# Cryptography
# Lecture six

## Stream Cipher (cont.)

*Assis prof. Dr. Saja Jasem Mohammed*

# NON LINEAR FEEDBACK SHIFT REGISTER

- **Non linear algorithms types:**

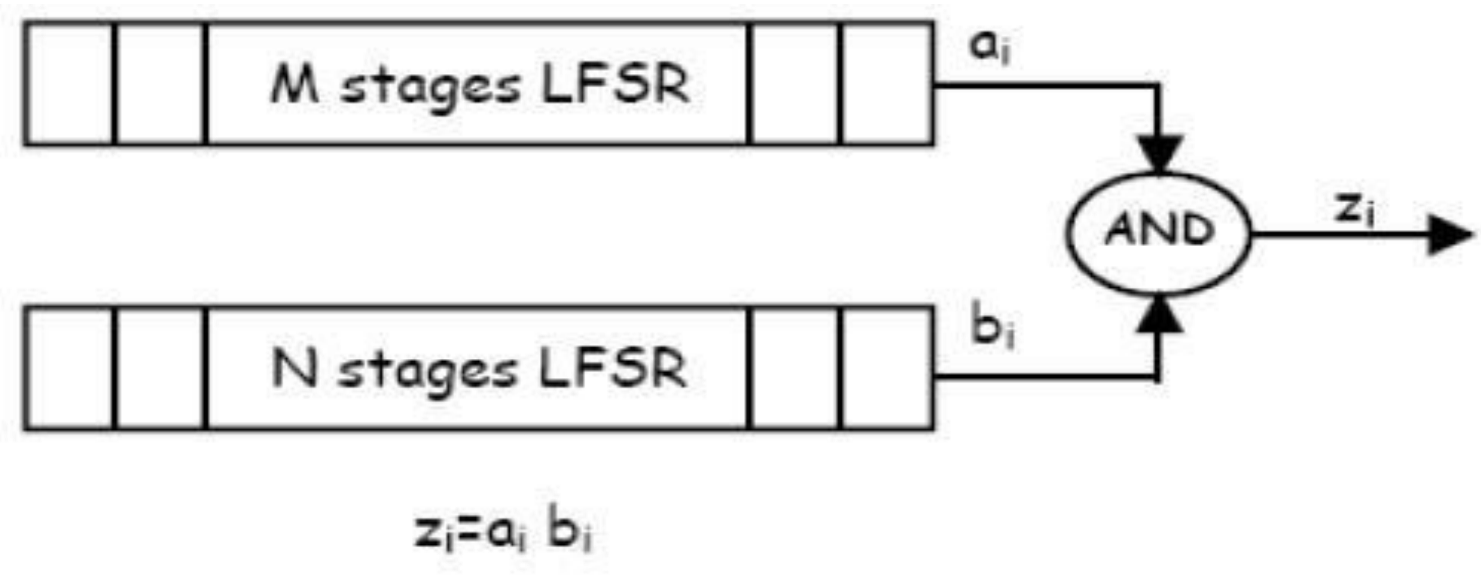
1.**Linear Feedback Shift Register (LFSR) with combining elements.**

- ✓ Hadamard algorithm
- ✓J-K flip flop
- ✓Geffe's algorithm

2. **Non Linear Feedback Shift Registers (NLFSR).**

# Hadamard Algorithm

- This algorithm consists of two linear feedback shift registers. Each one has a linear feedback function, which will give the maximum period.
- The length of these registers are different but has the property that the greatest common divisor between their length=1.
- i.e. let M and N equal the length of the shift registers, hence the gcd(M,N)=1

