Dynamic Linear Feedback Shift Registers: A Review

Fardous Mohamed Ali Eljadi[1], Imad Fakhri Taha Al Shaikhli[2]
Department of Computer Science
IIUM
Kuala Lumpur, Malaysia
[1]fma_m@hotmail.com, [2]imadf@iium.edu.my

***Abstract*—An improvement in the security of stream cipher is achieved by introducing dynamic polynomial switching in the Linear Feedback Shift Registers. Several researches declared that this introduction enhances the stream cipher's immunity to cryptanalysis. This paper aims to provide a comprehensive survey that summarizes the recent approaches for applying this idea for the purpose of shaping a clear vision of these designs. This vision will assist the development process of new designs.**

Keywords- Linear Feedback Shift Register, Dynamic feedback Shift Registe, stream cipher, cryptography.

I. INTRODUCTION

In recent years, the increasing use of the Internet and the growing exchange of digital information have led to the necessity of reinforcing security. Recently, one of the most commonly used techniques for security is cryptography. It produces the methods of building the most modern security protocols used to transmit information. In cryptography, there are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption). Symmetric encryption consists of two families of schemes which are block ciphers and stream ciphers. In stream cipher, plain text bits are combined with a pseudo-random bit sequence called a key stream. The output of this operation is called cipher text. It can be transformed back into its original form using the same key stream [1]. A pseudo-random sequence can be generated using a Linear Feedback Shift Register (LFSR). LFSRs are simple, fast, and easy to implement for both software and hardware. They are capable of generating pseudo-random sequences with the same uniform statistical distribution of 0's and 1's in a truly random sequence. However, they are not cryptographically secure, because the construction of an LFSR of length n-bits can be easily deduced by observing the 2n consecutive bit of its sequence using the Berlekamp-Massey algorithm[2]. Due to its inherent linearity, LFSR-based stream ciphers are vulnerable to several form of attacks, such as fast algebraic attack[3],and correlation attack [4].

In order to overcome the linearity of the bits generated using LFSR, several approaches are proposed [5, 6], some approaches concentrated on processing the output sequence of LFSRs using non-linear Boolean function to form a combination generator, while the other focused on processing several bits from the LFSR state using a non-linear function to form a filter generator [7].

Another approach concentrated on the working mechanism of a LFSR. Some approaches used the irregular clocking of the LFSR [8], while others introduced methods based on dynamically changing the Feedback polynomial of the LFSR in running time to form a Dynamic Linear Feedback Shift Register [9-19]. A combination of these approaches can be used to increase the overall security of the LFSR-based stream cipher. In this paper, we consider several existing Dynamic Linear Feedback Shift Register (DLFSR) constructions. An effort was made to analyze these constructions in order to assist the development process of future DLFSR designs.

This paper is organized in the following manner. Section 2 provides the theoretical background on LFSRs. In Section 3, some methods of introducing the nonlinearity in the output sequences of LFSRs are presented. DLFSR is introduced in section 4. Section 5 is made up of literature review regarding certain DLFSR constructions. After that, the paper discusses the reviewed constructions and concludes the work.

II. LINEAR FEEDBACK SHIFT REGISTERS

A feedback shift register consists of two parts: a shift register and a feedback function (see Fig. 1). The shift register is a sequence of bits. Its length is determined in bits; if it is n bits long, it is called n-bit shift register. All of the bits in the shift register are shifted one bit to the right each time a bit is needed. The new left-most bit is computed as a function of the other bits in the register. The feedback function is normally the XOR of selected bits in the register; the list of these bits is called a tap sequence. The output of the shift register is one bit, usually the least significant bit.

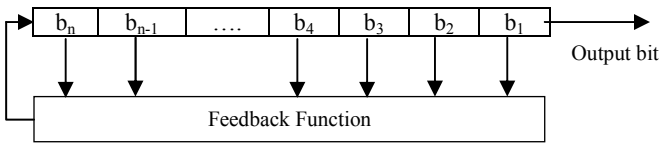

Figure 1. The general constructions of a linear feedback shift register.

