УДК 519.7 DOI 10.17223/20710410/62/3

ON THE NUMBER OF ℓ-SUITABLE BOOLEAN FUNCTIONS IN CONSTRUCTIONS OF FILTER AND COMBINING MODELS OF STREAM CIPHERS[1]

T. A. Bonich*, M. A. Panferov**, N. N. Tokareva*

*Novosibirsk State University, Novosibirsk, Russia,
**Sobolev Institute of Mathematics, Novosibirsk, Russia

E-mail: t.bonich@g.nsu.ru, m.panferov@g.nsu.ru, crypto1127@mail.ru

It is well known that every stream cipher is based on a good pseudorandom generator. For cryptographic purposes, we are interested in generating pseudorandom sequences with the maximum possible period. A feedback register is one of the most known cryptographic primitives that is used to construct stream ciphers. We consider periodic properties of pseudorandom sequences produced by filter and combiner generators (two known schemes of stream generators based on feedback registers). We analyze functions in these schemes that lead to output sequences of period at least a given number ℓ. We call such functions ℓ-suitable and count the exact number of them for an arbitrary n.

Keywords: *stream cipher, filter generator, combiner generator, Boolean function.*

О ЧИСЛЕ ℓ-ПОДХОДЯЩИХ БУЛЕВЫХ ФУНКЦИЙ В КОНСТРУКЦИЯХ ФИЛЬТРУЮЩЕЙ И КОМБИНИРУЮЩЕЙ МОДЕЛЕЙ ПОТОЧНЫХ ШИФРОВ

Т. А. Бонич*, М. А. Панферов**, Н. Н. Токарева*

*Новосибирский государственный университет, г. Новосибирск, Россия,
**Институт математики им. С. Л. Соболева, г. Новосибирск, Россия

Известно, что любой поточный шифр основан на хорошем генераторе псевдослучайных чисел. В криптографических целях изучаются различные способы генерации псевдослучайных последовательностей с максимально возможным периодом. Регистр сдвига с обратной связью — один из криптографических примитивов, который используется для построения поточных шифров. В работе изучаются периодические свойства псевдослучайных последовательностей, создаваемых фильтрующим и комбинирующим генераторами (известными схемами поточных генераторов на основе регистров сдвига с обратной связью). В этих схемах анализируются функции, которые приводят к выходным последовательностям с периодом не менее заданного числа ℓ. Мы называем такие функции ℓ-подходящими и подсчитываем их точное количество для произвольного n.

Ключевые слова: *поточный шифр, фильтрующий генератор, комбинирующий генератор, булева функция.*

[1]The work is supported by the Mathematical Center in Akademgorodok under the agreement No. 075-15-2022-282 with the Ministry of Science and Higher Education of the Russian Federation.

1. Introduction

Symmetric ciphers are usually divided into block and stream ciphers. Stream ciphers are considered as more fast but not as secure as block ciphers. One of the most known cryptographic primitives that is used to construct stream ciphers is a feedback shift register (FSR). There are many attacks and defenses on such ciphers and countermeasures against them, see, for instance, [1, 2].

The task of studying feedback registers leads to the problem of studying a pseudorandom sequence (gamma) generated by a feedback register [3]. Cryptographers who develop various pseudorandom number generators study the resulting gamma for the presence of the necessary properties. For example, it should have a large period, high linear complexity, and a uniform bit distribution [4]. It is often important that the sequence be reproducible [5]. Only if gamma has the required properties it can be considered for use in cryptographic applications [6]. An important property of the generated sequence is the randomness. There should be independence of values, unpredictability and uniform distribution [7]. Before using a pseudorandom sequence, it is necessary to evaluate its randomness. There are many different statistical tests for this, for example, NIST, Diehard, ENT test [8].

