Breaking Modified Bruer Generator by Solving the System of Linear Equations of the Generated Sequence

Falih Hassan Awaid

Email: falih_hassen@yahoo.com

Al-Rafidain College University- Software Engineering Dept.

Abstract: *Linear Feedback Shift Register (LFSR) systems are used widely in stream cipher systems field. Golomb used the recurrence relation to find the next state values of single LFSR depending on initial values, s.t. he can be considered the first who can construct a linear equations system of a single LFSR. Attacking of key generator means attempt to find the initial values of the combined LFSR's.*

In this paper, a Golomb's method introduced to construct a linear equations system of a single LFSR. This method developed to construct a linear equations system of key generator (a LFSR system) where the effect of combining function of LFSR is obvious. Finally, before solving the linear equations system, the uniqueness of the solution must be tested, then solving the linear equations system using one of the classical methods like Gauss Elimination. Find

the solution of linear equations system means find the initial values of the generator. One of the known generators; Modified Bruer generator, treated as a practical example of this work.

Keywords: ***Linear Feedback Shift Register (LFSR), System of Linear Equations (SLE), Gauss Elimination Method, Bruer generator.***

1. Introduction

The LFSR System (LFSRS) consists of two main basic units, the feedback 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 System's are depending on these two basic units. Figure (1) shows a simple diagram of LFSRS consists of n LFSR's.

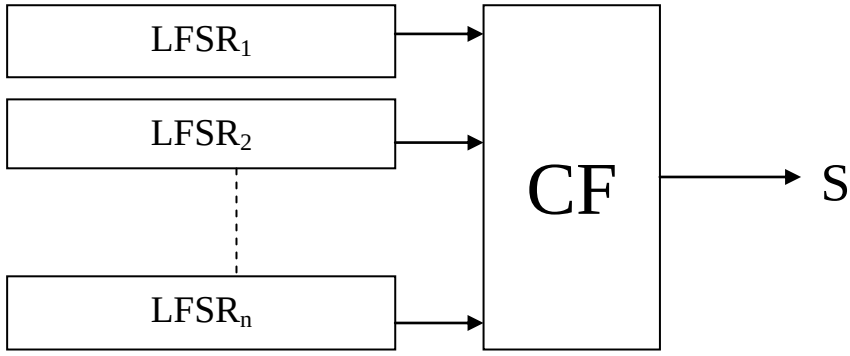

Figure (1) A system of n_LFSR's.

This paper aims to find the initial values of every LFSR in the system depending on the following information:

1. The length of every LFSR and its feedback function are known.
2. The CF is known.

3. The output sequence S (keystream) generated from the LFSRS is known, or part of it, practically, that means, a probable word attack be applied [1].

This work consists of three stages, constructing system of linear equations, testing the existence and the uniqueness of the solution of this system, and lastly, solving the system of linear equations.

2. Constructing a System of Linear Equations for Single LFSR

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

Let SR_r be 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}, $1\leq j\leq r$, 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 length m generated from SR_r. The generating of S depending on the following equation [3]:

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

Equation (1) represents the linear recurrence relation.
The objective is finding the A_0, when r, C_0 and S are known.

Let M be a r×r matrix called the generating matrix or characteristic matrix, which is describes the initial phase of SR_r, where the 1st column is the vector C_0 and the rest columns are the Identity matrix I without the last column.

$$M=(C_0|I_{\,r\times r-1}), \text{ where } M^0=I.$$

Let A_1 represents the new initial state 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,

$$A_i=A_{i-1}\times M,\ i=1,2, \qquad \ldots(2)$$

A_i represents the initial state of SR_r after i shifts.
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, A_i represents probability distribution and M be the transition matrix [4]. notice that:

$M^2=[C_1C_0|I_{r\times r-2}]$ and so on until 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.

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

Where C_i is the feedback vector after i shifts.
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:

$$A_0\times \mathbf{C}=S \qquad \ldots(6)$$

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

$$\mathbf{C}=(C_0C_1\ldots C_{r-1}) \quad \ldots(7)$$

The SLE can be formulated as:

$$Y=[\ \mathbf{C}^T|S^T] \quad \ldots(8)$$

Y represents the extended matrix of the SLE.

