# Cryptanalysis of McGuffin

Vincent Rijmen* Bart Preneel**

Katholieke Universiteit Leuven
ESAT-COSIC
K. Mercierlaan 94, B-3001 Heverlee, Belgium

{bart.preneel,vincent.rijmen}@esat.kuleuven.ac.be

**Abstract.** This paper shows that the actual proposal for an unbalanced Feistel network by Schneier and Blaze is as vulnerable to differential cryptanalysis as the DES.

## 1 McGuffin

Schneier and Blaze introduce in [SB95] a new kind of block ciphers: the *Generalized Unbalanced Feistel Network*. Together with the general architecture they give a complete specification of an example. The basic idea is to split the input of each round into unequal parts. In the example, the 64-bit input is split into a 48-bit input of the F-function, and a 16-bit part that is exored with the output of the F-function. The F-function consists of the 8 S-boxes of the DES, but the two middle output bits of each S-box are neglected in order to obtain a 16-bit output.

## 2 Differential Characteristics

In [Ma94] Matsui demonstrated that one can find the best differential characteristics and linear relations for the DES with a clever search algorithm. This encouraged us to try the same for McGuffin. For the DES it is very important to depart from very good starting values in order to obtain the characteristics in relatively short time (a few hours). For McGuffin, we had no good guesses for the starting values and became the best characteristics for two to 32 rounds in about the same time. This indicates that McGuffin is very vulnerable for differential cryptanalysis. Table 1 gives the probabilities of the best differential characteristics of McGuffin. It turns out that the probability of the best $2n$-round characteristic of McGuffin is significantly larger than the probability of

* N.F.W.O. research assistant, sponsored by the National Fund for Scientific Research (Belgium).

** N.F.W.O. postdoctoral researcher, sponsored by the National Fund for Scientific Research (Belgium).

the best $n$-round characteristic of the DES. From this viewpoint 32 rounds of McGuffin is weaker than 16 rounds of the DES. Figure 1 shows the four-round iterative building block of the best differential characteristic for McGuffin. It has a probability of $\frac{1}{149}$, which should be compared with $\frac{1}{234}$ for the best two-round iterative building block for a DES-characteristic. Since every input bit enters three S-boxes before it is modified, these probabilities are key dependent. This implies that the attack can probably be improved.

