Виконується адаптація і застосування методу оцінювання верхньої межі ймовірності двоциклових диференціалів для блокового симетричного шифру Калина, який прийнятий в 2015 році в якості українського стандарту ДСТУ 7624:2014. Відомі методи або дозволяють отримати тільки наближене значення даного параметра для цього шифру, або не можуть бути застосовані в явному вигляді через структурні особливості цього шифру. Використання наближеного значення ймовірності двоциклових диференціалів дає ще більшу похибку при оцінюванні ймовірностей диференціалів з великою кількістю циклів, а також при оцінюванні стійкості алгоритму шифрування до інших видів диференціальних атак.

Основні етапи методу, що використовується, наступні: визначення мінімальної кількості активних S-блоків; визначення вида диференційної характеристики, що має максимальну ймовірність; визначення кількості та ймовірностей додаткових диференційних характеристик.

В ході досліджень адаптований метод дозволив значно уточнити верхню межу ймовірності 2-циклових диференціалів для шифру «Калина». Ця межа становила ≈2–47,3, замість 2–40 при використанні методу для вкладених SPN шифрів (Nested SPN Cipher).

Уточнене значення верхньої межі ймовірності 2-циклових диференціалів дозволило уточнити і граничне значення ймовірності 4 циклових диференціалів. Для Калини-128 (розмір блоку 128 бітів) значення уточнено в 214,6 разів, для Калини-256 – в 229,2 разів, Калини-512 – в 258,4 разів.

Основною перевагою адаптованого для шифру Калина методу стала можливість істотного уточнення верхньої межі ймовірності 2-циклового диференціала. Недоліком адаптованого методу є прийняті допущення, такі як, наприклад, використання однієї підстановки замість чотирьох в оригінальному алгоритмі. Результатом цього припущення може стати те, що в реальному алгоритмі ймовірності 2-циклових диференціалів будуть ще меншими

Ключові слова: блокові шифри, криптографічна стійкість, Rijndael, AES, Rijndael-подібний шифр, ймовірність диференціала, диференційна характеристика, таблиця різностей, Калина, ДСТУ 7624:2014

UDC 004.056.55
DOI: 10.15587/1729-4061.2018.139682

ANALYSIS OF PROBABILITIES OF DIFFERENTIALS FOR BLOCK CIPHER "KALYNA" (DSTU 7624:2014)

V. Ruzhentsev
Doctor of Technical Sciences,
Associate Professor
Department of information technologies security
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
E-mail: viktor.ruzhentsev@nure.ua

V. Sokurenko
Doctor of Juridical Sciences,
Associate Professor, Rector
Kharkiv National University of Internal Affairs
L. Landau ave., 27, Kharkiv, Ukraine, 61000
E-mail: sokurenko@univd.edu.ua

Y. Ulyanchenko
Doctor of Science in Public Administration,
Associate Professor
Department of Economic Policy
and Management
Kharkiv Regional Institute of Public
Administration of the National Academy of
Public Administration attached
to the Office of the President of Ukraine
Moskovskyi ave., 75, Kharkiv, Ukraine, 61001
E-mail: y.ulyanchenko@gmail.com

1. Introduction

The acuteness of the problem of information security is becoming increasingly significant and global. Cryptographic algorithms that meet modern requirements are an integral part of solving this problem. Block Symmetric Ciphers (BSCs), which are one of the most common types of cryptographic algorithms, should provide high speed and resistance to known cryptanalytic attacks in accordance with modern requirements.

It is generally accepted that the differentials and their probabilities must be considered for analyzing the resistance of the BSC to differential attacks. Confirmation of this fact can be found in the works [1–3], in which the probabilities of differentials for the most common modern cipher AES are studied. The actual direction of research is the development of an approach to the estimation of the probabilities of differentials for the BSC Kalyna, which was adopted as the Ukrainian standard DSTU 7624:2014 in 2015.

2. Literature review and problem statement

The maximum probability of the differential is the main indicator, which reflects the resistance of the BSC to the differential cryptanalysis. It should be noted that most of the estimates received even for the most common cipher AES (Rijndael) for today are approximate. Thus, detailed and accurate estimates are obtained only for 2-round AES differentials in [4]. In [5], the well-known estimates for that time for 4-round differentials AES were substantially elaborated.

