FUNCTIONAL SAFETY AND SURVIVABILITY OF INFORMATION CONTROL ELLIPTIC-CURVE-BASED SYSTEMS: MODELS AND METHODS

Marek Aleksander[1], Mikolaj Karpinski[2], Grzegorz Litawa[3]

[1]State Higher Vocational School in Nowy Sacz, Poland
[2]University of Bielsko-Biala & State Higher Vocational School in Nowy Sacz, Poland
[3]National Ivan Puluj Technical University, Ukraine & State Higher Vocational School in Nowy Sacz, Poland

ALEKSANDER Marek A., Candidate of Science (PhD)

Date and place of birth: 1974, Nowy Sacz, Poland
Education: AGH University of Science and Technology in 2000 & Military University of Technology in 2004
Research interests: cryptology, mathematic modeling, wireless network security, electronics
Current position & Functions: director of Institute of Engineering
Publications: author and co-author of over 40 publications
E-mail: aleksmar@pwsz-ns.edu.pl

KARPINSKI Mikolaj P., Doctor of Science (DSc)

Date and place of birth: 1958, Baley, Chita Oblast, Russia.
Education: Lviv Polytechnic Institute, 1980.
Research interests: cybersecurity, computer systems and wireless networks, especially their security, in particular cryptographic methods of information defense, lighting engineering and electric and photometric measurements.
Current position & Functions: Chairman of Computer Science Division since 2009.
Publications: over 100 scientific publications including monographs, papers in domestic & foreign scientific journals, international conferences proceedings, patents etc.
E-mail: mkarpinski@ath.bielsko.pl

LITAWA Grzegorz K.

Date and place of birth: 1975, Stara Wies, Poland.
Education: University of Rzeszow in 2000, Pedagogical University of Cracow in 2001
Research interests: cryptography, cryptanalysis, calculations distracted, design of digital circuits with the use in cryptograph and computer network security.
Current position & Functions: Postgraduate student and assistant professor.
Publications: author and co-author of over 16 publications.
E-mail: glitawa@poczta.onet.pl

Abstract. *There is an analysis of functional safety and survivability of information control systems relying on elliptic curve-based calculations. Time required for solving a discrete logarithm on GF(p) elliptic curves was worked out. Presented were aspects of the use of FPGA systems whose calculations were based on Rademacher-Krestenson's remaining classes and parallel summing.*

Key words: *information control system, elliptic curve, functional safety, survivability, system of Rademacher-Krestenson's residual classes.*

1. Introduction

Economic potential growth of every country is closely connected with technological security. One of the most important factors ensuring this safety is information technology (IT), which is actually a tool for designing and implementing infrastructure security management system [1-3]. There is a growing attention paid to information protection and privacy issues [4-6]. Theoretically every fifth failure of nuclear power equipment or every fifth failure in space-rocket technology might be caused by neglected additional

safety deficits, that is information control systems (ICS). This is clearly an international issue and so there have been many international conferences held with respect to IT survivability and functional safety: DESSERT, DSN, EDCC, ESREL, SAM, SAFECOMP among others [3]. These researches along with development of integrated remote sensors constitute one of the leading directions in science and one of the greatest challenges for 21st century engineering. It was recognized as such, defined by National Science Foundation (NSF) and proposed to be realized in accordance with relevant Resolution of Ukrainian NAN Presidium. Another distinguished class comprises ICS based on elliptic curves (ICSEC) where cryptographic operations are carried out on elliptic curves – elliptic curve cryptography device (ECCD). This fact evokes need of designing, implementing and further development of appropriate models and methods for optimizing ICSEC survivability and functional safety. The aim of this article is to assess the functional safety and survivability of ECCDs. Procedures concerning research and assessment of the functional safety and survivability were based on specifically designed models increasing speed of basic arithmetic operations on GF(p) elliptic curves (ECs) [7]. One of basic factors determining encryption/decryption time and consequently safety of ECCD is the speed of EC point's addition process. All the most efficient algorithms, known today, for solving discrete logarithms exploit the addition process as one of the main calculations. It appears obvious that the EC point's addition process directly determines the time needed for solving the discrete logarithm problem and consequently sets the security level.

