МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

UDC 519.7 DOI 10.17223/20710410/38/4

SUBSTITUTION BLOCK CIPHERS WITH FUNCTIONAL KEYS[1]

G. P. Agibalov

National Research Tomsk State University, Tomsk, Russia

We define a substitution block cipher $\mathcal{C}$ with the plaintext and ciphertext blocks in $\mathbb{F}_2^n$ and with the keyspace $K_{s_0,n}(g)$ that is the set $\{f(x) : f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})));$ $\sigma_1, \sigma_2 \in \mathbb{F}_2^n; \pi_1, \pi_2 \in S_n\}$, where s_0 is an integer, $1 \leqslant s_0 \leqslant n$; $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a bijective vector function $g(x) = g_1(x)g_2(x) \ldots g_n(x)$ such that every its coordinate function $g_i(x)$ essentially depends on some $s_i \leqslant s_0$ variables in the string $x = x_1x_2 \ldots x_n$; S_n is the set of all permutations of the row $(1\ 2\ \ldots n)$; π_i and σ_i are the permutation and negation operations, that is, $(\pi = (i_1i_2 \ldots i_n)) \Rightarrow (\pi(a_1a_2 \ldots a_n) = a_{i_1}a_{i_2} \ldots a_{i_n})$, $(\sigma = b_1b_2 \ldots b_n) \Rightarrow ((a_1a_2 \ldots a_n)^\sigma = a_1^{b_1}a_2^{b_2} \ldots a_n^{b_n})$ and, for a and b in $\mathbb{F}_2$, $a^b = a$ if $b = 1$ and $a^b = \neg a$ if $b = 0$. Like g, any key f in $K_{s_0,n}(g)$ is a bijection on $\mathbb{F}_2^n$, $f(x) = f_1(x)f_2(x) \ldots f_n(x)$, and every its coordinate function $f_i(x)$ essentially depends on not more than s_0 variables in x. The encryption of a plaintext block x and the decryption of a ciphertext block y on the key f are defined in $\mathcal{C}$ as follows: $y = f(x)$ and $x = f^{-1}(y)$. Here, we suggest a known plaintext attack on $\mathcal{C}$ with the threat of discovering the key f that was used. Let $P_1, P_2, \ldots, P_m$ be some blocks of a plaintext, $C_1, C_2, \ldots, C_m$ be the corresponding blocks of a ciphertext, i.e., $C_l = f(P_l)$ for $l = 1, 2, \ldots, m$, and $P_l = P_{l1}P_{l2} \ldots P_{ln}$, $C_l = C_{l1}C_{l2} \ldots C_{ln}$. The object is to determine the coordinate function $f_i(x)$ of f for each $i \in \{1, 2, \ldots, n\}$. The suggested attack consists of two steps, namely we first determine the essential variables $x_{i_1}, \ldots, x_{i_s}$ of $f_i(x)$ and then compute a Boolean function $h(x_{i_1}, \ldots, x_{i_s})$ such that $h(a_{i_1}, \ldots, a_{i_s}) = f_i(a_1, \ldots, a_n)$ for all n-tuples $(a_1a_2 \ldots a_n) \in \mathbb{F}_2^n$. For determining the essential variables of f_i, we construct a Boolean matrix $||\inf D(f_i)||$ with the set of rows $\inf D(f_i)$, where $D(f_i) = \{P_l \oplus P_j : C_{li} \neq C_{ji};\ l, j = 1, 2, \ldots, m\}$, $C_{li} = f_i(P_l)$, $l = 1, \ldots, m$, $i = 1, \ldots, n$, and $\inf D(f_i)$ is the subset of all the minimal vectors in $D(f_i)$. Then the numbers of essential variables for f_i are the numbers of columns in the intersection of all covers of $||\inf D(f_i)||$ with the cardinalities not more than s_0, where a cover of a Boolean matrix M is defined as a subset C of its columns such that each row in M has '1' in a column in C. For computing $h(x_{i_1}, \ldots, x_{i_s})$, we first set $h(P_{li_1}, \ldots, P_{li_s}) = C_{li}$ for $l = 1, \ldots, m$ and then, if h_i is not yet completely determined on $\mathbb{F}_2^s$, we increase the number m of known blocks (P_i, C_i) of plain- and ciphertexts or extend h_i on $\mathbb{F}_2^s$ in such a way that the vector function $h = h_1h_2 \ldots h_n$ with the completely defined coordinate functions is a bijection on $\mathbb{F}_2^n$. We also describe some special known plaintext attacks on substitution block ciphers with keyspaces being subsets of $K_{s_0,n}(g)$.

Keywords: *substitution ciphers, block ciphers, functional keys, cryptanalysis, known plaintext attack, Boolean functions, essential variables, bijective functions.*

[1] The author was supported by the RFBR-grant no. 17-01-00354.

