Iterative Characteristics of DES and s^2-DES

Lars Ramkilde Knudsen

Aarhus University
Computer Science Department
Ny Munkegade
DK-8000 Aarhus C.

Abstract. In this paper we show that we are close at the proof that the type of characteristics used by Biham and Shamir in their differential attack on DES [3] are in fact the best characteristics we can find for DES. Furthermore we show that the criteria for the construction of DES-like S-boxes proposed by Kim [6] are insufficient to assure resistance against differential attacks. We show several good iterative characteristics for these S-boxes to be used in differential attacks. Finally we examine the probabilities of the two characteristics used by Biham and Shamir in [3]. We found that for some keys we do not get the probabilities used in the attack. We suggest the use of 5 characteristics instead of two in the attack on DES.

1 Introduction

In 1990 Eli Biham and Adi Shamir introduced *differential cryptanalysis*, a chosen plaintext attack on block ciphers that are based on iterating a cryptographically weak function r times (e.g. the 16-round Data Encryption Standard (DES)). The method proved strong enough to break several cryptosystems, Lucifer, GDES, Feal-4, Feal-8, Snefru a.o. and DES with a reduced number of rounds, i.e. less than 16 rounds [1, 2, 4].
In december 1991 Biham and Shamir published an improved differential attack that is capable of breaking the full 16-round DES [3]. The attack needs 2^{47} chosen plaintexts. The heart in differential attacks is the finding and the use of characteristics. In their attack Biham and Shamir use 2-round iterative characteristics. These characteristics are believed to be the best characteristics for an attack on 16-round DES, but so far no proof of this has been published in the open literature. We are close to the conclusion that this is in fact the case.
After the breaking of the full 16-round DES the question is if we can redesign DES to withstand this kind of attack. There has been a huge research on DES, since its publication in the mid 70's. Some of this work has been concentrating on the design of secure S-boxes. In [6] Kwangjo Kim provides a way of constructing DES-like S-boxes based on boolean functions satisfying the SAC (Strict Avalanche Criterion). Kim lists 5 criteria for the constructions, including "Resistance against differential attacks". Furthermore 8 concrete examples of these S-boxes, the s^2-DES S-boxes, are listed. The cryptosystem s^2-DES is

E.F. Brickell (Ed.): Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 497-511, 1993.

obtained by replacing all the 8 DES S-boxes by the 8 s^2-DES S-boxes, keeping everything else as in DES. It is suggested that s^2-DES withstands differential attacks better than DES. We show that this is indeed not the case. The conlusion is that Kims 5 criteria for the construction of DES-like S-boxes are insufficient to assure resistance against differential attacks.
In [1] Biham and Shamir observed that the probability of the two characteristics used in [3] will split into two depending on the values of certain keybits. In [3] this phenomena is not considered, and the estimates of complexity are calculated using average probabilities. This means that for some keys we will need more chosen plaintexts as stated in [3]. We think that exact probabilities should be used in the estimates of complexity and suggest the use of 3 additional characteristics to lower the need for chosen plaintexts for a successful attack.
In section 2 we show different models of iterative characteristics for DES and s^2-DES to be used in differential attacks. In section 3 and 4 we show concrete examples of these characteristics for DES and s^2-DES, the probabilities all being average values. In section 5 we consider the exact probabilities of iterative characteristics for DES.

2 Iterative characteristics for DES and s^2-DES

We expect the reader to be familiar with the general concepts of differential cryptanalysis and refer to [1, 8] for further details. In DES and s^2-DES equal inputs (to the F-function) always lead to equal outputs. This means that an inputxor equal to zero leads to an outputxor equal to zero with probability 1. This is the best combination of input/outputxors. In finding the best characteristics we therefore try to maximize the number of these *zero-rounds*. In the following we will show different models of iterative characteristics for DES and s^2-DES. In section 3 and 4 we will justify the usability of the models by showing concrete examples of these in DES and s^2-DES.

2.1 2-round iterative characteristics

Two consecutive zero-rounds in a characteristic of DES-like cryptosystems lead to equal inputs and outputs of all rounds. We get equal plaintexts resulting in equal ciphertexts, a trivial fact. The maximum occurrences of zero-rounds therefore is every second round. This situation evolves by using the 2-round characteristic as in [1]. In the following we will use this notation:

$$\begin{array}{cc} & (\Phi, 0) \\ 0 & \leftarrow \quad 0 \quad \text{prob. 1} \\ 0 & \leftarrow \quad \Phi \quad \text{prob. something} \\ & (0, \Phi) \end{array}$$

for the 2-round iterative characteristic.

2.2 3-round characteristics

In [7] Knudsen found that the best differential attack on LOKI89 [9] was based on a 3-round *fixpoint* characteristic. A fixpoint is an inputxor that can result in itself as an outputxor. Instead of looking for fixpoints we should in general look for, what we call, **twinxors**.