2. Model evaluation of functional security and survivability of ICSEC

Based on risk-oriented model evaluation of ICSEC safety mentioned in [8-11] the following is true

$$R(t) = p(t)\, D, \tag{1}$$

where non-dimensional value $R(t)$ – risk over time t related to some event, a value which is often referred to as safety indicator;

$p(t)$ – probability of the event, in other words probability that ICS enters dangerous state within time t;

D – coefficient, determined by management object, representing a set of all possible unwanted results caused by the event.

Let's assume fault-tolerant multiprocessor ICS [9] performance P to ICSEC state evaluation ratio as a base and let's introduce the following components:

p_{wwf} – probability that ICSEC works without failures;

f_s – safety function, that is the smallest subset of ICSEC functions of the highest priority responsible for preventing the system from entering dangerous state;

P_s – ICSEC performance required for safety function realization and under which there is a fault;

m – total number of safety functions;

p_{ds} – probability that ICSEC enters dangerous state within time t;

n – total number of processor devices in ICSEC;

n_{ECCD} – number of ECCD;

x – state vector of ICSEC;

X_{ds} – set corresponding to dangerous states of ICSEC;

a_i and a_j – vector x components corresponding to i^{th} processor device state and j^{th} ECCD ($a_i = a_j = 0$ – for failure, $a_i = a_j = 1$ – for working capacity;

P_i and P_j – performance of i^{th} processor device and j^{th} ECCD;

P_x – performance of ICSEC in state corresponding to vector x.

Taking questions [9] into account the following is true:

$$P_x = \sum_{i=1}^{n-n_{ECCD}} \alpha_i P_i + \sum_{j=1}^{n_{ECCD}} \alpha_j P_j \le P_s, \tag{2}$$

$$p_{ds}(t) = \sum_{x \in X_{ds}} p_x(t)\Big|_{\forall x \in X_{ds}}, \tag{3}$$

where:

$$p_x(t)\Big|_{\forall x \in X_{ds}} = \prod_{i=1}^{n} p_i^{\alpha_i} \left(1 - p_i\right)^{1-\alpha_i} - \prod_{j=1}^{n-n_{ECCD}} p_j^{\alpha_j} \left(1 - p_j\right)^{1-\alpha_j} \tag{4}$$

which makes it possible to calculate the probability of an event that ICSEC enters dangerous state within time t caused by efficiency decrease – a result of ECCD failures.

3. The fast point addition process reduces|decreases the discrete logarithm solving time

Taking into account complexity of calculations and expense of addition two points on an EC it turns out reasonable to use mixed representation where one of the coordinates is an affine coordinate and the other is a projective one. In such a case calculating the addition of points [12] comes down to 11 multiplications, without addition and subtraction field operations. These two do not contribute much to the overall calculation time. In cryptographic devices based on curves there are large amount of modular multiplications while traditional approach to multiplication in computers does not provide satisfying results. Therefore calculations based on Rademacher-Krestenson's bases were used as much more effective. Krestenson's algorithm allows multiplication to be simplified to addition processes using previously generated tables [13]. Assume a multiplication of two numbers x and y modulo number p. In the multiplier model X and Y are represented as binary sequences.

$$\begin{aligned} X &= x_{r-1}2^{r-1} + x_{r-2}2^{r-2} + x_i 2^i + \ldots + x_1 2^1 + x_0 2^0 \\ Y &= y_{r-1}2^{r-1} + y_{r-2}2^{r-2} + y_j 2^j + \ldots + y_1 2^1 + y_0 2^0 \end{aligned} \tag{5}$$

In order to find multiplication result of the above a matrix, shown in table 1, where $m_{ij} = 2^{i+j} / \bmod n$, is constructed.

