Laplace Transformation for Determining The Linear Equivalence of The Periodic Sequence

Raghad Kadhim Salih

Received on: 18/10/2005
Accepted on: 12/ 7/ 2006

Abstract

The research presents a proposed method with an algorithm written in Matlab language to determine the linear equivalence of the pseudo-random periodic sequences mathematically by using the Laplace transform. The proposed method enables the computation of the linear equivalence to determine the degree of the complexity of any periodic sequences produced from linear or nonlinear key generators. The procedure can be used 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 Laplace 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). Some examples are given for consolidating the accuracy of the results of this proposed method.

Keywords: Linear equivalence, Laplace transform, Periodic sequence and Berlekamp-Massey method.

محـــول لابـــلاس لتحـــديد المكافـــئ الخـــطي للمتتابـــعة الـــدوريـــة

الخلاصة

يقدم البحث طريقة مقترحة مع خوارزمية مطورة لحساب المكافئ الخطي رياضياً للمتتابعـــات الدورية عن طريق استخدام محول لابلاس حيث من الممكن حساب المكافئ الخطي لأي متتابعة دورية ثنائية أو غير ثنائية يتم إنتاجها من مولدات مفاتيح خطية وغير خطية. استخدمت لغـــة (Matla) لبرمجة هذه الطريقة. من الممكن ملاحظة كفاءة الطريقة و سهولة الحسابات فيهـــا حيث تمت مقارنة نتائج هذه الطريقة مع نتائج طريقة بيرليكامب ماسي من خلال بعض الأمثلة التوضيحية و قد تم الحصول على نتائج دقيقة لتحديد المكافئ الخطي للمتتابعات الدورية والتي تمتلك مكافئ خطي اكبر من نصف طول الدورة .

1. 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 pseudo-random (PR)

https://doi.org/10.30684/etj.25.2.9
2412-0758/University of Technology-Iraq, Baghdad, Iraq

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 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 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 that if the key of the cipher system is known, one can determine the plaintext from the ciphertext. Hence the PR key 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 $f(x)$:

$$f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} + x^n$$

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 Laplace transformation is used to determine the linear equivalence of the periodic sequences of the PR generators.

2. The Linear Equivalence

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. 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. The linear equivalence determines the degree of complexity of the periodic sequence of the PR generators [1,7].

3. 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) .

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 $F(D) = 1 + D^2+ D^3$.

4. The Laplace Transformation

The Laplace transformation is one of the major mathematical tools for analyzing linear continuous time system. It is a basic tool used in the solution of ordinary linear differential equations. The Laplace transform is used to transfer the continuous signal into algebraic equations which, in many cases, help the solution of problems.

The Laplace transform of a function $f(t)$ ($\mathcal{L}[f(t)]$) which is defined for (t>0) is defined by :-

$$\mathcal{L}[f(t)] = F(s) = \int_0^\infty e^{-st} f(t)dt \quad \ldots(1)$$

where (s) is an arbitrary complex number. The transformation in eq.(1) ignores all information contained in $f(t)$ prior to (t=0) [8,9].

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

***(1) Linearity Property* :**

If c_1 and c_2 are any constants while $F_1(t)$ and $F_2(t)$ are two functions defined for (t>0), then

$$\mathcal{L}[c_1F_1(t)+c_2F_2(t)] = c_1\mathcal{L}[F_1(t)]+c_2\mathcal{L}[F_2(t)] = c_1F_1(s)+c_2F_2(s).$$

***(2) Convolution Property* :**

If $\mathcal{L}[F(t)] = F(s)$ and $\mathcal{L}[G(t)] = G(s)$, then

$$\mathcal{L}[F(t)G(t)] = \int_0^t F(u)G(t-u)du = F(s)G(s).$$

***(3) Periodic Function Property* :**

If $F(t)$ has period T>0 where $F(t) = F(t+T)$, then

$$\mathcal{L}[F(t)] = F(s) = \frac{\int_0^T e^{-st}F(t)dt}{1-e^{-sT}}$$

5. Proposed Method for Linear Equivalence Determination Using Laplace Transform :

Periodic function property of the Laplace transform is used to determine the linear equivalence of the periodic 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 Laplace transform as follows :-

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

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

which has period (T), T>0 .

The sequence (*Seq*) can be written as:

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

where $F(t) = F(t+T)$, $T > 0$.

