ISSN 2519-2310

COMPUTER SCIENCE AND CYBERSECURITY

ISSUE 2(2) 2016

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 2(2) 2016

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 (June 24, 2016, protocol No. 8)

Editor-in-Chief:
Azarenkov Mykola, Karazin Kharkiv National University, Ukraine

Deputy Editors:
Kuznetsov Alexandr, Karazin Kharkiv National University, Ukraine
Rassomakhin Serghii, Karazin Kharkiv National University, Ukraine

Secretary:
Malakhov Serghii, Karazin Kharkiv National University, Ukraine

Editorial board:
Alekseychuk Anton, National Technical University of Ukraine "Kyiv Polytechnic Institute", Ukraine
Alexandrov Vassil Nikolov, Barcelona Supercomputing Centre, Spain
Babenko Ludmila, Southern Federal University, Russia
Biletsky Anatoliy, Institute of Air Navigation, National Aviation University, Ukraine
Bilogorskiy Nick, Cyphort, USA
Borysenko Oleksiy, Sumy State University, Ukraine
Brumnik Robert, GEA College, Metra Engineering Ltd, Slovenia
Dolgov Viktor, V. N. Karazin Kharkiv National University, Ukraine
Geurkov Vadim, Ryerson University, Canada
Gorbenko Ivan, V. N. Karazin Kharkiv National University, Ukraine
Iusem Alfredo Noel, Instituto Nacional de Matemática Pura e Aplicada (IMPA), Brazil
Kalashnikov Vyacheslav, Tecnológico University de Monterrey, México
Karpiński, Mikołaj University of Bielsko-Biala, Poland
Kavun Sergii, Kharkiv Educational and Research Institute of the University of Banking, Ukraine
Kazymyrov Oleksandr, EVRY Norge AS, Norway
Kemmerer Richard, University of California, USA
Kharchenko Vyacheslav, Zhukovskiy National Aerospace University (KhAI), Ukraine
Khoma Volodymyr, Institute «Automatics and Informatics», The Opole University of Technology, Poland
Kovalchuk Ludmila, National Technical University of Ukraine "Kyiv Polytechnic Institute", Ukraine
Krasnobayev Victor, V. N. Karazin Kharkiv National University, Ukraine
Kuklin Volodymyr, V. N. Karazin Kharkiv National University, Ukraine
Lazurik Valentin, V. N. Karazin Kharkiv National University, Ukraine
Lisitska Irina, V. N. Karazin Kharkiv National University, Ukraine
Mashtalir Volodymyr, V. N. Karazin Kharkiv National University, Ukraine
Maxymovych Volodymyr, Lviv Polytechnic National University, Ukraine
Murtagh Fionn, University of Derby, University of London, UK
Niskanen Vesa A., University of Helsinki, Finland
Oliynikov Roman, V. N. Karazin Kharkiv National University, Ukraine
Potii Oleksandr, V. N. Karazin Kharkiv National University, Ukraine
Raddum Håvard, Simula Research Laboratory, Norway
Rangan C. Pandu, Indian Institute of Technology, India
Romenskiy Igor, GFaI Gesellschaft zur Förderung angewandter Informatik e.V., Deutschland
Stakhov Alexey, International Club of the Golden Section, Canada
Świątkowska Joanna, CYBERSEC Programme, Kosciuszko Institute, Poland
Velev Dimiter, University of National and World Economy, Bulgaria
Watada Junzo, The Graduate School of Information, Production and Systems (IPS), Waseda University, Japan
Zadiraka Valeriy, Glushkov Institute of Cybernetics of National Academy of Sciences of Ukraine, Ukraine
Zholtkevych Grygoriy, V. N. Karazin Kharkiv National University, Ukraine

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

Published articles have been internally and externally peer reviewed

© V.N. Karazin Kharkiv National University, publishing, design, 2016

TABLE OF CONTENTS

Issue 2(2) 2016

UDC 681.3.04

CONCEPTION OF REALIZATION OF CRIPTOGRAPHIC RSA TRANSFORMATIONS WITH USING OF THE RESIDUE NUMBER SYSTEM

Viktor Krasnobayev[1], Alina Yanko[2], Sergey Koshman[3]

[1] V. N. Karazin Kharkiv National University, Svobody sq.,4, Kharkov, 61022, Ukraine
krasnobayev@karazin.ua

[2] Poltava National Technical Yuri Kondratyuk University, Pershotravnevyi av. 24, Poltava, 36011, Ukraine
al9_yanko@ukr.net

[3] Kharkov National Technical University of Agriculture named after Peter Vasylenko, Artyoma st., 44, Kharkiv, 61002, Ukraine
s_koshman@ukr.net

Reviewer: 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
Email: goldenmuseum@rogers.com

Received on May, 2016

Abstract: *The methods of rapid information processing aimed to reduce the time of realization of cryptographic RSA transformations are propounded in the paper. These methods are based on application of the principle of ring shift (PRS) in the module number system (MNS). MNS application, from point of view of increasing the speed of realization of cryptographic transformations with the open key, proves to be effective in organizing the process of realization of module integer arithmetic operations.*

Keywords: *specialized digital devices and systems, base of non-position number system, modular number system, cryptographic transformations.*

1 Introduction

Currently modern cryptotransformations with the open key are based on transformations of algebraic curves (elliptic curves (EC), hyper elliptic curves (HEC), Picard curves (PC) and superelliptic curves (SEC)) as well as on RSA systems [1-3]. The existing trend of development of cryptographic methods of information processing is aimed to increase the keys length that, in turn, results in decreasing the speed of cryptographic transformations with the open key. It is especially crucial for providing the set level of resistance during realization of cryptotransformations on EC in the special systems and devices with existing limitations in memory size and mass sizes, i.e. in those cases, where it is impossible to utilize powerful computers with many digits. This status determines the importance and actuality of development of methods of efficiency increasing, reliability and validity of cryptotransformations [4-5].

2 Sources of authors' research

The analysis of methods of increasing of efficiency of SC in Jacobean of HEC allows to ground theoretically and practically the dependence of efficiency of realization of operations of SC in Jacobean of HEC on the bulk of the following basic characteristics: the type of realization of cryptotransformations (software, hardware or software and hardware); the type of algorithm of SEC divisors; the set base field upon which this curve is set above; the type of curve; values of curve coefficients; the selected system of coordinates, in which divisors of Jacobean of HEC (affinor, projective, weighted and mixed) are presented; the accepted method of arithmetic transformations in Jacobean etc. The known methods of realization of algorithms of SEC (Kantor method of divisors addition, Koblits method, methods of arithmetic transformations of divisors in Jacobean of HEC of

© Krasnobayev V., Yanko A., Koshman S., 2016

the second, third and fourth type, methods of addition of divisors of different weight, Karatsuba method for modular multiplication and reduction in the field of polynominal functions, (the method based on some results of the "Chinese Theorem of Remainders" etc.) do not always meet the requirements of efficiency of cryptotransformations. Meantime, efficiency of application of codes of modular arithmetic, i.e. the modular number system (MNS), is highly appreciated in literature [6-7] for solving certain tasks of rapid digital information processing (tasks solving of digital filtration, tasks of realization FFT, DPF etc.).

3 Actual state of the problem and objectives of research

Mentioned above confirms the importance and actuality of development of methods and means for increasing the efficiency, especially of RSA cryptotransformations on the basis of application of MNS. It is connected with the fact that RSA system offered in 1977 is considered to be the most widely used cryptosystem with the open key at present [5,8].

The objective of the paper is to develop the method of rapid realization of cryptographic transformations with the open key, as well as the structural diagram of operating device (OD) of the special processor of cryptographic information processing (SPCIP) on the basis of MNS application.

According to [7], the influence of basic properties (independence, equality, and low digits existence of remainders presenting an operand) of MNS upon the structure and principles of functioning of SPCIP in MNS is examined. It is emphasized that low digits existence of remainders in presentation of digits in modular arithmetic enables a great choice of variants of system and technical solutions during realization of integer modular arithmetic operations.

It is known that there are four principles of realization of arithmetic operations in MNS: the principle of summation (on the basis of low digits of binary adders in modulus m_i of MNS); tabular principle (on the basis of the use of ROM); direct logical principle of realization of arithmetic operations based on description and realization of module operations at the level of the systems of switch functions, due to which the values of results of module operations are formed (it is better to utilize systole and programmable logical matrices as an element base for technical realization of this principle, as well as PLD); principle of ring shift (PRS) based on the application of ring shift registers (RSR).

The lack of process of transfer between digit remainders presented in MNS (inside the very remainder in modulus m_i between binary digits transfers exist) in the operands processed in SPCIP in the process of cryptotransformations (during realization of module operations) on the basis of PCC is one of main and the most attractive features of MNS.

4 Applied method of problem solving

In positional number system (PNS), implementation of arithmetic operation needs the sequential processing of digits of operands due to the rules determined by the content of this operation, and it can not be completed until the values of all of intermediate results, with taking into account of all connections between digits, are subsequently determined.

Thus PNS, in which information is obtained and processed in modern SPCIP, has the substantial gap – it has interdigital connections which affect the methods of realization of arithmetic operations, it needs complicated equipment, reduces validity of calculations, and restrict the speed of realization of cryptographic transformations. Therefore, the development of arithmetic which could be characterized by the lack of connections between digits is required. In this case MNS appears to be attractive. The given non-position number system possesses the significant property of independence of remainders from each other according to the accepted system of base. This independence offers wide opportunities in the construction of not only new machine arithmetic but also the principally new scheme of SPCIP realization, which in turn, extends increasingly the application of machine arithmetic.

According to many literary sources, the introduction of non-traditional methods of information

presenting and processing in digital systems with parallel structure is considered to be one of the means in increasing the efficiency of computer use, particularly, in so-called modular number systems which has maximum level of internal parallelism in the process organization of information processing. The MNS is referred to these systems.

5 General approach to task solving

We will consider the existing pre-conditions of the effective application of modular number system as the SPCIP system. They are as follows: - in SPCIP, digit information processing, like in MNS, is done only with integer numbers; - in SPCIP realization only of module arithmetic operations is performed; - realization of integer module arithmetic operations in SPCIP is performed in a positive numerical range; - basic operations during realization of RSA cryptosystem (more than 95%) are the operations of module multiplication and the operation of numbers squaring in modulus m_i is the most effective (from the point of view of performance speed of module arithmetic operations) realized in MNS; - due to increasing the length of one computer word l (the number of computer digits, (embedded processor, processor node) of cryptosystem), which is a special feature of modern development trend of SPCIP of RSA system, efficiency of application of MNS rises; - wide use of RSR in SPCIP during realization of RSA cryptotransformations; - the gap of the problem solving in PNS of essential increase of efficiency and reliability of SPCIP; - positive preliminary results of MNS efficient application for increasing the use efficiency and SPCIP reliability of the real time.

According to findings [9], the principle of realization of integer arithmetic operations is formulated in MNS, i.e. the PRS, which is characterized by a special feature – the result of arithmetic operation $(a_i \pm b_i) \bmod m_i$ with any in modulus m_i of MNS by determined set of base $\{m_j\}$ $(j = \overline{1,n})$, is determined without the calculation of values of sizes of partial sums S_i and values C_i of transfers of binary address in PNS, but only whereby the cycle shifts of the set digital structure. Indeed, the famous Cayley theorem establishes isomorphism between the elements of eventual abelian group and the elements of the group of transpositions.

It is deduced from Cayley theorem that the influence of elements of abelian group upon the group of all integer numbers is homomorphous. This case allows to organize the process of determination of the result of arithmetic operations in MNS by means of the application of PRS. So, an operand in MNS appears to be a set of *n* remainders $\{a_i\}$ formed by the successive division of initial number *A* to *n* of prime in pairs numbers $\{m_i\}$, for $(i = \overline{1,n})$. In this case the aggregate of remainders $\{m_i\}$ is directly equates with the sum *n* of Galois simple fields of this kind $\sum_{i=1}^{n} GF(m_i)$.

Due to the method of realization of arithmetic operations in MNS it is convenient and sufficient to consider a variant for the arbitrary eventual Galois field $GF(m_i)$ when $i = const$, i.e. for the concrete defined system of residues mod m_i. Application of mentioned above properties allows to realize the operations of module addition and subtraction in MNS whereby PRS by means of *n* ring $M = m_i([\log_2(m_i - 1)] + 1)$, i.e. by bit shift registers.

The arbitrary algebraic system can be presented in the kind of $S = (G, \otimes)$ – where G – is not an empty set; $\oplus$ – is the type of operation, defined for any of two elements a_i, $b_i \in G$. Operation $\oplus$ of addition in the set of classes of subtraction R, caused by the ideal J, forms a new ring called the ring of classes of subtraction R/J. It can be presented in the kind of Z/m_i, where Z – is a great number of integers 0, ±1, ±2,…. (if the base m_i of MNS is a simple number, then Z/m_i is a field). This case determines the possibility of realization of arithmetic operation of addition in MNS without transfers between digits by means of the ring shift of the content of digits.

6 Methods of realization of cryptographic transformations

On the basis of PRS offered in the paper the method of realization of arithmetic operations in MNS is propounded, i.e. the method of binary presentation of remainders (MBPR). Due to this method, the initial digital structure for every modulus (base) m_i of MNS appears to be as the content of the first line (column) of Cayley Table of module addition (subtraction) $(a_i \pm b_i) \bmod m_i$ of the kind presented in Fig. 1.

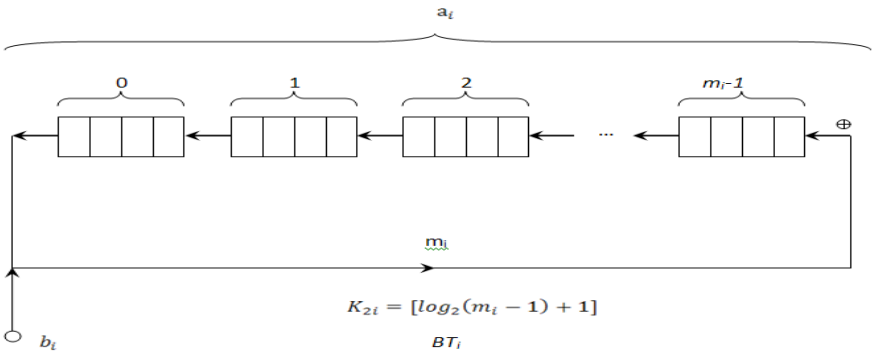


Fig. 1 – Adder in modulus m_i in MNS

Initial digital structure of content of RSR for every in modulus m_i can be presented in the kind of (1),

$$P^{(m_i)} = \left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \| \right] \quad (1)$$

where $\|$ – is the operation of concatenation (joining, agglutination); $P_v(a_v)$ – k-digital binary code which equals the a_v remainder of $(a_v = \overline{0, m_i - 1})$ number in modulus m_i; $k = \left[\log_2 (m_i - 1) + 1 \right]$.

For the set concrete modulus $m_i = 5$, the initial digital structure of content of RSD looks like:

$$P_{\text{init}}^{(5)} = \left[000 \| 001 \| 010 \| 011 \| 100 \right].$$

Thus, by means of used ring shift registers in PNS it is easily to realize arithmetic operations in MNS. So degrees of cyclic transpositions due to (1) are determined by the following formulae:

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \right] = \left[P_z(\alpha_z) \| P_{z+1}(\alpha_{z+1}) \| \ldots \| P_0(\alpha_0) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \right]^Z, \quad (2)$$

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \right]^{-Z} = \left[P_{m_i-1-z}(\alpha_{m_i-1-z}) \| \ldots \| P_{m_i-z}(\alpha_{m_i-z1}) \| \ldots \| \right.$$
$$\left. \| \ldots \| P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-z-2}(\alpha_{m_i-z-2}) \right]. \quad (3)$$

It should be mentioned that $\left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1}) \right]^{m_i} = \varepsilon$, i.e. if $z = m_i$ then all elements of well-organized set $\left\{ P_j(\alpha_i) \right\}$ $(j = \overline{0, m_i - 1})$ remain on its initial position.

During technical realization of this method, the first operand a_i determines the number a_{a_i} digit of $P_{a_i}(a_{a_i})$, with the content of the result of module operation in the modulus m_i, and the second operand b_i determines the number of digits of RSR *($b_i k$ - binary digits)*, which displays how many digits of the RSR content should be shifted (1). Fig. 2 present the chart of possible SPCIP operation device (OD) in MNS.

It is known that time of additional of two remainders $(a_i + b_i) \bmod m_i$ in MNS will be determined by the following mathematical expression:

$$T_{\substack{MNS \\ m_i}}^{(+)} = K_{1i} \cdot K_{2i} \cdot t_{shift}, \quad (4)$$

where: K_{1i} – is a value of the second b_i element in the sum $(a_i + b_i) \bmod m_i$ (the amount of digits of RSR which is subjected in positive (anticlockwise) direction of initial content shift of RSR), i.e $K_{1i} = \overline{0, m_i - 1}$; K_{2i} – is amount of binary digits in one RSR digit on modulus m_i, i.e $K_{2i} = \left[\log(m_i - 1)\right] + 1$; $K_{1i} \cdot K_{2i}$ – is the amount of shifted binary digits in positive direction of binary digits of RSR; $t_{shift} = 3 \cdot \tau_{le}$ – is the time of shift of one binary digit; τ_{le} – is the time of switch of one logical element (element And, OR).

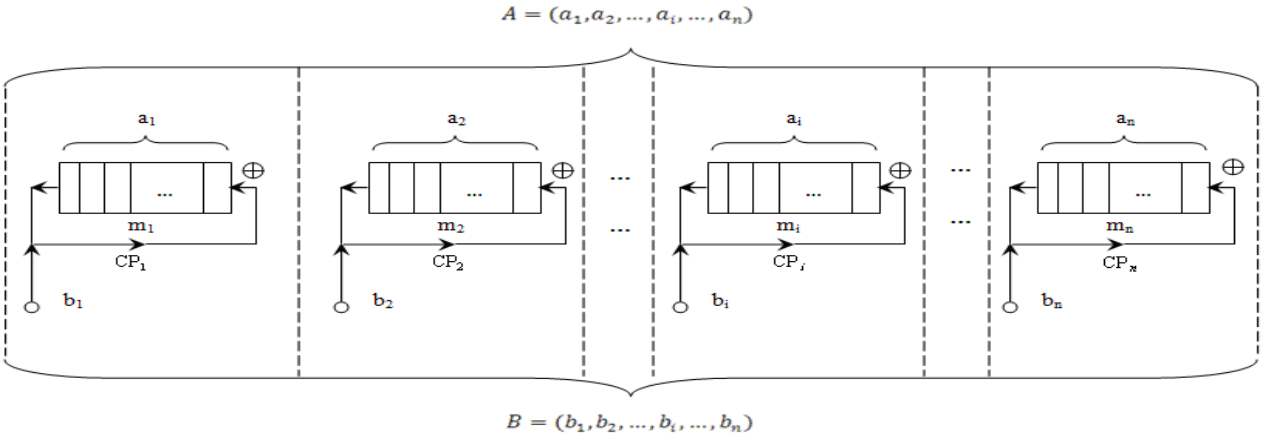


Fig. 2 – Chart of operation device of SPCIP for arbitrary MNS

Thus, for the arbitrary modulus m_i of MNS time of addition of two remainders a_i and b_i in modulus equals

$$T_{\substack{MNS \\ m_i}}^{(+)} = 3 \cdot K_{1i} \cdot \left\{\left[\log_2(m_i - 1)\right] + 1\right\} \cdot \tau_{le}. \quad (5)$$

In this case maximally possible value $T_{\substack{MNS \\ m_i}}^{(+)}$ for the arbitrary module m_i of MNS is equal to

$$T_{\substack{MNS \\ m_i \\ \max}}^{(+)} = 3 \cdot (m_i - 1) \cdot \left\{\left[\log_2(m_i - 1)\right] + 1\right\} \cdot \tau_{le}, \quad (6)$$

but for the given MNS maximal time of addition of two numbers $A = (a_1, a_2, \cdots, a_n)$ and $B = (b_1, b_2, \cdots, b_n)$ equals

$$T_{\substack{MNS \\ m_n \\ \max}}^{(+)} = 3 \cdot (m_n - 1) \cdot \left\{\left[\log_2(m_n - 1)\right] + 1\right\} \cdot \tau_{le}, \quad (7)$$

In general, the time of addition of two numbers $A = (a_1, a_2, \cdots, a_n)$ and $B = (b_1, b_2, \cdots, b_n)$ in MNS is determined by the time $T_{\substack{MNS \\ m_i}}^{(+)}$ of realization of module operation $(a_i + b_i) \bmod m_i$ in computer path (CP_i), i.e. in CIP, for which the case of $K_{1i} \cdot K_{2i} = \max$ is done from all $CP_j (j = \overline{1, n};\ i \neq j)$.

Examples of concrete implementation of operation of addition of two numbers in MNS for one byte $(l = 1)$ processor are propounded. For $l = 1$ MNS base can be as follows: $m_1 = 3$, $m_2 = 4$, $m_3 = 5$ and $m_4 = 7$. The simplified chart of operation device is presented for one byte $(l = 1)$ processor in MNS in Fig. 3.

Example 1. If the second operand is equal to $B = (10,10,100,001)$.

Then:

– for $CP_1(m_1=3)$ we have $b_1=10,\ K_{11}=2,\ K_{21}=\left[\log(m_i-1)\right]+1=2,$ and $K_{11}\cdot K_{21}=2\cdot 2=4$;

– for $CT_2(m_2=4)$ we have $b_2=10,\ K_{12}=2,\ K_{22}=2,$ and $K_{12}\cdot K_{22}=2\cdot 2=4$;

– for $CP_3(m_3=4)$ – $b_3=100,\ K_{13}=4,\ K_{23}=3$ and $K_{13}\cdot K_{23}=4\cdot 3=12$;

– for $CP_4(m_4=7)$ – $b_4=001,\ K_{14}=1,\ K_{24}=3$ – and $K_{14}\cdot K_{24}=1\cdot 3=3.$

It is apparent that the greatest number of shifted binary digits – 12 is occurred in the third computer path $\left(CP_3\right)$.Thus, the time of realization of two numbers *A* and *B* determined in MNS on the basis of the principle of ring shift, can be defined by the value of the second element *B*, and equals

$$T^{(+)}_{\substack{MNS\\ m_3}}=K_{13}\cdot K_{23}\cdot 3\cdot\tau_{le}=12\cdot 3\cdot\tau_{le}=36\cdot\tau_{le}.$$

Example 2. If $B=(10,11,001,001).$ Then we have:

– for $CP_1(m_1=3),\ b_1=2(10),\ K_{11}=2,\ K_{21}=2$ and $K_{11}\cdot K_{21}=2\cdot 2=4;$

– for $CP_2(m_2=4),\ b_2=3(11),\ K_{12}=3,\ K_{22}=2$ and $K_{12}\cdot K_{22}=3\cdot 2=6;$

– for $CP_3(m_3=5),\ b_3=1(001),\ K_{13}=1,\ K_{23}=3$ and $K_{13}\cdot K_{23}=1\cdot 3=3;$

– for $CP_4(m_4=7),\ b_4=1(001),\ K_{14}=1,\ K_{24}=3$ and $K_{14}\cdot K_{24}=1\cdot 3=3.$

Thus, the time of addition of numbers *A* and *B* is determined by the time of realization of operation $(a_2+b_2)\bmod m_2$ in the second expression CP_2 and equals

$$T^{(+)}_{\substack{MNS\\ m_2}}=K_{12}\cdot K_{22}\cdot 3\cdot\tau_{le}=3\cdot 2\cdot 3\cdot\tau_{le}=18\cdot\tau_{le}.$$

The comparative analysis of time of realization of operation of addition of two numbers *A* and *B* in PNS and in MNS is presented. The time $T^{(+)}_{PNS}$ of numbers addition A and B in PNS equals

$$T^{(+)}_{PNS}=(2\cdot\rho-1)t_s=(16\cdot l-1)\cdot 3\cdot\tau_{le},\qquad(8)$$

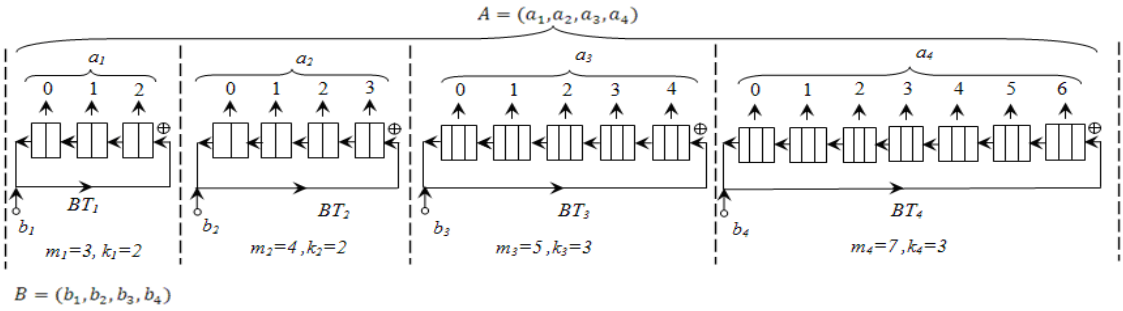


Fig. 3 – Simplified chart of operation device in MNS for one byte (l=1) SPCIP

where: $\rho=8\cdot l\ -\ l$ machine word (number digits of SPCIP for $l=\overline{1,4},8$); $t_s=3\cdot\tau_{le}$ – time of summation in $(i+1)$ binary digit of position adder of values $a_{i+1}+b_{i+1}+c_i$, i.e the time of determination of values C_{i+1} and S_{i+1}.

We take into account that due to existing method of two times reduction of maximum time of operation realization of module addition in MNS, we have for PRS

$$T^{(+)}_{\substack{MNS\\ \max}}=T^{(+)}_{\substack{MNS\\ m_n}}/2.\qquad(9)$$

We will introduce the coefficient α of relation of time of realization of operation of addition in PNS and in MNS, i.e.

$$\alpha=T^{(+)}_{PNS}/T^{(+)}_{\substack{MNS\\ \max}}=\frac{(16\cdot l-1)\cdot 3\cdot\tau_{le}\cdot 2}{(m_n-1)\cdot\left\{\left[\log_2(m_n-1)\right]+1\right\}\cdot 3\cdot\tau_{le}}=\frac{2\cdot(16\cdot l-1)}{(m_n-1)\cdot\left\{\left[\log_2(m_n-1)\right]+1\right\}}.\qquad(10)$$

Calculation and comparative analysis of time of implementation of arithmetic operations at cryp-

tographic transformations proved high efficiency of application of MBPR which is based on application of PCC, as compared to a method, applied in PNS (Table 1).

Table 1 – Data of comparative analysis of time of addition operation

l (ρ)	PNS	MNS			%
	$T_{ПСС}^{(+)} / 3 \cdot \tau_B$	m_n	K	$T_{MCC\ \max}^{(+)} / 3 \cdot \tau_B$	
1 (8)	15	7	3	9	40
2 (16)	31	13	4	24	22

These data are obtained without additional application of existing algorithms, application of which allows to reduce the time of realization of module arithmetic operations. Obtained analytical expressions (4), (5), (6), (7), (9), (10), (13) and the results of time of realization of arithmetic operations in MNS can be used for estimation and comparative analysis of calculable complication of algorithms of RSA of cryptotransformations.

7 Conclusions of research and perspectives

In this paper new methods of speed increasing of realization of cryptographic transformations in Galois fields are studied, in particular, particularly, the increase of efficiency of RSA of cryptotransformations with the open key. These methods are based on the application of PRS in MNS. The application of fundamental theoretical properties of MNS allows to organize effectively the process of realization of module operations in cryptographic tasks. The method of realization of arithmetic operations in MNS based on PRS, i.e. the method of binary presentation of remainders, is propounded for practical use. The analysis of efficiency of application of these methods and examples of concrete technical realization of module arithmetic operations proves their practicability. Given method of information processing is recommended to be practically used in SPCIP of the real time. Results of the research can be successfully applied in the systems and devices for processing enormous digital information of the real time.

Reference

[1] Adibzadeh F. Combination of Multiple Classifiers for Classifying the Diabetic Data/ F.Adibzadeh, M. H. Moradi // Biomedical Soft Computing and Human Sciences. – 2009. - Vol.14. - № 2. - P. 69-80.
[2] Iwase H. Development of General-Purpose Particle and Heavy Ion Transport Monte Carlo Code/H. Iwase, K. Niita, T. Nakamura // Journal of Nuclear Science and Technology. – 2002. - Vol. 39. - №. 11. - P.1142-1151.
[3] Banumathi A. Automated diagnosis and severity measurement of cyst / A. Banumathin et al. // Biomedical Soft Computing and Human Sciences. – 2009. - Vol.14. - № 2. - P. 103-108.
[4] Kasami T. Theory of encoding / T. Kasami, N. Tokura, Y. Ivadari. – M.: Mir, 1978. - 576 p.
[5] Shnaier B. Applied Cryptography. – M.: Triumph, 2002. – 797 p.
[6] Gorbenko I. D. Kriptoanalysis of cryptographic transformations in the groups of points of elliptic curves by the method of Pollarda / I. D. Gorbenko, S. I. Zbitnev, A. A. Polyakov // Radioengineering: All-Ukrainian bulletin of science and engineering. – 2001. - Issue 119. – P. 43-50.
[7] Krasnobayev V. A. Method for Realization of Transformations in Public-Key Cryptography / V. A. Krasnobayev // Telecommunications and Radio Engineering (USA). – 2007. - Vol. 66. - Issue 17. - P. 1559-1572.
[8] Akushskiy I. Ya. Machine arithmetic in remainders classes / I. Ya. Akushskiy, D. I. Yuditskiy. – M.: Soviet Radio, 1968. – 440p.
[9] Kolyada A. A. Modular structures of conveyer method of digital information processing / A. A Kolyada, I. T. Pak. - Minsk: University, 1992. – 256 p.

Рецензент: Олексій Стахов, д.т.н., проф., академік Академії інженерних наук України, Міжнародний Клуб Золотого Перетину, Онтаріо, Канада. E-mail: goldenmuseum@rogers.com

Надійшло: травень 2016.

Автори:
Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: krasnobaev_va@rambler.ru
Аліна Янко, аспірантка, Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна.

E-mail: al9_yanko@ukr.net
Сергій Кошман, к.т.н., доцент, Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна. E-mail: s_koshman@ukr.net

Концепція реалізації криптографічних перетворень RSA з використанням системи залишкових класів

Анотація. У статті представлені методи швидкої обробки інформації, які дозволяють скоротити час реалізації криптографічних RSA перетворень. Розроблені методи ґрунтуються на використанні принципу кільцевого зсуву у модулярній системі числення (МСЧ). Застосування МСЧ дозволило ефективно, з точки зору підвищення швидкодії реалізації криптографічних перетворень з відкритим ключем, організувати процес реалізації модульних цілочислових арифметичних операцій.

Ключові слова: спеціалізовані цифрові пристрої і системи, основа непозиційної системи числення, модулярна система числення, криптографічні перетворення.

Рецензент: Алексей Стахов, д.т.н., проф., академик Академии инженерных наук Украины, Международный Клуб Золотого Сечения, Онтарио, Канада. E-mail: goldenmuseum@rogers.com

Поступила: май 2016.

Авторы:
Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: krasnobaev_va@rambler.ru
Алина Янко, аспирантка, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава, Украина.
E-mail: al9_yanko@ukr.net
Сергей Кошман, к.т.н., доцент, Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков, Украина. E-mail: s_koshman@ukr.net

Концепция реализации криптографических преобразований RSA с использованием системы остаточных классов

Аннотация. В статье представлены методы быстрой обработки информации, которые позволяют сократить время реализации криптографических RSA преобразований. Разработанные методы основываются на использовании принципа кольцевого сдвига в модулярной системе счисления (МСС). Применение МСС позволило эффективно, с точки зрения повышения быстродействия реализации криптографических преобразований с открытым ключом, организовать процесс реализации модульных целочисленных арифметических операций.

Ключевые слова: специализированные цифровые устройства и системы, основание непозиционной системы счисления, модулярная система счисления, криптографические преобразования.

UDC 681.3.04

DESCRIPTION AND APPLICATIONS OF BINOMIAL NUMERAL SYSTEMS

Olexiy Borysenko[1], Vyacheslav Kalashnikov[2], Nataliya Kalashnykova[3]

[1] Department of Electronics and Computing, Sumy State University, Rimsky-Korsakov str. 2, Sumy 40007, Ukraine;
electron@sumdu.edu.ua

[2] Department of Systems & Industrial Engineering, ITESM, Campus Monterrey,
Av. Eugenio Garza Sada 2501 Sur, Monterrey, N.L., 64849, Mexico;
kalash@itesm.mx

[3] Department of Physics and Mathematics (FICA), Universidad Autónoma de Nuevo León (UANL), Avenida Universidad S/N,
San Nicolás de los Garza, Monterrey, N.L., 66450, Mexico;
nkalash@einstein.fcfm.uanl.mx

Reviewer: Alexandr Kuznetsov Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4,
Kharkov, 61022, Ukraine;
kuznetsov@karazin.ua

Received on April 2016

Abstract. *We develop a new class of positional numeral systems, namely the binomial ones, which form a subclass of generalized positional numeral systems (GPNS). The binomial systems have wide range of applications in the information transmission, processing, and storage due to their error-detection capabilities. In this paper, the binomial numeral systems are well-defined, their prefix and compactness properties are established. Algorithms of generating binomial coding words (non-uniform and uniform) are presented, as well as an enhanced procedure of construction of constant weight Boolean combinations based upon the non-uniform binomial coding words. The correctness of this procedure is established.*

Keywords*: generalized positional numeral systems, binomial numeral systems, constant weight codes.*

1 Introduction

Positional numeral systems are widely used in computing. More complicated numeral systems, in which the register's weight need not be equal to the power of the system's base (like, for example, in the binary or decimal system), have not been thoroughly studied as yet. Such generalized positional numeral systems (GPNS) may have quite useful properties, like being noise-proof, easy in generating permutations, etc. (see [1-3]). These properties allow one to exploit the GPNS to develop specialized digital de-vices with high computational speed, reliability, and very low size and weight parameters. Moreover, the GPNS may serve as a base for:

a) generation of codes and construction of coding devices for the thorough error-control when processing, transmitting, and storing information;
b) development of algorithms and devices used when information is compressed and/or coded;
c) efficient solution of combinatorial optimization problems.

When combinatorial objects are generated and numerated, researchers use to develop special methods for each individual problem, which can be characterized as a principal drawback of such an approach [4,5]. Therefore, a universal algorithm solving these problems at both the theoretical and practical levels would be very helpful. We propose a possible solution method based upon the GPNS. In particular, in this paper, a binomial numeral system is considered, which generates combinatorial objects making use of constant weight codes [6]. The total number of coding words in such codes is determined by binomial coefficients [7].

The generalized positional numeral systems (GPNS) allow one to develop efficient algorithms and specialized digital devices (based upon these algorithms) due to the similarity of their structures. Thus the device cost is saved, and the high computational speed is attained (due to the hardware implementation, up to ten times higher compared to the universal computers). Moreover, as

© Borysenko O., Kalashnikov V., Kalashnikova N., 2016

the GPNS are noise-proof, their digital devices use to be much more reliable and easy in trouble-shooting.

It is worthwhile to develop digital devices using a GPNS and completing mainly logical and the simplest arithmetical operations with integer numbers, because these operations are realized by the GPNS in the most efficient way.

Certain parts of such specialized devices, e.g. noise-proof counters, registers, etc., are of interest for the universal computers as well [8,9].

To cope with the problem of noise-proof storage and transmission of information, a lot of various codes, both error-detecting and error-correcting, have been developed. Among those codes, it is worthy to distinguish the codes that detect errors not only during the information transmission and storage but also while it is processed. This class also includes the codes based upon the GPNS, whose strong sides are: (i) the simplicity of algorithms and devices for detecting errors, (ii) the structural regularity, (iii) the possibility to regulate the code's redundancy and hence its error-detecting capability depending upon the channel's adaptability. Such codes are quite applicable in specialized automatic controlling systems, as the information's downloading, processing, transmission, and development of controlling actions are all based upon the same GPNS code.

