Two obvious relations:

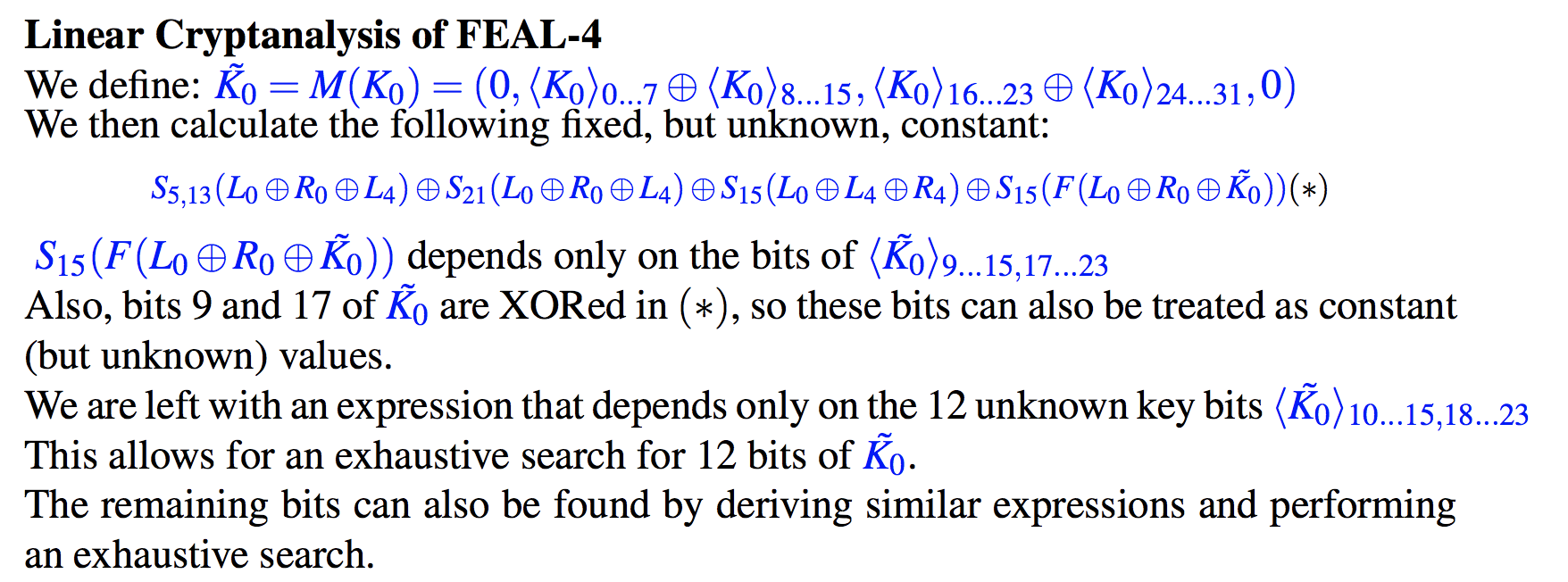
1:

X0 ⊕ Y1 ⊕ Y3 = K4 ⊕ L4

2:

L0 ⊕ Y0 ⊕ Y2 ⊕ L4 ⊕ K4 = K5 ⊕ R4

Attack k~:



Generate all possible 12 bit keys with bits at 10..15 && 18…23, 2^12 = 4096 different keys.

