New NLFSR Functions of Degree 3 with Optimal Periods

Ibraheem Al-Hejri and Sultan Almuhammadi
College of Computer Sciences and Engineering,
King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia
Emails: alhejri87@gmail.com, muhamadi@kfupm.edu.sa

***Abstract*—Feedback shift registers are common components typically used to generate pseudorandom sequences of bits which are essential in many security applications. Network security relies on the security of its components. Nonlinear feedback shift registers (NLFSRs) are known to be more secure than the linear ones. However, there is no mathematical foundation on how to construct NLFSR feedback functions with optimal periods. In this paper, we consider a new type of NLFSR functions of degree 3. Using our construction method, we propose 140 new functions of this type with optimal periods.**

***Index Terms*—NLFSR, Pseudorandom, Feedback Functions, Optimal Period.**

I. Introduction

Pseudorandom generators play a major role in network security. Examples include authentication [1], [2], error detection and correction [3], and data compression [4]. Several network protocols require the property of randomness to ensure security. For example, random numbers are used in generating the keys for public key encryption and digital signature algorithms. They are also used in symmetric key generation for session keys which are used in several network applications such as Transport Layer Security (TLS) protocol, Wi-Fi, E-mail security and Internet Protocol (IP) security. Moreover, random numbers are used in key distribution protocols, such as Kerberos protocol, and initialization values (IVs) for handshaking in order to prevent replay attacks [5], [6].

One of the most common and efficient ways to generate pseudorandom sequences is using feedback shift register (FSR). The general structure of an n-bit FSR is shown in Fig. 1, and it will be explained more formally in Section II.

A feedback shift register can be either linear (LFSR) or nonlinear (NLFSR) based on its internal feedback function. The LFSRs have been well-studied in the literature since 1960s [7], and most of the LFSR fundamental problems have been solved [8]. To find a feedback function with an optimal period for an LFSR of size n bits, we only need to use a primitive generator polynomial. On the other hand, the area of NLFSR has many problems that remain open. For example, there is no mathematical method to show how an NLFSR function with an optimal period can be constructed.

The state in an LFSR is linearly computed from the previous state, while the state in NLFSR is a non-linear transformation of the previous state [9]. This is a very important feature that gives an NLFSR its ability to produce a very secure pseudorandom sequence which is hard to break compared to the LFSR. Thus, to attack an NLFSR based on its output, at least $\Theta(2^n)$ sequence bits are needed to determine its internal structure, where n is the register size [10]. However, only $2n$ bits are sufficient to attack an LFSR of the same size.

Moreover, the degree of the function plays an important rule in the security of the output sequence and its ability to resist potential attacks. The higher the degree the function is, the more secure output bit sequence it produces. Which makes it more resistant to known attacks that target its order.

In this paper, we propose a new type of feedback functions of degree 3 with optimal periods. We used our construction method in [11] to construct 140 functions of this type for NLFSRs of sizes $5 \leq n \leq 25$. The rest of the paper is organized as follows. Section II presents the structures of feedback shift registers and related definitions. Section III reviews the related work. Section IV describes the construction and presents the new feedback functions with some useful remarks. Finally, the conclusion comes in Section V with some future work directions.

II. Preliminaries

An FSR consists of a shift-register to store the state, and a function to compute the feedback bit. The register has n binary storage cells, each cell $i \in \{0, 1, \ldots, n-1\}$ holds a single bit x_i in the state register. The feedback function $f : \{0,1\}^n \rightarrow \{0,1\}$ computes a feedback bit used as an input to the register to update the state using a shift operation.

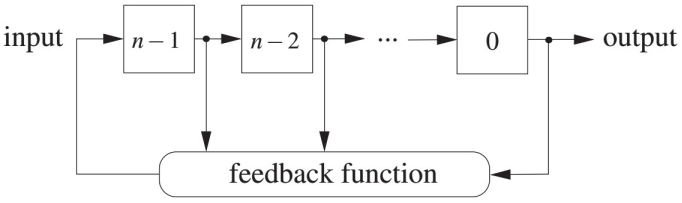

Fig. 1: An n-bit FSR general structure [8]

A vector of bits $X = (x_0, x_1, \ldots, x_{n-1})$ represents the state in feedback shift registers. The pseudorandom sequence of bits is generated by extracting the bits one-by-one from the shift-register. The initial state X_0 is a seed used to generate the output sequence of bits. From the current state, the feedback function computes x_n, which is the input to the FSR and it

updates the input cell $(n-1)$, while the value x_0 of the cell 0 determines the output of the FSR.

