RESEARCH

The improvement of period of pseudo random number sequence: An algebraic approach

Debashis Ghosh

Ghosh D. The improvement of period of pseudo random number sequence: An algebraic approach. J Pure Appl Math. 2023; 7(3):210-215.

ABSTRACT

Linear feedback shift registers are the fundamental structure of pseudo random number generators that are used in formation of channel key. Many methods were proposed for determining linear recurring sequences generated by Linear Feedback Shift Registers to enhance the period. In view of large-scale application of this sequence in security and privacy, a clocked controlled linear feedback shift register has been introduced, known as dynamic linear feedback shift register. In this article, we emphasis on dynamic linear feedback shift register scheme using combinatorial design having constant block length and algebraic structure to enhance the period. Such sequence has the vulnerability from attack. Our proposal for designing dynamic linear feedback shift register involves primitive polynomial over a finite field of prime powers. A counter example shown the practical implication of our theory that improve the period of the sequence than existing scheme. Finally, an effort was thru on properties of the generated sequence in terms of security aspect.

Key words: *Dynamic Linear Feedback Shift Register; Pseudo Random Number Generator; Primitive Polynomial; Linear Complexity*

INTRODUCTION

The rapid development of wireless communication makes the data transmission easier from any place. On contrary to that, the availability, privacy, and authenticity of any sensitive data like bank account number, password of different account, transmission of images etc. come under threat through various communication devices like smartphone, tab with others. To do a favor towards the cryptographic security of such data, stream cipher plays a vital role [1-11]. Here data is encrypted and decrypted bit by bit through the same key. For such an encryption process, we require a lengthy bit of binary strings, coming from pseudo random binary sequence generators. These efficient generators are the necessary device for the privacy of the system [12- 22]. The encryption and decryption, of such ciphers, are executed based on XOR operation with a lengthy key stream. Linear Feedback Shift Registers (LFSR) are widely employed for key stream generator, that have the virtue of perfect 0 − 1 statistical distribution, two-valued auto correlation, large period, low implementation cost with ready analysis using algebraic technique [9, 15, 20]. This device is mostly treated as the building blocks of many sequence generators from last two decades [2, 3, 7, 19]. A LFSR of a given size n is capable of producing maximal sequence (m − sequence) by passing through every non−zero state once and only once to give the period $N = 2^n - 1$, excluding the all−zero state, make a good choice for evolving a stream ciphers. In a series of publications, various techniques are developed for the generation of Pseudo Random Number Sequence (PRNs) by adopting different mathematical tools [4, 5, 10, 12, 14, 15, 19, 20, 23- 27]. Here our motivation is to describe a theoretical model for the generation of longer PRNs of having period greater than their linear span and having better unpredictability as well.

With the current development of better transmission and to resist various cryptographic attacks, LFSR based stream cipher under normal clocking, convert to DLFSR based on stream cipher using irregular modification of feedback functions and clocking mechanism [26, 24]. In 2002, [19]. Initiated a pseudo random sequence generator based on LFSR with dynamical feedback whose feedback polynomials are updated according to the state of another adjoining LFSR. Later in the year 2005, Babbage and Dodd proposed the Mickey stream

School of Applied Science and Humanities, Haldia Institute of Technology, Haldia, India

Correspondence: Debashis Ghosh, School of Applied Science and Humanities, Haldia Institute of Technology, Haldia, India, e-mail: ghoshdebashis10@gmail.com
Received: May 11, 2023, Manuscript No. puljpam-23-6415, Editor Assigned: May 13, 2023, Pre-QC No. puljpam-23-6415 (PQ), Reviewed: May 15, 2023, QC No. puljpam-23-6415 (Q), Revised: May 17, 2023, Manuscript No puljpam-23-6415 (R), Published: May 31, 2023, DOI:-10.37532/2752-8081.23.7(3).210-215

