Math-Net.Ru

Общероссийский математический портал

Е. К. Alekseev, Е. К. Karelina, О. А. Logachev, О построении корреляционно-имунных функций с использованием минимальных функций, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 2, 7–22

DOI: <https://doi.org/10.4213/mvk251>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.27.143

26 апреля 2023 г., 14:25:17

On construction of correlation-immune functions via minimal functions

E. K. Alekseev¹, E. K. Karelina², O. A. Logachev²

¹ *CryptoPro LLC, Moscow*

² *Lomonosov Moscow State University, Moscow*

Получено 01.II.2017

Abstract. The use of correlation-immune functions in a cryptographic primitive may provide resistance against some key compromising methods. Designing of modern cryptographic primitives poses the challenge of constructing correlation-immune functions of a relatively large number of arguments. This paper proposes a method combining two basic approaches of solving this problem: iterative and a direct-search ones. Proposed method is based on minimal correlation-immune functions. The functions constructed by this method have no obvious structural characteristics that may be used to distinguish them from a random function.

The first stage of the proposed method is an easily implemented iteration procedure, which allows to construct many special functions that depend on the desired number of variables. At the second stage the constructed functions are used by some search procedure to find functions with given cryptographic properties. For the second stage the paper presents the reduction of the problem of searching for a resilient function with a preassigned order to the problem of solving a system of linear pseudo-Boolean equations. We also study how to apply a modification of the proposed method in order to improve the cryptographic parameters of the known “good” functions by means of small changes. Examples of successful applications of the methods described are given.

This work was supported by The Russian Foundation for Basic Research, project 16-01-00470-a.

Key words: Boolean functions, correlation-immune functions

О построении корреляционно-иммунных функций с использованием минимальных функций

Е. К. Алексеев¹, Е. К. Карелина², О. А. Логачев²

¹ ООО «КРИПТО-ПРО», Москва

² Московский государственный университет им. М. В. Ломоносова, Москва

Аннотация. Использование корреляционно-иммунных функций в криптографическом примитиве может обеспечить его стойкость относительно ряда методов определения ключа. В настоящее время разработка криптографического примитива требует построения корреляционно-иммунных функций от довольно большого количества переменных. В работе предлагается метод, основанный на использовании минимальных корреляционно-иммунных функций и комбинирующий два базовых подхода к решению указанной проблемы: итеративный метод и метод направленного поиска. Функции, получающиеся с помощью предложенного метода, не имеют явных структурных характеристик, которые можно было бы использовать для их отличия от случайных функций. Первый этап метода — просто реализуемая итеративная процедура, позволяющая построить множество функций специального вида, зависящих от заданного числа переменных. На втором этапе из построенных функций с помощью процедуры поиска строятся функции с заданными криптографическими характеристиками. В работе описано сведение задачи построения устойчивых функций заданного порядка к задаче решения системы псевдобулевых уравнений. Исследуется вопрос об использовании модификации предложенного метода для улучшения криптографических характеристик известных «хороших» функций с помощью малых изменений. Приводятся примеры применения разработанных методов.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 16-01-00470-а.

Ключевые слова: булевы функции, корреляционно-иммунные функции

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 2, pp. 7–22 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

1. Introduction

A cryptographic property of a Boolean function is generally referred to as the property providing resistance relative to a method of analysis of a cryptographic primitive based on this function. Most of these properties have been formulated as a result of the analysis of symmetric cryptographic primitives such as stream ciphers, block ciphers and hash functions.

Examples of cryptographic properties of Boolean functions are non-linearity (resistance to a linear cryptanalysis [12]), correlation immunity (resistance to some methods of correlation analysis [9], [10]), nondegeneracy (resistance to a method of analysis based on algebraically degenerate approximations [3]) and algebraic immunity (resistance to algebraic methods of analysis [11]).

A deep understanding of the specific properties, along with the relations among them, is especially important in the context of synthesis problems, since it helps to design schemes optimal in terms of security and efficiency. One of the most complete and profound descriptions of the status of research in this field may be found in [6].

There are several approaches to the solution of the problem of constructing a Boolean function with a given set of cryptographic properties.

