SOME REMARKS ON THE CROSS CORRELATION ANALYSIS OF PSEUDO RANDOM GENERATORS

Sibylle Mund, Dieter Gollmann, Thomas Beth

Fakultät für Informatik
Universität Karlsruhe
7500 Karlsruhe, West Germany

ABSTRACT

Siegenthaler has shown how cross-correlation techniques can be applied to identify pseudo random generators consisting of linear feedback shift registers and a scrambling function [7]. These techniques may allow to attack one register in such a generator at a time. The original algorithm needs $O(R2^rN)$ operations to identify one register. (r denotes the length of the register examined, R the number of primitive polynomials of degree r, and N the minimal number of bits one has to observe). Employing Walsh-Hadamard transform this analysis can be done in $O(R(r2^r+N))$ operations [8].
We show that there exists a trade-off between the dimension of the Hadamard matrix and the number of bits required to compute the cross correlation coefficients. The complexity of this attack is $O(R(r2^{r-\delta}+2^\delta N))$. The integer δ can be selected so that the cost of the attack is minimized. The MSR-generator will serve as an example to demonstrate our algorithm.
Furthermore we examine the correlation immunity of the S-boxes used in the DES.

1. INTRODUCTION : CROSS CORRELATION ANALYSIS OF A CERTAIN CLASS OF PSEUDO RANDOM GENERATORS

We will give a short outline of the cross correlation techniques developed by Siegenthaler and of the improvements due to Xiao and Massey. Most of the technical details have been omitted and the reader is referred to [7] and [8] for a full description.

We consider pseudo random generators (Fig.1) consisting of a scrambling function f and s linear feedback shift registers (LFSR). We use (x_i^n) as a shorthand for $(x_i^n)_n$, the sequence generated by register i. The generator produces the sequence (z^n),

$$z^n := f(x_1^n,\ldots,x_s^n).$$

D. Chaum and W.L. Price (Eds.): Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 25-35, 1988.

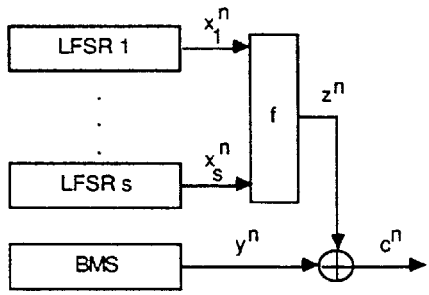

Fig.1 A Pseudo Random Generator consisting of s LFSRs and a scrambling function f

In our experiments we will encipher (y^n) , the output of a binary memory- less source (BMS) with $P(y^n=0)\neq 0.5$. The ciphertext (c^n) is thus defined by $c^n := y^n+z^n$ (addition mod 2). Siegenthaler has shown that cross correlation techniques can be used to identify initial state and feedback polynomial of register i independently of the other registers when f "leaks" some information from (x_i^n) to (z^n).

We will concentrate on the analysis of a single register. Let r denote the length of the register examined, R the number of primitve polynomials of degree r and N the minimal number of output bits necessary for the correlation analysis as established by Siegenthaler.

The correlation test works as follows. A feedback polynomial is selected. Let q_0 be a specially designated initial state of the register and let q_n be the state reached after n time steps. When we denote the state transition matrix of the register by A we have $q_n = A^n q_0$. Let C denote the output matrix of the register.

Let α_k denote the cross correlation between (c^n) and $(CA^n q_k)$, the output generated by the initial state q_k . If α_k exceeds the bound of the cross correlation test we assume that the correct feedback polynomial has been found and the initial state q_k can be computed. However, this inital state is not necessarily identified uniquely. If no α_k exceeds the bound the test is repeated for another feedback polynomial.

In the original version of the correlation attack $O(R\cdot N\cdot 2^r)$ operations are required to compute the feedback polynomial and initial state [7].

It is possible to speed up this attack by using the Walsh-Hadamard Transform to compute simultaneously the cross correlation between (c^n) and the outputs for all possible initial states of the given shift register [8].

The Walsh-Coefficients of a function $g:\{0,1\}^n \to \{-1,0,1\}$ are defined as

$$C(t) := 2^{-n} \sum_{v\in\{0,1\}^n} g(v)(-1)^{<t,v>} \qquad \text{for all } t\in\{0,1\}^n \ ,$$

where <t,v> is the real scalar product of the vectors t and v.

