Generating a Strong Key for a Stream Cipher Systems Based on Permutation Networks

Kadhem M. Hashem *

Date of acceptance 21/4/2007

Abstract:

The choice of binary Pseudonoise (PN) sequences with specific properties, having long period high complexity, randomness, minimum cross and auto- correlation which are essential for some communication systems.

In this research a nonlinear PN generator is introduced . It consists of a combination of basic components like Linear Feedback Shift Register (LFSR), β-element which is a type of RxR crossbar switches.

The period and complexity of a sequence which are generated by the proposed generator are computed and the randomness properties of these sequences are measured by well-known randomness tests.

Introduction:

A necessary condition for a sequence to be suitable for use as enciphering sequence in a stream cipher system is that it should " appear to be " random. The aim of this requirement is two-folded, firstly, to ensure that any statistical properties of the plain text are not reflected in the cipher text, secondary, to prevent a cryptanalyst who know a section of the enciphering sequences from successfully predicting subsequent bits of it [1] . One of the most important methods for generating (PN) sequences is the Linear Feedback Shift Register (LFSR). Figure -1 shows a general model for LFSR. It is known that some tapping can produce binary sequence with a period of $(2^n -1)$ bits and a two- valued auto-correlation with high value of "Index of Discrimination is defined as the difference between the in-phase value and the maximum of te out – phase value for the auto- correlation function .

The major problem with the linear sequence is the low complexity of 2n bits, which means that 2n consecutive bits determine the rest of the sequence.

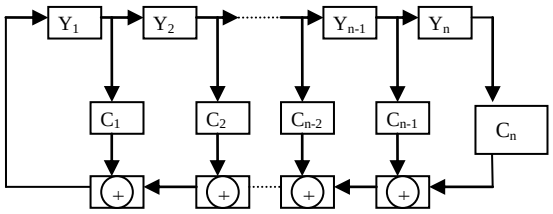

Fig .1 General diagram of a linear feedback shift register

Nonlinear generator:

2.1 General description:

Figure -2 shows a general diagram of our proposed nonlinear generator

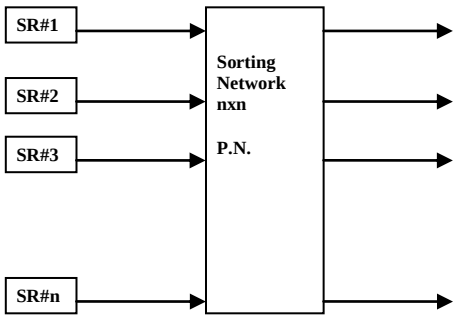

Figure -2: General diagram of nonlinear generator

* Department of Mathematics, College of Education University of AL-Qadisia

The sorting network is constructed from n consecutive β-element, which is a type of RxR crossbar switches. Each β-element accept (I_o,I_1) as input and produce (O_o,O_1) as output . In addition, β-element contains control line to determine the type of relation between the input and output, this line is denoted by C. β-element produces all possible permutations according to the value of C as follows:

If C=0 then, the output permutation is (0) (1)

If C=1 then, the output permutation is (0,1).

There exist many states to β – element:

1. T-state or straight state occurs when C=0, in this state the output is equal to the input at the same positions.

2. X-state occurs when C=1, this state exchange the positions of input to produce output.

3. Unspecified state occurs when C takes an unspecific value (c=d).

The following equations describe the relation between input and output.

$$O_0=\overline{C}\,I_0+CI_1 \quad \ldots\ldots\ldots 1$$

$$O_1= CI_0+\overline{C}\,I_1 \quad \ldots\ldots\ldots 2$$

The above equations may be rewritten using connectivity matrix as follows:

$$\begin{bmatrix} O_0 \\ O1 \end{bmatrix} = \begin{bmatrix} \overline{C} & C \\ C & \overline{C} \end{bmatrix} \begin{bmatrix} I_0 \\ I_1 \end{bmatrix}$$

2.2 Sorting network :

This network is a type of permutation networks, the basic component of that network is β-element . It is possible to merge two sorting networks with n and m inputs to get sorting network of (m+n) inputs. There are many algorithms to achieve the merge operation , Batche algorithm [3] , it seems to be ideal .