In 2015, the new BSC Kalyna was adopted in Ukraine as the standard DSTU 7624:2014. The algorithm is Rijndael-like, and the specification is given in [6, 7]. Certain dif-

ferences of this algorithm from AES make the methods [4, 5] inapplicable for this algorithm. These differences include, firstly, the use of nonlinear substitutions of a random type with controlled cryptographic parameters. Secondly, the use of an enlarged fixed matrix, which is multiplied by each column of a block within a linear transformation, which is an analogue of the MixColumn transformation in AES.

The use of the approach proposed in [2] and developed in [8] will also be problematic as a result of an increased fixed matrix, which is multiplied by each column of a block within the linear transform of the Kalyna cipher.

In [9], a method for evaluating the maximum probability of two-round differentials for Rijndael-like ciphers was proposed. This method, unlike the similar method previously known from [4], does not depend on the type of used nonlinear substitutions. However, in [9], the application of this method was demonstrated only for ciphers with algebraically constructed substitutions.

The study of the issue of estimating the maximum probability of differentials of BSCs including the Rijndael-like ciphers was presented in [10, 11]. The approach proposed in these works commonly uses the analysis of reduced cipher models (block size up to 16 bits) or the consideration of a small part of the block (up to 16 bits) and subsequent interpretation of the result for a full-length encryption algorithm. In [10], two-round differentials of some modern ciphers, including AES (Rijndael-128), are analyzed using this approach. The main disadvantage of the considered approaches are inaccurate, highly approximate results that are very different from the known ones.

In [12], the example of the consideration of reduced models with a 16-bit block of Rijndael-like ciphers demonstrated the validity of the estimates obtained by the method of [9] for ciphers with arbitrary substitutions. However, this method has never been applied for the new Ukrainian standard DSTU 7624:2014.

The upper bound of the probability of two-round differentials for this cipher can be obtained on the basis of the materials of the works [3, 13] and known maximum probability of passing the non-zero difference through the substitution, which is 2^{-5}. The resulting approximate upper border value will be $\left(2^{-5}\right)^8 = 2^{-40}$. Using of such an approximate value will give an even greater error in estimating the probabilities of differentials with a large number of rounds, as well as in assessing the resistance of the encryption algorithm to other types of differential attacks. Thus, the main problem issue of this work is to obtain a more precise value of the upper bound of the probability of two-round differentials for the Ukrainian standard of encryption DSTU 7624:2014.

3. The aim and objectives of the study

The aim of this work is to obtain a more precise value of the upper bound of the probability of two-round differentials for the Ukrainian standard of encryption DSTU 7624: 2014.

To achieve this aim, it is necessary to accomplish the following objectives:

– to adapt the method proposed in [9] for the new Ukrainian standard DSTU 7624: 2014;

– to estimate the upper bound of the probability of 2-round differentials for this cipher;

– to make a comparative analysis of the known and obtained values of the probability of a 2-round differential and the upper bounds of the probabilities of differentials with a large number of rounds.

4. Rijndael-like cipher Kalyna (DSTU 7624:2014)

A convenient way to represent a data block of the Rijndael-like cipher is a matrix in which each cell is a byte. Each round of Rijndael-like ciphers consists of four procedures: ByteSub (BS); ShiftRow (SR); MixColumn (MC); AddRoundKey.

During the ByteSub procedure, a nonlinear substitution for each block byte is made in accordance with a fixed 256-byte table.

The ShiftRow procedure performs the exchange (repositioning) of bytes between columns of the information block by cyclic shifting of the rows to different numbers of bytes.

The MixColumn procedure converts each column $a(x)$ into the word $b(x)$ by the following rule: $b(a(x))=c(x)\otimes a(x)$, where $c(x)$ is a fixed polynomial; $\otimes$ denotes an operation of multiplying polynomials with coefficients from GF (2^8) according to the selected module. This transformation is usually represented in the form of multiplying the vector a by the matrix c.

The AddRoundKey procedure performs a bitwise modulo 2addition of the data block and the fragment of an extended key of the corresponding size.

During the decryption, the inverse procedures are performed in reverse order.

There is a possibility to change the order of some of the transformations. For example, this is the case for the sequence of BS and SR. It's clear that it does not matter: first perform the BS substitution, and then rearrange the bytes, or vice versa. Because of the linearity of the transformation, MC can be changed in places with the AddKey transformation, but in this case you need to make an addition with a subkey for which the MC transformation is pre-executed.

