Constructing and Solving the System of Linear Equations Produced From LFSR Generators

F.H. Ail and A. A. Hussein
Department of Mathematics, College of Science, University Al-Mustansiriyah
Department of Mathematics ,Ibn-Al- Haitham College of Education, University of Baghdad

Abstract

Linear Feedback Shift Register (LFSR) systems are used widely in stream cipher systems field. Any system of LFSR's which wauldn't be attacked must first construct the system of linear equations of the LFSR unit. In this paper methods are developed to construct a system of linear/nonlinear equations of key generator (a LFSR's system) where the effect of combining (Boolean) function of LFSR is obvious. Before solving the system of linear/nonlinear equations by using one of the known classical methods, we have to test the uniqueness of the solution. Finding the solution to these systems mean finding the initial values of the LFSR's of the generator. Two known generators are used to test and apply the ideas of the paper, these generators are the linear system and Brüer system.

Introduction

A LFSR System (LFSRS) consists of two main basic units. First, is a LFSR function and initial state values (1). The second one is, the Combining Function (CF), which is a boolean function (2). Most of all stream cipher systems depend on these two basic units. Figure 1 shows a simple diagram of LFSR's consists of n LFSR's.
This paper aims to find the initial values of every LFSR in the system depending on the following information:

- The length of every LFSR and their feedback functions are known.
- The CF is known.
- The output sequence S (keystream) generated from the LFSRS or part of it known, or, practically, this means, a known plain attack is applied (1).

This research consists of three stages, constructing system of linear/nonlinear equations, test the uniqueness of the solution of this system, and lastly, solving the system of linear/ nonlinear equations.

Constructing A System of Linear/Nonlinear Equations

Before involving in solving the System of Linear Equations (SLE), it should show how could the SLE be of a single LFSR constructed, since it is considered as a basic unit of LFSRS. Let's assume that all LFSR's are maximum LFSR. This means, Period (P)=2^r-1, where r is LFSR length.

Constructing LES for Single LFSR

Let SR_r denotes a single LFSR with length r, let $A_0=(a_{-1},a_{-2},\ldots,a_{-r})$ be the initial value vector of SR_r, s.t. a_{-j}, $1\le j\le r$, be the component j of the vector A_0, in another word, a_{-j} is the initial bit of stage j of SR_r, let $C_0^T=(c_1,\ldots,c_r)$ be the feedback vector, $c_j\in\{0,1\}$, if $c_j=1$ that means the stage j is connected. Let $S=\{s_i\}_{i=0}^{m-1}$ be the sequence (or $S=(s_0,s_1,\ldots,s_{m-1})$ read "S vector") with a length m generated from SR_r. The generation of S depends on the following equation (3):

$$s_i=a_i=\sum_{j=1}^{r}a_{i-j}c_j \quad i=0,1,\ldots \qquad \ldots[1]$$

Equation [1] represents the linear recurrence relation.

The objective finds the A_0, when r, C_0 and S are known.
Let M be a r×r matrix, which describes the initial phase of SR_r
$M=(C_0|I_{r\times r-1})$, where $M^0=I$.

Let A_1 represents the new initial of SR_r after one shift, s.t.

$$A_1=A_0\times M=(a_{-1},a_{-2},\ldots,a_{-r})\begin{pmatrix} c_1 & 1 & \cdots & 0 \\ c_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ c_r & 0 & \cdots & 0 \end{pmatrix}=(\sum_{j=1}^{r} a_{-j}c_j\ ,a_{-1},\ldots,a_{1-r}).$$

In general,

$$A_i=A_{i-1}\times M,\ i=0,1,2,\ldots \qquad \ldots[2]$$

Equation [2] can be considered as a recurrence relation, so we have:

$$A_i=A_{i-1}\times M=A_{i-2}\times M^2=\ldots=A_0\times M^i \qquad \ldots[3]$$

The matrix M^i represents the i phase of SR_r, equations [2,3] can be considered as a Markov Process s.t., A_0, is the initial probability distribution, where A_i represents probability distribution and M is the transition matrix (3, 4).

notice that:

$M^2=[C_1C_0|I_{r\times r-2}]$ and so on until we get $M^i=[C_{i-1}\ldots C_0|I_{r\times r-i}]$, where $1\le i<r$.

When $C_P=C_0$ then $M^{P+1}=M$.