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:

s.t. A_0 is the initial state vector of SR_r,

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

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

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

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

(for simplicity we can omitted the sign (-)).
Then the SLE after using formula (8) is:

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

3. Modified Bruer Generator

3.1 Modified Bruer Generator Description

Bruer system as usual consists from odd LFSR's [5]. In this paper, 5 LFSR's are chosen, where the CF of this generator is:

$$F_5(x_1,x_2,x_3,x_4,x_5)=x_1x_2x_3+x_1x_2x_4+x_1x_2x_5+x_1x_3x_4+x_1x_4x_5+x_2x_3x_4 +x_2x_3x_5+x_1x_2x_3+x_2x_4x_5+x_3x_4x_5+x_1x_2x_3x_4+x_1x_2x_3x_5+x_1x_2x_4x_5 +x_1x_3x_4x_5+x_2x_3x_4x_5 \quad \ldots(10)$$

so this system is called modified.

3.2 Efficiency Criteria

1) **Periodicity**

The sequence S has period P(S) when $s_0=s_{P(S)}, s_1=s_{P(S)+1},\ldots$, the period of $LFSR_i$ denotes by $P(S_i)$, P(S) and $P(S_i)$ are least possible positive integers, so

$$P(S)=\text{lcm}(P(S_1),P(S_2),\ldots,P(S_n)) \quad \ldots(11)$$

The period P(S) of S, which product from key generator, depends on the LFSR unit only and there is no effect of CF unit.

P(S) will has lower bound when $r=r_i \ \forall 1\le i\le n$, and upper bound when $P(S_i)$ are relatively prime with each other therefore: $P(S_r)\le P(S)\le \prod_{i=1}^{n} P(S_i)$.

The objective is that key generator must have an upper bound to:

P(S) s.t.:

$$P(S)=\prod_{i=1}^{n} P(S_i) \qquad \ldots(12)$$

It's known earlier that $P(S_i)\le 2^{r_i}-1$, and if the $LFSR_i$ has maximum period then $P(S_i)= 2^{r_i}-1$ [3].

Theorem (1) [6]

$P(S)=\prod_{i=1}^{n}(2^{r_i}-1)$ if and only if the following conditions are holds:

1. $GCD_n(P(S_i))=1$,.
2. the period of each LFSR has maximum period ($P(S_i)= 2^{r_i}-1$).

For Modified Bruer generator $P(S)=\prod_{i=1}^{5}(2^{r_i}-1)$.

Example (2)

if $r_i=2,3,\ldots,6$ for i =1,...,5, then:

P(S)=l.c.m(3,7,15,31,63)
=l.c.m($3^1.5^0.7^0.31^0$, $3^0.5^0.7^1.31^0$, $3^1.5^1.7^0.31^0$,$3^0.5^0.7^0.31^1$, $3^2.5^0.7^1.31^0$)
= $3^{\max(0,1,2)}.5^{\max(0,1)}.7^{\max(0,1)}.31^{\max(0,1)}= 3^2.5^1.7^1.31^1=9765$.

2) Randomness

For our purposes, a sequence generator is pseudo-random if it has this property: It looks random. This means that it passes all the statistical tests of randomness that we can find [1].

Definition (1) [1]: A random bit generator is a device or algorithm which outputs a sequence of statistically independent and unbiased binary digits.

The sequence that is satisfied the 3-randomness properties called PRS [3]. The randomness criterion depends on LFSR's and CF units, therefore from the important conditions to get Pseudo Random Sequence is that the sequence must be maximal and the CF of LFSR system must be balance.

From the truth table of CF of modified Bruer, notice that the ratio of number of 0's to the total output of the function = 32 (2^5=32) is 0.5, this mean the number of 0's = 16 and so as the number of 1's, that's indicates that this generator can generates random sequence.

The truth table of CF is shown in table (1).

