Analyze of Complement Linear Model Using Probable Word Attack

Dr. Ayad Ghazi Naser Al-Shammari
Ministry of Education - General Directorate of Vocational Education
Email: dr_ayad64@yahoo.com

Abstract

In this paper we attempts to generalize Golomb's method which include constructing a linear equations system from output of a single shift register. The proposed method represented by constructing a linear equations system of complement linear model, where the effects of the combining function of shift registers is obvious. The attack kind applied in this work is a probable word attack. Before solving the linear equations system by using the known classical method, it must test the existence and uniqueness of the solution to obtain the initial values of the combined shift registers.

Keywords: stream cipher systems, linear feedback shift register, linear model, probable word attack.

1. Introduction

The Berlekamp-Massey algorithm is due to Massey in 1969 [1], the Berlekamp-Massey algorithm is only described for binary sequences to find the equevelent and shortest LFSR that generates the given sequence; it can be generalized to find the linear complexity of sequences over any field.

Although now dated, Rueppel in 1986 [2] provides a solid introduction to the analysis and design of stream ciphers. The results on the expected linear complexity and linear complexity profile of random sequences are from Chapter 4 of Rueppel.

In 1989, Staffelbach and Meier [3] presented two new so-called fast correlation attacks which are more efficient than Siegenthaler's attack in the case where the component LFSRs have sparse feedback polynomials, or if they have low-weight polynomial multiples (e.g., each having fewer than 10 non-zero terms) of not too large a degree.

In 1990, Jansen and Boekee [4] defined the maximum order complexity of a sequence to be the length of the shortest (not necessarily linear) feedback shift register (FSR) that can generate the sequence. An efficient linear-time algorithm for computing this complexity measure was also presented.

A comprehensive survey of correlation attacks on LFSR-based stream ciphers is the paper by Golić in 1994 [5]; the cases where the combining function is memoryless or with memory, as well as when the LFSRs are clocked regularly or irregularly, are all considered.

A PH. D. thesis "Use of GA in cryptanalysis of a class of stream cipher system" which introduced by Dr. Al-Ageelee [6] in 1998, this

work used Genetic Algorithm in cryptanalysis of class of stream cipher system depending on finding correlation between ciphertext and the output of some of LFSR.

The paper of Ahmed [7] contained the design of artificial neural networks for decryption i.e. getting distinguished polynomial for binary sequence with linear equivalence which is equal to 8 as well as getting the binary sequence that is related to the distinguished polynomial. And it was proved by the results that by using the Artificial Neural Networks were very appropriate for the decryption of the stream cipher systems.

Ali and Jaber [8] in 2009, introduce a paper aims to solve linear equations system for any number of variables using the Genetic Algorithms (GA). The application done by attacking stream cipher systems, choosing one Linear Feedback Shift Register (LFSR) in the performance of GA. The divided into two stages, first, constructing LES's for the LFSR, and the second, is attacking the variables of LES's which they are also the initial key values the of LFSR.

Every model of Linear Feedback Shift Register (LFSR) consists of two main basic units. First, is the Combining Function (CF), which is a boolean function, where the output bits (x_i) of each LFSR are input to CF with output (y) [9]. The second is the initial states binary values of LFSRs. Most of all stream cipher systems are depend on these two basic units.

This paper aims to find the initial values of every LFSR in the complement linear model depending on the following information [10]:

1. **The length of every LFSR and its feedback function are known.**
2. **The output sequence *S* (keystream) generated from the complement linear model is known, or part of it, practically, that means, a probable word attack be applied.**

This work consists of three stages, constructing linear equations system (LES), test the uniqueness of the solution of this system, and lastly, solving the linear equations system.

Figure (1) describes the block diagram of analyze any *n*-LFSR's model.

