Reconfigurable Systems

UAlg
UNIVERSIDADE DO ALGARVE

Jorge Semião

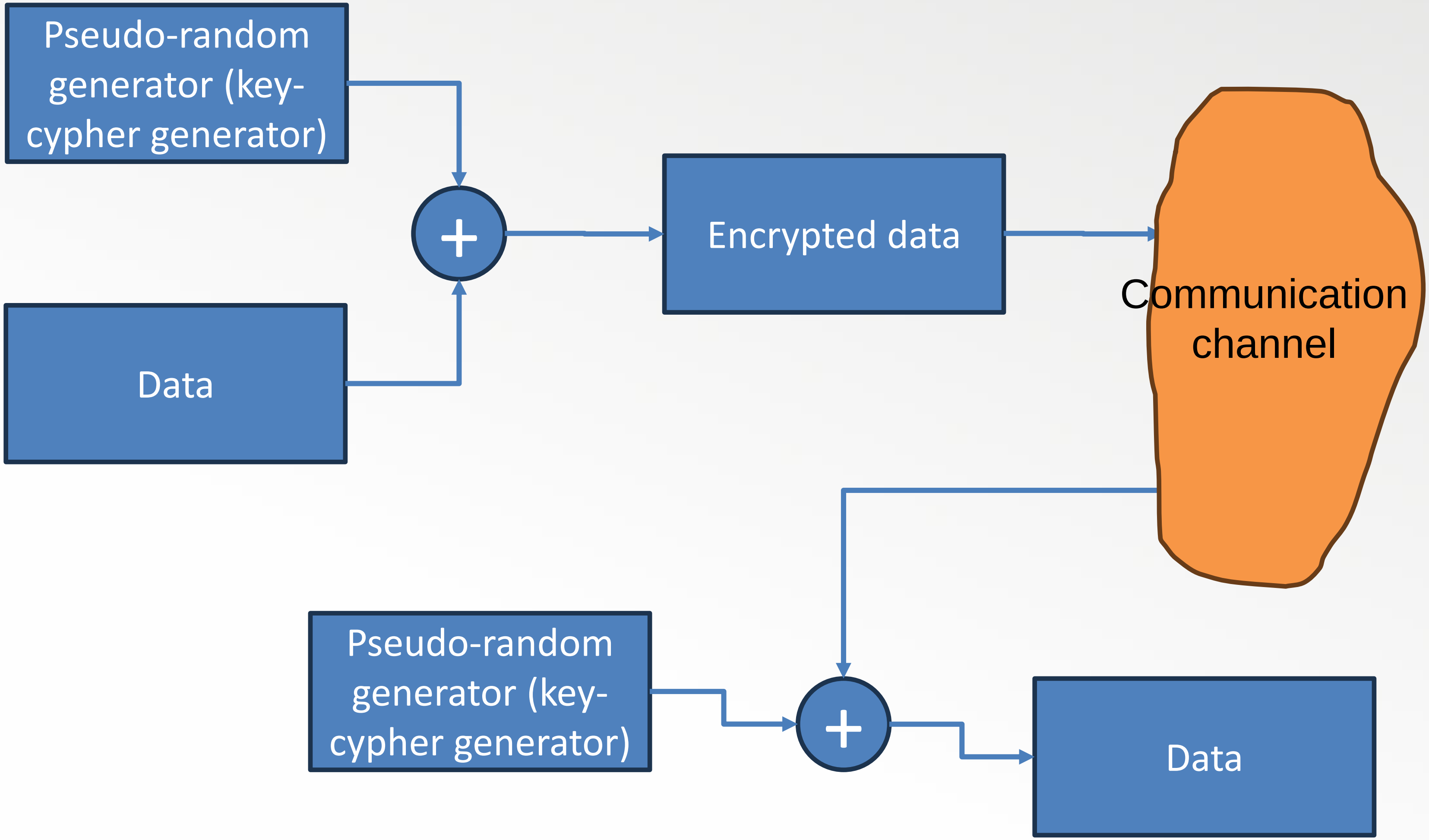
Instituto Superior de Engenharia

www.ualg.pt

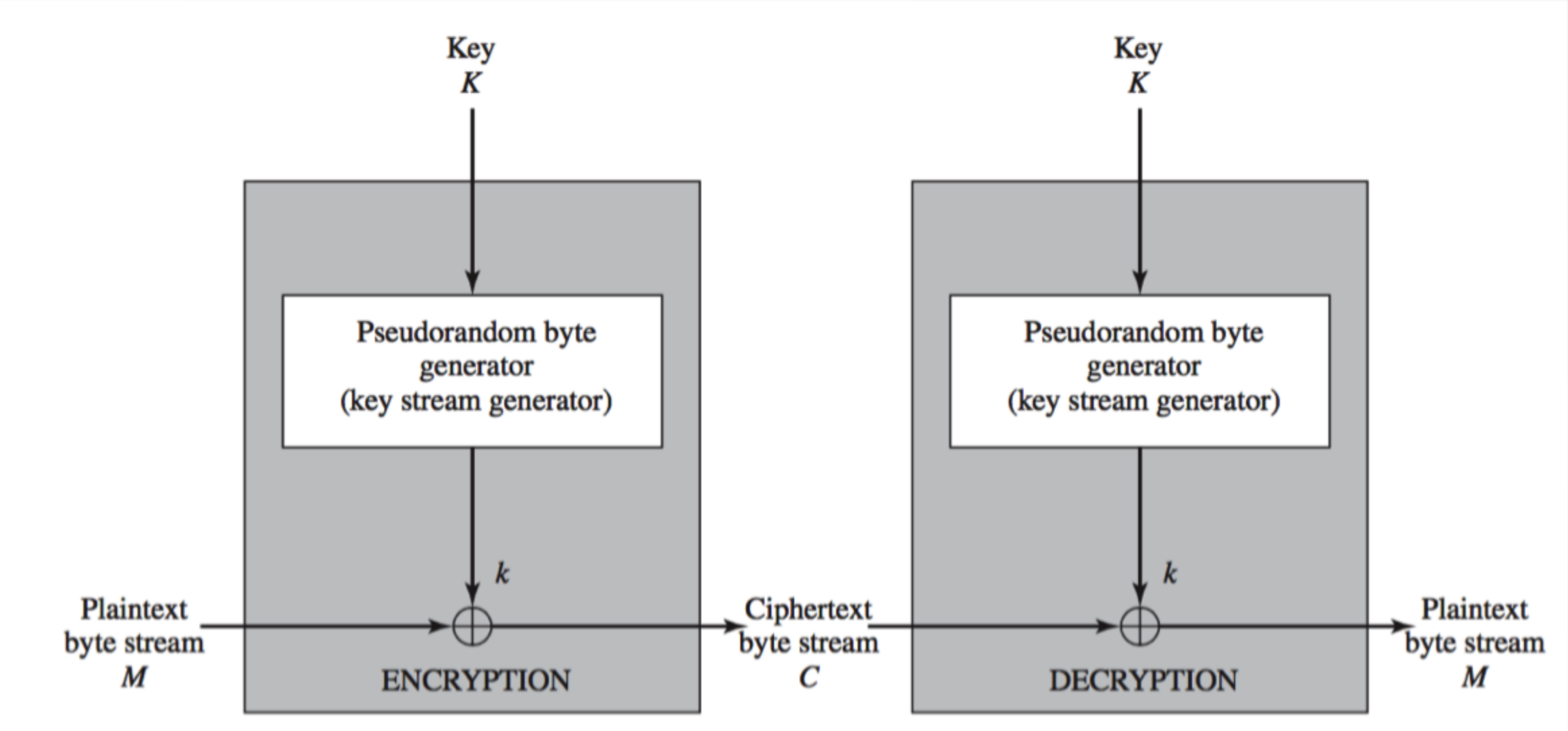
Assignment 2

- Implement in VHDL a sender and receiver stream cipher using 8-bit LFSR as key stream generator
- Implement one entity for the encryption and another for the decryption, to encrypt/decrypt 8 bits
- Simulate both entities together
- Create random words (8-bits) to be the transmitting data, and simulate the encryption, sending, decryption and data confirmation
- Use a single XOR gate as a cipher algorithm, to encrypt and decrypt data with the key stream