The simplest is the brute-force search method that checks all the functions of a sufficiently large suitable set. The advantage of this method is its simplicity and reliability. However, this method may be used in practice only for small dimensions (for example, the method is applicable to the selection of transformations $V_4 \rightarrow V_4$ as in the block cipher Magma [7], but is much less effective when choosing transformations $V_8 \rightarrow V_8$ as in the block cipher Kuznechik [7]). The sets from which the functions are selected have to be chosen keeping in mind that the selected functions should possess certain positive properties.

The examples are the sets of the Maiorana–McFarland classes and $\mathcal{PS}$ [6]. The possibility of effective enumeration in sets of these classes follow from the regularity of their structure: elements of these sets are parameterized by some algebraic structures which in the aggregate may be informally called a “basis”. For the Maiorana–McFarland class such a “basis” may thus be considered as a direct product of a set of permutations on V_n and a set of Boolean functions of n variables (the cardinality of the set in this case is equal to $(2^n)! \cdot 2^{2^n}$). Regularity of the function structure of such classes may lead to the existence of the unremovable weaknesses. It has been shown in [5] that the use of a function from the Maiorana–McFarland class as a nonlinear function in a filter generator may considerably reduce the resistance to the threat of a key compromise.

Another method is called iterative. It consists in selecting some suitable function of a small number of variables (choosed by a brute-force search method) and using it to construct functions of larger numbers of variables by mean of some procedures guaranteeing that the resulting functions have the necessary properties. The iterations should be continued until the number of variables of constructed function reaches the required value. A method of this type had been proposed in [8]. The main aim of this method is not to construct functions to be used in primitives, but to get results on the reachability of some theoretical upper bounds for different parameters. Each algorithmic step associated with the increase in the number of variables adds some structure into a function. The acquired property may not always be positive from the perspective of cryptography. For example, a function $f_{10.2}^4$ constructed in [8] is algebraically degenerate (that is shown in [2]), which may lead to weakness described in [3].

In this paper a method for constructing a function with specified cryptographic properties based on a combination of the above approaches is presented. With regard to the enumeration part, the guaranteed property is a correlation immunity of the k -th order, and the set where the search is performed is a linear space of a special kind. That is to say, in this case, the analogical informal “basis” mentioned above is the basis of the space consisting of k -minimal correlation-immune functions. A simple iterative method for their construction is proposed in the paper. Meanwhile the method of enlarging the number of variables of the function depends on significant randomization when choosing parameters at each step. As a result at the final step there are not those structural properties that may be used to distinguish the constructed functions from the random ones and as a consequence to weaken the security. Further we describe the reduction of the problem of the search for a resilient (correlation-immune and balanced) function with given order in the built-up space to the problem of solving a system of linear pseudo-Boolean equations.

The proposed approach to the function construction may be modified in order to study the “neighbourhoods” of the already known functions. The subject of the research may be the search for functions with better cryptographic characteristics in the neighborhood under consideration. The values of the given cryptographic function f need to be changed slightly so that this change would not significantly worsen a certain part of its properties. Other characteristics are calculated directly. This change of function f consists in replacing the minimal correlation-immune functions into which it may be decomposed by the minimal functions of the same weight from the function decomposition $f \oplus 1$.

We present examples of functions with given properties constructed by means of the main method and examples of applications of the second method to some known functions.

2. Basic concepts and notations

Let $\mathbb{F}_2$ be a finite field of 2 elements. For any $n \in \mathbb{N}$ let

$$V_n = (\mathbb{F}_2 \times \cdots \times \mathbb{F}_2) = \mathbb{F}_2^n$$

be a vector space of dimension n with the components from the field $\mathbb{F}_2$, $V_n^* = V_n \setminus \{0^n\}$, where $0^n = (0, \dots, 0) \in V_n$. A Boolean function of n variables is a mapping from V_n into $\mathbb{F}_2$. Constant Boolean functions are denoted by $\mathbf{1}$ and $\mathbf{0}$. The set of all Boolean functions of n variables is denoted by $\mathcal{F}_n$. The support $\text{supp}(f)$ of a Boolean function $f \in \mathcal{F}_n$ is a set