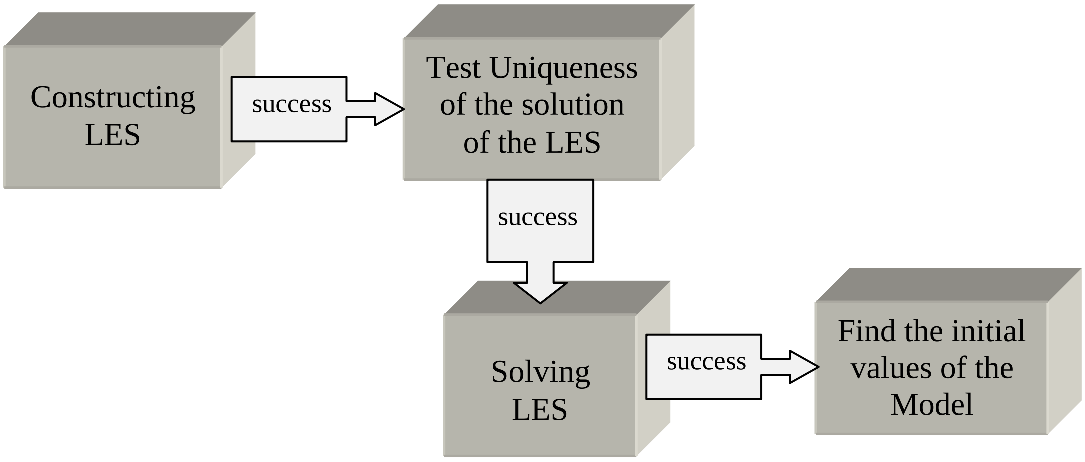
Constructing LES
success
Test Uniqueness of the solution of the LES
success
Solving LES
success
Find the initial values of the Model

Figure (1) Block diagram of analyze the LFSR model.

2. Golomb's Method

Before involving in solving the Linear Equations System (LES), it should show how could be the LES 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^L-1, where L is LFSR length. Now we will show how to construct LES for single LFSR.

Let SR_L be a single LFSR with length L, let $I_0=(a_{-1},a_{-2},\ldots,a_{-L})$ be the initial value vector of SR_L, s.t. a_{-j}, $1\le j\le L$, be the component j of the vector I_0, in another word, a_{-j} is the initial bit of stage j of SR_L, let $C_0^T=(c_1,\ldots,c_L)$ 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_L. The generation of S depending on the following equation [11]:

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

Equation (1) represents the linear recurrence relation.

The objective is finding the I_0, when L, C_0 and S are known.

Let G be a $L\times L$ matrix, which is describes the initial phase of SR_L:

G=$(C_0|I_{L\times L-1})$, where G^0=I.

Where G is called the Generating matrix.

Let I_1 represents the new initial of SR_L after one shift, s.t.

$$I_1=I_0\times G=(a_{-1},a_{-2},\ldots,a_{-L})\begin{pmatrix} c_1 & 1 & \cdots & 0 \\ c_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ c_L & 0 & \cdots & 0 \end{pmatrix}=(\sum_{j=1}^{L} a_{-j}c_j, a_{-1,} \ldots, a_{1-L}).$$

In general,

$I_i=I_{i-1}\times G$, $i=0,1,2,\ldots$
…(2)

Equation (2) can be considered as a recurrence relation, so we have:

$I_i=I_{i-1}\times G=I_{i-2}\times G^2=\ldots=I_0\times G^i$
…(3)

The matrix G^i represents the i phase of SR$_L$, equations (2,3) can be considered as a Markov Process s.t., I_0, is the initial probability distribution, I_i represents probability distribution and G be the transition matrix [11].
notice that:
$G^2=[C_1C_0|I_{L\times L-2}]$ and so on until get $G^i=[C_{i-1}\ldots C_0|I_{L\times L-i}]$, where $1\leq i<L$.
When $C_P=C_0$ then $G^{P+1}=G$.
Now let's calculate C_i [12] s.t.

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

Equation (1) can be rewritten as:

$I_0\times C_i=s_i$, $i=0,1,..,L-1$
…(5)

When $i=0$ then $I_0\times C_0=s_0$ is the 1st equation of the LES,
$i=1$ then $I_0\times C_1=s_1$ is the 2nd equation of the LES, and
$i=L-1$ then $I_0\times C_{L-1}=s_{L-1}$ is the Lth equation of the LES.

