ISSN 2519-2310

COMPUTER SCIENCE AND CYBERSECURITY

ISSUE 4(12) 2018

V. N. Karazin Kharkiv National University Publishing

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени В.Н. КАРАЗИНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
КОМПЬЮТЕРНЫЕ НАУКИ И КИБЕРБЕЗОПАСНОСТЬ
COMPUTER SCIENCE AND CYBERSECURITY
(CS&CS)

Issue 4(12) 2018

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
Международный электронный научно-теоретический журнал
International electronic scientific journal

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information communication systems and on information security problems based on advanced mathematical methods, information technologies and technical means.

Journal is published quarterly.
Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (February 25, 2019, protocol No. 3)

Editorial office:
Karazin Kharkiv National University
Svobody Sq., 6, office 315a, Kharkiv, 61022, Ukraine (*North building of University, 3th floor*)
Phone: +38 (057) 705-10-83
E-mail: *cscsjournal@karazin.ua*
Web-page: *http://periodicals.karazin.ua/cscs (Open Journal System)*

Published articles have been internally and externally peer reviewed

TABLE OF CONTENTS

Issue 4(12) 2018

UDC 004.056.55

METHOD OF 3D-STEGANOGRAPHY

Alexandr Kuznetsov[1], Oleh Stefanovych[1], Kateryna Kuznetsova[1], Mykola Pastukhov[2], Dmytro Prokopovych-Tkachenko[2]

[1] V. N. Karazin Kharkiv National University, Svobody Sq., 6, Kharkiv, 61022, Ukraine
kuznetsov@karazin.ua, stif1304@gmail.com, kate.kuznetsova.2000@gmail.com

[2] University of Customs and Finance, Volodymyr Vernadsky St., 2/4, Dnipro, 49000, Ukraine
denart66@gmail.com, omega2@email.dp.ua

Reviewer: Sergii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Kharkiv University of Technology "STEP", Malom'yasnitska St. 9/11, Kharkiv, 61010, Ukraine
kavserg@gmail.com

Received on September 2018

Abstract: *In this work, a new direction of technical steganography related to the concealment of information in the process of layer-by-layer creation (cultivation) of a solid-state object using various 3D-printing technologies was investigated. Information data is converted into a digital 3D-model of elementary physical objects that are placed inside this 3D-model of the container product. After printing, a solid object physically contains the hidden information that cannot be deleted or distorted without damaging the container product. In addition, the applied methods do not reduce the operational, aesthetic and any other properties of the finished product. The proposed complex is invariant to the method of layer-by-layer growing, that is, it can be equipped with any peripheral devices of 3D-printing of various manufacturers with any materials and principles of layer-by-layer creation.*

Keywords: *steganography; 3D-printing; hiding information data; 3D-model; laser scanners.*

1 Introduction

The steganography, in a broad sense, is such method of transmission of the coded information message in a case of when the fact of its existence is suppressed [1,2]. Unlike cryptography, steganography methods allow to replace unessential shares of data with confidential information so that it was impossible to suspect existence of the built-in secret message [1]. Today in connection with development of an ADP-equipment and new channels of communication there are new steganography methods, which are a cornerstone of information hiding in computer files. Computer files are containers, which possess the high level of redundancy (photo and video of the image, audio-files, text documents, etc.). Concealment is based on replacement of redundant data with information messages. Only the authorized officer who has the steganography key [1,2] can detect the fact of their existence.

In recent years there is a new direction of computer steganography based on concealment of information messages in artificially created containers in which redundancy is caused by technical features of storage, processing and/or data transfer [3-14]. Such methods of "technical" steganography are characterized on concealment of information messages in artificial containers, different by the nature. In particular, methods of network steganography as the carrier (container) use the packet transferred via network or set of data packets. Procedures of concealment and exception of information based on the use of features of functioning of network stack of data transfer protocols [3-6]. Creation of the covert cluster channels based on using of features of data storage in the modern file systems [7-9]. There are also other directions of development of technical steganography, in particular, based on using of artificial redundancy of three-dimensional (3D)-models of objects [10-14]. In recent years, three-dimensional models gained wide distribution in different branches, in particular, processing medical data, museum pieces and samples of cultural heritage, simulation models of industrial samples and productions, computer games and so forth. At the same time, steganography methods apply to protection of copyright of 3D-models, concealment of a certain information, protection against fortuitous distortions or certain errors, and so forth. So, researches of new methods of concealment of data with use 3D-technologies are perspective direction of the modern science.

This work describes new approach proposed in [15], about steganography concealment of data in solid objects using 3D-printing technology. This method transforms information messages into 3D-model, which is placed inside 3D-model of the container with subsequent printing (creation, cultivation). The appearance of the resulting solid object, its operational and aesthetic properties do not change during the process of embedding the information message. In addition, you cannot delete or distort this hidden message without destroying or significantly damaging the product. Consequently, we have new technology for steganography protection of information for covert transmission, to ensure copyright and the like.

2 Hiding Information Data

The prototype of complex of steganography protection was described in [15], in which information data hides by the process of layer-by-layer creation (cultivation) of the solid-state object using various 3D-printing technologies. The main idea is the embedding (steganography coding) of information data into digital 3D-model, whereby a solid object (a finished product or prototype for further using) creates (prints layer-by-layer). The embedding process is implemented using secret key data, excludes unauthorized access to protected information, violation of its integrity, authenticity and confidentiality. In addition, the applied steganography protection methods should not reduce the operational, aesthetic or any other properties of the finished product. So, the proposed complex (method) is invariant to the method of layer-by-layer growing, it can be equipped with any peripheral devices of 3D-printing of various manufacturers with any materials and principles of layer-by-layer creation [15]. The main idea of data concealment is placing an information message in the middle of an arbitrary computer model of physical object that can be printed on a 3D-printer: toy, figure, souvenirs, etc. The information message is converted to a binary form and each bit becomes a specific piece of the physical model. As an example (Fig. 1), each bit can be encoded by a three-dimensional cube of the specified size. The filling of the cube corresponds to the content: "0" corresponds to the empty (*not filled*) cube, "1" - filled. An informative sign can also be another, for example, filling with different materials, or with one material, but with different density, orientation, filling, the form of elementary "bit" physical models, and the like.

For automated coding was used specialized software OpenSCAD, which is intended for creating solid-state 3D CAD-objects. It is free and available for Linux/UNIX®, Microsoft Windows® and Apple® Mac OS X.

Fig. 2 demonstrates the coding of the information message "Tomorrow never comes until it's too late". Each message character is converted to binary form using the ASCII-code. Next, for the selected cubic form of "bit" models and 3×3×3 mm in size, each information bit is coded. For this purpose, software was developed that forms the appropriate source code, which is placed in the working field of the OpenSCAD program. Now in Fig. 2 all elementary physical models are grouped into a container with the size 11×3×10 mm of the corresponding cubes (*these settings are additionally set in software*).

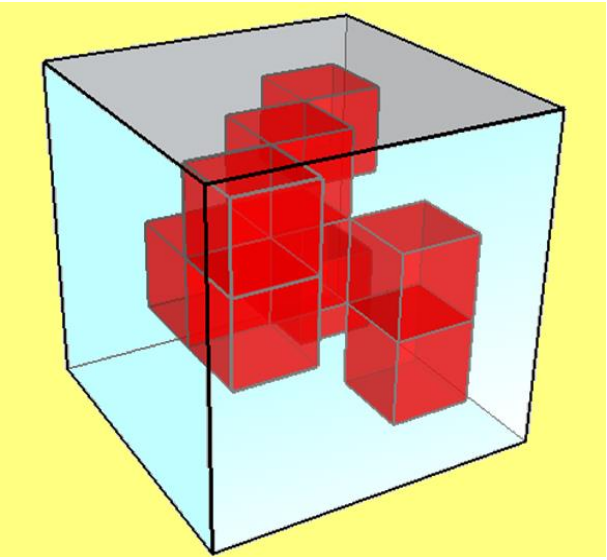


Fig.1 – Steganocoding of information message into a fragment of a computer model of physical object (*schematic representation*)

In Fig. 2 on the left, you can see the source code, which specifies the coordinates and size of three-dimensional cubes - carriers of information bits. On the right are the created three-dimensional model of the information message corresponding to all the given input parameters.

Thus, as a result of steganography coding, the information message first becomes a three-dimensional binary matrix, which turns into a computer model of physical object. The computer model of the binary matrix is placed in the middle of the basic model of the container, so that its edges do not extend beyond the outer body, as shown schematically in Fig. 3. At the same time, specialized software "MakerBot Desktop" was used for 3D-printing. The matrix in the middle of another model can be placed in different ways, for example: all filled cubes when printing on 3D-printer should be filled with different color materials; all the filled cubes should be left blank, when printing on 3D-printer. The disadvantage of the second method is the reduction of the final body weight, in a detailed analysis can give out the fact of the presence of secret message. Filling in bits with a different color (*or, for example, with another material*) reduces the probability of finding hidden message but increases the difficulty of its reading.

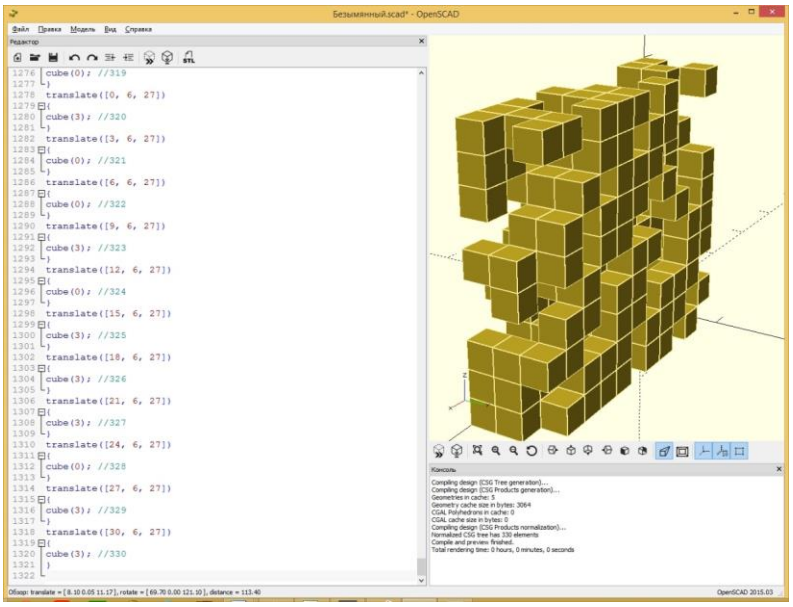


Fig. 2 – Example of steganography coding using the program OpenSCAD

Fig. 4 shows the process of layer-by-layer creation of the solid container object with built-in information message. On the left in this figure, schematic visualization of the printing process is shown, on the right - photograph of the real process on the 68th layer of 3D-printing, which was performed using the 3D-printer "Flashforge Creator Dual".

Fig. 5 shows the completion of the 3D-model printing and the finished product.

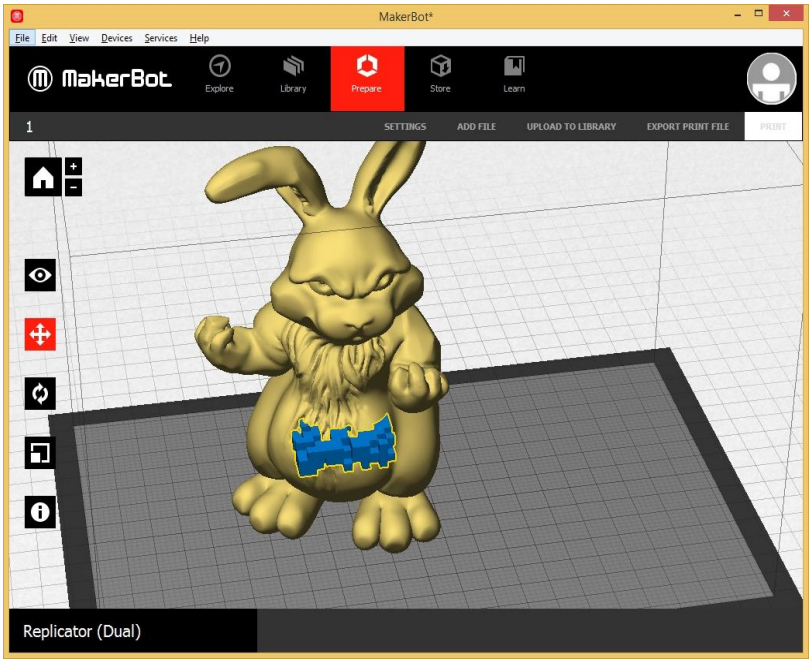


Fig. 3 – Placing three-dimensional model of the information message in the middle of the outer container model

3 Extracting of information data

The process of extracting the embedded data is performed by scanning the resulting solid object. The data received by the scanner is steganography decoded using secret key data. At this stage, various security services are provided, for example, integrity, authenticity, involvement, confidentiality and the like. To increase the reliability (*noise immunity*), the embedded data is additionally coded. As a result, it is possible to identify and/or correct the errors that occurred during layer-by-layer printing/scanning with given probability.

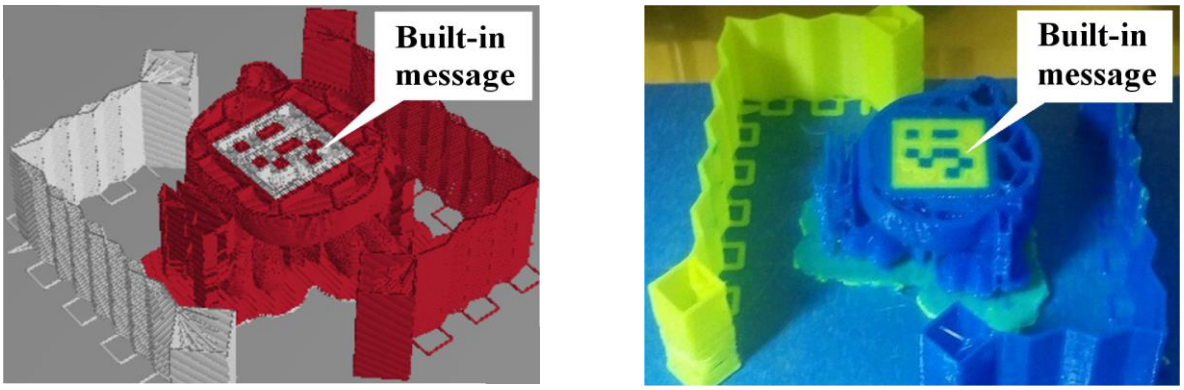
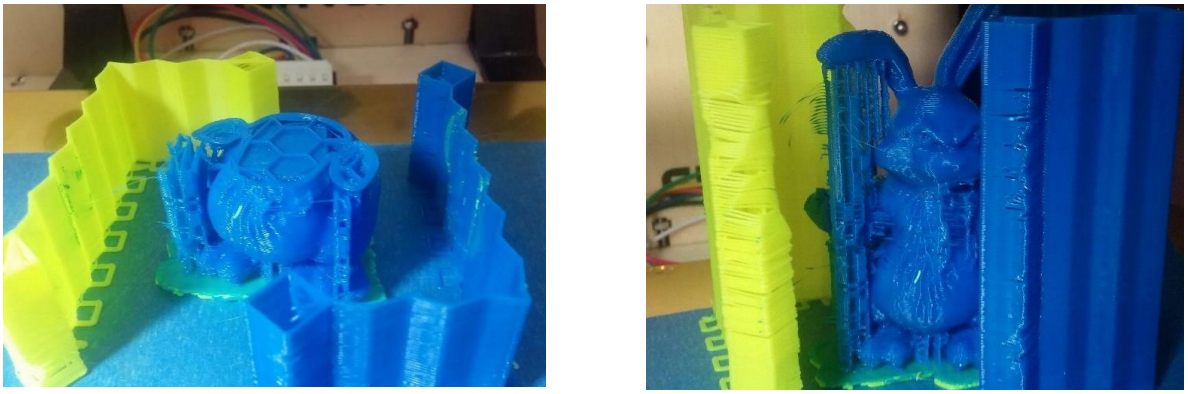


Fig. 4 – Layered creation of the solid container object with built-in information message



a) *b)*

Fig. 5 – Printing completion (*a*) and finished product (*b*) with built-in message

The proposed complex (method) can be used in various areas. For example, for the hidden transmission of information messages with the provision of various security services (*integrity, authenticity, involvement, confidentiality, etc.*). Removing, distorting or modifying embedded data is impossible without physical destruction of the finished product, the proposed complex (method) is ideally suited for ensuring the reliability of layered products, protecting them from unauthorized copying and unfair imitations, securing copyright, etc. [1,2].

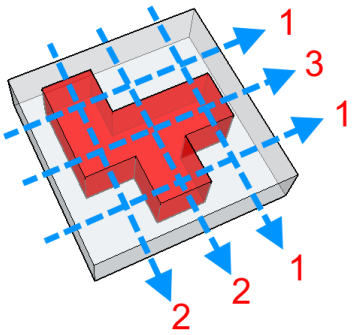
It should be noted that to date, reliable means of extracting information data have not been developed yet [15]. The main unresolved issue of the practical application of the proposed 3D-steganography complex is the uncertainty of a particular procedure of extracting embedded data by scanning the resulting solid body. In particular, the system can be completed with various peripheral devices of 3D-printing, which use different layer-by-layer technologies and different by physical properties materials. Corresponding procedures of scanning the resulting solid body must take these features into account and, if possible, ensure reliable and error-free retrieval of hidden data.

One of the possible directions in solving these problems is the use of laser scanners, in which a stream of coherent, monochromatic, polarized, and narrowly directed radiation flux is used. It decreases as a result of absorption in the medium in some pre-stipulated number of times. The following experimental studies were conducted to establish the possibility of reading of the hidden message from 3D-model that was layered (printed) on 3D-printer without damaging the model or message itself.

4 Description of the laboratory installation and experimental research

The main idea of the experiment is a narrowly focused laser irradiation of the finished product (with the built-in notification) at different angles and directions, sufficient to unambiguously determine the internal structure of the product. In this case, the initial dataset is the value of the radiation intensity, which decrease upon absorption.

The irradiation scheme of the finished product can be presented in simplified form in Fig. 6 on the left (*when encoding information bits with empty and filled cubes*). The indicated conditional value of the measurement result shown at the end of the arrows. This is a decrease in the radiation intensity (proportional to the thickness of the solid object). On the right in this figure, the values of the information bits are shown, which are expected to be extracted from the solid object.



1	0	0
1	1	1
0	1	0

a) *b)*

Fig. 6 – Simplified scheme of irradiation of the finished product (*a*) and the expected result of data extraction (*b*)

It is impossible to obtain any other information about the internal structure of the solid object. The placed filled fragments (and corresponding bits) must be uniquely extracted only from the measurement results. Represented in the figure on the left, the measurement results have two possible solutions, one of which does not correspond to the one shown on the right. This placement is a nomogram that can be used to form Japanese crossword puzzles. To simplify the experiment, a simple physical model was made in the form of stairs from ABS-plastic of yellow and blue colors. This shape allows to quickly change the thickness of the object filled with the material (Fig. 7).

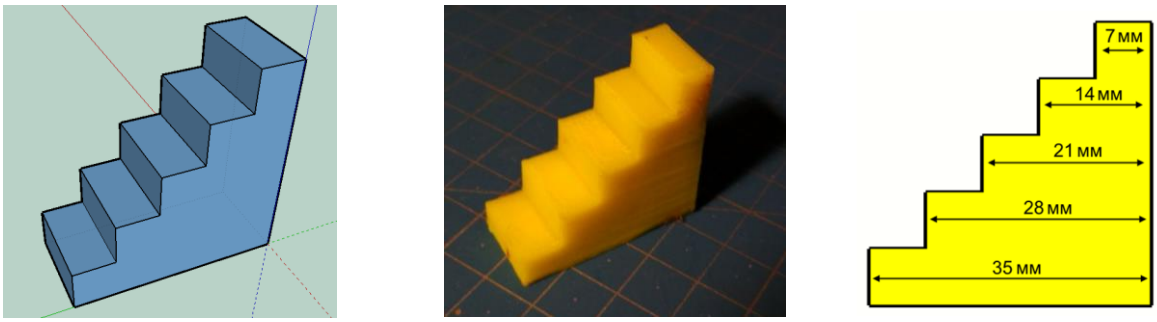


Fig. 7 – Simplified physical model of information data

In fact, there are six different values that conditionally correspond to the following information bit sequences:

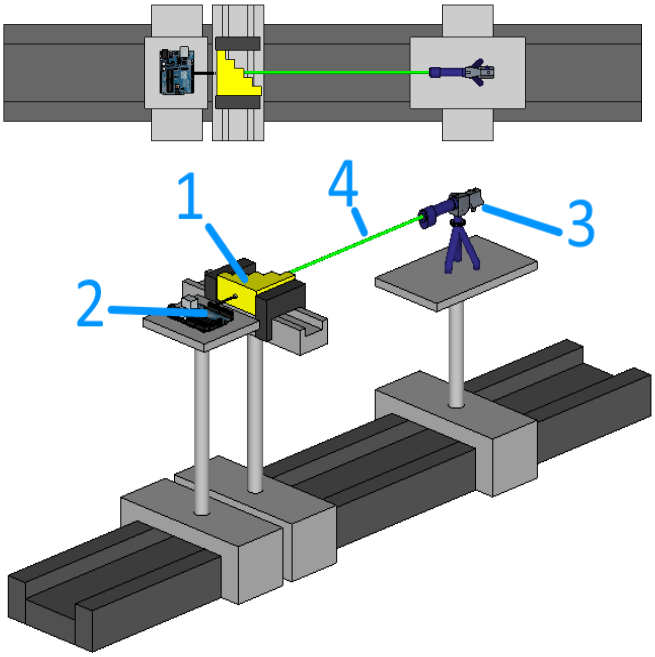
- without filling - bit sequence (00000);
- single fill (first step) - bit sequence (10000);
- two fillings (second step) - bit sequence (11000);
- three fillings (third step) - bit sequence (11100);
- four fillings (fourth step) - bit sequence (11110);
- five fillings (fifth step) - bit sequence (11111).

