Estimation of the Frequency Postulate for non-Linear Sequences Generated from Complement Product and Shrinking Generators

Asst. Lecturer Zainab Sadiq

Dept. of Mathematics
College of Science
Al-Mustansiriya University

Abstract

The Randomness is one of the basic criterions to measure stream cipher Efficiency. The stream cipher generator depends basically on Linear FeedBack Shift Register which is considered as one of the basic units of Stream Cipher Systems. In this paper, the frequency postulate of Randomness criteria is calculated theoretically for non-linear stream cipher systems before it be implemented or constructed (software or hardware), this procedure save time and costs. Two non-linear stream cipher generators are chosen to apply the theoretical studies; these key generators are the Complement Product and Shrinking Generators. The theoretical proofs of frequency estimation for the two key generators are introduced.

1. Introduction

Shift register sequences are used in both cryptography and coding theory. There is a wealth of theory about them; stream ciphers based on shift registers have been the workhorse of military cryptography since the beginnings of electronics. A feedback shift register is made up of two parts: a shift register and a feedback function. The shift register is a sequence of bits. (The length of a shift register is figured in bits). Each time a bit is needed, all of the bits in the shift register are shifted 1 bit to the right [1].

In 1967 [2] Golomb deduced three theorems about the maximal sequence generated from LFSR. One of the three Golomb's theorems deduced from the frequency postulate.

In 2009 [3] Al-Shammari, A. G., through his Ph. D. thesis, introduces four basic criterions which are: Periodicity, Linear Complexity, Randomness and Correlation Immunity used as basic criterions to measure Key Generator Efficiency. He can calculated these basic criterions theoretically for any key generator before it be implemented or constructed (software or hardware). This work introduces the mathematical proof of the good efficiency of the linear keygenerator deterministically.

In this paper, some studies are applied on the SCG sequences to determine the sequence frequency. The Basic efficiency for SCG can be defined as the ability of SCG and its sequence to withstand the mathematical analytic which the cryptanalyst applied on them, this ability measured by some basic criterions, the most important of is the randomness; one of the randomness postulates is the frequency postulate.

In the next part of this paper, the frequency postulate of randomness criterion will be discussed and introduce the basic conditions to obtain efficient SCG especially those related to frequency. It's important to mention that the zero input sequences must be avoided, this done when the non-all zeros initial values for LFSR's are chosen.

Let SCG consist of n-LFSR's have lengths $r_1,r_2,..,r_n$ respectively with $CF=F_n(x_1,x_2,\ldots,x_n)$, s.t. $x_i\in\{0,1\}$ $1\le i\le n$, represents the output of $LFSR_i$, let $S=\{s_0,s_1,\ldots\}$ be the sequence product from SCG and s_j, $j=0,1,\ldots$ represents elements of S. let S_i be the sequence i product from $LFSR_i$ with a_{ij} elements $1\le i\le n$, $j=0,1,\ldots,$.

2. Conditions of the Theoretical Estimation

There are some conditions must be hold to guarantee that the SCG has good statistical properties. The combined LFSR's must have maximum periods and the periods of LFSR's must be relatively prime with each others.

Definition (1) [3]: Let $GCD_2=gcd(\prod_{i=1}^{1} m_i, m_2.GCD_1)=gcd(m_1,m_2)$, for convenient let $GCD_1=1$ and so on the general form of the recursion equation will be:

$$GCD_n=gcd(\prod_{i=1}^{n-1} m_i, m_n.GCD_{n-1}) \quad \ldots(1)$$

where $n\geq 2$ s.t mi are positive integers, $\forall 1\leq i\leq n$.

Theorem (1) [3]:

Let $m_i \in Z+$, $\forall 1\leq i\leq n$ then:

$$lcm(m_1,m_2,\ldots,m_n)=\frac{\prod_{i=1}^{n} m_i}{GCD_n(m_i)} \quad \ldots(2)$$

where $GCD_n(m_i)$ defined in (1).