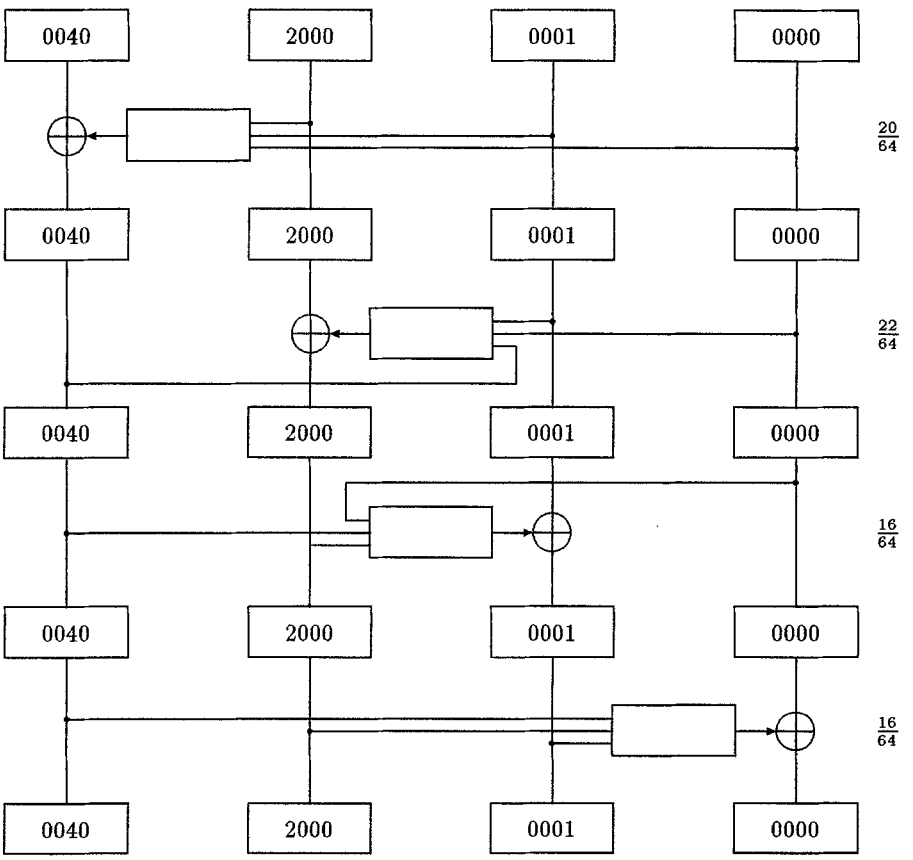


**Fig. 1.** The 4-round iterative building block of the best differential characteristic for McGuffin

Biham and Shamir [BS91] used a 13-round characteristic for their attack on the full DES. The first round is passed with probability one by enciphering large structures of plaintexts. The last two rounds are treated by the 2R-attack.

In our attack on McGuffin, we use a 27-round characteristic from the second to the $28^{\text{th}}$ round. Extended to the first round, this characteristic has an input

exor that is different from zero for S-box eight only. Since each S-box has only two output bits, only four different output exors are possible. Therefore we can pass the first round with probability one by enciphering structures of only eight plaintexts (in comparison to 8192 for the DES). Such a structure consists of the messages $P \oplus (v, 0000, 0000, 0000)$, $P \oplus \alpha \oplus (v, 0000, 0000, 0000)$, where $\alpha = (4040, 2000, 0001, 0000)$ and $v$ takes the values from the set {0000, 0001, 0002, 0003}.

We can apply a 4R-attack, because the diffusion of McGuffin is weaker than that of the DES. This attack gives the round key of the last round. Since the relation between master key and round keys is difficult to invert, we have to peel off the last round and repeat the attack on the reduced version of McGuffin.

**Table 1.** The probabilities of the best characteristics for McGuffin and the DES

| McGuffin | | DES | |
|---|---|---|---|
| $n$ | $\log_2(p)$ | $n$ | $\log_2(p)$ |
| 8 | -11.6 | 4 | -9.6 |
| 12 | -19.4 | 6 | -20.0 |
| 16 | -27.7 | 8 | -30.5 |
| 20 | -34.8 | 10 | -38.4 |
| 24 | -42.7 | 12 | -46.2 |
| 26 | -46.4 | 13 | -47.2 |
| 27 | -47.9 | | |
| 28 | -49.9 | 14 | -54.1 |
| 29 | -51.6 | | |
| 32 | -57.2 | 16 | -62.0 |

We checked whether the resistance of McGuffin against differential cryptanalysis could be improved by choosing two other output bits from the DES S-boxes. There are $12^8$ possibilities of choosing two different output bits from every S-box. We investigated only the twelve cases where one chooses in every S-box the same bits. It turns out that the current choice of output bits is neither the best nor the worst possible choice. Selecting the second and the first output bit from the S-boxes of the DES to be the first and second bit from the McGuffin S-boxes seems the best alternative: the probability for the best 27-round characteristic becomes $2^{-50.8}$.

The results we presented at the workshop contained a small error. After correction, we see that McGuffin is slightly more resistant against differential cryptanalysis than we first thought. The improvement is however not enough to make the cipher resistant against differential cryptanalysis.

## 3 Linear Relations

We searched for linear relations for up to 32 rounds of McGuffin. When searching for linear relations over several rounds, every 'forked branch' in the algorithm gives the cryptanalyst a choice. A linear relation can be viewed as the tracing of bits through the different rounds of the algorithm. Every 'forked branch' is then a 'crossroad' where the cryptanalyst can choose either way to follow the bits. As a consequence of the inbalance of McGuffin, there are 50 % more forked branches in each round than for the DES (48 'forked' bits instead of 32). On the other hand, the reduction of the output of the S-boxes reduces the number of possible linear approximations of each S-box with 80 % (only 3 possible output masks instead of 15). The effect of reducing the number of output bits on the expected value of the probability of the best linear relation is discussed in [Ny95].

