How to Speed-Up Your NLFSR-Based Stream Cipher

Elena Dubrova
Royal Institute of Technology (KTH), Stockholm, Sweden
dubrova@kth.se

Abstract— **Non-Linear Feedback Shift Registers (NLFSRs) have been proposed as an alternative to Linear Feedback Shift Registers (LFSRs) for generating pseudo-random sequences for stream ciphers. Conventional NLFSRs use the Fibonacci configuration in which the feedback is applied to the last bit only. In this paper, we show how to transform a Fibonacci NLFSR into an equivalent NLFSR in the Galois configuration, in which the feedback can be applied to every bit. Such a transformation can potentially reduce the depth of the circuits implementing feedback functions, thus decreasing the propagation time and increasing the throughput.**

I. Introduction

Our society greatly depends on security of electronic communications. Whether the communication path is as short as a wire between two chips or as long as the World Wide Web, communications security is important for integrity of our business and infrastructure.

To protect the confidential information from unauthorized or accidental disclosure, cryptographic methods are applied. A common approach is to use a stream cipher which combines plain text bits with a pseudo-random bit sequence [1], [2]. The resulting encrypted information can be transformed back into its original form only by an authorized user possessing the cryptographic key.

A pseudo-random sequence can be generated using a *Linear Feedback Shift Register (LFSR)*. LFSRs are simple, fast, and easy to implement in both, software and hardware. They are capable of generating pseudo-random sequences with the same uniform statistical distribution of 0's and 1's as in a truly random sequence [3]. However, they are not cryptographically secure because the structure of an n-bit LFSR can be easily deduced by observing $2n$ consecutive bit of its sequence [4], [5].

One solution to this problem is to feed the outputs of several parallel LFSRs into a non-linear Boolean function to form a combination generator [6], [7]. The combining function has to be carefully selected to ensure the security of the resulting scheme, for example, in order to prevent correlation attacks [8]. Other solutions are to combine several bits from the LFSR state using a non-linear function, or to use the irregular clocking of the LFSR [9], [10]. Examples of LFSR-based stream ciphers include A5/1 stream cipher which used to provide over-the-air communication privacy in the GSM cellular telephone standard [11], and E0 stream cipher which is used in the Bluetooth protocol [12], [13].

As another alternative, a *Non-Linear Feedback Shift Register (NLFSR)* whose current state is a non-linear function of its previous state can be used [14], [15], [16]. NLFSRs output sequences are normally very hard to predict and existing cryptanalytic methods, such as algebraic attacks [17], [18], are usually not applicable. An adversary might need $O(2^n)$ bits of the sequence to determine the structure of an n-bit NLFSR. A number of different implementations of NLFSR-based stream ciphers for RFID and smartcards applications have been proposed, including Achterbahn [19], Grain [20], Dragon [21], VEST [22], and [23].

In general, there are two ways to implement an NLFSR: in the Fibonacci configuration, or in the Galois configuration. The *Fibonacci* configuration, shown in Figure 1, is conceptually more simple. The Fibonacci type of NLFSRs consists of a number of bits numbered from left to right as $n-1, n-2, \ldots, 0$ with feedback from each bit to the $n-1$th bit. At each clocking instance, the value of the bit i is moved to the bit $i-1$. The value of the bit 0 becomes the output of the register. The new value of the bit $n-1$ is computed as some function of the previous values of other bits.

In the *Galois* type of NLFSR, shown in Figure 2, each bit i is updated according to its own feedback function. Thus, in contrast to the Fibonacci NLFSRs in which feedback is applied to the $n-1$th bit only, in the Galois NLFSRs feedback can be applied to every bit. Since the depth of the circuits implementing feedback functions of individual bits is usually smaller than the depth of the circuits implementing the feedback function of the Fibonacci NLFSR, the propagation time can potentially be reduced. This makes Galois NLFSRs particularly attractive for stream cipher applications in which high keystream generation speed is important [10], [6].