1. Introduction

In cryptography, the cryptosystems with the functional keys are widely used as cryptographic primitives including key-stream generators, s-boxes, cryptofilters, cryptocombiners, key hash functions as well as the symmetric and public-key ciphers, digital signature schemes. For the author, the research, including the definition, characterisation and cryptanalysis of such cryptosystems had beginnings at the 1960-th years. First object of this research was the key-stream generator based on a finite autonomous automaton (state machine) with the output function depending on a bounded number of coordinates of the automaton state and being the key of the generator and of the corresponding stream cipher [1, 2]. Later, two sets of symmetric iterative block ciphers with the functional keys were proposed [3]. They were constructed according to the known cryptographic schemes originally suggested by H. Feistel and implemented in the ciphers LUCIFER and DES and, therefore, were named after Lucifer and Feistel respectively. At the last years, our research in this area was related to definitions and cryptanalysis and synthesis methods for some other kinds of cryptalgorithms with functional keys including watermarking ciphers [4], finite automata cryptographic generators with two-valued controlled steps [5], and cryptautomata [6] where a cryptautomaton is described by a set C of automata networks and a set K of keys such that the choosing a key in K determines a network in C as a specific cryptographic algorithm. In the case, when the key contains transition and (or) output functions of some components in networks in C, we have a cryptosystem with the functional keys. In this paper, we describe another class of cryptosystems with functional keys, namely that named in the title.

2. Definition

Here is a general formal mathematical definition of the ciphers under consideration. Let $\mathcal{C}$ be a symmetric cipher and $\mathcal{C} = (X, Y, K, E, D)$, where X, Y, and K are the sets of plaintexts, ciphertexts and keys respectively and E and D are, respectively, the encryption and decryption algorithms, $E : X \times K \to Y$, $D : Y \times K \to X$ and $E(x, k) = y \Rightarrow D(y, k) = x$ for any $x \in X$, $y \in Y$, and $k \in K$. Suppose $X = Y = \mathbb{F}_2^n$, $K \subseteq B^n$, B is a class of Boolean functions having some bounded both computational and capacity complexities and depending on not more than n variables such that the mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, defined for $x \in X$ and $f_1 f_2 \ldots f_n \in K$ as $f(x) = f_1(x) f_2(x) \ldots f_n(x)$, is a bijection. In this case, the cipher $\mathcal{C}$ is said to be a *substitution block cipher with functional keys*, or, shortly, a *funkeysubcipher*. For each block $x = x_1 x_2 \ldots x_n \in X$, for each key $k = f_1 f_2 \ldots f_n \in K$, and for each ciphertext $y \in Y$ in it, we have $E(x, k) = f(x)$ and $D(y, k) = f^{-1}(y)$. Further, these equalities are called the *invertibility condition* of $\mathcal{C}$.

Note that in this definition, the bounded complexity of a function means the existence of its practical specification and computation.

As usually, there are two general problems in the funkeysubcipher theory — synthesis and analysis. The second problem is very typical of block ciphers and its solving ways significantly depend on the way the first problem is solved. According to the definition above, the first problem consists in generating a proper key space K, namely which is over a set B of Boolean functions of a bounded complexity, satisfies the invertibility conditions, and is great enough to withstand exhaustive search attacks. A method for solving this problem is described in the following section.

3. Synthesis method

Let IS_n denote the set of all invertible systems each consisting of n functions in B. Further, we also consider the systems in IS_n as Boolean bijective vector functions, that is, as substitutions on $\mathbb{F}_2^n$. To synthesize a funkeysubcipher $\mathcal{C} = (\mathbb{F}_2^n, K, \mathbb{F}_2^n, E, D)$, where $K \subseteq IS_n$, we need generating the vector functions in IS_n as keys in K. Without knowing how to generate all of them, we propose here to generate keys in K as some members of IS_n which can be obtained by inverse and permutation operations over bits on inputs and outputs of a chosen or given function in IS_n. For this purpose, we, first, introduce some auxiliary notations related to the permutation and inverse operations and, then, define some subsets of functions in B^n.

Let S_n be the set of all the permutations of numbers 1, 2, $\ldots$, n, namely $S_n = \{i_1 i_2 \ldots i_n : i_j \in \{1,2,\ldots,n\}; j \neq k \Rightarrow i_j \neq i_k; j,k \in \{1,2,\ldots,n\}\}$. For any permutation $\pi = i_1 i_2 \ldots i_n \in S_n$ and any vector $v = v_1 v_2 \ldots v_n$, let $\pi(v_j) = v_{i_j}$, $j = 1,2,\ldots,n$, and $\pi(v) = \pi(v_1)\pi(v_2)\ldots\pi(v_n) = v_{i_1} v_{i_2} \ldots v_{i_n}$. Also, if $v_1, v_2, \ldots, v_n$ are Boolean values (variables or constants) and $\sigma = b_1 b_2 \ldots b_n \in \mathbb{F}_2^n$, then let $v^\sigma = v_1^{b_1} v_2^{b_2} \ldots v_n^{b_n}$, where, for any Boolean values a and b, $a^b = \neg a$ if $b = 0$ and $a^b = a$ if $b = 1$. We say that $\pi(v)$ and v^σ are obtained by, respectively, *permutation* and *inverse* operations π and σ over v. In cases when $\pi = 12\ldots n$ or $\sigma = 11\ldots 1$, that is, the operations π or σ are identity ones, we write $\pi = 1$ or $\sigma = 1$ respectively.

