Paper

Distribution of the best nonzero differential and linear approximations of s-box functions

Krzysztof Chmiel

Abstract— In the paper the differential and the linear approximations of two classes of s-box functions are considered. The classes are the permutations and arbitrary functions with n binary inputs and m binary outputs, where $1 \le n = m \le 10$. For randomly chosen functions from each of the classes, the two-dimensional distributions of the best nonzero approximations are investigated. The obtained results indicate that starting from some value of n, the linear approximation of s-box functions becomes more effective than the differential approximation. This advantage of the linear approximation rises with the increase of n and for DES size s-boxes is not yet visible.

Keywords— differential cryptanalysis, linear cryptanalysis, substitution boxes.

1. Introduction

Differential and linear cryptanalysis belong to main topics in cryptology since they were introduced and successfully applied to the data encryption standard (DES). Unlike the differential cryptanalysis, which is essentially a chosen-plaintext attack [1, 10, 11], the linear cryptanalysis is essentially a known-plaintext attack and moreover is applicable to an only-ciphertext attack under some circumstances [2–12].

The basic idea of differential cryptanalysis is to analyze the effect of particular differences in plaintext pairs on the differences of the resultant ciphertext pairs. The differences are usually calculated as a result of XOR operation. Input XOR of a cipher algorithm causes a specified output XOR with some probability. The appropriate, approximate expression will be called the differential approximation. By the *differential approximation* of function $Y = f(X) : \{0,1\}^n \to \{0,1\}^m$ we mean an arbitrary equation of the form:

$$f(X) \oplus f(X \oplus X') = Y',$$

which is fulfilled with approximation probability $p = N(X',Y')/2^n$, where $X' \in \{0,\ldots,2^n-1\}, Y' \in \{0,\ldots,2^m-1\}$ and $N(X', Y')$ denotes the number of input pairs $(X, X \oplus X')$ for which the equation holds. The numbers X', Y' are called input and output *difference* respectively and the function $N(X',Y')$ is called the *counting function* of the approximation. The magnitude of p represents the *effectiveness* of the approximation. Among approximations we distinguish the *zero differential approximation* with $X' = Y' = 0$, which probability p is equal to 1 for arbitrary function f.

The basic idea of linear cryptanalysis is to describe a given cipher algorithm by a linear approximate expression, so-called linear approximation. In general, the *linear approximation* of function $Y = f(X) : \{0,1\}^n \to \{0,1\}^m$ is defined as an arbitrary equation of the form:

$$\bigoplus_{i \in Y'} y_i = \bigoplus_{j \in X'} x_j,$$

which is fulfilled with approximation probability $p = N(X',Y')/2^n$, where $X' \subseteq \{1,\ldots,n\}$, $Y' \subseteq \{1,\ldots,m\}$ and $N(X',Y')$ denotes the number of pairs (X,Y) for which the equation holds. The sets of indexes X',Y' are called input and output *mask* respectively and the function $N(X',Y')$ is called the *counting function* of the approximation. The *effectiveness* of the approximation is represented by magnitude of $|\Delta p| = |p - 1/2|$. By the *zero linear approximation* we mean approximation with $X' = Y' = \Phi$, which probability p is equal to 1 for arbitrary function f. Masks X',Y' are often denoted by numbers, corresponding to the zero-one representation of sets.

The set of all differential approximations of function f can be described in the form of the *approximation table* TDf, called in [1] the *difference distribution table*. The element $TDf[X',Y']$ of the table, is defined as follows:

$$TDf[X',Y'] = N(X',Y').$$

The maximum value of TDf, that corresponds to the best, i.e., most effective, nonzero differential approximation, is denoted by $\max TD$ and is defined by formula:

$$\max TD = \max\{TDf[X',Y'] : X' \neq 0 \vee Y' \neq 0\}.$$

Similarly, the set of all linear approximations of function f is represented in the form of the *approximation table* TAf. The element $TAf[X',Y']$ of the table, is defined as follows:

$$TAf[X',Y'] = \Delta N(X',Y') = N(X',Y') - 2^{n-1}.$$

The maximum absolute value of TAf, which corresponds to the best nonzero linear approximation, is denoted by $\max TA$ and is defined in the following way:

$$\max TA = \max\{|TAf[X',Y']| : X' \neq \Phi \vee Y' \neq \Phi\}.$$

The approximation tables of an example function f are presented in Table 1. There exist many effective approximations of the function, identified by nonzero values of

