جامـــعـة المـــســتـقـبـل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قســـم علوم الامن السيبراني

Cyber Security Department

Subject: Shift Registers and Their Types in Stream Ciphers

Class: 2nd

Lecturer: Asst.Lect Mustafa Ameer Awadh

Lecture: (4)

Study Year: 2024-2025

Introduction to Shift Registers

Shift registers are fundamental components in digital electronics, playing a crucial role in data storage, manipulation, and transfer. As a type of sequential logic circuit, they are designed to store multiple bits of data and facilitate the movement of this data in a controlled manner. Shift registers can shift data either to the left or to the right, making them versatile tools for various applications, including data serialization, parallel-to-serial conversion, and digital signal processing.

- Definition: A shift register is a sequential logic circuit that is used to store and shift data. It's composed of a series of flip-flops connected in a chain, where each flip-flop holds a single bit.
- Basic Structure: Typically consists of flip-flops connected in series, with outputs connected to the inputs of the next flip-flop.
- Data Shifting: Data moves from one flip-flop to the next on each clock cycle, which is why it's called a "shift" register.

Types of Shift Registers

- Serial-in Serial-out (SISO): Data enters one bit at a time and shifts out one bit at a time. Commonly used for data transmission. (fig.1 shows the SISO operation)
- Serial-in Parallel-out (SIPO): Data is input serially, and after shifting through the register, it's available at all output pins simultaneously. Useful for converting serial data to parallel format.

- Parallel-in Serial-out (PISO): Data is loaded into the register simultaneously (in parallel) and then shifted out serially. Useful for converting parallel data to serial.
- Parallel-in Parallel-out (PIPO): Data is loaded and output in parallel. Often used for temporary data storage.

These are used in digital systems for data storage, data transfer, and in cryptographic systems.

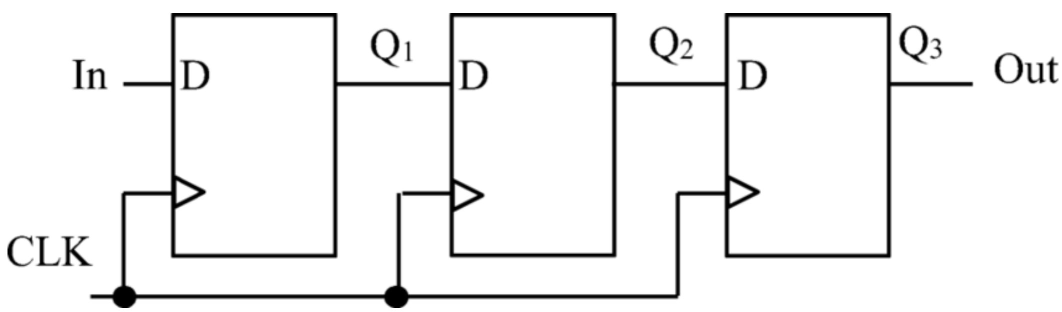

Fig.1 shows the SISO operation.

Initial State:

Assume all the flip-flops (Q1, Q2, and Q3) initially hold 0.**Clock Cycle 1** The data bit at the In input (e.g., 1) is transferred to Q1. Q1 now holds 1,and Q2 and Q3 still hold **Clock Cycle2** The value of Q1 (now 1) shifts to Q2, and a new bit at the In input enters Q1 .If In is 0, then Q1 = 0, Q2 = 1, and Q3 = 0.**Clock Cycle 3** The value of Q2 (now 1) shifts to Q3, and Q1 and Q2 receive new bits from the input and from Q1, respectively.

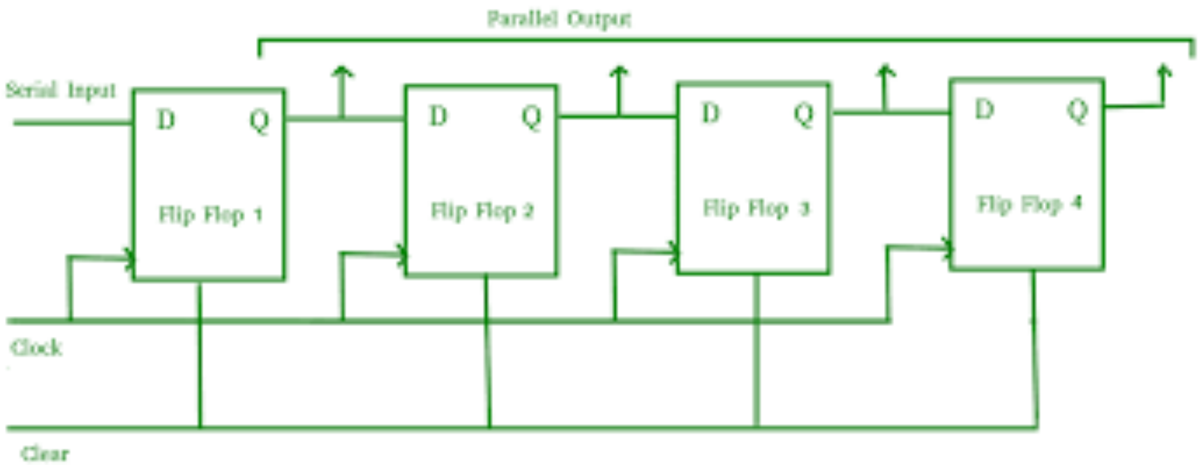

Fig.2 Shows SIPO operation.