Taking any $g(x_1, x_2, \ldots, x_n)$ in IS_n, σ_1, σ_2 in $\mathbb{F}_2^n$, and π_1, π_2 in S_n, we then can define a vector function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ as $f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$, $x = x_1 x_2 \ldots x_n$. Particularly, $g(x)$ can be the identical function, that is, for each i in $\{1,2,\ldots,n\}$ its coordinate function $g_i(x)$ can be equal to x_i. In any case, the table of the function $f(x)$ is obtained from the table of the function $g(x)$ by

- substituting columns corresponding to some variables for inverses (in σ_1),
- transposing (according to π_1) columns corresponding to some variables,
- substituting columns corresponding to some coordinate functions of $g(x)$ for inverses (in σ_2), and
- transposing (according to π_2) columns corresponding to some coordinate functions of the function $g(x)$.

In other words, $f(x)$ is computed from the function $g(x)$ by the inversion and transposition of some its inputs and outputs and, like g, is of a bounded complexity and satisfies the invertibility condition. Therefore, $f(x) \in IS_n$.

Define $K_n(g) = \{\pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1}))) : \sigma_1, \sigma_2 \in \mathbb{F}_2^n, \pi_1, \pi_2 \in S_n\}$. Thus, we get that $K_n(g) \subseteq IS_n$ and $|K_n(g)| \leqslant (2^n n!)^2$. Any subset $K \subseteq K_n(g)$ of an exponential cardinality can be taken as a synthesis result — the key space of a funkeysubcipher $\mathcal{C}$. The following subsets of $K_n(g)$ are possible candidates for playing this role:

$K_n(g,1) = \{g(x^{\sigma_1}) : \sigma_1 \in \mathbb{F}_2^n\}$, $|K_n(g,1)| \leqslant 2^n$;
$K_n(g,2) = \{g(\pi_1(x)) : \pi_1 \in S_n\}$, $|K_n(g,2)| \leqslant n!$;
$K_n(g,3) = \{g(\pi_1(x^{\sigma_1})) : \sigma_1 \in \mathbb{F}_2^n, \pi_1 \in S_n\}$, $|K_n(g,3)| \leqslant 2^n n!$;
$K_n(g,4) = \{g^{\sigma_2}(x) : \sigma_2 \in \mathbb{F}_2^n\}$, $|K_n(g,4)| \leqslant 2^n$;
$K_n(g,5) = \{g^{\sigma_2}(x^{\sigma_1}) : \sigma_1, \sigma_2 \in \mathbb{F}_2^n\}$, $|K_n(g,5)| \leqslant 2^{2n}$;
$K_n(g,6) = \{g^{\sigma_2}(\pi_1(x)) : \sigma_2 \in \mathbb{F}_2^n, \pi_1 \in S_n\}$, $|K_n(g,6)| \leqslant 2^n n!$;
$K_n(g,7) = \{g^{\sigma_2}(\pi_1(x^{\sigma_1})) : \sigma_1, \sigma_2 \in \mathbb{F}_2^n, \pi_1 \in S_n\}$, $|K_n(g,7)| \leqslant 2^{2n} n!$;
$K_n(g,8) = \{\pi_2(g(x)) : \pi_2 \in S_n\}$, $|K_n(g,8)| \leqslant n!$;
$K_n(g,9) = \{\pi_2(g(x^{\sigma_1})) : \sigma_1 \in \mathbb{F}_2^n, \pi_2 \in S_n\}$, $|K_n(g,9)| \leqslant 2^n n!$;
$K_n(g,10) = \{\pi_2(g(\pi_1(x))) : \pi_2, \pi_1 \in S_n\}$, $|K_n(g,10)| \leqslant (n!)^2$;

$K_n(g,11) = \{\pi_2(g(\pi_1(x^{\sigma_1}))) : \sigma_1 \in \mathbb{F}_2^n, \pi_1, \pi_2 \in S_n\}$, $|K_n(g,11)| \leqslant 2^n(n!)^2$;
$K_n(g,12) = \{\pi_2(g^{\sigma_2}(x)) : \sigma_2 \in \mathbb{F}_2^n, \pi_2 \in S_n\}$, $|K_n(g,12)| \leqslant 2^n n!$;
$K_n(g,13) = \{\pi_2(g^{\sigma_2}(x^{\sigma_1})) : \sigma_1, \sigma_2 \in \mathbb{F}_2^n, \pi_2 \in S_n\}$, $|K_n(g,13)| \leqslant 2^{2n} n!$;
$K_n(g,14) = \{\pi_2(g^{\sigma_2}(\pi_1(x))) : \sigma_2 \in \mathbb{F}_2^n, \pi_1, \pi_2 \in S_n\}$, $|K_n(g,14)| \leqslant 2^n(n!)^2$;
$K_n(g,15) = K_n(g)$.

4. Funkeysubciphers with key functions in a bounded number of essential variables

Let s_0 and n be some integers, $1 \leqslant s_0 \leqslant n$, and $B_{s_0,n}$ be the set of all Boolean functions $f(x_1,\ldots,x_n)$ essentially depending on not more than s_0 variables $x_1,\ldots,x_n$, that is, for any $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

$$f(x_1,\ldots,x_n) \in B_{s_0,n} \Leftrightarrow$$
$$\Leftrightarrow \exists s \leqslant s_0\ \exists i_1,\ldots,i_s \in \{1,\ldots,n\} \exists g : \mathbb{F}_2^s \to \mathbb{F}_2 (f(x_1,\ldots,x_n) = g(x_{i_1},\ldots,x_{i_s})).$$

The set of variables $x_{i_1},\ldots,x_{i_s}$ satisfying this equation is said to be a *sufficient subset* of arguments for the function f. If U is a sufficient subset for f and, for any $V \subset U$, V isn't a sufficient for f, then the variables in U are said to be *essential* arguments for f. For natural $s \leqslant s_0$, let $B^*_{s,n}$ be the set of all functions in $B_{s_0,n}$ essentially depending on exactly s variables. It is clear that $B_{s_0,n} = \bigcup\limits_{s=1}^{s_0} B^*_{s,n}$. We suppose that the number s_0 is small enough for accepting functions in $B_{s_0,n}$ to be of a bounded complexity.

