The Transformation from the Galois NLFSR to the Fibonacci Configuration

Lin Zhiqiang

College of Mathematics and Information Science, Guangzhou University,
Guangzhou 510006, China
linzhiqiang0824@yahoo.cn

Abstract. The Galois configuration of Nonlinear Feedback Shift Registers (NLFSRs) is attractive for stream ciphers for which high throughput is very important. In this paper, we prove that any Galois NLFSR can be transformed into an equivalent NLFSR in the Fibonacci configuration, which is the conventional configuration of NLFSRs. The transformation is mentioned in the proof. The mapping between the initial states of the Galois NLFSR and its equivalent Fibonacci configuration is also derived. Moreover, some properties of Galois NLFSRs are presented.

Keywords: Fibonacci NLFSR, Galois NLFSR, pseudo-random sequence, initial state, stream cipher

1 Introduction

Linear Feedback Shift Registers (LFSRs) are one of the most popular devices for generating pseudo-random sequences [1]. They are simple, fast, and easy to implement in software and hardware. LFSRs are widely used in many applications such as error correcting codes, test pattern generation and symmetric cryptography. The main disadvantage is that in a LFSR, the current state is a linear function of the previous state, thus cryptographically insecure. As an alternative, an Nonlinear Feedback Shift Register (NLFSR) whose current state is a nonlinear function of its previous state can be used [2]. The main application area of NLFSRs at present is cryptography [3]. The output sequences of NLFSRs are normally very hard to break with existing cryptanalytic methods [4,5]. Many NLFSR-based stream ciphers have been designed [6∼10].

The traditional configuration of NLFSRs is the Fibonacci configuration, shown in Fig. 1, which consists of n binary storage elements from left to right as $n-1, n-2, \cdots, 0$ and the feedback is applied to the $n-1$th bit only. Another type of NLFSRs called (n,k)-NLFSRs was introduced in [11]. An (n,k)-NLFSR can be considered as a generalization of the Ring type of LFSR to the nonlinear case [12]. In an (n,k)-NLFSR, the feedback can potentially be applied to every bit. It gives us a potential opportunity to compute each next state function in parallel, thus increasing the speed of output sequence generation. However, (n,k)-NLFSRs have several drawbacks:

1) The period of the output sequence of an (n, k)-NLFSR is not necessarily equal to the length of the longest cyclic sequence of its consecutive states.

2)An output sequence of a (n, k)-NLFSR with the period $2^n - 1$ does not necessarily satisfies the 1st and 2nd postulates of Golomb.

These drawbacks do not create any problems in the Fibonacci configuration [2]. A kind of (n, k)-NLFSRs which is similar to the Galois LFSRs, also called the Galois configuration (Fig.2) has been proposed [13]. It requires that any bit only can return to itself and the left bits of it in this configuration. A mapping between Fibonacci NLFSRs and Galois NLFSRs which satisfies the condition "uniform" has been presented [13,14]. The transformation from a given Fibonacci NLFSR to the equivalent uniform Galois NLFSRs can potentially reduce the depth of the circuits implementing feedback functions, thus decreasing the propagation time and increasing the throughput. A method of finding the fastest equivalent uniform Galois configuration for a given Fibonacci NLFSR has been mentioned in [15].

In [13], the author argued that a Galois NLFSR which does not satisfy the condition "uniform" may or may not has an equivalent Fibonacci configuration. For supporting this arguement, two examples have been presented. However, the one to show the nonexistence is incorrect since it is not a Galois NLFSR. In this paper, we prove that any Galois NLFSR can be equivalent to a Fibonacci configuration, and show the transformation. A method of finding matching initial states between the equivalent NLFSRs is also presented. Some properties of Galois NLFSRs are given by the transformation. These results are useful to analysis Galois NLFSRs.

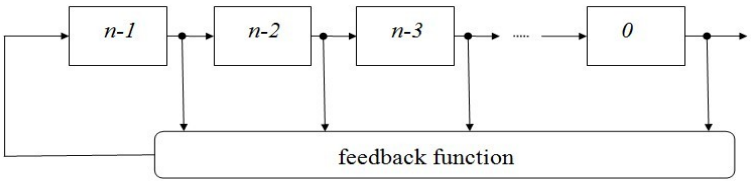

Fig. 1. The Fibonacci configuration of NLFSR

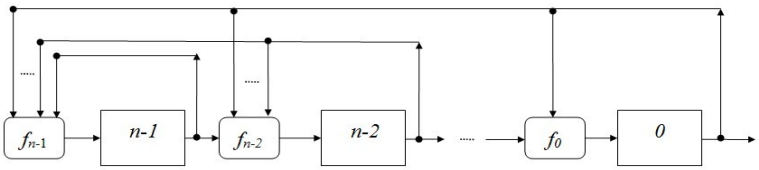

Fig. 2. The Galois configuration of NLFSR

2 Preliminaries

In this section, we describe basic definitions and notation used in this paper.

