES ciphers having maximal effectiveness. Depending on the particular encodings, it turns out that the effectiveness of interest may be larger but in most cases is smaller than that one for the original DES with the same number of rounds. The latter means that the complexity of successful linear cryptanalysis against these ciphers will mainly increase comparing to the DES itself. The present research extends in a natural way our previous work [Linear Cryptanalysis and Modified DES with Parity Check in the S-boxes, LNCS 9540* (*2016*), *pp. 60-78]*.

Keywords**:** *DES, S-boxes, parity check, linear cryptanalysis, linear characteristics.*

1. Introduction

The DES is the first publicly available block encryption algorithm which was also adopted as an (nowadays former) USA standard. It is well-known that the strength of DES lies in its only non-linear part – the so-called S-boxes. However, at the beginning (in 1970's, due to some reasons concerning national security) design criteria for the S-boxes of DES were classified what arose out many controversies. Later on, in the paper [4] some of the original design criteria were published and it became clear that the chosen S-boxes were much more resistant to differential cryptanalysis (a general cryptanalytic technique already known in the public domain from [2]) than if they had been picked up at random. Although the main topic of [4] is to show some of the safeguards against differential cryptanalysis built into the algorithm from the beginning, its author has pointed out as well a design criterion which is related to the just developed (at that time) new method known as

"linear cryptanalysis" [8]. Hereinafter, for the reader's convenience we recall that criterion in its stronger form ($S - 2'$) [4, p. 250]:

No linear combination of output bits of an S-box should be too close to a linear function of the input bits. (That is, if we select any subset of the four output bit positions and any subset of the six input bit positions, the fraction of inputs for which the XOR of these output bits equals the XOR of these input bits should not be close to 0 or 1, but rather should be near 1/2.)

Fortunately, this criterion (more precisely, the weaker form for a single output bit) was among the original requirements for DES and almost achieved in its final specification (see, also [6]). That is why, as pointed out in [4], the standard resisted in practice this new linear attack.

An extremal particular case of the aforementioned criterion is the following:

The XOR of the four output bits of any S-box must not be a constant.

But, what if this constraint is violated artificially? For instance, when setting an output bit of original S-box of the DES to be the parity check of the other three output bits which are kept unchanged.

What can be said at first glance about an S-box obtained in this way? Of course, considering such a box as a vector Boolean function, it is not onto the ambient binary space $\mathbf{F}_2^4$ taking as values only even/odd weight 4-bit tuples. Also, its nonlinearity in terms of the definition given in [11] vanishes. However, an S-box of this kind possesses single error-detection capability and therefore it is immune (to a certain extent) against fault-injection attacks during the execution time of the algorithm. In addition, such S-box satisfies automatically the criteria concerning spectrum of Hamming distances between its outputs, relevant in case of differential cryptanalysis (see, for details [4] or in summary [7, p. 301]).

In [3], we investigated the resistance against linear cryptanalysis of modified DES ciphers having S-boxes of the described type with parity check in a fixed (the same for all of them) position. It turns out that some-how in contrast to the common belief, the complexity of successful analysis of that kind increases (in three out of four possibilities) compared to the case of original DES. After the presentation of [3] at BalkanCryptSec 2015, Prof. K. Nyberg asked what would be the behaviour of such DES-like ciphers in the general situation when the described modifications are applied separately for each individual S-box. The results of our efforts in that direction are reported in the present paper.

In Section 2 we give some background notions and summarize our results from [3]. The motivation for this research is explained in Section 3. Sections 4 and 5 are devoted to our new results concerning the wider family of modified DES ciphers under consideration.

2. Background

Regarding modified DES ciphers, we advise the readers preferring mathematical description to check, e.g., [5, Ch. 7.5.1], while those who are interested more in implementations to consult [13] about details of the DES algorithm.

