УДК 519.7 DOI 10.17223/2226308X/13/23

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

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

It is well known that every stream cipher is based on a good pseudorandom generator. For cryptographic purposes, we are interested in generation of pseudorandom sequences of the maximal possible period. A feedback register is one of the most known cryptographic primitives that is used in construction of stream generators. We analyze periodic properties of pseudorandom sequences produced by filter and combiner generators equipped with nonlinear Boolean functions. We determine which nonlinear functions in these schemes lead to pseudorandom sequences of not maximal possible period. We call such functions unsuitable and count the exact number of them for an arbitrary n.

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

Remember that a *feedback shift register* (*FSR*) contains two parts: a binary block $x = (x_{n-1}, \ldots x_0)$ of length n and a feedback function $f : (x_{n-1}, \ldots, x_0) \to \{0, 1\}$, where f is a Boolean function in n variables. First, we fill the block x with concrete values of bits; together they form the *initial state* of the register. For functioning of the FSR, the time is considered to be discrete, i.e., it is divided into clock cycles. On each clock cycle, the value of $f(x)$ is calculated first, then the state $x = (x_{n-1}, \ldots, x_1, x_0)$ of the register changes to the state $x' = (x_{n-2}, \ldots, x_0, f(x))$, and the bit x_{n-1} is written as the first bit of the generated sequence *gamma*.

The properties of gamma generated by FSR are well studied in the case when f is a linear function. If f is nonlinear [1], then there are too many open questions with properties of gamma that all are connected to analysis of nonlinear recurrent sequences [2, 3]. That is why in cryptography some nonlinear *combinations* of linear FSRs are considered, for instance, filter and combining models of stream generators [4, 5].

In this paper, we analyze pseudorandom sequences produced by filter and combiner generators. Namely, we study which nonlinear functions h in these schemes lead to pseudorandom sequences such that their periods are not maximally possible. We call such functions *unsuitable* and count the exact number of them for an arbitrary n.

A *linear feedback shift register* (*LFSR*) consists of two parts: a binary vector $x = (x_{n-1}, \ldots x_0)$ of length n and a linear feedback function f in n variables. A *state* of the register is a filling of vector x. During encryption, the register changes its states under an action of the feedback function. *Gamma* is a pseudorandom sequence generated by LFSR.

Also, LFSR can be specified using feedback polynomials. It is a polynomial of degree n defining bits to be summed. If $f(x_{n-1}, \ldots, x_0) = a_0 x_{n-1} \oplus a_1 x_{n-2} \oplus \cdots \oplus a_{n-1} x_0$, then the corresponding feedback polynomial is defined as $p(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + 1$. If $p(z)$ is a primitive polynomial, then the period of a pseudorandom sequence generated by LFSR is maximal, i.e., is equal to $2^n - 1$. Thererfore, linear feedback shift registers are usually considered with primitive polinomials.

[1] The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

1. Functions for the filter model

The filter generator consists of a single shift register of length n with a linear feedback and uses a primitive polynomial to change states. A Boolean function $h(x_{n-1},\dots,x_0)$, applied to the current state, generates a pseudorandom sequence gamma.

Let $\gamma=(y_1y_2\dots y_{2^n-1})$, where $y_1=h(x_{n-1},\dots,x_0)$, $y_2=h(x_{n-2},\dots,x_0,f(x_{n-1},\dots,x_0))$, etc. Since the number of all nonzero states is equal to 2^n-1, the maximal period of gamma is 2^n-1 too. In this paper, we would like do determine all Boolean function h in n variables that lead to gammas with non-maximum period. Let us call such functions *unsuitable.*

Note that the number of them does not depend on a linear feedback function. But whether the function is suitable or not for a given generator depends on the feedback function. When we count the number of unsuitable functions h, we do not consider a specific set of states. We say that there is a certain number of different states which the generator uses (all sets, that primitive polynomials generate, fit this definition). Next, we study which pseudorandom sequences have the maximum length. We analyze the number of unsuitable sequences and then the number of unsuitable functions. Thus, our reasonings do not affect the specific order of the states. Accordingly, for any set of states which the generator uses, there is the number of unsuitable functions h exactly that we calculated.

Theorem 1. Let n be an integer and $2^n-1=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$, where p_i are distinct prime numbers, α_i are positive integers, s is a some number. Then the number of unsuitable Boolean functions in n variables for the filter generator with LFSR based on a primitive polynomial is equal to

$$2\sum_{\beta\in\mathbb{F}_2^s,\beta\neq0}(-1)^{\beta_1+\dots+\beta_s+1}2^{p_1^{\alpha_1-\beta_1}\dots p_s^{\alpha_s-\beta_s}},$$

where $\beta=(\beta_1,\dots,\beta_s)$.

