UDC 621.382-022.532(045)
DOI:10.18372/1990-5548.77.17960

[1]O. S. Melnyk,
[2]V. O. Kozarevych

AUTOMATED SIMULATION ENCRYPTION NANODEVICES

[1,2]Department of Electronics, Robotics, Monitoring & IoT Technologies
National Aviation University, Kyiv, Ukraine
E-mails: [1]oleksandr.melnyk@npp.nau.edu.ua, ORCID 0000-0003-1072-5526,
[2]viktoriia.kozarevych@npp.nau.edu.ua, ORCID 0000-0002-4380-0927

Abstract*—This article implements the method of automated simulation and design of new non-radiating nanoelectronic encryption modules. Currently, cryptographic equipment is practically not protected from electromagnetic attacks and information decryption, as it is created according to outdated complementary metal-oxide-semiconductor microtechnology. To increase the error-free operation of encryption devices, the article uses a system of automated design of nanodevices based on quantum cellular automata using majoritarian principles of their operation. Automated simulation proved that the consuption of the nanodevices developed in the work does not exceed $3{,}8\times10^{-23}$ J. Therefore, unmanned aerial vehicles equipped with the nanodevices developed in the article are completely protected from electromagnetic attacks. The results of automated modeling and verification using a computer design system QCADesigne fully confirmed the effectiveness of introducing single-electron nanodevices into encryption devices of unmanned systems. The proposed logic takes advantage of low power consumption quantum-dot cellular automata together with complicated clocking circuits as a paradigm of nanotechnology advances in encryption engineering.*

Index Terms—Quantum-dots cellular automata; majority gate; D-type flip-flop; shift nanoregister.

I. INTRODUCTION

Power analysis attacks were introduced in [1], [6] – [8], [10]. In fact, power and electromagnetic (EM) side-channels are the most important ones for implementation of block ciphers. The power consumption as well as the EM field surrounding a encryption module may leak a significant amount of information about the private key. The power consumption as well as the EM field that is caused by the current flowing in a cryptographic circuit implemented in complementary metal–oxide–semiconductor (CMOS) leak information about the private key [1]. This current is mainly caused by the charging or discharging of the capacitances of interconnected wires.

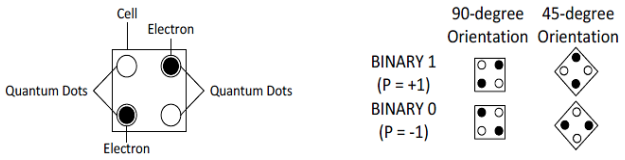
II. BASES OF QUANTUM CELLULAR AUTOMATA

Quantum-dot cellular automata (QCA) devices consist of a dielectric cell (20x20) nm with four quantum semiconductor dots 5 nm, located in the corners, and two mobile electrons. Their position is only dependent on a finite set of cell-values in the vicinity of defined cell [2], [9]. An isolated cell provides tunneling junctions with the potential barriers. They are controlled by local electric fields that are raised to prohibit electron movement and lowered to allow electron movement. Consequently, an isolated cell can have one of three states. A null state occurs when the barrier is lowered and the mobile electrons are free to localize on any dot. The other two states are polarizations that occur when the barrier is raised, and serve to minimize the energy state of the cell. Probability of cell is in one of polarization state can be correlated with charge density of each quantum dot, and can be found with the help of formula:

$$P = \frac{(\rho_1 + \rho_3) - (\rho_2 + \rho_4)}{(\rho_1 + \rho_3) + (\rho_2 + \rho_4)} = \pm 1,$$

where ρ_i is the electric charge density of each quantum dot of the cell.

Figure 1 shows basic QCA cell, its two possible orientations and polarization of electrons.



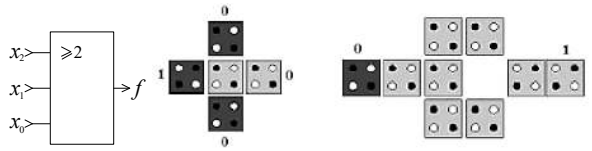
a) b)

Fig. 1. A cell of a quantum automata (a), its two ways of placement in space (b) and polarization ($P = \pm 1$)

Placing cells next to each other in a line and allowing them to interact we can provide flowing of a data down such wire. There are two methods of wire construction in dependence on 45 degree or 90 degree cell orientation theoretically, bun on practice it is difficult to manufactured nano-cells with different orientation [3].

