جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني

Department of Cyber Security

Subject:

Nonlinear Shift Register

Class:

Second

Lecturer:

Asst. raed alshmary

Lecture: (5)

Introduction

1. Linear Feedback Shift Register(LFSR)

A Linear Feedback Shift Register (LFSR) is a shift register that uses linear feedback to generate a sequence of bits, which can appear random but is deterministic based on an initial seed. LFSRs are fundamental in digital communications and cryptography due to their simplicity and efficiency in generating pseudo-random sequences. Historically, LFSRs emerged in the mid-20th century and became widely adopted in the design of stream ciphers, where they serve as key stream generators. In a stream cipher, the LFSR produces a sequence of bits (the key stream) that is XORed with plaintext bits to produce ciphertext, offering a method for encrypting data in a bit-by-bit fashion. The strength of an LFSR-based stream cipher lies in its ability to produce long, non-repeating pseudo-random sequences when configured with a maximal-length feedback polynomial, making it suitable for secure, lightweight encryption in systems with limited computational resources, such as early wireless communication and embedded systems.

2. Non-Linear Feedback Shift Register(LFSR)

A Nonlinear Feedback Shift Register (NLFSR) is an advanced type of shift register that, unlike the Linear Feedback Shift Register (LFSR), incorporates nonlinear feedback functions to produce more complex and less predictable sequences. This nonlinearity increases resistance to cryptanalysis, making NLFSRs a powerful tool in cryptography, especially for designing secure stream ciphers. While LFSRs were widely used in early cryptographic applications due to their simplicity and mathematical properties, they became vulnerable to linear attacks over time. NLFSRs, which emerged as a solution to these vulnerabilities, generate pseudo-random sequences that are far harder to analyze and

reverse-engineer due to their nonlinear feedback. In stream ciphers, NLFSRs serve as the core component for generating key streams, enhancing security by producing highly complex bit sequences that are XORed with plaintext to create ciphertext. This approach is particularly valuable in modern cryptographic systems requiring high security, such as secure wireless communications, where lightweight yet robust encryption is essential.

Types of Shift Registers in Stream Ciphers

Shift registers used in stream ciphers are specifically designed to maximize randomness and security. Here are the two main types:

1. Linear Feedback Shift Register (LFSR)

- Definition: An LFSR is a type of shift register where the input bit is a linear function (XOR) of its previous states.
- Structure: Contains a sequence of bits that "shift" positions on each clock cycle. Selected bits are XORed to produce the new bit that enters the shift register.
- Feedback Mechanism: Feedback taps are carefully selected to maximize the period (the number of unique states before repeating) and randomness.
- Example in Stream Ciphers:
    - LFSRs are commonly used in stream ciphers due to their simplicity and efficiency in generating pseudorandom sequences.
    - Example: The A5/1 cipher used in GSM mobile communications uses three LFSRs of different lengths.
- Advantages: Simple, fast, and hardware friendly.

- Disadvantages: Linear feedback makes it vulnerable to attacks like the Berblekamp-Massey algorithm, which can determine the structure of an LFSR and break the cipher if enough output bits are known.

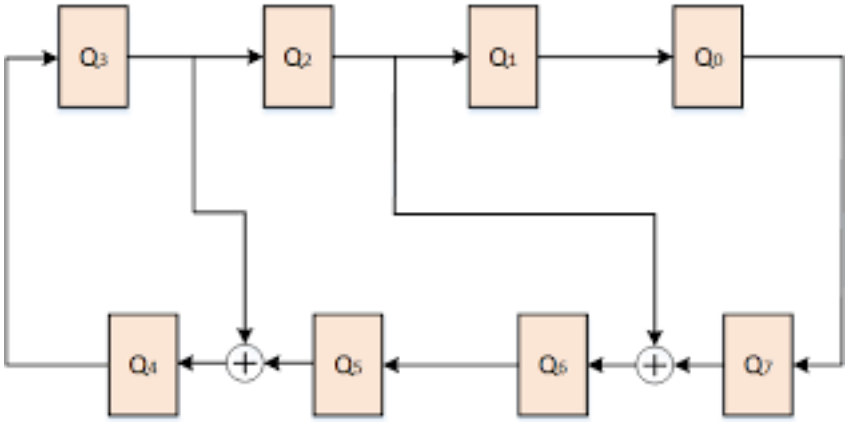

Fig.5 Linear Feedback Shift Register (LFSR)

➢ Basic Concepts of (LFSR)

1.**State**: The current configuration of bits in the register.

2.**Feedback Polynomial**: A polynomial that defines which bits are used to calculate the input. For example, for a 4-bit LFSR, a polynomial like $x^4 + x^3 + 1$ indicates that the 1st and 2nd bits are used for feedback.

3.**Initial State**: The starting state of the LFSR.

Example Calculation

Let's take a 4-bit LFSR with the feedback polynomial $x^4 + x^3 + 1$ and an initial state of 1011.

1.Initial State: 1011 (This is the binary representation)

2.Feedback Calculation:

The bits used for feedback are the 4th and 3rd bits.