Now let's calculate C_i (5) s.t.

$$C_i=M\times C_{i-1},\ i=1,2,\ldots \qquad \ldots[4]$$

Equation [1] can be rewritten as:

$$A_0\times C_i=s_i\ ,\ i=0,1,..,r-1 \qquad \ldots[5]$$

When i=0 then $A_0\times C_0=s_0$ is the 1st equation of the SLE,

i=1 then $A_0\times C_1=s_1$ is the 2nd equation of the SLE, and

i=r-1 then $A_0\times C_{r-1}=s_{r-1}$ is the rth equation of the SLE.

In general:

$$A_0\times C=S \qquad \ldots[6]$$

C represents the matrix of all C_i vectors s.t.

$C=(C_0C_1\ldots C_{r-1})$ ...[7]

The LES can be formulated as:

$Y=[\,C^T|S^T]$ ...[8]

Y represents the extended matrix of the LES.

Example (1)

Let the SR_4 has $C_0^T=(0,0,1,1)$ and $S=(1,0,0,1)$, by using equation [4], we get:

$$C_1=M\times C_0=\begin{pmatrix}0&1&0&0\\0&0&1&0\\1&0&0&1\\1&0&0&0\end{pmatrix}\begin{pmatrix}0\\0\\1\\1\end{pmatrix}=\begin{pmatrix}0\\1\\1\\0\end{pmatrix},$$ in the same way,

$$C_2=\begin{pmatrix}1\\1\\0\\0\end{pmatrix},C_3=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$$

From equation [6] we have:

$$A_0\begin{pmatrix}0&0&1&1\\0&1&1&0\\1&1&0&1\\1&0&0&1\end{pmatrix}=(1,0,0,1),$$ this system can be written as equations:

$a_{-3}+a_{-4}=1$
$a_{-2}+a_{-3}=0$
$a_{-1}+a_{-2}=0$
$a_{-1}+a_{-3}+a_{-4}=1$

Then the SLE after using formula [8] is:

$$Y=\left[\begin{array}{cccc|c} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{array}\right] \qquad \ldots[9]$$

Construction of SLE for LFSRS

Let's have n of SR_{r_j} with length r_j, j=1,2,…,n, with feedback vector $C_{0j}=\begin{pmatrix} c_{01j} \\ c_{02j} \\ \\ c_{0r_j,j} \end{pmatrix}$, and have unknown initial value vector $A_{0j}=(a_{1j},\ldots,a_{rj})$, so SR_{r_j} has $M_j=(C_{0j}|I_{r_j\times r_j-1})$

By using recurrence equation [4],

$C_{ij}=M_j\times C_{i-1,j}$, i=1,2,… …[10]

by using equation [5]:

$A_{0j}\times C_{ij}=s_{ij}$, i=0,1,…,r-1 and $S_j=(s_{0j},s_{1j},\ldots,s_{m-1,j})$.

S_j represents the output vector of SR_{r_j}, which of course, is unknown too. m represents the number of variables produced from the LFSR's with consideration to CF, in the same time it represents the number of equations which are needed to solve the SLE. Of course, there is n of SLE (one SLE for each SR_{r_j} with unknown absolute values).

Now, let A_0 be the extended vector for m variables, which consists of initial values from all LFSR's and C is the matrix of C_i vectors considering the CF, C_i represents the extended vector of all feedback vectors C_{ij}, then $A_0\times C=S$.

To apply the construction process, two known systems are chosen which are: the linear system and Brüer generator.

Linear System

As known, the outputs of every LFSR of the linear system are XORed with each other to gain the sequence S which is generated from this system.

Since the SR_{r_j} has r_j number of unknown initial values, then $m=\sum_{j=1}^{n} r_j$.

Now, all the vectors A_{0j} are extended from r_j to m as follows:

$A_{01}=(a_{-11},...,a_{-r_1 1},0...0,...,0...0)$

$A_{02}=(0...0,a_{-12},...,a_{-r_2 2},...,0...0)$

And so on..