However, Galois NLFSRs also have several drawbacks:

1) The period of the output sequence of a Galois NLFSR is not necessarily equal to the length of the longest cyclic sequence of its consecutive states [24].
2) An n-bit Galois NLFSR with the period 2^n-1 does not necessarily satisfy the 1st and the 2nd randomness postulates of Golomb [24]. An n-bit Fibonacci NLFSR with the period 2^n-1 always satisfy both postulates [3].

These drawbacks do not create any problems in the linear case because, for LFSRs, there exist a mapping between the Fibonacci and the Galois configurations. A Galois LFSR generating the same output sequence as a given Fibonacci LFSR (and therefore possessing none of the above mentioned drawbacks) can be obtained by reversing the order of the feedback taps and adjusting the initial state.

In the non-linear case, however, no mapping between the Fibonacci and the Galois configurations has been known until now. The problem of finding such a mapping is addressed in this paper. We demonstrate that, for each Fibonacci NLFSR, there exist a class of equivalent Galois NLFSRs which produce the same output sequence, and show how to transform a given Fibonacci NLFSR into an equivalent Galois NLFSR. This is carried out in the following three steps.

First, we investigate under which conditions a non-linear recurrence of order n describing the output sequences of an n-bit Galois NLFSR exists. We introduce a structure called *feedback graph*, which reflects the relation between variables of feedback functions. We show that a recurrence of order n exists if the feedback graph can be reduced to a single vertex.

Second, we examine what kind of feedback functions have feedback graphs which are reducible to a single vertex. We derive a sufficient condition characterizing these feedback functions. We call NLFSRs satisfying this condition *uniform*.

Finally, the proof of equivalence of two uniform NLFSRs is done by showing that two systems of non-linear equations describing the sequences of NLFSR's states can be reduced to the same non-linear recurrence.

978-3-9810801-5-5/DATE09 © 2009 EDAA

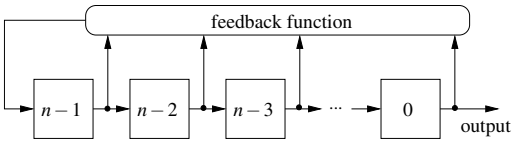

Fig. 1. The Fibonacci configuration of NLFSR.

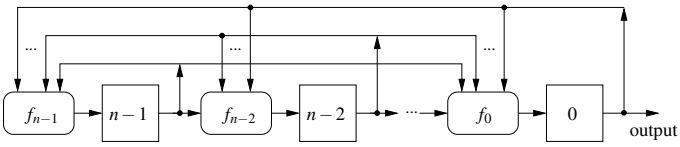

Fig. 2. The Galois configuration of NLFSR.

The formal proofs are not included in the paper due to the page limit. They can be found in [25].

II. Preliminaries

In this section, we describe basic definitions and notation used in the sequel. Most of our terminology is from [3].

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

$$f(x_0,\ldots,x_{n-1}) = \sum_{i=0}^{2^n-1} c_i \cdot x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{n-1}^{i_{n-1}},$$

where $c_i \in \{0,1\}$ and $(i_0 i_1 \ldots i_{n-1})$ is the binary expansion of i with i_0 being the least significant bit. Throughout the paper, we call a term of the ANF a *product-term*.

The *dependence set* (or *support set*) of a Boolean function f is defined by

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

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

Let $f_i: \{0,1\}^n \to \{0,1\}$ be the feedback function of the bit i of an n-bit NLFSR. All results in this paper as derived for NLFSRs whose feedback functions are *singular* functions of type

$$f_i(x_0,\ldots,x_{n-1}) = x_{i+1} \oplus g_i(x_0,\ldots,x_{n-1}), \tag{1}$$

where $g_i: \{0,1\}^{n-1} \to \{0,1\}$, $i+1 \notin dep(g_i)$, and the sign "+" is modulo n. For the Fibonacci type of NLFSRs, singularity guarantees that the state transition graph of an NLFSR consists of pure cycles, without branches. For the Galois type of NLFSRs, singularity alone is not sufficient. For example, an n-bit Galois NLFSR in which each function g_i in (1) is an AND of all $n-1$ variables but x_{i+1} is not branchless. Some extra conditions need to be imposed to ensure branchlessness of the Galois NLFSRs [3].

