What do DES S-boxes Say to Each Other ?

Nicolas T. Courtois, Guilhem Castagnos, and Louis Goubin

Axalto Cryptographic Research & Advanced Security,
36-38 rue de la Princesse, BP 45, 78430 Louveciennes Cedex, France
courtois@minrank.org, gcastagnos@louveciennes.sema.slb.com,
Louis.Goubin@louveciennes.sema.slb.com.

Abstract. The DES encryption standard resisted rather well to some 20 years of massive worldwide cryptanalysis effort. DES S-boxes also haven't an obvious algebraic structure that could lead to algebraic attacks. For all these reasons, DES is not only very widely implemented and used today, but triple DES and other derived schemes will probably still be around in ten or twenty years from now.

We suggest that, if an algorithm is so widely used, its security should still be under scrutiny, and not taken for granted. In this paper we study the S-boxes of DES. Many properties of these are already known, yet usually they concern one particular S-box. This comes from the known design criteria on DES, that strongly suggest that S-boxes have been chosen independently of each other.

On the contrary, we are interested in properties of DES S-boxes that concern a subset of two or more DES S-boxes. For example we study the properties related to Davies-Murphy attacks on DES, recall the known uniformity criteria to resist this attack, and discuss a stronger criterion that would allow to resist a larger class of attacks. More generally we study many different properties, in particular related to linear cryptanalysis and algebraic attacks. The interesting question is to know if there are any interesting properties that hold for subsets of S-boxes bigger than 2. Such a property has already been shown by Shamir at Crypto'85 (and independently discovered by Franklin), but Coppersmith *et al.* explained that it was rather due to the known S-box design criteria. Our simulations confirm this, but not totally. We also present several new properties of similar flavour. These properties come from a new type of algebraic attack on block ciphers that we introduce. What we find is not easily explained by the known S-box design criteria, and the question should be asked if the S-boxes of DES are related to each other, or they follow some yet unknown criteria. Similarly, we also found that the s^{5}DES S-boxes have an unexpected common structure that can be exploited in a certain type of generalised linear attack. This fact substantially decreases the credibility of s^{5}DES as a DES replacement. This paper has probably no implications whatsoever on the security of DES.

Key Words: block ciphers, S-box design, DES, s^{5}DES, linear cryptanalysis, Davies-Murphy attack, algebraic attacks on block ciphers, XSL, monomial equations, bi-monomial equations.

1 Introduction

The motivation of our study lies in the following remark from Brickell *et al.* [5]:

> "All the structure of the S-boxes that we have described appears to be the result of design principles.
> The question that remains is whether this is a complete list of the design principles used in creating the S-boxes. This question could be answered in the negative if further structure was discovered in the S-boxes that did not occur in the boxes created using these design principles."

In this paper we study various properties of S-boxes that are clearly not a consequence of the design principles. The goal of this paper is also to show that there is still a lot of open problems regarding different properties of S-boxes and their potential and real implications for the security of block ciphers.

2 Design Criteria

2.1 S-Box Design Principles

In his PhD thesis [6], Laurence Brown writes:

> "It has been stated [29] that there were 12 (possibly 13) criteria used, which resulted in about 1000 suitable S-boxes, of which the implementors chose 8."

As mentioned by Brickell *et al.* in [5],

> "We would like to know what properties the S-boxes were designed to satisfy. This information was never published and in fact, the only source for specific "design principles" appears to be responses from the NSA to a study of the DES made by the Lexar Corporation [24]. There were included in the report of the second workshop on the DES held by the NBS in 1976 [4]."

In their comments, the NSA labelled the following as "design criteria" for the S-boxes:

P1. No S-box is a linear or affine function of the input.
P2. Changing 1 input bit to an S-box results in changing at least 2 output bits.
P3. $S(x)$ and $S(x+\texttt{001100})$ must differ in at least 2 bits.

The following were labelled by the NSA as "caused by design criteria":

P4. $S(x) \neq S(x+\texttt{11ab00})$ for any choice of a and b.
P5. The S-boxes were chosen to minimize the difference between the number of 1's and 0's in any S-box output when any single input bit is held constant.

Another consequence of design criteria was noted by Meyer and Matyas in their book [30]:

P6. The S-boxes chosen required significantly more logical minterms to implement than a random choice would require. A minterm is a logical AND (boolean product) of input bits (and their negations), which form a necessary (but not sufficient) condition for a particular output bit to be asserted. An output bit may have its value completely described by the logical OR (boolean sum) of all its minterms. The number of minterms in such an expression (after simplification) is a measure of its complexity. In the worst case, for n input bits, $2n$ minterms may be needed to describe each output bit.

After the invention of differential cryptanalysis by Biham and Shamir [2], Don Coppersmith [9, 10] revealed the criteria[1] used in the S-box design two decades earlier:

1. Each S-box should have six bits of input and four bits of output. (In 1974 this was the largest size S-box that could be accommodated if DES were to fit on a single chip.)
2. No output bit of an S-box should be too close to a linear function of the input bits. (The S-boxes are the only nonlinear part of DES. Their nonlinearity is the algorithm's strength.)
3. Each "row" of an S-box should contain all possible outputs. (This randomizes the output.)
4. If two inputs to an S-box differ in exactly one bit, their outputs should differ in at least two bits.
5. If two inputs to an S-box differ exactly in the middle two bits, their outputs must differ by at least two bits. (Criteria (4) and (5) provide some diffusion.)
6. If two inputs to an S-box differ in their first two bits and agree on their last two, the two outputs must differ.
7. For any nonzero 6-bit difference between inputs, no more than 8 of the 32 pairs of inputs exhibiting that difference may result in the same output difference.

[1] Some of these criteria have been observed beforehand by various authors, e.g. in [19] but their full relevance was not understood.

Call an S-box "active" if not all input differences to the box are zero. The S-boxes were designed to increase the number of active boxes. This maxim, along with a simplifying assumption that S-box events are statistically independent, ensures that with n active S-boxes, the probability of a particular pattern holding through n boxes is $1/4^n$.

Coppersmith commented that a better criterion than (2) would have been:

2'. No linear combination of output bits of an S-box should be too close to a linear function of the input bits.

While neither (2) nor (2') could be perfectly achieved, (2') would have increased DES's ability to resist linear cryptanalysis. So would larger S-boxes, but these were not possible in the technology of the time. There were also criteria to promote further randomization by the permutation P.