The properties of the pseudorandom sequence generated by FSR are well studied in the case when f is a linear function (LFSR). If f is nonlinear (see [9, 10]), there are too many open questions related to pseudorandom sequences that all are connected to analysis of nonlinear recurrent sequences, for example, see [11] for further review. That is why some nonlinear combinations of LFSRs are usually considered, for instance, filter and combining models of stream generators [6].

Let us recall a few definitions. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A *Boolean function in n variables* is a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$. A *vector of values* for a given Boolean function f is the vector $\big(f(x^{(1)}), \ldots, f(x^{(2^n)})\big)$, where $x^{(1)}, \ldots, x^{(2^n)}$ are binary vectors in $\mathbb{F}_2^n$ that are lexicographically ordered. Any Boolean function f can be represented uniquely in its *algebraic normal form* (*ANF*): $f(x_1, \ldots, x_n) = \bigoplus\limits_{I \in \mathcal{P}(N)} a_I \Big(\prod\limits_{i \in I} x_i \Big)$, where $\mathcal{P}(N)$ is a power set of $N = \{1, \ldots, n\}$ and $a_I \in \mathbb{F}_2$. For a Boolean function f, the number of variables in the longest item of its ANF is called *the algebraic degree* of the function. If algebraic degree of f is not more than 1, then f is called *affine*. A function is called *linear* if it is affine and $f(0) = 0$. If algebraic degree of a function f is more than 1, then f is called *nonlinear*.

A feedback shift register consists of two parts: a binary block $x = (x_1, \ldots, x_n)$ of length n and a feedback function f, where f is a Boolean function in n variables. First, we fill the block x with constants, it is the *initial state* of the register. During the encryption process the register is changing its state using the feedback function. *Gamma* is a pseudorandom sequence generated by FSR. For functioning of the FSR the time is considered to be divided into clock cycles. On each clock cycle, the value $f(x)$ is calculated first, then the register state $x = (x_1, \ldots, x_{n-1}, x_n)$ goes to the state $x' = (x_2, \ldots, x_n, f(x))$, while the bit x_1 will be written as the first bit of the generated gamma. A *period* is a length of repeating part of gamma. If f is linear, we have LFSR. Similarly, *nonlinear feedback shift register* (NFSR) uses nonlinear Boolean function as a feedback function. It is known that LFSR can be also specified by a feedback polynomial. It is a polynomial of degree n defining bits to be summed. If $f(x_1, \ldots, x_n) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n$, then the corresponding feedback polynomial is defined as $p(z) = a_1 z^n + a_2 z^{n-1} + \ldots + a_n z + 1$, where $a_i \in \mathbb{F}_2$, $i = 1, \ldots, n$. If $p(z)$ is a *primitive polynomial*, i.e., the primitive element of the field $\mathrm{GF}(2^n)$ is its root,

then the period of a pseudorandom sequence generated by LFSR is maximal, i.e., is equal to $2^n - 1$. As a result, primitive polynomials are mainly used in LSFRs.

There are many stream ciphers based on LFSR and NFSR. One of them is Grain, developed in 2004 [12]. It is constructed by combining model based on two shift registers, one with linear feedback and one with nonlinear feedback, and a nonlinear output function. Both linear and nonlinear shift register sizes are 80 bits. Another one is A5/1 cipher from GSM standard [13]. It has three LSFRs of lengths 19, 22 and 23 bits with irregular clocking. The registers are clocked in a stop/go fashion using a majority rule. The output is the sum of the last bits of the three registers. We could also mention the Gollmann cascade [14]. This cipher is representative of epy combining model. It consists of a series of LFSRs that are clock-controlled by the previous LFSR. If all the LFSRs have the same length n, the linear complexity of a system with k LFSRs is equal to $n(2^n - 1)^{k-1}$. Other examples of ciphers that are based on LFSR and NFSR are Geffe generator, Jennings generator, and Beth — Piper Stop-and-Go generator.

