A Mathematical Approach for Computing the Linear Equivalence of a Periodic Key-Stream Sequence Using Fourier Transform

*Raghad Kadhim Salih** *Atheer Jawad Kadhim**

Received 14, March, 2009
Accepted 19, October, 2009

Abstract

A mathematical method with a new algorithm with the aid of Matlab language is proposed to compute the linear equivalence (or the recursion length) of the pseudo-random key-stream periodic sequences using Fourier transform. The proposed method enables the computation of the linear equivalence to determine the degree of the complexity of any binary or real periodic sequences produced from linear or nonlinear key-stream generators. The procedure can be used with comparatively greater computational ease and efficiency. The results of this algorithm are compared with Berlekamp-Massey (BM) method and good results are obtained where the results of the Fourier transform are more accurate than those of (BM) method for computing the linear equivalence (L) of the sequence of period (p) when (L) is greater than (p/2). Several examples are given for conciliated the accuracy of the results of this proposed method.

Key words : Fourier transform, Linear equivalence, Periodic key-stream sequence, Berlekamp-Massey method.

Introduction :

Cryptography, communication systems and information security are considered one of important sciences in the world, especially after using the computers in these sciences. The need to keep certain messages secret has been appreciated for thousands of years. The idea of a cipher system is to disguise confidential information in such a way that its meaning is unintelligible to an unauthorized person. The information to be concealed is called plaintext [1].

Cipher systems, communication systems and control systems are usually using pseudo-random (PR) generators. A PR generator is a mechanism for generating a PR periodic sequence of binary or real digits [2]. The sequence appears random in nature but in reality it is deterministic and available to the privileged users. It is called a pseudo-random sequence since there is no algorithm using a finite state machine which can produce a truly random sequence [3]. The PR key-stream periodic sequences are used as spectrum-spreading modulations for direct sequence, spread spectrum design for digital communication system, in wireless technique and as a key in encryption to produce the ciphertext in cipher systems [3,4].

The PR key-stream sequences are characterized by three properties which define the measure of security for these sequences. These properties are period, complexity and randomness. It is absolutely crucial

*Department of Applied Sciences/University of Technology .

that if the key of the cipher system is known, one can determine the plaintext from the ciphertext. Hence the PR key-stream sequence of the cipher system or communication system must have long period, high complexity and randomness properties to have acceptable security. The linear equivalence determines the degree of complexity of the PR periodic sequences. There are several methods to determine the linear equivalence of these PR periodic sequences like Berlekamp-Massey method and matrices techniques. The linear equivalence of a periodic sequence is defined as the length (n) of the smallest *linear feedback shift register* (LFSR) that can generate the sequence. We can characterize the LFSR of length (n) by the characteristic polynomial $f(x)$:

$$f(x) = c_0 + c_1x + c_2x^2 + ... + c_{n-1}x^{n-1} + x^n$$

where c_0 ,c_1, . . .,c_{n-1} are 0 or 1. The sequence must have high linear equivalence since for a sequence with a linear equivalence (n); (2n) consecutive bits of the generated sequence are needed to deduce the whole sequence, since if (2n) consecutive bits are given, a system of n-equations in (n) unknown variables can be written to find its unique solution [1,5,6].

James L. Massey [7] suggested an algorithm which is at the present time known as Berlekamp-Massey algorithm for computing the linear equivalence of the PR sequences and Baker, J.M. and Hughes, P. gave a new explanation of the Berlekamp-Massey algorithm using a method based on matrices technique [6]. The Fourier transformation is used to determine the linear equivalence of the periodic key-stream sequences of the PR generators.

The Linear Equivalence

The linear equivalence "L" (or the recursion length) of a periodic sequence is defined as the length (n) of the smallest LFSR that can generate the sequence (i.e. L=n). The polynomial of the linear equivalence is called the minimal characteristic polynomial. So the linear equivalence of the sequence is the degree of minimal characteristic polynomial that can generate the given sequence. If the entire sequence is known, then the linear equivalence can be determined and, in fact, how actually to generate the sequence on a register of that size. We show that, for a sequence with a known linear equivalence (L), the entire sequence is given when 2L consecutive bits are known, where (2L-1) consecutive bits are not enough to determine the sequence uniquely [1,2]. The linear equivalence determines the degree of complexity of the periodic key-stream sequences of the PR generators [1,7].