$A_{0n}=(0...0,0...0,\ ...,a_{-1n},...,a_{-r_n n})$

And let

$$A_0=\sum_{j=1}^{n} A_{0j}=(a_{-11},...,a_{-r_1 1},a_{-12},...,a_{-r_2 2},...,a_{-1n},...,a_{-r_n n})$$

In fact, A_0 represents a concatenation of all A_{0j} vectors respectively. The same process will be done on the feedback vectors C_{ij} which must be found first from equation [10]. Therefore, C_i will be the extended concatenation vector of all feedback C_{ij} vectors too, s.t.

$$C_i=\begin{pmatrix} C_{i1} \\ C_{i2} \\ \vdots \\ C_{in} \end{pmatrix},\ i=0,1,...,m-1$$

Since the CF is XOR, then S can be obtained from XORed which are all unknown S_j. Since m equations are needed, that means every LFSR shifts m movements, then:

$S_j=(s_{0j},s_{1j},...,s_{m-1,j})$, j=1,2,...,n, and $s_i=\sum_{j=1}^{n} s_{ij}$, i=0,1,...,m-1, (the sum here is XOR), then:

$$S=\sum_{j=1}^{n} S_j=(s_0,s_1,...,s_{m-1})$$

Fig.(2) illustrates the sequence S which is generated from the linear system.

So C can be obtained from equation [7] and by applying equation [6], the SLE can be constructed.

Example (2)

Let's have the following feedback vectors for 3 LFSR with length 2,3 and 4:

$C_{01}=\begin{pmatrix}1\\1\end{pmatrix}$, $C_{02}=\begin{pmatrix}1\\0\\1\end{pmatrix}$ and $C_{03}=\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$, then m=9.

And let S=(1,1,1,0,1,1,0,1,1).

By using equation [4],

$C_{01}=C_{31}=C_{61}=\begin{pmatrix}1\\1\end{pmatrix}$, $C_{11}=C_{41}=C_{71}=\begin{pmatrix}0\\1\end{pmatrix}$, and $C_{21}=C_{51}=C_{81}=\begin{pmatrix}1\\0\end{pmatrix}$.

$C_{02}=C_{72}=\begin{pmatrix}1\\0\\1\end{pmatrix}$, $C_{12}=C_{82}=\begin{pmatrix}1\\1\\1\end{pmatrix}$, $C_{22}=\begin{pmatrix}0\\1\\1\end{pmatrix}$, $C_{32}=\begin{pmatrix}1\\1\\0\end{pmatrix}$, $C_{42}=\begin{pmatrix}0\\0\\1\end{pmatrix}$, $C_{52}=\begin{pmatrix}0\\1\\0\end{pmatrix}$, $C_{62}=\begin{pmatrix}1\\0\\0\end{pmatrix}$.

$C_{13}=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$, $C_{23}=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$, $C_{33}=\begin{pmatrix}0\\1\\1\\1\end{pmatrix}$, $C_{43}=\begin{pmatrix}1\\1\\1\\0\end{pmatrix}$, $C_{53}=\begin{pmatrix}0\\1\\0\\1\end{pmatrix}$, $C_{63}=\begin{pmatrix}1\\0\\1\\0\end{pmatrix}$, $C_{73}=\begin{pmatrix}1\\1\\0\\1\end{pmatrix}$, $C_{83}=\begin{pmatrix}0\\0\\1\\1\end{pmatrix}$.

Then C_0^T=(1,1,1,0,1,1,0,0,1).

The SLE can be written as follows:

$$A_0\begin{pmatrix}1&0&1&1&0&1&1&0&1\\1&1&1&1&1&0&1&1&0\\1&1&0&1&0&0&1&1&1\\0&1&1&1&0&1&0&0&1\\1&1&1&0&1&0&0&1&1\\1&1&1&0&1&0&1&1&0\\0&0&1&1&1&1&0&1&0\\0&1&1&1&1&0&1&0&1\\1&1&1&1&0&1&0&1&1\end{pmatrix}=(1,1,1,0,1,1,0,1,1)$$

s.t. $A_0=(a_{-11},a_{-21},a_{-12},a_{-22},a_{-32},a_{-13},a_{-23},a_{-33},a_{-43})$, and the extended matrix Y can be calculated from equation [8] is:

$$Y=\left[\begin{array}{ccccccccc|c} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

Brüer Generator

As usual, this system consists of odd number (n) of LFSR's (in this case of study, we chose n=3 LFSR's). The CF of this generator is $F(x_1,x_2,x_3)=x_1x_2+x_1x_3+x_2x_3$ (5), for this reason $m=r_1r_2+r_1r_3+r_2r_3$. Its obvious that the mathematical system which is obtained is a system of non-linear equations (SNLE). The SNLE is converted to SLE in order to solve it.

