Noname manuscript No.
(will be inserted by the editor)

Linear and Differential Analysis of Small-Sized Random S-Boxes

Y. Alsalami · M. Khonji · C. Y. Yeun · T. Martin

Received: date / Accepted: date

Abstract S-boxes are used in cryptography in order to provide non-linearity in the design of cryptographic primitives such as block ciphers and hash functions. Some cryptographic primitives use bijective S-boxes as in the Advanced Encryption Standard (AES), and others use surjective S-boxes as in the Data Encryption Standard (DES). S-boxes can have inputs and outputs of the same length, i.e., 8 bits as in the case of AES (denoted by, $(8, 8)$-S-box), or alternatively their input length can be larger than its output length, i.e., 6 input bits to 4 output bits as in the case of DES (denoted by, $(6, 4)$-S-boxes). In this paper, we perform a statistical study of the linear and differential properties of randomly generated (n, m)-S-boxes, where $m \leq n$. We show that certain S-boxes with *good* linear and differential properties can be feasibly obtained via random search. We show further that certain types of S-boxes with specific desirable linear and differential properties are improbable to occur randomly if not impossible.

1 Introduction

Electronic communications nowadays are based on cryptographic primitives in order to provide confidentiality of the information being transmitted. Shanon in his seminal paper [18] highlighted two important concepts required to design any cryptographic primitive, namely, confusion and diffusion. Confusion means to provide as complex as possible relationship between the plaintext,

Y. Alsalami, C. Y. Yeun, and T. Martin
Khalifa University of Science, Technology and Research
Abu Dhabi, UAE
E-mail: yousuf.salami,cyeun,thomas.martin@kustar.ac.ae

M. Khonji
Masdar Institute of Science and Technology
Abu Dhabi, UAE
E-mail: mkhonji@masdar.ac.ae

the ciphertext and the key, is achieved nowadays by the use of nonlinear components in the design, such as the use of S-boxes. Diffusion, on the other hand, means to spread out the relationship between these bits as fast as possible, which is now achieved by the use of MDS (Maximum Distance Separable) [21] and Pseudo-Hadamard Transform [11] matrices for example.

S-boxes are crucial components of any cryptographic primitive. If such components are removed, these primitives can be easily broken by performing linear analysis to the inputs, outputs and the secret key. The secret key bits can then easily be deduced from the input and output bits using linear algebra methods like Gaussian elimination. Therefore, it is essential that the S-boxes used in any cryptographic primitive are nonlinear and very well crafted against linear attacks. The well-known block cipher AES uses a bijective S-box of 8 bits length for both input and output [20, 8], while DES block cipher uses 8 surjective S-boxes of 6 and 4 bits length for input and output, respectively [19]. Most other cryptographic primitives use either type of these S-boxes. For example, the PRESENT cipher uses bijective S-boxes of length 4 bits [5] and the hash function KECCAK uses a bijective S-box of length 5 bits [1].

In this paper, we study the linear and differential properties of bijective and surjective S-boxes. The procedure we follow is based on randomly generating large number of S-boxes of certain size, and we test their individual linear and differential indicators (See section 3 for formal definitions). Then, we keep the best and worst S-box generated so far with regard to these two measures. We also perform a statistical study of the S-boxes linear and differential properties. These two measures are used to thwart linear attacks and their generalizations of Matsui [12] and differential attacks of Biham and Shamir [4]. The linear indicator is intended to measure the linearity of the S-box we are using. (The lower this value, the better its resistance to linear attacks.) The differential indicator is also meant to measure the resistance of the S-box to differential attacks and its generalizations. (The lower this value, the better its resistance to differential attacks.) In block ciphers, designers use many rounds or iterations of simple functions in order to improve the overall performance of the cipher against both linear and differential attacks.

The rest of the paper is organized as follows. Section 2 presents the related work. Notations and methodology are presented in section 3. Section 4 presents the analysis on the tested DES-like S-boxes and their differential and linear properties. Section 6 discusses the future enhancements of our analysis and ideas to generalize to other types of S-boxes. Finally, Section 7 concludes our study.