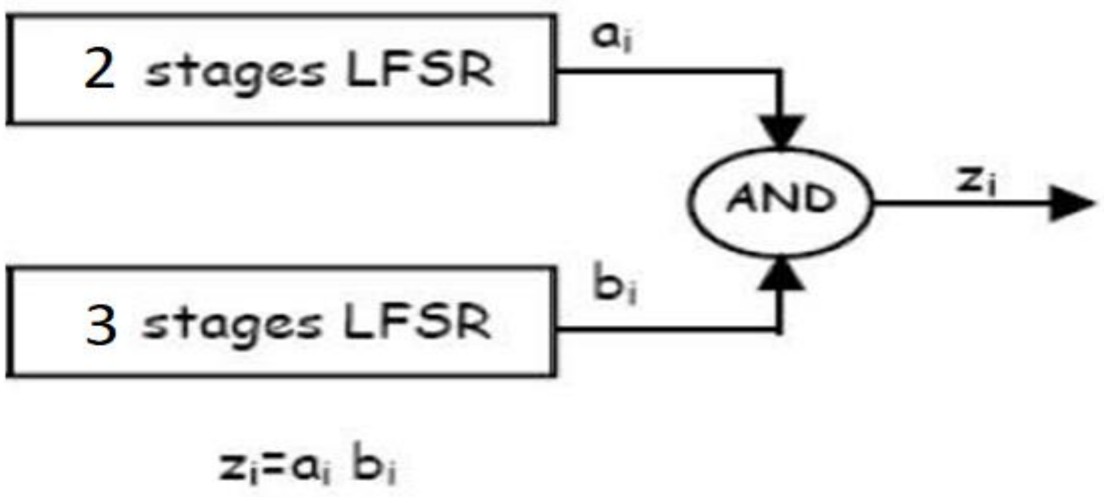


- When the gcd(M,N)=1, the period length of the final sequence is $(2^M-1)(2^N-1)$, which is the maximum period.

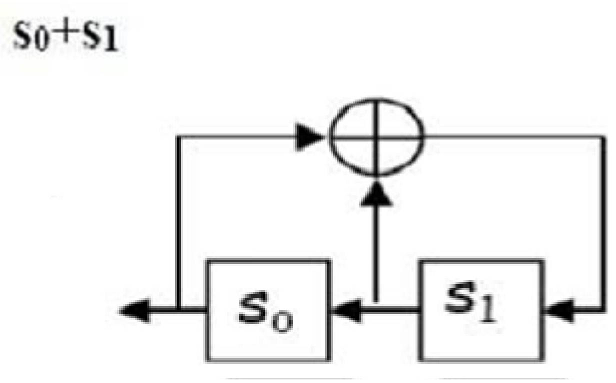
- Note: we can use the OR operation instead of AND

# Example:

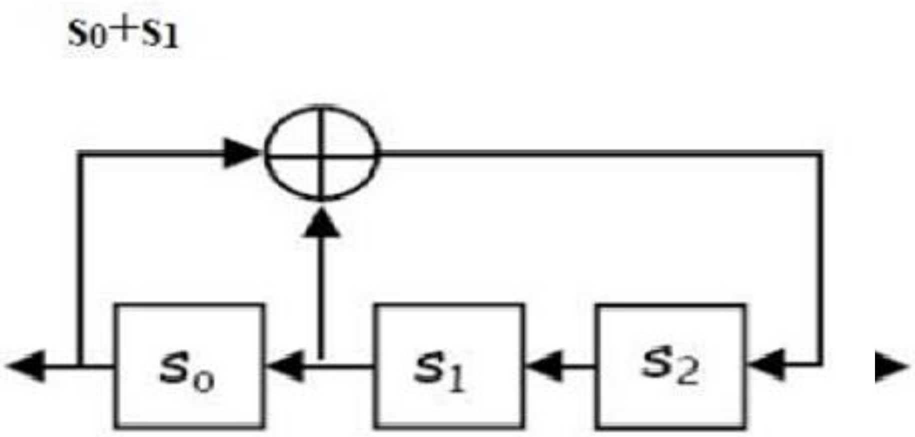
- We have two linear feedback shift registers with 2 and 3 stages respectively, with initial states [1,1] and [1,1,1] respectively.
- Apply the Hadamard algorithm to find the resulting sequence.