The initial value is:

$A_0=A_{01}A_{02}+A_{01}A_{03}+A_{02}A_{03}=(d_0,d_1,\ldots,d_{m-1})$,

s.t. $d_0=a_{-11}a_{-12}$, $d_1=a_{-11}a_{-22},\ldots,d_{m-1}=a_{r_2 2}a_{r_3 3}$, or it can be taken from the following equation:

$$d_k=\begin{cases} a_{-i1}a_{-j2}, \text{when } k=i*r_2+j, \text{s.t. } i=0,\ldots,r_1-1,\ j=0,\ldots,r_2-1 \\ a_{-i1}a_{-j3}, \text{when } k=i*r_3+j+r_1r_2, \text{s.t. } i=0,\ldots,r_1-1,\ j=0,\ldots,r_3-1 \\ a_{-i2}a_{-j3}, \text{when } k=i*r_3+j+r_1r_2+r_1r_3, \text{s.t. } i=0,\ldots,r_2-1,\ j=0,\ldots,r_3-1 \end{cases} \quad \ldots[11]$$

(this arrangement is not standard so it can be changed according to the researcher requirements).

In the same way, equation [11] can be applied on the feedback vector C_{ij}:

$C_i=C_{i1}C_{i2}+C_{i1}C_{i3}+C_{i2}C_{i3}$.

And the sequence S will be:
$S=S_1S_2+S_1S_3+S_2S_3$ s.t. $s_i=s_{i1}s_{i2}+s_{i1}s_{i3}+s_{i2}s_{i3}$,
s_i is the element i of S.
So the SNLE can be obtained by equation [6].

Fig.(3) illustrates the sequence S which is generated from Brüer Generator.

Example(3)

Let's use the same information of example (2), then:
m=26, S=(1,0,1,1,0,1,1,1,1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,0,1,1,0)

$$C_{01}=C_{31}=C_{61}=C_{91}=C_{12,1}=C_{15,1}=C_{18,1}=C_{21,1}=C_{24,1}=\begin{pmatrix}1\\1\end{pmatrix},$$

$$C_{11}=C_{41}=C_{71}=C_{10,1}=C_{13,1}=C_{16,1}=C_{19,1}=C_{22,1}=C_{25,1}=\begin{pmatrix}0\\1\end{pmatrix},$$

$$C_{21}=C_{51}=C_{81}=C_{11,1}=C_{14,1}=C_{17,1}=C_{20,1}=C_{23,1}=\begin{pmatrix}1\\0\end{pmatrix}.$$

$$C_{02}=C_{72}=C_{14,2}=C_{21,2}=\begin{pmatrix}1\\0\\1\end{pmatrix},C_{12}=C_{82}=C_{15,2}=C_{22,2}=\begin{pmatrix}1\\1\\1\end{pmatrix},$$

$$C_{22}=C_{92}=C_{16,2}=C_{23,2}=\begin{pmatrix}0\\1\\1\end{pmatrix},C_{32}=C_{10,2}=C_{17,2}=C_{24,2}=\begin{pmatrix}1\\1\\0\end{pmatrix},$$

$$C_{42}=C_{11,2}=C_{18,2}=C_{25,2}=\begin{pmatrix}0\\0\\1\end{pmatrix},C_{52}=C_{12,2}=C_{19,2}=\begin{pmatrix}0\\1\\0\end{pmatrix}, C_{62}=C_{13,2}=C_{20,2}=\begin{pmatrix}1\\0\\0\end{pmatrix}.$$

$$C_{03}=C_{15,3}=\begin{pmatrix}1\\0\\0\\1\end{pmatrix},C_{13}=C_{16,3}=\begin{pmatrix}1\\0\\1\\1\end{pmatrix},C_{23}=C_{17,3}=\begin{pmatrix}1\\1\\1\\1\end{pmatrix},C_{33}=C_{18,3}=\begin{pmatrix}0\\1\\1\\1\end{pmatrix},$$

$$C_{43}=C_{19,3}=\begin{pmatrix}1\\1\\1\\0\end{pmatrix},C_{53}=C_{20,3}=\begin{pmatrix}0\\1\\0\\1\end{pmatrix},C_{63}=C_{21,3}=\begin{pmatrix}1\\0\\1\\0\end{pmatrix},C_{73}=C_{22,3}=\begin{pmatrix}1\\1\\0\\1\end{pmatrix},$$

$$C_{83}=C_{23,3}=\begin{pmatrix}0\\0\\1\\1\end{pmatrix},C_{93}=C_{24,3}=\begin{pmatrix}0\\1\\1\\0\end{pmatrix},C_{10,3}=C_{25,3}=\begin{pmatrix}1\\1\\0\\0\end{pmatrix},C_{11,3}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix},C_{12,3}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix},$$

$$C_{13,3}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix},C_{14,3}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}.$$

by applying equation [4], C_0^T will be:

$C_0^T=(1,0,1,1,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,0,0,0,0,1,0,0,1)$.