The product of the numbers, that is coordinates X i Y, is calculated according to formula:

$$X \cdot Y \bmod n = \sum_{s,k=1}^{r-1} m_{sk} \bmod n \tag{6}$$

where $x_s, y_k = 1$. That means m_{sk} lies at the intersection of column and row for which respectful x_i i y_j equal 1.

The problem of addition multi-bit numbers was solved by using an algorithm presented in the work [14],

allowing to divide multi-bit numbers into words of specified length and also parallel addition [15] of all the words resulting from that division. The above

Table 1

Determining the transformation matrix module based on Rademacher–Krestenson

I	y_{r-1}	...	y_j	...	y_1	y_0
x_{t-1}	$m_{r-1\ r-1}$	---	$m_{r-1\ j}$	---	$m_{r-1\ 1}$	$m_{r-1\ 0}$
...	---	---	---	---	---	---
x_i	$m_{i\ r-1}$	---	m_{ij}	---	m_{i1}	m_{i0}
...	---	---	---	---	---	---
x_1	$m_{1\ r-1}$	---	m_{1j}	---	m_{11}	m_{10}
x_0	$m_{0\ r-1}$	---	m_{0j}	---	m_{01}	m_{00}

described ideas led to construction of an EC point addition unit applicable both in encryption information by GF(p) curves based algorithms and solving discrete logarithm. Further on there will be presented encryption speed tests of ElGamal algorithm, using the modularmultiplication approach versus the same algorithm using traditional basic operations. Moving back to the main topic of the discussion let's summarize that majority of algorithms finding the discrete logarithm use EC point addition technique, further on, increasing the speed of point addition leads to a reduce time needed for finding the solution. One of the fastest algorithm solving algorithms based on point addition strategy is Pollard's Rho Parallel Algorithm. System which we used for solving discrete logarithm on EC(p) use point addition technique based on calculations in Krestenson's bases.

4. Construction and tests of elliptic curve point addition unit in FPGA structures

The point addition unit in FPGA structure. Basic numerical operations were based on previously explained parallel addition and modulo multiplication in Krestenson's bases. A schematic of its structure is depicted in Fig.1.

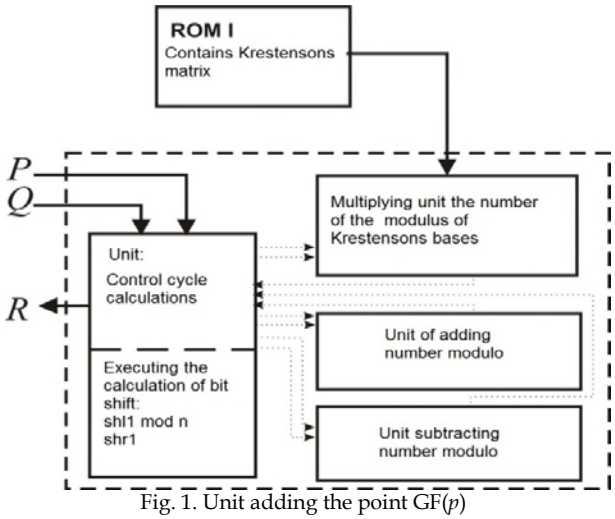

Fig. 1. Unit adding the point GF(*p*)

The point addition unit was tested on FPGA Stratix III EP3SL150F1152I4SL system. Generating results and synthesis allowed clock frequency as high as 44 MHz. Table 2 shows speed results for the addition unit for curves of various sizes.

Table 2

Speed of point GF(p) addition by adder in FPGA

GF(*p*)	Number addition / s
69	319444,4
92	234042,6
115	185344,8
138	148550,7
161	125000
184	107142,9

Such addition unit was used for encryption by the ElGamal algorithm with the use of a public key [16]. The test shows encryption of a 1024 kB file with keys of various lengths. Table 3 shows the results. Table 4 shows results for a similar test in the same conditions except that in this case the point addition calculations were carried out in a traditional manner.

