Linear Cryptanalysis of FEAL

Folker Hoffmann

Seminar: Block cipher cryptanalysis

May 2, 2011

Overview

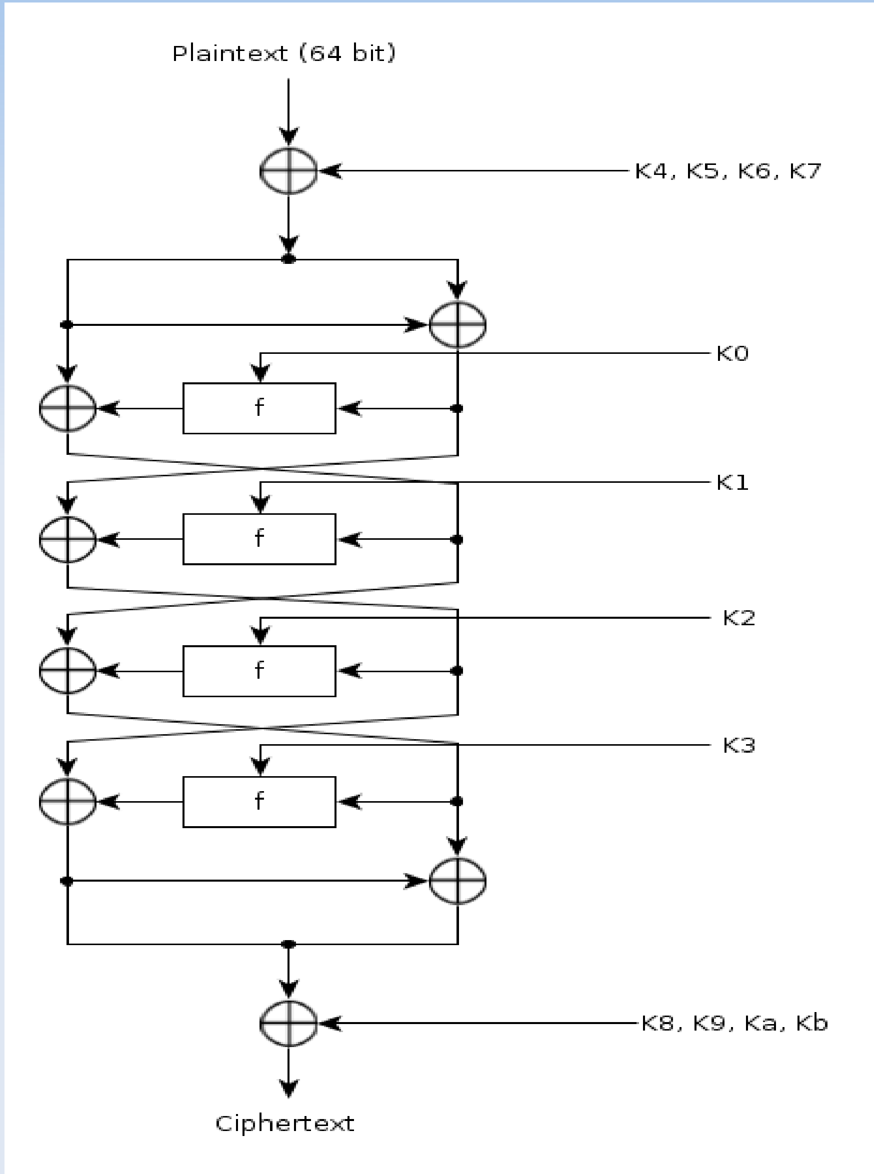
- FEAL
  - Encryption with FEAL
  - Modification of FEAL
- Linear Cryptanalysis
  - Idea
  - Linear equations in FEAL
  - Recovering the roundkeys

FEAL

- Fast Data Encipherment Algorithm
- Proposed in 1987
- Goal: It should be suitable for implementation in software on smart cards
- Different versions:
  - Number of rounds: 4, 8, N
  - Block size: 64, 128
    - FEAL-N, FEAL-NX
- Here: FEAL-4