Therefore,

$$Y=\left[\begin{array}{cccccccccccccccccccccccccccc|c}1&0&1&1&0&1&1&0&0&1&1&0&0&1&1&0&0&1&0&0&0&0&1&0&0&1&1\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\ 0&0&0&0&0&1&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0\end{array}\right]\ldots[12]$$

LES/NLES Constructing Algorithm can be introduced to illustrate the construction of SLE.

SLE Constructing Algorithm

INPUT : **READ** CR; {*Single LFSR(1)/Linear(2)/Brüer(3)* }
READ n; { *number of LFSR's in cryptosystems* }
FOR j := 1 **TO** n **Do**
BEGIN
READ r_j ;{ *Length of* $LFSR_j$}
READ C_{0j}^{T} vector; { *Feedback connection of* $LFSR_j$}
$M_j := (C_{0j} | I_{r_j \times r_j - 1})$;
READ A_0 vector; { *Initial values of* $LFSR_j$}
END;

INITILIZE : **CASE** CR **OF;**
1 : m := r;
$2 : m := \sum_{j=1}^{n} r_j$;
3: $m := r_1 * r_2 + r_1 * r_3 + r_2 * r_3$;
END; {end case of CR}

PROCESS : **FOR** i := 0 **TO** m-1 **Do**
BEGIN
FOR j = 1 **TO** n **Do**
BEGIN
$C_{ij} := M_j \times C_{i-1,j}$;
$s_{ij} := A_{0j} \times C_{ij}$;
END;
CASE CR **OF**
$2 : s_i := \sum_{j=1}^{n} s_{ij}$; { *XOR sum* }
$C_i := \sum_{j=1}^{n} C_{ij}$; {*Concatenation adding* }
3 : $s_i := s_{i1} * s_{i2} \oplus s_{i1} * s_{i3} \oplus s_{i2} * s_{i3}$;
$C_i := C_{01} * C_{02} + C_{01} * C_{03} + C_{02} * C_{03}$;{*concatenation*}
END; {end case of CR}
END;
FOR j = 1 **TO** n **Do** $S_j := (s_{0j}, s_{1j}, \ldots, s_{m-1,j})$;
CASE CR **OF**
$2 : S := \sum_{j=1}^{n} S_j$; { *XOR sum* }
3 : $S := S_1 * S_2 \oplus S_1 * S_3 \oplus S_2 * S_3$;
END; {end case of CR}
$\mathbf{C}^T := (C_0, C_1, \ldots, C_{m-1})$;
$\mathbf{Y} := [\mathbf{C}^T, \mathbf{S}^T]$;

OUTPUT : Augmented matrix **Y**;
END.

Test For The Uniquness Of The Solution Of Sle/Snle

Since the system consists of m variables, then there are 2^m-1 equations, but only m independent equations are needed to solve the system. If the system contains dependent equations, then the system has no unique solution (i.e. more than one solution or there is no solution). So first it should test the uniqueness of the system by calculating the rank of the system matrix ($r(C^T)$). If the rank equals the matrix degree ($deg(C^T)$), then the system has a unique solution, otherwise when ($r(C^T) < deg(C^T)$) the system has no unique solution.

In order to calculate $r(C^T)$ it should use the elementary operations to convert the C^T matrix to a simplest matrix by making, as many as possible, the elements of the matrix zero's. The elementary operations should be applied in matrix rows and columns (6).

The other method of testing the uniqueness of the solution is by finding the determinant of the matrix. The matrix C^T has a unique solution if and only if $|C^T| \neq 0$ (6).

Example (4)

Let's have the matrix $C^T=\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$, by using the elementary operations, the matrix can be converted to the matrix $C^{T*}=\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, this matrix has a rank = 4 =$deg(C^T)$, then the matrix has a unique solution.

In case of $r(C^T) < deg(C^T)$ (or $|C^T|=0$), this means the uniqueness condition is not satisfied, and we have to replace at least which is equation by another one not used before, then retest the uniqueness. This procedure is repeated until we obtain a SLE which has a unique solution.