Definition 1 *Twinxors, Γ and Φ, are xors for which $\Phi \leftarrow \Gamma$ and $\Gamma \leftarrow \Phi$, both combinations with a positive probability.*

[1] With twinxors we can build the following 3-round characteristic :

$$
\begin{array}{rcll}
 & (\Gamma, 0) & & \\
0 & \leftarrow & 0 & \text{prob. 1} \\
\Phi & \leftarrow & \Gamma & \text{some prob.} \\
\Gamma & \leftarrow & \Phi & \text{some prob.} \\
 & (0, \Phi) & &
\end{array}
$$

The characteristic is in fact only "half" an iterative characteristic. Concatenated with the characteristic with rounds no. 2 and 3 interchanged we obtain:

$$
\begin{array}{rcll}
 & (\Gamma, 0) & & \\
0 & \leftarrow & 0 & \text{prob. 1} \\
\Phi & \leftarrow & \Gamma & \text{some prob.} \\
\Gamma & \leftarrow & \Phi & \text{some prob.} \\
0 & \leftarrow & 0 & \text{prob. 1} \\
\Gamma & \leftarrow & \Phi & \text{some prob.} \\
\Phi & \leftarrow & \Gamma & \text{some prob.} \\
 & (0, \Gamma) & &
\end{array}
$$

In that way we get a 6-round iterative characteristic. Still we choose to call the 3-round characteristic an iterative characteristic.

2.3 4-round characteristic

As for the 3-round characteristic we look for a 4-round characteristic, which extended to 8 rounds becomes an iterative characteristic. It must have the following form:

$$
\begin{array}{rcll}
 & (\Gamma, 0) & & \\
0 & \leftarrow & 0 & \text{prob. 1} \\
\Phi & \leftarrow & \Gamma & \text{some prob.} \\
\Gamma \oplus \Psi & \leftarrow & \Phi & \text{some prob.} \\
\Phi & \leftarrow & \Psi & \text{some prob.} \\
 & (0, \Psi) & &
\end{array}
$$

It means that we have to find two inputxors Ψ and Γ both resulting in Φ and Φ resulting in the (xor-)difference between Ψ and Γ.

[1] The best twinxors for LOKI89 is obtained with $\Phi = \Gamma = 00400000_x$, i.e. fixpoints.

2.4 Longer characteristics

We can of course continue the search for n-round characteristics, $n > 4$. For every time we go one round further, we compare the characteristic we are now looking for with the best characteristic, we have found so far. We can easily find the best non-trivial input/outputxor combination in the *pairs xor distribution table.* From this probability we calculate the maximum number of different inputs to S-boxes we can have for the characteristic to be better than the one we have found.
By looking closer at the possible xor-combinations and the overall architecture of the cryptosystem we can calculate the minimum number of different inputs to S-boxes we must have for the particular characteristic. Using this minimum and the above maximum we find the possible combinations of input- and outputxors in the characteristic and compare the probability with the other characteristics we have found.
Of course characteristics do not have to contain a zero-round. Before making any conclusions about the best possible characteristic, we must check whether good characteristics of this kind exist.

3 DES

3.1 Properties

The following 5 properties of the DES S-boxes are well known.

1. No S-box is a linear of affine function.
2. Changing one bit in the input to an S-box results in changing at least two output bits.
3. The S-boxes were chosen to minimize the difference between the number of 1's and 0's when any single bit is held constant.
4. $S(\mathbf{x})$ and $S(\mathbf{x} \oplus (001100))$ differ in at least two bits.
5. $S(\mathbf{x}) \neq S(\mathbf{x} \oplus (11ef00))$ for any e and f.

A DES S-box consists of 4 rows of 4-bit bijective functions. The input to an S-box is 6 bits. The left outermost bit and the right outermost bit (the row bits) determine through which function the four remaining bits (the column bits) are to be evaluated. This fact gives us a 6'th property of the DES S-boxes important for differential cryptanalysis.

6. $S(\mathbf{x}) \neq S(\mathbf{x} \oplus (0abcd0))$ for any a, b, c and d, $abcd \neq 0000$.

The inner input bits for an S-box are input bits that do not affect the inputs of other S-boxes. We have two inner input bits for every S-box. Because of the P-permutation we have the following property also important for differential cryptanalysis.

- The inner input bits for an S-box, Si, come from S-boxes, whose inner input bits cannot come from Si.

Example: The inner input bits for $S1$ come from $S2$ and $S5$, whose inner input bits come from $S3$ and $S7$ respectively $S2$ and $S6$.

3.2 2-round iterative characteristics

As stated in [1, 3] the best characteristics for a differential attack on 16-round DES is based on a 2-round iterative characteristic. The following theorem was already proven in [5]. We give the proof in a different manner.

Theorem 1 *If two inputs to the F-function result in equal outputs, the inputs must differ in at least 3 neighbouring S-boxes.*

Proof: If the inputs differ only in the input to one S-box the expanded inputxor must have the following form: $00ab00$ (binary), where $ab \neq 00$. Because of properties 2 and 4 above, these inputs cannot give equal outputs. This also tells us that the inputs must differ in neighbouring S-boxes. If the inputs differ in only two neighbouring S-boxes, Si and $S(i+1)$, the two inputxors must have the following forms: $Si : 00abcd$ and $S(i+1) : cdef00$. Now

$cd \neq 00$, because of properties 2 and 4.
$cd \neq 01$, because of property 6 for $S(i+1)$.
$cd \neq 10$, because of property 6 for $S(i)$.
$cd \neq 11$, because of property 5 for $S(i+1)$.

