Linear Cryptanalysis of the FEAL-4 Cipher

Gokul Krishna Shrikanth
23266327

FEAL (Fast Data Encipherment Algorithm) is a symmetric key block cipher designed by Akihiro Shimizu and Shoji Miyaguchi in the late 1980s. Linear cryptanalysis is a technique used to analyse the behaviour of a cryptographic algorithm based on linear approximations.

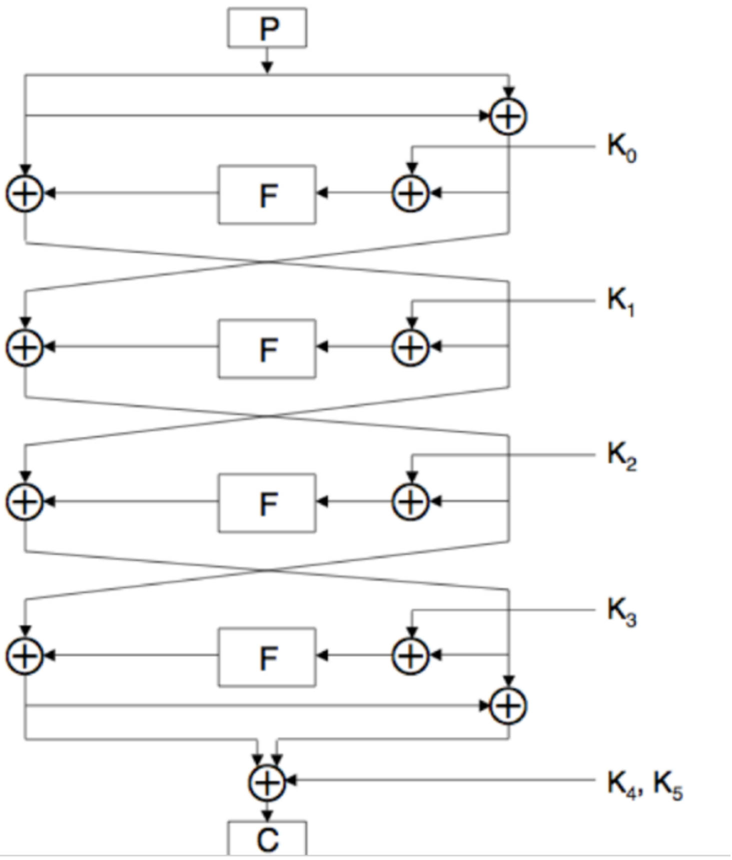
In linear cryptanalysis, the attacker tries to find linear relationships between the plaintext, ciphertext, and key bits. These linear approximations can then be used to derive information about the key by selecting linear expressions and verifying statistical biases in the behaviour of the algorithm.

The equations we can derive from the FEAL 4 cipher can be used to find the keys

X0 xor Y1 xor Y3 = K4 xor L4

L0 xor Y0 xor Y2 xor L4 xor K4 = K5 xor R4

We can compute only the 12 bits instead of the full 32 bits



From this above illustration, We can derive

We also define $S_{i,j,...}(X)$ to be the XOR of bits $i, j, ..$ of X, so $S_{i,j,...}(X) = x_i \oplus x_j \oplus \ldots$

And also from the lecture notes we can get the G0 and G1 relationships

Recall that G_0 and G_1 are defined as follows:

$$G_0(a,b) = (a+b \pmod{256}) <<< 2$$
$$G_1(a,b) = (a+b+1 \pmod{256}) <<< 2$$

So the following relationships hold:

- $S_5(G_0(a,b)) = S_7(a \oplus b)$
- $S_5(G_1(a,b)) = S_7(a \oplus b) \oplus 1$

Let X be the 32-bit input to the round function F, and Y be the 32-bit output, so $Y = F(X)$. We can then show that the following relationships hold:

1. $S_{13}(Y) = S_{7,15,23,31}(X) \oplus 1$
2. $S_{5,15}(Y) = S_7(X)$
3. $S_{15,21}(Y) = S_{23,31}(X)$
4. $S_{23,29}(Y) = S_{31}(X) \oplus 1$

The following relationships that we can derive are

S13(Y) = S7,15(X) xor S23,31(X) xor 1
S5(Y) = S15(Y) xor S7(X)
S15(Y) = S21(Y) xor S23,31(X) xor 1
S23(Y) = S29(Y) xor S31(X) xor 1

With the following relations and the formulas we can solve the keys, We will now see how to find the keys K0 to K5

Solving K0:
Since L4 = X0 xor Y1 xor Y3 xor K4 we can get
S23,24(L4) = S23,29(X0) xor S23,29(Y1) xor S23,29(Y3) xor S23,39(K4)
S23,29(X0) = S23,29(L0 xor R0)
S23,29(Y1) = S31(K1) xor S31(Y0) xor S31(L0) xor 1

S31(Y0) = S31 F(L0 xor R0 xor K0)

S23,29(L4) = S23,29(L0 xor R0 xor L4) xor S31(L4 xor R4 xor L0) xor S31 F(L0 xor R0 xor K0)

S13(L4 = S13(X0) xor S13(Y1) xor S13(Y3) xor S13(K4)

S13(X0) = S13(L0 xor R0)

S13(Y3) = S7,15,23,31(L4 xor R4) xor S7,15,23,31(K4 xor K5 xor K3) xor 1

S13(Y1) = S7,15,23,31(K1) xor S7,15,23,31(Y0) xor S7,15,23,31(L0) xor 1

S7,15,23,31(Y0) = S13(L0 xorR0 xorL4) xor S7,15,23,31(L0 xorL4 xorR4) xor S7,15,23,31 F(L0 xorR0 xorK0)

S5,15(L4) = S5,15 (X0) xor S5,15(Y1) xor S5,15(Y3) xor S5,15(K4)

S5,15(X0 = S5,15(L0 xor R0)

S5,15(Y3) = S7(L4 xor R4) xor S7(K4 xor K5 xor K3) xor 1

S5,15(Y1) = S7(K1) xor S7(Y0) xor S7(L0) xor 1

S7(Y0) = S7 F(L0 xor R0 xor K0) = S5,15(L0 xor R0 xor L4) xor S7(L0 xor L4 xor R4) xor S7 F(L0 xor R0 xor K0)

S15,21(L4) = S15,21(X0) xor S15,21(Y1) xor S15,21(Y3) xor S15,21(K4)

S15,21(X0) = S15,21(L0 xor R0)

S15,21(Y3) = S23,31(L4 xor R4) xor S23,31(K4 xor K5 xor K3) xor 1

S15,21(Y1) = S23,31(K1) xor S23,31(Y0) xor S23,31(L0) xor 1

S23,31(Y0) = S23,31 F(L0 xor R0 xor K0)
= S15,21(L0 xor R0 xor L4) xor S23,31(L0 xor L4 xor R4) xor S23,31 F(L0 xor R0 xor K0)

constant1 = S23,29(L0 xor R0 xor L4) xor S31(L4 xor R4 xor L0) xor S31 F(L0 xor R0 xor K0)
constant2 = S13(L0 xor R0 xor L4) xor S7,15,23,31(L0 xor L4 xor R4) xor S7,15,23,31 F(L0 xor R0 xor K0)
constant3 = S5,15(L0 xor R0 xor L4) xor S7(L0 xor L4 xor R4) xor S7 F(L0 xor R0 xor K0)

constant4 = S15,21(L0 xor R0 xor L4) xor S23,31(L0 xor L4 xor R4) xor S23,31 F(L0 xor R0 xor K0)

From the above we can derive

S5,13,21(L0 xor R0 xor L4) xor S15(L0 xor L4 xor R4) xor S15 F(L0 xor R0 xor K0)