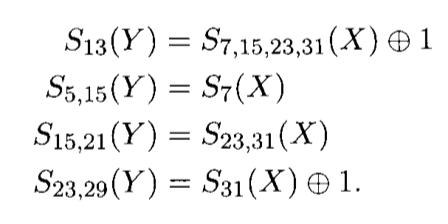
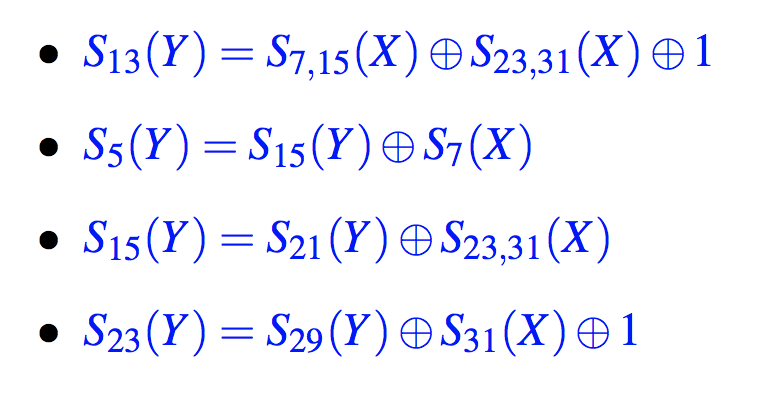
Calculate value from (\*), if it stays the same every time then save key as a candidate k~

Rather than iterating over all the key pairs for each key, it’s obvious we only need to keep track of the result of (\*) from the first try as we’re defining candidate keys as keys for which that result is a constant. If the result of calculating (\*) for key i not equal to result of (\*) with k i=1 then we can just move on to the next

If we reach the last pair and the result of (\*) holds, then add key to candidateKeys.

Attack k: calculat

Fig 2



Using relation 1 and the above : L4 = X0 ⊕ Y1 ⊕ Y3 ⊕ K4

S23,29(Y) = S31(X) ⊕ 1

**S23,29(L4) = S23,29(X0) ⊕ S23,29(Y1) ⊕ S23,29(Y3) ⊕ S23,29(K4)**

S23,29(X0) = S23,29(L0 ⊕ R0)

S23,29(Y1) = S23,29 **F**(X1 ⊕ K1)

= S23,29 **F**(L0 ⊕ Y0 ⊕ K1)

= S31(K1) ⊕ S31(Y0) ⊕ S31(L0) ⊕ 1

S31(Y0) = S31 **F**(X0 ⊕ K0)

= S31 **F**(L0 ⊕ R0 ⊕ K0)

S23,29(Y3) = S31(X3 ⊕ K3) ⊕ 1

= S31(L4 ⊕ K4 ⊕ R4 ⊕ K5 ⊕ K3) ⊕ 1

= S31(L4 ⊕ R4) ⊕ S31(K4 ⊕ K5 ⊕ K3) ⊕ 1

S23,29(L4) = S23,29(L0 ⊕ R0) ⊕ S31(K1) ⊕ S31 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S31(L0) ⊕ 1 ⊕ S31(L4 ⊕ R4) ⊕ S31(K4 ⊕ K5 ⊕ K3) ⊕ 1 ⊕ S23,29(K4)

= S23,29(L4) ⊕ S23,29(L0 ⊕ R0) ⊕ S31 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S31(L0) ⊕ 1 ⊕ S31(L4 ⊕ R4) ⊕ 1

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

**S13(L4) = S13(X0) ⊕ S13(Y1) ⊕ S13(Y3) ⊕ S13(K4)**

S13(X0) = S13(L0 ⊕ R0)

S13(Y3) = S7,15,23,31(X) ⊕ 1

= S7,15,23,31(L4 ⊕ K4 ⊕ R4 ⊕ K5 ⊕ K3) ⊕ 1

= S7,15,23,31(L4 ⊕ R4) ⊕ S7,15,23,31(K4 ⊕ K5 ⊕ K3) ⊕ 1

S13(Y1) = S13 **F**(X1 ⊕ K1)

= S13 **F**(L0 ⊕ Y0 ⊕ K1)

= S7,15,23,31(K1) ⊕ S7,15,23,31(Y0) ⊕ S7,15,23,31(L0) ⊕ 1

S7,15,23,31(Y0) = S7,15,23,31 **F**(X0 ⊕ K0)

= S7,15,23,31 **F**(L0 ⊕ R0 ⊕ K0)