Let the sequence S has period P(S), the period of $LFSR_i$ denotes by $P(S_i)$, P(S) and $P(S_i)$ are least possible positive integers, so

$$P(S)=lcm(P(S_1),P(S_2),\ldots,P(S_n)) \quad \ldots(3)$$

$$P(S)=\frac{\prod_{i=1}^{n} P(S_i)}{GCD_n(P(S_i))} \quad \ldots(4)$$

s.t. $GCD_n(P(S_i))=\gcd\left[\prod_{i=1}^{n-1} P(S_i), P(S_n)\cdot GCD_{n-1}(P(S_i))\right]$ [3]

If $P(S_i)$ are relatively prime with each other this mean $GCD_n(P(S_i))=1$ this implies:

$$P(S)=\prod_{i=1}^{n} P(S_i) \quad \ldots(5)$$

It's known earlier that $P(S_i)\leq 2^{r_i}-1$, and if the $LFSR_i$ has maximum period then $P(S_i)= 2^{r_i}-1$ [4].

Theorem (2) [3]

P(S)=$\prod_{i=1}^{n}(2^{r_i}-1)$ if and only if the following conditions are holds:

1. **$GCD_n(P(S_i))=1$,.**
2. **the period of each LFSR has maximum period ($P(S_i)=2^{r_i}-1$).**

3. Randomness

The sequence that is satisfied the three randomness properties called Pseudo Random Sequence (PRS) [2]. The randomness criterion depends on LFSR's and CF units, therefore from the important conditions to get PRS is, the sequence must be maximal and CF must be balance [4].

To guarantee the SCG to produces PRS, the sequence must pass randomness tests with complete period, these tests applied into two ways, on: [1]

1. **Global sequence for complete period and that is the right way (but it's hard to applied for high periods).**
2. **Local sequence for many times for various lengths less than the origin length.**

In this part, the 1st way will be applied theoretically for any period.

If $GCD_n(P(S_i))=1$ then,

$$P(S)=2^{\sum_{i=1}^{n}r_i}+(-1)\cdot(2^{r_1+\cdots+r_{n-1}}+\cdots+2^{r_2+\cdots+r_n}+\cdots+(-1)^{n-1}\cdot(2^{r_1}+\cdots+2^{r_n})+(-1)^n \quad \ldots(6)$$

Let R_m^t denotes the combination to sum m of numbers r_i from n of the numbers r_i, R_m denotes the set of all possibilities of R_m^t s.t.

$$R_m^t=\begin{pmatrix} r_1,r_2,\ldots,r_n \\ \sum_{j=1}^{m} r_{i_j} \end{pmatrix}$$ **$0\le m\le n$, $1\le i\le n$, $t\in\{1,2,\ldots,C_m^n\}$**

define $R_0=\{R_0^1\}$, $R_0^1=0$.

For instance let m=1 then $R_1=\{R_1^1,R_1^2,\ldots,R_1^{C_1^n}\}, R_1^1=r_1,\ldots,R_1^n=r_n$

If m=n then $R_n=\{R_n^1\}$, $R_n^1=\sum_{i=1}^{n} r_i$

So equation (6) can be written in compact formula:

$$P(S)=\sum_{k=0}^{n}(-1)^{k}\cdot\sum_{t=1}^{C_k^n}2^{R_{n-k}^t} \qquad \ldots(7)$$

4. Frequency Postulate

Golomb mentioned that in general , if the sequences S is periodic sequence of period n then in the cycle S^n of S, the number of 1′s differs from the number of 0′s by at most 1. This is which be called frequency postulate.