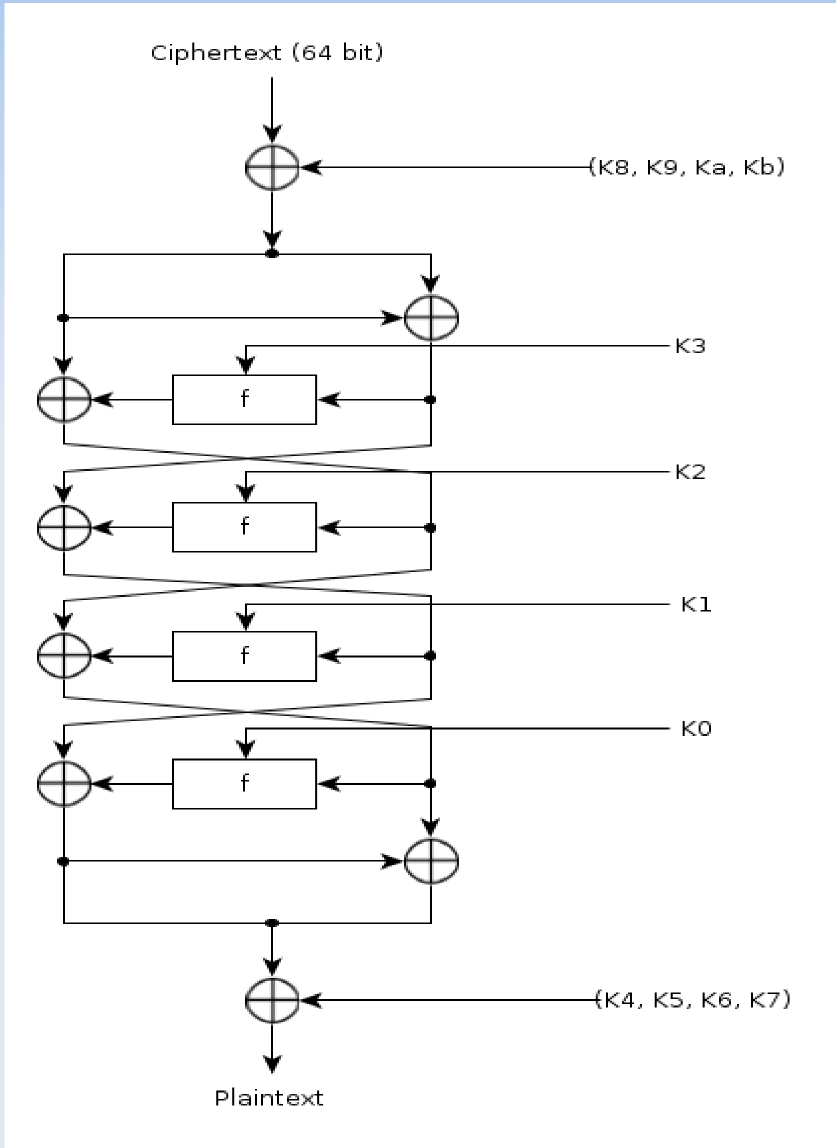
FEAL: Encryption

- Feistel cipher

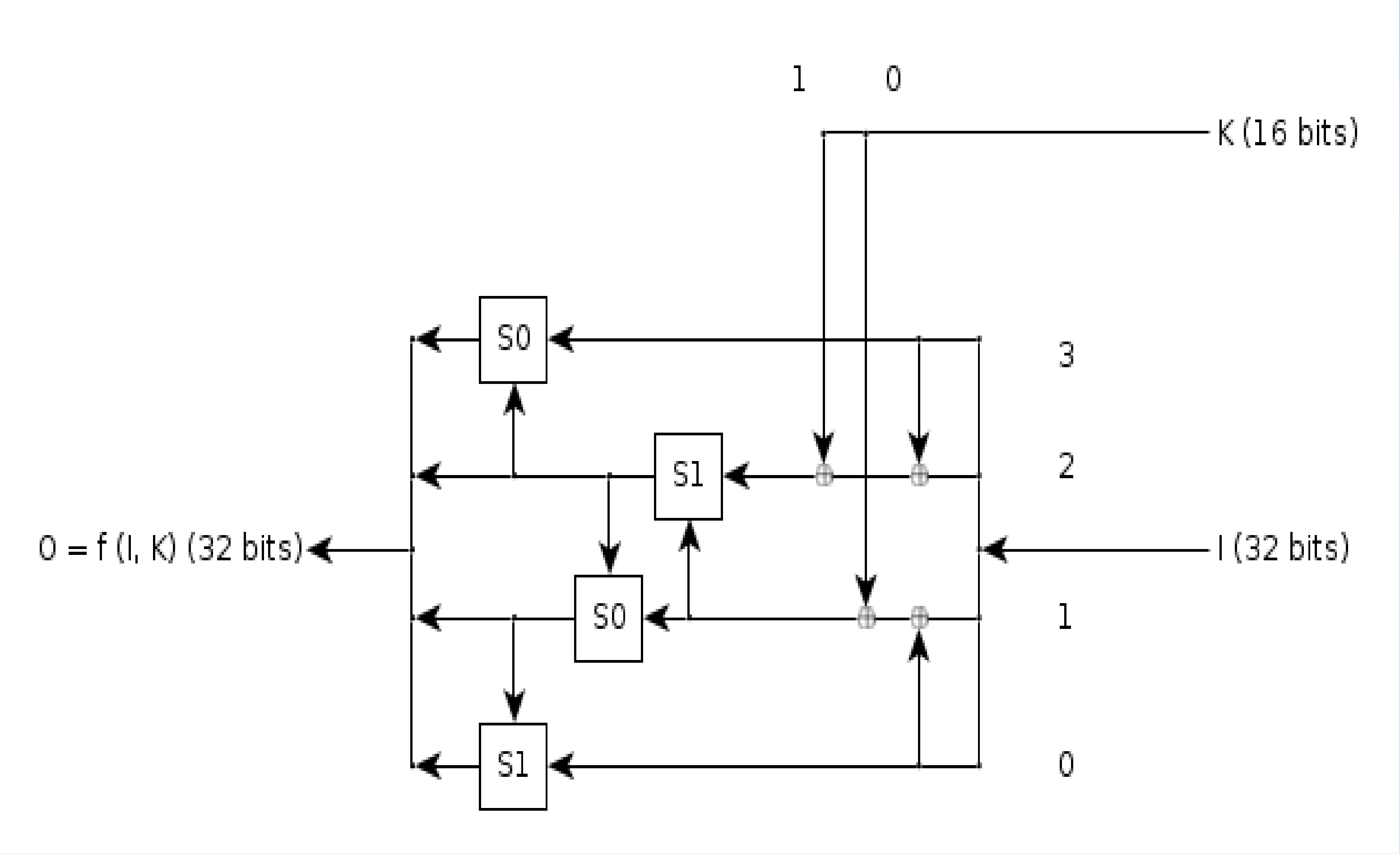


FEAL: Decryption

- Use the keys in reverse



The round function: f



The S-box

- Input: Two bytes X, Y + delta (0 or 1)
- Output: One byte

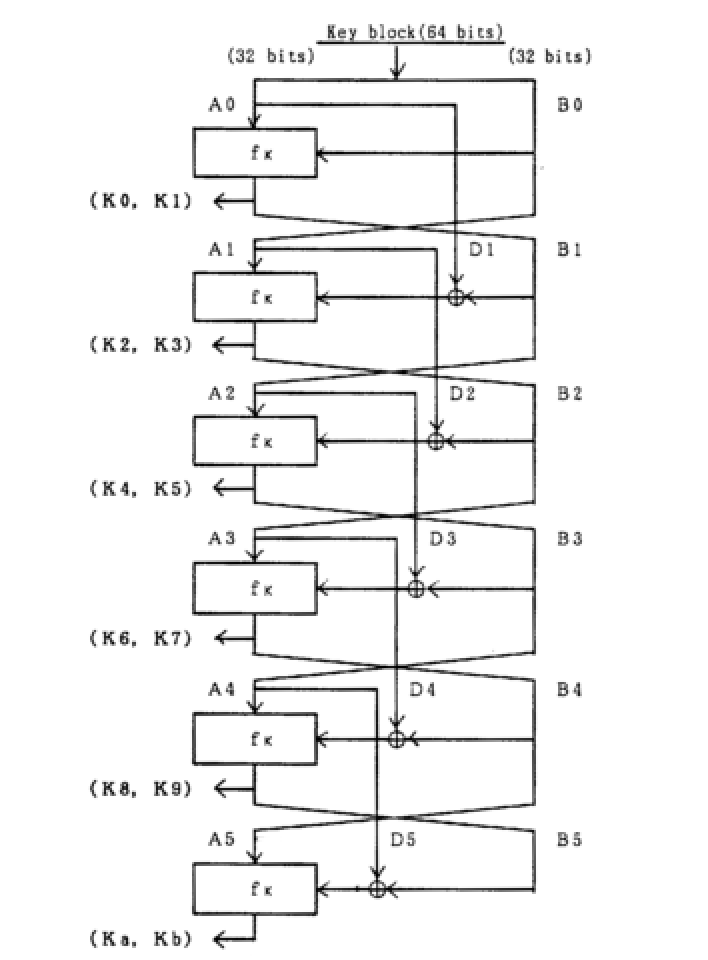
$$S(X, Y, delta) = ROT2((X + Y + delta) \bmod 256)$$

- Example: (delta = 1)

```
   00010011
+  10110011
+         1
=  11000111
```

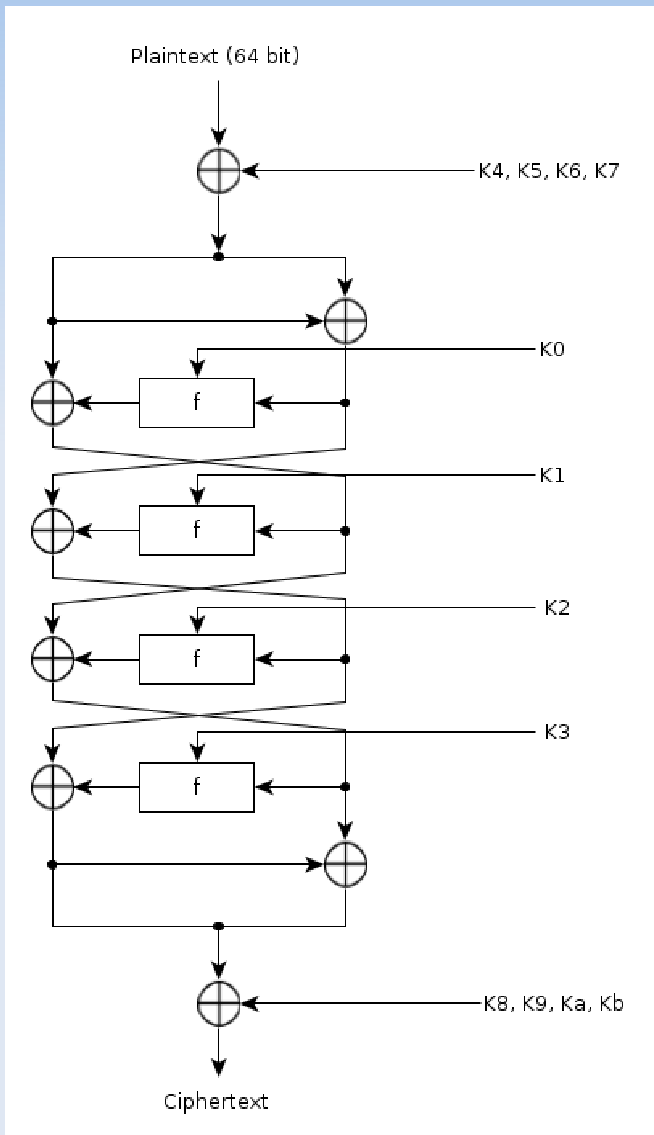
$$11000111 \xrightarrow{\text{Rot2}} 00011111$$