To conduct research, optical instruments were used from the laboratory of the Physical Optics Department of the Physics Faculty. It is known that each material has its own absorption index - the reciprocal of the distance, at which the monochromatic radiation flux forms a parallel ray, decreases as

a result of absorption in the medium to some predetermined number of times. The absorption coefficient is determined by the properties of the substance and in the general case depends on the wavelength λ of light. This dependence is the absorption spectrum of the substance. Lasers of the visible spectrum, which were in the laboratory, were used as monochromatic radiation. They are different in wavelength and radiation power. A ray of laser light passed through the body under investigation. Radiation, which was not absorbed by the plastic, fell on the photoresistor fixed on the other side. A photoresistor is a light-controlled variable resistor. The resistance of a photoresistor decreases with increasing incident light intensity. To read and process the data, the microcontroller "Arduino UNO" was used. The photoresistor was supplied with voltage 5 V. Depending on the degree of excitation of the photocell, its resistance was varied. The microcontroller measured voltage changes every 40 ms, digitized and sent them to personal computer.

Schematically, the laboratory device is shown in Fig. 8. It includes a test body made of plastic in the form of stairs (Fig. 7), laser as a source of directional irradiation of the finished product, photoresistor and microcontroller for reading scattered radiation. Photo of the collected laboratory installation and an enlarged photo of the process of optical irradiation shown in Fig. 8.

The software was developed to receive and display the current value of the photoresistor, calculate the arithmetic mean of the measurements made. Since the absorption spectrum of the substance was unknown for a solid body, all the lasers with different characteristics in the laboratory were used in the experiment (see Table 1).



1 - the solid object made of plastic in the form of stairs;
2 - photoresistor and microcontroller reading the data;
3 - laser;
4 - laser ray

Fig. 8 – The scheme of the laboratory installation

Each laser was exposed to different thicknesses of the body being examined and measurements were made of the percentage of light that passed through this section of the body. The step of variation of 7 mm was chosen considering the thickness of the laser ray, the thickness of which is within 5-6 mm. For the correctness of the experiment, the ray of laser radiation should completely fall on a section with one thickness. The microcontroller has a voltmeter, detects a voltage change in 5/1024 volts, so when digitizing an analog value, we get a number from 0 (*no light at all*) to 1024 (the max amount of light that a photoresistor can recognize).

Table 1 – Characteristics of lasers used in the experiment

Number	Wavelength, nm	Power, mW	Visible color
1	532	100	Green
2	650	25	Red
3	405	90	Violet
4	445	160	Blue
5	650	25	Red

5 The results of the experiment and their interpretation

The results of the experimental studies (*averaged over the measurements*) are presented in Table 2.

The sample from the yellow plastic absorbs less green laser radiation with a wavelength of $\lambda = 532$ nm. This is the output from the data in the table. Although both samples are made from the same kind of plastic, because of the color difference, they have completely different absorption values. The body, made of blue plastic, has a much larger absorption index. Even at the minimum thickness, the body absorbed light from each laser, which would suffice to determine the thickness.

Table 2 – Results of measurements

A sample of yellow color						
Laser number	Thickness, mm					
	0	**7**	**14**	**21**	**28**	**35**
1	1024	1001	775	162	33	4
2	1024	995	426	65	6	0
3	1024	995	97	5	1	0
4	1024	998	500	59	5	0
5	1024	995	336	57	4	0
Sample of blue color						
Laser number	Thickness, mm					
	0	**7**	**14**	**21**	**28**	**35**
1	1024	0	0	0	0	0
2	1024	0	0	0	0	0
3	1024	0	0	0	0	0
4	1024	0	0	0	0	0
5	1024	0	0	0	0	0

The obtained results for a sample of yellow material indicate that for different thicknesses we have different values of the radiation intensity and these differences are very significant. So, based on the measurement results, it is possible to recognize the thickness of the material, and, accordingly, determine the content of the hidden information bits.

6 Conclusions

In this work, a new direction of technical steganography related to the concealment of information in the process of layer-by-layer creation (cultivation) of solid-state object using various 3D-printing technologies was investigated. Information data are converted into digital 3D-model of elementary physical objects that are placed inside the 3D-model of the container product. After printing, the solid object physically contains hidden information that cannot be deleted or distorted without damaging the container. In addition, the applied methods do not reduce the operational, aesthetic and any other properties of the finished product.

The proposed complex (method) is invariant to the method of layer-by-layer growing, it can be equipped with any peripheral devices of 3D-printing of various manufacturers with any materials and principles of layer-by-layer creation. The process of extracting the embedded data is performed by scanning the resulting solid object. The uncertainty of the procedure for scanning the resulting solid body is the main unresolved issue regarding the practical application of the proposed 3D-steganography complex.

In this work, according to the results of experimental studies, it was established that it is possible in principle to read hidden message from 3D-model using laser scanners, in which the flux of coherent, monochromatic, polarized and narrowly directed radiation flux forms a parallel ray, decreases as a result of absorption in a medium into some a predetermined number of times. The obtained results for

a sample of yellow material indicate that for different thicknesses, we have different values of the radiation intensity and these differences are very significant. So, based on the measurement results, it is possible to recognize the thickness of the material, and, accordingly, determine the content of the hidden information bits. The results of the experimental studies given above are not final and need further clarification. In particular, the unresolved issue is the choice of the type and characteristics of the laser, the consistency of these characteristics with the properties of solid-state object materials, the adjustment of photoresistors, and the like. In addition, in our opinion, perspective is the conduct of experimental studies using other types of radiation, materials and colors of plastic.

References

[1] Katzenbeisser S., Petitcolas F. A. Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, MA, USA: Artech House, 2000. 220 p.
[2] Petitcolas F. A. P., Anderson R. J., Kuhn M. G. Information hiding-a survey. Proceedings of the IEEE.1999. Vol. 87, №7. P. 1062–1078.
[3] Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography and its detection. Soft Computing. 2011. Vol.15, №3. P. 505–515.
[4] Length based network steganography using UDP protocol/ Nair A. S., Kumar A., Sur A., Nandi S. 2011 IEEE 3rd International Conference on Communication Software and Networks. Xi'an, 2011. P. 726–730.
[5] Ahsan K., Kundur D. Practical data hiding in TCP/IP. ACM Workshop on Multimedia and Security, 2002. URL: https://www.gray-world.net/es/papers/acm02.pdf
[6] TCP/IP Timing Channels: Theory to Implementation / Sellke S. H., Wang C., Bagchi S., Shroff N. B. 2009. P. 2204–2212.
[7] Designing a cluster-based covert channel to evade disk investigation and forensics/ Khan H., Javed M., Khayam S.A., Mirza F. Computers & Security. 2011. Vol. 30, Issue 1. URL: https://www.sciencedirect.com/science/article/pii/ S016740481000088X
[8] Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel/ Khan H., Javed M., Khayam S.A., Mirza F. National University of Science & Technology (NUST), Islamabad 44000, Pakistan. URL: https://www.sigsac.org/ccs/CCS2009/pd/abstract_17.pdf
[9] Covert Channel for Cluster-based File Systems Using Multiple Cover Files / Morkevičius N., Petraitis G., A. Venčkauskas, J. Čeponis. Information Technology and Control. 2013. Vol. 42, №3. P. 32. URL:http://itc.ktu.lt/index.php/ITC/article/view/3328
[10] Rani R., Deep G. Digital 3D barcode image as a container for data hiding using steganography. 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). Solan, 2017. P. 325–330.
[11] Sun Z., Lu Z. M., Li Z. Reversible Data Hiding for 3D Meshes in the PVQ-Compressed Domain. 2006 International Conference on Intelligent Information Hiding and Multimedia. Pasadena, CA, USA, 2006. P. 593–596.
[12] A Benchmark for 3D Mesh Watermarking / Wang K., Lavoué G., Denis F., Baskurt A., He X. 2010 Shape Modeling International Conference. Aix-en-Provence, 2010. P. 231–235.
[13] 3D Multimedia Protection Using Artificial Neural Network /Motwani M. C., Bryant B. D., Dascalu S. M. , Harris Jr. F. C. 2010 7th IEEE Consumer Communications and Networking Conference. Las Vegas, NV, 2010. P. 1–5.
[14] Vasić B. Annotation of cultural heritage 3-D models by robust data embedding in the object mesh. 2014 22nd Telecommunications Forum Telfor (TELFOR). Belgrade, 2014. P. 842–849.
[15] Kuznetsov A.A., Kovalenko O.Yu. Steganographic protection of information using 3D printing. Information Security of the State, Society and Personality: A Collection of Abstracts of the All-Ukrainian Scientific and Practical Conference, April 16, 2015. Kirovograd: KNTU, 2015.P. 91–92. (in Ukrainian)

Рецензент: Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський технологічний університет "Шаг", вул. Малом'ясницька, 9/11, Харків, 61010, Україна. E-mail: kavserg@gmail.com

Надійшло: Вересень 2018.

Автори:

Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 6, Харків, 61022, Україна.
E-mail: kuznetsov@karazin.ua

Олег Стефанович, студент факультету комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна.
E-mail: stif1304@gmail.com

Катерина Кузнецова, студентка факультету комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна.
E-mail: kate.kuznetsova.2000@gmail.com

Миколай Пастухов, к.т.н., доцент, Університет митної справи та фінансів, вул. Володимира Вернадського 2/4, Дніпро, 49000, Україна.
E-mail: denart66@gmail.com

Дмитро Прокопович-Ткаченко, к.т.н., завідувач кафедрою кібербезпеки, Університет митної справи та фінансів, вул. Володимира Вернадського 2/4, Дніпро, 49000, Україна.
E-mail: omega2@email.dp.ua

Метод 3D-стеганографії.

Анотація. В цій роботі досліджено новий напрямок технічної стеганографії, який пов'язаний із приховуванням інформаційних даних в процесі пошарового створення (вирощування) твердотільного об'єкта при використанні різних технологій 3D-друку. Інформаційні дані перетворюються в цифрову 3D-модель елементарних фізичних об’єктів, які розміщуються всередині 3D-моделі виробу-контейнеру. Після роздрукування твердий об'єкт фізично містить приховану інформацію, яку неможливо видалити або спотворити без пошкодження контейнеру. Крім того, застосовані методи не знижують експлуатаційних, естетичних та будь яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються, а приховування є інваріантним способу пошарового вирощування, тобто можуть застосовуватися різні пристрої 3D-друку з будь-якими матеріалами і принципами пошарового створення.

Ключові слова: стеганографія; 3D-друк; приховування інформаційних даних; 3D-модель; лазерні сканери.

Рецензент: Сергей Кавун, доктор экономических наук, к.т.н., проф., Харьковский технологический университет "Шаг", ул. Маломясницкая, 9/11, Харьков, 61010, Украина. E-mail: kavserg@gmail.com

Поступила: Сентябрь 2018.

Авторы:

Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина.
E-mail: kuznetsov@karazin.ua

Олег Стефанович, студент факультету комп’ютерних наук, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина.
E-mail: stif1304@gmail.com

Екатерина Кузнецова, студентка факультета компьютерных наук, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина.
E-mail: kate.kuznetsova.2000@gmail.com

Николай Пастухов, к.т.н., доцент, Университет таможенного дела и финансов, ул. Владимира Вернадского, 2/4, Днепр, 49000, Украина.
E-mail: denart66@gmail.com

Дмитрий Прокопович-Ткаченко, к.т.н., заведующий кафедрой кибербезопасности, Университет таможенного дела и финансов, ул. Владимира Вернадского, 2/4, Днепр, 49000, Украина.
E-mail: omega2@email.dp.ua

Метод 3D-стеганографии.

Аннотация. В этой работе исследовано новое направление технической стеганографии, связанное с сокрытием информационных данных в процессе послойного создания (выращивания) твердотельного объекта при использовании различных технологий 3D-печати. Информационные данные преобразуются в цифровую 3D-модель элементарных физических объектов, которые размещаются внутри 3D-модели изделия-контейнера. После распечатки твердый объект физически содержит скрытую информацию, которую невозможно удалить или исказить без повреждения контейнера. Кроме того, применяемые методы не снижают эксплуатационных, эстетических и любых других свойств готового изделия, поскольку технологии, используемые для нанесения слоев, не модифицируются, а сокрытие является инвариантным к способу послойного выращивания, т.е. могут применяться различные устройства 3D-печати с любыми материалами и принципами послойного создания.

Ключевые слова: стеганография; 3D-печать; сокрытие информационных данных; 3D-модель; лазерные сканеры.

УДК 004.056.5

ПРО СЛАБКІСТЬ S ПЕРЕТВОРЕННЯ ШИФРУ СТРУМОК З ЛАНЦЮЖКА КЕРОВАНИХ S-БЛОКІВ

Костянтин Лисицький[1], Катерина Кузнецова[1]

[1] V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
lisickiy@ukr.net, kate.kuznetsova.2000@gmail.com

Reviewer: Roman Oliynikov, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
roliynykov@gmail.com

Received on October 2018

Анотація: *Обговорюються особливості побудування S-перетворення шифру Струмок. Зокрема, виконано аналіз пропозиції щодо побудови S-перетворення шифру Струмок з використанням керованих S-блоків. Оцінюються показники його випадковості. Показується, що воно за своєю ефективністю поступається відповідному оригінальному рішенню. З'ясовуються причини таких обставин.*

Ключові слова: *поточний шифр; випадкова підстановка; диференціальна ймовірність; S перетворення; лінійна змішуючи схема.*

1 Вступ

Раніше, в роботі [1], були викладені пропозиції щодо побудови, як попередньо очікувалося, поліпшеної конструкції S перетворення для поточного шифру Струмок. Тоді ми вважали, що застосування для побудови циклової функції ланцюжка з керованих S-блоків має привести до поліпшення динамічних показників приходу багаторазового повторення запропонованої конструкції S перетворення до випадкової підстановці. В даному контексті, під динамічними показниками приходу ітеративного продовження S перетворення до випадкової підстановці, слід розуміти мінімальне число повторень S перетворення в режимі шифрування, вхідного 64-х бітного блоку даних, після якого максимуми диференціальних ймовірностей переходів вхідних різниць у вихідні приходять до асимптотичних значенням, характерних для випадкових підстановок. Відповідні міркування в роботі [1] будувалися на аналізі мінімальної кількості S-блоків, що активізуються на перших циклах шифрування.

У даній роботі ми продовжили дослідження раніше запропонованої конструкції [1] та представляємо додаткові результати експериментів щодо оцінки реального числа S-блоків, які активізуються на кожному циклі при ітеративному продовженні перетворення. В роботі буде показано, що запропонована в [1] конструкція має слабкості, які роблять показники пропонованої конструкції такими, що поступаються оригінальній розробці, в наслідок чого перспективність пропонованої конструкції є явно сумнівною.

2 Альтернативна конструкція S перетворення

Сама конструкція, що була запропонована раніше, в роботі [1], представлена на рис. 1. Дана схема, в своєї основі, повторює конструкцію першого циклу шифру ШУП [2], тільки замість SL перетворень в даному випадку виступають байтові S-блоки (*керовані підстановки*), а замість підсумування за модулем 2 сегментів на вході першого SL перетворення тут використовується інша (*як раніше вважалося, більш ефективна*) схема лінійного змішування, що заснована на багатошаровому підсумуванні за модулем 2 сегментів вхідного блоку даних. Крім того, в даному випадку, підсумування виходу останнього S-блоку виконується тільки з виходом першого S-блоку.

Спочатку здійснюється розбивка вхідного блоку даних з 64 бітів на лівий і правий 32-х бітні підблоки, та формується новий 64-х бітний блок даних, що складається з нового лівого

32-х бітного підблоку, який одержується з допомогою підсумування за модулем 2 лівого і правого 32-х бітних підблоків вихідного блоку даних, і правого підблоку, шо повторює «старий» правий 32-х бітний підблок. Потім здійснюються аналогічні операції з новим лівим напівблоком і далі з новим лівим підблоком чергового напівблоку, де вже він зводиться до байтового розміру.

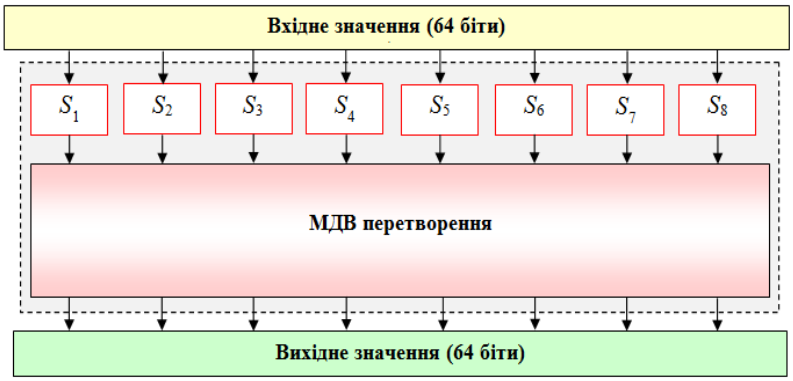


Рис. 1 – S перетворення шифру Струмок

Розміщення рядків з сум байтів після додавання за модулем 2 ілюструється нижче.

Вхідний рядок байтів: X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8

Після першого шару XOR маємо: $X_1 \oplus X_5$, $X_2 \oplus X_6$, $X_3 \oplus X_7$, $X_4 \oplus X_8$, X_5, X_6, X_7, X_8.

Після другого шару XOR: $X_1 \oplus X_5 \oplus X_3 \oplus X_7$, $X_2 \oplus X_6 \oplus X_4 \oplus X_8$, $X_3 \oplus X_7$, $X_4 \oplus X_8$, X_5, X_6, X_7, X_8.

Після третього шару XOR маємо хідні блоки даних: $X_1 \oplus X_5 \oplus X_3 \oplus X_7 \oplus X_2 \oplus X_6 \oplus X_4 \oplus X_8$, $X_2 \oplus X_6 \oplus X_4 \oplus X_8$, $X_3 \oplus X_7$, $X_4 \oplus X_8$, X_5, X_6, X_7, X_8.

В результаті на вході першого S-блоку маємо $X_1 \oplus X_5 \oplus X_3 \oplus X_7 \oplus X_2 \oplus X_6 \oplus X_4 \oplus X_8$ – суму всіх байтів входу.

Аналіз, якій було наведено в роботі [1], виконаний у припущенні, що при активізації будь-якого S-блоку отримують ненульові різниці входу усі наступні S-блоки та зроблений висновок, що при умові, коли для різниць сегментів пар входів виконується умова: $\Delta X_1 \oplus \Delta X_5 = 0$, $\Delta X_1 = \Delta X_5 \neq 0$, $\Delta X_5 = \Delta X_3 = \Delta X_7 = \Delta X_2 = \Delta X_6 = \Delta X_4 = \Delta X_8 = 0$, в запропонованому рішенні активізується мінімум 4-ри S-блоки першого циклу. – Тобто, в гіршому випадку ланцюжок з S-блокових перетворень запускається з п’ятого S-блоку. Отже, на першому циклі маємо 4-ри активних S-блоки, а на двох перших циклах маємо 12-ть активних S-блоків [1]. На трьох циклах активізується вже мінімум близько 20-ти S-блоків. Але як показали результати наступних експериментів, зроблений в роботі [1] висновок виявився хибним! В даній роботі ми намагаємося розібратися в чому ж тут справа.

