Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 284–289*

Narrow Sense Linear Cryptanalysis of a Family of Modified DES Ciphers with Even Weight S-boxes

Robert Tsenkov rcenkov@abv.bg
IMI-BAS, G. Bontchev Str. 8, 1113 Sofia, BULGARIA
Yuri Borissov youri@math.bas.bg
IMI-BAS, G. Bontchev Str. 8, 1113 Sofia, BULGARIA

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. It turns out, depending on the particular encodings, 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. This research extends in a natural way [1].

1 Introduction and Motivation

Although the main topic of [2] is to show some of the safeguards built into the DES algorithm against differential cryptanalysis, there has been pointed out also a design criterion which is related to the method known as "linear cryptanalysis" [5]. Hereinafter, for the reader's convenience we recall that criterion in its stronger form $(S-2')$ [2, 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 [3]). That is why, as pointed out in [2], 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 vectorial 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 [6], 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, in summary [4, p. 301]).

In [1], it is investigated the resistance against linear cryptanalysis (for short LC) 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, some-how unexpectedly, that 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 [1] at BalkanCryptSec 2015, Prof. K. Nyberg asked what would be the behavior 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.

2 Background

LC is a powerful technique for cryptanalysis of the modern block ciphers developed in the early 1990s [5]. 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 $\mathbf{P}, \mathbf{C}$ and $\mathbf{K}$ 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 $\mathbf{B}$. Among these relations (also called linear characteristics), the most valuable for cryptanalysis are those, effective ones, that hold true with probability deviating significantly from $1/2$. When a linear approximation holds with probability $p \neq 1/2$ for randomly given plaintext P and the corresponding ciphertext C, the magnitude $e = |p - 1/2|$, represents the *effectiveness* of that approximation. A linear characteristic is called *best characteristic* if the effectiveness of corresponding linear approximation is maximal. Let us remind as well that the number of plaintext/ciphertext pairs needed for a successful linear attack, is proportional to e^{-2}.

DEFINITION 2.1 *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 $0 \leq \alpha \leq 2^m - 1$ and $0 \leq \beta \leq 2^n - 1$, let $NS(\alpha, \beta)$ 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 "centered" value*

$$\mathcal{L}S(\alpha, \beta) = NS(\alpha, \beta) - 2^{m-1}$$

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

The effectiveness of a linear approximation of an S-box is deduced directly from its LAT, while the effectiveness of a round approximation (e.g. in Feistel networks) which involve two or more S-boxes can be computed applying in suitable way the so-called Piling-up Lemma from [5].

To present our results, we need some conventions and notations. We assume only even parity embedding. Parity 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 denote by $\mathcal{L}S(\pi; \alpha, \beta)$ the LAT's values of the S-box obtained through embedding a parity bit with mask π into the box S.

Proposition 2.2 *([1]) Let S_k be an S-box of the DES, π be a parity mask, and & denote tuple-wise* AND *operator. Then if $\alpha, \beta \neq 0$ it holds:*

(i) $\mathcal{L}S_k(\pi; \alpha, \beta) = \mathcal{L}S_k(\alpha, \beta)$ *for all α and β such that $\beta \& \pi = 0$;*
(ii) $\mathcal{L}S_k(\pi; \alpha, \beta) = \mathcal{L}S_k(\alpha, 15 - \beta)$ *for all α and $\beta < 15$ such that $\beta \& \pi \neq 0$;*
(iii) $\mathcal{L}S_k(\pi; \alpha, 15) = 0$ *for all α.*

We'd like to stress that, similarly to [1], the present work is focused on the *narrow* sense linear cryptanalysis. I.e., it is confined *within the framework of a LC with no more than one active S-box per round*, since our primary goal is to compare the results with those obtained for the original cipher [5] and the modified DES ciphers from [1] in this particular case of interest.

The next theorem shows the decreasing effectiveness for the DES-like ciphers considered in [1] when the number of rounds is small.

Theorem 2.3 *Every parity mask applied to the S-boxes of the DES leads to a reduction of the maximal effectiveness for the* 1*-round and* 3*-round versions of that cipher.*

In summary, the experiments from [1] show that multi-round LC against those ciphers has varying magnitude of complexity depending on the parity position chosen. 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 [1].

3 Optimal Linear Characteristics

First, we recall that subject of the present work is a family of modified DES ciphers whose parity position for each individual S-box is chosen independently at random. This family, of course, contains the ciphers considered in [1].