Due to the limitation of register size, n, there will be a repeated state eventually (when all the 2^n states are exhausted). The *period* of the FSR is defined as the length of the longest unrepeated output sequence. Let us now proceed formally.

Definition 1: Let $\mathbb{F}_2$ be the binary finite field and $\mathbb{F}_2[x]$ represent the ring of polynomials in undefined value of x with coefficients taken from $\mathbb{F}_2$. Assume that, $\mathbb{F}_2^n$ is an n-dimensional vector space over $\mathbb{F}_2$ which consists of n-tuples of $\mathbb{F}_2$ elements. Each function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is represented by a Boolean function of n variables. The elements sequence $s = (s_0, s_1, \dots)$ of $\mathbb{F}_2$ is known as a binary sequence. The sequence $s = (s_i)_{i=0}^{\infty}$ is *periodic* when there is a positive integer w such that $s_{i+w} = s_i, \forall i \geq 0$. The least such positive integer is called a *period*.

In a binary n-stage FSR, $\mathbb{F}_2^n$ is mapped into $\mathbb{F}_2^n$ as shown below, where F is the mapping function:

$$F(x_0, x_1, \dots, x_{n-1}) = ((x_1, \dots, x_{n-1}, f(x_0, x_1, \dots, x_{n-1}))$$

The feedback function is the Boolean function f over n-variables. If F is a linear transformation from $\mathbb{F}_2^n$ to itself, it is called a *linear feedback shift register* (LFSR), otherwise it is called a *nonlinear feedback shift register* (NLFSR). Moreover, if the function F is mapped as a bijection, it is called *non-singular* [12].

LFSRs have feedback functions of the following type:

$$f(x_0, x_1, \dots, x_{n-1}) = c_0 \cdot x_0 \oplus c_1 \cdot x_1 \oplus \dots c_{n-1} \cdot x_{n-1}$$

where $c_i \in \{0, 1\}$ for $i \in \{0, 1, \dots, n-1\}$). All terms in an LFSR are linear, like $(c_i \cdot x_i)$. However, NLFSRs include nonlinear terms. For example, an NLFSR of degree 2 includes at least one term of the form $(x_i \cdot x_j)$, where $i \neq j$.

Definition 2: The sequence of de Bruijn $(a_0, \dots, a_{2^n-1})$ of order n which consists of elements from $\mathbb{F}_2$ has a period of 2^n where each n-tuples appears exactly once.

Sainte-Marie [13] and de Bruijn [14] show that the number of sequences which are cyclic equivalent is given by:

$$B_n = 2^{2^{n-1}-n} \tag{1}$$

Definition 3: The modified version of de Bruijn sequence $(a_0, ..., a_{2^n-2})$ of order n is a sequence which has a period of 2^{n-1}.

In FSR, the all-zeroes state $(X = 0)$ should not be allowed at any given point, or otherwise the FSR will remain locked up at this state. If $X = 0$, then $f(X) = 0$ for all new states. Hence, the sequence s will be all zeros. Therefore, the maximum period of an FSR of size n is at most $2^n - 1$. It is important to include the output bit x_0 in the feedback function to maximize the period. Hence, the FSR can take the following form:

$$f(x_0, x_1, \dots, x_{n-1}) = x_0 + g(x_1, x_2, \dots, x_{n-1}) \tag{2}$$

Where g denotes to a Boolean function on $n-1$ variables.

Mayhew and Golomb [14] investigated sequences satisfying Definition 3. Gammel et al. [15] called these sequences primitive. In LFSRs, these sequences can be produced using primitive polynomials and the theory of such sequences is well-understood [16].