In general:

$I_0\times D=S$ …(6)

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

$D=(C_0C_1\ldots C_{L-1})$ …(7)

The LES can be formulated as:

$$Z=[\,D^{T}|S^{T}] \qquad \ldots(8)$$

Y **represents the extended matrix of the LES.**

<u>Example (1)</u>

Let the SR$_4$ has C_0^{T}=(0,1,0,0,1) and *S*=(1,0,0,1,1), by using equation (4), we get:

$$C_1=G\times C_0=\begin{pmatrix}0&1&0&0&0\\1&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\\1\end{pmatrix}=\begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix}$$

, in the same way, $C_2=\begin{pmatrix}0\\1\\1\\0\\1\end{pmatrix}$ **,** $C_3=\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix}$ **,**

$$C_4=\begin{pmatrix}1\\1\\1\\0\\1\end{pmatrix}.$$

From equation (6) we have:

$$I_0\begin{pmatrix}0&1&0&1&1\\1&0&1&1&1\\0&0&1&0&1\\0&1&0&1&0\\1&0&1&0&1\end{pmatrix}=(1,0,0,1,1),$$

this system can be written as equations:

$a_{-2}+a_{-4}+a_{-5}=1$

$a_{-1}+a_{-3}+ a_{-4}+a_{-5}=0$

$a_{-3}+a_{-5}=0$

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

$a_{-1}+a_{-3}+ a_{-5}=1$

Then the LES after using formula (8) is:

$$Z=\left[\begin{array}{ccccc|c}0&1&0&0&1&1\\1&0&0&1&0&0\\0&1&1&0&1&0\\0&1&0&1&0&1\\1&1&1&0&1&1\end{array}\right] \qquad \ldots(9)$$

3. Complement Linear Model

As known, the outputs of every LFSR of the complement linear model (CLM) are first complemented then XORed to gain the sequence *S* which is generating from this model. So the boolean function F_n is:

$$F_n(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{n\oplus}(x_j \oplus 1)$$

This generator acts analogously to the linear generator in the most properties, like randomness and correlation immune. But it's different in the output sequence and linear complexity [10].

This generator considered a weak linear complexity, despite of his good randomness (see Figure (2)).

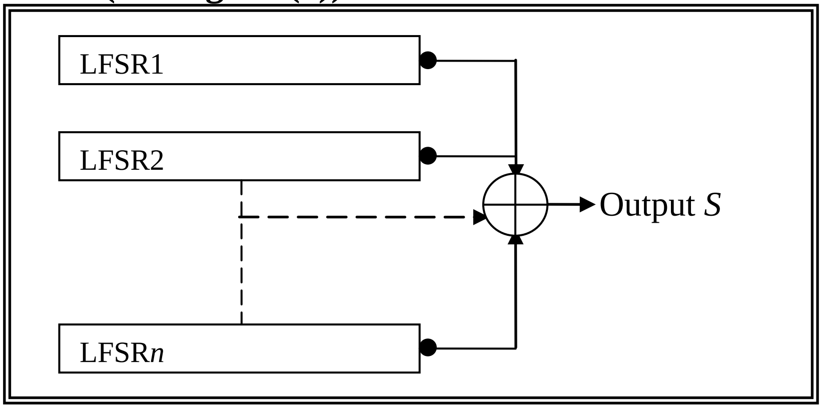

Figure (2) Complement Linear Model.

Where ● is the complement of the output of LFSR_i.

For *n*=3 the truth table of this generator will be shown in table (1).

table (1) The truth table of Complement Linear Model.

x_1	x_2	x_3	$x_1 \oplus 1$	$x_2 \oplus 1$	$x_3 \oplus 1$	F_3
0	0	0	1	1	1	1
0	0	1	1	1	0	0
0	1	0	1	0	1	0
0	1	1	1	0	0	1
1	0	0	0	1	1	0
1	0	1	0	1	0	1
1	1	0	0	0	1	1
1	1	1	0	0	0	0

The linear complexity (LC) of this generator is:

$$\text{LC}(\text{S}_{\text{CL}}) = \sum_{i=1}^{n} r_i$$

Where S_{CL} is the sequence generate from *n*-CLM.

