COMPLEXITY

Determination of complexity of pseudo-random sequence based on Z-transform

SATTAR BADER SADKHAN (*),
RAGHAD KADHIM SALIH (**)

SUMMARY. – *In recent years, stream cipher systems have played a big role especially in computer networks. Stream cipher systems depend on pseudo-random (PR) binary key sequences which are mixed with the plaintexts using addition with modulo two to produce the ciphertexts. The PR key sequences are characterized by three properties which define the measure of security for these sequences. These properties are period, complexity and randomness. There are several methods to determine the degree of complexity of these PR sequences like Berlekamp-Massey method, matrices techniques, and using software computing techniques (Neural Networks, Fuzzy Logic and Genetic Algorithms). This paper presents a proposed method to determine the degree of complexity of these PR sequences using one of the properties of the Z-transform which is periodic sequence property. This proposed method enable us to compute the degree of complexity of any periodic sequence produced from linear or nonlinear generators and accurate results are obtained. The steps of the proposed procedure are given, two different examples are illustrated, one of them for a PR sequence over GF(2), and the second example for PR sequence over GF(5).*

Key words: Stream cipher, Pseudo random sequence, complexity evaluation, Z-transform.

1. Introduction

Cryptography and information security are considered as one of important sciences in the world, especially after using the wide spread use of computers in many world wide applications. 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, while the resulted information is called ciphertext (1).

(*) University of Babylon, IRAQ; e-mail: drengsattar@ieee.org
(**) Department of Applied Sciences, University of Technology, Babylon, IRAQ

One of the well known cipher systems is the stream cipher system. Stream cipher system is very important system for the information security. In stream cipher system the pseudo random (PR) sequence (i.e. the key) is combined or mixed with the plaintext using modulo 2 addition to produce the ciphertext. It is absolutely crucial that if the key of the cipher system is known, one can determine the plaintext from the ciphertext. Hence the key or the PR sequence must have long period, high complexity and randomness properties to have acceptable security. The complexity of the PR sequence is the length of the minimum linear feedback shift register (LFSR) that can generate the sequence. The LFSR of length n can be characterized 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 $c_0, c_1, \ldots, c_{n-1}$ are 0 or 1. The PR sequence must have high complexity since for a sequence with a known complexity L, we need 2L consecutive bits to deduce the entire sequence, since if 2L consecutive bits are given, one can write a system of L-equations in L unknown variables and find its unique solution (1,2).

James L. Massey (3) suggested an algorithm which is known as Berlekamp-Massey algorithm for computing the complexity of the PR sequences and J.M. Baker and P. Hughes gave a new explanation of the Berlekamp-Massey algorithm using a method based on matrices (2).

The aim of this paper is to provide a proposed method for complexity evaluation of the Pseudo-Random Sequence using the Z-transform. The steps of the proposed procedure are given, two different examples are illustrated one of them for a PR sequence over GF(2), and the second example for PR sequence over GF(5).

2. The Z-transform

The Z-transform is an important tool for analyzing linear discrete time system. It is used to transfer sequences of numbers into algebraic equations of the variable z which, in many cases, helps the solution of problems (4).

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

$$Z\{f(k)\} = F(z) = \sum_{k=0}^{\infty} f(k) z^{-k} \qquad [1]$$

where z is an arbitrary complex number (4,5).

The Z-transform possesses many notable properties. Table 1 lists the salient properties enjoyed by the Z-transform.

Table 1
Properties of 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	Periodic-Sequence	$f(k)=f(k+N)$	$F(z)=\frac{z^N}{z^N-1}F_1(z)$
4	Convolution	$\sum_{i=0}^{k} f_1(k-i)f_2(i)$	$F_1(z)F_2(z)$
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 of solving the problems. It is well known that Z-transform is used successfully in many engineering problems. Some applications of Z-transform are (5):

1. Solution of the linear difference equation.
2. Transfer function.
3. Digital Filter Design.
4. Frequency Response.

3. Proposed method for complexity evaluation

Periodic sequence property of the Z-transform is used to determine the complexity of the PR sequence (which is used as the key sequence in stream cipher system).