For our purposes define g: $\{0,1\}^n \to \{-1,0,1\}$ by

$$g(q_n) := \begin{cases} (-1)^{c^n} & \text{for } 1 \le n \le N \\ 0 & \text{else} \end{cases}$$

I.e. we reorder the ciphertext (c^n) so that the output at time n is assigned to the position q_n. With $s_k := CA^k$ we then have

$$CA^n q_k = CA^{n+k} q_0 = CA^k A^n q_0 = \langle s_k, q_n \rangle$$

and furthermore

$$\alpha_k = \sum_{n=1}^{N} (-1)^{c^n \oplus CA^n q_k} = \sum_{n=1}^{N} (-1)^{c^n \oplus \langle s_k, q_n \rangle} = \sum_{n=0}^{2^r-1} g(q_n)(-1)^{\langle s_k, q_n \rangle} = C(s_k) .$$

Thus the cross correlation coefficients $(\alpha_0,\ldots,\alpha_{2^r-1})$ are the Walsh- Coefficients of our function g. These Walsh-Coefficients can be computed by multiplying the vector

$$g := (g(0), g(1), \ldots, g(2^r-1))$$

with the Hadamard matrix H_r. (The arguments of g are identified with binary strings of length n). The Hadamard-Matrices are defined recursivly by

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} , \qquad H_m = \begin{bmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{bmatrix} , \quad m \ge 2 .$$

The complexity of this algorithm is $O(R(r \cdot 2^r + r \cdot N))$. For each feedback polynomial we need $O(r \cdot 2^r)$ operations to compute $g \cdot H_r$ recursively [1], [3] and $O(r \cdot N)$ operations to initialize g.

2. A TRADE-OFF BETWEEN THE DIMENSION OF THE HADAMARD-MATRIX AND THE LENGTH OF CIPHERTEXT

If r grows N will lag behind 2^r. Therefore a substantial "portion" of g will be equal to 0 and thus not contribute to the computation of the correlation coefficients. Simply cutting down the dimension of the Hadamard-Matrix does not work. However, if the length of the ciphertext is increased one will again get a sufficient number of ciphertext bits in a shortened vector g . Thus a lower dimension Walsh-Transform will compute meaningful correlation coefficients.

This statement will now be explained in closer detail. We cut down the vector g by the factor 2^δ for some integer $\delta \geq 0$. Ciphertext bit c^n will contribute to $g(0),\ldots,g(2^{r-\delta}-1)$ exactly when $q_n < 2^{r-\delta}$. (Identify q_n with the integer that has binary expansion q_n).
Define $N_\delta := N \cdot 2^\delta$ and E_δ to be the expected number of states q_{k+n}, $0 \leq n \leq N_\delta - 1$, with $q_{k+n} < 2^{r-\delta}$. The expected value is taken over all initial states including the all-zero state. We have the following

LEMMA: $E_\delta = N$

PROOF: For all initial states q_k we have to count the number of states q_{k+n} with $q_{k+n} < 2^{r-\delta}$, $0 \leq n \leq N_\delta - 1$. To do so we count for all positions i, $0 \leq i \leq N_\delta - 1$, the number of initial states q_k so that $q_{k+i} < 2^{r-\delta}$. There are overall N_δ positions and $2^{r-\delta}$ such initial states for each position when we include the all-zero state. This gives

$$E_\delta = 2^{-r} \cdot N_\delta \cdot 2^{r-\delta} = 2^{-r} \cdot N \cdot 2^\delta \cdot 2^{r-\delta} = N \quad .$$

□

Thus we can expect a sufficient number of ciphertext bits to be considered in the computation of the cross correlation coefficients when we use the vector ($g(0),\ldots,g(2^{r-\delta}-1)$) and the Hadamard-Matrix $H_{r-\delta}$. Thereby we have a trade-off between the length of the ciphertext and the dimension of the Hadamard-Matrix. Increasing the length of the ciphertext by the factor 2^δ will reduce the dimension of the Hadamard-Matrix by the same factor. It is therefore possible to analyse the LFSR in

$$O\left(R((r-\delta)2^{r-\delta} + r \cdot N \cdot 2^\delta)\right)$$

steps. The best choice for δ is close to $(r-\log_2 N)/2$ (see Table 1). Note that this attack will only find the correct feedback polynomial . There are still 2^δ possible initial states corresponding to each correlation coefficient.