Table 1
Function f and its approximation tables TDf and TAf ($n = 4$, $m = 2$)

f		TDf					TAf				
X	$Y = f(X)$	X'	Y'				X'	Y'			
			0	1	2	3		0	1	2	3
0	3	0	16	0	0	0	0	8	–2	–1	1
1	3	1	10	0	2	4	1	0	–2	1	–1
2	3	2	6	0	2	8	2	0	0	1	1
3	0	3	6	0	2	8	3	0	0	3	–1
4	1	4	2	8	6	0	4	0	0	–1	**7**
5	3	5	2	8	6	0	5	0	0	–3	1
6	1	6	0	2	**12**	2	6	0	2	1	–1
7	1	7	2	4	10	0	7	0	2	–1	1
8	0	8	4	2	0	10	8	0	–4	1	1
9	0	9	2	0	2	**12**	9	0	0	–1	–1
10	3	10	8	2	0	6	10	0	–2	–5	1
11	3	11	8	2	0	6	11	0	2	1	–1
12	1	12	0	6	8	2	12	0	2	–3	–1
13	2	13	0	6	8	2	13	0	–2	–1	1
14	2	14	2	8	6	0	14	0	–4	–1	–1
15	2	15	2	**12**	2	0	15	0	0	1	1

the tables. The best nonzero differential approximations have $\max TD = 12$ and probability $p = 12/16$, while the best nonzero linear approximation has $\max TA = 7$ and probability $|\Delta p| = 7/16$.

The size of the approximation tables TDf and TAf of function f is equal to 2^{n+m} and the basic algorithms compute a single element of the tables in exponential time. The used in the investigation fast algorithms, presented in detail in [10], compute the approximation tables in time at worst linear for a single element, without memory needed for storage of the whole table.

2. Results

The presented in this chapter results of experiments concern the distribution of the best nonzero differential and linear approximations of two classes of s-box functions $Y = f(X)$. The classes are the permutations and arbitrary functions of the type $f : \{0,1\}^n \to \{0,1\}^m$, for $1 \le n = m \le 10$. For each value of n, the investigation was carried out for 1000 randomly chosen functions from the class. For each function, with use of the mentioned in the previous chapter fast algorithms, were calculated values of $\max TD$ and $\max TA$. Distribution of pairs $(\max TD, \max TA)$ was the goal of the computation. The obtained results are presented in Figs. 1–19.

For $n = m = 1$ (Fig. 1), the proportional distributions obtained for permutations and arbitrary functions are identical. For 100% of functions, from each of the classes, the obtained pair $(\max TD, \max TA)$ is equal to (2, 1).

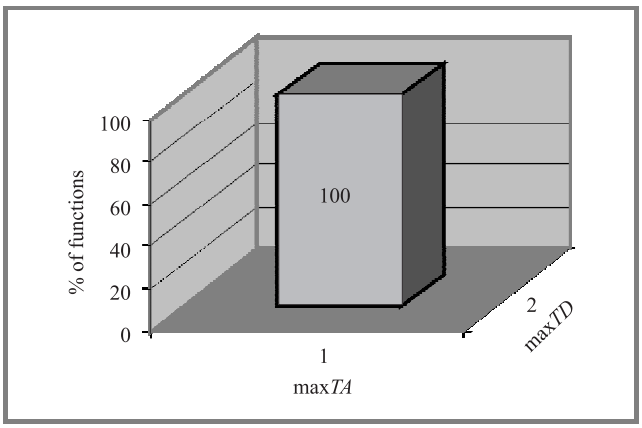

Fig. 1. Distribution for permutations and arbitrary functions ($n = 1$, $m = 1$).

For $n = m = 2$ (Figs. 2 and 3), the distributions for permutations and arbitrary functions differ. For 100% of permutations, the obtained pair $(\max TD, \max TA)$ is equal

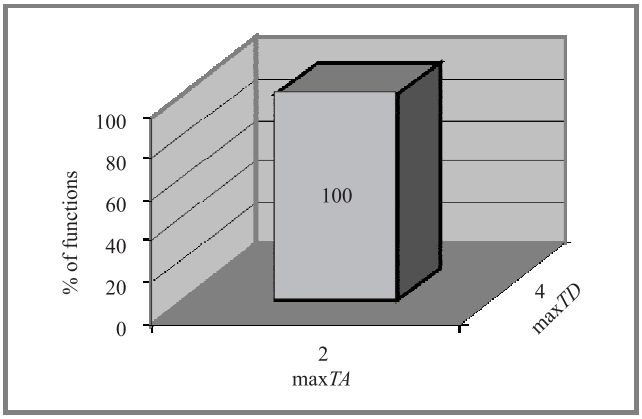

Fig. 2. Proportional distribution for permutations ($n = 2$, $m = 2$).