2 Related Works

In the paper [2], the authors study the linear and differential properties of DES-like S-boxes which are balanced $(6, 4)$-function in which the four rows of their truth tables are each a permutation $(4, 4)$-function. They first generate random S-boxes suitable for use in the DES S-boxes of around 2^{20} or almost

$1,000,000$ of size 6 input bits and 4 output bits. Then, they test all of these S-boxes for their maximum linear and differential indicators. They also keep the best and worst S-boxes in terms of these two values. The authors also emphasize that their analysis is geared towards getting optimal S-boxes when having 6 input bits and 4 output bits against linear [12] and differential attacks [4].

Previously, O'Connor has studied probabilistically what is the expected value for linear and differential indicators [15, 13]. His studies only focus on bijective S-boxes and he did not analyze surjective S-boxes with respect to linear and differential S-boxes. He only studied DES-like S-boxes which are a specific type of surjective S-boxes but not all in his paper [14]. We in this paper fill out this gap at least numerically and deduce concrete conclusions on their behaviour. With our analysis, surjective S-boxes can be selected with care with respect to linear and differential attacks when used by cryptographers in their design of cryptographic primitives.

Also in [17], the author studies the distribution of the DES-like S-boxes with respect to all the design criteria imposed on the S-boxes of the DES as mentioned in [7] to be consistent with the other components of the design. The author however did not study the linear and differential properties of such S-boxes without these additional restrictive constraints.

In this paper, we study such type of S-boxes, that is $(6, 4)$-S-boxes, and others as well with respect to the most powerful linear and differential attacks. We assume that the designers can carefully choose the other components which mostly provide diffusion properties to the block cipher design. The optimal components with respect to the diffusion is well known in the literature by the usage of MDS and pseudo-Hadamard matrices as it is done in the design of the AES [8, 20], Khazad [3], ARIA [10] and Anubis [16] for example.

3 Notations and Methodology

3.1 Notations

In this subsection, we present standard metrics and notations that are widely adopted in cryptanalyzing any block cipher, and specifically their S-boxes [6]. Denote an (n, m)-S-box (or simply an S-box when the size of input and output is irrelevant) by $S(x)$ which is a vectorial Boolean (n, m)-function or simply an (n, m)-function. Let $\mathbb{F}_2^n$ denote the vector space of dimension n over the finite field $\mathbb{F}_2 = \{0, 1\}$. Let $\mathbb{F}_2^{n*}$ denote the vector space $\mathbb{F}_2^n$ without the all zero vector, i.e. $\mathbf{0} = (0, \cdots, 0)$. The binary dot product between two vectors a and b is defined as $a \cdot b = \sum_{i=0}^{n} a_i b_i$.

To measure how linear or nonlinear an S-box is, we use the following common measure:

Definition 1 (Linear Property Indicator) Let $S(x)$ be an (n, m)-S-box. The *linear property indicator* of an $S(x)$ is denoted by $L(S)$ and is defined as:

$$L(S) \triangleq \max_{\substack{a \in \mathbb{F}_2^{n*} \\ b \in \mathbb{F}_2^{m*}}} \left| \left| \{x \in \mathbb{F}_2^n \mid a \cdot x = b \cdot S(x)\} \right| - 2^{n-1} \right| \tag{1}$$

We define also the Walsh transform of any (n, m)-function as:

Definition 2 Let $S(x)$ be an (n, m)-S-box. We define the Walsh transform of $S(x)$ at $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ as the discrete Fourier transform:

$$W_S(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S(x) + u \cdot x}$$

A related term which is also used widely in literature is the *nonlinearity* or the *linearity* of an (n, m)-function, which is defined as:

Definition 3 Let $S(x)$ be an (n, m)-S-box. The nonlinearity of $S(x)$ is:

$$\begin{aligned} \mathcal{NL}(S) &= 2^{n-1} - \frac{1}{2} \max_{\substack{v \in \mathbb{F}_2^{m*} \\ u \in \mathbb{F}_2^n}} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot S(x) + u \cdot x} \right| \\ &= 2^{n-1} - \frac{1}{2} \max_{\substack{v \in \mathbb{F}_2^{m*} \\ u \in \mathbb{F}_2^n}} \left| W_S(u, v) \right|. \end{aligned}$$

The quantity $\mathcal{L}_{max}(S) = \max_{\substack{v \in \mathbb{F}_2^{m*} \\ u \in \mathbb{F}_2^n}} \left| W_S(u, v) \right|$ is often called the linearity of the S-box $S(x)$. It is easy to show that the linear indicator is directly related to the nonlinearity and linearity. This is shown as:

$$\mathcal{L}_{max}(S) \triangleq 2L(S). \tag{2}$$

and we have also:

$$\mathcal{NL}(S) \triangleq 2^{n-1} - L(S). \tag{3}$$

Similarly, to measure the differential property of any S-box, we have the following common measure which we refer to as the differential indicator:

Definition 4 (Differential Property Indicator) Let $S(x)$ be an (n, m)-S-box. The *differential uniformity* of $S(x)$ is denoted by $\delta_{max}(S)$ and is defined as:

$$\delta_{max}(S) \triangleq \max_{\substack{a \in \mathbb{F}_2^{n*} \\ b \in \mathbb{F}_2^{m}}} \left| \{x \in \mathbb{F}_2^n \mid S(x) + S(x + a) = b\} \right| \tag{4}$$

In general, in order to resist linear and differential attacks, the designer has to keep these values as low as possible. These measures or their equivalents are used by cryptographers to assess the block cipher resistance against such attacks. For example in the AES block cipher, the designers keep these values as low as possible using certain mathematical techniques to construct such S-boxes [8].

3.2 Random Generation of the S-boxes

In the phase of randomly generating $(6, 4)$-S-boxes, a random permutation is done according to the *Knuth's shuffle* which guarantees the uniformity of the random generation [9]. We used standard *rand()* function in the C library which is seeded by milliseconds. This is to ensure that we have different S-boxes for our testing phase later. It is observed that the *rand()* function behaves almost uniformly. Otherwise, one may end up generating similar S-boxes which will shrink the search space.

3.3 Random Generation Algorithm

Algorithm 1 RandGenerate

Require: An (n, n)-S-box initially filled sequentially with items from $S(0) = 0$ to $S(2^n - 1) = 2^n - 1$; Number of output bits m.
Ensure: Having a randomly generated (n, m)-S-box $S(x)$.
1: **for** i from 0 to $2^n - 2$ **do**
2: Take a random number j such that $0 \leq j \leq 2^n - 2$.
3: Swap $S(i)$ and $S(i + j)$.
4: **end for**
5: **for** i from 0 to $2^n - 2$ **do**
6: $S(i) \leftarrow S(i)$ modulo 2^m.
7: **end for**
8: **return** random (n, m)-S-box $S(x)$

3.4 Experiment Setup

In our experiments, we generated over 1 million random S-boxes. Each S-box is tested with differential and linear cryptanalysis. We implemented all tests using C programming language compiled with "-O3" optimization flag. A well optimized C implementation generally obtains far better running time than any other high level programming language. Additionally, since our basic operations are addition and multiplication, it is preferable to have a self-contained implementation with a good degree of simplicity rather than using off-the-shelf computer algebra software (e.g., Mathematica, PARI/GP). The machine specifications are illustrated in 3.4.

4 Analysis of the Randomly Generated DES-like S-boxes and their Distribution Table

In this section, we will present our linear and differential cryptanalysis on the DES-like S-boxes which we have generated using Knuth's Shuffle method.