There is an alternative representation of round transformations when the ByteSub, MixColumns, AddKey, and ByteSub operations are combined into 32-bit super boxes (highlighted in color in Table 1).

Each of these super boxes works with one column of a data block. 4 such 32-bit super boxes with the addition of some linear transformations before and after are equivalent to two-round encryption (Table 1).

Two levels of super boxes, which run between SR, MC, AddKey and SR, are called mega box in [5]. One such 128-bit mega box, with the addition of some linear transformations before and after is equivalent to 4-round encryption (highlighted in color in Table 1).

The new BSC Kalyna was adopted as the Ukrainian standard DSTU 7624:2014 in 2015. This is a Rijndael-like algorithm, which has a number of changes compared with AES:

1) using of non-linear random substitutions with controlled cryptographic parameters;

2) using of an enlarged fixed matrix (8×8 bytes matrix size), which is multiplied by each column of the block (each column has the size of 8 bytes or 64 bits) within the linear transformation – the analogue of the MixColumn transformation in AES;

3) using of a new key expansion scheme that does not allow restoring the value of the source secret key from the value of one of the subkeys;

4) using of adding operations with different modules in AddKey transformations.

Table 1

An alternative representation of a sequence of transformations, a super box, a mega box

Original sequence of transformations for 4 rounds	Alternative sequence of transformations for 4 rounds	4 rounds using super boxes	4 rounds using mega boxes
AddKey0	AddKey0	AddKey0	AddKey0
BS1	SR1	SR1	SR1
SR1	BS1	4 super boxes 32 to 32 bits	mega box 128 to 128 bits
MC1	MC1		
AddKey1	AddKey1		
BS2	BS2		
SR2	SR2	SR2	
MC2	MC2	MC2	
AddKey2	AddKey2	AddKey2	
BS3	SR3	SR3	
SR3	BS3	4 super boxes 32 to 32 bits	
MC3	MC3		
AddKey3	AddKey3		
BS4	BS4		
SR4	SR4	SR4	SR4
MC4	MC4	MC4	MC4
AddKey4	AddKey4	AddKey4	AddKey4

The specification of this encryption algorithm is given in [6, 7]. The number of rounds depends on the size of the key and it is 10, 14 and 18 rounds for keys of 128, 256 and 512 bits, respectively. The size of the cipher's block is not less than the size of the key. Cipher variants with a block size of 128, 256, and 512 bits will be hereinafter denoted as Kalyna 128, Kalyna 192 and Kalyna 256, and blocks of these algorithms contain 2, 4, and 8 64-bit columns, respectively.

5. The main ideas of the approach used to determine the upper bound of probabilities for 2-round differentials

It is known that there is a possibility to perform an exact estimation of the upper bound of the probability of differentials for modern block ciphers only for a small number of rounds. For the Rijndael cipher, this number of rounds is 2, and the corresponding method was proposed in [4].

For the Rijndael cipher, the results obtained in [9] coincide with the results of [4]. At the same time, the estimation of the probabilities of two-round differentials uses the analysis of the properties of the differences tables of the cipher's S-boxes, which makes it possible to use this method for ciphers with arbitrary substitutions, which is the case for the Kalyna cipher. Numerous computational experiments in the study of reduced-size super boxes from 4 to 32 bits with the S-box size from 2 to 8 bits are described in [9]. Experiments on the search for 2-round differentials for such super boxes have shown that the differential having the maximum probability always contains a differential characteristic (DC), which also has a maximum probability. Using this fact, the proposed method contains the following basic steps:

1) determination of the minimum number of active S-boxes in the 2-round DC;

2) determination of the form of DC having the maximum probability;

3) determination of the number and probabilities of additional DCs;

4) determination of the maximum probability of a 2-round differential as a sum of the results from step 2 and 3.

The input data for this method are the fixed matrix which is used in the multiplication during the MC transformation and the S-boxes with their difference tables.

The presented above steps of the method are quite clear if we assume that the probability of a differential is the sum of the probabilities of all the DCs which belong to this differential. The most problematic in practice is the implementation of stage 3. The next section will demonstrate how the proposed approach can be implemented in the case of the encryption transformations of the Kalyna algorithm.