We first generate all the combinations of the 12 bit keys and then we calculate the value for every text pair to find K0

Solving K1:
After solving K0, we know that L0 xor Y0 xor Y2 xor L4 xor K4 = K5 xor R4 , From that we get these constant equations:
S23,29(R4) = S23,29(L0) xor S23,29(Y0) xor S23,29(Y2) xor S23,29(L4) xor S23,29(K4) xor S23,29(K5)

S23,29(Y2) = S31(L0 xor R0) xor S31(Y1) xor S31(K2) xor 1
S31(Y1) = S31 F(L0 xor F(L0 xor R0 xor K0) xor K1)
S23,29(Y0) = S31(L0) xor S31(R0) xor S31(K0) xor 1

S23,29(L0 xor L4 xor R4) xor S31 F(L0 xor F(L0 xor R0 xor K0) xor K1)

Solving them gives us the constant eq:
constant1 = S23,29(L0 xor L4 xor R4) xor S31 F(L0 xor F(L0 xor R0 xor K0) xor K1)
constant2 = S13(L0 xor L4 xor R4) xor S7,15,23,31 F(L0 xor F(L0 xor R0 xor K0) xor K1)
constant3 = S5,15(L0 xor L4 xor R4) xor S7 F(L0 xor F(L0 xor R0 xor K0) xor K1)
constant4 = S15,21(L0 xor L4 xor R4) xor S23,31 F(L0 xor F(L0 xor R0 xor K0) xor K1)
From these we can get

S5,13,21(L0 xor L4 xor R4) xor S15 F(L0 xor F(L0 xor R0 xor K0) xor K1)
We calculate K1 from S13(L0 xor L4 xor R4) xor S7,15,23,31 F(L0 xor F(L0 xor R0 xor K0) xor K1)

Solving K2:

Here we can use the formula
L4 = X0 xor Y1 xor Y3 xor K4
S23,29(L4) = S23,29(X0) xor S23,29(Y1) xor S23,29(Y3) xor S23,29(K4)

S23,29(Y3) = S31 F(L0 xor R0 xor F(L0 xor Y0 xor K1) xor K2) xor S31(L0 xor F(L0 xor R0 xor K0)) xor S31(K3) xor 1

We can derive that
S23,29(L0 xor R0xor L4) xor S31 F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2)

Finding the constants for K2

constant1 = S23,29(L0 xor R0xor L4) xor S31 F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2)
constant2 = S13(L0 xor R0xor L4) xor S7,15,23,31 F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2)
constant3 = S5,15(L0 xor R0xor L4) xor S7 F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2)
constant4 = S15,21(L0 xor R0xor L4) xor S23,31 F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2)
Form the above constant equations we can get
S5,13,21(L0 xor R0xor L4) xor S15 F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2)
With which we can repeat the same process by generating all the combinations 12 bits and finding the possible key.

Solving K3:
We use this formula
L0 xor Y0 xor Y2 xor L4 xor K4 = K5 xor R4, and take Y2
Y2 = F(L4 xor K4 xor Y3 xor K2)

S23,29(L0 xor L4 xor R4) xor S23,29(Y0) xor S23,29(Y2) xor S23,29(K4) xor S23,29(K5)
= S23,29(L0 xor L4 xor R4) xor S23,29(Y0) xor S31(L4) xor S31(Y3) xor 1
S23,29(Y0) = S31(L0) xor S31(R0) xor S31(K0) xor 1

S31(Y3) = S31 F(L0 xor F(L0 xor R0 xor K0) xor F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2) xor K3)
= S23,29(L0 xor L4 xor R4) xor S31(L0 xor R0 xor L4) xor S31 F(L0 xor F(L0 xor R0 xor K0) xor F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2) xor K3)