The delay time which be used to merge two sorting networks can be computed by the following equations:

T(m, 0)=T(0 , n)=0 ……..3

T(1, 1)=1 ……4

T(n , m)=1 + log (max (n, m)) for n, m>1 …5

The number of β-element which are needed to merge can be computed by the following recurrence relation:

$$C\ (m,\ n) = \begin{cases} mn & if\ \ mn < 1 \\ 2C(m/2, nl2) + \lfloor (m+n-1)l2 \rfloor & if\ \ mn > 1 \end{cases}$$

2.3 CHARACTERISTICS OF NONLINEAR GENERATOR:

Consider one stage of our proposed generator as shown in figure -3.

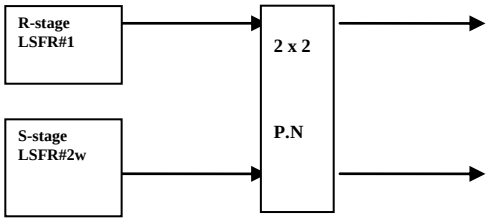

Figure 3:One stage of nonlinear generator

The important properties of the output sequence are analyzed as follows:

A- Period: Formally an infinite sequence $\{a_n\}$ is called periodic, if there exists an integer p≠0 such that $a_{t+p} = a_t$ for all t. If such an integer exists then $\{a_n\}$ is equal to $a_0\ a_1\ a_2 \ldots\ldots\ldots a_{p-1} a_0\ a_1 \ldots\ldots a_{p-1}\ a_0 \ldots\ldots$

The smallest value for p is called the period of the sequence and in this case, we say that $\{a_n\}$ is generated by $a_0\ a_1 \ldots\ldots a_{r-1}$ [4,5].

Theorem: If LFSR#1 has maximum period p_1,$p_1=2^r-1$ and LFSR#2 has maximum period p_2, $p_2=2^s-1$, and the greatest common divisor (gcd) between p1,p2 equal to 1 {$gcd(p_1,p_2)=1$} then the output sequence has a period equal $2p_1p_2$

Proof:let p be a period of a proposed generator, $p\neq1$,then the output of generator must be repeated after p_1p_2 of moves , and in each move the generator produces two bits . Therefore, there are $2p_1p_2$ bits generated by our generator because gcd $(p_1,p_2)=1$, and both p1,p2 divide p so that p is $2p_1p_2$

B-Randomness: The desired randomness properties are summarized as follows [4]:

❖postulate 1: Equal probabilities of 1's and 0's in the sequence.

❖postulate 2: Equal probabilities of each run of 1-bit in the sequence.

❖postulate 3: The auto correlation function should be with maximum index of discrimination .

For the linear maximal length sequence all above postulates are satisfied. However,
for the sequence generated our proposed generator, all above postulates are satisfied, and the sequence passes well-known randomness tests [4,5].

C-Complexity: The complexity of a periodic sequence is defined as the length of its linear equivalent, which is minimum number of consecutive bits which are required to predict the sub sequence of the sequence. There are several ways to determine the linear equivalent of any given binary sequence. The algorithm given by Massey [6] seems to be ideal.

In this study, many sequences are generated by our proposed generator by using linear feedback shift registers with maximum period and with different initial states. When we apply the Massey algorithm on these sequences we get complexity (length of linear equivalent) equal to p_1p_2 where p_1,p_2 are the period of first, and second register respectively, note that. The above study focuses on one stage of proposed generator, we generalized that study by using multiple LFSR s with different lengths, initial values and feedback functions, we get the same properties. For example when n=4 the design of our proposed generator is shown in figure 4 .
The complexity to whole generator is:

P1*P2……Pn where Pi : The period or LFSR# i

The generator will produce n-bits at each cycle (n is the number of LFSR which are used in design) so that this generator is faster than other generators , and the error is easy to detected.