2.1. Some basics of linear cryptanalysis

Linear cryptanalysis is a powerful technique for cryptanalysis of the modern block ciphers developed in the early 1990s. The attack in its full form was introduced in 1993 by Matsui [8] and was first applied to the DES. Speaking in brief, this attack relies on the existence of linear probabilistic approximations of the cipher having the form:

$$\mathbf{P}[\chi_P] + \mathbf{C}[\chi_C] = \mathbf{K}[\chi_K],$$

where **P**, **C** and **K** denote the plaintext, the corresponding ciphertext and the secret key, respectively, while $\mathbf{B}[\chi_B]$ stands for $B_{b_1} \oplus B_{b_2} \oplus \cdots \oplus B_{b_m}$ with $\chi_B = \{b_1, b_2, \ldots, b_m\}$ a subset of positions in the bit array **B**. Among these relations (also called characteristics), the most valuable for cryptanalysis are those, effective ones, that hold true with probability deviating significantly from 1/2. In practice, for the iterative block ciphers based on S-boxes, e.g., Feistel or SP networks, effective characteristics can be obtained by fixing the generic firmed correlations between the inputs and outputs of the individual S-boxes at first, and then concatenating these local 1-round linear dependencies through the involved round functions in multi-round ones.

A bit more formally, when a linear approximation holds with probability $p \neq 1/2$ for randomly given plaintext P and the corresponding ciphertext C, the magnitude of the *bias* $p - 1/2$, represents the *effectiveness* of that approximation. A linear characteristic is called *best characteristic* when the effectiveness of corresponding linear approximation is maximal.

It is deserved mentioning that the number of plaintext/ciphertext pairs needed for a linear attack with sufficiently high probability of success, is proportional to e^{-2}, where e denotes the effectiveness of the exploited characteristic. So, the effectiveness influences directly on the complexity of this kind of attacks.

The following definition, given for arbitrary S-box, is of vital importance for our considerations:

Definition 1 (see, e.g., [12]). For given $m \times n$ S-box regarded as mapping $S : \mathbf{F_2}^m \mapsto \mathbf{F_2}^n$, and given integers α and β, such that $0 \le \alpha \le 2^m - 1$ and $0 \le \beta \le 2^n - 1$, let $\mathrm{NS}(\alpha, \beta)$ be the number of times when the XOR-sum of the input bits masked by α coincides with the XOR-sum of the output bits masked by β. The table, where the vertical and the horizontal axes indicate α and β respectively, and each entry contains the "centred" value

$$\mathrm{LS}(\alpha, \beta) = \mathrm{NS}(\alpha, \beta) - 2^{m-1}$$

is referred to as Linear Approximation Table (LAT) for the S-box S.

Note that in case of the DES there are eight S-boxes, $S_1, \ldots, S_8$, $m = 6$ and $n = 4$.

The effectiveness of a linear approximation of an S-box is deduced directly from its LAT, while the effectiveness of a round approximation which involves two or more S-boxes can be computed applying the following lemma in suitable way.

Lemma 1 (Pilling-up Lemma [9]). Let Z_i, $1 \le i \le r$, be independent random variables whose values are 0 with probability p_i or 1 with probability $1 - p_i$. Then the probability that $Z_1 \oplus Z_2 \oplus \ldots \oplus Z_r = 0$ is

$$\frac{1}{2} + 2^{r-1} \prod_{i=1}^{r} \left(p_i - \frac{1}{2} \right).$$

The next proposition, stated as lemma by Matsui (see, e.g., [9]), expresses the main properties of the LATs in the DES.

Proposition 1. Let S_k be a S-box of the DES.

(i) $\mathrm{NS}_k(\alpha, \beta)$ is even.

(ii) If $\alpha = 1$, 32 or 33, then $\mathrm{NS}_k(\alpha, \beta) = 32$ for all β.

Apart from analyzing the properties of those LATs in his seminal papers [8-10], Matsui has found best linear characteristics for 3 to 20 rounds of the DES algorithm, and demonstrated different approaches (Algorithm 1 and Algorithm 2) for mounting attacks against various number of rounds of the cipher. The first experimentally verified cryptanalytic attack against the original (16-round) DES [10] was an improved variant of Algorithm 2 using two best statistically independent 14-round linear characteristics both having effectiveness of 1.19×2^{-21}. This maximal effectiveness is one amongst the other numerical results for 3-20 rounds [9, p. 33] which should be compared with the maximal effectiveness obtained for the same number of rounds in modified DES ciphers considered here.

2.2. Summary on linear cryptanalysis of DES with embedded parity check into the S-boxes

The goal of our previous work [3] was to clarify more comprehensively the intuition behind the claim that embedding parity check in the outputs of the S-boxes of DES will weaken this cipher facilitating significantly a linear cryptanalysis in the spirit of Matsui's classic one.