LFSRs are commonly used as part of key stream generators in stream ciphers. Certain criteria are considered for the parts of keystream generators. These criteria include

period, linear complexity, and statistical measures of the keystreams.

A. Period

The period of a shift register is the length of the output sequence before it starts repeating. If the feedback polynomial of the n-bit LFSR is primitive and its initial state is at a non-zero state, then the output sequence generated by this LFSR has the maximum period of 2^n -1. This sequence is called the maximum-length sequence, or m-sequence. The m-sequences possess excellent randomness properties [20].

B. Linear complexity

One essential metric used to evaluate LFSR-based generators is linear complexity, or linear span. This is described as the length (n) of the shortest LFSR that can imitate the generator output. Linear complexity is very important, because a simple algorithm, called the Berlekamp-Massey algorithm, can generate this LFSR after investigating only 2n bits of the keystream. Once this LFSR is generated, the stream cipher is broken. It is worth noting that a big linear complexity does not always indicate a secure generator. However, a small linear complexity does indicate an insecure one [2].

C. Statistical measures

Suitable metrics are required to examine the degree of randomness for binary sequences generated by random number generators. A number of statistical tests exist to determine the statistical behavior of the sequence. These tests usually check for random distribution, distribution of ones and zeroes in a sequence, linear dependence among fixed length substrings, the level of compression that can be carried out on tested sequence, and whether a sequence is complex enough to be considered random. Three well-known tests are the Federal Information Processing Standard tests (FIPS) [21] , Diehard suite [22], and National Institute of Standards and Technology Statistical Test Suite (NIST) [23].

III. INTRODUCING NONLINEARITY

The output sequences of LFSR have a linear structure. Therefore, the immediate output of LFSR is unsuitable to be used as a keystream. In order to use LFSRs in the design of keystream generators, their linearity must be destroyed. To achieve that, different methods have been introduced [7, 24, 25], which include:

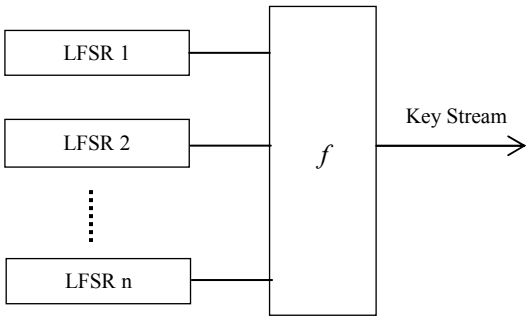

Figure 2. The Combination generator

A. Combination generators

In this generator, the output of several LFSRs is combined by a Boolean function *f* to produce the keystream. To generate a secure and random keystream, the Boolean function has to satisfy certain criteria. Fig. 2 illustrates the general construction of this generator.

B. Filter generators

Filter generators only use a single LFSR. A Boolean function generates the keystream by filtering the contents of the LFSR.

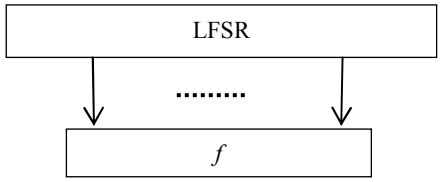

Figure 3. The Filter generator

C. Clock-controlled generators

A Clock-controlled generator has at least one LFSR, which is clocked in an irregular manner by some other part of the cipher.

In addition to the aforementioned methods, there is a method based on dynamic polynomial switching in the Linear Feedback Shift Registers. In the next section, we detail this method which is the main focus of this research.

IV. DYNAMIC LINEAR FEEDBACK SHIFT REGISTERS

The DLFSR is LFSR where the feedback taps are changed in running time [19]. As shown in Fig. 4, the conceptual design of a DLFSR is constructed of a main LFSR and an additional unit that controls the moment of time where the feedback taps are modified. The purpose of this design is to produce longer sequences with higher linear complexity than those produced by the LFSR. For doing that, the control unit modifies several feedback parameters. Therefore, the main DLFSR component is the algorithm of switching the polynomial [26].