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

[2] $$f(k) = f(k+N)$$

for all nonnegative k.

The Z-transform of the first period of the periodic sequence characterized by relationship [2] is

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

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:

$$F(z) = F_1(z) + z^{-N}F_1(z) + z^{-2N}F_1(z) + z^{-3N}F_1(z) + \ldots$$
$$= F_1(z)\left(1 + z^{-N} + z^{-2N} + z^{-3N} + \ldots\right)$$

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:

$$\sum_{m=0}^{\infty} z^{-mN} = \sum_{m=0}^{\infty}\left(z^{-N}\right)^m = \frac{z^N}{z^N - 1} \quad \text{for } |z| > 1$$

Hence, the Z-transform of the periodic sequence becomes

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

This property enables us to find the complexity L of the periodic PR sequences in stream cipher system as follows (6):

1. Evaluate $p_1(z)$ and $p_2(z)$ where:

$$p_1(z) = z^N F_1(z)$$

$$p_2(z) = z^N - 1.$$

2. Compute $P(z)$, $Q(z)$ and $F(z)$ as follows:

$$P(z) = \frac{p_1(z)}{gcd\left[p_2(z), p_1(z)\right]}$$

$$Q(z) = \frac{p_2(z)}{gcd\left[p_2(z), p_1(z)\right]}$$

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

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

3. Evaluate the complexity L of the PR sequence by:

$$L = deq\,[Q(z)],$$

where $deq\,[Q(z)]$ is the degree of the characteristic polynomial $Q(z)$.

Example 1

Consider the following Pseudo Random sequence S_i over GF(2):

$$S_i = 0010111,$$

where $i = 0, 1, \ldots, 6$ and the period $N = 7$.

In this example the Z-transform is proposed to determine the complexity of the sequence S_i from the degree of the characteristic polynomial $Q(z)$.

Hence, by taking the Z-transform to S_i we get:

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

$$p_2(z) = z^7 - 1$$

$$gcd\left[p_2(z), p_1(z)\right] = z^4 + z^2 + z + 1$$

and

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

Then, the complexity L of the PR sequence S_i is:

$$L = deq\left[Q(z)\right] = 3.$$

Example 2:

Consider the following sequence S_i over GF (5):

$$S_i = 2,1,4,3,1,0,0,1,2,4,1,1$$

$i = 0,1, \ldots,11$, with period 12.

The Z-transform is used to compute the complexity of the sequence S_i as given in Appendix 1. Also the Z-transform $F(z)$ is given in Appendix 1.

Then, the complexity L of the PR sequence S_i is:

$$L = deq\left[Q(z)\right] = 4$$

4. Conclusions

Deciphering of the ciphertext in stream 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 complexity in order to be difficult for the cryptanalyst to obtain the entire sequence when only small segment of it is known. There are several methods for computing the complexity of the PR sequences as Berlekamp-Massey method. The Z-transform was used properly to compute the complexity of the PR key sequences that determines the ability of security of these sequences. The results of the Z-transform are accurate to determine the complex-

ity for any real or binary PR sequence with any period. Moreover, the proposed method is computed easily in digital computer.

Appendix 1

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

$$p_2(z) = z^{12} - 1 = z^{12} + 4$$

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

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

REFERENCES

(1) Baker H.J., Piper F.C., *Cipher Systems: The Protection of Communications* (Northwood Publications, London 1982).

(2) Baker J.M., Hughs P.M., *Communications Speech and Vision*, J. Proc. I, IPIDDG 136, 1989.

(3) Massey J.L., *Shift Register Synthesis and BCH Decoding*, IEEE Trans. on Information Theory, **IT-15** (1), January 1969.

(4) Cadzow J.A., *Discrete-Time Systems*, (Englewood Cliffs, N.J., Prentice Hall, Inc., 1973).

(5) Ogata K., *Modern Control Engineering*, 3th Ed., (Printed in New Jersey, 1997).

(6) R.K. Salih, *Analysis of Pseudo Noise Generator Design for Communication Systems using State Space Method*, M.Sc. thesis, Univ. of Technology, Baghdad, June 2004.