$$\text{supp}(f) = \{x \in V_n \mid f(x) = 1\}.$$

The weight $\text{wt}(f)$ of a Boolean function $f \in \mathcal{F}_n$ is a cardinality of its support. The distance $\text{dist}(f, g)$ between $f \in \mathcal{F}_n$ and $g \in \mathcal{F}_n$ is the value of $\text{wt}(f \oplus g)$. The ordinate vector $f \in \mathcal{F}_n$ is a string $(f(x_{2^n-1}), \dots, f(x_0)) \in V_{2^n}$ (arguments are lexicographically ordered from right to left: $x_{2^n-1} = (1, 1, \dots, 1), \dots, x_1 = (0, 0, \dots, 0, 1), x_0 = (0, 0, \dots, 0)$). Algebraic degree $\deg(f)$ of a Boolean function $f \in \mathcal{F}_n$ of n variables is the number of variables in the largest monomial in ANF (Zhegalkin polynomial). For $u \in V_n$ a Boolean function l_u denotes a linear Boolean function $l_u(x) = \langle u, x \rangle$, where $\langle u, x \rangle = \bigoplus_{i=1}^n u_i \cdot x_i$ is a scalar product of vectors u and x . The number of essential variables of function l_u is equal to the weight of vector u . The set $\{l_u(x) \oplus b \mid u \in V_n, b \in \mathbb{F}_2\}$ of affine Boolean functions of n variables is denoted as $\mathcal{A}_n$. For a Boolean function $f \in \mathcal{F}_n$ its nonlinearity $\text{nl}(f)$ is the Hamming distance from the set of all affine functions $\mathcal{A}_n$:

$$\text{nl}(f) = \text{dist}(f, \mathcal{A}_n) = \min_{l \in \mathcal{A}_n} \text{dist}(f, l).$$

A Boolean function $f \in \mathcal{F}_n$ is correlation-immune of order m , $1 \leq m \leq n$ (further CI-function), if the equality $\text{wt}(f') = \text{wt}(f)/2^m$ holds for any subfunction f' of $n - m$ variables ([8]). In other words a Boolean function f has the maximal distance from the set of affine functions which essentially depend on $1, 2, \dots, m$ variables. A correlation-immune function of order m is also correlation-immune of any lower order, so we introduce the notation

$$\text{cor}(f) = \max\{m \in \mathbb{N} \mid f \text{ is correlation-immune of order } m\}.$$

Further we use the following notations:

$$\text{CI}(n, k) = \{f \in \mathcal{F}_n \mid \text{cor}(f) \geq k\} \quad \text{and} \quad \text{CI}(n) = \text{CI}(n, 1).$$

A balanced function $f \in \mathcal{F}_n$ is called k -resilient if $\text{cor}(f) \geq k$.

For the analysis of cryptographic properties of Boolean functions the Walsh–Hadamard transform is often used. The Walsh–Hadamard transform of a Boolean function $f \in \mathcal{F}_n$ is a function $W_f: V_n \rightarrow \mathbb{Z}$ such that $W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle u, x \rangle}$. The value $W_f(u)$ is called the Walsh–Hadamard coefficients (or Walsh coefficients). For example, there exists the following criteria of correlation-immunity of a function: a Boolean function $f \in \mathcal{F}_n$ is a correlation-immune function of order m , $0 < m \leq n$, if and only if for any vector $u \in V_n$ such that $1 \leq \text{wt}(u) \leq m$ the equality $W_f(u) = 0$ holds.

Let A be a $(n \times k)$ -matrix over $\mathbb{F}_2$ and $f \in \mathcal{F}_k$. Let f^A denotes a function from $\mathcal{F}_n$ defined by $f^A(x) = f(xA)$. The order of algebraic degeneracy $\text{AD}(f)$ of a Boolean function $f \in \mathcal{F}_n$ is the maximal possible value of $n - k$, where $0 \leq k \leq n$, such that there exist a function $g \in \mathcal{F}_k$ and a $(n \times k)$ -matrix A over $\mathbb{F}_2$ satisfying the equality $f = g^A$. Functions with $\text{AD}(f) > 0$ are algebraically degenerate. The set of all algebraically degenerate functions of n variables is denoted as $\text{DG}(n) = \{f \in \mathcal{F}_n \mid \text{AD}(f) > 0\}$. Nondegeneracy of a function $f \in \mathcal{F}_n$ (see [2]) is the following value:

$$\text{nd}(f) = \text{dist}(f, \text{DG}(n)).$$

3. Minimal correlation-immune functions

This section explains the meaning of k -minimal correlation-immune functions and provides a short overview of known properties of these objects.