Let $IS_{s_0,n}$ denote the set of all bijective Boolean vector functions each consisting of n coordinate functions in $B_{s_0,n}$. Balancedness of each coordinate function of a Boolean vector function f is the necessary condition for bijectivity of f. So the cardinality of $IS_{s_0,n}$ doesn't exceed the number $N_{s_0,n} = \left(\binom{n}{s_0}\binom{2^{s_0}}{2^{s_0-1}}\right)^n$, that is the number of all n-dimensional vectors with coordinates being balanced Boolean functions in s_0 variables taken in all possible ways from the set $\{x_1,\ldots,x_n\}$.

A *funkeysubcipher with key functions in a bounded number of essential variables* is a funkeysubcipher $\mathcal{C} = (\mathbb{F}_2^n, K, \mathbb{F}_2^n, E, D)$, where $K \subseteq IS_{s_0,n}$. To synthesize these ciphers, we need generating the key spaces K for them from vector functions in $IS_{s_0,n}$. Here, we propose to do this just in the same way as we have done above in the set IS_n using the inverse and permutation operations.

Namely, take a vector function $g(x_1,x_2,\ldots,x_n)$ in $IS_{s_0,n}$. Let $g = (g_1,\ldots,g_n)$. By the definition of $IS_{s_0,n}$, for every $i \in \{1,\ldots,n\}$, there exists a natural $s_i \leqslant s_0$ such that $g_i \in B^*_{s_i,n}$, that is, g_i essentially depends on s_i variables. Define $K_{s_0,n}(g) = \{\pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1}))) : \sigma_1,\sigma_2 \in \mathbb{F}_2^n, \pi_1,\pi_2 \in S_n\}$, where $x = x_1x_2\ldots x_n$. Thus, we get that $K_{s_0,n}(g) \subseteq IS_{s_0,n}$ and $|K_{s_0,n}(g)| \leqslant (2^n n!)^2$. Moreover, for any function $f = (f_1,\ldots,f_n) \in K_{s_0,n}(g)$ and any $i \in \{1,\ldots,n\}$, the number of essential variables of f_i equals s_j, the number of essential variables of g_j where $j = \pi_2^{-1}(i)$.

Any subset $K \subseteq K_{s_0,n}(g)$ of an exponential cardinality can be taken as the key space of the funkeysubcipher $\mathcal{C}$ with key functions in a bounded number of essential variables. In particular, this role can be successfully played by the subsets $K_{s_0,n}(g,j)$ that are formally defined, just as $K_n(g,j)$, $j = 1,2,\ldots,15$, have been done. For example, $K_{s_0,n}(g,7) = \{g^{\sigma_2}(\pi_1(x^{\sigma_1})) : \sigma_1,\sigma_2 \in \mathbb{F}_2^n, \pi_1 \in S_n\}$, $|K_{s_0,n}(g,7)| \leqslant 2^{2n}n!$, and $K_{s_0,n}(g,15) = K_{s_0,n}(g)$. The only difference is in the class of the function g that, for $K_n(g,j)$, belongs to IS_n and, for $K_{s_0,n}(g,j)$, belongs to $IS_{s_0,n}$.

To produce subsets $K \subseteq K_{s_0,n}(g)$ as key spaces for funkeysubciphers with key functions in a bounded number of essential variables, we need to have a capability to generate vector Boolean functions $g = (g_1 \dots g_n)$ in $I_{s_0,n}$ with various values of their parameters n, s_0, s_1, $\dots$, s_n. Unfortunately, we have no any exhaustive solution of this problem and can only present now a pair of some restricted relevant methods.

Let $IS^*_{s,n}$ denote the set of all bijective Boolean vector functions each consisting of n coordinate functions in $B^*_{s,n}$. The methods just mentioned construct functions from $IS^*_{s,n}$.

The first method is used in the case when $s \geqslant 3$ and $s|n$, i.e. $n = st$ for some $t \in \mathbb{N}$. It is proved in [7] that $IS^*_{s,s} \neq \varnothing$ for all $s \geqslant 3$. So, we can construct t functions $g^{(i)} = g_1^{(i)} \dots g_s^{(i)} \in IS^*_{s,s}$, $i = 1, \dots, t$. Then the function $g(x_1, \dots, x_n) = g_1^{(1)}(x_1, \dots, x_s) \dots g_s^{(1)}(x_1, \dots, x_s) g_1^{(2)}(x_{s+1}, \dots, x_{2s}) \dots g_s^{(2)}(x_{s+1}, \dots, x_{2s}) \dots g_1^{(t)}(x_{(t-1)s+1}, \dots, x_n) \dots g_s^{(t)}(x_{(t-1)s+1}, \dots, x_n)$ belongs to $IS^*_{s,n}$.