□

We have several 2-round iterative characteristics for DES, where the inputs differ in three neighbouring S-boxes. By consulting the *pairs XOR distribution table* for the 8 S-boxes we easily find the best possibilities. The two best of these are used in [3] to break the full 16-round DES using 2^{47} chosen plaintexts. The probability of the two characteristics is $\frac{1}{234}$ for the two rounds.

3.3 3-round iterative characteristics

The highest probability for a non trivial input/outputxor combination in DES is $\frac{1}{4}$. Because $(\frac{1}{4})^x \geq (\frac{1}{234})^{1.5} \Rightarrow x < 6$, there can be different inputs to at most 5 S-boxes for the two nonzero round together. Because of the P-permutation in DES, see Section 3.1., Φ and Γ must differ in the inputs to at least two S-boxes each. Property 2 of the S-boxes implies that at least one additional S-box have different inputs, making Φ and Γ together differ in the inputs to at least 5 S-boxes. The proof is given in the Appendix. For DES the best twinxors, which differ in the inputs to 5 S-boxes are: $\Phi = 31200000_x$ and $\Gamma = 00004200_x$. The probability for the 3-round iterative characteristic is $2^{-18.42}$. This probability is very low and there is in fact twinxors, which together differ in the inputs to 6 S-boxes with a higher probability, $\Phi = 03140000_x$ and $\Gamma = 00004014_x$. The probability for the 3-round iterative characteristic is $2^{-18.1}$. Both characteristics have a probability too low to be used in a successful differential attack.

3.4 4-round iterative characteristics

There can be different inputs to at most 7 S-boxes, because $(\frac{1}{4})^x \geq (\frac{1}{234})^2 \Rightarrow x < 8$, however there is no 4-round iterative characteristics for DES with a probability higher than for best 2-round iterative characteristic concatenated with itself. The proof is tedious and is given in the Appendix.

3.5 Longer characteristics

We believe that it can be proven that we cannot find n-round iterative characteristics, $n > 4$, with probabilities higher than for the best 2-round iterative characteristic concatenated with itself $\frac{n}{2}$ times. To obtain this for a 5-round iterative characteristic there can be different inputs to at most 9 S-boxes, as $(\frac{1}{4})^x \geq (\frac{1}{234})^{2.5} \Rightarrow x < 10$. It seems impossible that we can find such a characteristic different in the inputs to 9 S-boxes and all combinations with a probability close to the highest possible of $\frac{1}{4}$. If we go one round further to a 6-round iterative characteristic the doubt will be even bigger. Before making any conclusions for the best differential attack on DES using characteristics, we must also check that no non iterative characteristics exist, as stated in Section 2.4. These proofs are a topic for further research.

4 s²-DES

4.1 Properties

Kims s²-DES S-boxes do not have the DES properties 2, 4 and 5. They do have a property though that is part of property 2 for the DES S-boxes.

4a. $S(\mathbf{x}) \neq S(\mathbf{x} \oplus (a0000b))$ for $ab \neq 00$.

As the s²-DES S-boxes are build as 4 rows of 4-bit bijective functions, they have property 6 like the DES S-boxes.

4.2 2-round characteristics

Because of property 6 there is no 2-round iterative characteristic for Kims s²-DES S-boxes where the inputs differ only in one S-box, however the lack of property 5 enables us to build a 2-round iterative characteristic where the inputs differ in two neighbouring S-boxes. We have

$$0_x \leftarrow 00000580_x \text{ with prob. } \frac{8*10}{64*64} \simeq \frac{1}{51}$$

Extending this characteristic to 15-rounds yields a probability of $2^{-39.7}$. Using the original attack by Biham and Shamir [1] we will need about 2^{42} chosen plaintexts for a successful differential attack. To do a similar attack as by Biham and Shamir in [3] we construct a 13-round characteristic with probability 2^{-34}. The megastructures used in the attack will consist of 2^9 plaintexts and we will need a total of about 2^{35} chosen plaintexts for the attack. This being said without having studied the attack in details. The above characteristic is not the only 2-round iterative characteristic for s²-DES that is better than the best 2-round iterative characteristics for DES. We have several others, the two secondbest characteristics both with probability $\frac{6*10}{64*64} \simeq \frac{1}{68}$ are based on the combinations: $0_x \leftarrow 07e00000_x$ and $0_x \leftarrow 5c000000_x$.

4.3 3-round characteristics

The best non-trivial input/outputxor combination in s^2-DES has probability $\frac{1}{4}$. Therefore there can be at most 4 S-boxes with different inputs in the 3 rounds all together, as $(\frac{1}{4})^x \geq (\frac{1}{51})^{1.5} \Rightarrow x < 5$. As with DES, because of the P-permutation, Φ and Γ must differ in the inputs to at least two S-boxes each. Unlike for DES it is possible for two inputs different in only 1 bit to result in two outputs different in 1 bit. Therefore we can build a 3-round characteristic with $\Phi = 04040000_x$ and $\Gamma = 00404000_x$. The probability for the characteristic is $\frac{8*6*4*10}{64^4} \simeq 2^{-13.5}$. This is the best 3-round characteristic we have found for s^2-DES. We can build a 13-round characteristic to be used as in the attack in [3]. The probability for the characteristic is $2^{-52.5}$. However we can use the combinations from the 3-round characteristic to build 6-round "half"-iterative characteristics, which are better, as we will show later.