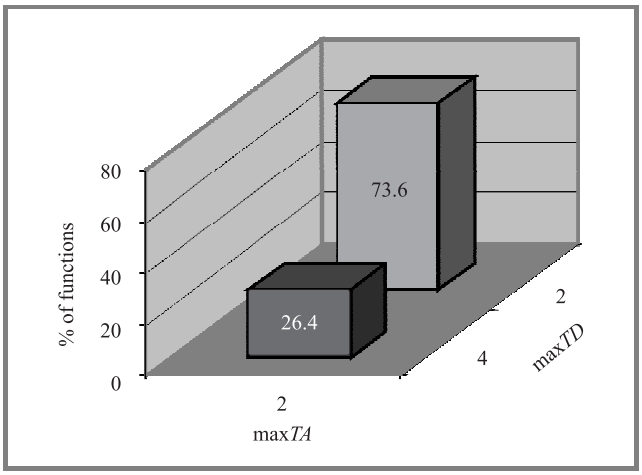

Fig. 3. Proportional distribution for arbitrary functions ($n = 2$, $m = 2$).

to (4, 2). For arbitrary functions, the same pair (4, 2) is obtained for 26.4% of functions while for remaining 73.6% of functions is obtained pair (2, 2). The results indicate, that

resistance to linear approximation of permutations and arbitrary functions with two input and output bits is the same, while about 3/4 of arbitrary functions are more resistant to differential approximation than permutations.

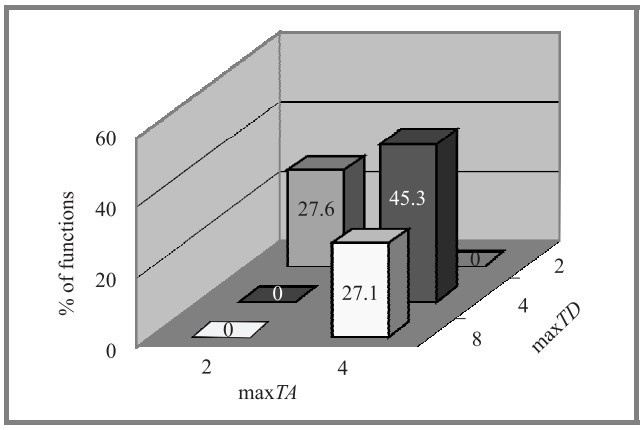

Fig. 4. Proportional distribution for permutations ($n = 3$, $m = 3$).

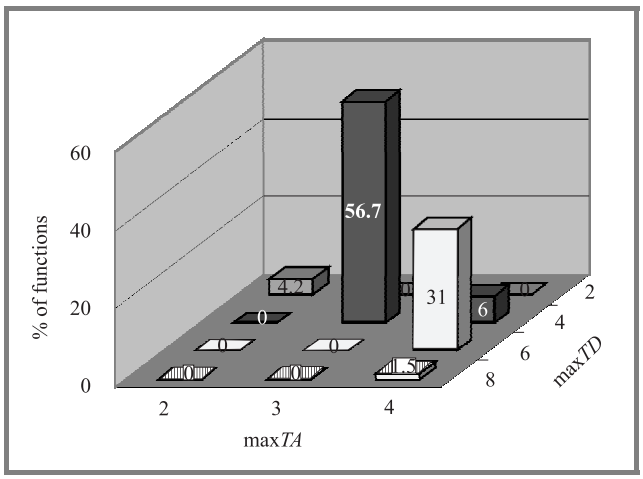

Fig. 5. Proportional distribution for arbitrary functions ($n = 3$, $m = 3$).

For $n = m = 3$ (Figs. 4 and 5), three different pairs $(\max TD, \max TA)$ are obtained for permutations while for arbitrary functions are obtained five different pairs, among which two pairs are dominant. Among permutations there are more functions with pair (8, 4) that are easiest to approximate as well as more functions with pair (2, 2) that are most difficult to approximate, than among arbitrary functions. It should be noticed, that for permutations the values of $\max TA$ are even while for arbitrary functions are odd as well. The values of $\max TD$ are even both for permutations and arbitrary functions.

For $n = m = 4$ (Figs. 6 and 7), there exist for permutations two dominant pairs and for arbitrary functions also two, but not the same. Both distributions have the evident maximum, which is obtained for the pair $(\max TD, \max TA)$ equal to (6, 6).

