# Linear Equivalence Determination of Key-Stream Sequence Using Z-Transform

Omar Mohammed Al-Faour * Shymaa Hussain Salih**
&
Shazad Shawki Ahmed Mohammed***

Date of acceptance 7/11/2005

## Abstract

The research presents a proposed method to compute or determine the linear equivalence of the key-stream sequences in stream cipher systems by using periodic sequence property of the Z-transform. This proposed method enables us to compute the linear equivalence of any periodic sequence produced from linear or nonlinear key-stream generators and accurate results are obtained.

**Key words :** Key-Stream sequence, Linear equivalence, Z-Transformation, Stream cipher system.

## 1. Introduction

Cryptography and data security are considered one of important sciences in the world, especially after using the computers in these sciences. They have played a big role in computer science for information security. The need to keep messages secret has been favored for thousands of years. The idea of a cipher system is to hide confidential data to be unknown to an unauthorized person. The information to be hidden is called plaintext. Generally, there are several approaches in cryptography such as classical methods, stream cipher and public-key method. Stream cipher system is considered one of important system for security of the information. The basic element in stream cipher system is the key stream generator which generates the key-stream sequence to be combined or mixed with the plaintext stream using modulo 2 addition to produce the ciphertext stream. It is obvious that if the key of the cipher system is known, the plaintext can be determined from the ciphertext. Hence the key sequence must have properties to have acceptable security. These properties are long period, high complexity and randomness properties [1,2]. The linear equivalence determines the degree of complexity of the key sequence. There are several methods to determine the linear equivalence of these key sequences like Berlekamp-Massey method and matrices techniques. The linear equivalence of a periodic sequence is defined as the length (n) of

* Dr, University of Technology
** University of Technology
*** University of Al-Sulaymaniya

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*) :

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

where $c_0, c_1, \ldots, c_{n-1}$ are 0 or 1. The key 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 [1,3,4].

James L. Massey [4] suggested an algorithm which is at the present time known as Berlekamp-Massey algorithm for computing the linear equivalence of the key sequences and J.M. Baker and P. Hughes gave a new explanation of the Berlekamp-Massey algorithm using a method based on matrices technique [5]. The Z-transform is used to determine the linear equivalence of the sequences which are used as a key in stream cipher system.

## 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 generated sequence [3,4,5].

## 3. The Z-Transform

The Z-transform is used to transfer sequences of numbers into algebraic equations which, in many cases, help the solution of problems. It is a rule by which a sequence of numbers is converted into a function of the transform variable (z).

The Z-transform of a sequence of numbers $\{f(k)\}$ which is identically zero for negative discrete time (i.e. $f(k) = 0$ for $k = -1,-2,-3,\ldots$) is defined by:

$$Z\{f(k)\} = F(z) = \sum_{k=0}^{\infty} f(k)z^{-k} \quad \ldots(1)$$

where z is an arbitrary complex variable [6,7].

The Z-transform possesses many important properties. These properties will prove to be useful in the analysis of discrete systems [6,7].

***a) Linearity Property :***

If $f_1$ (k) and $f_2$ (k) are two discrete signals have Z-transform $F_1$(z) and $F_2$(z) respectively, then :

$$Z\{a f_1(k) + b f_2(k)\} = a F_1(z) + b F_2(z) ,$$
$$k = 0,1,2,\ldots$$

where a and b are constants .

Proof :

From the definition of the Z-transform in eq.(1):

$$Z\{af_1(k) + bf_2(k)\} =$$
$$\sum_{k=0}^{\infty}\{af_1(k) + bf_2(k)\}z^{-k}$$
$$= a\sum_{k=0}^{\infty} f_1(k)z^{-k} + b\sum_{k=0}^{\infty} f_2(k)z^{-k}$$
$$= a F_1(z) + b F_2(z)$$

***b) Right-Shifting Property :***

Let m be a positive integer and let $f$ (k) be a sequence which is zero for (k < 0 ) . Further, let $F$ (z) be the Z-transform of $f$ (k) , then

$$Z\{ f(k-m) \} = z^{-m} F(z) \quad ,$$
$$k = 0,1,2,\ldots$$

Proof :