1st Golomb's theorem says that if LFSR with length r has maximal sequence then $N_r(0)=2^{r-1}-1$ and $N_r(1)=2^{r-1}$, where $N_r(a)$ denotes the number of bit "a" in the maximal sequence [2] s.t.:

$$P(r)=2^{r}-1=(2^{r-1}-1)+2^{r-1}=\sum_{a=0}^{1}N_r(a)$$

Let $N_S(a)$ be the frequency of bit "a" in S which generates from SCG then:

$$P(S)=\sum_{a=0}^{1}N_S(a)=N_{r_1}(0)\cdots N_{r_n}(0)+N_{r_1}(0)\cdots N_{r_n}(1)+\cdots+N_{r_1}(1)\cdots N_{r_n}(1) \qquad \ldots(8)$$

From this equation the act of CF will starts to distribute the ratio of "0" and "1" in S. If the terms of equation (8) rearranged s.t. $0=F(a_{i1},a_{i2},..,a_{in})$, $1\le i\le m_0$ for the 1st m_0 terms, and $1=F(a_{i1},a_{i2},..,a_{in})$, $1\le i\le m_1$ for 2nd m_1 terms $2^n=m_0+m_1$ then,

$$N_S(a)=\sum_{i=1}^{m_a}\prod_{j=1}^{n}N_{r_j}(a_{ij}) \qquad \ldots(9)$$

subject to $a=F(a_{i1},a_{i2},..,a_{in})$ s.t. $1\le i\le m_a$, a=0,1.

Where m_a denotes the number of states which are subject to the above condition [3].

In the next sections we will introduce new theorems, as Golomb do on LFSR, to show the frequency distribution for two famous SCG, these SCG are: complement Product and Shrinking SCG's.

5. Complement Product Generator (n-CPSCG)

The Product generator is defined by n-maximum-length LFSRs whose lengths $r_1, r_2,\ldots, r_n$, where $n\in Z^+$ are pair wise relatively prime, with AND combining function [5]:

$$F_n(x_1,x_2,..,x_n)=x_1\bullet x_2\bullet\ldots\bullet x_n=\prod_{i=1}^{n}x_i \qquad \ldots(10)$$

In this paper the complement product generator will be discussed. The generator takes the complement of the output of every LFSR. So, equation (10) can be written as follows:

$$F_n(x_1,x_2,..,x_n) = \prod_{i=1}^{n}(x_i \oplus 1) \quad \dots (11)$$

This generator considered weak, despite of his good linear complexity, because of his weak randomness (see Figure 1).

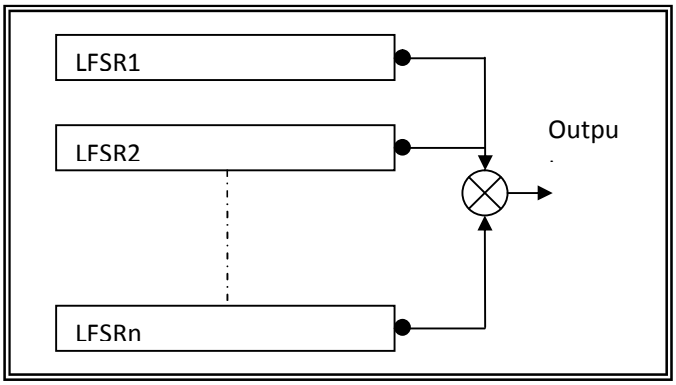

Figure 1 Complement Product CSG.

For n=3 the truth table of this generator will be shown in table (1).

table (1)The truth table of Complement Product CSG.

x_1	x_2	x_3	$x_1 \oplus 1$	$x_2 \oplus 1$	$x_3 \oplus 1$	F_n
0	0	0	1	1	1	1
0	0	1	1	1	0	0
0	1	0	1	0	1	0
0	1	1	1	0	0	0
1	0	0	0	1	1	0
1	0	1	0	1	0	0
1	1	0	0	0	1	0
1	1	1	0	0	0	0

The linear complexity (LC) of this generator is $LC(S_P) = \prod_{i=1}^{n}(r_i + 1)$

Where S_P is the sequence generate from n-CPSCG.

Assuming the degrees of the all combined primitive feedback polynomials are relatively primes.

