On Weaknesses of Non–surjective Round Functions

Vincent Rijmen* Bart Preneel†
Katholieke Universiteit Leuven, ESAT-COSIC
K. Mercierlaan 94, B-3001 Heverlee, Belgium

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

Extended Abstract

Abstract

We propose a new attack on Feistel ciphers with a non-surjective round function. CAST and LOKI91 are examples of such ciphers. We extend the attack towards ciphers that use a non–uniformly distributed round function and apply the attack to CAST.

1 Introduction

The Feistel structure is a very common structure for block ciphers, the most prominent example being the Data Encryption Standard [FI46]. Although DES has been a worldwide de facto standard since 1977, everybody agrees that it is reaching the end of its life time. The main reason is the size of the key, which is only 56 bits. The key size was already a topic of discussion in the seventies [DH77], and it was shown recently by M. Wiener that at present an exhaustive key search in 3.5 hours requires only 1 million US$ of equipment [W93]. Of more theoretical interest are recent cryptanalytic techniques such as differential [BS93] and linear [Ma93a, Ma94] cryptanalysis which provide techniques to recover the key faster than exhaustive search. Currently, they do not offer a threat for practical applications, but it can be expected that within the next five years

*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).

Appeared in *Designs, Codes and Cryptography 12(3)*, pp. 253–266, 1997.

practical attacks are developed. These problems can be overcome easily by using triple DES with two keys, at the cost of a reduced performance.

A second problem of the DES is the fact that it was designed taking into account 1977 hardware constraints. In spite of this, very fast software implementations have been reported (7 Mbit/s on a 80586/60MHz and 12 Mbit/s on a HP-715/80). However, algorithm designers hope to exploit in a more efficient way the present day computer architectures, and to achieve a better tradeoff between security and speed. In order to build on the experience gathered with the cryptanalysis of DES, most designers prefer to keep the Feistel structure. Examples of such proposals are FEAL [M91], LOKI91 [LOKI91], Blowfish [S94], and CAST [AT93, HT94, A94]. By introducing new structures for the round function, designers try to improve the performance and to reduce the vulnerability to differential and linear attacks. However, this might introduce new vulnerabilities, especially if the number of rounds is reduced in order to optimize the speed.

In this extended abstract we will concentrate on the weaknesses that are introduced by the use of non–surjective or, more general, non–uniform round functions. Several studies revealed that in general large S-boxes are more resistant against linear or differential cryptanalysis. It is even argued that one can choose random S-boxes and obtain a secure cipher. We show that this is not always true. In section 2 we describe the general principle of our attack. In section 3 we apply the attack to CAST and LOKI91. In section 4 we conclude by discussing some design principles.

2 General principle

We first explain our notation and then we present the attack and an extension.

2.1 Notation

Consider a Feistel cipher, consisting of n rounds (with n even). The plaintext input consists of two p–bit blocks L_0 and R_0, the key is denoted by K, the ciphertext by (L_n, R_n). Each round takes a $2p$–bit message input block (L_i, R_i) and a k–bit key input (K_i). The round output is given by:

$$\begin{aligned} R_i &= L_{i-1} \oplus F_i(K_i \oplus R_{i-1}) \\ L_i &= R_{i-1} \qquad\qquad\qquad i = 1, \ldots, n-1. \end{aligned}$$

For the last round (no swapping) this becomes:

$$\begin{aligned} L_n &= L_{n-1} \oplus F_n(K_n \oplus R_{n-1}) \\ R_n &= R_{n-1}\,. \end{aligned}$$

Appeared in *Designs, Codes and Cryptography 12(3)*, pp. 253–266, 1997.

Then the following relation holds:

$$\beta_n(L_0, R_0, K) = \bigoplus_{i=1}^{n/2} F_{2i}(K_{2i} \oplus R_{2i-1}) = R_0 \oplus L_n \quad n \geq 2, \text{ even.} \tag{1}$$

For unbalanced round functions F_{2i}, the sum β_n will be unbalanced if we assume that the round keys are independent. We expect that this also holds for most key schedulings. Since not all values of β_n have the same probability, an attacker gathers statistical information about the plaintext by looking at the ciphertext.

2.2 Basic attack

If we take the last round out of the sum, (1) becomes

$$\beta_{n-2}(L_0, R_0, K) = \bigoplus_{i=1}^{n/2-1} F_{2i}(K_{2i} \oplus R_{2i-1}) = R_0 \oplus L_n \oplus F_n(K_n \oplus R_n)\,. \tag{2}$$

Non–surjective round functions F_{2i} will result in a non–surjective β_{n-2} for small enough values of n. This is quantified in the following lemma.