Assuming the degrees of the all combined primitive feedback polynomials are relatively primes.

The correlation probability CP(S_i) of the sequences S_i generated from of output of LFSR$_i$ which is combined in the *n*-CLM is equal to 0.5 $\forall i$.

The complement linear model can't be attacked by correlation or fast correlation attack, so the system is immune [10].

In this manner we have two cases. These two cases depend on the number of combined LFSR's *n* in CLM, these cases are:

1. **Case (1): if *n* is even number:**

$$F_n(x_1,x_2,\dots,x_n)=\sum_{j=1}^{n\oplus}(x_j\oplus 1)=\sum_{j=1}^{n\oplus}x_j\oplus\underbrace{(1\oplus 1\oplus\cdots\oplus 1)}_{n-times}=\sum_{j=1}^{n\oplus}x_j$$

2. **Case (2): if *n* is odd number:**

$$F_n(x_1,x_2,\dots,x_n)=\sum_{j=1}^{n\oplus}(x_j\oplus 1)=\sum_{j=1}^{n\oplus}x_j\oplus\underbrace{(1\oplus 1\oplus\cdots\oplus 1)}_{n-times}=\sum_{j=1}^{n\oplus}x_j\oplus 1$$

This mean the complement linear model is analogues to complement of final output bit in the main sequence.

To but the two cases in one equation, $F_n(x_1,x_2,\dots,x_n)$ can be written as follows:

$$F_n(x_1,x_2,\dots,x_n)=\sum_{j=1}^{n\oplus}x_j\oplus t*1\text{, where } t=n\bmod 2.$$

Since the SR_{L_j} has L_j number of unknown initial values, then:

$$m=\sum_{j=1}^{n}L_j$$

4. Attacking of Complement Linear Model

4.1 LES construction for CLM

Let's have *n* of SR_{L_j} with length L_j, *j*=1,2,…,*n*, with feedback vector $C_{0j}=\begin{pmatrix}c_{01j}\\ c_{02j}\\ \vdots\\ c_{0L_jj}\end{pmatrix}$,and has unknown initial value vector $I_{0j}=(a_{-1j},\dots,a_{-Lj})$, so SR_{L_j} has $I_j=(C_{0j}|\, I_{L_j\times L_j-1})$

By using recurrence equation (4),

$C_{ij}=I_j\times C_{i-1,j}$, $i=1,2,\ldots$ …(10)

by using equation (5):

$I_{0j}\times C_{ij}=s_{ij}$, $i=0,1,\ldots,L-1$ **and** $S_j=(s_{0j},s_{1j},\ldots,s_{m-1,j})$.

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

Now, let I_0 be the extended vector form variables, which consists of initial values from all LFSR's and *D* is the matrix of C_i vectors considering the CF, C_i represents the extended vector of all feedback vectors C_{ij}, then $I_0\times D=S$.

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

$$I_{01}=(a_{-11},\ldots,a_{-L_1 1},0\ldots0,\ldots,0\ldots0)$$
$$I_{02}=(0\ldots0,a_{-12},\ldots,a_{-L_2 2},\ldots,0\ldots0)$$

And so on..

$$I_{0n}=(0\ldots0,0\ldots0,\ \ldots,a_{-1n},\ldots,a_{-L_n n})$$

And let

$$I_0=\sum_{j=1}^{n}I_{0j}=(a_{-11},\ldots,a_{-L_1 1},a_{-12},\ldots,a_{-L_2 2},\ldots,a_{-1n},\ldots,a_{-L_n n})=(\ell_0,\ell_1,\ldots,\ell_{m-1})$$

Where $\ell_0=a_{11}$, $\ell_1=a_{21},\ldots,\ell_{m-1}=a_{L_n n}$, or it can be deduced from the following formula:

$\ell_k=a_{ij}$, **where** $k=(i-1)+\sum_{h=1}^{j-1}L_h$, $j=1,2,\ldots,n$, $i=1,2,\ldots,L_j$. …(11)

In fact, I_0 represents a concatenation of all I_{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.

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

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

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

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

So D can be gotten from equation (7) and by applying equation (6), the LES can be constructed.

