Math-Net.Ru

Общероссийский математический портал

V. G. Mikhailov, A. V. Volgin, Устойчивость множеств решений систем уравнений при их случайных искажениях, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 3, 61–72

DOI: <https://doi.org/10.4213/mvk196>

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: 52.6.47.48

26 апреля 2023 г., 13:01:22

**The stability of sets of solutions
for systems of equations with random distortions²**

V. G. Mikhailov^{*}, A. V. Volgin^{}**

^{*} *Steklov Mathematical Institute of Russian Academy of Sciences, Moscow*

^{**} *Moscow State University of Information Technologies,
Radioengineering and Electronics, Moscow*

Получено 02.III.2015

Abstract. Let in a system of equations left sides be functions from $\{0, 1, \dots, N-1\}$ to $\{0, 1\}$ and in the other system all equations be obtained from the equations of the first one by random distortions of the truth tables of these functions. We find conditions on the probability laws of distortions under which the set of solutions of the second system includes all, some or no solutions of the first system.

Keywords: set of solutions of system of equations, binomial distribution, Boolean functions

Устойчивость множеств решений систем уравнений при их случайных искажениях

В. Г. Михайлов^{*}, А. В. Волгин^{}**

^{*} *Математический институт им. В. А. Стеклова Российской академии наук, Москва*

^{**} *Московский государственный университет информационных технологий, радиотехники и электроники, Москва*

Аннотация. Пусть в одной системе уравнений левые части являются функциями из $\{0, 1, \dots, N-1\}$ в $\{0, 1\}$, а в другой системе уравнения получены из уравнений первой случайными заменами части значений этих функций противоположными. Получены условия на вероятностные законы искажений функций, при которых множество решений искаженной системы включает в себя полностью или частично множество решений исходной системы или не пересекается с ним.

Ключевые слова: множество решений системы уравнений, биномиальное распределение, булевы функции

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 3, pp. 61–72 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

² The article was submitted by the Organizing Committee of the Symposium CTCrypt'2015

1. Introduction

The systems of equations and methods of their solutions are of great value for the cryptanalysis of symmetric ciphers ([1, 3]). The encryption algorithm defines a system of equations connecting known bits of the plaintext and ciphertext with unknown bits of a secret key. Some methods of searching the solution of systems of equations are based on the construction of “close” easily solved systems. The notion of “close” systems was introduced in [4, 5]: two systems are called “close” if the truth tables of corresponding functions in these systems differ in a small number of items. Here we investigate conditions under which there exist common solutions of such systems.

Let $N, T \in \mathbb{N}$. We consider a system of equations

$$f_t(x) = b_t, \quad t = 1, \dots, T, \quad (1)$$

where

$$f_t: \{0, 1, \dots, N-1\} \rightarrow \{0, 1\}, \quad b_t \in \{0, 1\},$$

and a similar system

$$\tilde{f}_t(x) = b_t, \quad t = 1, \dots, T, \quad (2)$$

where functions $\tilde{f}_1, \dots, \tilde{f}_t$, are obtained from functions $f_1, \dots, f_t$ by independent random distortions. For several types of joint probabilistic distributions of systems (1) and (2) we obtain conditions ensuring the following variants of asymptotic relations between the sets of solutions of these two systems as $N \rightarrow \infty, T = T(N) \rightarrow \infty$:

- conditions under which the probability of the absence of common solutions tends to 1;
- conditions under which the set of solutions of distorted system (2) contains the set of solutions of the system (1) with probability tending to 1;
- intermediate conditions under which the number of common solutions of two systems has a non-degenerate limit distribution (namely, the binomial distribution).

Let $\mathbf{B}(N)$ denote the set of all 2^N functions $f: \{0, 1, \dots, N-1\} \rightarrow \{0, 1\}$ and $\oplus$ denote the addition operator modulo 2. Note that substituting the functions $f_1 \oplus b_1, \dots, f_t \oplus b_t$ for $f_1, \dots, f_t$ we reduce the system (1) to a homogeneous system

$$f_t(x) = 0, \quad t = 1, \dots, T, \quad (3)$$

which will be considered in what follows.