The primitive sequence is a significant factor in the applications of cryptography. The number of primitive sequences jointly (in linear and nonlinear functions) is given by B_n in (1). We have $\phi(2^{n-1})/n$ primitive LFSRs, where ϕ refers to the Euler phi function. Since we have $2^{2^{n-1}}$ Boolean functions on $n-1$ variables, the probability of selecting a primitive NLFSR function of the form in (4) is given by:

$$\frac{(2^{2^{n-1}-n})}{2^{2^{n-1}}} = \frac{1}{2^n} \tag{3}$$

Thus, there are more NLFSRs than LFSRs [12].

Berlekamp-Massey algorithm [17] can be used to generate a given binary sequence of a minimal LFSR. Golomb's postulates [18] have characterized the properties of sequences created by LFSRs statistically.

An NLFSR can be implemented using either Fibonacci or Galois configuration. The Fibonacci configuration applies the feedback only to the input cell $(n-1)$ of the shift register as shown in Fig. 1, while the Galois configuration can potentially apply the feedback to any cell. Fig. 2 shows a 4-bit Fibonacci NLFSR with its feedback function $f(x_0, x_1, x_2, x_3) = x_0 \oplus x_1 \oplus x_2 \oplus x_1 \cdot x_2$.

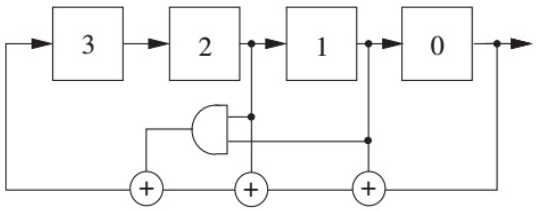

Fig. 2: A 4-bit Fibonacci NLFSR example. [8]

In LFSR system, there is a unique transformation between the configurations of Galois and Fibonacci. Therefore, we can reverse the order of LFSRs feedback taps and adjust the initial state to get the configuration of Galois from Fibonacci (or vice versa). In contrast, the NLFSR system does not have a unique transformation between Fibonacci and Galois configurations [19]–[21].

III. Related Work

Non-linear feedback shift register functions have been in the focus of many researchers. However, much of the work is either limited to particular cases [22], [23], or to a subset of functions for particular values of n (like $n = 1$, 3, 4, 11-13, 15-17, 19-21, 23, 31-33) [24]. The NLFSR problem in general is very hard due to the lack of the mathematical foundation on how to construct the feedback functions that give optimal periods.

Dubrova [8] presented Fibonacci NLFSR feedback functions of degree 2, with optimal periods of $2^n - 1$, for $4 \leq n \leq 25$, in the following three types:

- $f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \oplus x_c \cdot x_d$
- $f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \cdot x_c \oplus x_d \cdot x_e$
- $f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \oplus x_c \oplus x_d \oplus x_e \cdot x_h$

where $a, b, c, d, e, h \in \{1, 2, \ldots, n-1\}$, $x_i \in \{0, 1\}$, and the addition (XOR) and multiplication (AND) operations are in modulo 2. However, Dubrova's work did not list all the feedback functions having optimal periods. In addition, the author reported in [25] some NLFSR feedback functions with maximum periods of the following type:

$$f_4(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \oplus x_c \cdot x_d \cdot x_e \quad (4)$$

where $a, b, c, d, e \in \{1, 2, \ldots, n-1\}$, $x_i \in \{0, 1\}$, and the addition and multiplication operations are in modulo 2. This type is of degree 3 and, therefore, the feedback functions of this types are more secure than the ones in the previous three types. However, the list in [25] is incomplete, and many feedback functions are missing. The author gave no feedback functions with optimal periods for the sizes $n = 10, 21, 23$ and 24 of the type in Equation (4).

Mandal and Gong [26] proposed NLFSRs with optimal period to generate de Bruijn sequences of order $n = 23, 24$ and 27. In [27] they defined a relation between an NLFSR and a regular directed graph on a field extension, known as de Bruijn graph [28].

Poluyanenko [29] proposed an approach based on field-programmable gate arrays (FPGA). This approach proved the ability of FPGAs to generate NLFSR-based sequences of large sizes. The author successfully generated some sequences for sizes $n = 26, 27, 28$ and 29, without providing any complete list of these sizes.

