On the F-function of FEAL

Walter Fumy, Siemens AG
Systems Engineering Development, E STE 36
D-8520 Erlangen, West Germany

Abstract

The cryptographic strength of a Feistel Cipher depends strongly on the properties of its F-function. Certain characteristics of the F-function of the Fast Data Encipherment Algorithm (FEAL) are investigated and compared to characteristics of the F-function of the Data Encryption Standard (DES). The effects of several straight-forward modifications of FEAL's F-function are discussed.

Introduction

A (cryptographic) function is called *complete*, if each of its output bits depends on every input bit [5]. A block cipher which is not complete, may be vulnerable to a known plaintext attack [1]. As the example of the *Data Encryption Standard* (DES, [7]) shows, the F-function of a Feistel Cipher needs not to be complete in order to ensure completeness of the block cipher itself. Despite the fact that each output bit of its F-function only depends on 6 input bits, the DES is complete after 5 rounds [6].

Due to the principle of a Feistel Cipher which operates on the two halves L and R of an input block, at least 3 rounds are necessary for its completeness. The internal states of a Feistel Cipher develop in the following way:

initial state:	(L,	R)
after round 1:	(R,	$L+F_1(R)$)
after round 2:	($L+F_1(R)$,	$R+F_2(L+F_1(R))$)
after round 3:	($R+F_2(L+F_1(R))$,	$L+F_1(R)+F_3(R+F_2(L+F_1(R)))$)

A 3 round Feistel Cipher therefore is complete if F_2 is complete and if each of the output bits of F_3 depends on at least one of its input bits and each of the input bits of F_1 affects at least one of its output bits.

A function f exhibits the *avalanche effect*, if an average of one half of its output bits change whenever a single input bit is complemented. Moreover, f shows the *strict avalanche criterion* if each of its output bits changes with the probability of one half, when complementing one input bit [9]. The strict avalanche criterion includes the completeness of f. This property is considered essential for a "good" cryptographic transformation [9]. A random function will also exhibit the strict avalanche criterion.

The *dependence matrix* of a function $f:GF(2)^n \rightarrow GF(2)^m$ is a (nxm) matrix, whose entry $a_{i,j}$ gives the probability that the output bit j of f changes when its input bit i is complemented. The function f is complete if all elements in its dependence matrix have a nonzero value; it exhibits the strict avalanche criterion, if the value of every element is close to 0.5.

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 434-437, 1988.

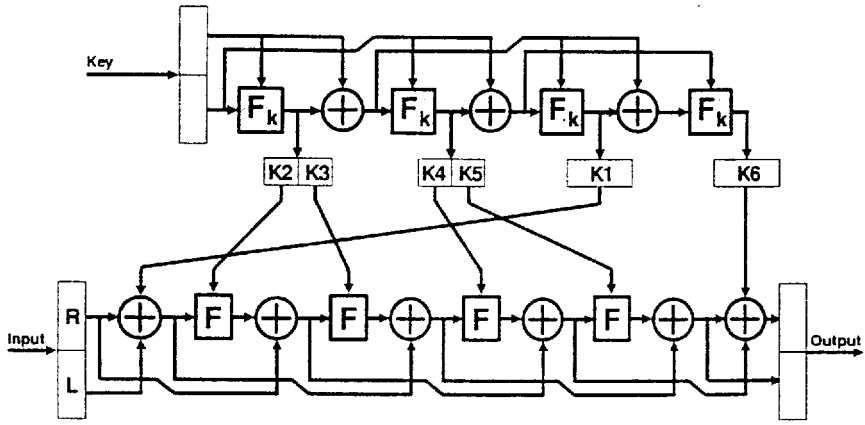

figure 1: Fast Data Encryption Algorithm (FEAL1)

The Fast Data Encipherment Algorithm

The *Fast Data Encipherment Algorithm* (FEAL) is a 6 round Feistel Cipher which operates on 64-bit blocks. Only 4 of its rounds make use of a non-trivial F-function (figure 1 shows FEAL1, [4], which slightly differs from the version given in [8]). The F-function of FEAL is shown in figure 2. The function F_K used for key expansion is similar to F. The structure of F is byte-oriented. Its cryptographic strength depends on a non-linear S-function defined by

$$S(x,y,\delta) = ROL2 ((\ x + y + \delta\ ) \bmod 256\ )$$

where: x, y: one byte data; δ: constant (0 or 1)
ROL2: 2-bit rotate left

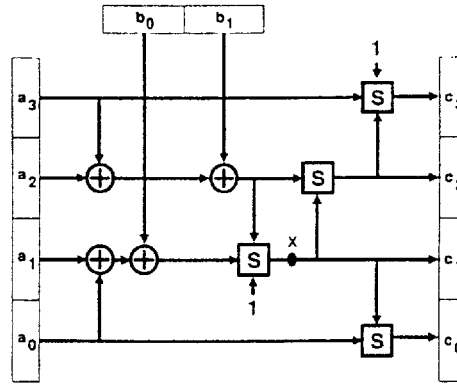

figure 2: F-function of FEAL

Analysis of the S-function reveals its incompleteness. Only one of its 8 output bits depends on every input bit. Moreover, its dependence matrix exhibits a very regular structure. Its upper half (which is identical to the lower half) is given below.