3 Результати експериментальних досліджень

Як з’ясувалося, слабкість, про яку йде мова, полягає в тому, що при з'єднанні керованих S-блоків в ланцюжок при однакових байтових різницях на входах сусідніх S-блоків з'являється можливість при проході на S-блоці вхідної різниці в ту ж саму вихідну різницю отримати на вході чергового S-блоку нульову вхідну різницю і розірвати ланцюжок переходів з S-блоків. Такі переходи відповідають діагональним елементам таблиць диференціальних різниць S-блоків, і ймовірність таких переходів виходить досить високою.

Таблиця 1 відображає результати експериментальних досліджень по визначенню реального числа активованих S-блоків для різних варіантів 3-циклового перетворення при активізації входу S-перетворення різними варіантами двобайтових ненульових різниць.

У таблиці 2 наводиться детальне уявлення розподілу S-блоків (практичних значень), що активізуються в межах ланцюжка на кожному циклі, при активації входу "удосконаленого" S-перетворення різними варіантами двобаштових різниць (*де, О – значення, що очікується*).

Якщо для випадку $\Delta X1 = \Delta X2 \neq 0$ на вході першого S-блоку виходить нульова вхідна різниця, то на вході другого S-блоку виявляється ненульова вхідна різниця, яка активізує всі наступні S-блоки (*виходить 7 активізованих S-блоків*), тобто в разі, наприклад, різниць $\Delta X2 = \Delta X3 \neq 0$, як свідчать результати експерименту (див. Табл. 3), замість очікуваних

Таблиця 1 – Кількість активованих S-блоків для різних варіантів 3-циклового перетворення

Ненульові байтові різниці	**КІЛЬКІСТЬ АКТИВОВАНИХ S-БЛОКІВ**											
	Варіант зі схемою змішування								**Без схеми змішування**			
	Схема змішування використовується на КОЖНОМУ циклі				Схема змішування використовується ТІЛЬКИ на 1-му циклі				Схема змішування НЕ ВИКОРИСТОВУЄТЬСЯ			
	1-й цикл	2-й цикл	3-й цикл	$\sum$	1-й цикл	2-й цикл	3-й цикл	$\sum$	1-й цикл	2-й цикл	3-й цикл	$\sum$
$\Delta X_1 = \Delta X_2 \neq 0$	7	6	6	19	7	6	6	19	1	6	6	13
$\Delta X_1 = \Delta X_3 \neq 0$	6	6	6	18	6	6	6	18	2	1	6	9
$\Delta X_1 = \Delta X_4 \neq 0$	2	6	6	14	2	6	6	14	3	6	6	15
$\Delta X_1 = \Delta X_5 \neq 0$	4	6	6	16	4	6	6	16	4	6	6	16
$\Delta X_1 = \Delta X_6 \neq 0$	4	4	6	14	4	6	6	16	5	6	6	17
$\Delta X_1 = \Delta X_7 \neq 0$	4	6	6	16	4	6	6	16	6	6	6	18
$\Delta X_1 = \Delta X_8 \neq 0$	3	4	6	13	3	3	6	12	7	6	6	19
$\Delta X_2 = \Delta X_3 \neq 0$	1	6	6	13	1	5	6	12	1	5	6	12
$\Delta X_2 = \Delta X_4 \neq 0$	6	6	6	18	6	6	6	18	2	1	6	9
$\Delta X_2 = \Delta X_5 \neq 0$	3	6	6	15	3	6	6	15	3	6	6	15
$\Delta X_2 = \Delta X_6 \neq 0$	4	5	5	15	4	6	6	16	4	6	6	16
$\Delta X_2 = \Delta X_7 \neq 0$	4	5	6	15	4	3	6	13	5	6	6	17
$\Delta X_2 = \Delta X_8 \neq 0$	4	6	6	16	4	3	6	13	6	6	6	18
$\Delta X_3 = \Delta X_4 \neq 0$	2	5	6	13	2	6	6	14	1	6	6	13
$\Delta X_3 = \Delta X_5 \neq 0$	2	3	6	11	2	6	6	14	2	6	6	14
$\Delta X_3 = \Delta X_6 \neq 0$	4	4	6	14	4	3	6	13	3	2	6	11
$\Delta X_3 = \Delta X_7 \neq 0$	3	4	4	11	3	7	6	16	4	6	6	16
$\Delta X_3 = \Delta X_8 \neq 0$	4	6	6	16	4	5	6	15	5	4	6	15
$\Delta X_4 = \Delta X_5 \neq 0$	3	6	6	15	3	2	6	11	1	6	6	13
$\Delta X_4 = \Delta X_6 \neq 0$	2	6	6	14	2	1	6	9	2	1	6	9
$\Delta X_4 = \Delta X_7 \neq 0$	5	5	6	16	5	4	6	15	3	2	6	11
$\Delta X_4 = \Delta X_8 \neq 0$	2	4	4	10	2	7	7	14	4	3	6	13
$\Delta X_5 = \Delta X_6 \neq 0$	4	6	6	16	4	6	6	16	1	5	6	12
$\Delta X_5 = \Delta X_7 \neq 0$	4	5	6	15	4	6	6	16	2	5	6	13
$\Delta X_5 = \Delta X_8 \neq 0$	5	6	6	17	5	4	6	15	3	4	6	13
$\Delta X_6 = \Delta X_7 \neq 0$	2	4	6	12	2	6	6	14	1	4	6	11
$\Delta X_6 = \Delta X_8 \neq 0$	4	5	5	14	4	5	5	14	2	1	6	9
$\Delta X_7 = \Delta X_8 \neq 0$	5	6	6	17	5	5	6	16	1	3	6	10
Мін кількість	*1*	*3*	*4*	*10*	*1*	*1*	*5*	*9*	*1*	*1*	*6*	*9*
Середнє число	*3,68*	*5,25*	*5,82*	*14,8*	*3,68*	*5,04*	*5,93*	*14,7*	*3*	*4,46*	*6*	*13,5*

Таблиця 2 - Значення, що не відповідають очікуваним результатам активізації S-блоків

Ненульові байтові різниці	**ПОЗИЦІЇ АКТИВОВАНИХ S-БЛОКІВ**					
	Схема змішування використовується на кожному циклі			Схема змішування використовується на кожному циклі		
	1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл	3-й цикл
$\Delta X_1 = \Delta X_4 \neq 0$ O = 7	2	2	5	2	5	6
	0110 0000	1100 0000	0111 1011	0110 0000	0111 0110	1101 1110
$\Delta X_1 = \Delta X_8 \neq 0$ O = 7	3	4	6	3	2	6
	0110 0001	1110 0001	1011 1101	0110 0001	0100 0001	1011 0111

Продовження таблиці 2

$\Delta X2 = \Delta X3 \neq 0$ O = 7	1	1	6	1	5	6
	0100 0000	1000 0000	1011 1101	0100 0000	0110 1110	1111 0011
$\Delta X_2 = \Delta X_5 \neq 0$ O = 7	3	6	6	3	2	6
	0111 0000	0110 1111	1111 1010	0111 0000	0111 1101	1111 0110
$\Delta X_2 = \Delta X_7 \neq 0$ O = 7	3	5	6	3	4	5
	0100 0011	1111 1000	1111 1100	0100 0011	0111 1000	1111 1000
$\Delta X_3 = \Delta X_4 \neq 0$ O = 7	2	2	6	2	5	6
	0110 0000	1100 0000	1101 1101	0110 0000	0110 1011	1111 0110
$\Delta X_3 = \Delta X_5 \neq 0$ O = 6	2	3	6	2	4	6
	0011 0000	1110 0000	1010 1111	0011 0000	0010 1011	0110 1111
$\Delta X_3 = \Delta X_6 \neq 0$ O = 6	4	6	6	4	3	6
	0111 1000	1100 1111	0111 1110	0111 1000	0111 0000	0111 1011
$\Delta X_3 = \Delta X_8 \neq 0$ O = 6	3	6	6	3	5	6
	0110 0001	0011 1111	1111 1001	0110 0001	0111 0110	1101 1101
$\Delta X_4 = \Delta X_5 \neq 0$ O = 7	3	6	6	3	5	5
	0111 0000	0011 1111	1101 0111	01110000	01101011	11101001
$\Delta X_4 = \Delta X_6 \neq 0$ O = 6	2	6	6	2	1	5
	00011000	11010111	01101111	00011000	00010000	01101111
$\Delta X_4 = \Delta X_7 \neq 0$ O = 7	4	6	6	4	4	6
	0110 0011	1110 1110	0111 1101	0110 0011	0111 1000	0011 1111
$\Delta X_5 = \Delta X_6 \neq 0$ O = 5	4	6	6	4	3	6
	0111 1000	0011 1111	1111 0101	0111 1000	0111 0000	0011 1111
$\Delta X_5 = \Delta X_7 \neq 0$ O = 6	4	5	6	4	3	6
	0011 1100	1111 1000	0011 1111	0011 1100	0011 1000	1010 1111
$\Delta X_6 = \Delta X_7 \neq 0$ O = 7	2	3	6	2	5	6
	0100 0100	0000 0111	1011 1101	0100 0100	0110 1101	1110 1101
$\Delta X_6 = \Delta X_8 \neq 0$ O = 5	3	6	6	3	3	6
	00011001	11101011	10110111	00011001	00010110	11101011
$\Delta X_7 = \Delta X_8 \neq 0$ O = 7	4	5	6	3	5	6
	0110 0011	1110 0011	1010 1111	0110 0010	0101 1101	0111 1110

шести активованих S-блоків виходить лише один активний S-блок. Це робиться за рахунок того, що при проході другого S-блоку при S(X2) = X2 на вході третього S-блоку виходить нульова вхідна різниця X2 = ΔX3 ≠ 0, яка розриває ланцюжок ненульових переходів різниць для наступних S-блоків.

Отже, отримані результати свідчать, про те що "удосконалені" схеми з додатним змішуванням сегментів на вході першого циклу мають показники не кращі ніж схема без змішуючого перетворення. Загальний висновок тут міститься в тому, що додатне лінійне перетворення практично не покращує показників випадковості схеми з ланцюжка керованих підстановок. Результати виявляються близькими (не краще ніж) до схеми S перетворення з множенням на МДВ матрицю, тобто з випадком, коли на першому циклі активізується лише один S-блок. Тобто активізація S-блоків першого циклу виявляється фіктивною (*не ефективною*). Таким чином, це значить, що лінійні перетворення на вході першого циклу не можуть покращити показників випадковості схеми.

Причиною цього виявляється те, що лінійні перетворення на вході першого циклу не забезпечують випадкового зв'язку між байтами на входах S-блоків і тому для цих S-блоків не виконується умова, що ймовірності переходів S-блоків не перемножуються, а скоріше підсумовуються.

Таблиця 3 – Статистичні дані ймовірності активізації 1-8-ми S-блоків для різних варіантів схеми

	Очікувана кількість активованих S-блоків	ВАРІАНТ ЗІ СХЕМОЮ ЗМІШУВАННЯ						БЕЗ СХЕМИ ЗМІШУВАННЯ		
		Схема змішування використовується на кожному циклі			Схема змішування використовується на 1-му циклі			Схема змішування не використовується		
		1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл	3-й цикл
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
$\Delta X_1 = \Delta X_2 \neq 0$	7	7 - 255 - 99.6%	6 - 28 - 10.98% 7 - 227 - 88.67%	6 - 19 - 7.42 % 7 - 236 - 92.18%	7 - 255 - 99.61%	5 - 14 - 5.47% 6 - 241 - 94.14%	6 - 25 - 9.76% 7 - 230 - 89.84%	1 - 112 - 43.75% 8 - 143 - 55.86%	6 - 22 - 8.59% 7 - 233 - 91.02%	6 - 23 - 8.98% 7 - 232 - 90.62%
$\Delta X_1 = \Delta X_3 \neq 0$	6	6 - 255 - 99.61%	6 - 27 - 10.55% 7 - 227 - 88.67% 8 - 1 - 0.39 %	6 - 31 - 12.11% 7 - 223 - 87.11% 8 - 1 - 0.39%	6 - 255 - 99.6%	4 - 2 - 0.78% 5 - 252 - 98.44% 6 - 1 - 0.39%	5 - 1 - 0.39% 6 - 23 - 8.98% 7 - 231 - 90.23%	2 - 152 - 59.37% 8 - 103 - 40.23%	6 - 13 - 5.08% 7 - 242 - 94.53%	6 - 20 - 7.81% 7 - 235 - 91.8%
$\Delta X_1 = \Delta X_4 \neq 0$	7	2 - 144 - 56.25% 7 - 111 - 43.36%	2 - 1 - 0.39% 6 - 18 - 7.03% 7 - 236 - 92.19%	5 - 1 - 0.39% 6 - 32 - 12.5 % 7 - 222 - 86.72%	2 - 168 - 65.62% 7 - 87 - 33.98%	5 - 14 - 5.47% 6 - 238 - 92.97% 7 - 3 - 1.17%	6 - 29 - 11.33% 7 - 226 - 88.28%	3 - 157 - 61.33% 8 - 98 - 38.28%	6 - 12 - 4.69% 7 - 243 - 94.92%	6 - 21 - 8.20% 7 - 234 - 91.40%
$\Delta X_1 = \Delta X_5 \neq 0$	4	4 - 255 - 99.60%	6 - 23 - 8.98 % 7 - 232 - 90.63%	6 - 27 - 10.55% 7 - 228 - 89.06%	4 - 255 - 99.61%	3 - 240 - 93.75% 4 - 15 - 5.86%	6 - 26 - 10.15% 7 - 229 - 89.45%	4 - 162 - 63.28% 8 - 93 - 36.33%	3 - 1 - 0.39% 6 - 15 - 5.86% 7 - 239 - 93.36%	6 - 21 - 8.20% 7 - 234 - 91.40%
$\Delta X_1 = \Delta X_6 \neq 0$	7	4 - 169 - 66.02% 7 - 86 - 33.59%	6 - 23 - 8.98% 7 - 231 - 90.23% 8 - 1 - 0.39%	6 - 33 - 12.89 % 7 - 222 - 86.72%	4 - 150 - 58.59% 7 - 105 - 41.02%	3 - 1 - 0.39% 5 - 4 - 1.56% 6 - 250 - 97.66%	5 - 1 - 0.39% 6 - 25 - 9.77% 7 - 228 - 89.06% 8 - 1 - 0.39%	5 - 167 - 65.23% 8 - 88 - 34.38%	4 - 1 - 0.39% 6 - 13 - 5.078% 7 - 241 - 94.14%	6 - 15 - 5.86% 7 - 240 - 93.75%
$\Delta X_1 = \Delta X_7 \neq 0$	6	4 - 155 - 60.54% 6 - 100 - 39.06%	5 - 1 - 0.39 % 6 - 24 - 9.37 % 7 - 230 - 89.84%	5 - 1 - 0.39 % 6 - 15 - 5.86 % 7 - 239 - 93.36%	4 - 163 - 63.67% 5 - 0 - 0% 6 - 92 - 35.94%	4 - 8 - 3.12% 5 - 245 - 95.70% 6 - 2 - 0.78%	6 - 23 - 8.98% 7 - 232 - 90.62%	6 - 167 - 65.23% 8 - 88 - 34.37%	6 - 16 - 6.25% 7 - 239 - 93.36%	6 - 24 - 9.37% 7 - 231 - 90.23%
$\Delta X_1 = \Delta X_8 \neq 0$	7	3 - 147 - 57.42% 6 - 66 - 25.78% 7 - 42 - 16.40%	4 - 1 - 0.39% 6 - 22 - 8.59% 7 - 232 - 90.62%	6 - 29 - 11.32% 7 - 226 - 88.28%	3 - 154 - 60.16% 6 - 62 - 24.22% 7 - 39 - 15.23%	2 - 1 - 0.39% 5 - 6 - 2.34% 6 - 248 - 96.88%	6 - 18 - 7.03% 7 - 237 - 92.58%	7 - 166 - 64.84% 8 - 89 - 34.77%	6 - 21 - 8.20% 7 - 233 - 91.02% 8 - 1 - 0.39%	5 - 1 - 0.39% 6 - 21 - 8.20% 7 - 233 - 91.02%

Продовження таблиці 3

1	2	3	4	5	6	7	8	9	10	11
$\Delta X_2 = \Delta X_3 \neq 0$	7	1 - 102 - 39.84% 7 - 153 - 59.77%	1 - 1 - 0.39% 6 - 30 - 11.72% 7 - 224 - 87.5%	6 - 20 - 7.81% 7 - 234 - 91.4% 8 - 1 - 0.39%	1 - 97 - 37.89% 7 - 158 - 61.72%	5 - 10 - 3.90% 6 - 245 - 95.70%	6 - 27 - 10.55% 7 - 228 - 89.06%	7 - 149 - 58.20%	5 - 15 - 5.86% 6 - 237 - 92.58% 7 - 3 - 1.172%	5 - 12 - 4.69% 6 - 243 - 94.92%
$\Delta X_2 = \Delta X_4 \neq 0$	5	5 - 255 - 99.60%	6 - 20 - 7.81% 7 - 235 - 91.8%	6 - 17 - 6.64% 7 - 238 - 92.97%	5 - 255 - 99.60%	3 - 4 - 1.56% 4 - 248 - 96.88% 5 - 3 - 1.17%	6 - 30 - 11.72% 7 - 225 - 87.89%	2 - 159 - 62.12% 7 - 96 - 37.5%	1 - 1 - 0.39% 5 - 12 - 4.69% 6 - 242 - 94.53%	5 - 13 - 5.07% 6 - 242 - 94.53%
$\Delta X_2 = \Delta X_5 \neq 0$	7	3 - 147 - 57.42% 7 - 108 - 42.19%	6 - 18 - 7.03% 7 - 237 - 92.58%	6 - 29 - 11.32% 7 - 226 - 88.28%	3 - 161 - 62.89% 7 - 94 - 36.72%	2 - 2 - 0.78% 5 - 13 - 5.08% 6 - 238 - 92.97% 7 - 2 - 0.78%	6 - 26 - 10.16% 7 - 229 - 89.45%	3 - 163 - 63.67% 7 - 92 - 35.93%	2 - 2 - 0.78% 5 - 10 - 3.90% 6 - 243 - 94.92%	5 - 13 - 5.08% 6 - 241 - 94.14% 7 - 1 - 0.39%
$\Delta X_2 = \Delta X_6 \neq 0$	3	3 - 255 - 99.61%	5 - 4 - 1.56% 6 - 164 - 64.06% 7 - 87 - 33.98%	5 - 1 - 0.39% 6 - 26 - 10.16% 7 - 228 - 89.06%	3 - 255 - 99.61%	2 - 220 - 85.94% 3 - 35 - 13.67%	5 - 3 - 1.17188% 6 - 172 - 67.1875% 7 - 80 - 31.25%	4 - 157 - 61.33% 7 - 98 - 38.28%	3 - 2 - 0.78% 5 - 11 - 4.3% 6 - 242 - 94.53%	5 - 20 - 7.81% 6 - 234 - 91.40% 7 - 1 - 0.39%
$\Delta X_2 = \Delta X_7 \neq 0$	7	3 - 100 - 39.06% 5 - 88 - 34.37% 7 - 67 - 26.17%	5 - 3 - 1.17% 6 - 26 - 10.15% 7 - 225 - 87.89% 8 - 1 - 0.39%	6 - 20 - 7.81% 7 - 235 - 91.8%	3 - 98 - 38.28% 5 - 101 - 39.45% 7 - 56 - 21.86%	4 - 1 - 0.39% 5 - 5 - 1.95% 6 - 249 - 97.27%	5 - 1 - 0.39% 6 - 25 - 9.77% 7 - 228 - 89.06% 8 - 1 - 0.39%	5 - 165 - 64.45% 7 - 90 - 35.16%	4 - 1 - 0.39% 5 - 12 - 4.68% 6 - 242 - 94.53%	5 - 9 - 3.51% 6 - 245 - 95.70% 7 - 1 - 0.39%
$\Delta X_2 = \Delta X_8 \neq 0$	7	4 - 175 - 68.35% 5 - 80 - 31.25%	6 - 13 - 5.08% 7 - 242 - 94.53%	6 - 24 - 9.37% 7 - 231 - 90.23%	4 - 162 - 63.28% 5 - 93 - 36.33%	3 - 4 - 1.56% 4 - 247 - 96.48% 5 - 4 - 1.56%	6 - 21 - 8.20% 7 - 233 - 91.01% 8 - 1 - 0.39%	6 - 150 - 58.59% 7 - 105 - 41.02%	5 - 12 - 4.68% 6 - 242 - 94.53% 7 - 1 - 0.39%	5 - 9 - 3.51% 6 - 245 - 95.70% 7 - 1 - 0.39%
$\Delta X_3 = \Delta X_4 \neq 0$	7	2 - 145 - 56.64% 6 - 40 - 15.62% 7 - 70 - 27.34%	2 - 1 - 0.39% 6 - 25 - 9.76% 7 - 229 - 89.45%	6 - 19 - 7.42% 7 - 236 - 92.18%	2 - 164 - 64.06% 6 - 36 - 14.06% 7 - 55 - 21.48%	5 - 6 - 2.34% 6 - 249 - 97.26%	6 - 25 - 9.76% 7 - 228 - 89.06% 8 - 2 - 0.78%	6 - 163 - 63.67%	4 - 3 - 1.17% 5 - 250 - 97.65% 6 - 2 - 0.78%	4 - 5 - 1.95% 5 - 248 - 96.87% 6 - 2 - 0.78%
$\Delta X_3 = \Delta X_5 \neq 0$	6	2 - 167 - 65.23% 6 - 88 - 34.37%	3 - 1 - 0.39% 6 - 23 - 8.98% 7 - 231 - 90.23%	6 - 28 - 10.93% 7 - 227 - 88.67%	2 - 151 - 58.98% 6 - 104 - 40.62%	4 - 7 - 2.73% 5 - 246 - 96.09% 6 - 2 - 0.78%	6 - 32 - 12.5% 7 - 223 - 87.1094%	2 - 157 - 61.32% 6 - 98 - 38.28%	1 - 2 - 0.78% 4 - 6 - 2.34% 5 - 244 - 95.31% 6 - 3 - 1.17%	4 - 9 - 3.51% 5 - 245 - 95.70% 6 - 1 - 0.39%