**= S13(L0 ⊕R0 ⊕L4) ⊕ S7,15,23,31(L0 ⊕L4 ⊕R4) ⊕ S7,15,23,31 F(L0 ⊕R0 ⊕K0)**

**S5,15(L4) = S5,15 (X0) ⊕ S5,15(Y1) ⊕ S5,15(Y3) ⊕ S5,15(K4)**

S5,15(X0) = S5,15(L0 ⊕ R0)

S5,15(Y3) = S7(X) ⊕ 1

= S7(L4 ⊕ K4 ⊕ R4 ⊕ K5 ⊕ K3) ⊕ 1

= S7(L4 ⊕ R4) ⊕ S7(K4 ⊕ K5 ⊕ K3) ⊕ 1

S5,15(Y1) = S5,15 **F**(X1 ⊕ K1)

= S5,15 **F**(L0 ⊕ Y0 ⊕ K1)

= S7(K1) ⊕ S7(Y0) ⊕ S7(L0) ⊕ 1

S7(Y0) = S7 **F**(X0 ⊕ K0)

= S7 **F**(L0 ⊕ R0 ⊕ K0)

**= S5,15(L0 ⊕R0 ⊕L4) ⊕ S7(L0 ⊕L4 ⊕R4) ⊕ S7 F(L0 ⊕R0 ⊕K0)**

**S15,21(L4) = S15,21(X0) ⊕ S15,21(Y1) ⊕ S15,21(Y3) ⊕ S15,21(K4)**

S15,21(X0) = S15,21(L0 ⊕ R0)

S15,21(Y3) = S23,31(X) ⊕ 1

= S23,31(L4 ⊕ K4 ⊕ R4 ⊕ K5 ⊕ K3) ⊕ 1

= S23,31(L4 ⊕ R4) ⊕ S23,31(K4 ⊕ K5 ⊕ K3) ⊕ 1

S15,21(Y1) = S15,21 **F**(X1 ⊕ K1)

= S15,21 **F**(L0 ⊕ Y0 ⊕ K1)

= S23,31(K1) ⊕ S23,31(Y0) ⊕ S23,31(L0) ⊕ 1

S23,31(Y0) = S23,31 **F**(X0 ⊕ K0)

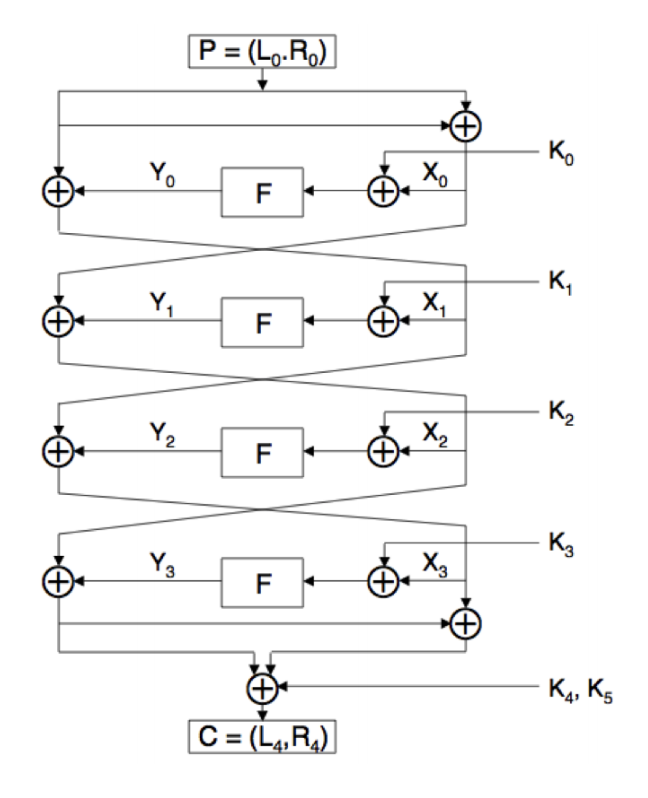
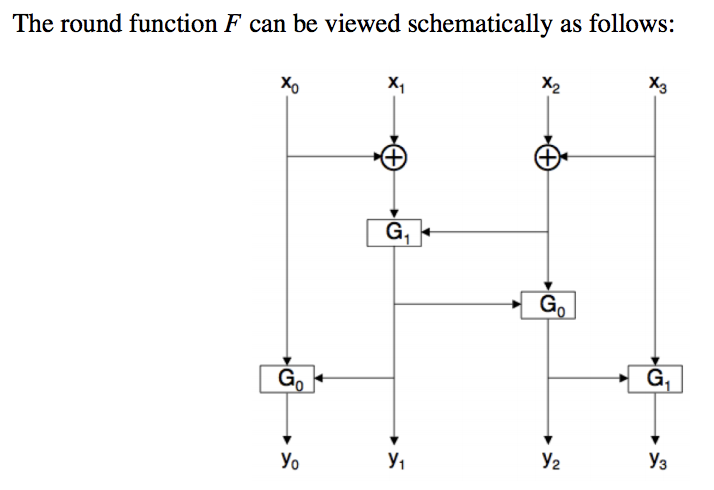
= S23,31 **F**(L0 ⊕ R0 ⊕ K0)