From the definition of the Z-transform :

$$Z\{f(k-m)\} = \sum_{k=0}^{\infty} f(k-m)z^{-k}$$

$= f(\text{-m}) + f(1\text{-m})z^{-1} + \ldots + f(0)\, z^{-m} + f(1)\, z^{-(m+1)} + \ldots$

$= z^{-m}\,[f(0) + f(1)\, z^{-1} + f(2)\, z^{-2} + \ldots\, ],$

$(f(k) = 0 \; for \; k < 0)$

$= z^{-m}\, F(z).$

***c) Left-Shifting Property :***

Let m be a positive integer and let $f$ (k) be a sequence which is zero for (k < 0 ). Further, let $F$ (z) be the Z-transform of $f$(k) , then

$$Z\{f(k+m)\} = z^m F(z) - \sum_{i=0}^{m-1} f(i) z^{m-i}$$

, k = 0,1,2,...

Proof :

From the definition of the Z-transform :

$Z\{f(k+m)\} =$

$\sum_{k=0}^{\infty} f(k+m)z^{-k} = f(m) + f(m+1)z^{-1} + f(m+2)z^{-2} + \cdots$

By adding and subtracting terms, we obtain :

$Z\{f(k+m)\} = z^m[f(0) + f(1)z^{-1} + \cdots +$
$f(m)z^{-m} + f(m+1)z^{-(m+1)} + \cdots$
$- f(0) - f(1)z^{-1} - \cdots - f(m-1)z^{-(m-1)}]$

or

$$Z\{f(k+m)\} = z^m F(z) - \sum_{i=0}^{m-1} f(i) z^{m-i}$$

**The following table lists the notable properties enjoyed by the Z-transform .**

| | *Property* | *Discrete Sequence* | *Z-Transform* |
|---|---|---|---|
| 1 | Linearity | $af(k) + bg(k)$ | $aF\,(z) + bG\,(z)$ |
| 2 | Right-Shifting | $f(k-m)$ | $z^{-m}F(z)$ |
| 3 | Convolution | $\sum_{i=0}^{k} f_1(k-i) f_2(i)$ | $F_1(z)F_2(z)$ |
| 4 | Periodic-Sequence | $f(k) = f(k+N)$ | $F(z) = \frac{z^N}{z^N - 1}\sum_{k=0}^{N-1} f(k)z^{-k}$ |
| 5 | Left-Shifting | $f(k+m)$ | $z^m F(z) - \sum_{i=0}^{m-1} f(i) z^{m-i}$ |

The Z-transform opens up new ways for solving the problems. It is well known that Z-transform is used successfully in many engineering problems. Some applications of Z-transform are [8] :

1. Solution of the linear difference equation.
2. Digital filter design.
3. Transfer function.

## 4. Proposed Method for Linear Equivalence Determination :

Periodic sequence property of the Z-transform is used to determine the linear equivalence of the sequence which is used as the key in stream cipher system.

A sequence of numbers which repeats itself every (N) discrete-time units is said to be periodic with period N . As such, these sequences satisfy the property:

$$f(k) = f(k+N) \quad \ldots(2)$$

for all nonnegative $k$ .

The Z-transform of the first period of the periodic sequence characterized by relationship (2) is :

$$F_1(z) = \sum_{k=0}^{N-1} f(k) z^{-k} \quad \ldots(3)$$

Since this first period is repeated every N discrete time units, it follows by the right shifting property that the Z-transform of the periodic sequence is given by :

$F(z) = F_1(z) + z^{-N} F_1(z) + z^{-2N} F_1(z) + z^{-3N} F_1(z) + \ldots$
$= F_1(z)\, [\, 1 + z^{-N} + z^{-2N} + z^{-3N} + \ldots]$

where $z^{-mN} F_1$ (z) designates the Z-transform of the *m*th period of the periodic sequence. The infinite sum within brackets is readily shown to be given by :

$$\sum_{m=0}^{\infty} z^{-mN} = \sum_{m=0}^{\infty} (z^{-N})^{m}$$

$$= \frac{z^{N}}{z^{N}-1} \quad \text{for } |z|>1$$

Hence, the Z-transform of the periodic sequence becomes ,

$$F(z) = \frac{z^{N}}{z^{N}-1} F_1(z) \quad \text{for } |z|>1$$

The following algorithm summarizes the steps for finding the linear equivalence (L) of the periodic sequences in stream cipher system .