Продовження таблиці 3

1	2	3	4	5	6	7	8	9	10	11
$\Delta X_3 = \Delta X_6 \neq 0$	6	4 - 197 - 76.95% 7 - 58 - 22.66%	6 - 31 - 12.10% 7 - 224 - 87.5%	6 - 32 - 12.5% 7 - 222 - 86.72%	4 - 199 - 77.73% 7 - 56 - 21.87%	3 - 1 - 0.39% 5 - 8 - 3.12% 6 - 245 - 95.70% 7 - 1 - 0.39%	6 - 22 - 8.59% 7 - 233 - 91.01%	3 - 159 - 62.1094% 6 - 96 - 37.5%	4 - 5 - 1.95% 5 - 249 - 97.27% 6 - 1 - 0.39%	4 - 17 - 6.64% 5 - 236 - 92.19% 6 - 2 - 0.78%
$\Delta X_3 = \Delta X_7 \neq 0$	2	2 - 255 - 99.61%	4 - 1 - 0.39% 5 - 167 - 65.23% 7 - 85 - 33.20% 8 - 2 - 0.78%	5 - 2 - 0.78% 6 - 21 - 8.20% 7 - 231 - 90.23% 8 - 1 - 0.39%	2 - 255 - 99.6%	1 - 160 - 62.5% 2 - 95 - 37.10%	4 - 4 - 1.56% 5 - 166 - 64.84% 6 - 3 - 1.17% 7 - 81 - 31.64% 8 - 1 - 0.39%	4 - 163 - 63.67% 6 - 92 - 35.93%	3 - 2 - 0.78% 4 - 4 - 1.56% 5 - 247 - 96.48% 6 - 2 - 0.78%	4 - 6 - 2.34% 5 - 247 - 96.48% 6 - 2 - 0.78%
$\Delta X_3 = \Delta X_8 \neq 0$	7	3 - 169 - 66.01% 6 - 64 - 25% 7 - 22 - 8.59%	6 - 25 - 9.78% 7 - 230 - 89.84%	6 - 23 - 8.98% 7 - 232 - 90.62%	3 - 161 - 62.89% 6 - 74 - 28.90% 7 - 20 - 7.81%	5 - 11 - 4.3% 6 - 243 - 94.92% 7 - 1 - 0.39%	6 - 27 - 10.54% 7 - 228 - 89.06%	5 - 169 - 66.01% 6 - 86 - 33.59%	4 - 7 - 2.73438% 5 - 248 - 96.87%	4 - 12 - 4.68% 5 - 242 - 94.53% 6 - 1 - 0.39 %
$\Delta X_4 = \Delta X_5 \neq 0$	7	3 - 163 - 63.68% 6 - 61 - 23.83% 7 - 31 - 12.11%	6 - 19 - 7.42% 7 - 236 - 92.19%	6 - 22 - 8.59% 7 - 233 - 91.02%	3 - 169 - 66.02% 6 - 54 - 21.09% 7 - 32 - 12.5%	5 - 11 - 4.29% 6 - 243 - 94.92% 7 - 1 - 0.39%	5 - 1 - 0.39% 6 - 31 - 12.11% 7 - 223 - 87.11%	1 - 97 - 37.89% 5 - 158 - 61.71%	3 - 3 - 1.17% 4 - 246 - 96.09% 5 - 6 - 2.34%	3 - 8 - 3.12% 4 - 241 - 94.14% 5 - 6 - 2.34%
$\Delta X_4 = \Delta X_6 \neq 0$	5	2 - 160 - 62.5% 5 - 95 - 37.11%	6 - 26 - 10.15% 7 - 229 - 89.45%	6 - 19 - 7.42% 7 - 236 - 92.18%	2 - 145 - 56.64% 5 - 110 - 42.97%	1 - 1 - 0.39% 3 - 3 - 1.17% 4 - 246 - 96.09% 5 - 5 - 1.95%	5 - 1 - 0.39% 6 - 25 - 9.76% 7 - 229 - 89.45%	2 - 153 - 59.76% 5 - 102 - 39.84%	3 - 1 - 0.39% 4 - 249 - 97.27% 5 - 5 - 1.95%	3 - 11 - 4.297% 4 - 239 - 93.35% 5 - 5 - 1.95%
$\Delta X_4 = \Delta X_7 \neq 0$	7	4 - 154 - 60.15% 5 - 66 - 25.78% 6 - 16 - 6.25% 7 - 19 - 7.42%	6 - 23 - 8.98% 7 - 231 - 90.23% 8 - 1 - 0.39%	5 - 1 - 0.39% 6 - 22 - 8.59% 7 - 232 - 90.62%	4 - 149 - 58.20% 5 - 70 - 27.34% 6 - 14 - 5.47% 7 - 22 - 8.59%	4 - 2 - 0.78% 5 - 11 - 4.29% 6 - 242 - 94.53%	6 - 26 - 10.15% 7 - 229 - 89.45%	3 - 164 - 64.06% 5 - 91 - 35.54%	2 - 1 - 0.39% 3 - 4 - 1.56% 4 - 247 - 96.48% 5 - 3 - 1.17%	3 - 9 - 3.52% 4 - 244 - 95.31% 5 - 2 - 0.78%
$\Delta X_4 = \Delta X_8 \neq 0$	1	1 - 255 - 99.6%	4 - 146 - 57.03% 6 - 69 - 26.95% 7 - 26 - 10.15% 8 - 14 - 5.47%	4 - 2 - 0.78% 6 - 18 - 7.03% 7 - 235 - 91.8%	1 - 255 - 99.60%	1 - 255 - 99.60%	4 - 150 - 58.59% 5 - 1 - 0.39% 6 - 65 - 25.39% 7 - 29 - 11.32% 8 - 10 - 3.90%	4 - 156 - 60.93% 5 - 99 - 38.67%	3 - 3 - 1.17% 4 - 249 - 97.26% 5 - 3 - 1.17%	3 - 2 - 0.78% 4 - 245 - 95.70% 5 - 8 - 3.12%

Продовження таблиці 3

1	2	3	4	5	6	7	8	9	10	11
$\Delta X_5 = \Delta X_6 \neq 0$	7	4 - 170 - 66.40% 6 - 48 - 18.75% 7 - 37 - 14.45%	6 - 17 - 6.64% 7 - 238 - 92.99%	6 - 27 - 10.55% 7 - 228 - 89.06%	4 - 158 - 61.71% 5 - 0 - 0% 6 - 63 - 24.61% 7 - 34 - 13.28%	3 - 1 - 0.39% 5 - 11 - 4.29% 6 - 243 - 94.9%	6 - 29 - 11.32% 7 - 226 - 88.28%	1 - 102 - 39.84% 4 - 153 - 59.76%	3 - 247 - 96.48% 4 - 8 - 3.13%	2 - 5 - 1.95% 3 - 235 - 91.8% 4 - 15 - 5.86%
$\Delta X_5 = \Delta X_7 \neq 0$	6	4 - 219 - 85.54% 6 - 36 - 14.06%	5 - 2 - 0.78% 6 - 22 - 8.59% 7 - 231 - 90.23%	6 - 25 - 9.76% 7 - 229 - 89.45% 8 - 1 - 0.39%	4 - 228 - 89.06% 6 - 27 - 10.54%	3 - 1 - 0.39% 4 - 4 - 1.56% 5 - 246 - 96.09% 6 - 4 - 1.56%	6 - 21 - 8.20% 7 - 234 - 91.40%	2 - 148 - 57.81% 4 - 107 - 41.8%	1 - 2 - 0.78% 2 - 1 - 0.39% 3 - 237 - 92.58% 4 - 15 - 5.9%	2 - 4 - 1.56% 3 - 242 - 94.53% 4 - 9 - 3.52%
$\Delta X_5 = \Delta X_8 \neq 0$	4	4 - 157 - 61.33% 6 - 86 - 33.59% 7 - 12 - 4.68%	3 - 1 - 0.39% 4 - 1 - 0.39% 6 - 28 - 10.94% 7 - 225 - 87.89%	5 - 1 - 0.39% 6 - 27 - 10.55% 7 - 227 - 88.67%	4 - 167 - 65.23% 5 - 1 - 0.39% 6 - 72 - 28.12% 7 - 15 - 5.86%	3 - 1 - 0.39% 5 - 12 - 4.69% 6 - 242 - 94.53%	6 - 24 - 9.37% 7 - 231 - 90.23%	3 - 158 - 61.72% 4 - 97 - 37.89%	2 - 1 - 0.39% 3 - 248 - 96.87% 4 - 6 - 2.34%	2 - 1 - 0.39% 3 - 241 - 94.14% 4 - 13 - 5.078%
$\Delta X_6 = \Delta X_7 \neq 0$	7	2 - 1 - 0.39% 4 - 102 - 39.84% 5 - 99 - 38.67% 6 - 32 - 12.5% 7 - 21 - 8.20%	3 - 1 - 0.39% 5 - 3 - 1.17% 6 - 28 - 10.94% 7 - 223 - 87.11%	6 - 33 - 12.89% 7 - 222 - 86.72%	2 - 4 - 1.56% 4 - 103 - 40.23% 5 - 94 - 36.71% 6 - 41 - 16.02% 7 - 13 - 5.08%	5 - 6 - 2.34% 6 - 247 - 96.48% 7 - 2 - 0.78%	6 - 23 - 8.98% 7 - 232 - 90.62%	1 - 101 - 39.45% 3 - 154 - 60.15%	2 - 222 - 86.71% 3 - 33 - 12.89%	1 - 2 - 0.78% 2 - 215 - 83.98% 3 - 38 - 14.84%
$\Delta X_6 = \Delta X_8 \neq 0$	5	3 - 161 - 62.89% 4 - 64 - 25% 5 - 30 - 11.71%	6 - 32 - 12.5% 7 - 223 - 87.10%	6 - 22 - 8.59% 7 - 233 - 91.02%	3 - 166 - 64.84% 4 - 55 - 21.48% 5 - 34 - 13.28%	3 - 5 - 1.95% 4 - 246 - 96.0% 5 - 4 - 1.56%	6 - 23 - 8.98% 7 - 231 - 90.23% 8 - 1 - 0.39%	2 - 162 - 63.28% 3 - 93 - 36.32%	2 - 222 - 86.72% 3 - 33 - 12.89%	1 - 1 - 0.39% 2 - 227 - 88.67% 3 - 27 - 10.54%
$\Delta X_7 = \Delta X_8 \neq 0$	7	4 - 154 - 60.15+5 6 - 87 - 33.98% 7 - 14 - 5.46%	5 - 1 - 0.39% 6 - 18 - 7.03% 7 - 236 - 92.19%	6 - 27 - 10.54% 7 - 228 - 89.06%	3 - 1 - 0.39% 4 - 165 - 64.45% 5 - 2 - 0.78% 6 - 78 - 30.47% 7 - 9 - 3.52%	5 - 11 - 4.3% 6 - 244 - 95.31%	6 - 22 - 8.6% 7 - 233 - 91.02%	1 - 95 - 37.11% 2 - 160 - 62.5%	1 - 147 - 57.42% 2 - 108 - 42.19%	1 - 163 - 63.67% 2 - 92 - 35.93%

4 Висновки

Пропозиція стосовно можливостей удосконалення шифру Струмок, що була висунута раніше автором роботі [1], виявляється помилковою. Так, раніше запропоноване рішення практично поступається за своїми показниками випадковості відповідному рішенню представленому у специфікації до шифру Струмок [3].

Наступний висновок, який має принципове значення, міститься в тому, що залишається справедливим раніше висловлене в роботі [2] загальне положення, згідно до якого мінімальне число активованих S-блоків перших циклів SPN шифрів дорівнює одному! Виключенням є лише шифр Лабіринт [4], в котрому використовується нелінійне доциклове перетворення (*перетворення з шару S-блоків на вході першого циклу*). Фактично це додаткове циклове перетворення.

Посилання

[1] Lisitzky, K. Stratehiia vyboru S-blokiv dlia neliniinoho peretvorennia shyfru Strumok. Kompiuterni nauky ta kiberbezpeka. 2018. № 2. P.4–11. URL: https://periodicals.karazin.ua/cscs/article/view/12025
[2] Dolgov V. I., Lisitska I. V., Lisitskyi K. Ye. The new concept of block symmetric ciphers design. TelecomRadEng. Vol. 76. Issue 2. P. 157–184.
[3] Matematychna struktura potokovoho shyfru Strumok / Gorbenko I.D., Kuznetsov O.O., Oleksyichuk A.M., V.A. Tymchenko. Radyotekhnyka. Kharkiv: KhTURE, 2018. Vyp. 193. P. 17–27.
[4] Golovashych S. A. Spetsyfykatsyia alhorytma blochnoho symmetrychnoho shyfrovanyia «Labyrynt». Prykladnaia radyoэlektronyka. Kharkiv: KhTURE, 2007. Vol. 6, №2. P. 230–240.

Reviewer: Roman Oliynikov, Doctor of Sciences (Eng.), Full Professor, V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine. E-mail: roliynykov@gmail.com

Received: October 2018.

Authors:
Konstantin Lisitzky, postgraduate student of the Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine. E-mail: lisickiy@ukr.net

Katerina Kuznetsova, computer science student**,** V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine. E-mail: kate.kuznetsova.2000@gmail.com

On the weakness S of the transformation of the cipher Strumok from the chain of controllable S-blocks.

Abstract. The peculiarities of the construction of the S-transform of the Stream cipher “Strumok” are discussed. In particular, an analysis of the preposition for constructing S-transformation of the stream cipher “Strumok” using controlled S-blocks is underway. His randomness scores are evaluated. It is shown that it is inferior to the effectiveness of the original proposal. The reasons of such circumstances turn out.

Keywords: current cipher; random substitution; differential probability; S-transformation; linear mixing scheme.

Рецензент: Роман Олейников, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина. Украина. E-mail: roliynykov@gmail.com

Поступила: Октябрь 2018.

Авторы:
Константин Лисицкий, аспирант кафедры безопасности информационных систем и технологий, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 4, Харьков, 61022, Украина.
E-mail: lisickiy@ukr.net

Екатерина Кузнецова, студентка факультета компьютерных наук, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 4, Харьков, 61022, Украина. E-mail: kate.kuznetsova.2000@gmail.com

О слабости S-преобразования шифра Струмок из цепочки управляемых S-блоков.

Аннотация. Обсуждаются особенности построения S-преобразования шифра “Струмок”. Выполнен анализ предложения по построению S-преобразования поточного шифра “Струмок” с использованием управляемых S-блоков. Оцениваются показатели его случайности. Показывается, что оно по своей эффективности уступает соответствующему оригинальному решению. Выясняются причины таких обстоятельств.

Ключевые слова: поточный шифр; случайная подстановка; дифференциальная вероятность; S-преобразование; линейная смешивающая схема.

UDC 004.056.55

IMPROVED MATHEMATICAL MODEL OF THE POST-QUANTUM ELETRONIC SIGNATURE MECHANISM

Yurij Gorbenko[1], Kateryna Isirova[2]

[1] JSC "Institute of Information Technologies", 12 Bakulin St., Kharkiv, 61166, Ukraine
GorbenkoU@iit.kharkov.ua

[2] V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
KaterinaIsirova@gmail.com

Reviewer: Vyacheslav Kalashnikov, Doctor of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, 64849, Mexico.
kalash@itesm.mx

Received on November 2018.

Abstract. *In the paper new electronic signature mechanisms which will be urgent in the post-quantum period development necessity is grounded. The main one time key mechanisms are briefly described. Problems related with Lamport OTS mechanism and Winternits OTS mechanism related to private and public keys sizes are revealed. Main evaluation criteria are defined. In the paper improved mechanism called POST which can be used in post-quantum period is proposed. POST mechanism is tends to avoid the disadvantages as previous ones. Also processes of signature generation and validation for POST mechanism are presented.*

Keywords: *post-quantum cryptography; post-quantum electronic signatures; improved mechanism POST; one time key mechanisms.*

1 Introduction

Development and standardization post-quantum asymmetric cryptographic transformation is one of the most important problems of our time. The leading states, including NIS, realizing the need to find new asymmetric cryptographic primitives electronic signature (ES) and asymmetric encryption to be relevant and can be used in post quantum period, announced a competition to develop standards of post quantum asymmetric cryptographic primitives [1-3]. Bids were accepted NIST until the 30th November 2017. They relate primarily asymmetric algorithms ES. The European Union (EU) is also active in the development and research of post-quantum asymmetric cryptographic standards, including standards post-quantum ES.

Conducted in technologically developed countries showed that one of the promising areas post-quantum ES creation, can be direction based on the use of hash functions and Merkle tree [6]. The basis of this trend assigned keys and single-use one time ES. Historically the current time and offered substantially explored these mechanisms for generating and using single-key ES based on hash functions (*symmetric cryptographic functions and traction*):

- Lamport mechanism of one time keys LOTS [7];
- Winternits mechanisms with one time keys WOTS, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8,10];
- modification mechanism of one time keys Biba, HORS, HORS +, HORS ++ and HORST [10].

2 Problem and opportunities

Significant development of ES mechanism based on OTS is Winternits OTS [4,8]. The fact is that although the Lamport OTS and Lamporta – Diffie OTS may provide the potential properties of cryptographic resistance (and indeed encryption), but the size and ES and OTS keys are quite large. Reducing the size of the ES mechanism achieved in ES with OTS as proposed in [4,13], called Winternits mechanism (W OTS) [8]. The idea Winternits mechanism is signed so that, unlike the Lamport OTS already several bits of hash - values using a sequence OTS single secret key. Another feature is the use Winternits mechanism aimed one-way function that we believe can be called

clutch function. The peculiarity of the clutch functions is possibility of public key obtained directly from the ES. In our view this is a crucial feature of the Winternits mechanism.

As in the Lamport OTS and Lamport – Diffie OTS mechanisms, the Winternits mechanism (WOTS) uses a one-way hash - function and cryptographic hash - function. Parameter Winternits ES $w \geq 2$ selected as the number of bits that must be signed (encrypted) simultaneously using a single key. ES is also an option WOTS using additional control method based on integrity checksum hash - value that is encrypted. Applying additional method of monitoring the integrity aims to reinforce stability Winternits OTS ES.

Also, the analysis showed that the main papers related to one time keys are used insufficiently "true" cryptographic evaluation criteria cryptographic stability and complexity. In our opinion, when evaluating and comparing different mechanisms of ES OTS, should at least use [5]:

- Lc, Lv and Lp - length, respectively classified Ks and public key ES in April and open;
- the number of secret Nk one time key ES WOTS that can be used with equal probability;
- entropy source key H (Nk) of the modification ES WOTS single key;
- secure a TB as expectation time disclosure of cryptographic system known in the application of analytical power and attacks by both classical and quantum computers and, in this case for example the definition of secret key provided and consequently ES single public key ES OTS;
- distance unity sources l_0 OTS one time ES secret keys;
- complexity of a successful crypto analysis Ic ES with OTS in the application of force;
- complexity of a successful crypto analysis Ia ES OTS in applying analytical methods.

Basic definitions and the application of the proposed criteria and indicators for assessing the ES from OTS to be applied in required in the analysis and comparison.

