FEAL-4 Basic Differential Attack

- If $A_0 \oplus A_1 = 0$ then $F(A_0) = F(A_1)$, p=1.
- If $A_0 \oplus A_1$= 0x80800000 then $F(A_0) \oplus F(A_1)$= 0x02000000, p=1
- Choose (P_0, P_1):
- $P_0 \oplus P_1$=0x8080000080800000
- P'= $P_0 \oplus P_1$, C'=$C_0 \oplus C_1$
- L'=0x02000000$\oplus$Z', Y'=0x80800000 $\oplus$ X'
- For C= (L,R) we have Y = L$\oplus$R
- Solve for sub-key K_3: Z'= 0x02000000$\oplus$L'
- Compute $Y_0 = L_0 \oplus R_0$, $Y_1 = L_1 \oplus R_1$
- Guess K_3 and compute guessed Z_0, Z_1
  - Note: $Z_i = F(Y_i \oplus K_3)$
- Compare true Z' to guessed Z'