Math-Net.Ru

Общероссийский математический портал

А. А. Kozhevnikov, S. V. Polikarpov, К. Е. Rumyantsev, О разностных свойствах симметричного криптоалгоритма, основанного на псевдодинамических подстановках, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 2, 91–102

DOI: <https://doi.org/10.4213/mvk186>

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: 18.234.156.22

26 апреля 2023 г., 14:11:25

On differential properties of a symmetric cryptalgorithm based on pseudo-dynamic substitutions

A. A. Kozhevnikov, S. V. Polikarpov, K. E. Rummyantsev

Southern Federal University, Taganrog, Russia

Получено 02.III.2015

Abstract. A general structure of a block cryptalgorithm “Collapser” based on pseudo-dynamic substitutions is proposed. Such approach allows to combine advantages of fixed substitutions (high speed implementation and efficient usage of computational resources) and dynamic substitutions (neutralization of statistical methods of cryptanalysis). The differential properties of reduced version of “Collapser” are compared with ones of random substitutions of similar order. It is shown that after 3 rounds “Collapser” looks as a random substitution.

Keywords: block cryptalgorithm, pseudo-dynamic substitution

О разностных свойствах симметричного криптоалгоритма, основанного на псевродинамических подстановках

А. А. Кожевников, С. В. Поликарпов, К. Е. Румянцев

ФГАОУ ВПО Южный федеральный университет, Таганрог

Аннотация. Предлагается общая структура блочного криптоалгоритма «Collapser», основанного на псевродинамических подстановках. Такой подход позволяет использовать преимущества как фиксированных подстановок (высокую скорость реализации и эффективное использование вычислительных ресурсов), так и динамических подстановок (стойкость к статистическим методам криптоанализа). Проведено сравнение разностных свойств уменьшенного варианта «Collapser» и случайных подстановок такого же порядка. Показано, что после 3 раундов преобразование «Collapser» близко к случайной подстановке.

Ключевые слова: блочный шифр, псевродинамические подстановки

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 2, pp. 91–102 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

1. Introduction

Importance of the development of new approaches to the synthesis of symmetric cryptoalgorithms resistant to all known cryptanalytic attacks is confirmed by the series of competitions on cryptographic algorithms held in recent years and high activity of scientific researches in this area. Methods of linear and differential cryptanalysis, and also their modifications are widely used in the security assessment of modern block cryptoalgorithms [1]. It should be noted that the basic elements ensuring the complexity (nonlinearity) of cryptographic transformation are substitutions (*S*-boxes). The specified methods of cryptanalysis are connected with the search and usage of weaknesses of substitutions; the efficiency of these methods are maximal for fixed substitutions [2, 3]. The main contemporary approaches to protect the block cryptoalgorithms from attacks are usage of a large number of encryption rounds (usually at least 8), more effective operations of hashing, selection of substitutions with the extremal characteristics: maximum nonlinearity, minimum autocorrelations and others [4–8].

Naturally, the methods of synthesis of fixed substitutions are nontrivial because a number of cryptographic properties should be simultaneously satisfied [1, 9–12]. In a typical situation the synthesized substitution has good values for one characteristic, and poor for another [7, 9]. The problem is compounded by the fact that substitutions with an ideal linear and differential characteristics don't exist [13].

Another obvious approach to protect the cipher from the linear and differential cryptanalysis is to use dynamic substitutions which are changing during the encryption process [14–18]. However, such approach doesn't guarantee automatic decrease in efficiency of linear and differential cryptanalysis. The effect may be obtained only if the statistical characteristics of dynamic substitutions are close to ideal (under the conditions of equiprobable dynamic change of substitution tables). Besides, the majority of researches on application of dynamic substitutions consider only the option of key-dependency of substitutions (Key-Dependent S-box) — when substitution modification depends on a value of a cryptographic key [14–18]. A number of cryptographic algorithms using this option are known [19–21], but considerable advantages in comparison to analogues were not obtained [5, 22].

In this paper a structure of block symmetric cryptoalgorithm based on the pseudo-dynamic substitutions is considered (*PD-sbox* [23, 24]). Pseudo-dynamic substitutions allow to combine advantages of fixed substitutions (high speed of work and efficient use of computing resources) and dynamic substitutions (protection from the statistical methods of cryptanalysis).