Almuhammadi et al. [11] proposed an efficient construction method. The authors used this method to construct the missing NLFSR feedback functions of the three types given in [8]. They presented complete lists of these types for all sizes $n = 4, 5, \ldots, 19$. These functions were of degree 2.

IV. Construction of the Feedback Functions

In this work, we use a construction method similar to the one we introduced in [11]. It is an efficient sequential NLFSR function construction, which sequentially enumerates all feedback functions of a given type. Then, the period is computed for each feedback function and its optimality is verified. This section explains the construction method and the new type considered in this work. Then it shows the proposed feedback functions and summarizes the results.

A. The Construction Method

The construction method consists of two parts:

1) *Sequential Function Generator*: which is an enumeration of the feedback functions.
2) *Period-Testing Algorithm*: which tests whether the generated function f has an optimal period of $2^n - 1$ or not.

The sequential function generator enumerates the feedback functions by incrementing the subscripts of the variables in a given feedback function. Then, the period-testing algorithm examines the generated function and computes its period by monitoring all the states until the initial state appears again. If the period of the function is $2^n - 1$, the construction method reports it as a feedback function with an optimal period. Otherwise, it is ignored, and a new function is generated and tested. The reader may refer to [11] for more details about this method and its proof of correctness.

B. The Type of the Feedback Functions

We consider a new type of NLFSR feedback functions of degree 3 defined in Equation (4).

In general, feedback functions of degree 3 have more non-linearity than those of degree 2 of the same size. Our goal is to generate a complete list of NLFSR feedback functions of degree 3 instead of the ones of degree 2 we presented in [11]. The degree of the feedback function is an essential factor in the security of the NLFSR. Higher degree increases the non-linearity of the feedback function, which makes it more resistant to potential attacks [30], [31]. For example, any Boolean function of low algebraic order can be evaluated in terms of a relatively low number of coefficients in its Algebraic Normal Form (ANF) even if the number of input variables is large. This is known as the low-order approximation attack [32]. Therefore, the higher the algebraic degree of a non-linear function is, the more difficult it is to approximate it with a vectorial Boolean function of low degree.

C. The Proposed Feedback Functions

The proposed feedback functions of this type are listed in Table I. Each entry in this table is of the form $n\ (0, a, b, c, d, e)$, where n is the size of the function, and a, b, c, d and e are the indices of the variables in Equation (4). If a constructed function is equivalent to an existing one, it will not be included in this list. Thus, the feedback functions listed here are pairwise nonequivalent, and different from the existing ones for this type.

D. Results Summary and Remarks

This paper completes the work in [25] by constructing all missing feedback functions with optimal periods for all sizes $n = 5, 6, ..., 25$ of this type. Using our construction method, we obtained 140 new NLFSR feedback functions with optimal periods of this type for $n = 5, 6, \ldots 25$. However, no new functions were found for $n = 21$, 23 or 24.

Table II shows the number of functions of this type for each size of $n = 5, 6, \ldots 25$. The table shows that we increase the number of the existing functions in [25] by the double for almost all values of n, where $5 \leq n \leq 25$. The proposed functions are nonequivalent to the existing ones (and nonequivalent pairwise). Moreover, there are no existing feedback functions of size $n = 10$, but we managed to construct 13 new functions for $n = 10$. The total number of all functions of this type has been improved from 127 to 267 functions. Finally, it is important to note that more research is still needed to come up with new types capable of producing more feedback functions with optimal periods.