One of the important problems arising while storing and transmitting information is its compression, like for example by the optimal coding based on the Shannon-Fano and Huffman codes [10,11]. Nowadays, the coding theory can boast with a quite wide arsenal of other ways to compress information, which however cannot exclude the development of new methods and/or improvement of the existing ones. One of those is the numeration of messages, which has the following advantages: (a) an algorithmic coding structure allowing an easy implementation, and (b) no need in a dictionary.

Application of a GPNS permits one to expand the class of numerated messages and thus improve and simplify the algorithmic and technical realization of the information compression.

Both the numeration and de-numeration processes based upon the GPNS can be efficiently used to code the information. Thus we can obtain noise proof codes of high stability and with simple keys used for the information security.

Finally, problems of combinatorial optimization are of special importance. In the most general form, these problems may even not have an objective function but stated in some preference terms. Such problems are usually solved by an exhaustive search, or when it is impossible, by random search procedures [2]. In both cases, the GPNS can provide many efficient ways of generating the combinatorial objects in order to find a path to an optimal solution.

Therefore, the generalized positional numeral systems (GPNS) propose a unified approach allowing one to solve efficiently a series of practical problems of various natures. As an example of such a GPNS, our paper presents a binary binomial numeral system. The latter is characterized with the use of binomial coefficients as weights of the binary digits [12-14].

The rest of the paper is arranged as follows. In Section 2, we define the principal structure of the binomial calculus system. Section 3 presents the mains results establishing the key properties of the binomial systems, namely, the prefix and the compactness properties. Finally, Section 4 deals with the algorithms to generate and numerate binomial combinations of various lengths (non-uniform codes), the constant length (uniform codes), and the constant weight combinations. Conclusion, acknowledgement and the reference list complete the paper.

2 Binomial Systems

Now we describe one of the GPNS, namely the binomial system with the binomial weights and the binary alphabet {0,1} [12-14].

In a *k*-binomial system with n registers (k < n), the quantitative equivalent *QAi* of a code combination $Ai = (a_{j-1}, a_{j-2}, \dots, a_0)$, $i = 0,1,\dots, P-1$, with $P = C_n^k$, where $j = j(i)$ is the combination's length, is defined as follows:

$$QA_i = a_{j-1}C_{n-1}^{k-q_i} + \dots + a_\ell C_{n-j+\ell}^{k-q_\ell+1} + \dots + a_0 C_{n-j}^{k-q_1}, \quad (1)$$

where the following conditions must hold: either

$$\begin{cases} q_0 = k, \\ j < n; \\ a_0 = 1, \end{cases} \tag{2}$$

or

$$\begin{cases} n - k = j - q_0, \\ q_0 < k; \\ a_0 = 0, \end{cases} \tag{3}$$

Here q_0 is the quantity of units (ones) in the binomial number, P is the range of the system, j is the quantity of registers (positions) in the binomial number (or, its length), $\ell = 0,1,\ldots, j\text{-}1$ is the register's ordinal number, q_ℓ is the sum of the digits occupying the registers (j-1) through ℓ, inclusively, i.e.

$$q_\ell = \sum_{i=\ell}^{j-1} a_i , \tag{3}$$

with $q_j = 0$.

A positional numeral system must be finite, effective, and well-defined.
However, it is not enough for a generalized positional system. In addition, it has to be a prefix code system, i.e. with the "prefix property": there is no valid code word in the system that is a prefix (start) of any other valid code word in the set. With a prefix code, a receiver can identify each word without requiring a special marker between words. The generalized positional numeral system should be also continuous, which means that for any number s from the system's range (except for the maximal number), there exists a combination, whose quantitative equivalent is equal to (s + 1). All these properties of the binomial numeral systems will be established in the next section.

3 The Binomial System is Finite, Effective, Prefix, and Well-Defined

Formula (1) shows that the binomial numeral system is *finite* and *effective*, because there exists a numeration algorithm, which, after a finite of number of steps, converts the coding combination A_i into its quantitative equivalent QA_i. Now the following theorem establishes the *prefix property* of the binomial numeral system. Although its proof was first given in [12], we repeat it here to make the paper self-contained.

Theorem 3.1. [12]. *The k-binomial numeral system with n registers (where k < n) is a prefix code system.*

Proof. Let a coding combination A_i satisfy conditions (2), i.e., let it contain exactly k units (ones). As the condition j < n in constraint (2) implies that the length of such combinations cannot exceed (n-1), then we conclude that the length j of A_i lies between k and $n - 1$, that is, $k \le j \le n - 1$.

Therefore, the number of zeros z in A_i can be equal to $z = 0,1,\ldots, n\text{-}k\text{-}1$, while the combinations length equals $j = k+z$. The total number of distinct combinations of the same length containing k ones and z zeros coincides with the number of combinations of z (zeros) among the total quantity of $(j - 1)$ elements, namely, $P = C_{k+z-1}^{z}$. The distinct combinations cannot evidently be prefixes of the others having the same length, hence in this case, the desired property holds. As for the combinations of different lengths, their values of z are also different. However, as the combinations in question always have 1 at the extreme right position (i.e., $a_0 = 1$), and the total number of 1's is equal to the same number k, it is clear that the longer combination, in its prefix part of the length equal to the total length of the shorter combination, contains at least one 1 (unit) less than the shorter combination. Therefore, the prefix property is valid for all coding combinations satisfying conditions (2).

Now consider the coding combinations satisfying (3). As the constraint $n\text{-}k=j\text{-}q_0$ clearly implies that the total number of zeros in these combinations is constant and equal to $n\text{-}k$, then the combination's generation process stops when the last, the $(n\text{-}k)$ -th zero appears at the right end position (i.e., $a_0 = 0$). The number of zeros $(n\text{-}k)$ summed with the number $q_0 = 0,1,\ldots,k\text{-}1$ of 1's defines the combination's total length as $j=n\text{-}k+q_0$. Therefore, the number of distinct combinations with q_0 units and $(n\text{-}k)$ zeros (including the zero in the right end position) coincides with the number of all possible combinations of q_0 elements among the total of $(j\text{-}1)$ positions, that is, $P = C_{n-k+q_0-1}^{q_0}$. Again, the prefix property for the combinations of the same length is evident. As for the combinations of the considered subclass having different length values, they also have different numbers of 0's. Consider two such coding combinations of length values equal to p and q, respectively, with, say, $p < q$. The shorter combination with the length p, which could be a prefix of the longer one, contains exactly $(n\text{-}k)$ zeros, the same as the longer combination has. However, the right end position of the longer combination is occupied by zero, hence the number of zeros in the longer combination's prefix of length p cannot exceed $(n\text{-}k\text{-}1)$, which clearly excludes the possibility for the shorter coding combination to be the prefix of the longer one.

Finally, it is straightforward that no coding combination satisfying (2) can be the prefix of a combination satisfying (3), and vice versa. This is due to the fact that the maximum number of 1's in any combination of the latter class is strictly less than that in every combination of the former class. Therefore, no combination of class (2) can be a prefix of a combination of class (3). In an analogous manner, it is easy to see that the maximum possible number of zeros in an arbitrary coding combination of subset (2) is strictly less than that in any combination of class (3), hence, no combination of subclass (3) can form a prefix of a combination from (2). Therefore, the prefix property is evidently valid for the whole set of combinations satisfying (2) or (3), which completes the proof of the theorem.

To show that the binomial system is well-defined, that is, two distinct coding combinations cannot be equivalent to the same numerical value, we prove the following result (again, see [12]).

Theorem 3.2. [12] *The k-binomial system with n registers (where k < n) is well-defined.*

Proof. The previous result (Theorem 3.1 with the prefix property) implies that any two distinct coding combinations have different digits (0 and 1) at least in one of the registers (counted from left to right). The digits in the registers (if any) preceding the first such register are common for both combinations, whereas the remaining (succeeding) part is called the proper part of each combination in this pair. If we prove that the proper parts of these two coding combinations cannot represent the same number, the binomial system is well-defined. Consider the proper parts of two coding combinations (without affecting generality, assume that the combinations have no coinciding preceding parts):

$$Aw = (a_\alpha, \ldots, a_0) \text{ and } As = (b_\beta, \ldots, b_0);$$

where

$$a_\alpha = 0;\ b_\beta = 1;\quad 0 \le \alpha, \le n - 1;\ 0 \le w;\ s \le P - 1; \text{ and } w \ne s.$$

It is not difficult to demonstrate (see the decription of the algorithm generating non-uniform binomial numbers in Section 4) that if in the coding combination A_w all the digits to the right from a_ were 1's (i.e., $a_m = 1$ for $m = 0, 1, \ldots, a\text{-}1$), whereas in A_s, vice versa, all the entries to the right from b_β were zero, that is, $b_t = 0$ for $t = 0, 1; \ldots, \beta\text{-}1$, then the distance
between the numbers QA_w and QA_s represented by the combinations A_w and A_s, respectively, would be the minimum possible one. Now we establish that this minimum distance is not zero. Indeed, by definition (1) and by the above assumptions, one has:

$$QA_\omega = 0 \cdot C_{n-j_\alpha+\alpha}^{k-q_{\alpha+1}} + 1 \cdot C_{n-j_\alpha+\alpha-1}^{k-q_{\alpha+1}} + 1 \cdot C_{n-j_\alpha+\alpha-2}^{k-q_{\alpha+1}-1} + \cdots + 1 \cdots C_{n-j_\alpha+\alpha-\alpha}^{k-q_{\alpha+1}-\alpha+1},$$

and

$$QA_s = 1 \cdot C_{n-j_\beta+\beta}^{k-q_{\beta+1}} + 0 \cdot C_{n-j_\beta+\beta-1}^{k-q_{\beta+1}-1} + 0 \cdot C_{n-j_\beta+\beta-2}^{k-q_{\beta+1}-1} + \cdots + 0 \cdots C_{n-j_\beta+\beta-\beta}^{k-q_{\beta+1}-1}.$$

Now since

$$QA_{\omega} = \sum_{i=1}^{\alpha} C_{n-j_{\alpha}+i-1}^{k-q_{\alpha+1}-\alpha+i} = C_{n-j_{\alpha}+\alpha}^{k-q_{\alpha+1}} - 1$$

and hence

$$QA_{s} = C_{n-j_{\beta}+\beta}^{k-q_{\beta+1}} = C_{n-j_{\alpha}+\alpha}^{k-q_{\alpha+1}} = QA_{\omega} + 1,$$

the latter relationships make it possible to conclude that $QA_{\omega} \neq QA_{s}$ and thus the minimum distance between them is 1, which completes the proof.

Theorems 3.1 and 3.2 have the following important corollary, which proves the compactness of the binomial numeral systems.

Corollary 3.1. The k-binomial system with n registers ($k < n$) *is compact, that is, its range is complete and covers all the integers between 0* and ($C_n^k - 1$).

Proof. According to formula (1), the maximal number represented in the *k*-binomial system with *n* registers is as follows:

$$QA_{P-1} = 1 \cdot C_{n-1}^{k-q_j} + 1 \cdot C_{n-2}^{k-q_j-1} + \cdots + 1 \cdot C_{n-j}^{k-q_1} = C_n^k - 1.$$

The minimal represented value is zero, hence the total number of the integers between the lower and upper bounds of the range is C_n^k. Meanwhile, it is not difficult to establish that the total number of coding combinations constructed by formula (1) and ending with 1 (i.e. satisfying (2)) is equal to

$$N_1 = \sum_{i=0}^{n-k-1} C_{n-2-i}^{n-k-1-i} = C_{n-1}^{n-k-1} = C_{n-1}^{k}.$$

Similarly, it can be proved that the total number of combinations generated by (1) and ending with 0, i.e. with condition (3), is:

$$N_0 = \sum_{i=0}^{k-1} C_{n-2-i}^{k-1-i} = C_{n-1}^{k-1}.$$

Therefore, the total number of distinct coding combinations in the *k*-binomial system equals

$$N = N_1 + N_0 = C_{n-1}^{k} + C_{n-1}^{k-1} = C_n^k.$$

By Theorem 3.2, the correspondence between the coding combinations and the represented integers is one-to-one, and the compactness of the *k*-binomial system with *n* registers is proved.

Remark 3.1. *It is straightforward that for the k-binomial calculus system with n registers, the range parameter P is equal to* C_n^k.

4 Algorithms Generating Binomial Combinations

Table 4.1 contains the binomial combinations and their quantitative equivalents for the *k*-binomial system with *n* registers, where *n = 6* and *k = 4*.

They are generated by the following algorithm:

Step 1. An initial combination A_0 consisting of (*n-k*) zeros is composed and referred to as a *key-word*.

Step 2. The digit 1 is put into the right end register, and zero is added to the right side of it.

Step 3. Step 2 is repeated while the number of 1's in the coding word is less than *k-1*. If the number of 1's is equal to *k-1*, then go to Step 4.

Step 4. If the right end position contains zero, we replace it with 1. Go to Step 5.

Step 5. Check the number of 1's in the coding combination: if it equals k but the 1's do not occupy the first *k* registers counted from left to right, go to Step 6. Otherwise, i.e. if the 1's occupy the first *k* registers counted from left to right, then **STOP**: all the combination have been generated.

Table 4.1 Binomial coding combinations of non-constant length *(non-uniform code)*

Binomial word	Its quantitative equivalent
00	$0C_5^4 + 0C_4^4 = 0$
010	$0C_5^4 + 1C_4^4 + 0C_3^3 = 1$
0110	$0C_5^4 + 1C_4^4 + 1C_3^3 + 0C_2^2 = 2$
01110	$0C_5^4 + 1C_4^4 + 1C_3^3 + 1C_2^2 + 0C_1^1 = 3$
01111	$0C_5^4 + 1C_4^4 + 1C_3^3 + 1C_2^2 + 1C_1^1 = 4$
100	$1C_5^4 + 1C_4^3 + 0C_3^3 = 5$
1010	$1C_5^4 + 0C_4^3 + 1C_3^3 + 0C_2^2 = 6$
10110	$1C_5^4 + 0C_4^3 + 1C_3^3 + 1C_2^2 + 0C_1^1 = 7$
10111	$1C_5^4 + 0C_4^3 + 1C_3^3 + 1C_2^2 + 1C_1^1 = 8$
1100	$1C_5^4 + 1C_4^3 + 0C_3^2 + 0C_2^2 = 9$
11010	$1C_5^4 + 1C_4^3 + 0C_3^2 + 1C_2^2 + 0C_1^1 = 10$
11011	$1C_5^4 + 1C_4^3 + 0C_3^2 + 1C_2^2 + 1C_1^1 = 11$
11100	$1C_5^4 + 1C_4^3 + 1C_3^2 + 0C_2^1 + 0C_1^1 = 12$
11101	$1C_5^4 + 1C_4^3 + 1C_3^2 + 0C_2^1 + 1C_1^1 = 13$
1111	$1C_5^4 + 1C_4^3 + 1C_3^2 + 1C_2^1 = 14$

Step 6. Update the keyword A_0 by putting 1 as a prefix before the beginning of the keyword (i.e., its left end). If the total number of 1's in the keyword is less than *k*, go to Step 2.

The binomial systems find various important applications, in which the following useful features are exploited: (*i*) the binomial systems are noise-proof in the information transmission, processing, and storage; (*ii*) they are able to search, generate and numerate coding combinations with a constant weight; (*iii*) they can be used to construct noise-proof digital devices. To detect errors with the aid of binomial coding combinations, they should be completed with zeros to obtain uniform *(n - 1)*-digital binomial coding words given in Table 4.2.

Table 4.2 Binomial coding combinations of a constant length (*uniform code*)

NN	Binomial word	Binomial uniform word
0	00	00000
1	010	01000
2	0110	01100
3	01110	01110
4	01111	01111
5	100	10000
6	1010	10100
7	10110	10110
8	10111	10111
9	1100	11000
10	11010	11010
11	11011	11011
12	11100	11100
13	11101	11101
14	1111	11110

The main tokens of errors in a binomial coding combination are either the number of 1's being greater than *k*, or the number of zeros exceeding (*n-k*). The principal feature of the binomial noise-proof code is its ability to detect errors while processing information. This feature allows one to arrange the throughout control in the information processing channels involving the digital devices.

4.1. *Generation of binomial coding combinations with a constant weight*

Next, Table 4.3 shows a transformation of binomial coding combinations to coding words with a constant weight: this is done by adding (to the right end) either 1's if the binomial combination contains (*n-k*) zeros, or adding zeros if the combination comprises *k* digits 1, until the combination's length reaches *n*.

Table 4.3 Binomial coding combinations of a constant weight

NN	**Binomial word**	**Binomial constant weight word**
0	00	001111
1	010	010111
2	0110	011011
3	01110	011101
4	01111	011110
5	100	100111
6	1010	101011
7	10110	101101
8	10111	101110
9	1100	110011
10	11010	110101
11	11011	110110
12	11100	111001
13	11101	111010
14	1111	111100

Each binomial combination (column 2 of Table 4.3) has the corresponding combination with the constant weight (column 3 of Table 4.3), hence the former is a compressed image of the latter. If one needs to label a combination with the constant weight by some traditional numeral system number (e.g., decimals of column 1 in Table 4.3), formula (1) has to be used. In the latter case, a compression of binomial numbers is completed.

Algorithms of search and generation of binomial combinations and those with constant weights can be also found in [14]. Now we describe one of modifications of such algorithms and prove its efficiency as follows. This method is based upon the fact that the range of binomial numbers of length n and with parameter *k* ($k < n$) coincides with the range of the constant weight coding combinations with k units among n registers. Therefore, the formal description of the algorithm is as follows:

Step 1. Select an arbitrary non-uniform binomial coding combination.

Step 2. If the coding combination ends with the digit 1, then put zeros into all registers up to the right end (register n), which is considered as auxiliary. The thus obtained combination ending with 0 will be the combination with the constant weight.

Step 3. If the coding combination ends with the digit 0, then set units (ones) into all registers up to the right end (register n, or the auxiliary register). The thus created combination ending with 1 will be the combination with the constant weight.

Step 4. Verify that the thus obtained combination is indeed with the constant weight by counting the total number of ones (units). If this number is k then the combination is indeed a desired one. Select another non-uniform binomial coding combination and go to Step 2. If all the non-uniform binomial coding combinations have been already selected, then **STOP**: all the constant weight combinations of this range have been generated.

The above algorithm generates the complete range of the corresponding combinations of the constant weight, which is confirmed by the following theorem.

Theorem 4.1. *With the aid of the above algorithm, for every non-uniform binomial combination of length n with parameter k (k < n), one obtains the unique corresponding coding combination with (the constant) weight k and length n.*

Proof. First, consider the case when the selected non-uniform binomial coding combination ends with the unit (i.e., with digit 1). According to the definition of the non-uniform binomial coding words, it implies that this combination has already had *k* units (digits 1). Making use of the above-described algorithm (Step 2), we need only to add several zeros into the registers to the right from the rightest 1 till the auxiliary register is filled, thus having obtained the combination with (the constant) weight *k*. It is clear that two different non-uniform binomial coding words cannot generate (with the aid of the above algorithm) the same constant weight combination: indeed, if otherwise, it would imply that one (the shorter) of these non-uniform binomial coding words is the prefix of the second (the longer) one, which would contradict Theorem 3.1.

Next, if the selected non-unifom binomial coding combination ends with 0, then, due to the description of the verified algorithm (see Step 3), we will insert 1's into all the registers to the right from the rightest zero, including the auxiliary register. According to the definition of the non-uniform binomial combination ending with zero, the total number of zeros in it is equal to (*n-k*); therefore, the constructed new combination will contain $n-(n-k)=k$ digits 1, i.e. it will have the (constant) weight *k*. Repeating exactly the proof for the first case (Step 2) given above, we conclude that different non-uniform binomial combinations ending with 0 will produce different combinations of (the constant) weight *k*. Finally, two constant weight combinations produced by different steps (Step 2 and Step 3) of the above algorithms cannot coincide due to the different digits in their auxiliary registers (0 for Step 2 and 1 for Step 3). The proof is complete.

5 Conclusion

In this paper, we have described the error-detecting binomial numeral systems capable of transmitting, processing and storing information. The systems can also generate and numerate combinatorial configurations, like, for example, coding words with a constant weight, as well as compositions, combinations with repetitions, etc. Moreover, the binomial systems can be applied to produce efficient information compression and defense. The latter is the goal of our further research.

6 Acknowledgements

The research activity of the second author was financially supported by the R&D Department (Cátedra de Investigación) CAT-174 of the Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM), Campus Monterrey, and by the SEP-CONACYT projects CB-2008-01-106664 and I0010-2009-01-122315, Mexico. Also, the work of the second and third authors was supported by the Russian Humanitarian Research Foundation (RGNF) within the project RGNF 08-02-00271, while the third author was supported by the PAICYT project No. CE250-09 and by the SEP-CONACYT project I0010-2009-01-118057.

References

[1] Stakhov A.P. Golden Section Codes / A.P. Stakhov. – Moscow: Radio and Communication, 1984. (In Russian).

[2] Stoyan Yu.G. Solution of Some Extremum Problems by the Method of Contracting Neighborhoods, Scientific Thinking / Yu.G. Stoyan, V.Z. Sokolovsky. – Kiev: Naukova Dumka, 1980. (In Russian).

[3] Borisenko A.A. Numerical coding based upon combinatorial calculus systems/ A.A. Borisenko // Theoretical and Applied Aspects of Program Systems Development (TAAPSD'2010): Proceedings of the International Conference, Kiev, Ukraine, October 04-08, 2010 / ed. M.S. Nikitchenko. – pp.98 – 104. (In Russian).

[4] Amel'kin V.A. Numerical Coding Methods / V.A. Amel'kin. – Novosibirsk: Nauka, 1986. (In Russian).

[5] Reingold E.M. Combinatorial Algorithms: Theory and Practice / E.M. Reingold, J. Nievergelt, N. Deo. – Prentice Hall [New Jersey]: Englewood Cliffs, 1977.

[6] Borisenko A.A. Binomial Coding / A.A. Borisenko, I.A. Kulik . – Sumy: Sumy State University, 2010. (In Russian).

[7] Anderson J.A. Discrete Mathematics with Combinatorics / J.A. Anderson. – Prentice Hall [New Jersey]: Upper Saddle River, 2001.
[8] Borisenko A.A. Binomial Calculus and Counters / A.A. Borisenko. – Sumy: Sumy State University, 2008. (In Russian).
[9] Oberman R.M.M. Counting and Counters / R.M.M. Oberman. – Hoboken [New Jersey]: Wiley & Sons, 1981.
[10] Tsymbal V.P. Information and Coding Theory / V.P. Tsymbal. – Kiev: Vyshaya Shkola, 1977. (In Russian).
[11] Kuz'min I.V. A Basic Theory of Information and Coding / I.V. Kuz'min, V.A. Kedrus. – Kiev: Vyshaya Shkola, 1977. (In Russian).
[12] Borisenko A.A. Binomial calculus: Advantages and prospects / A.A. Borisenko, V.V. Kalashnikov, N.I. Kalashnykova // ICIC Express Letters. – 2006. – №2. – pp.123-130.
[13] Borisenko A.A. Introduction to the Theory of Binomial Calculus / A.A. Borisenko. – Sumy: Universitetskaya Kniga, 2004. (In Russian).
[14] Borisenko A.A. Binomial Calculus: Theory and Applications / A.A. Borisenko. – Sumy: Universitetskaya Kniga, 2004. (In Russian).

Рецензент: Олександр Кузнецов, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна. E-mail: kuznetsov@karazin.ua

Надійшло: квітень 2016.

Автори:
Олексій Борисенко, д.т.н., проф., Сумський державний університет, Суми, Україна. E-mail: electron@sumdu.edu.ua
В'ячеслав Калашников, д.ф.-м.н., проф., департамент систем і промислового виробництва Технологічного університету Монтеррея, Монтеррей, Мексика. E-mail: kalash@itesm.mx
Наталя Калашникова, к.т.н., доц., автономный университет Нуэво-Леон, Сан Николас де Лос Гарса, Монтеррей, Мексика. E-mail: nkalash@einstein.fcfm.uanl.mx

Опис та застосування біноміальних систем числення.

Анотація. Розробляється новий вид позиційних систем числення, що отримали назву біноміальних, які утворюють підклас узагальнених позиційних систем числення (УПСЧ). Вони мають широку область застосування при передачі, обробці та зберіганні інформації завдяки забезпеченню можливості виявлення помилок і генерування різних комбінаторних конфігурацій. Наведені алгоритми формування біноміальних кодових слів (рівномірних і нерівномірних) та побудови на цій основі рівноважних кодових комбінацій з постійною вагою. Показано коректність цієї процедури.

Ключові слова: позиційні системи числення, кодування, комбінаторика, біноміальні числа.

Рецензент: Александр Кузнецов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kuznetsov@karazin.ua

Поступила: апрель 2016.

Авторы:
Алексей Борисенко, д.т.н., проф., Сумской государственный университет. Сумы, Украина. E-mail: electron@sumdu.edu.ua
Вячеслав Калашников, д.ф.-м.н., проф., департамент систем и промышленного производства Технологического университета Монтеррея, Монтеррей, Мексика. E-mail: kalash@itesm.mx
Наталья Калашникова, доц., к.т.н., автономный университет Нуэво-Леон, Сан Николас де Лос Гарса, Монтеррей, Мексика. E-mail: nkalash@einstein.fcfm.uanl.mx

Описание и применение биномиальных систем счисления.

Аннотация. Разрабатывается новый вид позиционных систем счисления, называемых биномиальными, который образует подкласс обобщенных позиционных систем счисления (ОПС). Они имеют широкую область применения при передаче, обработке и хранении информации благодаря обеспечению возможности обнаружения ошибок и генерирования различных комбинаторных комбинаций. Представлены алгоритмы формирования биномиальных кодовых слов (равномерных и неравномерных) и построения на их основе равновесных кодовых комбинаций с постоянным весом. Показана корректность этой процедуры.

Ключевые слова: позиционные системы счисления, кодирование, комбинаторика, биномиальные числа.

УДК 004.056.55

ВЫБОР ОБРАЗУЮЩИХ ПОЛИНОМОВ ДЛЯ РЕГИСТРА СДВИГА С НЕЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ ВТОРОГО ПОРЯДКА ГЕНЕРИРУЮЩИХ ПОСЛЕДОВАТЕЛЬНОСТЬ С МАКСИМАЛЬНЫМ ПЕРИОДОМ

Александр Потий[1], Николай Полуяненко[2]

[1] Харьковский национальный университет имени В.Н. Каразина, площадь Свободы, 4, г. Харьков, 61022, Украина
potav@ua.fm

[2] Харьковский национальный университет радиоэлектроники, соискатель кафедры БИТ
rsnos@mail.ua

Рецензент: Виктор Долгов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: dolgovvi@mail.ru

Поступила в феврале 2016

Аннотация. *Рассмотрена модель генератора псевдослучайной последовательности на основе регистров сдвига с нелинейной обратной связью второго порядка. Сформулированы дополнительные требования к виду полинома, ограничивающее множество полиномов при выборе генерирующего последовательность с максимальным периодом. Приведено выражение для определения количества полиномов, не удовлетворяющих сформулированным требованиям. Дана количественная оценка влияния каждого требования на отсекаемое множество полиномов. Сформулированы рекомендации по применению указанных требований.*

Ключевые слова: *поточные шифры, регистры сдвига, нелинейные системы.*

1 Введение

В настоящее время многие структуры генераторов поточных шифров (рис.1) основаны на идее синхронного, классического суммирующего генератора и принадлежат к классу схем с равномерным движением регистра. К таким структурам относятся: SNOW, SOBER (t16, t32, 128), TURING. Основными элементами таких структур, как правило, является регистр сдвига с линейной обратной связью (РСЛОС) и схема усложнения.

Надежные криптоалгоритмы основываются на принципе, в соответствии с которым, силовая атака (*т.е. атака, в основу которой положен полный перебор всех возможных комбинаций ключа*) должна быть наиболее эффективна по сравнению с остальными предлагаемыми видами атак (*аналитическими или статистическими*).

Рис. 1 – Общая модель структуры генераторов поточных шифров

Для усложнения выходной последовательности в структуру генератора поточных шифров вводится нелинейность. Существуют различные пути введения нелинейности [1]. В большинстве современных поточных шифров нелинейная функция вводиться на выходе генератора для усложнения выходной последовательности одного или нескольких линейных рекуррентных регистров сдвига.

© Потий А., Полуяненко Н., 2016

Наряду с разнообразными подходами [2-4], одним из возможных способов усложнения является внесение нелинейности в саму рекуррентную последовательность, путем введения нелинейности в обратную связь регистров сдвига. Кроме того, в настоящее время важную роль играют системы генерации случайных чисел, основанные на регистрах сдвига с нелинейной обратной связью (РСНОС) [5]. Преимущество таких систем заключается в следующем:

– выходная последовательность имеет те же характеристики, что и хорошо изученные РСЛОС (*прохождение тестов на случайность генерируемой последовательности*);

– структура (объем памяти, количество операций на один выходной бит, архитектура производства) практически идентично РСЛОС;

– нелинейность уже введена в регистр, что не требует дополнительного усложнения (а как следствия, дополнительного объема оперативной памяти и дополнительных вычислительных операций), т.е. соотношения время/память аналогично РСЛОС;

– отсутствие простых алгоритмов для восстановления структуры РСНОС по генерируемой ими последовательности, таких как, например алгоритм Берлекэмпа-Мэсси для РСЛОС;

– простота в программной и аппаратной реализации;

– значительно большее количество комбинаций обратной связи при одинаковой длине регистра. Если у РСЛОС длины L количество всех возможных комбинаций обратных связей определяется как 2^L, то у РСНОС той же длины их будет $2^{\frac{L^2+L}{2}}$.

К недостаткам применения РСНОС следует отнести то, что на сегодняшний день даже такую простую характеристику, как период формируемой РСНОС гаммы, трудно определить.

На этапе проектирования и создания генератора случайных чисел основополагающим моментом является выбор образующего полинома РСНОС, который будет генерировать последовательность с максимально возможным периодом. В дальнейшем, последовательность, которая имеет максимально возможную длину, будем называть М-последовательностью, а образующие полиномы РСНОС, которые генерируют М-последовательности – М-полиномами.

Однако, утверждать, что случайным образом взятый полином является М-полиномом, не проведя соответствующую проверку генерируемой последовательности, невозможно. Для достаточно большой степени такого рода полиномов провести вычислительную проверку одной последовательности (с целью определения ее периода), является достаточно трудоемкой задачей. Причем, процент М-полиномов от всех возможных, уменьшается по степенной зависимости с увеличением степени полиномов и, следовательно, поиск хотя бы одного М-полинома (для высокой степени) представляет относительно сложную задачу.

В качестве примера можно привести следующие оценки. Для РСНОС длиной L=128 полное количество возможных РСНОС составляет 2^{8256}. При этом, пользуясь оценочной формулой из [6], часть полиномов, которые могут генерировать М-последовательность, будет составлять менее $3 \cdot 10^{-77}$ от общего количества возможных.

Целями данной статьи являются выработка рекомендаций, касающихся методики выбора М-полинома для РСНОС и обоснование точной количественной оценки верхней границы числа М-полиномов в зависимости от длины РСНОС.

2 Общая модель РСНОС второго порядка

Рассмотрим систему генерации псевдослучайной двоичной последовательности основанной на РСНОС. В качестве обратной связи будем использовать побитовое сложение (обозначенное знаком – $\oplus$) и нелинейную функцию – умножения (обозначенное знаком – $\otimes$). Через L обозначим количество ячеек в регистре сдвига На рис. 2 представлен пример изучаемой модели РСНОС при $L=4$.

В данном случае блок умножения определяет наличие обратной связи. Так, при $a_{ij}=1$ соответствует наличию связи, а при $a_{ij}=0$ - отсутствию такой связи. В общем случае обратную связь для такой системы можно задать в следующем виде:

$$q_1(t+1)=\sum_{i=1}^{L}\sum_{j=i}^{L}a_{ij}q_i(t)q_j(t), \qquad (1)$$

где мы учитываем, что $q_i \cdot q_i = q_i$ (т.е. умножение значения регистра самого на себя не дает никакого изменения). Как следствие, на рис. 2 знак ⊗ между i и i регистром опущен.

При рассмотрении рис.2 следует учитывать следующие допущения и сокращения: $a_{ij} \in \{0,1\}$ - блок умножения; $q_i(t) \in \{0,1\}$ - значение i-ого регистра в момент времени t; ⊕ – знак суммы; ⊗ – знак умножения; Q – генерируемая последовательность (бит). Кроме того, коэффициенты a_{ij} будем считать *линейными коэффициентами*, если $i = j$ и, соответственно, *нелинейными коэффициентами* – если $i \neq j$.

Нелинейная функция (1) обратной связи состоит из суммы произведений двух регистров. Назовем такую нелинейность – нелинейностью второго порядка.

Заметим, что если все коэффициенты в блоке умножения $a_{ij} = 0$ для всех $i \neq j$, то такой частный случай рассматриваемой модели, будет представлять собой РСЛОС.

Обозначим через n_L полное количество коэффициентов в блоке умножения, т.е. максимально возможное количество $a_{ij} \neq 0$. Тогда для РСНОС 2-го порядка n_L определяется однозначно для заданного L следующим выражением:

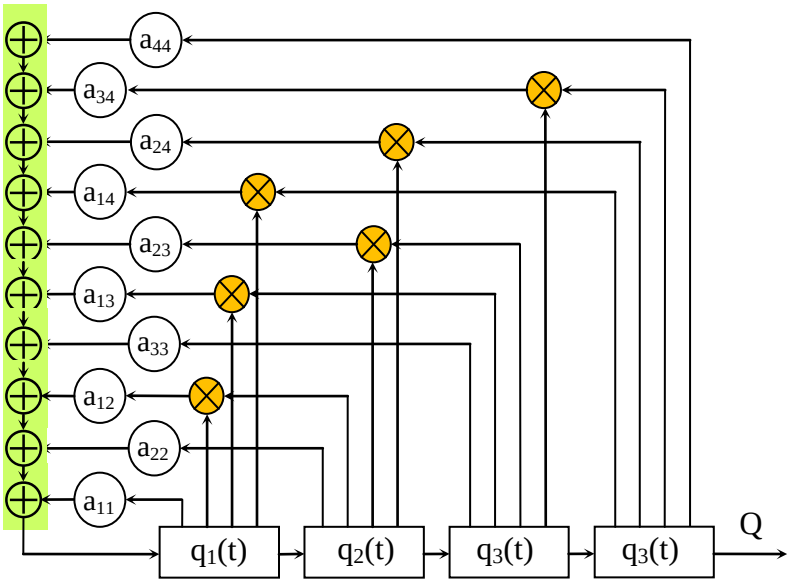


Рис. 2 – Общий вид генератора ПСП на РСНОС при $L=4$

$$n_L = \frac{L \cdot (L+1)}{2}.$$

Обозначим через Λ_0 полное множество всех комбинаций значений, которые могут принимать коэффициенты обратных связей a_{ij} в РСНОС второго порядка [6]:

$$\Lambda_0 = 2^{n_L}.$$

Заметим, что при использовании РСЛОС количество обратных связей, которыми можно варьировать, равно L (т.е. $n_L = L$) и $\Lambda_0 = 2^L$.

3 Требования к виду РСНОС второго порядка для формирования последовательности с максимальным периодом

В работе [6] были сформулированы требования, которым должен отвечать полином генерирующий М-последовательность. Приведем их:

Требование 1. Для обеспечения максимального периода линейный коэффициент обратной связи от последнего регистра должен присутствовать всегда, т.е.: $a_{LL} = 1$.

Требование 2. Сумма всех ненулевых коэффициентов обратной связи a_{ij} должна быть четным числом, т.е.: $\sum_{i,j=1}^{L} a_{ij}$ - четное число.

Требование 3. Не должно быть нелинейной обратной связи, полученной от выходного регистра и любого другого регистра, т.е.: $\forall a_{iL} = 0, i = \overline{\{1, L-1\}}$.

Требование 4. Образующий полином РСНОС второго порядка, который генерирует М-последовательность, не должен быть симметричным сам к себе, т.е.: $a_{ij} \neq a_{(L-j)(L-i)}$.