1/64	1/128	1	1/2	1/4	1/8	1/16	1/32
1/32	1/64	0	1	1/2	1/4	1/8	1/16
1/16	1/32	0	0	1	1/2	1/4	1/8
1/8	1/16	0	0	0	1	1/2	1/4
1/4	1/8	0	0	0	0	1	1/2
1/2	1/4	0	0	0	0	0	1
1	1/2	0	0	0	0	0	0
0	1	0	0	0	0	0	0

Since the S-function is not complete, the F-function of FEAL can not be complete. An analysis of the powers of F results in F^i being complete for $i > 1$ and exhibiting the strict avalanche criterion for $i > 2$ (see figure 4). In this respect the F-function of FEAL does better than the F-function of DES where F^j is complete for $j > 2$ and shows the strict avalanche criterion for $j > 3$ (see also figure 4). For this reason FEAL is complete after 4 rounds whereas DES needs 5 rounds in order to become a complete block cipher (see figure 3).

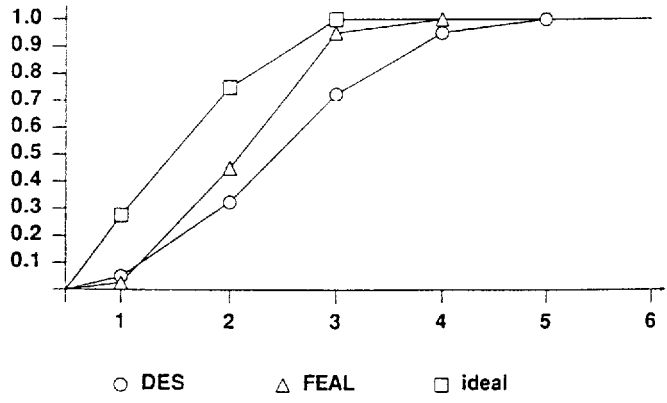

figure 3: Increasing completeness of DES and FEAL

Modifications of FEAL's F-function

There are straight-forward modifications of FEAL's F-function that will further improve the properties discussed above. Moreover, these modifications allow the introduction of a non-linear function that can be chosen at random and will therefore overcome any distrust of the S-functions.

D.Davies has suggested to modify FEAL's F-function by replacing the operation ROL2 by an 8-bit S-box [2]. By this modification 4 (possibly different) S-boxes are added to the F-function. Although a randomly chosen S-Box will show the strict avalanche criterion, the modified F-function will not exhibit the same property. It is complete, however, and F^i will show the strict avalanche criterion for $i > 1$ (see figure 4).

We suggest a modification that uses only one additional 8-bit S-Box in the position marked by X in figure 2. The input of this S-Box depends on every byte of the input of F. Its output affects every byte of the output of F. The effect of this modification is similar to the effect of the modification discussed above. The modified F-function is complete and F^i will exhibit the strict avalanche criterion for $i > 1$ (see figure 4).

Both modifications of FEAL's F-function will counteract den Boer's cryptanalysis of this cipher [3].

		F	F^2	F^3	F^4
DES	dependence	0.188	0.875	1.000	**1.000**
	mean	0.119	0.375	0.493	**0.500**
	variance	0.063	0.027	0.00053	**0.00026**
FEAL	dependence	0.883	1.000	**1.000**	**1.000**
	mean	0.308	0.481	**0.500**	**0.500**
	variance	0.112	0.013	**0.00026**	**0.00024**
FEAL + 1 S-Box	dependence	1.000	**1.000**	**1.000**	**1.000**
	mean	0.505	**0.499**	**0.500**	**0.500**
	variance	0.00096	**0.00024**	**0.00026**	**0.00026**
FEAL + 4 S-Boxes	dependence	1.000	**1.000**	**1.000**	**1.000**
	mean	0.503	**0.501**	**0.500**	**0.500**
	variance	0.00054	**0.00025**	**0.00026**	**0.00024**

figure 4: Comparison of different F-functions

References

[1] Chaum, D.; Evertse, J.-H.: *Cryptanalysis of DES with a Reduced Number of Rounds*, in: Advances in Cryptology - Crypto '85, H.C.Williams ed, Lecture Notes in Computer Science, **218** (1986), 192-211

[2] Davies, D.W.: private communication (1987)

[3] den Boer, B.: *Cryptanalysis of FEAL*, presented at Crypto '87

[4] ISO: *Introduction to a New Encipherment Algorithm FEAL*, ISO/TC97/SC20/WG1 N36 (1985)

[5] Kam, J.B.; Davida, G.I.: *Structured Design of Substitution-Permutation Encryption Networks*, IEEE Trans. Computers, **28** (1979), 747-753

[6] Meyer, C.H.; Matyas, S.M.: *Cryptography: A New Dimension in Computer Data Security*, (John Wiley & Sons, New York, 1982)

[7] National Bureau of Standards: *Data Encryption Standard*, FIPS Publ. 46, Washington D.C., 1977

[8] Shimizu, A.; Miyaguchi, S.: *Fast Data Encipherment Algorithm FEAL*, presented at Eurocrypt 1987

[9] Webster, A.F.; Tavares, S.E.: *On the Design of S-Boxes*, in: Advances in Cryptology - Crypto '85, H.C.Williams ed, Lecture Notes in Computer Science, **218** (1986), 523-534