Before describing the results from [3] we recall some necessary conventions and notations. Without loss of generality we may assume even parity embedding. Parity bit masks can take values 1, 2, 4 and 8 or their 4-bit representations. For instance, the mask 1000 (or mask with value 8) shows presence of a parity bit at the left-most position in the output of some S-box. Also, we will denote by $\mathrm{LS}(\pi; \alpha, \beta)$ the LAT's values of the S-box obtained through embedding a parity bit with mask π into the box S.

The next proposition summarizes main properties of the considered S-boxes.

Proposition 2 [3]. Let S_k be an S-box of DES, π be a parity bit mask, and & denotes tuple-wise AND operator. Then if $\alpha \neq 0$ and $\beta \neq 0$ it holds:

(i) $\mathrm{LS}_k(\pi; \alpha, \beta) = \mathrm{LS}_k(\alpha, \beta)$ for all α and β such that $\beta \,\&\, \pi = 0$;

(ii) $\mathrm{LS}_k(\pi; \alpha, \beta) = \mathrm{NS}_k(\alpha, 15 - \beta)$ for all α and $\beta < 15$ such that $\beta \,\&\, \pi \neq 0$;

(iii) $\mathrm{LS}_k(\pi; \alpha, 15) = 0$ for all α;

in addition, it holds:

(iv) $\mathrm{LS}_k(\pi; 0, \beta) = 0$ for all $\beta : 15 > \beta > 0$;

(v) $\mathrm{LS}_k(\pi; 0, 15) = 32$ and $\mathrm{LS}_k(\pi; 0, 0) = 32$;

(vi) $\mathrm{LS}_k(\pi;\alpha,0)=0$ for all $\alpha\neq 0$.

Proposition 2 (i)-(ii) mean that the new LAT is symmetric, in a sense, the half of its columns (where the parity position does not participate) is preserved and the remaining half of columns is replaced with a mirror copy of the preserved one. Also, by contrast to the original DES, Proposition 2 (v) shows the existence of an 1-round linear characteristic with zero input mask and non-zero output mask having non-zero bias. However, since this characteristic is deterministic it cannot be utilized in practice *within the framework of a linear cryptanalysis with at most one active S-box per round*. We would like to stress that, like our previous [3], the present article is focused on this *narrow* sense linear cryptanalysis, because its primary goal is to compare the results with those obtained for the original cipher [9] and the modified DES ciphers from [3] in that particular case of interest.

The next theorem proven in [3] shows the decreasing effectiveness for modified DES ciphers with small number of rounds having S-boxes of parity check in the same position.

Theorem 1. Every parity mask applied to the S-boxes of DES leads to a reduction of the maximal effectiveness of the 1-round and 3-round linear characteristics for that cipher.

To explore the behaviour of thus modified ciphers for larger number of rounds, we developed our own search algorithm for finding best multi-round characteristics. This algorithm incorporates some specific features of the considered ciphers (e.g., the so-called modified Knudsen observation), and has very efficient C++ implementation. In summary, the experiments based on the created tools show that multi-round linear cryptanalysis towards those ciphers has varying magnitude of complexity depending on the chosen parity position. Also, when comparing to that against the DES itself with the same number of rounds, the complexity can diminish but mostly grows. For instance, in case of 16 rounds, the complexity of successful linear attacks increases in three out of the four possibilities. For details of the developed algorithmic technique and the yielded results, we refer to [3].

3. Motivation and statement of the current research

The question pointed in the Introduction motivated us to perform an examination in the following two directions:

1. Studying the behaviour (from the perspective of linear cryptanalysis) of a wider family of modified DES ciphers whose parity check position into each individual S-box is picked up arbitrarily and independently from those into the others.

2. Comparing the yielded results to those already known for the original DES cipher and the modified ciphers studied in [3].

Of course, when attacking a given cipher by the method of linear cryptanalysis, the effectiveness of the best linear characteristics is of crucial importance. Lower effectiveness implies worse probability for success of the linear attacks, although conversely larger one does not always provide better conditions for mounting these attacks. However, from the designer's point of view, the

resistance of cipher towards these particular attacks increases in the former case and therefore its cryptographic strength will grow as whole. Rephrasing that, an additional goal might be of interest in respect to the modified DES ciphers considered here. Namely, to choose the pattern of parity checks in such a way that maximal effectiveness is on the desirable level.