4.4 4-round characteristics

There can be at most 5 S-boxes with different inputs, because $(\frac{1}{4})^x \geq (\frac{1}{51})^2 \Rightarrow x < 6$, and again we exploit the fact that s^2-DES S-boxes do not have property 2. We construct a 4-round characteristic based on the following combinations:

$$
\begin{aligned}
&00000002_x \leftarrow 0000006e_x \text{ with prob. } \tfrac{8*10}{64*64}\\
&00080000_x \leftarrow 00020000_x \text{ with prob. } \tfrac{8}{64}\\
&00000002_x \leftarrow 0000002e_x \text{ with prob. } \tfrac{6*10}{64*64}
\end{aligned}
$$

We have $P(00000002_x) = 00020000_x$ and $P(00080000)_x = 00000040_x = 0000006e_x \oplus 0000004e_x$. The total probability for the 4-round characteristic is $2^{-14.77}$. Extended to 13 rounds we obtain a probability of $2^{-44.3}$.

4.5 Longer characteristics

A 5-round iterative characteristic will have to differ in the inputs to at least 6 S-boxes. However we can find 6-round iterative characteristics also different in the inputs to only 6 S-boxes as indicated above. The P-permutation makes it impossible to have $\Phi \rightarrow \Gamma$ and $\Gamma \rightarrow \Phi$, where both Φ and Γ differ only in the inputs to one S-box. However it is possible to have Φ, Γ, Ψ and Ω, all four different only in the input to one S-box and such that $\Phi \rightarrow \Gamma$, $\Gamma \rightarrow \Psi$, $\Psi \rightarrow \Omega$ and $\Omega \rightarrow \Phi$. We use this observation to construct a 6-round characteristic:

$$
\begin{array}{rcll}
 & (\Phi\ ,\ 0) & & \\
0 & \leftarrow & 0 & \text{prob. 1} \\
\Gamma & \leftarrow & \Phi & \text{some prob..} \\
\Psi & \leftarrow & \Gamma & \text{some prob.} \\
\Gamma \oplus \Omega & \leftarrow & \Phi \oplus \Psi & \text{some prob.} \\
\Phi & \leftarrow & \Omega & \text{some prob.} \\
\Omega & \leftarrow & \Psi & \text{some prob.} \\
 & (0, \Psi) & &
\end{array}
$$

With $\Phi = 04000000_x$, $\Gamma = 00004000_x$, $\Psi = 00040000_x$ and $\Omega = 00400000_x$ we get a total probability for the 6-round characteristic of $\frac{8*10*8*6*4*6}{64^6} \simeq 2^{-19.5}$. Extended to 13 rounds the probability becomes 2^{-39}. Starting with (Γ , 0) we get a similar 6-round characteristic with probability $2^{-19.5}$. Starting with (Ψ , 0) or (Ω , 0) yields a 6-round characteristic with probability $2^{-19.8}$. These 6-round characteristics differ in the inputs to 6 S-boxes, that is, different inputs to one S-box per round in average.
If we try to construct n-round iterative characteristics, $n > 6$, we find that we will get more than one S-box difference per round in average.

4.6 Conclusion on Kims s²-DES S-boxes.

The above illustrates that we have to ensure that DES-like S-boxes have the six properties listed in section 3.1. The fact that for s²-DES two inputs different only in the inputs to 2 neighbouring S-boxes can result in equal outputs enables us to build 2-round iterative characteristic more than 4 times as good as the best 2-round characteristic for DES. The fact that two S-box inputs different in only one bit can result in outputs different in one bit enables us to construct a 4-round and a 6-round iterative characteristic both better for differential attacks on s²-DES than the 2-round characteristic for DES. Furthermore we must check that there is no 2-round iterative characteristic where only 3 neighbouring S-boxes differ in the inputs with a too high probability. For the s²-DES S-boxes the best such characteristic is based on the combination $dc000002_x \leftarrow 0_x$. It has probability $\frac{10*10*14}{64^3} \simeq \frac{1}{187}$. This is higher than the best 2-round characteristic for DES and illustrates that we should also consider this in the construction of DES-like S-boxes.

5 Probabilities of iterative characteristics

5.1 DES

As stated earlier the best characteristics for a differential attack on DES are based on 2-round iterative characteristics. The two best of these have the following inputxors in the second round: $\Phi = 19600000_x$ and $\Gamma = 1b600000_x$. Both xors lead to equal outputs with probability $\frac{1}{234}$. However this probability is only an "average" probability. As stated in [1, section 6.5], if the sixth keybit used in S2 is different from the second keybit used in S3 the probability for Φ increases to $\frac{1}{146}$ and the probability for Γ decreases to $\frac{1}{585}$. If the two keybits are equal the probabilities will be interchanged. We call these keybits, **critical** keybits for Φ and Γ. In their attack on DES [3] Biham and Shamir use these two characteristics to build 13-round characteristics, where six rounds have inputxor Φ or Γ. The probability is claimed to be $(\frac{1}{234})^6 \simeq 2^{-47.22}$. But depending on the values of the six pairs of critical keybits the probability for Φ will vary from $(\frac{1}{146})^6 \simeq 2^{-43.16}$ to $(\frac{1}{585})^6 \simeq 2^{-55.16}$ and the other way around for Γ. Using both characteristics as in [3] we are ensured to get one characteristic with a probability of

Table 1. The probabilities for the best 13-round characteristic obtained by using the 2 characteristics Φ and Γ.

