FEAL

FEAL

- Fast data Encryption ALgorithm
- Invented, promoted by NTT in 1987
  - Japanese telecommunications monopoly
- Designed as replacement for DES
- And to be fast and efficient
  - With modest security
- Original version (FEAL-4) found to be weak
  - Many "improved" versions followed
  - All are flawed to some degree

FEAL-4

- Here, we consider FEAL-4
- Important in history of cryptanalysis
- Differential crypytanalysis developed to attack FEAL-4
  - Powerful method to analyze block ciphers
- We present differential and linear attacks on FEAL-4

Differential and Linear Attacks

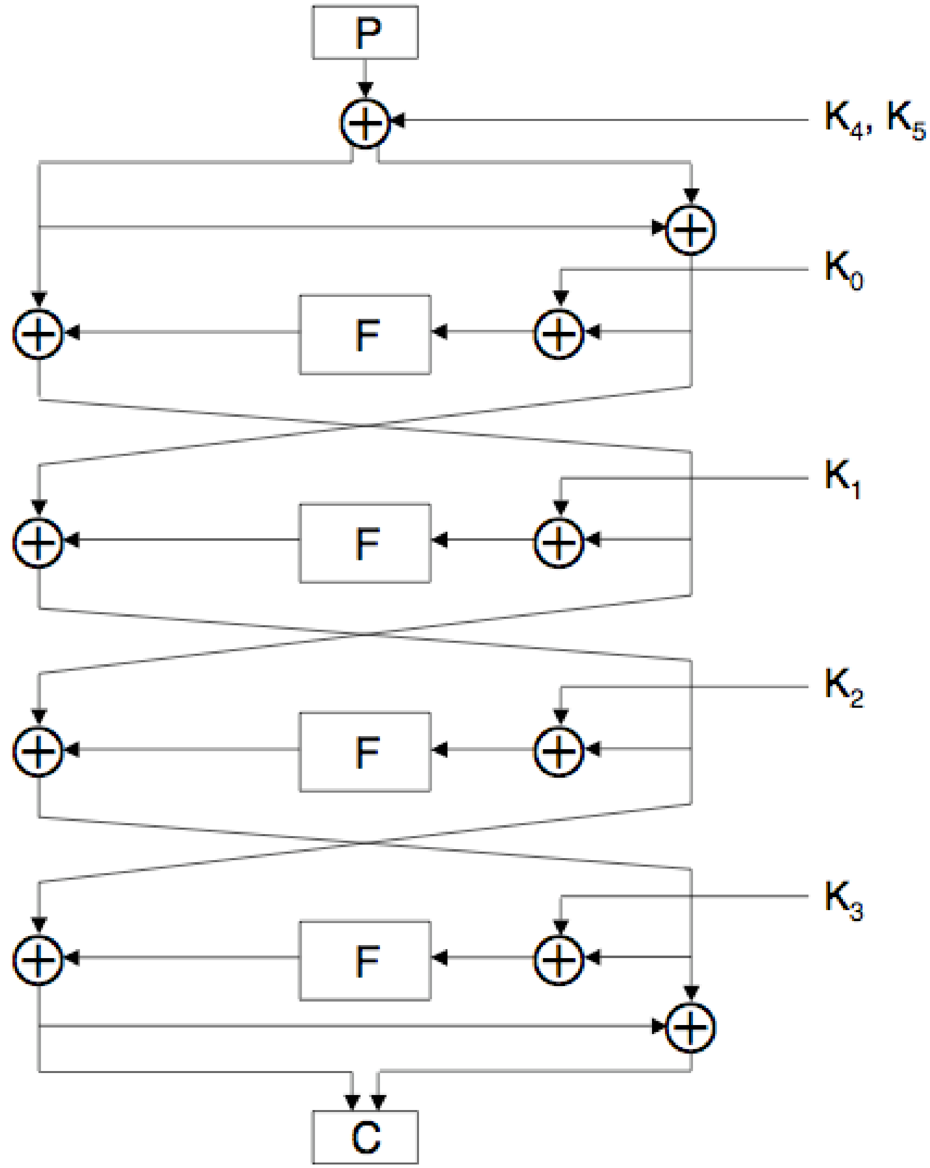
- Differential and linear attacks are usually only of theoretical interest
  - Large chosen (known) plaintext requirement
- FEAL-4 is an exception
- Both differential and linear attacks on FEAL-4 are practical
  - So these attacks fit theme of the book
  - And introduce important cryptanalysis methods