TABLE I: Proposed NLFSR feedback functions

5 $(0,2,4,1,2,3)$	10 $(0,8,9,4,5,9)$
5 $(0,2,4,1,2,4)$	10 $(0,8,9,6,8,9)$
5 $(0,2,4,1,3,4)$	11 $(0,2,10,3,8,10)$
5 $(0,2,4,2,3,4)$	11 $(0,4,8,1,7,10)$
6 $(0,3,4,1,3,5)$	11 $(0,4,10,1,2,10)$
6 $(0,3,4,2,3,4)$	11 $(0,4,10,3,4,7)$
6 $(0,3,4,2,3,5)$	11 $(0,4,10,3,5,6)$
6 $(0,3,4,2,4,5)$	11 $(0,4,10,4,6,9)$
6 $(0,4,5,1,2,4)$	11 $(0,5,7,1,3,4)$
6 $(0,4,5,1,2,5)$	11 $(0,5,7,4,7,9)$
6 $(0,4,5,2,3,4)$	11 $(0,7,9,1,3,8)$
6 $(0,4,5,2,4,5)$	11 $(0,7,9,2,3,4)$
7 $(0,2,6,1,3,5)$	11 $(0,7,9,2,3,9)$
7 $(0,2,6,1,3,6)$	11 $(0,7,9,4,9,10)$
7 $(0,2,6,1,4,5)$	11 $(0,7,10,2,6,10)$
7 $(0,3,5,1,2,3)$	11 $(0,8,10,2,8,9)$
7 $(0,3,5,1,2,5)$	11 $(0,8,10,6,7,10)$
7 $(0,3,5,1,3,4)$	12 $(0,3,10,1,5,6)$
7 $(0,3,5,1,4,6)$	12 $(0,3,10,2,3,5)$
7 $(0,3,5,2,4,5)$	12 $(0,3,10,4,7,11)$
7 $(0,3,5,2,4,6)$	12 $(0,4,9,1,4,11)$
7 $(0,3,5,3,5,6)$	12 $(0,4,11,2,4,11)$
7 $(0,3,6,2,4,6)$	12 $(0,6,7,4,7,10)$
8 $(0,2,7,1,2,7)$	12 $(0,6,11,1,2,5)$
8 $(0,2,7,2,3,5)$	12 $(0,6,11,5,7,10)$
8 $(0,2,7,2,3,7)$	12 $(0,6,11,6,7,10)$
8 $(0,2,7,2,4,5)$	12 $(0,6,11,6,7,11)$
8 $(0,2,7,2,5,6)$	12 $(0,7,8,1,2,8)$
8 $(0,2,7,2,6,7)$	12 $(0,7,8,2,3,4)$
8 $(0,2,7,3,4,7)$	12 $(0,7,8,5,8,11)$
8 $(0,4,5,2,5,7)$	12 $(0,8,9,4,5,11)$
8 $(0,4,5,3,4,7)$	12 $(0,9,10,3,7,11)$
8 $(0,4,5,4,5,7)$	12 $(0,9,11,3,5,11)$
8 $(0,4,7,1,3,7)$	12 $(0,10,11,2,3,10)$
8 $(0,4,7,1,4,5)$	13 $(0,5,11,1,3,5)$
8 $(0,4,7,1,6,7)$	13 $(0,6,10,1,4,7)$
8 $(0,4,7,2,4,6)$	13 $(0,6,12,2,8,12)$
8 $(0,4,7,3,4,5)$	13 $(0,6,12,3,4,10)$
8 $(0,4,7,4,6,7)$	13 $(0,6,12,7,8,9)$
8 $(0,6,7,1,2,3)$	13 $(0,8,12,1,2,10)$
8 $(0,6,7,1,5,6)$	13 $(0,11,12,3,5,7)$
8 $(0,6,7,2,3,4)$	14 $(0,2,13,3,7,9)$
8 $(0,6,7,2,3,6)$	14 $(0,4,13,10,11,13)$
8 $(0,6,7,3,6,7)$	14 $(0,5,10,9,11,12)$
8 $(0,6,7,4,5,6)$	14 $(0,5,10,9,12,13)$
9 $(0,3,7,2,3,8)$	14 $(0,6,9,2,3,13)$
9 $(0,3,7,3,7,8)$	14 $(0,6,9,5,6,13)$
9 $(0,3,7,4,5,6)$	14 $(0,7,10,2,6,12)$
9 $(0,4,6,1,2,5)$	14 $(0,7,10,4,6,10)$
9 $(0,4,6,1,7,8)$	14 $(0,8,11,5,6,10)$
9 $(0,4,6,2,5,6)$	14 $(0,8,11,6,12,13)$
9 $(0,4,6,3,4,5)$	14 $(0,12,13,6,10,12)$
9 $(0,4,6,4,5,6)$	15 $(0,5,13,8,9,10)$
9 $(0,4,6,4,5,8)$	15 $(0,7,9,2,3,12)$
9 $(0,5,7,1,3,4)$	15 $(0,7,11,2,6,7)$
9 $(0,5,7,4,7,8)$	15 $(0,12,14,2,3,8)$
9 $(0,6,8,1,2,8)$	16 $(0,8,9,2,4,11)$
9 $(0,6,8,1,3,5)$	16 $(0,8,9,6,8,10)$
9 $(0,6,8,3,6,7)$	16 $(0,8,15,5,8,9)$
10 $(0,2,9,1,2,5)$	17 $(0,10,13,2,14,16)$
10 $(0,4,8,1,5,9)$	18 $(0,9,16,1,12,13)$
10 $(0,5,8,1,3,4)$	18 $(0,10,11,6,8,9)$
10 $(0,5,8,3,6,8)$	18 $(0,10,17,3,6,8)$
10 $(0,5,8,6,8,9)$	19 $(0,8,13,2,10,14)$
10 $(0,5,9,2,4,6)$	19 $(0,9,11,7,12,16)$
10 $(0,6,9,1,2,6)$	19 $(0,9,17,6,11,14)$
10 $(0,6,9,1,5,7)$	20 $(0,6,15,9,10,17)$
10 $(0,6,9,4,8,9)$	20 $(0,12,13,8,12,17)$
10 $(0,7,8,2,5,7)$	22 $(0,16,17,12,17,20)$
10 $(0,8,9,1,4,9)$	25 $(0,9,21,2,4,24)$