The analysis of the basic mechanisms of one time keys - Lamport OTS, OTS Winternits (WOTS, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8,9]) and modification mechanism of one time keys (Biba, HORS, HORS +, HORS ++ and HORST) do not meet the requirements of space and time complexity, which greatly complicates the implementation post-quantum ES based on hash functions. The fact is that when trying to reduce the size of the keys and the ES is a dESarture from the true perfect ES [13-15]. However, in our view, there is the possibility of building a ES post-quantum based OTS keys as perfekt OTS (POTS) [13], the properties are almost not inferior Lamport mechanism. Therefore, we consider the nature, the study of properties, advantages and disadvantages, as well as conditions and opportunities for improved use of POTS mechanism in various applications post-quantum period.

3 Improved mathematical model of the post-quantum electronic signature mechanism

Terms. In Winternits OTS (WOTS) ES mechanism exists over the Lamport mechanism, the ability to produce shorter ES, but the number of private and public keys with increasing parameter w increases significantly. Also generally WOTS mechanism that is adequate for the characteristics of the Lamport mechanism significantly increased temporal and spatial complexity. The specified limits the use of Winternits mechanisms (WOTS, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8,9]) for the case when the requirement should be similar to that performed Lamport mechanism. There is no possibility to use the private key for both signature and some much larger number of hash - value (WFTS) [9]. Using this idea, consider an improved POTS mechanism with one time keys, which are the main advantages of reducing the lengths of one-time keys (*private and public key*) and the length of the ES. There are also options for its use and WFTS.

As in LOTS and LDOTS, in an enhanced POTS mechanism or will use the one-way hash – function

$$f: \{0, 1\}^{l} \rightarrow \{0, 1\}^{l} \quad (1)$$

and required cryptographic hash - function

$$g: \{0, 1\}^{*} \rightarrow \{0, 1\}^{l}.$$

In ES first message *M* made hash message *M* using coherent (typically cryptographic) hash - functions with parameters *Pr* and computed hash – value

$$h_M = H(M, Pr)) \tag{2}$$

Further value h_M essentially means replacing the encrypted blocks w bits of hash - value h_M one time secret key encryption process this continues for all blocks of bits hash - value h_M.

So, l_h bit hash – value h_M replaced (encrypted) once the keys essentially steady course codes as a sequence of bits h_M replaced one time secret random order. Sequence l_k secret sequence is the message M. This ES ES with a selected x_i or y_i sequences is as open and accessible to users (*verifyer*) of the domain and the offender (*crypto analytics*). Later this ES in the appropriate format transmitted and stored along with the message and is its single ES. In the case of POTS ES mechanism consists of k random sequences, and $k \le l_h$.

Key generation mechanism for POTS. We assume that the parameter $w \ge 1$ determines the number of bits of hash - value that should be signed simultaneously, ie replaced by a secret key. Moreover, if $w = 1$ have particular case - OTS Lamport mechanism of keys. If $w \ge 2$ have a common Winternits mechanism submission, although further validation and encryption function is modified.

In the POTS mechanism ES (encryption) is performed (not necessarily) by applying to all w_b block conversion type

$$z = Z(w_b) \tag{3}$$

Therefore, w bits of the block are displayed in bits w * new unit. Moreover L_{bi} length b_i Block can be either more or less length L_{bi*} bloc b_i^* Derived from transformation (3).

Immediately note that the main difference POTS mechanism is that it applies each transformation b_i block according to [13] in this form. If

$$0 \le b_i \le (2^w / 2) - 1 \tag{4}$$

then each b_i encrypted block (replaced) sequentially secret key from the set X, or encrypted (*replaced*) sequentially secret key from the set Y.

Also, similar to the generalization Winternits define parameters t_1, t_2, t as [7,8]

$$t_1 = \left\lceil l / \log_2 w^* \right\rceil, t_2 = \left\lceil \log_2 t_1((w^* - 1)) / \log_2 w^* \right\rceil + 1, \quad t = t_1 + t_2. \tag{5}$$

We assume that the hash - value message supplied in blocks b_i (b_i^*) type

$$d = bt1\text{-}1 \,||\, .bi. . \,||\, b0, \tag{6}$$

can determine the checksum in the form [7]

or as

$$c^* = \sum_{i=1}^{t_1} (w^* - 1 - b_i^*), \tag{7}$$

$$c^* = \sum_{i=1}^{t_1 1} (2^{w^*} - b_i^*). \tag{8}$$

In the POTS model is not excluded that the parameters t_1, t_2, t can be defined otherwise. In mechanisms POTS data hash - value d (6) and checksum C (7) and (8) can encrypt different handicap, such as a checksum with more or less depending on the requirements of the handicap.

However, a preliminary analysis showed that the type conversion functions blocks (3) and (4) can significantly affect the cryptographic resistance to existing and potential attacks. Therefore, one of the important objectives of this study is to determine the conversion functions, which will allow to provide shorter secret and public keys, and reduce the length of the ES, providing acceptable cryptographic resistance to existing and potential attacks from classical and quantum computers.

After you convert (6) or (7) checksum C^* in blocks of bits w^* concatenation of hash - value (6) d and then runs simultaneous identical encryption POTS and verification. Note that checksums are

calculated arbitrarily depending on the need. Also mentioned ES d and checksums *C* (7) and (8), etc., can be encrypted worthy of OTS.

Specification of parameters for POTS. To make ES refine your first signature - *t1*, *t2* and *t*. If the length of L_s random or pseudorandom sequence multiples w^*. Then *t1* determines the number of blocks of bits hash - value that will be signed (encrypted) a secret key. In this case

$$t = t1 = n / w^* \tag{9}$$

If n is not a multiple w^*, The last block is less than w^* bits, so the number of bits required to sign necessary to increase the way that *t1* was intact. In (8) *t2* determines the number of blocks by which filed checksum. Generally

$$t^* = t1 + t2 \tag{10}$$

Without loss of both theoretical and practical presentation and research WOTS can (*but not necessarily*) considered that the length of the block *w = 1,2,3,3., 4.6...* . Under this condition for each unique encryption w_i vacancies in general

$$N_w = 2^w,\ w = 2,3,4,5,6... \ . \tag{11}$$

random sequences each secret key.

In case (4) for each encryption w_i unit must

$$N_w = 2 \tag{12}$$

random sequences each secret key. Therefore, depending on the value of *w*, *U* gain to reduce the length of the secret key in general to respect POST is WOST

$$U = 2^{w-1} \tag{13}$$

ES secret key POTS $X_d\ (w^*)$, $Y_d(w^*)$ is a sequence of *t* secret keys sets

$$\begin{aligned} X_d(w^*) &= (x_{t-1},\ldots,\ x_i,\ \ldots,\ x_0) \\ Y_d(W^*) &= (y_{t-1},\ldots,\ yi,\ \ldots,\ y_0) \end{aligned} \tag{14}$$

the length of each of the sequences secret $l(w^*)$.

Each set (14) secret keys $X_d\ (w^*)$, $Y_d(w^*)$ is part of the secret (*private*) key.

Public key verification mechanism for ES POTS calculated way hash secret keys (14) using one or directed cryptographic hash - functions *f(g)*. Due *t* get 2 sets of keys to open each:

$$\begin{aligned} H_d(X) &= H(x_{t-1}),\ldots,\ \mathrm{H}(x_i),\ \ldots,\ \mathrm{H}(x_0) \\ H_d(Y) &= H(y_{t-1}),\ldots,\ \mathrm{H}(y_i),\ \ldots,\ \mathrm{H}(y_0) \end{aligned} \tag{15}$$

length of hash - value l_h Each secret key sequence.

Developing a mechanism for POTS ES.

Let the message M have hash - value

$$g(M) = h = (h_l,...,h_i,...,h_0), \tag{16}$$

which should be signed using cryptographic hash - function *g*.

In general, if l_h not fold w^*. Then l_h added to the required number of zeros, so that the length l_h had multiple w^*. Line l_h bits divided into *t* blocks $b_{t-1},...,b_i,...,b_0$ length of w bits each. But we will consider, as a rule, without losing generality case (9).

Further to ES and ES validation rules will apply when the length of the block will change. In fact, as a result of this transformation *w* bits b_i unit displayed in bits $w^* b_i^*$ the new unit, and the length L_{hi^*} new unit b_i^* can be either more or less length L_{hi} bloc b_i derived from transformation (7).

Thus the POTS mechanism implemented following the previous transformation:

- line l_h bit hash - value is divided into blocks t $b_{t-1},...,b_i,...,b_0$ w bits length of each block;
- w bit b_i blocks appear in the new bit w^* b_i^* blocks, and active case when $b_i^* = b_i$;
- w^* new bit blocks (3) b_i^* encrypted using a secret key ($X_d(b_i^*)$, $Y_d(b_i^*)$) according to (12) - (14) with a length of each of the sequences secret $l(w^*)$.

Thus, unlike Winternits mechanism, the POTS mechanism w bits b_i. Blocks are displayed in bits w^* b_i^* blocks that may have a shorter and more towards w.

The result is as follows ES

$$\{M; Z^* = (\{x_{t^*-1} \mid y_{t^*-1}\}), \{x_{t^*-2} \mid y_{t^*-2}\},...,\{x_i \mid y_i\},...,\{x_0 \mid y_0\}) =$$
$$\left\{M, Z^* = (z_{t^*}, z_{t^*-1},..., z_i ,..., z_0^*)\right\} \quad (17)$$

In (17) the symbol " | " means that when encryption ES appears in one of the sequences used secret - x_i or y_i, defined i - by unit of length w^* bits. Further parameter t^* means the number of blocks that can be both more and less than t, and equal to t.

Check ES mechanism for POTS. Check ES carried out in that order.

1. Using cryptographic hash - hash function g made Message M^* for which the test is ES The result is a hash – value

$$h_{Mi^*} = g(M^*, \Pr). \quad (18)$$

If the length of h_{Mi^*} not a multiple of w, then the string of bits h_{Mi^*} in accordance with the agreement a number of zeros is added, so that the length h_{Mi^*} was a multiple of w. Line h_{Mi^*} bits is divided into blocks t^* $b_{t^*-1},...,b_i,...,b\ 0$ length w^* bits each.

2. In accordance with the values b_i blocks h_{Mi^*} verification of the public key ES (15) selected hash - value $H(x_i)$ or $H(y_i)$, because we find that

$$Z^* = (\{H(x_1) \mid H(y_1)\}), \{H(x_2) \mid H(y_2)\},...,\{H(x_i) \mid H(y_i)\},...,\{H(x_n) \mid H(y_n)\}) =$$
$$(z_{t-1}^*, z_{t-2}^*,..., z_i^*,..., z_0^*). \quad (19)$$

3. Finally, the user has received a signed message hash all sequences ES (17), gets them hash – value

$$(H(z_{t^*}), H(z_{t^*-1}),..., H(z_i),..., H(z_0)) \quad (20)$$

and compares the values with the values (17), i.e. $(z_{t^*}, z_{t^*-1},..., z_i,..., z_0)$. If all t^* when comparing values coincide, the ES is a real, otherwise the ES considered distorted.

4 Conclusions

The idea of the Winternits mechanism is signed so that, unlike the Lamport OTS already several bits of hash - values using a sequence OTS single secret key. Another feature is the use Winternits mechanism aimed one way function that we believe can be called clutch function. The peculiarity of the functions clutch is possibility of public key obtained directly from the ES. In our view this is a crucial feature of the mechanism Winternits.

The analysis of the basic mechanisms of one time keys - Lamporta OTS, OTS Winternits (WOTS, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$) And modification mechanism of one time keys (Biba, HORS, HORS +, HORS ++ and HORST) do not meet the requirements of space and time complexity, which greatly complicates the implementation post-quantum ES based on hash functions. However, in our view, there is the possibility of building a ES post-quantum based OTS keys as perfekt OTS (POTS) [13].

Preliminary analysis showed that the type conversion functions blocks (5) can significantly affect and cryptographic resistance to existing and potential attacks. Therefore, one of the important objectives of this study is to determine the conversion functions, which will allow to provide shorter secret and public keys, and reduce the length of the ES, providing acceptable cryptographic resistance to existing and potential attacks from classical and quantum computers.

Thus, the offer of the use of POTS mechanisms one time keys and also as a result of one-time ES, can make conclusions about the possibility of their use in ES post-quantum mechanisms based on hash - functions.

References

[1] Koblitz N. Menezes A. J. A riddle wrapped in an enigma. URL:https://eprint.iacr.org/2015/1018.pdf
[2] Report on Post-Quatum Cryptography / Chen L. and all. NISTIR 8105 (DRAFT). URL:http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf
[3] Mosca M. Setting the Scene for the ETSI Quantum-safe Cryptography Workshop. 1st Quantum-Safe-Crypto Workshop: E-proceedings. Sophia Antipolis, Sep. 26-27. 2013. P.25–28. URL: https://docbox.etsi.org/workshop/2013/201309_crypto/e-proceedings_crypto_2013.pdf
[4] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework.
[5] Post-quantum cryptography and mechanisms for its implementation / Gorbenko I.D. and all. Radiotechnics. 2016. Vol. 186. P. 32–52.
[6] Merkle R. A certified digital signature. Advances in Cryptology - CRYPTO '89 / Gilles Brassard, editor. Springer, 1990. Vol. 3.35 of LNCS. P. 218–238.
[7] Lamport L. Constructing digital signatures from a one way function. SRI International Computer Science Laboratory: Technical. Report SRI-CSL-98, 1979. URL:https://www.microsoft.com/en-us/research/uploads/prod/2016/12/Constructing-Digital-Signatures-from-a-One-Way-Function.pdf
[8] Hülsing A. W-OTS + - shorter signatures for hash-based signature schemes. Progress. in Cryptology - AFRICACRYPT 2013 / A. Youssef, A. Nitaj, and A.-E. Hassanien, editors. Springer, 2012. Vol. 7918 of LNCS. P. 173–188.
[9] SPHINCS: practical stateless hash-based Signatures. A certified digital signature / D. J. Bernstein and all. Advances in Cryptology - CRYPTO '89 / Gilles Brassard, editor. Springer, 1990. Vol. 3.35 of LNCS. P. 218–238.
[10] SPHINCS: practical stateless hash-based Signatures / D. J. Bernstein and all. URL: djb@cr.yp.to. daira@leastauthority.com, zooko@leastauthority.com.
[11] Gorbenko, I., Ponomar, V. Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application. EasternEuropean Journal of Enterprise Technologies. 2017. Vol. 2, Issue 9(86). P. 21–32. URL: http://journals.uran.ua/eejet/article/view/96321/93.881.12
[12] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework.
[13] Horbenko Yu.I., Melnyk T.V., Horbenko I.D. Analysis of potential post-quantum electronic signatures based on the hash - functions. Radiotechnics. 2017. Vol. 189. P. 115–131.
[14] Gorbenko Yu. Methods of construction of and Analysis, standardization and application KRSM: Monograph / Ed. Gorbenko I. D. Kharkov: Fort, 2015. 958 p.
[15] Horbenko Yu.I., Hanzya R.S. Stability analysis top cryptosystem against quantum cryptanalysis algorithm based on Grover. Data protection: Scientific journal. 2014. P. 22–28.

Рецензент: В'ячеслав Калашников, д.ф.-м.н., проф., Технологический університет Монтеррея, пр. Еухеніо Гарса Сада 2501, Монтеррей, 64849, Мексика.
E-mail: kalash@itesm.mx

Надійшло: Листопад 2018.

Автори:
Юрій Горбенко, к.т.н., перший заступник головного конструктора ПАТ «Інститут інформаційних технологій», вул. Бакуліна, 12, Харків, 61166, Україна.
E-mail: GorbenkoU@iit.kharkov.ua
Катерина Ісірова, аспірантка, Харківський національний університет ім. В. Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна.
E-mail: KaterinaIsirova@gmail.com

Удосконалений механізм одноразових ключів для постквантового періоду на основі геш–функцій.

Анотація. Обгрунтовано необхідність розробки нових механізмів електронного підпису, які будуть актуальними і можуть застосовуватися в постквантовий період. Виявлено проблеми, пов'язані з механізмами одноразової підписи Lamport і Winternits щодо розмірів особистих і відкритих ключів. Визначено основні критерії оцінки. У роботі пропонується вдосконалений механізм POST, який може бути використаний в пост квантовому періоді. Механізм POST позбавлений недоліків, описаних в попередніх механізмах. Також описані процеси генерації і перевірки підпису для механізму POST.

Ключові слова: постквантова криптографія; постквантові електронні підписи; вдосконалений механізм POST; механізми одноразових ключів.

Рецензент: Вячеслав Калашников, д.т.н., проф., Технологический университет Монтеррея, пр. Еухенио Гарса Сада 2501, Монтеррей, 64849, Мексика.
E-mail: kalash@itesm.mx

Поступила: Ноябрь 2018.

Авторы:
Юрий Горбенко, к.т.н., первый заместитель главного конструктора АО "Институт информационных технологий", ул. Бакулина, 12, Харьков, 61166, Украина.
E-mail: GorbenkoU@iit.kharkov.ua

Екатерина Исирова, аспирантка, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы, 4, Харьков, 61022, Украина.
E-mail: KaterinaIsirova@gmail.com

Усовершенствованный механизм одноразовых ключей для постквантового периода на основе хеш-функций.

Аннотация. Обоснована необходимость разработки новых механизмов электронной подписи, которые будут актуальными и могут применяться в постквантовый период. Выявлены проблемы, связанные с механизмами одноразовой подписи Lamport и Winternits относительно размеров личных и открытых ключей. Определены основные критерии оценки. В работе предлагается усовершенствованный механизм POST, который может быть использован в постквантовом периоде. Механизм POST лишен недостатков, описанных в предыдущих механизмах. Также описаны процессы генерации и проверки подписи для механизма POST.

Ключевые слова: постквантовая криптография; постквантовые электронные подписи; усовершенствованный механизм POST; механизмы одноразовых ключей.

UDC 004.056.55

MATHEMATICAL MODEL FOR THE FINGERPRINT MINUTIAE DISTORTION

Sergey Rassomakhin[1], Alexandr Kuznetsov[1], Vladimir Shlokin[1], Anna Uvarova[2]

[1] V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
rassomakhin@karazin.ua, kuznetsov@karazin.ua, vshlokin@ukr.net,

[2] Yuzhnoye State Design Office, Dnipro, 3 Krivorozhskaya St., 49008, Ukraine
annet.uvarova@gmail.com

Reviewer: Serhii Toliupa, Doctor of Sciences (Engineering), Full Prof., Taras Shevchenko National University of Kiev, 81 Lomonosova St., Kyiv, 03189, Ukraine.
tolupa@i.ua

Received on October 2018

Abstract. *This paper involves the research of biometric fingerprint images, minutiae and the mathematical probabilistic model of their distortion. The suggested model is based on heuristic analysis of the fingerprint scanning results with account for the nature of the potential errors. She allows to model a typical minutiae behavior in the biometric fingerprint images. The most typical distortion types were modeled, including the displacement of the fingerprint`s geometrical center, fingerprint rotation, minutiae deletion, as well as the distance changes between minutiae pairs.*

Keywords: *biometric authentication; fingerprint images; minutia.*

1 Introduction

Biometric authentication is being widely used in the current information systems [1-21]. The most developed methods in this area include face identification [1-4], retina identification [5-8], identification using fingerprint ridges [9-16] etc. At the same time, the problem of minutiae distortion modeling stands out as one of the most complex in the field of fingerprint authentication, the main biometric authentication method [15,16]. This paper involves examination of biometric fingerprint images [9-16], as well as the development of mathematical probabilistic model for the minutiae distortion. To analyze the distribution of characteristics and the errors that occur during fingerprint processing we use the database [17]. We also use SourceAFIS package [18,19] as the main tool for fingerprint processing.

The results of analysis made allowed us to identify the following main factors that lead to differences in several portraits of the same fingerprint: - geometric center displacements caused by a change in the position of the object in the scan field; - rotation of images arising for the same reasons; - "erasure" or the appearance of "false" minutiae due to incorrect settings of the scanner algorithm or the entry of foreign objects in the scanning field; - drifting of the relative location of minutiae due to errors in the recognition algorithm.

Let us consider in detail each type of distortion, we will investigate the most significant factors for possible modeling of fingerprint minutiae distortions.

2 The modeling of geometric center displacement error

These errors occur due to inaccuracy of the location of the scan object relative to the center of the scan field. To describe the distribution of such errors, it is advisable to use the unimodal trapezoidal centered probability density function (PDF) of the form:

$$\Phi\left(d_y\right), \Phi\left(d_x\right) = \begin{cases} 12.5 \cdot d_x + 3.75 & if \quad -0.3 \le d_x < -0.1; \\ 2.5 & if \quad -0.1 \le d_x \le 0.1; \\ -12.5 d_x + 3.75 & if \quad 0.1 < d_x \le 0.3; \\ 0 & if \quad \left|d_x\right| > 0.3. \end{cases} \quad (1)$$

We use the inverse function method.