Solving The Sle

When we would be sure that the SLE has a unique solution, the SLE can be solved by using one of the most common classical methods, its Gauss Elimination method. This method is chosen since it has less complexity than other methods. As its known that, this method depends on two main stages, first, is by converting the matrix Y to up triangular matrix, and the second one, is finding the converse solution (6). Example (5) shows the solving of a single SLE for one LFSR.

Solving SLE algorithm can introduce an illustration of the steps which solve the SLE.

Solving SLE Algorithm
INPUT: **READ** CR; {*Single LFSR(1)/Linear(2)/Brüer(3)*}
: **CALL** SLE Constructing;
INITIALIZE: Find Augmented Matrix Y;
PROCESS : **REPEAT**
CALL Uniqueness Test;
CALL Rank Test;
IF $r(\mathbf{C}^T) < \deg(\mathbf{C}^T)$ THEN
Replace old equation with new one in SLE;
UNTIL $r(\mathbf{C}^T) = \deg(\mathbf{C}^T)$;
CALL Gauss Elimination Method;
OUTPUT : Find A_0;
END.

Example (5)

Let's use the matrix Y of equation [9], after applying the elementary operations, the up triangular matrix is then:

$$Y' = \left[\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right]$$

Now applying the converse solution to get the initial value vector: $A_0=(0,0,0,1)$.

The SLE of n_LFSR's is more complicated than SLE of a single LFSR, especially, if the CF is a high order (non-linear) function. First, it should solve the variables which consist of multiplying more than one initial variable bits of the combined LFSR's. As an example of Brüer Generator, its going to solve the variables d_k, $1\le k\le m-1$, then solving the initial values a_{ij} since d_k is represented by multiplying two initial bits. In other words, every system has its own LES system because of the CF, so it has its own solving method.

As an example to find the variables a_{ij} of Brüer Generator, first, the solution vector A_0 is divided into 3 parts, these parts have lengths $r_1\times r_2$, $r_1\times r_3$ and $r_2\times r_3$. The first part which consists of $A_{01}.A_{02}$, can be divided in r_1 of parts, each with length r_2, then $A_{02}=(d_0,d_1,\ldots,d_{r_2-1})$ when

$a_{11}=1$, that means we find a_{11} and A_{02}, but if the first r_2 variables ($k=0,1,\ldots,r_2-1$) are zero's that means $a_{11}=0$, and A_{02} cannot be found yet. The process is continued until all A_{01} and A_{02} elements are found. So it is not hard to found A_{03} if the same technique is applied. Notice later, that only $r_1\times r_2+r_3$ bits are needed from A_0 to find the variables a_{ij}.

In the next example, the SLE system Y which is mentioned in example (3) will be solved.

Example (6)

When solving the SLE of equation [12], then the solved vector of solution is:

$A_0=(d_0,d_1,\ldots d_{25})=(0,1,1,0,0,0,1,1,0,1,0,0,0,0,0,0,0,0,1,1,0,1,1,1,0,1)$.

$A_{01}.A_{02}=(0,1,1,0,0,0)\rightarrow a_{11}.A_{02}=(0,1,1)\rightarrow a_{11}=1$ and $A_{02}=(0,1,1)$.

$a_{21}.A_{02}=(0,0,0)\rightarrow a_{21}=0\rightarrow A_{01}=(1,0)$.

In the same way we get A_{03}=(1,1,0,1).
The problem is solved from 2×3+4=10 bits only.

Conclusion

- If we change our attack from a known plain attack to cipher attack only, which means, changing in the sequence S (non-pure absolute values), so we shall find a new technique to isolate the right equations in order to solve the SLE.
- It is not hard to construct a SLE of any other LFSR systems, of course, we have to know all the necessary information (CF, the number of combined LFSR's and their lengths and tapping).

References

1. Schneier, B. (1997) "*Applied Cryptography (Protocol, Algorithms and Source Code in C.*" Second Edition, John Wiley & Sons Inc.
2. Whitesitt, J. E.(1995) "*Boolean Algebra and its Application*", Addison-Wesley, Reading, Massachusetts, April.
3. Brüer, J. O.(1983) "*On Nonlinear Combination of Linear Shift Register Sequences*", Internal Report, Cryptologia Magazine, XVII: (2) 187-201.
4. Golomb, S.W.(1982) "*Shift Register Sequences*" San Francisco: Holden Day 1967, Reprinted by Aegean Park Press in.
5. Papoulis, A. (2001) "*Probability Random Variables, and Stochastic Process*", McGraw-Hill College, October.
6. Jennings, A. and Mckeown, (1992) "*Matrix Computation*", John Wiley & Sons Inc., November.