Table 3

1024 kB encryption speed of ElGamal algorithm adding curve points based on Rademacher-Krestenson's residuals

GF(*p*)	Time (s)
89	37
97	40
109	43
131	79
163	111
191	127

Table 4

1024 kB encryption speed of ElGamal exploiting standard algorithms for curve points adding

GF(*p*)	Time (s)
89	104
97	131
109	145
131	243
163	339
191	440

As we can clearly see from tables 3 and 4 implementation of Krestenson's bases addition strategy, in an adequate environment, almost doubles the encryption speed of traditional approach. Fig. 2 shows times needed to encrypt a file using keys of various length.

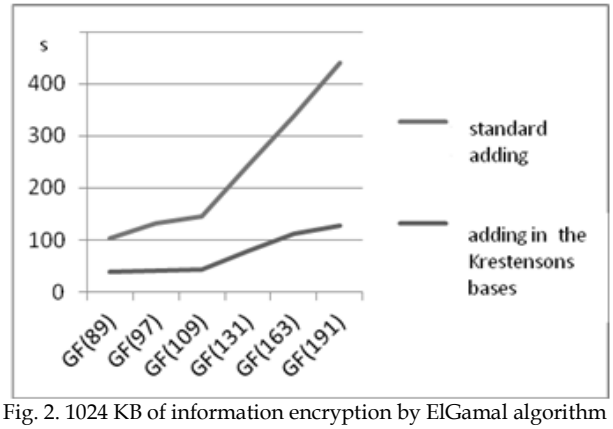

Fig. 2. 1024 KB of information encryption by ElGamal algorithm using various methods of adding points in GF(p)

5. Solving a discrete logarithm problem

Knowing the impact of Krestenson's residuals system on the efficiency of point addition process we can focus on the strength of cryptographic algorithms based on higher order fields.

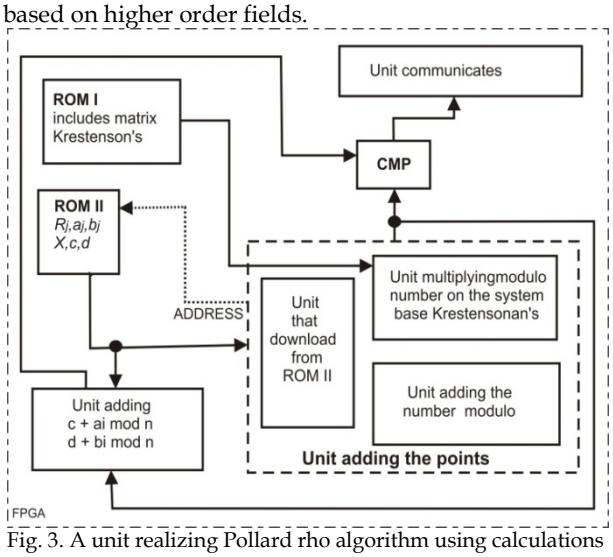

Fig. 3. A unit realizing Pollard rho algorithm using calculations based on Krestenson's bases

Schematic in Fig.3 shows a hardware model for Pollard's Rho algorithm realization in FPGA system – a process directly determining the speed of the algorithm functioning. The addition unit uses algorithms based on Rademacher–Krestenson's remaining classes.

Table 5

Number of iterations for various curves GF(p)

GF(*p*)	Iterations /s
69	321678,3
92	235294,1
115	186147,2
138	149090,9
161	125391,8
184	107438

Speed tests were carried out on Stratix III EP3SL150F1152I4SL, results and synthesis allowed clock frequency 44 MHz. Table 5 shows speed scores for hardware FPGA unit. Fig. 4 shows results of rho Pollard calculation speed tests.