Stream Cipher diagram


Pseudo-random generator (key-cypher generator)
Data
+
Encrypted data
Communication channel
Pseudo-random generator (key-cypher generator)
+
Data

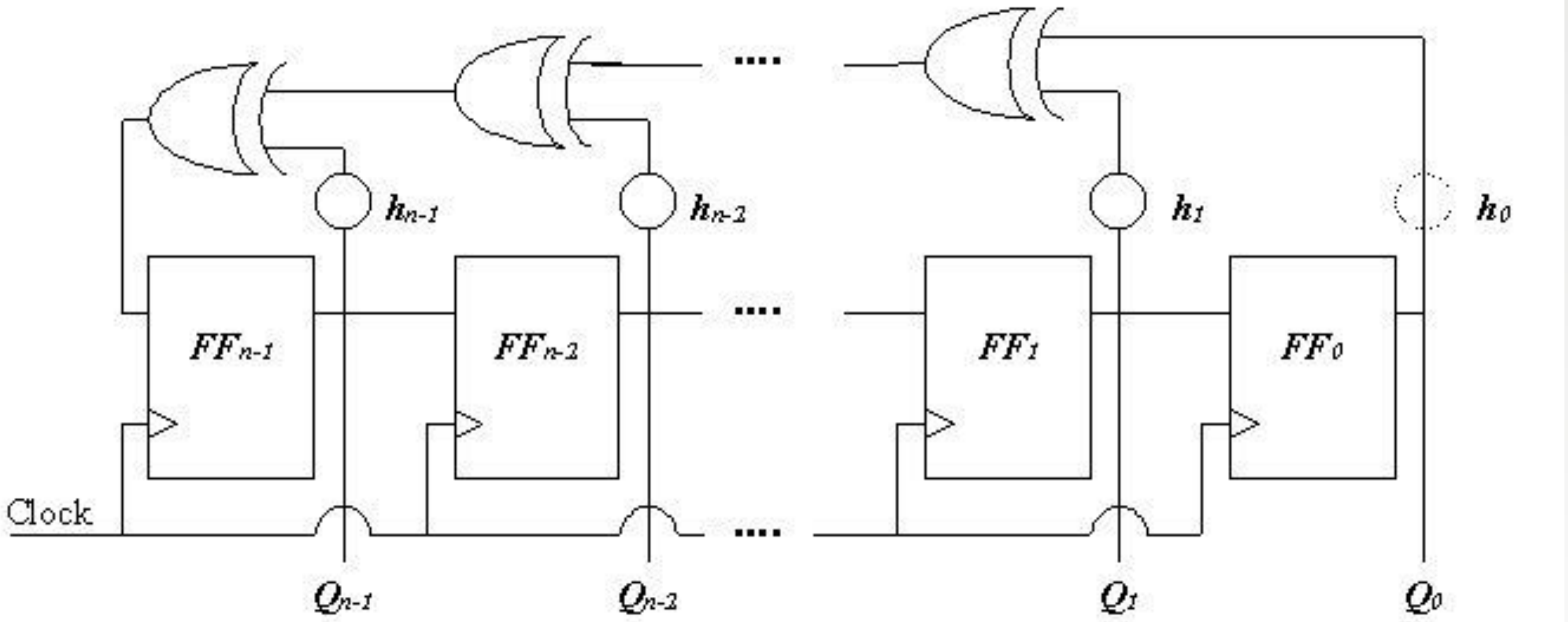
Stream Cipher diagram


Key
K
Pseudorandom byte generator (key stream generator)
k
Plaintext byte stream M
ENCRYPTION
Ciphertext byte stream C
Key
K
Pseudorandom byte generator (key stream generator)
k
DECRYPTION
Plaintext byte stream M