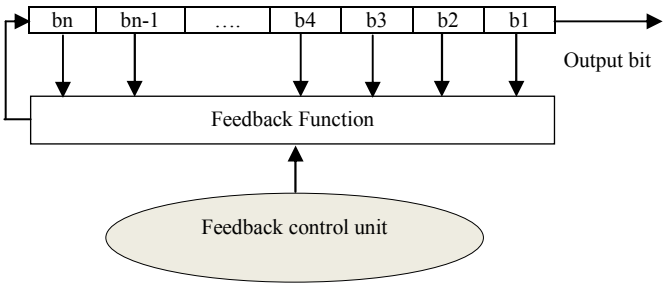

Figure 4. The general construction of a DLFSR.

The dynamic feedback control mechanism converts the deterministic linear recurrence of some registers into a probabilistic recurrence. This effectively protects against several attacks. The attacker has to guess the inputs to the

dynamic feedback control unit first to perform an attack. This guessing is very difficult due to the irregular modification. Therefore, irregular modification of the feedback function improves the security of the stream cipher[13, 14]. There are several DLFSR designs. In the next section, some of these designs are reviewed.

V. Overview of the DLFSR Constructions

In 2002, Mita et al [27] presented a pseudorandom sequence generator based on a DLFSR whose feedback taps are updated based on the state of a secondary LFSR. A predefined set of primitive polynomials are used to exchange the taps. A simple example is presented, and the properties of the output sequence are studied and compared with the output of a conventional LFSR of similar size. The results of the analysis indicate a big improvement in terms of security level for the introduced stream cipher.

In [28], the stream cipher called Mickey was introduced by Babbage and Dodd. It consists of two LFSRs of the same length connected in such a manner that both registers mutually control their corresponding feedbacks.

In 2006, a pseudo-random bit generator was proposed based on dynamically changing the primitive polynomial of a LFSR, controlled by a decoder circuit and a counter that divides the operation time of each polynomial [29]. A specific set of taps are used to change the feedback polynomials. The statistical properties of the proposed and the classical LFSRs are tested using FIPS tests. The results show that both generators have similar randomness and statistical properties. In addition, a methodology, based on a multiperceptron neural network is used. The results show that the proposed generator has an excellent inviolability property (the attribute of being secured against violation).

In the same year, Horant and Guinee [12] introduced a stream cipher construction that is based on the A5/1 cipher majority voting function. The proposed generator structure consists of five LFSRs that are connected to a Dynamic Feedback Polynomial switching block. Each LFSR has a clocking tap that controls its clock and polynomial switching time. When a LFSR is unclocked, its taps are changed. Each register has a set of five feedback polynomials that are used to change its taps. The results indicate that the proposed generator has excellent statistical properties via both the NIST and Diehard test suites.

In 2007, Kiyomoto et al [14] introduced the stream cipher K2. It relies on two LFSRs and a non-linear function. The feedback polynomial of the main LFSR is controlled by two bits of the secondary LFSR state. Therefore, four polynomials are selected to change the taps. The NIST test suite is used to evaluate the statistical properties of the generated sequence and the results confirmed that these properties are good.

In 2008, a DLFSR construction, which had an algorithm to generate irreducible polynomials, was introduced by Molina-Rueda et al [18]. A number of irreducible polynomials are generated in the initialization stage by Blum Blum Shub generator [30]. Then, the generated polynomials are scrambled in a pseudorandom way in order to increase the unpredictability. The proposed generator is implemented in software as a test of the viability. The average speed of this generator after the setup phase is 100bit/sec.

The Rakaposhi stream cipher was presented in 2009 by Cid et al [11]. It consists of a LFSR, whose feedback polynomial is chosen among four different options controlled by two bits of Non-LFSR state. The output sequence is generated by applying a non-linear function to the output of both registers. The NIST Test Suite is used to evaluate this cipher. The results indicate that the statistical properties of the Rakaposhi output sequence are good.