Berlekamp-Massey Method

Berlekamp-Massey (BM) technique [5,6,7] uses the description based on the synthesis of a shift register where it is used to determine the linear equivalence and the minimal characteristic polynomial that can generate the given sequence .

Berlekamp-Massey method gives:

1. The polynomial C(D) reciprocal of the characteristic polynomial F(D) of the minimal LFSR that can generate the given sequence, where :

$$C(D) = D^n F(\frac{1}{D}) = 1+c_{n-1}D+\ldots+ c_1D^{n-1}+c_0D^n$$

and

$$F(D)=c_0+c_1D+\ldots+c_{n-1}D^{n-1}+D^n .$$

2. The linear equivalence (L) of the sequence .

BM technique is explained in the following algorithm :

BM Algorithm :

Step 1:

Input:

(1) The period (n) of the sequence (S).

(2) The digits S_i , i=0,2,…,n-1 of the sequence (S).

Step 2:

Put C(D) =1, B(D) =1, L=0 , b=1 ,

x=1 and N=0

Step 3:

If N = n , then stop. Otherwise compute (d):

$$d = S_N + \sum_{i=1}^{L} c_i S_{N-i}$$

Step 4:

If d = 0 , then x = x +1 , and go to (step 7)

Step 5:

If d ≠0 and 2L > N , then

- C(D) = C(D) - $db^{-1}D^xB(D)$
- x = x+1
- go to (step 7)

Step 6:

If d ≠0 and 2L ≤ N , then

- T(D) = C(D)
- C(D) = C(D) - $db^{-1}D^xB(D)$
- L = N+1- L
- B(D) = T(D)
- b = d
- x=1

Step 7:

N = N+1

and go to (step 3) .

Step 8:

From the polynomial C(D) find the characteristic polynomial F(D) as:

$$F(D) = D^n C(\frac{1}{D}) = c_0 + c_1 D + \cdots + c_{n-1} D^{n-1} + D^n \cdot$$

Example:

Consider the following sequence : S_i=0011101, where i = 0,1,…,6 and the period n=7 .

By applying BM algorithm the linear equivalence (L) of the sequence S_i=3 and the polynomial C(D) (reciprocal of F(D)) = 1+D+ D^3 .

Therefore, the minimal characteristic polynomial F(D) = 1 + D^2+ D^3.

Fourier Transformation:

The Fourier transformation is one of the major mathematical tools for analyzing linear continuous time system. It is a basic tool used in the solution of initial and boundary value problems. The Fourier transform is used to transfer the continuous signal into algebraic equations, where it transfers the differential form into algebraic form which, in many cases, helps the solution of problems.

The Fourier transform of a function $f(t)$ which is defined on $(-\infty, \infty)$ is defined by:

$$£[f(t)] = F(s) = \int_{-\infty}^{\infty} e^{ist} f(t) dt \quad \ldots \quad (1)$$

where ($£[f(t)]$) is the Fourier transform of a function $f(t)$, (s) is an arbitrary complex number. [8].

The Fourier transform possesses many notable properties. Some of the salient properties enjoyed by the Fourier transform are given in the following [9,10]:

(1) Linearity Property :

If c_1 and c_2 are any constants while $F_1(s)$ and $F_2(s)$ are Fourier Transforms of $F_1(t)$ and $F_2(t)$ respectively, then:

$$£[c_1F_1(t) + c_2F_2(t)] = c_1 £[F_1(t)] + c_2 £[F_2(t)]$$

$$= c_1F_1(s) + c_2F_2(s).$$

(2) Convolution Property :

If $\pounds[F(t)] = F(s)$ and $\pounds[G(t)] = G(s)$, then

$$\pounds[F(t)G(t)] = \pounds\left[\int_{-\infty}^{\infty} F(u)G(t-u)du\right] = \pounds[F(\mathrm{t})]\cdot\pounds[G(t)] = F(\mathrm{s})G(\mathrm{s})$$

(3) Shifting Property :

If $\pounds[F(t)] = F(s)$ then $\pounds$

$$[e^{iat}F(t)] = \int_{-\infty}^{\infty} F(t)e^{i(s+a)t}dt = F(s+a)$$

Proposed Method for Computing the Linear Equivalence of the Periodic Sequence Using Fourier Transform:

In this section Fourier transform is used to compute the linear equivalence of the periodic key-steam PR sequence.