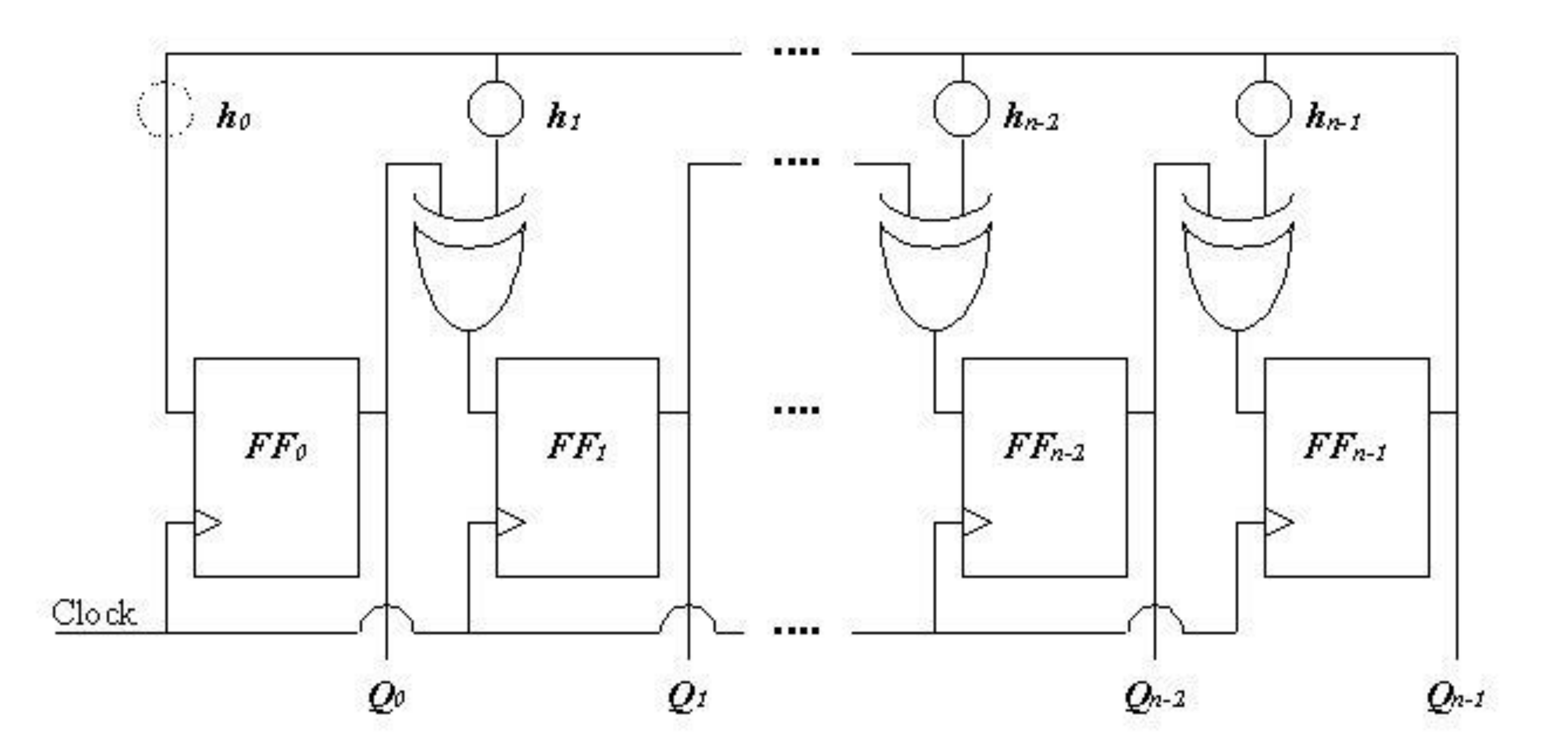
LFSR (Linear Feedback Shift-Register)

- Pseudo-random generator
- Only specific feedback loops generate 2^n-1 pseudo-random patterns (other loops are not used)
- May act as a key stream generator in cryptography
- A different seed will produce different patterns
- Two possible architectures: Linear or Modular