In this paper, we analyze pseudorandom sequences produced by filter and combiner generators. Namely, we study functions in these schemes that lead to pseudorandom sequences with a period not less than a given ℓ. We call such functions *ℓ-suitable* and count the exact number of them for an arbitrary n.

This paper is a modified continuation of the previous one [15].

2. The analysis of gamma for linear feedback shift register generators

2.1. Filter generators

The filter generator consists of a single LFSR of length n and uses a primitive polynomial to change states. A Boolean function $h(x_1, \ldots, x_n)$ applied to the current state generates a pseudorandom sequence (gamma). Let us note that the number of all possible functions $h(x_1, \ldots, x_n)$ is equal to 2^{2^n}. The work of the filter generator is shown in [16].

Let gamma be defined as $\gamma = (y_1, y_2, \ldots, y_{2^n-1})$, where $y_1 = h(x_1, \ldots, x_n)$, $y_2 = h(x_2, \ldots, x_n, f(x_1, \ldots, x_n))$, etc., and $f(x_1, \ldots, x_n)$ is the feedback function. Since the number of all nonzero states is equal to $2^n - 1$, the maximum possible value of the gamma period is also $2^n - 1$. We would like to determine all ℓ-suitable Boolean functions h in n variables. Functions which lead to gammas with a period less than a given ℓ we would call *ℓ-unsuitable*. Note that the number of such functions does not depend on a linear feedback function. But whether the function is ℓ-suitable or not for the given generator, depends on the feedback function. When we count the number of ℓ-suitable functions h, we do not consider a specific set of states. We say that there is a certain number of different states used by the generator (all sets that are generated by primitive polynomials fit this definition). Next, we study which pseudorandom sequences have the period not less than a given ℓ. We analyze the number of ℓ-unsuitable functions and the number of ℓ-suitable functions. Thus, our reasonings do not affect the specific order of the states. Therefore, there will be the exact calculated number of ℓ-suitable functions h for any set of states used by the generator.

Let us provide some examples of ℓ-suitable and ℓ-unsuitable functions. Let $n = 4$ be the length of a shift register, $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2$ be a feedback function, and $p(z) = z^4 + z^3 + 1$ be a corresponding primitive polynomial. Let $h_1(x_1, x_2, x_3, x_4) = x_2x_1 \oplus x_3x_1 \oplus x_3x_2 \oplus x_4x_1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$ and $h_2(x_1, x_2, x_3, x_4) = x_4x_2x_1 \oplus x_2x_1 \oplus x_3x_2 \oplus x_3 \oplus 1$ be Boolean functions in n variables. We present generated gamma for these functions in the Table.

States	0001	0010	0100	1001	0011	0110	1101	1010
$h_1(x_1, x_2, x_3, x_4)$	1	0	0	1	0	0	1	0
$h_2(x_1, x_2, x_3, x_4)$	1	0	1	1	0	1	1	0

States	0101	1011	0111	1111	1110	1100	1000	0001
$h_1(x_1, x_2, x_3, x_4)$	0	1	0	0	1	0	0	1
$h_2(x_1, x_2, x_3, x_4)$	1	0	1	1	0	0	1	1

Note that h_1 and h_2 generate the gamma with periods 3 and 15. If $\ell = 15$, i.e., we need a gamma with maximum period, then h_1 is an ℓ-unsuitable function, h_2 is a ℓ-suitable function.

To begin with, we show the calculation of the number of ℓ-unsuitable sequences. The number of aperiodic Boolean sequences has been studied in [17], we present our calculations of the number U_ℓ of sequences with a period less than ℓ (ℓ-unsuitable sequences).