**M-LFSR1**



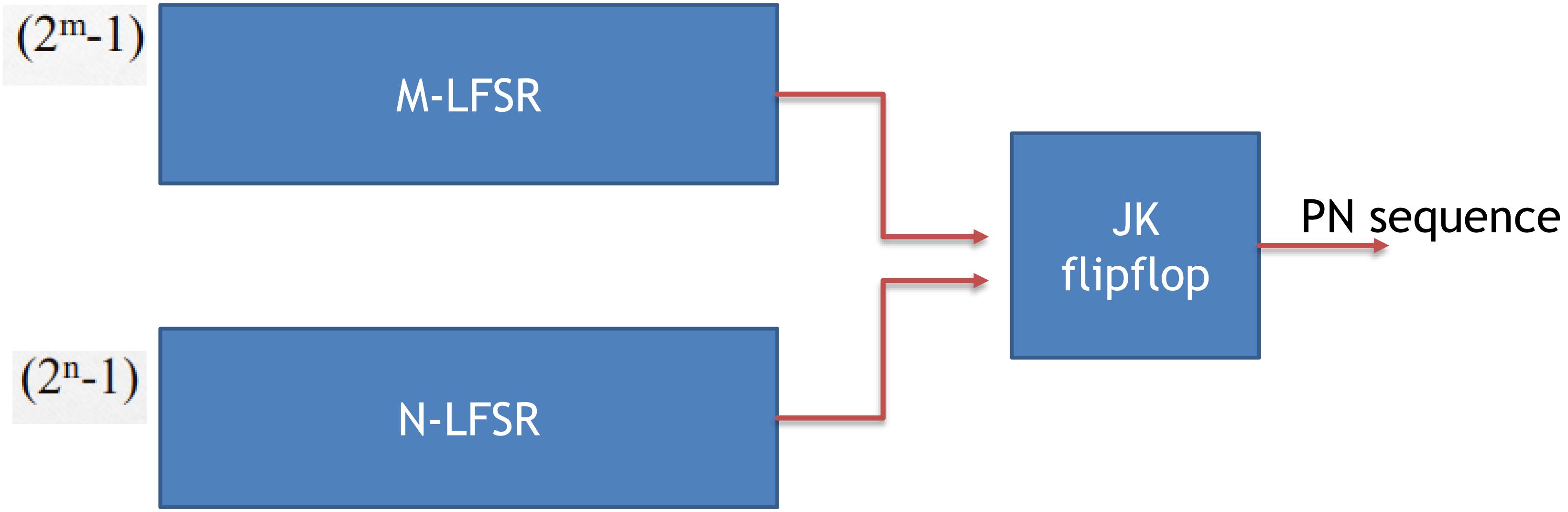
**N-LFSR2**

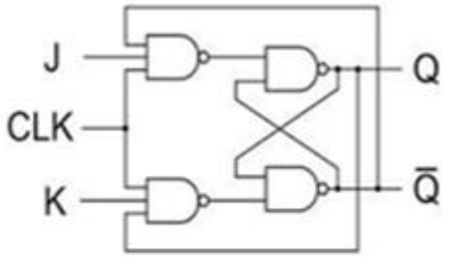


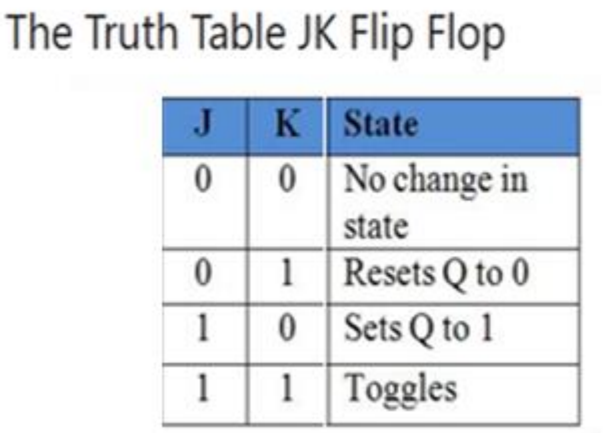
**Note: Since gcd(2,3)=1, hence the period of the resulting sequence =3*7=21.**

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| B | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| z | | | | | | | | | | | | | | | | | | | | | |