Определение: Два полинома с максимальной степенью *L* будем называть *симметричными полиномами*, если РСНОС на их основе будут порождать симметричные последовательности. То есть, если два полинома вырабатывают две различные последовательности Q_1 и Q_2 с периодом *T*, то для любой точки отсчета в последовательности Q_1 найдется точка отсчета в последовательности Q_2, такая, что при чтении справа налево (слева направо) для последовательности Q_1 она будет полностью идентична последовательности Q_2 при чтении слева направо (справа налево) на всем периоде *T*.

Кроме того в работе [6] представлены выражения обеспечивающие подсчет количества полиномов, не удовлетворяющих указанным выше требованиям. Так, если через $\Lambda^{1,2,3,4}$ обозначить количество полиномов, не удовлетворяющих выше перечисленным требованиям, а через Λ^m обозначим количество полиномов, не удовлетворяющих m-му требованию, то это множество будет определяться следующими формулами:

$$\Lambda^1 = \Lambda^2 = 2^{[n_L - 1]}, \quad \Lambda^3 = 2^{[n_L - (L-1)]} \cdot \left(2^{[L-1]} - 1\right),$$

$$\Lambda^4 = 2^{\left[\frac{L^2-k}{4}+L\right]}, \qquad \Lambda^{1,2,3,4} = 2^{[n_L]} \cdot \left(1 - 2^{-[L+1]}\right) + 2^{\left[\frac{L^2-k}{4}-1\right]}$$

где $k = 0$ – для четных L; $k = 1$ – для нечетных L.

Продолжим изучение полиномов и генерируемых на их основе последовательностей. Для этого рассмотрим ряд полиномов, у которых из всех слагаемых присутствует только одно линейное слагаемое (исходя из требования 1, это должно быть слагаемое наивысшего порядка, т.е. $a_{LL} = 1$) и любое количество нелинейных слагаемых. Для примера возьмем *L=4*, и рассмотрим полиномы вида:

$x^4 + x^2x^1 + 1$; $x^4 + x^3x^2 + 1$; $x^4 + x^3x^1 + x^2x^1 + 1$; $x^4 + x^4x^1 + x^3x^1 + x^2x^1 + 1$ и так далее.

Если изучить последовательности, которые генерируют такие полиномы при различных начальных состояниях, то можно увидеть, что из всего множества колец состояний, которые будут принимать регистры (и из всех возможных периодов *T*), во всех случаях будет иметь место одно и тоже кольцо состояний регистра ($1000 \to 0100 \to 0010 \to 0001 \to 1000$) с периодом равным длине РСНОС.

Перемножение двух любых ячеек такого регистра, при начальном заполнении ячеек регистра одной единицей и всеми нулями, дает в результате всегда ноль. Следовательно, любой РСНОС при рассмотренном начальном заполнении будет эквивалентен (*порождать идентичную последовательность*) полиному вида – $x^L + 1$. На основе вышеизложенного, сформулируем очередное требование.

Требование 5. У полинома на основе РСНОС второго порядка, который может генерировать последовательность максимального периода, должно быть больше одного ($a_{LL} = 1$ из требования 1) линейного коэффициента обратных связей, т.е.:

$$\sum_{i=1}^{L-1} a_{ii} \geq 1$$

Получим оценку количества РСНОС, которые не удовлетворяют требованию 5 и, следовательно, могут быть исключены из рассмотрения при поиске М-полинома только из анализа образующего полинома.

Обозначим через Λ^5 полное количество РСНОС длины L, которые не удовлетворяют требованию 5. Расположим коэффициенты обратных связей в виде матрицы

$$\begin{matrix} a_{11} & a_{12} & a_{13} & \dots & a_{1L} \\ & a_{22} & a_{23} & \dots & a_{2L} \\ & & a_{33} & \dots & a_{3L} \\ & & & \dots & \dots \\ & & & & a_{LL} \end{matrix}. \qquad (2)$$

Тогда Λ^5 будет соответствовать множеству возможных комбинаций значений коэффициентов a_{ij}, исключая главную диагональ (*так как на ней расположены коэффициенты только линейной обратной связи*) и коэффициента a_{LL}. Число таких комбинаций составляет 2^{t+1}, где: t – количество коэффициентов нелинейных обратных связей; 2^1 – число вариаций с коэффициентом a_{LL}. Значение t можно определить из рассматриваемого треугольника (2)

$$\frac{L\cdot(L-1)}{2}.$$

Таким образом, полное количество РСНОС длины L, не удовлетворяющих требованию 5, будет равно:

$$\Lambda^5 = 2^{\frac{L\cdot(L-1)}{2}+1}.$$

Учитывая, что $n_L - L = \frac{L\cdot(L+1)}{2} - L = \frac{L\cdot(L-1)}{2}$, вышеприведенное равенство можно представить как:

$$\Lambda^5 = 2^{n_L-(L-1)}.$$

Следует подчеркнуть, что множество полиномов, которые не соответствуют требованию 5, пересекается с множеством полиномов, которые отсекаются требованиями 1-4.

Пусть Λ – общее количество допустимых полиномов, которые образуют РСНОС второго порядка, т.е. таких, которые из полного множества всех возможных полиномов удовлетворяют предъявляемым к ним требованиям и, следовательно, могут генерировать М-последовательности.

С учетом выдвинутых пяти требований Λ будет определяться по формуле:

$$\Lambda = 2^{\left[\frac{L\cdot(L-1)}{2}-1\right]}\cdot\left(1-2^{[1-L]}\right) - 2^{\left[\frac{L^2-k}{4}-1\right]}\cdot\left(1-2^{\left[\frac{k-L}{2}\right]}\right)$$

где $k=0$ – для четных L; $k=1$ – для нечетных L.

Оставшиеся РСНОС с $L=4$, отвечающие требованиям 1÷5, но не генерирующие М-последовательность, будут генерировать кольца вида $(1010)\rightarrow(0101)\rightarrow(1010)$. Формирование колец такого вида происходит при условии, что присутствующие линейные и нелинейные коэффициенты a_{ij}, в указанных состояниях, будут друг друга компенсировать. Например, коэффициенты вида: $\underline{1}0\underline{1}0\ 010\ 00\ 1$; $\underline{1}\underline{1}\underline{1}0\ 000\ 00\ 1$ и симметричные им $01\underline{1}0\ 000\ \underline{1}0\ 1$; $00\underline{1}0\ 010\ \underline{1}0\ 1$ (здесь и далее при такой записи коэффициенты a_{ij} из выражения (1) будут представлены в линейной форме, т.е. – $a_{11}a_{12}a_{13}a_{14}\ a_{22}a_{23}a_{24}\ a_{33}a_{34}\ a_{44}$). Подчеркнутые комбинации, в указанных состояниях регистра, компенсируют друг друга. Причем, не важно, какие еще будут нелинейные комбинации, их сумма всегда (*в указанных состояниях*) даст ноль.

То же самое будет и при взаимном отсутствии подчеркнутых слагаемых. Компенсировать линейные обратные связи могут и линейные комбинации, как пример: $\underline{\underline{1}}100\,000\,\underline{\underline{10}}\,1$; $\underline{\underline{1}}000\,010\,\underline{\underline{10}}\,1$.

Для принятия регистрами исходного состояния необходимо, чтобы в результате второго такта на вход подавалась единица. Этого можно добиться, если только $a_{22} \neq 1$ и $a_{24} \neq 1$ или же $a_{22} = a_{24} = 1$, при условии, что $a_{44} = 1$ или же $a_{22} = 1$ или $a_{24} = 1$, при условии, что $a_{44} \neq 1$.

Рассмотрим вариант с L=5. В данном случае также будет присутствовать кольцо вида: $(10101) \to (01010) \to (10101)$. Но, в отличие от предыдущего случая, для получения такого кольца, необходимо, чтобы обратные связи в первом такте не компенсировали друг друга.

На втором такте, необходимым условием для повторения состояния РСНОС является наличие $a_{22} = 1$ или $a_{44} = 1$, или же нелинейного коэффициента $a_{24} = 1$, а также последняя из возможных комбинаций, когда все $a_{22} = a_{44} = a_{24} = 1$.

Полученный результат можно распространить и для более высоких значений L. На рис. 3 представлены коэффициенты для четного (L=6) и нечетного (L=7) количества регистров, а также аналогичные кольца с периодом $T = 2$. В круглые скобки взяты те коэффициенты, которые могут изменить генерируемое значение на первом такте работы, а в квадратные – влияющие на выходное значение, только на втором такте. Остальные коэффициенты a_{ij} можно опустить из рассмотрения, так как на любом такте они будут давать ноль.

(a_{11})	a_{12}	(a_{13})	a_{14}	(a_{15})	a_{16}
	$[a_{22}]$	a_{23}	$[a_{24}]$	a_{25}	$[a_{26}]$
		(a_{33})	a_{34}	(a_{35})	a_{36}
			$[a_{44}]$	a_{45}	$[a_{46}]$
				(a_{55})	a_{56}
					$[a_{66}]$

а)

(a_{11})	a_{12}	(a_{13})	a_{14}	(a_{15})	a_{16}	(a_{17})
	$[a_{22}]$	a_{23}	$[a_{24}]$	a_{25}	$[a_{26}]$	a_{27}
		(a_{33})	a_{34}	(a_{35})	a_{36}	(a_{37})
			$[a_{44}]$	a_{45}	$[a_{46}]$	a_{47}
				(a_{55})	a_{56}	(a_{57})
					$[a_{66}]$	a_{67}
						(a_{77})

б)

$(101010) \to (010101) \to (101010)$

в)

$(1010101) \to (0101010) \to (1010101)$

г)

Рис. 3 – Коэффициенты обратных связей для L=6 (а), L=7 (б) и последовательности, генерирующие такие системы для L=6 (в) и L=7 (*г*)

Следует обратить внимание, что в круглые скобки взяты коэффициенты a_{ij} у которых индексы i и j являются нечетными числами, а в квадратных только те коэффициенты a_{ij} у которых индексы i и j являются четными числами. Таким образом, на основании выше изложенного, можно сформулировать следующее утверждение.

Требование 6. Необходимым условием образующего М-полинома РСНОС второго порядка является одновременное невыполнение следующей пары условий:

- четность количества коэффициентов $a_{ij} = 1$, индексы i и j которых являются нечетными числами (на рис. 2 коэффициенты в круглых скобках);
- нечетность количества коэффициентов $a_{ij} = 1$, индексы i и j которых являются четными числами (на рис. 2 коэффициенты в квадратных скобках), или то же самое в формульном выражении:

$$\sum_{i,j \in A} a_{ij} \begin{cases} \text{четное число, где } A \text{ все множество нечетных чисел от 1 до } L; \\ \text{нечетное число, где } A \text{ все множество четных чисел от 1 до } L. \end{cases}$$

Количество полиномов, удовлетворяющих требованию 6 можно получить, рассмотрев запись коэффициентов a_{ij} в матричном виде (рис. 3 (а) и (б)). Коэффициенты, взятые в круглые и квадратные скобки, если их взять по отдельности, образуют треугольник, эквивалентный исходному треугольнику, но со сторонами в два раза меньшими. Это позволяет получить методику для подсчета количества возможных комбинаций из указанных коэффициентов. Обозначим через Λ^6 количество комбинаций a_{ij}, которые не удовлетворяют требованию № 6. Тогда Λ^6 определяется как:

$$\Lambda^6 = 2^{\left\lfloor \frac{L\cdot(L+1)}{2}-2 \right\rfloor}.$$

Исключая пересекаемое множество полиномов одновременно не удовлетворяющее нескольким из вышеприведенных требований, получим выражение для точного подсчета количества полиномов, не удовлетворяющих требованиям с 1 по 6, для $L \geq 4$:

$$\Lambda^{1,2,3,4,5,6} = 2^{n_L-1} + \frac{1}{2}\cdot 2^{n_L-1} + \frac{1}{4}\cdot\left\{ 2^{n_L-(L-1)}\cdot(2^{L-1}-1) + \frac{1}{2^{L-1}}\cdot\left(2^{\frac{L^2-k}{4}+L} + 2^{n_L-(L-1)} + \right.\right.$$
$$\left.\left. + 2^{n_L-2} - \left[2^{\frac{L^2-k}{4}+L-\frac{L-k}{2}} + k\cdot 2\cdot 2^{\frac{L^2-k}{4}+L-2} + 2^{n_L-L-1} - k\cdot 2\cdot 2^{\frac{L^2-k}{4}-\frac{L-k}{2}+L-2} \right] \right) \right\}, \quad (3)$$

где $k=0$, при L – четном; $k=1$, при L – нечетном.

Выражение (3) позволяет определить точное количественное значение числа полиномов, не отвечающих предъявленным к ним требованиям и, следовательно, не способных сгенерировать последовательность с максимальным периодом.

4 Количественная оценка полученных результатов

Таким образом, сформулированы еще два требования (5 и 6) к виду полиномов, которые дополнительно исключают полиномы, не являющиеся М-полиномами. Рассмотрим влияние каждого требования на алгоритм поиска М-полиномов.

Для ускорения расчетов имеет смысл оценить какую часть из всего множества можно исключить, проведя анализ вида образующего полинома РСНОС с точки зрения предъявленных требований, а также – в какой последовательности желательно проводить тестирование, чтобы повысить вероятность отсечки не М-полиномов на начальном этапе проверки.

На рис. 4 приведены расчетные значения полиномов: - полное множество возможных полиномов (Λ_0) для заданного L; - количество полиномов, которые удовлетворяют требованиям 1÷6 (т.е. $\Lambda_0 - \Lambda^{1,2,3,4,5,6}$) и могут потенциально генерировать М-последовательность; - количество полиномов которые генерируют последовательность максимальной длины (*установленное вычислительным путем*); - полное множество возможных полиномов для РСЛОС (*это частный случай РСНОС при котором все нелинейные коэффициенты обратных связей равны нулю*).

Представленные на рис. 4 данные позволяют качественно оценить множество полиномов, которые можно использовать в генераторах поточных шифров, а также обеспечивают возможность оценить тенденцию их увеличения с ростом L. В этой связи важно подчеркнуть, что при проектировании поточных шифров на основе РСНОС количество возможных вариантов образующих М-полиномов многократно превосходит количество возможных схем для РСЛОС (*включающих в себя даже не М-последовательности*) при одинаковых L.

Приведем число образующих полиномов РСНОС не удовлетворяющих всем вышеперечисленным требованиям. Для количественной оценки воспользуемся нормированными величинами. Полученные данные сведены в Таблицу 1 (*где Λ^m - множество полиномов, не удовлетворяющих одному из шести сформулированных требований; m - номер требования предъявляемого к виду полиному*).

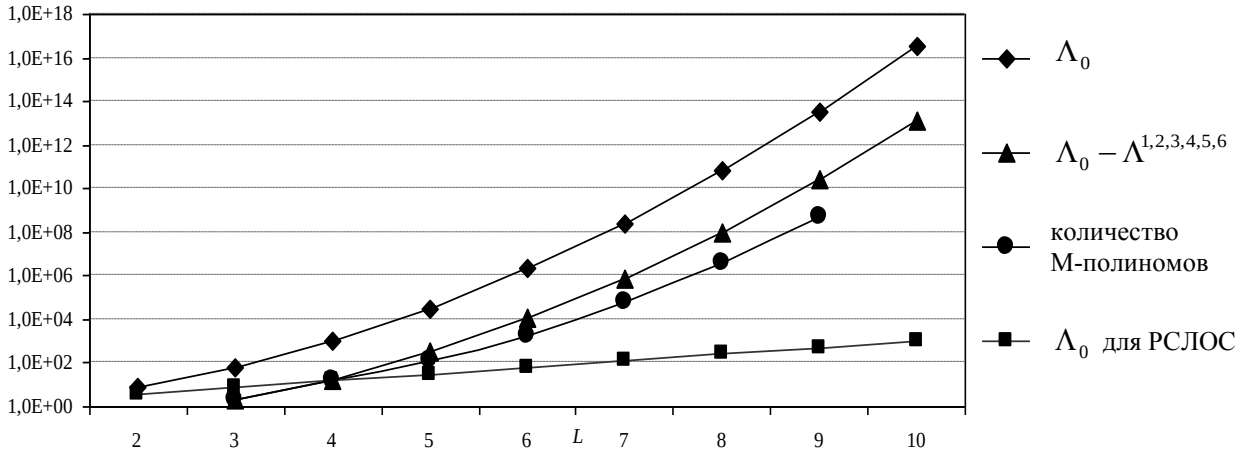


Рис. 4 – Количество полиномов в зависимости от длины РСНОС

Анализ данных таблицы позволяет утверждать, что при предъявлении к виду полинома требований 1÷6, уже при *L=10* отсекается порядка 99,9% от всего множества полиномов, причем с ростом значения *L (следует из (3))* этот процент растет по степенной зависимости.

Таблица 1 – Относительное количество полиномов, не удовлетворяющих требованиям 1÷6

L	Λ_0	$\frac{\Lambda^1}{\Lambda_0}$	$\frac{\Lambda^2}{\Lambda_0}$	$\frac{\Lambda^3}{\Lambda_0}$	$\frac{\Lambda^4}{\Lambda_0}$	$\frac{\Lambda^5}{\Lambda_0}$	$\frac{\Lambda^6}{\Lambda_0}$	$\frac{\Lambda^{1,2,3,4,5,6}}{\Lambda_0}$
2	8	0,5	0,5	0,5	1	0,5	0,25	1,000000
3	64	0,5	0,5	0,75	0,5	0,25	0,25	0,968750
4	1024	0,5	0,5	0,875	0,25	0,125	0,25	0,984375
5	32768	0,5	0,5	0,9375	0,0625	0,0625	0,25	0,989380
6	2097152	0,5	0,5	0,96875	0,015625	0,03125	0,25	0,994431
7	$2{,}7\cdot10^{8}$	0,5	0,5	0,984375	0,001953	0,015625	0,25	0,997119
8	$6{,}9\cdot10^{10}$	0,5	0,5	0,992188	0,000244	0,007813	0,25	0,998547
9	$3{,}5\cdot10^{13}$	0,5	0,5	0,996094	$1{,}5\cdot10^{-5}$	0,003906	0,25	0,999270
10	$3{,}6\cdot10^{16}$	0,5	0,5	0,998047	$9{,}5\cdot10^{-7}$	0,001953	0,25	0,999635
11	$7{,}4\cdot10^{19}$	0,5	0,5	0,999023	$3{,}0\cdot10^{-8}$	0,000977	0,25	0,999817
12	$3{,}0\cdot10^{23}$	0,5	0,5	0,999512	$9{,}3\cdot10^{-10}$	0,000488	0,25	0,999908
13	$2{,}5\cdot10^{27}$	0,5	0,5	0,999756	$1{,}5\cdot10^{-11}$	0,000244	0,25	0,999954
14	$4{,}1\cdot10^{31}$	0,5	0,5	0,999878	$2{,}3\cdot10^{-13}$	0,000122	0,25	0,999977

Кроме того из таблицы 1 следует, что максимальный вклад в отсечении полиномов, не генерирующих М-последовательность, дает требование № 3. Таким образом, при осуществлении поиска М-полиномов из всего множества возможных, для заданного *L*, необходимо в первую очередь проверять его на соответствие требованию № 3, а затем требованиям 1, 2 и 6. После этого осуществляется проверка требованию 5 и в последнюю очередь требованию 4.

В пользу указанного алгоритма выбора полиномов говорит тот факт, что проверку на соответствия требованиям № 3 и № 1 легко реализовать программным способом, при этом затрачиваемое машинное время – меньше, чем при проверке на соответствие требованиям №№ 2, 4 и 6.

Подводя итог вышесказанному, следует отметить следующее: - несмотря на малое количество полиномов, отсекаемых требованием № 4 *(по сравнению с требованием 3)*, им все же нельзя пренебрегать. Так, например, при больших значениях *L* требование 4 все равно отсекает достаточно большое множество не М-полиномов. При этом сложность при проверке с

помощью анализа генерируемой последовательности или другими известными способами, намного выше, чем анализ вида полинома.

В качестве примера приведем следующие расчеты: для $L=9$ число возможных полиномов $\Lambda_0 = 35\,184\,372\,088\,832$ (возьмем за 100%); требованием 3 отсекается 35 046 933 135 360 полиномов (что составляет 99,6%); остаток 137 438 953 472 полиномов (0,39%). При предъявлении к виду полиномов требований с 1 по 6 остается 25 668 894 720 полиномов (0,073%), что в 5,4 раза меньше, чем предыдущее число. При этом количество М-полиномов, полученных экспериментальным путем, будет всего 519 239 794, что составляет 0,0015% от общего множества или же 2% от множества полиномов соответствующих требованиям 1÷6.

Ссылки

[1] Ivanov M.A. Kriptograficheskie metody zashchity informatsii v komp'yuternykh sistemakh i setyakh / M.A. Ivanov . – Moskva: Kudits-obraz, 2001. – 368 s.
[2] Beth T. The stop-and-go generator, Proceeding Eurocrypt / T. Beth, F.C. Piper // Springer- Verlag Lecture Notes in Computer Science. – 1984 . – №209.
[3] Chambers W.G. Clock-controlled shift-registers in binary sequence generators / W.G. Chambers // IEEE Proceedings. – 1988. – 135 p.
[4] Klapper A. Large periods nearly de Bruijn FCSR sequences / A. Klapper, M. Goresky. – Cryptology EuroCrypt, 1995.
[5] Potochnye shifry / Asoskov A.V., Ivanov M.A., Mirskii A.A. i dr. – Moskva: Kudits-obraz, 2003. – 336 s.
[6] Potii A.V. Analiz svoistv registrov sdviga s nelineinoi obratnoi svyaz'yu vtorogo poryadka generiruyushchikh posledova-tel'nost' s maksimal'nym periodom / A.V. Potii, N.A. Poluyanenko // Prikladnaya radioelektronika. – 2008. – № 3. – S. 282-290.
[7] Stasev Yu.V., Potii A.V, Izbenko Yu.A. Issledovanie metodov kriptoanaliza potochnykh shifrov [Elektronnyi resurs]. – Rezhim dostupa: http://www.nrjetix.com/fileadmin/doc/publications/articles/stasev_potiy_izbenko_ru.pdf.

Reviewer: Viktor Dolgov, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: dolgovvi@mail.ru

Received: February 2016.

Authors:
Oleksandr Potii, Doctor of Sciences (Engineering), Full Professor, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: potav@ua.fm
Nikolay Poluyanenko, applicant of the Department of ITS, Kharkiv National University of Radio Electronics. E-mail: rsnos@mail.ua

The selection of forming polynomials for shift register with nonlinear feedback second order that generates the sequence with maximum period.

Abstract. Model pseudo-random sequence generator based on shift registers with nonlinear feedback second order is considered. Additional requirements for type of polynomial are formulated. They limit the set of polynomials which generate a sequence with maximum period. The expression to determine the number of polynomials that do not meet the requirements is given. Quantitative estimation of the impact of each request on cuts the set of polynomials is given. Recommendations for the use of these requirements are formulated.

Keywords: stream ciphers, shift registers, nonlinear systems.

Рецензент: Віктор Долгов, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: dolgovvi@mail.ru

Надійшло: лютий 2016.

Автори:
Олександр Потій, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: potav@ua.fm
Микола Полуяненко, здобувач кафедри БІТ, Харківській національний університет радіоелектроніки. E-mail: rsnos@mail.ua

Вибір утворюючих поліномів для регістра зсуву з нелінійним зворотним зв'язком другого порядку, що генерують послідовність з максимальним періодом.

Анотація. Розглянуто модель генератора псевдовипадкової послідовності на основі регістрів зсуву з нелінійним зворотним зв'язком другого порядку. Сформульовано додаткові вимоги до виду полінома, що обмежують множену при виборі полінома, що генерує послідовність з максимальним періодом. Наведено вираз для визначення кількості поліномів, що не задовольняють наведеним вимогам. Надана кількісна оцінка впливу кожній з вимог на множену поліномів, що відсікається. Надані рекомендації щодо застосування зазначених вимог.

Ключові слова: потокові шифри, регістри зсуву, нелінійні системи.

UDC 621, 621.3.037.37

THE GOLDEN SECTION, FIBONACCI NUMBERS, MATHEMATICS OF HARMONY AND "GOLDEN" SCIENTIFIC REVOLUTION

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
goldenmuseum@rogers.com

Reviewer: Serghii Rassomakhin, Doctor of Sciences (Engineering), Full Professor, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
rassomakhin@karazin.ua

Received on May 2016

Abstract. *The Publishing House "World Scientific" recently published two fundamental books: Alexey Stakhov "The Mathematics of Harmony" (2009) and Alexey Stakhov and Samuil Aranson "The "Golden" Non-Euclidean Geometry" (2016). In the given article the author develops the Mathematics of Harmony and "Golden" Non-Euclidean Geometry as a new interdisciplinary direction of modern science based on the golden section, Fibonacci numbers and their generalizations. The newest discoveries in different fields of modern science based on the Mathematics of Harmony, namely, mathematics (a general theory of hyperbolic functions and a solution to Hilbert's Fourth Problem, algorithmic measurement theory and "golden" number theory), computer science (the "golden" information technology), crystallography (quasi-crystals), chemistry (fullerenes), theoretical physics and cosmology (Fibonacci-Lorentz transformations, the "golden" interpretation of special theory of relativity and "golden" interpretation of the Universe evolution), botany (new geometric theory of phyllotaxis), genetics ("golden" genomatrices) and so on, creats a general picture of the "Golden" Scientific Revolution, which can influence fundamentally on the development of modern science and education.*

Keywords: *golden section, mathematics of harmony, binomial coefficients, Pascal's triangle, Fibonacci and Lucas hyperbolic functions, Hilbert's Fourth Problem, Fibonacci matrices, "golden" matrices*.

The article is dedicated to the blessed memory of my father Peter Stakhov, student of historical faculty of Kharkov University and soldier of the famous Kharkov studbat, who died heroically in October 1941, near Moscow.

Alexey Stakhov

Preface

Differentiation of modern science and its division into separate branches do not allow often seeing the overall picture of science and the main trends of scientific development. However, in science there are research objects, which unite disparate scientific facts into a single picture. The *golden section* is one of these scientific objects. The ancient Greeks raised the *golden section* at the level of "aesthetic canon" and "major ratio" of the Universe. For centuries or even millennia, starting from **Pythagoras, Plato, Euclid,** this ratio was the subject of admiration and worship of eminent minds of humanity - in the Renaissance, **Leonardo da Vinci, Luca Pacioli, Johannes Kepler**, in the 19 century - **Zeizing, Lucas, Binet**. In the 20 century, the interest in this unique irrational number increased in the mathematical community, due to the works of Russian mathematician **Nikolay Vorobyov** and the American mathematician **Verner Hoggatt**.

We are developing in this article a new approach to Euclid's *Elements* (*Proclus hypothesis*) with purpose to find there the sources of new mathematical theory – the *Mathematics of Harmony*, based on the golden section and Platonic solids, and then basing on this approach to predict the most important trends and directions of modern science, which can lead to global processes in modern sci-

© Stakhov A., 2016

ence called *"Golden" Scientific Revolution*. The present article is a result of author's research in the field of the golden section, Fibonacci numbers and their applications in modern science [1-37].

In 1996 the lecture *The Golden Section and Modern Harmony Mathematics* (The Seventh International Conference on Fibonacci Numbers and Their Applications. Graz, Austria, July 15-19, 1996) [14] Alexey Stakhov put forward the concept of the Mathematics of Harmony as a new interdisciplinary direction of modern science. It plays an important integrating role for modern science and allows bringing together all scientific disciplines from the general point of view - the *golden section*. The ideas of the article [14] have been continued and generalized in two fundamental books published by World Scientific: Alexey Stakhov "*The Mathematics of Harmony. From Euclid to Contemporary Mathematics and Computer Science*" (2009) [11] and Alexey Stakhov and Samuil Aranson "The "Golden" Non-Euclidean Geometry" (2016) [83].

The main objective of this article is to consider modern science from this point of view. By means of collection and generalization of all the scientific facts and theories related to the *golden section*, the author have suddenly opened for himself the global picture of the Universe based on the *golden section*, and saw the main trend of modern science - the resurgence of the interest in the ideas of **Pythagoras, Plato and Euclid** on the numerical harmony of the Universe and the *golden section* what may result in the *"Golden" Scientific Revolution*. This revolution shows itself, first of all, in modern mathematics *("Golden" Fibonacci Goniometry* and *Hilbert's Fourth Problem*), theoretical physics (*Fibonacci-Lorentz transformations* and *"golden" interpretation of the Universe evolution*), and computer science (*«Golden» Information Technology*) and could become the basis for the mathematical education reform based on the ideas of harmony and the *golden section*.

1 Introduction

1.1. ***Mathematics. The Loss of Certainty.*** What is mathematics? What are its origins and history? What distinguishes mathematics from other sciences? What is the subject of mathematical research today? How does mathematics influence on the development of modern scientific revolution? What is a connection of mathematics and its history with mathematical education? All these questions always were interesting for both mathematicians, and representatives of other sciences. Mathematics was always a sample of scientific strictness. It is often named "Tsarina of Sciences," what is reflection of its special status in science and technology. For this reason, the occurrence of the book *Mathematics. The Loss of Certainty* [39], written by **Morris Kline** (1908-1992), Professor Emeritus of Mathematics Courant Institute of Mathematical Sciences (New York University), became a true shock for mathematicians. The book is devoted to the analysis of the crisis, in which mathematics found itself in the 20-th century as a result of its "illogical development."

Morris Kline's view on the deep connection of mathematics to theoretical natural sciences is expressed in the following words:

"Science had been the life blood and sustenance of mathematics. Mathematicians were willing partners with physicists, astronomers, chemists, and engineers in the scientific enterprise. In fact, during the 17th and 18th centuries and most of the 19th, the distinction between mathematics and theoretical science was rarely noted. And many of the leading mathematicians did far greater work in astronomy, mechanics, hydrodynamics, electricity, magnetism, and elasticity than they did in mathematics proper. Mathematics was simultaneously the queen and the handmaiden of the sciences."

However, according to the opinion of famous mathematicians **Felix Klein, Richard Courant** and many others, starting from 20-th century mathematics began to lose its deep connections with theoretical natural sciences and to concentrate its attention on its inner "pure" problems.

Thus, by following to **Felix Klein, Richard Courant** and other famous mathematicians, **Morris Kline** asserts that **the main reason of the contemporary crisis of mathematics is the severance of the relationship between mathematics and theoretical natural sciences, what is the greatest "strategic mistake" for the 20th century mathematics**.

1.2. *Dirac's Principle of Mathematical Beauty.* By discussing the fact why mathematics needs in theoretical natural sciences, we should address to *Dirac's Principle of Mathematical Beauty.* On May 13, 2006, the eminent Russian mathematician and academician Vladimir Arnold presented a public lecture: *"The complexity of finite sequences of zeros and units, and the geometry of finite functional spaces"* [40] at the Moscow Mathematical Society. Let us consider some of its general ideas. Arnold notes:

1. In my opinion, mathematics is simply a part of physics, that is, it is an experimental science, which discovers for mankind the most important and simple laws of nature.

2. We must begin with a beautiful mathematical theory. Dirac claims: "If this theory is really beautiful, then it necessarily appears as a perfect model of important physical phenomena. It is necessary to search for these phenomena to develop applications of the beautiful mathematical theory and to interpret them as predictions of new laws of physics." Thus, according to Dirac, all new branches of physics, including relativistic and quantum, are developing in this way.

At Moscow University there is a tradition that the distinguished visiting-scientists are requested to write on a blackboard a self-chosen inscription. When Dirac visited Moscow in 1956, he wrote *"A physical law must possess mathematical beauty."* This inscription is the famous *Principle of Mathematical Beauty* that Dirac developed during his scientific life. No other modern physicist has been preoccupied with the concept of beauty more than Dirac.

Paul Adrien Maurice Dirac
(1902-1984)

Thus, according to Dirac, the *Principle of Mathematical Beauty* is the primary criterion for a mathematical theory to be used as a model of physical phenomena. Of course, there is an element of subjectivity in the definition of the "beauty" of mathematics, but the majority of mathematicians agrees that "beauty" in mathematical objects and theories nevertheless exist.

Let's examine some of "beautiful" mathematical objects, which have a direct relation to the theme of this article.

1.3. *Platonic Solids.* We can find the beautiful mathematical objects in Euclid's *Elements*. As is well known, in Book XIII of his *Elements* Euclid presented a theory of 5 regular polyhedrons called *Platonic Solids* (Fig.1). Really, these remarkable geometrical figures got very wide applications in theoretical natural sciences; in particular, in crystallography (*quasi-crystals*), chemistry (*fullerenes*), biology and so on what is brilliant confirmation of *Dirac's Principle of Mathematical Beauty.*

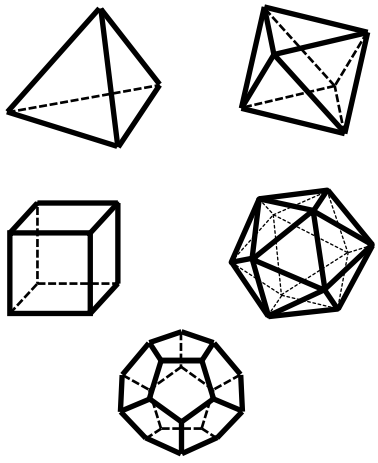


Fig. 1 - Platonic Solids: *tetrahedron, octahedron, cube, icosahedron, dodecahedron*

1.4. ***Binomial coefficients, the binomial formula, and Pascal's triangle.***

For the given non-negative integers *n* and *k*, there is the following beautiful formula that sets the *binomial coefficients*:

$$C_n^k = \frac{n!}{k!(n-k)!}, \tag{1}$$

where $n!=1\times2\times3\times\ldots\times n$ is a *factorial* of *n.*

One of the most beautiful mathematical formulas, the *binomial formula*, is based upon the *binomial coefficients*:

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \ldots + C_n^k a^{n-k}b^k + \ldots + C_n^{n-1}ab^{n-1} + b^n. \tag{2}$$

There is a very simple recurrence method for the calculation of the *binomial coefficients* based on their following graceful properties called *Pascal's rule*:

$$C_{n+1}^k = C_n^{n-1} + C_n^k. \tag{3}$$

By using the recurrence relation (3) and taking into consideration that $C_n^0 = C_n^n = 1$ and $C_n^k = C_n^{n-k}$, we can construct the following beautiful table of *binomial coefficients* called *Pascal's triangle* (see Table 1).

Table 1 - Pascal's triangle

							1											
						1		1										
					1		2		1									
				1		3		3		1								
			1		4		6		4		1							
		1		5		10		10		5		1						
	1		6		15		20		15		6		1					
1		7		21		35		35		21		7		1				
	1		8		28		56		70		56		28		8		1	
1		9		36		84		126		126		84		36		9		1

1.4. ***Fibonacci and Lucas numbers.*** Let us consider the simplest recurrence relation:

$$F_n = F_{n-1} + F_{n-2}, \tag{4}$$

where $n=0,\pm1,\pm2,\pm3,\ldots$. This recurrence relation was introduced for the first time by the famous Italian mathematician **Leonardo of Pisa** (nicknamed **Fibonacci**).

For the seeds

$$F_0 = 0 \text{ and } F_1 = 1, \tag{5}$$

the recurrence relation (4) generates a numerical sequence called *Fibonacci numbers* (see Table 2).

In the 19th century the French mathematician **Francois Edouard Anatole Lucas** (1842-1891) introduced the so-called *Lucas numbers* (see Table 2) given by the recurrence relation

$$L_n = L_{n-1} + L_{n-2} \tag{6}$$

with the seeds

$$L_0 = 2 \text{ and } L_1 = 1 \tag{7}$$

Table 2 shows the so-called "extended" Fibonacci and Lucas numbers, which are considered for positive and negative values of the index n. It follows from Table 2 that the "extended" Fibonacci and Lucas numbers build up two infinite numerical sequences, each possessing graceful mathematical properties.

Table 2 - The "extended" Fibonacci and Lucas numbers

n	***0***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
F_n	*0*	*1*	*1*	*2*	*3*	*5*	*8*	*13*	*21*	*34*	*55*
F_{-n}	*0*	*1*	*-1*	*2*	*-3*	*5*	*-8*	*13*	*-21*	*34*	*-55*
L_n	*2*	*1*	*3*	*4*	*7*	*11*	*18*	*29*	*47*	*76*	*123*
L_{-n}	*2*	*-1*	*3*	*-4*	*7*	*-11*	*18*	*-29*	*47*	*-76*	*123*

As can be seen from Table 2, for the odd indices $n=2k+1$ the elements F_n and F_{-n} of the *Fibonacci sequence* coincide, that is, $F_{2k+1}=F_{-2k-1}$, and for the even indices $n=2k$ they are opposite in sign, that is, $F_{2k}=-F_{-2k}$. For the Lucas numbers L_n all is vice versa, that is, $L_{2k}=L_{-2k}; L_{2k+1}=-L_{-2k-1}$.