In 2010, a new version of stream cipher modified SNOW 2.0 based on dynamic feedback was introduced [13]. Dynamic feedback is determined using dynamic number generator function. The analysis and experimental results show that the suggested technique has more resistance against Guess and Determine attacks compared to static feedback based modified SNOW 2.0.

In [10], Bajaj suggested using DLFSR instead of LFSR in the A5/1 stream cipher . Four different feedback polynomials for each LFSR are selected. The feedback polynomials are chosen such that there would be only one tap that is different in all tap configurations of an LFSR. A LFSR changes its feedback polynomial after it generates twice more bits than its length. The proposed stream cipher passed all the NIST's random tests.

The Heraclitus stream cipher was proposed in 2011 by Colbert et al [31]. The authors used a key dependent structure, whose variable parameters are the number of registers, the length of registers, and the feedback polynomials of the registers. A fixed set of irreducible polynomials (one for each register) and the hash function SHA512 [32] are used to generate the feedback polynomials. The variable parameters are changed every 2^{64} frames of a session.

In 2013, The J3Gen generator was presented by Melià-Seguí et al [16]. Its construction is based on a DLFSR, with a number of feedback polynomials selected by a round robin scheme. The feedback polynomial is changed after a given number of DLFSR cycles. The authors introduced a hardware implementation of J3Gen, and evaluated it regarding nonlinearity of the design, different design parameters, and defining the key-equivalence security.

The authors in [26] used experimental methods to choose the parameters of DLFSR switching algorithm. They compared between the Diehard statistical tests results of the LFSR and DLFSR generators. This comparison confirmed that DLFSR pseudo random sequences have better statistical properties than the conventional ones.

In [33], the authors considered the autocorrelation and the cross-correlation of the generator that proposed by Mita et al [27], and the results showed high correlation. They concluded that Mita's DLFSR output sequences are not appropriate for using in cryptographic or code division multiple access applications.

In 2014, Peninado et al[19] presented a DLFSR model that consisted of two LFSR and a counter .The main LFSR

polynomial is controlled by a counter, whose value depends on the internal state of the secondary LFSR. A comparative analysis of the proposed DLFSR design with other DLFSR designs is performed. The results indicate that the introduced design is better than others in certain aspects.

VI. DISCUSSION

The main DLFSR component is the algorithm of switching the polynomial [26]. It has two parameters: the set of feedback taps which will be used to change the feedback polynomials, and the method of changing these polynomials.

Determining the set of polynomials that will be used to change the feedback function is very important in DLFSRs. While some approaches used a predefined set of primitive polynomials, others used algorithms to generate these polynomials. When a predefined set of primitive polynomials is used, it is usually chosen in a particular way [10, 29], where the primitive polynomials with the lowest number of inner taps are selected in order to decrease the hardware's complexity. Moreover, the biggest set of the selected primitive polynomials having many common taps is selected in order to minimize the number of XOR gates within the feedback control unit. In [13, 18, 31], the approaches used algorithms to generate taps. In the initialization stage , a set of irreducible polynomials are generated instead of the primitive ones in order to reduce the time complexity of generating primitive polynomials that involves factorization of primes [2]. The complexity of the algorithms that are used to generate irreducible polynomials presents an overhead in setting up the cipher but they increase unpredictability. On the other hand, using a predefined set of feedback polynomials provides significant time and implementation efficiencies with the availability of low cost memory on most devices.

Another important consideration is the way of switching the feedback polynomials. There are two methods that can be used to switch the taps: regular and irregular methods. When the taps are changed in a regular manner, they are changed every specific amount of time. For instance, in [29] and [15], a counter was used to equally divides the operation time of each polynomial. In [10], the taps are reset with another one after 2n bits of the sequence. Some approaches used irregular ways to change the feedback bits. In other words, the moment of change is not fixed and usually depends on some bits within the operated registers. For example, in [12] when a LFSR is unclocked , its taps are changed. In [11, 14], the feedback function of the main register is changed according to the value of certain bits in the control register. Using irregular ways to change the feedback bits is more secure than using regular ones, because these ways increase the nonlinearity of the produced sequence.