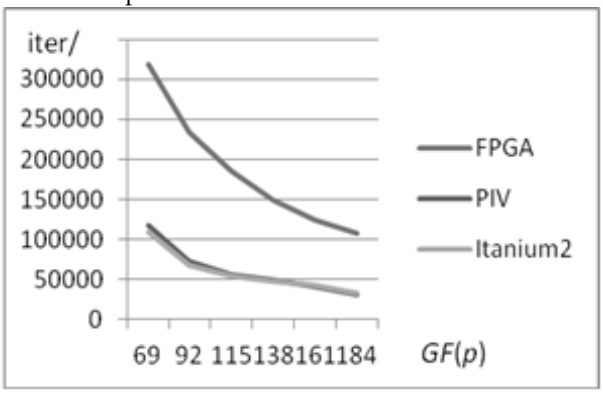

Fig. 4. Number of iterations done by Pollard's rho algorithm for various curves GF(p)

Consider the scores gathered in table 5 and the equation for average estimated solving time of a discrete logarithm by rho Pollard $\sqrt{(\pi n/2)}$ method.

Table 6

Estimated time required to find a discrete logarithm for various EC *GF*(*p*)

GF(*p*)	Time (day)
69	0,84
92	3295
115	$12*10^6$
138	$4,2*10^{10}$
161	$1,7*10^{14}$
184	$5,8*10^{17}$

Table 6 presents estimated strength of a cryptographic algorithm, determined by discrete logarithm problem solution, for curves of various sizes. The presented results refer to a single FPGA unit realizing a single random walk. A parallel rho Pollard algorithm increases the speed of finding discrete logarithm proportionally to the number of used random walks. The method relies on multiple random walks done simultaneously. The sense of this idea comes down to having many units, each realizing its own random walk and writing data into a common base. Many such units working parallel result in a linearly higher speed of finding points on random walks. A model consisting of 120 programmable FPGA units [17], described in work [18], makes up so called COPACOBANA FPGA cluster [18] which carries out parallel Pollard's Rho algorithm and generates large numbers of iterations per second – shown in table 7.

Table 7

Number of iterations for various GF(*p*) in system realizing 120 random walks

GF(*p*)	Iterations / s
69	38601398
92	28235294
115	22337662
138	17890909
161	15047022
184	12892562

Table 8 shows the strength of cryptographic algorithm with 120 random walks.

Table 8

Estimated time required to find a discrete logarithm for different GF(*p*) using 120 units

GF(p)	Time (day)
GF(69)	0,007
GF(92)	27
GF(115)	100790
GF(138)	$3,5*10^8$
GF(161)	$1,4*10^{12}$
GF(184)	$4,9*10^{15}$

6. Conclusion

The article comprises an analysis of the force of a cryptographic algorithm as well as functional security of cryptographic systems based on *GF(p)*. Implementation of calculations relying on Krestenson's bases and parallel addition resulted in two times higher throughput with the use ElGamala method. Fast addition algorithms allow us to test and verify the safety of ECCD. Functional safety and survivability of ICSEC based algorithm were tested with the use of previously described methods. The proposed system realizing

calculations on ECs and taking advantage of Krestenson's bases may reach even three times faster random walk realization for certain curves. As it has already been discussed, the force of a cryptographic algorithm is 27 days for elliptic curve *GF*(92) and $3{,}8*10^9$ years for *GF*(160) elliptic curve. The strength is calculated using a cryptoanalysis system based on 120 FPGA units. There are other efficient methods for increasing performance of implementation of elliptic curve cryptography, which are scheduled to be carried out in the future.

References

[1] J. Chen, Y. Wang, X. Wang. On-Demand Security Architecture for Cloud Computing // Computer. – 2012. – Vol. 45, No 7. – P. 73-78. – ISSN 0018-9162.

[2] N.G. Leveson. Safeware: System Safety and Computers // Reading, Massachusetts: Addison-Wesley, 1995. – 680 p.

