Chapter 1

FEAL-NX

FEAL was a general design proposed by NTT in 1987. It depended on several parameters, including the number of rounds. Since it was proposed, several cryptanalysis methods were found, and the parameters were adapted accordingly. The proposed version suggests to use at least 32 rounds. This high number may make the performance quite poor, but performances are beyond the scope of this report.

1.1 Design Properties

1.1.1 Basic Properties

The FEAL-NX design is quite simple. It uses only exclusive or (XOR), additions of 8-bit numbers (modulo 256) and circular rotation of two bits for 8-bit strings. This makes the implementation of simple microprocessors very straightforward (like for instance on Motorola 6805 processors). Modern processors may take advantage of built in 8-bit operations (like the MMX technology).

FEAL-NX does not include any other operation. In particular, there is neither table look up, nor any other nonlinear operation. Since all used operations are linear, we may consider that FEAL-NX is very weak. However the nonlinear structures (namely, the $\mathbf{Z}_2^8$ vector space and the $\mathbf{Z}_{256}$ ring) are not compatible. Having a high number of rounds makes the linearity incompatibility behave nonlinearly.

1.1.2 Symmetries

We can note that the key scheduling algorithm is quite symmetric. For instance, the sequence $Q_1 \oplus Q_2, Q_1, Q_2$ is repeatedly used to produce subkeys.

It is therefore not difficult to derive conditions on the key such that it will produce a periodic set of subkeys.

A key (A, B, Q_1, Q_2) which produces a subkey sequence of period 6 must fulfill following conditions:

1. $f_K(A, B \oplus Q_1 \oplus Q_2) = 0$
2. $f_K(B, A \oplus Q_1) = A$
3. $f_K(0, A \oplus Q_2) = B$

A simple computer search program has furnished following examples: the key `0x23E699E2 1DD7FEA5 960BD469 CA59F7D1` produces the subkey sequence K_i = `0x0000`, K_{i+1} = `0x0000`, K_{i+2} = `0x23E6`, K_{i+3} = `0x99E2`, K_{i+4} = `0x1DD7`, K_{i+5} = `0xFEA5` for $i = 1, 7, 13, ...$ Other examples of keys are

- `0xC3284B4A AD3D694B 98802047 207274B9`
- `0x3E162B10 C16A9E32 4B1EF3EA 66B1AF37`

There are 2^{32} keys having a subkey sequence with a period of 6. It is however not clear how to exploit this property.

1.1.3 Pre and Post Processing

FEAL-NX starts with a pre-processing which consists in two phases:

1. XOR with subkeys
2. XOR of the left half onto the right half.

We notice that these phases are commutative. Finally, the second phase seems to be totally useless for security since any attack against a variant of FEAL-NX in which this second phase is omitted can be transformed into an attack against the full FEAL-NX.

Similarly, FEAL-NX ends with a post-processing which consists in two phases:

1. XOR of the left half onto the right half
2. XOR with subkeys.

The first phase is totally useless for security.

1.2 Differential and Linear Cryptanalysis

The literature already investigated the resistance of FEAL-NX against differential and linear cryptanalysis and gave evidence that no characteristic can be used. We did another experiment in order to get the minimal number of rounds for an iterative characteristic in a simple model: realizing that non linearity is only introduced by carry bits in addition, assuming that all carry bits are zero, we have a linear function. We can thus express one round as a linear mapping L. Differential and linear characteristic will necessarily be given by L. Thus, an iterative characteristic against r rounds must necessarily correspond to a fixed point of L^r.

