Celebrating the 25th year of FEAL

- A New Prize Problem -

August 21 2012

Mitsuru Matsui
Mitsubishi Electric Corporation

FEAL

(Fast data Encipherment ALgorithm)

- Designed by Miyaguchi and Shimizu (NTT)
- 64-bit block cipher family with the Feistel structure
  - 4 rounds (1987)
  - 8 rounds (1988)
  - N rounds(1990) N=32 recommended
- Key size is 64 bits (later extended to 128 bits as FEAL-X)
- First commercially successful cipher in Japan
- Inspired many new ideas, including linear cryptanalysis

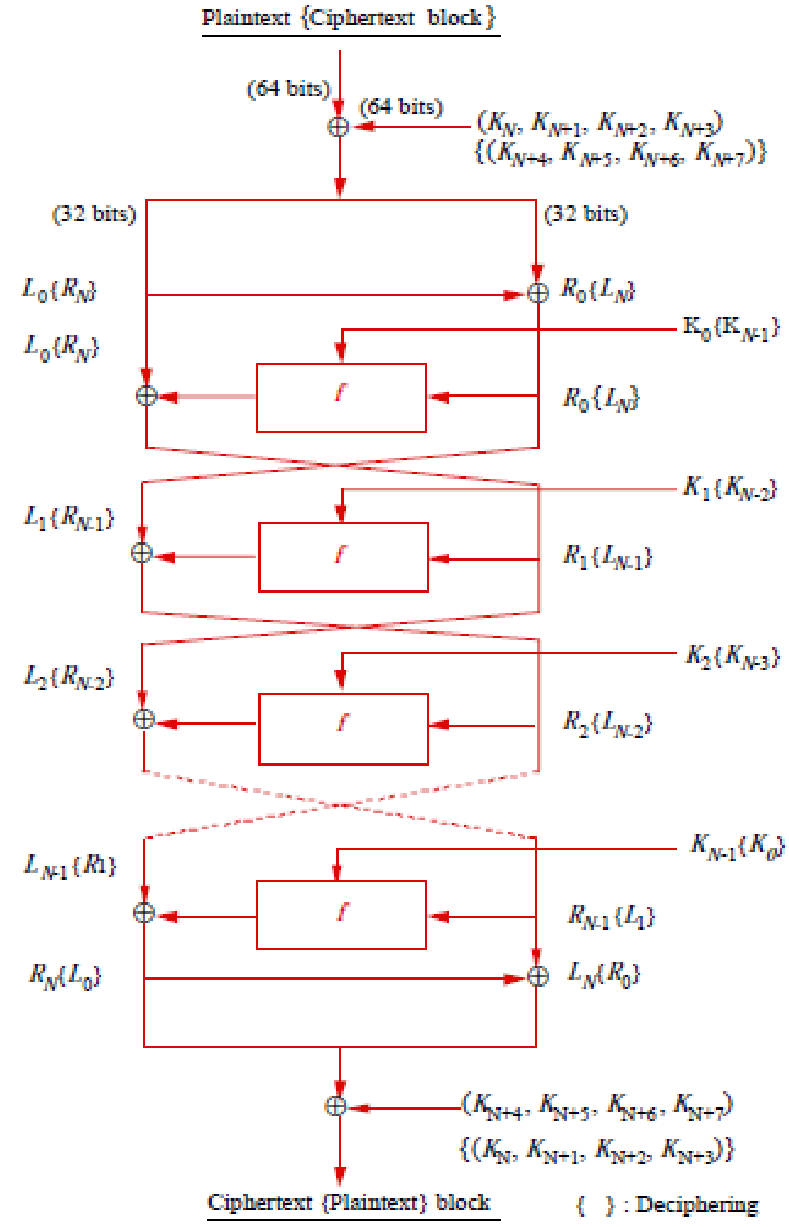
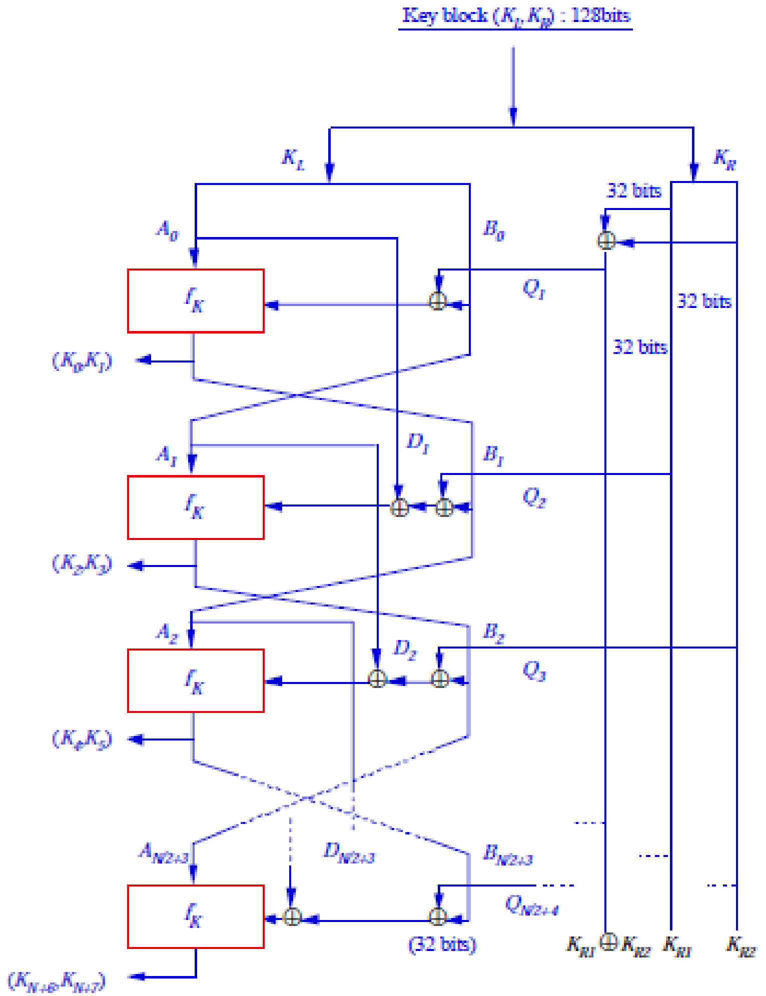