**= S15,21(L0 ⊕R0 ⊕L4) ⊕ S23,31(L0 ⊕L4 ⊕R4) ⊕ S23,31 F(L0 ⊕R0 ⊕K0)**

Could have constructed other constants from Fig 2, including the one shown in the lecture notes and used a combination to find k0, but the one I choose depends on all the bits the other would put together so for simplicity purposes I decided to this one as it will give the same result.

Search the remaining 20 bits, 2^20 = 1048576

Attack k1~:

Using relation 1 and the above : L4 = X0 ⊕ Y1 ⊕ Y3 ⊕ K4

R4 = L0 ⊕ Y0 ⊕ Y2 ⊕ X2 ⊕ Y3 ⊕ K5

X2 ⊕ Y3 = L4 ⊕ K4

R4 = L0 ⊕ Y0 ⊕ Y2 ⊕ L4 ⊕ K4 ⊕ K5

S5(Y) = S15(Y)⊕S7(X) **= S5,15(L0 ⊕R0 ⊕L4) ⊕ S7(L0 ⊕L4 ⊕R4) ⊕ S7 F(L0 ⊕R0 ⊕K0)**

­­­­

S13(Y) = S7,15(X)⊕S23,31(X)⊕1 **= S13(L0 ⊕R0 ⊕L4) ⊕ S7,15,23,31(L0 ⊕L4 ⊕R4) ⊕ S7,15,23,31 F(L0 ⊕R0 ⊕K0)**

S15(Y) = S21(Y)⊕S23,31(X) **= S15,21(L0 ⊕R0 ⊕L4) ⊕ S23,31(L0 ⊕L4 ⊕R4) ⊕ S23,31 F(L0 ⊕R0 ⊕K0)**

­

S23(Y) = S29(Y)⊕S31(X)⊕1 **= S23,29(L0 ⊕ R0 ⊕ L4) ⊕ S31(L4 ⊕ R4 ⊕ L0) ⊕ S31 F(L0 ⊕ R0 ⊕ K0)**

L0 ⊕ Y0 ⊕ Y2 ⊕ L4 ⊕ K4 = K5 ⊕ R4

Using relation 2 and the above : R4 = L0 ⊕ Y0 ⊕ Y2 ⊕ L4 ⊕ K4 ⊕ K5

S23,29(Y) = S31(X) ⊕ 1

**S23,29(R4) = S23,29(L0) ⊕ S23,29(Y0) ⊕ S23,29(Y2) ⊕ S23,29(K4) ⊕ S23,29(K5)**

S23,29(Y2) = S23,29 **F**(X2 ⊕ K2)

= S23,29 **F**(X0 ⊕ Y1 ⊕ K2)

= S31(X0) ⊕ S31(Y1) ⊕ S31(K2) ⊕ 1

= S31(L0 ⊕ R0) ⊕ S31(Y1) ⊕ S31(K2) ⊕ 1

= S31(L0 ⊕ R0) ⊕ S31 **F**(X1 ⊕ K1) ⊕ S31(K2) ⊕ 1

= S31(L0 ⊕ R0) ⊕ S31 **F**(L0 ⊕ Y0 ⊕ K1) ⊕ S31(K2) ⊕ 1

= S31(L0 ⊕ R0) ⊕ S31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ S31(K2) ⊕ 1