2. Main theorem

For an arbitrary function $f \in \mathbf{B}(N)$ we define the sets

$$A_0(f) = \{x \in \{0, 1, \dots, N-1\} : f(x) = 0\}$$

and

$$A_1(f) = \{x \in \{0, 1, \dots, N-1\} : f(x) = 1\}.$$

For an integer v , $0 \leq v \leq |A_0(f)|$, we put

$$B_0(f, v) = \{g \in \mathbf{B}(N) : |A_1(g) \cap A_0(f)| = v\}.$$

A probability distribution of the function g on the set $B_0(f, v)$ will be called a *uniform distribution with respect to zeros of the function f* if

$$\mathbf{P}\{A_1(g) \cap A_0(f) = A\} = \frac{1}{\binom{|A_0(f)|}{v}} \quad (4)$$

for each subset $A \subset A_0(f)$ of cardinality $|A| = v$.

The condition (4) means that the set $A_1(g) \cap A_0(f)$ is distributed as a sample of size v without replacement from the set $A_0(f)$. The distribution of the set $A_1(g) \setminus A_0(f)$ may be arbitrary.

It follows, for example, that

$$\mathbf{P}\{x \in A_0(g)\} = 1 - \frac{v}{|A_0(f)|} \quad \text{for all } x \in A_0(f). \quad (5)$$

In a similar way we introduce a notion of the *uniform with respect to ones of the function f* distribution on the set

$$B_1(f, u) = \{g \in \mathbf{B}(N) : |A_0(g) \cap A_1(f)| = u\}.$$

For any such distribution

$$\mathbf{P}\{x \in A_1(g)\} = 1 - \frac{u}{|A_1(f)|} \quad \text{for all } x \in A_1(f).$$

Let $f_1, \dots, f_t$ be functions from (3) and $v_1, \dots, v_t$ be integers such that $0 \leq v_t < |A_0(f_t)|$, $t = 1, \dots, T$. We will suppose that functions $\tilde{f}_1, \dots, \tilde{f}_t$ are independent and for each $t = 1, \dots, T$ the function $\tilde{f}_t$ has distribution on the set $B_0(f_t, v_t)$ which is uniform with respect to zeros of the function f_t .

Let S denote the set of solutions of homogeneous system (3) and $\tilde{S}(v_1, \dots, v_t)$ denote the set of solutions of system of random equations

$$\tilde{f}_t(x) = 0, \quad t = 1, \dots, T. \quad (6)$$

Remark 1. In this paper we consider “triangular schemes”: the functions $f_1, \dots, f_t$ may vary as $N, T = T(N) \rightarrow \infty$. Conditions on the functions $f_1, \dots, f_t$ will be specified in corresponding statements.

Theorem 1. Let the left sides $\tilde{f}_1, \dots, \tilde{f}_t$ of equations in the system (6) be independent random functions from the sets $B_0(f_1, v_1), \dots, B_0(f_t, v_t)$ having uniform distributions with respect to zeros of the functions $f_1, \dots, f_t$ correspondingly. Let $|S| \geq 1$ and $N, T \rightarrow \infty$. Then:

1) functions $f_1, \dots, f_t$ are varying in such a way that

$$\sum_{t=1}^T \frac{v_t}{|A_0(f_t)|} - \ln |S| \rightarrow \infty, \quad (7)$$

then

$$\mathbf{P}\{\tilde{S}(v_1, \dots, v_t) \cap S = \emptyset\} \rightarrow 1;$$

2) functions $f_1, \dots, f_t$ are varying in such a way that $|S| = \text{const}$ and

$$\sum_{t=1}^T \frac{v_t}{|A_0(f_t)|} \rightarrow \kappa \in (0, \infty), \quad \max_{t=1, \dots, T} \frac{v_t}{|A_0(f_t)|} \rightarrow 0, \quad \sum_{t=1}^T \frac{1}{|A_0(f_t)|} \rightarrow 0, \quad (8)$$

then the distribution of the random variable $|\tilde{S}(v_1, \dots, v_t) \cap S|$ converges to the binomial distribution with parameters $(|S|, e^{-\kappa})$;