Fig. 1 Data randomization of FEAL-NX (Ciphering/Deciphering algorithm)



$K_{2(r-1)}$: Left half of B_r (16bits)

$K_{2(r-1)+1}$: Right half of B_r (16bits)

Number of iterations is (N/2)+4.

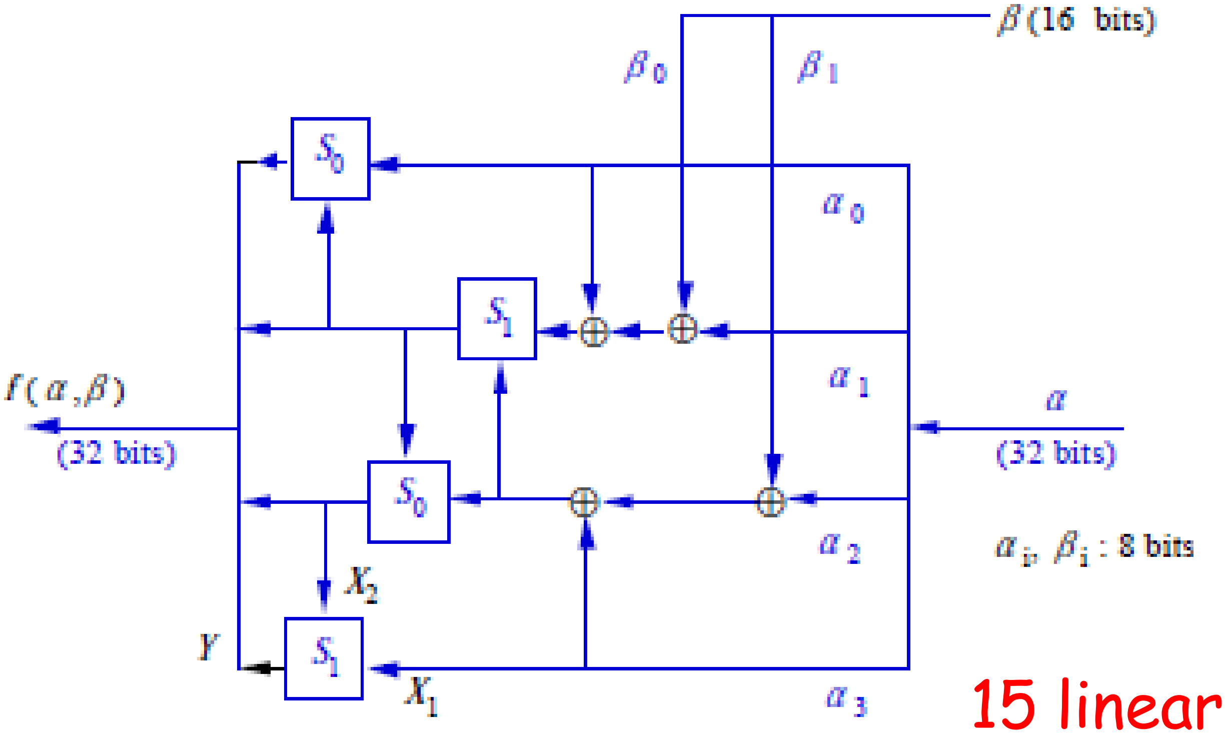
$Q_r = K_{R1} \oplus K_{R2}$ r = 1,4,7,...