# J-K FLIP FLOP ALGORITHM







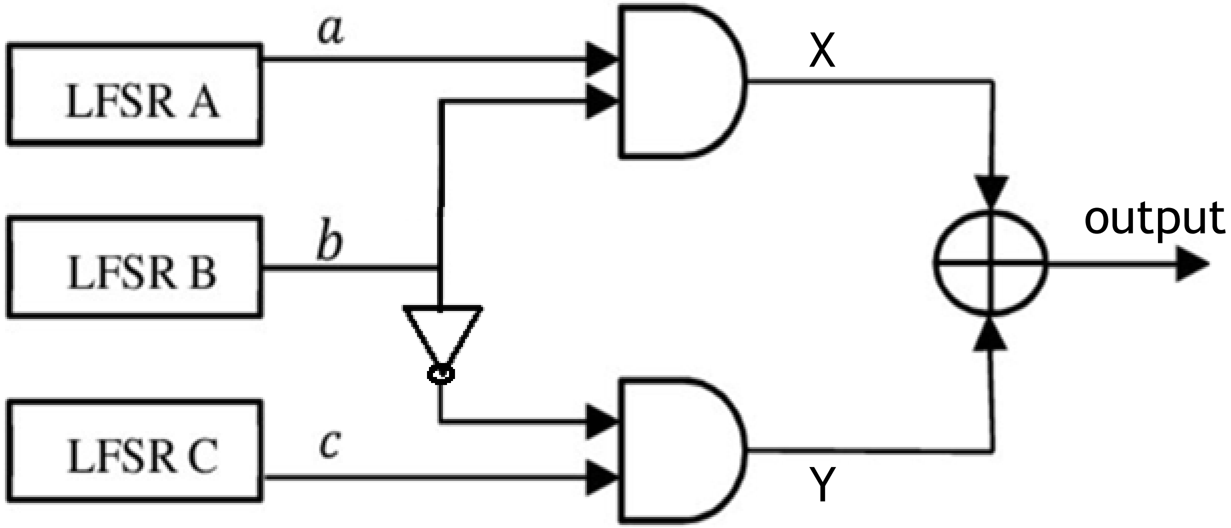
The Truth Table JK Flip Flop

| J | K | State |
|---|---|---|
| 0 | 0 | No change in state |
| 0 | 1 | Resets Q to 0 |
| 1 | 0 | Sets Q to 1 |
| 1 | 1 | Toggles |

Initial value of memory=0

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| B | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| z | | | | | | | | | | | | | | | | | | | | | |

# Geffe’s Generator algorithm



| a | b | c | X | Y | output |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 |

X=a and b
Y= ~ b And c
Output = X Xor Y

**This keystream generator sequence length is (2^A - 1)*(2^B - 1)*(2^C- 1)**

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| B | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| C | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| Z | | | | | | | | | | | | | | | | | | | | | |

# H.W.

LFSR1 M=4, F= S0 + S3, 1011
LFSR2 N=3, F= S0 + S2, 101
LFSR3 L=2, F= S0 + S1, 11
Find the Max Sequence using:

1. Geffe’s generator
2. J.K. flipflop

# Non Linear Feedback Shift Registers (NLFSR)

- **Non linear feedback shift register** (of this type ) is a shift register whose input bit is a non-linear function of its previous state.
- It is  a shift register contains modulo2 adder (**XOR**) with modulo2 multiplier (**AND**) in its feedback function.
- The maximum sequence length is **2^n.**
- The function **must** have logic one.
- **Each stage must appear** at least one in the feedback function.

# Example

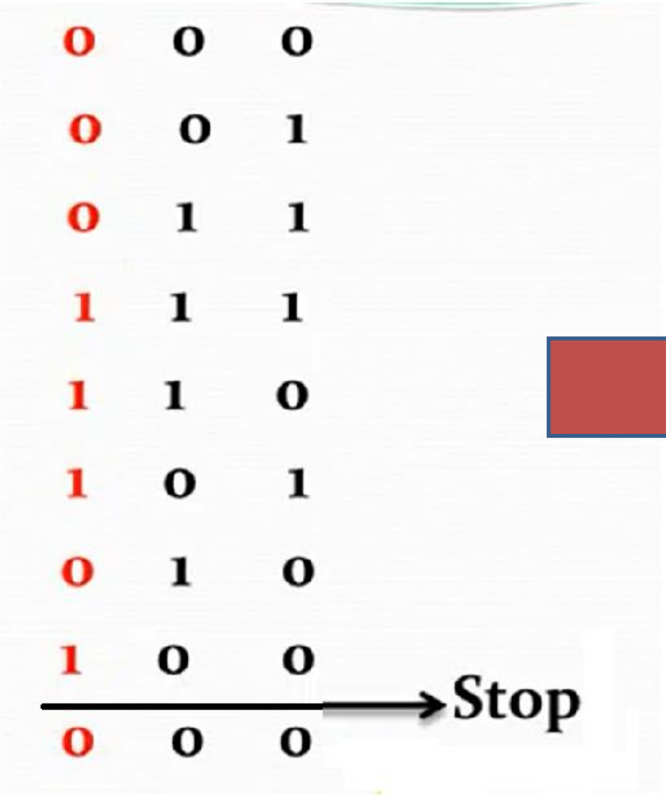
- Suppose You have NLFSR with 3 flipflops and feedback function