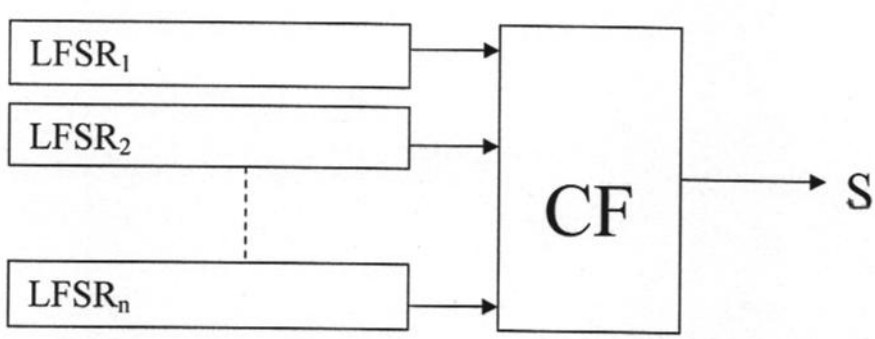

Fig. (1) A system of n_LFSR's

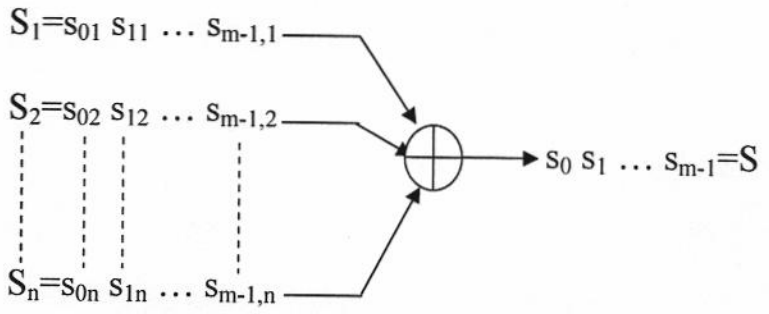

Fig. (2) Linear system

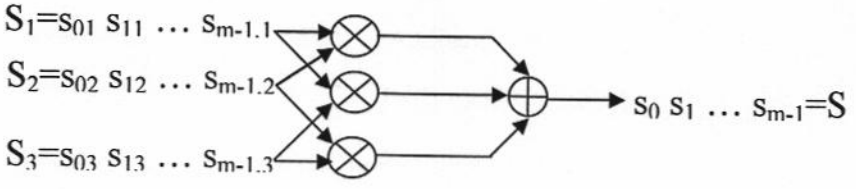

Fig. (3) Brüer generator

بناء وحل نظام من المعادلات الخطية الناتج من مولدات المسجل الزاحف الخطي

فائز حسن علي وعادل عبد الكاظم حسين
قسم الرياضيات ،كلية العلوم،الجامعة المستنصرية
قسم الرياضيات ،كلية التربية ابن الهيثم،جامعة بغداد

الخلاصة

لقد استخدمت انظمة المسجل الزاحف الخطي ذو التغذية التراجعية بشكل واسع في مجال انظمة التشفير الانسيابي. قبل الشروع في مهاجمة اي نظام يعتمد في بنائه على المسجلات الزاحفة، وعليه يجب بناء نظام معادلات خطية لوحدة المسجل الزاحف. في هذا البحث تم تطوير طريقة لبناء نظم خطية/اولاخطية للمولدات العشوائية (نظم المسجلات الزاحفة)، اذ يظهر تأثير الدالة المركبة (المنطقية) للمولد. وقبل الشروع بحل تلك النظم، علينا اختبار توافر ووحدانية الحل لتلك النظم ومن ثم حل هذا النظام باستخدام احدى الطرائق التقليدية المعروفة. ان حل تلك النظم يعني ايجاد القيم الابتدائية للمسجلات الزاحفة المشتركة في المولد.

أستعمل نظامان معروفين يعتمدان في بنائهما على المسجلات الزاحفة الخطية- لاختبار وتطبيق فكرة البحث وهما: المنظومة الخطية ومولد بريو.