The Laplace transform of the above periodic function according to property (3) in section (4) is :

$$\mathcal{L}[F(t)] = F(s) = \frac{\int_0^T e^{-st}F(t)dt}{1-e^{-sT}} = \frac{P(s)}{Q(s)} \quad \ldots(4)$$

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

$$P(s) = \int_0^T e^{-st}F(t)dt = \int_0^1 a_0e^{-st}dt + \int_1^2 a_1e^{-st}dt + \mathbf{L} + \int_{T-1}^T a_{T-1}e^{-st}dt \quad \ldots(5)$$

and

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

The results of eq.(5) is :

$$P(s)=\frac{1}{s}\left[\begin{array}{l}a_0e^{0}-a_0e^{-s}+a_1e^{-s}-\\ a_1e^{-2s}+\mathbf{L}+a_{T-1}e^{-(T-1)s}\\ -a_{T-1}e^{-Ts}\end{array}\right] \quad \ldots(7)$$

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

$$G(s)=a_0e^{0}-a_0e^{-s}+a_1e^{-s}-a_1e^{-2s}+\mathbf{L}+a_{T-1}e^{-(T-1)s}-a_{T-1}e^{-sT} \quad \ldots(8)$$

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

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 :

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

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

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

$$G(s)=a_0e^{0}+a_1e^{-s}+a_2e^{-2s}+\mathbf{L}+a_{T-1}e^{-(T-1)s} \quad \ldots(11)$$

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

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

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

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

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 :

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

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

$$M(x)=x^nC(\frac{1}{x})$$
$$=c_n+c_{n-1}x+\mathbf{L}+c_0x^n$$

where $C(x)=c_0+c_1x+\mathbf{L}+c_nx^n$, (n) is the degree of the polynomial $C(x)$ and $c_0,c_1,\mathbf{K},c_n$ 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 ***Lap****lace transform* for finding the ***l****inear* ***e****quivalence* (L) of the periodic sequence.

LAPLE Algorithm:

Step 1:

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

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

Step 2:

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

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

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 :

$$G(s) = a_0 e^0 + a_1 e^{-s} + a_2 e^{-2s} + \mathbf{L} + a_{T-1} e^{-(T-1)s}$$

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 :

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

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

Step 8:

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

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

$$= c_n + c_{n-1}x + \mathbf{L} + c_0 x^n$$

where

$C(x) = c_0 + c_1 x + \mathbf{L} + c_n x^n$, (n) is the degree of the polynomial *C*(*x*) and $c_0, c_1, \mathbf{K}, c_n$ 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.

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

6. Illustrative Examples :

Example (1) **:**

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

Seq=0011101 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).

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

$$\mathcal{L}[F(t)] = F(s) = \frac{\int_0^7 e^{-st}F(t)dt}{1-e^{-7s}} = \frac{P(s)}{Q(s)} \quad .$$

Hence, by applying (LAPLE) algorithm the following results are obtained :

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

$$G(s)=e^{-2s}+e^{-3s}+e^{-4s}+e^{-6s}$$

$$Q(s)=(1-e^{-7s})\bmod 2=1+e^{-7s}$$

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

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

$$E(s)=e^{-2s} \text{ and } C(s)=e^{-3s}+e^{-s}+1$$

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

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

Therefore,

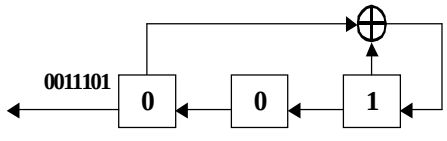
$$M(x) = x^3 C(\frac{1}{x}) = 1 + x^2 + x^3$$

Then, the linear equivalence (L) of the PR 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

btained 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).

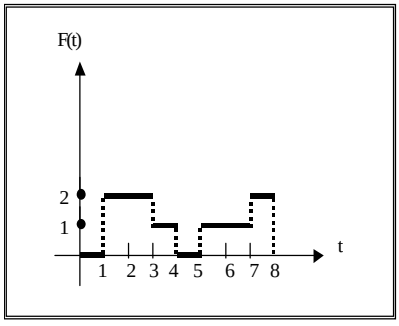


Fig.(2) The function F(t) in example (2).

By applying (LAPLE) algorithm the following results are obtained :

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

$$G(s)=2e^{-s}+2e^{-2s}+e^{-3s}+e^{-5s}+e^{-6s}+2e^{-7s}$$

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

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

where :

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

$$E(s)=2e^{-s} \quad \text{and}$$

$$C(s)=2e^{-2s}+2e^{-s}+1$$

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

$$\Rightarrow C(x)=2x^2+2x+1.$$

Therefore,

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

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 Laplace transform has 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 (LAPLE) algorithm the following results are obtained :

$$P(s)=\frac{1}{s}\left[\begin{array}{l}4-e^{-s}+3e^{-s}-3e^{-2s}+\\ 6e^{-2s}-6e^{-3s}+6e^{-3s}-\\ 6e^{-4s}+6e^{-4s}-6e^{-5s}+\\ 5e^{-5s}-5e^{-6s}+e^{-6s}-\\ e^{-7s}+3e^{-7s}-3e^{-8s}+\\ 4e^{-8s}-4e^{-9s}+6e^{-9s}-\\ 6e^{-10s}+5e^{-11s}-5e^{-12s}\end{array}\right]$$

$$G(s)=4+3e^{-s}+6e^{-2s}+6e^{-3s}+6e^{-4s}+5e^{-5s}+e^{-6s}+3e^{-7s}+4e^{-8s}+6e^{-9s}+5e^{-11s}$$

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

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

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

$$E(s)=4e^{-2s}+6e^{-s}+3$$

and

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

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

$$x^r=e^{-rs}\qquad(0\le r\le 12)$$

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

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 Laplace 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 Laplace transform and Berlekamp-Massey (BM) method respectively by applying (LAPLE) and (BM) algorithms respectively.