The algebraic normal form (ANF) of a Boolean function f: $\{0,1\}^n \to \{0,1\}$ is a polynomial in GF(2) of type

$$f(x_0, \cdots, x_{n-1}) = \sum_{i=0}^{2^n-1} c_i \prod_{k=0}^{n-1} x_k^{i_k}$$

where $c_i \in \{0,1\}$ and $(i_0, i_1, \cdots, i_{n-1})$ is the binary expansion of i with i_0 being the least significant bit.

Definition 1. *The dependence set of a Boolean function f is*

$$dep(f) = \{i | f|_{x_i=0} \neq f|_{x_i=1}\}$$

where $f|_{x_i=j} = f(x_0, \cdots, x_{i-1}, j, x_{i+1}, \cdots, x_{n-1})$ for $j \in \{0,1\}$.

Definition 2. *A sequence $s = (s_0, s_1, s_2, \cdots)$ is eventually periodic if there exists two integers $N \geq 0$ and $T > 0$ so that*

$$s_i = s_{i+T}$$

for all $i \geq N$. If $N = 0$, the sequence is called a purely periodic sequence.

An NLFSR consists of n binary storage elements, called bits. The order set of values of these bits is called a state of the NLFSR. We denote a state at time t by $(s_0[t], s_1[t], \cdots, s_{n-1}[t])$. t can be an arbitrary integer since we can take the initial time to a smaller integer. At every clock cycle, the next state is determined from the current state by updating the values of all bits simultaneously to the values of the corresponding feedback functions f_i $(0 \leq i \leq n-1)$. The output of an NLFSR is the value of the 0th bit.

Definition 3. *Two NLFSRs are equivalent if their sets of output sequences are equal.*

All NLFSRs considered in this paper have feedback functions of type

$$f_i(x) = x_{(i+1) \ mod \ n} \oplus g_i(x_0, \cdots, x_i) \quad (0 \leq i \leq n-1) \tag{1}$$

where g_i is a Boolean function.

If for all $0 \leq i \leq n-2$ the feedback function are of type $f_i = x_{i+1}$, we call it the Fibonacci configuration (Fig. 1). Otherwise, we call it the Galois configuration (Fig. 2).

An NLFSR of type (1) can be described by a system of n nonlinear equations:

$$\begin{cases} s_0[t] = s_1[t-1] \oplus g_0(s_0[t-1]) \\ s_1[t] = s_2[t-1] \oplus g_1(s_0[t-1], s_1[t-1]) \\ \cdots \\ s_{n-2}[t] = s_{n-1}[t-1] \oplus g_{n-2}(s_0[t-1], s_1[t-1], \cdots, s_{n-2}[t-1]) \\ s_{n-1}[t] = s_0[t-1] \oplus g_{n-1}(s_0[t-1], s_1[t-1], \cdots, s_{n-1}[t-1]). \end{cases} \tag{2}$$

Definition 4. *An n-bit NLFSR is uniform if for some* $0 \leq \tau < n$*:*
(a) $f_i(x) = x_{i+1}$ *for* $0 \leq i < \tau$*,*
(b) $f_i(x) = x_{(i+1) \bmod n} \oplus g_i(x_0, \cdots, x_\tau)$ *for* $\tau \leq i < n$
where g_i *is a nonzero Boolean function.*

Any Fibonacci NLFSR is uniform. In [13], the author has discussed the transformation from a Fibonacci NLFSR and its equivalent uniform Galois NLFSRs. In this paper, we consider a more general problem: The relationship between Galois NLFSRs (not necessarily uniform) and Fibonacci NLFSRs.

3 The Transformation from the Galois NLFSR to the Fibonacci Configuration

We prove that any Galois NLFSR can be transformed into an equivalent Fibonacci NLFSR and show the transformation in this section.