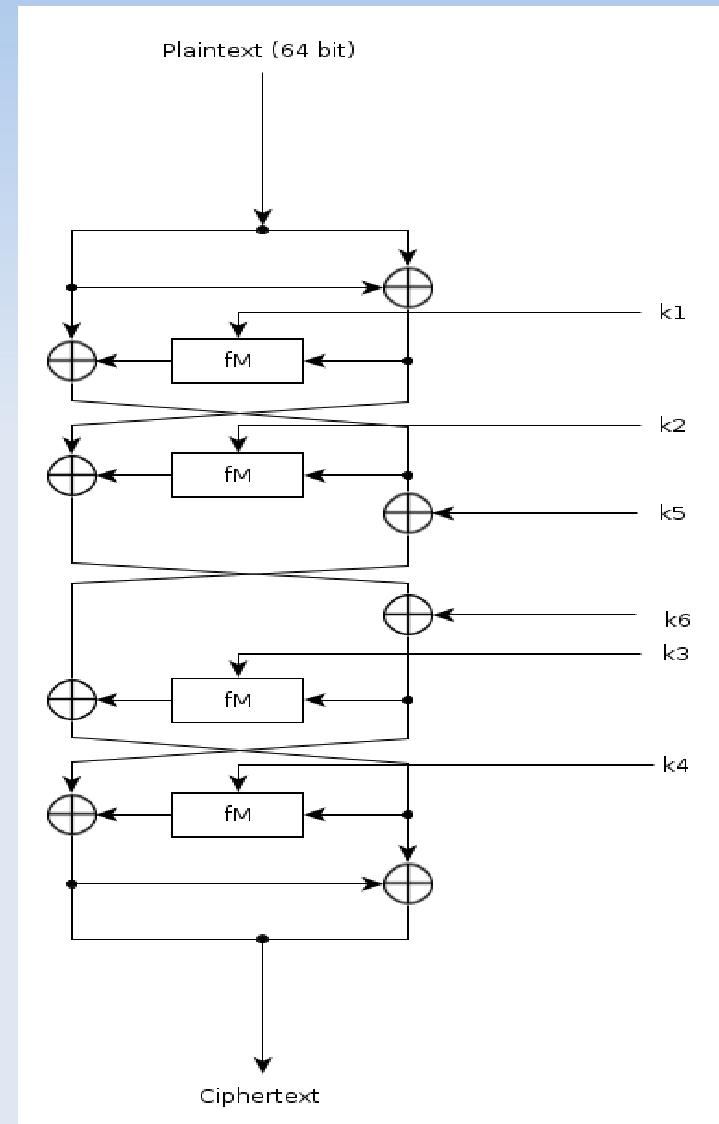
Key schedule



(Based on the image of the key schedule of FEAL-8 in: Shimizu & Miyaguchi: Fast Data Encipherment Algorithm FEAL, 1988)

