Lecture Three

Stream Cipher and Shift Register

9. Engineering Concepts of Shift Register

A **feedback shift register** is made up of two parts: a shift register and a **feedback function** (see figure (7)). The shift register is a sequence of bits, (the length of a shift register is figured in bits). Each time a bit is needed, all of the bits in the shift register are shifted 1 bit to the right. The new left-most bit is computed as a function of the other bits in the register. The output of the shift register is 1 bit, often the least significant bit. The period of a shift register is the length of the output sequence before it starts repeating.

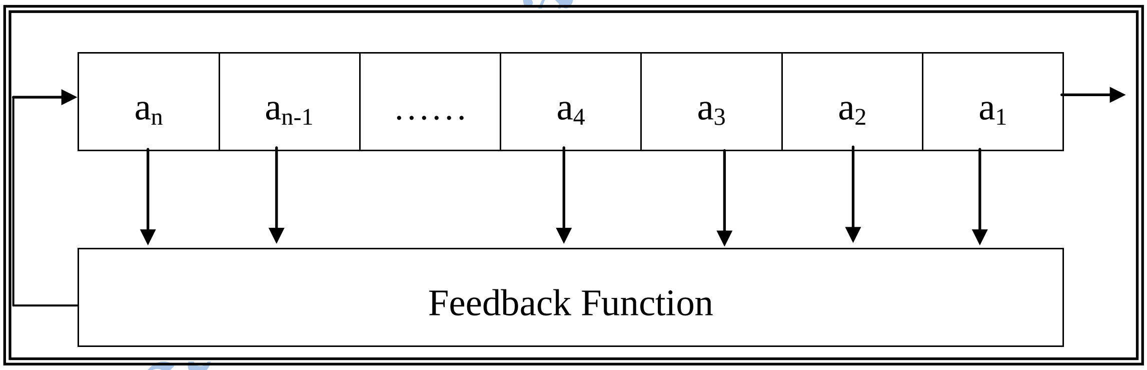

Figure (7) Feedback Shift Register.

Cryptographers have liked stream ciphers made up of shift registers: They are easily implemented in digital hardware. We will only touch on the mathematical theory. Ernst Selmer, the Norwegian governments' chief cryptographer, worked out the theory of shift register sequences in 1965. Solomon Golomb, an NSA mathematician, wrote a book with Selmers results and some of his own.

The simplest kind of feedback shift register is a **Linear Feedback Shift Register** (LFSR), as described in figure (8). The feedback function is simply the XOR of certain bits in the register; the list of these bits is called a **tap sequence**. Because of the simple feedback sequence, a large body of mathematical theory can be applied to analyzing LFSRs. Cryptographers like to analyze sequences to convince themselves that they are random enough to be secure. LFSR's are the most common type of shift registers used in cryptography.

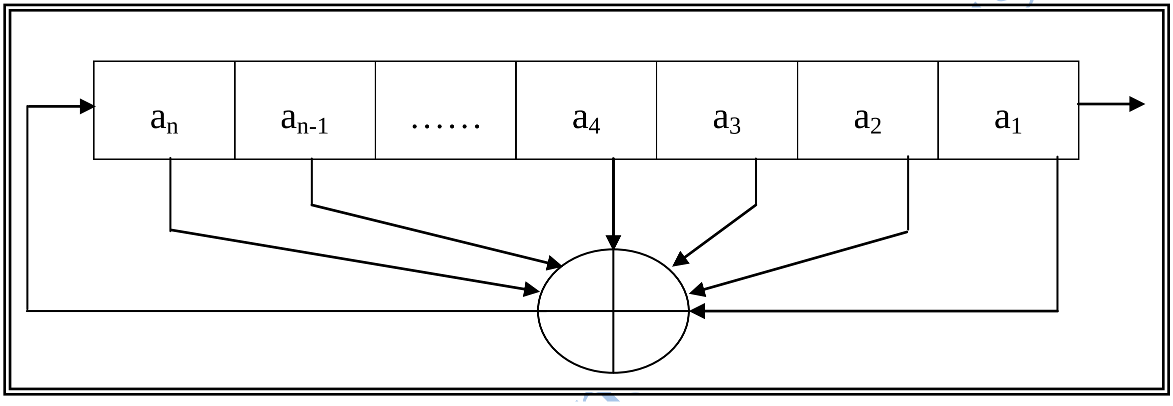

Figure (8) Linear Feedback Shift Register.

For example, a 3-bit LFSR tapped at the first and third bit. If it is initialized with the value 111, it produces the following sequence of internal states before repeating:

1	1	1
0	1	1
1	0	1
0	1	0
0	0	1
1	0	0
1	1	0

The output sequence is the string of least significant bits: 1110100…

In order for a particular LFSR to be a **maximal-period LFSR**, the polynomial formed from a tap sequence plus the constant 1 must be a primitive polynomial mod 2. The degree of the polynomial is the length of the shift register. A primitive polynomial of degree n is an irreducible polynomial.

Most practical stream-cipher designs center around LFSR. In the early days of electronics, they were very easy to build. A shift register is nothing more than an array of bit memories and the feedback sequence is just a series of XOR gates. A LFSR-based stream cipher can give you a lot of security with only a few logic gates.

Linear feedback shift registers (LFSRs) are used in many of the keystream generators that have been proposed in the literature. There are several reasons for this:

1. LFSRs are well-suited to hardware implementation.
2. They can produce sequences of large period.
3. They can produce sequences with good statistical properties.
4. Because of their structure, they can be readily analyzed using algebraic techniques.

A linear feedback shift register (LFSR) of length L consists of L stages (or delay elements) numbered 0,1,…,L−1, each capable of storing one bit and having one input and one output; and a clock which controls the movement of data. During each unit of time the following operations are performed:

1. The content of stage 0 is output and forms part of the output sequence.
2. The content of stage i is moved to stage i−1 for each i, 1≤i≤L−1.
3. The new content of stage L−1 is the feedback bit sj which is calculated by adding together modulo 2 the previous contents of a fixed subset of stages 0,1,…,L−1.

Every output sequence (i.e., for all possible initial states) of an LFSR $\langle L, C(D)\rangle$ is periodic if and only if the connection polynomial C(D) has degree L.

If $C(D) \in Z_2[D]$ is a primitive polynomial of degree L, then $\langle L, C(D)\rangle$ is called a **maximum-length LFSR**. The output of a maximum-length LFSR with non-zero initial state is called an **m-sequence**.