Lemma 1. *The output sequences of a Fibonacci NLFSR can be generated by a nonlinear recurrence of order n of type:*

$$s_0[t] = \sum_{i=0}^{2^n-1} (a_i \prod_{k=0}^{n-1} s_0^{i_k}[t-n+k]) \tag{3}$$

where $a_i \in \{0,1\}$ *and* $(i_0, i_1, \cdots, i_{n-1})$ *is the binary expansion of* i *with* i_0 *being the least significant bit. On the contrary, given a nonlinear recurrence* (3)*, there exists a Fibonacci NLFSR whose output sequences can be generated by it.*

Proof. An n-bit Fibonacci NLFSR can be described by (2) with $g_i = 0$ for $0 \leq i \leq n-2$, i.e., $s_i[t] = s_{i+1}[t-1]$ for $0 \leq i \leq n-2$. It implies that $s_j[t-1] = s_0[t+j-1]$ for $1 \leq j \leq n-1$. Then the system of equations (2) can be reduced to an equation by replacing $s_j[t-1]$ to $s_0[t+j-1]$ for $1 \leq j \leq n-1$ in the last equation, i.e.,

$$s_0[t+n-1] = s_0[t-1] \oplus g_{n-1}(s_0[t-1], \cdots, s_0[t+n-2]). \tag{4}$$

Hence we have

$$s_0[t] = s_0[t-n] \oplus g_{n-1}(s_0[t-n], \cdots, s_0[t-1]).$$

On the contrary, given a nonlinear recurrence (3), by replacing $s_j[t-1]$ to $s_0[t+j-1]$ for $1 \leq j \leq n-1$, we can get the matching Fibonacci NLFSR with the feedback function $f_{n-1} = \sum_{i=0}^{2^n-1} (a_i \prod_{k=0}^{n-1} x_k^{i_k})$. □

Theorem 1. *A Galois NLFSR can be transformed into an equivalent Fibonacci configuration.*

Proof. Given a Galois NLFSR described by (2), we have

$$s_i[t-1] = s_{i-1}[t] \oplus g_{i-1}(s_0[t-1], s_1[t-1], \cdots, s_{i-1}[t-1])$$

for $1 \le i \le n-1$ by the first equation to the $n-1$th equation of (2). Then from the first equation to the $n-1$th equation, we iteratively substitute for $s_i[t-1]$ $(1 \le i \le n-1)$ their equivalent expressions:

Step 1: By the first equation, we have

$$s_1[t-1] = s_0[t] \oplus g_0(s_0[t-1]).$$

Step 2: By the second equation, we have

$$\begin{aligned} s_2[t-1] &= s_1[t] \oplus g_1(s_0[t-1], s_1[t-1]) \\ &= s_0[t+1] \oplus g_0(s_0[t]) \oplus g_1(s_0[t-1], s_0[t] \oplus g_0(s_0[t-1])) \\ &= s_0[t+1] \oplus h_1(s_0[t-1], s_0[t]) \end{aligned}$$

where $h_1(s_0[t-1], s_0[t]) = g_0(s_0[t]) \oplus g_1(s_0[t-1], s_0[t] \oplus g_0(s_0[t-1]))$.

...

Step i: By the ith equation, we have

$$s_i[t-1] = s_0[t+i-1] \oplus h_{i-1}(s_0[t-1], \cdots, s_0[t+i-2]).$$

where $h_{i-1}(s_0[t-1], \cdots, s_0[t+i-2]) = g_0(s_0[t+i-2]) \oplus g_1(s_0[t+i-3], s_0[t+i-2] \oplus g_0(s_0[t+i-3])) \oplus \cdots \oplus g_{i-1}(s_0[t-1], s_0[t] + g_0(s_0[t-1]), \cdots, s_0[t+i-2] \oplus h_{i-2}(s_0[t-1], \cdots, s_0[t+i-3]))$.

...

Therefore, the system of n equations (2) can be reduced to an equation through substituting $s_i[t-1]$ $(1 \le i \le n-1)$ for their equivalent expressions $s_0[t+i-1] \oplus h_{i-1}(s_0[t-1], \cdots, s_0[t+i-2])$ in the last equation:

$$\begin{aligned} &s_0[t+n-1] \oplus h_{n-2}(s_0[t], \cdots, s_0[t+n-2]) \\ &= s_0[t-1] \oplus h_{n-1}(s_0[t-1], \cdots, s_0[t+n-2]) \end{aligned} \tag{5}$$

where $h_{n-1}(s_0[t-1], \cdots, s_0[t+n-2]) = g_{n-1}(s_0[t-1], s_0[t]+g_0(s_0[t-1]), \cdots, s_0[t+n-2] \oplus h_{n-2}(s_0[t-1], \cdots, s_0[t+n-3]))$, i.e.,

