EDITORIAL

"COMPUTATIONAL ASPECTS OF CRITICAL INFRASTRUCTURES SECURITY", "SECURITY AND POST-QUANTUM CRYPTOGRAPHY"

Lead Guest Editor: Alexandr Kuznetsov
Guest Editors: Robert Brumnik, Vyacheslav Kalashnikov, Sergii Kavun

In the recent years, a large amount of literature on the computational aspects of critical infrastructures security has emerged, much of it focusing on cryptography, cyber, informational and economical security, theory, methods, approaches and algorithms associated with certain classes of such problems. The topic proposed to treat in this special issue goes one jump further in attempting to deal with computational aspects of critical infrastructures security. Such classes of critical infrastructures security problems often arise in engineering, computing and software applications: robotics, Internet of things, different environments control problems, approaches and techniques applied to all types of information and communication technologies, and so forth.

Last but not least, a lot of new applied problems in the area of computational aspects of critical infrastructures security have recently arisen that can be efficiently solved only by the new scientific methods, approaches and algorithms. Among them there are informational and economical security problem, designing of encryption algorithms with consideration known attacks analysis problems, symmetric ciphers problems, highly practical and commercial importance of security, safety and protection R&D, and so forth, even if we mention only part of such applications or approaches. Computational aspects of critical infrastructures security models to describe informational and economical processes are also the most popular new themes in the area of critical infrastructures security.

The primary purpose of the special issue is to discuss these problems with the researchers working in this and in adjacent areas, scientific and practical problems of information and economic security of different countries.

This special issue at the International Scientific Journal of Computing includes selected invited papers presented at the scientific seminars of cybersecurity departments of V.N. Karazin Kharkiv National University and Taras Shevchenko National University (Ukraine), as well as 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2019), which was held in Metz, France, September 18-21, 2019. The discussion of research results was attended by leading scientists in the field of computer science and cybersecurity from Mexico, Poland, Slovenia, Georgia, Kazakhstan, Ukraine, Russia, China and many other countries.

The article "*Data Errors Control in the Modular Number System Based on the Nullification Procedure*" by ***Victor Krasnobayev, Sergey Koshman, Sergey Moroz, Vyacheslav Kalashnikov, Vitaliy Kalashnikov*** is devoted to the study of computationally effective methods for error control using operations in the system of residue classes.

Error control in the modular number system is a non-positional operation. It requires development of special methods, designed to increase the efficiency of this procedure. This method is designed to verify the correct implementation of the computing process of computer systems and components. It is assumed that error in one module remainder does not affect the residue values corresponding to other modules (bases) of the modular number system. The essence of the proposed method is that, when performing the procedure of zeroing in the modular number system, operation of determining is combined in time. This makes it possible to increase the efficiency of information control, presented in the modular number system. In addition, the use of arithmetic calculations in the system of residue classes makes it possible to ensure not only error control, but also to increase the reliability of computer calculations, fault tolerance, and survivability, including during implementing cryptographic means of protecting information.

The article "*Combining and Filtering Functions in the Framework of Nonlinear-Feedback Shift Register*" by ***Alexandr Kuznetsov, Oleksandr Potii, Nikolay Poluyanenko, Oleksii Smirnov, Igor Stelnyk, Danylo Mialkovsky*** is devoted to the study of new directions in the field of symmetric stream ciphers. In particular, in this paper, we study methods for constructing nonlinear-feedbacks shift registers, evaluate their main characteristics and cryptographic indicators.

Strong cryptography of stream ciphers is determined according to the ability of the generated

pseudorandom sequence to resist analytical attacks. One of the main components of the pseudorandom stream cipher sequence generating algorithm is Boolean functions for combining and filtering. The paper considers the possibility of applying nonlinear-feedback shift registers that generates a maximum length sequence as a combining or filtering function. The main indicators of cryptographic resistance of such functions as: balance, the prohibitions presence, correlation immunity and nonlinearity are examined in this work. The study analyzes and demonstrates correlation immunity and nonlinearity experimental values for all nonlinear feedback shift registers that generates a maximum length sequence, for register sizes up to 6 cells inclusively, and register sizes up to 9 cells inclusively with algebraic degree of the polynomial under 2. The possibility of optimizing the process of selecting Boolean functions according to the criteria of maximum correlation immunity and nonlinearity with various algebraic degrees and minimization of the number of monomials in the polynomial is studied. These results will undoubtedly be useful in substantiating the basic cryptographic elements of promising symmetric ciphers, which function reliably even in the case of using quantum methods of cryptographic analysis.