A sequence of numbers which repeats itself every (T) discrete-time units is said to be periodic with period T. The linear equivalence can be determined mathematically using Fourier transform as follows:-

Consider the following periodic sequence (*Seq*) of numbers over GF(q) where GF(q) is the Galois field of order (q) and (q) is a prime number (q>1) :

$$Seq = a_0, a_1, a_2, \ldots, a_{T-1} \quad \ldots (2)$$

which has period (T), T>0 .

The sequence (*Seq*) can be written as a periodic function F(t) which is:

$$F(t) = \begin{cases} a_0 & 0 \le t < 1 \\ a_1 & 1 \le t < 2 \\ \vdots & \vdots \\ a_{T-1} & T-1 \le t < T \end{cases} \quad \ldots (3)$$

where $F(t) = F(t+T)$, $T > 0$ and (t) is an integer $(t \ge 0)$.

To find the Fourier transform in eq.(1) of the above periodic function F(t) in eq.(3) which has period T>0, the transformation in eq.(1) ignores all information contained in $F(t)$ prior to (t=0), since t>0.

Hence,

$$\pounds[F(t)] = \pounds[F(t+T)] = \int_0^{\infty} e^{ist}F(t)dt$$

$$= \int_0^{T} e^{ist}F(t)dt + \int_T^{2T} e^{ist}F(t)dt + \int_{2T}^{3T} e^{ist}F(t)dt + \cdots$$

In the first integral let $t = u$, in the second integral let $t = u + T$, In the third integral let $t = u + 2T$, etc. Then

$$\pounds[F(t)] = \int_0^{T} e^{isu}F(u)du + \int_0^{T} e^{is(u+T)}F(u+T)du + \int_0^{T} e^{is(u+2T)}F(u+2T)du + \cdots$$

$$= \int_0^{T} e^{isu}F(u)du + e^{isT}\int_o^{T} e^{isu}F(u)du + e^{2isT}\int_0^{T} e^{isu}F(u)du + \cdots$$

$$= (1 + e^{isT} + e^{2isT} + \cdots)\int_0^{T} e^{isu}F(u)du$$

$$= \frac{\int_0^{T} e^{isu}F(u)du}{1 - e^{isT}}$$

where we have used the periodicity to write

$F(u+T) = F(u), F(u+2T) = F(u), \ldots,$

and the fact that: $(1 + k + k^2 + k^3 + \cdots) = \dfrac{1}{1-k} \quad |k| < 1 \cdot$

Hence,

$$\pounds[F(t)] = F(s) = \frac{\int_0^{T} e^{ist}F(t)dt}{1 - e^{isT}} = \frac{P(s)}{Q(s)} \quad \ldots (4)$$

From eq.(3) and eq.(4) one gets the following equations :

$$P(s) = \int_0^{T} e^{ist}F(t)dt$$

$$= \int_{0}^{1} a_0 e^{ist}\, dt + \int_{1}^{2} a_1 e^{ist}\, dt + \cdots + \int_{T-1}^{T} a_{T-1} e^{ist}\, dt$$
… (5)

and

$$Q(s) = 1 - e^{isT} \quad \ldots (6)$$

The results of eq.(5) is :

$$P(s) = \frac{1}{is}\left[-a_0 e^{0} + a_0 e^{is} - a_1 e^{is} + a_1 e^{2is} - \cdots - a_{T-1} e^{i(T-1)s} + a_{T-1} e^{iTs}\right]$$
… (7)

Let $P(s) = \frac{1}{is} G(s)$, where

$$G(s) = -a_0 e^{0} + a_0 e^{is} - a_1 e^{is} + a_1 e^{2is} - \cdots - a_{T-1} e^{i(T-1)s} + a_{T-1} e^{isT}$$
… (8)

Then, $$F(s) = \frac{\frac{1}{is} G(s)}{Q(s)} \quad \ldots (9)$$

Hence, the linear equivalence can be found from eq.(9) as follows :-

a) Since the arithmetic operations over Galois field of order q (GF(q)), then *Q*(s) in eq.(6) can be written as :

$$Q(s) = (1 - e^{isT}) \bmod q = 1 \oplus_q e^{isT} \quad \ldots (10)$$

where $\oplus_q$ is a modulo (q) addition.