$$s_0[t] = s_0[t-n] \oplus \varphi(s_0[t-n], \cdots, s_0[t-1])$$

where $\varphi(s_0[t-n], \cdots, s_0[t-1]) = h_{n-2}(s_0[t-n+1], \cdots, s_0[t-1]) \oplus h_{n-1}(s_0[t-n], \cdots, s_0[t-1])$. By Lemma 1, this nonlinear recurrence is equivalent to an n-bit Fibonacci NLFSR with the feedback function $f_{n-1} = x_0 \oplus \varphi(x_0, \cdots, x_{n-1})$. □

In [13], the author argued that for a nonuniform Galois NLFSR, there may or may not exists an equivalent Fibonacci NLFSR. To support the viewpoint, two examples have been presented in the paper. One example to prove the existence is as follows:

Example 1. Consider a 4-bit nonuniform Galois NLFSR with the following feedback functions:

$$\begin{aligned} f_0 &= x_1 \oplus x_0 \\ f_1 &= x_2 \\ f_2 &= x_3 \\ f_3 &= x_0 \oplus x_2 x_3. \end{aligned}$$

The author investigated the output sequence of it and found the equivalent Fibonacci NLFSR. However, we can get the equivalent Fibonacci NLFSR without simulating it. First, the Galois NLFSR can be described by

$$\begin{aligned} s_0[t] &= s_1[t-1] \oplus s_0[t-1] \\ s_1[t] &= s_2[t-1] \\ s_2[t] &= s_3[t-1] \\ s_3[t] &= s_0[t-1] \oplus s_2[t-1]s_3[t-1]. \end{aligned}$$

Then

$$\begin{aligned} s_1[t-1] &= s_0[t] \oplus s_0[t-1] \\ s_2[t-1] &= s_1[t] = s_0[t+1] \oplus s_0[t] \\ s_3[t-1] &= s_2[t] = s_1[t+1] = s_0[t+2] \oplus s_0[t+1]. \end{aligned}$$

Hence we have $s_0[t+3] \oplus s_0[t+2] = s_0[t-1] \oplus (s_0[t+1] \oplus s_0[t])(s_0[t+2] \oplus s_0[t+1])$, i.e., $s_0[t] = s_0[t-4] \oplus s_0[t-2] \oplus s_0[t-1] \oplus s_0[t-3]s_0[t-2] \oplus s_0[t-3]s_0[t-1] \oplus s_0[t-2]s_0[t-1]$. Therefore the equivalent Fibonacci NLFSR is of the feedback function $f = x_0 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3$.

We can see that the cost of logic gates of an nonuniform Galois NLFSR and its equivalent Fibonacci NLFSR may not equal through Example 1. Hence it is interesting to find a transformation from a Fibonacci NLFSR to some nonuniform Galois NLFSRs with less cost of logic gates. Unfortunately, we find that this problem seems more difficult than factorization of a polynomial.

Another example to prove the nonexistence in [13] is as follows:

Example 2. A 4-bit NLFSR with the following feedback functions:

$$\begin{aligned} f_0 &= x_1 \oplus x_0x_1 \\ f_1 &= x_2 \oplus x_0 \oplus x_0x_2 \oplus x_0x_1x_2 \\ f_2 &= x_3 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_0x_2 \oplus x_1x_2 \\ f_3 &= x_0 \oplus x_1x_3. \end{aligned}$$

However, this example is incorrect since it is not a Galois NLFSR: $x_1 \in dep(f_0)$ and $x_2 \in dep(f_1)$ are both not in accord with the definition of the Galois configuration.

4 Matching Initial States and some Properties

This section firstly gives a method of finding the matching initial states between a Galois NLFSR and its equivalent Fibonacci configuration. Then some properties of Galois NLFSRs will be presented.