We also assume that the ANF of the sub-function g_i does not contain the product-term "1". This assumption does not cause any loss of generality, because any Fibonacci NLFSR N with the feedback function $f(x_0,x_1,\ldots,x_{n-1}) = x_0 \oplus (1 \oplus g(x_1,x_2,\ldots,x_{n-1}))$, has a complement NLFSR N_c with the feedback function $f(x_0,x_1,\ldots,x_{n-1}) = x_0 \oplus g(x_1,x_2,\ldots,x_{n-1})$ which generates a sequence which is a complement of the sequence generated by N.

The *period* of an NLFSR is the length of the longest cyclic output sequence it produces. The period of an n-bit NLFSR can be less or equal to 2^n.

Let $s_i(t)$ denote the value of the shift register bit i at time t. The sequence of states of an n-bit NLFSR with singular feedback functions can be described by a system of n non-linear equations of type:

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

The *non-linear recurrence of order n* describing the sequence of values of the bit i of an n-bit NLFSR is the expression of type

$$s_i(t) = \sum_{j=0}^{2^n-1} (a_j \cdot \prod_{k=0}^{n-1} s_i^{j_k}(t-n+k)), \tag{3}$$

where $a_j \in \{0,1\}$, $\sum$ is modulo 2, $(j_0 j_1 \ldots j_{n-1})$ is the binary expansion of j with j_0 being the least significant bit, and $s^{j_k}(t-n+k)$ is defined as follows

$$s_i^{j_k}(t-n+k) = \begin{cases} s_i(t-n+k), & \text{for } j_k = 1, \\ 1, & \text{for } j_k = 0. \end{cases}$$

III. A Condition for Existence of a Non-Linear Recurrence

In this section, we formulate a condition for existence of a non-linear recurrence of order n describing the output sequence of an n-bit NLFSR. First, we introduce some definitions which are necessary for the presentation of the main result.

Definition 1: Two NLFSRs are equivalent if their sets of output sequences are equivalent.

Definition 2: The feedback graph of an n-bit NLFSR is a directed graph with n vertices $v_0,\ldots,v_{n-1}$ which represent the bits $0,\ldots,n-1$ of the NLFSR, respectively. There is an edge from v_i to v_j if $i \in dep(f_j)$.

Definition 3: The operation substitution, denoted by $sub(v_i,v_j)$, is defined for any vertex v_i which has a unique predecessor v_j. The substitution $sub(v_i,v_j)$ removes v_i from the feedback graph and, for each successor v_k of v_i, replaces the edge (v_i,v_k) by an edge (v_j,v_k).

Definition 4: Given a feedback graph G, the reduced feedback graph of G is a graph obtained by repeatedly applying the substitution to each vertex of G with the input degree 1, until no more substitutions can be applied.

It is easy to show that the order of applying the substitution does not influence the resulting reduced feedback graph, i.e. it is unique for a given G.

Lemma 1: If the feedback graph of an n-bit NLFSR can be reduced to a single vertex v_i, then there exist a non-linear recurrence of order n describing the sequence of values of the bit i.