S23,29(Y0) = S23,29 **F**(X0 ⊕ K0)

= S23,29 **F**(L0 ⊕ R0 ⊕ K0)

**S23,29(L0 ⊕ R4) ⊕** S31(L0 ⊕ R0) **⊕** S23,29 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ 1

**S**5,15 **(L0 ⊕ R4) ⊕** S7(L0 ⊕ R0) **⊕** S5,15 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S7 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ 1

**S**15,21 **(L0 ⊕ R4) ⊕** S23,31(L0 ⊕ R0) **⊕** S15,21 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S23,31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ 1

**S**13 **(L0 ⊕ R4) ⊕** S7,15,23,31 (L0 ⊕ R0) **⊕** S13 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S7,15,23,31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ 1

**S**5,13,21 **(L0 ⊕ R4) ⊕** S15 (L0 ⊕ R0) **⊕** S5,13,21 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S15 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ 1

R4 = L0 ⊕ Y0 ⊕ Y2 ⊕ L4 ⊕ K4 ⊕ K5

**S23,29(R4)** = **S23,29(L0)** ⊕ **S23,29(**Y0) ⊕ **S23,29(**Y2) ⊕ **S23,29(**L4 ⊕ K4) ⊕ **S23,29(**K5)

= **S23,29(L0 ⊕ R4)** ⊕ **S23,29(**Y0) ⊕ **S23,29(**Y2) ⊕ **S23,29(**L4 ⊕ K4) ⊕ **S23,29(**K5)

= **S23,29(L0 ⊕ R4)** ⊕ **S23,29(**Y0) ⊕ **S23,29(**Y2) ⊕ **S23,29(**L4 ⊕ K4)

**S23,29(**Y0) = S23,29 **F**(X0 ⊕ K0)

= S23,29 **F**(L0 ⊕ R0 ⊕ K0)

= S31(K0) ⊕ S31(R0) ⊕ S31(L0) ⊕ 1

= **S23,29(L0 ⊕ R4)** ⊕ S31(K0) ⊕ S31(R0) ⊕ S31(L0) ⊕ 1 ⊕ **S23,29(**Y2) ⊕ **S23,29(**L4 ⊕ K4)

= **S23,29(L0 ⊕ R4)** ⊕ S31(K0) ⊕ S31(R0) ⊕ S31(L0) ⊕ 1 ⊕ S31(L0 ⊕ R0) ⊕ S31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ S31(K2) ⊕ 1 ⊕ **S23,29(**L4 ⊕ K4)

= **S23,29(L0 ⊕ R4)** ⊕ S31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ **S23,29(**L4 ⊕ K4)

= **S5,15(L0 ⊕ R4)** ⊕ S7 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ **S5,15(**L4 ⊕ K4)

= **S15,21(L0 ⊕ R4)** ⊕ S23,31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ **S15,21(**L4 ⊕ K4)

= **S13(L0 ⊕ R4)** ⊕ S7,15,23,31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ **S13(**L4 ⊕ K4)

= **S5,13,21(L0 ⊕ R4)** ⊕ S15 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ **S5,13,21 (**L4 ⊕ K4)

= **S5,13,21(L0 ⊕ R4)** ⊕ S15 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ **S5,13,21 (**L4)

= **S5,13,21(L0 ⊕ R4 ⊕ L4)** ⊕ S15 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1)

S23,29(Y) = S31(X) ⊕ 1

**S23,29(L4) = S23,29(X0) ⊕ S23,29(Y1) ⊕ S23,29(Y3) ⊕ S23,29(K4)**

S23,29(X0) = S23,29(L0 ⊕ R0)

S23,29(Y1) = S23,29 **F**(X1 ⊕ K1)

= S23,29 **F**(L0 ⊕ Y0 ⊕ K1)