6. Probabilities of two-round differentials for the Kalyna cipher

6. 1. Super boxes of the Kalyna cipher

The Super box consists of the ByteSub, MixColumns, AddKey, and ByteSub operations and works with one column of the data block. The Super box of Kalyna works with a 64-bit block and it is impossible to research such a super box in a "power" way.

4 different substitutions are used as 8-to-8-bit S-boxes. The substitutions are formed randomly with the control of the following parameters: the maximum value in the difference table (for all substitutions this value is equal to 8), the maximum value in the table of linear approximations (for all substitutions this value is 26), the degree of nonlinearity (for all substitutions this value is 7). The difference tables of the S-boxes are important in the differential probability estimation. The number of maximum values, "8", in the difference tables for these 4 substitutions is 15, 9, 7 and 9. Obviously, the substitution with 15 maximum values in the difference table will allow us to construct a two-round differential that will have the maximum probability. Therefore, further we will consider the worst case, when only one such substitution is used in the BS transformation of the cipher (Fig. 1).

```
14 9D B9 E7 67 4C 50 82 CA E5 1D 31 0A C6 B2 51
A2 D8 54 90 D0 CE 2D 7D C7 7E D7 94 DF 83 8E 6C
66 D2 6F 16 1E 76 FE CC AA 5A 8F 17 BD 2C AC EA
7B 65 A9 10 C0 92 EE BE 6A 6E 48 96 95 E9 32 BC
A1 42 D5 A7 81 B4 5F E6 C2 5D AD 3A B7 0C 8D 01
98 FD 12 02 75 13 0F 6B 22 E2 AB F7 7F BA 97 D1
64 D9 C4 59 AF 23 33 37 DE AE 60 05 63 A8 52 A5
4E E0 DD 71 F2 24 34 57 47 A4 B3 9E 2F C1 B8 CB
2B D4 0D 36 91 8B 9C 26 25 61 A3 D6 EB 35 53 F4
2E 88 80 E4 30 DB FC 0E 77 8C 93 A6 78 06 E1 EC
F9 03 A0 27 DA EF 5C 00 7A 45 E8 40 1A 4B 5E 73
C3 FF F5 F3 B0 C5 49 21 FA 11 39 84 43 38 85 07
F0 79 46 F8 E3 1F 09 B6 CD 55 1C 1B FB 7C ED 6D
15 56 86 20 68 4A 41 4F D3 99 08 F6 3F 89 62 04
CF C8 69 9F 19 5B 44 9B 87 B1 3D BB DC 2A BF 58
3C 8A 18 3E 72 0B 28 4D B5 9A C9 74 29 F1 3B 70
```

Fig. 1. Substitution S0 of the cipher Kalyna (in hexadecimal format)

It is expected that this version in comparison with the original will have higher probabilities of the differentials and, accordingly, lower level of security.

The number of cells in the substitution difference table, excluding the first row and the first column, is

255×255=65,025. Table 2 shows the statistical information about the difference table for the selected substitution.

Table 2

Statistical information for the difference table of the 8-to-8-bit substitution

Values	Number of values in the difference table
"8"	15
"6"	246
"4"	3,423
"2"	24,996
"0"	36,345

Table 2 demonstrates that 56 % of the difference table's values are "0", and 44 % are non-zero values.

Denote the fixed matrix that is used in the MixColumns (MC) by M

$$M=\begin{bmatrix}1&1&5&1&8&6&7&4\\4&1&1&5&1&8&6&7\\7&4&1&1&5&1&8&6\\6&7&4&1&1&5&1&8\\8&6&7&4&1&1&5&1\\1&8&6&7&4&1&1&5\\5&1&8&6&7&4&1&1\\1&5&1&8&6&7&4&1\end{bmatrix}.$$

Thus, the main transformations of the Kalyna's super box are presented.

6. 2. Search for maximum probability DC

The computational experiments performed for reduced models and presented in [9, 12] confirmed the following regularities. First, to find DC, which has the maximum probability, you should look for the path of difference transformation with the minimum total number of active substitutions. For Kalyna, this value is 9. Second, the maximum must be the number of duplicate values of the difference at the inputs of both levels of substitutions. During the analysis of the matrix multiplication operation, such a path of difference transformation was determined for the Kalyna cipher. Expression (1) shows the procedure of multiplication of the column by the matrix M.

$$\begin{bmatrix}x\\x\\0\\0\\0\\0\\0\\0\end{bmatrix}\times M=\begin{bmatrix}0\\5x\\3x\\x\\ex\\9x\\4x\\4x\end{bmatrix}. \qquad (1)$$

The input column contains the same non-zero values of the difference x in the first two bytes and the zero difference in the remaining bytes.