Suppose we want to define a sufficiently large set of functions that are guaranteed to have correlation immunity of k -th order, $k \geq 1$. One of the simplest algebraic structures that allows the effective construction of its elements is a linear space. It is easy to see ([1]) that if $f, g \in \text{CI}(n, k)$ and $f \cdot g = \mathbf{0}$ (further functions with disjoint supports will be called *orthogonal*), then $f \oplus g \in \text{CI}(n, k)$. So the linear space L with the basis consisting of orthogonal functions $f_1, \dots, f_r \in \text{CI}(n, k)$ is a subset of the set $\text{CI}(n, k)$. Could this subspace be embedded into the larger space with the same property? This basis may be extended by a function $g = f_1 \oplus \dots \oplus f_r \oplus \mathbf{1}$ that belongs to a set $\text{CI}(n, k)$ due to the conditions specified above. Its support does not overlap with supports of other functions from the basis. Therefore, further we will consider only bases satisfying the condition $f_1 \oplus \dots \oplus f_r = \mathbf{1}$. The subspace which contains the subspace L and preserves the property of being the subset of set $\text{CI}(n, k)$ may be constructed not only by adding functions but also by the decomposition of existing functions f_i into sums of orthogonal functions $f'_i, f''_i \in \text{CI}(n, k)$. Then for the construction of superspace for L the function f_i is excluded from the basis of L and functions f'_i, f''_i are added.

The basis of the space L for which it is impossible to construct a superspace by this way consists of functions $f \in \text{CI}(n, k)$, which could not be represented as a sum $f = f' \oplus f''$ of functions $f', f'' \in \text{CI}(n, k)$ such that $f' \cdot f'' = \mathbf{0}$. Such functions will be called *k-minimal correlation-immune functions* (in this paper such functions will be called *k-minimal* for short).

The spaces with the basis consisting of mutually orthogonal functions are also useful, because the Walsh coefficient (except for the corresponding zero-argument) of the sum of any basis functions is equal to the sum of the Walsh coefficients of these functions. In the general case it is necessary to calculate the convolution of Walsh coefficients of summand (see [6]). As was mentioned above the apparatus of the Walsh coefficients is a powerful tool for the study of cryptographic properties of Boolean functions. Such structure of the considered spaces is used in Section 4.2 to reduce the problem of construction of resilient function of a given order to the problem of solving a system of linear pseudo Boolean equations.

A special case of *k-minimal* function was first investigated in [1]. In this paper the notion of 1-minimal function was introduced in order to investigate the structure of the set $\text{CI}(n)$. In [1] the following inequalities have been proven for a 1-minimal function $f: \text{cor}(f) \leq 2$, where equality is achievable (an example of a function of 7 variables exists), and for $n \geq 4$ the inequality $\text{wt}(f) < 2^{n-1}$ is true. Also the exact formula for the number of minimal functions of weight 4 has been proven. In [4] the numbers of 1-minimal functions of 4 and 5 variables has been estimated (32 and 1240 respectively), and also their classification under the Jevons group has been composed (see [6]).

4. Construction of resilient functions

In this section we describe a method for construction of the linear space of functions embedded in the set $\text{CI}(n, k)$, and reduction of the problem of resilient function of a given order construction to the problem of solving a system of linear pseudo Boolean equations.

4.1. Construction of 1-minimal functions with a given number of variables

The obvious method for constructing the above-mentioned space $L \subset \text{CI}(n, k)$ with a basis consisting of *k-minimal* functions $f_1, \dots, f_r$, $f_i \cdot f_j = \mathbf{0}$, $f_1 \oplus \dots \oplus f_r = \mathbf{1}$ is the decomposition of function $\mathbf{1}$ into a sum of such functions. Since $\text{cor}(\mathbf{1}) = n$, such decomposition exists for any k . The only known method of construction of such decomposition is a brute force search: in the beginning we assume $g = \mathbf{1}$, we are looking for *k-minimal* function f_1 whose support is nested within the support of g , when such function is found we are changing g by $g \oplus f_1$ and looking for f_2 taking in mind new g and so on.