Table (1) Truth table of CF of modified Bruer generator.

x_1	x_2	x_3	x_4	x_5	F_5
0	0	0	0	0	0
0	0	0	0	1	0
0	0	0	1	0	0
0	0	0	1	1	0
0	0	1	0	0	0
0	0	1	0	1	0
0	0	1	1	0	0
0	0	1	1	1	1
0	1	0	0	0	0
0	1	0	0	1	0
0	1	0	1	0	0
0	1	0	1	1	1
0	1	1	0	0	0
0	1	1	0	1	1
0	1	1	1	0	1
0	1	1	1	1	1
1	0	0	0	0	0
1	0	0	0	1	0
1	0	0	1	0	0
1	0	0	1	1	1
1	0	1	0	0	0
1	0	1	0	1	1
1	0	1	1	0	1
1	0	1	1	1	1
1	1	0	0	0	0
1	1	0	0	1	1
1	1	0	1	0	1
1	1	0	1	1	1
1	1	1	0	0	1
1	1	1	0	1	1
1	1	1	1	0	1
1	1	1	1	1	1
0.6875	0.6875	0.6875	0.6875	0.6875	0.5
Correlation Probability (CP_i) for each LFSR					Ratio of "0"

Note: the shaded cells means the similarity between x_i and the output of CF.

3) Linear Complexity

The Linear Complexity is defined as the length, of the shortest LFSR (which is equivalent LFSR) that can mimic the generator output. Any sequence generated by a finite-state machine over a finite field has a finite linear complexity [7].

Let's denotes the Linear Complexity for the generated sequence by LC(S), then it can by calculated by:

$$LC(S)=r_1r_2r_3+r_1r_2r_4+r_1r_2r_5+r_1r_3r_4+r_1r_4r_5+r_2r_3r_4+r_2r_3r_5+r_1r_2r_3+r_2r_4r_5 +r_3r_4r_5+r_1r_2r_3r_4+r_1r_2r_3r_5+r_1r_2r_4r_5+r_1r_3r_4r_5+r_2r_3r_4r_5.$$

Example (3)

Let's use the same information mentioned in example (2), then:

$$LC(S)=2*3*4+2*3*5+2*3*6+2*4*5+2*4*6+2*5*6+3*4*5+3*4*6 +3*5*6+4*5*6$$
$$=2*3*4*5+2*3*4*6+2*3*5*6+2*4*5*6+3*4*5*6=1624$$

4) Correlation Immunity

Correlation can be defined as the relation between the sequence of CF=F_n from the key generator and the sequences that are combined each other by CF. This relation caused because of the non-linearity of the function F_n. The correlation probability CP(x), in general, represents the ratio between the number of similar binaries of two sequences to the length of the compared part of them. F_n has m^{th} order CI, if the output z of F_n is statistically independent from m output from m-sequences $(x_1,x_2,...,x_m)$, of n combined sequences s.t. $m \leq n$.

Notes from table (1) (from the shaded cells) that the number of similarity between x_i and the output of CF is 16 bits from the total number 32 bits $\forall i$, then the correlation probability (CP_i) can be calculated as:

$$CP_i = 22/32 = 0.6875, \text{ for } i = 1,2,\ldots,5.$$

Let's denotes the Correlation Immunity for the generated sequence by CI(S), then it can by calculated by:

CI(S) = 0,

since the number of immune $x_i = 0$.

This indicates that this generator can be attacked by correlation attack or fast correlation attack [8].

4. Constructing A SLE for modified Bruer Generator

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

By using recurrence equation (4),

$$C_{ij}=M_j\times C_{i-1,j},\ i=1,2,\ldots \qquad \ldots(13)$$

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 of CF, in the same time its represents the number of equations which are be 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's back to Modified Bruer system, 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 $A_0\times\mathbf{C}=S$.