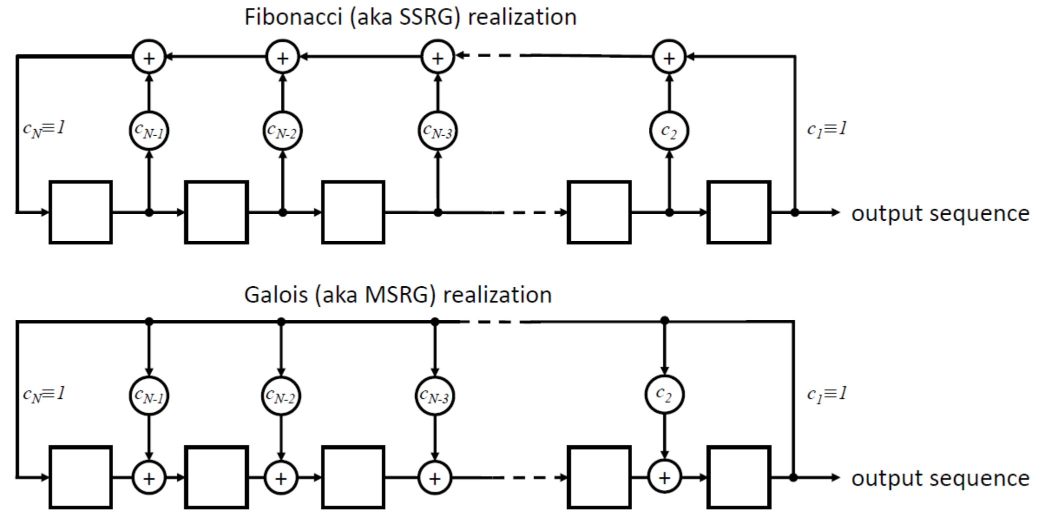
LFSR (Linear Feedback Shift-Register) – Linear type (or Fibonacci)



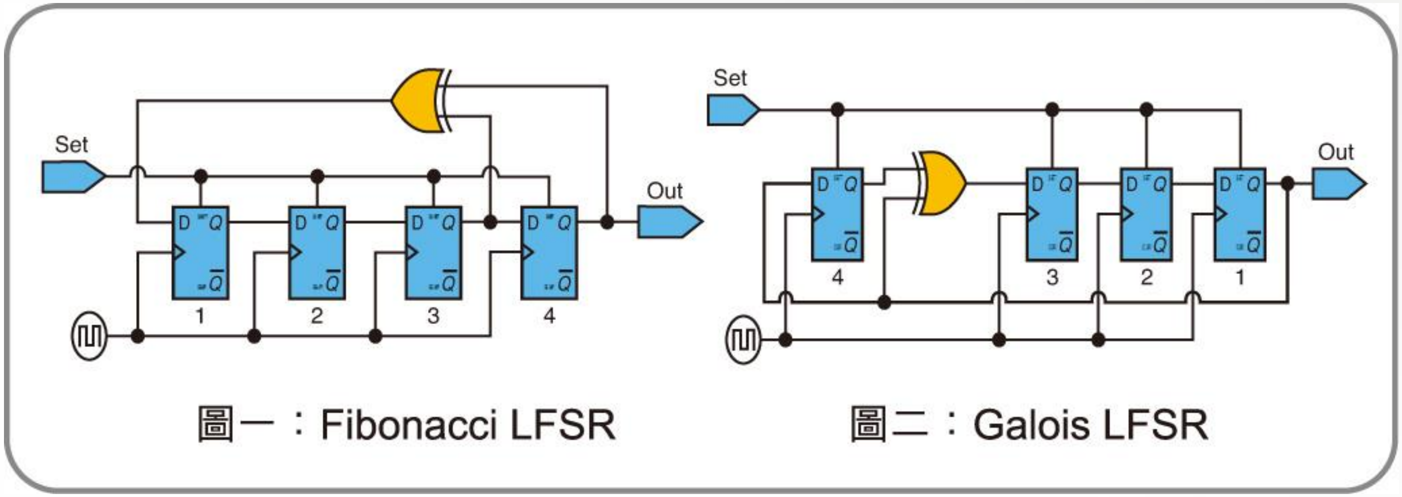
LFSR (Linear Feedback Shift-Register) – Modular type (or Galois)