cipher for hardware implementation [1]. They also used dynamic feedback controlled for their generation of pseudo random number sequence. Two years after, Kiyomoto et al. [14], proposed a wordoriented stream ciphers with irregular clocking known to be K2 with some modification in Mickey. The most enlighten step to design the cipher is to update by modifying the scrambling operation. They also analyzed the security aspect of their cipher against different kind of attacks and gives a better resistance except side- channel attack. But the weakness against various attacks of the Kiyomoto cipher has observed by Orumiehchiha et al. in the year 2013 [21]. By that time, in 2009, Rakaposhi stream cipher come into light [4]. This is a successor of Kiyomoto stream cipher in terms of low–cost hardware implementations. Here the key-stream is produced by giving the inputs from both the sub-registers. Same year, a true random number generator scheme is proposed based on LFSR with having several feedback polynomials using round robin scheme. Peinado et al. modify the proposal by a mathematical model, based on merging and shuffling two sequences which leads to DNA Sequencing, to get a better prediction on period and linear span of the sequence [24]. Later on, some more approaches are made like irregular clocking of the LFSR, depending on dynamically changing the feedback polynomial of the LFSR in running time to form a Dynamic Linear Feedback Shift Register in [13, 25, 27]. To defend various cryptographic attacks, we also emphasis our article on the enhancement of the period of the random sequence. The mathematical tool that we use, is not only the irreducible polynomial but also use a table constructed by the combinatorial design concept to generate the feedback computation of the DLFSR. In a Galois Field of prime order ≥ 3 have more than one irreducible polynomial. We use all those irreducible monic polynomials of particular order. To reduce the correlation among the bits generated, we also make a random choice among all irreducible polynomials for defending the correlation attack.

The article is organized in the following manner. In section 2, technical preliminaries relevant to DLFSR is formally discussed. In section 3, we describe our mathematical model and explain the method by giving an example. Finally, we compute the maximal possible period of the generated sequence. Section 4, deals with the properties of the generated sequence. Lastly, the conclusion is in section 5 to end the article. We compute the period associated to the feedback position with respect to one irreducible polynomial using MATLAB code.

TECHNICAL PRELIMINARIES

In this section, we describe definition and some basic properties relevant to linear feedback shift registrar and finite fields. For details study on this, author refers the reader [10, 8]. Throughout in this article, we work with binary sequence, a member of GF (2) – Galois field or finite field of order 2.

Every finite field either is of order prime or prime power. Here in our article, we consider the base field as GF (2), the smallest finite field.

Definition 1

A linear feedback shift registers of length r over GF (2), with co-efficient $q_1, \ldots, q_r \in GF(2)$ is a sequence generator whose every state is an element of the sequence sting, like

$$s = (a_0, a_1, \ldots, a_{r-1}) \in GF(2^r),$$

and output is a_0, where the state change operation τ is given by

$$(a_0, a_1, \ldots, a_{r-1}) \to (a_1, a_2, \ldots, a_{r-1}, \sum_{i=1}^{r} q_i a_{r-i})$$

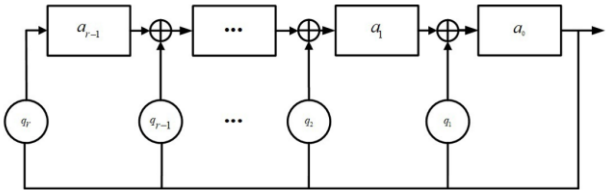

Figure 1) *Galois configuration of LFSR*

The above recursion relation is homogeneous and linear.
Each block has the capacity to hold a bit of information. In each time unit of a clock, that modulates a normal LFSR to make changes the followings:

1. a_0 is the output bit of the LFSR.
2. a_i shifted to a_{i-1}, for $i = 1, 2, \ldots, r-1$.
3. The last bit i.e., a_{r-1} computed by XOR–ed the feedback element q_i's of the LFSR.

Figure 1, shows a normal LFSR with its feedback tapping.

In this state diagram of LFSR, every state will have a unique successor and unique predecessor. In many cases, we observe that the output sequence of an LFSR, depends on the initial states, on changing the initial string make changes in the period of the sequence.

The connecting polynomial with a LFSR is given by

$$P(x) = 1 + q_1 x + q_2 x^2 + \ldots + x^r \in \mathbf{Z}_2[x]$$

with $q_r \neq 0$ for LFSR to be genuinely with r stages. Otherwise, the recursion becomes of degree less than r.