1.5. ***Cassini' formula.*** In the 17th century the famous astronomer **Giovanni Domenico Cassini** (1625-1712) deduced the following beautiful formula, which connects three adjacent "extended" Fibonacci numbers in the Fibonacci sequence:

$$F_n^2 - F_{n-1}F_{n+1} = (-1)^{n+1}. \tag{8}$$

This wonderful formula evokes a reverent thrill, if we imagine that this formula is valid for any value of *n* (*n* can be any integer within the limits of $-\infty$ to $+\infty$). The alternation of +1 and -1 in the formula (8) within the sequential passage of all "extended" Fibonacci sequence leads to genuine aesthetic enjoyment by its rhythm and beauty.

1.6. **The Golden Section.** *If we take the ratio of two adjacent Fibonacci numbers F_n / F_{n-1} and direct this ratio towards infinity, we come at the following unexpected result:*

$$\lim_{n\to\infty}\frac{F_n}{F_{n-1}} = \Phi = \frac{1+\sqrt{5}}{2}, \tag{9}$$

where Φ is the famous irrational number, which is the positive root of the algebraic equation:

$$x^2 = x+1. \tag{10}$$

The number Φ has many beautiful names – *the golden section, golden number, golden mean, golden proportion,* and *the divine proportion* (see **Scott Olsen,** page 2 [40]).

The *golden section* or *division of a line segment in extreme and mean ratio* descended to us from Euclid's *Elements* [42]. Over the many centuries the *golden section* has been the subject of enthusiastic worship by outstanding scientists and thinkers including **Pythagoras, Plato, Leonardo da Vinci, Luca Pacioli, Johannes Kepler** and several others.

Note that formula (9) is sometimes called *Kepler's formula* after **Johannes Kepler** (1571-1630) who deduced it for the first time. Many outstanding mathematicians of the past century have proved the uniqueness of the *golden ratio* among other real numbers. In this connection, we should like to draw attention to the brochures of the Russian mathematicians **Alexander Khinchin** (1894-1959) [43] and **Nikolay Vorobyov** (1925-1995) [44]. As it is shown in these works, the unique feature of the *golden ratio* for number theory is the fact that among all irrational numbers **the *golden ratio* is most slowly approximated by rational fractions.** That is, we are talking about the representation of *golden ratio* in the form of a continued fraction as follows:

$$\Phi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + ...}}} \tag{11}$$

If now we will be approximating the *golden ratio* (11) by rational fractions m/n, which are convergent for Φ, then we come to the numerical sequence consisting of the ratios of the neighboring Fibonacci numbers:

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, ... \to \Phi = \frac{1+\sqrt{5}}{2}.$$

But these ratios represent the famous botanic *Law of phyllotaxis* [45], according to which pine cones, cacti, pineapples, sunflower heads, etc are formed. In other words, Nature uses the unique mathematical feature of the *golden ratio* in its remarkable constructions! This means that the *golden ratio* is not "mathematical fiction" because this unique irrational number exists in Nature! That is, the Fibonacci numbers are a brilliant embodiment of *Dirac's Principle of Mathematical Beauty.*

1.7. ***Binet's formulas.*** In the *19th* century, French mathematician **Jacques Philippe Marie Binet (**1786-1856**)** deduced the two magnificent *Binet's formulas*:

$$F_n = \frac{\Phi^n - (-1)^n \Phi^{-n}}{\sqrt{5}}; \; L_n = \Phi^n + (-1)^n \Phi^{-n}. \tag{12}$$

The analysis of *Binet's formulas* (12) gives us a possibility to feel "aesthetic pleasure" and once again to be convinced in the power of human intellect! Really, we know that the Fibonacci and Lucas numbers F_n and L_n always are integers. On the other hand, any power of the *golden ratio* is irrational number. It follows from *Binet's formulas* (12) that the integer numbers F_n and L_n can be represented as the difference or the sum of irrational numbers, the powers of the *golden ratio*!

1.8. ***How the golden mean is reflected in modern mathematics and mathematical education?*** It is well known the following Kepler's quote, concerning the *golden ratio*:

"Geometry has two great treasures: one is the Theorem of Pythagoras; the other, the division of a line into extreme and mean ratio. The first, we may compare to a measure of gold; the second we may name a precious stone."

Johannes Kepler (1571-1630)

The above Kepler's statement raises the significance of the *golden ratio* on the level of *Pythagorean Theorem,* one of the most famous theorems of geometry. As a result of the unilateral approach to mathematical education each schoolboy knows *Pythagorean Theorem*, but he has rather vague idea about the *golden ratio,* the second "treasure of geometry." The majority of school textbooks on geometry originate to Euclid's *Elements*. But then we can ask the question: why in the majority of them there is very small description of Euclidean *golden ratio*? There is an impression that "the materialistic pedagogics" has thrown out the *golden ratio* from mathematical education on the dump of

the "doubtful scientific concepts" together with astrology and others esoteric sciences where the *golden ratio* is widely used. We can consider this sad fact as one of the "strategic mistakes" of modern mathematical education [32,33].

Alexey Losev (1893 - 1988), the Russian prominent philosopher and researcher for the aesthetics of Ancient Greece and Renaissance, expressed his relation to the *golden ratio* and *Plato's cosmology* in the following words (cited from [46]):

"From Plato's point of view, and generally from the point of view of all antique cosmology, the Universe is a certain proportional whole that is subordinated to the law of harmonious division, the golden ratio... Greek system of cosmic proportions is considered sometimes in literature as curious result of unrestrained and preposterous fantasy. Full anti-scientific helplessness sounds in the explanations of those who declare this. However, we can understand the given historical and aesthetical phenomenon only in the connection with integral comprehension of history, that is, by using dialectical-materialistic idea of culture and by searching the answer in peculiarities of the ancient social existence."

We can ask the question: how the *golden ratio* is reflected in contemporary mathematics? Unfortunately, the answer is the following: only in the most impoverished manner. In mathematics, Pythagoras and Plato's ideas are considered sometimes as a "curious result of unrestrained and preposterous fantasy." Therefore, the majority of mathematicians consider the study of the *golden ratio* and its applications as an empty pastime, which is unworthy for serious mathematicians.

Unfortunately, we can also find neglectful relation to the *golden ratio* in contemporary theoretical physics. In 2006 "BINOM" publishing house (Moscow) published the interesting scientific book *Metaphysics: Century XXI* [47]. In the Preface to the book, its compiler and editor Professor **Vladimirov** *(Moscow University)* wrote:

"The third part of this book is devoted to a discussion of numerous examples of the manifestation of the golden ratio in art, biology and our surrounding reality. However, paradoxically, the golden ratio is not reflected enough in contemporary theoretical physics. In order to be convinced of this fact, it is enough to merely browse 10 volumes of Theoretical Physics by Landau and Lifshitz. The time has come to fill this gap in physics, all the more given that the golden ratio is closely connected with metaphysics and 'trinitarity' [the 'triune' nature of things]."

Thus, the neglect of the *golden ratio* and its scanty reflection in modern mathematics, mathematical education and theoretical physics is one more "strategic mistake" of modern mathematics, mathematical education and theoretical physics [32,33].

2. Proclus hypothesis: revolutionary idea in the mathematics history

As is known, the first mathematical knowledge originated in the ancient civilizations (Babylon, Egypt and other countries) and they were used for the solution of two important practical problems: *counting* of things and *measurement* of time and distances [48]. Ultimately, the *problem of counting* led to the first fundamental mathematical notion – *natural numbers*. The *problem of measurement* underlies *geometry* origin and then, after the discovery of *incommensurable line segments*, led to the second fundamental mathematical notion – *irrational numbers*. Natural and irrational numbers are the basic notions of the *Classical Mathematics*, which had originated in the ancient Greek science. When we study the ancient Greek science, we should point out on one more important problem, which had influenced fundamentally on the development of the Greek science, including mathematics. We are talking on the *harmony problem*, which was formulated for the first time by Pythagoras, Plato and other ancient thinkers. The harmony problem was connected closely with the *golden ratio*, which was raised in the ancient Greece to the level of aesthetic canon and main mathematical constant of the Universe.

There is very interesting point of view on Euclid's *Elements* suggested by **Proclus Diadochus** (412-485), the best commentator on Euclid's *Elements* [49]. As it is well-known, the concluding book of Euclid's *Elements*, Book XIII, is devoted to the description of the theory of the *five regular polyhedra* (Fig. 1), which played a predominate role in *Plato's cosmology*. They are well known in modern science under the name *Platonic Solids*.

Proclus had paid special attention to this fact. Usually, the most important data are presented in the final part of a scientific work. Based on this fact, Proclus put forward hypothesis that Euclid created his *Elements* primarily not for the description of the axiomatic approach to geometry (although this is very important), but in order to give a systematic theory of the construction of the 5 Platonic Solids, in passing throwing light on some of the most important achievements of the ancient Greek mathematics. Thus, Proclus' hypothesis allows one to suppose that it was well-known in ancient science that the *Pythagorean Doctrine on the Numerical Harmony of the Cosmos* and *Plato's Cosmology*, based on the regular polyhedra, were embodied in Euclid's *Elements*, the greatest Greek work of mathematics. From this point of view, **we can interpret Euclid's *Elements* as the first attempt to create a Mathematical Theory of Harmony what was the primary idea of the ancient Greek science**. This historical information is primary data for the development of new approach to the history of mathematics, described in [29,33,35,36].

A new approach to the mathematics origins is presented in Fig. 2. We can see that three "key" problems - *counting problem, measurement problem*, and *harmony problem* - underlie mathematics origin. The first two "key" problems resulted in the origin of two fundamental mathematics notions - *natural numbers* and *irrational numbers* that underlie the *Classical Mathematics*. The *harmony problem,* connected with the *division in the extreme and mean ratio* (Proposition II.11 of Euclid's *Elements*), resulted in the origin of the *Harmony Mathematics* - a new interdisciplinary direction of contemporary science, which has relation to contemporary mathematics, mathematical education, theoretical physics, and computer science. Such approach had resulted in the conclusion, which is unexpected for many mathematicians.

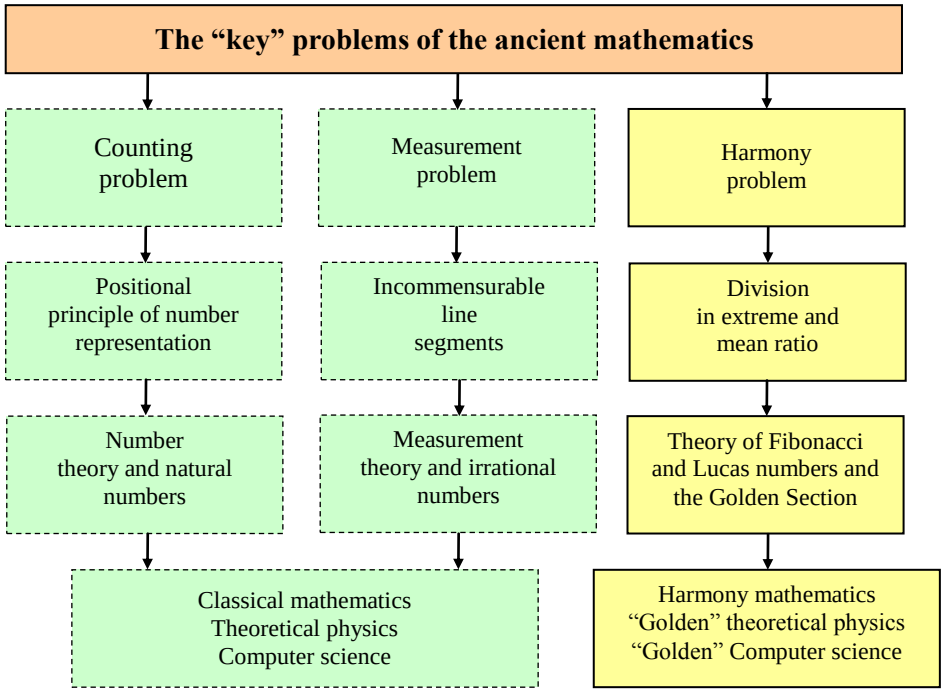


Fig. 2 - Three "key" problems of the ancient mathematics

Prove to be, in parallel with the *Classical Mathematics* one more mathematical direction - the *Harmony Mathematics* - was developing in ancient science. Similarly to the *Classical Mathematics,* the *Harmony Mathematics* takes its origin in Euclid's *Elements.* However, the *Classical Mathematics* accents its attention on "axiomatic approach," while the *Harmony Mathematics* is based on the *golden section* (Theorem II.11) and *Platonic Solids* described in the Book XIII of Euclid's *Elements.* Thus, Euclid's *Elements* is a source of two independent directions in the mathematics development - *Classical Mathematics* and *Harmony Mathematics*.

We affirm that the three greatest mathematical discoveries of the ancient mathematics – *positional principle of number representation, incommensurable line segments,* and *division in extreme and mean ratio (the golden section)* – were those mathematical discoveries, which influenced fundamentally on the mathematics at the stage of its origin. The *positional principle of number representation* (Babylon) became the "key" principle for the development of the concept of *natural numbers* and *number theory.* The *incommensurable line segments* led to the development of the concept of *irrational numbers.* The concepts of *natural numbers* and *irrational numbers* are two great mathematical concepts, which underlie the *Classical Mathematics.* The *division in extreme and mean ratio,* named later *the golden section,* is the third fundamental mathematical discovery, which underlies the *Mathematics of Harmony.*

During many centuries the main forces of mathematicians were directed on the creation of the *Classical Mathematics,* which became *Czarina of Natural Sciences.* However, the forces of many prominent mathematicians - since **Pythagoras, Plato** and **Euclid, Pacioli, Kepler** up to **Lucas, Binet, Vorobyov, Hoggatt** and so on - were directed on the development of the basic concepts and applications of the *Harmony Mathematics*. Unfortunately, these important mathematical directions developed separately one from other. A time came to unite the *Classical Mathematics* and the *Harmony Mathematics.* This unusual union can result in new scientific discoveries in mathematics and natural sciences. The newest discoveries in natural sciences, in particular, *Shechtman's quasicrystals* based on *Plato's icosahedron* (Nobel Prize of 2011) and *fullerenes* based on the *Archimedean truncated icosahedron* (Nobel Prize of 1996) do demand this union. All mathematical theories and directions should be united for one unique purpose to discover and explain Nature's Laws.

A new approach to the mathematics history (see Fig. 2) is very important for school mathematical education. This approach introduces in natural manner the idea of *harmony* and the *golden section* into school mathematical education. This allows to give pupils access to ancient science and to its main achievement – the *harmony idea* – and to tell them on the most important architectural and sculptor works of the ancient arts, based on the *golden section* (*Cheops pyramid, Nefertity, Parthenon, Doriphor, Venus* and so on).

3 The Mathematics of Harmony as a "beautiful" mathematical theory

The Mathematics of Harmony is described in [1-37]. The Mathematics of Harmony suggests new recurrence relations, which generates new numerical sequences and new numerical constants, which can be used for modeling different processes and phenomena of Nature. The most important of them are the following:

3.1. ***Generalized Fibonacci p-numbers***. For a given p=0, 1, 2, 3, ... they are given by the following general recurrence relation [1]:

$$F_p(n)=F_p(n-1)+F_p(n-p-1);\quad F_p(0)=0, F_p(1)=F_p(2)=...=F_p(p)=1. \quad (13)$$

Note that the recurrence formula (13) generates an infinite number of different recurrence sequences because every p generates its own recurrence sequences, in particular, the binary sequence 1, 2, 4, 8, 16, … for the case p=0 and classical Fibonacci numbers 1, 1, 2, 3, 5, 8, 13, … for the case p=1.

3.2. ***Generalized Lucas p-numbers*** are given by the following general recurrence relation:

$$L_p(n)=L_p(n-1)+L_p(n-p-1);\quad L_p(0)=p+1, L_p(1)=L_p(2)=...=L_p(p)=1, \quad (14)$$

where p= 0, 1, 2, 3, ... is a given non-negative integer.

Note that the recurrence formula (14) generates an infinite number of different recurrence sequences because every p generates its own recurrence sequences, in particular, the binary sequence 1, 2, 4, 8, 16, … for the case p=0 and classical Lucas numbers 2, 1, 3, 4, 7, 11, 18, … for the case p=1.

3.3. ***The golden p-proportions.*** It is easy to prove [1] that the ratio of the adjacent Fibonacci and Lucas *p*-numbers aims in limit ($n\to\infty$) for some constant, that is,

$$\lim_{n\to\infty}\frac{F_p(n)}{F_p(n-1)}=\frac{L_p(n)}{L_p(n-1)}=\Phi_p, \tag{15}$$

where Φ_p is a positive root of the following algebraic equation:

$$x^{p+1}=x^p+1, \tag{16}$$

which for $p=1$ is reduced to the algebraic equation (10).

Note that the result (15) is a generalization of *Kepler's formula* (9) for the classical Fibonacci and Lucas numbers ($p=1$).

The positive root of Eq. (16) was named *golden p-proportion* [1]. It is easy to prove [1] that the powers of the *golden p-proportions* are connected between themselves by the following identity:

$$\Phi_p^n=\Phi_p^{n-1}+\Phi_p^{n-p-1}=\Phi_p\times\Phi_p^{n-1}, \tag{17}$$

where $n=0,\pm1,\pm2,\pm3,\ldots$. It follows from (17) that each power of the "golden *p*-proportion" is connected with the preceding powers by the "additive" correlation $\Phi_p^n=\Phi_p^{n-1}+\Phi_p^{n-p-1}$ and by the "multiplicative" correlation $\Phi_p^n=\Phi_p\times\Phi_p^{n-1}$ (similarly to the classical "*golden mean*").

3.4. ***Generalized Fibonacci*** $\lambda-$***numbers.*** Let $\lambda>0$ is a given positive real number. Then we can consider the following recurrence relation [48-50]:

$$F_\lambda(n)=\lambda F_\lambda(n-1)+F_\lambda(n-2);\ F_\lambda(0)=0, F_\lambda(1)=1. \tag{18}$$

First of all, we note that for the case $\lambda=1$ the recurrence relation (18) is reduced to the recurrence relation (4), which for the seeds (5) generates the classical *Fibonacci numbers*: 0, 1, 1, 2, 3, 5, 8, 13, …. For other values of λ the recurrence relation (18) generates infinite number of new recurrence numerical sequences. In particular, for the case $\lambda=2$ the recurrence relation (18) generates the so-called *Pell numbers*: 0, 1, 2, 5, 12, 29, 70, … .

Table 3 shows the four "extended" Fibonacci λ-sequences, corresponding to the cases of $\lambda=1,2,3,4$.

Table 3 - The "extended" Fibonacci λ-numbers ($\lambda=1,2,3,4$)

n	0	1	2	3	4	5	6	7	8
$F_1(n)$	0	1	1	2	3	5	8	13	21
$F_1(-n)$	0	1	−1	2	−3	5	−8	13	−21
$F_2(n)$	0	1	2	5	12	29	70	169	408
$F_2(-n)$	0	1	−2	5	−12	29	−70	169	−408
$F_3(n)$	0	1	3	10	33	109	360	1189	3927
$F_3(-n)$	0	1	−3	10	−33	109	−360	1199	−3927
$F_4(n)$	0	1	4	17	72	305	1292	5473	23184
$F_4(-n)$	0	1	−4	17	−72	305	−1292	5473	−23184

3.5. ***Generalized Cassini's formula: a unique property of the Fibonacci*** λ***-numbers***. Cassini's formula (8) is one of the most remarkable identities for the classical Fibonacci numbers.

By studying the Fibonacci λ*-numbers*, **Alexey Stakhov** found in [38] the following unique mathematical property of the Fibonacci $\lambda-$*numbers*, which is true for all $\lambda=1,2,3,\ldots$:

$$F_\lambda^2(n)-F_\lambda(n-1)F_\lambda(n+1)=(-1)^{n+1}. \tag{19}$$

As for the case $\lambda=1$ the formula (19) is reduced to the well-known Cassini's formula (8), the formula (19) was named in [38] generalized Cassini's formula, which sounds as follows.

For the given $\lambda=1,2,3,...$ the quadrate of any Fibonacci λ-number $F_\lambda(n)$ are always different from the product of the two adjacent Fibonacci *λ-numbers* $F_\lambda(n-1)$ and $F_\lambda(n+1)$, which surround the initial Fibonacci *λ-number* $F_\lambda(n)$, by the number 1; herewith the sign of the difference of 1 depends on the parity of n: if n is even, then the difference of 1 is taken with the sign "minus", otherwise, with the sign "plus".

Until now, we have assumed that only the classic Fibonacci numbers have this unusual property, given by Cassini's formula (8). However, as is shown in [38], a number of such numerical sequences are infinite. All the Fibonacci *λ-numbers*, generated by the recurrence relation (18) have similar property, given by the generalized Cassini's formula (19)!

As is well known, a study of integer sequences is the area of number theory. The Fibonacci *λ-number* are integers for the cases *λ=1,2,3,…* . Therefore, for many mathematicians in the field of number theory, the existence of the infinite number of the integer sequences, which are given by (18) and satisfy to the generalized Cassini's formula (19), may be a great surprise!

3.6. ***Metallic means.*** It follows from (18) the following algebraic equation:

$$x^2-\lambda x-1=0, \tag{20}$$

which for the case $\lambda=1$ is reduced to (10). A positive root of Eq. (20) produces infinite number of new "harmonic" constants – the *golden λ-proportions*, which are expressed by the following general formula:

$$\Phi_\lambda=\frac{\lambda+\sqrt{4+\lambda^2}}{2}. \tag{21}$$

According to **Vera W. Spinadel** [50], the *golden λ-proportions* (21) are called also *metallic means* by analogy to the classical *golden mean.*

If we take $\lambda=1,2,3,4$ in (21), then we get the following mathematical constants having, according to **Vera W. Spinadel,** special titles:

$$\begin{gathered}\Phi_1=\frac{1+\sqrt{5}}{2}\ \left(\text{the golden mean, } \lambda=1\right);\ \Phi_2=1+\sqrt{2}\left(\text{the silver mean, } \lambda=2\right);\\ \Phi_3=\frac{3+\sqrt{13}}{2}\left(\text{the bronze mean, } \lambda=3\right);\Phi_4=2+\sqrt{5}\left(\text{the cooper mean, } \lambda=4\right).\end{gathered} \tag{22}$$

Other metallic means ($\lambda\geq 5$) do not have special names:

$$\Phi_5=\frac{5+\sqrt{29}}{2};\quad \Phi_6=3+2\sqrt{10};\quad \Phi_7=\frac{7+2\sqrt{14}}{2};\quad \Phi_8=4+\sqrt{17}.$$

The *metallic means* (21) possess two remarkable properties [49]:

$$\Phi_\lambda=\sqrt{1+\lambda\sqrt{1+\lambda\sqrt{1+\lambda\sqrt{...}}}};\quad \Phi_\lambda=\lambda+\cfrac{1}{\lambda+\cfrac{1}{\lambda+\cfrac{1}{\lambda+...}}}. \tag{23}$$

which are generalizations of similar properties for the classical *golden mean* $(\lambda=1)$:

$$\Phi=\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{...}}}};\quad \Phi=1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+...}}}. \tag{24}$$

4 Introduction into new theory on hyperbolic functions

4.1. ***A history of hyperbolic functions and hyperbolic geometry.*** Although **Johann Heinrich Lambert** (*1728-1777*), a French mathematician, is often credited with introducing hyperbolic functions, hyperbolic sine and cosine

$$sh(x)=\frac{e^x-e^{-x}}{2};\qquad ch(x)=\frac{e^x+e^{-x}}{2}, \tag{25}$$

it was actually **Vincenzo Riccati** (*1707-1775*), Italian mathematician, who did this in the middle of the 18th century. Riccati found the standard *addition formulas*, similar to trigonometric identities, for hyperbolic functions as well as their derivatives. He revealed the relationship between the hyperbolic functions and the exponential function. For the first time, Riccati used the symbols *sh* and *ch* for the hyperbolic sine and cosine.

In 1826, the Russian mathematician **Nikolay Lobachevski** (*1792-1856*) made revolutionary mathematical discovery. We are talking on the *non-Euclidean geometry*. This *Lobachevski's geometry* is also named *hyperbolic geometry* because all mathematical relations of *Lobachevski's geometry* are based on the hyperbolic functions (25). The first published work on non-Euclidean geometry, Lobachevski's article *About the Geometry Beginnings*, was published in 1829 in *The Kazan Bulletin.* Three years later Hungarian mathematician **Janosh Bolyai** (*1802-1860*) published the article on non-Euclidean geometry, called the *Appendix.* After Gauss' death it was clear that he also had developed geometry similar to those of Lobachevski and Bolyai. A revolutionary significance of hyperbolic geometry consists of the fact that this geometry is beginning of *hyperbolic ideas* in theoretical natural sciences. We recall two remarkable properties of classical hyperbolic functions (25):

$$\textbf{Parity property}: sh(-x)=-sh(x);\quad ch(-x)=ch(x). \tag{26}$$

$$\textbf{Analog of Phythagoras theorem}: ch^2x-sh^2x=1. \tag{27}$$

4.2. ***Hyperbolic Fibonacci and Lucas functions.*** In 1984 **Alexey Stakhov** published the book *Codes of the Golden Proportion* [3]. In this book *Binet's formulas* (12) were represented in the form not used in earlier mathematical literature:

$$F_n=\begin{cases}\dfrac{\Phi^n+\Phi^{-n}}{\sqrt{5}}, n=2k+1\\ \dfrac{\Phi^n-\Phi^{-n}}{\sqrt{5}}, n=2k\end{cases};\quad L_n=\begin{cases}\Phi^n+\Phi^{-n}, n=2k\\ \Phi^n-\Phi^{-n}, n=2k+1\end{cases}, \tag{28}$$

where $k=0,\pm1,\pm2,\pm3,\ldots$.

The similarity of *Binet's formulas* (28) to the classical hyperbolic functions (25) is so striking that the formulas (28) can be considered to be a prototype of a new class of hyperbolic functions, based on the *golden ratio*. That is to say, **Alexey Stakhov** in 1984 [3] predicted the appearance of a new class of hyperbolic functions, *hyperbolic Fibonacci and Lucas functions*. The first article on *hyperbolic Fibonacci and Lucas functions* was published by the Ukrainian mathematicians **Alexey Stakhov** and **Ivan Tkachenko** in 1993 [13] (by recommendation of academician **Yuri Mitropolski**). More recently, early of 21-th century, **Alexey Stakhov** and **Boris Rosin** have developed this idea further and introduced in [18] the so-called symmetrical hyperbolic Fibonacci and Lucas functions.

Symmetrical hyperbolic Fibonacci sine and cosine

$$sF(x)=\frac{\Phi^x-\Phi^{-x}}{\sqrt{5}};\ cF(x)=\frac{\Phi^x+\Phi^{-x}}{\sqrt{5}} \tag{29}$$

Symmetrical hyperbolic Lucas sine and cosine

$$sL(x)=\Phi^{x}-\Phi^{-x};\quad cL(x)=\Phi^{x}+\Phi^{-x}. \tag{30}$$

4.3. ***Hyperbolic and recursive properties of the symmetrical hyperbolic Fibonacci and Lucas functions***. Note that the symmetrical hyperbolic functions (29), (30), on the one hand, are similar to the classical hyperbolic functions (25), on the other hand, they are generated by *Binet's formulas* (28), given the *extended" Fibonacci and Lucas sequences*. This leads to the following features of the functions (29), (30), which we call ***hyperbolic*** and ***recursive*** properties of the functions (29), (30).

Hyperbolic properties

It is proved in [18], that the symmetrical hyperbolic Fibonacci and Lucas functions (29), (30) retain all the known properties of the classical hyperbolic functions (25). In this case, for example, the properties (26), (27) look as follows:

Parity property:

$$\begin{cases} sF(-x)=-sF(x); & cF(-x)=cF(x) \\ sL(-x)=-sL(x); & cL(-x)=cL(x) \end{cases} \tag{31}$$

Analogs of Pythagoras theorem:

$$\left[cF(x)\right]^{2}-\left[sF(x)\right]^{2}=\frac{4}{5};\left[cL(x)\right]^{2}-\left[sL(x)\right]^{2}=4. \tag{32}$$

Recursive properties

On the other hand, as it follows from a comparison of *Binet's formulas* (28) with the symmetrical functions (29), (30), the following unique properties connects the "extended" Fibonacci and Lucas sequences (28) with the symmetrical hyperbolical Fibonacci and Lucas functions (29), (30):

$$F_{n}=\begin{cases} sF(n) \text{ for } n=2k \\ cF(n) \text{ for } n=2k+1 \end{cases}; \tag{33}$$

$$L_{n}=\begin{cases} sL(n) \text{ for } n=2k+1 \\ cL(n) \text{ for } n=2k \end{cases}. \tag{34}$$

where $k=0,\pm1,\pm2,\pm3,\ldots$.

Note that **the property, given by the formulas (33), (34), is unique because the classical hyperbolic functions (25) do not possess such property**.

The properties (33), (34) gives us the right to name the functions (29), (30) the ***recursive hyperbolic functions.***

Let us consider the examples of the *recursive property* of the functions (29), (30) [18].

Theorem 1. *The following relations, which are similar to the recursive relations for the Fibonacci and Lucas numbers* $F_{n+2}=F_{n+1}+F_{n}$ *and* $L_{n+2}=L_{n+1}+L_{n}$, *are valid for the recursive hyperbolic Fibonacci and Lucas functions:*

Recursive relation for the Fibonacci hyperbolic functions:

$$\begin{aligned} sF(x+2)&=cF(x+1)+sF(x) \\ cF(x+2)&=sF(x+1)+cF(x) \end{aligned} \tag{35}$$

Recursive relation for the Lucas hyperbolic functions:

$$\begin{aligned} sL(x+2)&=cL(x+1)+sL(x) \\ cL(x+2)&=sL(x+1)+cL(x) \end{aligned}$$

Theorem 2 (a generalization of Cassini's formula for continues domain). *The following relations, which are similar to Cassini's formula* $F_n^2 - F_{n+1}F_{n-1} = (-1)^{n+1}$, *are valid for the recursive hyperbolic Fibonacci functions:*

Cassini's formula :

$$\left[sF(x)\right]^2 - cF(x+1)cF(x-1) = -1 \tag{36}$$
$$\left[cF(x)\right]^2 - sF(x+1)sF(x-1) = 1$$

4.4. ***Fibonacci and "golden" matrices: a unique class of square matrices***

Fibonacci Q-matrices

It is known that a square matrix *A* is called *non-singular*, if its determinant is not equal to zero, that is

$$\det A \neq 0. \tag{37}$$

In linear algebra, the non-singular square (n×n)-matrix is called invertible *because every non-singular matrix A has inverse matrix* A^{-1}, *which is connected with the initial* square *matrix A by the following correlation:*

$$AA^{-1} = I_n, \tag{38}$$

where I_n *is the identity (n×n)-matrix.*

The *Fibonacci Q-matrix*

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \tag{39}$$

introduced in [53] is a partial case of the non-singular matrix.

If we raise the *Q*-matrix (39) to the *n*-th power, we obtain:

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}. \tag{40}$$

It follows from *Cassini formula* (8), that the determinant of the *Q*-matrix (40) is equal:

$$\det Q^n = (-1)^n \tag{41}$$

Fibonacci G_λ-matrices

Alexey Stakhov introduced in [30] the so-called *Fibonacci* G_λ *– matrix*:

$$G_\lambda = \begin{pmatrix} \lambda & 1 \\ 1 & 0 \end{pmatrix}, \tag{42}$$

where $\lambda > 0$ is a given positive real number. It is clear that for the case $\lambda=1$ the Fibonacci G_λ *– matrix* (42) is reduced to the Fibonacci *Q-matrix* (39).

The Fibonacci G_λ *– matrix* (42) is generating matrix for the Fibonacci λ - *numbers* (18) and has the following properties [30]:

$$G_\lambda^n = \begin{pmatrix} F_\lambda(n+1) & F_\lambda(n) \\ F_\lambda(n) & F_\lambda(n-1) \end{pmatrix} \tag{43}$$

$$\det G_\lambda^n = (-1)^n. \tag{44}$$

The "golden" matrices

Alexey Stakhov has introduced in [26] a special class of the square matrices called *"golden" matrices*. Their peculiarity consists of the fact that the *hyperbolic Fibonacci functions* (29) are elements of these matrices. Let us consider the simplest of them [26]:

$$Q_0(x)=\begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix};\ Q_1(x)=\begin{pmatrix} sFs(2x+2) & cFs(2x+1) \\ cFs(2x+1) & sFs(2x) \end{pmatrix} \quad (45)$$

If we calculate the determinants of the matrices (45), we obtain the following unusual results:

$$\det Q_0(x)=1;\ \det Q_1(x)=-1. \quad (46)$$

4.5. ***Theory of Fibonacci Numbers as a "Degenerate" Case of the Theory of the Recursive Hyperbolic Fibonacci and Lucas Functions.*** As follows from Theorems 1 and 2, the two *"continuous"* identities (35), (36) for the recursive hyperbolic Fibonacci and Lucas functions always correspond to one *"discrete"* identity for the "extended" Fibonacci and Lucas numbers. Conversely, we can obtain the *"discrete"* identity for the "extended" Fibonacci and Lucas numbers by using two corresponding *"continuous"* identities for the recursive hyperbolic Fibonacci and Lucas functions (29), (30). As the "extended" Fibonacci and Lucas numbers, according to (33), (34), are the *"discrete"* cases of the recursive hyperbolic Fibonacci and Lucas functions (29), (30), this means that due the introduction of the *recursive hyperbolic Fibonacci and Lucas functions* (29), (30) [18], the classical *"theory of Fibonacci numbers"* [44] as if *"degenerates,"* because this theory is a partial (*"discrete"*) case of the more general (*"continuous*) theory of the *recursive hyperbolic Fibonacci and Lucas functions* (29), (30). This conclusion is another unexpected result, which follows from the theory of the recursive hyperbolic Fibonacci and Lucas functions [18]. Such approach requires a **revision** of the existed "theory of Fibonacci numbers" [44] from the point of view of the more general (continues) theory of the *recursive hyperbolic Fibonacci and Lucas functions* (29), (30).

5. General theory of the recursive hyperbolic functions

5.1. ***Gazale's formulas for Fibonacci and Lucas $\lambda-$numbers as analog of Binet's formulas.*** Based on the *metallic means* (21), **Midchat Gazale** deduced in [51] the following remarkable formula, which allows representing the *Fibonacci λ - numbers* by the *metallic means* (21):

$$F_\lambda(n)=\frac{\Phi_\lambda^n-(-1)^n\Phi_\lambda^{-n}}{\sqrt{4+\lambda^2}}. \quad (47)$$

The formula (47) was named in [30] *Gazale's formula for the Fibonacci λ - numbers* after **Midchat Gazale** [51].