The correlation probability CP(S_i) of the sequences S_i generated from of output of $LFSR_i$ which is combined in the n-CPSCG. It can be calculated by the following Lemma (1).

Lemma (1): for all inputs of the product function consists of n-LFSR's, the $CP=0.5+1/2^n$.

Proof:

Since the complement of the product function gives output zero's every where accept for the state when all inputs are zeros's the corresponding output is one, then for all zero's and all one's inputs are identical to the corresponding output of the product function, then the CP_1 is:

$$CP_1(S) = 2/2^n \quad \text{...(a)}$$

Where n is the number of combined LFSR's.

Half of the rest inputs is 2^n-2 are zero's, so they are identical to the corresponding output of the product function, then the CP_2 is:

$$CP_2 = \frac{\frac{2^n-2}{2}}{2^n} = \frac{2^{n-1}-1}{2^n} \quad \text{...(b)}$$

The final CP is the sum of the CP's in equations (a) and (b), then

$$CP = \frac{2}{2^n} + \frac{2^{n-1}-1}{2^n} = \frac{2^{n-1}+1}{2^n} = 0.5 + \frac{1}{2^n} \quad \text{...(12)}$$

Table (2) shows some values of correlation probability for n=2...8 depending on equation (11).

Table (2) some values of CP for n=2...8 using on equation (12).

n	2	3	4	5	6	7	8
CP	0.75	0.625	0.5625	0.53125	0.515625	0.5078125	0.507421875

In the next theorem the frequency of "1" ($N_S(1)$) in the generated sequence from n-CPSCG can be calculated.

Theorem (3): Let $N_S(a)$ be the number of a-bit in the sequence S generated from n-CPSCG, $a \in \{0,1\}$, then:

$$N_S(1) = 2^{\sum_{i=1}^{n} r_i - n} - (2^{r_1+r_2+\cdots+r_{n-1}-(n-1)} + \cdots + 2^{r_2+\cdots+r_n-(n-1)}) + \cdots + (-1)^{n-1}(2^{r_1-1} + \cdots + 2^{r_n-1}) + (-1)^n \quad \text{...(13)}$$

Proof:

Recall equations (8) and (9).

P(S)= $N_{r_1}(0).N_{r_2}(0)\cdots N_{r_n}(0)+\ldots+N_{r_1}(1).N_{r_2}(1)\cdots N_{r_n}(1)$

$N_S(1)$= $\prod_{i=1}^{n} N_{r_i}(0) = N_{r_1}(0).N_{r_2}(0)\cdots N_{r_n}(0) = (2^{r_1-1}-1)\cdot(2^{r_2-1}-1)\cdots(2^{r_n-1}-1)$

$N_S(1)$= $2^{\sum_{i=1}^{n} r_i - n} - (2^{r_1+r_2+\cdots+r_{n-1}-(n-1)}+\cdots+2^{r_2+\cdots+r_n-(n-1)})+\cdots+(-1)^{n-1}(2^{r_1-1}+\cdots+2^{r_n-1})+(-1)^n$

From the result of the above theorem:

$N_S(0)$=P(S)- $2^{\sum_{i=1}^{n} r_i - n} - (2^{r_1+r_2+\cdots+r_{n-1}-(n-1)}+\cdots+2^{r_2+\cdots+r_n-(n-1)})+\cdots+(-1)^{n-1}(2^{r_1-1}+\cdots+2^{r_n-1})+(-1)^n$ **…(14)**

$N_S(0)$= $(2^n-1)\cdot 2^{\sum_{i=1}^{n} r_i - n} - (2^{n-1}-1)\cdot(2^{r_1+r_2+\cdots+r_{n-1}-(n-1)}+\cdots+2^{r_2+\cdots+r_n-(n-1)})+\cdots+(-1)^{n-1}(2^{r_1-1}+\cdots+2^{r_n-1})$