From CF the number of variables (m) are:

$$m=r_1r_2r_3+r_1r_2r_4+r_1r_2r_5+r_1r_3r_4+r_1r_4r_5+r_2r_3r_4+r_2r_3r_5+r_1r_2r_3+r_2r_4r_5+r_3r_4r_5 +r_1r_2r_3r_4+r_1r_2r_3r_5+ r_1r_2r_4r_5+r_1r_3r_4r_5+r_2r_3r_4r_5.$$

The initial value is:

$$A_0=A_{01}A_{02}A_{03}+A_{01}A_{02}A_{04}+A_{01}A_{02}A_{05}+A_{01}A_{03}A_{04}+A_{01}A_{04}A_{05}$$
$$+A_{02}A_{03}A_{04}+A_{02}A_{03}A_{05}+A_{01}A_{02}A_{03}+A_{02}A_{04}A_{05}+A_{03}A_{04}A_{05}$$
$$+A_{01}A_{02}A_{03}A_{04}+A_{01}A_{02}A_{03}A_{05}+A_{01}A_{02}A_{04}A_{05}+A_{01}A_{03}A_{04}A_{05}$$
$$+A_{02}A_{03}A_{04}A_{05}= (x_0,x_1,\ldots,x_{m-1}),$$
s.t. $x_0=a_{-11}a_{-12}a_{-13}$, $x_1=a_{-11}a_{-12}a_{-23},\ldots,x_{m-1}= a_{-r_2 2}a_{-r_3 3}a_{-r_4 4}a_{-r_5 5}$

(this arrangement is not standard so it can be changed according to the researcher requirements). For simplicity let's denote the unknowns of SR_1 by 'a', SR_2 by 'b', and so on, let's denote the unknowns of SR_5 by 'e', and so on, therefore:

$$x_0=a_1b_1c_1,\ x_1=a_1b_1c_2,\ldots,x_{m-1}= b_{r2}c_{r3}d_{r4}e_{r5} \qquad \ldots(14)$$

In the same way, equation (14) can be applied on the feedback vector C_{ij}:

$$C_i=C_{i1}C_{i2}C_{i3}+C_{i1}C_{i2}C_{i4}+C_{i1}C_{i2}C_{i5}+C_{i1}C_{i3}C_{i4}+C_{i1}C_{i4}C_{i5}+C_{i2}C_{i3}C_{i4}$$
$$+C_{i2}C_{i3}C_{i5}+C_{i1}C_{i2}C_{i3}+C_{i2}C_{i4}C_{i5}+C_{i3}C_{i4}C_{i5}+C_{i1}C_{i2}C_{i3}C_{i4}+C_{i1}C_{i2}C_{i3}C_{i5}$$
$$+C_{i1}C_{i2}C_{i4}C_{i5}+C_{i1}C_{i3}C_{i4}C_{i5}+C_{i2}C_{i3}C_{i4}C_{i5}.$$

And the sequence S will be:

$$S=S_1S_2S_3+S_1S_2S_4+S_1S_2S_5+S_1S_3S_4+S_1S_4S_5+S_2S_3S_4+S_2S_3S_5+S_1S_2S_3$$
$$+S_2S_4S_5+S_3S_4S_5+S_1S_2S_3S_4+S_1S_2S_3S_5+S_1S_2S_4S_5+S_1S_3S_4S_5+S_2S_3S_4S_5$$
s.t.

$$s_i=s_{i1}s_{i2}s_{i3}+s_{i1}s_{i2}s_{i4}+s_{i1}s_{i2}s_{i5}+s_{i1}s_{i3}s_{i4}+s_{i1}s_{i4}s_{i5}+s_{i2}s_{i3}s_{i4}+s_{i2}s_{i3}s_{i5}$$
$$+s_{i1}s_{i2}s_{i3}+s_{i2}s_{i4}s_{i5}+s_{i3}s_{i4}s_{i5}+s_{i1}s_{i2}s_{i3}s_{i4}+s_{i1}s_{i2}s_{i3}s_{i5}+s_{i1}s_{i2}s_{i4}s_{i5}$$
$$+s_{i1}s_{i3}s_{i4}s_{i5}+s_{i2}s_{i3}s_{i4}s_{i5},$$
where s_i is the element i of S.

So the SLE can be obtained by equation (6).

Figure (2) shows the sequence S which is generated from modified Bruer Generator [5].