The last observation is related to the results of the reviewed papers. Several papers indicated that DLFSRs have good statistical properties [11, 12, 14, 26]. Moreover, the authors in [26] found out that the statistical properties of DLFSR are better than the statistical properties of LFSR. Besides, the papers [13, 27, 29] agreed that DLFSR generator sequences have better inviolability property when compared to the LFSR generator sequences. However, the authors in [26, 33] stated that the quality of generated sequences of DLFSR depends on the parameters of this kind of generator. Therefore, there is a need for developing theoretical and experimental methods to optimize the process of choosing the parameters of switching algorithm in the DLFSR design. Table1 illustrates a brief description of the reviewed generators that evaluated their generated sequences using statistical measurement methods.

TABLE1. DESCRIPTION OF THE REVIEWED GENERATORS THAT USED STATISTICAL MEASUREMENT METHODS TO VALIDATE THEIR OUTPUT.

Generator	Feedback polynomials	Polynomial changing method	Statistical measurement method	Results
Mita et al's generator [27]	Predefined	Regular	FIPS	Excellent
Mita et al's generator [29]	Predefined	Regular	FIPS	Pass
Horant and Guinee's generator [12]	Predefined	Irregular	NIST Diehard	Excellent
K2 [14]	Predefined	Irregular	NIST	Good
Rakaposhi [11]	Predefined	Irregular	NIST	Good
Bajaj's generator [10]	Predefined	Regular	NIST	Pass

VII. CONCLUSION AND FUTURE WORK

The DLFSR is a promising concept in strengthening the security of stream cipher. In this paper, several DLFSR constructions are reviewed, and their polynomial switching algorithms are studied. Based on our observations, the polynomial switching algorithms include predefined or generated sets of polynomials, and the changing process can be done in regular or irregular manner. The pros and cons of each method are discussed.

There are evidences that DLFSR generator sequences have better inviolability and statistical properties when compared to the LFSR generator sequences [13, 26, 27]. However, good inviolability and statistical properties of the DLFSR generator can be achieved when the parameters of switching algorithm are correctly chosen [26, 33]. Hence, developing theoretical and experimental methods for choosing suitable parameters for these generators is very important, and it will be addressed in our future research.

REFERENCES

[1] B. Preneel, C. Paar, and J. Pelzl, Understanding cryptography: a textbook for students and practitioners: Springer, 2009.

[2] B. Schneier, Applied cryptography: protocols, algorithms, and source code in C, 1996.

[3] N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in Advances in Cryptology—EUROCRYPT 2003, ed: Springer, 2003, pp. 345-359.

[4] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," Journal of Cryptology, vol. 1, pp. 159-176, 1989.

[5] A. Klein, "Non-linear Combinations of LFSRs," in Stream Ciphers, ed: Springer London, 2013, pp. 59-89.

[6] V. S. Pendluri, P. Gupta, and R. Majumdar, "Design and implementation of keystream generator with improved security," in Advanced Communication Technology (ICACT), 2011 13th International Conference on, 2011, pp. 1626-1631.

[7] F. Masoodi, S. Alam, and M. Bokhari, "An Analysis of Linear Feedback Shift Registers in Stream Ciphers," International Journal of Computer Applications, vol. 46, pp. 46-49, 2012.

[8] A. Kanso, "Clock-controlled shrinking generator of feedback shift registers," in Information Security and Privacy, 2003, pp. 443-451.

[9] S. Babbage and M. Dodd, "The MICKEY stream ciphers," in New Stream Cipher Designs, ed: Springer, 2008, pp. 191-209.

[10] N. Bajaj, "Enhancement of A5/1: Using variable feedback polynomials of LFSR," in Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on, 2011, pp. 55-60.

[11] C. Cid, S. Kiyomoto, and J. Kurihara, "The rakaposhi stream cipher," in Information and Communications Security, ed: Springer, 2009, pp. 32-46.

[12] D. Horan and R. Guinee, "A novel keystream generator using pseudo random binary sequences for cryptographic applications," 2006.