For $n = m = 5$ (Figs. 8 and 9), there are visible bars in the diagrams for the values of $\max TD$ equal to 6, 8 and 10.

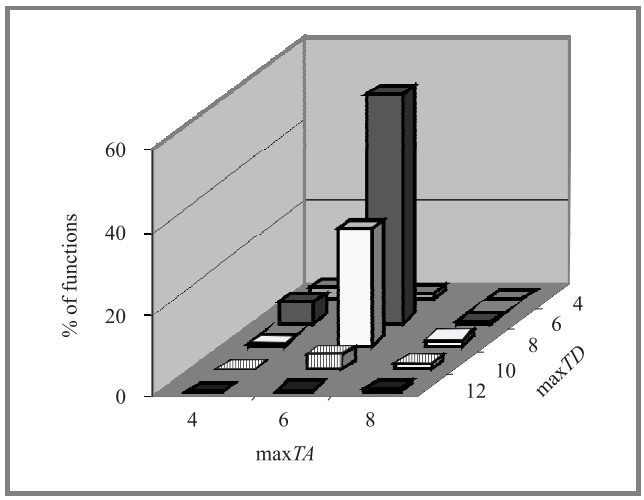

Fig. 6. Proportional distribution for permutations ($n = 4$, $m = 4$).

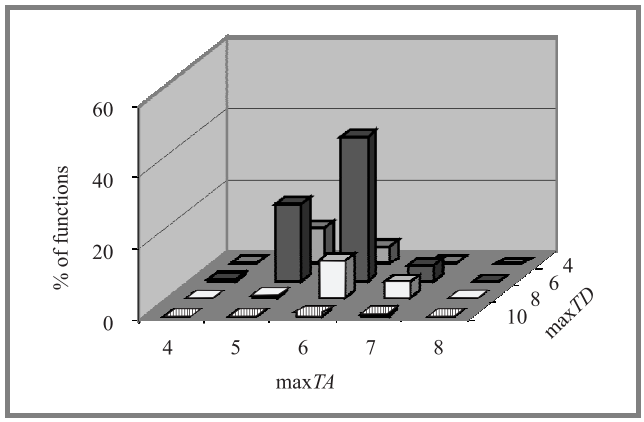

Fig. 7. Proportional distribution for arbitrary functions ($n = 4$, $m = 4$).

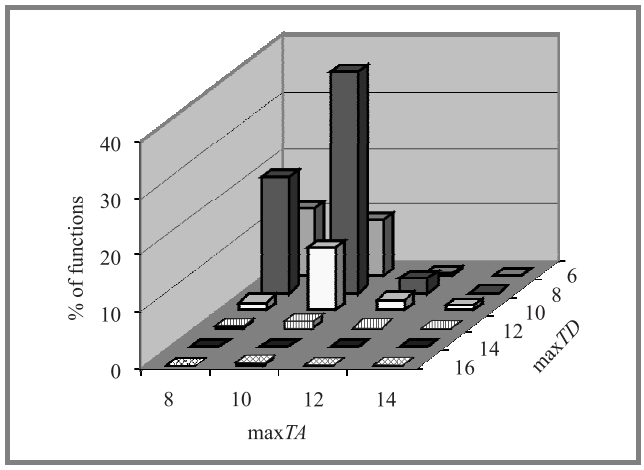

Fig. 8. Proportional distribution for permutations ($n = 5$, $m = 5$).

The maximum of distribution is less for arbitrary functions, because of the even and odd values of $\max TA$.

For $n = m = 6$ (Figs. 10 and 11), there are visible in the distributions for permutations and arbitrary functions, two significant series of results for $\max TD$ equal to 8 and 10.

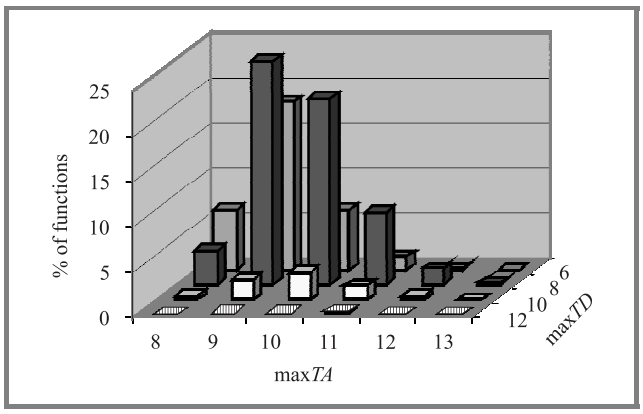

Fig. 9. Proportional distribution for arbitrary functions ($n = 5$, $m = 5$).