3) if functions $f_1, \dots, f_t$ are varying in such a way that

$$|S| \sum_{t=1}^T \frac{v_t}{|A_0(f_t)|} \rightarrow 0, \quad (9)$$

then

$$\mathbf{P}\{\tilde{S}(v_1, \dots, v_t) \supseteq S\} \rightarrow 1.$$

Remark 2. The statement of the theorem 1 and its proof are valid for all distributions on $B(f_t, v_t)$, which are uniform with respect to the zeros of functions f_t , $t = 1, \dots, T$. These distributions may be different for different equations. The following type of random distortions of the system (1) is particularly interesting. For a function $f \in \mathbf{B}(N)$ and integers $0 \leq v^{(1)} < |A_1(f)|$ and $0 \leq v^{(0)} < |A_0(f)|$ we put

$$B(f, v^{(1)}, v^{(0)}) = \{g \in \mathbf{B}(N) : |A_0(g) \cap A_1(f)| = v^{(1)}, |A_1(g) \cap A_0(f)| = v^{(0)}\}.$$

Note that

$$B(f, v^{(1)}, v^{(0)}) \subset B(f, v^{(0)}), \quad |B(f, v^{(1)}, v^{(0)})| = \binom{|A_1(f)|}{v^{(1)}} \binom{|A_0(f)|}{v^{(0)}}.$$

The uniform distribution on the set $B(f, u, v)$ is uniform with respect to both zeros and ones of the function f . So, substitution of functions $f_t^* = f_t \oplus b_t$ for f_t , $t = 1, \dots, T$, in system (1) and $\tilde{f}_t^* = \tilde{f}_t \oplus b_t$ for $\tilde{f}_t$, $t = 1, \dots, T$, in system

$$\tilde{f}_t(x) = b_t, \quad t = 1, \dots, T, \quad (10)$$

transforms these systems into the systems with zero right hand sides. Moreover,

$$A_0(f_t^*) = A_{b_t}(f_t), \quad t = 1, \dots, T.$$

Thus we obtain the following statement. Let $S_{b_1, \dots, b_t}$ denote the set of solutions of the system (1) (which is equivalent to the system $f_t^*(x) = 0$, $t = 1, \dots, T$) and $\tilde{S}_{b_1, \dots, b_t}$ denote the set of solutions of the system (10) (which is equivalent to the system $\tilde{f}_t^*(x) = 0$, $t = 1, \dots, T$).

Corollary 1. *Let the left hand sides of equations in the system (10) are obtained by an independent equiprobable sampling of functions $\tilde{f}_1, \dots, \tilde{f}_t$ from the sets $B(f_1, v_1^{(1)}, v_1^{(0)}), \dots, B(f_t, v_t^{(1)}, v_t^{(0)})$ respectively. Let $N, T \rightarrow \infty$ and functions $f_1^*, \dots, f_t^*$ satisfy the condition $|S_{b_1, \dots, b_t}| \geq 1$. Then:*

1) if

$$\sum_{t=1}^T \frac{v_t^{(b_t)}}{|A_{b_t}(f_t)|} - \ln |S_{b_1, \dots, b_t}| \rightarrow \infty,$$

then $\mathbf{P}\{\tilde{S}_{b_1, \dots, b_t} \cap S_{b_1, \dots, b_t} = \emptyset\} \rightarrow 1$;

2) if functions $f_1^*, \dots, f_t^*$ are varying in such a way that $|S_{b_1, \dots, b_t}| = \text{const}$ and

$$\begin{aligned} \sum_{t=1}^T \frac{v_t^{(b_t)}}{|A_{b_t}(f_t)|} &\rightarrow \varkappa \in (0, \infty), \\ \max_{t=1, \dots, T} \frac{v_t^{(b_t)}}{|A_{b_t}(f_t)|} &\rightarrow 0, \\ \sum_{t=1}^T \frac{1}{|A_{b_t}(f_t)|} &\rightarrow 0, \end{aligned}$$

then the distribution of random variable $|\tilde{S}_{b_1, \dots, b_t} \cap S_{b_1, \dots, b_t}|$ converges to the binomial distribution with parameters $(|S_b|, e^{-\varkappa})$;

3) if

$$|S_{b_1, \dots, b_t}| \sum_{t=1}^T \frac{v_t^{(b_t)}}{|A_{b_t}(f_t)|} \rightarrow 0,$$

then $\mathbf{P}\{\tilde{S}_{b_1, \dots, b_t} \supseteq S_{b_1, \dots, b_t}\} \rightarrow 1$.