2. Functions for the combining model

Combiner generators use several linear feedback shift registers. Each register has its own length n_i and uses its primitive polynomial for changing states. A Boolean function $h(X_1,\dots,X_m)$ generates the pseudorandom sequence gamma where X_i is a register bit string i. Since we do not use the zero state in combiner generator, the total number of states does not exceed $(2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)$. In this case, the maximum is reached at $\gcd(n_i,n_j)=1$, where $i,j=1,\dots,m$, $i\neq j$, and if all LFSRs have primitive feedback polynomials. Then the Boolean function can generate a gamma with period from 1 to $(2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)$.

We consider a more general model of a combiner generator that is applied in ciphers Grain [6] and Bean [7]. 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. In this case, the combiner generator, in which the function depends only on the extreme bits of the registers, is included in the model we consider. In a nonlinear model sometimes it is more convenient to work with several smaller registers than with one large. It should be noted that the model that we consider can be used not only in cases of all linear or all non-linear registers, but also in cases of mixed registers (i.e., some registers are linear, some are non-linear).

Theorem 2. Let n be an integer, $\sum\limits_{i=1}^{m}n_i=n$, $(2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)=$ $=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$, where p_i are different prime numbers, $\alpha_i>0$, s is an integer. Then the number of unsuitable 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

$$2^{2^{n_1+n_2+\cdots+n_m}-(2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_m}-1)} \sum_{\beta\in\mathbb{F}_2^s,\beta\neq 0} (-1)^{\beta_1+\cdots+\beta_s+1} 2^{p_1^{\alpha_1-\beta_1}\ldots p_s^{\alpha_s-\beta_s}},$$

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

3. Functions for models with nonlinear registers

A *nonlinear feedback shift register* (*NFSR*) consists of two parts: a binary vector $x = (x_{n-1}, \ldots x_0)$ of length n and a nonlinear state function $f : (x_{n-1}, \ldots, x_0) \to \{0, 1\}$ in n variables.

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

Theorem 3. Let n be an integer. Then the number of unsuitable Boolean functions in n variables for the filter generator with NFSR of the maximal possible period is equal to $2^{2^{n-1}}$.

There is an another question related to NFSRs: how to determine for which nonlinear feedback functions NFSR of length n has the maximal possible period 2^n? This question is hard and still open.

We kindly thank the reviewer for careful reading of our paper and significant remarks.

REFERENCES

1. *Key E.* An analysis of the structure and complexity of nonlinear binary sequence generators. IEEE Trans. Inform Theory, 1976, no. 22, pp. 732–736.
2. *Gluhov M. M., Elizarov V. P., Nechaev A. A.* Algebra [Algebra]. Moscow, Gelios ARV Publ., 2003. (in Russian)
3. *Roman'kov V. A.* Vvedenie v kriptografiyu [Introduction to Cryptography]. Moscow, Forum Publ., 2012. (in Russian)
4. *Tokareva N. N.* Simmetrichnaya kriptografiya. Kratkiy kurs [Symmetric Cryptography. A Short Course]. Novosibirsk, NSU Publ., 2012.
5. *Carlet C.* Boolean functions for cryptography and error-correcting codes. Eds. P. Hammer and Y. Crama. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, Cambridge Univ. Press, 2010. Ch. 8, pp. 257–397. `www.math.univ-paris13.fr/~carlet/`.
6. *Hell M., Johansson T., and Meier W.* A stream cipher for constrained environments. Int. J. Wireless Mobile Comput., 2007, vol. 2, no. 1, pp. 86–93.
7. *Kumar N., Ojha S., Jain K., and Lal S.* BEAN: A lightweight stream cipher. Proc. 2nd Intern. Conf. SIN'2009, ACM, 2009, pp. 168–171.

UDC 621.391.7 DOI 10.17223/2226308X/13/24

EFFICIENT S-REPETITION METHOD FOR CONSTRUCTING AN IND-CCA2 SECURE MCELIECE MODIFICATION IN THE STANDARD MODEL

Y. V. Kosolapov, O. Y. Turchenko

The paper is devoted to the construction of IND-CCA2-secure modification of the McEliece cryptosystem in the standard model. The modification uses S-repetition