Different gates can be constructed with QCA to compute various logic and arithmetic functions. The

basic logic gates in QCA are the majority gate (a) and inverter (b) on Fig. 2.



a) b)

Fig. 2. Majority gate (a) and inverter (b) in QCA

The output cell will polarized to the majority of polarization of input cells. The Boolean expression for majority function with inputs x_2, x_1 and x_0 is $f = maj(x_2, x_1, x_0) = x_2x_1 \vee x_2x_0 \vee x_1x_0$.

By fixing the polarization of any one input of the majority gate as logic 0 or logic 1, we obtain AND gate or an OR gate respectively:

$$f_{AND} = \text{maj}(x_2, x_1, 0) = x_2x_1,$$

$$f_{OR} = \text{maj}(x_2, x_1, 1) = x_2 \vee x_1.$$

Creation of a fixed cell can be done within manufactured process and constant signals do not need to be routed within the circuit

III. Energetic Attacks and Countermeasures

A power consumption (e.g. the side channel) of a encryption module depends on many parameters. Only one of them is the private key. However, the fact that the side-channel output depends on the private key is often sufficient to reveal it. In order to exploit this dependency between the side-channel output and the private key, an attacker usually builds a model of the side channel. This model is typically not very complex. In fact, attacks conducted in practice have shown that very simple models are often sufficient to reveal the private key. Figure 3 depicts the principles of a side-channel attack [2]. On the left side, the figure shows the physical device that is attacked. Its side-channel output is determined by the private key, the input and the output of the device and by many other parameters. Some of them are known by the attacker, while others are not. The model of the side channel used by the attacker is shown on the right side in Fig. 3. The model may consider additional parameters besides the key, the input and the output of the module. However there is always a certain imperfectness of the model.

Several countermeasures to power and EM attacks have been proposed so far; however, each technique may lead to design complexity, more power consumption, size and speed issues of the entire encryption modules. All these strategies can be categorized in two groups: namely, they either try to randomize the intermediate result or take advantage of circuits with data and power consumption independency. These techniques can be implemented in architecture, logic, and algorithm or protocol level. The QCA circuits we introduce in this work takes advantage of QCA technology with low power consumption and data independency together with complicated clocking scheme that makes it very difficult to make power consumption models for encryption engineering implemented in QCA logic.

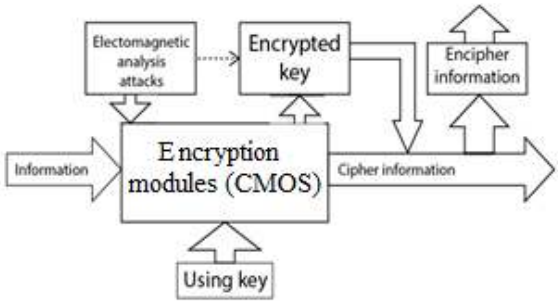


Fig. 3. Principles of energetic attacks

IV. Encryption Sequential QCA Circuits

Although we can always get similar functionality of sequential logic from a QCA wire segment spread across several clocking zones, i.e. a basic wire implements the master-slave-type data storage, based on neighboring clocking zones acting as flip-flop stages, to make a more secure logic style we added an additional logic signal “clock”. To describe the consequent sequential logic we introduce a QCA D-Type flip-flop in this part. The structure of a D-type latch [4] has been shown in Fig. 4.