Definition 2

A polynomial of degree n over GF (q) is said to be irreducible, if the polynomial could not be able to express as a product of polynomials of degree less than n and more than 0.

Definition 3

A polynomial is said to be monic, if the coefficient of the highest degree term in the polynomial is 1.
By a monic irreducible polynomial of degree n over GF (p), we can construct a finite field of order p^n, can construct a finite field of order p^n, for some prime p, where $q = p^n$. The number of monic irreducible polynomials of degree n over GF (q), is denoted by $M_n(q)$, and is given by [16].

$$M_n(q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}},$$

where $\mu(d)$ is called the Mobius function.
The finite fields which are of prime orders p, are constructed under modulo operation, modulo p. Whereas of prime power are

constructed with the help of a polynomial, namely irreducible polynomials defined over base field. The necessary and sufficient condition for an $L-$stage LFSR to produce an $m-$sequence of period $2^r - 1$ is that the characteristic polynomial should be of degree r, known as primitive over $GF(2^r)$.

Here in our method to improve the period, we use the monic irreducible polynomial, which are distinct in enumeration depending upon the finite field order and the degree of the polynomial. Choice of the field and the irreducible polynomial do influence the period of the sequence but the initiation of binary string does not influence the output as well as the period of the sequence. Hence the period of the sequence is seed independent except all-zero state. Thus, the sequence generated is called maximal length linear feedback shift register sequence.

DESCRIPTION OF PSEUDO RANDOM BIT GENERATOR USING DLFSR

The DLFSR generator originated by the accumulation of two different LFSRs: the main register, the LFSR of length n and an associated register, controlled by register, of length m. The control register has authority over the primitive feedback polynomial, it runs cyclically all possible the $2^{mn}-1$ non-zero states and produces a maximal-length control sequence, that gives a PN-sequence. The maximal sequences or $m-$sequences are obtained when the n−degree feedback polynomial is primitive.

In addition, the later register is connected to a decoder that, its present state, and a fixed rule, selects from a table of the feedback polynomial of the LFSR of same length n. The Dynamic Characteristic Polynomial (DCP) block introduces the logic circuitry to implement the feedback corresponding to the chosen polynomial. In this way, different LFSRs can be realized inside the LFSR$-n$ as long as the process of sequence generation is carried out. The DLFSR is a LFSR in which the feedback polynomial is modified in running time. The theoretical model of a DLFSR consists of dual LFSRs of which one is for the key generation along with an additional module for controlling to choose a different feedback polynomial from the primitive list. In instant time, it will be checked with the last feedback polynomial, if different then proceed as before for the generation of key stream. The sequence produced by the DLFSR having a cycle structure in such a way that the final LFSR state corresponding to feedback polynomial $f_i(x)$ is then use for the initial state corresponding to feedback polynomial $f_{i+1}(x)$. This process will continue until it touches all the feedback polynomials in the list.

A model of key stream generator

In this construction, we consider finite fields and their primitive polynomials as basic ingredients. Consider a prime number p and any positive integer n, then there will be a finite field of order $q = p^n$, denoted by $GF(p^n)$. To construct a finite field of such order, we need a primitive polynomial of degree n with coefficients from $GF(p)$. Let α be a non-zero element from $GF(p^n)$, for $n \geq 3$, that could generate all the elements, other than zero. α is a root of that primitive polynomial. $GF(p^n)^*$ become a field under the operation of modulo the primitive polynomial and modulo n for the degree of the polynomials. Each element of such field will define the support set corresponding to that element of $GF(p^n)^*$. Thus, it will generate p^n-1 non−zero positions. Therefore, we now produce the multiplication tables with the help of non−zero elements of $GF(p^n)$ under modulo multiplication of $GF(p^n)^*$. The elements of initial column of the table be multiplied by α, α^2, α^3..., α^{n-1}, consecutively to construct remaining $(n-1)$ tables, respectively. Now we put the same position elements in each table combining in a new table into concatenation structure. Thus, each position, say (i, j), will have n-elements. These n positions are then use as the support set or the feedback positions of the primary LFSR for initialization. As a criteria of support set, we consider only non-repeating members. Each of these non−repeating members is then use in LFSR to generate the random bit sequence. Instead of using the polynomials directly, we make use of a combinatorial arrangement of feedback positions in LFSR according to each $(i, j)-$th position in the table, with the help of primitive elements to moderate the period of the sequence. We then shuffle the positions in a cyclic rotation to get a new arrangement of tapping positions. This will also randomize the sequence under extensive period. The sum of resultant periods of the generated random binary sequence as well as randomization of the choice of polynomial enhanced the period.