Based on the above reasoning, we set to our study two additional targets:

- to look for some reasonable criteria for optimality;
- to search for patterns of parity check positions (among all possible combinations of them into the S-boxes) satisfying these criteria.

4. Optimal linear characteristics for small number of rounds

In the general case of many (more than 3) rounds the number of possibilities for internal chaining of the 1-round characteristics increases prohibitively enough. However, for small number of rounds we obtain a clear and precise understanding without computer assistance.

Clearly, the effectiveness of the best 1-round characteristics for the DES-like cipher of considered type is determined by the maximal magnitude of the elements in its LATs. In order to derive the effectiveness of interest, we perform a thorough analysis of the LATs of the original DES which in turn allows some deductions about the modified ones.

We distinguish one kind of elements in these tables defined as follows.

Definition 2. The entry $\mathrm{LS}_k(\alpha, \beta)$, $0 \le \alpha \le 63$, $1 \le \beta \le 14$, from the LAT of an S_k of the DES is called *invariant when parity check is applied* (or *simply invariant*) if

$$|\mathrm{LS}_k(\alpha, \beta)| = |\mathrm{LS}_k(\pi; \alpha, \beta)| \quad \text{for every parity mask } \pi.$$

Obviously, Proposition 2 (i)-(ii) imply that $\mathrm{LS}_k(\alpha, \beta)$ is invariant if and only if when $|\mathrm{LS}_k(\alpha, \beta)| = |\mathrm{LS}_k(\alpha, 15-\beta)|$.

Let I be the set of all invariant entries from LATs and $M_I := \max\{|L| : L \in I\}$. The next proposition shows the reasoning for Definition 2.

Proposition 3. Let π_k be a parity mask applied to S_k of the DES, $1 \le k \le 8$. Then

$$M_I \le \max_{k,\alpha,\beta} \{|\mathrm{LS}_k(\pi_k; \alpha, \beta)|\},$$

where the maximum is on all values $1 \le k \le 8$, $1 \le \alpha \le 63$ and $1 \le \beta \le 14$.

Proof: The equalities $|\mathrm{LS}_k(\alpha, \beta)| = |\mathrm{LS}_k(\pi_k; \alpha, \beta)|$ for invariant entries $\mathrm{LS}_k(\alpha, \beta)$ imply that the set $\{|L| : L \in I\}$ coincides with the union $\bigcup_{k=1}^{8} \{|\mathrm{LS}_k(\pi_k; \alpha, \beta)| : \mathrm{LS}_k(\alpha, \beta) \in I\}$. The latter is, of course, a subset of the whole $\bigcup_{k=1}^{8} \{|\mathrm{LS}_k(\pi_k; \alpha, \beta)|\}$, and the assertion follows. ■

In other words, the above proposition says that the maximum of magnitudes of the invariant elements determines a lower bound on the effectiveness of the best

1-round characteristics of a modified DES cipher. As an immediate consequence, we obtain the following corollary.

Corollary 1. Under the assumptions of Proposition 3 and $\bar{\pi} = (\pi_1, \pi_2, \ldots, \pi_8)$, we have

$$\min_{\bar{\pi}} \max_{k,\alpha,\beta} \{|\mathrm{LS}_k(\pi_k; \alpha, \beta)|\} \geq M_I.$$

Let us remind that we deal by default with a linear cryptanalysis in narrow sense, i.e., with no more than one active S-box per round.

Theorem 2. Let π_7 be the parity mask applied to the S-box S_7 of the DES. Then:

(i) The maximal possible effectiveness of the best 1-round characteristics for modified DES cipher is obtained if $\pi_7 \neq 4$. There are two unique elements of the LATs in this case possessing the highest magnitude 18.

(ii) If $\pi_7 = 4$ then the effectiveness of the best 1-round characteristics for such a DES-like cipher is of minimal possible value 0.25.

(iii) The corresponding extremal effectiveness of the best 3-round characteristics is achieved at the same assumptions. These effectiveness are $2(18/64)^2 \approx 0.1582$ and 0.1250, respectively.