Lemma 1 *Denote by f the fraction of p-bit vectors that are a possible output of the round function, and by f_{n-2} the fraction of possible values for β_{n-2}. If the round functions are behave as 'random functions':*

$$f_{n-2} = 1 - (1 - f_{n-4} \cdot f)^{2^p}\,. \tag{3}$$

Proof: We can write

$$\beta_{n-2} = \beta_{n-4} \oplus F_{n-2}\,.$$

A value X is a possible value for β_{n-2} iff

$$X = Y \oplus Z\,, \tag{4}$$

and Y, Z are possible values for β_{n-4} and F_{n-2} respectively. There are 2^p solutions for (4). A value for β_{n-2} is impossible iff for all solutions (X, Y) holds that X or Y is impossible. By application of the product rule we obtain

$$1 - f_{n-2} = (1 - f_{n-4} \cdot f)^{2^p}\,.$$

■

A non–surjective β_{n-2} makes the following attack possible. For all values K_n calculate the right hand side of (2) by use of the known plaintext R_0 and the ciphertext L_n. Check whether this is a possible value for β_{n-2}. Wrong key guesses will eventually produce a value that is outside the range of β_{n-2}. Since there are 2^k possible round keys K_n, we need on average $-k/\log_2(f_{n-2})$

Appeared in *Designs, Codes and Cryptography 12(3)*, pp. 253–266, 1997.

plaintext/ciphertext pairs to determine the right value of K_n. The work factor of the attack is $2^k/(1-f_{n-2})$.

For small values of k, one can search for several round keys at once. This way, f_{n-4} can be used instead of f_{n-2}.

2.3 Statistical attack

Equation (3) shows that for larger values of n, f_{n-2} goes very fast to 1. But β_{n-2} will not be uniformly distributed: all outputs are possible, but they don't occur with the same probability. For still larger values of n, β_{n-2} becomes close to a "random function", which should be a design goal. Our attack can be modified to deal with surjective but unbalanced β_n's. First calculate the relative probabilities for each possible value of β_{n-2}. Then calculate the right hand side of (2) for every value of K_n and for every known plaintext–ciphertext pair. It is now possible to calculate the a posteriori probability for the key candidates.

By Bayes' rule we can express the probability $\Pr(K_n|R_0,L_n)$ that K_n is the correct key, given R_0 and L_n:

$$\Pr(K_n|R_0,L_n) = \frac{\Pr(K_n)\Pr(R_0,L_n|K_n)}{\Pr(R_0,L_n)} = \frac{\Pr(K_n)\Pr(\beta_{n-2})}{\Pr(\beta_n)}\,.$$

Let us denote with $\Pr^i(K_n)$ the probability that K_n is the right key after the processing of the i–th known plaintext ($\Pr^0(K_n)=1/2^k$). We have

$$\Pr{}^i(K_n) = \frac{\Pr^{i-1}(K_n)\Pr(\beta^i_{n-2})}{\Pr(\beta^i_n)} = \frac{1}{2^k}\prod_{j=1}^{i}\frac{\Pr(\beta^j_{n-2})}{\Pr(\beta^j_n)}\,.$$

This expression can be evaluated for each key candidate and assigns to each round key a probability that can be used for a ranking of the most probable keys.

3 Application to CAST and LOKI91

3.1 CAST

The round function of CAST is constructed as follows: if $b_1b_2b_3b_4$ denotes the four byte input, the output is obtained by adding the output of the four S-boxes:

$$F(b_1b_2b_3b_4) = S_1[b_1]\oplus S_2[b_2]\oplus S_3[b_3]\oplus S_4[b_4]\,.$$

The four S_i are tables with eight input and 32 output bits. Since each S-box has only eight input bits, its output can only take 256 values in GF(2^{32}). If the four S-boxes are selected at random, the expected number of possible outputs is $(1-e^{-1})\times 2^{32}$, where e denotes the natural logarithm base. This value can also be computed from (3), since adding the outputs of the S-boxes corresponds to concatenating rounds. Table 1 gives the f-values for the combination of 1, 2, 3, and 4 S-boxes.

# S-boxes	f
1	5.96×10^{-8}
2	1.53×10^{-5}
3	3.90×10^{-3}
4	6.32×10^{-1}

Table 1: f-values for the combination of 1 to 4 S-boxes.

The CAST S-boxes are constructed from eight–bit bent functions that are the Walsh transforms of the concatenation of four six–bit bent functions. We constructed S-boxes following this design principle and obtained the same value for f.

We can summarize the CAST key scheduling in the following way: for each round first an "initial value" of two bytes is calculated from the master key. This calculation is simple for the first rounds, and more complicated for the last round. These two bytes are expanded in a non-linear way to the 32–bit round key. The entropy of each round key is therefore at most 16 bits. This enables us to search for three round keys at once.

We can apply the simple attack on six rounds of CAST. Equation (2) becomes:

$$\beta_4 = F_2 = R_0 \oplus L_6 \oplus F(K_4 \oplus R_6 \oplus F(K_5 \oplus L_6 \oplus F(K_6 \oplus R_6))) \oplus F(K_6 \oplus R_6). \quad (5)$$

R_0 is a part of the plaintext, L_6 and R_6 form the ciphertext. K_4, K_5, and K_6 are the round keys we are searching for. Note that by swapping plaintext and ciphertext, we can apply the same attack to find K_1, K_2, and K_3. The work factor of the attack is then 1.5×2^{48}. The number of required texts is only $-\log(2^{48})/\log(1 - e^{-1}) \approx 82$. Note that in [HT94] it is estimated that the required number of known plaintexts to break six rounds of CAST with a linear attack is at least 2^{18}.