The specified path of the difference contains the minimum total number of active substitutions – 2+7=9, with 3 difference value x and 2 difference value $4x$ at the inputs of both levels of substitutions.

Taking into account the data from Table 2, there are 15 variants of the value of the difference x at the output of the first level of permutations, for which a transition of difference may occur with a probability of 8/256. The probability that for the value of the difference $4x$ also there will be a transition with a probability of 8/256 is 15/255. Then the expected number of cases where two first-level difference transitions and two out of seven transitions of the second-level difference of the substitutions will have a probability of 8/256, will be

$$15\cdot\frac{15}{255}=\frac{225}{255}\approx 0,88.$$

The expected number of cases where even at least one another transition of the second-level difference will have a probability of 8/256 will be even lower. However, as can be seen from Table 2, there are many transitions with a probability of 6/256 in the difference table. Therefore, for the remaining 5 values of the difference in the input of the second level of permutations ($5x$, $3x$, x, ex, $9x$) with a probability close to 1,there will be transitions with probability 6/256. Then the final probability of such a basic DC will be

$$\left(\frac{8}{256}\right)^4\cdot\left(\frac{6}{256}\right)^5=\frac{243\cdot 2^9}{2^{64}}.$$

The second stage of the method is completed.

6. 3. Number and probabilities of additional DCs

Now the number and probabilities of additional DC should be estimated.

Taking into account Table 2, there are $\approx 254\cdot 0,44\approx 112$ possible additional variants of the difference at the output of substitutions of level 1. It is important that the values at the output of these two substitutions should be the same, since otherwise there will not be zero difference in the first byte of the output of MC difference.

In accordance with expression (1), at the input of level 2 of the substitutions there will be 6 different non-zero values of the difference. The probability that for each of these six separate active substitutions there will be a transition to the output value determined by basic DC is 0.44. Then the probability that for all 6 cases the necessary transitions of the difference will be possible will be $(0,44)^6$; and the expected number of additional DCs will be $112\cdot(0,44)^6\approx 0,8$. Thus, most likely that there will be only one additional DC. According to the data from Table 2, most transitions will have a probability of 2/256 in this additional DC. Even if half of these transitions will have a probability of 4/256, then, compared with the probability of the basic DC, the probability of additional DCs will be insignificant:

$$\left(\frac{4}{256}\right)^4\cdot\left(\frac{2}{256}\right)^5=\frac{2^5}{2^{64}}.$$

The upper bound of the probability of a 2-round differential is the result of summing the values obtained in subsections 6.2 and 6.3:

$$\frac{243\cdot 2^9}{2^{64}}+\frac{2^5}{2^{64}}\approx 2^{-47,3}.$$

7. Discussion of the results obtained using known and new methods

The upper bound values of the probabilities of differentials can be obtained for SPN-ciphers using the theorem from [13].

Theorem ([13]). If n S-boxes are used in the SPN-cipher, and the linear transformations provide the number of branches equal to $n–t$, then the probability of a differential covering 2 and more rounds will be bounded above by the value of p^{n-t-1}, where p is the maximum probability of a non-zero difference transition through the S-box.

For the ciphers that use nested SPN structures, the theorem is proved in [3]. According to this theorem, the value of the differential probability is bounded above by the value

$$p^{(n_1-(t_1+1))(n_2-(t_2+1))}, \quad (2)$$

where n_1 is the number of S-boxes in each super box, n_2 is the number of super boxes in the block, $n_1–t_1$ and $n_2–t_2$ are the branch number provided by the lower and upper levels of the diffusion transformations, respectively.

For the Rijndael-128 cipher, according to these theorems, the upper bound of the probability of a 2-round differential is $\left(2^{-6}\right)^4 = 2^{-24}$, and the upper bound of the probability of the 4-round differential – $\left(2^{-24}\right)^4 = 2^{-96}$. The methods proposed in [4, 9] allow getting a more accurate estimation for the upper bound of the probability of a 2-round differential: $\frac{13}{2^{32}} \approx 2^{-28,3}$. Then the corresponding upper bound of the probability of the 4-round differential will be $\left(2^{-28,3}\right)^4 = 2^{-113,2}$.