In an invited talk [11] at Crypto'2000, Don Coppersmith mentioned the list of permanent members of the IBM team that designed DES: Alan Konheim, Roy Adler, Bill Notz, Lynn Smith, Horst Feistel, Alan Tritter, Bryant Tuckerman, Carl Meyer, Edna Grossman, Bob McNeill, Walt Tuchmann, Jon Oseas, Don Coppersmith (all in Yorktown or Kingston). He also mentioned the following list of design criteria:

1. 6 bits in, 4 bits out.
2. No output bit "too close" to linear function of inputs.
3. Fix two outer bits (autoclave): the rest is a permutation of 4 bits. In other words, $\Delta_{\text{in}} = \texttt{0wxyz0} \Rightarrow \Delta_{\text{out}} \neq 0$.
4. $\Delta_{\text{in}} = \texttt{001100} \Rightarrow |\Delta_{\text{out}}| \geq 2$.
5. $\text{Prob}(\Delta_{\text{out}} = 0 | \Delta_{\text{in}}) \leq \frac{8}{32}$.
6. $\text{Prob}(\Delta_{\text{out}} = 0 | \Delta_{\text{in}}) \leq$ stricter but *ad hoc*.
7. $\Delta_{\text{in}} = \texttt{11xy00} \Rightarrow \Delta_{\text{out}} \neq 0$.
8. Implementation should use at most 47 gates.

Around 1976, the IBM team estimated the complexity of a chosen ciphertext attack to be 2^{46}.

3 Our Methodology and Notations

We call $y_1, \ldots y_4$ the output bits of the S-box, y_1 being the most significant (or rather the leftmost) bit. We call $x_1, \ldots x_6$ the input bits of the S-box, x_1 being the leftmost bit. In some other papers, for example in [35], the inputs are called A,B,C,D,E,F, with A corresponding to our x_1. The outputs are then called W,X,Y,Z with W being our y_1.

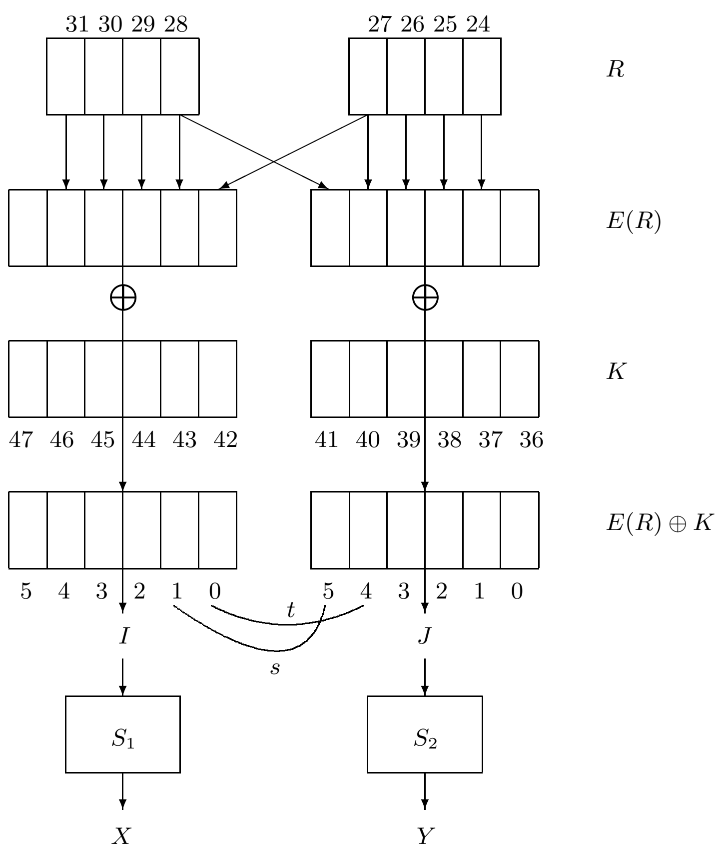
In a study of S-boxes of DES, it is possible to compare the S-boxes to random S-boxes of the same size. This is not a bad idea in general, as random S-boxes are expected to result in a secure cipher if they are big enough. However, in the design of DES the S-boxes are very small, designed to fit within the very basic IC technology of the early 70's. Therefore many of the design criteria give properties that are better than can be achieved with random S-boxes, for example in terms of differential characteristic probabilities. Thus, in order to see if the design of the S-boxes can be explained by the known design criteria, one should compare them not to random S-boxes but to another set of S-boxes that already satisfy all these criteria. This is what we do in the present paper, the basis for comparison is the set of S-boxes known as s^5DES and given in [28], also designed to provide better resistance to linear, differential and Davies-Murphy attacks.

4 Davies-Murphy Attacks, Designing Better S-boxes and s^{5}DES

4.1 Key Properties Leading to Davies-Murphy Attacks

The Davies-Murphy line of attacks [17, 1] is based on the fact that, for two consecutive S-boxes in DES (for example 1-2, 2-3 or 8-1), two bits are connected (modulo XORing with some key bits) to the other S-box. The exact connections are given on the following picture:

Table 1. The Principle of Davies-Murphy Attack on DES (here for S-boxes 1 and 2)



Thus, if s denotes the XOR of I_1 and J_5 (second bit from the right in the first S-box XORed with the first bit from the left in the second S-box), it is by construction of DES a known linear combination of key bits.
For example for S-boxes 1 and 2 we have the following two equations:

$$s \stackrel{def}{=} I_1 \oplus J_5 = K_{43} \oplus K_{41}$$
$$t \stackrel{def}{=} I_0 \oplus J_4 = K_{42} \oplus K_{40}$$

During the DES encryption the couple (s, t) being fixed, it constitutes an a priori knowledge that will have consequences on the output distribution of (X, Y). Though each of X and Y is distributed uniformly, the joint distribution is not uniform and depends on (s, t), and in fact as we will see later only on $s \oplus t$.

In general, let S_p and S_q be two consecutive S-boxes, with $q = p+1, p = 1 \ldots 7$ or $(p, q) = (8, 1)$. Let I and J be their inputs, and let $X = S_p(I)$ and $Y = S_q(J)$ be their outputs.
We recall that the S-boxes are permutations when the two "side" bits are fixed. This property plays an essential role in the attack. It implies that, if the distribution of (I, J) is uniform, then the distribution of (X, Y) will be uniform, and moreover each output value will be taken exactly 16 times, once for each choice of (I_5, I_0, J_5, J_0). We call $\mathcal{U}$ this distribution. In DES, the distribution of (I, J) is not uniform, and satisfies the conditions $I_1 \oplus J_5 = s$ and $I_0 \oplus J_4 = t$. Let $\mathcal{V}_{st}$ be the resulting distribution of (X, Y).
In order to have the full description of $\mathcal{V}_{st}$ we will use the following notations:

$$D(X, Y, s, t) = Card\{I, J \in \mathbf{F}_2^6, I_1 \oplus J_5 = s, I_0 \oplus J_4 = t, S_p(I) = X, S_q(J) = Y\}$$

