Period length optimization linear feedback shift register by adopting bistable multivibrator

P Utomo, M K M Nasution and M S Lydia
Faculty of Computer Sciences and Information Technology, Universitas Sumatera Utara, Medan, Indonesia
Email: utomopryo@gmail.com

Abstract. Linear Feedback Shift Register (LFSR) is one of the algorithms for getting keys in the form the random number that keeps changing unpredictably in cryptographic systems. But the random number generated by the algorithm has a repetitive period of numbers. Repetition of the number will reappear when the LFSR reaches the limit of maximum length and to be new period based on the previous composition of the number that generated. It will make a weakness of the cryptographic system because it will make it easier to break the key of the cryptographic system that using pseudo-random generator based the number at the previous period. Therefore, this research tries to increase the maximum length of the LFSR algorithm by adopting the bistable multivibrator system steps that applied to electronics. The bistable multivibrator has the ability to change high state to low state and vice versa when it triggered. The adoption process of the bistable multivibrator system is by interpreting high state as a value of "1" and low state as a value of "0". The changes output of the bistable multivibrator will then be used to influence the LFSR algorithm works with XOR gate. Experiments carried out by producing pseudo-random numbers using 30-bit registers 30 times and 4-bit registers 60 times successfully increasing the maximum length with the result twice from the previous maximum period length. Thus the LFSR optimization results with bistable multivibrator have a better impact than the normal LFSR for use in cryptographic systems.

1. Introduction
Cryptography is the way to secure data or information by relying on keys to encrypted data. Cryptography use two ways to using the keys. It is symmetric keys and asymmetric keys. The asymmetric keys commonly get the key from the generation of the pseudo-random number. Some pseudo-random number generator algorithms that have been combined with cryptography such as Linier Feedback Shift Register (LFSR), Blum-Blum Shub (BBS), Chaotic and etc [1-3]. The goal is the keys always come up with change unpredictable so that it is increasingly difficult to solve [4]. To get numbers that appear randomly there are many ways that can be done [5]. But apparently, not all of these methods are safe to used. The pseudo-random number Generator (PRNG) algorithm must passed the statistical test first so that they are suitable to be combined with cryptographic systems [6]. Although some algorithms have passed statistical tests, there are still some weaknesses in pseudo-random number generator algorithms [7]. Pseudo-random numbers were generated are only looked random because there are the repetitive on the generation of numbers based on the mathematical calculations applied by the algorithm [8-9].
In the LFSR algorithm, the generation of random numbers uses mathematical calculations that follow the Primitive Polynomial LFSR function. By following the equation of the function there will be numbers arranged randomly with maximum long sequence. But in reality, the sequence of numbers that have been generated appear to be periodic repetitions. After the generated number reaches the maximum limit, the continuation of the generated number will repeat the sequence in the previous period. The maximum length limit of numbers in the sequence of periods is different for each quantity of LFSR bits used. The maximum length can be calculated by equation $2^n - 1$ where "n" is quantity of the bits register when it follows the Primitive Polynomial LFSR function [1].

The bistabil multivibrator is the basis of a data memory storage besides that it is also used as a pulse counter as a synchronization of input time-variable signals for some reference time signals. The nature of its output which can change if triggered only produces two possibilities, namely high voltage (1) or low voltage (0).

Based on these problems, this research aims to optimize by increasing the maximum length with try to do the experiment where the output of bistable multivibrator will affect the LFSR algorithm to generating a period of a pseudo-random number. So that the sequence of pseudo-random numbers that are generated has a higher level of randomness.

2. Research Methods
Figure 1 is a illustration in the pseudo-random number generation process of the Linear Feedback Shift Register algorithm which will be affected by the bistable multivibrator output.