The most laborious is to construct k -minimal function f_i such that $\text{supp}(f) \subset \text{supp}(g)$. We may effectively construct only 1-minimal functions of weight 2 and 4 because their structure is quite regular and well known (e.g. these functions are algebraically degenerate, see [1]). In another cases we can only test randomly chosen f_i such that $\text{supp}(f_i) \subset \text{supp}(g)$ for k -minimality. Here, the smaller $\text{wt}(g)$ the faster we find desired f_i .

In this section we describe an iterative method of constructing k -minimal functions of a given number of variables. The method is especially effective for the construction of 1-minimal functions. But in some cases this method allows to construct k -minimal functions for $k > 1$, however, the larger is the value of k , the smaller is the efficiency of the method.

Since, as mentioned above, the proposed method is especially effective for $k = 1$, a description of the method is given for this case.

During the first step 1-minimal functions of a small number of variables are constructed. These functions may be found using a simple brute force computing or taking from known sets (see, for example, [4]). At the second step the number of variables of 1-minimal functions constructed as a result of the first step increases.

Now describe a method of increasing the number of variables of 1-minimal functions.

The truth table of a function $f \in \mathcal{F}_n$ is called the matrix T_f of order $\text{wt}(f) \times n$. The rows of this matrix are lexicographically-ordered vectors from $\text{supp}(f)$. For example, for a function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_3 \in \mathcal{F}_3$

$$T_f = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Let

$$\mathcal{F}_n^w = \{f \in \mathcal{F}_n \mid \text{wt}(f) = w\}.$$

For any $w \in \{1, \dots, 2^n\}$ define the map $\text{AC}^{(w)} :$

$$\text{AC}^{(w)} : \mathcal{F}_n^w \times V_w \times \{1, \dots, n+1\} \mapsto \mathcal{F}_{n+1}^w.$$

The function $g = \text{AC}_{v,i}^{(w)}(f) = \text{AC}^{(w)}(f, v, i)$ is defined as follows. The matrix $\text{wt}(f) \times (n+1)$ is formed by inserting vector v of dimension w in the truth table T_f as i -th column (i -th and following columns of T_f are shifted to the right). The rows of formed matrix constitute a support of a function g . If $i = n+1$, then the column is inserted as the last column.

The proofs of the following statements are given in Appendix.

Theorem 1. *Let $f \in \text{CI}(n)$ and $w = \text{wt}(f)$. Then for any $v \in V_w$ such that $\text{wt}(v) = w/2$ and for any $i \in \{1, \dots, n+1\}$*

$$g = \text{AC}_{v,i}^{(w)}(f) \in \text{CI}(n+1).$$

Let $\text{MCI}(n, k)$ be a set of k -minimal functions of n variables.

Theorem 2. *Let $f \in \text{MCI}(n, 1)$ and $w = \text{wt}(f)$. Then for any $v \in V_w$ such that $\text{wt}(v) = w/2$, and for any $i \in \{1, \dots, n+1\}$*

$$g = \text{AC}_{v,i}^{(w)}(f) \in \text{MCI}(n+1, 1).$$

By Theorem 2 the map AC may be used to increase the number of variables of 1-minimal functions. The presence of variable parameters v and i allows to obtain the set of minimal functions of a larger number of variables using the “start” function $f \in \text{MCI}(n, 1)$.

For construction of k -minimal functions, $k > 1$, by means of the map AC the condition $\text{wt}(v) = w/2$ is no longer sufficient. The problem of developing the effective methods for construction of k -minimal functions for $k > 1$ is not solved at the moment.

Besides the use in the synthesis, Theorems 1 and 2 may be used for research of the structure of minimal functions.

4.2. Search for a function with a given order of correlation immunity

This section describes the reduction of the problem search for a resilient function with a given order in the space that is formed by mutually orthogonal k -minimal functions to the problem of solving a system of linear pseudo Boolean equations.