FEAL-4 Cipher

- FEAL-4 is a 4-round Feistel cipher with a 64-bit block and 64-bit key
- Several different (but equivalent) ways to describe the cipher
- 1st description for differential attack
  - 64-bit key → six 32-bit subkeys
  - Round function F maps 32 bits to 32 bits

FEAL-4 Cipher

- Plaintext: P
- Ciphertext: C
- Round function: F
- 32-bit subkeys: $K_0, K_1, \ldots, K_6$
- XOR: $\oplus$
- Very simple cipher!



FEAL-4 Round Function

- Define

  $G_0(a,b) = (a + b \pmod{256}) \lll 2$

  $G_1(a,b) = (a + b + 1 \pmod{256}) \lll 2$

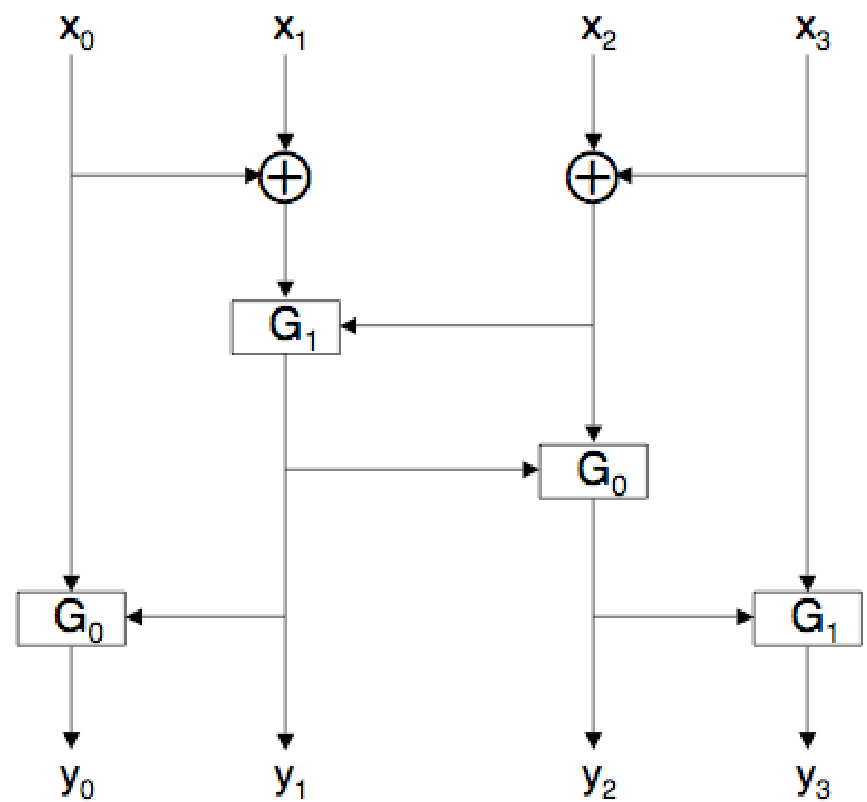
- Where "<<<" is left cyclic shift (rotation)
- Then $F(x_0,x_1,x_2,x_3) = (y_0,y_1,y_2,y_3)$ where

  $y_1 = G_1(x_0 \oplus x_1, x_2 \oplus x_3)$ $\quad$ $y_0 = G_0(x_0, y_1)$

  $y_2 = G_1(y_1, x_2 \oplus x_3)$ $\quad$ $y_3 = G_1(y_2, x_3)$

FEAL-4 Round Function

- Schematic of FEAL-4 round function
  - Note the XORs
- Differential attack: "difference" is XOR
- By considering differences, the cipher is simplified



FEAL-4 Differential Attack

- A **chosen plaintext** attack
- Two plaintexts, specified difference
  - Difference is known as a **characteristic**
- For example if X is the characteristic,

  $P_0 \oplus P_1 = X$
- Note, we can choose P_0 at random and let

  $P_1 = P_0 \oplus X$
- Are there any useful characteristics?