Lemma 1. Let $\ell = q_1^{\omega_1} q_2^{\omega_2} \dots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$. Then the number of ℓ-unsuitable sequences is equal to

$$U_\ell = \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} \left((-1)^{\beta_1 + \dots + \beta_k + 1} 2^{q_1^{\omega_1 - \beta_1} \dots q_k^{\omega_k - \beta_k}} \right), \text{ where } \beta = (\beta_1, \dots, \beta_k).$$

Proof. We can count the number of ℓ-unsuitable sequences of length ℓ only. Consider sequences of length $\ell = q_1^{\omega_1} q_2^{\omega_2} \dots q_k^{\omega_k}$ with a period less than ℓ. Let A_i be a set of sequences that can be divided on q_i identical subsequences, $i = 1, \dots, k$. Then $A_i \cap A_j$ is a set of sequences that can be divided on $q_{i \cdot j}$ identical subsequences, where $i \neq j$, $i, j = 1, \dots, k$. Then $A_i \cup A_j$ is a set of sequences that can be divided on q_i or q_j identical subsequences, where $i \neq j$, $i, j = 1, \dots, k$. Hence, all ℓ-unsuitable sequences belong to the set $\bigcup\limits_{i=1}^{k} A_i$, and $U_\ell = |\bigcup\limits_{i=1}^{k} A_i|$. When a sequence is divided into q_i identical subsequences, the length of the subsequence is equal to $q_1^{\omega_1} q_2^{\omega_2} \dots q_i^{\omega_i - 1} \dots q_k^{\omega_k}$. Since the elements of the subsequences are in $\{0, 1\}$, then

$$|A_i| = 2^{q_1^{\omega_1} q_2^{\omega_2} \dots q_{(i-1)}^{\omega_{(i-1)}} q_i^{\omega_i - 1} q_{(i+1)}^{\omega_{(i+1)}} \dots q_k^{\omega_k}},$$

$$|A_i \cap A_j| = 2^{q_1^{\omega_1} q_2^{\omega_2} \dots q_{(i-1)}^{\omega_{(i-1)}} q_i^{\omega_i - 1} q_{(i+1)}^{\omega_{(i+1)}} \dots q_{(j-1)}^{\omega_{(j-1)}} q_j^{\omega_j - 1} q_{(j+1)}^{\omega_{(j+1)}} \dots q_k^{\omega_k}},$$

$$\dots$$

$$\Big| \bigcap_{i=1}^{k} A_i \Big| = 2^{q_1^{\omega_1 - 1} q_2^{\omega_2 - 1} \dots q_k^{\omega_k - 1}}.$$

Therefore, we can compute $|\bigcup\limits_{i=1}^{k} A_i|$ using the inclusion-exclusion principle:

$$\Big| \bigcup_{i=1}^{k} A_i \Big| = \sum_{i=1}^{k} |A_i| - \sum_{1 \leqslant i < j \leqslant k} |A_i \cap A_j| + \sum_{1 \leqslant i < j < t \leqslant k} |A_i \cap A_j \cap A_t| - \dots$$

$$+ (-1)^{k-1} |A_1 \cap A_2 \cap \dots \cap A_k| = \sum_{i=1}^{k} 2^{q_1^{\omega_1} q_2^{\omega_2} \dots q_{(i-1)}^{\omega_{(i-1)}} q_i^{\omega_i - 1} q_{(i+1)}^{\omega_{(i+1)}} \dots q_k^{\omega_k}} -$$

$$- \sum_{1 \leqslant i < j \leqslant k} 2^{q_1^{\omega_1} q_2^{\omega_2} \dots q_{(i-1)}^{\omega_{(i-1)}} q_i^{\omega_i - 1} q_{(i+1)}^{\omega_{(i+1)}} \dots q_{(j-1)}^{\omega_{(j-1)}} q_j^{\omega_j - 1} q_{(j+1)}^{\omega_{(j+1)}} \dots q_k^{\omega_k}} +$$

$$\ldots + (-1)^{k-1} 2^{q_1^{\omega_1-1} q_2^{\omega_2-1} \ldots q_k^{\omega_k-1}} = \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} \left((-1)^{\beta_1 + \cdots + \beta_k + 1} 2^{q_1^{\omega_1-\beta_1} \ldots q_k^{\omega_k-\beta_k}} \right),$$

where $\beta = (\beta_1, \ldots, \beta_k)$. ■

Let us prove the main result for filter generators.