Let $L \subset \text{CI}(n, k)$ be a linear space with a basis $f_1, \dots, f_r \in \text{CI}(n, k)$ and $f_i \cdot f_j = 0$ for any $i \neq j$. Suppose we want to find $(k+m)$ -resilient function g in the space L , in other words this function must satisfy the conditions

$$\text{wt}(g) = 2^{n-1} \quad \text{and} \quad \text{cor}(g) \geq (k+m), m \geq 1,$$

or to prove that such function doesn't exist in the space L .

Since the basis of the space L consists of mutually orthogonal functions, then for any u , $\text{wt}(u) > 0$, and for any $g = b_1 \cdot f_1 \oplus \dots \oplus b_r \cdot f_r$, $b_1, \dots, b_r \in \mathbb{F}_2$, the following equation is true:

$$W_g(u) = b_1 \cdot W_{f_1}(u) + \dots + b_r \cdot W_{f_r}(u).$$

For g to be a CI-function of order $k + m$ it is necessary and sufficient that for any u , $1 \leq \text{wt}(u) \leq k + m$, the equality

$$W_g(u) = 0$$

is true. Since

$$f_i \in CI(n, k),$$

then

$$W_{f_i}(u) = 0$$

for any u such that

$$1 \leq \text{wt}(u) \leq k.$$

Consequently, similar equations hold for g .

In order to check whether the function g satisfies the condition

$$\text{cor}(g) \geq k + m,$$

it is sufficient to verify correctness of

$$\binom{n}{k+1} + \dots + \binom{n}{k+m}$$

equations

$$b_1 \cdot W_{f_1}(u) + \dots + b_r \cdot W_{f_r}(u) = 0$$

for all u such that

$$k + 1 \leq \text{wt}(u) \leq k + m.$$

Further, since the supports of the functions of the basis do not intersect, then condition $\text{wt}(g) = 2^{n-1}$ is true if

$$b_1 \cdot \text{wt}(f_1) + \dots + b_r \cdot \text{wt}(f_r) = 2^{n-1}.$$

In order to find $(k + m)$ -resilient function $g \in L$, it is sufficient to find $(0, 1)$ -solutions $(b_1, \dots, b_r)$ of a system of

$$\binom{n}{k+1} + \dots + \binom{n}{k+m} + 1$$

linear equations

$$\begin{cases} b_1 \cdot W_{f_1}(u) + \dots + b_r \cdot W_{f_r}(u) = 0 \\ \quad \text{for } u \text{ with } k + 1 \leq \text{wt}(u) \leq k + m, \\ b_1 \cdot \text{wt}(f_1) + \dots + b_r \cdot \text{wt}(f_r) = 2^{n-1}. \end{cases}$$

Since the target solutions are only $(0, 1)$ -solutions, this system is a pseudo Boolean system. This reduction allows to use different methods of solving such system for the construction of $(k + m)$ -resilient Boolean function. In particular, we can effectively check whether the space L contains resilient functions of a given order by checking the compatibility of this system of equations over the field of real numbers. The problem of estimating the probability of passing such checking by system without $(0, 1)$ -solutions is open.

5. Using minimal functions for the analysis of neighbourhoods of known functions

The approach described above may be used not only for the construction of cryptographic functions “from scratch”. Suppose that there exists some function $f \in \mathcal{F}_n$ of a given number of arguments, which satisfies only a part of the necessary requirements. Such case may arise after the appearance of a previously unknown cryptanalytic method which weakens the security of f .

The function f with $\text{cor}(f) \geq k$ may be a base for constructing a basis $\mathcal{M}$ consisting of k -minimal functions. This basis will be constructed in such a way that f is contained in the space L formed by functions from $\mathcal{M}$. For this purpose it's sufficient to create the basis $\mathcal{M}$ from orthogonal k -minimal functions, which constitute the decompositions of functions f and $f \oplus 1$.

When searching for functions from L satisfying the specified requirements the main part of these functions are taken from the decomposition of f , and a few functions are taken from the decomposition of $f \oplus 1$. These few functions are chosen to change the weight of the sum of already selected functions to the desired value. Thus the resulting functions have a relatively short distance from f , that is belong to some “neighbourhood” of the function f . At the same time the order of correlation-immunity of resulting functions isn't smaller than k .

The effectiveness of the described approach to the construction of the basis consisting of k -minimal functions currently has no rigorous justification, that is, it is not known whether spaces constructed by this way are guaranteed to contain a lot of “good” functions. However in the next section the results obtained by this method are described.