= S31(K1) ⊕ S31(Y0) ⊕ S31(L0) ⊕ 1

S31(Y0) = S31 **F**(X0 ⊕ K0)

= S31 **F**(L0 ⊕ R0 ⊕ K0)

S23,29(Y3) = S23,29 **F**(X3 ⊕ K3)

= S23,29 **F**(Y2 ⊕ X1 ⊕ K3)

= S31(Y2) ⊕ S31(X1) ⊕ S31(K3) ⊕ 1

= S31 **F**(X2 ⊕ K2) ⊕ S31(X1) ⊕ S31(K3) ⊕ 1

= S31 **F**(X0 ⊕ Y1 ⊕ K2) ⊕ S31(L0 ⊕ Y0) ⊕ S31(K3) ⊕ 1

= S31 **F**(X0 ⊕ Y1 ⊕ K2) ⊕ S31(L0 ⊕ **F**(X0 ⊕ K0)) ⊕ S31(K3) ⊕ 1

= S31 **F**(L0 ⊕ R0 ⊕ Y1 ⊕ K2) ⊕ S31(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0)) ⊕ S31(K3) ⊕ 1

= S31 **F**(L0 ⊕ R0 ⊕ **F**(X1 ⊕ K1) ⊕ K2) ⊕ S31(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0)) ⊕ S31(K3) ⊕ 1

= S31 **F**(L0 ⊕ R0 ⊕ **F**(L0 ⊕ Y0 ⊕ K1) ⊕ K2) ⊕ S31(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0)) ⊕ S31(K3) ⊕ 1

**S23,29(L4) =** S23,29(L0 ⊕ R0) **⊕ S23,29(Y1) ⊕ S23,29(Y3) ⊕ S23,29(K4)**

**=** S23,29(L0 ⊕ R0⊕ **L4**) **⊕** S31(K1) ⊕ S31 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S31(L0) ⊕ 1 **⊕ S23,29(Y3)**

**=** S23,29(L0 ⊕ R0⊕ **L4**) ⊕ S31 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S31(L0) ⊕ 1 **⊕** S31 **F**(L0 ⊕ R0 ⊕ **F**(L0 ⊕ Y0 ⊕ K1) ⊕ K2) ⊕ S31(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0)) ⊕ S31(K3) ⊕ 1

**=** S23,29(L0 ⊕ R0⊕ **L4**) ⊕ S31 **F**(L0 ⊕ R0 ⊕ K0) ⊕ S31(L0) **⊕** S31 **F**(L0 ⊕ R0 ⊕ **F**(L0 ⊕ Y0 ⊕ K1) ⊕ K2) ⊕ S31(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0))

**=** S23,29(L0 ⊕ R0⊕ **L4**) **⊕** S31 **F**(L0 ⊕ R0 ⊕ **F**(L0 ⊕ S31 **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ K2)