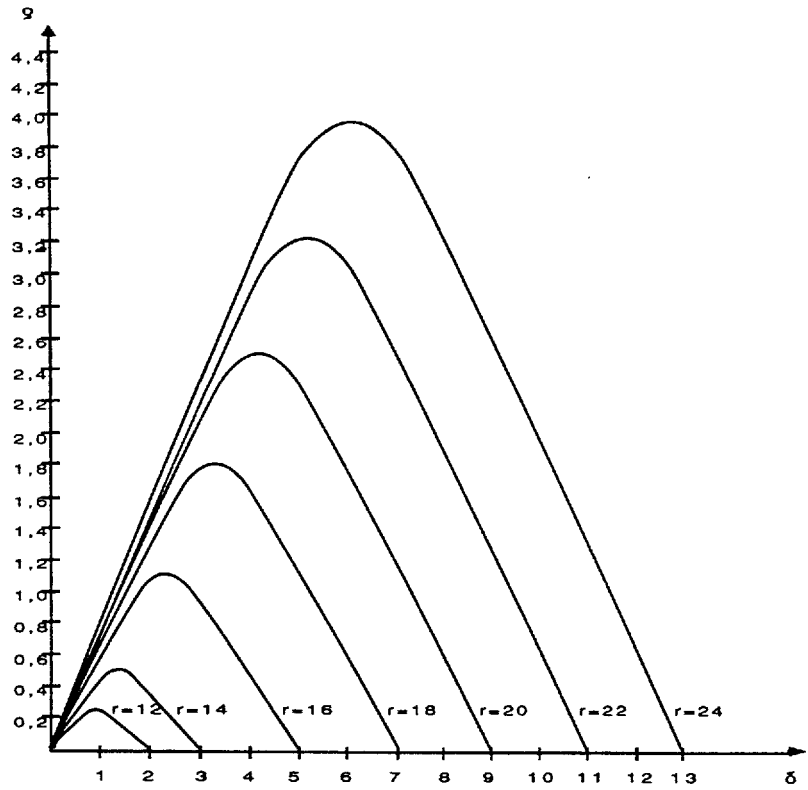

Table 1. Schematic plot of the ratio $g := \ln (R(r2^r+rN) / R((r-\delta)2^{r-\delta}+rN2^{\delta}))$

3. THE ANALYSIS OF THE MSR-GENERATOR

The MSR-generator (Fig.2) consists of two LFSR and a multiplexer that takes the state of the first register to decide which position of the second register shall be tapped to give the output. An algebraic analysis of the MSR-generator can be found in [2].

For each register cell we have to compute the probability that its content and the output of the generator are equal. This probability has to be different from 0.5 to allow a cross correlation attack. We assume that x_j and y_k are statistically independent for all j,k , $1 \le j \le m$, $1 \le k \le n$. We also assume that the positions y_k are tapped with equal probability.

Let m be the length of the first register and let $x_1,...,x_m$ be the contents of its register cells. Let n be the length of the second register and $y_1,...,y_n$ the contents of its register cells. Let z be the output of the MSR-generator.

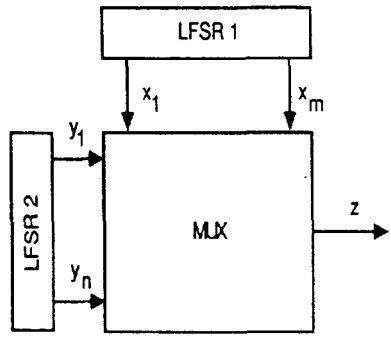

Fig.2 The MSR-Generator

We have for the first register

$$P(x_j=z) = \sum_{i=1}^{n} P(x_j = y_i)\cdot P(y_i \text{ is tapped}) = \sum_{i=1}^{n} \frac{1}{2}\cdot\frac{1}{n} = \frac{1}{2} \quad .$$

Thus the first register cannot be attacked directly by correlation analysis. The analysis of the second register gives

$$P(y_k=z) = P(y_k \text{ is tapped}) + \sum_{i=1, i\neq k}^{n} P(y_i \text{ is tapped})\cdot P(y_i=y_k)$$

$$= \frac{1}{n} + \sum_{i=1, i\neq k}^{n} \frac{1}{n}\cdot\frac{1}{2} = \frac{1}{2} + \frac{1}{n}\cdot\frac{1}{2} \quad .$$

As $P(y_k = z) \neq 0.5$ the correlation analysis is feasible.