In order to compute $D(X, Y, s, t)$, for a fixed couple (s, t), we will consider all possible cases for $(i, j, k, l) \stackrel{def}{=} (I_1, I_0, J_5, J_4)$. Knowing that $i \oplus k = s$ and $j \oplus l = t$ are fixed, there are in fact only 4 possibilities for (i, j, k, l). In each of these cases, the pre-image chosen for one S-box does not influence the other and it is easier to count. We introduce two other notations:

$$e(X, i, j) = Card\{I \in \mathbf{F}_2^6, I_1 = i, I_0 = j, S_p(I) = X\}$$

$$f(Y, k, l) = Card\{J \in \mathbf{F}_2^6, J_5 = k, J_4 = l, S_q(I) = X\}.$$

Then, counting over all the 4 possible cases for (i, j, k, l), we get:

$$D(X, Y, s, t) = \sum_{i,j} e(X, i, t \oplus j) f(Y, s \oplus i, j).$$

It can be seen that the uniform distribution $\mathcal{U}$ is partitioned in 4 distributions $\mathcal{V}_{00}$, $\mathcal{V}_{01}$, $\mathcal{V}_{10}$ and $\mathcal{V}_{11}$. Moreover it can bee seen that there is a symetry that implies that there are only two different (and complementary) distributions.
We note $\overline{s} := s \oplus 1$ (the negation). We will show that $\forall X, Y, D(X, Y, s, t)$ depends only on $s \oplus t$. For this, it is sufficient to show that, for all (s, t) the distribution $\mathcal{V}_{st}$ defined by $(X, Y) \mapsto D(X, Y, \overline{s}, \overline{t})$ is identical to $\mathcal{V}_{\overline{s}\overline{t}}$ defined by $(X, Y) \mapsto D(X, Y, s, t)$.
This fact is due to the S-box design criterion about 4 permutations, already used above. This criterion implies the following facts:

$$\forall j \in \mathbf{F}_2, e(X, 0, j) + e(X, 1, j) = 2$$

$$\forall k \in \mathbf{F}_2, f(Y, k, 0) + f(Y, k, 1) = 2$$

$$\sum_{i,j} e(X, i, j) = \sum_{k,l} f(Y, k, l) = 4$$

From this we get:

$$\begin{aligned} D(X, Y, \overline{s}, \overline{t}) &= \sum_{i,j} e(X, \overline{i}, t \oplus j) f(Y, s \oplus i, \overline{j}) \\ &= \sum_{i,j} (2 - e(X, i, t \oplus j))(2 - f(Y, s \oplus i, j)) = D(X, Y, s, t) \end{aligned}$$

It is also possible to show that $D(X, Y, \overline{s}, t) + D(X, Y, s, t) = 8$ (this is due to the fact that now the uniform distribution $\mathcal{U}$ is partitioned into only 2 distributions $\mathcal{U}_{s \oplus t=0}$ and $\mathcal{U}_{s \oplus t=1}$ that have therefore to be complimentary). From all the above, one can derive a "symmetric" formula for $D(X, Y, s, t)$ due to Davies and Murphy [17], in the following form:

$$D(X, Y, s, t) = 4 + (-1)^{s \oplus t} e(X) f(Y) \qquad (\#)$$

with by definition $e(X) \stackrel{def}{=} e(X, 0, 0) - e(X, 0, 1)$ and $f(Y) \stackrel{def}{=} f(Y, 0, 0) - f(Y, 1, 0)$.
This formula (#) is quite strong, yet from the above we see that it is due only to the way consecutive S-boxes are connected in DES and to the fact that the S-boxes are constructed as 4 permutations depending on the two "side bits" in the input.
The key property (#) is precisely what allows to mount efficient attacks on DES. Indeed, it is possible to see that it extends in an interesting way to several rounds of DES, see [17]. In this paper we do not study the Davies-Murphy attack, we only study the S-boxes and their resistance against the attack.

4.2 Our simulations on $e()$ and $f()$

All the information on S-boxes necessary in the Davies-Murphy attack can be derived from the following table that gives the values of $(e(X), f(X))$ for each S-box and each value of X. To the best of our knowledge this table has never been published so far: Davies and Murphy [17] only publish the resulting distribution $(X, Y) \mapsto D(X, Y, s, t)$ for the pair (S_1, S_2) while the most interesting pair is apparently (S_7, S_8) (which we confirm). From the table that follows, all the distributions may be computed. (Apparently these results can also be found in [16], but this paper was never published and is not widely available).

Table 2. Simulations on Davies-Murphy Attack on DES: values of $(e(X), f(X))$

	X															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0,1	-1,0	2,0	0,0	0,0	1,0	0,-1	-1,0	-1,-1	0,-1	-2,0	1,0	-1,-1	1,1	1,1	0,1
S_2	0,-1	-1,-1	2,0	-1,1	-2,0	2,0	0,1	0,0	0,1	2,0	0,-2	-2,0	1,0	0,-1	-1,1	0,1
S_3	-1,0	0,-1	0,0	0,1	0,0	0,1	-1,0	0,0	0,-2	1,0	1,1	1,0	0,0	-1,-1	0,1	0,0
S_4	-1,0	0,-1	-2,0	0,1	0,0	0,1	-1,0	2,0	2,0	1,0	0,-1	0,0	0,-1	-2,0	0,1	1,0
S_5	0,0	0,0	-1,0	0,0	1,1	-2,0	0,1	2,0	0,-2	0,0	0,0	0,0	0,1	0,-1	0,0	0,0
S_6	0,0	0,1	0,0	0,-2	-1,0	1,-1	-1,1	0,1	-1,0	0,0	0,1	0,0	2,0	-1,0	1,-1	0,0
S_7	0,2	-1,-1	0,1	0,-1	0,0	0,0	1,-1	1,-1	0,0	1,1	0,0	0,0	1,-1	-2,0	-2,0	1,1
S_8	0,0	-1,0	-1,-1	0,1	0,0	2,0	-1,1	0,-1	0,1	-1,-1	1,0	1,0	0,-1	0,1	0,-2	0,2

4.3 Local Uniformity Criteria or How to Resist the Davies-Murphy Attack

We recall that $D(X, Y, s, t) = 4 + (-1)^{s \oplus t} e(X) f(Y) \quad (\#)$. In order to make this uniform, we need to have $e(X)f(Y) = 0$. This can be done, for example, if the S-boxes verify **one** of the following properties:

1. For every S-box and for every X, $e(X) = 0$.
2. For every S-box and for every X, $f(X) = 0$.
3. For every other S-box (for example all the S-boxes with odd numbers), and for all X, $e(X) = f(X) = 0$.

In Section 4 of [1], the authors give conditions written in terms of differentials, and that are sufficient respectively to achieve points 1 and 2.

Design Criterion 4.3.1. For every S-box,
$$\forall x, S(x) \neq S(x \oplus (0abc11)_b), \forall a, b, c.$$
Design Criterion 4.3.2. For every S-box,
$$\forall x, S(x) \neq S(x \oplus (11abc0)_b), \forall a, b, c.$$
Similarly, it is easy to see that we may also achieve point 3 by the following:

Design Criterion 4.3.3. For every second S-box, both conditions of Criterion 4.3.2 and Criterion 4.3.2 hold.

In order to make DES secure against the Davies-Murphy attack it is sufficient that **one** of these criteria is satisfied. For example, in [28], the authors replace the S-boxes of DES by a new set of S-boxes, reportedly following all the known design criteria, and having better resistance against Davies-Murphy attacks. We verified that these S-boxes satisfy the Design Criterion 4.3.2 (cf. (D-1) in Section 3) to achieve $f = 0$. However, we saw that these S-boxes do **not** verify our Criteria 4.3.1 and 4.3.3.

