Linear feedback shift registers essay sample

Law, Security

Abstract: Linear Feedback Shift Registers (LFSRs) are considered powerful methods for generating pseudo-random bits in cryptography algorithm applications. In this paper it is shown that the linear dependencies in the generated random bit sequences can be controlled by adding a chaotic logistic map to the LFSR’s systems. The structure of the LFSR’s output sequence in combination with a chaotic map is analyzed and proved to have at least as much uniformity than the corresponding set for the linear components individually. In order to understand that using the proposed PRBG is reliable in secure algorithms, the NIST suite test have been taken on the proposed method, finally to compare the proposed PRNG output sequence features with the two types of LFSRs (Fibonacci and Galois).
Keywords: Linear Feedback Shift Register, Random Number, Chaotic Map, NIST.

1. Introduction

In the modern world of computers, network security is the main concern which relies on the use of cryptography algorithms. high quality random number generation is a basic subject of cryptography algorithms and the importance of a secure random number generator design cannot be underestimated. Most common generation techniques about RNGs involve truly random and pseudorandom number generators. For a brief introduction in various types of RNGs: Truly Random Number Generators (RNGs) is a computer algorithm, which generates a sequence of statistically independent random numbers. Actually these generators require a naturally occurring source of randomness phenomena (i. e. as a non-deterministic system). Most practical implementations design a hardware device or a software program

based on RNGs to produce a bit sequence which is statistically independent. Pseudo-Random Bit Generators (PRBGs) are implemented by an algorithm that is actually a finite state machine; reliable RNGs which are implemented by these methods should pass several statistical tests to prove their usefulness [2-4]. With the mention of these points, the security of the entire cryptographic system such as RSA and DES and the other secure algorithms relies on the randomness quality of the generator [5, 6].

PRNGs are based on the algorithmic function, so the outputs of these methods are not truly random. In the last two decades several works in this area have been implemented based on chaotic systems [7]. Chaotic system is a natural phenomenon that behaves chaotic in the specific system's parameters [8]. Chaotic maps are sensitive to initial conditions; this makes them sensitive to minimal change of information from the input thus heavily varying the output when input sequence changes by the minute. Chaotic maps compute quickly in the regular machine and are able to create sequences with extremely long cycle lengths [9].

Linear feedback shift register (LFSR) is a shift register which is able to generate random bits (with the mention of amount of registers [1-3]). In the LFSR input bit is a linear function (i. e. it's an exclusive-or function) of its previous state. It's a shift register which input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value. The initial value of the LFSR is called the seed, LFSR's operation is deterministic, and so the stream of values produced by the register is completely determined by its algorithm and current (or previous) state. The theory of the Linear Feedback

Shift Registers (LFSRs) is based on the polynomial form, so in the blow equation p and q are the binary digits: (1)

In this paper we design a new random number generator by using a LFSR generator with a combination of logistic chaotic maps. [10]. The proposed random bit generator is based on a combination of logistic chaotic maps as a chaotic system in the LFSR algorithm, which of course increases the complexity in output sequence of the LFSR and becomes difficult for an intruder to extract information about the cryptography system. In the next section, we briefly introduce the LFSR algorithm, which is a basic building block of the proposed pseudo random bit generator. 2. Linear Feedback Shift Register

The LFSR is a shift register that when the signal generator is clocked, each register generates a signal based on the previous registers (see Figure 1). In this system some of the outputs are combined in an exclusive-or arrangement of elements to form a feedback mechanism. A LFSR can be designed by performing a XOR’s function on the output of the registers. Figure 2 shows a LFSR based on three D-flip flops which are clocked synchronically.

Fig. 1. Three-Bit Shift Register [7]

Fig. 2. Liner Feedback Shift Register [7]

Based on these theoretical points, the condition of the best performance in the LFSRs occurs when the outputs of the D-flip flops are loaded with a random seed value so the linear feedback shift registers make very good

pseudorandom bit generators, it will be able to generate pseudorandom bit sequence of 1s and 0s.

The LFSR generators are defined by the mathematical model:

For an example of positive integer’s s and w, See Refs. [11–13] for more details. The result is that the maximal period length in the specific LFSR’s system with the n registers is . The longest period in the same LFSR’s systems should be found an n as exponent primitive polynomial. In the security field, the period length is very important because it makes the sequence unpredictable. However, the basic solution for this problem is to produce an n exponent primitive polynomial (i. e. n is the large number and reliable sequence length in secure algorithm) with the increased number of D-flip flops. This idea may not work very well, because the number of the registers is limited.