The second method starts from $g^{(1)}(x_1, \dots, x_s) = g_1 \dots g_s \in IS^*_{s,s}$ too. Then we construct the function $g^{(2)}(x_1, \dots, x_s, x_{s+1}) = g_1 \dots g_s h$ where $h = x_{s+1} \oplus q(x_1, \dots, x_s)$ and $q \in B^*_{s-1,s}$. It is proved in [8] that $g^{(2)} \in IS^*_{s,s+1}$. Repeating this step, we successively obtain the functions $g^{(3)} \in IS^*_{s,s+2}$ (using the functions $h = x_{s+2} \oplus q(x_1, \dots, x_s, x_{s+1})$ and $q \in B^*_{s-1,s+1}$), $\dots$, $g^{(n+s-1)} \in IS^*_{s,n}$.

5. Cryptanalysis

5.1. Cryptanalysis problem

In this section, we consider the cryptanalysis problem for funkeysubciphers giving our attention to ciphers with key functions in bounded numbers of essential variables. Moreover, we confine the consideration to ciphers with key spaces $K = K_{s_0,n}(g, j)$, where g is an arbitrary function in $(B_{s_0,n})^n$ and j can be assigned any value from $\{1, \dots, 15\}$. However, for some parameter j values, the cryptanalysis methods proposed here actually hold for ciphers with the wider key spaces, particularly with $K = K_n(g, j)$.

We assume that the cryptanalyst exploits a known plaintext attack with the threat of total break (secret key recovery). This means that he possesses some blocks $P_1, \dots, P_m$ of a plaintext and corresponding blocks $C_1, \dots, C_m$ of a ciphertext and tries to determine the key that was used, that is, a function $f(x) \in K = K_{s_0,n}(g, j)$ such that $C_l = f(P_l)$ for all $l \in \{1, \dots, m\}$. According to Kerckhoff's principle, it is supposed that the cryptanalyst knows the cipher $\mathcal{C} = (\mathbb{F}_2^n, K, \mathbb{F}_2^n, E, D)$ being used. Particularly, he knows the key space $K = K_{s_0,n}(g, j)$ and its parameters $g \in (B_{s_0,n})^n$, $n \in \mathbb{N}$, $s_0 \leqslant n$, and $j \in \{1, \dots, 15\}$. The knowledge of the function $g(x_1, \dots, x_n)$ yields the knowledge of its inverse g^{-1}, coordinate functions $g_1, \dots, g_n$ in $B_{s_0,n}$ and the sets $X_1, \dots, X_n$ of their essential variables respectively, $X_i \subseteq X = \{x_1, \dots, x_n\}$, $i = 1, \dots, n$. On the base of this information, the cryptanalyst has to determine the coordinate functions $f_1, \dots, f_n$ of a key function $f(x_1, \dots, x_n)$ in $K_{s_0,n}(g, j)$ which satisfies the equalities $f(P_l) = C_l$ for all $l \in \{1, \dots, m\}$. Here, for each $i \in \{1, \dots, n\}$, the function f_i belongs to $B_{s_0,n}$, its essential variables form a subset $U_i \subseteq X$, and $|U_i| = |X_i| = s_i$ if the permutation π_2 in the expression for $K_{s_0,n}(g, j)$ is the identity one. For the cryptanalyst, to determine the function f_i means to determine the set U_i of its essential variables and the value of f_i for each combination of values of variables in U_i.

Below we first give a general solution of the problem comprising the all fifteen partial cases of it and then present specific solutions for some of these cases.

5.2. General cryptanalysis method

The method concerns the funkeysubcipher $\mathcal{C}$ with the general key space $K = K_{s_0,n}(g) = \{\pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1}))) : \sigma_1, \sigma_2 \in \mathbb{F}_2^n, \pi_1, \pi_2 \in S_n\}$ which includes the partial key spaces $K_{s_0,n}(g,j)$ for all $j \in \{1,\ldots,15\}$.

Recall that we have a string of Boolean variables $x = x_1x_2\ldots x_n$, a vector Boolean function $g(x) = g_1(x)g_2(x)\ldots g_n(x)$ with coordinate functions $g_1,\ldots,g_n$, where $g_i \in B^*_{si,n}$ for $1 \leqslant s_i \leqslant s_0$ and $i = 1,\ldots,n$, the blocks of a plain text $P_1,\ldots,P_m$ and the corresponding blocks of a ciphertext $C_1,\ldots,C_m$.

Let $k \in K$ and $C_l = C_{l1}C_{l2}\ldots C_{ln}$, $l = 1,\ldots,m$. Denote $f(x) = f_1(x)f_2(x)\ldots f_n(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$. Then $f_i \in B_{s_0,n}$, $k = f(x)$, $C_l = f(P_l)$, and $C_{li} = f_i(P_l)$, $l = 1,\ldots,m$ and $i = 1,\ldots,n$.