Remark 1: The first two criteria allow to select DES S-boxes independently of each other, and yet to become fully resistant against the "basic" Davies-Murphy attack using two consecutive S-boxes.

Remark 2: Though one of the above criteria allows to resist the "basic" Davies-Murphy attack, in the next section we will see that the s^{5}DES S-boxes are not yet perfect against "the general idea of Davies-Murphy attacks" that could use several consecutive S-boxes.

4.4 About Global Uniformity Criteria

A good cipher should resist not only all the known attacks, but if possible, also potential or future attacks. In the previous section we saw that it is possible quite easily to insure that the Davies-Murphy attack with pairs of S-boxes will not work. The question is, how to make sure that there will be no similar attacks using, for example 3 or 4 consecutive S-boxes ?

The extension of Davies-Murphy for 3 consecutive S-Boxes has already been considered [17, 28]. The design of s^{5}DES specifically prevents the Davies-Murphy attack on triplets of S-boxes. In this paper we want to define a more general resistance criterion that encompasses the resistance against the extension of the attack for 4 and more S-boxes.

For this, given a Feistel cipher defined by several rounds $\Psi(f) : \{0,1\}^{2n} \rightarrow \{0,1\}^{2k}$ of the form:

$$\Psi(f) \stackrel{def}{=} \begin{cases} L \leftarrow R \\ R \leftarrow L \oplus f_K(R) \end{cases}$$

More or less informally, we require the following properties:

a For a fixed K, the output distribution $\{0,1\}^k \rightarrow \{0,1\}^k$ defined by $R \mapsto f_K(R)$ should be as close to uniform as possible.

b This distribution, if not uniform, should depend on the key K in "a complex way".

For comparison, here are the statistics obtained for DES and s^{5}DES:

Table 3. Global uniformity in one round of DES vs. s^{5}DES

n	# of values taken n times	
	DES	s^{5}DES
0	1371894909	68006170
1	1831024093	4159136276
2	898337028	67652370
3	121636222	171832
4	63911645	648
5	3725130	0
6	3702019	0
7	69289	0
8	643992	0
9	9632	0
10	8369	0
11	0	0
12	4720	0
13	0	0
14	0	0
15	0	0
16	248	0

Comparison: First of all we see that for a fixed K, DES round function is not bijective. This property has previously been noted by many authors, see [19, 29, 18]. Here we jump into more quantitative analysis and observe that: 32 % of outputs are never taken, 43 % of outputs are taken once, 21 % are taken twice etc. 3 % are taken three times etc. In comparison, for s^{5}DES, the distribution is much more close to uniform, 96 % of outputs are taken exactly once, and only 1.6 % are never taken. Clearly s^{5}DES is a very good cipher compared to DES (but yet not perfect) also for our new (global) security criterion.

Are These Relevant to the Security of DES and s^{5}DES ?

The answer to this question is not obvious. In fact there is not only doubt whether the observed property are at all relevant to security of DES and s^{5}DES, but also, which, DES ro s^{5}DES is indeed a stronger design. Below we present some arguments:

1. For sure, our requirement assures that even if we use all the outputs of the round function the Davies-Murphy attack is impossible.
2. However creating "optimal" security against one attack may introduce other weaknesses. The actual design choices of DES and any other cipher are usually rather a matter of compromise between conflicting criteria.
3. In the best version of Davies-Murphy attack, the S-boxes 7 and 8 only are exploited, and for this pair it can be seen from table 2 and formula (#) that, when $s \oplus t = 0$, there are exactly two values X, Y that are not taken: $(13, 15)$ and $(14, 15)$. This accounts for $2 \cdot 2^{4 \cdot 6}$ values that are not taken in the global distribution above, i.e. for 0,8 %. The remaining 31 % are not exploited in the Davies-Murphy attack. This may suggest that there may be better attacks on DES that would use more than 2 consecutive S-boxes or/and combine known properties. Unfortunately:
4. This remark have been suggested by one of the referees of FSE 2004. The probability distribution observed for DES ressembles that of a random function except at 11 and 16. If we replace the round function by a random function, the Luby-Rackoff theory allows to prove that the cipher is secure. Therefore, one should not think that such a biased output is by itself insecure.
5. Yet all hope is not lost: The real question is how the biased distribution depends on the key and if this leads to properties that can be combined for several rounds. We don't know if this remark on DES can lead to more efficient attacks than those that are already known.
6. As concerning s^{5}DES, we observe that the distribution for s^{5}DES is much more uniform than for DES (though it is not perfect). But this does not necessarily mean that s^{5}DES is stronger than DES.

Clearly, our strict uniformity requirement is probably too strong to protect practical Feistel ciphers against practical attacks. Besides, it is an open problem to know if there is a set of S-boxes that satisfies all the design criteria and giving a strictly uniform distribution.

4.5 Davies-Murphy Attacks and Linear Cryptanalysis

Linear cryptanalysis of DES was not known when the Davies-Murphy attacks were developed in the 80s [15, 17, 16]. At Eurocrypt'94, Biham remarked on page 347 of [3] that all the existing Davies-Murphy attack contain a linear attack, and moreover the complexity of the two is roughly the same, i.e. the Davies-Murphy attacks **are** in a way linear attacks. Thomas Pornin has also studied general criteria of resistance against Davies-Murphy attacks, see [34]. In this light, it appears to us that in general, all Davies-Murphy attacks on an arbitrary cipher should be seen as a multiple approximation linear attacks (see [26]).

5 Experimental Facts on DES Related to Linear Cryptanalysis

In this Section we study a property that at the time of discovery seemed very surprising because it holds simultaneously for several DES S-boxes. We will see that it is not so surprising. However in Section 6 we present similar and even more surprising properties.

5.1 Linear Characteristics Common to Several S-boxes

In a paper published at Crypto'85 [35], Shamir shows that a strong bias (also discovered by Franklin in his PhD thesis), is present in all S-boxes of DES. There is a strong correlation between the second input bit x_2 and the XOR of all output bits $y_1 \oplus y_2 \oplus y_3 \oplus y_4$. However later Don Coppersmith *et al.* observed that this fact could to some extent be explained by the known design criteria on DES S-boxes, see [35].

To see this, we looked at the number of linear characteristics of the form

$$\sum_i \alpha_i x_i + \sum_i \beta_i y_i = \gamma$$

that are true a probability somewhat $\neq 1/2$ for several S-boxes. Given a linear approximation (α, β) We count the number A_i of outputs for which the approximation is true. Then we will compute the following three statistics:

1. A being the average of the A_i,
$$A = \frac{1}{8} \sum_{i=1}^{8} A_i$$
The expected value of A is 32.
2. D will mesure the deviation from the actual average, i.e.
$$D^2 = \sum_{i=1}^{8} (A_i - A)^2$$
3. D' will mesure the deviation from the expected average, i.e.
$$D'^2 = \sum_{i=1}^{8} (A_i - 32)^2$$

In the following table we show some leading results, all those for which $D \geq 5$, sorted by the decreasing values of D.