## PSPZT Algorithm

**Step 1:**
Input the sequence $f$(k) of period (N) , where k = 0,1,2,…,N-1 .

**Step 2:**

Compute $F_1(z) = \sum_{k=0}^{N-1} f(k) z^{-k}$

**Step 3:**
Evaluate $p_1(z)$ and $p_2(z)$ as :
$p_1(z) = z^N F_1(z)$
$p_2(z) = z^N - 1$

**Step 4:**
According to the arithmetic operations over Galois field of order (q) (GF(q)) where (q ) is a prime number (q>1) put :

$$P_2(z) = (z^N - 1) \bmod q = z^N \oplus_q (-1)$$

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

**Step 5:**
Find the greatest common divisor of the two polynomials $p_2(z)$ and $p_1(z)$ ($\gcd(p_2(z), p_1(z))$)over GF(q) as follows:

A) Input the two polynomials $p_1(z)$ and $p_2(z)$ where the degree of $p_2(z)$ is greater than or equal to $p_1(z)$ .

b) According to the arithmetic operations over GF(q), compute r where r is the remainder from dividing $p_2(z)$ by $p_1(z)$ by using modulo (q) in addition.

c) If r =0 then :

1)
$$\gcd(p_2(z), p_1(z)) = p_1(z)$$

```
2) go to (step d)
     else
   set : $p_2(z) = p_1(z)$
         $p_1(z) = r$
   and go to (step b).
d)End.
```

**Step 6:**
Compute P(z), C(z) and F(z) as follows:-

$$P(z) = \frac{p_1(z)}{\gcd(p_2(z), p_1(z))} \quad ,$$

$$C(z) = \frac{p_2(z)}{\gcd(p_2(z), p_1(z))}$$

and $$F(z) = \frac{P(z)}{C(z)} \ .$$

where $\gcd(p_2(z), p_1(z))$ is the greatest common divisor of the two polynomials $p_2(z)$ and $p_1(z)$.

**Step 7:**
Evaluate the linear equivalence (L) of the key sequence by :

$$L = \deg(C(z)) \ ,$$

where $\deg(C(z))$ is the degree of the characteristic polynomial $C(z)$.

## 5. Illustrative Examples :

***Example (1) :***

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

$f(k)$ = 0010111 , where $k$ = 0,1,…,6 and the period N=7 .

In this example the Z-transform is proposed to determine the linear equivalence of the sequence $f(k)$ from the degree of the characteristic polynomial $C$(z).

Hence, by applying the algorithm (PSPZT) we get :

$$p_1(z) = z^7 \sum_{k=0}^{6} f(k) z^{-k} = z^5 + z^3 + z^2 + z$$

$$p_2(z) = z^7 - 1 = (z^7 - 1) \bmod 2 = z^7 \oplus_2 (-1) = z^7 + 1$$

…(4)

According to the (step 5) in (PSPZT) algorithm the $\gcd(p_2(z), p_1(z))$ is computed by using modulo (2) in arithmetic operations as follows :

$$p_2(z) = z^7 + 1$$
$$p_1(z) = z^5 + z^3 + z^2 + z \quad \rightarrow \quad r = z^4 + z^2 + z + 1$$

$$p_2(z) = z^5 + z^3 + z^2 + z$$
$$p_1(z) = z^4 + z^2 + z + 1 \quad \rightarrow \quad r = 0$$

$$\therefore \gcd(p_2(z), p_1(z)) = z^4 + z^2 + z + 1 \ldots(5)$$

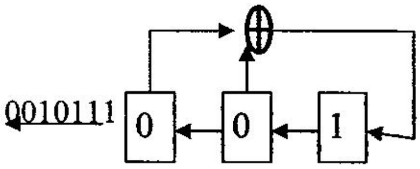
and from eq.(4) and eq.(5)

$$F(z) = \frac{z}{z^3 + z + 1} = \frac{P(z)}{C(z)} \quad .$$

Then, the linear equivalence (L) of the key sequence $f(k)$ is :-

$$L = \deg(C(z)) = 3 \quad .$$

This can be verified directly by generating the minimal characteristic polynomial $C$(z) of 3-stage LFSR using the first three consecutive bits (i.e. the initial state 001 ) from the sequence $f(k)$ as it is illustrated in the following figure:



***Example (2) :***

Consider the following sequence over GF(5) :-

$f(k)$ = 2,1,4,3,1,0,0,1,2,4,1,1 $k$= 0,1,…,11 with period 12 .