[13] S. Khan, A. Khan, S. Khayal, T. Naz, S. Bashir, and F. Khan, "Dynamic feedback based modified SNOW 2.0," in Emerging Technologies (ICET), 2010 6th International Conference on, 2010, pp. 250-255.

[14] S. Kiyomoto, T. Tanaka, and K. Sakurai, "K2: A Stream Cipher Algorithm using Dynamic Feedback Control," in SECRYPT, 2007, pp. 204-213.

[15] F. Maqsood, O. Farooq, and W. Ahmad, "LFSR and PLA based complex code generator for stream cipher," in Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT'09. International, 2009, pp. 268-271.

[16] J. Melià-Seguí, J. Garcia-Alfaro, and J. Herrera-Joancomartí, "J3Gen: A PRNG for low-cost passive RFID," Sensors, vol. 13, pp. 3816-3830, 2013.

[17] R. Mita, G. Palumbo, S. Pennisi, and M. Poli, "A novel pseudo random bit generator for cryptography applications," in Electronics, Circuits and Systems, 2002. 9th International Conference on, 2002, pp. 489-492.

[18] A. Molina-Rueda, F. Uceda-Ponga, and C. F. Uribe, "Extended period LFSR using variable TAP function," in Electronics, Communications and Computers, 2008. CONIELECOMP 2008, 18th International Conference on, 2008, pp. 129-132.

[19] A. Peinado, J. Munilla, and A. Fúster-Sabater, "Improving the Period and Linear Span of the Sequences Generated by DLFSRs," in International Joint Conference SOCO'14-CISIS'14-ICEUTE'14, 2014, pp. 397-406.

[20] C. S. Lamba, "Design and analysis of Stream Cipher for Network security," in Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, 2010, pp. 562-567.

[21] P. FIPS, "140-2: Security requirements for cryptographic modules," National Institute of Standards and Technology, 2001.

[22] G. Marsaglia, "DIEHARD statistical tests," Florida state university,(http://www. stat. fsu. edu/pub/diehard/), 1995.

[23] A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, et al., "Statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST special publication," 2010.

[24] A. A. Kanso, "Encryption system with variable number of registers," Computers & electrical engineering, vol. 36, pp. 199-212, 2010.

[25] P. Deepthi, D. S. John, and P. Sathidevi, "Design and analysis of a highly secure stream cipher based on linear feedback shift register," Computers & Electrical Engineering, vol. 35, pp. 235-243, 2009.

[26] R. Stepien and J. Walczak, "Comparative analysis of pseudo random signals of the LFSR and DLFSR generators," in Mixed Design of Integrated Circuits and Systems (MIXDES), 2013 Proceedings of the 20th International Conference, 2013, pp. 598-602.

[27] R. Mita, G. Palumbo, S. Pennisi, and M. Poli, "Pseudorandom bit generator based on dynamic linear feedback topology," Electronics Letters, vol. 38, pp. 1097-1098, 2002.

[28] S. Babbage and M. Dodd, "The stream cipher MICKEY (version 1)," ECRYPT Stream Cipher Project Report, vol. 15, p. 2005, 2005.

[29] R. Mita, G. Palumbo, and M. Poli, "Pseudo-random sequence generators with improved inviolability performance," IEE Proceedings-Circuits, Devices and Systems, vol. 153, pp. 375-382, 2006.

[30] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," SIAM Journal on computing, vol. 15, pp. 364-383, 1986.

[31] B. Colbert, A. H. Dekker, and L. M. Batten, "Heraclitus: A LFSR-based stream cipher with key dependent structure," in Communications and Signal Processing (ICCSP), 2011 International Conference on, 2011, pp. 141-145.

[32] I. F. Al-shaikhli, M. A. Alahmad, and K. Munthir, "Hash Function of Finalist SHA-3: Analysis Study," Information Technology (IJACSIT), vol. 2, 2013.

[33] A. Peinado and A. Fúster-Sabater, "Generation of pseudorandom binary sequences by means of linear feedback shift registers (LFSRs) with dynamic feedback," Mathematical and Computer Modelling, vol. 57, pp. 2596-2604, 2013.