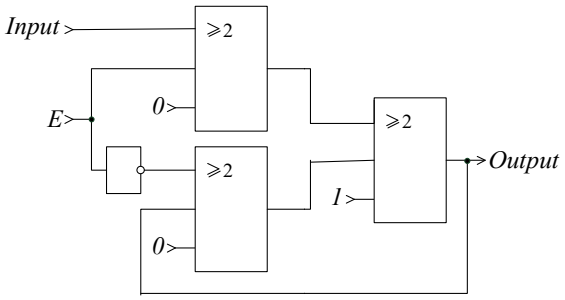


Fig. 4. Structure of a D-latch

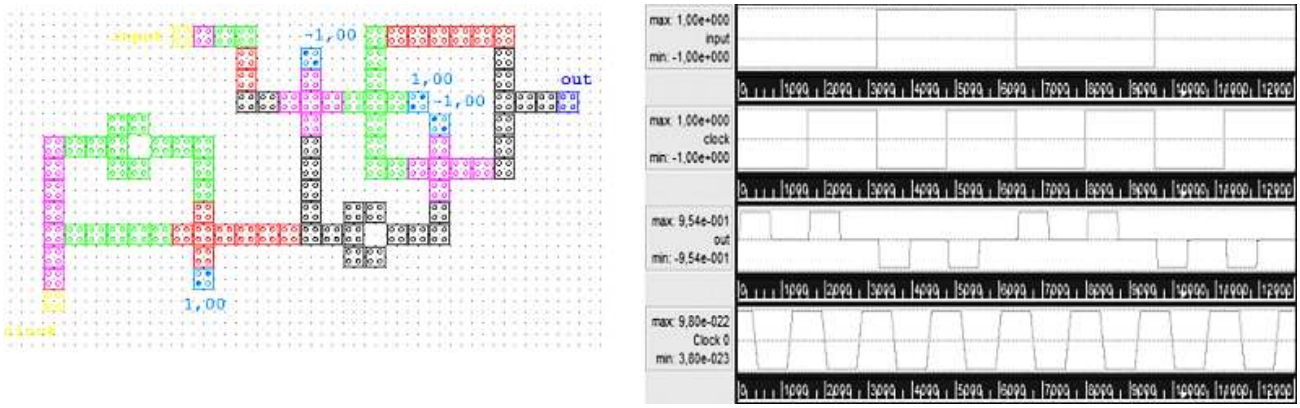
The large area of the circuit and the limitation in the length of QCA wires are main issues when implementing and fabricating circuits in QCA technology. By taking advantage of a level to edge converter, it is possible to improve the D-type QCA flip-flop. The level to edge converter exploits the intrinsic stages of clocking and zones in QCA. The converter consists of an AND gate and an inverter. The original signal is multiplicated with its inverted

delayed copy. The result is generation of short pulses at the rising edge of the original signal. The D-type nanoflip-flop implemented with this technique has been shown in Fig. 5a. Logic equation in the bulean majority bases D-type flip-flop for states Q_t and Q_{t-1} are as follows:

$$Q_t = CD \vee \bar{C}Q_{t-1},$$

$$Q_t = \text{maj}\big(\text{maj}(C, D, -1), \text{maj}(\bar{C}, Q_{t-1}, -1), 1\big),$$

where C and D are pulse synchronization codes and encryption information.



a) b)

Fig. 5. QCA D-type flip-flop (a) and simulation of waveforms (b)

The simulation results obtained with QCA Designer [3] verifies the functionality of the proposed D-type nanoflip-flop (Fig. 5b).

Register is a cascade of flip-flops integrating the same controlling circuits that is used for data receiving, processing and transmitting of encryption information.

Serial register is used often to transform parallel type code to serial and on the contrary. Using serial code in cryptography is caused by need to transmit big amounts of binary information through the limited number of connecting lines. The big quantity of connective conductors is necessary for the parallel transfer of digits. Transmitting encryption codes in a serial way, bit by bit, on the one conductor, allows reducing sizes of connecting lines.

The circuit of a serial (shift) register, that is built on D-type flip-flops, allows performing the transformation serial type encryption code to parallel show of Fig. 6.