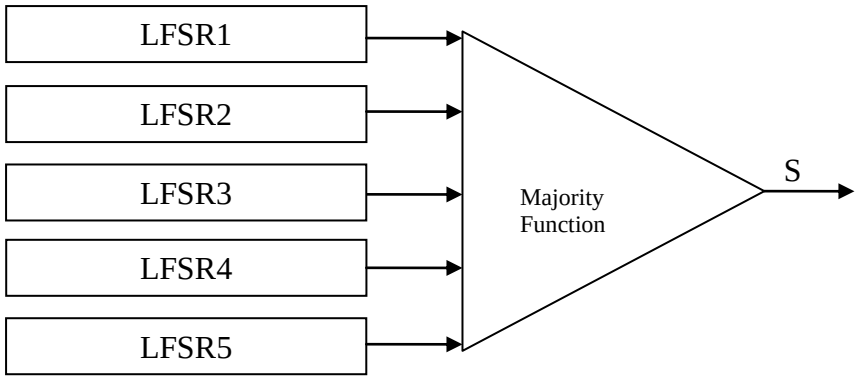

Figure (2) modified Bruer generator [5].

Example (4)

Let's have the following feedback vectors for 5 LFSR's with lengths 2,3,4,5 and 6:

$C_{01}=\begin{pmatrix}1\\1\end{pmatrix}$, $C_{02}=\begin{pmatrix}1\\0\\1\end{pmatrix}$, $C_{03}=\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$, $C_{04}=\begin{pmatrix}0\\1\\0\\0\\1\end{pmatrix}$, $C_{05}=\begin{pmatrix}1\\0\\0\\0\\0\\1\end{pmatrix}$ then m=1624.

Let the output sequences be: S=(1,1,1,1,1,1,0,…,0,1,1,1,0,1,1,0,0)

$C_{0,1}=C_{3,1}=C_{6,1}=C_{9,1}=\ldots=C_{1620,1}=C_{1623,1}=\begin{pmatrix}1\\1\end{pmatrix}$, $C_{1,1}=C_{4,1}=C_{7,1}=C_{10,1}=\ldots$

$=C_{1618,1}=C_{1621,1}=\begin{pmatrix}0\\1\end{pmatrix}$, $C_{21}=C_{51}=C_{81}=C_{11,1}=\ldots=C_{1619,1}=C_{1622,1}=\begin{pmatrix}1\\0\end{pmatrix}$.

$C_{0,2}=\ldots=C_{1617,2}=\begin{pmatrix}1\\0\\1\end{pmatrix}$, $C_{1,2}=\ldots=C_{1618,2}=\begin{pmatrix}1\\1\\1\end{pmatrix}$, $C_{2,2}=\ldots=C_{1619,2}=\begin{pmatrix}0\\1\\1\end{pmatrix}$, $C_{3,2}=\ldots=C_{1620,2}=\begin{pmatrix}1\\1\\0\end{pmatrix}$, $C_{4,2}=\ldots=C_{1621,2}=\begin{pmatrix}0\\0\\1\end{pmatrix}$, $C_{5,2}=\ldots=C_{1622,2}=\begin{pmatrix}0\\1\\0\end{pmatrix}$, $C_{6,2}=\ldots=C_{1623,2}=\begin{pmatrix}1\\0\\0\end{pmatrix}$.

$C_{0,3}=\ldots=C_{1609,3}=\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$, $C_{1,3}=\ldots=C_{1610,3}=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$, $C_{2,3}=\ldots=C_{1611,3}=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$, $C_{3,3}=\ldots=C_{1612,3}=\begin{pmatrix}0\\1\\1\\1\end{pmatrix}$,

And so on until we get:

$C_{12,3}=\ldots.=C_{1621,3}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$, $C_{13,3}=\ldots=C_{1622,3}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$, $C_{14,3}=\ldots=C_{1623,3}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$.