FEAL-4 Differential Attack

- Note: $A_0 \oplus A_1 = 0$ implies $F(A_0) = F(A_1)$
- Easy to show that if

  $A_0 \oplus A_1 = \text{0x80800000}$

  then for round function F we have

  $F(A_0) \oplus F(A_1) = \text{0x02000000}$
- And it holds with probability 1
- Differential attack is based on this

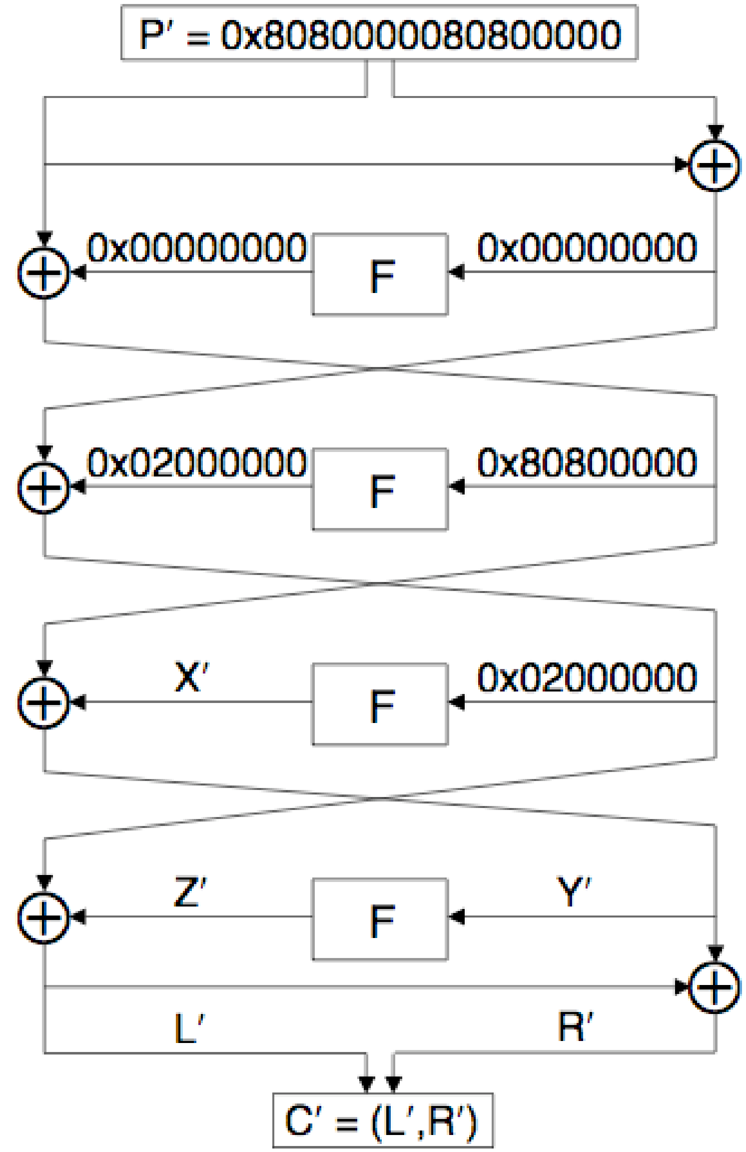
FEAL-4 Differential Attack

- Choose plaintext P_0 and P_1 so that

  $P_0 \oplus P_1 = \text{0x8080000080800000}$
- Given corresponding C_0 and C_1
- Let $P' = P_0 \oplus P_1$ and $C' = C_0 \oplus C_1$
- Consider P' as it passes thru cipher
  - Under "$\oplus$" subkeys drop out of cipher