#Keys ($\log_2$)	Probability ($\log_2$)
51.00	-43.16
53.58	-45.16
54.88	-47.16
54.30	-49.16

at least $(\frac{1}{146*585})^3 \simeq 2^{-49.16}$. Table 1 shows the probabilities and for how many keys they will occur.

It means that for one out of 32 keys, we will get a 13-round characteristic with the highest probability and for about one out of three keys we will get the lowest probability. We found that for other 2-round iterative characteristics the probability splits into more than one depending on equality/inequality of certain critical keybits. It turns out that we can find 2-round iterative characteristics for which the best of these probabilities is better than for the lowest for Φ and Γ. For the 2-round characteristic (with inputxor) 00196000_x we have only one probability. It means that regardless of the key values this characteristic will have a probability of $\frac{1}{256}$. Table 2 shows the probabilities for Φ and Γ and for the 2-round iterative characteristics, whose best probability is higher than $\frac{1}{256}$.

Table 2. Exact probabilities for 11 characteristics.

Characteristic	Probabilities (1/n)	Average Prob.(1/n)
19600000_x	146, 585	234
$1b600000_x$	585, 146	234
00196000_x	256	256
$000003d4_x$	210, 390	273
$4000001d_x$	205, 1024	341
19400000_x (+)	0, 195	390
$1b400000_x$ (+)	195, 0	390
40000019_x ($)	248, 390, 744, 1170	455
$4000001f_x$ ($)	248, 390, 744, 1170	455
$1d600000_x$ (+)	205, 512, 819, 2048	468
$1f600000_x$ (+)	205, 512, 819, 2048	468

It seems unlikely that we can find n-round characteristic, $n > 2$, for which the exact probabilities will be higher than for the above mentioned 2-round iterative characteristics. The subkeys in DES are dependent, therefore some keybits might be critical for one characteristic in one round and for another characteristic in another round. For example by using characteristic 19400000_x we have the two probabilities $\frac{1}{195}$ and 0. But this division of the probability depends on the values of the same critical keybits as for Φ and Γ and we would get a probability of

$\frac{1}{146}$ for either Φ or Γ. The characteristics marked with (+) in Table 2 depends on the values of the same critical keybits as for Φ and Γ. Doing an attack on DES similar to the one given in [3], this time using the first 5 of the above characteristics will give us better probabilities for a 13-round characteristic. Table 3 shows the best probabilities and for how many keys these will occur. The above

Table 3. The probabilities for the best 13-round characteristic obtained by using 5 characteristics.

#Keys ($\log_2$)	Probability ($\log_2$)
51.00	-43.16
53.58	-45.16
49.64	-46.07
49.64	-46.29
54.88	-47.16
50.90	-47.18
54.10	-48.00

probabilities are calculated by carefully examining the critical keybits for the 5 characteristics in the rounds no. 3, 5, 7, 9, 11 and 13, i.e. the rounds where we will expect the above inputxors to be. By using the two characteristics in Table 2 marked with (\$) in addition would yield slightly better probabilities. However the best probability we would get by using these characteristics is $(\frac{1}{248})^6 \simeq 2^{-47.7}$ and it would occur only for a small number of keys.
As indicated in Table 3 we are ensured to get a characteristic with a probability of at least 2^{-48}. However the megastructures of plaintexts and analysis will become more complex. Whether using 5 characteristics instead of two will dramatically increase the complexity of the analysis remains an open question.

5.2 s^2-DES

The best characteristic for an attack on s^2-DES is, as we saw earlier, a 2-round iterative characteristic with (average) probability of $\frac{1}{51}$. The exact probabilities of this characteristic is $\frac{1}{57}$ and $\frac{1}{46}$ making the probability for a 13-round characteristic vary from 2^{-35} to 2^{-33}. It means that even in the worst case the characteristic is far better than the best characteristics for DES.

A Appendix

In this section we give the proofs of the claims given in Sect. 3.3 and 3.4.
Notation: Let Γ be an xor-sum of two inputs Y, Y^* to the F-function. Then $\Delta S(\Gamma)$ is the set of S-boxes, whose inputs are different after the E-expansion of Y and Y^*. Furthermore $\#\Delta S(\Gamma)$ denotes the number of S-boxes in $\Delta S(\Gamma)$. Example: Let $\Gamma = 0f000000_x$ (hex), then $\Delta S(\Gamma) = \{S1, S2, S3\}$ and $\#\Delta S(\Gamma) = 3$.

Note that xor-addition is linear in both the E-expansion and the P-permutation of DES. In the proofs below the following Tables and lemmata are used. Table 4 shows for each of the 8 S-boxes, which S-boxes are affected by the output of the particular S-box. Numbers with a subscript indicate that the particular bit affects one S-box directly and another S-box via the E-expansion. Example: If the output of $S1$ is 6_x (hex), then S-boxes 5 and 6 are directly affected and S-box 4 is affected after the E-expansion in the following round. Table 5 shows the *reverse* of Table 4, i.e. for every S-box it is shown which S-boxes from the preceding round affect the input.

