Lecture Three

Stream Cipher and Shift Register

10. Mathematical Model of LFSR's-Systems

Every LFSR's-system consists of two main units, the LFSR unit and Combining Function (CF).

10.1 LFSR Unit

Every LFSR's-system consists of collection of linear shift registers, every one shifted alone in one time, as the nature of connection function, each LFSR produces independent sequence.

The LFSR unit depends on:

- LFSR's length.
- Connection function.
- The initial values of LFSR.

Two LFSR's are said to be similar if they have equal length and the same connection function, otherwise the called different. The single LFSR considered the smallest LFSR's-system.

10.2 Combining Function Unit

The Combining Function, denoted by F_n, is a Boolean function (we focus on Boolean function defined on GF(2)) its inputs are the sequences generated from each LFSR. If $x_1,x_2,\ldots,x_n$ are input of F_n s.t. $x_i \in GF(2)$, $i=1,2,\ldots,n$ then:

$$F_n(x_1,x_2,\ldots,x_n)=a_0 \oplus \sum_{i=1}^{n} a_i x_i \oplus \sum_{i,j} a_{ij} x_i \oplus \ldots \oplus a_{12\ldots n} \prod_{i=1}^{n} x_i \qquad \ldots(10.1)$$

Where $a_0,a_i,a_{ij},\ldots,a_{12\ldots n} \in GF(2)$ are the coefficients for combination of LFSR's combined in Boolean function.

Example (10.1):

1. if all the coefficients are zero's except $a_i=1$, $\forall i$, then:

$$L_n(x_1,x_2,\ldots,x_n)=\sum_{i=1}^{n} x_i \qquad \ldots(10.2)$$

   This function is the linear function.

2. if all the coefficients are zero's except $a_{12\ldots n}=1$, then:

$$P_n(x_1,x_2,\ldots,x_n)=\prod_{i=1}^{n} x_i \qquad \ldots(10.3)$$

   This function is the non-linear product function.

3. if all the coefficients are zero's except $a_{12}= a_{13}= a_{23}=1$, then:

$$M_n(x_1,x_2,\ldots,x_n)=x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \qquad \ldots(10.4)$$

   This function is non-linear called majority function.

The combining function depends on following elements:

- **Input sequences**: they are the sequences which are generated form LFSR's.

- **Output sequence**: It's the sequence which produced from mixing the input sequences of combining function.

Definition (10.1): We called the function F_n **balance** function if $p(z=0)=p(z=1)=\frac{1}{2}$, where z is the output variable of combining function and p(z) is the probability of the output z=0 or 1, otherwise it is not balance.

Definition (10.2): We called the function F_n **symmetric** function if the arrangement of the input sequences don't effect on the output sequence.

10.3 Boolean Table of Combining Function

It's also called Truth Table of combining function, it’s a table represent the behavior of the Boolean function for all input possibilities. As usual, its consists of n+1 column, n are the inputs variables x_i of F_n and one for output of function F_n, and 2^n row, because for n inputs there are 2^n possible. The important benefit of truth table is finding the output value of each combination of inputs. And since the feedback function is Boolean function then we can express this function as truth table.

Example (10.2):

The truth tables of functions mentioned in equations (10.2), (10.3) and (10.4) can be expressed in table (2), when use n=3.

Table (2) Truth table of three functions for n=3.

Input			**Output**		
x_1	x_2	x_3	L_3	P_3	M_3
0	0	0	0	0	0
0	0	1	1	0	0
0	1	0	1	0	0
0	1	1	0	0	1
1	0	0	1	0	0
1	0	1	0	0	1
1	1	0	0	0	1
1	1	1	1	1	1

Remark (10.1): form table (2), notice the following:

1. Since n=3 then there are $2^3=8$ input possible.
2. L_3 and M_3 are balance, but P_3 is not.
3. All three functions are symmetric.

The other benefit of truth table, when the inputs and output of the truth table is known but the function is not then the logical expression of the function can be known from the truth table, as shown in table (3).

If x_i denotes the variable x in the input i and $X=(x_1,x_2,\ldots,x_n)$, then:

$h_j(X)=\prod_{i=1}^{n} a_i$, $j=1,\ldots,2^n$.

s.t.

$$a_i=\begin{cases} x_i\oplus 1, & x_i=0 \\ x_i, & x_i=1 \end{cases}$$

The values of a_i changes when j changes, and then sum and multiply (module 2), therefore the logical expression of combining function is:

$$F_n(x_1,x_2,\ldots,x_n)=\sum_{i=1}^{2^n \oplus} h_j(X)b_j \qquad \ldots(10.5)$$

Where b_j denotes the output of the function at row j.

Table (3) Boolean table for unknown function.

x_1	x_2	$\cdots$	x_n	h(X)	F_n
0	0	$\cdots$	0	$(x_1\oplus1)(x_2\oplus1)\cdots(x_n\oplus1)$	b_1
0	0	$\cdots$	1	$(x_1\oplus1)(x_2\oplus1)\cdots x_n$	b_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	$\cdots$	0	$x_1x_2\cdots(x_n\oplus1)$	b_{2^n-1}
1	1	$\cdots$	1	$x_1x_2\cdots x_n$	b_{2^n}

Example (10.3):

Let's have the truth table of unknown function F_3, we attempt to find the logical expression of F_3.

Input			**Output**
x_1	**x_2**	**x_3**	**F_3**
0	0	0	1
0	0	1	0
0	1	0	0

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

Then the logical expression of the function F_3 is:

$$F_3(x_1,x_2,x_3)=(x_1\oplus 1)(x_2\oplus 1)(x_3\oplus 1)\oplus(x_1\oplus 1)x_2x_3\oplus x_1(x_2\oplus 1)x_3\oplus x_1x_2x_3$$

$$= x_1x_2\oplus x_1\oplus x_2\oplus x_3\oplus 1$$