b) Ignore the negative terms from *G*(s) in eq.(8) to be :

$$G(s) = a_0 e^{is} + a_1 e^{2is} + a_2 e^{3is} + \cdots + a_{T-1} e^{isT}$$
… (11)

c) Simplify the function *F*(*s*), where $F(s) = \frac{\frac{1}{is} G(s)}{Q(s)}$ using eq.(10) and eq.(11) to be:

$$F(s) = \frac{\frac{1}{is} E(s)}{C(s)}$$ where

$$E(s) = \frac{G(s)}{\gcd(Q(s), G(s))} ,$$

$$C(s) = \frac{Q(s)}{\gcd(Q(s), G(s))}$$

and $\gcd(Q(s), G(s))$ is the greatest common divisor of $Q(s)$ and $G(s)$ in eq.(10) and eq.(11) respectively.

d) Convert C(s) in step (c) into the polynomial *C*(*x*) by using the relation :

$$x^{r} = e^{irs} \qquad (0 \le r \le T).$$

e) Find the polynomial *M*(*x*) using the polynomial *C*(*x*) in step (d) as follows :

$$M(x) = x^{n} C\left(\frac{1}{x}\right) = c_n + c_{n-1} x + \cdots + c_0 x^{n}$$

where $C(x) = c_0 + c_1 x + \cdots + c_n x^{n}$, (n) is the degree of the polynomial *C*(*x*) and $c_0, c_1, \ldots, c_n$ are the coefficients of *C*(*x*).

f) The linear equivalence (L) can be determined as :

$$L = Deg(M(x))$$

where $Deg(M(x))$ is the degree of the characteristic polynomial *M*(*x*) and *M*(*x*) is the characteristic polynomial of the minimal LFSR that can generate the given sequence.

The following algorithm summarizes the steps for using the ***F**ourier **t**ransform* for finding the ***l**inear **e**quivalence* (L) of the periodic key-stream PR sequence.

FT-LE Algorithm:

Step 1:

Input the sequence (*Seq*) over GF(q) of period (T) ,T>0

$$Seq = a_0, a_1, \ldots, a_{T-1}$$

Step 2:

Take the Fourier transformation to the periodic sequence in step(1) by using :

$$F(s)=\frac{\int_0^T e^{ist}F(t)dt}{1-e^{isT}}=\frac{P(s)}{Q(s)}$$

where $F(t)$ in eq.(3).

Step 3:

From step (2) find G(s) in eq.(8) and Q(s) in eq.(10).

Step 4:

Ignore the negative terms from G(s) in (step 3) to be :

$$G(s)=a_0e^{is}+a_1e^{2is}+a_2e^{3is}+\cdots+a_{T-1}e^{isT}$$

Step 5:

Find the greatest common divisor of the two polynomials Q(s) and G(s) ($\gcd(Q(s),G(s))$) over GF(q) as follows:

a) Input the two polynomials G(s) and Q(s) where the degree of Q(s) is greater than or equal to G(s).

b) According to the arithmetic operations over GF(q), compute r where r is the remainder from dividing Q(s) by G(s) using modulo (q) in addition.

c) If r =0 then :

- $\gcd(Q(s),G(s))=G(s)$
- go to (step d)

else

- Set: Q(s)=G(s)
  G(s) = r
- Go to (step b)

d) End.

Step 6:

Simplify the function F(s) in step (2) using G(s) in step (4) and Q(s) in step (3) to be :

$$F(s)=\frac{\frac{1}{is}E(s)}{C(s)}$$ where

$$E(s)=\frac{G(s)}{\gcd(Q(s),G(s))}\ ,$$

$$C(s)=\frac{Q(s)}{\gcd(Q(s),G(s))}\ ,$$

and $\gcd(Q(s),G(s))$ is the greatest common divisor of $Q(s)$ and $G(s)$ in eq.(10) and eq.(11) respectively.

Step 7:

Convert $C(s)$ in step (6) into the polynomial $C(x)$ by using the relation:

$x^r=e^{irs}$, $(0\le r\le T)$.