Given a Galois NLFSR, we can find the equivalent Fibonacci NLFSR by the method introduced in the proof of Theorem 1. We iteratively substitute for $s_i[t-1]$ $(1 \leq i \leq n-1)$ their equivalent expressions such as:

$$\begin{cases} s_1[t-1] = s_0[t] \oplus g_0(s_0[t-1]) \\ s_2[t-1] = s_0[t+1] \oplus h_1(s_0[t-1], s_0[t]) \\ \cdots \\ s_{n-2}[t-1] = s_0[t+n-3] \oplus h_{n-3}(s_0[t-1], \cdots, s_0[t+n-4]) \\ s_{n-1}[t-1] = s_0[t+n-2] \oplus h_{n-2}(s_0[t-1], \cdots, s_0[t+n-3]). \end{cases} \tag{6}$$

If the Galois NLFSR is initialized to a state $(s_0[t_0-1], \cdots, s_{n-1}[t_0-1])$, we can get the values of $s_0[t_0], \cdots, s_0[t_0+n-2]$ through iteratively solving the first equation to the last equation of (6). By Lemma 1, if we let the initial state of the equivalent Fibonacci NLFSR be $(s_0[t_0-1], \cdots, s_0[t_0+n-2])$, then the output sequence is expressed by the recurrence (4) with this initial state, which is also the output sequence of the Galois NLFSR with the initial state $(s_0[t_0-1], \cdots, s_{n-1}[t_0-1])$. On the contrary, if the equivalent Fibonacci NLFSR is initialized to the state $(s_0[t_0-1], \cdots, s_0[t_0+n-2])$, we can directly compute the matching initial state $(s_0[t_0-1], \cdots, s_{n-1}[t_0-1])$ of the Galois NLFSR by (6).

This method seems more general, more direct and clearer than the method introduced in [14], which discusses the mapping of initial states between a Fibonacci NLFSR and its equivalent uniform Galois NLFSRs.

Example 3. Consider the 4-bit Galois NLFSR of Example 1. We get a system of equations:

$$\begin{cases} s_1[t-1] = s_0[t] \oplus s_0[t-1] \\ s_2[t-1] = s_0[t+1] \oplus s_0[t] \\ s_3[t-1] = s_0[t+2] \oplus s_0[t+1]. \end{cases}$$

If the Galois NLFSR is initialized to the state $(s_0[t_0-1], s_1[t_0-1], s_2[t_0-1], s_3[t_0-1]) = (0110)$, then the corresponding initial state of the equivalent NLFSR is $(s_0[t_0-1], s_0[t_0], s_0[t_0+1], s_0[t_0+2]) = (0100)$.

By (6), we can directly get the following property of Galois NLFSRs:

Proposition 1. *The ith bit* $(1 \leq i \leq n-1)$ *of a Galois NLFSR is equivalent to the combination of some bits of the equivalent Fibonacci NLFSR. The combination is determined by* (6)*. Moreover, the period of an ith bit sequence* $(1 \leq i \leq n-1)$ *is a factor of the period of the output sequence, and the period of an ith bit sequence* $(1 \leq i \leq n-1)$ *which is not of all* 1 *or all* 0 *is equal to the output sequence if the period of the output sequence is prime.*

Proof. The proof is trivial by (6). □

As we know, the state transition graph of a Fibonacci NLFSR consists of pure cycles if and only if the feedback function of type: $f_{n-1} = x_0 \oplus g_{n-1}(x_1, \cdots, x_{n-1})$ [2]. For the Galois configuration, the state transition graph seems difficult to be

investigated since the period of an output sequence is not necessarily equal to the length of the longest cyclic of their states. However, we can determine which type of Galois NLFSRs can output purely periodic sequences.

Proposition 2. *The output sequences of a Galois NLFSR are all purely periodic if and only if the feedback function of type:* $f_0 = x_1$ *and* $f_i = x_{(i+1) \ mod \ n} \oplus g_i(x_1, \cdots, x_i)$ *for* $1 \leq i \leq n-1$.

Proof. By Theorem 1, a Galois NLFSR described by (1) is equivalent to a Fibonacci NLFSR with the feedback function $f = x_0 \oplus \varphi(x_0, \cdots, x_{n-1})$ where the polynomial φ is computed by the iterative method in the proof of Theorem 1. Then the output sequences are purely periodic if and only if $x_0 \notin dep(\varphi)$ since a period of a Fibonacci NLFSR always equals the longest cyclic sequence of its consecutive states. By (5), $x_0 \notin dep(\varphi)$ is equivalent to $s_0[t-1] \notin dep(h_{n-1})$ where

$$h_{n-1} = g_{n-1}(s_0[t-1], s_0[t] + g_0(s_0[t-1]), \cdots, s_0[t+n-2] \oplus h_{n-2}(s_0[t-1], \cdots, s_0[t+n-3]))$$

where

$$h_j(s_0[t-1], \cdots, s_0[t+j-1]) = g_0(s_0[t+j-1]) \oplus g_1(s_0[t+j-2], s_0[t+j-1] \oplus g_0(s_0[t+j-2])) \oplus \cdots \oplus g_j(s_0[t-1], s_0[t] + g_0(s_0[t-1]), \cdots, s_0[t+j-1] \oplus h_{j-1}(s_0[t-1], \cdots, s_0[t+j-2]))$$

for $0 \leq j \leq n-2$. Hence $s_0[t-1] \notin dep(h_{n-1})$ is equivalent to $s_0[t-1] \notin dep(h_j)$ for $0 \leq j \leq n-1$.