The Z-transform is used to compute the linear equivalence of the sequence $f(k)$ by applying the algorithm (PSPZT) as follows:

$$p_1(z) = z^{12} \sum_{k=0}^{11} f(k) z^{-k} = 2z^{12} + z^{11} + 4z^{10} +$$
$$3z^9 + z^8 + z^5 + 2z^4 + 4z^3 + z^2 + z$$

$$p_2(z) = z^{12} - 1 =$$
$$(z^{12} - 1) \bmod 5 = z^{12} \oplus_5 (-1) = z^{12} + 4$$

$$\gcd(p_2(z), p_1(z)) = z^8 + z^7 - 3z^6 + 3z^5 +$$
$$3z^4 + 4z^3 + 2z^2 + 2z + 1$$

And $F(z) = \dfrac{3z^4 + z^3 + z^2 + 4z}{4z^4 + z^3 + 2z^2 + 3z + 1}$

$$= \frac{2z^4 + 4z^3 + 4z^2 + z}{z^4 + 4z^3 + 3z^2 + 2z + 4} = \frac{P(z)}{C(z)} \quad .$$

Then, the linear equivalence (L) of the sequence $f(k)$ is :-

$$L = \deg(C(z)) = 4 \quad .$$

This can be verified directly by generating the sequence $f(k)$ from the minimal characteristic polynomial $C$(z) using the first four consecutive bits (i.e. the initial state 2,1,4,3) from the sequence $f(k)$ .

In this example, the Z-transform determined the linear equivalence of the non-binary sequences also.

## 6. Conclusion :

The decryption of the cryptogram in stream cipher system depends on knowing the key sequence of it. Hence, the key sequence must have high linear equivalence to have high complexity in order to be difficult for the interceptor to obtain the whole sequence and knowing the plaintext. In this work the Z-transform was successfully employed to compute the linear equivalence of the key sequences that determines the ability of security of these sequences. The results of the proposed method are accurate to determine the linear equivalence for any real or binary sequence with any period. Moreover, the proposed method is computed easily in digital computer.

## 7. References :

1. Baker , H.J. and Piper, F.C. 1982. Cipher Systems: The Protection of Communications, Northwood Publications ,London.
2. Song Yan. 2001. Number Theory for Computing, Printed in Germany, Springer-Verlag.
3. Wikd P. 2002. Linear Feedback Shift Registers , www.sss-mag.com/ pdf/ lfsr.pdf .
4. Baker, J.M. and Hughs, P.M. 1989., Communications Speech and Vision , Jr., Proc.I , IPIDDG 136.
5. Massey , J.L. 1986. Shift Register Synthesis and BCH Decoding , IEEE Trans. ,on Information Theory ,Vol.IT-15, No.3 .
6. James A. Cadzow 1973. Discrete-Time Systems , Englewood Cliffs, N. J. , Prentice Hall, Inc.
7. Ogata, Katsuhiko 1997. Modern Control Engineering , Third Edition, Printed in the New Jersey .
8. Cruz, R.L. 1996. Introduction to The Z-Transform , www.spd.eee.strath .ac.uk/~interact/ztransform/page3.html-2k.

# تحديد المكافئ الخطي لمتتابعة الانسياب الرئيسي باستخدام تحويل Z

عمر محمد الفاعور* شيماء حسين صالح ** شازاد شوقي احمد محمد***

* دكتوراه، الجامعة التكنولوجية
** الجامعة التكنولوجية
*** جامعة السليمانية

## الخلاصة

يقدم هذا البحث طريقة مقترحة لحساب و تحديد المكافئ الخطي لمتتابعة الانسياب الرئيسي (متتابعة المفتاح) في أنظمة التشفير الانسيابي عن طريق استخدام إحدى خواص تحويل Z وهي خاصية المتتابعة الدورية حيث ممكن حساب المكافئ الخطي لأي متتابعة دورية يتم إنتاجها من مولدات مفاتيح خطية وغير خطية و قد تم الحصول على نتائج دقيقة.