[3] V.S. Kharchenko. Analysis of the problems of safeware engineering: the project TEMPUS-SAFEGUARD // Radioelectronic and Computer Systems. – 2010. – No (48). – P. 297-300. (in Ukrainian)

[4] M. Karpinski. Information Security // Warsaw: Measurements, Automation and Monitoring. – 2012. – 280 p. – ISBN 978-83-930505-3-6. (in Polish)

[5] R.L. Lagendijk, Z. Erkin, M. Barni. Encrypted Signal Processing for Privacy Protection // IEEE Signal Processing Magazine. – 2013. – Vol. 30, No 1. – P. 82-105.– ISSN 1053-5888.

[6] R. Oppliger. Security and Privacy in an Online World // Computer. – 2011. – Vol. 44, No 9. – P. 21-22. – ISSN 0018-9162.

[7] D. Hankerson, A. Menezes, S. Vanstone. Guide to elliptic curve cryptography // NY: Springer, 2004. – 332 p.

[8] Bakhmach E.T., Herasimenko A.D., Golovir V.A. et al. Fail-safe information control systems on programmable logic / Kharchenko V.S., Sklyar V.V. (eds). – Kharkiv: National Aerospace University "KhAI"; Kirovohrad: RPC "Radiy". – 2008. – 380 p. (in Russian)

[9] V.O. Romankevych, M.S.Milad, S.O. Poleschuk . Functional safety evaluation for the reconfigurable fault-tolerant multiprocessor control systems // Applied Mathematics and Computing – AMC-2011: III Scientific Conference, April 13-15, 2011. – P. 157-161. (in Ukrainian)

[10] I. Ahmed, S. Obermeier, M. Naedele, G.G. Richard. SCADA Systems: Challenges for Forensic Investigators // Computer. – 2012. – Vol. 45, No 12. – P. 73-78. – ISSN 0018-9162.

[11] M.A. Yastrebenetsky, V.N. Vasilchenko, S.V. Vinogradska et al. Nuclear Power Plants Safety: Instrumentation and Control Systems / Yastrebenetsky M.A. (ed.). – Kiev: Technika. – 2004. ¬ 472 p. (in Russian) (Translated in English in 2007 by US Nuclear Regulatory Commission).

[12] I. Blade I., G. Seroussi, N. Smart. Krzywe eliptyczne w kryptografii // Warszawa: TAO. – 2004. – 234 p.

[13] I. Yakymenko, M. Kasyanchuk, Y. Nykolajchuk. Matrix algorithms of processing of the information flow in computer systems based on theoretical and numerical Krestenson's basis // TCSET'2010, February 23-27, 2010, Lviv-Slavske, Ukraine. – P. 241.

[14] P.C. Oorschot, M.J. Wiener. Parallel collision search with cryptanalytic applications // Journal of Cryptology. – 1999. – No 12. – P. 1-28.

[15] A.H. Makoha, B.U. Zuj. [Electronic resource] : The arithmetic of large integers in parallel computer systems // 20.03.2007. – http://revolution.allbest.ru /mathematics /00011260_0.html (in Russian)

[16] O. Ugus, A. Hessler, D. Westhoff. [Electronic resource] : Performance of Additive Homomorphic EC-ElGamal Encryption for TinyPEDS, Technical Report, 6 // Fachgespräch "Drahtlose Sensornetze", July 2007. – http://www.ist-ubisecsens.org/publications/ EcElgamal- UgHesWest.pdf

[17] T. Guneysu, Ch. Paar, L. Pelzl. [Electronic resource]: On the Security of Elliptic Curve Cryptosystems against Attacks with Special-Purpose Hardware // SHARCS'06, 2006. – http://www.hyperelliptic.org/tanja/SHARCS/talks06/ ecc_rub.pdf

[18] T. Guneysu, G. Pfeiffer, C. Paar, M. Schimmler. Three years of evolution cryptanalysis with copacobana [Electronic resource] // SHARCS '09, 2009. http://www.hyperelliptic.org/tanja/SHARCS/ record2.