3. Distortion by changing random numbers of values of functions

Let $\mathcal{P}_1, \dots, \mathcal{P}_t$ be given probability distributions on the set $\{0, 1, \dots, N-1\}$ and $\varsigma_1, \dots, \varsigma_t$ be independent random variables with distributions $\mathcal{P}_1, \dots, \mathcal{P}_t$ correspondingly. Let for each $i = 1, \dots, T$ the function f_i corresponds to the set $C_1(f_i, k)$, $k = 0, 1, \dots, N-1$, of functions $g \in \mathbf{B}(N)$ which differ from f_i exactly at k values $x \in \{0, 1, \dots, N-1\}$.

Now we introduce the functions $\tilde{f}_1, \dots, \tilde{f}_t$ as follows. For each $i = 1, \dots, T$ we obtain the value of the random variable ς_i with distribution $\mathcal{P}_i$. Further, if $\varsigma_i = k$, then the random function $\tilde{f}_i$ should be chosen from the set $C_1(f_i, k)$ with probabilities

$$\mathbf{P}\{\tilde{f}_i = g \mid \varsigma_i = k\} = \frac{1}{|C_1(f_i, k)|}, \quad g \in C_1(f_i, k).$$

Let

$$\tilde{f}_t(x) = 0, \quad t = 1, \dots, T, \quad (11)$$

be a system of random equations with functions obtained from functions $f_1, \dots, f_t$ as described above. Let $\tilde{S}(\mathcal{P}_1, \dots, \mathcal{P}_t)$ be the set of solutions of the system (11).

Theorem 2. Let the left-hand sides $\tilde{f}_1, \dots, \tilde{f}_t$ of equations in the system (11) be obtained as described above. Let $N, T \rightarrow \infty$, let functions $f_1, \dots, f_t$ are varying in such a way that $|S| = \text{const} \geq 1$, and distributions $\mathcal{P}_1, \dots, \mathcal{P}_t$ satisfy conditions

$$\mathbf{D}_{\mathcal{P}_t \zeta_t} = O(\mathbf{E}_{\mathcal{P}_t \zeta_t}) \quad \text{uniformly in } t = 1, \dots, T. \quad (12)$$

Then:

1) if

$$\frac{1}{N} \sum_{t=1}^T \mathbf{E}_{\mathcal{P}_t \zeta_t} \rightarrow \infty,$$

then $\mathbf{P} \{ \tilde{S}(\mathcal{P}_1, \dots, \mathcal{P}_t) \cap S = \emptyset \} \rightarrow 1$;

2) if

$$\begin{aligned} \frac{1}{N} \sum_{t=1}^T \mathbf{E}_{\mathcal{P}_t \zeta_t} &\rightarrow \varkappa \in (0, \infty), \\ \max_{t=1, \dots, T} \frac{\mathbf{E}_{\mathcal{P}_t \zeta_t}}{N} &\rightarrow 0, \\ \sum_{t=1}^T \frac{1}{|A_0(f_t)|} &\rightarrow 0, \end{aligned}$$

then the distribution of the random variable $|\tilde{S}(\mathcal{P}_1, \dots, \mathcal{P}_t) \cap S|$ converges to the binomial distribution with parameters $(|S|, e^{-\varkappa})$;

3) if

$$\frac{1}{N} \sum_{t=1}^T \mathbf{E}_{\mathcal{P}_t \zeta_t} \rightarrow 0,$$

then $\mathbf{P} \{ \tilde{S}(\mathcal{P}_1, \dots, \mathcal{P}_t) \supseteq S \} \rightarrow 1$.

Remark 3. The condition (12) of the theorem 2 may be dropped if condition of item 1) is enhanced by the relation

$$\max_{t=1, \dots, T} \frac{\mathbf{D}_{\mathcal{P}_t \zeta_t}}{N} < m_1, \quad m_1 = \text{const} > 0$$

and the conditions of item 2) are enhanced by the relation

$$T \max_{t=1, \dots, T} \frac{\mathbf{D}_{\mathcal{P}_t \zeta_t}}{N} < m_2, \quad m_2 = \text{const} > 0.$$

Let us consider two particular cases.