If *z*:*unif* $[0,1]$, then to obtain a random variable d_x with distribution (1) it is necessary to use the transformation:

$$d_x(z)=\begin{cases}\sqrt{0.16\cdot z}-0.3 & if\ \ 0\le z<0.25;\\ 0.4\cdot z-0.2 & if\ \ 0.25\le z\le 0.75;\\ -\sqrt{0.16\cdot(1-z)}+0.3 & if\ \ 0.75<z\le 1.\end{cases} \quad (2)$$

It is fair to assume that displacement errors having the PDF (2) act independently on the coordinates X, Y of the unit fingerprint portrait.

The correctness of the transformation (2) is illustrated by a histogram of the computational experiment results in Fig. 1.

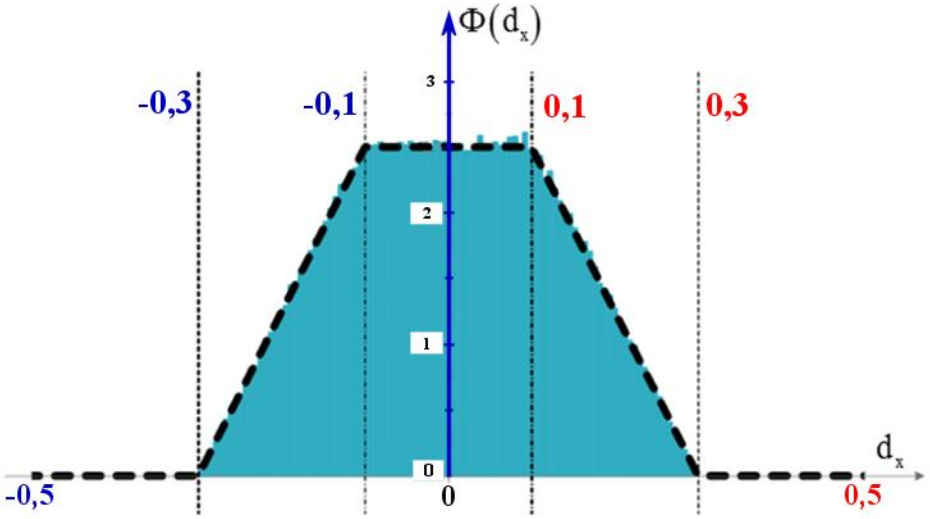


Fig. 1 – Result of statistical tests of the random coordinate error generator

3 The modeling of minutiae erasure and false appearance minutiae errors

The distribution of erasure errors can be parametrized by the value p_E - the erasure probability of a single individual characteristic point on the fingerprint portrait. Assuming the independence of erasure errors, their distribution can be described by the usual discrete binomial distribution:

$$P_E(k)=\sum_{i=0}^{k}\binom{i}{N}\cdot {p_E}^{i}\cdot(1-p_E)^{N-i}, \quad (3)$$

where $P_E(k)$ - the probability of erasure is not more than k minutiae of the portrait; N - the number of minutiae detected, determined by the distribution

$$Q(N_i)=\binom{i}{30}\cdot\left(\frac{1}{2}\right)^{30},\ i\in[0,30], N_i\in[15,45],$$

where $Q(N_i)$ is the probability that the number of minutiae of the portrait (*taking into account minutiae masked outside the unit square*) will be a value N_i.

The size of the parameter p_E for various methods of fingerprint processing, in our opinion, can be located within. $0<p_E\le 0.1$. To simulate the erasure process after obtaining the portrait model (Table 1), using a random generator which is uniformly distributed in a unit number interval, the vector $Z=\{z_1,z_2,\cdots,z_N\}$ is generated, the elements of which z_i:*unif* $[0,1]$, $i=1\ldots N$.

On the basis of the vector Z, an erasure vector $E=\{e_1,e_2,\cdots,e_N\}$ is calculated whose elements have a binary value and are obtained by a functional transformation of the vector coordinates Z:

$$e_i=\left\lfloor\frac{z_i}{1-p_E}\right\rfloor,\quad e_i=[0,1],\ i=1\ldots N. \tag{4}$$

Next, the rows in the portrait table (Table 1), which have numbers that correspond to the ordinal numbers of the unit vector E elements, are removed from the table and, accordingly, from the portrait of minuses.

We base the probabilistic description of the errors associated with the false minutiae appearance on Poisson distribution:

$$\Pr(K)=\frac{\lambda_A{}^K}{K!}e^{-\lambda_A} \tag{5}$$

where $\Pr(K)$ - probability of K false minutiae appearance on the portrait sample; λ_A - an empirically determined mathematical expectation of the false minutiae number.

Table. 1 – Portrait matrix

№	X	Y	φ	№	X	Y	φ
1	0.21	-0.07	0.6	**15**	0.01	0.39	0.15
2	0.28	0.18	0.58	**16**	-0.05	-0.55	0.08
3	0.12	-0	0.49	**17**	0.51	0.5	0.64
4	0.19	0.31	0.74	**18**	-0.25	-0.34	0.55
5	0.07	-0.68	0.62	**19**	0.23	-0.41	0.41
6	0.05	-0.12	0.8	**20**	0.13	-0.41	0.47
7	-0.25	0.33	0.58	**21**	0.14	0.08	0.15
8	-0.01	0.42	0.91	**22**	0.06	0.23	0.74
9	0.17	0.15	0.73	**23**	-0.05	0.17	0.83
10	0.12	0.23	0.67	**24**	0.69	0.31	0.87
11	0.3	0.54	0.32	**25**	0.1	0.7	0.3
12	0.64	-0.14	0.31	**26**	-0.33	-0.3	0.13
13	0.13	0.44	0.11	**27**	-0.17	-0.11	0.78
14	0.09	-0.05	0.85	**28**	0.15	0.08	0.61

Approximation of a random variable - the number of false minutiae in a portrait subject to the Poisson distribution (5) is achieved using a random generator $unif[0,1]$ and a conventional binomial distribution as follows. Based on the statistical processing of a sufficient number of portraits, the mathematical expectation of the number of false minutiae in one portrait λ_A is determined empirically. As a rule, $0.1\le\lambda_A\le 0.5$ (in this case, minutiae additions tend to occur less likely than erasures). A vector is generated with elements uniformly distributed in the unit interval $z_i\sim unif[0,1],\ i=1\ldots M$. Then, on the basis of a transformation similar to (4), we get an addition vector $A=\{a_1,a_2,\cdots,a_M\}$ of binary elements obtained according to:

$$a_i=\left\lfloor\frac{z_i}{1-\frac{\lambda_A}{M}}\right\rfloor,\quad a_i=[0,1],\ i=1\ldots M. \tag{6}$$

The number of unit elements in the vector is subject to the binomial law (3) with the parameter $P_E=\frac{\lambda_A}{M}$. Then the number of added false minutiae of the portrait is determined by the square of

the length of the vector A:

$$K = |A|^2 = \sum_{i=1}^{M} a_i . \quad (7)$$

The approximation of the Poisson distribution (5) will be all the more accurate the larger the selected value M. For an acceptable approximation of the Poisson distribution given $\lambda_A \ll 1$, it suffices to require following inequality:

$$M \geq \lambda^{-1}. \quad (8)$$

The simulation of the appearance of false minutiae is made on the basis of the value obtained as a result of the computational experiment, determined by (7): table 1 adds K rows (when $K = 0$ rows are not added). The generation of values for the added rows is the same as for existing points in the table - using $z \sim unif[0,1]$. This does not exclude the case when additional points will be outside the unit square and will be disguised on the original portrait.

4 The modeling of image rotation errors

To model rotation errors, we accept the following conventions for the Cartesian coordinate system of the unit square of the fingerprint portrait.

Portrait image rotation around the geometric center of the unit square with coordinates $[0,0]$ is conveniently modeled by rotating the coordinate axes on the plane by a specified angle α (Fig. 2).

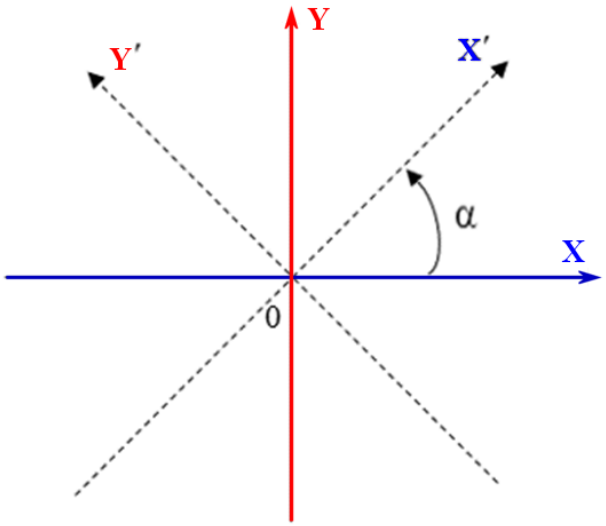


Fig. 2 – Rotation illustration

The zero value of the rotation angle corresponds to the axis $0X$; the positive direction of the angle is the counterclockwise movement. It should be borne in mind that turning the axes by an angle α is equivalent to rotating the original image (*in $X\ 0\ Y$ coordinates*) in the opposite direction by an angle $-\alpha$ (in $X'0Y'$ coordinates). It is known that the relationship between the coordinates of an arbitrary point $\begin{pmatrix} X \\ Y \end{pmatrix}$ in the original coordinate system $X\ 0\ Y$ and the coordinates of the new point $\begin{pmatrix} X' \\ Y' \end{pmatrix}$ in the system $X'0Y'$ deployed at the angle α is given in the matrix form by the following expression:

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = U(\alpha) \cdot \begin{pmatrix} X \\ Y \end{pmatrix},$$

where

$$U(\alpha) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}. \quad (9)$$

Using the transformation (9) allows you to define an algorithm for modeling the image rotation. Let G – be the portrait matrix (Table 1) of the size $(N \times 3)$. We divide it into submatrices

$G=\left(XY\|\varphi\right)$, where XY is a submatrix of the size $\left(N\times 2\right)$, containing N rows with a pair of coordinates X and Y for each of the N points of the original portrait; φ – is a vector column containing the angle values for N corresponding points normalized in the interval $\left[0,1\right]$.

The rotation of portrait minutiae by an angle (given in radians) is achieved by transforming the submatrix: XY:

$$XY'=U\left(-\alpha\right)\cdot\left(XY\right)^{T}, \tag{10}$$

where $\left(XY\right)^{T}$ – transposed submatrix XY.

The change in the vector φ associated with the rotation of the portrait is determined by the formula:

$$\varphi'=\left(\varphi-\frac{\alpha}{2\cdot\pi}\right)\bmod 1-\left\lfloor\left(\varphi-\frac{\alpha}{2\cdot\pi}\right)\bmod 1\right\rfloor, \tag{11}$$

where the operation $\left("\arg"\right)\bmod 1$ extracts the fractional part of "arg", with respect to the sign.

The matrix of the portrait rotated by the angle α is determined by combining the resulting submatrix and the vector:

$$G'=\left(\left(XY'\right)^{T}\|\varphi'\right). \tag{12}$$

Rotation errors are determined by the distribution of the random rotation angle α. Empirical considerations allow us to limit the range of possible values within a right angle

$$\alpha\in\left[-\frac{\pi}{4},+\frac{\pi}{4}\right], \tag{13}$$

and to show the requirements of unimodality and centering to the PDF. To simulate a random value α, we use a method based on the central limit theorem and allows us to approximate a truncated normal distribution by summing a limited number of centered random numbers uniformly distributed in a single range. We use the approximation of the normal distribution by summing the four linearly transformed random variables z_i:$unif\left[0,1\right]$, $i\in 1,\ldots,4$. The restriction (13) corresponds to the normalized values, then the realization of the random normalized rotation angle is obtained by a functional transformation of the form:

$$\alpha_H=\sum_{i=1}^{4}\left(\frac{z_i-0.5}{16}\right). \tag{14}$$

The approximated normal PDF has the form:

$$f\left(\alpha_H\right)=\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{{\alpha_H}^2}{2\sigma^2}\right),\ \sigma=\sqrt{\frac{1}{3\cdot 256}}. \tag{15}$$

In Fig. 3 shows the form of the function (15) (dashed line) and the histogram of the probability distribution of the approximation (14) obtained with the number of tests equal to 10^5.

As can be seen, the use of only four terms in the sum of expression (14) provides a good approximation of the normal PDF.

The absolute value of the random angle of rotation does not exceed the limits specified above $\pm 45^{o}$, and the RMS value is

$$\sigma=\sqrt{\frac{1}{3\cdot 256}}\cdot 360^{o}=0.036\cdot 360^{o}\approx 13^{o}.$$

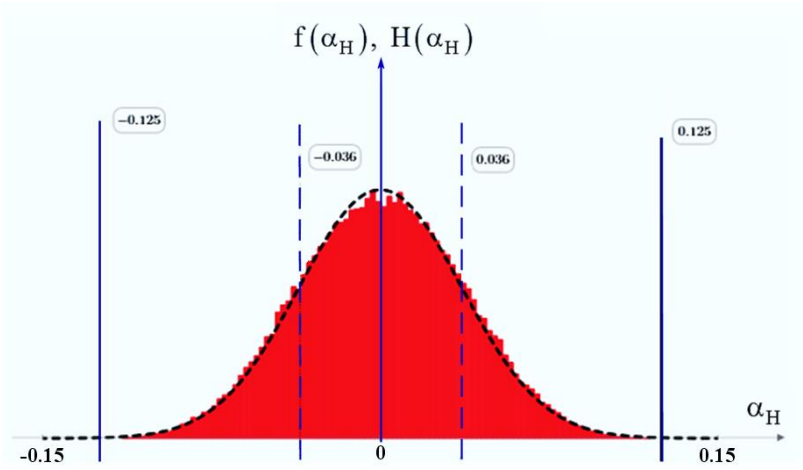


Fig. 3 – PDF and histogram of the approximation of the PDF of the normalized random rotation angle

Thus, as a result of the studies, this section based on the analysis of the experimental data of biometric fingerprint images developed an analytical probabilistic model for the formation and processing of minutiae that takes into account various quantitative and qualitative characteristics (*the density of minutiae distribution and linear displacements of the fingerprint center, the possibility of loss and / or appearance of new minutiae, the presence of angular errors, etc.*). The developed model allows us to generalize and formalize the process of minutiae generation, as well as to justify theoretical suggestions and recommendations for their processing in computerized access control systems.

5 Conclusions

Biometric authentication methods are being widely used in modern computerized access control systems. At the heart of their construction lies the processing of control points of various biometric images (*the iris of the eye, the outline of the face, the hand, papillary lines, etc.*). The analysis showed that the most widely used methods of processing fingerprint control points (minutiae), allowing reliably identifying a specific user and implementing various security services.

The proposed analytical probability model of minutiae distortions takes into account various quantitative and qualitative characteristics (*the density of minutiae distributions and linear displacements of the fingerprint center, the distribution of the minutiae angles, the possibility of loss and / or appearance of new minutiae, the presence of angular errors, etc*.). This allows us to generalize and formalize the process of minutiae generation, in order to be used in computerized access control systems and in other important applications [20-21].

References

[1] Recognizing faces with PCA and ICA / Draper B.A., Baek K., Bartlett M.S., Beveridge J.R. Computer Vision and Image Understanding. 2003. Issue 91. P. 115–137.
[2] How should we represent faces for automatic recognition? / Craw I., Costen N.P., Kato T., Akamatsu S. IEEE Trans. Pat. Anal. Mach. Intel. 1999. Issue 21. P. 725–736.
[3] Xiang C., Fan X.A., Lee T.H. Face recognition using recursive Fisher linear discriminant. Communications, Circuits and Systems. 2004. Vol. 2. P. 27–29.
[4] ISO/IEC 19794-5. Information technology – Biometric data interchange formats – Part 5: Face image data.
[5] Daugman J. How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology.2004. Vol. 14, №1. P. 21–30.
[6] Architecture of a Search Engine for Massive Comparison in an Iris Biometric System / Liu-Jimenez J., Sanchez-Reillo R., Lindoso A., Daugman J.G. Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology. Lexington, KY, 2006. P. 103–108.
[7] Person identification technique using human iris recognition / Christel-Loic T., Lionel M., Lionel T., Michel R. Proc. of Vision Interface. 2002. P. 294–299.
[8] ISO/IEC 19794-6. Information technology – Biometric data interchange formats – Part 6: Iris image data.

[9] Handbook of Fingerprint Recognition / Maltoni D., Maio D., Jain A.K., Prabhakar S. New York: Springer, 2003.
[10] Xudong Jiang, Wei-Yun Yau. Fingerprint minutiae matching based on the local and global structures. Proceedings 15th International Conference on Pattern Recognition. ICPR-2000. Barcelona, 2000 Vol. 2. P. 1038–1041.
[11] A real-time matching system for large fingerprint databases / Ratha N. K., Karu K., Chen Sh., Jain A. K. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1996. Vol. 18, №8. P. 799–813.
[12] ISO/IEC 19794-2. Information technology – Biometric data interchange formats – Part 2: Finger minutiae data.
[13] ISO/IEC 19794-3. Information technology – Biometric data interchange formats – Part 3: Finger pattern spectral data.
[14] ISO/IEC 19794-4. Information technology – Biometric data interchange formats – Part 4: Finger image data.
[15] Privacy Enhancing Technologies for Biometric Data. 2015. URL: http://www.cs.haifa.ac.il/~orrd/PrivDay/2015/
[16] Privacy Enhancing Technologies for Biometric Data. 2016. URL: http://www.cs.haifa.ac.il/~orrd/PrivDay/
[17] FVC2004. Fingerprint Verification Competetion. Databases. URL: http://bias.csr.unibo.it/fvc2004/databases.asp
[18] SourceAFIS for Java and .NET. URL: https://sourceafis.machinezoo.com/
[19] SourceAFIS Fingerprint recognition library for .NET and experimentally for Java. URL: https://sourceforge.net/projects/sourceafis/
[20] Rusyn B., Prudyus I., Ostap V. Fingerprint image enhancement algorithm. The Experience of Designing and Application of CAD Systems in Microeletronics. Proceedings of the 6th International Conference. CADSM. 2001. P. 193–194.
[21] A new method of fingerprint key protection of grid credential / Varetskyy Y., Rusyn B., Molga A., Ignatovych A. Advances in Intelligent and Soft Computing. 2010. Vol. 84. P. 99–103.

Рецензент: Сергій Толюпа, д.т.н., проф., Київський національний університет імені Т. Шевченка, Київ, 03189, Україна. E-mail: tolupa@i.ua

Надійшло: Жовтень 2018.

Автори:

Сергій Рассомахін, д.т.н., зав. кафедри Безпеки інформаційних систем і технологій, Харківський національний університет ім. В. Н. Каразіна, майдан Свободи 6, Харків, 61022, Україна. E-mail: rassomakhin@karazin.ua

Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 6, Харків, 61022, Україна. E-mail: kuznetsov@karazin.ua

Володимир Шлокін, директор Інноваційного центру, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи, 6, Харків, 61022, Україна. E-mail: vshlokin@ukr.net

Анна Уварова, провідний інженер, Конструкторське бюро «Південне» ім. М.К. Янгеля», вул. Криворізька 3, Дніпро, 49008, Україна. E-mail: annet.uvarova@gmail.com

Математична модель спотворення відбитків пальців.

Анотація. Дана стаття включає в себе дослідження біометричних зображень відбитків пальців, мінуцій та математичної імовірнісної моделі їх спотворення. Запропонована модель заснована на евристичному аналізі результатів сканування відбитків пальців з урахуванням характеру потенційних помилок. Вона дозволяє моделювати типову поведінку мінуцій в біометричних зображеннях відбитків пальців. Були змодельовані найбільш типові типи спотворень, включаючи зміщення геометричного центру відбитка пальця, обертання відбитка пальця, видалення дрібних деталей, а також зміни відстані між мінуціями.

Ключові слова: біометрична аутентифікація; зображення відбитків пальців; мінуції.

Рецензент: Сергей Толюпа, д.т.н., проф., Киевский национальный университет имени Т. Шевченко, Киев, 03189, Украина. E-mail: tolupa@i.ua

Поступила: Октябрь 2018.