Explanation with example for p = 2 and n = 5

Here, we generalize the scheme by constructing a feasible structure for some particular value of n and p, but the result is true for arbitrary choice of n and for any prime p, if possible. For simplicity in all respect, we consider $p = 2$ and $n = 5$. There must be a finite field of order 2^5. Among the three primitive polynomials, we consider $x^5 + x^2 + 1$ for our purpose. A non-zero element α, is the image placed in the position 2, taken from $GF(2^5)$. This primitive element would generate all the non-zero elements of the field of order 31. Those are given in the following table, Table 1.

TABLE 1
Elements generated by the irreducible polynomial

Following are the 31 elements of *GF* (2^5)

α	$\alpha 2$	$\alpha 3$	$\alpha 4$
$\alpha^2 + 1$	$\alpha^3 + \alpha$	$\alpha^4 + \alpha^2$	$\alpha^3 + \alpha^2 + 1$
$\alpha^4 + \alpha^3 + \alpha$	$\alpha^4 + 1$	$\alpha^2 + \alpha + 1$	$\alpha^3 + \alpha^2 + \alpha$
$\alpha^4 + \alpha^3 + \alpha^2$	$\alpha^4 + \alpha^3 + \alpha^+1$	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^4 + \alpha^3 + \alpha + 1$
$\alpha^4 + \alpha + 1$	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^3 + \alpha^2$
$\alpha^4 + \alpha^3$	$\alpha^4 + \alpha^2 + 1$	$\alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$
$\alpha^4 + \alpha^3 + 1$	$\alpha^4 + \alpha^2 + \alpha + 1$	$\alpha^3 + \alpha + 1$	$\alpha^4 + \alpha^2 + \alpha$
$\alpha^3 + 1$	$\alpha^4 + \alpha$	1	XXXXX

For α is one of the primitive elements that generates all distinct 31 elements under the operation modulo 31. Now we construct the table with all 31 elements with 0 of *GF* (2^5). The next 4 tables will be formulated by multiplying the first column with α, α^2, α^3, α^4 respectively. Accordingly, the positions are going to change in their respective tables. Finally, put all the 5 positions from 5 different tables as concatenation form, in their respective boxes, originated in each position of the table in a new *supportive table*. Since we are not considering the repetitions, therefore after removing all repeated position elements from the supportive table is given below, Table 2.

TABLE 2
Different tapping positions

252628328	293032412	31322614	1718202432	32392113
1820243216	262832824	303241228	2481632	32515311
192228832	232632124	293261810	1114203224	326181026
212642432	273210306	29212328	1722322028	32721179
142032248	222883216	263212420	612241632	51432412
152243224	233012832	253214102	1118322820	21232824
252202432	32927317	11028328	2332182230	32111135
2232202812	264243216	321030622	102081632	51812328
213222226	27628832	311032124	1930203224	321410218
256322028	291042432	32137273	1932261422	32151391
183228204	22432248	301283216	1428241632	15322614
192322820	23643224	311412832	1732302618	143241228
118202432	92628328	133032412	3217192331	133261810
3218223014	220243216	102832824	18481632	13212328
321925529	32228832	72632124	2714203224	103212420
122322028	52642432	113210306	3221311927	93214102
302032248	322222610	62883216	2212241632	211432412
312243224	32235125	73012832	2718322820	181232824
732182230	92202432	171028328	3225111523	151032124
322614226	632202812	104243216	3229231119	211812328
330203224	53222226	11628832	3028241632	141283216
332261422	96322028	131042432	3231292517	151412832
323026182	23228204	6432248	3213715	__
132302618	32322820	7643224	32261430	__

Among the above, only few are giving the proper period of the sequence generating with any seed value of 32-bit length. In the following Table 3, the support set position with their periods is given.