Lemma (2): In the n-CPSCG, $\lim_{r_i\to\infty}(N_S(1)/P(S)) = \frac{1}{2^n}$**, 1≤i≤n.**

Proof:

$$\frac{N_S(1)}{P(S)} = \frac{\prod_{i=1}^{n}(2^{r_i-1}-1)}{\prod_{i=1}^{n}(2^{r_i}-1)}$$

As $r_i\to\infty$, then $2^{r_i}-1\to 2^{r_i}$ **and** $2^{r_i-1}-1\to 2^{r_i-1}$ **(ignore 1), then:**

$$\therefore \frac{N_S(1)}{P(S)} \approx \frac{2^{\sum_{i=1}^{n} r_i - n}}{2^{\sum_{i=1}^{n} r_i}} = \frac{1}{2^n}$$

Example (1):

Table (3) shows the proportion of $N_S(1)$ to P(S) for various n-cPSCG.

Table (3) the proportion of $N_S(1)$ to P(S) for various n-cPSCG.

n	r_i	$N_S(1)$	P(S)	Proportion	
				Expected	Observed
2	2,3 2,5 5,7 7,11	3 15 945 64449	21 93 3937 259969	0.25	0.143 0.161 0.240 0.248
3	2,3,5 3,4,5 4,5,7 4,5,11	45 315 6615 107415	651 3255 59055 951855	0.125	0.070 0.097 0.112 0.113
Mm	2,3,5,7 3,4,5,7	2835 19845	82766 413385	0.0625	0.034 0.048

6. Shrinking CSG (2-SHCSG)

The shrinking generator [6] uses a different form of clock control than the previous generators. It's a relatively new keystream generator, having been proposed in 1993. Nevertheless, due to its simplicity and provable properties, it is a promising candidate for high-speed encryption applications. In the shrinking generator, a control LFSR1 is used to select a portion of the output sequence of a second LFSR2. The keystream produced is, therefore, a shrunken version (also known as an irregularly decimated subsequence) of the output sequence of LFSR2 depicted in Figure (2).

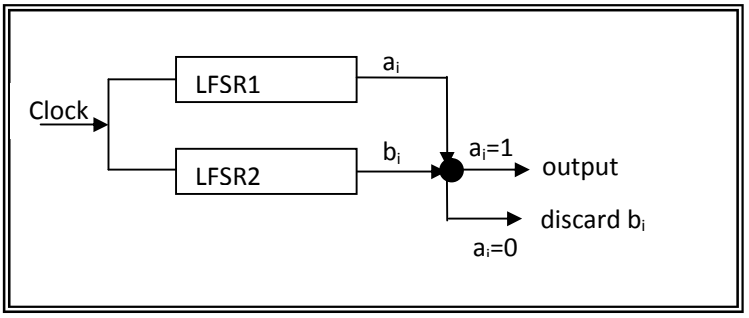

Figure (2) Shrinking CSG [6].

Shrinking Generator Algorithm is as follows:

A control LFSR1 is used to control the output of a second LFSR2.

The following steps are repeated until a keystream of desired length is produced.

1. Registers LFSR1 and LFSR2 are clocked.
2. If the output of LFSR1 is 1, the output bit of LFSR2 forms part of the keystream.
3. If the output of LFSR1 is 0, the output bit of LFSR2 is discarded.

More formally, let the output sequences of LFSR1 and LFSR2 be $a_0,a_1,a_2,...$ and $b_0,b_1,b_2,...$, respectively. Then the keystream produced by the shrinking generator is $x_0,x_1,x_2,...$, where $x_j=bi_j$, and, for each $j\geq 0$, i_j is the position of the j^{th} 1 in the sequence $a_0,a_1,a_2,....$

This idea is simple, reasonably efficient, and looks secure. If the feedback polynomials are sparse, the generator is vulnerable, but no other problems have been found. Even so, it's new. One implementation problem is that the output rate is not regular; if LFSR1 has a long string of zeros then the generator outputs nothing. The authors suggest buffering to solve this problem [6].Practical implementation of the shrinking generator is discussed in [7].