As an example, consider the 4-bit Fibonacci NLFSR with the feedback function $f_3 = x_0 \oplus x_1 \oplus x_2 \oplus x_1x_3$. Its sequence of states can be described by the following equations:

$$\begin{cases} s_3(t) = s_0(t-1) \oplus s_1(t-1) \oplus s_2(t-1) \oplus s_1(t-1)s_3(t-1) \\ s_2(t) = s_3(t-1) \\ s_1(t) = s_2(t-1) \\ s_0(t) = s_1(t-1). \end{cases}$$

This NLFSR generates the following output sequence with the period 15:

$$111011000101001\ldots$$

The feedback graph of this NLFSR is shown in Figure 3(a). It can be reduced to a single vertex as follows:

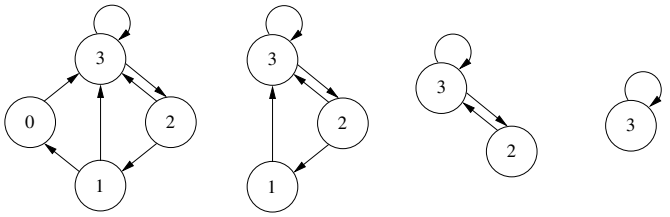

Fig. 3. Reduction steps for the feedback graph of the Fibonacci NLFSR from the example: (a) initial graph; (b) after $sub(v_0, v_1)$; (c) after $sub(v_1, v_2)$; (d) after $sub(v_2, v_3)$.

1) $sub(v_0, v_1)$ reduces the graph to Figure 3(b). This is equivalent to substituting $s_0(t)$ by $s_1(t-1)$ into the equation of $s_3(t)$:

$$s_3(t) = s_1(t-2) \oplus s_1(t-1) \oplus s_2(t-1) \oplus s_1(t-1)s_3(t-1).$$

2) $sub(v_1, v_2)$ reduces the graph to Figure 3(c). This is equivalent to substituting $s_1(t)$ by $s_2(t-1)$ into the equation of $s_3(t)$:

$$s_3(t) = s_2(t-3) \oplus s_2(t-2) \oplus s_2(t-1) \oplus s_2(t-2)s_3(t-1).$$

3) $sub(v_2, v_3)$ reduces the graph to Figure 3(d). This is equivalent to substituting $s_2(t)$ by $s_3(t-1)$ into the equation of $s_3(t)$:

$$s_3(t) = s_3(t-4) \oplus s_3(t-3) \oplus s_3(t-2) \oplus s_3(t-3)s_3(t-1).$$

This gives us the non-linear recurrence describing the sequence of values of the bit 3. Since other bits repeat the value of the 3rd bit, the recurrence is identical for all bits, and thus for the output of the NLFSR.

It is easy to see that the feedback graph of an n-bit Fibonacci NLFSR can always be reduced to a single vertex v_{n-1}. Therefore, for a Fibonacci NLFSR, a non-linear recurrence of type (3) always exists. Its coefficients a_i, $i \in \{0, 1, \ldots, 2^n - 1\}$, are equal to the coefficients c_i of the ANF of the feedback function f_{n-1}.

IV. A Transformation from the Fibonacci to the Galois NLFSRs

In this section, we show how to transform a Fibonacci NLFSR into an equivalent Galois NLFSR.

Let A_f denote the set of all product-terms of the ANF of the function f. Throughout the section, we use P to denote a subset of A_f and p to denote an element of A_f.

Definition 5: Let f_a and f_b be feedback functions of bits a and b of an n-bit NLFSR, respectively. The operation shifting, denoted by $f_a \xrightarrow{P} f_b$, moves a set of product-terms $P \subseteq A_{f_a}$ from the ANF of f_a to the ANF of f_b. The index of each variable x_i of each product-term in P is changed to $x_{(i-a+b) \bmod n}$.

For example, if initially we have a 4-bit NLFSR with the following feedback functions:

$$\begin{aligned} f_3 &= x_0 \oplus x_1x_3 \\ f_2 &= x_3 \\ f_1 &= x_2 \\ f_0 &= x_1 \end{aligned}$$

then, after the shifting $f_3 \xrightarrow{\{x_1x_3\}} f_2$, these functions change to:

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

Definition 6: The terminal bit τ of an n-bit NLFSR is the bit with the maximal index which satisfies the following condition: For all bits i such that $i < \tau$, the feedback function f_i is of type $f_i = x_{i+1}$.