Thus, the cryptanalysis problem is as follows: for every $i \in \{1,\ldots,n\}$ and given equalities $C_{li} = f_i(P_l)$, $l = 1,\ldots,m$, determine the function $f_i(x)$. The problem is divided into two subproblems: find out essential variables of the function f_i and compute its values for all possible values of these variables. In connection with the first subproblem, we need to note that the number of essential variables of f_i depends on whether the permutation π_2 in $f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$ is the identity one or not. If the answer is "yes", then f_i has the same number s_i of essential variables as g_i. Otherwise we can only say that this number is less or equal to $\max\{s_1,\ldots,s_n\}$ and doesn't exceed s_0.

To solve the first subproblem, we now present some auxiliary results. Let $f'(x_1,\ldots,x_n)$ be a, possibly, partial Boolean function given by two subsets $M^0_{f'} \subseteq \mathbb{F}_2^n$ and $M^1_{f'} \subseteq \mathbb{F}_2^n$ so that $\alpha \in M^b_{f'} \Leftrightarrow f'(\alpha) = b$, $b \in \mathbb{F}_2$.

We first define the following sets:

$$D(f') = \{\alpha \oplus \beta : \alpha \in M^0_{f'}, \beta \in M^1_{f'}\},$$
$$\inf D(f') = \{\delta : \delta \in D(f'),\ \neg\exists\delta' \in D(f')(\delta' < \delta)\},$$

where for $\delta = d_1\ldots d_n$ and $\delta' = d'_1\ldots d'_n$ in $\mathbb{F}_2^n$, $\delta' < \delta \Leftrightarrow \delta' \neq \delta \ \&\ \forall t \in \{1,\ldots,n\}\ (d'_t \leqslant d_t)$. Particularly, in our case,

$$D(f_i) = \{P_l \oplus P_j : C_{li} \neq C_{ji},\ l,j = 1,2,\ldots,m\}.$$

We next construct the Boolean matrix $M' = ||\inf D(f')||$ with the set of rows that is equal to inf $D(f')$. The columns in M' with the numbers 1, 2, ..., n are assigned to variables $x_1, x_2, \ldots, x_n$ respectively. A subset J of them is said to be a *cover* of M' if for each row in M', there is a column in J with the value 1 in this row. The cover J is *minimal* if it doesn't contain as a subset another cover of M'.

At last, we note that in [9] we have proved that a subset of variables $U = \{x_{j_1},\ldots,x_{j_s}\}$ is sufficient for f' iff the subset J of columns in M' with the numbers $j_1,\ldots,j_s$ is a cover of M', and U is essential for f' iff J is a minimal cover of M'. Moreover, U is a unique subset of essential variables for f' iff J is a unique cover of M'; in this case, each row in M' is a unit vector e_j (with a 1 in the j-th coordinate and 0's elsewhere) and $U = \{x_{j_1},\ldots,x_{j_s}\}$ if all the rows in M' are $e_{j_1},\ldots,e_{j_s}$.

Also, in [10], we have proved that a subset of variables $\{x_{j_1},\ldots,x_{j_s}\}$ is a unique subset of essential variables for a function f' in $B_{s_0,n}$ iff all the covers of the matrix $||\inf D(f')||$, the cardinalities of which don't exceed s_0, have a non-empty intersection consisting of columns with the numbers $j_1,\ldots,j_s$.

So, finding a unique subset of essential variables (if it exists) for the function f_i in $B_{s_0,n}$ and thus solving the first cryptanalysis subproblem is reduced to computing, for the matrix $||\inf D(f_i)||$, the intersection of all covers whose cardinalities are not more than s_0. The computational complexity of this work is $\mathrm{O}(2^{s_0})$.

Under the known essential variables $x_{i_1}, \ldots, x_{i_{s_i}}$ of f_i, any solution of the second cryptanalysis subproblem for $i \in \{1, \ldots, n\}$ can be obtained as $f_i(x) = h_i(x_{i_1}, \ldots, x_{i_{s_i}})$, where $h_i : \mathbb{F}_2^{s_i} \to \mathbb{F}_2$, the vector function $h_1(x_{1_1}, \ldots, x_{1_{s_1}})h_2(x_{2_1}, \ldots, x_{2_{s_2}}) \ldots h_n(x_{n_1}, \ldots, x_{n_{s_n}})$ is a bijection on $\mathbb{F}_2^n$, and, for all $\alpha = a_1 a_2 \ldots a_n \in \mathbb{F}_2^n$, if $\alpha = P_l$ and $l \in \{1, \ldots, m\}$, then $h_i(a_{i_1}, \ldots, a_{i_{s_i}}) = C_{li}$.

In particular, if for each $i \in \{1, \ldots, n\}$, the set $\{x_{i_1}, \ldots, x_{i_{s_i}}\}$ is a unique subset of essential variables for f_i and $P = \{P_{li_1} P_{li_2} \ldots P_{li_{s_i}} : l = 1, \ldots, m\} = \mathbb{F}_2^{s_i}$, then the solution $f(x)$ of the cryptanalysis problem for the cipher $\mathcal{C}$ is unique and, for $i \in \{1, \ldots, n\}$, it has $f_i(x) = h_i(x_{i_1}, \ldots, x_{i_{s_i}})$, where $h_i(P_{li_1} P_{li_2} \ldots P_{li_{s_i}}) = C_{li}$, $l \in \{1, \ldots, m\}$.