TABLE 3
The periods associated for different tapping positions

Support Set of LFSR	Period	Support Set of LFSR	Period	Support Set of LFSR	Period
6, 12, 24, 16, 32	65534	10, 20, 8, 16, 32	65534	17, 32, 30, 26, 18	6035421
22, 12, 24, 16, 32	65534	27, 18, 32, 28, 20	10485755	26, 20, 8, 16, 32	65534
32, 27, 17, 29, 21	2162622	25, 26, 28, 32, 8	520065	18, 20, 24, 32, 16	65534
25, 6, 32, 20, 28	186277	3, 32, 26, 14, 22	299593	1, 32, 30, 26, 18	430185
14, 20, 32, 24, 8	49146	27, 32, 10, 30, 6	166005	22, 28, 8, 32, 16	64770
2, 20, 24, 32, 16	65534	6, 32, 20, 28, 12	65534	5, 32, 22, 2, 26	166005
2, 32, 28, 20, 4	65534	31, 32, 2, 6, 14	430185	30, 32, 4, 12, 28	65534
29, 32, 6, 18, 10	299593	26, 32, 12, 4, 20	65534	31, 10, 32, 1, 24	149431
30, 12, 8, 32, 16	65534	31, 14, 12, 8, 32	2097151	7, 26, 32, 12, 4	558831
7, 26, 32, 1, 24	1168146	17, 10, 28, 32, 8	26738637	18, 12, 8, 32, 16	49146
10, 4, 24, 32, 16	64770	7, 6, 4, 32, 24	520065	1, 5, 7, 13, 32	4161409
32, 26, 1, 4, 30	608685	32, 5, 15, 3, 11	1081311	13, 21, 2, 32, 8	1048575
1, 32, 12, 3, 28	1360170	14, 12, 8, 32, 16	65534	15, 14, 1, 28, 32	1048572

This will give a random sequence of various periods, the total period of which is 6, 27, 36, 929. Now on shuffling those support set in cyclic order will randomize the sequence effectively and the period be 6, 27, 36, 929 × 39! This will be extensively high enough by adding the other irreducible polynomials into account.

CRYPTOGRAPHICAL PROPERTIES OF THE SEQUENCE

Period of the sequence

The above calculation is made for only one irreducible polynomial of degree 5. There are 6 such polynomials over *GF* (2). The period of the binary sequence could be improved by more than 6 times of such calculated period. On the other hand, increasing the length of the sequence the period will automatically be enhanced.

Furthermore, if we use the round robin system for choosing the primitive polynomials of degree 5, it will not only improve the randomness of the sequence but also strengthen the performance for key stream generator.

Linear complexity

A LFSR of length *n* consists of *n* registers containing single bit each, initially, called the seed value. Using the primitive polynomials, we generate the tapping sequence and combine them with the shifted bit by bit XORing modulo 2. If the sequence be $(s_0, s_1, ..., s_n)$. Then the tapping bits are computed by a simple dot product. The linear combination of them will generate the feedback bit. Let the tapping sequence is

$T = (t_0, t_1, ..., t_n)$

where,

$$t_i = \begin{cases} 0, & \text{if the feedback is passive} \\ 1, & \text{if the feedback is active} \end{cases}$$

Thus, the sequence generates satisfying the linear recurrence function. This pseudo random sequence generated by the process involving LFSR with such a tapping criterion give the higher linear complexity − which is the necessary condition for the better security.

CONCLUSION

This paper proposes a theoretical approach for the modification of the period and increase the scrambling of the sequence. Such a modification will improve the randomization property for the binary sequence to make it more robust to attack and also none the sequence are interleaved. It has also been observed in cumulative sum test to identify the number of $1's$ and $0's$ in the sequence are approximately the same, as would be expected for equi-distribution. For future research, this proposal can be related with developing fully functional version technique and software tool for the users and applied to practical applications.

CONFLICT OF INTEREST

The author declares that there is no conflict of interest.