Proof: (i) The highest magnitude of an element of the LATs of DES is 20 and there is a unique such element, namely $\mathrm{LS}_5(16,15) = -20$. On the other hand, by Proposition 2(iii) this element is eliminated (vanishes) from the LAT of S_5 whenever a parity check is embedded. The next two (by magnitude) values are $\mathrm{LS}_1(16,15) = \mathrm{LS}_7(59,4) = -18$. The former vanishes by the same reason as above, while the latter preserves its value if $\pi_7 \neq 4$ according to Proposition 2 (i)-(ii) (note that $\mathrm{LS}_7(59,11) = 2$). We also have $\mathrm{LS}_7(\pi_7; 59,11) = \mathrm{LS}_7(\pi_7; 59,4) = -18$, which implies that there are two unique elements of the LATs with maximal magnitude 18 if $\pi_7 \neq 4$ with corresponding effectiveness 18/64=0.28125. This completes the proof.

(ii) As we have already seen there are no invariant entries having magnitude larger than 16, however, two entries of this kind are $\mathrm{LS}_4(43,6) = 16$ and $\mathrm{LS}_4(43,9) = -16$. Thus, $M_I = 16$, and Corollary 1 implies that the minimum of the maximal by magnitude element in modified LATs is not less than 16. Moreover, since 16 is the next value (after 20 and 18), the elimination of these two largest values will provide its maximum value for some modified DES cipher. But, as shown above, this elimination happens if $\pi_7 = 4$. Finally, the effectiveness of the best 1-round characteristics in this case equals, of course, to 16/64 = 0.25.

(iii) This follows from (i), (ii), and the fact that best 3-round characteristic can be constructed using twice a best 1-round non-trivial characteristic (see Proposition 4 (ii) in [3]). To compute the effectiveness of those best 3-round characteristics, we apply the Piling-up Lemma. ■

Remark 1. For completeness, notice that due to the special Feistel structure, the task for finding effective linear approximations for 2-rounds of the considered ciphers is reduced to the 1-round task for the two halves of the plaintext/ciphertext

block. That is why we do not pay special attention to the issues of 2-round linear cryptanalysis.

5. Optimal linear characteristics for many rounds

In the general case an exhaustive search over all members of the considered family of ciphers is carried out in order to find globally optimal best multi-round characteristics. Also, let us mention that finding best characteristics for each individual cipher is performed by the algorithm from [3] specially designed for this purpose.

5.1. Optimal characteristics with respect to better opportunities for attacking

Looking for optimal parity mask patterns in this case means searching of

$$\max_{\pi} \max_{l} \{\text{eff}\},$$

where l is a linear characteristic for the corresponding number of rounds, eff is its effectiveness and π is a combination of the eight parity bit masks.

The results are contained in the Table 1 where the effectiveness of the best linear characteristics in three instances is compared.

Table 1. Maximizing the effectiveness of the best characteristics

n	DES	Equal parity positions		Maximizing patterns		
	Effectiveness	Max effectiveness	Mask	Max effectiveness	Number	Pattern
3	0.781×2^{-2}	0.632×2^{-2}	8	0.632×2^{-2}	49152	11 112 812
4	0.976×2^{-4}	0.562×2^{-4}	1	$*0.765\times2^{-4}$	4096	11 241 821
5	0.610×2^{-5}	0.562×2^{-5}	1	$*0.765\times2^{-5}$	4096	11 184 821
6	0.976×2^{-8}	0.703×2^{-8}	1	$*0.717\times2^{-8}$	2304	11 422 118
7	0.976×2^{-9}	0.527×2^{-9}	1	0.527×2^{-9}	4096	11 121 418
8	0.610×2^{-10}	0.703×2^{-11}	1	0.703×2^{-11}	4096	11 121 412
9	0.953×2^{-13}	0.878×2^{-13}	1	0.878×2^{-13}	4096	11 121 212
10	0.762×2^{-14}	0.659×2^{-14}	1	0.659×2^{-14}	4096	11 111 114
11	0.953×2^{-15}	0.988×2^{-16}	1	0.988×2^{-16}	4096	11 111 888
12	0.596×2^{-16}	0.659×2^{-17}	1	0.659×2^{-17}	4096	11 121 242
13	0.745×2^{-18}	0.878×2^{-19}	1	0.878×2^{-19}	4096	11 121 218
14	0.596×2^{-20}	0.617×2^{-20}	1	0.617×2^{-20}	4096	11 121 412
15	0.596×2^{-21}	0.926×2^{-22}	1	0.926×2^{-22}	4096	11 121 244
16	0.745×2^{-23}	0.617×2^{-23}	1	0.617×2^{-23}	4096	11 121 411
17	0.582×2^{-25}	0.772×2^{-25}	1	0.772×2^{-25}	4096	11 121 411
18	0.931×2^{-27}	0.579×2^{-26}	1	0.579×2^{-26}	4096	11 121 221
19	0.582×2^{-27}	0.869×2^{-28}	1	0.869×2^{-28}	4096	11 111 842
20	0.727×2^{-10}	0.579×2^{-29}	1	0.579×2^{-29}	4096	11 121 288