The goal of our research is an assessment of differential properties of reduced versions of the proposed cryptoalgorithm “Collapser” in order to confirm the efficiency of the general structure and application of pseudo-dynamic substitutions of *PD-sbox*.

2. Pseudo-dynamic substitutions

The structure of a pseudo-dynamic substitution (Fig. 1) is based on the fixed substitutions *sbox* [23]. An argument of each fixed substitution will be parameterized by the individual value of a state S^i , where i is a number of the fixed substitution (from 0 to $K - 1$). The current value of a state $S = \{S^0, S^1, S^2, \dots, S^{K-1}\}$ sets one substitution from all set of possible substitutions of *PD-sbox*. We will call a substitution obtained by a concrete value of S the equivalent (generated) substitution for *PD-sbox*. Respectively, the number of various equivalent substitutions for *PD-sbox* is defined by the quantity of possible states of S .

Fig. 1. The structure of pseudo-dynamic substitution

It is supposed that values of a state S are not necessarily fixed and may be changed dynamically during the encryption process, and that their probabilistic properties correspond to the uniform distribution.

The general form of the expression describing the structure of pseudo-dynamic substitution of *PD-sbox*, is the following:

$$Y = \bigoplus_{i=0}^{K-1} sbox_i(X \oplus S^i). \quad (1)$$

where *sbox* is a fixed substitutions, K is a number of fixed substitutions, X denotes input bits; Y — output bits; S — bits of a state of a pseudo-dynamic substitution; $\oplus$ — addition modulo 2.

We have performed a primary analysis of differential and linear characteristics of a pseudo-dynamic substitution *PD-sbox* [24]. In the case of dynamical equiprobable changing of a state S both differential and linear characteristics are close to ideal ones (after averaging over all possible substitutions). This property protects from the existing linear and differential attacks. However, the relevant structure of cryptoalgorithm is necessary for the complete description of *PD-sbox* properties. Here we consider a version of such structure called “Collapser” (a black hole) to assess its differential properties.

3. Notation and parameters of a cryptoalgorithm “Collapser” structure

$PD-sbox$ — pseudo-dynamic substitution,

L_{block} — length of the block of text, in bits,

L_{key} — length of a secret key, in bits,

nr — number of rounds of encryption,

M — number of input bits of pseudo-dynamic substitution of *PD-sbox*,

$N_{words} = L_{block}M$ — number of input words in the block,

$K \geq N_{words}$ — number of the fixed substitutions as a part of *PD-sbox*,

$N_{rows} = K \geq N_{words}$ — number of rows of a matrix of state values,

$m = \{m_0, m_1, \dots, m_{N_{words}-1}\}$ — vector of the initial message,

$a = \{a_0, a_1, \dots, a_{N_{words}-1}\}$ — vector of values at the end of the 1st round,

$b = \{b_0, b_1, \dots, b_{N_{words}-1}\}$ — vector of values at the end of the 2nd round,

$c = \{c_0, c_1, \dots, c_{N_{words}-1}\}$ — ciphertext vector,

IV — initialization vector,

i — number of a column (corresponds to number of the word),

j — line number,

$s_{i,j}^{nr}$ — state values,

$k_{i,j}^{nr}$ — values of an expanded key,

x_i^{nr} — input value of a pseudo-dynamic substitution of *PD-sbox*,

y_i^{nr} — output value of a pseudo-dynamic substitution of *PD-sbox*.

4. A short description of block cryptoalgorithm “Collapser” structure

Figure 2 shows the easily scalable structure of a block cryptoalgorithm under the general name “Collapser”. It is represented by a sequence of the linked pseudo-dynamic substitutions of *PD-sbox*.

Fig. 2. The structure of "Collapser"

The structure is compactly presented in the form of a source code (for example, in language C). An example of a pseudo-code of the program for the encryption function (when $nr = 3$) is the following:

```

1 ENCRYPT_BLOCK_DEADLOOP (M_IN[], C_OUT[], IV[], KEY[]) {
2
3   UNIT A[NWORDS], B[NWORDS], C[NWORDS], S[NROWS];
4
5   FOR (J=0; J<NROWS; J++) { S[J]=IV[J]; }
6
7   ROUND_FUNC (M_IN, A, S, KEY, RAPID_MIX); // PROCESS ROUND 1
8   ROUND_FUNC ( A, B, S, KEY, RAPID_MIX); // PROCESS ROUND 2
9   ROUND_FUNC ( B, C, S, KEY, SHADOW); // PROCESS ROUND 3
10
11  FOR (J=0; J<NROWS; J++) {C_OUT[J]=C[J]; }
12 }

```

The minimum number of rounds of encryption is $nr \geq 3$ and is predetermined by the structure of cryptoalgorithm.