Step 8:

Use the polynomial $C(x)$ to find the polynomial $M(x)$ as follows :

$$M(x)=x^nC(\frac{1}{x})$$

$$=c_n+c_{n-1}x+\cdots+c_0x^n$$

where

$C(x)=c_0+c_1x+\cdots+c_nx^n$, (n) is the degree of the polynomial $C(x)$ and $c_0,c_1,\ldots,c_n$ are the coefficients of $C(x)$.

Step 9:

Determine the linear equivalence (L) by :

$$L=Deg(M(x))$$

where $Deg(M(x))$ is the degree of the characteristic polynomial $M(x)$ and $M(x)$ is the characteristic polynomial of the minimal LFSR that can generate the given sequence.

FT-LE algorithm enables the computation of the linear equivalence accurately for any binary or non-binary periodic PR sequences produced from linear or nonlinear generators.

Illustrative Examples :

<u>Example (1)</u> **:**

Consider the following PR periodic key-stream sequence over GF(2) :-

Seq=<u>0011101</u> 0011101 … , where the period T=7 .

The function F(t) can be obtained from the first period of the above sequence using eq.(3) as follows :-

$$F(t)=\begin{cases}0 & 0\le t<2\\ 1 & 2\le t<5\\ 0 & 5\le t<6\\ 1 & 6\le t<7\end{cases}$$

The function F(t)=F(t+T) is shown in figure (1).

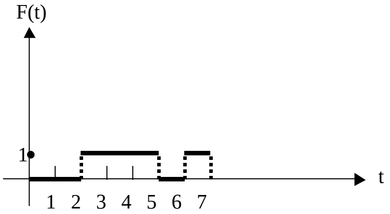


Figure (1) The function F(t) in example (1).

According to eq.(4) the Fourier transform of *F*(t) = *F*(t+T) is :

$$\pounds[F(t)]=F(s)=\frac{\int_0^7 e^{ist}F(t)dt}{1-e^{7is}}=\frac{P(s)}{Q(s)}$$

Hence, by applying (FT-LE) algorithm the following results are obtained :

$$P(s)=\frac{1}{is}\left[-e^{2is}+e^{3is}-e^{3is}+e^{4is}-e^{4is}+e^{5is}-e^{6is}+e^{7is}\right]$$

$$G(s)=e^{3is}+e^{4is}+e^{5is}+e^{7is}$$
$$Q(s)=(1-e^{7is})\bmod 2=1+e^{7is}$$

and $F(s)=\dfrac{\frac{1}{is}E(s)}{C(s)}$ where:

$\gcd(Q(s),G(s))=e^{4is}+e^{2is}+e^{is}+1,$

$E(s)=e^{3is}$ and $C(s)=e^{3is}+e^{is}+1.$

The polynomial $C(x)$ is obtained from $C(s)$ by using the relation: $x^r=e^{ris}\quad(0\le r\le 7)$

$\Rightarrow C(x)=x^3+x+1.$

Therefore,

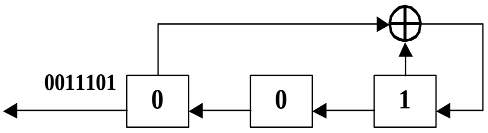
$M(x)=x^3C(\frac{1}{x})=1+x^2+x^3$

Then, the linear equivalence (L) of the PR key-stream sequence (*Seq*) is :-

$$L=Deg(M(x))=3\ .$$

where *M*(*x*) is the characteristic polynomial of the minimal LFSR that can generate the sequence (*Seq*) .

The result of this example can be verified directly by generating the minimal characteristic polynomial *M*(*x*) of 3-stage LFSR using the first three consecutive bits (i.e. the initial state 001) from the sequence (*Seq*) as it is illustrated in the following figure:



The results of *M*(*x*) and (L) in this example are the same results as those of F(D) and (L) in the example in section (3) where F(D) and (L) are obtained by using Berlekamp-Massey (BM) method.

Example (2) :

Consider the following PR periodic sequence over GF(3) :-

Seq=0,2,2,1,0,1,1,2 where the period T=8 .

The function F(t) can be obtained from the PR sequence (*Seq*) using eq.(3) as follows :-

$$F(t)=\begin{cases} 0 & 0\le t<1 \\ 2 & 1\le t<2 \\ 2 & 2\le t<3 \\ 1 & 3\le t<4 \\ 0 & 4\le t<5 \\ 1 & 5\le t<6 \\ 1 & 6\le t<7 \\ 2 & 7\le t<8 \end{cases}$$

The function F(t)=F(t+T) is shown in figure (2).