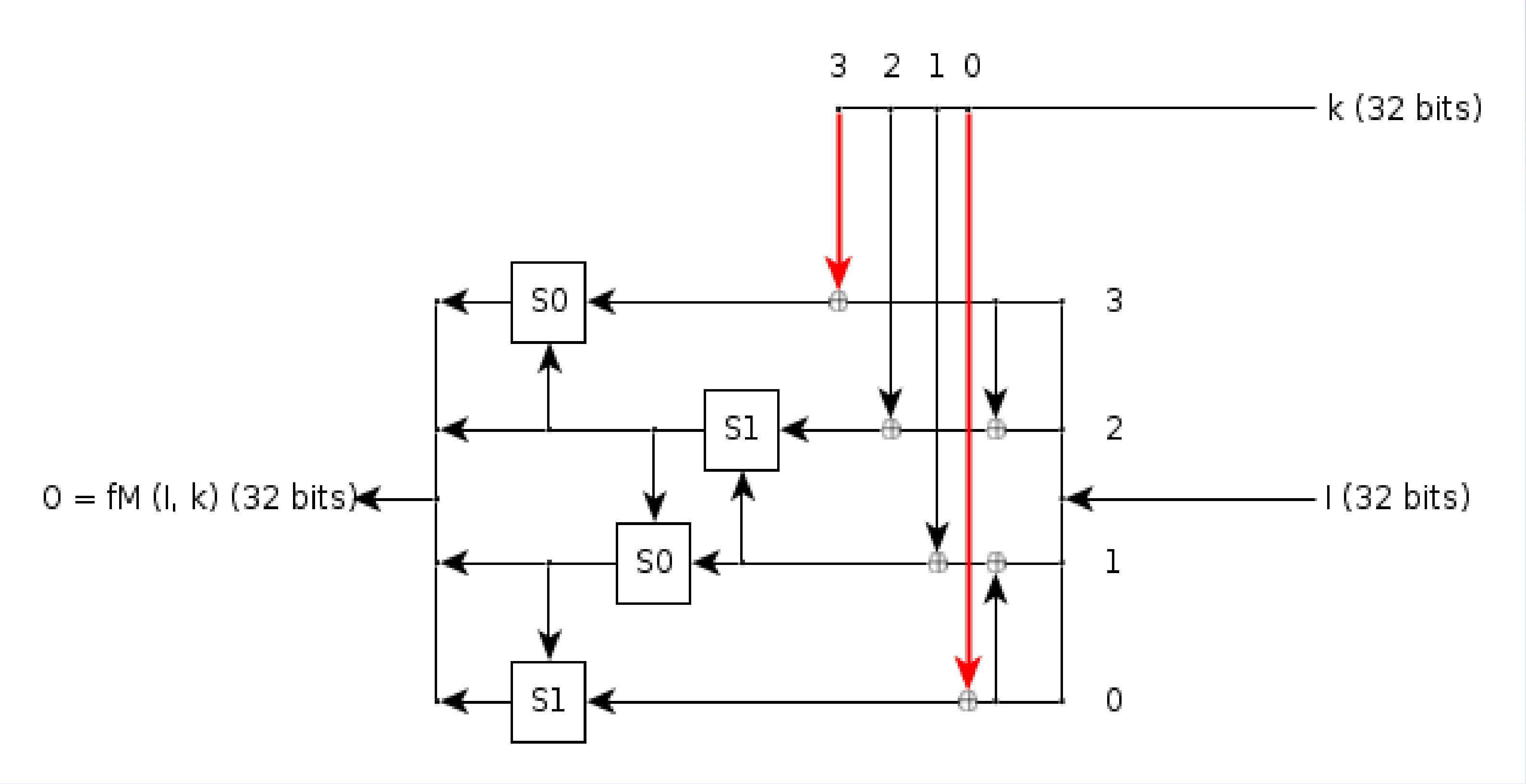
Rearrangement of FEAL



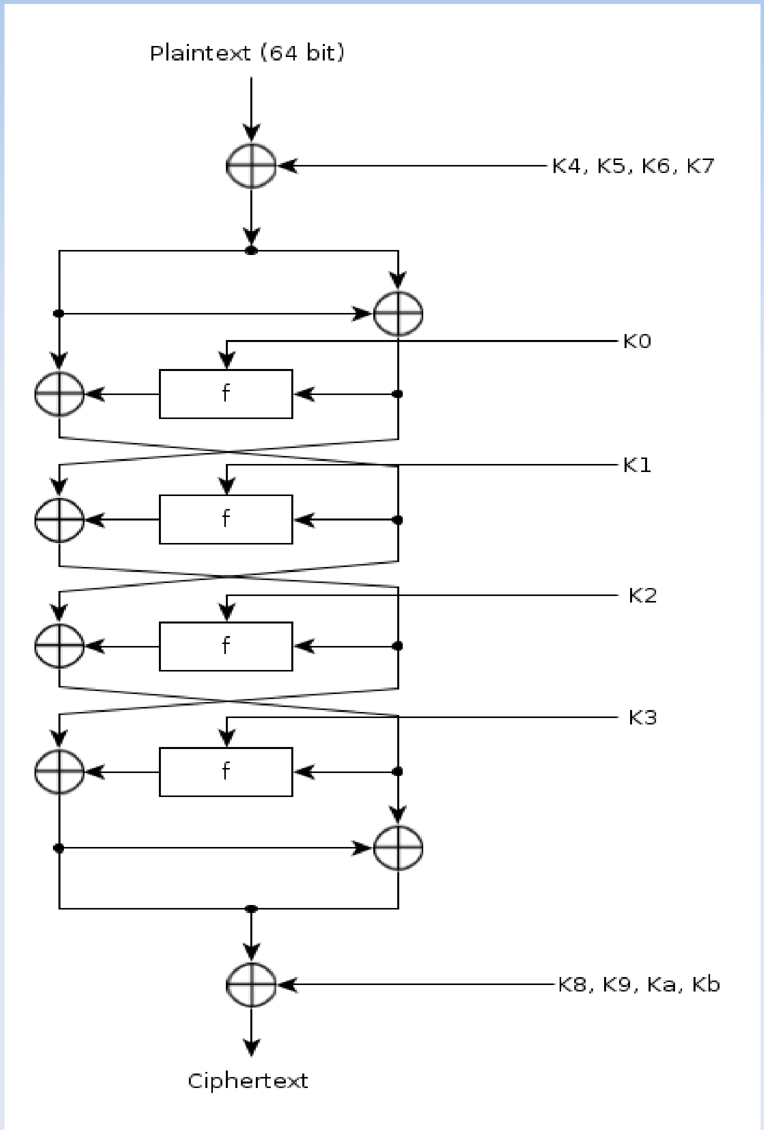


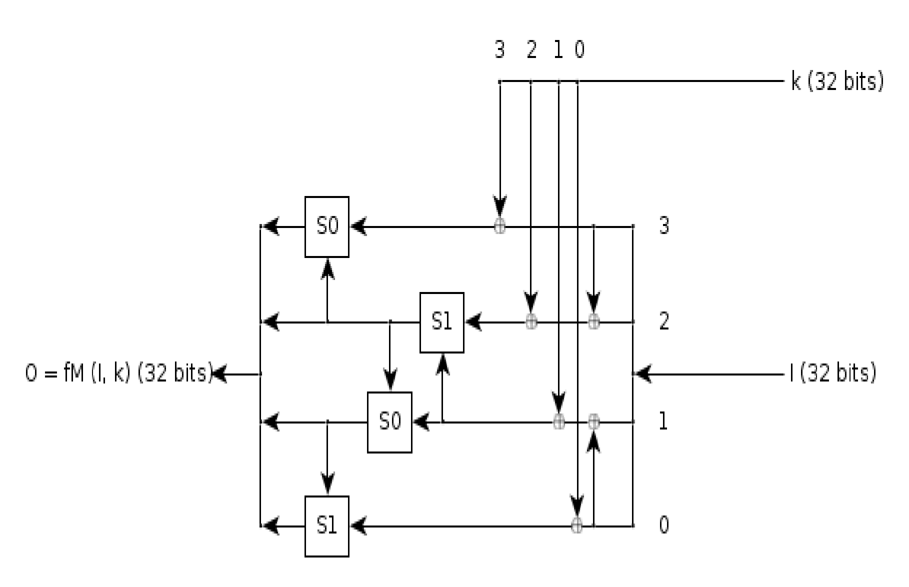
Rearrangement of FEAL

- Key affects each byte

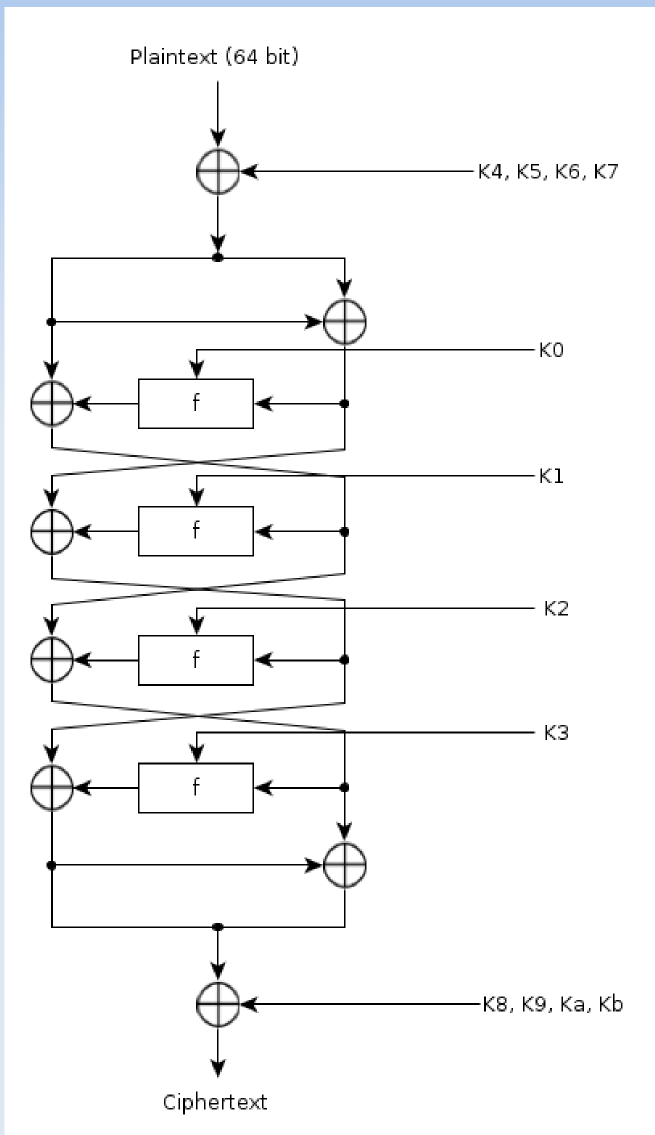


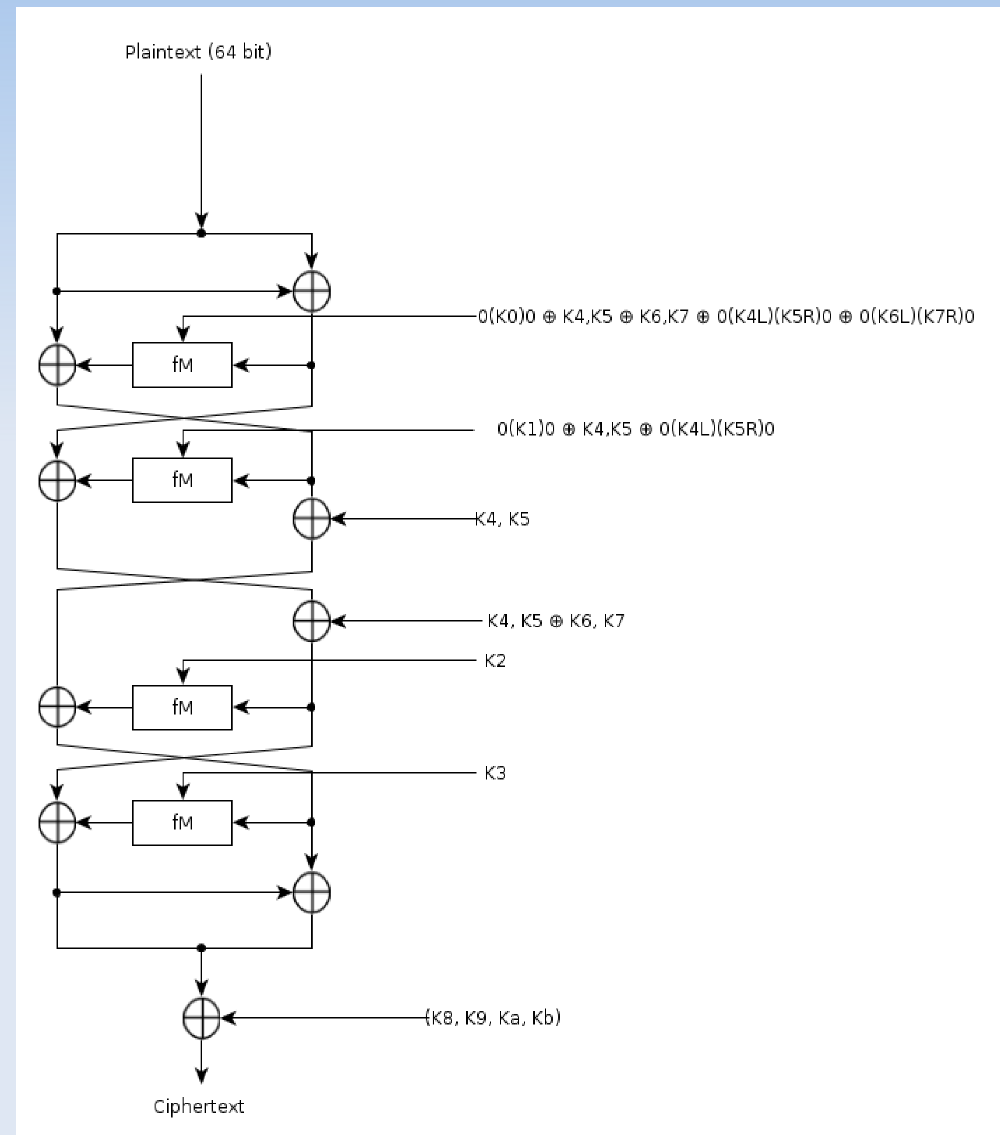
Rearrangement of FEAL