Feedback bit = 1 (4th bit) XOR 0 (3rd bit) = 1.

3.Shift the Register:

Shift right: The new state becomes 1101.

The new feedback bit is inserted at the leftmost position.

4.Repeat:

Next State Calculation:

Current state: 1101

Feedback: 1 (4th) XOR 1 (3rd) = 0.

Shift: New state = 0110.

Next State: 0110

Feedback: 0 (4th) XOR 1 (3rd) = 1.

Shift: New state = 1011.

2. Nonlinear Feedback Shift Register (NLFSR)

- Definition: Similar to LFSRs, but the feedback function is nonlinear, making them harder to analyze and predict.
- Structure: Uses non-linear functions (e.g., AND, OR , XOR combinations) in feedback to create complex sequences.

- Usage in Stream Ciphers:
  - NLFSRs are used in some modern stream ciphers to improve security over LFSRs.
  - They can generate more complex and unpredictable key streams, making them resilient to traditional cryptanalysis methods.

Example in

- Stream Ciphers: Grain and Trivium are two lightweight stream ciphers that use NLFSRs as part of their key stream generation mechanism.
- Advantages: More secure than LFSRs against linear attacks.
- Disadvantages: More complex and computationally demanding, which can affect performance.

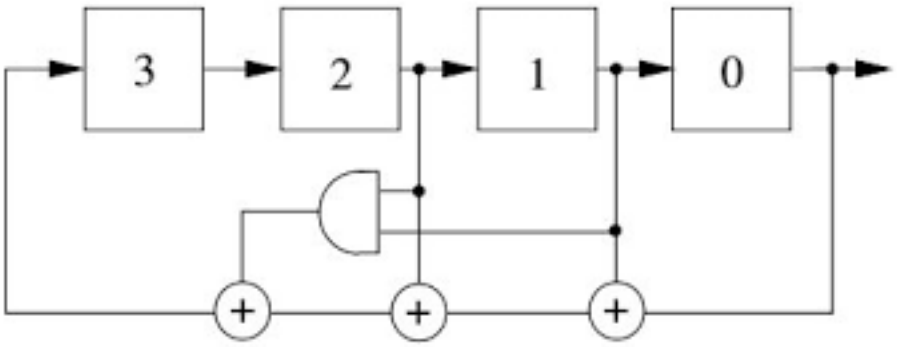

Fig.6 Nonlinear Feedback Shift Register (NLFSR)

➢ Basic Concept of NLFSR

1. **Registers**: An NLFSR is composed of a series of registers (or bits). Each bit in the register can be either 0 or 1.
2. **Feedback Function**: A non-linear function determines how the feedback bit is calculated. This function often involves operations like XOR, AND, OR, and NOT.
3. **Feedback Process**: In each cycle, the NLFSR shifts the bits to the right, and the feedback bit, calculated using the non-linear function, is placed in the leftmost bit.

Example NLFSR Calculation

Consider a simple NLFSR with a 4-bit register. Let's define:

- **Initial State**: 1010
- **Non-linear Feedback Function**: $f(x1, x2, x3, x4) = x1 \oplus (x2 \wedge x4)$

Here:

- $\oplus$: XOR
- $\wedge$: AND

In each cycle:

1. Calculate the new leftmost bit using the feedback function.
2. Shift all bits to the right.
3. Insert the new bit into the leftmost position.

Step-by-Step Calculation

Cycle 1

- **Current State**: 1010
- **Feedback Bit Calculation**: $f(x1, x2, x3, x4) = 1 \oplus (0 \wedge 0) = 1 \oplus 0 = 1$
- **New State**: 1101

Cycle 2

- **Current State**: 1101
- **Feedback Bit Calculation**: $f(x1, x2, x3, x4) = 1 \oplus (1 \wedge 1) = 1 \oplus 1 = 0$
- **New State**: 0110

Cycle 3

- **Current State**: 0110
- **Feedback Bit Calculation**: $f(x1, x2, x3, x4) = 0 \oplus (1 \wedge 0) = 0 \oplus 0 = 0$
- **New State**: 0011

Cycle 4

- **Current State**: 0011
- **Feedback Bit Calculation**: $f(x1, x2, x3, x4) = 0 \oplus (0 \wedge 1) = 0 \oplus 0 = 0$
- **New State**: 0001

And so on. The NLFSR will continue to generate a sequence based on this feedback function.

3. Combining LFSRs and NLFSRs in Stream Ciphers

- Hybrid Stream Ciphers: Some stream ciphers use a combination of LFSRs and NLFSRs to balance performance and security. The LFSR provides speed and simplicity, while the NLFSR adds nonlinearity and complexity.

- Examples:
  - Trivium: A lightweight stream cipher used in IoT devices, combines multiple LFSRs and NLFSRs to create a highly secure but efficient keystream generator.

  - Grain: Another lightweight cipher that integrates LFSRs and NLFSRs for secure encryption in resource-constrained environments.