Iteratively computing h_j from h_0 to h_{n-1} with the given g_i $(0 \leq i \leq n-1)$, it is easy to get that $s_0[t-1] \notin dep(h_j)$ for $0 \leq j \leq n-1$ is equivalent to $x_0 \notin dep(g_i)$ for $0 \leq j \leq n-1$. □

5 Conclusions

In this paper, we show how to transform a Galois NLFSR into the Fibonacci configuration and how to find the matching initial states between the two equivalent NLFSRs. Some properties of the output sequences and the sequences of other bits of the Galois NLFSRs are presented.

Some problems of NLFSRs are still open. One problem is finding a transformation from a Fibonacci NLFSR to some nonuniform Galois NLFSRs with less cost of logic gates. Perhaps the most important one is finding a systematic procedure for constructing NLFSRs with a guaranteed long period.

References

1. David, R.: Random Testing of Digital Circuits. Marcel Dekker, New York (1998)
2. Golomb, S.: Shift Register Sequences. Aegean Park Press (1982)

3. Schneier, B.: Applied cryptography: protocols, algorithms, and source code in C, 2nd edn. John Wiley & Sons, Inc., New York (1995)
4. Jansen, C.J.: Investigations On Nonlinear Streamcipher Systems: Construction and Evaluation Methods. Ph.D. Thesis, Technical University of Delft (1989)
5. Ronce, C.A.: Feedback Shift Registers. LNCS, vol. 169. Springer, Heidelberg (1984)
6. Hell, M., Johansson, T., Maximov, A., Meier, W.: The Grain family of stream ciphers. In: Robshaw, M.J.B., Billet, O. (eds.) New Stream Cipher Designs. LNCS, vol. 4986, pp. 179-190. Springer, Heidelberg (2008)
7. Cannière, C., Preneel, B.: Trivium. In: Robshaw, M.J.B., Billet, O. (eds.) New Stream Cipher Designs. LNCS, vol. 4986, pp. 244-266. Springer, Heidelberg (2008)
8. Gittins, B., Landman, H.A., O'Neil, S., Kelson, R.: A presentation on VEST hardware performance, chip area measurements, power consumption estimates and benchmarking in relation to the AES, SHA-256 and SHA-512. Cryptology ePrint Archive, Report 415 (2005)
9. Gammel, B.M., Göttfert, R., Kniffler, O.: An NLFSR-based stream cipher. In: Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS 2006), Island of Kos, Greece, pp. 2920-2924 (May 2006)
10. K. Chen, M. Henricken, W. Millan, J. Fuller, L. Simpson, E. Dawson, H. Lee, and S. Moon, Dragon: A Fast Word Based Stream Cipher eSTREAM, ECRYPT Stream Cipher Project, Report 2005/006 (2005)
11. Dubrova, E., Teslenko, M., Tenhunen, H.: On analysis and synthesis of (n, k)-non-linear feedback shift registers. In: Proceedings of Design and Test in Europe Conference (DATE 2008), Munich, Germany, pp. 133-137 (March 2008)
12. Mrugalski, G., Rajski, J., Tyszer, J.: Ring generators-New devices for embedded test applications. Transactions on Computer-Aided Design of Integrated Circuits and Systems 23(9), 1306-1320 (2004)
13. Dubrova, E.: A transformation from the Fibonacci to the Galois NLFSRs. IEEE Transactions on Information Theory, 5263-5271 (November 2009)
14. E. Dubrova. Finding matching initial states for equivalent NLFSRs in the Fibonacci to the Galois configurations. IEEE Transactions on Information Theory, 56(6): 2961-2967, June (2010)
15. J.-M. Chabloz, S. Mansouri, and E. Dubrova. An algorithm for constructing a fastest Galois NLFSR generating a given sequence. In C. Carlet and A. Pott, editors, Sequences and Their Applications - SETA 2010, volume 6338 of Lecture Notes in Computer Science, pages 41-54. Springer Berlin / Heidelberg (2010)