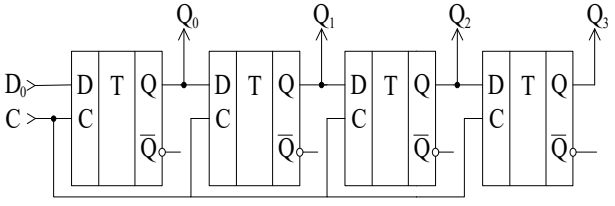


Fig. 6. Serial D-type flip-flop register

V. Results and Disscution

Logic Boolean and majority equations of serial nanoregister with the right shift state on D-type flip-flop are as follow:

$$Q_0 \to Q_1 \to Q_2 \to Q_3,$$

$$Q_0 = CD \vee \bar{C}D, (CQ_0 \vee \bar{C}Q_0) \to Q_1 \text{ and so on;}$$

$$Q_0 = \text{maj}\big(\text{maj}\big(C, D, 0\big), \text{maj}\big(\bar{C}, D, 0\big), 1\big),$$

$$Q_1 = \text{maj}\big(\text{maj}\big(C, Q_0, 0\big), \text{maj}\big(\bar{C}, Q_0, 0\big)1\big) \to Q_2$$

and so on.

The states of all outputs for shift register show in Table I.

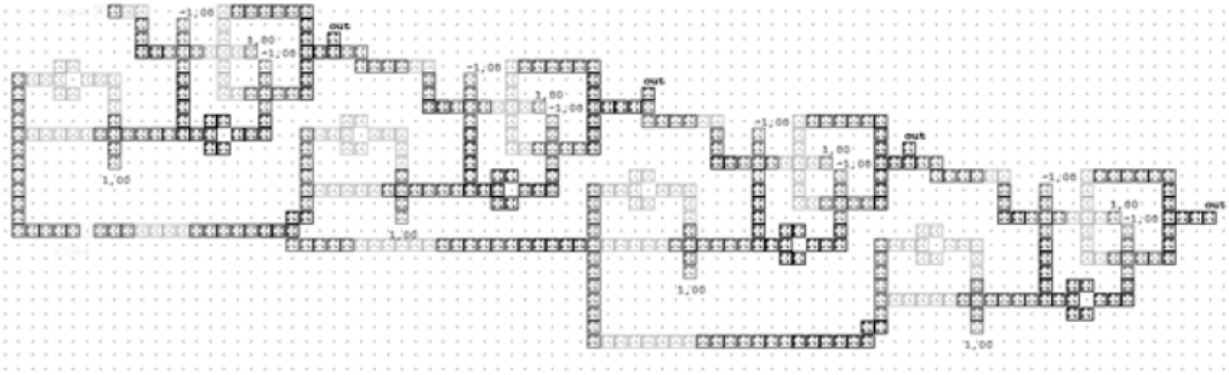
Table I. Truth Table for Four Outputs Nanoregister

n	D	Q_0	Q_1	Q_2	Q_3
0	0	0	0	0	0
1	1	0	1	0	0
2	0	1	0	1	0
3	1	0	0	0	1

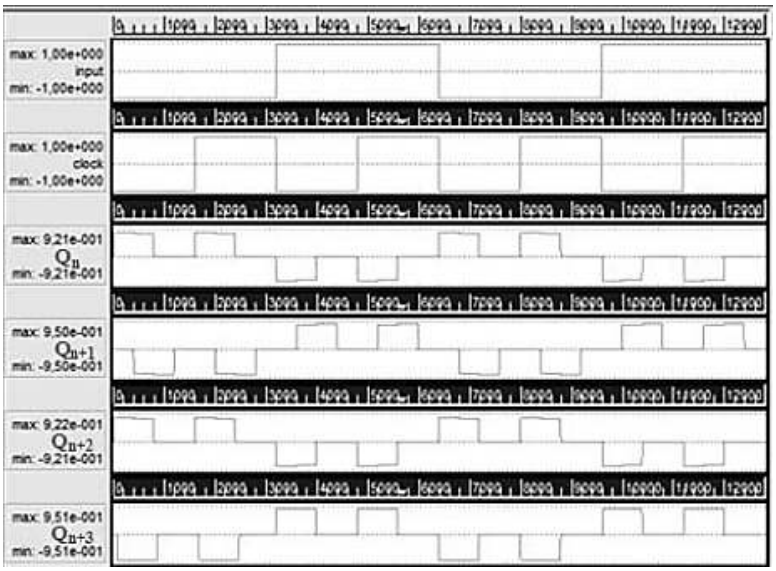
Nanocircuit of this register is showed on Fig. 7, and is designed on a tablet field QCA Designer, as well as results of modeling of corresponding time response waveforms.