In the case of $P \neq \mathbb{F}_2^{s_i}$, the following problem arises: given a partially defined Boolean function $f'(x_1, \ldots, x_n)$ and a subset $\{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}$, find (if exists) a completely defined Boolean function $h(x_{i_1}, \ldots, x_{i_s})$ such that $h(a_{i_1} a_{i_2} \ldots a_{i_s}) = f'(a_1 a_2 \ldots a_n)$ for each n-tuple $(a_1 a_2 \ldots a_n)$ from the domain of f'. This problem is a special case of the known problem of completing a partial function in a functional class and isn't a subject of this research.

For making references to the general cryptanalysis method described here, we name it GCM. The core of GCM is the algorithm for finding, for a given partially defined Boolean function $f'(x_1, \ldots, x_n)$ from $B_{s_0,n}$, such a function $h(x_{i_1}, \ldots, x_{i_s}) \in B^*_{s,n}$ that $h(x_{i_1}, \ldots, x_{i_s}) = f'(x_1, \ldots, x_n)$ on the domain of f'. We denote this algorithm by $\mathcal{B}$.

As for the parameters of the cryptanalysis problem, namely $g, \sigma_1, \sigma_2, \pi_1, \pi_2$, GCM doesn't depend directly on them both in the contents and in a result. This is not an accidental fact, but it is because these parameters are not really the key k of the cipher $\mathcal{C}$, they only form the expression $\pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$ to specify a bijective function $f : \mathbb{F}^n \to \mathbb{F}^n$ which is in fact the key k of $\mathcal{C}$ and the result of GCM execution over the given pairs (P_i, C_i), $i = 1, \ldots, n$.

5.3. Some particular cryptanalysis methods

Some particular cryptanalysis methods for a cipher $\mathcal{C}$ under consideration can be obtained by applying GCM to ciphers $\mathcal{C}_j$ with key spaces $K_{s_0,n}(g, j)$ for $j \in \{1, \ldots, 14\}$. We think of these methods as key space limitations of the general method and denote by GCM_j. For example, GCM_9 and GCM_{14} are GCM for ciphers with key spaces $K = K_{s_0,n}(g, 9) = \{\pi_2(g(x^{\sigma_1})) : \sigma_1 \in \mathbb{F}_2^n, \pi_2 \in S_n\}$ and $K = K_{s_0,n}(g, 14) = \{\pi_2(g^{\sigma_2}(\pi_1(x))) : \sigma_2 \in \mathbb{F}_2^n, \pi_1, \pi_2 \in S_n\}$ respectively.

Now, we consider some other particular cryptanalysis methods that are not exactly key space limitations of GCM, but give special solutions to some ciphers $\mathcal{C}_j$ with limited key spaces.

Cases $j = 1, 4, 5$

Describing cryptanalysis methods in these cases, we limit our exposition to determination of the inverse operations for obtaining f from g.

Let $g^{-1} = (g_1^{-\prime}, g_2^{-\prime}, \ldots, g_n^{-\prime})$, $f^{-1} = (f_1^{-\prime}, f_2^{-\prime}, \ldots, f_n^{-\prime})$, $\sigma_1 = \sigma_{11}\sigma_{12} \ldots \sigma_{1n}$, $\sigma_2 = \sigma_{21}\sigma_{22} \ldots \sigma_{2n}$, $P_l = P_{l1}P_{l2} \ldots P_{ln}$, and $C_l = C_{l1}C_{l2} \ldots C_{ln}$, $l = 1, 2, \ldots, m$.

In the *case* $j = 1$, where $K = K_{s_0,n}(g, 1) = \{g(x^{\sigma_1}) : \sigma_1 \in \mathbb{F}_2^n\}$, the cryptanalysis problem is trivial because, for every $l \in \{1, \ldots, m\}$, $C_l = g(P_l^{\sigma_1})$, $P_l^{\sigma_1} = g^{-1}(C_l)$, $P_{li}^{\sigma_{1i}} = g_i^{-\prime}(C_l)$, $i \in \{1, \ldots, n\}$, and σ_{1i} is computed by using the Boolean implication

$$(a^b = c) \Rightarrow (b = 1 \Leftrightarrow c = a),$$

namely $\sigma_{1i} = 1 \Leftrightarrow g_i^{-\prime}(C_l) = P_{li}$ for all $i \in \{1, 2, \ldots, n\}$ and some (any) $l \in \{1, \ldots, m\}$, particularly for $l = 1$.

By the same reason, the problem is trivial in the *case* $j = 4$, where $K = K_{s_0,n}(g, 4) = \{g^{\sigma_2}(x) : \sigma_2 \in \mathbb{F}_2^n\}$, because $C_l = g^{\sigma_2}(P_l)$, $C_l^{\sigma_2} = g(P_l)$ and σ_2 is computed by using the same implication: $\sigma_{2i} = 1 \Leftrightarrow g_i(P_l) = C_{li}$, $i = 1, 2, \ldots, n$.