6. The results of application of the proposed methods

This section briefly lists the specific results obtained by the approaches and methods that have been described above. The missing details, such as, for example, the vectors of values for considered functions are given in Appendix.

Consider the function $f_{10,2}^4 \in \mathcal{F}_{10}$ from [8], which will be denoted by f_T . This function has the following parameters:

$\text{wt}(f_T) = 512$	$\text{cor}(f_T) = 6$	$\text{deg}(f_T) = 3$	$\text{nl}(f_T) = 384$	$\text{nd}(f_T) = 0$
------------------------	-----------------------	-----------------------	------------------------	----------------------

The trouble with this function from the cryptographic viewpoint is its algebraic degeneracy ($\text{nd}(f_T) = 0$). Using the method described in Section 5 (functions f_T and $f_T \oplus \mathbf{1}$ were decomposed into sums of 128 1-minimal functions with the weight 4), the new function g_T is constructed with the following parameters:

$\text{wt}(g_T) = 512$	$\text{cor}(g_T) = 2$	$\text{deg}(g_T) = 7$	$\text{nl}(g_T) = 360$	$\text{nd}(g_T) = 8$
------------------------	-----------------------	-----------------------	------------------------	----------------------

This function is not algebraically degenerate, and decrease of correlation-immunity $\text{cor}(g_T)$ and nonlinearity $\text{nl}(g_T)$ is offsetted by a significant increase of the parameter $\text{deg}(g_T)$. At the same time $\text{dist}(f_T, g_T) = 40$.

The similar method was applied to the filter function $f_c \oplus \mathbf{1}$, where f_c is used in stream cipher LILI128 [13]. This function of 10 variables has the following parameters:

$\text{wt}(f_c) = 512$	$\text{cor}(f_c) = 3$	$\text{deg}(f_c) = 6$	$\text{nl}(f_c) = 480$	$\text{nd}(f_c) = 80$
------------------------	-----------------------	-----------------------	------------------------	-----------------------

After using the method described in Section 5 the new function g_c is constructed with the following parameters:

$\text{wt}(g_c) = 512$	$\text{cor}(g_c) = 3$	$\text{deg}(g_c) = 6$	$\text{nl}(g_c) = 480$	$\text{nd}(g_c) = 112$
------------------------	-----------------------	-----------------------	------------------------	------------------------

The function g_c is not worse than the function f_c on any parameter, and the value of algebraic degeneracy $\text{nd}(g_c)$ greatly exceeds $\text{nd}(f_c)$. At the same time $\text{dist}(f_c \oplus \mathbf{1}, g_c) = 288$. Thus by means of the proposed approaches the function g_c is constructed and using g_c instead of f_c in the cipher LILI128 may improve its cryptographic properties.

In conclusion we give an example of constructing of a function without the use of known “good” functions. In the space consisting from 1-minimal functions of 10 variables with the weight 2 the 7-resilient function f_2 is found with the following parameters:

$\text{wt}(f_2) = 512$	$\text{cor}(f_2) = 7$	$\text{deg}(f_2) = 2$	$\text{nl}(f_2) = 256$	$\text{nd}(f_2) = 0$
------------------------	-----------------------	-----------------------	------------------------	----------------------

This function achieves the upper bound for nonlinearity for 7-resilient functions (see, for example, [8]). Functions with the same parameters may be constructed by the method described in [8].

7. Open problems

The concept of a minimal correlation-immune function has been introduced recently, so nowadays there is a number of open issues related to the properties of these functions. The following problems are the most important in the context of the main theme of this article in our opinion.

1. Searching for efficient criteria of the k -minimality of a given function.
2. Developing a method of increasing the number of variables of k -minimal functions, $k > 1$, which is as effective as for the $k = 1$.
3. Developing of efficient method of searching for balanced functions with a given values of nonlinearity/nondegeneracy/algebraic immunity in the space generated by k -minimal functions.

8. Conclusion

In this paper the approach to the construction of Boolean functions with a given cryptographic parameters is given. This method is based on a combination of iterative and exhaustive search methods. On the basis of this approach a method of synthesis a resilient functions with a given order is developed, which uses minimal correlation-immune functions. Functions constructed by this method have no obvious structural features that could help to distinguish them from random functions.