LFSR examples


Fibonacci (aka SSRG) realization

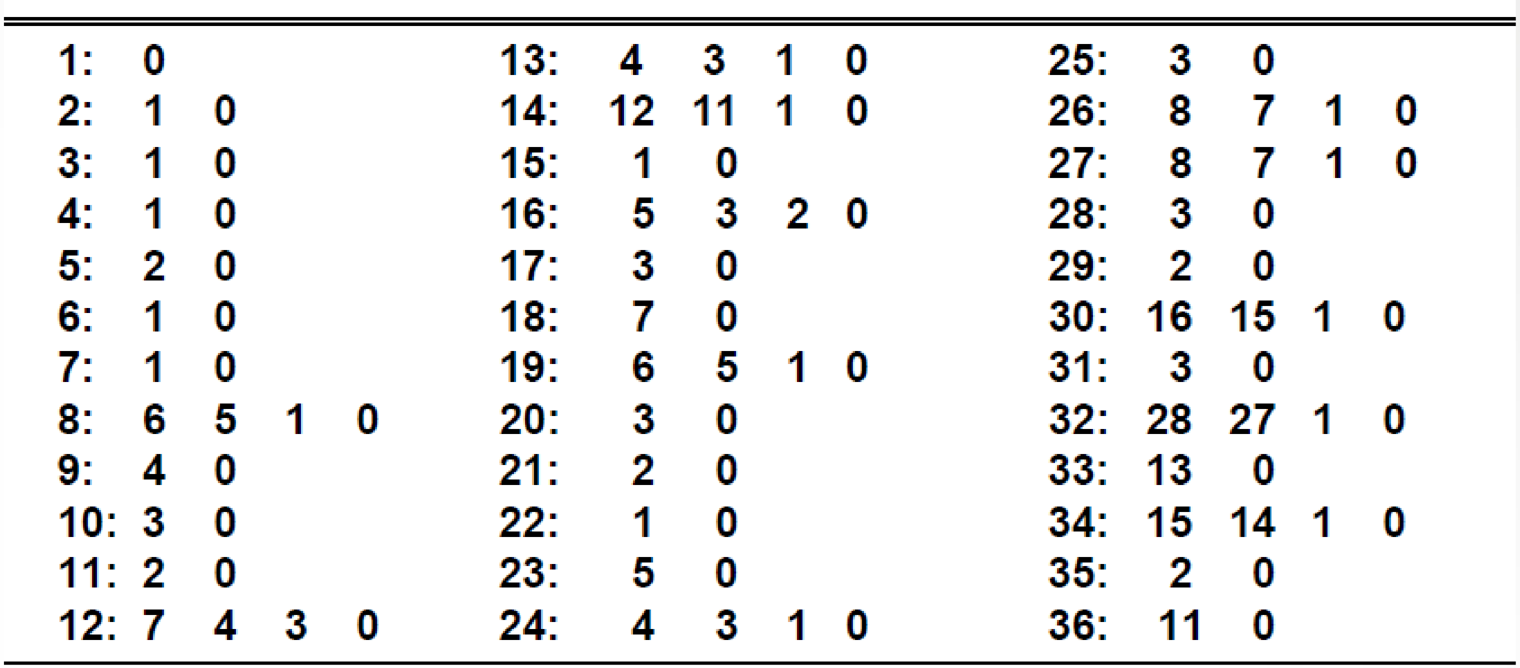
Galois (aka MSRG) realization


圖一：Fibonacci LFSR

圖二：Galois LFSR

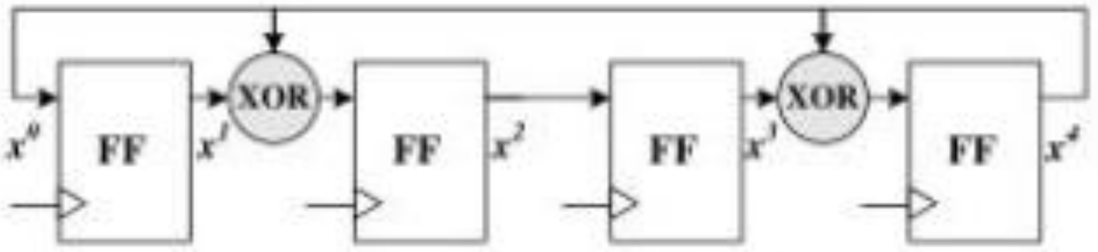
LFSR – Primitive polynomial

- The feedback loops that generate 2^n-1 diferente patterns
- Ex: $x^4+x^1+1^0$ is a 4-bit LFSR with loops in FF 1 and 0