Computing the minimal polynomial of L, we obtained

$$\mu_L(x) = (1 + x + x^4)^8.$$

Let $\lambda_1, \ldots, \lambda_4$ be the four roots of this polynomial in the closure field of this polynomial. We know that the eigenvalues of L^r are the λ_i^r. We know that a linear mapping has a fixed point if and only if 1 is an eigenvalue. Thus, we have an iterated characteristic on r rounds if and only if we have $\lambda_i^r = 1$ for some i. This would mean that $1 + x + x^4$ and $1 + x^r$ have a common root, which is equivalent to $\gcd(1 + x + x^4, 1 + x^r) \neq 1$. Since $1 + x + x^4$ is an irreducible polynomial, this is equivalent to the fact that $1 + x + x^4$ divides $1 + x^r$. The $1 + x + x^4$ polynomial has four roots in $\mathrm{GF}(2^4)$. We notice that since $\mathrm{GF}(2^4)^*$ has an order of 15, so all roots have an order which is a factor of 15: 1, 3, 5 or 15. Since 1 is not a root, the order cannot be 1. Since $1, x, x^2, x^3$ is a basis of $\mathrm{GF}(2^4)$ as a linear space over $\mathrm{GF}(2)$, x^3 cannot be equal to 1. Thus the minimal r such that $1 + x + x^4$ divides $1 + x^r$ is necessarily 5 or 15. We can check that $1 + x + x^4$ does not divide $1 + x^5$. Therefore the minimal number of rounds for an iterative characteristic is 15.

We did not have time to continue the analysis. We believe that a linear algebra approach may yield interesting weaknesses in FEAL-NX eventually. Although FEAL-NX looks pretty resistant at a first glance and seems to have resisted to attacks for many years, we think that the intrinsic linearity and simplicity may still hide unexplored weaknesses.

1.3 Other Attacks

1.3.1 Truncated Differentials

We can investigate truncated differentials as we did for CS-CIPHER.[1]

We consider differentials in which we identify zero-byte differences and nonzero-byte differences. We have 256 possible zero-nonzero-byte combinations for a difference over 64-bit strings. Only a few one-round characteristics are possible with these combinations, which can be represented by oriented edges in a graph of 256 vertices.

For instance, the f function makes the

$$**00 \rightarrow *000$$

differential feasible. It occurs when the first two byte differences are equal because they cancel each other. Therefore the

$$0*00**00 \rightarrow **000*00$$

differential on one round is feasible.

Additionally, we put on the edges a weight which is the number of odd events on single bytes which are required in order to achieve the differential. In the

$$**00 \rightarrow *000$$

differential on f, one single odd event on bytes is required, namely the cancellation of the first two-byte differences. Therefore the

$$0*00**00 \rightarrow **000*00$$

has a weight of one.

A differential on r rounds is a path of length r in the graph. The total weight of the path (which is the sum of all edge weights) gives the probability of the whole differential, by raising 2^{-8} to this power. The Floyd algorithm computes the paths of given length and shortest weights.

In the case of FEAL-NX, such a computation gives as result a minimal non-zero weight of 15 for a path of length 32. Thus, we can conclude that there exists no useful truncated differential.

[1] See "On the Security of CS-CIPHER" by Vaudenay, Fast Software Encryption, LNCS 1636 pp. 260–274, Springer-Verlag 1999.

1.3.2 Side Channel Cryptanalysis

The design of FEAL-NX makes hard to implement side channel attacks like power analysis, fault analysis, ... Actually FEAL-NX only uses bit rotations by two positions, additions, XOR and byte moves. It does not use data-dependent rotation, multiplication or table look up.

In a simple (and powerful) model of power analysis, we can trace the Hamming weight of the CPU registers during the whole computation. This leads to straightforward analysis. For instance we can just submit chosen plaintext pairs which differ by only one bit and look of the Hamming weights after a XOR with the first subkeys. This recovers one bit of the key. We can repeat it many times until we recover all the subkey bits, then all the subkeys.

This means that embedded systems must care about power analysis and have hardware protection against it.

1.3.3 Weak Keys

We have raised unexpected properties in the key schedule which produce keys for which the subkeys are periodic. This class of keys may be vulnerable against some kind of attack as a class of weak keys. We did not have time to investigate further.

1.3.4 Related Keys

The key schedule opens the way to related key attacks as shown below.

If we let $K_R = ab$ where a and b are 32-bit strings, the Q_i sequence is

$$(a \oplus b, a, b, a \oplus b, a, b, \dots).$$

If we now let $K_R = b(a \oplus b)$, the Q_i sequence becomes

$$(a, b, a \oplus b, a, b, a \oplus b, \dots)$$

which thus consists in a shift by one round.