Theorem 1. Let $n \in \mathbb{N}$ and ℓ is a divisor of $2^n - 1$, $\ell = q_1^{\omega_1} q_2^{\omega_2} \ldots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$. Then the number of ℓ-suitable Boolean functions in n variables for the filter generator with LFSR based on a primitive polynomial of degree n is equal to

$$2^{2^n} - 2 \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} \left((-1)^{\beta_1 + \ldots + \beta_k + 1} 2^{q_1^{\omega_1-\beta_1} \ldots q_k^{\omega_k-\beta_k}} \right), \text{ where } \beta = (\beta_1, \ldots, \beta_k).$$

Proof. From Lemma 1 we know the number U_ℓ of ℓ-unsuitable sequences of the length $2^n - 1$. We can write all states of the register one by one and from one state we get the second one as the next state. Consider the vector of values of a Boolean function h that generates our gamma. Since there is no zero state in the set of states (it generates the cycle of length 1), function h can take any value (0 or 1) on zero vector. That is why there are exactly two Boolean functions that generate the same sequence.

Hence, the number of ℓ-unsuitable functions is equal to $2\,U_\ell$. Then, the number of ℓ-suitable functions is $2^{2^n} - 2\,U_\ell$. ■

Similarly, we propose to count the number of Boolean functions in n variables leading to gammas with period exactly equal to ℓ.

Theorem 2. Let $n \in \mathbb{N}$ and ℓ is a divisor of $2^n - 1$, $\ell = q_1^{\omega_1} q_2^{\omega_2} \ldots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$. Then the number of Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the filter generator with LFSR based on a primitive polynomial of degree n is equal to

$$2^{\ell+1} - 2 \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} \left((-1)^{\beta_1 + \ldots + \beta_k + 1} 2^{q_1^{\omega_1-\beta_1} \ldots q_k^{\omega_k-\beta_k}} \right), \text{ where } \beta = (\beta_1, \ldots, \beta_k).$$

Proof. To calculate the number of functions that lead to gammas with a period exactly equal to ℓ, we take the number of functions that lead to gammas with a period not greater than ℓ and subtract the number of functions that lead to gammas with a period less than ℓ.

The number of functions that lead to gammas with a period not greater than ℓ is equal to $2^{\ell+1}$. The remaining arguments are similar to those given in the proof of Theorem 1. ■

2.2. Combining model

Combiner generators use several LFSRs. Each register has its own length n_i and uses its own primitive polynomial for changing states. A Boolean function $h(X_1, \ldots, X_m)$ generates a pseudorandom sequence gamma, where X_i is a bit string of register i. The work of the combiner generator is shown in [16].

Since we do not use zero state in LFSR, the total number of states does not exceed $N = (2^{n_1} - 1)(2^{n_2} - 1) \ldots (2^{n_m} - 1)$. In this case, the maximum is reached when $(n_i, n_j) = 1$ for all $i, j \in \{1, \ldots, m\}$, $i \neq j$, and if all LFSRs have primitive feedback polynomials. Then a Boolean function can generate a gamma with a period ranging from 1 to N.

We consider a more general model of a combiner generator. This generalized combining model is used in ciphers such as Grain [12]. Note that the classical combining model does not allow to describe a number of modern stream ciphers based on the more complicated operating with bits from different registers.