FEAL-4 Differential Attack

- Characteristic for P′ gets us half way thru
- Can then work backwards from C′
- Try to meet in middle
  - Note L′,R′ are known



FEAL-4 Differential Attack

- We have $L' = \text{0x02000000} \oplus Z'$
- Which give us Z'
- Also, $Y' = \text{0x80800000} \oplus X'$
- Note: For $C = (L,R)$ we have $Y = L \oplus R$
- Now we can solve for subkey K_3
  - Next slide…

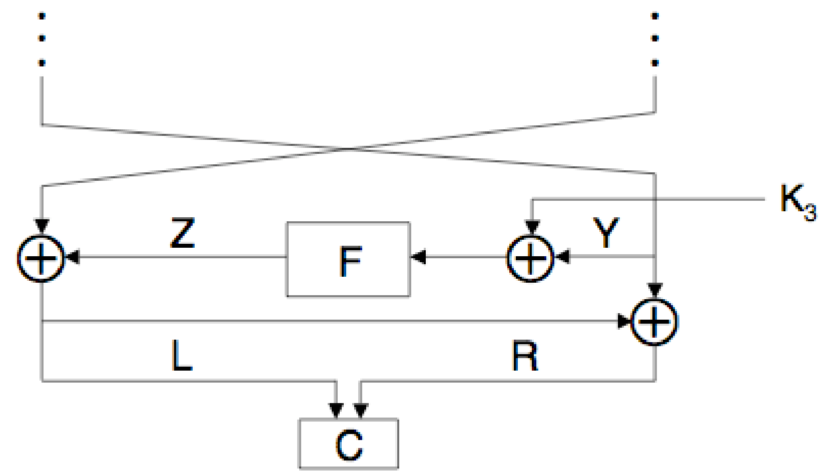
FEAL-4 Differential Attack

- We have

  $Z' = 0x02000000 \oplus L'$

- Compute

  $Y_0 = L_0 \oplus R_0,\ Y_1 = L_1 \oplus R_1$



- Guess K_3 and compute putative Z_0, Z_1
  - Note: $Z_i = F(Y_i \oplus K_3)$
- Compare true Z' to putative Z'

FEAL-4 Differential Attack

- Using 4 chosen plaintext pairs
  - Work is of order 2^{32}
  - Expect one K_3 to survive
- Good divide and conquer strategy
- But it is possible to do better!
  - Can reduce work to about 2^{17}
- Relies on structure of F function
  - See next slide...

FEAL-4 Differential Attack

- For 32-bit word $A=(a_0,a_1,a_2,a_3)$, define $M(A) = (z,\ a_0 \oplus a_1,\ a_2 \oplus a_3,\ z)$ where z is all-zero byte
- For all possible $A=(z,a_0,a_1,z)$, compute $Q_0 = F(M(Y_0) \oplus A)$ and $Q_1 = F(M(Y_1) \oplus A)$
- Can be used to find 16 bits of K_3