Alexey Stakhov deduced in [30] *Gazale's formula for the Lucas λ - numbers*:

$$L_\lambda(n)=\Phi_\lambda^n+(-1)^n\Phi_\lambda^{-n} \quad (48)$$

Note that for the case $\lambda = 1$ the formulas (47) and (48) are reduced to *Binet's formulas* (12). The formula (48) is analytical representation of new recurrence sequence, *Lucas $\lambda-$numbers,* which are given by the recurrence formula:

$$L_\lambda(n)=\lambda L_\lambda(n-1)+L_\lambda(n-2);\ L_\lambda(0)=2, F_\lambda(1)=\lambda. \quad (49)$$

It is easy to prove [30] that *Gazale's formulas* can be represented in the following form:

$$F_\lambda(n)=\begin{cases} \dfrac{\Phi_\lambda^n-\Phi_\lambda^{-n}}{\sqrt{4+\lambda^2}} & \text{for} \quad n=2k \\ \dfrac{\Phi_\lambda^n+\Phi_\lambda^{-n}}{\sqrt{4+\lambda^2}} & \text{for} \quad n=2k+1 \end{cases} \quad (50)$$

$$L_\lambda(n)=\begin{cases} \Phi_\lambda^n-\Phi_\lambda^{-n} & \text{for} \quad n=2k+1 \\ \Phi_\lambda^n+\Phi_\lambda^{-n} & \text{for} \quad n=2k \end{cases} \quad (51)$$

Note that for the case *p=1 Gazale's formulas* (50), (51) are reduced to *Binet's formulas* (28). But *Binet's formulas* (12), (28) are well known in mathematics and belong to the category of outstand-

ing mathematical formulas, like *Euler's formula* and other formulas, which underlie the basis of mathematics. But *Gazale's formulas* (47), (48), (50), (51) are a generalization of *Binet's formulas* (12), (28) and therefore rightfully *Gazale's formulas* (47), (48), (50), (51) can be attributed to the category of outstanding mathematical formulas.

5.2. ***Self-similarity and recursion: Gazale's hypothesis.*** In mathematics, a **self-similar** object is exactly or approximately similar to a part of itself (i.e. the whole has the same shape as one or more of the parts). Many objects in the real world, such as coastlines, are statistically self-similar: parts of them show the same statistical properties at many scales. **Self-similarity** is a typical property of fractals and underlies botanic phenomenon of *phyllotaxis*. **Recursion** is the process of repeating items in a self-similar way and is brilliant example of reflection of *self-similarity principle* in mathematics. All the recurrent relations (4), (6), (13), (14), (18), (49) are based on the *self-similarity principle.*

Gazale's book *Gnomon. From Pharaohs to Fractals* [51] is devoted to mathematical justification of the *principle of self-similarity.* In this book, **Midhat Gazale** put forward the following hypothesis.

Gazale's hypothesis: *"A key role in the study of self-similarity play a numerical sequences, which I call here the Fibonacci sequence of the order m, where*

$$F_{m,n+2} = F_{m,n} + mF_{m,n+1}.\text{"} \tag{52}$$

If we compare the recurrence relation for the Fibonacci sequences of the order m, given by (52), to the introduced above Fibonacci λ*-numbers*, given by the recurrence relation (18), we come to the unexpected conclusion that the recurrence relations (18) and (52) coincide if we take: $m = \lambda$. This means that **the Fibonacci λ*-numbers* play a key role in the study of the principle of *self-similarity*.**

5.3. ***Recursive hyperbolic Fibonacci and Lucas λ-functions.*** In 2006 **Alexey Stakhov** has developed in [30] the so-called *hyperbolic Fibonacci and Lucas λ-functions,* which are a generalization of the *symmetrical hyperbolic Fibonacci and Lucas functions* (29), (30):

Hyperbolic Fibonacci λ-sine

$$sF_\lambda(x) = \frac{\Phi_\lambda^x - \Phi_\lambda^{-x}}{\sqrt{4+\lambda^2}} = \frac{1}{\sqrt{4+\lambda^2}}\left[\left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}\right)^x - \left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}\right)^{-x}\right] \tag{53}$$

Hyperbolic Fibonacci λ-cosine

$$cF_\lambda(x) = \frac{\Phi_\lambda^x + \Phi_\lambda^{-x}}{\sqrt{4+\lambda^2}} = \frac{1}{\sqrt{4+\lambda^2}}\left[\left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}\right)^x + \left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}\right)^{-x}\right] \tag{54}$$

Hyperbolic Lucas λ-sine

$$sL_\lambda(x) = \Phi_\lambda^x - \Phi_\lambda^{-x} = \frac{1}{\sqrt{4+\lambda^2}}\left[\left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}\right)^x - \left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}\right)^{-x}\right] \tag{55}$$

Hyperbolic Lucas λ-cosine

$$cL_\lambda(x) = \Phi_\lambda^x + \Phi_\lambda^{-x} = \frac{1}{\sqrt{4+\lambda^2}}\left[\left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}\right)^x + \left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}\right)^{-x}\right] \tag{56}$$

The formulas (53)-(56) give an infinite number of hyperbolic functions because every real number $\lambda > 0$ generates its own class of the hyperbolic functions (53)-(56). In particular, for the case $\lambda = 1$ the hyperbolic functions (53)-(56) are reduced to the *symmetrical hyperbolic Fibonacci and Lucas functions* (29), (30).

By comparing the *"extended" Fibonacci and Lucas* $\lambda-$*numbers*, represented by *Gazale's formulas* (50), (51) to the functions (53)-(56), it is easy to establish the following simple relationship between them:

$$F_\lambda\ n\ = \begin{cases} sF_\lambda\ n\ , & n = 2k \\ cF_\lambda\ n\ , & n = 2k+1 \end{cases}; L_\lambda\ n\ = \begin{cases} cL_\lambda\ n\ , & n = 2k \\ sL_\lambda\ n\ , & n = 2k+1. \end{cases} \tag{57}$$

For the case *p=1* the formulas (57) are reduced to the relationships (33), (34).

5.4. ***Hyperbolic and recursive properties of hyperbolic Fibonacci and Lucas λ-functions.*** Let us study the properties of the hyperbolic Fibonacci and Lucas λ-functions (53) – (56).

Hyperbolic properties (example)

As example of hyperbolic properties for the functions (53) – (56) we consider the formulas for **analogs of Pythagoras Theorem**:

$$\left[cF_\lambda(x)\right]^2 - \left[sF_\lambda(x)\right]^2 = \frac{4}{4+\lambda^2}; \left[cL_\lambda(x)\right]^2 - \left[sL_\lambda(x)\right]^2 = 4 \tag{58}$$

Note that for the case λ=1 the formulas (58) are reduced to the formulas (32).

Recursive properties (examples)

$$F_\lambda(n+2) = \lambda F_\lambda(n+1) + F_\lambda(n) \to \begin{cases} sF_\lambda(x+2) = \lambda cF_\lambda(x+1) + sF_\lambda(x) \\ cF_\lambda(x+2) = \lambda sF_\lambda(x+1) + cF_\lambda(x) \end{cases} \tag{59}$$

$$F_\lambda^2(n) - F_\lambda(n-1)F_\lambda(n+1) = (-1)^{n+1} \to \begin{cases} \left[sF_\lambda(x)\right]^2 - cF_\lambda(x+1)cF_\lambda(x-1) = -1 \\ \left[cF_\lambda(x)\right]^2 - sF_\lambda(x+1)sF_\lambda(x-1) = 1 \end{cases} \tag{60}$$

6 Hilbert's Fourth Problem and "Golden" Hyperbolic Geometry: revolution in hyperbolic geometry

6.1. ***Hilbert's Fourth Problem*****.** In the lecture *Mathematical Problems* presented at the *Second International Congress of Mathematicians* (Paris, 1900), **David Hilbert** (*1862 – 1943*) had formulated his famous 23 mathematical problems. These problems determined considerably the development of the 20th century mathematics. This lecture is a unique phenomenon in the mathematics history and in mathematical literature. The Russian translation of Hilbert's lecture and its comments are given in the work [54]. In particular, *Hilbert's Fourth Problem* is formulated in [54] as follows:

"Whether is possible from the other fruitful point of view to construct geometries, which with the same right can be considered the nearest geometries to the traditional Euclidean geometry".

In particular, **Hilbert** considered that *Lobachevski's geometry* and *Riemannian geometry* are nearest to the *Euclidean geometry*. In mathematical literature *Hilbert's Fourth Problem* is sometimes considered as formulated very vague what makes difficult its final solution. As it is noted in Wikipedia [55], *"the original statement of Hilbert, however, has also been judged too vague to admit a definitive answer."*

In spite of critical attitude of mathematicians to *Hilbert's Fourth Problem*, we should emphasize great importance of this problem for mathematics, particularly for geometry. Without doubts, Hilbert's intuition led him to the conclusion that *Lobachevski's geometry* and *Riemannian geometry*

do not exhaust all possible variants of non-Euclidean geometries. *Hilbert's Fourth Problem* directs attention of mathematicians at finding new non-Euclidean geometries, which are the nearest geometries to the traditional Euclidean geometry.

6.2. ***A solution to Hilbert's Fourth Problem based on the Mathematics of Harmony.*** As is known, the classical model of *Lobachevski's plane* in *pseudo-spherical coordinates* $(u,v), 0<u<+\infty, -\infty<v<+\infty$ with the Gaussian curvature *K= -1 (Beltrami's interpretation of hyperbolic geometry on pseudo-sphere)* has the following form:

$$(ds)^2=(du)^2+sh^2(u)(dv)^2, \tag{61}$$

where *ds* is an element of length and *sh*(*u*) is hyperbolic sine.

In connection with *Hilbert's Fourth Problem*, **Alexey Stakhov** and **Samuil Aranson** suggested in [83] an infinite set of models (in dependence on real parameter $\lambda>0$) of *Lobachevski's plane* at the coordinates (u,v), $0<u<+\infty$, $-\infty<v<+\infty$ of the *Gaussian curvature K= -1*, such that the metric form looks as follows:

$$(ds)^2=\ln^2(\Phi_\lambda)(du)^2+\frac{4+\lambda^2}{4}\left[sF_\lambda(u)\right]^2(dv)^2, \tag{62}$$

where $\Phi_\lambda=\frac{\lambda+\sqrt{4+\lambda^2}}{2}$ is the *metallic mean* and $sF_\lambda(u)$ is *hyperbolic Fibonacci λ-sine*.

The partial cases of the metric *λ-forms* of Lobachevski's plane (*golden, silver, bronze, cooper*), corresponding to different values of the parameter λ=1,2,3,4, are given in Table 4.

Table 4 – Metric λ-forms of Lobachevski's plane

Title	λ	Φ_λ	Analitical formula
General form	$\lambda>0$	$\Phi_\lambda=\frac{\lambda+\sqrt{4+\lambda^2}}{2}$	$(ds)^2=\ln^2(\Phi_\lambda)(du)^2+\frac{4+\lambda^2}{4}\left[sF_\lambda(u)\right]^2(dv)^2$
"Golden" form	$\lambda=1$	$\Phi_1=\frac{1+\sqrt{5}}{2}\approx 1.61803$	$(ds)^2=\ln^2(\Phi_1)(du)^2+\frac{5}{4}\left[sFs(u)\right]^2(dv)^2$
"Silver" form	$\lambda=2$	$\Phi_2=1+\sqrt{2}\approx 2.1421$	$(ds)^2=\ln^2(\Phi_2)(du)^2+2\left[sF_2(u)\right]^2(dv)^2$
"Bronze" form	$\lambda=3$	$\Phi_3=\frac{3+\sqrt{13}}{2}\approx 3.30278$	$(ds)^2=\ln^2(\Phi_3)(du)^2+\frac{13}{4}\left[sF_3(u)\right]^2(dv)^2$
"Cooper" form	$\lambda=4$	$\Phi_4=2+\sqrt{5}\approx 4.23607$	$(ds)^2=\ln^2(\Phi_4)(du)^2+5\left[sF_4(u)\right]^2(dv)^2$
Classical form	$\lambda_e\approx 2.350402$	$\Phi_{\lambda_e}=e\approx 2.7182$	$(ds)^2=(du)^2+sh^2(u)(dv)^2$

Thus, these considerations result in the conclusion that the *λ-models of Lobachevski's plane* (62), based on the *recursive Fibonacci hyperbolic functions* (53), (54), result in an infinite number of new hyperbolic geometries, having general title *"Golden" Hyperbolic Geometry,* which together with the classical *Lobachevski geometry*, *Riemannian geometry* and *Minkovski geometry "can be considered the nearest geometries to the traditional Euclidean geometry"* (**David Hilbert**).

A new solution to Hilbert's Fourth Problem is brilliant confirmation of effective application of the Mathematics of Harmony to the solution of complicated mathematical problems.

7 New scientific principles based on the Golden Section

7.1. Generalized principle of the golden section. There are some general principles of the division of the whole (the "Unit") into two parts. The most known from them are dichotomy principle, which is based on the trivial identity

$$1=2^0=2^{-1}+2^{-1}, \tag{63}$$

and golden section principle based on the identity:

$$1 = \Phi^0 = \Phi^{-1} + \Phi^{-2}, \tag{64}$$

where $\Phi = \left(1+\sqrt{5}\right)/2$ is the *golden mean*.

It follows from the identity (17) more general principle

$$1 = \Phi_p^0 = \Phi_p^{-1} + \Phi_p^{-p-1}, \tag{65}$$

which is called in [23] the *Generalized Principle of the Golden Section*.

Consider the examples of the use of the Generalized Principle of the Golden Section *(65) in some natural phenomena.*

7.2. ***Mathematical theory of biological populations.*** As is known, Fibonacci numbers are a result of the solution to *Fibonacci's problem of "rabbit" reproduction*. Let us recall that the *Law of "rabbit" reproduction* boils down to the following rule. Each mature rabbit's pair *A* gives birth to a newborn rabbit pair *B* during one month. The newborn rabbit's pair becomes mature during one month and then in the following month said pair starts to give birth to one rabbit pair each month. Thus, the maturing of the newborn rabbits, that is, their transformation into a mature pair is performed in 1 month. We can model the process of "rabbit reproduction" by using two transitions:

$$A \rightarrow AB \tag{66}$$

$$B \rightarrow A. \tag{67}$$

Note that the transition (66) simulates the process of the newborn rabbit pair *B* birth and the transition (66) simulates the process of the maturing of the newborn rabbit pair *B*. The transition (66) reflects an *asymmetry* of rabbit reproduction because the mature rabbit pair *A* is transformed into two non-identical pairs, the mature rabbit pair *A* and the newborn rabbit pair *B*.

Note that we should treat "rabbits" in *Fibonacci's problem of "rabbit" reproduction* as some biological objects. For example, as is shown in [11], family tree of honeybees is based strictly on Fibonacci numbers.

Note that *Fibonacci's problem of "rabbit" reproduction* is a primary problem of the *mathematical theory of biological populations* [56].

By using the model of "rabbit reproduction," which is described by the transitions (66) and (67), we can generalize the *problem of "rabbit" reproduction* in the following manner. Let us give a non-negative integer $p \geq 0$ and formulate the "*generalized Fibonacci's problem of "rabbit" reproduction"* for the condition when the transition of newborn rabbits into mature state is realized for *p* month, where $p = 0, 1, 2, 3, \ldots$.

It is clear that for the case $p=1$ the generalized variant of the "rabbit reproduction" problem coincides with the classical "rabbit reproduction" problem formulated by Fibonacci in 13th century.

Note that the case $p=0$ corresponds to the "idealized situation," when the rabbits become mature at once after birth. One may model this case by using the transition:

$$A \rightarrow AA. \tag{68}$$

It is clear that that the transition (68) reflects *symmetry* of "rabbit reproduction" when the mature rabbit pair *A* turns into two identical mature rabbit pairs *AA*. It is easy to show that for this case the rabbits are reproduced according to the above *dichotomy principle* (63), that is, the amount of rabbits doubles each month: 1, 2, 4, 8, 16, 32, … .

It is easy to prove that for the general case $p \geq 0$ a process of the "rabbit reproduction" is modelled by the recurrence relation (18) generating the *generalized Fibonacci p-numbers*. This means that the *generalized Fibonacci p-numbers* model some general principle of "rabbit reproduction" called the *generalized asymmetry principle of organic nature.*

7.3. ***Fibonacci's division of biological cells.*** At first appearance the above formulation of the *generalized problem of "rabbit reproduction"* appears to have no real physical sense. However, we should not hurry to such a conclusion! The article [57] is devoted to the application of the *generalized Fibonacci p-numbers* for the simulation of biological cell growth. The article affirms that *"in kinetic analysis of cell growth, the assumption is usually made that cell division yields two daughter*

cells symmetrically. The essence of the semi-conservative replication of chromosomal DNA implies complete identity between daughter cells. Nonetheless, in bacteria, insects, nematodes, and plants, cell division is regularly asymmetric, with spatial and functional differences between the two products of division…. Mechanism of asymmetric division includes cytoplasmic and membrane localization of specific proteins or of messenger RNA, differential methylation of the two strands of DNA in a chromosome, asymmetric segregation of centrioles and mitochondria, and bipolar differences in the spindle apparatus in mitosis." In the models of cell growth based on the Fibonacci 2- and 3-numbers are analyzed [57].

The authors of [57] made the following important conclusion: *"Binary cell division is regularly asymmetric in most species. Growth by asymmetric binary division may be represented by the generalized Fibonacci equation …. Our models, for the first time at the single cell level, provide rational bases for the occurrence of Fibonacci and other recursive phyllotaxis and patterning in biology, founded on the occurrence of regular asymmetry of binary division."*

8 The Mathematics of Harmony: a renaissance of the oldest mathematical theories

8.1. ***Algorithmic measurement theory.*** The first crisis in the foundations of mathematics was connected with a discovery of *incommensurable line segments.* This discovery turned back mathematics and caused the appearance of *irrational numbers.*

In 19-th century, **Dedekind** and then **Cantor** made an attempt to create a general measurement theory. For this purpose, they introduced the additional axioms into the group of the *continuity axioms*. For instance, let us consider *Cantor's axiom*.

Cantor's continuity axiom (Cantor's principle of nested segments). *If an infinite sequence of segments is given on a straight line A_0B_0, A_1B_1, A_2B_2, …, A_nB_n, …, such that each next segment is nested within the preceding one, and the length of the segments tends to zero, then there exists a unique point, which belongs to all the segments.*

The main result of the mathematical measurement theory that is based on the *continuity axioms* is a proof of the existence and uniqueness of the solution q of the *basic measurement equality*:

$$Q=qV, \tag{69}$$

where V is a measurement unit, Q is a measurable segment, and q is any real number named a *result of measurement*.

However, the *Cantor's axiom* raises the most doubts. According to this axiom, a measurement is a process, which is completed during infinite time. Such idea is a brilliant example of the Cantorian style of mathematical thinking based on the concept of *actual infinity*. However, this concept was subjected to sharp criticism from the side of the representatives of constructive mathematics. The famous Russian mathematician **A.A. Markov** (*1903-1979*) wrote [58]: *"We cannot imagine an endless, that is, never finished process as complete process without rough violence over intellect, which rejects such contradictory fantasies."*

As the concept of *actual infinity* is an internally contradictory notion ("the completed infinity"), this concept cannot be a reasonable basis for the creation of *constructive mathematical measurement theory*. If we reject Cantor's axiom, we can try to construct mathematical measurement theory on the basis of the idea of *potential infinity*, which underlies the *Eudoxus-Archimedes' axiom*. The *constructive approach* to measurement theory led to the creation of the so-called *algorithmic measurement theory* [1].

Algorithmic measurement theory led to new, "optimal" measurement algorithms based of the *generalized Fibonacci p-numbers*. The main outcome of the *algorithmic measurement theory* [1] is that every "optimal" measurement algorithm generates a new positional numeral system. It is proved in [1] that all the known positional numeral systems (binary, decimal, ternary, duodecimal and so on) are generated by the corresponding "optimal" measurement algorithms, which are partial cases of some very general class of the "optimal" measurement algorithms, which generate very unusual positional numeral systems. From these general reasoning's, we can conclude that the

algorithmic measurement theory [1] resulted in *general theory of positional numeral systems*, that is, in new mathematical theory, which is not existed before in mathematics.

The so-called *Fibonacci's measurement algorithm* generates the so-called *Fibonacci p-code*:

$$N = a_nF_p(n) + a_{n-1}F_p(n\text{-}1) + ... + a_iF_p(i) + ... + a_1F_p(1), \quad (70)$$

where N is natural number, $a_i \in \{0, 1\}$ is a binary numeral of the i-th digit of the code (70); n is the digit number of the code (70); $F_p(i)$ is the i-th digit weight calculated in accordance with the recurrence relation (18). The abridged notation of the sum (70) has the following form:

$$N = a_n\, a_{n-1} \,...\, a_i \,...\, a_1. \quad (71)$$

Note that the notion of the *Fibonacci p-code* (70) includes an infinite number of different positional "binary" representations of natural numbers because every p produces its own *Fibonacci p-code* (p=0,1,2,3,…). In particular, for the case p=0 the Fibonacci p-code (70) is reduced to the classical binary code:

$$N=a_n2^{n-1}+a_{n-1}2^{n-2}+...+a_i2^{i-1}+...+a_12^0 \quad (72)$$

For the case p=1 the Fibonacci p-code (70) is reduced to the following sum:

$$N = a_nF_n + a_{n-1}F_{n-1} + ... + a_iF_i + ... + a_1F_1. \quad (73)$$

Note that Fibonacci's representation (73) in the "Fibonacci numbers theory" [53] is called *Zekendorf's sum* after Belgian researcher **Eduardo Zekendorf** (1901-1983). For the case $p=\infty$ all Fibonacci p-numbers in (70) are equal to 1 identically and then the *Fibonacci p-code* (70) is reduced to the sum

$$N = \underbrace{1+1+...+1}_{N} \quad (74)$$

which is known in number theory as *Euclidean definition of natural number.*

Thus, the *Fibonacci p-code* (70) is a wide generalization of the classical *binary code* (72), *Zekendorf's sum* (73) and *Euclidean definition of natural numbers* (74).

8.2. ***The "golden" number theory.*** As is known, the first definition of a number was made in the Greek mathematics. We are talking about the *Euclidean definition of natural numbers* (74). In spite of utmost simplicity of the *Euclidean definition* (74), we should note that all number theory begins from the definition (74). This definition underlies many important mathematical concepts, for example, the concept of the *prime* and *composed* numbers, and also the concept of *divisibility* that is one of the major concepts of number theory. Here we would like to note that in mathematics only *natural numbers* have a strong definition (74); all other real numbers do not have such a strong definition.

Within many centuries, mathematicians developed and defined more exactly a concept of *number*. In 17-th century, that is, in period of the creation of new science, in particular, new mathematics, different methods of the "continuous" processes study was developed and the concept of a real number again goes out on the foreground. Most clearly, a new definition of this concept is given by **Isaac Newton** (*1643 – 1727*), one of the founders of mathematical analysis, in his *Arithmetica Universalis* (1707):

"We understand a number not as the set of units, however, as the abstract ratio of one magnitude to another magnitude of the same kind taken for the unit."

This formulation gives us a general definition of numbers, rational and irrational. For example, the binary system

$$A=\sum_i a_i 2^i \quad (75)$$

is the example of *Newton's definition,* when we chose the number 2 for the unit and represent a number as the sum of the number 2 powers.

Bergman's numeral system

In 1957 the American mathematician **George Bergman** published the article *A number system with an irrational base* [59]. In this article Bergman developed very unusual extension of the notion of the binary positional numeral system. He suggested using the "golden mean" $\Phi = \left(1+\sqrt{5}\right)/2$ as a base of a special positional numeral system. If we use the sequences Φ^i {i=0, ±1, ±2, ±3, …} as "digit weights" of the "binary" numeral system, we get the "binary" numeral system with irrational base Φ:

$$A = \sum_i a_i \Phi^i \tag{76}$$

where A is real number, a_i are binary numerals 0 or 1, i = 0, ± 1, ± 2, ± 3 …, Φ^i is the weight of the *i-th* digit, Φ is the base or radix of the number system (76).

Unfortunately, Bergman's article [59] did not be noticed in that period by mathematicians. Only journalists were surprised by the fact that **George Bergman** made his mathematical discovery in the age of 12 years! In this connection, the Magazine *TIMES* had published the article about mathematical wunderkind of America.

Codes of the Golden p-proportions

Bergman's system (76) allows the following generalization [3]. Consider the set of the following standard line segments:

$$S_p = \left\{\Phi_p^i\right\},\ i = 0, \pm 1, \pm 2, \pm 3, \ldots \tag{77}$$

where $p \geq 0$ is a given integer, Φ_p is the golden *p*-proportion, a real root of the characteristic equation (20). Remind that the powers of the golden *p*-proportions Φ_p^i are connected between themselves with the mathematical identity (17).

By using the set (77), we can "construct" the following positional representation of real numbers:

$$A = \sum_i a_i \Phi_p^i\ , \tag{78}$$

Where $a_i \in \{0, 1\}$ is a binary numeral of the *i*-th digit of the positional representation (78), i = 0, ±1, ±2, ±3, … , Φ_p is a radix of the numeral system (78). We shall name the sums (78) *codes of the golden p-proportion.* Note, that a theory of these codes is described in Stakhov's 1984 book [3].

The formula (78) "generates" an infinite number of different positional numeral systems because every p (p=0, 1, 2, 3, …) leads to its own numeral system of the kind (78). Note, that for p=0 the radix $\Phi_p = \Phi_0 = 2$ and the numeral system (78) is reduced to the classical binary system, the base of modern computers. For the case p=1 the golden mean $\Phi = \left(1+\sqrt{5}\right)/2$ is the radix of numeral system (78) and, therefore, the numeral system (78) is reduced to *Bergman's system* (76).

Note that for the case $p > 0$ all the radices Φ_p of numeral system (78) are irrationals. This means that the numeral system (78) set a general class of numeral systems with irrational radices. However, for the case $p = 0$ we have the only exception, because for this case the numeral system (78) is reduced to the classical binary system.

The main conclusion from this study is the following. The researchers by **George Bergman** [59] and **Alexey Stakhov** [3] resulted in the discovery of new class of positional numeral systems – *numeral systems with irrational radices,* which can become a basis for new information technology – *"Golden" Information Technology.*

New properties of natural numbers

Let us study the formulas (76) and (78) from number-theoretical point of view. First of all, let us say that the expressions (76) and (78) can be seen as a new (constructive) definition of real num-

bers. It is clear that the sum of (78) specifies an infinite number of such representations because every integer $p \geq 0$ gives its own positional representation in the form (78). Every positional presentation (78) divides all real numbers into two groups, *constructive numbers*, which may be represented as the finite sum of the golden *p*-proportions in the form of (78), and *non-constructive numbers*, which can not be represented in the form of the finite sum (78).

Thus, the definitions (76) and (78) are sources for the new number theory – the *"golden" number theory*. This theory is described for the first time in Stakhov's article [17] (the article [17] was published by recommendation of academician Yuri Mitropolski) and then in the article [79]. Based on this approach, **Alexey Stakhov** has discovered in [17, 79] new properties of natural numbers. Let us consider them for the case of *Bergman's system* (76), which is partial cases of the codes of the golden *p*-proportions (78) for the case *p*=1. Let us represent some natural number *N* in *Bergman's* system:

$$N = \sum_i a_i \Phi^i . \tag{79}$$

It is proved in [17,79] that for arbitrary natural number *N* the sum (79) consists of the finite number of terms, that is, arbitrary natural number *N* is *constructive number* in the system (79). In further we will name the sum (79) Φ*-code of natural number N*. It is proved in [17,79] that this property is valid for all *codes of the golden p-proportions* (78).

The Z-property of natural numbers is based on the following simple reasoning. Let us consider the Φ*-code* of natural number *N* given by the sum (79). It is known [11] the following formula, which connects the golden mean powers $\Phi^i \left(i = 0, \pm 1, \pm 2, \pm 3, ...\right)$ with the Fibonacci and Lucas numbers:

$$\Phi^i = \frac{L_i + F_i \sqrt{5}}{2} . \tag{80}$$

If we substitute Φ^i, given by (80), in the formula (79), then after simple transformation we can write the expression (79) as follows:

$$2N = A + B\sqrt{5}, \tag{81}$$

where

$$A = \sum_i a_i L_i \tag{82}$$

$$B = \sum_i a_i F_i . \tag{83}$$

By studying the "strange" expression (81), we can conclude that the identity (81) can be valid for the arbitrary natural number *N* only if the sum (83) is equal to 0 ("zero"), and the sum (82) is double of *N*, that is,

$$B = \sum_i a_i F_i = 0 \tag{84}$$

$$A = \sum_i a_i L_i = 2N. \tag{85}$$

Let us compare now the sums (84) and (79). Since the binary numerals a_i in these sums coincide, it follows that the expression (84) can be obtained from the expression (79) by simple substitution of every power of the golden mean Φ^i instead the Fibonacci number F_i, where the discrete variable i takes its values from the set $\{0, \pm 1, \pm 2, \pm 3, \ldots\}$. However, according to (84) the sum (83) is equal to 0 independently of the initial natural number *N* in the expression (79). Thus, we have discovered a new fundamental property of natural numbers, which can be formulated through the following theorem.

Theorem 3 (*Z*-property of natural numbers). *If we represent an arbitrary natural number N in Bergman's system (79) and then substitute the Fibonacci number* F_i *instead the power of the golden mean* Φ^i *in the expression (79), where the discrete variable i takes its values from the set*

{0,±1,±2,±3,…}, then the sum that appear as a result of such a substitution is equal to 0 independently on the initial natural number N, that is, we get the identity (84).

The expression (85) can be formulated as the following theorem.

Theorem 4 (*D*-property). *If we represent an arbitrary natural number N in Bergman's system (79) and then substitute the Lucas number* L_i *instead the power of the golden mean* Φ^i *in the expression (79), where the discrete variable i takes its values from the set {0,±1,±2,±3,…}, then the sum that appears as a result of such a substitution is equal to 2N independently of the initial natural number N, that is, we get the identity (85).*

Thus, Theorems 3 and 4 provide new fundamental properties of natural numbers [17,79]. It is surprising for many mathematicians to find that the new mathematical properties of natural numbers were only discovered at the end of the 20th century, that is, 2½ millennia after the beginning of their theoretical study. The *golden mean* and the *Fibonacci and Lucas numbers* play a fundamental role in this discovery. This discovery connects together two outstanding mathematical concepts of Greek mathematics - *natural numbers* and the *golden section.* This discovery is the next confirmation of the fruitfulness of the constructive approach to the number theory based upon *Bergman's system* (79) and *codes of the golden p-proportions* (78).

9. The "Golden" information technology: a revolution in computer science

9.1. ***Fibonacci computers.*** The introduced above new positional representations – *Fibonacci p-codes* (70), *Bergman system* (76) and *codes of the golden p-proportions* (78) can be the sources of new computer projects – *Fibonacci computers.* This concept, first described in Stakhov's book [1], is one of the important ideas of modern computer science. The essence of the concept consists of the following. Modern computers are based on the binary system (75), which represents all numbers as the sums of the binary numbers with binary coefficients, 0 and 1. However, the binary system (75) is non-redundant numeral system what does not allow detecting errors, which could appear in computer in the process of its exploitation. In order to eliminate this shortcoming, **Alexey Stakhov** suggested in [1,3] to use the *Fibonacci p-codes* and *codes of the golden p-proportions.*

International recognition of the *Fibonacci Computer concept* began after Stakhov's lecture in Vienna on the joint meeting of the Austrian Computer and Cybernetic Societies in 1976. The very positive reaction to Stakhov's lecture by the Austrian scientists, including Professor **Aigner,** Director of the Mathematics Institute of the Graz Technical University, Professor **Trappel**, President of the Austrian Cybernetic society, Professor **Eier,** Director of the Institute of Data Processing of the Vienna Technical University, and also Professor **Adam** the representative of the Faculty of Statistics and Computer Science of Johannes Kepler Linz University, caused the decision of the Soviet Government to patent Stakhov's inventions in the Fibonacci computer field abroad. The general outcome of the Fibonacci invention patenting surpassed all expectations. 65 foreign patents on various devices for the Fibonacci computer were given by the State Patent Offices of the U.S., Japan, England, France, Germany, Canada, Poland and GDR. These patents testify to the fact that the Fibonacci computer was a world class innovation, because the Western experts could not challenge the Soviet Fibonacci computer inventions. This means, as a result, the Fibonacci patents are the official legal documents, which confirm Soviet priority in this computer direction.

Any expert, who is interested in the Fibonacci computer project, will ask the question: what Fibonacci computer research is done in other countries? Some publications of American scientists on the Fibonacci arithmetic and applications in the Fibonacci computer field are presented in [60-63].

It is important to note the recent applications of the Fibonacci *p*-codes (70) to *digital signal processing* [64,65]. In the Russian science the idea of the use of Fibonacci *p*-numbers for the design of super-fast algorithms for digital signal processing were actively developed by the Professor **Vladimir Chernov**, Doctor in Physics and Mathematics at Samara the Images Processing Institute of the Russian Academy of Science [64]. Also Fibonacci *p*-numbers for the development of super-fast algorithms for digital signal processing are widely used by the research group from the Tampere

International Center for Signal Processing (Finland). As is shown in the book [65], the super fast algorithms for digital signal processing requires a processing of numerical data represented in the Fibonacci *p*-codes (70). This means that for the realization of such super-fast transformations requires for the specialized *Fibonacci signal processors*! This is why the problem of *Fibonacci* processor development is of vital concern today!

9.2. ***The "golden" ternary mirror-symmetrical arithmetic.*** In 1958 the ternary *Setun* computer was designed in Moscow University under supervision of **Nikolay Brousentsov.** Its peculiarity was the use of ternary numeral system:

$$A = \sum_i c_i 3^i , \tag{86}$$

where $c_i \in \{1, 0, \bar{1}\}$ is a ternary numeral of the *i*-th digit, 3^i is the weight of the *i-th* digit.

Many modern computer experts have come to the conclusion that the ternary computer design principle may bec ome an alternative in the future of computer progress. In this connection, it is important to recall the opinion of well-known Russian scientist, Prof. **Dmitry Pospelov**, on the ternary-symmetrical numeral system (86). In his book [66] he wrote: *"The barriers, which stand in the way of application of ternary-symmetric number systems in computers, are of a technical character. Until now, economical and effective elements with three stable states have not been developed. As soon as such elements will be designed, a majority of computers of the universal kind and many special computers will most likely be re-designed so that they will operate on the ternary-symmetric number system."* Also, American scientist Donald Knuth expressed the opinion [67] that one day the replacement of "flip-flop" by "flip-flap-flop" will occur.

Alexey Stakhov in [16] has developed a new ternary arithmetic, which is original synthesis of the ternary number system (86), used by **Nikolay Brousentsov** (Fig. 3) in the Setun computer, and *Bergman's system* (76). With purpose to explain new ternary representation of numbers, based on the *golden mean*, let us consider infinite sequence of the even powers of the *golden mean*:

$$\{\Phi^{2i}\}, i = 0, \pm 1, \pm 2, \pm 3, \ldots , \tag{87}$$

where $\Phi = (1+\sqrt{5})/2$ is the *golden mean*.

It is proved in [16] that we can represent all integers (positive and negative) as the following sum called *ternary Φ-code of integer N*:

$$N = \sum_{i=-\infty}^{+\infty} c_i \left(\Phi^2\right)^i , \tag{88}$$

where $c_i \in \{1, 0, \bar{1}\}$ is a ternary numeral of the *i-th* digit, $(\Phi^2)^i$ is the weight of the *i*-th digit of the positional representation (88), and $\Phi^2 = (3+\sqrt{5})/2 \approx 2.618$ is a radix of numeral system (88).

Fig. 3 - Donald Knuth (*born 1938*) and Nikolay Brousentsov (*1925-2014*)

The article *Brousentsov's Ternary Principle, Bergman's Number System and Ternary Mirror-Symmetrical Arithmetic* [16] published in *The Computer Journal* (England) got a high approval of the two outstanding computer specialists - **Donald Knuth** (Fig. 3)**,** Professor-Emeritus of Stanford University and the author of the famous book *The Art of Computer Programming* [67], and **Nikolay Brousentsov,** Professor of Moscow University, a principal designer of the fist ternary Setun computer. And this fact gives a hope that the ternary mirror-symmetrical arithmetic [16] can become a source of new computer projects in the nearest time.