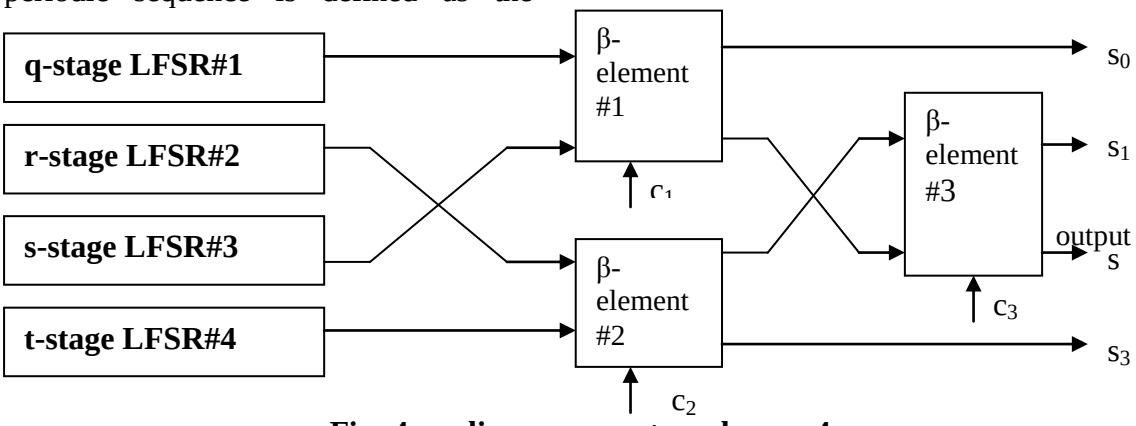

Fig -4 nonlinear generator when n=4

Analysis of Results:

In this study binary sequences generated by the proposed generator with different number of linear feed back shift are registers with different lengths and different initial states. These sequences are satisfy all the previous characteristics and pass well known randomness tests.

These sequences can be used as a strong key in a stream cipher systems to ensure the information security provided in such systems.

The design of our generator can be implemented by using simple and standard components, also, it is easy to simulate on the computer.

The permutation networks which produce all possible permutations give more complexity to the sequences that generated by random number generators.

References:

1. Carter , G. , 1989 . Statistical tests for randomness Racal comsec Itd . England

2. Edward , J. , 1971 . Generation of Binary sequences with Controllable complexity . IEEE . Translation on Information Theory .

3. Henery Baker , P. , 1982 . Cipher system the protection of communication . Northwood.

4. Hopcroft , J. , 2001 . Introduction to Automata Theory language and computation . Addison Wesley.

5. Stelling , W. , 2003 . cryptography and Network security . Principle and Practice . 3rd edition . Person Education International . IMC.USA.

6.الداودي . بيمان مجيد ، 2002 . سلاسل ماركوف التبولوجية .رسالة ماجستير. كلية التربية جامعة تكريت.

7.الدوري طه حميد ، 1998 . حول الديناميكا الرمزية ، رسالة ماجستير ، كلية التربية الجامعة المستنصرية.

توليد مفتاح قوي لأنظمة التشفير الانسيابي يعتمد على شبكات التبديل

كاظم مهدي هاشم*

* قسم الرياضيات /كلية التربية /جامعة القادسية

الخلاصة:

إن اختيار سلسلة الأرقام العشوائية ذات الخصائص الخاصة بالعشوائية ضرورية لبعض أنظمة الاتصالات.

في هذا البحث تم اقتراح مولد للأرقام العشوائية يتكون من مكونات أساسية بسيطة (مسجل الإزاحة الخطي وعنصر بيتا) وباستخدام هذا المولد تم توليد عدة سلاسل من الأرقام الثنائية وتم اختبارها باستخدام الاختبارات القياسية المعروفة.