<u>Example (2)</u>

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

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

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

By using equation (4),

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

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

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

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

The LES can be written as follows:

$$I_0\begin{pmatrix} 1&0&1&1&0&1&1&0&1\\ 1&1&1&1&1&0&1&1&0\\ 1&1&0&1&0&0&1&1&1\\ 0&1&1&1&0&1&0&0&1\\ 1&1&1&0&1&0&0&1&1\\ 1&1&1&0&1&0&1&1&0\\ 0&0&1&1&1&1&0&1&0\\ 0&1&1&1&1&0&1&0&1\\ 1&1&1&1&0&1&0&1&1 \end{pmatrix}=(1,1,1,0,1,1,0,1,1)$$

s.t. $I_0=(a_{-11},a_{-21},a_{-12},a_{-22},a_{-32},a_{-13},a_{-23},a_{-33},a_{-43})$, and the extended matrix Z which is can be calculated from equation (8) is:

$$Z=\left[\begin{array}{ccccccccc|c} 1&1&1&0&1&1&0&0&1&1\\ 0&1&1&1&1&1&0&1&1&1\\ 1&0&0&1&1&1&1&1&1&1\\ 1&1&1&1&0&0&1&1&1&0\\ 0&1&0&0&1&1&1&1&0&1\\ 1&0&0&1&0&0&1&0&1&1\\ 1&1&1&0&0&1&0&1&0&0\\ 0&1&1&0&1&1&1&0&1&1\\ 1&0&1&1&1&0&0&1&1&1 \end{array}\right] \qquad \ldots(12)$$

4.2 Test Uniqueness of the Solution of LES Produced From CLM

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. So first it should test the uniqueness of the system by calculating the rank of the system matrix (r(D^T)). If the rank equal the matrix degree (deg(D^T)), then the system has unique solution, else (r(D^T)< deg(D^T)) the system has no unique solution.

In order to calculate the r(D^T) it has to use the elementary operations to convert the D^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 a matrix rows and columns [13].

Example (3)

Let's have the matrix $D^{T}=\begin{pmatrix}0&1&0&1&1\\1&0&1&1&1\\0&0&1&0&1\\0&1&0&1&0\\1&0&1&0&1\end{pmatrix}$,

by using the elementary operations, the matrix can be converted to the matrix $D^{T*}=\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}$,

this matrix has rank =5=deg(D^{T}) then the matrix has unique solution.

4.3 Solving the LES Produced From CLM

After be sure that the LES has unique solution, the LES 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 its 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 [13]. Example (4) shows the solving of a single LES for one LFSR.

<u>Example (4)</u>

Let's use the matrix *Y* of equation (9), since *n*=1, then *S* '=S⊕1=(1,0,0,1,1) ⊕1, so *S* '=(0,1,1,0,0).

After applying the elementary operations, and then the up triangular matrix is:

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

Now applying the backward solution to get the initial value vector of *Z '*:

I_0=(1,0,1,1,1).

4.4. Solving LES of LCM

Since the unknowns a_{ij}'s are arranged in C_{ij} vector in sequence style for the linear system, s.t. $X(k)=x_k=a_{ij}$, where $k=(i\text{-}1)+\sum_{h=1}^{j-1} L_h$, $j=1,2,\dots,n$, $i=1,2,\dots,L_j$, so it's more easier from other non-linear generators. In another words, that means every single variable x_k corresponding to single unknown a_{ij}.

We can calculate values of i and j from k value, where $0\le k\le m\text{-}1$ and where $j=1,2,\dots,n$; $i=1,2,\dots,L_j$, to find the initial values a_{ij} by helping of equation (11) and using, find initial values for linear system algorithm.

<u>Example (5):</u>

Let's solve the matrix Y (of equation (12)) mentioned in example (2). First we have to find $S\,'=S\oplus 1$.

After applying the elementary operations, and then find the vector X by:

$k=0,1,\dots,8$, $L_1=2$, $L_2=3$ and $L_3=4$, $j=1,2,3$.

$X = (0,1,0,0,1,0,0,0,1)$,

Notice, when k=1,4 and 8 $x_k=1$; otherwise $x_k=0$.