The article "*Properties and Formation of OFDM and Derived Signals*" by ***Alexander Zamula, Vladyslav Morozov, Nataliya Kalashnykova, Robert Brumnik*** is devoted to the improvement of mobile communication technologies with increased reliability and security indicators, using the latest advances in coding theory, complex discrete signals and cryptography. The article discusses the technologies of generating signals used in mobile, information and telecommunication systems, and also provides an analysis of promising technologies that can be used in wireless communication systems of broadband access. It is shown that the widely used modulation scheme with orthogonal frequency division (OFDM) has a number of drawbacks, which can lead to a decreasing in the system performance. Alternative technologies for generating signals are presented, in particular, a technology based on windowed signal processing (W-OFDM), a technology based on time division (w-OFDM); UFMC technology and others to eliminate the disadvantages of OFDM technology. New points of view are proposed on the use of multi-carrier transmission technology in the form of multiplexing with orthogonal frequency division (in order to increase the security of modern wireless broadband access communication systems from external and internal threats), a class of non-linear discrete cryptographic sequences to form a physical data carrier – signal. This new direction, proposed by the authors, develops in their recent works, and it is associated with the use of the latest achievements in cryptography to solve applied problems of generating pseudo-noise sequences and using them to generate complex discrete signals.

The article "*Optimization of Lifetime in Wireless Monitoring Networks*" by ***Yuliia Kovalova, Tetyana Babenko, Oleksandr Oksiiuk, Larysa Myrutenko*** is devoted to modeling wireless telecommunication monitoring networks with autonomous power sources. This direction has been very actively developing in recent years, and it is used in various applied problems, for example, for monitoring traffic safety and production, for monitoring the functioning of public utilities, agriculture, etc. One of the basic requirements for the construction of a wireless monitoring network with autonomous power supply is the guaranteed network lifetime. Up-to-date challenges in the field of wireless monitoring networks are creation of universal hardware platforms that allow for usage of widespread proprietary transceivers of different manufacturers aiming at creating network topologies raising energy efficiency and lifetime of WMN. The article describes a model of a wireless network allowing evaluation of its lifetime by energy parameters and dynamic reconfigurations induced by external influence. On the basis of the represented test results one may conclude that energy consumption is defined by the level of the application stack of the protocol ZigBee and doesn't depend on PHY and MAC layers of the protocol 802.15.4. Considering energy consumption of the data transmission process, potential increase in the lifetime of the devices and network as a whole is mostly controlled by the sizes of useful messages.

The article "*Differential Cryptanalysis of the Lightweight Block Cipher Cypress-256*" by ***Mariia Rodinko, Roman Oliynykov, Khalicha Yubuzova*** presents the results of studies of the effectiveness of one of the options for constructing lightweight (low-resource) block symmetric ciphers. The authors continue the cycle of their articles on the Cypress-256 block cipher which was developed by them. This crypto primitive refers to low-resource algorithms that are in demand in various fields, for example, for implementing security mechanisms on the Internet of things, when using RFID tags, building simple and cheap devices, etc.

This paper presents the results of differential cryptanalysis of the lightweight block cipher Cypress-256. It is proposed the searching method for multi-round differential characteristic of the block cipher Cypress-256. The searching assumes 1) building a big set of one-round differential characteristics and search for possible combinations of one-round characteristics into multi-round ones;

2) extending one-round differential characteristics with the probability up to certain threshold into multi-round characteristics. The following experiments show that the most probable one-round differential characteristics have input differences with 4-6 active bits which are distributed between different words. Besides that, high-probable one-round differential characteristics, which output differences have a small Hamming weight, cannot be extended to build high-probable multi-round differential characteristics. Due to application of the method assuming extension of one-round differential characteristics into multi-round ones, the differential characteristic up to 6 rounds was built, so 10-round block cipher Cypress-256 is resistant to differential cryptanalysis according to the requirements of practical criterion.