FEAL-4 Differential Attack

- For all possible $A=(z,a_0,a_1,z)$, compute

$Q_0 = F(M(Y_0) \oplus A)$ and $Q_1 = F(M(Y_1) \oplus A)$

- When $A = M(K_3)$ by defn of F, we have

  $\langle Q_0 \oplus Q_1 \rangle_{8\ldots23} = \langle Z' \rangle_{8\ldots23}$

  where $\langle X \rangle_{i\ldots j}$ is bits i thru j of X

- Can recover K_3 with about 2^{17} work

FEAL-4 Differential Attack

- Primary for K_3

```
// Characteristic is 0x8080000080800000
```
P_0 = random 64-bit value
$P_1 = P_0 \oplus$ 0x8080000080800000
// Given corresponding ciphertexts
// $C_0 = (L_0, R_0)$ and $C_1 = (L_1, R_1)$
$Y_0 = L_0 \oplus R_0$
$Y_1 = L_1 \oplus R_1$
$L' = L_0 \oplus L_1$
$Z' = L' \oplus$ 0x02000000
for $(a_0, a_1) = (\texttt{0x00}, \texttt{0x00})$ **to** $(\texttt{0xff}, \texttt{0xff})$
    $Q_0 = F(M(Y_0) \oplus (\texttt{0x00}, a_0, a_1, \texttt{0x00}))$
    $Q_1 = F(M(Y_1) \oplus (\texttt{0x00}, a_0, a_1, \texttt{0x00}))$
    if $\langle Q_0 \oplus Q_1 \rangle_{8 \ldots 23} == \langle Z' \rangle_{8 \ldots 23}$ **then**
        Save (a_0, a_1)
    end if
next (a_0, a_1)

- Secondary for K_3

// P_0, P_1, C_0, C_1, Y_0, Y_1, Z' as in primary
// Given list of saved (a_0, a_1) from primary
for each primary survivor (a_0, a_1)
    for $(c_0, c_1) = (\texttt{0x00}, \texttt{0x00})$ **to** $(\texttt{0xff}, \texttt{0xff})$
        $D = (c_0, a_0 \oplus c_0, a_1 \oplus c_1, c_1)$
        $\tilde{Z}_0 = F(Y_0 \oplus D)$
        $\tilde{Z}_1 = F(Y_1 \oplus D)$
        if $\tilde{Z}_0 \oplus \tilde{Z}_1 == Z'$ **then**
            Save D // candidate subkey K_3
        end if
    next (c_0, c_1)
next (a_0, a_1)

- Assuming only one chosen plaintext pair

FEAL-4 Differential Attack

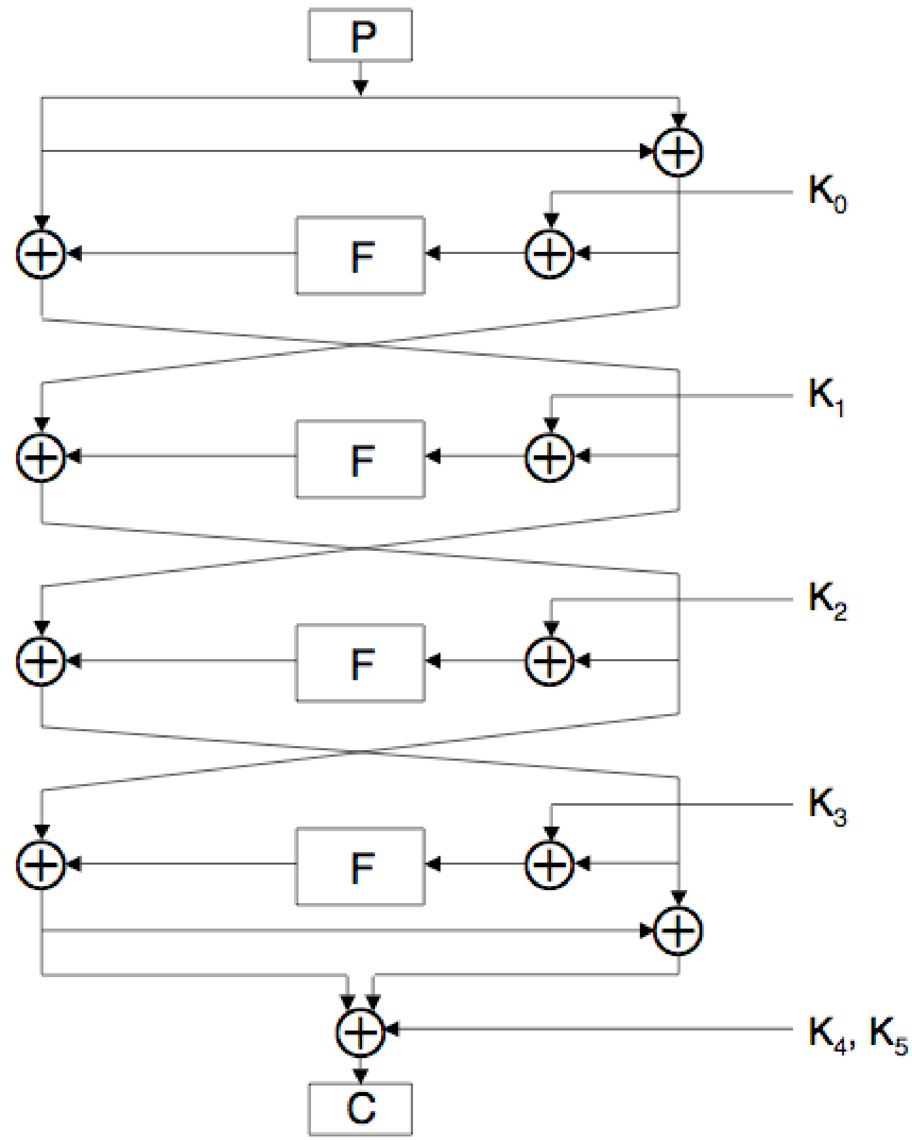
- Once K_3 is known, can successively recover K_2,K_1,K_0 and finally K_4,K_5
  - Attack is similar in each case
  - Some require different characteristics
  - There are a few subtle points
- See the homework problems!