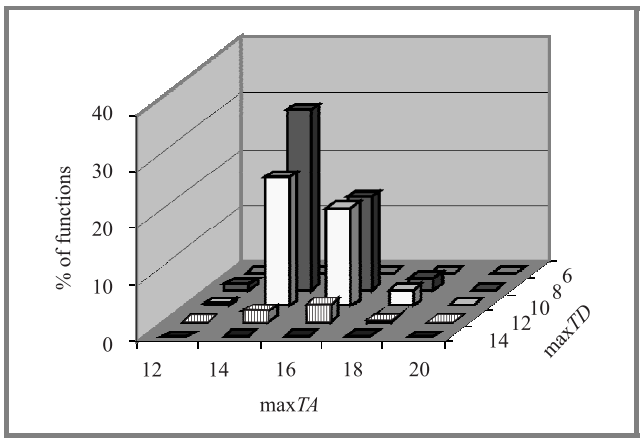

Fig. 10. Proportional distribution for permutations ($n = 6$, $m = 6$).

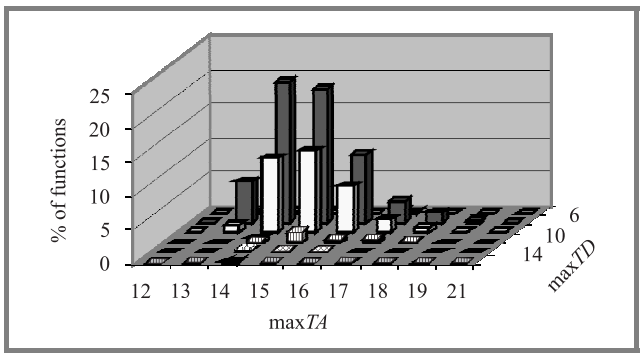

Fig. 11. Proportional distribution for arbitrary functions ($n = 6$, $m = 6$).

For $n = m = 7$ (Figs. 12 and 13), there are visible three series of results for $\max TD$ equal to 8, 10 and 12, in the distributions for permutations and arbitrary functions. The middle series is clearly dominant.

For $n = m = 8$ (Figs. 14 and 15), there are visible in the distributions for permutations and arbitrary functions, two significant series of results for $\max TD$ equal to 10 and 12. The series are rather equivalent this time. No one of them dominates.

For $n = m = 9$ (Figs. 16 and 17), in the distributions for permutations and arbitrary functions, are visible two series

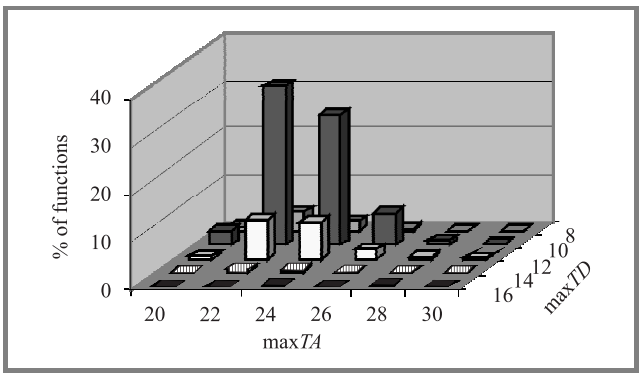

Fig. 12. Proportional distribution for permutations ($n = 7$, $m = 7$).

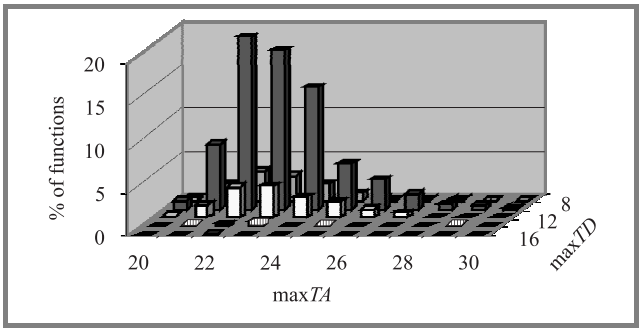

Fig. 13. Proportional distribution for arbitrary functions ($n = 7$, $m = 7$).