Using the value obtained in Section 6 for a 2-round differential and the presented above theorem from [13], the upper bounds of the probabilities of differentials for variants of the Kalyna cipher with the size of block 128, 192 and 256 bits can be substantially elaborated (Table 3).

The upper bounds of the probabilities of the 2- and 4-round differentials for the Kalyna cipher presented in Table 3, obtained using the method proposed in section 6, are the most accurate of the known.

The studies presented in this paper are a continuation of the studies presented in [4, 9, 12].

The main advantage of the method adapted for the Kalyna cipher is the possibility to get a more accurate value for the upper bound of the probability of a 2-round differential (the first column of Table 3). The disadvantage of the adapted method is the assumptions that were made, such as, for example, the use of one substitution instead of four in the original algorithm. The result of this assumption can be that the real probability of 2-round differentials could be even smaller than the obtained value.

Table 3

The upper bounds of the probabilities of differentials for the Kalyna cipher

Evaluation options	2-round differential	4-round differential, Kalyna-128	4-round differential, Kalyna-256	4-round differential, Kalyna-512
Using (2)	$\left(2^{-5}\right)^8 = 2^{-40}$	$\left(2^{-40}\right)^2 = 2^{-80}$	$\left(2^{-40}\right)^4 = 2^{-160}$	$\left(2^{-40}\right)^8 = 2^{-320}$
Proposed method	$2^{-47,3}$	$\left(2^{-47,3}\right)^2 = 2^{-94,6}$	$\left(2^{-47,3}\right)^4 = 2^{-189,2}$	$\left(2^{-47,3}\right)^8 = 2^{-378,4}$

8. Conclusions

1. The adaptation and application of the previously proposed method of [9, 12] for the Rijndael-like Kalyna cipher, which in 2015 was adopted as the Ukrainian standard DSTU 7624: 2014, were made.

2. The application of the adapted method has made it possible to get a more precise value of the upper bound of the probability of 2-round differentials for the Kalyna cipher. This upper bound is $\approx 2^{-47,3}$, instead of 2^{-40} with using (2).

3. The more precise value of the upper bound of the probability of 2-round differentials made it possible to get a more precise boundary value of the probability of 4-round differentials. For Kalyna-128, the value is specified $2^{14,6}$ times, for Kalyna-256 – $2^{29,2}$ times, for Kalyna-512 – $2^{58,4}$ times.

References

1. Provable Security against Differential and Linear Cryptanalysis for the SPN Structure / Hong S., Lee S., Lim J., Sung J., Cheon D., Cho I. // Lecture Notes in Computer Science. 2001. P. 273–283. doi: https://doi.org/10.1007/3-540-44706-7_19
2. Keliher L., Meijer H., Tavares S. Improving the Upper Bound on the Maximum Average Linear Hull Probability for Rijndael // Lecture Notes in Computer Science. 2001. P. 112–128. doi: https://doi.org/10.1007/3-540-45537-x_9
3. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis / Sano F., Ohkuma K., Shimizu H., Kawamura S. // IEICE Trans. Fundamentals. 2003. P. 37–46.
4. Daemen J., Rijmen V. Two-Round AES Differentials. URL: https://eprint.iacr.org/2006/039.pdf
5. Computational aspects of the expected differential probability of 4-round AES and AES-like ciphers / Daemen J., Lamberger M., Pramstaller N., Rijmen V., Vercauteren F. // Computing. 2009. Vol. 85, Issue 1-2. P. 85–104. doi: https://doi.org/10.1007/s00607-009-0034-y
6. Results of Ukrainian national public cryptographic competition / Oliynykov R., Gorbenko I., Dolgov V., Ruzhentsev V. // Tatra Mountains Mathematical Publications. 2010. Vol. 47, Issue 1. P. 99–113. doi: https://doi.org/10.2478/v10127-010-0033-6
7. Granger R., Kleinjung T., Zumbrägel J. On the discrete logarithm problem in finite fields of fixed characteristic. URL: https://eprint.iacr.org/2015/685.pdf
8. Keliher L., Sui J. Exact maximum expected differential and linear probability for two-round Advanced Encryption Standard // IET Information Security. 2007. Vol. 1, Issue 2. P. 53. doi: https://doi.org/10.1049/iet-ifs:20060161
9. Ruzhentsev V. I. Two-rounds AES differentials probability estimation // Applied Radio Electronics. 2011. Vol. 10, Issue 2. P. 116–121.