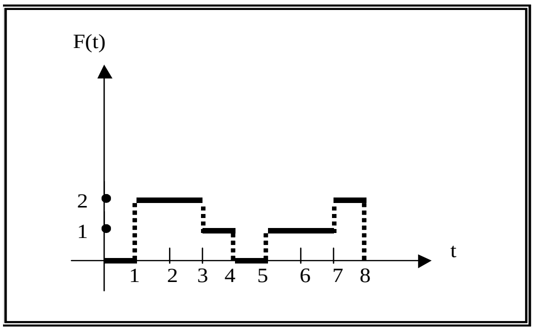


Fig.(2) The function F(t) in example (2).

By applying (FT-LE) algorithm the following results are obtained :

$$P(s)=\frac{1}{is}\left[-2e^{is}+2e^{2is}-2e^{2is}+2e^{3is}-e^{3is}+e^{4is}-e^{5is}+e^{6is}-e^{6is}+e^{7is}-2e^{7is}+2e^{8is}\right]$$

$$G(s)=2e^{2is}+2e^{3is}+e^{4is}+e^{6is}+e^{7is}+2e^{8is}$$

$$Q(s)=(1-e^{8is})\bmod 3=1+2e^{8is}$$

and $F(s)=\dfrac{\frac{1}{is}E(s)}{C(s)}$ where :

$$\gcd(Q(s),G(s))=2e^{6is}+e^{5is}+e^{4is}+e^{2is}+2e^{is}+2$$

,

$E(s)=e^{2is}$ and

$$C(s)=e^{2is}+e^{is}+2$$

The polynomial *C*(*x*) is obtained from *C*(*s*) by using the relation: $x^r=e^{ris}\quad(0\le r\le 8)$

$$\Rightarrow C(x)=x^2+x+2\,.$$

Therefore,

$M(x)=x^2C(\frac{1}{x})=1+x+2x^2$ and the linear equivalence (L) of the PR sequence (*Seq*) is:

$$L=Deg(M(x))=2$$

where *M*(*x*) is the minimal characteristic polynomial that can generate the sequence (*Seq*) .

The result can be verified directly by generating the minimal characteristic polynomial *M*(*x*) using the first two consecutive bits (i.e. the initial state 0,2) from the sequence *Seq*.

In this example, the Fourier transform determined the linear equivalence of the non-binary sequence also.

Example (3) :

Consider the following PR periodic sequence over GF(7) :-

Seq=4,3,6,6,6,5,1,3,4,6,0,5 where the period T=12 .

The function F(t) can be obtained from the PR sequence (*Seq*) using eq.(3) as follows :-

$$F(t)=\begin{cases}4 & 0\le t<1\\ 3 & 1\le t<2\\ 6 & 2\le t<5\\ 5 & 5\le t<6\\ 1 & 6\le t<7\\ 3 & 7\le t<8\\ 4 & 8\le t<9\\ 6 & 9\le t<10\\ 0 & 10\le t<11\\ 5 & 11\le t<12\end{cases}$$

By applying (FT-LE) algorithm the following results are obtained :

$$P(s)=\frac{1}{is}\begin{bmatrix}-4+e^{is}-3e^{is}+3e^{2is}-6e^{2is}+6e^{3is}-6e^{3is}+6e^{4is}-6e^{4is}+6e^{5is}-5e^{5is}+5e^{6is}\\ -e^{6is}+e^{7is}-3e^{7is}+3e^{8is}-4e^{8is}+4e^{9is}-6e^{9is}+6e^{10is}-5e^{11is}+5e^{12is}\end{bmatrix}$$

$$G(s)=e^{is}+3e^{2is}+6e^{3is}+6e^{4is}+6e^{5is}+5e^{6is}+e^{7is}+3e^{8is}+4e^{9is}+6e^{10is}+5e^{12is}$$

$$Q(s)=(1-e^{12is})\operatorname{mod}7=1+6e^{12is}$$

and $F(s)=\dfrac{\frac{1}{is}E(s)}{C(s)}$ where

$$\gcd(Q(s),G(s))=3e^{9is}+6e^{8is}+6e^{7is}+5e^{6is}+e^{5is}+2e^{4is}+e^{3is}+2e^{2is}+3e^{is}+6$$

, $E(s)=4e^{3is}+6e^{2is}+3e^{is}$ and

$C(s)=2e^{3is}+3e^{2is}+4e^{is}+6$.