In this paper the transformations are proposed, and their applicability to the realisation of the first step of the developed method is shown. The reduction of the problem of search for resilient function with a given order at the second step of proposed method to the problem of solving a system of linear pseudo Boolean equations is described. Also the approach to improve the method's characteristics with using known «good» cryptographic functions is proposed. Examples of the successful application of this method are given. For example, we have constructed a function that is not worser than the filter function in the stream cipher LILI128 with respect to many cryptographic parameters and exceeds it by nondegeneracy. So it may improve the cryptographic properties of this cipher.

The authors are grateful to Grigory Anatolyevich Karpunin, Grigory Borisovich Marshalko and Andrei Mihailovich Zubkov for their valuable comments and constructive criticism.

References

- [1] Alekseev E. K., “Some algebraic and combinatorial properties of correlation-immune Boolean functions”, *Diskretnaya matematika*, **22**:3 (2010), 110–126 (in Russian).
- [2] Alekseev E. K., “Some measures of nonlinearity of Boolean functions”, *Prikladnaya diskretnaya matematika*, № 2 (2011), 5–16 (in Russian).
- [3] Alekseev E. K., “Filtering generator attacks with function close to algebraically degenerate”, *Sbornik statej molodyh uchenyh fakul'teta VMK MSU*, № 8 (2011), 19–32 (in Russian).
- [4] Alekseev E. K., Karelina E. K., “Classification of correlation-immune and minimal correlation-immune functions of 4 and 5 variables”, *Diskretnaya matematika*, **27**:1 (2015), 22–33 (in Russian).
- [5] Kuschinskaja L. A., “Research in applicability limits of shift register-based stream ciphers cryptanalysis methods”, *Master degree thesis. MSU, CMC Faculty* (2015) (in Russian), 34 pp.
- [6] Logachev O. A., Salnikov A. A., Smyshlyaev S. V., Yashchenko V. V., *Boolean functions in coding theory and cryptology*, Moscow: URSS, 2015 (in Russian), 576 pp.
- [7] *GOST R 34.12–2015. Information technology. Information security. Block ciphers*: Federal Agency on Technical Regulating and Metrology, 2015 (in Russian).
- [8] Tarannikov Yu. V., “Correlation-immune and resilient Boolean functions”, *Matematicheskie voprosy kibernetiki*, **11** (2002), 91–148 (in Russian).
- [9] Siegenthaler T., “Decrypting a class of stream cipher using ciphertext only”, *IEEE Trans. Comput.*, **34**:1 (1985), 81–85.
- [10] Meier W., Staffelbach O., “Fast correlation attacks on certain stream ciphers”, *J. of Cryptology*, **1** (1989), 159–176.
- [11] Courtois N., Meier W., “Algebraic attacks on stream ciphers with linear feedback”. In: “*EUROCRYPT'03*”, Lect. Notes Comput. Sci., **2656**, 346–359.
- [12] Matsui M., “Linear cryptanalysis method for DES cipher”. In: “*EUROCRYPT'93*”, Lect. Notes Comput. Sci., **765**, 1994, 386–397.
- [13] Dawson E., Clark A., Golich J., Millan W., Penna L., Simpson L., “The LILI-128 keystream generator”. In: “*Proc. of the first NESSIE workshop*”, 2000, 1–14.

9.3. The proof of Theorem 2

Proof. From Theorem 1 it follows that $g \in \text{CI}(n+1)$. It remains to prove that g is a 1-minimal function.

Assume that this is not true. Then from the support of a function g a subset may be selected which is a support of function h with $\text{cor}(h) \geq 1$. Then the i -th column is deleted from the table T_h (it corresponds to the insertion of column v in the table T_f). The result is a matrix with non-repeated rows, because these rows correspond to certain rows of the matrix T_f . By arranging these rows lexicographically we get a new truth table of some function h' , where $\text{supp}(h') \subset \text{supp}(f)$. Further we use the arguments from the proof of Theorem 1. The columns of $T_{h'}$ are balanced because they are columns of the table T_h , and $\text{cor}(h) \geq 1$. So $\text{cor}(h') \geq 1$, and this contradicts with the minimality of the original function f . $\square$