The article "*Detection Method of the Probable Integrity Violation Areas in FPGA-Based Safety-Critical Systems*" by ***Kostiantyn Zashcholkin, Oleksandr Drozd, Yulian Sulima, Olena Ivanova, Ihor Perebeinos*** explored hardware security issues, in particular, studied methods to counter a Hardware Trojan (HT). A HT is a malicious modification of the circuitry of an integrated circuit. A hardware Trojan is completely characterized by its physical representation and its behavior. The payload of an HT is the entire activity that the Trojan executes when it is triggered. In general, malicious Trojans try to bypass or disable the security fence of a system: it can leak confidential information by radio emission. HT's also could disable, derange or destroy the entire chip or components of it. In this article the features of integrity monitoring of FPGA-based safety-critical systems are considered. Hardware Trojans are distinguished as one of the most dangerous types of malicious integrity violation of FPGA-based systems. The study has proved that Hardware Trojans can be implanted into the system (or system project) during its planned modification. In particular, it happens when the integrity monitoring, based on the hash sum usage, does not operate. Before running the integrity monitoring, one should ensure that Hardware Trojans were not implanted. Authors proposed the method for detecting the hardware Trojans location in the space of FPGA-based components of safety-critical systems. The method is based on the analysis of addressing to the values of calculated LUT units for these components in the normal and emergency modes of system operation. The hardware module for addressing the registration in accordance with the proposed method is implemented.

The article "*Fuzzy Recurrent Mappings in Multiagent Simulation of Population Dynamics Systems*" by ***Dmytro Chumachenko, Oleksandr Sokolov, Sergiy Yakovlev*** explores population modeling. This is an important area of research, especially in the context of modern challenges and threats caused by overpopulation of the planet, as well as the possible spread of global infectious diseases (pandemics). The article links global security issues with the complex tasks of describing, modeling and predicting the size of a population. The paper deals with the problems of analyzing multi-agent models of population dynamics. The problems studied are caused by a number of uncertainties associated with variables, boundary conditions, initial states, parameter values, etc. To solve this problem, a linguistic fuzzy model which allows describing systems of population dynamics in a more realistic way, has been developed. Population dynamics is described by a set of rules, each of which involves entry and exit in the form of fuzzy sets or fuzzy functions, which are applied iteratively. The complexity of describing the processes of population dynamics systems, the presence of fuzzification and defuzzification algorithms, and the use of fuzzy sets and linguistic variables make it necessary to develop new methods for analyzing such systems. The approaches proposed in the article to the study of systems of population dynamics make it possible to apply a unified description of processes of different nature in the form of a production set of rules.

The article "*Studies on Practical Cryptographic Security Analysis for Block Ciphers with Random Substitutions*" by ***Berik Akhmetov, Sergiy Gnatyuk, Vasyl Kinzeryavyy, Khalicha Yubuzova*** explores the techniques of cryptanalysis of symmetric ciphers. Today theory of analysis and security verification of block ciphers with fixed substitution nodes against linear and differential cryptanalysis (LDC) is developed. There are also symmetric block ciphers with substitution nodes defined by round keys. Random substitution nodes improve security of ciphers and complicate its cryptanalysis. But through it all, quantitative assessment is an actual and not simple task as well as the derivation of formulas for practical security verification for block ciphers with random substitution nodes against LDC. In this paper analytical upper bounds of parameters characterized practical security of symmetric block ciphers with random substitution nodes against LDC were given. These assessments generalize known analogs on block ciphers with random substitution nodes and give a possibility to verify security improving against LDC. By using the example of block cipher Kalyna-128, it was shown that random substitution nodes using allows to improve upper bounds of linear and differential parameters average probabilities in 246 and 290 times respectively. The study is novel in that it is one of the few in the cryptology field to calculate analytical upper bounds

of BC practical security against LDC methods as well as to show and prove that using random substitutions allows to improve upper bounds of linear and differential parameters. The security analysis using quantitative parameters gives possibility to evaluate various symmetric block ciphers or other cryptographic algorithms and their ability to provide necessary and sufficient security level in information and communication systems.

Thus, this collection of articles presents topics in the areas of "Computational Aspects of Critical Infrastructures Security", "Security and Post-Quantum Cryptography". Hope this will be an interesting for reading!

Prof. Alexandr Kuznetsov
V. N. Karazin Kharkiv National University,
Svobody sq., 6, Kharkiv, 61022, Ukraine
kuznetsov@karazin.ua

Prof. Vyacheslav Kalashnikov
Tecnológico de Monterrey,
Eugenio Garza Sada av. 2501,
64849 Monterrey, Nuevo León, México,
kalash@itesm.mx

Dr. Robert Brumnik
GEA College,
Dunajska cesta 156, 1000 Ljubljana, Slovenia
brumnik.robert@gmail.com

Prof. Sergii Kavun
Kharkiv University of Technology "STEP",
Malom'yasnitska st. 9/11,
61010, Kharkiv, Ukraine,
kavserg@gmail.com