It is obvious from the comparison between table (1) and table (2), the results of Laplace transform are more accurate than those of Berlekamp-Massey (BM) method for computing the linear equivalence for determining the complexity of the PR 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, Laplace transform enables the computation of the linear equivalence to determine the degree of the complexity of these PR sequences with high accuracy.

5. Conclusion:

The description of the ciphertext in cipher system depends on the availability of the key of the ciphertext. So, one of the important properties of the PR key 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 Laplace transform was successfully employed to compute the linear equivalence of the PR sequences which are produced from linear and nonlinear generators. It has been shown that the proposed method is comparable in accuracy with BM method. The results show a marked improvement for determining the linear equivalence. From some illustrative examples in table (1) and table (2) the following points are drawn :

1- The Laplace 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 sequences.

2- 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).

6. References :

1. Baker , H.J. and Piper, F.C., Cipher Systems: The Protection Of Communications, Northwood Publications, London,1982.

2. Shiff, Maurice L. , Pseudo-Noise Codes from Spread Spectrum Scene Online , www.sss-mag.com/png2. html - 13k , March 19, 2002 .

3. John Koeter , LFSR Generator Implementations, www.Newwaveinstruments.com/ resources/articles/msequenceline

ar_feedback_shiftregisterlfsr.htm - 60k , 2003.

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

5. Song, Yan., Number Theory For Computing, Printed in Germany, Springer-Verlag, 2000.

6. Baker, J.M. and Hughs, P.M. "Communications Speech and Vision", Jr. Proc.I , IPIDDG 136, Vol.1, p. 115-119, 1989.

7. Massey , J.L., "Shift Register Synthesis and BCH Decoding" IEEE Trans. on Information Theory, Vol.IT-15, No.3, p.140-146, January, 1969.

8. Marry, R., Laplace Transform, Schaum's Outline Series, New York, Prentice Hall, Inc., 1973.

9. Karniel, Amir and Gideon, F. Inbar, Linear System Description, www.visl.technion.ac.il/karniel/pub/karnielInbar/ModernTechNs/ch21.pdf., 2004.

10. Kuo, Benjamin C., Automatic Control System, Third Edition, Printed in the New Jersey, 1997.

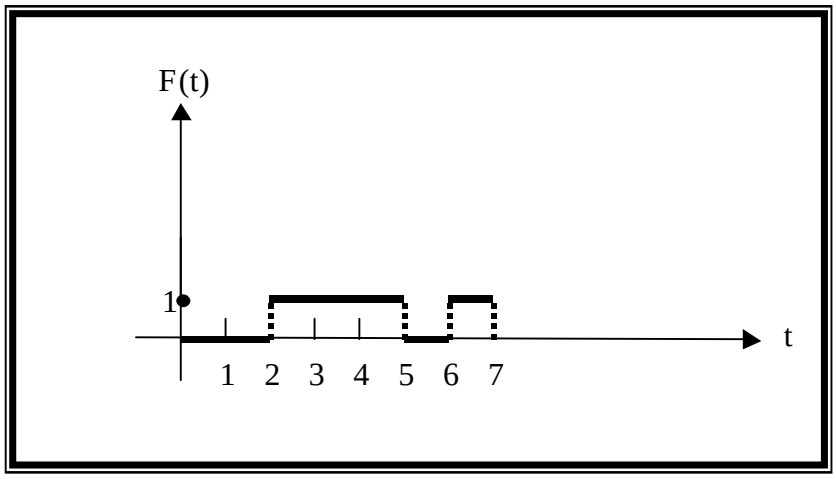


Figure (1) The function F(t) in example (1).

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

	PR sequences	Period	Laplace transform (LAPLE) algorithm			
			$M(x)$	L	Output sequence of $M(x)$	Period
1	0011101	7	$x^3 + x^2 + 1$	3	0011101	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	1111001000011010	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	1010010110000111	16

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

	PR sequences	Period	Berlekamp-Massey method (BM) algorithm			
			F(D)	L	Output sequence of F(D)	Period
1	0011101	7	$D^3 + D^2 + 1$	3	0011101	7
2	1010110010000111	15	$D^4 + D^3 + 1$	4	101011001000111	15
3	1001011000001001001	21	$D^6+D^4+D^2+D+1$	6	100101100000101001	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	0001011000111111	15	$D^8+ D^6+D^4+D^3+D^2+D+1$	8	000101100011111101101 0…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	101001011000011111101…1110011101	511