REFERENCES

1. Babbage S, Dodd M. The MICKEY Stream Ciphers. New Stream Cipher Des. 2008;4986:191-209.

2. Blum M, Micali S. How to generate cryptographically strong sequences of pseudo random bits in providing sound foundations for cryptography. Assoc Comput Mach. 2019;227-40.
3. Catarino P. On k-Pell hybrid numbers. J Discrete Math Sci Cryptogrvol. 2019;22(1):83–89.
4. Cid C, Kiyomoto S, Kurihara J. The RAKAPOSHI Stream Cipher. Inf Commun Secur. 2009;927:32-46.
5. Ding L, Guan J. Cryptanalysis of Mickey family of stream ciphers. Secur Commun Netw. 2013;6:396-941.
6. Dridi F, El AS, El HY, et al. The Design and FPGA-Based Implementation of a Stream Cipher Based on a Secure Chaotic Generator. Appl Sci. 2021;11(2):652.
7. Durga RS, Rashmika CK, Madhumitha ONV, et al. Design and Synthesis of LFSR based Random Number Generator. Third Int Conf Smart Syst Inven Technol. 2020;438-42.
8. Ghosh D. An extension of binary cyclotomic sequences having order $2^l t$". Discrete math algorithms appl.
9. Golic JD. Period of interleaved and non-uniformly decimated sequences. IEEE Trans Inf Theory. 1998;44(3):1257–60.
10. Golomb S. Shift Register Sequences. Aegean Park Press. 1982.
11. Jiao L, Hao YL, Feng DG. Stream cipher designs: a review. China Inform Science. 2020;63(3):1–25.
12. Kanso A. Clock-controlled shrinking generator of feedback shift registers. Australas conf Inf secur priv. 2003;443-51.
13. Klein A. Non-linear Combinations of LFSRs. Stream Ciphers. 2013;1550:59-89.
14. Kiyomoto S, Tanaka T, Sakurai K. K2: A stream cipher algorithm using Conference on Security and Cryptography. Barcelona. 2007;204-13.
15. Liu L, Miao S, Hu H, et al. Pseudo random bit generator based on non-stationary logistic maps. IET Inf Security. 2016;10(2):87-94.
16. Lidl N, Neiderreiter H. Finite Fields: Encyclopedia of Mathematics and its Application. Addison Wesley. 2012.
17. Luengo EA. A brief and understandable guide to pseudo-random number generators and specific models for security. Stat Surv. 2022;16:137-81.
18. Luo W, Takeuchi N, Chen O, et al. Low-autocorrelation random number generator based on adiabatic quantum-flux-parametron logic. IEEE Trans Appl Supercond. 2021;31(5):1-5.
19. Mita R, Palumbo G, Pennisi S, et al. A novel pseudo random bit generator for cryptography applications. Electron Circuits Syst. 2022;2:489-92.
20. Nannipieri P, Di MS, Baldanzi L, et al. True random number generator based on Fibonacci-Galois ring oscillators for FPGA. Appl Sci. 2021;11(8):3330.
21. Orumiehchiha MA, Pieprzyk J, Shakour E, et al. Security Evaluation of Rakaposhi Stream Cipher. LNCS. 2013;7863:361-71.
22. Panda AK, Ray CK. Modified Dual-CLCG method and its VLSI architecture for pseudo-random bit generation. IEEE Trans Circuits Syst I: Regul Pap. 2019;66:989-1002.
23. Peinado A, Fúster SA. Generation of pseudorandom binary sequences by means of LFSRs with dynamic feedback. Math Comput Model. 2013;57:2596-604.
24. Peinado A, Petrovic S. Dynamic LFSRs as an alternative to LFSRs in extended fields - A comparative study. Nor IKT-konf forsk utdanning. 2022;3.
25. Rashid MI, Ferdaus F, Talukder BMSB, et al. True random number generation using latency variations of FRAM. IEEE Trans Very Large-Scale Integr Syst. 2020;29(1):14–23.
26. Reddy A, Indrasena M. Siva KA, et al. A secured cryptographic system based on DNA and a hybrid key generation approach. Biosystems. 2020;197:1-10.
27. Tupparwar S, Mohankumar N. A Hybrid True Random Number Generator using Ring Oscillator and Digital Clock Manager. 6th Int Conf Inven Comput Technol. 2021; 290-94.