Table 4. Simultaneous Linear Approximations in DES

DES				
A	D	D'	α	β
25.50	**35.30**	44.36	**010000**	**1111**
27.50	23.96	40.40	111011	0100
27.50	18.92	37.63	111111	0010
36.75	17.42	61.22	000100	1111
36.50	14.35	59.73	001011	0011
27.25	12.94	34.35	010000	1101
36.75	11.98	59.90	011001	1010
27.50	11.22	34.41	111111	1000

s^5DES				
A	D	D'	α	β
37.50	24.12	65.42	100010	1101
36.50	22.76	62.29	111111	0010
26.00	11.66	30.59	100010	1011
36.50	10.86	58.99	101110	1101
26.75	10.17	32.06	001010	0111
27.50	8.83	33.70	110110	0110
36.75	7.97	59.23	111000	0101

The property discovered by Shamir in [35] happens to be the leading result in the left table. If we remove this leading property with $D = 35.30$, we see no difference whatsoever between the behaviour of DES and s^5DES. This confirms the idea that these properties can be accounted for by the known design criteria on the S-boxes, as claimed by Coppersmith *et al.*, see [35].

6 Experimental Facts on DES Related to Algebraic Attacks

6.1 Algebraic Attacks on Block Ciphers

In this paper we do not present any attack, we only study the DES S-boxes. We will however study properties that are (at least remotely) motivated or related to some known attacks.
The study of monomial equations (and later of bi-monomial equations) is motivated, as we will explain below, by the XSL-type attacks on block ciphers [8]. Though it is not proven that these attacks work, and is quite unclear what is the exact complexity of these attacks, the cautionary (or "paranoid") approach in the design of block ciphers will be to counter such attacks. And it is not so hard to achieve. Following [8], to prevent algebraic attacks, one should make sure that the S-boxes of the cipher are not described by a small system of multivariate equations with a small number of monomials. In theory it cannot be avoided, and obviously every S-box can always be described by a system of r multivariate equations with t monomials, with some big (r, t). In practice it will be true for random S-boxes: it is shown in [8] that the complexity of the XSL attack is (at least) double-exponential in the size of the S-box. However, for many practical ciphers, the S-boxes are usually selected to be **better** than random in many respects, and for good reasons. Therefore, we propose not to switch back to random S-boxes, but to add design criteria. We will therefore require that "good" S-boxes should (in addition to many known criteria) also behave better or as good as random in this aspect. Thus, still following [8], we need to make sure that t is always quite big and that r/t is quite small, (at least compared to random S-boxes of the same size).
In [8], authors study mainly multivariate equations of small degree (2 or 3). However it is (apparently) not necessary that the equations are of small degree in order to apply the XSL approach (however they cannot be completely arbitrary either, and should for example contain linear monomials in order to connect with other equations of the cipher). Following the (heuristic and approximative) results of [8], what would decrease the complexity of the alleged XSL attack, is to find a small set of t monomials with small t, for example $t = 100$, and exhibit some r equations with r not much smaller than t, for example $r = 50$, and hopefully more, the ideal situation would be to have $r \approx t$.

6.2 Monomial Equations

A simple way to obtain a system of equations with $r \approx t$ is to use monomial equations, i.e. equations that are composed of only one monomial, for example it can be seen that for the AES/Rijndael S-box we have always $0 = x_8y_1y_5y_6y_7y_8$.
In general the existence of a large number of such equations can be shown by probability considerations. For example if we consider a DES-size S-box with $s = 6$ inputs, the term $x_1x_5x_4x_3x_2$ is equal to 1 only with probability 2^{-5} and the number of inputs x for which it is 1 is exactly $2^s * 2^{-5} = 2$. If we multiply this term by for example y_2, the probability that y_2 is 0 for all these two inputs is quite big: 2^{-2}.
Thus we see that for a randomly chosen S-box, with probability only 2^{-2}, the equation $0 = x_1x_5x_4x_3x_2y_2$ is true with probability 1. The same is true for a large number of similar equations.
It is not at all certain that for such (very special) equations the XSL attack will work well. However, again the "paranoid" approach would be to study these equations.
We have compared the number of monomial equations found for the DES, s^{5}DES and a random S-box of the same size.

Table 5. Monomial Equations in DES vs s^5DES

random S-box	DES S-box								s^5DES S-box							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
$0 - 463$	170	140	179	145	207	154	153	173	167	170	189	135	133	136	100	170

Statistical properties: We look at the average values and standard deviations of the values we obtained.

	1000 random S-boxes	DES S-boxes	s^5DES S-boxes
mean value	207.8	165.1	150.0
standard deviation	86.8	20.4	27.0

We see that the design criteria constrain the number of monomial equations in a small interval around 160, whereas they vary a lot for random S-boxes.

6.3 Interesting Remark Concerning the Design of Block Ciphers

In our simulations we found, quite surprisingly, that though as explained above the existence of such monomial equations is a natural phenomenon, there are S-boxes that have no such equations whatsoever. We obtained 0 for exactly 6.4% of random S-boxes of the same size as in DES. From the algebraic attacks proposed in [8] with low-degree equations, the conclusion was that one should use random S-boxes[2]. Yet, we see that some S-boxes could be stronger than random S-boxes of the same size against algebraic attacks with monomial equations. A possible conclusion would be:

Design Criterion 6.3.1. A “paranoid” S-box should have a small number of monomial equations in order to resist potential algebraic attacks.

We emphasise the fact that it is not demonstrated that algebraic attacks on block ciphers from [8] do indeed work, and even less certain for algebraic attacks that would use/mix with equations having a quite small number of monomials but being of higher degree than in [8].

6.4 Bi-Monomial Equations

For all DES S-boxes, we also computed the exact number equations that have two monomials. These are divided in two parts, equations having one and two monomials. We also computed the exact number monomials that appear in these two sets of equations put together, that turns out to be lower than expected. Again, the results are compared to random S-boxes of the same size and to the set of s^5DES S-boxes from [28].

Table 6. Bi-monomial Equations in DES vs s^5DES

	random S-box	DES S-box								s^5DES S-box							
		1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1 monomial	$0 - 463$	170	140	179	145	207	154	153	173	167	170	189	135	133	136	100	170
2 monomials	$233 - 524$	360	385	322	362	303	345	379	329	352	324	309	367	381	354	442	310
all monomials	$606 - 703$	587	588	565	569	569	556	589	546	582	540	560	561	566	560	600	546

Observations: We see that the behaviour of s^5DES is similar to DES. Nothing suspicious is found so far.

[2] For random S-boxes the complexity of algebraic attacks is expected to be double-exponential in the size of the S-box

6.5 Bi-Monomial Equations Common for Several S-boxes

We looked at the number of bi-monomial equations that are true simultaneously for several different S-boxes.