$Q_r = K_{R1}$ r = 2,5,8,...

$Q_r = K_{R2}$ r = 3,6,9,...

$K_R = (K_{R1}, K_{R2})$

Fig. 2 Key schedule of FEAL-NX



$Y = S_0(X_1, X_2) = \mathrm{Rot2}((X_1+X_2) \bmod 256)$

$Y = S_1(X_1, X_2) = \mathrm{Rot2}((X_1+X_2+1) \bmod 256)$

Y : output (8 bits), X_1/ X_2 : inputs (8 bits),

Rot2 (Y) : a 2-bit left rotation on 8-bit data Y

Fig. 3 f -function of FEAL-NX

15 linear relations exist

$\alpha[x_1]+\beta[x_2]+f(\alpha,\beta)[x_3]=0$

Security of FEAL

- 4-round version
  - 100-10000 chosen plaintexts [Boer 88]
  - 20 chosen plaintexts [Murphy 90]
  - 8 chosen plaintexts [Biham, Shamir 91] differential
  - 200 known plaintexts [Tardy-Corfdir, Gilbert 91]
  - 5 known plaintexts [Matsui, Yamagishi 92] pre-linear
- 8-round version
  - 10000 chosen plaintexts [Tardy-Corfdir, Gilbert 90] diff
  - 2000 chosen plaintexts [Biham, Shamir 91] differential
  - 2^{15}-2^{28} known plaintexts [Matsui, Yamagishi 92] pre-linear
  - 2^{24} known plaintexts [Biham 94] linear

An Old Prize Problem

- Announced at Crypto'89 rump session.
  - "The FEAL-8 Cryptosystem and a Call for Attack"
- 2^{10} plaintext-ciphertext pairs were given.
- Good news: first winner receives 1,000,000 yen.
- Bad news: the deadline expired 22 years ago.
- Remains unsolved (or forgotten).
- A brute force is now feasible (64-bit key) but not easy.

The New Prize Problem

- The target cipher: FEAL-8X
  - FEAL cipher with 8 rounds and 128-bit key
  - Same as FEAL-8 except its key scheduling part
- 2^b plaintext-ciphertext pairs are given ($b \leq 20$).
- Good news: winner (min b, first) receives $1500.
- Bad news: brute force is infeasible (128-bit key)
- Deadline: CRYPTO 2013
- For more details, see https://docs.google.com/open?id=0B3xMqN36HCf2eDVzb191R1VHY0k

Another Motivation

Recent cryptanalysis of symmetric primitives assumes a very (often too) powerful opponent…

related-(sub)key, adaptive-chosen-ciphertext/IV, related-algorithm(!), weak key, distinguishing… with 2^{250} data/time/memory complexity….

If an attacker is allowed to access up to, say, only 2^{20} known-plaintexts in a single key model, then to what extent a cipher can be simpler ?

Conclusions

Let's recall and thank the FEAL cipher for its contribution to the history of block ciphers.

If you have found a solution (a secret key) for any b, please send it to fealXXyears@gmail.com. (Quiz: find hidden 2 digit number XX).

For the specification of the FEAL cipher family, See http://info.isl.ntt.co.jp/crypt/eng/archive/index.html#feal