An example of a pseudo-code of the program for round function follows:

```

1 ROUND_FUNC(IN[], OUT[], S[], KEY[][], TYPE) {
2
3   FOR(I = 0; I < NWORDS; I++) {
4     Y = 0;
5     FOR (J = 0; J < NROWS; J++) {
6       S[J] ^= KEY[I][J];
7       S[J] = SBOX[J][S[J]];
8       Y ^= S[J];
9     }
10    OUT[I] = IN[I] ^ Y;
11    FOR (J = 0; J < NROWS; J++) {
12      IF (TYPE == RAPID_MIX) S[J] ^= OUT[I];
13      IF (TYPE == SHADOW) S[J] ^= IN[I];
14    }
15  }
16 }

```

It is supposed that values of the key array are obtained by means of expansion of an initial key, which is not considered within this work.

Generally, *PD-sbox* is represented by 4 operations — expansions (Expand), mixing with an expanded key (Mixkey), the block of nonlinear substitutions (Nonlinear substitution), narrowings (Shrink). Coupling of pseudo-dynamic substitutions of *PD-sbox* is carried out through the state values $s_{i,j}^{nr}$, that allow to accumulate consecutively the entropy and nonlinearity in the state $s_{i,j}^{nr}$. There are two options of connection of *PD-sbox*: with the intensive mixing of state values $s_{i,j}^{nr}$ (RAPID MIX, Fig. 3) and with the masking of state values $s_{i,j}^{nr}$ (SHADOW, Fig. 4). “SHADOW” is implemented in the last round of encryption for “whitening”.

Fig. 3. A pseudo-dynamic substitution, “RAPID MIX” type

Fig. 4. A pseudo-dynamic substitution, "SHADOW" type

The block transformation being not bijective, this structure is applicable only to encryption modes which do not require reversibility of transformation. For example, CTR mode, calculation of hash values or message authentication codes are of this type. It should be noted that the proposed structure of cryptoalgorithm may be transformed to bijective function by breaking the connection between rounds $s_{i,j}^{nr}$ and changing the direction of inclusion of *PD-sbox* (from left to right and vice versa), but this will decrease the total nonlinearity of transformation.

5. Basic principles laid down in "Collapser"

The justification of the proposed structure of cryptoalgorithm will be considered in separate papers. We outline briefly the basic principles laid down in "Collapser".

1. Transition from the size of the input block ($Lblock$) to the size of the state ($Lblock \cdot Nrows$) (expansion).
2. Nonlinear transformation is applied to the state, which size is $Lblock \cdot Nrows$. This allows to maximize complexity (nonlinearity) of cryptographic transformation.
3. Obtaining output values by mapping the results of transformations from state of size ($Lblock \cdot Nrows$) to size of output block ($Lblock$) (shrinking).
4. Application of dynamically changing substitutions based on *PD-sbox* to protect from differential and linear attacks.
5. The special structure of the cryptographic algorithm allowing efficient use of the pseudo-dynamic substitution *PD-sbox*:

5.1. The minimum number of types of operations — only additions modulo 2 (XOR) and substitutions are used.

5.2. Accumulation and transfer of entropy of a state $s_{i,j}^{nr}$ between successively connected *PD-sbox*'es within the round of encryption for maximizing dynamics of change of substitutions.

5.3. Accumulation of nonlinearity of transformations through values of a state $s_{i,j}^{nr}$ between successively connected *PD-sbox*'es within the round of encryption.

5.4. Intensive (rapid) mixing of state values $s_{i,j}^{nr}$ between successively connected *PD-sbox*'es within the round of encryption.

5.5. Protecting from the cryptanalytic attacks based on the restriction of manipulations with input values and accumulation of statistics.