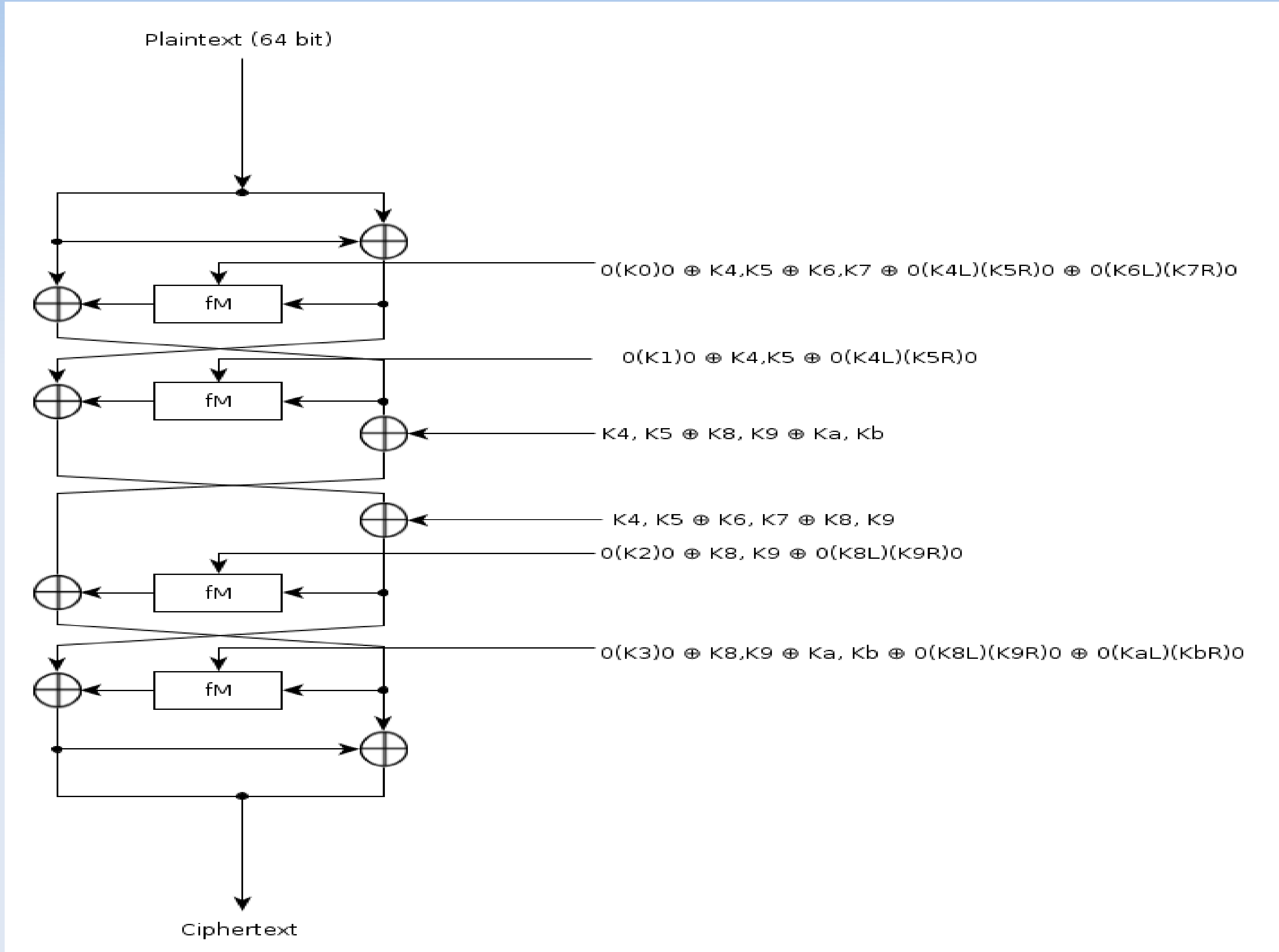


Rearrangement of FEAL

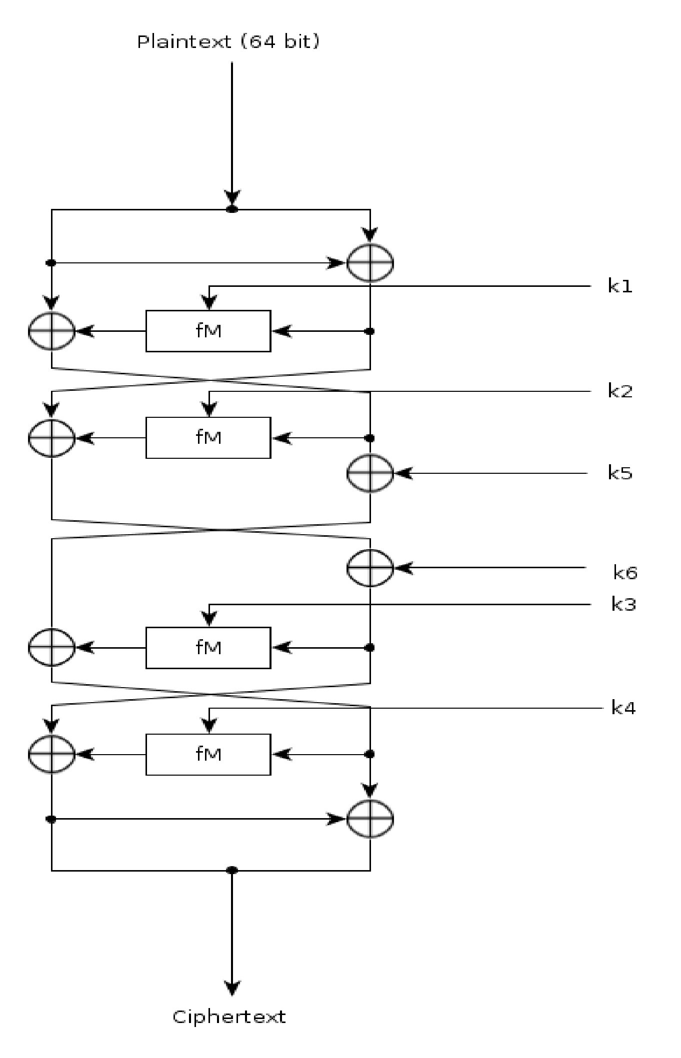




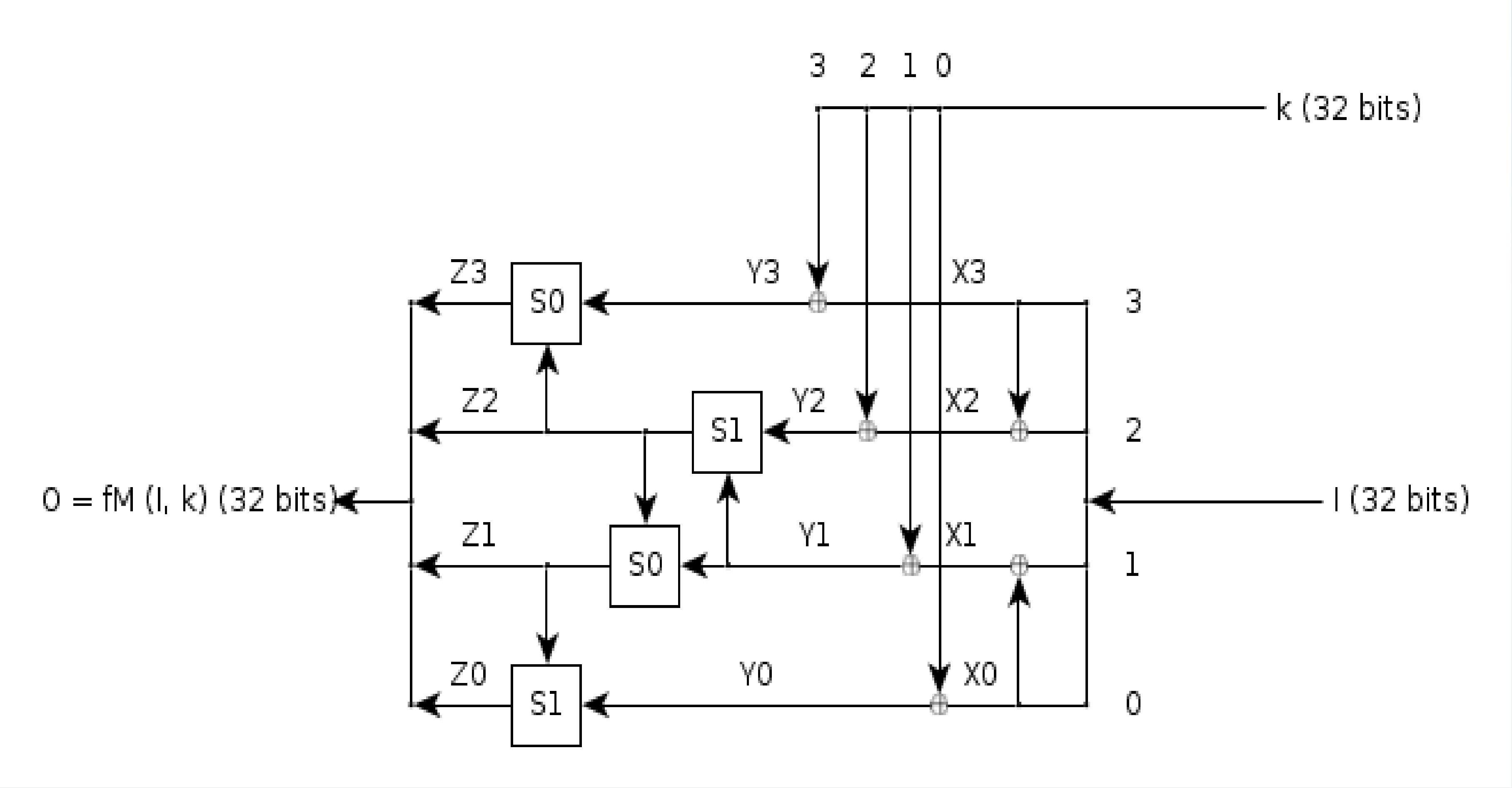
Rearrangement of FEAL



Rearrangement of FEAL



Example: fM



3 2 1 0
k (32 bits)
Z3
S0
Y3
X3
3
Z2
S1
Y2
X2
2
O = fM (I, k) (32 bits)
I (32 bits)
Z1
S0
Y1
X1
1
Z0
S1
Y0
X0
0