Let $min\_index(f)$ ($max\_index(f)$) denote the smallest (largest) index of variables in $dep(f)$. For example, if $f = x_3 \oplus x_0x_2$, then $min\_index(f) = 0$ and $max\_index(f) = 3$.

Definition 7: An n-bit NLFSR is uniform if:

(a) all its feedback functions are of type (1), and

(b) for all its bits i such that $i > \tau$, the following condition holds:

$$max\_index(g_i) \leq \tau, \tag{4}$$

where τ is the terminal bit of the NLFSR.

Note that any Fibonacci NLFSR satisfies the condition (b) of the Definition 7.

Lemma 2: If an NLFSR is uniform, then its feedback graph can be reduced to a single vertex.

The above condition is sufficient, but not necessary. For example, the following 5-bit NLFSR is not uniform, but can be reduced to a single vertex:

$$\begin{aligned} f_4 &= x_0 \oplus x_1 \\ f_3 &= x_4 \oplus x_0x_1 \\ f_3 &= x_3 \oplus x_4 \\ f_1 &= x_2 \oplus x_0 \\ f_0 &= x_1. \end{aligned}$$

The following theorem is the main result of the paper. It presents a sufficient condition for equivalence of two NLFSRs. Note, that it is formulated for shiftings on subfunctions g_i of the singular feedback functions f_i (see the expression (1)). The variable x_{i+1} is excluded because its shifting always results in a non-uniform NLFSR.

Theorem 1: Given a uniform NLFSR with the terminal bit a, a shifting $g_a \xrightarrow{P} g_b$, $P \subseteq A_{g_a}$, $b < a$, results in an equivalent NLFSR if the transformed NLFSR is uniform as well.

It is easy to see that, for any Fibonacci NLFSR, shifting can always reduce the index of the initial terminal bit $n-1$ at least by 1. It reduces the index of the terminal bit exactly by 1 if the subfunction g_{n-1} of the Fibonacci NLFSR contains a product-term with $max\_index(g_{n-1}) = n-1$ and $min\_index(g_{n-1}) = 1$. The smaller the difference between $max\_index(g_{n-1})$ and $min\_index(g_{n-1})$, the more the index of the initial terminal bit can be reduced.

V. Fully Shifted Galois NLFSRs

Usually, there are multiple ways to transform a Fibonacci NLFSR into a Galois NLFSR. Therefore, it is useful to define the "border" case which shows us which bit is the minimal possible terminal bit and how far down each product-term can be shifted.

Definition 8: An NLFSR is fully shifted if no product-term of any function g_a can be shifted to a function g_b with the index $b < a$ without violating the condition (4).

Note that the fully shifted Galois NLFSR is unique for a given Fibonacci NLFSR. Next, we show how to construct it.

Algorithm 1: Given a uniform n-bit Fibonacci NLFSR N, the fully shifted Galois NLFSR $\hat{N}$ which is equivalent to N is obtained as follows.

First, the terminal bit τ of $\hat{N}$ is computed as:[1]

$$\tau = \max_{\forall p \in A_{g_{n-1}}} (max\_index(p) - min\_index(p)), \tag{5}$$

[1]More strictly, the equation (5) gives us the maximal index of the bit from which the feedback can be taken. For NLFSRs, this bit coincides with the terminal bit. For LFSRs, the equation (5) always evaluates to 0, while the terminal bit is equal to $(n-1) - max\_index(g_{n-1})$.