5.6. Masking the state values $s_{i,j}^{nr}$ by introducing uncertainty in the transition from larger dimension to smaller ($2^{M \cdot N_{rows}} \rightarrow 2^M$).

5.7. Additional transfer of values of a state $s_{i,j}^{nr}$ between rounds to increase the uncertainty and nonlinearity of transformations.

6. Simplicity of scalability of cryptoalgorithm structure with various lengths of blocks and keys.

6. Assessment of full differentials for reduced versions of cryptoalgorithm "Collapser"

In order to determine the resistance against differential cryptanalysis we use the approach proposed in [5] and based on the determination of the full differentials distribution for reduced versions of cryptoalgorithms and comparison of the obtained results with the distribution of full differentials for random substitutions of similar order. As indicators we will use the maximum value of differential probability (DP_{max}^f) and average maximum value of differential probability (ADP_{max}^f) for key dependent function f . For random substitution of the order $2^{L_{block}}$ in [5] a theoretical estimate for ADP_{max}^f in the form $ADP_{max}^f \leq (L_{block} + 4)$ was proposed.

For the experiment 4 fixed bijective substitutions were created for $M = 4$ bits (Table 1) in a random way.

Table 1. Fixed substitution components *PD-sbox*

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$sbox_0(X)$	5	B	E	F	6	A	0	8	C	D	1	4	2	9	7	3
$sbox_1(X)$	7	8	6	0	B	E	A	C	5	4	1	9	D	F	3	2
$sbox_2(X)$	E	5	4	F	8	0	6	D	A	7	3	B	2	C	1	9
$sbox_3(X)$	4	5	1	B	E	3	6	2	7	0	A	C	9	D	F	8

Depending on the configuration, *PD-sbox* includes from 2 to 4 fixed substitutions ($N_{rows} = 2 \dots 4$). Taking into account restriction $N_{words} = N_{rows}$, the length of the block $L_{block} = N_{words} \cdot M$ was equal to 8, 12 and 16 bits respectively.

For each configuration differential properties were obtained for 100 keys. The results are shown in the columns "Collapser" of Tables 2–4.

In addition, for the analysis of dynamics of differential characteristics changing, we took values of a state $s_{i,j}^{nr}$ on a certain step as output values for the corresponding substitution of *PD-sbox* in the structure of cryptoalgorithm (see Fig. 2). So, $step = 0$ corresponds to a condition of the initial *PD-sbox* located in the upper left corner of structure in Figure 2. The number of a step is defined as $step = (nr - 1) \cdot N_{words} + i$. The results obtained are given in the columns of the same title.

For comparison, in the column "Random subst" we present the values for 100 randomly generated bijective substitutions of the corresponding order.

Table 2. Maximum values in tables of differences for $N_{words} = N_{rows} = 2$ and $M = 4$ ($L_{block} = 8$ bit)

	step=2 nr=2	step=3 nr=2	step=4 nr=3	step=5 nr=3	Collapser	Random subst.
ADP_{max}^f	256	50,82	12,56	11,28	11,2	11,44
DP_{max}^f	256	64	18	14	14	16

Table 3. Maximum values in tables of differences $N_{words} = N_{rows} = 3$ and $M = 4$ ($L_{block} = 12$ bit)

	step=5 nr=2	step=6 nr=3	step=7 nr=3	step=8 nr=3	Collapser	Random subst.
ADP_{max}^f	141,04	124,68	15,34	15,34	15,52	15,5
DP_{max}^f	226	170	18	18	20	20

Table 4. Maximum values in tables of differences $N_{words} = N_{rows} = 4$ and $M = 4$ ($L_{block} = 16$ bit)

	step=7 nr=2	step=8 nr=3	step=9 nr=3	Collapser	Random subst.	babyAES
ADP_{max}^f	81,78	19,06	19,24	18,98	19	19,326
DP_{max}^f	192	22	24	22	22	20

7. Conclusions

The results (tables 2-4) agree with the principles laid down in the structure of “Collapser”.

1. The first round ($nr = 1$) of encryption serves for the primary set of uncertainty and nonlinearity of values of states $s_{i,j}^{nr}$. Because the substitutions of *PD-sbox* are switching consequently, the greatest uncertainty is achieved on the last step of a round.