10. Lysytska I. V. Comparing on effectiveness of superboxes for some modern cipher // Radioelectronics, computer science, management. 2012. Issue 1. P. 37–44.
11. Dolgov V. I., Kuznetsov A. A., Isaev S. A. Differential properties of block symmetric ciphers submitted to the Ukrainian competition // Electronic simulation. 2011. Vol. 33, Issue 6. P. 81–99.
12. Ruzhentsev V. I. The probabilities of two-rounds differentials for Rijndael-like ciphers with random substitutions // Applied Radio Electronics. 2014. Vol. 13, Issue 3. P. 235–238.
13. Practical and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks / Kang J.-S. K., Hong S. H., Lee S. L., Yi O. Y., Park C. P., Lim J. L. // ETRI Journal. 2001. Vol. 23, Issue 4. P. 158–167. doi: https://doi.org/10.4218/etrij.01.0101.0402

Запропоновано модель детектора об'єктів і критерій ефективності навчання моделі. Модель містить 7 перших модулів згорткової мережі Squeezenet, два згорткові різномасштабні шари, та інформаційно-екстремальний класифікатор. Як критерій ефективності навчання моделі детектора розглядається мультиплікативна згортка частинних критеріїв, що враховує ефективність виявлення об'єктів на зображенні та точність класифікаційного аналізу. При цьому додаткове використання алгоритму ортогонального узгодженого кодування при обчисленні високорівневих ознак дозволяє збільшити точність моделі на 4 %.

Розроблено алгоритм навчання детектора об'єктів за умов малого обсягу розмічених навчальних зразків та обмежених обчислювальних ресурсів, доступних на борту малогабаритного безпілотного апарату. Суть алгоритму полягає в адаптації верхніх шарів моделі до доменної області використання на основі алгоритмів зростаючого розріджено кодуючого нейронного газу та симуляції відпалу. Навчання верхніх шарів без вчителя дозволяє ефективно використати нерозмічені дані з доменної області та визначити необхідну кількість нейронів. Показано, що за відсутності тонкої настройки згорткових шарів забезпечується 69 % виявлених об'єктів на зображеннях тестової вибірки Inria Aerial Image. При цьому після тонкої настройки на основі алгоритму симуляції відпалу забезпечується 95 % виявлених об'єктів на тестових зображеннях.

Показано, що використання попереднього навчання без вчителя дозволяє підвищити узагальнюючу здатність вирішальних правил та прискорити ітераційний процес знаходження глобального максимуму при навчанні з учителем на вибірці обмеженого обсягу. При цьому усунення ефекту перенавчання здійснюється шляхом оптимального вибору значення гіперпараметру, що характеризує ступінь покриття вхідних даних нейронами мережі

Ключові слова: зростаючий нейронний газ, детектор об'єктів, інформаційний критерій, алгоритм симуляція відпалу

UDC 004.891.032.26:629.7.01.066
DOI: 10.15587/1729-4061.2018.139923

IMPROVING THE EFFECTIVENESS OF TRAINING THE ON-BOARD OBJECT DETECTION SYSTEM FOR A COMPACT UNMANNED AERIAL VEHICLE

V. Moskalenko
PhD, Associate Professor*
E-mail: systemscoders@gmail.com
A. Dovbysh
Doctor of Technical Sciences, Professor,
Head of Department*
E-mail: a.dovbysh@cs.sumdu.edu.ua
I. Naumenko
PhD, Senior Researcher, Colonel
Research Center for Missile Troops and Artillery
Gerasima Kondratyeva str., 165, Sumy, Ukraine, 40021
E-mail: 790895@ukr.net
A. Moskalenko
PhD, Assistant*
E-mail: a.moskalenko@cs.sumdu.edu.ua
A. Korobov
Postgraduate student*
E-mail: artemkorr@gmail.com
*Department of Computer Science
Sumy State University
Rimskoho-Korsakova str., 2, Sumy, Ukraine, 40007

1. Introduction

Unmanned aviation is widely used in the tasks of inspection of technological and residential facilities, protection and reconnaissance activities, as well as in the sphere of transportation of small size loads. One of the ways to increase the functional efficiency of the unmanned aerial vehicle (UAV) is to introduce technologies of artificial in-