10 The important "golden" discoveries in botany, biology and genetics

10.1. ***Bodnar's geometry.*** The phyllotaxis phenomenon shows itself in inflorescences and densely packed botanical structures, such as, *pinecones, pineapples, cacti, sunflowers, cauliflowers* and many other structures. As is well known, according to phyllotaxis law the numbers of the left-hand and right-hand spirals on the surface of phyllotaxis objects (Fig. 4) are always the adjacent Fibonacci numbers: 1, 1, 2, 3, 5, 8, 13, 21, 34, ... Their ratios

$$\frac{1}{1},\frac{2}{1},\frac{3}{2},\frac{5}{3},\frac{8}{5},\frac{13}{8},\frac{21}{13},\dots, \tag{89}$$

are called a *symmetry order* of phyllotaxis objects. The phyllotaxis phenomenon is exciting the best minds of humanity during many centuries (**Johannes Kepler, André Weil, Allan Turing** and others).

a) *b)* *c)*

Fig. 4 - Pyllotaxis structures: - pine cone (*a*); - pineapple (*b*); - Romanesque cauliflower (*c*)

The *puzzle of phyllotaxis* consists of the fact that a majority of bio-forms changes their phyllotaxis orders (95) during their growth. It is known, for example, that sunflower disks that are located on the different levels of the same stalk have different phyllotaxis orders; moreover, the more the age of the disk, the more its phyllotaxis order. This means that during the growth of the phyllotaxis object, a natural modification (an increase) of symmetry happens and this modification of symmetry obeys the law:

$$\frac{2}{1}\to\frac{3}{2}\to\frac{5}{3}\to\frac{8}{5}\to\frac{13}{8}\to\frac{21}{13}\to\dots . \tag{90}$$

The law (90) is called *dynamic symmetry.*

Note that the change of orders of phyllotaxis (90) carried out in strict accordance with the *Principle of self-similarity,* that is, all phyllotaxis structures are *self-similar* structures.

Recently the Ukrainian researcher **Oleg Bodnar** had developed very interesting geometric theory of phyllotaxis [45]. He proved that phyllotaxis geometry is a special kind of hyperbolic geometry based on the *"golden" hyperbolic functions* similar to the recursive hyperbolic Fibonacci and Lucas functions (29). Such approach allows explaining geometrically how the "Fibonacci spirals" appear

on the surface of phyllotaxis objects in process of their growth. ***Bodnar's geometry*** [45] **is of fundamental importance because it touches on fundamentals of theoretical natural sciences, in particular, this discovery gives a strict geometrical explanation of the *phyllotaxis law* and *dynamic symmetry* based on *Fibonacci numbers*.**

10.2. ***The Golden Section and a heart.*** During many years the Russian biologist **Vladimir Tsvetkov** had fulfilled fundamental scientific researches on the theme *The Golden Section and a Heart* [68,69]. This led to the following conclusions. The *golden mean* is displayed very widely in the work of the heart and all its systems. The main purpose of this work is a creation of stable and energy-optimal system. The mode of the *golden section* brings to maximum economy of energy and building material. The *golden harmony* of the heart activity corresponds to physiological calm of human body. In this state the heart works in economic, "golden" mode. After stopping any physical load, a blood circulation of the body and heart after some time returns back to the "golden" mode as the most economical one. The state of calm is prevailing over the life for even a very active animal. Therefore we can say that the heart and body aim for the *golden harmony* of "opposites"! The availability of the *golden mean* in a wide variety of different heart systems confirms the universality of the *golden mean* for the heart work. **The *golden harmony* is a "sign of quality" of a cardiac system and the heart in the whole.**

10.3. Fibonacci's resonances of genetic code. ***Among the biological concepts* [70] *that are well formalized and have a level of general scientific significance, the genetic code takes special precedence. Discovery of the striking simplicity of the basic principles of the genetic code places it amongst the major modern discoveries of mankind. This simplicity consists of the fact that inheritable information is encoded in the texts from three-lettered words* - triplets *or* codonums *compounded on the basis of the alphabet that consists of the four characters or nitrogen bases:* A *(*adenine*),* C *(*cytosine*),* G *(*guanine*),* T *(*thiamine*). The given system of the genetic information represents a unique and boundless set of diverse living organisms and is called* genetic code*.***

In 1990 **Jean-Claude Perez**, an employee of IBM, made a rather unexpected discovery in the field of the *genetic code*. He discovered the mathematical law that controls the self-organization of bases *A, C, G* and *T* inside of the DNA. He found that the consecutive sets of the DNA nucleotides are organized in frames of remote order called *RESONANCES*. Here, the resonance means a special proportion that divides the DNA sequence according to Fibonacci numbers (1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144 …).

The key idea of Perez's discovery, called the *DNA SUPRA-code*, consists of the following. Let us consider some fragment of the genetic code that consists of the *A, C, G* and *T* bases. Suppose that the length of this fragment is equal to some Fibonacci number, for example, 144. If a number of the *T*-bases in the DNA fragment is equal to 55 (Fibonacci number), and a total number of the *C, A* and *G* bases is equal to 89 (Fibonacci number), then this fragment of the genetic code forms is a *RESONANCE*, that is, a proportion between three adjacent Fibonacci numbers (55:89:144). Here it is permissible to consider any combinations of the bases, that is, *C* against *AGT*, *A* against *TCG*, or *G* against *TCA*. The discovery consists of the fact that the arbitrary DNA-chain forms some set of the *RESONANCES*. As a rule, the fragments of the genetic code of the length equal to the Fibonacci number F_n are divided into the subset of the *T*-bases, and the subset of the remaining *A, C, G* bases; here the number of *T*-bases is equal to the Fibonacci number F_{n-2} and the total number of the remaining *A,C, G* bases is equal to the Fibonacci number F_{n-1}, where $F_n=F_{n-1}+F_{n-2}$. If we make a systematic study of all the Fibonacci fragments of the genetic code, we can obtain a set of the resonances that is called the *SUPRA-code of DNA*.

10.4. ***"Golden" genomatrices.*** Recently the Russian researcher **Sergey Petoukhov** made an original discovery in genetics [70]. Petoukhov's discovery [70] shows a fundamental role of the *golden mean* in genetic code. This discovery gives further evidence that the *golden mean* underlies all *Organic Nature*! It is difficult to estimate the full impact of Petoukhov's discovery for the development of modern science. It is clear that this scientific discovery is of revolutionary discovery in this field.

11 The revolutionary "golden" discoveries in crystallography, chemistry, theoretical physics and cosmology

11.1. ***Quasi-crystals: revolutionary discovery in crystallography*****.** According to the *main law of crystallography*, there are strict restrictions imposed on the structure of a crystal. According to classical ideas, the crystal is constructed from one single cell. The identical cells should cover a plane densely without any gaps. As we know, the dense filling of a plane can be carried out by means of *equilateral triangles, squares* and *hexagons*. A dense filling of the plane by means of *pentagons* is impossible, that is, according to the main law of crystallography *pentagonal symmetry* is prohibited for mineral world.

On November 12, 1984 in a small article, published in the authoritative journal *Physical Review Letters*, the experimental proof of the existence of a metal alloy with exclusive physical properties was presented. The Israeli physicist **Dan Shechtman** was one of the authors of this article. A special alloy, discovered by Professor Shechtman in 1982 and called *quasi-crystal*, is the focus of his research. By using methods of electronic diffraction, Shechtman found new metallic alloys having all the symptoms of crystals. Their diffraction pictures were composed from the bright and regularly located points similar to crystals. However, this picture is characterized by the so-called *icosahedral* or *pentagonal* symmetry, strictly prohibited according to geometric reasons. Such unusual alloys are called *quasi-crystals.*

Quasi-crystals are revolutionary discovery in crystallography. The concept of quasi-crystals generalizes and completes the definition of a crystal. **Gratia** wrote in the article [71]: *"A concept of the quasi-crystals is of fundamental interest, because it extends and completes the definition of the crystal. A theory, based on this concept, replaces the traditional idea about the 'structural unit,' repeated periodically, with the key concept of the distant order. This concept resulted in a widening of crystallography and we are only beginning to study the newly uncovered wealth. Its significance in the world of crystals can be put at the same level with the introduction of the irrational numbers to the rational numbers in mathematics."*

What is the practical significance of the discovery of quasi-crystals? Gratia writes in [71] that *"the mechanical strength of the quasi-crystals increased sharply; here the absence of periodicity resulted in slowing down the distribution of dislocations in comparison to the traditional metals. This property is of great practical significance: the use of the "icosahedral" phase allows for light and very stable alloys by means of the inclusion of small-sized fragments of quasi-crystals into the aluminum matrix."*

Note that **Dan Shechtman** published his first article on the quasi-crystals in 1984, that is, exactly 100 years after the publication of Felix Klein's *Lectures on the Icosahedron* in 1884 [72]. This means that this discovery is a worthy gift to the centennial anniversary of Klein's book, in which the famous German mathematician predicted an outstanding role for the icosahedron in future scientific development.

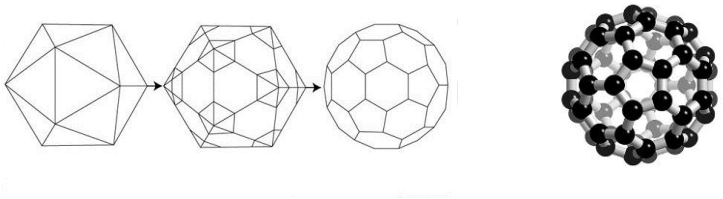
In 2011 **Dan Shechtman** won the Nobel Prize in chemistry for this discovery.

11.2. ***Fullerenes: revolutionary discovery in chemistry.*** *Fullerenes* are an important modern discovery in chemistry. This discovery was made in 1985, several years after the quasi-crystal discovery. The "fullerene" is named after **Buckminster Fuller** (*1895 -1983*), the American designer, architect, poet, and inventor. Fuller created a large number of inventions, primarily in the fields of design and architecture.

The title of *fullerenes* refers to the carbon molecules C_{60}, C_{70}, C_{76}, and C_{84}. We start from a brief description of the C_{60} molecule. This molecule plays a special role among the *fullerenes.* It is characterized by the greatest symmetry and as a consequence is highly stable. By its shape, the molecule C_{60} (Fig. 4, on the right) has the structure of *Archimedean truncated regular icosahedron* (Fig. 4, on the left).

The atoms of carbon in the molecule C_{60} are located on the spherical surface at the vertices of 20 regular hexagons and 12 regular pentagons; here each hexagon is surrounded by three hexagons and

three pentagons, and each pentagon is surrounded by five hexagons. The most striking property of the C_{60} molecule is its high degree of symmetry. There are 120 symmetry operations that convert the molecule into itself making it the most symmetric molecule.



a) b)

Fig.4 - Archimedean truncated icosahedron (*a*) and the molecule C_{60} (*b*)

It is not surprising that the shape of the C_{60} molecule has attracted the attention of many artists and mathematicians over the centuries. As mentioned earlier, the *truncated icosahedron* was already known to Archimedes. The oldest known image of the *truncated icosahedron* was found in the *Vatican library*. This picture was from a book by the painter and mathematician **Piero della Francesca**. We can find the truncated icosahedron in Luca Pacioli's *Divina Proportione* (1509). Also **Johannes Kepler** studied the Platonic and Archimedean Solids actually introducing the name *truncated icosahedron* for this shape.

The fullerenes, in essence, are "man-made" structures following from fundamental physical research. They were discovered in 1985 by **Robert F. Curl, Harold W. Kroto and Richard E. Smalley**. The researchers named the newly-discovered chemical structure of carbon C_{60} the *buckminsterfullerene* in honor of **Buckminster Fuller**. In 1996 they won the Nobel Prize in chemistry for this discovery.

Fullerenes possess unusual chemical and physical properties. At high pressure the carbon C_{60} becomes firm, like diamond. Its molecules form a crystal structure as though consisting of ideally smooth spheres, freely rotating in a cubic lattice. Owing to this property, C_{60} can be used as firm greasing (dry lubricant). The fullerenes also possess unique magnetic and superconducting properties.

11.3. ***Fibonacci's interpretation of Mendeleev's Periodical Table.*** Recently the Russian researchers **Shilo** and **Dinkov** have suggested in the work [73] very interesting interpretation of *Mendeleev's Periodical Law* of chemical elements. The essence of this suggestion consists of the following. The Great Russian scientist **Dmitry Mendeleev** suggested the *Periodical Law* 137 years ago. During this time, *Mendeleev's Periodical Law* played a huge role in the development of not only chemistry, but also of physics, biology, geochemistry, mineralogy, petrology, crystallography, and other sciences. In other words, it has stimulated scientific progress in all areas, where chemical elements are the basis of natural or artificial processes. But during this time scientists of different specialties in one or another form expressed dissatisfaction concerning Mendeleev's *Periodical Law*, despite the acclaim of its brilliant fundamental properties.

As it is emphasized in [73], Dmitry Mendeleev suggested a spiral form of the *Periodical System* yet in his first article on this topic. This was his brilliant prediction. Later in his total article *Periodical regularity of chemical elements* Mendeleev wrote: *«In fact, all the distribution of elements is uninterrupted and corresponds, in some degree, to spiral function».* It is asserted in [73] that, in the first days of the *Periodical Law* discovery, Mendeleev had used a dual form of the *Periodic Law*. Now it is clear that all Mendeleev's intuitive and prophetic ideas can be combined in the spatial helical form of the *Periodic Law*.

By studying *Mendleev's Peridical System* from this point of view, **Shilo** and **Dinkov** came in [73] to the important conclusion: *"Thus, the spatial curve (spiral), where chemical elements are placed, are located inside the cone or Lobachevski's pseudo-sphere. The chemical elements are presented of this spiral in discrete points (or «balls»). Projection of the elements on the horizontal plane, that is, on the cone base, presents Fibonacci's spiral, that is, such a spiral, where difference between atomic numbers of any two consecutive chemical elements is equal to Fibonacci numbers."*

Shilo and **Dinkov** pointed in [73] different relations, which determine a connection of the *Periodical System* with the *golden mean* and *Fibonacci numbers*:

1. A ratio of the number of the even mass nuclides of to the number of the even mass nuclides is equal to $2\times89 / 2\times55 \approx \Phi$, where Φ is the *golden mean.*

2. A ratio the number of the even charge nuclides to the number of the odd charge nuclides is equal to $220/68 \approx \Phi$, where Φ is the *golden mean.*

3. If we arrange in the increase order the 165 even-even nuclides, we get that the well-known "magic" neutron numbers 2, 8, 14, 20, 28, 50, 82, 126 correspond to the following nuclide numbers of our arrangement: 1, 3, 8. 13, 21, 55, 110=2×55, 165=3×55.

It seems that **Shilo** and **Dinkin's** distribution of the chemical elements, based on *Fibonacci numbers*, offers great opportunities to predict new properties of chemical elements what plays sometimes a decisive role in their use. And we can agree with the following **Shilo** and **Dinkin**'s assertion: *"If we move in this way, we inevitably will come to a completely new understanding of many processes and phenomena; perhaps, we even will change our ideas on the Universe."*

11.4. ***El Nashie's E-infinity theory.*** Prominent theoretical physicist and engineering scientist **Mohammed S. El Nashie** is a world leader in the field of the golden mean applications to theoretical physics, in particular, quantum physics [74–76]. El Nashie's discovery of the *golden mean* in the famous physical two-slit experiment-which underlies quantum physics–became a source for many important discoveries in this area, in particular, the *E-infinity theory*. It is also necessary to note the contribution of Slavic researchers to this important area. The book [77], written by the Byelorussian physicist **Vasyl Pertrunenko,** is devoted to the applications of the *golden mean* in quantum physics and astronomy.

11.5. ***Fibonacci-Lorentz transformations and the "golden" cosmological interpretation of the Universe evolution.*** As is known, *Lorentz's transformations* used in special relativity theory (SRT) are the transformations of the coordinates of the events (x, y, z, t) at the transition from one inertial coordinate system (ICS) K to another ICS K', which is moving relatively to ICS K with a constant velocity V.

The transformations were named in honor of Dutch physicist **Hendrik Antoon Lorentz** (*1853-1928*), who introduced them in order to eliminate the contradictions between *Maxwell's electrodynamics* and *Newton's mechanics*. *Lorentz's transformations* were first published in 1904, but at that time their form was not perfect. The French mathematician **Jules Henri Poincaré** (*1854-1912*) brought them to modern form.

In 1908, that is, three years after the promulgation of SRT, the German mathematician **Hermann Minkowski** (*1864-1909*) gave the original geometrical interpretation of *Lorentz's transformations*. In *Minkowski's space*, a geometrical link between two ICS K and K' are established with the help of *hyperbolic rotation*, a motion similar to a normal turn of the Cartesian system in *Euclidean space*. However, the coordinates of x' and t' in the ICS K' are connected with the coordinates of x and t of the ICS K by using classical hyperbolic functions. Thus, *Lorentz's transformations* in *Minkowski's geometry* are nothing as the relations of *hyperbolic trigonometry* expressed in physics terms. This means that *Minkowski's geometry* is hyperbolic interpretation of SRT and therefore it is a revolutionary breakthrough in geometric representations of physics, a way out on a qualitatively new level of relations between physics and geometry.

Alexey Stakhov and **Samuil Aranson** put forward in [37] the following hypotheses concerning the "golden" SRT:

1. The first hypothesis concerns the *light velocity in vacuum*. As is well known, the main dispute concerning the SRT, basically, is about the *principle of the constancy of the light velocity in vacuum*. In recent years a lot of scientists in the field of cosmology put forward a hypothesis, which puts doubt the permanence of the light velocity in vacuum - a fundamental physical constant, on which the basic laws of modern physics are based. Thus, **the first hypothesis is that the light velocity in vacuum was changed in process of the Universe evolution.**

2. Another fundamental idea involves with the factor of the *Universe self-organization* in the process of its evolution. According to modern view [82], a few stages of self-organization and degradation can be identified in process of the Universe development: *initial vacuum, the emergence of superstrings, the birth of particles, the separation of matter and radiation, the birth of the Sun, stars, and galaxies, the emergence of civilization, the death of Sun, the death of the Universe.* The main idea of the article [37] is to unite the fact of the *light velocity change* during the Universe evolution with the factor of its *self-organization*, that is, to introduce a dependence of the light velocity in vacuum from some *self-organization parameter ψ,* which does not have dimension and is changing within: $\left(-\infty<\psi<+\infty\right)$. The light velocity in vacuum *c* is depending on the "self-organization" parameter $\psi\ \left(-\infty<\psi<+\infty\right)$ and this dependence has the following form:

$$c=c(\psi)=\bar{c}(\psi)c_0\cdot \tag{91}$$

As follows from (91), the *light velocity in vacuum* is a product of the two parameters: c_0 and $\bar{c}(\psi)$. The parameter c_0 = *const*, having dimension [$m.sec^{-1}$], is called *normalizing factor.* It is assumed in [37] that the constant parameter c_0 is equal to *Einstein's light velocity in vacuum* (2.998×10^8 $msec^{-1}$) divided by the *golden mean* $\Phi=\left(1+\sqrt{5}\right)/2\approx1,61803$. The dimensionless parameter $\bar{c}(\psi)$ is called *non-singular normalized Fibonacci velocity of light in vacuum.*

3. The *"golden" Fibonacci goniometry* is used for the introduction of the *Fibonacci-Lorentz transformations,* which are a generalization of the classical *Lorentz transformations.* We are talking about the matrix

$$\Omega(\psi)=\begin{pmatrix} cFs(\psi-1) & sFs(\psi-2)\\ sFs(\psi) & cFs(\psi-1)\end{pmatrix}, \tag{92}$$

whose elements are *symmetric hyperbolic Fibonacci functions* (29). The matrix $\Omega(\psi)$ of the kind (92) is called *non-singular two-dimensional Fibonacci-Lorentz matrix* and the transformation

$$\begin{pmatrix}\xi\\ x_1\end{pmatrix}=\begin{pmatrix} cFs(\psi-1) & sFs(\psi-2)\\ sFs(\psi) & cFs(\psi-1)\end{pmatrix}\begin{pmatrix}\xi'\\ x_1'\end{pmatrix} \tag{93}$$

is called *non-singular two-dimensional Fibonacci-Lorentz transformations.* The above approach to the SRT led to the new ("golden") cosmological interpretation of the Universe evolution and to the change of the light velocity before, in the moment, and after the bifurcation, called *Big Bang.*

Based on this approach, **Alexey Stakhov** and **Samuil Aranson** have obtained in [37] new cosmological results in the Universe evolution, beginning with the «Big Bang». In particular, they put forward a hypothesis that there are two "bifurcation points" in the Universe evolution. The first one corresponds to the *"Big Bang",* and the second one corresponds to the transition of the Universe from the *Dark Ages* to the *Shining Period,* where light and first stars have arisen. The speed of light immediately after the second "Bifurcation point" is very high, but as far as the evolution of the Universe the speed of light starts to drop and reaches the limit value C≈300000 km/sec^{-1}.

12 The latest results and publications in the field of Mathematics of Harmony

The ancient Greeks raised the *golden section* at the level of "aesthetic canon" and "major ratio" of the Universe. For centuries or even millennia, starting from **Pythagoras, Plato, Euclid**, this geometric discovery has been the subject of admiration and worship of eminent minds of humanity - in the Renaissance, **Leonardo da Vinci, Luca Pacioli, Johannes Kepler**, in the 19 century -

Zeizing, Lucas, Binet. In 20-th century, the interest in this unique irrational number increased in mathematics, thanks to the works of Russian mathematician **Nikolay Vorobyov** and American mathematician **Verner Hoggatt**. The development of this direction led to the appearance of the *Mathematics of Harmony* [36] as a new interdisciplinary theory of modern science.

The Mathematics of Harmony is now the actively developing mathematical discipline, which expands the scope of its applications and already goes out to the level of mathematical and physical MILLENIUM PROBLEMS [80,81,83]. Let us consider new mathematical results, obtained in the works [49,79,80,81,83]:

1. The article [49] is very important article for the mathematics history. It turns over our ideas about Euclid's *Elements* and the history of mathematics, starting from Euclid. This article is especially important for mathematical education because it brings nearer mathematics to Nature and fine arts and makes mathematics more interesting discipline for learning. **Introduction of the course "Mathematics of Harmony" into the educational programs of schools, colleges and universities can be a revolutionary idea in modern education.**

2. The article [79] is developing the concept of the "golden" number theory, described above. **A discovery of new and unusual properties of natural numbers is a basic mathematical result of the article** [79].

3. The article [80] is devoted to original solution of the most complicated mathematical problem of 20th century, the *Hilbert Fourth Problem.* The *metallic means* by Vera Spinadel [50] and following from them *hyperbolic λ-Fibonacci and Lucas functions* underlie this solution. This solution puts forward a new challenge for theoretical natural sciences, *a search of new hyperbolic worlds of Nature similar to "Bodnar's geometry"* [45], based on the *golden ratio*. **The basic idea of the article [80] is the fact that Hilbert Fourth Problem is MILLENNIUM PROBLEM in Geometry that is still not be understood by modern mathematicians.**

4. The article [81] is very interesting article from the point of view of theoretical physics. The article gives original solution of one of the important physics MILLENNIUM PROBLEMS, the problem of FINE-STRUCTURE CONSTANT, formulated in 2000 by the prominent American physicist **David Gross**. The solution is based on the non-traditional version of the special theory of relativity, which follows from the Fibonacci-Lorentz transformations [37] arising from the theory of the "golden" matrices [26]. On the basis of this approach in the article [81] it is studied changing the FINE-STRUCTURE CONSTANT, depending on the age of the Universe since the Big Bang. **It is shown that the FINE-STRUCTURE CONSTANT in fact is not a physical constant, but is physical dimensionless quantity whose value is dependent on the age of the Universe.**

5. The article [82] is a development of the well-known Stakhov's work on Fibonacci *p*-codes and codes of the golden *p*-proportions [1-5] as new arithmetical and informational foundations of computer science and digital metrology for mission-critical applications. **Designing Fibonacci and "golden" computer and measurement systems for mission-critical applications can be revolutionary idea for future informational technology.**

6. The book "The "Golden" Non-Euclidean Geometry" [83] summarizes the results of the latest applications of the "Mathematics of Harmony", set out in the articles [49,79,80,81,83]. The book [83] is a further development of the book "The Mathematics of Harmony" [11]. The main goal of the book [83] is to show that the "Mathematics of Harmony" [11] is an actively developing direction of contemporary science and that the "Mathematics of Harmony" [11] is indeed a source for new and original scientific ideas and concepts.

Instead Conclusion: New Challenge for Theoretical Natural Sciences Based on the Mathematics of Harmony and "Golden" Hyperbolic Geometry

Although the "Mathematics of Harmony" contains in itself a large number of new scientific findings concerning mathematics (*Proclus hypothesis, "golden" number theory and new properties of*

natural numbers, Hilbert's Fourth Problem), computer science (*numeral systems with irrational radices, conception of Fibonacci computers and ternary mirror-symmetrical arithmetic*) and theoretical physics (*Fibonacci-Lorenz transformations and Fibonacci special theory of relativity*), however the main scientific result of the research, described in [80,83], is **a proof of the existence of an infinite number of new hyperbolic functions, *Fibonacci hyperbolic λ-functions*, based on the "metallic proportions".** For the given λ=1,2,3,.. each class of the Fibonacci hyperbolic λ-functions, "generates" new hyperbolic geometry, which leads to the appearance in the "physical world" specific hyperbolic geometries with mathematical properties, based on the "metallic proportions." **The main peculiarity of these new hyperbolic functions, based on "metallic proportions" and Gazale's formulas, is a recursive character of these hyperbolic functions.** This means that the "golden" hyperbolic geometries are also recursive, and they embody in themselves the **Principle of Self-similarity**, which is the basis of **self-organizing systems of Nature.** This is the main difference between the "golden" hyperbolic geometries and classical hyperbolic geometry created by Lobachevski.

The new geometric theory of phyllotaxis, created by Oleg Bodnar [45], is brilliant example of real existing of the "golden" geometry in Nature. Bodnar proved that "the world of phyllotaxis" is a specific "golden hyperbolic world," in which "hyperbolicity" manifests itself in the "Fibonacci spirals" on the surface of "phyllotaxis objects."

Recall that "Bodnar's geometry" [45] is based on the recursive Fibonacci hyperbolic functions:

$$\begin{cases} sFs(x) = \dfrac{\Phi^{x} - \Phi^{-x}}{\sqrt{5}} \\ cFs(x) = \dfrac{\Phi^{x} + \Phi^{-x}}{\sqrt{5}} \end{cases} \tag{94}$$

which are connected with the "extended" Fibonacci numbers, given by *Binet's formulas* (28), by the formulas (33):

$$F_n = \begin{cases} sF(n) \text{ for } n = 2k \\ cF(n) \text{ for } n = 2k+1 \end{cases}. \tag{95}$$

The property (95) defines a recursive character of the hyperbolic functions (94) and following from them "golden" hyperbolic geometry. Unfortunately, this fundamental property of the new hyperbolic functions, based on the *metallic proportions* Φ_λ, in comparison with the classical hyperbolic functions, based on Euler's number ***e*** still not understood by many modern mathematicians, excepting mathematicians-thinkers such as Academician **Yuri Mitropolsky**, head of the Ukrainian School of Mathematics, Russian Professor **Samuil Aranson**, one of the leading mathematicians of Russia in the field of topology and geometry, awarded in 2016 by the **GOLD MEDAL of Euro Chamber** for outstanding achievements in the field of science, and also Canadian Professor **M. W. Wong** *(York University),* Editor-in-Chief of the Series on Analysis, Applications and Computation (World Scientific), who recommended the book "The "Golden" Non-Euclidean Geometry" for publication in the World Scientific. Also some philosophers-thinkers such as American Prof. **Scott Olsen,** Russian Prof. **Sergey Abachiev**, and Belarusian philosopher **Eduard Soroko** praised the scientific direction of Alexey Stakhov. We present some excerpts from reviews of famous scientists.

Academician Yuri Mitropolsky [84]:

"One may wonder what place in the general theory of mathematics this work may have. It seems to me-that in the last few centuries-as Nikolay Lobachevsky said, "Mathematicians have turned all their attention to the advanced parts of analytics, and have neglected the origins of Mathematics and are not willing to dig the field that has already been harvested by them and left behind." As a result, this has created a gap between "Elementary Mathematics" - the basis of modern mathematical education - and "Advanced Mathematics." In my opinion, the Mathematics of Harmony developed by Professor Stakhov fills that gap. The Mathematics of Harmony is a huge theoretical contri-

bution to the development of "Elementary Mathematics," and as such should be considered of great importance for mathematical education".

Professor Scott Olsen [85]: *"Now for the past two years I have worked very closely with Prof. Stakhov, editing his book, The Mathematics of Harmony: from Euclid to Contemporary Mathematics and Computer Science, scheduled for publication by World Scientific later this summer in 2009. Some of us are convinced that* ***his insights in this work are so remarkable, that it may well change not only the way we view the history of mathematics, but the future development of mathematics in its applications to the natural sciences.*** *In particular, I have found that Professor Stakhov's knowledge of the Golden Section in both its intricacies and ramifications for the natural sciences is the actual state of the art in academia. I know this because I have researched the subject for over 35 years, and in 2006 published the award winning book, The Golden Section: Nature's Greatest Secret".*

A conception of the "Golden" Non-Euclidean Geometries greatly expands the number of possible hyperbolic functions with recursive properties. It is proved in [83] that a number of the recursive hyperbolic geometries is equal infinity, because every $\lambda=1,2,3,\ldots$ "generates" its own "golden" recursive hyperbolic geometry.

In the book [83], the notion of the *normalized distance* between classical Lobachevski's geometry with the base ***e*** (*Euler number*) and the "golden" hyperbolic geometries with the bases Φ_λ (*metallic proportions*) has been introduced.

The famous irrational number $\Phi=\frac{1+\sqrt{5}}{2}\approx 1.618$ (*the golden ratio*) is the base of the hyperbolic functions (94). The *normalized distance* between *Bodnar's geometry* and *Lobachevski's geometry* is equal $\rho_{12}\approx 0.7336$.

For the first time, the simplest example of the recursive hyperbolic functions has been described in **Stakhov & Rozin's** 2004 article [18] and later **Alexey Stakhov** generalized the result of the article [18] in Stakhov's 2006 article [30]. A detailed study of the *recursive Fibonacci hyperbolic λ-functions* was done in **Stakhov & Aranson's** 2016 article [80] and 2016 book [83]. Basing on the success of *Bodnar's geometry* [45], one can put forward in front to theoretical physics, chemistry, crystallography, botany, biology, and other branches of theoretical natural sciences **the challenge to search new ("harmonic") hyperbolic worlds of Nature, based on other classes of the Fibonacci hyperbolic *λ-functions*** (53), (54).

However, the *"golden" hyperbolic functions* (94), which underlie the *hyperbolic phyllotaxis world*, are a special case of the *hyperbolic Fibonacci λ-functions* ($\lambda=1$). In this regard, there is every reason to suppose that other types of hyperbolic functions, the *Fibonacci hyperbolic λ-functions*, can be the basis for modeling of new "hyperbolic worlds," which possibly can really exist in Nature. Modern science did not find these special "hyperbolic worlds" until now, because the recursive hyperbolic Fibonacci functions were unknown until early 21th century [18,30]. In this case, perhaps, the next candidate for the new "hyperbolic world" of Nature may be, for example, **"silver" hyperbolic functions**:

$$\begin{cases} sF_2(x)=\dfrac{\Phi_2^x-\Phi_2^{-x}}{\sqrt{8}}=\dfrac{1}{2\sqrt{2}}\left[\left(1+\sqrt{2}\right)^x-\left(1+\sqrt{2}\right)^{-x}\right], \\ cF_2(x)=\dfrac{\Phi_2^x+\Phi_2^{-x}}{\sqrt{8}}=\dfrac{1}{2\sqrt{2}}\left[\left(1+\sqrt{2}\right)^x+\left(1+\sqrt{2}\right)^{-x}\right] \end{cases} \quad (96)$$

which are connected with *Pell numbers* and are based on the "silver mean" $\Phi_2=1+\sqrt{2}\approx 2.41$, called also *Leonardo da Vinci's constant*.

In this regard, we should draw a special attention to the fact that the new hyperbolic geometry, based on the "silver" hyperbolic functions (96), is the closest to Lobachevski's geometry, based of the classical hyperbolic functions with the base $e\approx 2.71$. Its normalized distance to Lobachevski's geometry is equal $\rho_{12}\approx 0.1677$ what is the smallest among all the distances between "golden" hyperbolic *λ-forms* (62) and Lobachevski's metric form (61). It allows from here the assump-

tion that the "silver" hyperbolic functions (96) and the generated by them "silver" hyperbolic geometry can be soon be found in Nature after *Bodnar's geometry*, based on the "golden" hyperbolic functions (94).

Taking into consideration the above reasoning's, we can conclude that the recursive hyperbolic geometries, based on the *Principle of Self-similarity*, is the new direction in the development of Lobachevski's hyperbolic geometry and therefore searching new hyperbolic worlds of Nature, based on recursive hyperbolic geometries, may lead to new scientific discoveries.

References

[1] Stakhov A.P. Introduction into algorithmic measurement theory / A.P. Stakhov. – Moscow: Soviet Radio, 1977. – 288 p. (In Russian).

[2] Stakhov A.P. Algorithmic measurement theory / A.P. Stakhov. – Moscow: Znanie, 1979. – 64 p. – (Series "Mathematics and Cybernetics". – 1979. – Issue 6). (In Russian).

[3] Stakhov A.P. Codes of the golden proportion/ A.P. Stakhov. – Moscow: Radio and communications, 1984. – 151 p. (In Russian).

[4] Noise-tolerant codes: Fibonacci computers. Moscow: Znanie, 1989. - (Series "Radio Electronics and Communications". - 1989. – Issue 6). (In Russian).

[5] Stakhov A.P. Computer Arithmetic based on Fibonacci Numbers and Golden Section: New Information and Arithmetic Computer Foundations / A.P. Stakhov. – Toronto: SKILLSET-Training, 1997.

[6] Stakhov A.P. Introduction into Fibonacci Coding and Cryptography / A.P. Stakhov, V. Massingua, A.A. Sluchenkova. – Kharkov: Osnova, 1999. (In Russian).

[7] The Golden Section: Theory and Applications: [ed. by A.P. Stakhov] // Boletin de Informatica University Eduardo Mondlane, Mozambique. – 1999. – № 9/10.

[8] Stakhov A.P. Museum of Harmony and Golden Section: mathematical connections in Nature, Science and Art / A.P. Stakhov, A.A. Sluchenkova. – Vinnitsa: ITI, 2003.

[9] Stakhov A.P. Hyperbolic Fibonacci and Lucas Functions: a New Mathematics for Living Nature / A.P. Stakhov. – Vinnitsa: ITI, 2003.

[10] Stakhov A.P. Da Vinci code and Fibonacci series / A.P. Stakhov, A.A. Sluchenkova, I.G. Tscherbakov. – Sanct-Peterburgh: Piter, 2006. – 320 p.

[11] Stakhov A.P. The Mathematics of Harmony. From Euclid to Contemporary Mathematics and Computer Science/ A.P. Stakhov; [Assisted by Scott Olsen]. – New Jersey; London; Singapore; Hong Kong: World Scientific, 2009. – 748 p.

[12] Stakhov A.P. The Golden Section in the measurement theory/ A.P. Stakhov// Computers & Mathematics with Applications. – 1989. – Volume 17. – № 4 – 6.

[13] Stakhov A.P. Hyperbolic Fibonacci trigonometry/ A.P. Stakhov, I.S. Tkachenko// Reports of the Ukrainian Academy of Sciences. – 1993. – Volume 208. – № 7. (In Russian).

[14] Stakhov A.P. The Golden Section and Modern Harmony Mathematics/ A.P. Stakhov // Applications of Fibonacci Numbers. – 1998. – Volume 7. – P.323 – 399.

[15] Stakhov A.P. A generalization of the Fibonacci Q-matrix/ A.P. Stakhov // Reports of the Ukrainian Academy of Sciences. - 1999. – № 9.

[16] Stakhov A.P. Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic/ A.P. Stakhov // The Computer Journal. – 2002. – Vol. 45. – № 2. – P. 222 – 236.

[17] Stakhov A.P. The generalized golden sections and a new approach to geometric definition of a number/ A.P. Stakhov // Ukrainian Mathematical Journal. – 2004. – Vol. 56. (In Russian).

[18] Stakhov A. On a new class of hyperbolic function/ A. Stakhov, B. Rozin // Chaos, Solitons & Fractals. – 2004. – Vol. 23. – Issue 2. – P.379 – 389.

[19] Stakhov A. The Golden Shofar / A. Stakhov, B. Rozin // Chaos, Solitons & Fractals. – 2005. – Vol. 26. – Issue 3. – P.677 – 684.

[20] Stakhov A. The "golden" algebraic equations / A. Stakhov, B. Rozin // Chaos, Solitons & Fractals. – 2005. – Vol. 27. – Issue 5. – P.1415 – 1421.