Theorem 3. Let $n, m, n_1, \ldots, n_m \in \mathbb{N}$, $\sum\limits_{i=1}^{m} n_i = n$, and ℓ is a divisor of $(2^{n_1}-1)\ldots\times$ $\times(2^{n_m}-1)$, $\ell = q_1^{\omega_1} q_2^{\omega_2} \ldots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$, $k \in \mathbb{N}$. Then the number of ℓ-suitable Boolean functions in n variables for the combiner generator with LFSRs of lengths $n_1, \ldots, n_m$ all based on primitive polynomials is equal to

$$2^{2^n} - 2^{2^n-(2^{n_1}-1)\ldots(2^{n_m}-1)} \sum_{\beta\in\mathbb{F}_2^k, \beta\neq 0} \left((-1)^{\beta_1+\ldots+\beta_k+1} 2^{q_1^{\omega_1-\beta_1}\ldots q_k^{\omega_k-\beta_k}}\right),$$

where $\beta = (\beta_1, \ldots, \beta_k)$.

Proof. Number of ℓ-unsuitable sequences for the combiner generators is equal to U_ℓ, in view of Lemma 1. Since we use only $(2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_m}-1)$ states and the total number of states is equal to $2^{n_1}\,2^{n_2}\ldots 2^{n_m} = 2^n$, then we have $2^n - (2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_m}-1)$ states, where our function can be equal to 0 or 1. Therefore, for one of these states we have two functions. Thus, the number of ℓ-unsuitable Boolean functions in n variables for the combiner generators equals $2^{2^n-(2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_m}-1)}\,U_\ell$. Then, the number of ℓ-suitable functions is equal to $2^{2^n} - 2^{2^n-(2^{n_1}-1)\ldots(2^{n_m}-1)}\,U_\ell$. ■

Similarly, we propose to count the number of Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the combiner generator with LFSRs of lengths $n_1, \ldots, n_m$.

Theorem 4. Let $n, m, n_1, \ldots, n_m \in \mathbb{N}$, $\sum\limits_{i=1}^{m} n_i = n$, and ℓ is a divisor of $(2^{n_1}-1)\ldots\times$ $\times(2^{n_m}-1)$, $\ell = q_1^{\omega_1} q_2^{\omega_2} \ldots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$, $k \in \mathbb{N}$. Then the number of Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the combiner generator with LFSRs of lengths $n_1, \ldots, n_m$ all based on primitive polynomials is equal to

$$2^{\ell+(2^n-(2^{n_1}-1)\ldots(2^{n_m}-1))} - 2^{2^n-(2^{n_1}-1)\ldots(2^{n_m}-1)} \sum_{\beta\in\mathbb{F}_2^k, \beta\neq 0} ((-1)^{\beta_1+\ldots+\beta_k+1} 2^{q_1^{\omega_1-\beta_1}\ldots q_k^{\omega_k-\beta_k}}),$$

where $\beta = (\beta_1, \ldots, \beta_k)$.

Proof. The proof is similar to that of Theorem 2 with the remark that the number of functions that lead to gammas with a period not greater than ℓ is equal to $2^{\ell+(2^n-(2^{n_1}-1)\ldots(2^{n_m}-1))}$. ■

3. Functions for models with nonlinear registers

A nonlinear feedback shift register (NFSR) consists of two parts: a binary vector $x = (x_1, \ldots, x_n)$ of length n and a nonlinear state function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ in n variables.

Similarly to the linear case, let us consider the filter generator. We assume that NFSR passes over all 2^n states, i.e., it has the maximum possible period.

Theorem 5. Let $n \in \mathbb{N}$ and $\ell = 2^t$, $t \leqslant n$. Then the number of ℓ-suitable Boolean functions in n variables for the filter generator with NFSR of the maximum possible period is equal to $2^{2^n} - 2^{2^{t-1}}$.

Proof. The number of ℓ-unsuitable sequences for the filter generator with NFSR is equal to $2^{2^{t-1}}$. Since we use all the states then the number of ℓ-unsuitable sequences is equal to the number of ℓ-unsuitable Boolean functions. Hence, the number of ℓ-unsuitable Boolean functions in n variables for the filter generator with NFSR is equal to $2^{2^{t-1}}$. Therefore, the number of ℓ-suitable functions is $2^{2^n} - 2^{2^{t-1}}$. ■

Similarly, we propose to count the number of Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the filter generator with NFSR.