Linear Cryptanalysis

- Known plaintext attack
- Basic idea: Find linear approximations of the cipher:
- $C[i_1] \oplus C[i_2] \oplus \ \dots \ \oplus C[i_n] \oplus P[j_1] \oplus \dots \oplus P\,[j_m]$

$$\oplus K[k_1] \oplus \ \dots \ \oplus K[k_t] \oplus fM(I_1, k_1)[f_1] = 1 \text{ (or 0)}$$

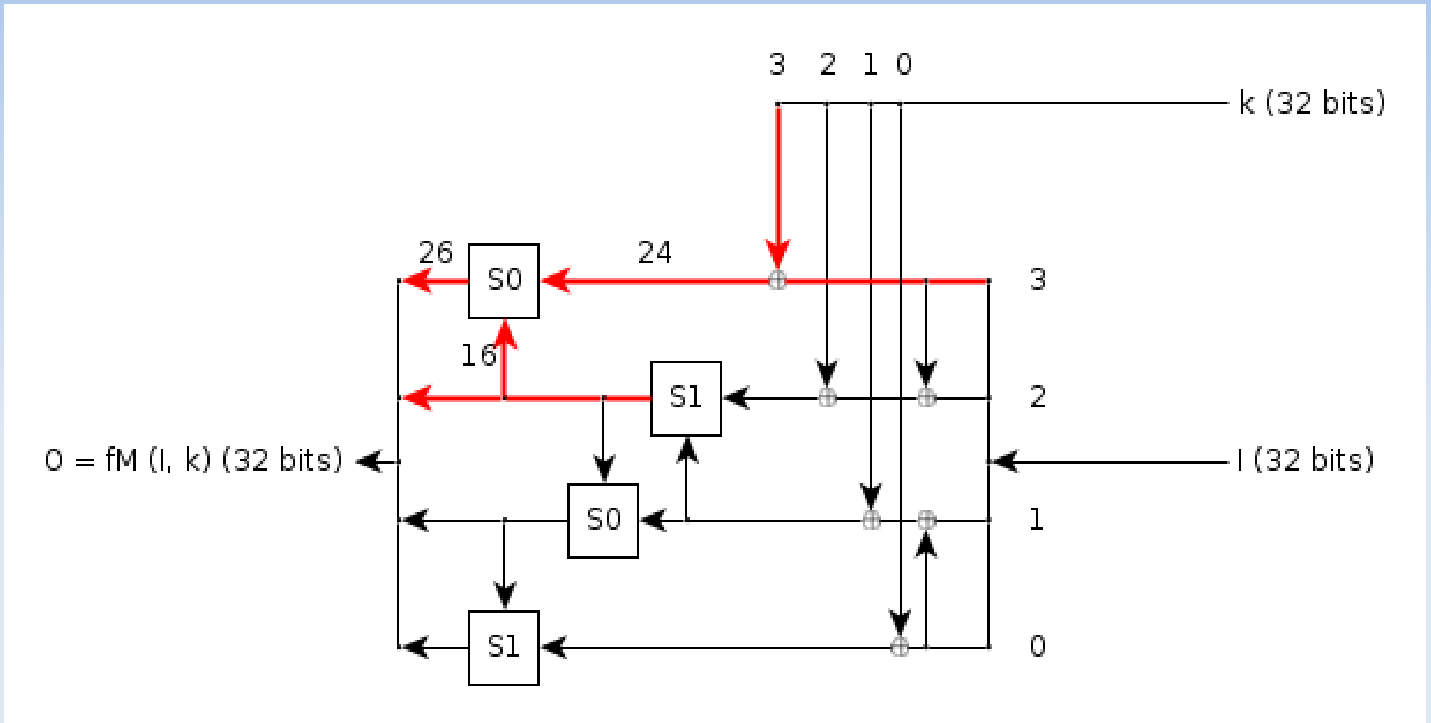
$$= C[i_1, i_2, \dots, i_n] \oplus P[j_1, \dots, j_m] \oplus K[k_1, \dots, k_t] \oplus$$

$$fM(I_1, k_1)[f_1] = 1 \text{ (Or = 0)}$$

Linear Cryptanalysis

- $C[i_1, i_2, \ldots, i_n] \oplus P[j_1, \ldots, j_m] \oplus K[k_1, \ldots, k_t] \oplus$ $fM(I_1, k_1)[f_1] = 1$ (Or $= 0$)
- For fixed k:
- $C[i_1, i_2, \ldots, i_n] \oplus P[j_1, \ldots, j_m] \oplus fM(I_1, k_1)[f_1] =$ const (0 or 1)

Linear approximation of fM



$O[26] = I[24] \oplus K[24] \oplus O[16]$

$\Leftrightarrow O[26,16] = I[24] \oplus K[24]$

Reminder: S0(X, Y) = ROT2((X + Y) mod 256)

$$\begin{array}{r} 101 \\ +\ \ 011 \\ \hline 1000 \end{array}$$

Xor

Linear approximation of fM

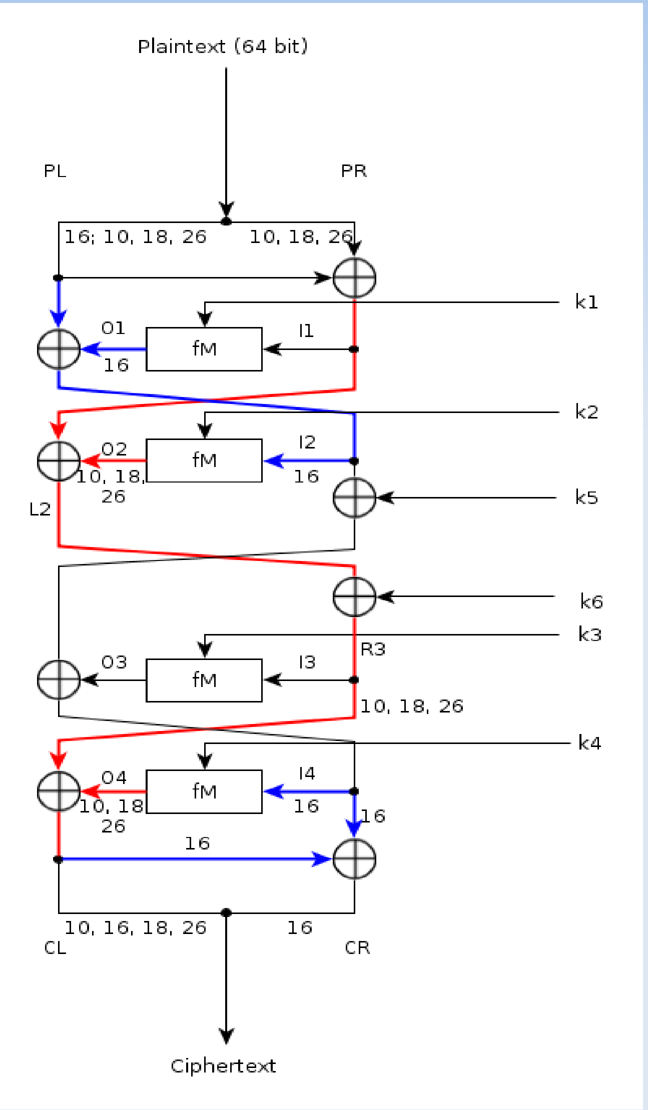
- On a similar way:
  - $O[2,8] = I[0] \oplus K[0] \oplus 1$
  - $O[2,8,10,16] = I[8] \oplus K[0,8] \oplus 1$
  - $O[10, 18, 26] = I[16] \oplus K[16,24] \oplus 1$
  - $O[16,26] = I[24] \oplus K[24]$
- These equations are always true