Positive pulses of logic “1” are corresponded by positive polarizations + P = 1, and negative pulses of logic “0” – by negative polarizations – P = 0 respectively.

The simulated layout is based in QCA cell sized (20x20) nm, with 4 quantum dots each having a diameter of 5 nm, and the distance between the center of cells being 20 nm. The dimensions of the full multiplier design are (500x1760) nm and total number of cells in 466. The energie consumption of on clock period form from $3.8\text{x}10^{-23}J$ to $9.8\text{x}10^{-22}J$ (Fig. 5b).



a)



b)

Fig. 7. Shift register on 4 D-type flip-flops (a) and QCADesigner simulation results (b)

For a reduced area on the crystal, another D-type flip-flop format is proposed, the nanocircuit of which is shown in Fig. 8a. In Figure 8b shows the waveforms of operation, which completely coincide with the diagrams of the previous, complicated D-type flip-flop circuit in Fig. 5.

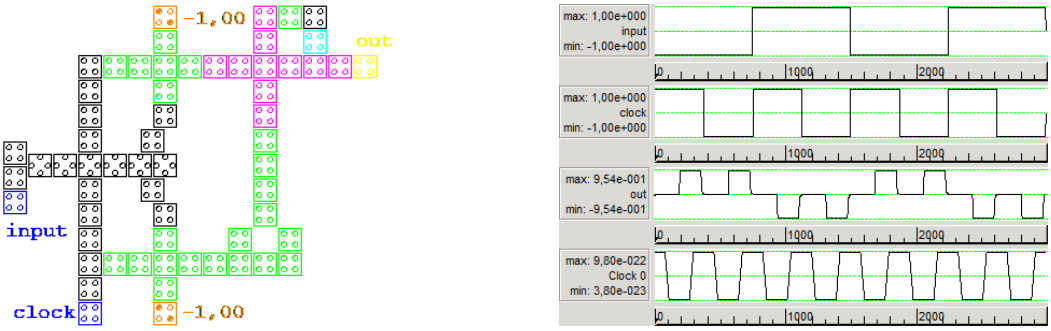
The states of all outputs for shift register show in Table II.

Nanocircuit of this register is showed on Fig. 8, and is designed on a tablet field QCADesigner, as well as results of modeling of corresponding time response waveforms. Positive pulses of logic "1" are corresponded by positive polarizations + P = 1, and negative pulses of logic "0" – by negative polarizations – P = 0 respectively.