Theorem 6. Let $n \in \mathbb{N}$ and $\ell = 2^t$, where $t \leqslant n$. Then the number of ℓ-suitable Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the filter generator with NFSR of the maximum possible period is equal to $2^\ell - 2^{2^{t-1}}$.

Proof. To calculate the number of functions that lead to gammas with period exactly equal to ℓ, we take the number of functions that lead to gammas with a period not greater than ℓ (i.e., 2^ℓ) and subtract the number of functions that lead to gammas with a period less than ℓ (i.e., $2^{2^{t-1}}$). ■

There is another question related to NFSRs: how to determine for which nonlinear feedback functions NFSR of length n generates gamma with the maximum possible period 2^n? This question is still open.

REFERENCES

1. *Golić J. D.* On the security of nonlinear filter generators. LNCS, 1996, vol. 1039, pp. 173–188.
2. *Courtois N. T. and Meier W.* Algebraic attacks on stream ciphers with linear feedback. LNCS, 2003, vol. 2656, pp. 345–359.
3. *Salhab O., Jweihan N., Jodeh M. A., et al.* Survey paper: Pseudo random number generators and security tests. J. Theor. Appl. Inform. Technology, 2018, vol. 96, pp. 1951–1970.
4. *Hamza R.* A novel pseudo random sequence generator for image-cryptographic applications. J. Inform. Security Appl., 2017, vol. 35, pp. 119–127.
5. *Goresky M. and Klapper A.* Algebraic Shift Register Sequences. Cambridge, Cambridge University Press, 2012. 496 p.
6. *Menezes A. J., Van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. Boca Raton, CRC Press, 1996. 780 p.
7. *Márton K., Suciu A., Săcărea C., and Cret O.* Generation and testing of random numbers for cryptographic applications. Proc. Romanian Academy, 2012, vol. 13, pp. 368–377.
8. *Parvees M. Y. M., Samath J. A., and Bose B. P.* Cryptographically secure diffusion sequences — an attempt to prove sequences are random. Advances in Big Data and Cloud Computing. Advances in Intelligent Systems and Computing, 2019, vol. 750, pp. 433–442.
9. *Key E. L.* An analysis of the structures and complexity of nonlinear binary sequence generators. IEEE Trans. Inform. Theory, 1976, vol. 22, pp. 732–736.
10. *Gorodilova A. A.* Ot kriptoanaliza shifra k kriptograficheskomu svoystvu bulevoy funktsii [From cryptanalysis to cryptographic property of a Boolean function]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 16–44. (in Russian)
11. *Gluhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra [Algebra]. Moscow, Gelios ARV Publ., 2003. 336 p. (in Russian)
12. *Hell M., Johansson T., and Meier W.* Grain: A stream cipher for constrained environments. Intern. J. Wireless Mobile Computing, 2007, vol. 2, no. 1, pp. 86–93.
13. *Canteaut A.* A5/1. Encyclopedia of Cryptography and Security, Boston, Springer, 2011, pp. 1–2.
14. *Gollmann D.* Kaskadenschaltungen taktgesteuerter Schieberegister als Pseudozufallszahlengeneratoren. PhD thesis, Johannes Kepler Universität Linz, Wien, 1986. (in German)
15. *Bonich T. A., Panferov M. A., and Tokareva N. N.* On the number of unsuitable Boolean functions in constructions of filter and combining models of stream ciphers. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2020, vol. 13, pp. 78–80.

16. *Carlet C.* Boolean functions for cryptography and error-correcting codes. Y. Crama and P. L. Hammer (eds.). Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge, Cambridge University Press, 2010, pp. 257–397.
17. *Golomb S. W.* Shift Register Sequences. San Francisco, Holden-Day, 1967.