TABLE II: Number of feedback functions of size n

n	Existing	Proposed	Sum
5	4	4	8
6	8	8	16
7	11	11	22
8	22	22	44
9	14	14	28
10	-	13	13
11	15	15	30
12	17	17	34
13	7	7	14
14	11	11	22
15	4	4	8
16	3	3	6
17	1	1	2
18	3	3	6
19	3	3	6
20	2	2	4
21	-	-	-
22	1	1	2
23	-	-	-
24	-	-	-
25	1	1	2
Total	127	140	267

V. Conclusion and Future Work

In this paper, we extended the study done by Dubrova and provided a complete list of all the NLFSR feedback functions with optimal periods of a degree 3 type. These functions are of sizes ranges from $n = 5$ through 25. There were 127 existing feedback functions of this type. However, our construction method found 140 more new functions of this type, and brought the total to 267 functions. Degree 3 feedback functions make the NLFSR output more secure pseudorandom bit sequences capable of resisting the low-order approximation attack.

This work can be further extended for future work in the following directions:

- Constructing feedback functions with larger values of n.
- Exploring new types of feedback functions of degree 3 and higher.
- Searching for types that yields more functions with optimal periods.
- Providing complete lists of NLFSR feedback functions with optimal periods for these types and sizes.

These directions will enrich the field of NLFSR and provide network security designers with more secure alternatives for pseudorandom bit generators.

Acknowledgment

The authors would like to thank King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, for supporting this research. Figures and descriptions in this paper were provided by the authors and are used with permission.

REFERENCES

[1] L. Zhou and S. Chakrabartty, "Secure dynamic authentication of passive assets and passive iots using self-powered timers," in *Circuits and Systems (ISCAS), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 1–4.

[2] D. Upadhyay, P. Sharma, and S. Sampalli, "Enhancement of GSM stream cipher security using variable taps mechanism and nonlinear combination functions on linear feedback shift registers," in *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2*. Springer, 2016, pp. 175–183.

[3] J. McCluskey, "High speed calculation of cyclic redundancy codes," in *Proceedings of the 1999 ACM/SIGDA seventh international symposium on Field programmable gate arrays*. ACM, 1999, p. 250.

[4] G. Mrugalski, J. Rajski, and J. Tyszer, "Ring generators-new devices for embedded test applications," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 23, no. 9, pp. 1306–1320, 2004.

[5] B. A. Forouzan and D. Mukhopadhyay, *Cryptography and network security (Sie)*. McGraw-Hill Education, 2011.

[6] W. Stallings, *Network Security Essentials: Applications and Standards*. Pearson, 2016.