Linear approximation of FEAL

- $\underline{O[10, 18, 26] = I[16] \oplus K[16,24] \oplus 1}$

- $I_2[16] = fM(PL \oplus PR, k_1)[16] \oplus PL[16]$
- $O_2[10, 18, 26] = k_2[16, 24] \oplus 1$

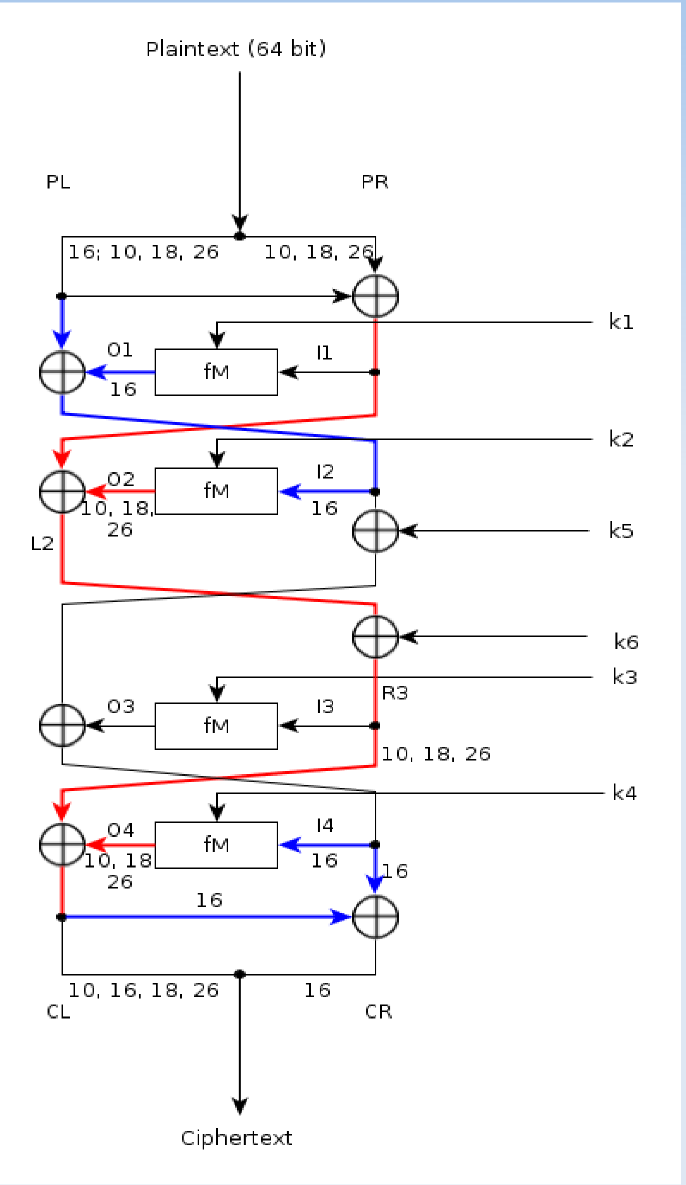
  $\oplus\ fM(PL \oplus PR, k_1)[16] \oplus PL[16]$
- $L_2[10, 18, 26] = PR[10, 18, 26] \oplus PL[10, 18, 26] \oplus O_2[10, 18, 26]$



Linear approximation of FEAL

- $O[10, 18, 26] = I[16] \oplus K[16,24] \oplus 1$
- $L_2[10, 18, 26] = PR[10, 18, 26] \oplus PL[10, 18, 26] \oplus k_2[16, 24] \oplus 1$

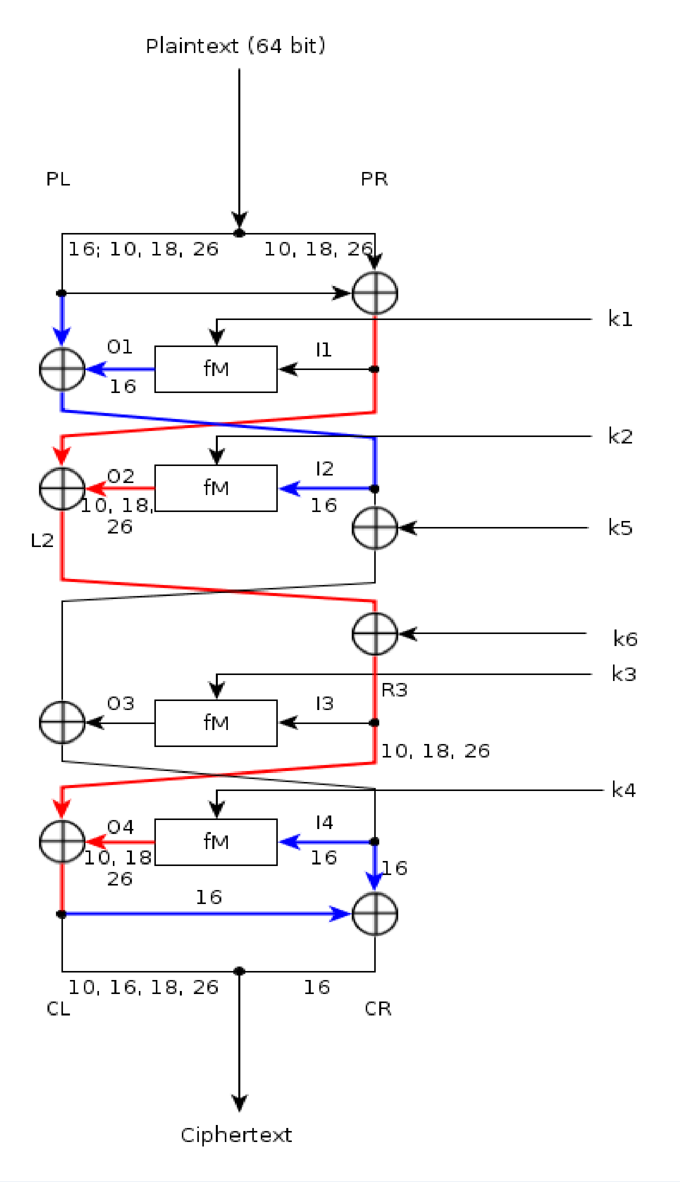
  $\oplus\ fM(PL \oplus PR, k_1)[16] \oplus PL[16]$
- $R_3\,[10, 18, 26] = L_2\,[10, 18, 26] \oplus k_6[10, 18, 26]$



Linear approximation of FEAL

- $O[10, 18, 26] = I[16] \oplus K[16,24] \oplus 1$

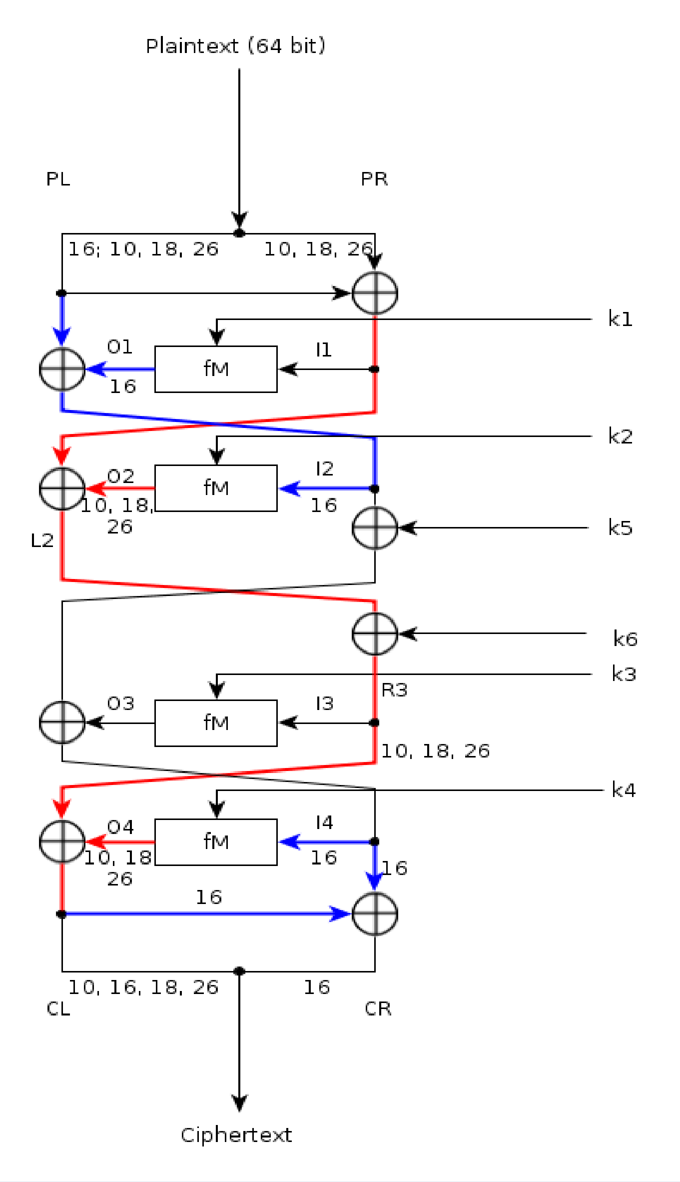
- $I_4[16] = CR[16] \oplus CL[16]$
- $O_4[10, 18, 26] = CR[16] \oplus CL[16] \oplus k_4[16,24] \oplus 1$