The first is for the original DES algorithm, the second is when the parity bit positions are the same for all S-boxes as in [3], and the third is about optimal pattern of parity bit positions when the maximal effectiveness of the best characteristics is achieved. Examples for optimal masks are given in the second multi-column; in the third one, the number of optimal mask patterns is given together with examples of patterns. All computations are performed for 3-20 rounds. The patterns are given as sequences of the values of parity bit masks for all S-boxes.

It can be seen that experimentally determined number $49152 = 4^8 - 4^7$ of optimal patterns for 3 rounds is in agreement with Theorem 2(i). The same holds for the computed effectiveness, which is in correspondence with Theorem 2(iii).

The effectiveness values that are greater than those for the original cipher are given in italic in the table. The presence of only few of them confirms the tendency that the effectiveness of the best characteristics for larger number of rounds mostly diminish but may even grow depending on the parity bit position.

The values of (globally) maximal effectiveness are marked by *; they are better than the corresponding values for fixed parity position in all S-boxes. The existence of such instances leads to the conclusion that *independent choice of parity bit positions may provide better opportunities for attacking*.

5.2. Optimal characteristics with respect to resistance against attacking

Here, we consider the task for optimization in opposite direction, i.e. to assure maximal resistance against attacking. Using the same notations as in the previous subsection the search yields the form

$$\min_{\pi} \max_{l} \{\mathrm{eff}\}.$$

Correspondingly, Table 2 comprises the results of the performed search.

Table 2. Minimizing the effectiveness of the best characteristics

n	DES	Equal parity positions		Minimizing patterns		
	Effectiveness	Max effectiveness	Mask	Max effectiveness	Number	Pattern
3	0.781×2^{-2}	0.500×2^{-2}	4	0.500×2^{-2}	16384	11 111 141
4	0.976×2^{-4}	0.820×2^{-5}	2	$*0.632\times2^{-5}$	224	84 148 281
5	0.610×2^{-5}	0.878×2^{-7}	2	$*0.711\times2^{-7}$	200	81 122 221
6	0.976×2^{-8}	0.527×2^{-10}	8	$*0.738\times2^{-11}$	330	21 222 281
7	0.976×2^{-9}	0.820×2^{-13}	2	0.820×2^{-13}	3072	21 112 221
8	0.610×2^{-10}	0.738×2^{-15}	2	$*0.732\times2^{-15}$	184	81 812 241
9	0.953×2^{-13}	0.562×2^{-17}	2	$*0.861\times2^{-18}$	464	22 222 888
10	0.762×2^{-14}	0.562×2^{-20}	2	$*0.984\times2^{-21}$	674	21 212 281
11	0.953×2^{-15}	0.861×2^{-22}	2	$*0.738\times2^{-22}$	184	81 812 241
12	0.596×2^{-16}	0.562×2^{-24}	2	$*0.791\times2^{-25}$	560	21 212 281
13	0.745×2^{-18}	0.711×2^{-27}	2	0.711×2^{-27}	1652	21 212 221
14	0.596×2^{-20}	0.830×2^{-30}	2	0.830×2^{-30}	2348	21 212 221
15	0.596×2^{-21}	0.562×2^{-31}	2	$*0.922\times2^{-32}$	1728	21 112 281
16	0.745×2^{-23}	0.830×2^{-34}	2	$*0.791\times2^{-34}$	184	81 812 241
17	0.582×2^{-25}	0.968×2^{-37}	2	0.968×2^{-37}	1664	21 224 484
18	0.931×2^{-27}	0.562×2^{-38}	2	$*0.553\times2^{-39}$	770	22 222 282
19	0.582×2^{-27}	0.968×2^{-41}	2	$*0.830\times2^{-41}$	184	81 812 241
20	0.727×2^{-10}	0.889×2^{-44}	2	0.889×2^{-44}	1808	21 212 221