Machine	Product	Intel(R) Core(TM)2 Duo CPU @ 1.66GHz
	RAM	1GB
	Bus	64 bits
Operating System	Linux 2.6.34 with GCC version 4.2.4	

Table 1 System configuration of the platform which performs the S-boxes testing

4.1 Distribution Table of the DES-like S-boxes in terms of their Linear and Differential Indicators

After running the test for 3,676 seconds or 1 hour and 1 minute, we have found the following distribution of the S-boxes in terms of their maximum differential and linear indicators. Also, the reader should be very clear that this test has been run several times and this is only one instance of these runs. The others look the same in terms of the distribution.

We present the distribution of these linear and differential indicators in Figure 1 and Table 2 and we note that we did not get values for the differential indicator higher than 30 and for the linear indicator lower than 10. It is important to keep in mind that for a linear or almost linear S-box, one can obtain easily higher values for the differential and linear indicators.

L\ δ_{max}	**12**	**14**	**16**	**18**	**20**	**22**	**24**	**26**	**28**	**Sums**
10	174	591	181	31	2	0	0	0	0	979
12	10559	131768	111500	30168	5338	796	105	7	0	290241
14	5469	161872	248296	98979	23385	4241	740	124	15	543121
16	413	26204	66551	37938	11219	2446	505	93	14	145383
18	8	1888	7760	6136	2151	523	118	20	2	18606
20	0	60	558	579	270	63	19	1	2	1552
22	0	0	23	45	29	7	2	1	0	107
24	0	0	1	1	0	0	0	0	0	2
Total	16623	322383	434870	173877	42394	8076	1489	246	33	

Table 2 Distribution of Linear L and Differential δ_{max} properties of randomly generated DES-like $(6, 4)$-S-boxes.

In fact to be more precise, we did not count the number of S-boxes where L or $\delta_{max} < 10$ or where L or $\delta_{max} > 28$. In fact, the output of running our program will print for you the S-boxes corresponding to these values exceptionally. Therefore, there is no loss of information here but only the counting is done excluding these extremes.

4.2 Best and Worst DES-like $(6, 4)$-S-boxes

The highest δ_{max} we have obtained is 30 and the lowest one is 12. For L, the highest L is 24 and the lowest L is 10. Therefore, the best S-box (i.e. with

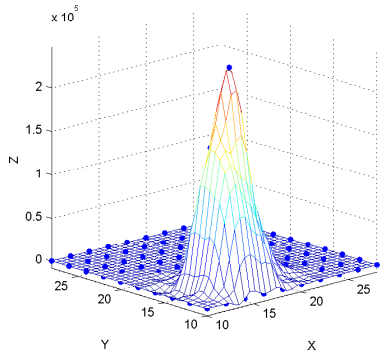

Fig. 1 Distribution of the differential and linear indicators of the random DES-like $(6, 4)$-S-boxes. The z-axis represents the the number of $(6, 4)$-S-boxes satisfying (δ_{max}, L) in the (x-axis,y-axis) respectively

the lowest L and δ_{max} together) is with $\delta_{max} = 12$ and $L = 10$. And the worst S-Box (i.e. with the highest L and δ_{max} together) is with $\delta_{max} = 28$ and $L = 20$ or when $\delta_{max} = 26$ and $L = 22$. Here we list some of the S-boxes with their δ_{max} and L values:

- S-box with worst found δ_{max}: This corresponds to Table 3.
- S-box with worst found L: This corresponds to Table 4.

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

Table 3 S-box with $\delta_{max} = 30$ and $L = 16$:

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

Table 4 S-box with $\delta_{max} = 16$ and $L = 24$:

– S-box with worst found δ_{max} and L: This corresponds to Table 5.

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

Table 5 S-box with $\delta_{max} = 26$ and $L = 20$:

– S-box with best found δ_{max} and L: This corresponds to Table 6.

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

Table 6 S-box with $\delta_{max} = 12$ and $L = 10$:

The maximum number of S-boxes which are generated randomly corresponds to the pair $(\delta_{max}, L) = (16, 14)$ which has almost 25% of the total number of S-boxes generated. Then, the next pair $(\delta_{max}, L) = (14, 14)$ has a percentage of 16% and thirdly the pair $(14, 12)$ according to Table 7.