Example (2): (shrinking generator with artificially small parameters) Consider a shrinking generator with component LFSR1=<3,1+D+D^3> and LFSR2 =<5,1+D^3+D^5>.

Suppose that the initial states of LFSR1 and LFSR2 are [1,0,0] and [0,0,1,0,1], respectively. The output sequence of LFSR1 is the 7-periodic sequence with cycle

a^7 = 0, 0, 1, 1, 1, 0, 1,

While the output sequence of LFSR2 is the 31-periodic sequence with cycle

b^{31} = 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0.

The keystream generated is

S_{SH} = 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0,....

Fact (1): (properties of the shrinking generator) Let LFSR1 and LFSR2 be maximum-length LFSRs of lengths r_1 and r_2, respectively, and let S_{SH} be an output sequence of the shrinking generator formed by LFSR1 and LFSR2, If $gcd(r_1,r_2)=1$, then the period $P(S_{SH})$:

$P(S_{SH})= N_{r_1}(1).N_{r_2}(0) + N_{r_1}(1).N_{r_2}(1) = 2^{r_1-1}\cdot(2^{r_2-1}-1) + 2^{r_1-1}\cdot 2^{r_2-1} = 2^{r_1+r_2-1} - 2^{r_1-1}$ **...(15)**

Establishes that the output sequence of a shrinking generator satisfies the basic requirements of high period, high linear complexity, and good statistical properties.

In the next theorem the frequency of "1" ($N_S(1)$) in the generated sequence from 2-SHSCG can be calculated.

Theorem (4): Let $N_S(a)$, a=0,1 be the number of bit (a) in the sequence S_{SH} generated from 2-SHCSG, then:

$N_S(0)=$ $2^{r_1+r_2-2}-2^{r_1-1}$**, and,**

$N_S(1)=$ $2^{r_1+r_2-2}$

Proof:

Recall equations (8) and (9), and when n=2 for 2-SHSCG, only $N_{r_i}(1)$ **is active, then:**

$N_S(0)=$ $N_{r_1}(1).N_{r_2}(0)=2^{r_1-1}\cdot(2^{r_2-1}-1)=2^{r_1+r_2-2}-2^{r_1-1}$ **…(16)**

and,

$N_S(1)=$ $N_{r_1}(1).N_{r_2}(1)=2^{r_1-1}\cdot 2^{r_2-1}=2^{r_1+r_2-2}$ **…(17)**

Example (3):

Table (4) shows the values of $N_S(0)$ and $N_S(1)$ for different r_i of 2-SHSCG.

Table (4) the values of $N_S(0)$ and $N_S(1)$ for different r_i of 2-SHSCG.

Ex.	r_i		$P(S_i)$		$N_S(a)$		$P(S_{SH})$
	r_1	r_2	$P(S_1)$	$P(S_2)$	$N_S(0)$	$N_S(1)$	
1	2	3	3	7	2*3=6	2*4=8	14
2	3	4	7	15	4*7=28	4*8=32	60
3	3	5	7	31	4*15=60	4*16=64	124
4	4	5	15	31	8*15=120	8*16=128	248
5	3	7	7	127	4*63=252	4*64=256	508
6	5	7	31	127	16*63=1008	16*64=1024	2032

Lemma (3): In the 2-SHSCG, $N_S(a)/P(S)=0.5$, a=0,1, when r_i be as large as possible,1≤i≤2.

