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
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

$S(X, Y, \delta) = \text{ROT2}((X + Y + \delta) \mod 256)$

- Example: ($\delta = 1$)

\[
\begin{array}{c}
00010011 \\
+ 10110011 \\
+ 1 \\
\hline
= 11000111
\end{array}
\]

$\text{Rot2}$

\[
00010011 + 10110011 + 1 = 11000111 \\
\text{Rot2} \\
00011111
\]
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

 Plaintext (64 bit) -> K4, K5, K6, K7

 K0 -> f

 K1 -> f

 K2 -> f

 K3 -> f

 K8, K9, Kα, Kβ -> Ciphertext

 Plaintext (64 bit) -> k1, k2, k3, k4, k5

 fM

 Ciphertext
Rearrangement of FEAL

- Key affects each byte
Rearrangement of FEAL
Rearrangement of FEAL

Plaintext (64 bit)

K4, K5, K6, K7

K0

K1

K2

K3

K8, K9, K8, K6

Ciphertext

0(k0)0 @ K4, K5 @ K5, K7 @ 0(k4l) 0(k5r) 0 @ 0(k6l) 0(k7r) 0

0(k1)0 @ K4, K5 @ 0(k4l) 0(k5r)

K4, K5

K6, K7

K2

K3

(K8, K9, K8, K6)

Ciphertext
Rearrangement of FEAL

Plaintext (64 bit)

\[ \text{Plaintext} \rightarrow f_M \rightarrow k_1 \rightarrow f_M \rightarrow k_2 \rightarrow f_M \rightarrow k_5 \rightarrow f_M \rightarrow k_6 \rightarrow f_M \rightarrow k_3 \rightarrow f_M \rightarrow k_4 \rightarrow \text{Ciphertext} \]
Example: $f_M$
Linear Cryptanalysis

- Known plaintext attack
- Basic idea: Find linear approximations of the cipher:

\[
C[i_1] \oplus C[i_2] \oplus \ldots \oplus C[i_n] \oplus P[j_1] \oplus \ldots \oplus P[j_m] \\
\oplus K[k_1] \oplus \ldots \oplus K[k_t] \oplus fM(I_1, k_1)[f_1] = 1 \text{ (or 0)}
\]

\[
= C[i_1, i_2, \ldots, i_n] \oplus P[j_1, \ldots, j_m] \oplus K[k_1, \ldots, k_t] \oplus fM(I_1, k_1)[f_1] = 1 \text{ (Or = 0)}
\]
Linear Cryptanalysis

- \[ C[i_1, i_2, ..., i_n] \oplus P[j_1, ..., j_m] \oplus K[k_1, ..., k_t] \oplus fM(I_1, k_1)[f_1] = 1 \text{ (Or = 0)} \]

- For fixed \( k \):
  
  \[ C[i_1, i_2, ..., i_n] \oplus P[j_1, ..., j_m] \oplus fM(I_1, k_1)[f_1] = \text{const (0 or 1)} \]
Linear approximation of $f_M$


Reminder: $S0(X, Y) = \text{ROT2}((X + Y) \mod 256)$
On a similar way:

- $O[2,8] = I[0] \oplus K[0] \oplus 1$
- $O[2,8,10,16] = I[8] \oplus K[0,8] \oplus 1$
- $O[10, 18, 26] = I[16] \oplus K[16,24] \oplus 1$

These equations are always true
Linear approximation of FEAL

- \( O_{10, 18, 26} = I_{16} \oplus K_{16, 24} \oplus 1 \)
- \( I_{2_{16}} = f_M(PL \oplus PR, k_1)[16] \oplus PL[16] \)
- \( O_{2_{10, 18, 26}} = k_2[16, 24] \oplus 1 \oplus f_M(PL \oplus PR, k_1)[16] \oplus PL[16] \)
- \( L_{2_{10, 18, 26}} = PR[10, 18, 26] \oplus PL[10, 18, 26] \oplus O_{2_{10, 18, 26}} \)
Linear approximation of FEAL

- \( O[10, 18, 26] = I[16] \oplus K[16,24] \oplus 1 \)
- \( L_2[10, 18, 26] = \text{PR}[10, 18, 26] \oplus \text{PL}[10, 18, 26] \oplus k_2[16, 24] \oplus 1 \oplus fM(\text{PL} \oplus \text{PR}, k_1)[16] \oplus \text{PL}[16] \)
- \( R_3[10, 18, 26] = L_2[10, 18, 26] \oplus k_6[10, 18, 26] \)
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

- $\text{CL}[10, 18, 26] = O_4[10, 18, 26] \oplus R_3[10, 18, 26]$
Linear approximation of FEAL

- \( fM(k_1, \text{PL} \oplus \text{PR})[16] \)
  \( \oplus \text{PL}[10, 16, 18, 26] \oplus \text{PR}[10, 18, 26] \)
  \( \oplus \text{CR}[16] \oplus \text{CL}[10, 16, 18, 26] \)
  \( = k_2[16, 24] \oplus k_6[10, 18, 26] \oplus k_4[16, 24] \)

= const (either 1 or 0 for a particular key)
Recover $k_1$

- $f_M(k_1, PL \oplus PR)[16]$
- 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 $k_1$:
  - $O[2,8] = I[0] \oplus K[0] \oplus 1$
  - $O[2,8,10,16] = I[8] \oplus K[0,8] \oplus 1$
  - $O[10, 18, 26] = I[16] \oplus K[16,24] \oplus 1$
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