Table 4. Where the bits from an S-box goes to

S1 → 3 $_2$	5 $_4$	6	8
S2 → 4 $_3$	7 $_8$	1	5
S3 → 6 $_7$	4 $_5$	8	2
S4 → 7	5 $_6$	3	1 $_8$
S5 → 2 $_3$	4	7 $_6$	1
S6 → 1 $_2$	8 $_7$	3	5
S7 → 8 $_1$	3 $_4$	6	2
S8 → 2 $_1$	7	4	6 $_5$

Table 5. Where the bits for an S-box come from

S1	S2	S3	S4	S5	S6	S7	S8
4 2 5 6	8 3 7 5	1 4 6 7	2 5 8 3	1 2 6 4	8 7 1 3	5 4 8 2	6 3 1 7

The next five lemmata follow from Table 4 and 5.

Lemma 1 *The six bits that make the input for an S-box, Si, come from six distinct S-boxes and not from Si itself.*

Lemma 2 *The middle six input bits for two neighbouring S-boxes come from six distinct S-boxes.*

Lemma 3 *The middle ten input bits for three neighbouring S-boxes come from all 8 S-boxes. Six of the ten bits come from six distinct S-boxes and four bits come from the remaining two S-boxes.*

Lemma 4 *The middle two bits in the input of an S-box Si, the inner input bits, come from two S-boxes, whose inner input bits cannot come from Si.*

Lemma 5 *Let Φ and Γ be two input sums, where $\Phi \rightarrow \Gamma$. If $\#\Delta S(\Phi) = \#\Delta S(\Gamma) = 2$ then for at least one S-box of $\Delta S(\Gamma)$ the inputs differ in only one bit.*

Theorem 2 *For twinxors, Γ and Φ , i.e. $\Gamma \rightarrow \Phi$ and $\Phi \rightarrow \Gamma$, the inputs to at least 5 S-boxes are different. That is, $\#\Delta S(\Gamma) + \#\Delta S(\Phi) \geq 5$.*

Proof: 1. $\#\Delta S(\Gamma) = 1$. The inputs to $\Delta S(\Gamma)$ differ in the inner input bits, i.e. at most two bits. Because of properties 2 and 4 of the DES S-boxes $\#\Delta S(\Phi) \geq 2$. The inputs of $\Delta S(\Phi)$ differ in at most one bit each. Because of property 2 the outputs of Φ differ in at least four bits. Therefore $\Phi \not\rightarrow \Gamma$.
2. $\#\Delta S(\Gamma) = 2$. Because of the symmetry of the characteristic we have immediately $\#\Delta S(\Phi) \geq 2$. There are two cases to consider:

a. $\Delta S(\Gamma)$ are not neighbours. Because of properties 2 and 4 the outputs of both S-boxes in $\Delta S(\Gamma)$ will differ in at least two bits, making $\#\Delta S(\Phi) \geq 3$ according to Table 4.
b. $\Delta S(\Gamma)$ are neighbours. From Lemma 2 it follows that the outputs of $\Delta S(\Phi)$ differ in at most one bit each. Property 2 requires the inputs of $\Delta S(\Phi)$ to differ in at least two bits each. From Table 4 it follows that the only way two neighbouring S-boxes in Γ can make the inputs of $\Delta S(\Phi)$ differ in at least two bits each, is when $\#\Delta S(\Phi) = 3$. This is however not possible for all two neighbouring S-boxes. For example let $\Delta S(\Gamma) = \{S5, S6\}$, then it is possible to get $\Delta S(\Phi) = \{S1, S2, S3\}$ where for each S-box the inputs differ in two bits. But for $\Delta S(\Gamma) = \{S1, S2\}$ there will always be at least one S-box in $\Delta S(\Phi)$, whose inputs differ in only one bit.

3. $\#\Delta S(\Gamma) \geq 3$. Because of the symmetry of twinxors $\#\Delta S(\Phi) \geq 2$. □

We want to show that there is no 4-round iterative characteristic with a probability higher than the best 2-round iterative characteristic concatenated with itself. First we prove

Theorem 3 *For a 4-round iterative characteristic with input sums Γ, Φ and Ψ, see Section 2.2,*

$$\#\Delta S(\Gamma) + \#\Delta S(\Phi) + \#\Delta S(\Psi) \geq 7.$$

Furthermore, for at least one of the input sums, the inputs to three neighbouring S-boxes differ.

Proof: We are looking for input sums Γ, Φ and Ψ, such that $\Gamma \rightarrow \Phi$, $\Psi \rightarrow \Phi$ and $\Phi \rightarrow \Gamma \oplus \Psi$. Note that $\Delta S(\Gamma) \cap \Delta S(\Psi) \neq \emptyset$ and that if $\Delta S(\Gamma)$ are neighbours then so are $\Delta S(\Psi)$.
1. $\#\Delta S(\Gamma) = 1$. From the proof of Theorem 2 we have $\#\Delta S(\Phi) \geq 2$, and each of the inputs to those S-boxes differ in exactly one bit.

a. $\#\Delta S(\Phi) = 2$. The S-boxes in $\Delta S(\Phi)$ are not neighbours and the inputs differ in one inner input bit, therefore each of the outputs differ in at least two bits. From a close look at Table 4 it follows that if $\Delta S(\Gamma) = S7$ then it is possible to get $\#\Delta S(\Psi) = 3$, but then for one S-box $\in \Delta S(\Psi)$, not $S7$, the inputs differ in only one bit, an inner input bit. If $\Delta S(\Gamma) \neq S7$ then $\#\Delta S(\Psi) \geq 4$ and for at least one S-box, not $\Delta S(\Gamma)$, the inputs differ in only one bit. Therefore $\Psi \not\rightarrow \Phi$.

b. $\#\Delta S(\Phi) \geq 3$. The outputs for every S-box of $\Delta S(\Phi)$ differ in at least two bits. It follows easily from Table 4 that $\#\Delta S(\Gamma \oplus \Psi) \geq 4$. Since $\Delta S(\Gamma) \subseteq \Delta S(\Psi)$, $\#\Delta S(\Psi) \geq 4$.