**Table 2.** The probabilities of the best linear relations for McGuffin and the DES

| McGuffin | | DES | |
|---|---|---|---|
| $n$ | $\log_2(\lvert p-0.5\rvert)$ | $n$ | $\log_2(\lvert p-0.5\rvert)$ |
| 4 | -2.0 | 2 | -1.7 |
| 8 | -5.0 | 4 | -4.0 |
| 12 | -9.7 | 6 | -8.0 |
| 16 | -13.7 | 8 | -10.7 |
| 20 | -18.4 | 10 | -14.4 |
| 24 | -21.9 | 12 | -16.8 |
| 28 | -26.6 | 14 | -20.8 |
| 30 | -28.6 | 15 | -21.8 |
| 32 | -30.1 | 16 | -23.4 |

The probabilities of $2n$-round relations for McGuffin are lower than the probabilities of $n$-round DES-relations (cf. Table 2). This means that a straightforward application of Matsui's algorithm 2 would need $2^{2\times(28.6-20.8)} \times 2^{43} = 2^{58.6}$ plaintexts in order to find 12 bits of the round keys of the first and the last round. This is still faster than exhaustive key search. In order to determine the remaining part of these two round keys, other linear relations should be used.

The structure of the best 30-round linear relation is shown in Figure 2.

In Sect. 2 we showed that McGuffin could be strengthened against differential cryptanalysis by selecting other output bits from the DES S-boxes. Selecting the second and the first output bit produced the strongest cipher. We searched also for the linear relations of this adapted version. It has approximately the same resistance against linear cryptanalysis as the original version.

structure: - - E - - - A - B C D - - - A - B C D - - - A - B C D - - -

| | box (1-8) | $\alpha$ | $\beta$ | $2\lvert p-0.5\rvert$ |
|---|---|---|---|---|
| E | 4 | $3_X$ | $2_X$ | 0.1250 |
| A | 4 | $38_X$ | $1_X$ | 0.3125 |
| B | 2 | $26_X$ | $1_X$ | 0.1875 |
| C | 6 | $15_X$ | $1_X$ | 0.1875 |
| D | 4 | $2F_X$ | $1_X$ | 0.3125 |

**Fig. 2.** Structure of the optimal 30-round linear relation

## 4 Conclusion

McGuffin is not more resistant against a differential attack than the DES. Selecting other output bits from the DES S-boxes strenghtens the algorithm. Modifying a scheme with only existing attacks in mind however is not a good design principle. The extension of the linear attack to McGuffin is not as straightforward as the extension of the differential attack, but we feel that the increase in security against this attack is marginal. A more detailed study will probably reveal a linear-like attack with about the same probability for success as the linear attack on the DES (e.g., by using multiple linear relations [KR95]).

### Acknowledgements

We would like to thank David Wagner for helpful comments.

## References

[BS90] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, Vol. 4, No. 1, 1991, pp. 3–72.

[BS91] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," *Technion Technical Report # 708*, December 1991. (See also *Proceedings of Crypto'92, LNCS 740*, E.F. Brickell, Ed., Springer Verlag, pp. 487–496.)

[FI46-77] FIPS 46, *"Data Encryption Standard,"* National Bureau of Standards, 1977.

[KR95] B. Kaliski and M. Robshaw, "Linear cryptanalysis using multiple approximations and FEAL," *Fast Software Encryption*, these proceedings, pp. 249–264.

[Ma93a] M. Matsui, "Linear cryptanalysis method for DES cipher," *Advances in Cryptology, Proc. Eurocrypt'93, LNCS 765*, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 386–397.

[Ma93b] M. Matsui, "Cryptanalysis of DES cipher (I)," December 1993, preprint.

[Ma94] M. Matsui, "On correlation between the order of S-boxes and the strength of DES", *Advances in Cryptology, Proc. Eurocrypt'94, LNCS*, A. De Santis, Ed., Springer-Verlag, to appear.

[Ny95] K. Nyberg, "S-boxes and round functions with controllable linearity and differential uniformity," *Fast Software Encryption*, these proceedings, pp. 111–130.

[SB95] B. Schneier and M. Blaze, "The MacGuffin block cipher algorithm," *Fast Software Encryption*, these proceedings, pp. 97–110.