The LFSRs are split into two family devices called the Fibonacci and the Galois representations. In the two next subsections we introduce the Fibonacci LFSR and the Galois LFSR [12-15]. 2. 1. Galois LFSRs

The Galois is presented in the blow equations:

(4)

So the value of results:

(5)

And the product xa is given that simply have been resulted by multiplication of x in the equation (5): (6)

Thus as x is the root of the last equation, we obtain:

(7)

The above equation is the main description of the Galois device feedback computation. In Figure 3, a Galois device is represented as: (8)

Fig. 3. Galois LFSR setup

2. 2. Fibonacci LFSRs

The Fibonacci implementation is the simple shift register which is given by the Fibonacci representation. Let the value of a’ expressed in the following equation: (9)

With the mention of the transposed function the value of a’ would be: (10)

So the value of the xa is obtained in the fallowing equation by the replace of a as xa function which are given by: (11)

Finally:

(12)

The two last equations are the best descriptions of the main part of a Fibonacci LFSR’s systems. In Figure 4, it’s represented as: (13)

Fig. 4. Fibonacci LFSR setup

The properties of LFSR have been deeply studied in Ref. [16-18]. In this paper we will improve the period lengths in these LFSRs generators by adding a chaotic system in a part of the LFSR’s algorithm and create a novel Chaotic Linear Feedback Shift Register (CLFSR). In the next section we are going to describe the importance of chaotic maps in cryptography function.

3. Chaotic Logistic Map

The concept of the chaotic behaviors is related to the positive value of Lyapunov exponents. It is described by following assumptions: Let and be an independent element of tangent space at and the value of mentioned of the n-iteration of F at s in the direction of . So the Lyapunov exponent is given by the specific limited in the equation 14: (14)

The dynamic system presented by F when where is the state space, so the dynamic system has the chaotic behavior if only the value of the Lyapunov exponent in the specific system parameter is positive [16-19]. These chaotic behaviors shown by the simple mathematical model which is used to describe the growth of biological populations are used in the initial population of GA. The mathematical form of the chaotic logistic map is given as:

(15)

Where xn is the state variable, which lies in the interval [0.. 1] and r is called system parameter which can have any value between [1.. 4]. In the next section a novel combination of the LFSR's system will be described and the chaotic map will be proved by the following presented theorem [1- 3]. 4. Combining LFSR with Chaotic Map

Now let us express as a LFSR, as a chaotic logistic map and the output function as: (16)

The sign of represents the operator XOR on the binary sequence of and . The bit sequence of selection (i. e. the B set with bit size), so observed in the expansion of , the string of bit formed by concatenating the bits , the string

of bits in the expansion of and by this order in the (i-1)th level (i. e. in the expansion of) the string of bits where: (17)

It is assumed that is the size of (ith bit selection). Defining as an independent parameter of the jth set, the value of is the corresponding sets of bit strings, it means that the value of the is the corresponding sets of bit string for . By mentioning these assumption the random bit generator is B-equidistributed if is equidistributed [20].

Fig. 5. Chaotic system combined with a LFSR system

For non-liner generators, the uniformity of ti is often evaluated by discrepancy bounds [20], it’s an average over an entire family of generators. Certain types of non-linear generators (like chaotic maps) tend to perform better than the linear ones in statistical tests [17-20]. Figure 5 shows how a LFSR (M-box) combines with a chaotic system (N-box). So with this complete definition, we now have a theorem:

Theorem 1. If B is the bit selection of a sequence generated by (output of a LFSR exclusive-or chaotic map), and is a B-equidistribution for B of size , then is equidistributed (where is a bit vector of size) for any , and is also B-equidistributed. Proof. The fundamental aspect for proving this theorem is based on the reason that in the sample sequence if then and if then (i. e. if only if). On the other hand, it is clear that: , it means that the distribution of the output sequence that is generated by LFSR XOR chaotic logistic map is equal to union of LFSR’s distribution and chaotic logistic map’s distribution). It is equidistributed if and only if is equidistributed. With the mentioning of

these facts the unions of equidistributed sets generate equidistributed set, so is equidistributed. 5. Statistical Testing

The new method for generating secure random numbers is evaluated by the NIST test suite which is a theoretical analysis and experiment program. 5. 1. NIST statistical test suite

The NIST tests suite is a statistical package involving 15 tests which are based on hypothesis testing. Also The NIST tests suite focuses on a variety of different types of non-randomness. These tests focus on a variety of different types of non-randomness that could occur in the sequence. [5] 5. 2. Experiment results

In our test, m is the sample size and in which m = 2000 and = 1- 0. 01 = 0. 99 for the present analysis. So the range of an acceptable proportion is [0. 9833245, 0. 9966745]. The quantitative results of the proportions are given in Table 1 for various statistical tests of the NIST suite [5]. Table 1. NIST test results

Accepted p-value in the NIST suite test with the mentioned initial values, should be in interval [0. 9833245, 0. 9966745]; so the p-values of our purposed method is in this interval and then the 15 tests of the NIST suite have been passed as shown In Fig. 6.

Fig. 6. NIST test result (Red is the Proposed PRNG, Blue represents Galois and Green is Fibonacci) 6. Conclusion

In this paper we presented a novel method to generate random bit sequence by combination of LFSR’s system and chaotic logistic map and it has been

proved in a reliable theorem. At the end, we compared it with the same other methods such as Fibonacci LFSR and Galois LFSR, and the result was shown in table 1.

Acknowledgments

The author wish to thank the editor Professor G. Najafpour, Dr. H. Hassanpour and my teacher Mr. H. Rahimov for their valuable comments. In the end should be appreciated the efforts of Shahrood University of Technology’s ITC research center.