Proof:

$$\frac{N_S(0)}{P(S)}=\frac{2^{r_1+r_2-2}-2^{r_1-1}}{2^{r_1+r_2-1}-2^{r_1-1}}=\frac{2^{r_1-1}(2^{r_2-1}-1)}{2^{r_1-1}(2^{r_2}-1)}=\frac{2^{r_2-1}-1}{2^{r_2}-1}$$

As r_2 be as large as possible, then $2^{r_2}-1\rightarrow 2^{r_2}$ **(ignore 1), then:**

$$\therefore \frac{N_S(0)}{P(S)} = \frac{2^{r_2-1}}{2^{r_2}} = \frac{1}{2} = 0.5$$

$$\frac{N_S(1)}{P(S)} = \frac{2^{r_1+r_2-2}}{2^{r_1+r_2-1} - 2^{r_1-1}} = \frac{2^{r_1-1}(2^{r_2-1})}{2^{r_1-1}(2^{r_2}-1)} = \frac{2^{r_2-1}}{2^{r_2}-1}$$

As r_2 be as large as possible, then $2^{r_2}-1 \rightarrow 2^{r_2}$ (ignore 1), then:

$$\therefore \frac{N_S(1)}{P(S)} = \frac{2^{r_2-1}}{2^{r_2}} = \frac{1}{2} = 0.5 \qquad \text{...(18)}$$

Example (4):

Table (5) shows the proportion of $N_S(0)$ and $N_S(1)$ to P(S) for various 2-SHSCG.

Table (5) the proportion of $N_S(0)$ and $N_S(1)$ to P(S) for various 2-SHCSG.

Ex.	r_i		$N_S(a)$		P(S)	Proportion of $N_S(a)$		
	r_1	r_2	$N_S(0)$	$N_S(1)$		Expected	Observed	
							$N_S(0)$	$N_S(1)$
1	2	3	6	8	14	0.5	0.428	0.572
2	3	4	28	32	60		0.467	0.533
3	3	5	60	64	124		0.484	0.516
4	4	5	120	128	248		0.484	0.516
5	3	7	252	256	508		0.496	0.504
6	5	7	1008	1024	2032		0.496	0.504

7. Applying of Chi-Square Tests on Study Cases

In this part we will apply chi-square test on the results gotten from calculations of frequency postulate on two study cases.

Let K be the number of categories in the sequence S, c_i be the category i, $N(c_i)$ be the observed frequency of the category c_i, p_i the probability of occurs of the category c_i, then the expected frequency E_i of the category c_i is $E_i = P(S) \cdot p_i$, the T (chi-square value) can be calculated as follows [8]:

$$T = \sum_{i=1}^{K} \frac{(N(c_i) - E_i)^2}{E_i} \qquad \text{...(19)}$$

Assuming that T distributed according to chi-square distribution by $\upsilon = K-1$ freedom degree by α as significance level (as usual $\alpha = 0.05\%$), which it has T_0 as a pass mark. If $T \leq T_0$ then the hypothesis accepted and the sequence pass the test, else we reject the hypothesis and the sequence fails to pass the test, this mean that T not distributed according to chi-square distribution.

Let $N(c_a)=Ns(a)$, for a=0,1.

To apply Hypothesis test:

H_0: $Ns(0) \approx Ns(1)$, while,

H_1: there are a big difference between Ns(0) and Ns(1).

Then we apply the hypothesis test for the difference between two frequencies using chi-square distribution:

$$T=\frac{(N_S(0)-N_S(1))^2}{P(S)} \sim \chi^2(1), \text{ s.t. } \upsilon=1.$$

Example (5):

In order to test our results we have to suggest an example suitable to our two studied cases. Let $r_1=9$ and $r_2=11$. In Frequency test $\upsilon= 1$, with $\alpha=0.05\%$, then $T_0=3.84$ (see chi-square table).

1. **2-CPSCG: $P(S_P)= 1046017$. From equation (13) we get $N_S(1)= 260865$, and $N_S(0)=P(S)–N_S(1)=785152$,**
   $T=\frac{(785152-260865)^2}{1046017}$ = 262784.313 >> $T_0=3.84$, then S generated from 2-CPCSG fail to pass the test and we refuse the hypothesis H_0 and accept H_1, this means there is a big difference between $N_S(0)$ and $N_S(1)$.
2. **2-SHSCG: $P(S_{SH})=524032$ from equation (17), we get $N_S(1)=262144$, and $N_S(0)=P(S)–N_S(1)=261888$,**
   $T=\frac{(261888-262144)^2}{524032}$ = 0.1251 < $T_0=3.84$, then S generated from 2-SHCSG passes the test and we accept the hypothesis H_0 and refuse H_1, this means there is no big difference between $N_S(0)$ and $N_S(1)$.