It can be seen again that the experimentally determined number $16384 = 4^7$ of optimal patterns for 3 rounds is in agreement with Theorem 2 (ii). The same holds in respect to the effectiveness which equals to the already proven in Theorem 2 (iii).

The values of minimal effectiveness of the best characteristics which cannot be reached when the parity bit position is the same for all S-boxes are marked by *. It can be seen that there are a lot of such instances. Their existence means that *by independent choice of parity bit positions one could design ciphers with better resistance towards linear attacks*.

6. Conclusion

In this work, we have studied a large family of ciphers derivable from the DES and having an endowment to thwart differential and some fault-injection attacks. Presumably, by their construction these ciphers are suspected to be vulnerable in linear attacks. After examining the strength of them against linear cryptanalysis, we could conclude that they possess good resistance (in most cases even better than the DES itself) towards the primary attacks of indicated type. However, before final recommendation, it remains to investigate the behavior of these ciphers against the existing more sophisticated forms of linear cryptanalysis. But, in any case, their practical utilization has to be preceded by a well-considered preprocessing on the primary clear data bearing in mind the lessons from [1].

***Acknowledgments*:** This work was partially supported under the Bulgarian NSF contract I01/0003. The second author is also with South-Western University (Faculty of Mathematics and Natural Sciences), Blagoevgrad, Bulgaria.

References

1. Angelova, V., Y. Borissov. Plaintext Recovery in DES-Like Cryptosystems Based on S-Boxes with Embedded Parity Check. – Serdica Journal of Computing, Vol. **7**, 2013, No 3, pp. 257-270.
2. Biham, E., A. Shamir. Differential Cryptanalysis of DES-Like Cryptosystems. – Journal of Cryptology, Vol. **4**, 1991, No 1, Springer, pp. 3-72.
3. Borissov, Y., P. Boyvalenkov, R. Tsenkov. Linear Cryptanalysis and Modified DES with Parity Check in the S-Boxes. – In: 2nd Conference on Cryptography and Information Security in the Balkans, LNCS, Vol. **9540**, Springer, 2016, pp. 60-78.
4. Coppersmith, D. The Data Encryption Standard (DES) and Its Strength Against Attacks. – IBM Journal of Research and Development, Vol. **38**, 1994, No 3, pp. 243-250.
5. Cusick, T. W., P. Stanica. Cryptographic Boolean Functions and Applications. San Diego, Academic Press, Elsevier Inc., 2009.
6. Hellman, M., R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohlig, P. Schweitzer. Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard. – SEL **76-042**, 9 September 1976.
7. Konheim, A. G. Computer Security and Cryptography. New Jersey, John Wiley & Sons, Inc., 2007.
8. Matsui, M. Linear Cryptanalysis Method of DES Cipher. – Advances in Cryptology – EUROCRYPT'93, LNCS, Vol. **765**, Springer, 1994, pp. 386-397.
9. Matsui, M. Linear Cryptanalysis of DES Cipher (I), Version 1.03.
   http://www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/Matsui-LC.pdf
10. Matsui, M. The First Experimental Cryptanalysis of the Data Encryption Standard. – In: Advances in Cryptology – CRYPTO'94, LNCS, Vol. **839**, Springer, 1994, pp. 1-11.
11. Nyberg, K. On the Construction of Highly Nonlinear Permutation. – In: Advances in Cryptology – EUROCRYPT'92, LNCS, Vol. **658**, Springer, 1993, pp. 92-98.
12. Pieprzyk, J., C. Charnes, J. Seberry. On the Immunity of S-Boxes Against Linear Cryptanalysis.
    citeseerx.ist.psu.edu
13. Schneier, B. Applied Cryptography. Second Edition. New Jersey, John Wiley & Sons, Inc., 1996.