1. **D Flip-Flops (Flip Flop 1, Flip Flop 2, Flip Flop 3, Flip Flop 4)**:
   - Each block labeled D is a D flip-flop, used to store one bit.
   - Each flip-flop has a D input (data), a Q output, a clock input (Clock), and a clear input (Clear).
   - When a clock pulse is applied, the bit on the D input is transferred to the Q output.
2. **Serial Input**:
   - The Serial Input is where data enters the shift register one bit at a time.
   - With each clock pulse, this data bit shifts through the flip-flops.
3. **Clock**:
   - The clock signal (Clock) is connected to each flip-flop, ensuring synchronized data transfer with each clock pulse.
   - This clock pulse moves data from one flip-flop to the next.

4. **Clear**:
    - The Clear input resets all flip-flops.
    - When activated, it sets the output Q of each flip-flop to 0, effectively clearing the register.
5. **Parallel Output**:
    - The outputs (Q) of each flip-flop are used as parallel outputs.
    - After the data has been shifted through all the flip-flops, it can be read simultaneously from each Q output.

3. Shift Registers in Cryptography

- Importance in Cryptography: Shift registers are key components in digital cryptography, especially for generating pseudorandom sequences in stream ciphers.
- Role in Stream Ciphers: Stream ciphers use shift registers to produce a key stream, which is then XORed with plaintext bits to create cipher-text. This process requires high-quality pseudo-randomness.

4. 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:

4.1 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.

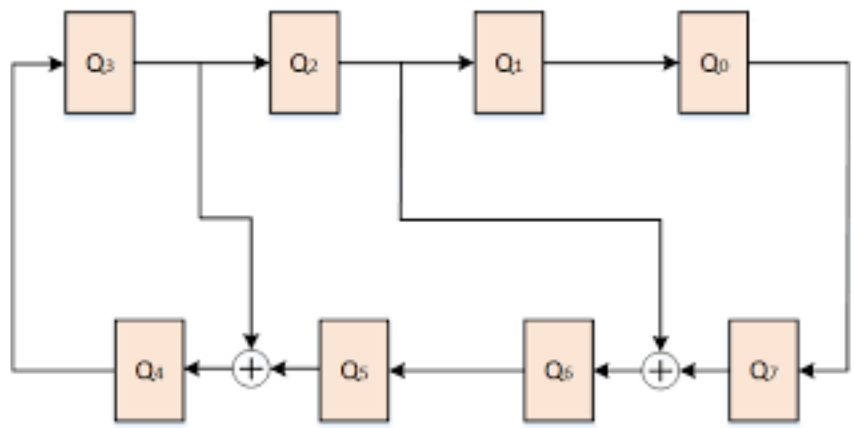

Fig.3 Linear Feedback Shift Register (LFSR)

Basic Concepts

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 $x\text{^}4\ +\ x\text{^}3\ +\ 1$ 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.

4.2 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.

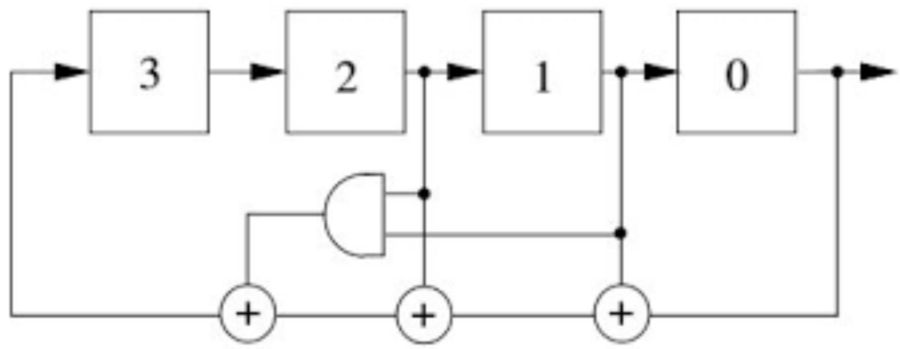

Fig.4 Nonlinear Feedback Shift Register (NLFSR)

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.

5. 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.

6. Applications of Shift Registers in Stream Ciphers

- Mobile Communication: Ciphers like A5/1 and A5/2 for GSM mobile networks use LFSRs to generate keystreams.
- Wireless Protocols: Many wireless protocols, including Bluetooth and Wi-Fi, rely on stream ciphers with LFSRs and NLFSRs to secure data transmission.
- IoT Devices: Lightweight stream ciphers that use shift registers (like Grain and Trivium) are popular in IoT due to their minimal computational requirements.

7. Security Concerns and Attack Techniques

- Correlation Attacks: Attackers exploit statistical weaknesses in LFSRs to correlate the keystream with certain states of the shift register.

- Berlekamp-Massey Algorithm: This algorithm can reconstruct the structure of an LFSR if enough keystream bits are available, making it easy to predict future output.
- Countermeasures:
    - Use NLFSRs to increase complexity.
    - Combine multiple LFSRs and NLFSRs with different feedback mechanisms.
    - Regularly reseed the shift registers to prevent long-term correlations.

8. Advantages and Disadvantages of Using Shift Registers in Stream Ciphers

- Advantages:
    - Efficient in hardware, allowing for high-speed cryptographic applications.
    - Simple to implement and analyze, especially in the case of LFSRs.
- Disadvantages:
    - LFSRs are vulnerable to various cryptographic attacks due to their linearity.
    - NLFSRs, though more secure, are complex to design and may consume more power.