**Agenda**

1. **Stream Cipher**
   1. **Mobile Communication**
      1. **2G (GSM) A5/1**
      2. **3G**
      3. **4G**
   2. **Wireless Communication**
      1. **RC4 (WEP)**

IMEI

M

SIM (contains multiple variables)

Data travels in the form of stream

Stream cipher encrypt bit by bit

Encryption: yi = e(xi) = xi + si mod 2 => yi = xi ⊕ si

Decryption: xi = d(yi) = yi + si mod 2 => xi = yi ⊕ si

Xi, yi, si {0, 1}

Sn, ……., s3, s2, s1 Sn, ……., s3, s2, s1

Xn, …..x3,x2,x1 yi xn, …x3, x2, x1

Xi = 1 0 0 0 0 0 1

Si = 0 1 0 1 1 0 1

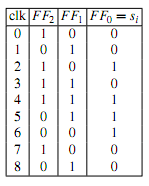
Yi = 1 1 0 1 1 0 0

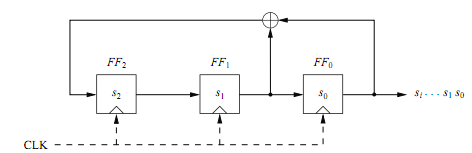
Yi = 1 1 0 1 1 0 0

Si = 0 1 0 1 1 0 1

Xi = 1 0 0 0 0 0 1

LFSR – Linear Feedback Shift Register

A5/1 – 2G cipher for voice



1 0 0

0 1 0

1 0 1

1 1 0

1 1 1

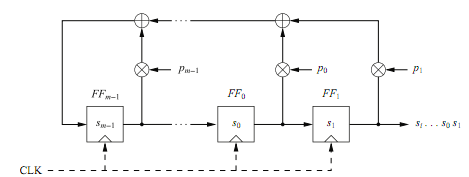
m = 3 // no of FF

P0 = 1, P1 = 1, P2 = 0

P(x) = xm + Pm-1 xm-1 + …..+ P1 x1 + P0 x0

= x3 + P2 x2 + P1 x1 + P0 x0

= x3 + x + 1



P(x) = x4 + x3 + x2 + x + 1

M = 4

P0 = P1 = P2 = P3 = 1

P(x) = x4 + x3 + x2 + 1

m = 4

P0 = 1, P1= 0, P2 =1, p3= 1

m = 4

p0 = 1, p1=0, p2=1, p3=1

P(x) = x4 + P3 x3 + P2 x2 + P1 x1 + P0 x0

P0 = 1

P1 = 0

P2 = 1

P3 = 0

P(x) = x4 + P2 x2 + 1 . 1

P(x) = x4 + x2 + 1

P(x) = x5 + x4 + x3 + ~~x~~~~2~~ ~~+ x~~ + 1