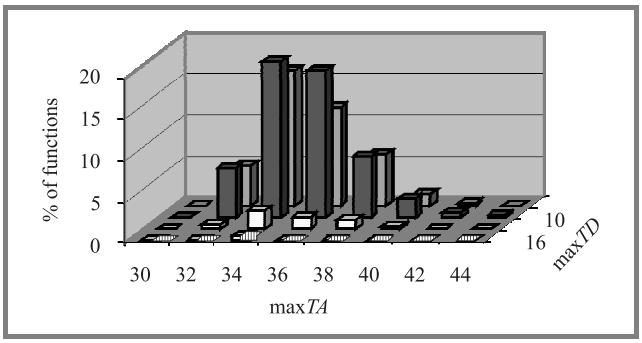

Fig. 14. Proportional distribution for permutations ($n = 8$, $m = 8$).

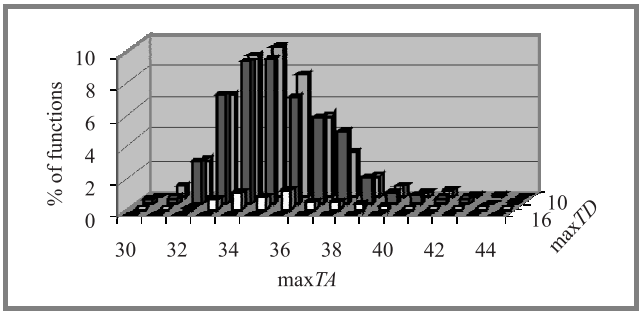

Fig. 15. Proportional distribution for arbitrary functions ($n = 8$, $m = 8$).

of results for $\max TD$ equal to 12 and 14. The series for $\max TD$ equal to 12 is clearly dominant.

For $n = m = 10$ (Figs. 18 and 19), there are visible two significant series of results for $\max TD$ equal to 12 and 14,

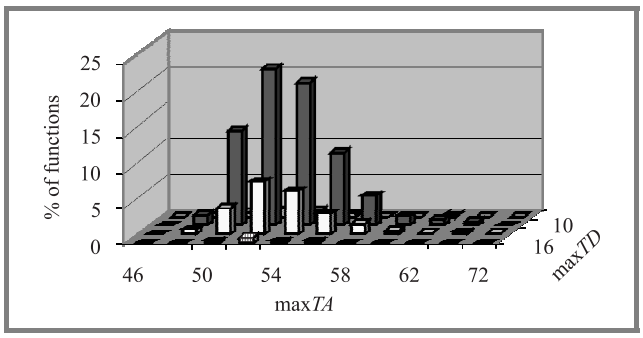

Fig. 16. Proportional distribution for permutations ($n = 9$, $m = 9$).

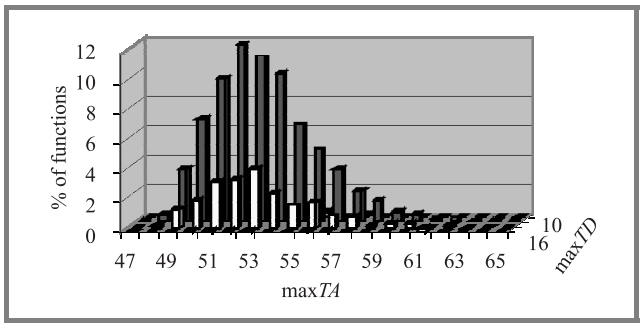

Fig. 17. Proportional distribution for arbitrary functions ($n = 9$, $m = 9$).

in the distributions for permutations and arbitrary functions. The series for value 14 of $\max TD$ is not so dominant like in the case of $n = m = 9$.

Considering the results for $1 \leq n = m \leq 10$, presented in Figs. 1–19 we can observe, that the significant for distributions ranges of $\max TD$ and $\max TA$ as well as the values of pairs $(\max TD, \max TA)$ for which are obtained maxima

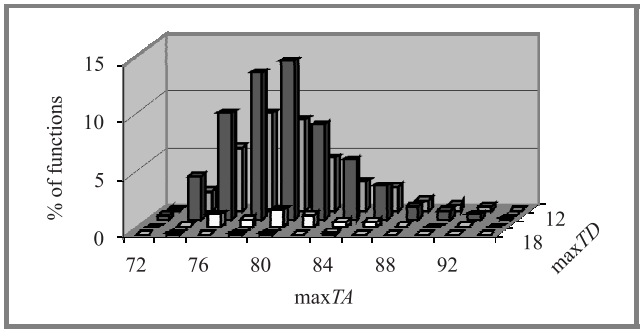

Fig. 18. Proportional distribution for permutations ($n = 10$, $m = 10$).