Table 7. Simultaneous Bi-monomial Equations in DES vs s⁵DES

	8 random S-boxes	DES S-boxes	s^5DES S-boxes
1 S-box	2359	2049	2174
2 S-boxes	183	241	265
3 S-boxes	15	32	37
4 S-boxes	3	**21**	6
5 S-boxes	2	**12**	0
6 S-boxes	0	0	0
7 S-boxes	0	**2**	0
8 S-boxes	0	0	0

The behaviour of s^5DES is not really different that for random S-boxes. We see however that the DES S-boxes are somewhat special: there are equations that are true simultaneously for 7 of them. This in itself is not yet extraordinary, and it could occasionally happen even for random S-boxes.

6.6 A Closer Look at Simultaneous Bi-Monomial Equations

In this section we study the leading bi-monomial equations the are common for at least 5 or more S-boxes. For s^5DES, no such equations exist, and therefore these equations probably do not result at all form the known design criteria on DES.
Here are all the equations true for some subset of 7 S-boxes:

$$\begin{array}{ll} & \text{S-boxes} \\ \left\{\begin{array}{l} x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_5\, x_6\, y_1 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, y_1 \end{array}\right. & \begin{array}{l} 11110111 \\ 11110111 \end{array} \end{array}$$

And here are all the equations true for some subset of 5 S-boxes:

$$\begin{array}{ll} & \text{S-boxes} \\ \left\{\begin{array}{l} x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, y_4 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, y_2 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_4\, x_5\, y_1 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_4\, x_3\, x_6\, y_1 \\ \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_4\, x_5\, y_1\, y_2 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_3\, x_5\, x_6\, y_1\, y_2 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_3\, x_4\, x_5\, x_6\, y_1\, y_2 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_3\, x_4\, x_5\, x_6\, y_1\, y_2 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_5\, x_6\, y_1\, y_2 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_4\, x_6\, y_1\, y_2 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_2\, x_3\, x_4\, x_5\, x_6\, y_1\, y_2 \\ x_1\, x_2\, x_3\, x_4\, x_5\, x_6 = x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, y_1\, y_2 \end{array}\right. & \begin{array}{l} 11001101 \\ 10110110 \\ 10110110 \\ 10110011 \\ \\ 10110110 \\ 10110110 \\ 10110110 \\ 10110110 \\ 10110110 \\ 10110110 \\ 10110110 \\ 10110110 \end{array} \end{array}$$

We observe that x_3 is present in all equations, this however might be a consequence of the design criteria. We also observe that these equations clearly distinguish y_2 and y_1. This cannot be a consequence of the known design criteria, as these are invariant modulo any permutation of the y_i. On the contrary up till now, the output of DES S-boxes were believed to be of "equivalent status", as stated by Davies on page 92 of [15].
We also observe that these equations clearly distinguish S-boxes 2, 5 and 8, and no such distinction can be a consequence of the design criteria.

Can All This Happen by Accident ?

First of all, the existence of equations such as $x_1x_2x_3x_4x_5x_6 = x_1x_2x_3x_4x_5x_6y_1y_2$ is not so surprising, given a fixed equation, the probability it is true for a random S-boxes is not small, can be even 1/4, see 6.2. There one can admit that it can happen simultaneously for several S-boxes (even if clearly, we observe a difference in Table 7). Accordingly, we observe the set of last 8 equations, among the equations that are true for 5 S-boxes. It is very homogenous: the set of S-boxes for which these equations are true is exactly the same, and the product of y_i that appears in these equations is exactly the same. Yet we assume that all this is normal and could have happened by accident.

Then, we want to know what is the probability, for this subset, of obtaining always the same subset of 5 S-boxes, in each of the 8 cases. A naive estimation is that it would be about $\binom{8}{5}^{-7} \approx 2^{-41}$. Unfortunately, as pointed out by a referee of FSE'2003, this estimation is not correct. This is because all these 8 Boolean equations are highly correlated. A tentative estimation that we will not detail suggests that the probability of this happening is only about 2^{-14}. In practice less, because we assumed that the statistics of DES contained in Table 7 are normal.

We offer no real conclusion. Though it seems that the observed properties are not a consequence of known design criteria, and can hardly happen by chance, the probability they actually do happen is not so small. They could easily be a consequence of some yet unknown design criteria that increase some probabilities. It is very unlikely that these properties are useful in some kind of attack on DES.

Remark: At Eurocrypt'94 Matsui studies [32] the security of DES against differential and linear attacks considering different orders of S-boxes. Rearranging S-boxes is related to different properties shown in this paper, but it cannot possibly explain them (for example why bits y_2 and y_1 are distinguished in DES ?). To the best our knowledge, no known attacks on DES do explain these properties.

7 Conclusion

DES is the most important cryptographic algorithm ever made. Though DES keys of 56 bits are now completely out of date, one should not forget that there millions of them in use, and the triple-DES will probably still be widely used for many years to come. In the meantime the cryptographic research advances, and therefore the security of DES should not be taken for granted. In particular one should think not only about known attacks on DES, but also try to think what could be the future attacks.

In this paper we raised an important question that received so far very little attention: have the S-boxes of DES been chosen independently of each other on some criteria (as currently believed) or are they also some global design criteria for the whole set ? With regard to this question, we studied many different properties of DES subsets of 2 or more S-boxes. We defined a general security criterion on the round function that encompasses a large class of attacks including the Davies-Murphy attack. We also studied other properties related to linear cryptanalysis and algebraic attacks on block ciphers. We presented some marginal, but not really conclusive evidence that the S-boxes of DES have NOT been chosen independently of each other. This is clearly not included in the known design criteria.

Accidentally, we introduced a new type of algebraic attack on block ciphers (based on the XSL attack from [8]), and a new rather "paranoid" criterion to resist such attacks (even if it is not demonstrated that such attacks will work in practice). We show that none of the S-boxes of DES or s^{5}DES satisfy this criterion. We show however that there exist S-boxes that do satisfy it. This could be of independent interest.

This paper also shows that the design of s^5DES, claimed much better than DES, is far from being perfect. We were surprised to find that also the S-boxes of s^5DES have NOT been chosen independently of each other, and this (again) can hardly be explained by the (even extended) design criteria on "improved DES". In addition, s^5DES still does not achieve our global uniformity criterion for the outputs of the round function $F()$. These properties do seriously decrease the credibility of s^5DES as a DES replacement. On the contrary, as long as there is some uncertainty concerning the security of AES [8], it is possible that it is DES (or rather triple DES), that will for many people remain the best choice as a trusted encryption algorithm. In spite of and also **because** it is under intense scrutiny of the research community.
Acknowledgments. We thank Eli Biham and anonymous referees of FSE 2003 for valuable comments.