– In the first case each function $f_t \in \mathbf{B}(N)$ is associated with the just introduced set $C_1(f_t, d_t)$, $t = 1, \dots, T$, of functions $g \in \mathbf{B}(N)$ differing from f_t exactly at d_t values of $x \in \{0, \dots, N-1\}$. It is supposed that the uniform probability distributions on the sets $C_1(f_1, d_1), \dots, C_1(f_t, d_t)$ are given.

– In the second case each function $f_t \in \mathbf{B}(N)$ is associated with the set $C_2(f_t, d_t)$, $t = 1, \dots, T$, of functions $g \in \mathbf{B}(N)$ differing from f_t at no more than d_t values of $x \in \{0, 1, \dots, N-1\}$. It is supposed that the uniform probability distributions on the sets $C_2(f_1, d_1), \dots, C_2(f_t, d_t)$ are given.

We denote by $\tilde{S}_1(d_1, \dots, d_t)$ and $\tilde{S}_2(d_1, \dots, d_t)$ the sets of solutions of the system (11) with distortions as in the first and the second cases respectively.

Corollary 2. *Let the left-hand sides of equations in the system (11) be obtained by independent random uniform choice of functions $f_1, \dots, f_t$ from sets $C_1(f_1, d_1), \dots, C_1(f_t, d_t)$ or from sets $C_2(f_1, d_1), \dots, C_2(f_t, d_t)$, let $N, T \rightarrow \infty$ and functions $f_1, \dots, f_t$ are varying in such a way that $|S| = \text{const} \geq 1$. Then:*

1) if

$$\frac{1}{N} \sum_{t=1}^T d_t \rightarrow \infty,$$

then $\mathbf{P}\{\tilde{S}_1(d_1, \dots, d_t) \cap S = \emptyset\} \rightarrow 1$ and $\mathbf{P}\{\tilde{S}_2(d_1, \dots, d_t) \cap S = \emptyset\} \rightarrow 1$;

2) if

$$\begin{aligned} \frac{1}{N} \sum_{t=1}^T d_t &\rightarrow \varkappa \in (0, \infty), \\ \max_{t=1, \dots, T} \frac{d_t}{N} &\rightarrow 0, \\ \sum_{t=1}^T \frac{1}{|A_0(f_t)|} &\rightarrow 0, \end{aligned}$$

then the distributions of random variables

$$|\tilde{S}_1(d_1, \dots, d_t) \cap S| \quad \text{and} \quad |\tilde{S}_2(d_1, \dots, d_t) \cap S|$$

converges to the binomial distribution with parameters $(|S|, e^{-\varkappa})$;

3) if

$$\frac{1}{N} \sum_{t=1}^T d_t \rightarrow 0,$$

then $\mathbf{P}\{\tilde{S}_1(d_1, \dots, d_t) \supseteq S\} \rightarrow 1$ and $\mathbf{P}\{\tilde{S}_2(d_1, \dots, d_t) \supseteq S\} \rightarrow 1$.

4. Conclusion

The problem considered in the paper admits the following interpretation. It is known that the statistical approximations are of great value for the cryptanalysis (see, e. g., [2], [3]). So it is natural to consider the functions $f_1, \dots, f_t$ in the initial system of equations (1) as the universal statistical approximations for all functions from corresponding sets $C_2(f_i, d_i)$ if the values $d_1, \dots, d_t$ are not too large. Remind that $C_2(f, k)$ is the set of those functions $g \in \mathbf{B}(N)$ which differ from the function f at no more than k values of $x \in \{1, \dots, N-1\}$. An analogous interpretation in somewhat different setting was suggested in [6].

Let we have to solve the system of equations

$$g_t(x) = 0, \quad t = 1, \dots, T, \quad (13)$$

with left hand sides $g_t \in C_2(f_t, d_t)$, $t = 1, \dots, T$. If these functions correspond the hypothesis on their randomness and uniformity of distribution, then according to the corollary 2 the substitution of functions f_t for g_t in the left hand sides of the system (13) gives the system

$$f_t(x) = 0, \quad t = 1, \dots, T, \quad (14)$$

such that all its solutions satisfy the system (13) with probability tending to 1 as $N, T \rightarrow \infty$.