**=** S23,29(L0 ⊕ R0⊕ **L4**) **⊕** S31 **F**(L0 ⊕ R0 ⊕ **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ K2)

R4 = L0 ⊕ Y0 ⊕ Y2 ⊕ X2 ⊕ Y3 ⊕ K5

**S23,29(R4) = S23,29(L0) ⊕ S23,29(Y0) ⊕ S23,29(Y2) ⊕ S23,29(**X2**) ⊕ S23,29(**Y3**) ⊕ S23,29(K5)**

**S23,29(L0 ⊕ R4) ⊕ S23,29(Y0) ⊕ S23,29(Y2) ⊕ S23,29(X0 ⊕ Y1) ⊕ S23,29(**Y3**)**

**S23,29(L0 ⊕ R4) ⊕ S23,29(Y0) ⊕ S23,29(Y2) ⊕ S23,29(X0) ⊕ S23,29(Y1) ⊕ S23,29(**Y3**)**

**S23,29(L0 ⊕ R4) ⊕ S23,29(Y0) ⊕ S23,29(Y2) ⊕ S23,29(**L0 ⊕ R0**) ⊕ S23,29(Y1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29(Y0) ⊕ S23,29(Y2) ⊕ S23,29(Y1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29 F(X0 ⊕ K0) ⊕ S23,29(Y2) ⊕ S23,29(Y1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29 F(**L0 ⊕ R0 **⊕ K0) ⊕ S23,29(Y2) ⊕ S23,29(Y1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29 F(**L0 ⊕ R0 **⊕ K0) ⊕ S23,29(Y2) ⊕ S23,29 F(X1 ⊕ K1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29 F(**L0 ⊕ R0 **⊕ K0) ⊕** S23,29 **F**(X0 ⊕ Y1 ⊕ K2) **⊕ S23,29 F(L0 ⊕ Y0 ⊕ K1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29 F(**L0 ⊕ R0 **⊕ K0) ⊕** S23,29 **F**(L0 ⊕ R0 ⊕ Y1 ⊕ K2) **⊕ S23,29 F(L0 ⊕ Y0 ⊕ K1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29 F(**L0 ⊕ R0 **⊕ K0) ⊕** S23,29 **F**(L0 ⊕ R0 ⊕ **F(L0 ⊕ Y0 ⊕ K1)** ⊕ K2) **⊕ S23,29 F(L0 ⊕ Y0 ⊕ K1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29 F(**L0 ⊕ R0 **⊕ K0) ⊕** S23,29 **F**(L0 ⊕ R0 ⊕ **F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1)** ⊕ K2) **⊕ S23,29 F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S23,29 F(**L0 ⊕ R0 **⊕ K0) ⊕** S23,29 **F**(L0 ⊕ R0 ⊕ **F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1)** ⊕ K2) **⊕ S23,29 F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S31(**L0) ⊕ **S31(**R0) **⊕ S31(K0) ⊕ 1 ⊕** S23,29 **F**(L0 ⊕ R0 ⊕ **F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1)** ⊕ K2) **⊕ S23,29 F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S31(**L0 ⊕ R0) **⊕ 1 ⊕** S23,29 **F**(L0 ⊕ R0 ⊕ **F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1)** ⊕ K2) **⊕ S23,29 F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S31(**L0 ⊕ R0) **⊕ 1 ⊕** S23,29 **F**(L0 ⊕ R0 ⊕ **F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1)** ⊕ K2) **⊕ S31(L0) ⊕ S31(F(**L0 ⊕ R0 **⊕ K0)) ⊕ S31(K1) ⊕ 1 ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S31(**R0) **⊕** S23,29 **F**(L0 ⊕ R0 ⊕ **F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1)** ⊕ K2) **⊕ S31(F(**L0 ⊕ R0 **⊕ K0)) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S31(**R0) **⊕ S31(**L0) ⊕ **S31(**R0) ⊕ **S31 F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1)** ⊕ **S31(**K2) **⊕ 1 ⊕ S31(F(**L0 ⊕ R0 **⊕ K0)) ⊕ S23,29(**Y3**)**

**S23,29(R0 ⊕ R4) ⊕ S31(**L0) ⊕ **S31 F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1) ⊕ 1 ⊕ S31 F(**L0 ⊕ R0 **⊕ K0) ⊕ S23,29(**Y3**)**