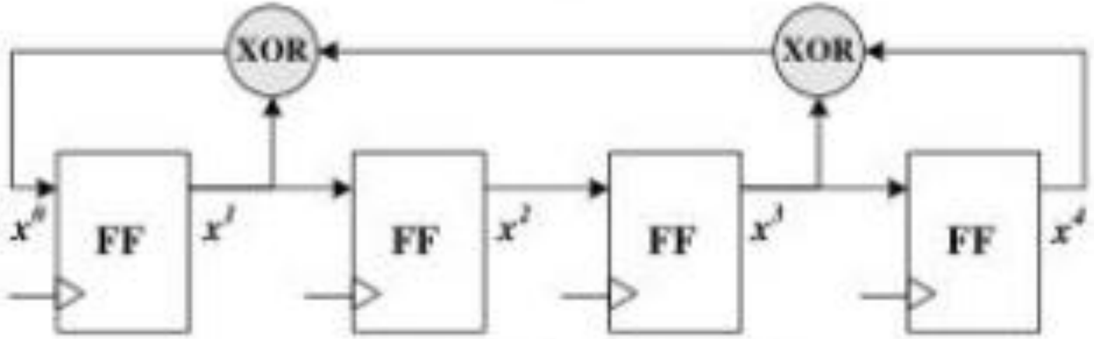


1:	0				13:	4	3	1	0	25:	3	0		
2:	1	0			14:	12	11	1	0	26:	8	7	1	0
3:	1	0			15:	1	0			27:	8	7	1	0
4:	1	0			16:	5	3	2	0	28:	3	0		
5:	2	0			17:	3	0			29:	2	0		
6:	1	0			18:	7	0			30:	16	15	1	0
7:	1	0			19:	6	5	1	0	31:	3	0		
8:	6	5	1	0	20:	3	0			32:	28	27	1	0
9:	4	0			21:	2	0			33:	13	0		
10:	3	0			22:	1	0			34:	15	14	1	0
11:	2	0			23:	5	0			35:	2	0		
12:	7	4	3	0	24:	4	3	1	0	36:	11	0		

LFSR – Primitive polynomial



Internal Feedback/Type I
LFSR



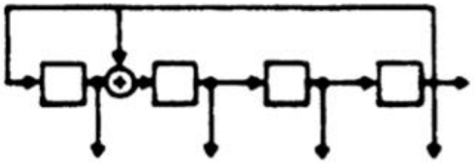
External Feedback/Type II
LFSR

$$P(x) = x^0 + x^1 + x^3 + x^4$$

LFSR – Primitive polynomial

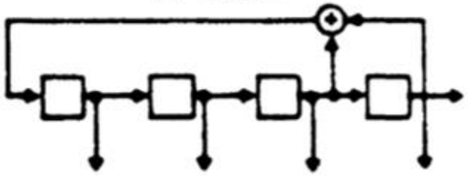
IE Type

$X^4 + X + 1$



EE Type

$X^4 + X + 1$



Clock	A^0	A^1	A^2	A^3	Decimal Value	A^0	A^1	A^2	A^3	Decimal Value
Initial State	0	0	0	1	—	0	0	0	1	—
1	1	1	0	0	12	1	0	0	0	8
2	0	1	1	0	6	0	1	0	0	4
3	0	0	1	1	3	0	0	1	0	2
4	1	1	0	1	13	1	0	0	1	9
5	1	0	1	0	10	1	1	0	0	12
6	0	1	0	1	5	0	1	1	0	6
7	1	1	1	0	14	1	0	1	1	11
8	0	1	1	1	7	0	1	0	1	5
9	1	1	1	1	15	1	0	1	0	10
10	1	0	1	1	11	1	1	0	1	13
11	1	0	0	1	9	1	1	1	0	14
12	1	0	0	0	8	1	1	1	1	15
13	0	1	0	0	4	0	1	1	1	7
14	0	0	1	0	2	0	0	1	1	3
15	0	0	0	1	1	0	0	0	1	1
16	1	1	0	0	12	1	0	0	0	8