In the same process we get $C_{i,4}$ and $C_{i,5}$, for i=1,2,…,1623.
by applying equation (4), C_0^T will be:
C_0^T=(1,0,0,1,0,0,0,0,1,0,0,1, 1,0,0,1,0,0,0,0,1,0,0,1,…,1,0,0,0,0,1).
Therefore, then the augmented (1623×1623) matrix Y will be:

$$Y = \left(\begin{array}{l} 1\,0\,0\,1\,0\,0\,0\,0\ldots0\,0\,0\,0\,1\,0\,0\,1 \mid 1 \\ 0\,0\,0\,0\,0\,0\,0\,0\ldots1\,1\,0\,0\,0\,0\,0\,0 \mid 1 \\ \\ \qquad\qquad . \\ \qquad\qquad . \\ 0\,0\,0\,0\,1\,1\,1\,1\ldots0\,0\,0\,0\,0\,0\,0\,0 \mid 0 \\ 0\,1\,1\,1\,0\,0\,0\,0\ldots0\,0\,0\,0\,0\,0\,0\,0 \mid 0 \end{array}\right) \quad \ldots(15)$$

5. Test The Uniqueness of The Solution of SLE

Since the system 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. So first it should test the uniqueness of solution of the system by many ways like calculating the rank of the system matrix ($r(\mathbf{C}^T)$) or by finding the determinant of the matrix. If the rank equal the matrix degree ($deg(\mathbf{C}^T)$), then the system has unique solution, else ($r(\mathbf{C}^T) < deg(\mathbf{C}^T)$) the system has no unique solution.

In order to calculate the $r(\mathbf{C}^T)$ it has to use the elementary operations to convert the $\mathbf{C}^T$ matrix to a simplest matrix by making, as many as possible of, the matrix elements zero's. The elementary operations should be applied in the rows and columns of the matrix $\mathbf{C}^T$, if it converts to Identity matrix then $r(\mathbf{C}^T)=deg(\mathbf{C}^T)=m$, then we can judge that $\mathbf{C}^T$ has unique solution [9].

Example (5)

Let's have the matrix $\mathbf{C}^T=\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$, by using the elementary operations, the matrix can be converted to the matrix $\mathbf{C}^{T*}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$,

this matrix has rank =4=deg($\mathbf{C}^T$) then the matrix has unique solution.

For modified Bruer generator, we obtain that the SLE has unique solution, of course we have to chose 1624 independent equations not all are in sequence order.

6. Solving The SLE

After be sure that the SLE has unique solution, the SLE can be solved by using one of the most common classical methods, its Gauss Elimination method. This method chosen since it has lower complexity than other methods. As known, this method depending in two main stages, first, converting the matrix Y to up triangular matrix, and the second one, is finding the converse solution [8]. Example (6) shows the solving of a single SLE for one LFSR.

Example (6)

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

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

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

The SLE of 5_LFSR's is more complicated than SLE of a single LFSR, specially, if the CF is high order (non-linear) function. First, it should solve the variables which are consists of multiplying more than one initial variable bits of the combined LFSR's.

As an example of modified Bruer generator, its going to solve the variables d_k, $1 \le k \le m-1$, then solving the initial values a_{-ij} since x_k is represented by multiplying three initial bits in 10 terms, and four initial bits in 5 terms. In another word, every system has

its own SLE system because of the CF, so it has own solving method.

As an example to find the variables a_{-ij} of modified Bruer generator, after solving the SLE we found that 91 variables (x_k) equal (1) from the whole number of variables, s.t.:

$x_{23}=x_{53}=x_{89}=x_{129}=x_{177}=x_{237}=x_{297}=x_{369}=x_{459}=x_{579}=x_{699}=x_{843}=x_{1023}$
$=x_{1263}=x_{1623}= 1.$

From equation (14), we know that every x_k is consists from product of three or four unknowns, where a_i,b_j,c_k,d_l,e_n are initial values the five LFSR's contribute in modified Bruer generator s.t. i=1,2,3,4,5. The SLE system Y which mentioned in example (4) will be solved in the next example.