2. On the second round ($nr = 2$) of encryption due to input of the state value $s_{i,j}^{nr}$ from the first round, there are interrelations between elements of vector $b = \{b_0, b_1, \dots, b_{N_{words}-1}\}$, that leads to intensive growth of transformation nonlinearity. However, the second round is not enough for achieving the necessary transformation nonlinearity. For example, there is a short way (in only one substitution of *PD-sbox*) between values b_0 and $m_{(N_{words}-1)}$ through the value of state $s_{0,j}^2 = s_{N_{words},j}^1$.

3. In the third round ($nr = 3$) of encryption the sufficient complexity of dependencies between all the elements of the vector of ciphertext $c = \{c_0, c_1, \dots, c_{N_{words}-1}\}$ is achieved. The minimum number of substitutions transforming the words of initial message into the words of ciphertext equals to N_{words} and is realised between the words $m_{(N_{words}-1)}$ and c_0 . After the junction of the 2nd and 3rd rounds (at the beginning of the 3rd round) the distribution of differentials for values $s_{i,j}^{nr}$ of states becomes closer to that of random substitutions; this corroborates the hypothesis on high nonlinearity.

4. Despite of considerable differences between the distributions of differentials for values $s_{i,j}^{nr}$ of a state at the first steps of the 3rd round (step=3 for tables 2 and step=6 for table 3) the final distribution of differentials for values of the ciphertext (column “Collapser”) corresponds to that of random substitutions. This confirms the property of masking the values of a state $s_{i,j}^{nr}$ due to introduction of uncertainty upon transition from larger dimension to smaller one ($2^{M \cdot N_{rows}} \rightarrow 2^M$) when forming output values.

The results presented should be considered as an initial assessment of differential properties of the proposed structure of cryptoalgorithm “Collapser”. This algorithm needs additional research.

8. Acknowledgements

The work is supported by Ministry of Education and Science of the Russian Federation. Theme № 213.01-11 / 2014-9.

References

- [1] Preneel B., Biryukov A., De Canni'ere C., Örs S. B., Oswald E., Van Rompay B., Granboulan L., Dotta E., Martinet G., Murphy S., Dent A., Shipsey R., Swart C., White J., Dichtl M., Pyka S., Schafheutle M., Serf P., Biham E., Barkan E., Braziler Y., Dunkelman O., Furman V., Kenigsberg D., Stolin J., Quisquater J.-J., Ciet M., Sica F., Raddum H., Knudsen L., Parker M., "Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 — Version 0.15 (beta)" (2004), iii+829 pp., <https://www.cosic.esat.kuleuven.be/nessie/Bookv015.pdf>.
- [2] Matsui M., "Linear cryptanalysis method for DES cipher". In: "*Advances in Cryptology—EUROCRYPT'93*", Lect. Notes Comput. Sci., **765** 1994, 386–397.
- [3] Biham E., Shamir A., "Differential cryptanalysis of DES-like cryptosystems", *J. Cryptology*, **4**:1 (1991), 3–72.
- [4] Braeken A., Nikov V., Nikova S., Preneel B., "On Boolean functions with generalized cryptographic properties". In: "*Progress in Cryptology—INDOCRYPT 2004*", Lect. Notes Comput. Sci., **3348** 2005, 120–135.
- [5] Dolgov V. I., Kuznetsov A. A., Isaev S. A., "Differential properties of block symmetric ciphers", *Elektr. modelir.*, **33**:6 (2011), 81–99 (in Russian).
- [6] Gorbenko I. D., Dolgov V. I., Lisitskaya I. V., Oleynikov R. V., "New ideology of the block symmetric ciphers security estimation against differential and linear cryptanalysis", *Prikl. radioelektr.*, **9**:3 (2010), 312–320 (in Russian).
- [7] Kazymyrov O., Oliynykov R., "Application of vectorial Boolean functions for substitutions generation used in symmetric cryptographic transformation", *Sistemy obrabotki informacii* (Kharkiv), **6**:104 (2012), 97–102 (in Russian).
- [8] Logachev O. A., Salnikov A. A., Yaschenko V. V., *Boolean functions in the coding theory and cryptology*, Moscow: MCCME, 2004 (in Russian), 470 pp.
- [9] Ivanov G., Nikolov N., Nikova S., "Reversed genetic algorithms for generation of bijective S-boxes with good cryptographic properties", *IACR Cryptology ePrint Archive*, 19 pp., <https://eprint.iacr.org/2014/801.pdf>.
- [10] Beelen P., Leander G., "A new construction of highly nonlinear S-boxes", *Cryptogr. Commun.*, **4**:1 (2012), 65–77.
- [11] Fu S., Matsuura K., Li C., Qu L., "Construction of highly nonlinear resilient S-boxes with given degree", *Des. Codes Cryptogr.*, **64**:3 (2012), 241–253.
- [12] Kazymyrov O., Kazymyrova V., Oliynykov R., "A method for generation of high-nonlinear S-boxes based on gradient descent", *IACR Cryptology ePrint Archive*, 9 pp., <https://eprint.iacr.org/2013/578.pdf>.
- [13] Tokareva N. N., "Generalizations of bent functions. A survey", *Diskretn. Anal. Issled. Oper.*, **17**:1 (2010), 34–64 (in Russian); English Translation, *J. Appl. Industr. Math.*, **5**:1 (2011), 110–129.
- [14] Zaibi G., Peyrard F., Kachouri A., Fournier-Prunaret D., Samet M., "A new design of dynamic S-Box based on two chaotic maps". In: "*ACS/IEEE International Conference on Computer Systems and Applications—AICCSA 2010*", Piscataway, NJ: IEEE, 2010, 1–6.
- [15] Ahmad M., Khan P. M., Ansari M. Z., "A simple and efficient key-dependent S-box design using Fisher–Yates shuffle technique". In: "*Recent Trends in Computer Networks and Distributed Systems Security*", SNDS 2014, Commun. Comput. Inf. Sci., **420**, 2014, 540–550.