Авторы:

Сергей Рассомахин, д.т.н., зав. кафедры Безопасности информационных систем и технологий, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина. E-mail: rassomakhin@karazin.ua

Александр Кузнецов, д.т.н., проф., Академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина. E-mail: kuznetsov@karazin.ua

Владимир Шлокин, директор Инновационного центра, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы, 6, Харьков, 61022, Украина. E-mail: vshlokin@ukr.net

Анна Уварова, ведущий инженер, Конструкторское бюро «Южное» им. М.К. Янгеля», ул. Криворожская 3, Днепр, 49008, Украина. E-mail: annet.uvarova@gmail.com

Математическая модель искажения отпечатков пальцев.

Аннотация. Данная статья включает в себя исследование биометрических изображений отпечатков пальцев, минуций и математической вероятностной модели их искажения. Предложенная модель основана на эвристическом анализе результатов сканирования отпечатков пальцев с учетом характера потенциальных ошибок. Она позволяет моделировать типичное поведение минуций в биометрических изображениях отпечатков пальцев. Были смоделированы наиболее характерные типы искажений, включая смещение геометрического центра отпечатка пальца, вращение отпечатка пальца, удаление мелких деталей, а также изменение расстояния между минуциями.

Ключевые слова: биометрическая аутентификация; изображения отпечатков пальцев; минуции.

УДК 004.056

АВТОМАТИЗОВАНИЙ ПОШУК ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІЗ ЗАСТОСУВАННЯМ МЕТОДІВ ГЛИБИННОГО НАВЧАННЯ

Кирило Чернов[1], Єгор Єрьомін[1], Марія Попова[1], Олексій Шаповал[1], Євген Котух[2]

[1] Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
kirillfilippsky@gmail.com, suvenick2@gmail.com, mariia.popova26@gmail.com, alex.shapoval@protonmail.com

[2] Університет митної справи та фінансів, вул. Володимира Вернадського 2/4, Дніпро, 49000, Україна
yevgenkotukh@gmail.com

Reviewer: Олександр Оксіюк, д.т.н., проф., Київський національний університет імені Т. Шевченка, вул. М. Ломоносова 81, Київ, 03189, Україна.
o.oksiuk@gmail.com

Надійшло: Листопад 2018.

Анотація: *Наведено теоретичну інформацію про тестування програмного забезпечення методом фаззінгу. Розглянуто технології навчання з підкріпленням та використання інтелектуального фаззінгу в процесі тестування програмного забезпечення. Описано алгоритм, за допомогою якого реалізуються зазначені методи та технології. Запропоновані статистичні результати досліджень, які були проведені під час тестування деяких програм та утиліт, призначених для повсякденного використання, а також програми, розробленої студентами.*

Ключові слова: *фаззінг; тестування; навчання з підкріпленням; Q-learning.*

1 Аналіз літератури та постановка задачі дослідження

Фаззінг – це метод тестування програмного забезпечення та відкритого коду на наявність вразливостей безпеки шляхом повторного тестування з подачею вхідних даних, що мутовані [1]. Повторне тестування проводиться методом випадкових мутації та майже завжди час, за який проводилось тестування, не є оптимальним. В цій роботі розглянуто проблему інтелектуального фаззінгу та методи її вирішення [7]. Основною метою авторів є розробка технології, що може орієнтуватися та приймати відповідні рішення, посилаючись на досвід, отриманий безпосередньо під час проведення тестування. Для рішення цього питання використано технологію машинного навчання, а саме навчання з підкріпленням (Reinforcement learning) за алгоритмом deep Q-learning [6], який реалізує максимально можливу винагороду, визначену в процесі розробки, використовуючи аналіз вихідних даних програми та доступні винагороди. Це дозволяє застосовувати оптимальні мутації вхідних даних. Таким чином, агент отримує можливість навчитися формувати оптимальну політику дій для отримання максимальної винагороди. В межах даної роботи пропонується алгоритм і відповідна комп'ютерна модель процесу фаззінгу із застосуванням глибинного навчання, та проводяться дослідження ефективності автоматизованого пошуку вразливостей у порівняні із тестуванням методом випадкової мутації. При проведенні тестування застосовується метод «чорного ящика», тобто інформація, яку ми маємо під час тестування, представляє собою лише результат роботи програми та вхідні дані, які їй необхідні для виконання [1].

2 Алгоритм інтелектуального фаззінгу

При проведенні дослідження ми прийшли до формування такої проблеми процесу фаззінгу: при випадковій генерації вхідних даних використовуваний час не є оптимальним, адже виконується процедура звичайного перебору варіантів. Їх може бути дуже багато, в результаті чого на вхід подається величезна кількість мутацій, які не приносять користі для процесу тестування. Оскільки процес фаззінгу представляє собою виконання циклу задач в визначеній середі (програмі), де на її вхід подається послідовність, яка пройшла деяку операцію му-

тації, ідеальним варіантом для вирішення подібної проблеми є технологія машинного навчання – навчання з підкріпленням (*Reinforcement learning*). Кращим прикладом використання такого алгоритму є програма AlphaGO, що розроблена компанією Google DeepMind в 2015 році. Вона стала першою в світі програмою, яка виграла партію в гру "го" у професіонала вищого рангу Лі Седоля [2].

Поєднавши фаззінг та навчання з підкріпленням, в результаті ми отримали систему, що здатна формувати правила вибору визначеної мутації. Вона подає на вхід мутовані дані і в залежності від вихідних даних програми формує нагороду для того, щоб при подальшому тестуванні спиратися на власний досвід та вибирати оптимальні мутації для конкретного випадку. Таким чином кількість мутації, що не несуть внеску в процес тестування, значно зменшиться. Це в свою чергу, як очікується, прискорить тестування. Схема розробленої системи представлена на рис. 1.

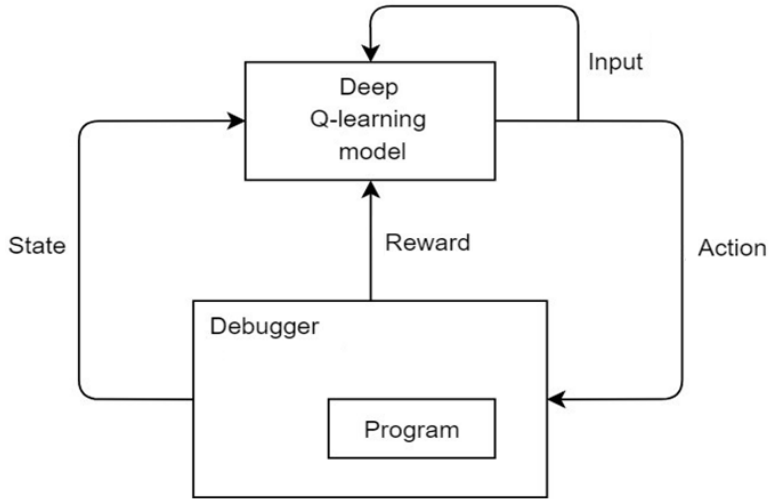


Рис. 1 – Схема алгоритму інтелектуального фаззінгу

Процес тестування починається з визначення початкових не мутованих вхідних даних. Формат залежить від типу фаззінгу. Сформовані пакети подаються на вхід програми, а за допомогою спеціальних засобів дебаггінгу визначається реакція програми. З отриманих даних (*це може бути час виконання програми, покриття коду, код завершення програми та ін*.) формується стан системи State, який, в разі необхідності, підлягає попередній обробці та подається в обробленому вигляді на вхід Deep Q-learning model, що в свою чергу приймає рішення про дію Action, котру слід прийняти наступною. В цей самий час, залежно від вибраної дії та отриманого стану програми, формується нагорода Reward для алгоритму. За допомогою винагороди алгоритм розуміє поставлене йому задачу і в процесі навчання визначає оптимальну поведінку для її виконання. Також алгоритм запам'ятовує дії які принесли йому максимальну нагороду для досягнення поставленої мети *(знаходження помилки, вивід програми з ладу, та ін*.), та в подальших раундах тестування, на власному досвіді, вирішує яку дію слід вчинити. При розрахунку наступної дії попередні вхідні дані підлягають мутації відповідно до дії, яку було вибрано. На вхід програми подаються вже "нові" мутовані дані. Ця процедура повторюється до дих пір, поки алгоритм не досягне поставленої йому цілі. Запропонована модель використовує Марківський процес прийняття рішень, а якщо більш точніше, то – deep Q-learning [3].

3 Навчання з підкріпленням (*Reinforcement learning*)

Навчання з підкріпленням – це обчислювальний підхід розуміння та автоматизації цілеспрямованого навчання і прийняття рішень. Він відрізняється від інших відомих алгоритмів машинного навчання тим, що агент навчається безпосередньо при взаємодії з середовищем, не посилаючись на зразкові приклади [3]. Цей алгоритм, перш за все, спрямований на вирі-

шення труднощів, які виникають при взаємодії з середовищем для досягнення довгострокових дій. Він використовує формальну структуру Марківського процесу прийняття рішень [3], визначення взаємодії між агентом і середовищем з точки зору станів, дій та нагород. Зазначені особливості включаються до себе розуміння причин та наслідків, а також наявність чітких цілей. При цьому, поняття цінності та функції цінності є основними ознаками методів навчання з підкріпленням.

Як було зазначено раніше, взаємодія агента з середовищем може бути розглянута, як Марківський процес прийняття рішень $M = (S, A, P)$, де S – набір станів системи, A – набір дій, P – множина перехідних ймовірностей. Для кожної пари стан – дія $(s, a) \in S \times A$, множина P це набір ймовірностей $P(s' \vee s, a)$, де s' це наступний стан системи. Тоді агент, розглядаючи можливі стани системи при вибраній дії, де кожному переходу відноситься своя нагорода $r(s, a)$, вивчає оптимальну поведінку, яка максимізує нагороду.

Під час процесу навчання основною метою алгоритму є максимізація кінцевої суми нагород:

$$R = \sum_{t=0}^{\infty} \gamma^t r_{t+1},$$

де $\gamma \in (0,1)$ – коефіцієнт знижки, що визначає пріоритет винагороди з плином часу. Вибір дії a_t при стані s_t визначається політикою дії $a_{t\pi}(\vee s_t)$. Політика π прикріпляє розглянуті можливі стани до дій, що в свою чергу визначає поведінку агенту.

Нехай очікувана кумулятивна нагорода для агенту, який слідкує політиці π визначається як:

$$Q^{\pi}(s, a) = E\left[\sum_{t=0}^{\infty} \gamma^t r_{t+1} \vee s_0 = s, a_0 = a\right].$$

Тоді проблему знаходження оптимального значення $Q_{\pi}(s, a)$ можна звести до процедури апроксимації функції. Для досягання цього необхідно лише оновлювати $Q_{\pi}(s, a)$ після кожної ітерації отримання нагороди [4]. Це визначається як

$$Q(s_t, a_t) = Q(s_t, a_t) + \alpha,$$

де α – швидкість навчання (*learning rate*).

Всю процедуру можна записати в такій послідовності: агент отримує стан s_t, приймає дію $a_t = \arg\max(Q(s_t, a))$, що визначає нагороду r_t, та спричиняє перехід системи в стан $s_t + 1$. Отримуючи нагороду r_t та стан $s_t + 1$, агент визначає кращу можливу дію $a_t + 1 = \arg\max(Q(s, a))$. Далі він оновлює значення $Q(s_t, a_t)$.

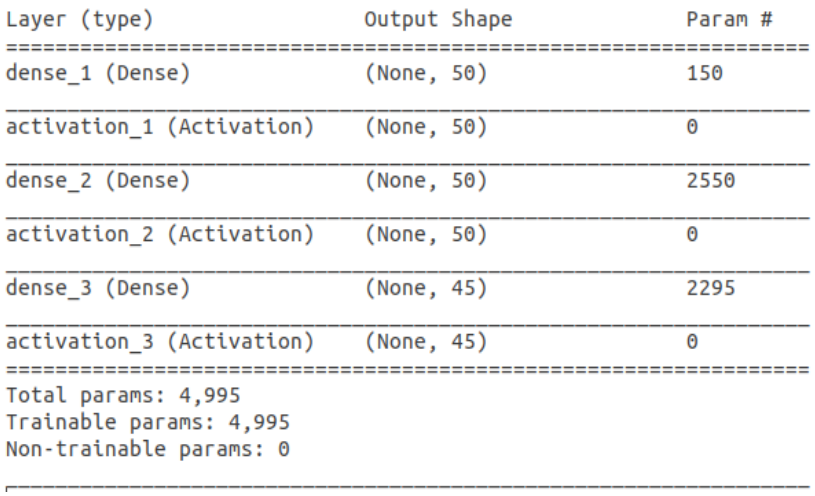
Для апроксимації функції $Q(s_t, a_t)$ використовуються глибокі нейронні мережі (*чим і визначається назва deep Q-learning*), де в свою чергу, метою є мінімізація функції втрати:

$$L = (r + \gamma \cdot \max(Q(s_t + 1, a_t)) - Q(s_t, a_t)^2.$$

4 Результати моделювання

Було змодельоване процес запуску програмного забезпечення, що піддається тестуванню, і розроблено спеціальні логічні тести, в яких програма повертала код помилки при визначених вхідних даних для порівняння роботи фаззінгу з допомогою штучного інтелекту та без нього. Можливі стани системи представляються у вигляді даних, що формуються при завершенні програми. Далі ці дані передаються нейронній мережі, яка складається з одного вхідного шару, двох прихованих шарів по 50 нейронів кожний та функції активації *(Rectified Linear Unit)*: $f(x) = \max(0, x)$. Вихід нейронної мережі має 45 елементів, що представляють собою кількість можливих мутацій.

Повна схема нейронної мережі для апроксимації функції $Q(s_t, a_t)$, представлена на рис. 2.



Layer (type)	Output Shape	Param #
dense_1 (Dense)	(None, 50)	150
activation_1 (Activation)	(None, 50)	0
dense_2 (Dense)	(None, 50)	2550
activation_2 (Activation)	(None, 50)	0
dense_3 (Dense)	(None, 45)	2295
activation_3 (Activation)	(None, 45)	0

Total params: 4,995
Trainable params: 4,995
Non-trainable params: 0

Рис. 2 – Схема нейронної мережі

Навчання мережі здійснено за допомогою алгоритму градієнтного спуску Adam [4].

Нехай $f(\theta)$ – шумна цільова функція: стохастична скалярна функція, що є диференційованою відносно параметру θ. Ми зацікавлені в мінімізації очікуваної вартості цієї функції, $E\left[f(\theta)\right]$ відносно параметру θ. За допомогою $f_1(\theta),\ldots,f_T(\theta)$ позначаємо реалізацію стохастичної функції в наступних кроках $1,\ldots,T$. Стохастичність може виходити від оцінки на випадкових підмножинах (міні-група) точок даних або від шуму функції. При $g_t = \nabla_\theta f_t(\theta)$ ми позначаємо градієнт, тобто вектор часткових похідних f_t відносно θ, який оцінюється за часом t. Алгоритм оновлює експоненціальні рухливі середні значення градієнту (m_t) та квадрату градієнту (v_t), де гіперпараметри $\beta_1, \beta_2 \in [0,1]$ контролюють експоненціальні швидкості розкладання цих рухливих середніх. Самі рухливі середні – оцінки першого моменту (*середнє значення*) і другого моменту (*не центрована дисперсія*) градієнта. Проте ці рухливі середні ініціюються як вектори нулів, що призводить до оцінки моментів, котрі зміщуються у напрямку до нуля, особливо в початкових часових кроках, та коли показники розкладання невеликі (наприклад, значення β_s близьке до 1). Корисна якість полягає в тому, що цієї упередженості ініціалізації можна легко запобігти, отримуючи виправлені помилки m_{bt} та v_{bt}.

Структура алгоритму, що розглядається, представлена нижче.

Необхідні вхідні дані:

- α : Швидкість навчання
- $\beta_1, \beta_2 \in [0,1)$: Експоненціальні показники розпаду для оцінок моменту (стандартні налаштування $\beta_1 = 0.9, \beta_2 = 0.999$)
- $f(\theta)$: Стохастична функція з параметром θ
- θ_0 : Вектор початкових параметрів

Алгоритм:

$m_0 \leftarrow 0$ (*Ініціалізувати перший вектор моменту*)

$v_0 \leftarrow 0$ (*Ініціалізувати другий вектор моменту*)

$t \leftarrow 0$ (*Ініціалізувати час*)

while θ_t не зійшлась:

$t \leftarrow t+1$

$g_0 \leftarrow \nabla\theta f_t(\theta_t - 1)$ (*Взяти градієнт відносно стохастичної функції під час* t)

$m_t \leftarrow \beta_1 \bullet m_t - 1 + (1 - \beta_1) \bullet g_t$ (*Оновити відхилену оцінку першого моменту*)

$v_t \leftarrow \beta_2 \bullet v_t - 1 + (1 - \beta_2) \bullet g_{2t}$ (*Оновити відхилену оцінку другого моменту*)

$m_b t \leftarrow \frac{m_t}{1 - \beta_{t_1}}$ (*Обчислити виправлену оцінку першого моменту*)

$yb_t \leftarrow \frac{y_t}{1 - \beta_{t_2}}$ (*Обчислити виправлену оцінку другого моменту*)

$\theta_t \leftarrow \theta_t - 1 - \alpha \bullet \frac{mb_t}{\sqrt{vb_t}}$ (*Оновити параметри*)

end while

return θ_t (*Розраховані параметри*)

Мутації вхідних даних були вибрані на основі стандартного списку: збільшення та зменшення довжини рядка, цілочисленні вставки, додавання спеціальних символів (наприклад, "%s", який також може викликати помилки). Було створено 45 функцій і поміщено до словнику для їх подальшого використання.

Нагороду система отримувала, якщо час виконання системи був більшим за попередній та при виникненні помилок під час тестування. При знаходженні помилки алгоритм закінчує роботу. При формуванні такого типу нагороди ми зіткнулися з проблемою, коли алгоритм вже знайшов одну помилку, почав її викликати кожного разу за для отримання максимальної нагороди. Щоб уникнути цієї проблеми ми встановили дві константи: $\gamma \in (0,1)$ – коефіцієнт знижки та $\varepsilon \in (0,1)$ – швидкість розвідки. Про першу константу вже було зазначено раніше. Друга константа визначає наскільки алгоритм буде здатен до відкриття нових рішень, тобто з вірогідністю ε буде вибрана випадкова дія, а з вірогідністю $1 - \varepsilon$ буде вибрана максимально вигідна дія.

Гіпотеза – наукове припущення, що висувається для пояснення будь-якого явища і потребує перевірки на досліді та теоретичного обґрунтування для того, щоб стати достовірною науковою теорією [8].

Статистична гіпотеза – будь-яке твердження (припущення), яке стосується вигляду чи параметрів розподілу деякої ознаки досліджуваних об'єктів [8].

Тестування гіпотез проводиться в такій послідовності дій:

1. Здійснюється обчислення певної статистики, розподіл якої відомий.
2. Знаходиться *P-value* для обчислених результатів.
3. Робляться відповідні висновки в залежності від критерію значущості та значенні *P-value*.

Для проведення тестування ми розробили спеціальний тест, в якому була визначена помилка. Гіпотеза нашого експерименту полягає в тому, чи є тестування за допомогою нашого алгоритму швидшим, ніж випадковий вибір дій. Коефіцієнт знижки встановлений 0.9, а швидкість розвідки 0.5. Остання зменшується в 0.99 разів після кожної епохи. Для перевірки гіпотези було використано критерій Ст'юдента [5].

Критерій Ст'юдента – загальна назва класу методів статистичної перевірки гіпотез (*статистичних критеріїв*), заснованих на порівнянні з розподілом Ст'юдента. Найчастіші випадки застосування цього критерію пов'язані з перевіркою рівності середніх значень у двох вибірках [5]. Щоб використовувати цей критерій треба задовольнити деяким умовам: нормальний розподіл початкових даних та рівність дисперсії.

Першою групою були результати тестування за допомогою запропонованого алгоритму, а в іншій групі були результати випадкового вибору мутації. Тестування проводилось в наступній послідовності: генерується 15 експериментів, наприкінці кожного записується кількість

мутацій, яка знадобилася для знаходження помилки. Відповідні результати експериментів представлені в Таблиці 1.

Таблиця 1 – Результати тестування

№	Deep Q-learning model	Випадковий вибір мутації
1	3671	3686
2	1191	1897
3	1879	3164
4	1640	3233
5	1966	10446
6	1585	5358
7	1135	1134
8	4877	752
9	2465	2157
10	3266	3684
11	1895	2026
12	2093	2993
13	1150	295
14	1181	3381
15	1153	358

Результати розрахунку критерію Ст'юдента: $t = -12.40$.

Число степенів свободи дорівнює: $v = 2n - 2 = 2 \times 15 - 2 = 28$.

При критерії значущості $\alpha = 0.01$ та $P - value = 2.763$, оскільки $t < P - value$, наша гіпотеза приймається. Результат є статистично значущим при заданому критерії, якщо, за умови вірності нульової гіпотези, ймовірність випадкового виникнення такого ж або більш екстремального результату менша від заданого рівня (0.01).