Let $K_L = \phi c$ and $K_R = ab$. In addition we let

$$d = f_K(\phi, a \oplus b).$$

We now consider a new key K' such that $K'_L = cd$ and $K'_R = b(a \oplus b)$. This key generates a sequence $(K'_0, K'_1, \dots)$. We notice that $K'_i = K_{i+2}$. The K and K' keys are thus related. As for the previous section, we had no time to explore this unexpected property.

1.3.5 Decorrelation

A good way to get security insurance for block ciphers is decorrelation. In the case of FEAL-NX, the round function has a too low entropy. Actually, it is fairly easy to distinguish f from a random function with only one known input and output pair. We just inverse the substitution part of f on the known output, and we check that the first and last bytes correspond to the known input. This holds with probability 1 for f, and with probability 2^{-16} for a random function. The decorrelation of f to the order one is thus at least $2 \times (1 - 2^{-16})$. This cannot be used in order to lower bound the decorrelation of FEAL-NX with known techniques.

1.4 Available Literature

The FEAL cipher family has been widely studied in the literature. The original family member was FEAL-4 (4 rounds) [18]; this version has been broken using a chosen plaintext attack with 100 to 10000 ciphertexts [4]. As a consequence, the number of rounds was increased to 8, keeping the f-function unchanged [18, 12]. FEAL-8 was successfully broken by differential cryptanalysis [3]. Two new versions were then added to the family, FEAL-N with any even number N of rounds and FEAL-NX [13] which has an extended 128-bit key. However, Biham and Shamir note [3] that FEAL-N can be broken for any $N \leq 31$ faster than exhaustive search using differential cryptanalysis.

Other attacks against early family members have been published: [5] breaks FEAL-8 with 10000 encryptions. [14] breaks FEAL-4 using only 20 encryptions.

Several papers have studied the security of the FEAL family regarding generic attacks. FEAL-NX seems to be out of reach of a linear cryptanalysis [15, 16], a differential cryptanalysis [7] and impossible differentials attacks [1]. In [6], it is argued that FEAL-8 doesn't have a closure structure with high probability.

1.5 Conclusion

FEAL-NX is the oldest of the four block ciphers in this category. This should suggest a high confidence. However this should be considered with the fact that several earlier versions were successfully broken, so maybe FEAL-NX did not receive the expected interest from the community of cryptanalysis experts.

No efficient attack against FEAL-NX is known anyway. During the short time schedule the authors of the present report were given, some interesting strange properties were found.

- keys for which the subkey sequence is periodic,
- an apparently useless (at least for security) pre and post processing,
- an intrinsic linear structure.

Known techniques from decorrelation theory did not succeed to get security insurances. On the other hand, FEAL-NX is, due to its simplicity, one of the most secure ciphers against known side channel cryptanalysis techniques. Implementation should however care about power analysis and take hardware protections.

Despite the apparent resistance of FEAL-NX against known cryptanalysis techniques, we still believe that its intrinsic linearity may lead to weaknesses that we do not know how to use at this time. We believe that FEAL-NX inherited from a weak structure which has been artificially strengthen by increasing the number of rounds. From our experience we speculate that security could eventually collapse. If FEAL-NX should be used for sensitive information protection, we recommend to perform an extra (deeper) analysis.

Here are our conclusion about FEAL-NX.

1. **Discovery of unexpected internal properties: "·".** Due to simplicity, S_0 and S_1 hide many simple properties like bit flip propagation.
2. **Randomness provided by the key schedule: "−".** We discovered symmetries.
3. **Resistance against differential and linear cryptanalysis: "·".** We suspect unexpected properties.
4. **Resistance against side channel attacks: "++".** Simplicity does not open weaknesses.
5. **Maturity of the algorithm: "++".** The age of FEAL-NX and the importance of literature is a good sign.
6. **Overall security confidence: "·".** We still believe in unknown weaknesses.
7. **Beauty of the design: "+".** We appreciate simplicity.