[21] Stakhov A. Theory of Binet's formulas for Fibonacci and Lucas p-numbers / A. Stakhov, B. Rozin // Chaos, Solitons & Fractals. – 2005. – Vol. 27. – Issue 5. – P.1162 – 1177.

[22] Stakhov A. The continuous functions for the Fibonacci and Lucas p-numbers / A. Stakhov, B. Rozin // Chaos, Solitons & Fractals. – 2006. – Vol. 28. – Issue 4. – P. 1014 – 1025.

[23] Stakhov A. The Generalized Principle of the Golden Section and its applications in mathematics, science, and engineering / A. Stakhov // Chaos, Solitons & Fractals. – 2005. – Vol. 26. – Issue 2. – P. 263 – 289.

[24] Stakhov A. Fundamentals of a new kind of Mathematics based on the Golden Section / A. Stakhov // Chaos, Solitons & Fractals. – 2005. – Vol. 27. – Issue 5. – P.1124 – 1146.

[25] Stakhov A. Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory / A. Stakhov // Chaos, Solitons & Fractals. – 2006. – Vol.30. – Issue 1. – P. 56-66.

[26] Stakhov A. The "golden" matrices and a new kind of cryptography / A. Stakhov // Chaos, Solitons & Fractals. – 2007. – Vol.32. – Issue 3. – P. 1138 – 1146.

[27] Stakhov A. The Golden Section, Fibonacci series and new hyperbolic models of Nature / A. Stakhov, B. Rozin // Visual Math-

ematics. – 2006. – Vol. 8. – № 3. – (http://members.tripod.com/vismath/pap.htm).
[28] Stakhov A.P. The golden section, sacred geometry, and harmony mathematics / A.P. Stakhov // Metaphysics: Century XXI / [compiler and editor Y.S. Vladimirov]. – Moscow: BINOM, 2006 . – P. 174 – 215. (In Russian).
[29] Stakhov A. Three "key" problems of mathematics on the stage of its origin, the "Harmony Mathematics" and its applications in contemporary mathematics, theoretical physics and computer science / A. Stakhov // Visual Mathematics. – 2007. – Vol. 9. – № 3. – (http://members.tripod.com/vismath/pap.htm).
[30] Stakhov A.P. Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions and the improved method of the "golden" cryptography / A.P. Stakhov // Academy of Trinitarism, Moscow: № 77 – 6567, publication 14098, 21.12.2006. – (http://www.trinitas.ru/rus/doc/0232/004a/02321063.htm). (In Russian).
[31] Stakhov A.P. Hyperbolic Fibonacci and Lucas functions: a history and applications / A.P. Stakhov// Academy of Trinitarism, Moscow, № 77 – 6567, publication 14429, 31.05.2007. – (www.trinitas.ru/rus/doc/0232/009a/02321057.htm). (In Russian).
[32] Stakhov A.P. "Strategic mistakes" in the mathematics development/ A.P. Stakhov // Academy of Trinitarism, Moscow, № 77 – 6567, publication 14555, 27.08.2007. – (www.trinitas.ru/rus/doc/0232/004a/02321070.htm). (In Russian).
[33] Stakhov A.P. Three "Key" Problems of Mathematics on the Stage of its Origin and the "Harmony Mathematics" as Alternative Way of Mathematics Development / A.P. Stakhov // Mathematics & Design: Fifth International Mathematics & Design Conference – V M&D. – Blumenau: Nova Letra, 2008. – P.88 – 102.
[34] Stakhov A.P. Design of a New Coding Theory and Cryptography Based on the Fibonacci and "Golden" Matrices / A.P. Stakhov, A.A. Sluchenkova // Mathematics & Design: Fifth International Mathematics & Design Conference – V M&D. - Blumenau: Nova Letra, 2007. – P. 154 – 165.
[35] Stakhov A.P. The "Strategic Mistakes" in the Mathematics Development and the Role of the Harmony Mathematics for Their Overcoming /A.P. Stakhov // Visual Mathematics. – 2008. – Vol.10. – №3. – (http://www.mi.sanu.ac.yu/vismath/stakhov2008a/index.html).
[36] A.P. Stakhov. The Mathematics of Harmony: Clarifying the Origins and Development of Mathematics // Congressus Numerantium. – 2008. – № 193.
[37] Stakhov A.P. "Golden" Fibonacci Goniometry, Fibonacci-Lorentz Transformations, and Hilbert's Fourth Problem / A.P. Stakhov, S.Ch. Aranson // Congressus Numerantium. – 2008. – № 193. – P.119 – 156.
[38] Stakhov A. A generalization of the Cassini formula / Alexey Stakhov // Visual Mathematics. – 2012. – Vol. 14. – № 2. – (http://www.mi.sanu.ac.rs/ vismath/stakhovsept2012/cassini.pdf).
[39] Kline M. Mathematics: The Loss of Certainty / Morris Kline. – New York : Oxford University Press, 1980. – 366 p.
[40] Arnold V. A complexity of the finite sequences of zeros and units and geometry of the finite functional spaces: Lecture at the session of the Moscow Mathematical Society, May 13, 2007. – (http://elementy.ru/lib/430178/430281).
[41] Olsen Scott The Golden Section: Nature's Greatest Secret / Scott Olsen. – New York: Walker Publishing Company, 2006. – 58 p.
[42] Herz-Fischler R. A Mathematical History of the Golden Number / Roger Herz-Fischler. – New York: Dover Publications, Inc., 1998. – 195 p.
[43] Khinchin A.Ja. Continued Fractions / A.Ja. Khinchin. - Mineola, N.Y.: Dover Publications, 1997. – [first published in Moscow, 1935].
[44] Vorobyov N.N. Fibonacci numbers / N.N. Vorobyov. – Moscow: Nauka, 1978**.** (In Russian).
[45] Bodnar O. Y. The Golden Section and Non-Euclidean Geometry in Nature and Art / O. Y. Bodnar. – Lvov: Svit, 1994. (In Russian).
[46] Soroko E.M. Structural harmony of systems / E.M. Soroko. – Minsk: Nauka i technika, 1984. (In Russian).
[47] Metaphysics: Century XXI / [compiler and editor Y.S. Vladimirov]. – Moscow: BINOM, 2006. (In Russian).
[48] Kolmogorov A.N. Mathematics in its historical development / A.N. Kolmogorov. – Moscow: Nauka, 1961. (In Russian).
[49] Stakhov A.P. Proclus Hypothesis / A.P. Stakhov // British Journal of Mathematics & Computer Science. – 2016. – № 13 (06). – P.1 – 22.
[50] Spinadel de Vera W. From the Golden Mean to Chaos / Vera W. de Spinadel. – Nueva Libreria, 1998. – [second edition in Nobuko, 2004].
[51] Gazale Midhat J. Gnomon. From Pharaohs to Fractals / Midhat J. Gazale. – Princeton; New Jersey: Princeton University Press, 1999.
[52] Kappraff Jay Beyond Measure. A Guided Tour Through Nature, Myth, and Number / Jay Kappraff. – Singapore; New Jersey; London; Hong Kong: World Scientific, 2002.
[53] Hoggat Jr. V.E. Fibonacci and Lucas Numbers / V.E. Hoggat Jr. – Boston, MA: Houghton Mifflin, 1969.
[54] Hilbert D. Hilbert's Problems / D. Hilbert; general edition P.S. Alexandrov. – Moscow: Nauka, 1969. (In Russian).
[55] Hilbert's Fourth Problem. Wikipedia**.** The Free Encyclopedia. – http://en.wikipedia.org/wiki/Hilbert's_fourth_problem . – Title from the screen.
[56] Dynamical theory of biological populations. – Moscow: Nauka, 1974.
[57] Spears C.P. Asymmetric cell division: binomial identities for age analysis of mortal vs. immortal trees / C.P. Spears, M. Bicknell-Johnson // Applications of Fibonacci Numbers. – 1998. – Vol. 7.
[58] Markov A.A. On a logics of constructive mathematics / A.A. Markov. – Moscow: Znanie, 1972 . (In Russian).
[59] Bergman G. A number system with an irrational base / G. Bergman // Mathematics Magazine. – 1957. – № 31.
[60] Monteiro P. Minimal and maximal Fibonacci representations: Boolean generation / P. Monteiro, R. Newcomb // The Fibonacci Quarterly. – 1976. – Vol.14. – № 1.

[61] Ligomenides P. Equivalence of some binary, ternary, and quaternary Fibonacci Computers / P. Ligomenides, R. Newcomb // Proceeding of the Eleventh International Symposium on Multiple-Valued Logic, Norman, Oklahoma, May 1981.
[62] Ligomenides P. Complement representations in the Fibonacci computer / P. Ligomenides, R. Newcomb // Proceedings of the Fifth Symposium on Computer Arithmetic, Ann Arbor, Michigan, May 1981.
[63] Hoang V.D. A class of arithmetic burst-error-correcting codes for the Fibonacci Computer : PhD Dissertation / V.D. Hoang. – University Maryland, December 1979.
[64] Chernov V.M. Fivonacci-Mersenne and Fibonacci-Fermat discrete transforms / V.M. Chernov, M.V. Pershina. // Boletin de Informatica of the Eduardo Mondlane University. – 1999. – Special Issue :The Golden Section: Theory and Applications. – № 9/10.
[65] Stankovic R.S. Fibonacci Decision Diagram / R.S. Stankovic, M.R. Stankovic, J.T. Astola, K. Egizarian. – Tampere International Center for Signal Processing, 2000.
[66] Pospelov D.A. Arithmetical foundations of computers / D.A. Pospelov. – Moscow: Vyshaja shkola, 1970. (In Russian).
[67] Knuth D.E. The Art of Computer Programming. Vol.2. Semi-Numerical Algorithms / D.E. Knuth. – Addison-Wesley, 1969.
[68] Tsvetkov V.D. Heart, the Golden Section, and Symmetry / V.D. Tsvetkov. – Puschino: ONTI PNZ RAU, 1997. (In Russian).
[69] Tsvetkov V.D. The Golden Section and a Heart / V.D. Tsvetkov. Puschino: ONTI PNZ RAU, 2008. (In Russian).
[70] Petoukhov S.V. Metaphysical aspects of the matrix analysis of genetic code and the golden section / S.V. Petoukhov // Metaphysics: Century XXI. – Moscow: BINOM, 2006 . (In Russian).
[71] Gratia D. Quasi-crystals / D. Gratia // Uspechi physicheskich nauk. – 1988 . – Vol. 156. (In Russian).
[72] Klein F. Lectures on isosahedron and solutions to the 5th degree equation / Felix Klein. – Moscow: Nauka, 1989.
[73] Shilo N.A. Fenotypical system of atoms for the development of Mendeleev's ideas / N.A. Shilo, A.V. Dinkov // Moscow: Academy of Trinitarism, Electronic publication № 77 – 6567, 14630, 09.11.2007. – (http://www.trinitas.ru/rus/doc/0232/009a/02321073.htm).
[74] El Nashie M.S. Is Quantum Space a Random Cantor Set with a Golden Mean Dimension at the Core? / M.S. El Nashie // Chaos, Solitons & Fractals. – 1994. - Vol. 4. – Issue 2.
[75] El Nashie M.S. On a class of general theories for high energy particle physics / M.S. El Nashie // Chaos, Solitons & Fractals. – 2002. – Vol. 14.
[76] El Nashie M.S. Hilbert space, Poincaré dodecahedron and golden mean transfiniteness / M.S. El Nashie // Chaos, Solitons & Fractals. – 2007. – Vol. 31. – Issue 4.
[77] Petrunenko V.V. The Golden Section of quantum states and its astronomical and physical manifestations / V.V. Petrunenko. – Minsk: Pravo i economika, 2005. (In Russian).
[78] Shulman M.K. Reflections on the code of a nature and on self-organizing matter. – (http://www.chronos.msu.ru/ RREPORTS/shulman_razmyshlenia.htm). – Title from the screen.
[79] Stakhov A.P. The "Golden" Number Theory and New Properties of Natural Numbers / A.P. Stakhov // British Journal of Mathematics & Computer Science. – 2015. – Vol. 11. – Issue 6. – P. 1-15.
[80] Stakhov A.P. Hilbert's Fours Problem as a Possible Candidate on the MILLENNIUM PROBLEM in Geometry / A.P. Stakhov, S.Ch. Aranson // British Journal of Mathematics & Computer Science. – 2016. – Vol. 12. – Issue 4. – P.1 -25.
[81] Stakhov A.P. The Fine-Structure Constant as the Physical-Mathematical MILLENNIUM PROBLEM / A.P. Stakhov, S.Ch. Aranson // Physical Science International Journal. – 2016. – Vol. 9. – Issue 1. – P.1 - 36.
[82] Stakhov A.P. Fibonacci p-codes and Codes of the "Golden" p-proportions: New Informational and Arithmetical Foundations of Computer Science and Digital Metrology for Mission-Critical Applications /A.P. Stakhov // British Journal of Mathematics & Computer Science. – 2016.
[83] Stakhov A.P. Assisted by Scott Olsen. The "Golden" Non-Euclidean Geometry. Hilbert's Fourth Problem, "Golden" Dynamical Systems, and the Fine-Structure Constant / A.P. Stakhov, S.Ch. Aranson. – London; New Jersey; Singapore; Beijing; Shanghai; Hong Kong; Taipei; Chennai: World Scientific , 2016.
[84] Mitropolsky Y.A. Commentary on the Scientific Research of Ukrainian Scientist Professor, Doctor of Computer Science Alexey Stakhov / Y.A. Mitropolsky // Academy of Trinitarism, Moscow: № 77 – 6567, publication 12452, 2005. – (http://www.trinitas.ru/rus/doc/0232/006a/02320005.htm). – Title from the screen.
[85] Olsen S. A. Professor Alexey Stakhov is an absolute genius of modern science (in Honor of Alexey Stakhov's 70th Birthday) / Scott A. Olsen // Academy of Trinitarism, Moscow: № 77 – 6567, publication 15281, 2009. – (http://www.trinitas.ru/rus/doc/0232/012a/02322061.htm). – Title from the screen.

Рецензент: Сергій Рассомахін, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: rassomakhin@karazin.ua

Надійшло: травень 2016.

Автори:
Олексій Стахов, д.т.н., проф., академік Академії інженерних наук України, Міжнародний Клуб Золотого перетину, Болтон, Онтаріо, Канада. E-mail: goldenmuseum@rogers.com

Золотий перетин, числа Фібоначчі, математика гармонії і "золота" наукова революція.
Анотація. Видавничий дім "World Scientific" нещодавно опублікував дві фундаментальні праці: "Математика гармонії" (2009), автор Олексій Стахов, і '"Золота' неевклідова геометрія" (2016), авторів Олексія Стахова і Самуїла Арансона. У пред-

ставленій статті автор розвиває математику гармонії і 'золоту' неевклідову геометрію як новий меж-дисциплінарний напрямок сучасної науки, що засноване на золотому перетині, числах Фібоначчі та їх узагальненнях. Новітні відкриття в різних галузях сучасної науки, що засновані на математиці гармонії, а саме, математики (загальної теорії гіперболічних функцій і вирішенні четвертої проблеми Гільберта, алгоритмічної теорії вимірювання і 'золотий' теорії алгоритмів), комп'ютерних науках ('золота' інформаційна технологія), кристалографія (квазікристали), хімія (фулерени), теоретична фізика та космологія (перетворення Фібоначчі-Лоренца, 'золота' інтерпретація спеціальної теорії відносності і 'золота' еволюція Всесвіту), ботаніка (нова геометрична теорія філотаксису), генетика ('золоті' геноматриці) і т.д., створює загальну картину 'золотої' наукової революції, яка може фундаментально впливати на розвиток сучасної науки і освіти.

Ключові слова: золотий перетин, математика гармонії, біноміальні коефіцієнти, трикутник Паскаля, гіперболічні функції Фібоначчі і Люка, четверта проблема Гілберта, матриці Фібоначчі, "золоті" матриці.

Рецензент: Сергей Рассомахин, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: rassomakhin@karazin.ua

Поступила: май 2016.

Авторы:
Алексей Стахов, д.т.н., проф., академик Академии инженерных наук Украины, Международный Клуб Золотого сечения, Болтон, Онтарио, Канада. E-mail: goldenmuseum@rogers.com

Золотое сечение, числа Фибоначчи, математика гармонии и “золотая” научная революция.

Аннотация. Издательский дом “World Scientific” недавно опубликовал две фундаментальные работы: "Математика гармонии" (2009), автор Алексей Стахов, и "'Золотая' неевклидова геометрия" (2016), авторов Алексея Стахова и Самуила Арансона. В представленной статье автор развивает математику гармонии и 'золотую' неевклидову геометрию как новое междисциплинарное направление современной науки, основанное на золотом сечении, числах Фибоначчи и их обобщениях. Новейшие открытия в разных областях современной науки, основанные на математике гармонии, а именно, математики (общей теории гиперболических функций и решении четвертой проблемы Гильберта, алгоритмической теории измерения и 'золотой' теории алгоритмов), компьютерных науках ('золотая' информационная технология), кристаллография (квазикристаллы), химия (фуллерены), теоретическая физика и космология (преобразования Фибоначчи-Лоренца, 'золотая' интерпретация специальной теории относительности и 'золотая' эволюция Вселенной), ботаника (новая геометрическая теория филлотаксиса), генетика ('золотые' геноматрицы) и т.д., создает общую картину 'золотой' научной революции, которая может фундаментально повлиять на развитие современной науки и образования.

Ключевые слова: золотое сечение, математика гармонии, биномиальные коэффициенты, треугольник Паскаля, гиперболические функции Фибоначчи и Люка, четвертая проблема Гильберта, матрицы Фибоначчи, “золотые” матрицы.

UDC 004.056.55

KEY SCHEDULE OF BLOCK SYMMETRIC CIPHERS

Alexandr Kuznetsov[1], Yuriy Gorbenko[1], Ievgeniia Kolovanova[1]

V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
kuznetsov@karazin.ua, YuGorbenko@iit.kharkov.ua, e.kolovanova@gmail.com

Reviewer: Victor Dolgov, Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
dolgovvi@mail.ru

Received on June 2016.

Abstract. We investigate combinatorial properties of the block symmetric ciphers key schedule in the assumption that the cyclic (round) keys are generated randomly, with equal probability and independently of each other. The model of random homogeneous substitution is used for an abstract description of this formation. Analytical expressions allow us to estimate the power of implemented encryption-decryption maps set, obtain estimates of the probability properties of round keys sequences and ratios of the average number of different key sequences to power of different master keys set. The simulation results confirm the accuracy and validity of these analytical expressions.

Key words: key schedule, cyclic keys, combinatorial properties, block symmetric ciphers.

1 Problem statement and analysis of the literature

Ciphering is widely used in modern information and telecommunication systems for information protection and security. Ciphering is a reversible cryptographic transformation of open data to hide its semantic content from unauthorized user (attacker). Bijective processes of encryption and decryption of plaintext blocks and ciphertext blocks are parameterized by key data, which is the same for symmetric cryptographic transformation [1].

Most of block symmetric ciphers (BSC) are iterative [1], so the encryption is realized by cyclically repeating reversible round function (Fig. 1). The round (cyclic) keys $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ are used for parameterization of round transformations at each iteration of BSC. These keys are formed by extending (key scheduling) the master key $K^{(x)}$ [1].

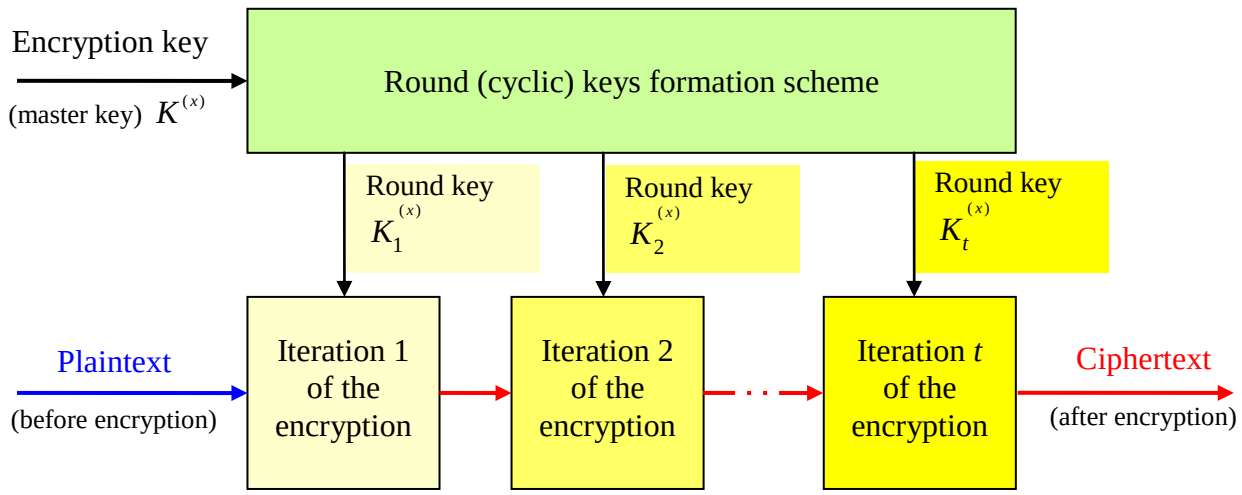


Fig. 1 - Block diagram of an iterative block cipher

© Kuznetsov A., Gorbenko Y., Kolovanova Ie., 2016

The structure of iterative BSC key schedule and simplicity of round keys formation and/or interdependence are used in the known attacks on the key schedule construction, especially slide attack [2-4], related-key attack [5-7], etc [1].

In the simplest case the key schedule construction can consist of master key repetition for each round. A similar approach was used in the formation of cyclic keys in the Soviet symmetric algorithm of cryptographic transformation GOST (State Standard) 28147-89, which is now also the encryption standard of Ukraine DSTU (State Standards of Ukraine) GOST 28147: 2009 [1]. However, in the case where to the input of each round function (see. Fig. 1) a certain key is fed, and this key is the same for all rounds, the cipher becomes vulnerable to slide attack [2,3]. The option when deployment function involves cyclic repetition of a certain set of round keys (round self-similarity ciphers) can also be easily reduced to this case [4].

To confront the key schedule cryptanalytic attacks modern BSC use the complicated round keys schedule construction implemented using conversion cipher transformations. One of these BSC is the US national standard FIPS -197 (AES) [8,9], adopted in 2001. It is an international algorithm, which is the most prevalent in today's security protocols. The key schedule of BSC AES is a linear array of 4-byte words. The first elements of the array contain master encryption key, the rest are determined recursively by modulo summation of two previous items. For certain positions of the array additional cipher transformation is also applied, in particular, the nonlinear permutation data block, and cyclic shift and etc. [8,9]. As a result, a sequence of round key $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ is formed which non-linearly dependent's on the original master key $K^{(x)}$, and this additional nonlinearity can effectively resist slide attacks on key schedule [1].

Related-key attacks were first proposed in [5] and further developed in [6,7]. In particular, the first cryptanalytic attack on the basis of related keys on a full-cipher AES-192 and AES-256 (variants of FIPS-197 with key lengths 192 and 256 bits) was described in [7]. It should be noted that the attacks in [7] are more effective than the full search of master keys, i.e. we can talk with certainty about the actual decrease of standardized cryptographic algorithm resistance.

Thus, the attacks on the key schedule are continuously improved and their possible use represents a real security threat to modern information systems and technologies [1-7]. Efficient BSC must effectively resist to the key schedule attacks and the key schedule construction must not contain any vulnerabilities caused by the simplicity of formation and the mutual dependence of cyclic keys [11]. In fact, we are talking about "ideal" round keys deployment, when each element of the sequence $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ are generated randomly, with equal probability, and independently of the other cyclic keys. Only in this case we can talk with certainty about the futility of the key schedule attacks because each round BSC is parameterized by randomly chosen value and would operate independently from other iterations of the encryption scheme (see. Fig. 1).

As an example of the key schedule schemes development we can use the algorithm "Kalyna", adopted as a national standard of BSC in Ukraine [12]. It has enhanced the cyclic key schedule construction, due to the use of special one-way functions. The cyclic keys of BSC "Kalyna" are formed as a result of several rounds of encryption, parameterized by auxiliary key. The auxiliary key, in its turn, is also formed as a result of multiple rounds encryption parameterized by master key. In other words, the separate elements of the cyclic keys sequence $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ are generated by independent encrypting of various input data blocks on different keys. Assuming that applied encryption implements are a random substitution (permutation) of data blocks [13-14], then the resulting round keys are generated randomly, with equal probability and independently of each other [11,15]. In particular, in [15] the properties of the key schedule of BSC "Kalyna" are investigated to confirm the resilience of the cipher to related-key attacks and attacks on implementation.

It should be noted that, even under random, equiprobable and independent formation of the round key the corresponding sequence can be the same, what is equivalent to reduction the power of encryption-decryption implemented maps set.

The aim of this work is to analyses combinatorial properties of BSC key schedules, provided that cyclic keys are generated randomly, with equal probability and independently of each other. The model of random homogeneous substitution is used for an abstract description of this formation. The practical benefit of this research results consists in providing its interpretation in order to assess the properties of the key schedule in recently adopted national standard BSC of Ukraine.

2 Random substitution as a model for the cyclic keys formation

Let us consider the definition and basic properties of a random substitution (permutation) [13,14], that will be used further to assess the probability properties of round key sequences.

In combinatorics, a permutation is an ordered set of numbers $1,2,\ldots,n$, that is a bijection on the set $\{1,2,\ldots,n\}$, which puts the *i*-th elements of the set in correspondence to the i number. The number n in this case is called the order (degree) of permutation [13,14].

The substitution s of arbitrary set $Y=\{y_1,y_2,...,y_n\}$ is a rule that each element y_i of set Y puts in correspondence some other element $s(y_i)$ [13,14]:

$$s=\begin{pmatrix} y_1 & y_2 & \ldots & y_n \\ s(y_1) & s(y_2) & \ldots & s(y_n) \end{pmatrix}.$$

In group theory the substitution is a bijection of this set into itself, i.e. substitution s degrees n is considered as a permutation of the elements of the set $Y=\{y_1,y_2,...,y_n\}$ and for all $i=1,2,...,n$ corresponding $s(y_i)\in Y$.

The function $s(y_i)$ value for a specific element $y_i\in Y$ will be called the implementation of substitution s in *i*-th point.

The composition of substitutions s_u and s_w degree n is defined as the consistent fulfillment of the set Y elements permutation [13,14]:

$$s_u\circ s_w=\begin{pmatrix} y_1 & y_2 & \ldots & y_n \\ s_u(s_w(y_1)) & s_u(s_w(y_2)) & \ldots & s_u(s_w(y_n)) \end{pmatrix},\ s_u(s_w(y_i))\in Y.$$

Concerning operations of sequential substitutions execution the set of all $n!$ permutations degree n forms a group, called the symmetric group and denoted as $S_n=\{s_1,s_2,...,s_{n!}\}$.

By definition [13,14], random substitution (permutation) s_x is the random vector $\{s_x(y_1),s_x(y_2),...,s_x(y_n)\}$, where all elements take values from the Y set and the probability of a match of any two elements is equal to 0. In other words, a random substitution is randomly chosen permutation from the set S_n

$$s_x=\begin{pmatrix} y_1 & y_2 & \ldots & y_n \\ s_x(y_1) & s_x(y_2) & \ldots & s_x(y_n) \end{pmatrix},\ s_x\in S_n,\ x\in\{1,2,...,n!\},$$

defined by a set (vector) of random values $\{s_x(y_1),s_x(y_2),...,s_x(y_n)\}$, that match probabilities satisfy the following condition:

$$\forall i\neq j\in\{1,2,...,n\}: P(s_x(y_i)=s_x(y_j))=0.$$

Thus, under the implementation of a random substitution s_x we mean the specific implementation of random vector $\{s_x(y_1),s_x(y_2),...,s_x(y_n)\}$ and the corresponding value of the $s_x(y_i)$ function we will call the implementation of a random substitution s_x in the *i* -th point.

Independent random substitution is called such a random permutation $\{s_x(y_1),s_x(y_2),...,s_x(y_n)\}$, for which is true

$$P(s_x) = \frac{P(s_x(y_1))P(s_x(y_2))...P(s_x(y_n))}{\sum_{u=1}^{n!} P(s_u(y_1))P(s_u(y_2))...P(s_u(y_n))}.$$

If $\forall i,u \in \{1,2,...,n\} : P(s_u(y_i)) = n^{-1}$ then

$$P(s_x) = \frac{P(s_x(y_1))P(s_x(y_2))\dots P(s_x(y_n))}{\sum_{u=1}^{n!} P(s_u(y_1))P(s_u(y_2))\dots P(s_u(y_n))} = \frac{n^{-n}}{\sum_{u=1}^{n!} n^{-n}} = \frac{1}{n!} \quad (1)$$

and s_x is called the random, equiprobable and independent (or, in abbreviated form, homogeneous) random substitution.

Thus, the concept of a random homogeneous substitution corresponds to a uniform probabilistic distribution on the set $S_n = \{s_1, s_2, ..., s_{n!}\}$ with the independent implementation of random vectors

$$\{s_x(y_1), s_x(y_2), ..., s_x(y_n)\} \quad (2)$$

$$s_x \in S_n, \ \forall x \in \{1,2,...,n!\} : P(s_x) = (n!)^{-1}.$$

Modern BSC are commonly described by the random homogeneous substitution model [1,11], i.e. it is a standard assumption that probabilistic properties of a processed data blocks bijection implemented by encryption function, satisfies the characteristics of a random substitution.

Indeed, if random, equiprobable and independent selection of the master key $K^{(x)}$ is associated with the choice of substitution $s_x \in S_n$, then the resulting ciphering transformation will match a random, equiprobable and independent comparison of ciphertext blocks to plaintext blocks on all possible options of bijective mapping, parameterized by key. For instance, for l-bit cipher with a k bit master key the model of random substitution will consist of subset

$$S'_n = \{s'_1, s'_2, ..., s'_{2^k}\} \subset S_n = \{s_1, s_2, ..., s_{n!}\}$$

with random, equiprobable and independent 2^k substitutions degree $n = 2^l$ (acting on the set $Y = \{y_1, y_2, ..., y_{2^l}\}$ of binary data blocks). At that the choice of substitution $s'_x \in S'_n \subset S_n$ (implementation of random vector $\{s_x(y_1), s_x(y_2), ..., s_x(y_{2^l})\}$) is set randomly, with equal probability and independently of selected k-bit master key $K^{(x)}$ value.

We use the properties of random homogeneous substitution for the analysis of round key sequences probability characteristics. For this purpose, on the set S'_n we define the uniform probabilistic distribution:

$$\forall i \in \{1,2,...,2^l\}, \forall u \in \{1,2,...,2^k\} : P(s_u(y_i)) = 2^{-l},$$

i.e. all probabilities of comparison of i-th block from y_i and u-th block from $s_u(y_i)$ are equal to each other and do not depend on i or $.u..$ Therefore, the probability of a random selection of substitution $s'_x \in S'_n \subset S_n$ (and the corresponding encryption master key) does not depend on the type of substitution, and defined as the inverse value of the power of the master keys set. Using (1) we get the next form:

$$P(s'_x) = \frac{P(s'_x(y_1))P(s'_x(y_2))\dots P(s'_x(y_{2^l}))}{\sum_{u=1}^{2^k} P(s'_u(y_1))P(s'_u(y_2))\dots P(s'_u(y_{2^l}))} = \frac{2^{-nl}}{\sum_{u=1}^{2^k} 2^{-nl}} = 2^{-k}. \quad (3)$$

Applying the considered model of random homogeneous substitution to analyse the probability properties of the key schedule elements we can estimate probabilities of coincidence of individual cyclic keys and their sequences, assuming that the round keys are generated randomly, equiprobable and independent from each other.

3 Probabilistic Properties of cycle keys

Let us introduce the following notations. Let randomly, equiprobably (probability is equal to 2^{-k}) and independently generated master key $K^{(x)}$ with length k bit be the input of key schedule construction (fig. 1). Then we note the sequence of t formed round keys as $K_{p\kappa}^{(x)} = \{K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}\}$, where every $K_i^{(x)}$ is the i-th cyclic key with length l-bit.

Let us assume that the cyclic keys $K_i^{(x)}$ are independent implementations of a random homogeneous substitution in the *i*-th point:

$$\forall i \in \{1,2,...,t\} : K_i^{(x)} = s'_x(y_i),$$

i.e. they are generated randomly, equiprobably and independently from each other, and for every $K_i^{(x)}$ the specific implementation of a random substitution $s'_x \in S'_n \subset S_n$ (implementation of the vector $\{s'_x(y_1), s'_x(y_2), ..., s'_x(y_n)\}$) is independent of $i \in \{1,2,...,t\}$.

Consider the probabilistic properties of randomly generated round key $K_i^{(x)}$ values for some fixed i. We estimate the average number of different values of cyclic key can be formed using all 2^k values of master keys $K^{(x)}$.

Lemma. The average number of different l-bit cyclic keys $K_i^{(x)}$ formed by 2^k implementations of the random homogeneous substitution is defined by expression:

$$N(k,l) = 2^l(1-(1-2^{-l})^{2^k}) \approx 2^l\left(1-\left(\frac{1}{e}\right)^{2^{k-l}}\right) \approx 2^l\left(1-(0,37)^{2^{k-l}}\right). \quad (4)$$

Proof. If the formation scheme of every cyclic key from the sequence $K_{p\kappa}^{(x)}$ is described by the model of a random homogeneous substitution with probability (1) of selection $s'_x \in S'_n \subset S_n$ (by the entered master key $K^{(x)}$), then, by definition, for any fixed $i \in \{1,2,...,t\}$ the probability of $K_i^{(x)}$ does not depend on $y_i \in Y = \{y_1, y_2, ..., y_{2^l}\}$ or $K^{(x)}$ and it is defined as the inverse of the power of the set Y, i.e. it is equal to $P(s'_x(y_i) = K_i^{(x)}) = 2^{-l}$. Master keys $K^{(x)}$ are selected independently from each other and corresponding events $s'_x(y_i) = K_i^{(x)}$ are independent. Therefore, we can use the formula for finding the probability of target event M times in N tests (Bernoulli formula):

$$P(N,M) = C_N^M(1-P(s'_x(y_i) = K_i^{(x)}))^{N-M}(P(s'_x(y_i) = K_i^{(x)}))^M = C_N^M(1-2^{-l})^{N-M}(2^{-l})^M.$$

The value $P(N,M)$ specifies the probability that at N independent implementations of random homogeneous substitution in i-th point a specific round key $K_i^{(x)} = s'_x(y_i)$ appears exactly M times. The value

$$P(2^k,0) = (1-2^{-l})^{2^k}$$

specifies probability that at $N = 2^k$ independent implementations of random substitution in i-th point (in full set of master keys $K^{(x)}$ values) the round key $K_i^{(x)} = s'_x(y_i)$ will not appear a single time.

Inverse value

$$P(2^k,>0) = 1-P(2^k,0) = \sum_{i=1}^{2^k} C_{2^k}^i (1-2^{-l})^{2^k-i}(2^{-l})^i = 1-(1-2^{-l})^{2^k} \quad (5)$$

specifies probability of an event when at 2^k independent tests the round l- bit length key $K_i^{(x)}$ will be formed at least once.

Power of different *ℓ-bit* values set is equal to 2^ℓ where each of these values in 2^k independent implementations of the vector (2) appears at least once in i-th point of random substitution with prob-

ability (5). I.e. for 2^k different master keys $K^{(x)}$ defining vector (2) implementation by the key schedule construction it will be formed in average

$$N(k,l) = 2^l P(2^k, >0) = 2^l (1-(1-2^{-l})^{2^k})$$

different round keys $K_i^{(x)}$. Using substitution $(1-2^{-l})^{2^l} \approx e^{-1}$ gives us a simplified formula in the right side of the expression (3), and, thus, completes the proof.