7. Conclusions

1. **In this work we prove deterministically that the complement Product generator fail in frequency randomness test, while we prove deterministically that the Shrinking generator passes the frequency randomness test, in another word, it's have good statistical frequency properties.**
2. **These theoretical studies can be applied on other kind of SCG,s to calculate the frequency of these SCG,s which are use combining functions with some combinations of variables.**
3. **As future work we may apply other properties of randomness criterion like, serial run, poker and autocorrelation on non-linear SCG.**
4. **The frequency test is not enough to judge on the sequence that has good randomness tests we still have the run and autocorrelation test.**
5. **We recommend that not to use the complement Product generator in cryptography since its fail to pass the frequency test then it may fail to passes the other randomness tests and not to use shrinking generator in cryptography since it's still weak even it passes the randomness tests.**

8. References

[1]. Stallings, W**., "*Cryptography and Net-work Security: Principles and Practices*",** Pearson Prentice-Hall, 4th Edition, 2006**.**

[2]. Golomb, S. W**., "*Shift Register Sequences*"** San Francisco: Holden Day 1967.

[3]. Al-Shammari, A. G**., "*Mathematical Modeling and Analysis Technique of Stream Cipher Cryptosystems*",** Ph. D. Thesis, University of Technology, Applied Sciences, 2009.

[4]. Brüer, J. O**., "*On Nonlinear Combinations of Linear Shift Register Sequences*"** Internal Report LITH-ISY-1-0572, 1983.

[5]. Schneier B**., "*Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C* ",** Wiley Computer Publishing, John Wiley & Sons, Inc., 1996.

[6]. Coppersmith, D. Krawczyk, H. and Mansour, Y**., "*The Shrinking Generator*",** Advances in Cryptology—CRYPTO '93 Proceedings, Springer–Verlag, 1994, pp. 22–39.

[7]. Krawczyk, H**., "*The Shrinking Generator: Some Practical Considerations*",** Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer–Verlag, 1994, pp. 45–46**.**

[8]. Martinez, W. L. and Martinez, A. R**., "*Computational Statistics Handbook with MATLAB*",** Chapman & Hall/CRC, Library of Congress Cataloging-in-Publication Data, 2002.

التخمين لفرضية التردد للمتتابعات غير الخطية المولدة من المولد الضربي المتمم والمولد المتقلص

م.م. زينب صادق جعفر

الجامعة المستنصرية

المستخلص

تعتبر العشوائية (Randomness) من اهم مقاييس الكفاءة الاساسية لمولدات مفاتيح نظم التشفير الانسيابي (Stream Cipher Systems). مولد المفاتيح يعتمد بشكل اساسي على المسجل الزاحف الخطي ذو التغذية الخلفية (Linear Feedback Shift Register) كونه أحد الوحدات الاساسية لنظم التشفير الانسيابي. في هذا البحث، تم حساب خاصية التردد، باعتبارها احد اسس العشوائية، لمتتابعة مولدة من مولد مفاتيح غير خطي نظرياً. قبل تنفيذ النظام عمليا (برمجيا او مادياً)، وهذا الاسلوب سوف يوفر الوقت والجهد والكلفة لمصمم الشفرة. تم اختيار مولدي مفاتيح غير خطية لتطبيق الدراسة النظرية للبحث هما المولد الضربي المتمم (Complement Product) والمولد المتقلص (Shrinking). لقد تم حساب فرضية التردد باثبات نظري لكل من المولدين موضوع البحث.