Differential Attacks

- In FEAL-4, differential for K_3 holds with probability 1
- In most differential attacks, probability is small, which
  - Increases chosen plaintext requirement
  - Increases work factor
- Differential cryptanalysis seldom practical
- Usually only a theoretical tool

FEAL-4 Linear Attack

- Consider equivalent form of FEAL-4
- Known plaintext attack…



FEAL-4 Linear Attack

- Let X be 32-bit word, $X = (x_0,x_1,\ldots,x_{31})$
- Define $S_{i,j}(X) = x_i \oplus x_j$ and $S_i(X) = x_i$
  - Also extends to sum of more than 2 bits
- Attack uses fact that for bytes a and b, $S_7(a \oplus b) = S_7(a + b \pmod{256})$
- Recall $G_0(a,b) = (a + b \pmod{256}) \lll 2$, so that $S_5G_0(a,b) = S_7(a \oplus b)$
- Also, $S_5G_1(a,b) = S_7(a \oplus b) \oplus 1$

FEAL-4 Linear Attack

- Have $S_5 G_0(a,b) = S_7(a \oplus b)$
- And $S_5 G_1(a,b) = S_7(a \oplus b) \oplus 1$
- Let Y = F(X), where X,Y are 32-bit words
- Then it can be shown that

$$S_{13}(Y) = S_{7,15,23,31}(X) \oplus 1$$

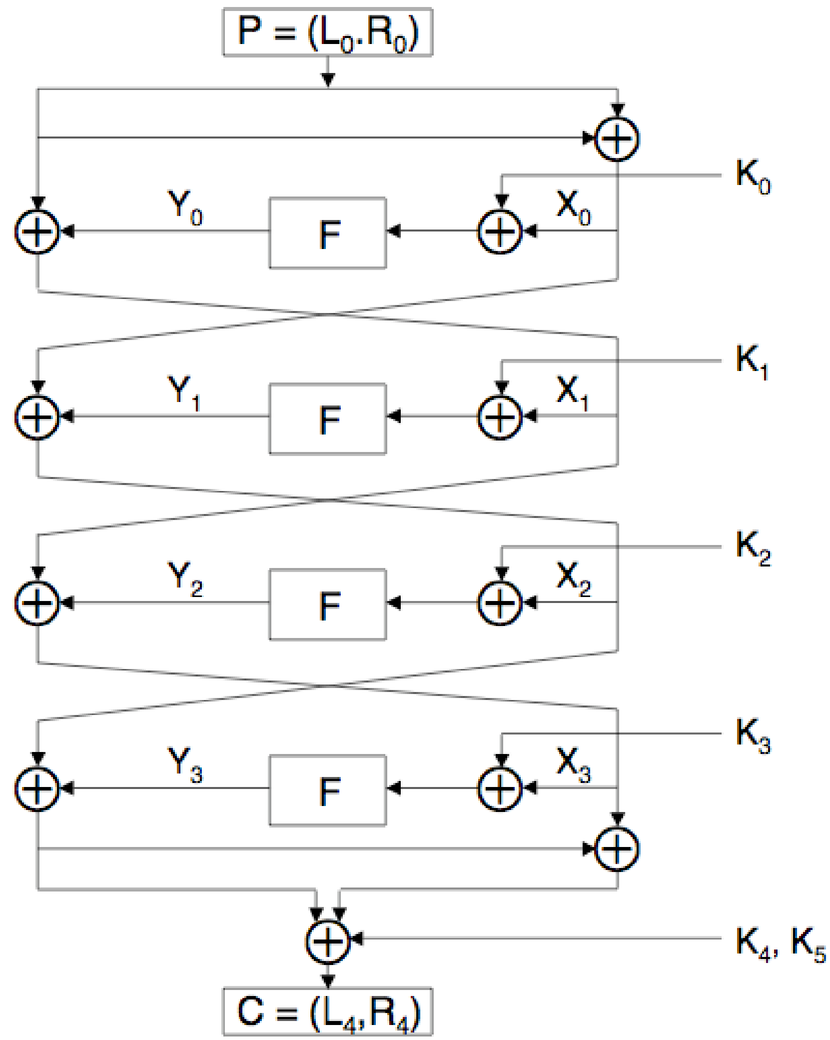
$$S_5(Y) = S_{15}(Y) \oplus S_7(X)$$

$$S_{15}(Y) = S_{21}(Y) \oplus S_{23,31}(X)$$

$$S_{23}(Y) = S_{29}(Y) \oplus S_{31}(X) \oplus 1$$

FEAL-4 Linear Attack

- Label FEAL-4 intermediate steps
- Use formulas on previous slide…



FEAL-4 Linear Attack

- It can be shown that

  $$a = S_{23,29}(L_0 \oplus R_0 \oplus L_4) \oplus S_{31}(L_0 \oplus L_4 \oplus R_4) \oplus S_{31}F(L_0 \oplus R_0 \oplus K_0)$$

- Where $a = S_{31}(K_1 \oplus K_3 \oplus K_4 \oplus K_5) \oplus S_{23,29}(K_4)$
- Treat a as unknown, but constant