UDC 519.718 : 539.3 (045)

Александер М.А., Карпінський М.П., Літава Г.К. Функціональна безпека та живучість інформаційно-укравляючих систем на основі еліптичних кривих: моделі і методи

Анотація. *Наведено аналіз функціональної безпеки та живучості інформаційно-керуючих систем, в засобах яких застосовуються обчислення на еліптичних кривих. Оцінено час, необхідний для знаходження дискретного логарифма еліптичної кривої над полем GF (p). Висвітлено аспекти застосування пристроїв ПКВМ, в яких обчислення ґрунтуються на використанні системи залишкових класів Радемахера-Крестенсона і паралельного сумування.*

Ключові слова: *інформаційно-управляюча система, еліптична крива, функціональна безпека, живучість, система залишкових класів Радемахера-Крестенсона.*

Александер М.А., Карпинский Н.П., Литава Г.К. Функциональная безопасность и живучесть информационно-управляющих систем на основе эллиптических кривых: модели и методы

Аннотация. *Приведен анализ функциональной безопасности и живучести информационно-управляющих систем, в средствах которых применяются вычисления на эллиптических кривых. Оценено время, необходимое для нахождения*

дискретного логарифма эллиптической кривой над полем GF(p). Освещены аспекты применения устройств ППВМ, в которых вычисления основаны на использовании системы остаточных классов Радемахера-Крестенсона и параллельного суммирования.
Ключевые слова: *информационно-управляющая система, эллиптическая кривая, функциональная безопасность, живучесть, система остаточных классов Радемахера-Крестенсона.*

Отримано *28 січня 2013 року*, затверджено редколегією *4 березня 2013 року*

КЛАСИФІКАЦІЯ ТРИРОЗРЯДНИХ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ДЛЯ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Віра Бабенко[1], Ольга Мельник[2], Руслан Мельник[2]

[1] Одеська національна академія зв'язку ім. О.С. Попова, Україна
[2]Академія пожежної безпеки імені Героїв Чорнобиля, Україна

БАБЕНКО Віра Григорівна, к.т.н.

Рік та місце народження: 1984 рік, м. Золотоноша, Черкаська область, Україна.
Освіта: Черкаський державний технологічний університет, 2006 рік.
Посада: докторант Одеської національної академії зв'язку ім. О.С. Попова з 2011 року.
Наукові інтереси: криптографічні методи захисту інформації.
Публікації: більше 40 наукових публікацій, серед яких монографії, навчально-методичні розробки, навчальні посібники, наукові статті.
E-mail: zolot_verba@rambler.ru

МЕЛЬНИК Ольга Григорівна, к.т.н.

Рік та місце народження: 1987 рік, м. Черкаси, Україна.
Освіта: Академія пожежної безпеки імені Героїв Чорнобиля, 2009 рік; Черкаський національний університет імені Богдана Хмельницького, 2010 рік.
Посада: доцент кафедри будівельних конструкцій з 2012 року.
Наукові інтереси: методи та засоби побудови комп'ютеризованих систем прогнозування, розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного перетворення.
Публікації: більше 30 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: melnyk_olja_2012@mail.ru

МЕЛЬНИК Руслан Павлович

Рік та місце народження: 1987 рік, м. Ульяновка, Кіровоградська область, Україна.
Освіта: Академія пожежної безпеки імені Героїв Чорнобиля, 2009 рік.
Посада: ад'юнкт з 2010 року.
Наукові інтереси: розробка математичних методів захисту інформації та алгоритмів їх реалізації на основі операцій криптографічного перетворення.
Публікації: більше 15 наукових публікацій.
E-mail: indigo211212@gmail.com

Анотація. *У даній статті представлено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації в залежності від складності елементарних функцій та способу перетворення інформації елементарними функціями кожної групи.*

Ключові слова: *трирозрядні елементарні функції, матричні операції, розширені матричні операції, схема реалізації.*