We have used also simple C programs to produce the differential and linear distribution tables which corresponds to the DES $(6, 4)$-S-boxes as shown in Table 8 or other randomly generated S-boxes like the above ones.

Rank	(δ_{max}, L)	#S-boxes	Percentage
1	(16,14)	248,296	24.83%
2	(14,14)	161,872	16.19%
3	(14,12)	131,768	13.18%
4	(16,12)	111,500	11.15%
5	(18,14)	98,979	9.90%
6	(16,16)	66,551	6.66%
7	(18,16)	37,938	3.79%
8	(18,12)	30,168	3.02%
9	(14,16)	26,204	2.62%
10	Others	86,724	8.67%

Table 7 Rankings of the randomly generated DES-like $(6, 4)$-S-boxes classes in terms of their differential and linear indicators

DES S-box #	δ_{max}	L
1	16	18
2	16	16
3	16	16
4	16	16
5	16	20
6	16	14
7	16	18
8	16	16

Table 8 Differential and linear indicators of the DES $(6, 4)$-S-boxes

5 Analysis of Balanced Bijective and Surjective (n, m)-S-boxes where $m \leq n$

5.1 Analysis of $(4, m)$-S-boxes

We observe from Tables 9, 10 and 11 that we did not obtain any S-boxes with differential uniformity of 14. This is a nice observation but it does not directly affect the problem of choosing good S-boxes because a differential uniformity of 14 is a bad choice cryptographically. We also know from different sources that a bijective APN $(4, 4)$-function does not exist by exhaustively testing out all of these bijective $(4, 4)$-functions.

We also know from theory that bent $(4, 2)$-functions exist and have a differential uniformity of 4. However, they are not balanced. Also, we know that differentially 6-uniform $(4, 2)$-functions exist as well from Chapter 5. However,

it is not known whether all differentially 6-uniform $(4, 2)$-functions are not balanced or there exist some balanced ones.

$L\backslash\delta_{max}$	**4**	**6**	**8**	**10**	**12**	**14**	**16**	**RSum**
4	3595	4930	260	0	0	0	0	8785
6	1570	54612	27777	3541	256	0	1	87757
8	0	566	1631	927	323	0	11	3458
CSum	5165	60108	29668	4468	579	0	12	

Table 9 Distribution of Linear L and Differential δ_{max} properties of randomly generated $(4, 4)$-S-boxes.

$L\backslash\delta_{max}$	**6**	**8**	**10**	**12**	**14**	**16**	**RSum**
4	151789	156045	12001	1312	0	120	321267
6	36990	417731	180412	27397	0	232	662762
8	0	1995	6942	6561	0	473	15971
CSum	188779	575771	199355	35270	0	825	

Table 10 Distribution of Linear L and Differential δ_{max} properties of randomly generated $(4, 3)$-S-boxes.

$L\backslash\delta_{max}$	**8**	**10**	**12**	**14**	**16**	**RSum**
4	913658	4086404	1077119	0	42720	6119901
6	0	1844387	1914770	0	50178	3809335
8	0	0	48474	0	22290	70764
CSum	913658	5930791	3040363	0	115188	

Table 11 Distribution of Linear L and Differential δ_{max} properties of randomly generated $(4, 2)$-S-boxes.

5.2 Analysis of $(5, m)$-S-boxes

In this category of S-boxes, we have observed from these tables that when m decreases, the linear indicator values decrease and the differential uniformity increases. We know from Chapter 5 that differentially 6-uniform $(5, 3)$-functions exist but it is not known whether all of them are balanced or not. From Table **??** in Appendix B, this can be seen that possible differentially 6-uniform $(5, 3)$-S-boxes can occur if we test more S-boxes in this category as can be predicted from the values in this table.