Let the numbers $d_1, \dots, d_t$ satisfy more restrictive condition than in Corollary 2:

$$\frac{\ln N}{N} (d_1 + \dots + d_t) \rightarrow 0. \quad (15)$$

For typical statistical approximations the values d_t/N , as a rule, are separated from 0 and therefore does not satisfy this condition.

Of course, the substitution mentioned is useful only if the system (14) admits sufficiently simple solution. As an example we suppose that $\{0, 1, \dots, N-1\} = \{0, 1, \dots, 2^n - 1\} = \{0, 1\}^n$ and consider functions from $\{0, \dots, 2^n - 1\}$ to $\{0, 1\}$ as Boolean functions of n variables. Then the systems (13) and (14) may be represented as

$$g_t(x_1, \dots, x_n) = 0, \quad t = 1, \dots, T, \quad (13a)$$

$$f_t(x_1, \dots, x_n) = 0, \quad t = 1, \dots, T. \quad (14a)$$

As simply solvable system we take the systems of linear Boolean equations. So we will suppose that $f_1, \dots, f_t$ are linear Boolean functions.

For linear function f and sufficiently small (as compared with 2^N) number k all functions $C_2(f, k)$ different from f are nonlinear ones. Therefore we may suppose that functions g_t in the left hand sides of the system (13a) are nonlinear, and that functions f_t are their statistical approximations.

The main question is how to detect the existence of a suitable statistical approximation for the system (13a) and how to find it. Below we suggest a procedure of searching for linear approximation f_t for functions $g_t \in C_2(f_t, d_t)$. It is simpler then analogous procedure in traditional problems.

1. For each $t=1, \dots, T$ we choose (by random or some other method) $n+1$ different pairs (argument value, function value) from the truth table of the function g_t . These pairs uniquely determine a linear function f_t^* as a candidate for the linear statistical approximation f_t of the function g_t . In view of (15) we may suppose that truth tables of functions g_t and f_t are so similar that $f_t^* = f_t$ with probability approximately equal to 1.

2. A system of linear equations

$$f_t^*(x_1, \dots, x_n) = 0, \quad t = 1, \dots, T, \quad (16)$$

is solved.

3. All solutions of the system (16) are checked whether they are the solutions of the system (13a). If the result is positive, then the linear approximation of the system (13a) is found and some of its solutions are obtained. In the opposite case the system (13a) most likely does not have appropriate linear statistical approximation.

The authors are grateful to A. M. Zubkov for support and helpful comments.

References

- [1] Agibalov G. P., "Methods of the solution of systems of equations over a finite field", *Vestnik Tomskogo Gosudarstv. Univ., Prilozhenie*, **17** (2006), 4–9 (in Russian).
- [2] Balakin G. V., "Introduction to the theory of systems of random equations", *Trudy po diskretnoi matematike*, **1**, 1997, 1–18 (in Russian).
- [3] Matsui M., "Linear cryptanalysis method for DES cipher", *Lect. Notes Comput. Sci.*, **765**, 1993, 386–397.
- [4] Mikhailov V. G., "Estimate for the accuracy of the Poisson approximation for the number of empty cells in an equiprobable scheme for group allocation of particles, and applications", *Trudy Matem. Inst. im. V. A. Steklova RAS*, **282**, 2013, 165–180 (in Russian); English transl.: *Proc. Steklov Inst. Math.*, **283**, 2013, 157–171.
- [5] Volgin A. V., "Asymptotic properties of sets of solutions of systems of distorted equations". In: *Abstracts of conference SIBECRYPT'14*, 2014, 48 (in Russian).
- [6] Babash A. V., "Solving automaton equations with distortions in the automaton transition function", *Problemy Peredachi Informatzii*, **38**:3 (2002), 62–71 (in Russian); English transl.: *Probl. Inf. Transmiss.*, **38**:3 (2002), 218–226.

5. Appendix

Proof of Theorem 1.