![Figure 1. LFSR Generation Process Scheme with Bistabil Multivibrator Output](image)

The input value for empty registers in generating the pseudo-random number is done by taking the value of the XOR result between the value of the LFSR feedback function and the output value of bistable multivibrator that triggered by shifting bits in the register. The shifted register's value will trigger a bistable multivibrator to change the output value so that the bistable multivibrator output value will continue to change when it will generating pseudo-random number. The adoption of bistable multivibrator output values is done by reversing the previous output value with NOT gate automatically when triggered so that the value appears like the bistable multivibrator output value applied to electronics. The new value obtained will then fill n the empty bits in the register so that it generates a new pseudo-random number.
3. Results and Discussion
At this stage, researchers conducted experiments by generating a pseudo-random number Linear Feedback Shift Register optimized with output bistable multivibrator so get the maximum length for a longer number period. Each algorithm performs an experiment by generating pseudo-random numbers using 3-bit registers 30 times dan 4-bit registers 60 times. The comparison of pseudo-random numbers generated is as follows:

![Figure 2. LFSR Generation Flowchart with Bistabil Multivibrator.](image)

![Figure 3. Generation of the LFSR on the 3-bits registers.](image)
Figure 3 shows there is a repetition of the pseudo-random number generation period in the 8th order on 3-bit registers. This proves that the normal LFSR only has the maximum length of the number period only up to 7th. The increase in the length of the period from the results of the optimization of the length of the period can be seen in Figure 4 where the loop period is found in the 16th order.

The same thing happens in experiments on 4-bit registers. Figure 5 shows there is a repetition of the pseudo-random number generation period in the 16th order where the experiment uses the normal LFSR algorithm. The increase in the length of the period from the results of the optimization of the length of the period can be seen in Figure 6 where the loop period is found in the 32nd order.

4. Conclusion
Based on the results of the research described, it can be concluded that the LFSR algorithm optimized with the bistable multivibrator output has the ability to generate a pseudo-random number twice the longer period than the Linear Feedback Shift Register algorithm without experiencing optimization. That way it will be more difficult for cryptanalysts or people who want to break codes for personal interests and harm others in breaking data.
References

[1] Aïssa B, Khaled M and Lakhdar G 2014 Implementation of blum blum shub generator for message encryption Proc. Int. Conf. on Control, Engineering & Information Technology ISSN 2356-5608 pp. 118-123.

[2] Rahimov H, Babaei M and Farhadi M 2011 Cryptographic PRNG based on combination of LFSR and chaotic logistic map Applied Mathematics Vol. 2 No. 12 2011 pp. 1531-1534 doi: 10.4236/am.2011.212217.

[3] Som S and Ghosh S 2012 A stream cipher cryptosystem based on linear feedback shift register International Journal of Mathematical Archive ISSN 2229–5046 Vol. 3 No. 2 2012 pp. 362-372.

[4] Borujeni S E 2002 Cryptography by pseudo random number generator 1st Int. IEEE Symp. Intelligent Systems 2002 pp. 244-247 doi: 10.1109/IS.2002.1044262.

[5] Haahr M 1999 Introduction to randomness and random number random.org https://cran.r-project.org/web/packages/random/vignettes/random-essay.pdf.

[6] Bassham III L E, Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Levenson M, Vangel M, Banks D, Heckert A, Dray J and Vo S 2010 A statistical test suite for random and pseudorandom number generators for cryptographic applications NIST Special Publication 800-22 Rev. 1a. doi:10.6028/NIST.SP.800-22r1a.

[7] Kelsey J, Schneier B, Wagner D and Hall C 1998 Cryptanalytic attacks on pseudorandom number generators. S. Vaudenay, Ed Springer-Verlag Fast Software Encryption, LNCS 1372 pp.168-188.

[8] Abinaya N S and Prakasam P 2014 Performance analysis of maximum length LFSR and BBS method for cryptographic application Int. Conf. on Electronics and Communication Systems (ICECS) Coimbatore, 2014, pp. 1-5 doi:10.1109/ ECS.2014.6892699.

[9] Yan S Y 2002 Number theory for computing 2nd Edition. Springer-Verlag : Berlin. Heidelberg. New York. Barcelona. Hong Kong. London. Milan. Paris. Tokyo.