Another important observation from these tables is that in Tables **??** and **??** in Appendix B we have balanced S-boxes having differential uniformity in the range $[2^{n-m}, 2^{n-m+1}]$. This gives an answer to this interesting question

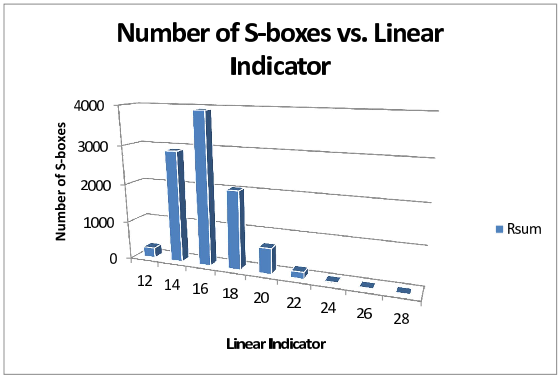

Fig. 2 Distribution of the linear indicators L of the random $(7, 1)$-S-boxes.

we have raised in Chapter 5 before. We know also that balanced APN $(5, 5)$-S-boxes exist within this category as with Gold, Kasami, Welch, Niho, Inverse and Dobbertin $(5, 5)$-functions. We also observe that the Boolean $(5, 1)$-S-boxes have a differential uniformity always divisible by 4. This observation is also visible in the $(7, 1)$-S-boxes as well. Whether this behaviour is specific to these Boolean $(n, 1)$-functions or for an of them is an interesting theoretical question.

When we plot the distribution of the randomly generated S-boxes versus the linear indicator we get the following probability distribution. In Figure 2, we plot the linear indicator versus the number of $(7, 1)$-S-boxes which are randomly generated and that satisfy each linear indicator. In other words, we plot the **RSum** of Table **??** from Appendix B. This probability distribution looks similar to that of a Gamma probability distribution with a given mean and spread factor. It remains open how to fit such graphs with the Gamma probability distribution.

In Figure 3, we plot the differential uniformity versus the number of $(7, 1)$-S-boxes which are randomly generated and that satisfy each differential uniformity, which we refer to by **CSum** in Table **??** from Appendix B.

6 Discussion and Further Enhancements

In order to improve our analysis, we propose the following enhancements to be done on our testing procedures and the following generalizations for our analysis as well:

– Testing more random S-boxes will give more insight into what can be done to improve the S-boxes of the DES until we reach all the possible DES $(6, 4)$-S-boxes. By testing more S-boxes, we can get possibly more insights into what is possible and impossible to get for the extreme low values of

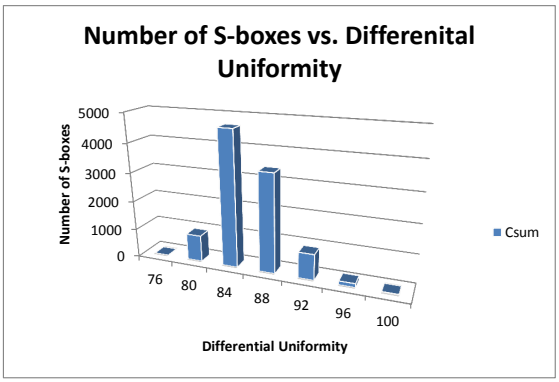

Fig. 3 Distribution of the differential uniformities δ_{max} of the random $(7,1)$-S-boxes.

the differential and linear indicator of these S-boxes when $\frac{n}{2} < m < n$ for n is even and when $m < n$ when n is odd.

- One can do improve the generation process by generating the random S-boxes only once and keeping track of such S-boxes generated so that one is certain that some S-boxes do not occur twice or more. Even though the method we are using does not generate much repetition of S-boxes, it will give more certain results.
- One can implement the additional criteria of the S-boxes of DES mentioned in [7] in order to eliminate so many of the randomly selected S-boxes and cryptanalyze such S-boxes. This would guarantee efficient elimination and sieving procedure for such a large number of possible S-boxes.