For the most simple case $k = l$ (equality of ciphertext block length to key length) the probability (5) gets the form

$$P(2^l, >0) = \sum_{i=1}^{2^l} C_{2^l}^i (1-2^{-l})^{2^l - i} (2^{-l})^i = 1 - P(2^l, 0) = 1 - (1-2^{-l})^{2^k} \approx 1 - e^{-1} \approx 0,63$$

and the ratio of the average number $N(k,l)$ of different round keys $K_i^{(x)}$ to the number of 2^k different master keys $K^{(x)}$ under $k = l$ is determined as

$$\delta(k,l) = \frac{N(k,l)}{2^k} = \frac{2^l (1 - P(2^k, 0))}{2^k} = P(2^l, >0) \approx 1 - e^{-1} \approx 0,63 \qquad (6)$$

what corresponds to the formula (27) in [15].

Under $k \neq l$ formula (6), as well as formula (27) in [15], is not satisfied, and we need to estimate the ratio $\delta(k,l)$ according to the general formula

$$\delta(k,l) = \frac{N(k,l)}{2^k} = 2^{l-k}(1-(1-2^{-l})^{2^k}) \approx 2^{l-k}\left(1 - \left(\frac{1}{e}\right)^{2^{k-l}}\right) \approx 2^{l-k}\left(1 - (0,37)^{2^{k-l}}\right). \qquad (7)$$

Let us consider an example of using these relations.

Fig. 2 and 3 show dependency of the probabilities (5) and the relationships (7) for the blocks of length $0 \le l \le 16$ and keys $0 \le k \le 16$. It is obvious that even for such small lengths l and k which do not exceed 16 bits, there is a sharp transition from very small values (almost equal to zero values $P(2^k, >0)$ and $\delta(k,l)$), to very large values (close to unity). This is true for the dependency $P(2^k, >0)$, and the multiplier 2^{l-k} in (7) smoothes the final function (7), inverting the high-quality form of the dependency (5).

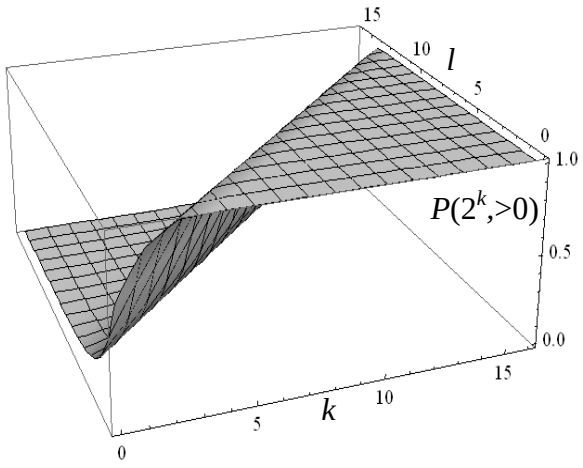


Fig. 2 - Dependence $P(2^k, >0)$, if $0 \le l \le 16$ and $0 \le k \le 16$

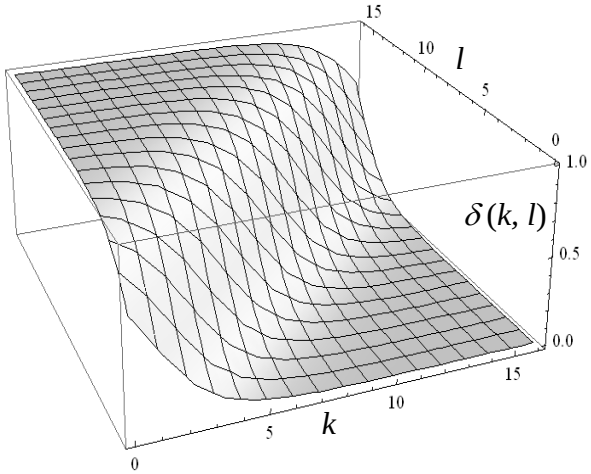


Fig. 3 - Dependence $\delta(k,l)$, if $0 \le l \le 16$ and $0 \le k \le 16$

Table 1 summarizes the values of the ratio of the different cyclic keys $K_i^{(x)}$ average number $N(k,l)$ to the number 2^k of different master keys $K^{(x)}$ for the most common values l and k in modern BSC and their scale models.

Data presented in Table 1 is calculated by the simplified formula on the right hand side of formula (7) using the Wolfram Alpha system computing algorithms [1,7]. These calculated values show efficiency of obtained analytical formulas for the round keys probability characteristics estimation.

Table 1 - The ratio of the average number of different l-bit cyclic keys $K_i^{(x)}$ formed by 2^k implementation of the random homogeneous substitution to the power of different master keys $K^{(x)}$ set

	k =16	***k =32***	***k =64***	***k =128***	***k =256***	***k =512***
***l* = 16**	0,63	$1{,}52\cdot10^{-5}$	$3{,}55\cdot10^{-15}$	$1{,}93\cdot10^{-34}$	$5{,}66\cdot10^{-73}$	$4{,}89\cdot10^{-150}$
***l* = 32**	$1-7{,}63\cdot10^{-6}$	0,63	$2{,}33\cdot10^{-10}$	$1{,}26\cdot10^{-29}$	$3{,}71\cdot10^{-68}$	$3{,}20\cdot10^{-145}$
***l* = 64**	$1-1{,}78\cdot10^{-15}$	$1-1{,}16\cdot10^{-10}$	0,63	$5{,}42\cdot10^{-20}$	$1{,}59\cdot10^{-58}$	$1{,}38\cdot10^{-135}$
***l* = 128**	$1-9{,}63\cdot10^{-35}$	$1-6{,}31\cdot10^{-30}$	$1-2{,}71\cdot10^{-20}$	0,63	$2{,}94\cdot10^{-39}$	$2{,}54\cdot10^{-116}$
***l* = 256**	$1-2{,}83\cdot10^{-73}$	$1-1{,}85\cdot10^{-68}$	$1-7{,}97\cdot10^{-59}$	$1-1{,}47\cdot10^{-39}$	0,63	$8{,}64\cdot10^{-78}$
***l* = 512**	$1-2{,}44\cdot10^{-150}$	$1-1{,}60\cdot10^{-145}$	$1-6{,}89\cdot10^{-136}$	$1-1{,}27\cdot10^{-116}$	$1-4{,}32\cdot10^{-78}$	0,63

To estimate probabilistic properties of cyclic keys $K_{p\kappa}^{(x)}$ sequences we summarize the positions of the lemma proved above for random, equiprobable and independent values $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$. Let us estimate the average number of different sequences $K_{p\kappa}^{(x)}$ that is generated using all 2^k values of master keys $K^{(x)}$. The following theorem is true.

Theorem. The average number of different cyclic keys sequences $K_{p\kappa}^{(x)} = \{K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}\}$, that is formed by 2^k independent implementations of random homogeneous substitution in i-th point, $i \in \{1,2,...,t\}$, is defined by:

$$N(k,l,t) = 2^l\left(1-(1-2^{-tl})^{2^k}\right) \approx 2^{tl}\left(1-\left(\frac{1}{e}\right)^{2^{k-tl}}\right) \approx 2^{tl}\left(1-(0{,}37)^{2^{k-tl}}\right). \quad (8)$$

Proof is a generalization of the lemma`s results in the case of $K_{p\kappa}^{(x)} = \{K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}\}$ sequences formation. Indeed, in accordance with the assumption of $K_i^{(x)}$ cyclic keys generating by the independent implementations of random homogeneous substitution in i-th point, for each $i \in \{1,2,...,t\}$ the probability of $K_i^{(x)}$ does not depend on $y_i \in Y = \{y_1, y_2, ..., y_{2^l}\}$ or $K^{(x)}$. This probability is equal to $P(s'_x(y_i) = K_i^{(x)}) = 2^{-l}$. The joint probability of independent events is the product of the probabilities of these events, i.e.:

$$P(K_{p\kappa}^{(x)} = \{K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}\}) = \prod_{i=1}^{t} P(s'_x(y_i) = K_i^{(x)}) = 2^{-tl}.$$

Master keys $K^{(x)}$ are selected independently from each other and the corresponding events $K_{p\kappa}^{(x)} = \{K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}\}$ are independent too. Therefore, using the Bernoulli formula just as in the lemma proof, we obtain the expression

$$P(N,M,t) = C_N^M (1-2^{-tl})^{N-M} (2^{-tl})^M,$$

which specifies the probability of the case that in N independent implementations the sequence $K_{pк}^{(x)}$ would appear exactly M times. The value

$$P(2^k,>0,t)=\sum_{i=1}^{2^k}C_{2^k}^{i}(1-2^{-tl})^{2^k-i}(2^{-tl})^{i}=1-P(2^k,0,t)=1-(1-2^{-tl})^{2^k} \qquad (9)$$

gives the probability of the case when in 2^k independent tests the specific sequence $K_{pк}^{(x)}$ is formed at least once.

The power of different t-sequences sets of l-bit values is equal to 2^{tl}, and each of these sequences with the probability (9) appear at the output of the round key schedule construction at least once. I. e. for 2^k different master keys $K^{(x)}$ that specify the implementations of random homogeneous substitution the cyclic key schedule construction it will be formed in average

$$N(k,l,t)=2^{tl}(1-P(2^k,0,t))$$

different $K_{pк}^{(x)}=\{K_1^{(x)},K_2^{(x)},...,K_t^{(x)}\}$ sequences, what under $(1-2^{-l})^{2^l}\approx e^{-1}$ simplification gives the target formula (8). This theorem allows us to obtain expression to estimate the ratio of different $K_{pк}^{(x)}$ sequences average number to the power of different $K^{(x)}$ master keys set:

$$\delta(k,l,t)=\frac{N(k,l,t)}{2^k}=2^{tl-k}(1-(1-2^{-tl})^{2^k})\approx 2^{tl-k}\left(1-\left(\frac{1}{e}\right)^{2^{k-tl}}\right)\approx 2^{tl-k}\left(1-(0,37)^{2^{k-tl}}\right) \qquad (10)$$

For convenience of $\delta(k,l,t)$ relations calculations we can write formula (10) in a different way. In the majority of practically important cases of block cipher (for instance, in estimating the properties of the BSC "Kalyna" key schedule) the master key length k is a multiple of the block length l, i.e. the ratio $k=ml$ is true, what after substitution in (10) it gives

$$\delta(ml,l,t)=2^{l(t-m)}(1-(1-2^{-tl})^{2^{ml}})\approx 2^{l(t-m)}\left(1-\left(\frac{1}{e}\right)^{2^{l(m-t)}}\right)\approx 2^{l(t-m)}\left(1-(0,37)^{2^{l(m-t)}}\right). \qquad (11)$$

Formula (11) shows that increasing of the multiplicity m is equivalent, in a probabilistic sense, to the corresponding decreasing of the sequence $K_{pк}^{(x)}=\{K_1^{(x)},K_2^{(x)},...,K_t^{(x)}\}$ length t. And conversely, the increasing of round keys sequence length t decreases the probability (9) as well master key length. A typical demonstration of this effect would be symmetry of function graphs relative to values l and k (Fig. 2,3). In this sense, the calculated values $\delta(ml,l,t)$ for the case $l\in\{16,32\}$ and $m,t\in\{1,2,4,8,16\}$ can be obtained from the data in Table 1 when selecting column with symbols ml and rows with symbols tl. As an example, table 2 shows the calculated values1 $\delta(ml,l,t)$ for $l=32$, which fully comply to the data presented in Table 1.

Table 2 - The ratio of the average number of different cyclic keys sequences to the power of set of different master keys length of $l=32$

	m = 1	**m = 2**	**m = 4**	**m = 8**	**m = 16**
t = 1	0,63	$2{,}33\cdot10^{-10}$	$1{,}26\cdot10^{-29}$	$3{,}71\cdot10^{-68}$	$3{,}20\cdot10^{-145}$
t = 2	$1-1{,}16\cdot10^{-10}$	0,63	$5{,}42\cdot10^{-20}$	$1{,}59\cdot10^{-58}$	$1{,}38\cdot10^{-135}$
t = 4	$1-6{,}31\cdot10^{-30}$	$1-2{,}71\cdot10^{-20}$	0,63	$2{,}94\cdot10^{-39}$	$2{,}54\cdot10^{-116}$
t = 8	$1-1{,}85\cdot10^{-68}$	$1-7{,}97\cdot10^{-59}$	$1-1{,}47\cdot10^{-39}$	0,63	$8{,}64\cdot10^{-78}$
t = 16	$1-1{,}60\cdot10^{-145}$	$1-6{,}89\cdot10^{-136}$	$1-1{,}27\cdot10^{-116}$	$1-4{,}32\cdot10^{-78}$	0,63

[1] *Values* $\delta(ml,l,t)$ *in tables 2-4 are calculated using simplified formula e* $\delta(ml,l,t)\approx 2^{l(t-m)}\left(1-e^{-2^{l(m-t)}}\right)$

The calculated values $\delta(ml,l,t)$ for cases $l \in \{64,128,256\}$, $m \in \{1,2,4,8\}$ and $t \in \{1,2,4,8,16\}$ are shown in Table 3.

The calculated values in Table 3 improve data on $\delta(k,l,t)$ estimation in [15]. The conclusion about virtually identical of the round keys sequences powers and encryption master keys in [15] is true. Data in the Table 3 clearly confirms this pattern. For all considered and practically significant relationships l and k, when $t > m$ is true, the ratio of the average number of different round keys sequences to the power of the different master keys set only slightly differs from unity. With further increasing of the round key sequence t length this difference rapidly decreases.

Table 3 - The ratio of the average number of different round keys sequences to the power of different master keys set

	***m* = 1**	***m* = 2**	***m* = 4**	***m* = 8**
***l* = 64**				
***t* = 1**	0,63	$1{,}52\cdot10^{-5}$	$5{,}66\cdot10^{-73}$	$4{,}89\cdot10^{-150}$
***t* = 2**	$1 - 7{,}62\cdot10^{-6}$	0,63	$3{,}71\cdot10^{-68}$	$3{,}20\cdot10^{-145}$
***t* = 4**	$1 - 1{,}78\cdot10^{-15}$	$1 - 1{,}16\cdot10^{-10}$	0,63	$8{,}64\cdot10^{-78}$
***t* = 8**	$1 - 2{,}44\cdot10^{-150}$	$1 - 1{,}60\cdot10^{-145}$	$1 - 1{,}27\cdot10^{-116}$	0,63
***t* = 16**	$1 - 5{,}13\cdot10^{-290}$	$1 - 9{,}46\cdot10^{-271}$	$1 - 3{,}22\cdot10^{-232}$	$1 - 3{,}73\cdot10^{-155}$
***l* = 128**				
***t* = 1**	0,63	$2{,}94\cdot10^{-39}$	$2{,}54\cdot10^{-116}$	$1{,}89\cdot10^{-270}$
***t* = 2**	$1 - 1{,}47\cdot10^{-39}$	0,63	$8{,}64\cdot10^{-78}$	$6{,}44\cdot10^{-232}$
***t* = 4**	$1 - 1{,}27\cdot10^{-116}$	$1 - 4{,}32\cdot10^{-78}$	0,63	$7{,}45\cdot10^{-155}$
***t* = 8**	$1 - 9{,}46\cdot10^{-271}$	$1 - 3{,}22\cdot10^{-232}$	$1 - 3{,}74\cdot10^{-155}$	0,63
***t* = 16**	$1 - 5{,}26\cdot10^{-579}$	$1 - 1{,}79\cdot10^{-540}$	$1 - 2{,}07\cdot10^{-463}$	$1 - 2{,}78\cdot10^{-309}$
***l* = 256**				
***t* = 1**	0,63	$8{,}64\cdot10^{-78}$	$6{,}44\cdot10^{-232}$	$3{,}58\cdot10^{-540}$
***t* = 2**	$1 - 4{,}32\cdot10^{-78}$	0,63	$7{,}45\cdot10^{-155}$	$4{,}15\cdot10^{-463}$
***t* = 4**	$1 - 3{,}22\cdot10^{-232}$	$1 - 3{,}73\cdot10^{-155}$	0,63	$5{,}56\cdot10^{-309}$
***t* = 8**	$1 - 1{,}79\cdot10^{-540}$	$1 - 2{,}08\cdot10^{-463}$	$1 - 2{,}78\cdot10^{-309}$	0,63
***t* = 16**	$1 - 5{,}54\cdot10^{-1157}$	$1 - 6{,}42\cdot10^{-1080}$	$1 - 8{,}61\cdot10^{-926}$	$1 - 1{,}55\cdot10^{-617}$
***l* = 512**				
***t* = 1**	0,63	$7{,}46\cdot10^{-155}$	$4{,}15\cdot10^{-463}$	$1{,}28\cdot10^{-1079}$
***t* = 2**	$1 - 3{,}73\cdot10^{-155}$	0,63	$5{,}56\cdot10^{-309}$	$1{,}72\cdot10^{-925}$
***t* = 4**	$1 - 2{,}08\cdot10^{-463}$	$1 - 2{,}78\cdot10^{-309}$	0,63	$3{,}09\cdot10^{-617}$
***t* = 8**	$1 - 6{,}42\cdot10^{-1080}$	$1 - 8{,}60\cdot10^{-926}$	$1 - 1{,}55\cdot10^{-617}$	0,63
***t* = 16**	≈ 1	≈ 1	≈ 1	$1 - 4{,}79\cdot10^{-1237}$

To confirm the adequacy and accuracy of the obtained results and our conclusions driven by these results the numerical experiment was executed. The experiment essence is counting the ratios

of the average number of different round keys sequences to power 2^k of the set of different master keys. To simulate the random substitution a simple function of random number generation, integrated into the environment of rapid applications development Embarcadero RAD Studio for Microsoft Windows from Embarcadero Technologies company, was used [18]. Each observation included estimation of sample mean (empirical average) of 100 model implementations. Each model implementation included calculation of the ratio of the average number of different round keys sequences to power 2^k of the set of different master keys.

In the experiment, we estimated both the sample means $\delta^*(ml,l,t)$ and sample variance D when the sample size of 100 elements. The results are summarized in Table 4. The last column of this table shows the accuracy values ε of the estimated characteristics for a given level of significance $\alpha = 0,05$.

Table 4 - Results of experimental researches and their comparison with theoretical calculations

	$\delta(ml,l,t)$	$\delta^*(ml,l,t)$	D	ε
***l* = 4, *m* = 1**				
***t* = 1**	0,632121	0,6453125	0,005716	0,014818
***t* = 2**	0,969391	0,969125	0,001758	0,008218
***t* = 3**	0,998049	0,9983125	0,000110	0,002056
***t* = 4**	0,999878	0,999875	0,000008	0,000554
***l* = 4, *m* = 2**				
***t* = 1**	0,062500	0,062500	0	0
***t* = 2**	0,632121	0,633074	0,000372	0,003780
***t* = 3**	0,969391	0,969675	0,000103	0,001989
***t* = 4**	0,998049	0,997934	0,000008	0,000554
***l* = 4, *m* = 3**				
***t* = 1**	0,003906	0,003906	0	0
***t* = 2**	0,062500	0,062500	0	0
***t* = 3**	0,632121	0,632152	0,000023	0,000940
***t* = 4**	0,969391	0,969492	0,000007	0,000519
***l* = 8, *m* = 1**				
***t* = 1**	0,632121	0,632836	0,000360	0,003719
***t* = 2**	0,998049	0,998051	0,000007	0,000519
***t* = 3**	0,999992	0,999961	0,000002	0,000277
***l* = 8, *m* = 2**				
***t* = 1**	0,003906	0,003906	0	0
***t* = 2**	0,632121	0,632176	0,000002	0,000277
***t* = 3**	0,998049	0,998063	$2,98 \cdot 10^{-8}$	$3,38 \cdot 10^{-5}$

As can be seen from the values in Table 4, results of experimental research fully confirm the validity of theoretical assumptions. In all cases the calculated values $\delta(ml,l,t)$ and obtained empirical

data $\delta^*(ml,l,t)$ differ on not more than ε (the absolute value of the error), and the probability with which the specified accuracy is achieved (the accuracy estimation) is 0,95. Since the accuracy characterizes the repeatability and stability of experiments [19], it can be argued that in 95% of the cases the value $\delta^*(ml,l,t)$ will differ from $\delta(ml,l,t)$ less than ε.

4 Conclusions and prospects for further researches

Our research of BSC round keys probabilistic properties have shown that even under random, equiprobable and independent formations the used key sequences can be the same, what inevitably reduces the power of implemented encryption-decryption mapping sets.

To describe the round keys schedule construction an abstract model of random substitution parameterized by encryption master key value was used. The obtained analytical relations allow us to estimate the probability properties of BSC cycle keys. In particular, the probability of multiple matching of round keys for a given number of the random homogeneous substitution implementations (a given number of master keys) is defined by Bernoulli formula. This ratio gives us an estimate of the probability of events when the specific round key will be generated at least once on the all set of master keys, i.e., it allows us to estimate the average number of different round keys on the output of formation scheme. The final result is also generalized on sequences of arbitrary length round keys, i.e., we can get numerical estimates of the probability properties of all BSC key schedule elements using the defined model.

Calculated values of ratios of the average number of different round keys sequences to power of different master keys sets provided in Tables 2,3, give an idea about ciphering of all admissible encryption-decryption mappings set. In particular, the given calculated values for the most important practical cases when the lengths of data blocks l and the keys $k = ml$ indicate that the number of rounds $t < m$, with probability close to unity, the specific round keys sequence will not be formed on the all set of master keys. This is equivalent to the fact, that average number of different round keys sequences will be negligible compared to the power of the of different master keys, i.e., the large number of mappings "plaintext - ciphertext" from the all set 2^k of maps would not be realized. And conversely, for the case $t > m$ the ratio of the average number of different round key sequences to the power of the master keys set almost does not differ from unity. With a further increase of t this difference decreases rapidly and it must be assumed that in such key schedule all valid mappings "plaintext - ciphertext" from a complete set 2^k of maps will be implemented. The conducted simulation modeling of the "ideal" key schedule construction allowed to obtain empirical estimates that coincide with theoretical calculations by formulas (9) - (11), what confirms the reliability and validity of research results. In particular, for all investigated cases the calculated values and obtained empirical data do not differ significantly (the relative error value < 3%), and the probability that the specified accuracy is achieved (the estimation accuracy) is 0,95. Therefore, we can argue that in 95% of the cases the calculated values and empirical data differ by less than error value.

It should be noted that the obtained analytical expressions and shown calculated values correspond to the hypothetical case of random, equiprobable and independent formation of round keys, i.e. to the "ideal" key schedule in the probabilistic aspect. The actual key schedule constructions are based on deterministic algorithms, parameterized by value of the encryption master key. Therefore, the obtained estimates on a random homogeneous substitution should be used as the upper limits for the probabilistic properties of round key sequences: the key schedule of real BSC can only approach in its characteristics to this "ideal" case and it does not improve the given calculated values.

The practical impact of these results lies in their immediate interpretation to estimate the probability properties of key schedule elements in the new national standard of BSC of Ukraine [12]. If the assumption that the cyclic keys of BSC "Kalyna" are independent implementations of random homogeneous substitution (i.e. it is formed random, equiprobability and independently of each other) is true, then the conclusion about virtually identical the powers of round keys sequences and encryption master keys is theoretically proven and the calculated values shown in Table 3 clearly confirm this regularity. Using in the new standard the "ideal" key schedules in addition to providing

resistance of cipher to the related keys attacks and to the attacks on implementation [15] allows to fully implement the key space of master keys and a corresponding set of maps "plaintext - ciphertext".

As perspective directions for further research one can mention the search or, at least, estimation the probability properties of subsets of the so-called BSC equivalent keys, when several different by value master keys lead to the formation of identical cyclic keys sequences, giving the identical bijective encryption-decryption mappings. In other words, the existence of the equivalent keys subsets reduces the power of the "plaintext - ciphertext" maps set, and the number of the key information that is numerically equal to the certainty measure of secret encryption parameters is also reduced. In addition, the existence of several master keys which are different by value, but equivalent by encryption function can be used by an attacker to implement cryptanalytic attacks, for instance, based on the substitution of protected information by false data in the case using of BSC in generation of message authentification code mode.

References

[1] Gorbenko I.D. Prykladna kryptologija. Teorija. Praktyka. Zastosuvannja: Pidruchnyk dlja vyshhyh navchal'nyh zakladiv / I.D. Gorbenko, Ju.I. Gorbenko. – Harkiv: Fort, 2013. – 880 s.
[2] Biryukov A. Slide Attacks / A.Biryukov, D.Wagner // Fast Software Encryption: 6th International Workshop, FSE'99 Rome, Italy, March 24–26, 1999 Proceedings. – Springer Berlin Heidelberg, 1999. – P. 245 – 259.
[3] Chalermpong Worawannotai, Isabelle Stanton A Tutorial on Slide Attacks [Electronic Resource]. – Way of access: http://www.eecs.berkeley.edu/~isabelle/slideattacks.pdf. – Title from the screen.
[4] Biryukov A. Advanced Slide Attacks / A. Biryukov, D. Wagner // Advances in Cryptology – EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14-18, 2000 Proceedings. – Springer Berlin Heidelberg, 2000. – P. 589 – 606.
[5] Biham E. New types of cryptanalytic attacks using related keys / E.Biham // Springer-Verlag. – 1994. – № 4. – P. 229 – 246.
[6] Ciet M., Piret G., Quisquater J.-J. Related-Key and Slide Attacks: Analysis, Connections, and Improvements (Extended Abstract) [Electronic Resource]. – Way of access: http://citeseer.ist.psu.edu. – 2002. – Universite catholique de Louvain, Louvain-la-Neuve, Belgium. – Title from the screen.
[7] Biryukov A. Related-Key Cryptanalysis of the Full AES-192 and AES-256/ A. Biryukov, D. Khovratovich // Springer Berlin Heidelberg. – 2009. – P. 1 – 8.
[8] Daemen J. AES proposal: Rijndael / J. Daemen, V. Rijmen [Electronic Resource]. – Way of access: http://www.nist.gov/aes. – 1998. – Title from the screen.
[9] FIPS-197: Advanced Encryption Standard (AES) // National Institute of Standards and Technology. – 2001 [Electronic Resource]. – Way of access: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. – Title from the screen.
[10] Polozhennja pro porjadok zdijsnennja kryptografichnogo zahystu informacii' v Ukrai'ni, zatverdzhene Ukazom Prezydenta Ukrai'ny vid 22 travnja 1998 roku N 505/98.
[11] Rozrobka novogo blokovogo symetrychnogo shyfru: Zvit za pershyj etap NDR «Algorytm» (promizhnyj) / nauk. ker. I. D. Gorbenko; AT «IIT». – Kharkiv, 2014. – Tom 4. – 304 s.
[12] Informacijni tehnologii'. Kryptografichnyj zahyst infomacii'. Algorytm symetrychnogo blokovogo peretvorennja: DSTU 7624:2014. – K.: Minekonomrozvytku Ukrai'ny, 2015. – 238 s. – (Nacional'nyj standart Ukrai'ny).
[13] Sachkov V. N. Vvedenie v kombinatornye metody diskretnoi matematiki / V.N. Sachkov. – Moskva: Nauka, 1982. – 384 s.
[14] Sachkov V. N. Veroyatnostnye metody v kombinatornom analize / V.N.Sachkov. – Moskva: Nauka, 1978. – 287 s.
[15] Olijnykov R. V. Metody analizu i syntezu perspektyvnyh symetrychnyh kryptografichnyh peretvoren': avtoref. dys. na zdobuttja nauk.stupenja d-ra tehn. nauk: 05.13.05 / R. V. Olijnykov; HNURE. – Harkiv, 2014. – 42 c. – ukr.
[16] NIST Special Publication 800-38D. Block Cipher Modes [Electronic Resource]. – Way of access: http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html. – Title from the screen.
[17] Voprosno-otvetnaya sistema Wolfram Alpha Modes [Electronic Resource]. – Way of access: http://www.wolframalpha.com /. – Title from the screen.
[18] Integrirovannaya sreda razrabotki Embarcadero RAD Studio [Electronic Resource]. – Way of access: http://www.embarcadero.com/ products/rad-studio. – Title from the screen.
[19] Venttsel' E.S. Teoriya veroyatnostei i ee inzhenernye prilozheniya: Ucheb. posobie dlya vtuzov / E.S. Venttsel', L.A. Ovcharov. – 2-e izd., ster. – Moskva: Vyssh. shkola, 2000. – 480 s.

Надійшло: червень 2016.

Автори: Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: kuznetsov@karazin.ua
Юрій Горбенко, к.т.н., с.н.с., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: YuGorbenko@iit.kharkov.ua
Євгенія Колованова, к.т.н., ст. викладач, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: e.kolovanova@gmail.com

Ключовий розклад блокових симетричних шифрів.

Анотація: Досліджуються комбінаторні властивості ключового розкладу блокових симетричних шифрів в припущенні, що циклові (раундові) ключі формуються випадково, рівноймовірно і незалежно один від одного. Для абстрактного опису такого формування використовується модель випадкової однорідної підстановки. Отримані аналітичні вирази дозволяють оцінити потужність множини реалізованих відображень зашифрування-розшифрування, отримати оцінки імовірнісних властивостей послідовностей раундових ключів і відносин середнього числа різних ключових послідовностей до потужності множини різноманітних майстер-ключів. Результати імітаційного моделювання підтверджують достовірність і обгрунтованість отриманих аналітичних виразів.

Ключові слова: ключовий розклад, циклові ключі, комбінаторні властивості, блокові симетричні шифри.

Рецензент: Виктор Долгов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: dolgovvi@mail.ru

Поступила: июнь 2016.

Авторы: Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kuznetsov@karazin.ua
Юрий Горбенко, к.т.н., с.н.с, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: YuGorbenko@iit.kharkov.ua
Евгения Колованова, к.т.н., ст. преподаватель, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: e.kolovanova@gmail.com

Ключевое расписание блочных симметричных шифров.

Аннотация: Исследуются комбинаторные свойства ключевого расписания блочных симметричных шифров в предположении, что цикловые (раундовые) ключи формируются случайно, равновероятно и независимо друг от друга. Для абстрактного описания такого формирования используется модель случайной однородной подстановки. Полученные аналитические выражения позволяют оценить мощность множества реализуемых отображений зашифрования-расшифрования, получить оценки вероятностных свойств последовательностей раундовых ключей и отношений среднего числа различных ключевых последовательностей к мощности множества различных мастер-ключей. Результаты имитационного моделирования подтверждают достоверность и обоснованность полученных аналитических выражений.

Ключевые слова: ключевое расписание, цикловые ключи, комбинаторные свойства, блочные симметричные шифры.

EDITOR-IN-CHIEF:

Mykola Azarenkov
Doctor of Sciences (Physics and Mathematics),
Full Professor, Academician of the National Academy of Sciences of Ukraine,
V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: azarenkov@karazin.ua

DEPUTY EDITORS:

Alexandr Kuznetsov
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: kuznetsov@karazin.ua

Serghii Rassomakhin
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: rassomakhin@karazin.ua

SECRETARY:

Serghii Malakhov
Ph.D., Senior Researcher,
V. N. Karazin Kharkiv National University,
Svobody sq., 4, Kharkiv, 61022, Ukraine
E-mail: malakhov@karazin.ua

EDITORIAL BOARD:

Junzo Watada
Doctor of Engineering, Professor,
The Graduate School of Information, Production and Systems (IPS), Waseda University,
2-7 Hibikino, Wakamatsuku, Kitakyushu, Fukuoka 808-0135, Japan
E-mail: junzow@osb.att.ne.jp

Vyacheslav Kalashnikov
Doctor of Sciences (Physics and Mathematics),
Full Professor, Department of Systems and Industrial Engineering, Tecnológico de Monterrey,
Eugenio Garza Sada av. 2501, 64849 Monterrey,
Nuevo León, México
E-mail: kalash@itesm.mx

Vassil Nikolov Alexandrov
Ph.D., Professor,
Barcelona Supercomputing Centre,
Jordi Girona, 29, 3rd floor, Edifici Nexus II,
E-08034 Barcelona, Spain
E-mail: vassil.alexandrov@bsc.es

Alfredo Noel Iusem
Ph.D., Professor,
Instituto Nacional de Matemática Pura e Aplicada (IMPA),
Estrada Dona Castorina 110, Jardim Botânico,
Rio de Janeiro, RJ, CEP 22460-320, Brazil
E-mail: iusp@impa.br

ГОЛОВНИЙ РЕДАКТОР:

Микола Азарєнков
доктор фізико-математичних наук, професор,
академік Національної академії наук України,
Харківський національний університет
імені В. Н. Каразіна, майдан Свободи 4,
м. Харків, 61022, Україна
E-mail: azarenkov@karazin.ua

ЗАСТУПНИКИ ГОЛОВНОГО РЕДАКТОРА:

Олександр Кузнецов
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: kuznetsov@karazin.ua

Сергій Рассомахін
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: rassomakhin@karazin.ua

ВІДПОВІДАЛЬНИЙ СЕКРЕТАР:

Сергій Малахов
кандидат технічних наук, ст. науковий співробітник,
національний університет імені В. Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна
E-mail: malakhov@karazin.ua

РЕДАКЦІЙНА КОЛЕГІЯ:

Джунзо Ватада
доктор технічних наук, професор,
Вища школа інформації, виробництва і систем Університету Васеда,
2-7 Хібікіно, Вакаматсуку, Кітак'юшу, Фукуока 808-0135, Японія
E-mail: junzow@osb.att.ne.jp

В'ячеслав Калашников
доктор фізико-математичних наук, професор,
департамент систем і промислового виробництва Технологічного університету Монтеррея,
пр. Еухеніо Гарса Сада 2501, 64849 Монтеррей,
Нуево-Леон, Мексика
E-mail: kalash@itesm.mx

Василь Ніколов Александров
доктор філософії, професор,
Барселонський суперкомп'ютерний центр,
Хорді Жирона, 29, 3-й поверх, Едіфічі Нексус II,
E-08034 Барселона, Іспанія
E-mail: vassil.alexandrov@bsc.es

Альфредо Ноель Юсем
доктор філософії, професор,
Національний інститут теоретичної та прикладної математики,
Естрада Дона Касторіна 110 Жардін-Ботанико,
Ріо-де-Жанейро, RJ CEP 22460-320, Бразилія
E-mail: iusp@impa.br

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,
350 Victoria Street, 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
E-mail: 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
Ph.D., 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, 1360 Fornebu, Norway
E-mail: oleksandr.kazymyrov@evry.com

Mikołaj Karpiński
Doctor of Sciences (Engineering), Full Professor,
University of Bielsko-Biala,
ul. Willowa 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 - Спільнота 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 Геворков
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
E-mail: 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 Ренген
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,
76 Prószkowska Street, 45-758 Opole, Poland
E-mail: xoma@wp.pl

Joanna Świątkowska
Ph.D., CYBERSEC Programme Director,
Senior Research Fellow of the Kosciuszko Institute,
Feldmana ul. 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, CA 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

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

Valeriy 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

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, Prospect Peremohy, 03056, Kyiv-56, Ukraine
E-mail: lusi.kovalchuk@gmail.com

Володимир Хома
доктор технічних наук, професор,
Інститут «Автоматика та інформатика», Технологічний університет Ополе,
вул. Пружовська 76, 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
Ph.D., професор,
факультет інформатики, Каліфорнійський університет,
Санта-Барбара, 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

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

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, Prospect Peremohy, 03056, Kyiv-56, Ukraine
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,
12 Bandera st., Lviv, 79013, Ukraine
E-mail: vmax@polynet.lviv.ua

Oleksiy Borysenko
Doctor of Sciences (Engineering), Full Professor, Sumy State University,
2, Rymskogo-Korsakova st., 40007 Sumy, Ukraine
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
E-mail: abelnau@ukr.net

Sergii Kavun
Doctor of Sciences (Economics), Ph.D. (Engineering), Full Professor, Department of Information Technologies, Kharkiv Educational and Research Institute of the University of Banking,
Peremogy av. 55, Kharkiv, 61174, Ukraine
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., 61070, Kharkiv, Ukraine
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

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

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

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

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

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

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

Сергій Кавун
доктор економічних наук, кандидат технічних наук, професор, кафедра інформаційних технологій,
Харківський навчально-науковий інститут ДВНЗ "Університет банківської справи",
пр. Перемоги 55, м. Харків, 61174, Україна
E-mail: kavserg@gmail.com

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Статті пройшли внутрішнє та зовнішнє рецензування.

Наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

Випуск 2(2) 2016

Міжнародний електронний науково-теоретичний журнал

Англійською, українською, російською мовами

Комп'ютерне верстання – Федоренко В.В.

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

V. N. Karazin Kharkiv National University Publishing