The polynomial $C(x)$ is obtained from $C(s)$ by using the relation

$x^r=e^{ris}\quad(0\le r\le 12)$

$\Rightarrow C(x)=2x^3+3x^2+4x+6$.

Therefore,

$$M(x)=x^3C(\frac{1}{x})=2+3x+4x^2+6x^3$$

and the linear equivalence (L) of the PR sequence (*Seq*) is :-

$$L=Deg(M(x))=3$$

where $M(x)$ is the minimal characteristic polynomial that can generate the sequence (*Seq*) .

The result can be verified directly by generating the minimal characteristic polynomial $M(x)$ using the first three consecutive bits (i.e. the initial state 4,3,6) from the sequence *Seq*.

For a comparison between the results of Fourier transform and Berlekamp-Massey (BM) method, table (1) and table (2) present the linear equivalence (L) with the minimal characteristic polynomial of some PR sequences using Fourier transform and Berlekamp-Massey (BM) method respectively by applying (FT-LE) and (BM) algorithms respectively.

Table (1) The Fourier transform for finding the linear equivalence with the minimal characteristic polynomial.

	PR key-stream sequences	Period	*Fourier transform (FT-LE) algorithm*			
			$M(x)$	L	Output sequence of $M(x)$	Period
1	1110010	7	x^3+x+1	3	1110010	7
2	101011001000111	15	x^4+x^3+1	4	101011001000111	15
3	100101100000 101001001	21	$x^6+x^4+x^2+x+1$	6	100101100000 101001001	21
4	10100011	8	$x^7+x^6+x^5+x^4+x^3+x^2+x+1$	7	10100011	8
5	1110001	7	$x^6+x^5+x^4+x^3+x^2+x+1$	6	1110001	7
6	000101100011111	15	$x^{10}+x^8+x^5+x^4+x^2+x+1$	10	000101100011111	15
7	1111001000011010	16	$x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	15	11110010000110 10	16
8	9,10,6,0,2,5,4,8 over GF(11)	8	$3x^7+3x^6+3x^5+3x^4+3x^3+3x^2+3x+3$	7	9,10,6,0,2,5,4,8	8
9	1010010110000111	16	$x^{12}+x^8+x^4+1$	12	10100101100001 11	16

Table (2) The Berlekamp-Massey (BM) method for finding the linear equivalence with the minimal characteristic polynomial.

	PR key-sream sequences	Period	*Berlekamp-Massey method (BM) algorithm*			
			F(D)	L	Output sequence of F(D)	*Period*
1	1110010	7	D^3+D+1	3	1110010	7
2	101011001000111	15	D^4+D^3+1	4	101011001000111	15
3	100101100000101001001	21	$D^6+D^4+D^2+D+1$	6	100101100000101001001	21
4	10100011	8	$D^4+D^3+D^2+1$	4	1010001	7
5	1110001	7	D^4+D+1	4	111000100110101	15
6	000101100011111	15	$D^8+D^6+D^4+D^3+D^2+D+1$	8	0001011000111111011010…0110	255
7	1111001000011010	16	$D^{10}+D^9+D^8+D^5+D^3+D+1$	10	111100100010110101010001000…11110010	93
8	9,10,6,0,2,5,4,8 over GF(11)	8	D^2+3D+7	2	9,10,6,0,2,5,4,8,3,1	10
9	1010010110000111	16	$D^9+D^8+D^7+D^6+D^5+D^4+D^3+D+1$	9	10100101100001111110…111001101	511

It is obvious from the comparison between table (1) and table (2), the results of Fourier transform are more accurate than those of Berlekamp-Massey (BM) method for computing the linear equivalence for determining the complexity of the PR key-stream sequence from the first period of the sequence. Since from the fourth to ninth row in table (2), we notice the output sequence of the characteristic polynomial F(D) is not the same PR sequence with the same period exactly while the results in table (1) has high accuracy for determining the linear equivalence because the output sequence of $M(x)$ is the same given PR sequence with the same period. Hence, Fourier transform enables the computation of the linear equivalence to determine the degree of the complexity of these PR sequences with high accuracy.