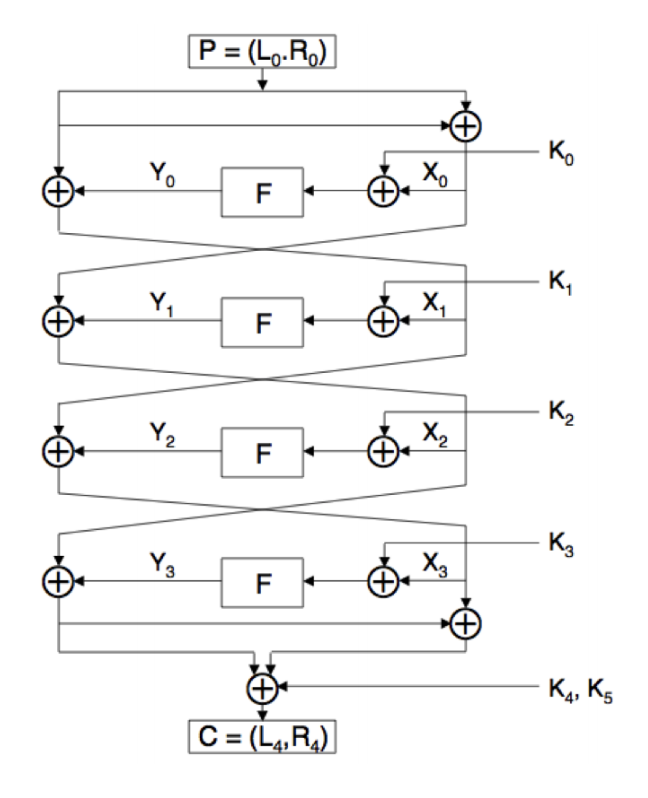
**S31(**L0) ⊕ **S31 F(**L0 ⊕ R0 **⊕ K0) ⊕ S31 F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1) S23,29(R0 ⊕ R4) ⊕ ⊕ 1 ⊕ S23,29(**Y3**)**

**S31(**L0) ⊕ **S31 F(**L0 ⊕ R0 **⊕ K0) ⊕ S31 F(L0 ⊕ F(**L0 ⊕ R0 **⊕ K0) ⊕ K1) S23,29(R0 ⊕ R4) ⊕ ⊕** S23,29 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ **F**(L0 ⊕ R0 ⊕ **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ K2) ⊕ K3) **⊕ 1**

S23,29(Y3) = S23,29 **F**(X3 ⊕ K3)

= S23,29 **F**( **F**(X0 ⊕ Y1 ⊕ K2) ⊕ L0 ⊕ Y0 ⊕ K3)

= S23,29 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ **F**(L0 ⊕ R0 ⊕ **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ K2) ⊕ K3)



R4 = L0 ⊕ Y0 ⊕ Y2 ⊕ L4 ⊕ K4 ⊕ K5

**= S23,29(L0 ⊕** L4 **⊕ R4) ⊕ S23,29(Y0) ⊕ S23,29(Y2) ⊕ S23,29(K4) ⊕ S23,29(**K5**)**

**Y2 = L4 K4 Y3 K2**

**= S23,29(L0 ⊕** L4 **⊕ R4) ⊕ S23,29(Y0) ⊕ S23,29 F(L4 ⊕ K4 ⊕ Y3 ⊕ K2)**

**= S23,29(L0 ⊕** L4 **⊕ R4) ⊕ S23,29(Y0) ⊕ S31(L4) ⊕ S31(K4) ⊕ S31(Y3) ⊕ S31(K2) ⊕ 1**

**= S23,29(L0 ⊕** L4 **⊕ R4) ⊕ S23,29(Y0) ⊕ S31(L4) ⊕ S31(Y3) ⊕ 1**

**= S23,29(L0 ⊕** L4 **⊕ R4) ⊕** S23,29 **F**(L0 ⊕ R0 ⊕ K0) **⊕ S31(L4) ⊕ S31(Y3) ⊕ 1**

**= S23,29(L0 ⊕** L4 **⊕ R4) ⊕** S31(L0) ⊕ S31(R0) ⊕ S31(K0) **⊕ 1 ⊕ S31(L4) ⊕ S31(Y3) ⊕ 1**

**= S23,29(L0 ⊕** L4 **⊕ R4) ⊕** S31(L0 ⊕ R0 **⊕ L4) ⊕ S31(Y3)**

S31(Y3) = S31 **F**(X3 ⊕ K3)

= S31 **F**( **F**(X0 ⊕ Y1 ⊕ K2) ⊕ L0 ⊕ Y0 ⊕ K3)

= S31 **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ **F**(L0 ⊕ R0 ⊕ **F**(L0 ⊕ **F**(L0 ⊕ R0 ⊕ K0) ⊕ K1) ⊕ K2) ⊕ K3)

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