We will demonstrate the cross correlation attack on a MSR-generator with m=12, n=14 and feedback polynomials $x^{12}+x^6+x^4+x+1$ and $x^{14}+x^{10}+x^6+x+1$. The initial states are 0000 0000 0001 and 0000 0000 0000 10 respectively. The multiplexer reads positions 3,7,4 of register 1. This 3-bit number serves as an index for the array (2,10,4,8,11,5,7,9). The entries in this array determine which position of register 2 will be tapped. The error probabilities for the test are $p_m = 0.9$ (dismissing the correct LFSR) and $p_f = 1/(R_{14}\, 2^{14})$ (accepting a wrong LFSR). We have $R_{14} = 756$ and $N = 2^{12}$.

The result of the correlation attack for the correct choice of the feedback polynomial is shown in Table 2. The attack was performed for δ=2, δ=1, and δ=0. The bound for significant Walsh-Coefficients is 430. Note that all significant positions are already highlighted by the attack with $\delta = 2$.

vectors s for δ=0 : δ=1 : δ=2	initial states for δ=0	Walsh-Coefficients δ=0 : δ=1 : δ=2
0 : 0 : 0000 0011 0000	0000 0100 0001 11	504/493/572
0 : 0 : 0000 0110 0000	0000 0010 0000 11	536/551/516
0 : 0 : 0000 1100 0000	0000 0001 0000 01	436/525/546
0 : 0 : 0001 0001 0001	0111 1001 0010 11	584/583/642
0 : 0 : 0001 1000 0000	0000 0000 1000 00	536/585/612
0 : 0 : 0011 0000 0000	0000 0000 0100 00	480/483/546
0 : 0 : 1100 0000 0000	0000 0000 0001 00	500/465/542
0 : 1 : 1000 0000 0000	0000 0000 0000 10	-528/575/614

Table 2. Value and position of the significant Walsh-Coefficients for δ=2, δ=1, δ=0. The initial states are only given for δ=0.

4. ANALYSIS OF THE DES S-BOXES

The S-boxes in the DES are non-linear functions with six inputs, say x_1, x_2, x_3, x_4, x_5, x_6 , and four outputs, say z_1,z_2,z_3,z_4 . The inputs x_1 and x_6 choose one of four different mappings from x_2,x_3,x_4,x_5 to the outputs. These mappings can be described as permutations of the numbers 0 to 15. The 8 DES S-boxes are given in Appendix 1.

The Walsh-Coefficients of input/output pairs:

We examine the amount of information that leaks through an S-box from one input to an output. These cross correlations can be measured by the Walsh-Coefficients with Hamming-Weight 1. Table 3 gives the Walsh- Coefficients for all input/output pairs (x_i,z_j) , i=2,..,5 , j=1,..4 . The Walsh-Coefficients corresponding to the inputs x_1 and x_6 are zero for all S-boxes and all outputs.

Paths in the DES:

We investigate the amount of information leakage through several rounds of the DES. We consider therefore the full set of S-boxes and look for instances where an input/output pair with large Walsh-Coefficient is linked to another such input/output pair. Enumerate the inputs x_2, x_3, x_4, x_5 of the 8 S-boxes by 0 to 31. The outputs are enumerated likewise. Let i->j denote an input/output pair and j<=>k the permutation due to wire crossing (see Appendix 2). The largest Walsh-Coefficients for input/ output pairs are of size 12. Considering the permutation in each round they correspond to the transitions 1->16 and 9->29. Obviously there is no way of getting a path of length two with Walsh-Coefficients of size 12 assigned to all transitions. For Walsh-Coefficients of size 8 one obtains at most paths of length two. Only Walsh-Coefficients of size 4 will give cycles and thus complete paths through the DES.

S-Box 1: $x_i \backslash z_j$	z_1	z_2	z_3	z_4
x_2	0	-4	4	4
x_3	-8	-12	-4	8
x_4	-4	-4	-4	4
x_5	4	-4	-4	-4

S-Box 2: $x_i \backslash z_j$	z_1	z_2	z_3	z_4
x_2	0	0	-8	0
x_3	-4	-4	4	0
x_4	0	4	4	-4
x_5	0	0	0	0

S-Box 3: $x_i \backslash z_j$	z_1	z_2	z_3	z_4
x_2	4	4	4	0
x_3	-4	0	12	0
x_4	0	4	0	-8
x_5	0	0	-4	4

S-Box 4: $x_i \backslash z_j$	z_1	z_2	z_3	z_4
x_2	-4	4	-4	-4
x_3	8	0	0	-8
x_4	4	-4	-4	-4
x_5	0	8	8	0