In view of uniformity of the distribution of the function $\tilde{f}_t$ with respect to zeros of the function f_t , and the equality (5) we have

$$\mathbf{P} \{ \tilde{f}_t(x) = 0 \} = 1 - \frac{v_t}{|A_0(f_t)|} \quad \text{for each } x \in S, \quad t = 1, \dots, T. \quad (17)$$

Let us prove the statement 1). It follows from the independence of distortions of separate functions in systems (1) and (5) that for each $x \in S$

$$\mathbf{P} \{ x \in \tilde{S}(v_1, \dots, v_t) \} = \prod_{t=1}^T \mathbf{P} \{ \tilde{f}_t(x) = 0 \} = \prod_{t=1}^T \left(1 - \frac{v_t}{|A_0(f_t)|} \right), \quad (18)$$

consequently,

$$\mathbf{E} |S \cap \tilde{S}(v_1, \dots, v_t)| = \sum_{x \in S} \mathbf{P} \{ x \in \tilde{S}(v_1, \dots, v_t) \} = |S| \prod_{t=1}^T \left(1 - \frac{v_t}{|A_0(f_t)|} \right). \quad (19)$$

Now it follows from (7) and (19) that

$$\mathbf{E} |S \cap \tilde{S}(v_1, \dots, v_t)| \leq |S| \exp \left\{ - \sum_{t=1}^T \frac{v_t}{|A_0(f_t)|} \right\} \rightarrow 0.$$

Therefore, $\mathbf{P} \{ \tilde{S}(v_1, \dots, v_t) \cap S = \emptyset \} \rightarrow 1$.

Let us prove the statement 3). The formula (17) implies the equalities

$$\mathbf{P} \{ \tilde{f}_t(x) = 1 \} = \frac{v_t}{|A_0(f_t)|} \quad \text{for each } x \in S, \quad t = 1, \dots, T, \quad (20)$$

and we obtain from (20) that

$$\mathbf{P} \{ x \notin \tilde{S}(v_1, \dots, v_t) \} \leq \sum_{t=1}^T \mathbf{P} \{ \tilde{f}_t(x) = 1 \} = \sum_{t=1}^T \frac{v_t}{|A_0(f_t)|} \quad \text{for each } x \in S.$$

Consequently,

$$\mathbf{E} |S \setminus \tilde{S}(v_1, \dots, v_t)| \leq \sum_{x \in S} \mathbf{P} \{ x \notin \tilde{S}(v_1, \dots, v_t) \} \leq |S| \sum_{t=1}^T \frac{v_t}{|A_0(f_t)|}. \quad (21)$$

According to the condition (9) the right hand side of (21) tends to 0. Therefore, $\mathbf{P} \{ \tilde{S}(v_1, \dots, v_t) \supseteq S \} \rightarrow 1$.

The proof of the statement 2) is based on the following statement.

Lemma. *If conditions of the statement 2) of the Theorem 1 are fulfilled and*

$$P = \prod_{t=1}^T \left(1 - \frac{v_t}{|A_0(f_t)|} \right),$$

then there exists an absolute constant $C < \infty$ such that

$$\begin{aligned} & \max_r \left| \mathbf{P} \{ |\tilde{S}(v_1, \dots, v_t) \cap S| = r \} - \binom{|S|}{r} P^r (1-P)^{|S|-r} \right| \leq \\ & \leq C \sum_{t=1}^T \frac{1}{|A_0(f)| - v_t}. \end{aligned}$$

A tedious proof of the Lemma is analogous to the proof of Lemma 1 from [4] and is not given here.

Let us prove the statement 2). It follows from (8) that

$$\sum_{t=1}^T \frac{1}{|A_0(f_t)| - v_t} \rightarrow 0.$$

So, according to Lemma the distribution of the cardinality of the set $\tilde{S}(v_1, \dots, v_t) \cap S$ approaches the binomial distribution $\text{Bi}(|S|, P)$. Further, it follows from the condition (8) of the theorem that $P \rightarrow e^{-\varkappa}$. So, the distribution $\text{Bi}(|S|, P)$ converges to the distribution $\text{Bi}(|S|, e^{-\varkappa})$. The same is true for the distribution of the cardinality of the set $|\tilde{S}(v_1, \dots, v_t) \cap S|$. The Theorem 1 is proved. $\square$