References

1. Eli Biham and Alex Biryukov, *An Improvement of Davies' Attack on DES,* Journal of Cryptology, vol. 10, Nb. 3, pp. 195-205, Summer 1997.
2. Eli Biham and Adi Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*. Journal of Cryptology, vol. 4, pp. 3-72, IACR, 1991.
3. Eli Biham: *On Matsui's Linear Cryptanalysis,* Eurocrypt'94, LNCS 950, Springer-Verlag pp. 341-355.
4. D.K. Branstead, J. Gait, S. Katzke, *Report of the Workshop on Cryptography in Support of Computer Security*. National Bureau of Standards, September 21-22, 1976, NBSIR 77-1291, September 1977.
5. E.F. Brickell, J.H. Moore, M.R. Purtill, *Structure in the S-Boxes of DES,* Crypto'86, LNCS 1440, pp. 3-7, Springer, 1986.
6. L.P. Brown, *Analysis of the DES and the Design of the LOKI Encryption Scheme,* PhD Thesis, Dept. Computer Science, UC UNSW, ADFA, Canberra, Australia, 1991.
7. L.P. Brown, J. Seberry, *On the design of permutation P in DES type cryptosystems,* Eurocrypt'89, LNCS 434, pp. 696-705. Springer, 1990.
8. Nicolas Courtois and Josef Pieprzyk: *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations,* Asiacrypt 2002, LNCS 2501, pp.267-287, Springer, A preprint with a different version of the attack is available at `http://eprint.iacr.org/2002/044/`.
9. Don Coppersmith, *The Data Encryption Standard (DES) and its strength against attacks,* Technical Report RC 18613, IBM T.J. Watson Center, December 1992.
10. Don Coppersmith, *The Data Encryption Standard (DES) and its strength against attacks,* IBM Journal of Research and Development, Vol. 38, n. 3, pp. 243-250, May 1994.
11. Don Coppersmith, *The development of DES, Invited Talk, Crypto'2000, August 2000.*
12. *Nicolas T. Courtois: Feistel Schemes and Bi-Linear Cryptanalysis,* To be presented at Crypto 2004,
13. Joan Daemen, Vincent Rijmen: *AES proposal: Rijndael,* The latest revised version of the proposal is available on the internet, `http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf`
14. Joan Daemen, Vincent Rijmen: *The Design of Rijndael. AES - The Advanced Encryption Standard,* Springer-Verlag, Berlin 2002. ISBN 3-540-42580-2.
15. D.W. Davies, *Some Regular Properties of the Data Encryption Standard,* Crypto'82, pp. 89-96, Plenum Press, New-York, 1982.
16. D. Davies: *Investigation of a potential weakness in the DES algorithm,* July 1987 (revised January 1990), preprint.
17. D. Davies and S. Murphy, *Pairs and Triplets of DES S-Boxes,* Journal of Cryptology, vol. 8, Nb. 1, pp. 1-25, 1995.
18. Marc Davio, Yvo Desmedt, Marc Fosseprez, René Govaerts, Jan Hulsbosch, Patrik Neutjens, Philippe Piret, Jean-Jacques Quisquater, Joos Vandewalle, Pascal Wouters: *Analytical Characteristics of the DES.* In David Chaum editor, Crypto 1983, pp. 171-202, Plenum Press, New York, 1984.

19. Yvo Desmedt: *Analysis of the Security and New Algorithms for Modern Industrial Cryptography,* PhD thesis, KU Leuven, Leuven, Belgium, October 1984.
20. Horst Feistel: *Cryptography and computer privacy;* Scientific American, vol. 228, No. 5, pp. 15-23, May 1973.
21. *Data Encryption Standard*, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).
22. *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Bureau of Standards, Gaithersburg, MD (1999). Available from `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`
23. M.E. Hellman, R. Merkle, R. Schroppel, L. Washington, W. Diffie, S. Pohlig, and P. Schweitzer: *Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard,* Technical report, Stanford University, U.S.A., September 1976.
24. M.E. Hellman, R. Merkle, R. Schroppel, L. Washington, W. Diffie, S. Pohlig, and P. Schweitzer: *Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard,* Technical report, Stanford University, U.S.A., September 1976.
    Known also as "Lexar Report", Lexar Corporation, Unpublished Report, 11611 San Vicente Blvd., Los Angeles, 1976.
25. Pascal Junod: *On the complexity of Matsui's attack,* Selected Areas in Cryptography (SAC'01), Toronto, Canada, LNCS 2259, pp. 199-211, Springer, 2001.
26. Burton S. Kaliski Jr, and M.J.B. Robshaw. *Linear Cryptanalysis Using Multiple Approximations,* Crypto'94, LNCS, Springer, pp. 26-39.
27. J.B. Kam and G.I. Davida: *Structured design of substitution-permutation encryption networks;* IEEE Trans. on Computers, Vol. C-28, 1979, pp.747-753.
28. Kwangjo Kim. Sangjin Lee, Sangjoon Park, Daiki Lee: *Securing DES S-boxes against Three Robust Cryptanalysis,* SAC'95, pp.145-157.
29. A.G. Konheim, Cryptography, Seminars of Excellence, ORSYS Institute, Amsterdam, June 9-11, 1986.
30. C.H. Meyer, S.M. Matyas, *Cryptography: A New Dimension in Data Security*, John Wiley & Sons, New-York, 1982.
31. M. Matsui: *Linear Cryptanalysis Method for DES Cipher,* Eurocrypt'93, LNCS 765, Springer, pp. 386-397, 1993.
32. M. Matsui, *On correlation between the order of S-boxes and the strength of DES,* Eurocrypt'94, LNCS 950, pp. 366-375, Springer, 1995.
33. M.Matsui: *The First Experimental Cryptanalysis of the Data Encryption Standard,* Advances in Cryptology: Proc. of CRYPTO '94, LNCS 839, Springer, pp. 1-11, 1994.
34. Thomas Pornin: *Optimal Resistance Against the Davies and Murphy Attack.* In Asiacrypt 1998, LNCS 1514, Springer, pp. 148-159, 1998.
35. Adi Shamir: *On the security of DES,* Crypto'85, LNCS 218, Springer, pages 280-281.

A What do s^{5}DES S-boxes Say to Each Other ?

We have seen that the S-boxes of DES have not been chosen independently of each other. It does not however mean that DES is not secure. It does not mean either that s^{5}DES is more secure than DES.
In fact, in this section we will show that also for s^{5}DES, quite surprisingly the S-boxes have **NOT** been chosen independently of each other.
We know from Section 4.3 that in order to resist the basic Davies-Murphy attack with pairs of S-boxes, it is sufficient that for each of the S-boxes, we always have $f(X) = 0$, and this can be for example achieved following the Design Criterion 4.3.2.
It can be seen that the Design Criterion 4.3.2 implies that, in the table of the S-box, for two lines that have the same parity, (i.e. lines 0 and 2 or 1 and 3) the left halves of the lines are permutations of the same subset A or B (the other halves are their complements A^c and B^c in $\{0..16\}$). Therefore we always have the following structure:

s$_1^5$	
A	A^c
B	B^c
A	A^c
B	B^c

Yet, what we discovered is that the same sets A, B have been reused, for no apparent reason, for other S-boxes of s^{5}DES:

Table 8. The Unexpected Common Structure Between Different S-boxes of s^{5}DES

s$_1^5$		s$_2^5$		s$_3^5$		s$_4^5$		s$_5^5$		s$_6^5$		s$_7^5$		s$_8^5$	
A	A^c	A^c	A	C	C^c	A^c	A	C	C^c	D	D^c	C^c	C	A	A^c
B	B^c	B^c	B	B	B^c	B^c	B	B^c	B	B	B^c	B^c	B	B	B^c
A	A^c	A^c	A	C	C^c	A^c	A	C	C^c	D	D^c	C^c	C	A	A^c
B	B^c	B^c	B	B	B^c	B^c	B	B^c	B	B	B^c	B^c	B	B	B^c

Legend: each half-line is filled with a permutation of sets $A, B, C, D, A^c, B^c, C^c, D^c$ with:
$A = \{1, 2, 4, 7, 9, 10, 12, 15\}$, $B = \{1, 2, 4, 7, 8, 11, 13, 14\}$, $C = \{1, 2, 5, 6, 8, 11, 12, 15\}$, $D = \{2, 3, 4, 5, 8, 9, 14, 15\}$.