S-Box 5: $x_i \backslash z_j$	z_1	z_2	z_3	z_4
x_2	0	0	-4	4
x_3	-4	0	4	0
x_4	0	0	-4	4
x_5	8	-4	-4	8

S-Box 6: $x_i \backslash z_j$	z_1	z_2	z_3	z_4
x_2	-8	0	0	4
x_3	4	-8	-4	4
x_4	4	4	4	0
x_5	4	4	0	0

S-Box 7: $x_i \backslash z_j$	z_1	z_2	z_3	z_4
x_2	-4	0	4	-4
x_3	-8	-4	0	-8
x_4	8	0	4	8
x_5	4	8	4	0

S-Box 8: $x_i \backslash z_j$	z_1	z_2	z_3	z_4
x_2	0	0	0	0
x_3	-4	0	4	0
x_4	4	0	-4	-4
x_5	-4	-4	0	4

Table 3. The Walsh Coefficients for input/output pairs. Inputs x_1 and x_6 have been omitted. The coefficients have not been scaled by 2^{-6}.

4 -> 6 <=> 1 -> 3 <=> 30	13 -> 12 <=> 25 -> 27 <=> 6
4 -> 6 <=> 1 -> 0 <=> 8	15 -> 13 <=> 19 -> 16 <=> 7
4 -> 6 <=> 1 -> 1 <=>16	15 -> 13 <=> 19 -> 19 <=> 2
13 -> 12 <=> 25 -> 24 <=> 31	15 -> 14 <=> 9 -> 10 <=> 29

Table 4. Paths through two rounds of DES for input/output pairs with Walsh-Coefficients of size 8

Walsh-Coefficients of randomly selected S-boxes:

We have generated random S-boxes and computed their Walsh-Coefficients to examine whether the DES S-boxes had been chosen specifically to minimize cross correlation effects (conf. [4]). The S-boxes were constructed according to the following criteria .

P0. The mappings selected by x_1 and x_6 are permutations of <0,..,15> .
P1. No S-box is a linear or affine function of the input.

Further criteria used in the definition of the DES S-boxes (see e.g. [4]) have not been considered in this analysis. Because of property P0 the (unscaled) Walsh-Coefficients are always divisible by 4. Table 5 gives the relative frequency of the Walsh-Coefficients of input/output pairs for these randomly selected S-boxes and for the DES S-boxes. Table 6 gives the distribution of the maximal Walsh-Coefficients for each row and for each output of an S-box (*conf.* [6]). The statistics are based on 88 random S-boxes. In both instances the distributions for DES S-boxes and random S-boxes are rather similar. This suggests that non-linearity already explains the cross-correlation properties of the DES S-boxes.

5. CONCLUSION

The Walsh-Transform is a useful tool for the cross correlation analysis of pseudo random generators. We have shown how a further speed-up can be achieved in the analysis of a class of generators built from shift registers. The complexity of the attack still depends exponentially on the length of the register. However, this makes even a small reduction in the size of the exponent all the more interesting for practical applications.
We have also examined the correlation properties of the DES S-boxes. No obvious weakness was encountered. Experiments with randomly generated S-boxes seem to indicate that cross correlation properties have not been a special criterion in the design of the DES S-boxes. It remains a research problem to check this assumption in a proper statistical framework.

LITERATURE

[1] K.G.Beauchamp, "Applications of Walsh and Related Functions", Academic Press, 1984

[2] T.Beth, P.Heß, K.Wirl, "Kryptographie", Teubner, Stuttgart,1983

[3] T.Beth, "Verfahren der Schnellen Fourier-Transformation", Teubner, Stuttgart,1984

[4] E.F.Brickell, J.H.Moore, M.R.Purtill, "Structures in the S-Boxes of the DES (extended abstract)", Springer, LNCS 263, pp.3-8, 1987

[5] A.G.Konheim, "Cryptography, a Primer", Wiley, New York, 1981

[6] R.A.Rueppel, "Analysis and Design of Stream Ciphers", Springer, Heidelberg, 1986

[7] T.Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphertext Only", IEEE Trans.Comp.,Vol. C-34, No.1, pp.81-85,1985

[8] Guo-Zhen Xiao, J.L.Massey, " A Spectral Approach to Correlation-Immune Combining Functions", to appear