Conclusion :

The decryption of the ciphertext in cipher system depends on the availability of the key-stream of the ciphertext. So, one of the important properties of the PR key-stream sequence is to have high linear equivalence to have high complexity in order to be difficult for the cryptanalyst to obtain the entire sequence when only small segment of it is known.. The results of the Fourier transform show a marked improvement for computing the linear equivalence. It has been shown that the proposed method is comparable in accuracy with BM method. From some illustrative examples in table (1) and table (2) the following points are listed:

1- The Fourier transform was successfully employed to compute the linear equivalence of the binary or real PR key-stream sequences which are produced from linear and nonlinear generators.

2- The Fourier transform gives better accuracy than BM method for determining the linear equivalence and so it enables the computation of the complexity which determines the ability of security of PR key-stream sequences.

3- When the linear equivalence (L) of the given sequence of period (p) is greater than (p/2) then BM method fails to determine the minimal characteristic polynomial which generates the same given sequence with the same period (p) exactly, since BM method is based on the synthesis of a shift register by taking one bit from the given sequence each time, so the linear equivalence (L) changes if only (d $\neq$ 0) and ($2L \leq N$) where :

$$d = S_N + \sum_{i=1}^{L} c_i S_{N-i} \ .$$

Therefore, when (d=0), L is not changed, see section (3).

References :

1.Baker, H.J. and Piper, F.C.1982. Cipher Systems: The Protection of Communications, Northwood Publications, 1st edition, London, pp 406.

2.Salih, R.K.2007. Asymptotic Behavior of the Linear Equivalence Determination of the Periodic Sequence, Engi. & Techno. J. 25(3):228-240.

3.Kadhim, A.J. 2007. A Mathematical Development of Gordon, Mills and Welch Generator Using Galois Field and Trace Polynomials, Engi. & Techno. J. 25(8):958-968.

4.Marvin, K.S., Jim, K.O., Robert, A.S. and Barry, K.L.1985. Spread Spectrum Communications, John Wiley & Sons Inc., Vol.1, USA, pp 430.

5.Song, Yan. J.2000.Number Theory for Computing, Springer-Verlag, 3rd edition, Germany pp 324.

6.John, D.O.2004. LFSR Synthesis and Spread Spectrum Decoding in Digital Communication System, IE Tr. on Inf. Theory, IT-28(6):858-864.

7.Maskar, S.L. and Das, J.H.2003. Concatenated Sequences for Spread Spectrum Systems, IEEE Tr. on Aerospace and Electronic systems, AES-17(3):342-349.

8.Joun, M.R.1973. Fourier Transform, Prentice Hall Inc., Schaum's Outline Series, New York, pp 261.

9.Kuo, B.C.1997. Automatic Control System, Printed in the New Jersey, Third Edition, USA, pp 278.

10. Bracewell, R.D. 1975.The Fourier Transform and Its Applications, Mc Graw-Hill Book Company, 2nd edition, New York, pp 304.

طريقة رياضية لحساب المكافئ الخطي لمتتابعة انسياب المفتاح الدورية باستخدام محول فورير

رغد كاظم صالح ***أثير جواد كاظم***

*قسم العلوم التطبيقية /الجامعة التكنولوجية.

الخلاصة:

يقدم البحث طريقة مقترحة مع خوارزمية مطورة لحساب المكافئ الخطي رياضياً لمتتابعات انسياب المفتاح الدورية باستخدام محول فورير اذ من الممكن حساب المكافئ الخطي لأية متتابعة دورية ثنائية أو غير ثنائية يتم إنتاجها من مولدات مفاتيح خطية وغير خطية باستخدام هذا المحول. استخدمت لغة (Matlab) لبرمجة هذه الطريقة. من الممكن ملاحظة كفاءة الطريقة و سهولة الحسابات فيها اذ تمت مقارنة نتائج هذه الطريقة بنتائج طريقة بيرليكامب ماسي من خلال بعض الأمثلة التوضيحية و قد تم الحصول على نتائج دقيقة لتحديد المكافئ الخطي للمتتابعات الدورية و التي تمتلك مكافئاً خطياً اكبر من نصف طول الدورة .