Since the sum of two CAST round functions is surjective, the simple attack is not applicable to more than six rounds. The statistical attack needs a table of size 2^{32}. Although this is not infeasible, we are currently unable to actually implement this attack. We are developing an implementation for a mini-version of CAST that operates on a four byte input and with S-boxes that consist of 16 4–bit functions.

3.2 LOKI91

The round function of LOKI91 takes a 32–bit message input and exors this with a 32–bit round key. These 32 bits are expanded to 48 bits and split into four

Appeared in *Designs, Codes and Cryptography 12(3)*, pp. 253–266, 1997.

parts. Each part enters the 12×8–bit S-box. This produces the $8 \times 4 = 32$ output bits. Note that of the 48 input bits to the nonlinear part, 32 bits are pairwise equal. In [Kn94] L. R. Knudsen observed that this implies that the output can only take a fraction of $\frac{8}{13}$ of the possible values.

Each round key consists of 32 bits. The key scheduling of LOKI91 is such that $K_{2i} = K_{2i-1} <<< 12,\ i = 1, 2, \ldots, 8$, where $<<<$ denotes "left wise rotation." Therefore we can search for the round keys of two rounds at once, and apply the basic attack to five rounds of LOKI91. We did not implement the statistical attack for LOKI91. Since f is about the same for LOKI91 and CAST, we expect comparable results, except for the fact that we only can peel off two rounds.

4 Discussion

We have shown that the use of uniformly distributed round functions is probably a good design criterion for Feistel ciphers. Feistel ciphers that make use of non–surjective round functions should use a number n of rounds that is large enough to make β_{n-2} at least surjective. In order to counter the statistical attack, the sum should have a distribution which is close to uniform. We conjecture that the deviations of the different outputs squared approximates the number of required known plaintexts. Therefore this type of attack will become infeasible for a large number of rounds.

With respect to the key scheduling of CAST [A94], we can say that round keys with 16 bit entropy are inadequate. The computational cost for an attacker to peel off several rounds is too low. This makes CAST more vulnerable to our attack than LOKI91.

5 Acknowledgement

We wish to thank L.R. Knudsen for helpful comments on the application of the attack to LOKI91.

References

[AT93] C.M. Adams and S.E. Tavares, "Designing S-boxes for ciphers resistant to differential cryptanalysis," *Proc. of the 3rd symposium on State and Progress of Research in Cryptography*, W. Wolfowicz, Ed., Fondazione Ugo Bordoni, 1993, pp. 181–190.

[A94] C.M. Adams, "Simple and effective key scheduling for symmetric ciphers," *Proc. of SAC'94, Workshop on Selected Areas in Cryptography.*

[BS93] E. Biham and A. Shamir, *"Differential Cryptanalysis of the Data Encryption Standard,"* Springer-Verlag, 1993.

[DH77] W. Diffie and M. Hellman, "Exhaustive cryptanalysis of the NBS data encryption standard," *Computer*, pp. 74–78, 1977.

[DM95] D. Davies and S. Murphy, "Pairs and triples of DES S-boxes," *Journal of Cryptology*, Vol. 8, No. 1, 1995, pp. 1–26.

[FI46] *"Data Encryption Standard,"* Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[HT94] H.M. Heys and S.E. Tavares, "On the security of the CAST encryption algorithm," *Canadian Conference on Electrical and Computer Engineering*, Sept. 1994, Halifax, Canada.

[Kn94] L.R. Knudsen, "Block ciphers – analysis, design and applications," *PhD. Thesis, DAIMI PB–485*, Aarhus University, 1994.

[LOKI91] L. Brown, M. Kwan, J. Pieprzyk and J. Seberry, " Improving resistance against differential cryptanalysis and the redesign of LOKI," *Advances in Cryptology, Proc. AsiaCrypt'91, LNCS 453*, H. Imai, R. L. Rivest and T. Matsumoto, Eds., Springer-Verlag, 1993, pp. 36–50.

[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.

[Ma94] M. Matsui, "The first experimental cryptanalysis of the Data Encryption Standard," *Advances in Cryptology, Proc. Crypto'94, LNCS 839*, Y. Desmedt, Ed., Springer-Verlag, 1994, pp. 1–11.

[M91] S. Miyaguchi, "The Feal cipher family," *Advances in Cryptology, Proc. Crypto'90, LNCS 537*, S. Vanstone, Ed., Springer-Verlag, 1991, pp. 627–638.

[S94] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," *Fast Software Encryption, LNCS 809*, R. Anderson, Ed., Springer-Verlag, 1994, pp. 191–204.

[W93] Wiener, M., 1993, "Efficient DES key search," presentation at Rump Session of Crypto (August, 1993), Santa Barbara, CA. Available as TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994.

Appeared in *Designs, Codes and Cryptography 12(3)*, pp. 253–266, 1997.