7 Conclusion

AES and DES S-boxes are not randomly selected but they have been tested against many cryptanalysis attacks taken into consideration at the design stages. However, at that time when DES was designed their S-boxes were chosen to thwart differential attacks but not all types of linear attacks as stated by Coppersmith in [7]. Coppersmith also mentioned that they have designed DES S-boxes to avoid other attacks as well which are not covered in our cryptanalysis here. AES on the other hand has been selected to withstand both linear and differential attacks. Additionally, our cryptanalysis based on linear and differential characteristics provides a very good and essential tool for testing bijective S-boxes, as in AES, and surjective S-boxes, as in DES, for any block cipher which have to be resistant against differential and linear cryptanalysis. We have seen that the linear and differential properties for these types of S-boxes follow a certain probability distribution most likely the

Gamma distribution. It remains open what are the exact parameters for this probability distribution. We also hope that our analysis can stimulate more research in proving the existence or in-existence of certain types of surjective (n, m)-S-boxes.

References

1. 202 FP (2015) Sha-3 standard: Permutation-based hash and extendable-output functions. Information Technology Laboratory, National Institute of Standards and Technology
2. Alsalami Y, Martin T, Yeun CY (2015.) Linear and differential properties of randomly generated des-like substitution boxes. Lecture Notes in Electrical Engineering 330:517–524
3. Barreto P, Rijmen V (2000) The khazad legacy-level block cipher. Primitive submitted to NESSIE 97
4. Biham E, Shamir A (1991) Differential cryptanalysis of des-like cryptosystems. Journal of CRYPTOLOGY 4(1):3–72
5. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C (2007) PRESENT: An ultra-lightweight block cipher. Springer
6. Carlet C (????) Vectorial boolean functions for cryptography. chapter of the monography boolean methods and models, y. crama and p. hammer eds
7. Coppersmith D (1994) The data encryption standard (des) and its strength against attacks. IBM journal of research and development 38(3):243–250
8. Daemen J, Rijmen V (1998) Aes proposal: Rijndael
9. Knuth D (1968) The art of computer programming 1: Fundamental algorithms 2: Seminumerical algorithms 3: Sorting and searching
10. Kwon D, Kim J, Park S, Sung SH, Sohn Y, Song JH, Yeom Y, Yoon EJ, Lee S, Lee J, et al (2004) New block cipher: Aria. In: Information Security and Cryptology-ICISC 2003, Springer, pp 432–445
11. Massey JL (1994) Safer k-64: A byte-oriented block-ciphering algorithm. In: Fast Software Encryption, Springer, pp 1–17
12. Matsui M (1994) Linear cryptanalysis method for des cipher. In: Advances in CryptologyEUROCRYPT93, Springer, pp 386–397
13. O'Connor L (1994) On the distribution of characteristics in bijective mappings. In: Advances in CryptologyEUROCRYPT93, Springer, pp 360–370
14. O'Connor L (1994) On the distribution of characteristics in composite permutations. In: Advances in CryptologyCRYPTO93, Springer, pp 403–412
15. O'Connor L (1995) Properties of linear approximation tables. In: Fast Software Encryption, Springer, pp 131–136
16. Rijmen V, Barreto P (2000) The anubis block cipher. Submission to NESSIE

17. Roelse P (2007) The design of composite permutations with applications to des-like s-boxes. Designs, Codes and Cryptography 42(1):21–42
18. Shannon CE (1949) Communication theory of secrecy systems. Bell Systems Technical Journal 28(4):656–715
19. of Commerce: National Institute of Standards USD, Technology (1977) Data encryption standard. In: In FIPS PUB 46-2, Federal Information Processing Standards Publication
20. of Commerce: National Institute of Standards USD, Technology (2001) Advanced encryption standard. In: In FIPS PUB 197, Federal Information Processing Standards Publication, pp 19–22
21. Vaudenay S (1995) On the need for multipermutations: Cryptanalysis of md4 and safer. In: Fast Software Encryption, Springer, pp 286–297