Linear approximation of FEAL

- CL[10, 18, 26]

  $= O_4\,[10, 18, 26] \oplus R_3[10, 18, 26]$



Linear approximation of FEAL

- $fM(k_1, PL \oplus PR)[16]$

  $\oplus PL[10, 16, 18, 26] \oplus PR[10, 18, 26]$

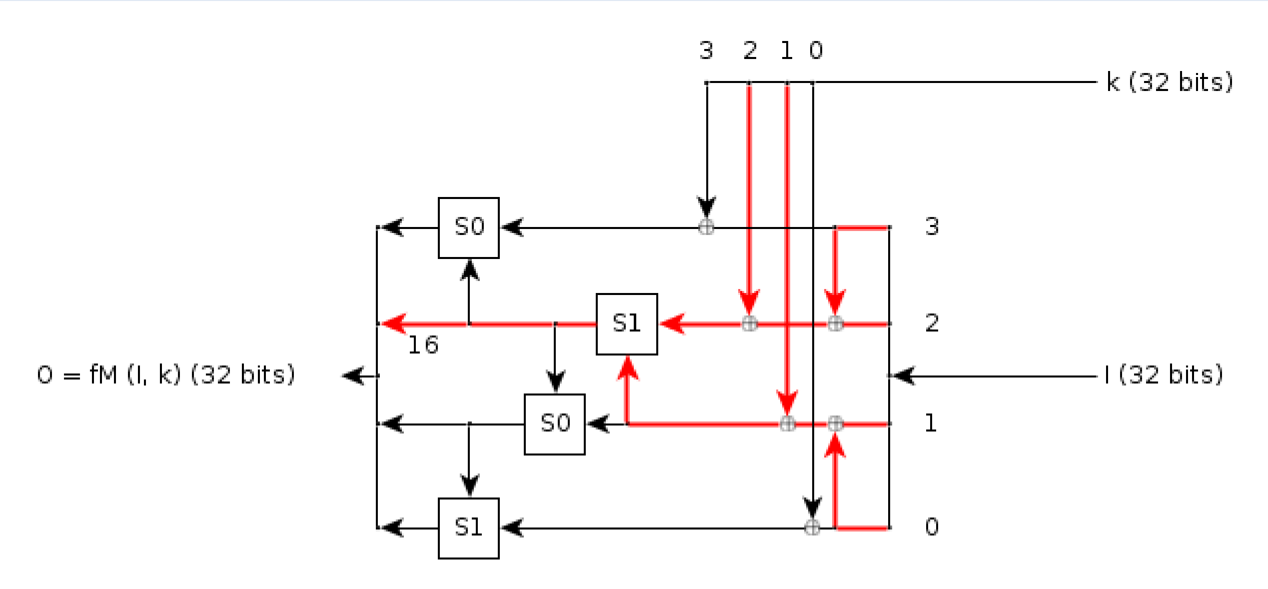
  $\oplus CR[16] \oplus CL[10, 16, 18, 26]$

  $= k_2[16,24] \oplus k_6[10,18,26] \oplus k_4[16, 24]$

  = const (either 1 or 0 for a particular key)

Recover k_1

- $fM(k_1, PL \oplus PR)[16]$
- Determine k_1, such that the previous equation holds
- Max: 2^16 operations. That is in a possible range.

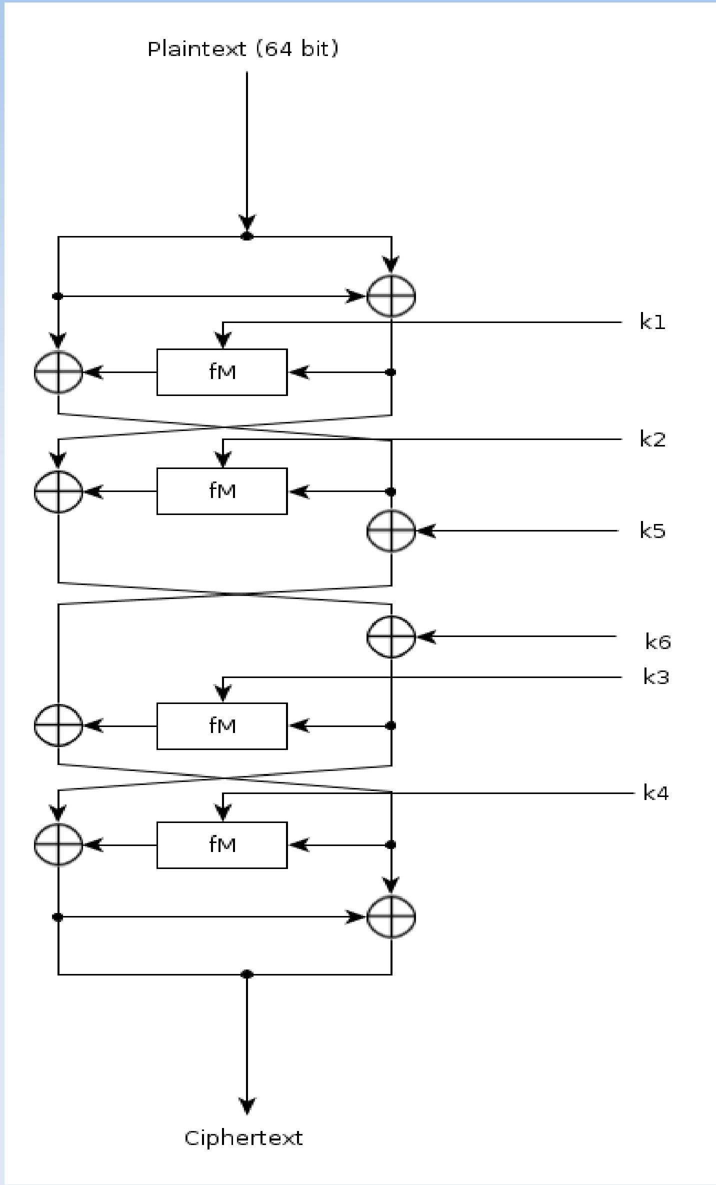


Recover k_1

- Use the other approximations to recover the rest of k_1:
  - $O[2,8] = I[0] \oplus K[0] \oplus 1$
  - $O[2,8,10,16] = I[8] \oplus K[0,8] \oplus 1$
  - $[\ O[10, 18, 26] = I[16] \oplus K[16,24] \oplus 1\ ]$
  - $O[16,26] = I[24] \oplus K[24]$

Recover the other subkeys

- k_2, k_3, k_4 are recovered in an equal way
- k_5, k_6 then follow directly



Runtime of this attack

- Implemented by Matsui & Yamagishi
- with a 25 Mhz computer, 1992

- 2 seconds with 10 known plaintexts
- 350 seconds with 5 known plaintexts

Generalisation to more rounds

- FEAL-8 is breakable with this method
- Using 2^28 plaintexts
- Runtime: 2^50 subkeys are searched.
- Details: Matsui & Yamagishi, 1992, A New Method for Known Plaintext Attack of FEAL cipher

Recapitulation

- FEAL-4
- Modification of FEAL-4
- Linear cryptanalysis
  - Linear equations in f
  - Linear equations in FEAL-4 depending on k_1
  - Exhaustive key search
  - Repeat this for k_2, k_3, ...

Sources

- Shimizu & Miyaguchi: Fast Data Encipherment Algorithm FEAL, 1988

  Advances in Cryptology, EUROCRYPT '87
- Matsui & Yamagishi: A New Method for Known Plaintext Attack of FEAL Cipher, 1993

  Advances in Cryptology – EUROCRYPT '92
- Stamp & Low: Applied Cryptanalysis: Breaking Ciphers in the Real World, 2007