Calculating the constants
constant1 = S23,29(L0 xor L4 xor R4) xor S31(L0 xor R0 xor L4) xor S31 F(L0 xor F(L0 xor R0 xor K0) xor F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2) xor K3)
constant2 = S13(L0 xor L4 xor R4) xor S7,15,23,31(L0 xor R0 xor L4) xor S7,15,23,31 F(L0 xor F(L0 xor R0 xor K0) xor F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2) xor K3)

constant3 = S5,15(L0 xor L4 xor R4) xor S7(L0 xor R0 xor L4) xor S7 F(L0 xor F(L0 xor R0 xor K0) xor F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2) xor K3)

constant4 = S15,21(L0 xor L4 xor R4) xor S23,31(L0 xor R0 xor L4) xor S23,31 F(L0 xor F(L0 xor R0 xor K0) xor F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2) xor K3)
We get,

S5,13,21(L0 xor L4 xor R4) xor S15(L0 xor R0 xor L4) xor S15 F(L0 xor F(L0 xor R0 xor K0) xor F(L0 xor R0 xor F(L0 xor F(L0 xor R0 xor K0) xor K1) xor K2) xor K3)

Since we have found K0, K1, K2 and K3. We can get K4 and K5 easily from the relations

K4 = L0 xor R0 xor Y1 xor Y3 xor L4
K5 = L0 xor R0 xor Y1 xor Y3 xor L0 xor Y0 xor Y2 xor R4

Finally we have to check the keys, We can do that from the code shared where it has a method decrypt().

The 256 Valid Key Combinations:
In the file result.txt

0x65454c49	0x6fd87b73	0x76558e59	0x1c339c15	0x4e673d7e	0xfe0fb8a4
0x65454c49	0x6fd87b73	0x76558e59	0x1c331c95	0x4e673d7c	0xfe0fb8a6
0x65454c49	0x6fd87b73	0x76558e59	0x9cb39c15	0x4c673d7e	0xfc0fb8a4
0x65454c49	0x6fd87b73	0x76558e59	0x9cb31c95	0x4c673d7c	0xfc0fb8a6
0x65454c49	0x6fd87b73	0x76550ed9	0x1c339c17	0x4e673d7e	0xfe0fb8a6
0x65454c49	0x6fd87b73	0x76550ed9	0x1c331c97	0x4e673d7c	0xfe0fb8a4
0x65454c49	0x6fd87b73	0x76550ed9	0x9cb39c17	0x4c673d7e	0xfc0fb8a6
0x65454c49	0x6fd87b73	0x76550ed9	0x9cb31c97	0x4c673d7c	0xfc0fb8a4
0x65454c49	0x6fd87b73	0xf6d58e59	0x1e339c15	0x4e673d7e	0xfc0fb8a4
0x65454c49	0x6fd87b73	0xf6d58e59	0x1e331c95	0x4e673d7c	0xfc0fb8a6
0x65454c49	0x6fd87b73	0xf6d58e59	0x9eb39c15	0x4c673d7e	0xfe0fb8a4
0x65454c49	0x6fd87b73	0xf6d58e59	0x9eb31c95	0x4c673d7c	0xfe0fb8a6
0x65454c49	0x6fd87b73	0xf6d50ed9	0x1e339c17	0x4e673d7e	0xfc0fb8a6
0x65454c49	0x6fd87b73	0xf6d50ed9	0x1e331c97	0x4e673d7c	0xfc0fb8a4
0x65454c49	0x6fd87b73	0xf6d50ed9	0x9eb39c17	0x4c673d7e	0xfe0fb8a6
0x65454c49	0x6fd87b73	0xf6d50ed9	0x9eb31c97	0x4c673d7c	0xfe0fb8a4
0x65454c49	0x6fd8fbf3	0x76558e5b	0x1c339c15	0x4e673d7c	0xfe0fb8a6
0x65454c49	0x6fd8fbf3	0x76558e5b	0x1c331c95	0x4e673d7e	0xfe0fb8a4

…… etc