3.1 For Small Number of Rounds

To derive the effectiveness of the best 1-round characteristics in this case, we perform a thorough analysis of the LATs of the original DES.

DEFINITION 3.1 *The entry* $\mathcal{L}S_k(\alpha,\beta)$, $1 \le \alpha \le 63$, $1 \le \beta \le 14$, *from the LAT of an* S_k *of the DES is called* invariant when applying parity check *(or simply* invariant*) if*

$$|\mathcal{L}S_k(\alpha,\beta)| = |\mathcal{L}S_k(\pi;\alpha,\beta)|$$

for each parity mask π.

Let I be the set of all invariant entries from LATs and $M_I := \max_{\mathcal{L}\in I} |\mathcal{L}|$. The next proposition shows the reasoning for Definition 3.1.

Proposition 3.2 *Let* π_k *be a parity mask applied to* S_k *of the DES,* $1 \le k \le 8$. *Then*

$$\max_{k,\alpha,\beta} \{|\mathcal{L}S_k(\pi_k;\alpha,\beta)|\} \ge M_I = 16,$$

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

As an immediate consequence, we obtain the following corollary.

Corollary 3.3 *Under the assumptions of Proposition 3.2 and* $\overline{\pi} = (\pi_1, \pi_2, \ldots, \pi_8)$, *we have*

$$\min_{\overline{\pi}} \max_{k,\alpha,\beta} \{|\mathcal{L}S_k(\pi_k;\alpha,\beta)|\} \ge 16.$$

Theorem 3.4 *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 iff* $\pi_7 \ne 4$. *There are exactly two 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 equal to* 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.*

Proofs of the aforementioned statements will be presented in an extended paper.

3.2 For Many Rounds

Looking for optimal parity mask patterns means either searching of

$$\max_{\overline{\pi}} \max_{l} \{e(l)\}$$

or

$$\min_{\overline{\pi}} \max_{l} \{e(l)\},$$

depending on the aims: either to determine when the conditions for attacking are more favorable or to increase cipher's resistance, respectively. In the above, $\overline{\pi}$ denotes the combination of the eight parity masks for the corresponding cipher, and $e(l)$ denotes the effectiveness of linear characteristic l obtained through narrow sense LC.

In order to find globally optimal best multi-round characteristics, a search by computer over all ciphers from the considered family was carried out, and the determination of the maximal effectiveness for each individual cipher was done by the add-hoc algorithm from [1].

The specific numerical results for 3 to 20 rounds will be published in the extended paper due to lack of space. In summary, these results show that:

- For 3 rounds, there is an agreement with Theorem 3.4;
- There are no modified DES ciphers with worse resistance towards narrow sense LC than the DES itself except for 5,14,17 and 18-round versions;
- There are no modified DES ciphers providing better opportunities for linear attacks comparing with the DES-like ciphers from [1] excluding 4,5 and 6-round versions;
- For all rounds, by independent choice of parity positions one can construct ciphers with better resistance towards linear attacks than the DES; the same holds true in regard to the DES-like ciphers from [1] except for 3,7,13,14,17 and 20-round versions (in the latter cases the best maximal effectiveness coincide).

4 Conclusion

In this work, we have studied an wide 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, the resistance of these ciphers against other known forms of linear cryptanalysis should be investigated.

References

[1] Y. Borissov, P. Boyvalenkov, R. Tsenkov: *Linear cryptanalysis and modified DES with parity check in the S-boxes,* Second Conference on Cryptography and Information Security in the Balkans: Springer LNCS 9540, pp. 60 - 78, (2016).

[2] D. Coppersmith: *The Data Encryption Standard (DES) and its strength against attacks,* IBM Journal of Research and Development 38(3), pp. 243-250 (1994).

[3] M. Hellman, 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, Sept. 9, 1976.

[4] A.G. Konheim: *Computer Security and Cryptography.* John Wiley & Sons Inc., New Jersey, 2007.

[5] M. Matsui: *Linear cryptanalysis of DES cipher (I), version 1.03.* Available from http://www.cs.bilkent.edu.tr/˜selcuk/teaching/cs519/Matsui-LC.pdf

[6] K. Nyberg, *On the construction of highly nonlinear permutation,* EUROCRYPT'92: Springer LNCS 658, pp. 92-98.