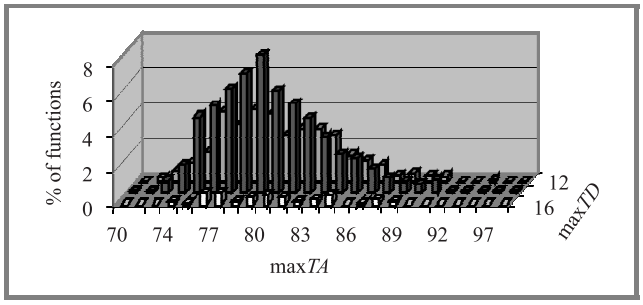

Fig. 19. Proportional distribution for arbitrary functions ($n = 10$, $m = 10$).

of distributions, are about the same for permutations and arbitrary functions. The values of maxima are greater for permutations. It follows from the fact, that for $n \geq 3$, the values of $\max TA$ are even for permutations while for arbitrary functions are odd as well. Thus, we can say that the results obtained for permutations and arbitrary functions are similar.

Comparing the differential and the linear approximation we can observe, that the ranges of $\max TD$ are narrow while the ranges of $\max TA$ are wide. With the increase of $n = m$ the values of $\max TA$ rise much faster than the values of $\max TD$. It means that the linear approximation of s-box functions becomes much more effective than the differential approximation. This advantage of the linear approximation starts at some value of $n = m$ and rises with the increase of this value.

3. Results for DES size s-boxes

The presented in this chapter results concern the distribution of the best nonzero differential and linear approximations of permutations with 6 input bits and 4 output bits. Similarly to definition of DES s-boxes, by permutation in this case we mean a set of four 4-bit permutations. In general, for $n > m$, by permutation we mean in fact a set of 2^{n-m} m-bit permutations. The results in detail are presented in Table 2 and illustrated in Fig. 20.

Table 2

Results of experiments for permutations – DES size ($n = 6$, $m = 4$)

$\max TD$	$\max TA$					Total
	10	12	14	16	18	
12	0	6	5	3	0	14
14	1	144	141	33	4	323
16	1	107	255	65	12	440
18	0	24	94	41	5	164
20	0	3	28	14	2	47
22	0	3	3	4	1	11
24	0	0	0	0	1	1
Total	2	287	526	160	25	1000

For DES size s-boxes, the advantage of the linear approximation over the differential one is not yet visible. The range of $\max TD$ is from 12 to 24 and the range of $\max TA$ is from 10 to 18. So the values of $\max TD$ and $\max TA$ are comparable.

The distribution of the best nonzero approximations enables to evaluate the quality of constructed s-boxes. The less the values of $\max TD$ and $\max TA$ the better is the s-box. The quality of DES s-boxes *S1–S8* is presented in Table 3. The value of $\max TD$ for all s-boxes is equal to 16. The best s-box of DES is *S6* with $\max TA = 14$ and the worst is *S5* with $\max TA = 20$.

It follows from Table 2, that for 25.5% of randomly selected s-boxes, the obtained pair $(\max TD, \max TA)$ is equal to (16, 14). Thus, parameters of s-box *S6* correspond to

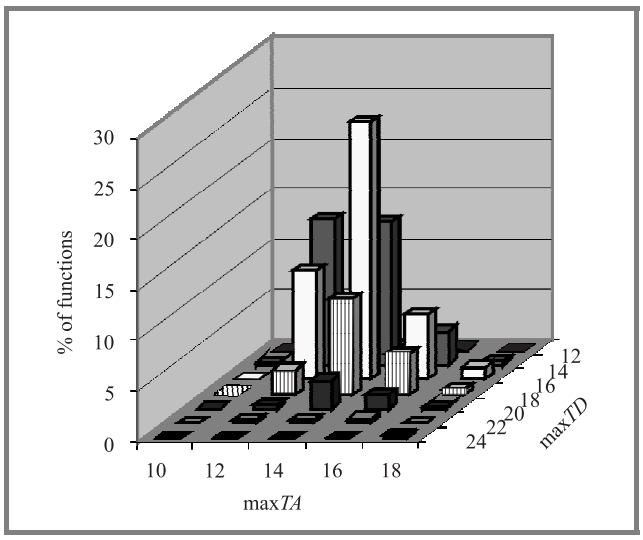

Fig. 20. Proportional distribution for permutations – DES size ($n = 6$, $m = 4$).