- Exhaust over all choices for K_0
  - Test all known plaintext/ciphertext pairs
  - If a is not constant, putative K_0 is incorrect

FEAL-4 Linear Attack

- Linear attack to find K_0

// Given (plaintext,ciphertext) pairs (P_i, C_i), $i = 0, 1, 2, \ldots, n-1$
for $K = 0$ **to** $2^{32} - 1$ // putative K_0
    count[0] = count[1] = 0
    for $i = 0$ **to** $n - 1$
        j = bit computed in right-hand-side of (4.37)
        count[j] = count[j] + 1
    next i
    if count[0] == n **or** count[1] == n **then**
        Save K // candidate for K_0
    end if
next K

FEAL-4 Linear Attack

- Possible to improve on linear attack of previous slide
  - Exhaust for 12 bits of K_0 first, then…
  - Work is much less than 2^{32} (see text)
- Can extend this attack to recover other subkeys

Confusion and Diffusion

- Modern block ciphers employ both confusion and diffusion
- FEAL-4 is a Feistel cipher
  - With round function $F(X \oplus K_i)$
  - Diffusion: shift bytes in F and bits in G_0, G_1
  - Confusion: XOR of K_i and addition
- FEAL-4: diffusion and confusion are weak

FEAL-4 Conclusion

- Weak block cipher
- Important in modern cryptanalysis
  - Many variants in FEAL cipher family
  - All broken
- Differential cryptanalysis developed for FEAL
- Good example to illustrate both linear and differential attacks

Linear and Differential Attacks

- Important tools to analyze ciphers
  - Used in block cipher design
- Seldom practical methods of attack for block ciphers
- Will see again with hash functions
  - In particular, differential attacks