In the *case* $j = 5$, where $K = K_{s_0,n}(g, 5) = \{g^{\sigma_2}(x^{\sigma_1}) : \sigma_1, \sigma_2 \in \mathbb{F}_2^n\}$, we have $C_l = g^{\sigma_2}(P_l^{\sigma_1})$, $C_l^{\sigma_2} = g(P_l^{\sigma_1})$, and $P_l^{\sigma_1} = g^{-1}(C_l^{\sigma_2})$. For every pair (σ_2, l), where $\sigma_2 \in \mathbb{F}_2^n$ and $l = 1, 2, \ldots, m$, compute the value $\sigma_1^{(\sigma_2,l)} = \sigma_{11}^{(\sigma_2,l)}\sigma_{12}^{(\sigma_2,l)} \ldots \sigma_{1n}^{(\sigma_2,l)}$ of the vector σ_1 in $\mathbb{F}_{2^n}$ by using the algorithm of the case $j = 1$, namely

$$\sigma_{1i}^{(\sigma_2,l)} = 1 \Leftrightarrow g_i^{-\prime}(C_l^{\sigma_2}) = P_{li}, i = 1, \ldots, m.$$

The result of the cryptanalysis is a pair (σ_1, σ_2) satisfying the equality $\sigma_1 = \sigma_1^{(\sigma_2,l)}$ for all $l \in \{1, \ldots, m\}$. Note that this answer is not sure to be unique. The computational complexity of the algorithm is $\mathrm{O}(2^n)$.

Note that the attacks described in these cases successfully work on ciphers with $K = K_n(g, j)$ for $j = 1, 4, 5$ respectively and $g \in IS_n$.

Case $j = 7$

In this case, $K = K_{s_0,n}(g, 7) = \{g^{\sigma_2}(\pi_1(x^{\sigma_1})) : \sigma_1, \sigma_2 \in \mathbb{F}_2^n, \pi_1 \in S_n\}$ and the cipher under consideration is $\mathcal{C}_7$ that is the partial case of $\mathcal{C}$, where $\pi_2 = 1$. Besides, the ciphers $\mathcal{C}_j$ for all $j \in \{1, \ldots, 6\}$ are partial cases of $\mathcal{C}_7$, and the cryptanalysis problem for them can be solved by any method solving this problem for $\mathcal{C}_7$. The method presented here is an amplification of GCM, namely, instead of method $\mathcal{B}$, a method $\mathcal{A}$ is used, which takes into attention the condition $\pi_2 = 1$, yielding the fact that a function $f_i(x)$ to be found has the same number s_i of essential variables as the known function g_i. So, finding essential variables for f_i is reduced in $\mathcal{A}$ to finding, for the matrix $||\inf D(f_i)||$, a minimal cover of the given cardinality — s_i. The computational complexity of the last problem doesn't exceed $\binom{n}{s_i}$. In other details, the cryptanalysis method for $\mathcal{C}_7$ coincides with GCM.

Some program implementations of algorithms $\mathcal{A}$ and $\mathcal{B}$ and the results of their thorough testing on computers have been presented in [2].

REFERENCES

1. *Agibalov G. P. and Levashnikov A. A.* Statisticheskoe issledovanie zadachi opoznaniya bulevykh funktsiy odnogo klassa [Statistical study of the identifying problem for a class of Boolean functions]. Proc. ASDA Conf., Novosibirsk, 1966, pp. 40–45. (in Russian)
2. *Agibalov G. P. and Sungurova O. G.* Kriptoanaliz konechno-avtomatnogo generatora klyuchevogo potoka s funktsiey vykhodov v kachestve klyucha [Cryptanalysis of a finite-state keystream generator with an output function as a key]. Vestnik TSU. Prilozhenie, 2006, no. 17, pp. 104–108. (in Russian)
3. *Agibalov G. P.* SIBCiphers — simmetrichnye iterativnye blochnye shifry iz bulevykh funktsiy s klyuchevymi argumentami [SIBCiphers — symmetric iterative block ciphers composed of Boolean functions depending on small number of variables]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2014, no. 7, pp. 43–48. (in Russian)
4. *Agibalov G. P.* Watermarking ciphers. Prikladnaya Diskretnaya Matematika, 2016, no. 1(31), pp. 62–66.
5. *Agibalov G. P. and Pankratova I. A.* O dvukhkaskadnykh konechno-avtomatnykh kriptograficheskikh generatorakh i metodakh ikh kriptoanaliza [About 2-cascade finite

automata cryptographic generators and their cryptanalysis]. Prikladnaya Diskretnaya Matematika, 2017, no. 35, pp. 38–47. (in Russian)

6. *Agibalov G. P.* Kriptoavtomaty s funktsional'nymi klyuchami [Cryptautomata with functional keys]. Prikladnaya Diskretnaya Matematika, 2017, no. 36, pp. 59–72. (in Russian)
7. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables. Proc. CSIST'2016, Minsk, BSU Publ., 2016, pp. 519–521.
8. *Pankratova I. A.* Ob obratimosti vektornykh bulevykh funktsiy [On the invertibility of vector Boolean functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2015, no. 8, pp. 35–37. (in Russian)
9. *Agibalov G. P.* Minimizatsiya chisla argumentov bulevykh funktsiy [Number minimization for variables a partial Boolean function depends on]. Problemy Sinteza Tsifrovykh Avtomatov, Moscow, Nauka Publ., 1967, pp. 96–100. (in Russian)
10. *Agibalov G. P.* O nekotorykh doopredeleniyakh chastichnoy bulevoy funktsii [Some completions of partial Boolean function]. Trudy SPhTI, 1970, iss. 49, pp. 12–19. (in Russian)