Example (7)

$x_{23}=a_2*b_3*c_4=1$, this means $a_2=b_3=c_4=1$ and $x_{53}=a_2*b_3*d_5=1$ this means $a_2=b_3=d_5=1$ and so on until we found all the initial values of all LFSR's contribute the modified Bruer generator. After applying the above process we get:

- $A_{01}=(a_1,a_2)=(a_{-11},a_{-21})=(0,1)$.
- $A_{02}=(b_1,b_2,b_3)=(a_{-12},a_{-22},a_{-32})=(0,0,1)$.
- $A_{03}=(c_1,c_2,c_3,c_4)=(a_{-13},a_{-23},a_{-33},a_{-43})=(0,0,0,1)$.
- $A_{04}=(d_1,d_2,d_3,d_4,d_5)=(a_{-14},a_{-24},a_{-34},a_{-44},a_{-54})=(0,0,0,0,1)$.
- $A_{05}=(e_1,e_2,e_3,e_4,e_5,e_6)=(a_{-15},a_{-25},a_{-35},a_{-45},a_{-55},a_{-65})=(0,0,0,0,0,1)$.

7. Conclusions

1) If we change our attack from 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.

2) 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).

3) Notice that m is high (m=1624) because of the non-linearity of the combining function CF (majority function), and because of changing the non-linear variables to new variables, so we think that it can keep m as number of non-linear variables and solving the non-linear system by using direct methods after applying the suitable modifying.

References

[1]. Schneier, B., "***Applied Cryptography (Protocol, Algorithms and Source Code in C***." Second Edition, John Wiley & Sons Inc. 1997.

[2]. Whitesitt, J. E., "***Boolean Algebra and its Application***", Addison-Wesley, Reading, Massachusetts, April, 2005.

[3]. Golomb, S.W., "***Shift Register Sequences***" San Francisco: Holden Day, 1967, Reprinted by Aegean Park Press in 1982.

[4]. Papoulis, A. "***Probability Random Variables, and Stochastic Process***", McGraw-Hill College, October, 2005.

[5]. Brüer, J. O., "***On Nonlinear Combinations of Linear Shift Register Sequences***" Internal Report LITH-ISY-1-0572,1983.

[6]. Al-Shammari, A. G., "***Mathematical Modeling and Analysis Technique of Stream Cipher Cryptosystems***", Ph. D. Thesis, University of Technology, Applied Sciences, 2009.

[7]. Massey, J. L., "***Cryptography and System Theory***", Proceedings of the 24th Allerton Conference on Communication, Control, and Computers, 1-3 Oct. 1986.

[8]. Siegenthaler, T., "***Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications***", IEEE Transactions on Information Theory, v. IT-30, n. 5, pp. 776-780, Sep. 1984.

[9]. Jennings, A. and Mckeown, "***Matrix Computation***", John Wiley & Sons Inc., November, 2003.

كسر مولد برور المحور من خلال حل نظام المعادلات الخطية الخاص بالمتابعة المخرجة له

فالح حسن عويد
كلية الرافدين الجامعة / قسم هندسة البرامجيات

المستخلص

لقد استخدمت انظمة المسجل الزاحف الخطي ذو التغذية التراجعية بشكل واسع في مجال انظمة التشفير الانسيابي ، استخدم كولومب العلاقة التكرارية لا يجاد قيم الحالة التالية لمسجل زاحف منفرد بالاعتماد على القيم الابتدائية له لذلك اعتبر اول من أنشأ نظام معادلات خطية لمسجل زاحف منفرد ، ان مهاجمة مولد مفاتيح يعني محاولة ايجاد القيم الابتدائية لمسجلاته الزاحفة .

في هذا البحث ، تم أولاً عرض طريقة كولومب لإنشاء نظام معادلات خطية لمسجل زاحف منفرد ، ثانياً ، تم تطوير هذه الطريقة لإنشاء نظام معادلات خطية لمولد مفاتيح (منظومة مسجلات زاحفة) والتي يظهر فيها جلياً تأثير الدالة المركبة ، وأخيراً ، وقبل الشروع بحل ذلك النظام الخطي ، علينا اختبار توفر وحدانية الحل لهذا النظام ومن ثم حل هذا النظام باستخدام احدى الطرق التقليدية المعروفة مثل طريقة كاوس للحذف ، ان حل نظام المعادلات الخطية يعني ايجاد القيم الابتدائية للمسجلات الزاحفة المشتركة في المولد ، ان مولد برور المحور ، وهو من المولدات المعروفة ، سيكون المثال العملي المراد مهاجمته في هذا البحث .