2. $\#\Delta S(\Gamma) = 2$. By the symmetry of the characteristic $\#\Delta S(\Psi) \geq 2$ and therefore $\#\Delta S(\Phi) \leq 3$. There are two cases to consider:

a. $\Delta S(\Gamma)$ are not neighbours. Because of properties 2 and 4 $\#\Delta S(\Phi) \geq 3$ leaving only the possibility that $\#\Delta S(\Psi) = 2$ and $\#\Delta S(\Phi) = 3$. The S-boxes in $\Delta S(\Phi)$ must be neighbours. If not, let Si be an isolated S-box, different in the inputs in only inner bits. The outputs of Si differ in at least two bits, that must go to the inner bits of the two S-boxes in $\Delta S(\Gamma)$, since $\Delta S(\Gamma) = \Delta S(\Psi)$. But that is not possible according to Lemma 4.

b. $\Delta S(\Gamma)$ are neighbours.

i) $\#\Delta S(\Phi) = 1$. The outputs of $\Delta S(\Phi)$ differ in at least two bits. From Table 4 it follows easily that for at least one S-box $\in \Delta S(\Psi)/\Delta S(\Gamma)$ the inputs differ in only one bit and $\Psi \not\rightarrow \Phi$.

ii) $\#\Delta S(\Phi) = 2$. Assume that $\#\Delta S(\Psi) = 2$. If $\Delta S(\Gamma) = \Delta S(\Psi)$ then the outputs of $\Delta S(\Phi)$ can differ in at most one bit each, according to Lemma 2. But by Lemma 5, the inputs of at least one S-box in $\Delta S(\Phi)$ differ in only one bit, a contradiction by property 2. Therefore $\Delta S(\Gamma) \neq \Delta S(\Psi)$. Since $\Delta S(\Gamma) \cap \Delta S(\Psi) \neq \emptyset$ and $\Delta S(\Gamma)$ are neighbours we must have $\Delta S(\Gamma) = \{S(i-1), Si\}$ and $\Delta S(\Psi) = \{S(i), S(i+1)\}$ or vice versa. The outputs from $S(i-1)$ in Γ must be equal as must the outputs from $S(i+1)$ in Ψ. Therefore $\Gamma \oplus \Psi$ must have the following form (before the expansion):

$$S(i-1) \,||\, S(i) \,||\, S(i+1) = 0xyz \,||\, 1**1 \,||\, 0vw0 \;,$$

where '*' is any bit, $xyz \neq 000$ and $vw \neq 00$. From Table 5 it follows that $\Phi \not\rightarrow \Gamma \oplus \Psi$ for $\#\Delta S(\Phi) = 2$ and therefore $\#\Delta S(\Psi) \geq 3$.

iii) $\#\Delta S(\Phi) = 3$. Then $\#\Delta S(\Psi) = 2$. If $\Delta S(\Gamma) \neq \Delta S(\Psi)$ then the differences in the inputs to Φ is the effect of one S-box. For every S-box in $\Delta S(\Phi)$ the inputs differ in only one bit, therefore $\Phi \not\rightarrow \Gamma \oplus \Psi$. By similar reasoning we find that for both S-boxes in $\Delta S(\Gamma)$ the outputs have to differ. Furthermore $\Delta S(\Phi)$ are neighbours. Assume that they are not. Then the outputs of the isolated S-box differ in at least two bits and from Table 4 it follows that they affect at least 2 not neighbouring or 3 neighbouring S-boxes, a contradiction with $\Delta S(\Gamma) = \Delta S(\Psi)$.

3. $\#\Delta S(\Gamma) = 3$. Because of the symmetry in the characteristic we already covered the cases where $\Delta S(\Psi) < 3$. Therefore $\#\Delta S(\Gamma) = \#\Delta S(\Psi) = 3$ and $\#\Delta S(\Phi) = 1$. $\Delta S(\Gamma)$ must be neighbours. Furthermore $\Delta S(\Gamma) = \Delta S(\Psi)$ otherwise $\Phi \not\rightarrow \Gamma \oplus \Psi$. □

Theorem 4 *There are no 4-round iterative characteristics with a probability higher than* $(\frac{1}{234})^2$.