Only four different sets are used in s^5DES, instead of potentially $2 \cdot 8 = 16$ different sets that could be used. Moreover, in the second and the last lines, one always has B or B^c for all the eight S-boxes.
As a consequence of this observation, when $x_6 = 1$ and x_2 is fixed, the set of outputs of the S-boxes is B or B^c. This may potentially lead to many different attacks. We propose here two directions.

A.1 Bi-Linear Cryptanalysis of s^{5}DES

In a paper to be presented at Crypto 2004 [12] Courtois introduces the bi-linear cryptanalysis of block ciphers. The analysis of s^{5}DES S-boxes w.r.t. this new attacks shows the following very surprising fact, clearly closely related to our observations of Fig. 8.

Fact A.1.1 (Best Bi-Linear Characteristics of s^{5}DES). For each of the s^{5}DES S-boxes, there is exactly one bi-linear equation that is true with probability 1:

```
S1. 1+x[2]+          y[2]+y[3]+y[4]+x[6]*y[1] = 0
S2.   x[2]+          y[2]+y[3]+y[4]+x[6]*y[1] = 0
S3. 1+x[2]+     y[1]+     y[3]+y[4]+x[6]*y[2] = 0
```

```
S4.   x[2]+           y[2]+y[3]+y[4]+x[6]*y[1] = 0
S5. 1+x[2]+x[6]+y[1]+      y[3]+y[4]+x[6]*y[2] = 0
S6. 1+x[2]+     y[1]+y[2]+y[3]+      x[6]*y[4] = 0
S7.   x[2]+     y[1]+      y[3]+y[4]+x[6]*y[2] = 0
S8. 1+x[2]+           y[2]+y[3]+y[4]+x[6]*y[1] = 0
```

These allow to build bi-linear attacks on reduced (and full) versions of s^{5}DES, for example we have the following fact :

Fact A.1.2 (Weakness of s^{5}DES). Though for linear cryptanalysis s^{5}DES is substantially stronger than DES, for bi-linear cryptanalysis, there are 3-round characteristics for that are **better** than best existing 3-round characteristic that exist in DES.

For details we refer to the extended version of [12].

A.2 Linear Cryptanalysis and s^{5}DES

The quadratic equations described in the previous section imply only one product, and therefore we can use these to derive several linear equations on the S-boxes of s^{5}DES that will be true with very high probability (these remain still closely related to our observation of Fig. 8). Thus we obtain that the round function of S^{5}DES have many linear approximations that have low probabilities, and present a surprisingly regular structure:

Table 9. Interesting Linear Approximations Found for s^{5}DES

S1	16/64	I[1]	O[17 23 31]	S5	16/64	I[17]	O[8 25 3]
S1	16/64	I[1]	O[9 17 23 31]	S5	48/64	I[17]	O[8 14 25 3]
S1	16/64	I[1 5]	O[17 23 31]	S5	16/64	I[17 21]	O[8 25 3]
S1	48/64	I[1 5]	O[9 17 23 31]	S5	16/64	I[17 21]	O[8 14 25 3]
S2	48/64	I[5]	O[28 2 18]	S6	16/64	I[21]	O[4 29 11]
S2	48/64	I[5]	O[13 28 2 18]	S6	16/64	I[21]	O[4 29 11 19]
S2	48/64	I[5 9]	O[28 2 18]	S6	16/64	I[21 25]	O[4 29 11]
S2	16/64	I[5 9]	O[13 28 2 18]	S6	48/64	I[21 25]	O[4 29 11 19]
S3	16/64	I[9]	O[24 30 6]	S7	48/64	I[25]	O[32 22 7]
S3	16/64	I[9]	O[24 16 30 6]	S7	48/64	I[25]	O[32 12 22 7]
S3	16/64	I[9 13]	O[24 30 6]	S7	48/64	I[25 29]	O[32 22 7]
S3	48/64	I[9 13]	O[24 16 30 6]	S7	16/64	I[25 29]	O[32 12 22 7]
S4	48/64	I[13]	O[20 10 1]	S8	16/64	I[29]	O[27 15 21]
S4	48/64	I[13]	O[26 20 10 1]	S8	16/64	I[29]	O[5 27 15 21]
S4	48/64	I[13 17]	O[20 10 1]	S8	16/64	I[29 1]	O[27 15 21]
S4	16/64	I[13 17]	O[26 20 10 1]	S8	48/64	I[29 1]	O[5 27 15 21]

It is quite strange for a cipher that have been proposed mainly to resist Matsui's linear cryptanalysis of DES. It is possible that, for single linear approximations, s^{5}DES resists linear cryptanalysis better than DES, but for some kind of multiple linear attack (the idea was proposed in [26]), s^{5}DES could be less secure that DES. This requires further research.

A.3 Tentative Conclusion on s^{5}DES

We see that the S-boxes of s^{5}DES have not been chosen independently of each other, and this for a completely unknown reason. It is not implied either by any of the published design criteria on DES S-boxes, nor it is implied by the Davies-Murphy attacks (for this it is sufficient to select sets A and B independently for each S-box).

The authors of s^{5}DES do NOT claim that the S-boxes have been chosen independently of each other. At page 6 of [28] they give a Condition 4 (L-3) that gives different requirements for each S-box, which is motivated by avoiding iterative linear approximations that would hold for 4 rounds. Therefore, each of the S-boxes of s^{5}DES have been designed following a slightly different set of criteria. Yet, if we look at this Condition 4 (L-3) of [28], there is no apparent link with the strange properties we discovered, for example nothing suggests that the neighbour S-boxes 1 and 8 would be built with exactly the same sets as it is shown in Table 8.

The observed properties are disturbing, cannot happen by chance, are not explained by the authors, and do not appear to result from the set of design criteria given in the paper [28]. Unfortunately the authors did not publish the source code that allows to obtain these S-boxes. The observed properties could be a consequence of sloppy design, introducing unnecessary similarities between the S-boxes. It might also result from the fact that in computer simulations the authors did only find about two or three 8 S-boxes satisfying all the criteria, and the authors somewhat derived 8 S-boxes from these S-boxes.

It is an open problem to see of these properties allow to break s^{5}DES. Yet they substantially decrease the credibility of s^{5}DES as a DES replacement. For example, we have seen that they lead to bi-linear attacks on reduced versions of s^{5}DES that are better than for DES, see [12].