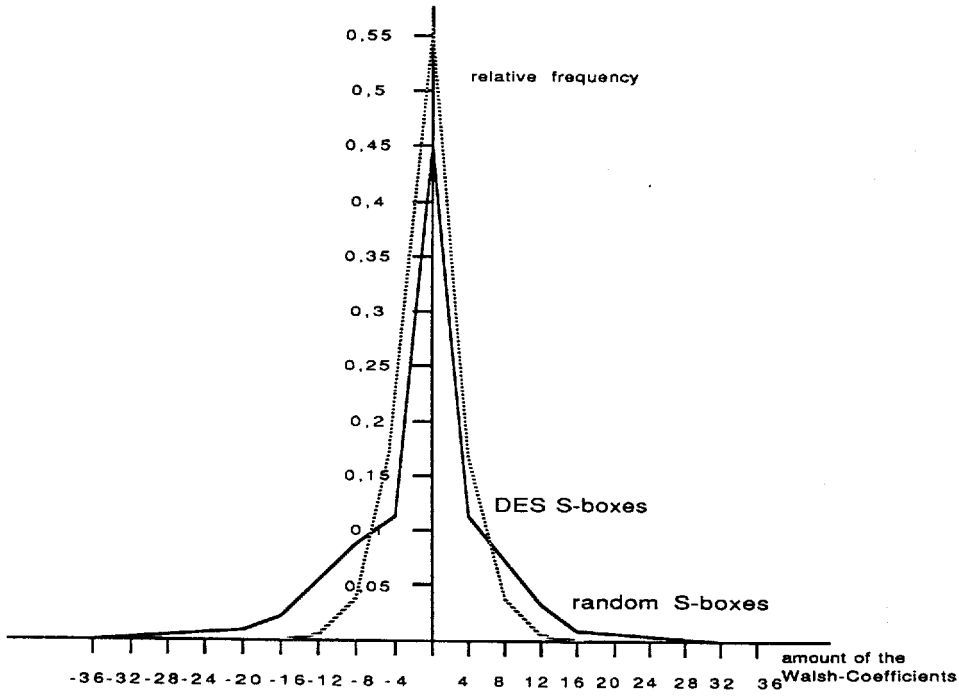

Table 5. Distribution of Walsh-Coefficients of input/output pairs for DES S-boxes and for randomly selected S-boxes.

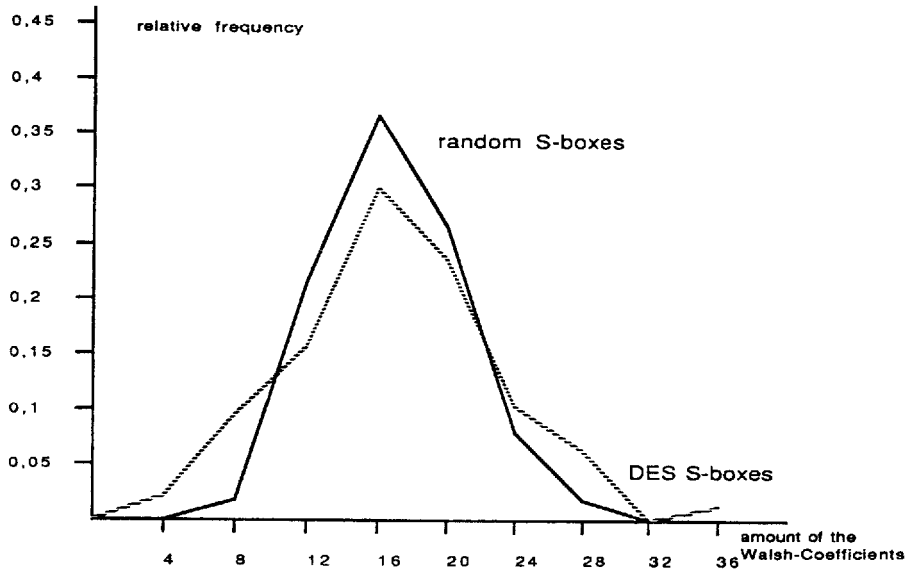

Table 6. Distribution of the maximal Walsh-Coefficients for DES S-boxes and randomly selected S-boxes.

Appendix 1: The DES S-boxes [5]:

S-Box 1:	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S-Box 2:	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	12	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S-Box 3:	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S-Box 4:	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S-Box 5:	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S-Box 6:	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S-Box 7:	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S-Box 8:	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Appendix 2: The DES wire crossing [5]:

P : DES Wire Crossing

15	6	19	20
28	11	27	16
0	14	22	25
4	17	30	9
1	7	23	30
31	26	2	8
18	12	29	5
21	10	3	24