Proof: From the proof of Theorem 3 we find that to have a 4-round iterative characteristic, the inputs to seven S-boxes must be different in the three nonzero rounds. Furthermore for at least one round the inputs to three neighbouring S-boxes must be different. There are three cases to consider. Case A: By Lemma

	$\Delta S(\Gamma)$	$\Delta S(\Phi)$	$\Delta S(\Psi)$
Case A	2	2	3
Case B	2	3	2
Case C	3	1	3

5 we know that for at least one S-box in $\Delta S(\Phi)$ the inputs differ in only one bit. Furthermore for at least one of the three neighbouring S-boxes in $\Delta S(\Psi)$ the outputs must be equal, otherwise $\Gamma \not\rightarrow \Phi$. There are two cases to consider:

1. For both S-boxes in $\Delta S(\Phi)$ the inputs differ in only one bit. By property 2 the outputs differ in at least two bits each. For every three neighbouring S-boxes in Ψ we know the only two possible S-boxes of $\Delta S(\Phi)$ by Lemma 3 and Table 5. Example: If $\Delta S(\Psi) = \{S1, S2, S3\}$ then $\Delta S(\Phi) = \{S5, S6\}$. Furthermore the outputs of either $S1$ or $S3$ must be equal.
   We have eight triples of three neighbouring S-boxes in Ψ to examine and from Table 4 and 5 it follows that there are only three possible values for $\Delta S(\Psi)$ and $\Delta S(\Phi)$. From the *pairs xor distribution table* we find that the best combination for $\Psi \rightarrow \Phi$ has probability $\frac{8\times12\times10}{64^3}$. But then the probability for a 4-round iterative characteristic $\mathrm{P(4R)} \leq \frac{1}{4^4} \times \frac{8\times12\times10}{64^3} < (\frac{1}{234})^2$.
2. For one of the S-boxes in $\Delta S(\Phi)$ the inputs differ in one bit, for the other S-box the inputs differ in two bits. For every three neighbouring S-boxes of Ψ there are only two possibilities for the S-box in $\Delta S(\Phi)$, whose inputs differ in only one bit. From a closer look at Table 4 it follows that $\Delta S(\Phi)$ must be neighbours and there are only two possible values for $\Delta S(\Psi)$ and $\Delta S(\Phi)$. From the *pairs xor distribution table* we find that the best combination for $\Psi \rightarrow \Phi$ has probability $\frac{12\times10\times4}{64^3}$. But then the probability for the 4-round iterative characteristic $\mathrm{P(4R)} \leq \frac{1}{4^4} \times \frac{12\times10\times4}{64^3} < (\frac{1}{234})^2$.

Case B: The three S-boxes in $\Delta S(\Phi)$ are neighbours. From the proof of Theorem 3 we have $\Delta S(\Gamma) = \Delta S(\Psi)$. Then by Lemma 2 the outputs of each of the three neighbouring S-boxes in $\Delta S(\Phi)$ can differ in at most one bit, therefore the inputs must differ in at least two bits each by property 2. Then it follows from Table 5 that for each of the S-boxes in $\Delta S(\Gamma)$ the outputs must differ in two bits. For every triple of three neighbouring in $\Delta S(\Phi)$ there is only one possible way for the inputs to differ and only one possibility for $\Delta S(\Gamma)$. The best combination of $\Delta S(\Gamma)$ and $\Delta S(\Phi)$ gives a probability for the 4-round iterative characteristic $\mathrm{P(4R)} \leq \frac{12\times12\times16\times(8\times4)^2}{64^7} < (\frac{1}{234})^2$.
Case C: From Theorem 3 we have $\Delta S(\Gamma) = \Delta S(\Psi)$. The only possibility we have for a 4-round iterative characteristic of this kind is when $\Delta S(\Gamma) = \{S2, S3, S4\}$

and $\Delta S(\Phi) = \{S7\}$. The best combinations yields a probability for the 4-round iterative characteristic $P(4R) \leq \frac{1}{4^4} \times \frac{14 \times 8 \times 8}{64^3} < (\frac{1}{234})^2$. □

References

1. Eli Biham, Adi Shamir. *Differential Cryptanalysis of DES-like Cryptosystems.* Journal of Cryptology, Vol. 4 No. 1 1991.
2. Eli Biham, Adi Shamir. *Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer.* Extended abstract appears in Advances in Cryptology, proceedings of CRYPTO 91.
3. Eli Biham, Adi Shamir. *Differential Cryptanalysis of the full 16-round DES.* Technical Report # 708, Technion - Israel Institute of Technology.
4. Eli Biham, Adi Shamir. *Differential Cryptanalysis of Feal and N-Hash.* Extended abstract appears in Advances in Cryptology, proceedings of EuroCrypt 91.
5. Y. Desmedt, J-J. Quisquater, M. Davio. *Dependence of output on input in DES: Small avalanche characteristics.* Advances in Cryptology: Proceedings of CRYPTO 84. Springer Verlag, Lecture Notes 196.
6. Kwangjo Kim. *Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC.* To appear in the proceedings from ASIACRYPT'91, Lecture Notes, Springer Verlag.
7. Lars Ramkilde Knudsen. *Cryptanalysis of LOKI.* To appear in the proceedings from ASIACRYPT'91, Lecture Notes, Springer Verlag.
8. Xueija Lai, James L. Massey, Sean Murphy. *Markov Ciphers and Differential Cryptanalysis.* Advances in Cryptology - EUROCRYPT'91. Springer Verlag, Lecture Notes 547.
9. Lawrence Brown, Josef Pieprzyk, Jennifer Seberry. *LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications.* Advances in Cryptology - AUSCRYPT '90. Springer Verlag, Lecture Notes 453, pp. 229-236, 1990.