Then, each product-term $p \in A_{g_{n-1}}$ with $min\_index(p) \leq (n-1)-\tau$ is shifted to $g_{n-1-min\_index(p)}$:

$$g_{n-1} \xrightarrow{\{p\}} g_{n-1-min\_index(p)}.$$

and each product-term $p \in A_{g_{n-1}}$ with $min\_index(p) > (n-1)-\tau$ is shifted to g_τ:

$$g_{n-1} \xrightarrow{\{p\}} g_\tau.$$

Theorem 2: Algorithm 1 correctly computes the fully shifted Galois NLFSR for a given Fibonacci NLFSR.

As an example, consider the following 32-bit Fibonacci NLFSR which is used in the NLFSR-based stream cipher from [23]:

$$\begin{aligned} f_{31} \;=\; & x_0 \oplus x_2 \oplus x_6 \oplus x_7 \oplus x_{12} \oplus x_{17} \oplus x_{20} \oplus x_{27} \oplus x_{30} \oplus x_3x_9 \\ & \oplus\; x_{12}x_{15} \oplus x_4x_5x_{16}. \end{aligned}$$

Its corresponding fully shifted Galois NLFSR has the terminal bit $\tau = 12$ and the following feedback functions:

$$\begin{aligned} f_{29} &= x_{30} \oplus x_0 & f_{24} &= x_{25} \oplus x_0 \\ f_{28} &= x_{29} \oplus x_0x_6 & f_{19} &= x_{20} \oplus x_0 \oplus x_0x_3 \\ f_{27} &= x_{28} \oplus x_0x_1x_{12} & f_{14} &= x_{15} \oplus x_0 \\ f_{25} &= x_{26} \oplus x_0 & f_{12} &= x_{13} \oplus x_1 \oplus x_8 \oplus x_{11}. \end{aligned}$$

The functions which are omitted are of type $f_i = x_{i+1}$ where"+" is modulo 32.

We can further reduce the depth of the circuits implementing feedback functions as follows:

$$\begin{aligned} f_{29} &= x_{30} \oplus x_0 & f_{19} &= x_{20} \oplus x_0 \\ f_{28} &= x_{29} \oplus x_0x_6 & f_{16} &= x_{17} \oplus x_{12} \\ f_{27} &= x_{28} \oplus x_0x_1x_{12} & f_{14} &= x_{15} \oplus x_0 \\ f_{25} &= x_{26} \oplus x_0 & f_{13} &= x_{14} \oplus x_{12} \\ f_{24} &= x_{25} \oplus x_0 & f_{12} &= x_{13} \oplus x_1. \\ f_{20} &= x_{21} \oplus x_1x_4 & & \end{aligned}$$

Note, that shifting does not increase the number of binary operations in the ANFs of the feedback functions. This number is always the same as the one of the initial Fibonacci NLFSR. So, we can decrease the depth of the circuits implementing feedback functions without increasing the number of 2-input gates in these circuits.

To check how this theoretical advantage translates into the actual propagation time and area, we synthesized ten Fibonacci NLFSRs used in the stream cipher from [23][2] in 0.25 μm standard cell CMOS-technology using VHDL and compared them to their Galois counterparts. Our experimental result show that, on average, the Galois configuration allows us to increase the throughput 1.76 times and to reduce the area by 19%.

VI. Conclusion

In this paper, we show how to transform a Fibonacci NLFSR into the Galois configuration. Such a transformation can potentially reduce the depth of the circuits implementing feedback functions, thus increasing the throughput. Our experimental results on 10 NLFSRs from the stream cipher from [23] show that, on average, the presented technique allows us to increase the throughput 1.76 times and to reduce the area by 19%.

Acknowledgments

The author would like to thank Shohreh Sharif and Ali Houmani for their help with the experimental results.

[2]The stream cipher from [23] consists of ten NLFSR of sizes 22, 23, 24, 25, 26, 27, 28, 29, 31 and 32 bits which work in parallel. The outputs of NLFSR are combined using a non-linear Boolean function.

References

[1] B. Schneier, *Applied cryptography (2nd ed.): protocols, algorithms, and source code in C*. New York, NY, USA: John Wiley & Sons, Inc., 1995.