- [16] Pradeep L. N., Bhattacharjya A., “Random key and key dependent S-box generation for AES cipher to overcome known attacks”. In: “*Security in Computing and Communications*”, SSCC 2013, Commun. Comput. Inf. Sci., **377**, 2013, 63–69.
- [17] Hosseinkhani R., Javadi H. H. S., “Using cipher key to generate dynamic S-box in AES cipher system”, *Int. J. Comput. Sci. Secur.*, **6**:1 (2012), 19–28.
- [18] Mahmoud E. M., El Hafez A. A., Elgarf T. A., Zekry A., “Dynamic AES-128 with key-dependent S-box”, *Int. J. Engrg Res. Appl.*, **3**:1 (2013), 1662–1670, http://www.ijera.com/papers/Vol3_issue1/IW3116621670.pdf.
- [19] Schneier B., “Description of a new variable-length key, 64-bit block cipher (Blowfish)”. In: “*Fast Software Encryption*”, Lect. Notes Comput. Sci., **809**, 1994, 191–204.
- [20] Kuznetsov A. A., Sergienko R. V., Nausko A. A., “Symmetric cryptographic algorithm ADE (Algorithm of Dynamic Encryption)”, *Prikl. radioelektr.*, **6**:2 (2007), 241–249 (in Russian).
- [21] Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M. J. B., Seurin Y., Vikkelsoe C., “PRESENT: an ultra-lightweight block cipher”. In: “*Cryptographic Hardware and Embedded Systems – CHES 2007*”, Lect. Notes Comput. Sci., **4727**, 2007, 450–466.
- [22] Borghoff J., Knudsen L. R., Leander G., Thomsen S. S., “Cryptanalysis of PRESENT-like ciphers with secret S-boxes”. In: “*Fast Software Encryption*”, FSE 2011, Lect. Notes Comput. Sci., **6733**, 2011, 270–289.
- [23] Polikarpov S. V., Rummyantsev K. E., Kozhevnikov A. A., “Pseudodynamical substitution tables: the base of contemporary symmetric cryptoalgorithms”, *Nauchn. obozr.*, № 12 (2014), 162–166 (in Russian).
- [24] Polikarpov S. V., Rummyantsev K. E., Kozhevnikov A. A., “Pseudodynamical substitution tables: A study of differential characteristics”. In: “*Fiziko-matematicheskie metody i informatzionnye tekhnologii v estestvoznanii, tekhnike i gumanitarnykh naukakh*”, Kirov: MCNIP, 2015, 77–89 (in Russian).