[7] S. W. Golomb *et al.*, *Shift register sequences*. Aegean Park Press, 1967.

[8] E. Dubrova, "A list of maximum-period nlfsrs," 2012.

[9] C. J. A. Jansen, "Investigations on nonlinear streamcipher systems: construction and evaluation methods," 1989.

[10] E. Dubrova, "Generation of full cycles by a composition of nlfsrs," *Designs, codes and cryptography*, vol. 73, no. 2, pp. 469–486, 2014.

[11] S. Almuhammadi, I. Al-Hejri, G. B. Talib, and A. Gaamel, "Nlfsr functions with optimal periods," in *International Conference on Computational Science and Its Applications*. Springer, 2018, pp. 67–79.

[12] T. Rachwalik, J. Szmidt, R. Wicik, and J. Zabłocki, "Generation of nonlinear feedback shift registers with special-purpose hardware," in *Communications and Information Systems Conference (MCC), 2012 Military*. IEEE, 2012, pp. 1–4.

[13] C. F. Sainte-Marie, "Solution to question nr. 48," *L'intermédiaire des Mathématiciens*, vol. 1, pp. 107–110, 1894.

[14] G. L. Mayhew and S. W. Golomb, "Linear spans of modified de bruijn sequences," *IEEE transactions on information theory*, vol. 36, no. 5, pp. 1166–1167, 1990.

[15] B. M. Gammel, R. Göttfert, and O. Kniffler, "The achterbahn stream cipher," *Submission to eSTREAM*, 2005.

[16] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*. Cambridge university press, 1994.

[17] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[18] S. Golomb, "Shift register sequences. laguna hills, ca aegean," 1982.

[19] E. Dubrova, "A transformation from the fibonacci to the galois nlfsrs," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 5263–5271, 2009.

[20] J.-M. Chabloz, S. S. Mansouri, and E. Dubrova, "An algorithm for constructing a fastest galois nlfsr generating a given sequence." in *SETA*. Springer, 2010, pp. 41–54.

[21] E. Dubrova, "Finding matching initial states for equivalent nlfsrs in the fibonacci and the galois configurations," *IEEE transactions on information theory*, vol. 56, no. 6, pp. 2961–2966, 2010.

[22] M. Liu, S. S. Mansouri, and E. Dubrova, "A faster shift register alternative to filter generators," in *Digital System Design (DSD), 2013 Euromicro Conference on*. IEEE, 2013, pp. 713–718.

[23] A. Castro Lechtaler, M. Cipriano, E. García, J. Liporace, A. Maiorano, and E. Malvacio, "Model design for a reduced variant of a trivium type stream cipher," *Journal of Computer Science & Technology*, vol. 14, 2014.

[24] H. Fredricksen, "A survey of full length nonlinear shift register cycle algorithms," *SIAM review*, vol. 24, no. 2, pp. 195–221, 1982.

[25] "Maximum period nlfsrs," https://people.kth.se/~dubrova/nlfsr.html, Accessed on January 26, 2019.

[26] K. Mandal and G. Gong, "Cryptographic d-morphic analysis and fast implementations of composited de bruijn sequences," Technical Report CACR 2012-27, University of Waterloo, Tech. Rep., 2012.

[27] K. Mandal and G. Gong, "Probabilistic generation of good span n sequences from nonlinear feedback shift registers," *University of Waterloo*, 2012.

[28] I. J. Good, "Normal recurring decimals," *Journal of the London Mathematical Society*, vol. 1, no. 3, pp. 167–169, 1946.

[29] N. Poluyanenko, "Development of the search method for non-linear shift registers using hardware, implemented on field programmable gate arrays," *EUREKA: Physics and Engineering*, no. 1, pp. 53–60, 2017.

[30] B. Amaral, S. Darachev, M. Ludvigsson, R. Molazem, and A. M. Casanova, "S-box analysis."

[31] G. Ivanov, N. Nikolov, and S. Nikova, "Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties," *Cryptography and Communications*, vol. 8, no. 2, pp. 247–276, 2016.

[32] W. Millan, "Low order approximation of cipher functions," in *Cryptography: Policy and Algorithms*. Springer, 1996, pp. 144–155.