[2] H. C. van Tilborg, *Encyclopedia of Cryptography and Security*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005.

[3] S. Golomb, *Shift Register Sequences*. Aegean Park Press, 1982.

[4] J. Massey, "Shift-register synthesis and bch decoding," *IEEE Transactions on Information Theory*, vol. 15, pp. 122–127, 1969.

[5] J. D. Golic, "On the linear complexity of functions of periodic GF(q) sequences," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 69–75, 1989.

[6] M. Robshaw, "Stream ciphers," Tech. Rep. TR - 701, July 1994.

[7] Y. Tarannikov, "New constructions of resilent Boolean function with maximum nonlinearity," *Lecture Notes in Computer Science*, vol. 2355, pp. 66–77, 2001.

[8] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *J. Cryptol.*, vol. 1, no. 3, pp. 159–176, 1989.

[9] R. Bialota and G. Kawa, "Modified alternating k generators," *Des. Codes Cryptography*, vol. 35, no. 2, pp. 159–174, 2005.

[10] K. Zeng, C. Yang, D. Wei, and T. R. N. Rao, "Pseudo-random bit generators in stream-cipher cryptography," *Computer*, 1991.

[11] E. Biham and O. Dunkelman, "Cryptanalysis of the A5/1 GSM stream cipher," in *INDOCRYPT '00: Proceedings of the First International Conference on Progress in Cryptology*, (London, UK), pp. 43–51, Springer-Verlag, 2000.

[12] B. Lohlein, "Attacks based on conditional correlations against the nonlinear filter generator," citeseer.ist.psu.edu/554481.html.

[13] O. Y. Shaked, "Cryptanalysis of the Bluetooth E0 cipher," citeseer.ist.psu.edu/744254.html.

[14] C. J. Jansen, *Investigations On Nonlinear Streamcipher Systems: Construction and Evaluation Methods*. Ph.D. Thesis, Technical University of Delft, 1989.

[15] C. A. Ronce, *Feedback Shift Registers*, vol. 169. Lecture Notes in Computer Science, 1984.

[16] M. J. B. Robshaw, *On Binary Sequences with Certain Properties*. Ph.D. Thesis, University of London, 1992.

[17] A. Canteaut, "Open problems related to algebraic attacks on stream ciphers," in *WCC*, pp. 120–134, 2005.

[18] A. Maximov, *Some Words on Cryptanalysis of Stream Ciphers*. Ph.D. Thesis, Lund University, 2006.

[19] B. Gammel, R. Göttfert, and O. Kniffler, "Achterbahn-128/80: Design and analysis," in *SASC'2007: Workshop Record of The State of the Art of Stream Ciphers*, pp. 152–165, 2007.

[20] M. Hell, T. Johansson, and W. Meier, "Grain - a stream cipher for constrained environments," citeseer.ist.psu.edu/732342.html.

[21] K. Chen, M. Henricken, W. Millan, J. Fuller, L. Simpson, E. Dawson, H. Lee, and S. Moon, "Dragon: A fast word based stream cipher," in *eSTREM, ECRYPT Stream Cipher Project*, 2005. Report 2005/006.

[22] B. Gittins, H. A. Landman, S. O'Neil, and R. Kelson, "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 2005/415, 2005. http://eprint.iacr.org/.

[23] B. M. Gammel, R. Göttfert, and O. Kniffler, "An NLFSR-based stream cipher," in *ISCAS*, 2006.

[24] E. Dubrova, M. Teslenko, and H. Tenhunen, "On analysis and synthesis of (n,k)-non-linear feedback shift registers," in *Design and Test in Europe*, pp. 133–137, 2008.

[25] E. Dubrova, "An equivalence preserving transformation from the Fibonacci to the Galois NLFSRs." http://arxiv.org/abs/0801.4079.