5 Висновки

Як свідчать результати експериментів час тестування за допомогою розробленого алгоритму кращий ніж час тестування з використанням випадкових мутацій, навіть за умови, що алгоритм не навчався перед початком проведення експерименту.

Запропонований авторами роботи алгоритм, в його порівнянні з алгоритмом з випадковим тестуванням, знаходить помилку за значно меншу кількість мутацій (2076, проти 2832), та, в середньому, знаходить помилку на 30% швидше.

Посилання

[1] Sutton M., Greene A., Amini P. Fuzzing: Brute Force Vulnerability Discovery. Boston, MA, USA: Addison-Wesley Professional, 2007. URL: https://www.oreilly.com/library/view/fuzzing-brute-force/9780321446114/
[2] AlphaGo Games – English. URL: https://deepmind.com/research/alphago/match-archive/alphago-games-english/
[3] Sutton R.S., Barto A.G. Reinforcement learning: An introduction. MIT press Cambridge, 1998. URL: http://incompleteideas.net/book/bookdraft2017nov5.pdf
[4] Kingma D. P., Ba J. Adam: A Method for Stochastic Optimization. URL: https://arxiv.org/pdf/1412.6980.pdf
[5] t-kryterii Stiudenta. URL: http://fpo.bsmu.edu.ua/static/t-kryteriy-styudenta
[6] Li Yu. Deep Reinforcement Learning: An Overview. URL:https://arxiv.org/pdf/1810.06339.pdf
[7] Böttinger K., Godefroid P., Singh R. Deep Reinforcement Fuzzing. URL: https://arxiv.org/pdf/1801.04589.pdf
[8] Deviniak O. Statystychni hipotezy ta yikh perevirka. 2014. URL: http://stat.org.ua/statclasses/hypotheses-testing/ Deviniak Statystychni hipotezy ta yikh perevirka

Reviewer: Oleksandr Oksiiuk, Doctor of Sciences (Engineering), Full Professor, Taras Shevchenko National University of Kiev 81 Lomonosova St., Kyiv, 03189, Ukraine. E-mail: o.oksiuk@gmail.com

Received on November 2018.

Authors:
Kyrylo Chernov, Student, V. N. Karazin National University, Kharkov, Ukraine.
E-mail: kirillfilippsky@gmail.com
Yehor Yeromin, Student, V. N. Karazin National University, Kharkov, Ukraine.
E-mail: suvenick2@gmail.com
Popova Mariia, Student, V. N. Karazin National University, Kharkov, Ukraine.
E-mail: mariia.popova26@gmail.com
Shapoval Oleksiy, Student, V. N. Karazin National University, Kharkov, Ukraine.
E-mail: alex.shapoval@protonmail.com
Yevgen Kotukh, Ph.D., Associative professor of the Department Cybersecurity of the University of Customs and Finance, Dnipro, Ukraine. E-mail: yevgenkotukh@gmail.com

Automated software vulnerability testing using in-depth training methods.

Abstract. Theoretical information about testing of software using fuzzing method. The technologies of reinforcement training and intellectual fuzzing in the software testing process. An algorithm is described with the help of which the indicated methods and technologies are realized. Statistical results of studies that were conducted during the testing of some programs and utilities intended for everyday use, as well as the program developed by the students are offered.

Keywords: fuzzing; testing; reinforcement learning; Q-learning.

Рецензент: Александр Оксиюк, д.т.н., проф., Киевский национальный университет имени Т. Шевченко, ул. Ломоносова 81, Киев, 03189 Украина. E-mail: o.oksiuk@gmail.com

Поступила: Ноябрь 2018.

Авторы:
Кирилл Чернов, студент, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: kirillfilippsky@gmail.com
Егор Ерёмин, студент,Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: suvenick2@gmail.com
Мария Попова, студент, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: mariia.popova26@gmail.com
Алексей Шаповал, студент, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: alex.shapoval@protonmail.com
Евгений Котух, к.т.н., доцент кафедры кибербезопасности, Университет таможенного дела и финансов, Днепр, Украина.
E-mail: yevgenkotukh@gmail.com

Автоматизированный поиск уязвимостей программного обеспечения с применением методов глубинного обучения.

Аннотация. Приведена теоретическая информация о тестировании программного обеспечения методом фаззинга. Рассмотрены технологии обучения с подкреплением и интеллектуального фаззинга в процессе тестирования программного обеспечения. Описан алгоритм, с помощью которого реализуются указанные методы и технологии. Предложены статистические результаты исследований, которые были проведены во время тестирования некоторых программ и утилит, предназначенных для повседневного использования, а также программы разработанной студентами.

Ключевые слова: фаззинг; тестирование; обучение с подкреплением; Q-learning.

Vesa A. Niskanen
Ph.D., Adjunct Professor,
Department of Economics & Management, University of Helsinki,
P.O. Box 27 (Latokartanonkaari 9), 00014 Helsinki, Finland
E-mail: vesa.a.niskanen@helsinki.fi

Igor Romenskiy
Doktor für physikalische-mathematische Wissenschaften, GFaI Gesellschaft zur Förderung angewandter Informatik e.V.,
Volmerstraße 3, 12489 Berlin, Deutschland
E-mail: iromensky@mail.ru

Alexey Stakhov
Doctor of Sciences (Engineering), Full Professor,
Academicians of the Academy of Engineering Sciences of Ukraine,
International Club of the Golden Section,
6 McCreary Trail, Bolton, Ont., L7E 2C8, Canada
E-mail: goldenmuseum@rogers.com

Vadim Geurkov
Ph.D., Associate Professor,
Department of Electrical and Computer Engineering
Ryerson University,
Victoria St., 350, Toronto, Ontario, M5B 2K3, Canada
E-mail: vgeurkov@ee.ryerson.ca

Fionn Murtagh
Ph.D., Professor,
Department of Computing and Mathematics, University of Derby,
Kedleston Road, Derby DE22 1GB, UK
Email: f.murtagh@derby.ac.uk
Department of Computing, Goldsmiths,
University of London,
New Cross, London SE14 6NW, UK
E-mail: f.murtagh@gold.ac.uk

C. Pandu Rangan
PhD, FNAE, Senior Professor,
Department of Computer Science and Engineering,
Indian Institute of Technology,
Madras, Chennai, 600036, India
E-mail: prangan55@gmail.com

Håvard Raddum
Ph.D.,
Simula Research Laboratory, P.O. Box 134, 1325 Lysaker, Norway
E-mail: haavardr@simula.no

Oleksandr Kazymyrov
Ph.D.,
EVRY Norge AS,
Snarøyveien 30A, Fornebu, 1360, Norway
E-mail: oleksandr.kazymyrov@evry.com

Mikołaj Karpiński
Doctor of Sciences (Engineering), Full Professor,
University of Bielsko-Biala,
Willowa St., 2, 43-309, Bielsko-Biala, Poland
E-mail: mkarpinski@ath.bielsko.pl

Веса А. Нисканен
доктор філософії, ад'юнкт професор,
департамент економіки та менеджменту, Університет Гельсінкі,
Р.О. Бокс 27 (Латокартанонкаарі 9), 00014 Гельсінкі, Фінляндія
E-mail: vesa.a.niskanen@helsinki.fi

Ігор Роменський
доктор фізико-математичних наук,
GFaI - Спілка з просування прикладної інформатики,
Фольмерштрассе 3, 12489 Берлін, Німеччина
E-mail: iromensky@mail.ru

Олексій Стахов
доктор технічних наук, професор, академік Академії інженерних наук України,
Міжнародний Клуб Золотого Перетину,
6 МаккКрері Трейл, Болтон, Онтаріо, L7E 2C8, Канада
E-mail: goldenmuseum@rogers.com

Вадим Геурков
доктор філософії, доцент,
факультет електротехніки та обчислювальної техніки університету Раєрсон, 350 Вікторія-стріт, Торонто, Онтаріо, M5B 2K3, Канада
E-mail: vgeurkov@ee.ryerson.ca

Фінн Мерта
доктор філософії, професор,
факультет обчислювальної математики університету Дербі,
Кедлестон Роад, Дербі DE22 1GB, Великобританія
Email: f.murtagh@derby.ac.uk
факультет обчислень Голдсмітського коледжу Лондонського університету,
Нью-Крос, Лондон SE14 6NW, Великобританія
E-mail: f.murtagh@gold.ac.uk

С. Панду Ранган
доктор філософії, FNAE, старший викладач,
факультет комп'ютерних наук та інженерії Індійського технологічного інституту,
Мадрас, Ченнаї - 600036, Індія
E-mail: prangan55@gmail.com

Ховард Радум
доктор філософії,
науково-дослідна лабораторія Симула, Р.О. Бокс 134, 1325, Лісакер, Норвегія
E-mail: haavardr@simula.no

Олександр Казіміров
доктор філософії,
EBPI Норге АС,
Снаройвиен 30А, 1360 Форнебу, Норвегія
E-mail: oleksandr.kazymyrov@evry.com

Микола Карпінський
доктор технічних наук, професор,
Університет Бельсько-Бяла,
вул. Віллова 2, 43-309 Бельсько-Бяла, Польща
E-mail: mkarpinski@ath.bielsko.pl

Volodymyr Khoma
Doctor of Sciences (Engineering), Full Professor,
Institute «Automatics and Informatics», The Opole University of Technology,
Prószkowska St., 76, 45-758, Opole, Poland
E-mail: xoma@wp.pl

Joanna Świątkowska
Ph.D., CYBERSEC Programme Director,
Senior Research Fellow of the Kosciuszko Institute,
Feldmana St., 4/9-10, 31-130, Kraków,
Poland
E-mail: joanna.swiatkowska@ik.org.pl

Nick Bilogorskiy
Director of Security Research,
Cyphort, 5451 Great America Parkway, Suite 225,
Santa Clara, California, 95054, USA
E-mail: nick@novaukraine.org

Richard Kemmerer
Ph.D., Professor,
Computer Science Department, University of California,
Santa Barbara, California, 93106, USA
E-mail: kemm@cs.ucsb.edu

Dimiter Velev
Ph.D., Professor,
Department of Information Technologies and Communications, Faculty of Applied Informatics and Statistics, University of National and World Economy,
„8-ми декември“ St., UNSS - Studentski grad, 1700
Sofia, Bulgaria
E-mail: dgvelev@unwe.bg

Robert Brumnik
Ph.D., Professor Assistant,
GEA College, Dunajska cesta 156, 1000 Ljubljana, Slovenia
Metra Engineering Ltd, Špruha 19, 1236 Trzin, Slovenia
E-mail: robert.brumnik@metra.si

Stephan Dempe
Ph.D., Professor,
Department of Mathematics and Computer Science,
Technical University Bergakademie Freiberg, Germany
Akademischestrafte 6, D-09596, Freiberg,
Germany
E-mail: dempe@math.tu-freiberg.de

Ludmila Babenko
Doctor of Sciences (Engineering), Full Professor,
Institute of Computer Technologies and Information Safety of Southern Federal University
Chekhov St., 2, Taganrog, Rostov obl., Russia
E-mail: blk@tsure.ru

Valerii Zadiraka
Doctor of Sciences (Physics and Mathematics),
Full Professor, Academician of the National Academy of Sciences of Ukraine, Glushkov Institute of Cybernetics (GIC) of National Academy of Sciences of Ukraine,
40 Glushkov Av., Kyiv, 03187, Ukraine
E-mail: zvk140@ukr.net

Володимир Хома
доктор технічних наук, професор,
Інститут «Автоматика та інформатика», Технологічний університет Ополе,
76 Пружовська Вулиця, 45-758 Ополе, Польща
E-mail: xoma@wp.pl

Джоана Святковська
доктор філософії, директор програми CYBERSEC,
старший науковий співробітник Інституту Костюшки
вул. Фельдман 4 / 9-10, 31-130 Краків,
Польща
E-mail: joanna.swiatkowska@ik.org.pl

Нік Білогорський
директор з досліджень безпеки,
Цифорт, 5451 Гріт Америка Парквей, Люкс 225,
Санта-Клара, Каліфорнія 95054, США
E-mail: nick@novaukraine.org

Річард Кеммерер
PhD., професор,
факультет інформатики, Каліфорнійський університет,
Санта-Барбарі, CA 93106, США
E-mail: kemm@cs.ucsb.edu

Дімітер Велев
доктор філософії, професор,
кафедра інформаційних технологій і комунікацій,
факультет прикладної інформатики та статистики,
Університет національної та світової економіки,
вул. "8-ми декември", UNSS - Студентські град, 1700
Софія, Болгарія
E-mail: dgvelev@unwe.bg

Роберт Брумнік
доктор філософії, доцент,
GEA коледж, Дунайська цеста 156, 1000 Любляна, Словенія
Метра Інжиніринг ЛТД, Шпруха 19,1236 Тржин, Словенія
E-mail: robert.brumnik@metra.si

Стефан Демп
доктор філософії, професор,
факультет математики та інформатики, технічний університет Фрайберзької Гірничої Академії, Німеччина
Akademischestrafte 6, D -09596, Фрайберг, Німеччина
E-mail: dempe@math.tu-freiberg.de

Людмила Бабенко
доктор технічних наук, професор,
Інститут комп'ютерних технологій та інформаційної безпеки Південного федерального університету
вул. Чехова 2, Таганрог, Ростовська обл., Росія
E-mail: blk@tsure.ru

Валерій Задірака
доктор технічних наук, професор,
академік Національної академії наук України,
Інститут кібернетики імені В.М. Глушкова Національної академії наук України,
проспект Академіка Глушкова, 40, Київ, 03187, Україна
E-mail: zvk140@ukr.net

Ludmila Kovalchuk
Doctor of Sciences (Engineering), Associate Professor,
Department of mathematical methods of information security Institute of Physics and Technology,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
37, Peremohy Av., Kyiv, 03056, Ukraine
E-mail: lusi.kovalchuk@gmail.com

Людмила Ковальчук
доктор технічних наук, доцент,
кафедра математичних методів захисту інформації фізико-технічного інституту
національного технічного університету України «КПІ»,
03056, Київ, пр. Перемоги, 37, НТУУ "КПІ"
E-mail: lusi.kovalchuk@gmail.com

Anton Alekseychuk
Doctor of Sciences (Engineering), Associate Professor,
Department of application of means of cryptographic and technical defense of information, Institute of Special Communication and Information Security,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
37 Peremohy Av., Kyiv, 03056, Ukraine
E-mail: alex-dtn@ukr.net

Антон Олексійчук
доктор технічних наук, доцент,
кафедра застосування засобів криптографічного та технічного захисту інформації Інституту спеціального зв'язку та захисту інформації національного технічного університету України «КПІ»,
03056, Київ, пр. Перемоги, 37, НТУУ "КПІ"
E-mail: alex-dtn@ukr.net

Volodymyr Maxymovych
Doctor of Sciences (Engineering), Full Professor,
Institute of Computer Technologies, Automation and Metrology (ICTA), Lviv Polytechnic National University,
Bandera St., 12, Lviv, 79013, Ukraine
E-mail: vmax@polynet.lviv.ua

Володимир Максимович
доктор технічних наук, професор,
Інститут комп'ютерних технологій, автоматики та метрології Національного університету
«Львівська політехніка»,
вул. Степана Бандери, 12, м. Львів, 79013, Україна
E-mail: vmax@polynet.lviv.ua

Oleksiy Borysenko
Doctor of Sciences (Engineering), Full Professor,
Sumy State University,
Rymskogo-Korsakova St., 2, Sumy, 40007, Ukraine
Email: 5352008@ukr.net

Олексій Борисенко
доктор технічних наук, професор,
Сумський державний університет,
вул. Римського-Корсакова, 2, 40007 Суми, Україна
E-mail: 5352008@ukr.net

Anatoliy Biletsky
Doctor of Sciences (Engineering), Full Professor,
Institute of Air Navigation, National Aviation University,
Kosmonavta Komarova Av., 1, Kyiv, 03058, Ukraine
Email: abelnau@ukr.net

Анатолій Білецький
доктор технічних наук, професор,
навчально-науковий інститут аеронавігації національного авіаційного університету,
пр. Космонавта Комарова 1, Київ, 03058, Україна
Email: abelnau@ukr.net

Serhii Kavun
Doctor of Sciences (Economics), Ph.D. (Engineering), Full Professor,
Kharkiv University of Technology "STEP",
Malomyasnitska St., 9/11, Kharkiv, 61010, Ukraine
E-mail: kavserg@gmail.com

Сергій Кавун
доктор економічних наук, кандидат технічних наук, професор,
Харківський технологічний університет "ШАГ",
вул. Малом'ясницька, 9/11, м. Харків, 61010, Україна
E-mail: kavserg@gmail.com

Vyacheslav Kharchenko
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, N.Ye. Zhukovskiy National Aerospace University – Kharkiv Aviation Institute (KhAI),
17 Chkalov St., Kharkiv, 61070, Ukraine
E-mail: v_s_kharchenko@ukr.net

В'ячеслав Харченко
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Національний аерокосмічний університет
ім. М. Є. Жуковського,
вул. Чкалова, 17, 61070, м. Харків, Україна
E-mail: v_s_kharchenko@ukr.net

Valentin Lazurik
Doctor of Sciences (Physics and Mathematics),
Full Professor, V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: vtlazurik@karazin.ua

Валентин Лазурик
доктор фізико-математичних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: vtlazurik@karazin.ua

Volodymyr Kuklin
Doctor of Sciences (Physics and Mathematics), Full Professor, V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: kuklinvm1@gmail.com

Володимир Куклін
доктор фізико-математичних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: kuklinvm1@gmail.com

Ivan Gorbenko
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: gorbenkoi@iit.kharkov.ua

Іван Горбенко
доктор технічних наук, професор, академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: gorbenkoi@iit.kharkov.ua

Victor Krasnobayev
Doctor of Sciences (Engineering), Full Professor,
Honourable Inventor of Ukraine,
Honourable Radio Specialist of the USSR,
V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: krasnobayev@karazin.ua

Віктор Краснобаєв
доктор технічних наук, професор, заслужений винахідник України, почесний радист СРСР,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: krasnobayev@karazin.ua

Irina Lisitska
Doctor of Sciences (Engineering), Full Professor,
Corresponding Member of the Academy of Applied Radioelectronics Sciences,
V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: lisitska@karazin.ua

Ірина Лисицька
доктор технічних наук, професор,
член-кореспондент Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: lisitska@karazin.ua

Oleksandr Potii
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: potav@ua.fm

Олександр Потій
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: potav@ua.fm

Viktor Dolgov
Doctor of Sciences (Engineering), Full Professor,
Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: dolgovvi@mail.ru

Віктор Долгов
доктор технічних наук, професор,
академік Академії наук прикладної радіоелектроніки,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: dolgovvi@mail.ru

Roman Oliynikov
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: roliynykov@gmail.com

Роман Олійников
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: roliynykov@gmail.com

Volodymyr Mashtalir
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: mashtalir@kture.kharkov.ua

Володимир Машталір
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: mashtalir@kture.kharkov.ua

Grygoriy Zholtkevych
Doctor of Sciences (Engineering), Full Professor,
V. N. Karazin Kharkiv National University,
Svobody Sq., 4, Kharkiv, 61022, Ukraine
E-mail: g.zholtkevych@karazin.ua

Oleksandr Oksiiuk
Doctor of Sciences (Engineering), Full Professor,
Taras Shevchenko National University of Kiev
Lomonosova St., 81, Kyiv, 03189, Ukraine
E-mail: o.oksiuk@gmail.com

Serhii Toliupa
Doctor of Sciences (Engineering), Full Professor,
Taras Shevchenko National University of Kiev
Lomonosova St., 81, Kyiv, 03189, Ukraine
E-mail: tolupa@i.ua

Григорій Жолткевич
доктор технічних наук, професор,
Харківський національний університет
імені В.Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: g.zholtkevych@karazin.ua

Олександр Оксіюк
доктор технічних наук, професор,
Київський національний університет імені Т. Шевченка
вул. М. Ломоносова, 81, 03189, м. Київ, Україна
E-mail: o.oksiuk@gmail.com

Сергій Толюпа
доктор технічних наук, професор,
Київський національний університет імені Т. Шевченка
вул. М. Ломоносова, 81, 03189, м. Київ, Україна
E-mail: tolupa@i.ua

Статті пройшли внутрішнє та зовнішнє рецензування.

Наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 4(12) 2018

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, російською мовами

Комп'ютерне верстання – Єсіна М.В., Федоренко В.В.

61022, Харків, майдан Свободи, 6
Харківський національний університет імені В.Н. Каразіна

V. N. Karazin Kharkiv National University Publishing

CS&CS

2018