  **f=1+ S0+S1+S1S2**, what is the output keystream sequence?

**Solution steps :**

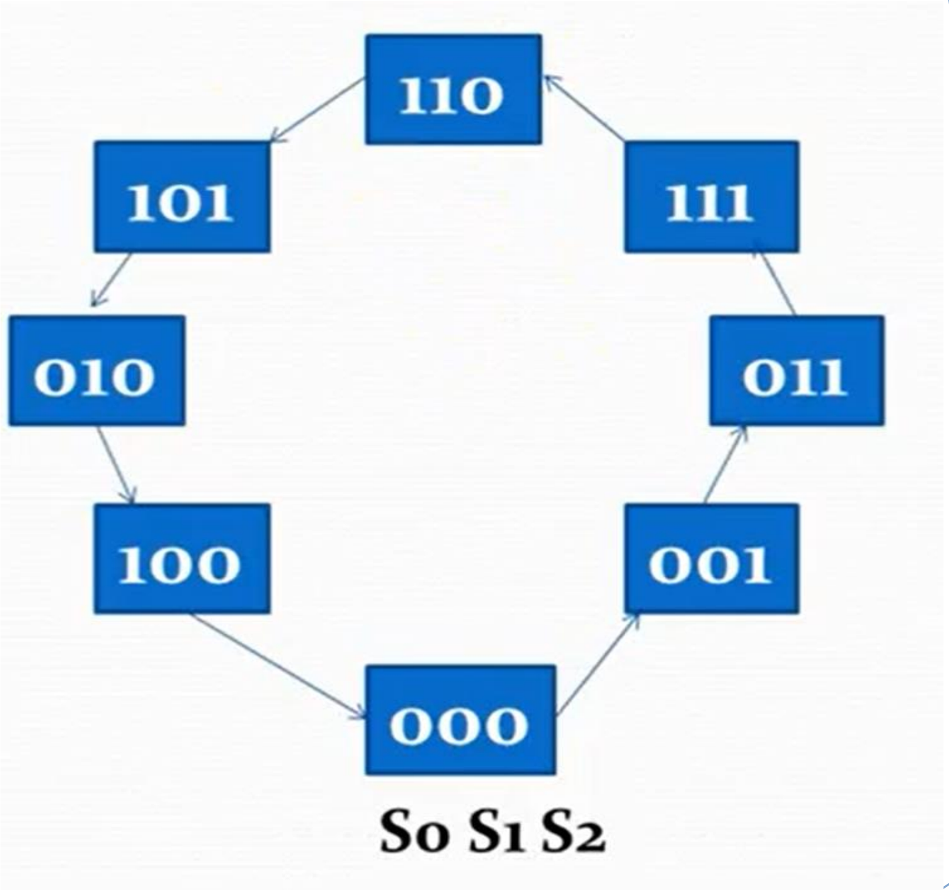
- Find maximum sequence (using truth table).
- Convert to a **state diagram**.
- Check numbers of ones and zeros

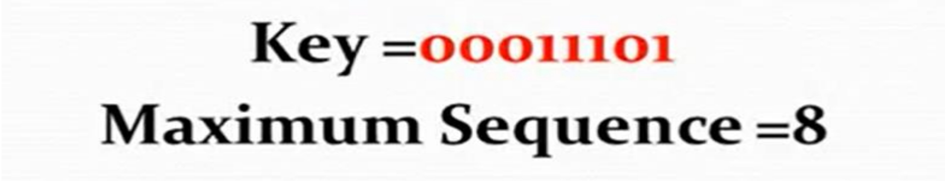
# The solution:



| S0 | S1 | S2 | |
|---|---|---|---|
| 0 | 0 | 0 | |
| 0 | 0 | 1 | |
| 0 | 1 | 1 | |
| 1 | 1 | 1 | |
| 1 | 1 | 0 | |
| 1 | 0 | 1 | |
| 0 | 1 | 0 | |
| 1 | 0 | 0 | → Stop |
| 0 | 0 | 0 | |

State diagram





Key =00011101

Maximum Sequence =8

no. of 0’s = no. of 1’s =4 ➔ random seq.