Now can we found the following results from table (2):

Table (2) the initial values of CLM from X vector.

k	0	1	2	3	4	5	6	7	8
i,j	1,1	2,1	1,2	2,2	3,2	1,3	2,3	3,3	4,3
a_{ij}	0	1	0	0	1	0	0	0	1
L_j	$L_1=2$		$L_2=3$			$L_3=4$			

5. <u>Conclusions</u>

1. **If we change our attack from known probable word 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 LES.**
2. **It is not hard to construct a LES of any other LFSR models; of course, we have to know all the necessary information (CF, the number of combined LFSR's and their lengths and tapping).**
3. **We can find the determinant of the augmented matrix Z to investigate the uniqueness of the solution of the linear system.**

<u>References</u>

[1]. Massey, J. L., "*Shift-register synthesis and_BCH decoding*", IEEE Transactions on Information_Theory, 15 (1969), 122–127.

[2]. Rueppel, R. A., "*Analysis and Design of Stream Ciphers*" Springer-Verlag, Berlin, 1986Whitesitt, J. E., "*Boolean Algebra and its Application*", Addison-Wesley, Reading, Massachusetts, April, 1995.

[3]. Staffelbach, O. and Meier, W., "*Fast Correlation Attacks on Certain Stream Ciphers*", Journal of Cryptology, 1 (1989), 159–176.

[4]. Jansen, C. J. and Boekee, D. E., "*On the Significance of the Directed Acyclic Word Graph in Cryptology*", Advances in Cryptology–AUSCRYPT '90 (LNCS 453), 318–326, 1990.

[5]. Golić, J., "*On the Security of Shift Register Based Keystream Generators*", R. Anderson, editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 90–100, Springer-Verlag, 1994.

[6]. Al-Algeelee S. A., "*Use of GA in Cryptanalysis of a Class of Stream Cipher System*", PH. D. Thesis, University of Technology, 1998.

[7]. Ahmad I. A., "*Using Neural Networks In Cryptanalysis Stream Cipher Systems*", Mansoura Journal for Computer Science and Information Systems, Volume 1, Number 0, Jan. 2005.

[8]. Ali F. H. and Jaber A. S., "*Solving Linear Equations Systems Using Genetic Algorithm*", The 10th Scientific Conference, Al-Mansour University College & Iraqi Association for Libraries & Information - Iraq, No#.14, pp.121-137, 24-25/Oct./2009.

[9]. Gilbert W. J. and Nicholson W. K., "*Modern Algebra with Applications*", Second Edition, John Wiley & Sons, Inc., Hoboken, New Jersey, 2004.

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

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

[12]. Schay, G., "*Introduction to Probability with Statistical Applications*", University of Massachusetts Boston, Department of Mathematics, USA, 2007.

[13]. Thomas T. S., "*Applied Linear Algebra and Matrix Analysis*", Springer Science + Business Media, LLC, 2007.

تحليل نموذج المتمم الخطي باستخدام المهاجمة بالكلمة المحتملة

د. اياد غازي ناصر الشمري

وزارة التربية – المديرية العامة للتعليم المهني

مستخلص

في هذا البحث نحاول تعميم طريقة كولومب التي تضمنت انشاء نظام معادلات خطية من مخرجات مسجل زاحف منفرد. الطريقة المقترحة تتمثل بانشاء نظام معادلات خطية للنموذج المتمم الخطي، حيث يظهر تأثير الدالة المركبة للمسجلات الزاحفة بشكل واضح. ان اسلوب المهاجمة المستخدم في هذا العمل هو المهاجمة باسلوب الكلمة المحتملة. قبل حل نظام المعادلات الخطي باستخدام احد الطرق الكلاسيكية، يجب تنفيذ اختبار وجود ووحدانية الحل للحصول بعدها على القيم الابتدائية للمسجلات الزاحفة المشتركة بالموديل.

مفاتيح الكلمات: نظم التشفير الانسيابي, المسجل الزاحف الخطي ذو التغذية الخلفية, النموذج الخطي, المهاجمة باستخدام الكلمة المحتملة.