Table 3
Quality of DES s-boxes *S1-S8*

max TD	max TA					
	10	12	14	16	18	20
12						
14						
16			*S6*	*S2* *S3* *S4* *S8*	*S1* *S7*	*S5*

the maximum of the distribution. There are 40.5% of s-boxes with parameters better than of s-box *S6*. We have obtained, that among three randomly selected s-boxes, two of them are not worse than the best s-box of DES *S6* and one of them is better. On the other hand, the value 20 of max TA of the worst s-box *S5*, was not obtained for any of the 1000 randomly selected s-boxes. The quality of DES s-boxes is obviously not the best possible one.

4. Conclusion

The basic algorithms to compute a single element of the approximation tables TDf and TAf are of exponential complexity. The presented in [10] fast algorithms compute the values of max TD and max TA in at worst linear time for a single element, without memory needed for storage of the whole table. The fast algorithms were used to calculate the distribution of pairs $(\max TD, \max TA)$ for randomly chosen permutations and arbitrary functions with n binary inputs and m binary outputs, where $1 \leq n = m \leq 10$. For both classes of functions, the obtained results were similar. The main conclusion is that starting from some value of n, linear approximation of s-box functions becomes much more effective than differential approximation. Moreover, this advantage of linear approximation rises with the increase of n and for DES size s-boxes is not yet visible.

References

[1] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*. New York: Springer-Verlag, 1993.

[2] K. Chmiel, "Linear cryptanalysis of the reduced DES algorithms", in *Proc. Reg. Conf. Milit. Commun. Inform. Syst. 2000*, Zegrze, Poland, 2000, vol. 1, pp. 111–118.

[3] K. Chmiel, "Linear approximation of some s-box functions", in *Proc. Reg. Conf. Milit. Commun. Inform. Syst. 2001*, Zegrze, Poland, 2001, vol. 1, pp. 211–218.

[4] K. Chmiel, "On some models of arithmetic sum function linear approximation", in *Proc. NATO Reg. Conf. Milit. Commun. Inform. Syst. 2002*, Zegrze, Poland, 2002, vol. 2, pp. 199–204.

[5] K. Chmiel, "Linear approximation of arithmetic sum function", in *Artificial Intelligence and Security in Computing Systems*, J. Sołdek and L. Drobiazgiewicz, Eds. Boston: Kluwer, 2003, pp. 293–302.

[6] K. Chmiel, "Linear approximation of arithmetic subtraction function", in *Proc. NATO Reg. Conf. Milit. Commun. Inform. Syst. 2003*, Zegrze, Poland, 2003, pp. 1–6.

[7] K. Chmiel, "Linear approximation of structures with selectors", in *Proc. 6th NATO Reg. Conf. Milit. Commun. Inform. Syst. 2004*, Zegrze, Poland, 2004, pp. 269–273.

[8] K. Chmiel, "On arithmetic subtraction linear approximation", in *Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems*, J. Pejaś and A. Piegat, Eds. New York: Kluwer, 2005, pp. 125–134.

[9] K. Chmiel, "Fast computation of approximation tables", in *Information Processing and Security Systems*, K. Saeed and J. Pejaś, Eds. New York: Springer, 2005, pp. 125–134.

[10] K. Chmiel, "Differential and linear approximation of s-box functions", in *Image Analysis, Computer Graphics, Security Systems and Artificial Intelligence Applications*, K. Saeed *et al*., Eds. Białystok: University of Finance and Management in Białystok, 2005, vol. 1, pp. 191–200.

[11] A. Górska, K. Górski, Z. Kotulski, A. Paszkiewicz, and J. Szczepański, "New experimental results in differential – linear cryptanalysis of reduced variants of DES", in *Proc. 8th Int. Conf. Adv. Comput. Syst. ACS'2001*, Mielno, Poland, 2001, vol. 1, pp. 333–346.

[12] M. Matsui, "Linear cryptanalysis method for DES cipher", in *Advances in Cryptology Eurocrypt'93*, T. Helleseth, Ed. New York: Springer-Verlag, 1994, pp. 386–397.

Krzysztof Chmiel is an adjunct at Poznań University of Technology, Poland. His research and scientific interests focus on data security in information systems and cryptology, especially methods of designing and cryptanalysis of cryptographic algorithms. He is author of a number of publications on differential and linear approximation of block ciphers and their component functions.

e-mail: Chmiel@sk-kari.put.poznan.pl
Institute of Control and Information Engineering
Poznań University of Technology
Marii Skłodowskiej-Curie Sq. 5
60-965 Poznań, Poland