TABLE II. TRUTH TABLE FOR FIVE OUTPUTS NANOREGISTER

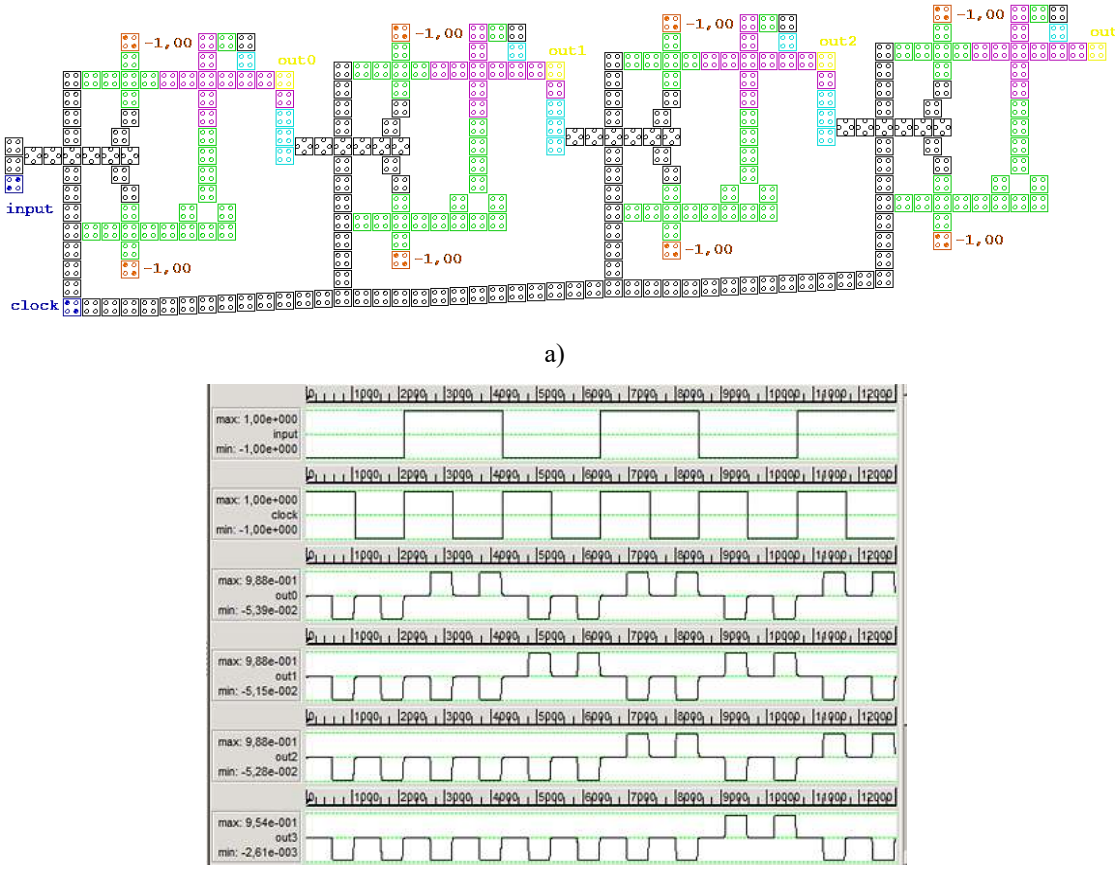
n	D	Q_0	Q_1	Q_2	Q_3
0	0	0	0	0	0
1	1	1	0	0	0
2	0	0	1	0	0
3	1	1	0	1	0
4	0	0	1	0	1

In Figure 9a and on the QCAD simulation tablet, a circuit of an encryption nanoregister is built, which occupies a 27% smaller area on a 410x1170 nm crystal, and the number of quantum automata is reduced from 466 to 318. The results of automated simulation of time diagrams (Fig. 7b), obviously, coincide.



a) b)

Fig. 8. QCA D-type nanoflip-flop (*a*) and simulation of waveforms (*b*)



a)

b)

Fig. 9. Shift nanoregister on 4 D-type flip-flops (a) and QCADesigner simulation results (b)

V. Conclusions

Energetic attacks seriously threaten encryption modules as they can be implemented with relatively inexpensive equipment's. In this work, a new approach to implementation of quantum encryption modules via QCA technology has been presented. Majority logic style was introduced through design of a D-type flip-flop with additional 'clock' signal as a result of nanotechnology advances in developing novel countermeasures and designing more secure cryptography shift register.

References

[1] E. Ramini, S. M. Nejad. *Secure clocked QCA logic for implementation of cryptographic processors*. 2009 applies Electronics, Pilsen 9-10. September, 2009.

[2] C. S. Lent and P. D. Tougaw, "A Device architecture for computing with quantum dots", *Proc. of the IEEE*, 1997. https://doi.org/10.1109/5.573740

[3] K. Walus, *QCADesiner: A CAD Tool for an Emerging Nano-Technology*, Micronet Annual Workshop, 2003.

[4] N. I. Pakulov, V. F. Ukhanov, and P. N. Chernyshov, *Mazhoritarnyy printsip postroyeniya nadezhnykh uzlov i ustroystv TSVM*, Moskva: Sov. radio, 1974, 184 p. [in Russian]

[5] V. A. Luzhetskyi and O. V. Dmytryshyn, "Alternative modes of block encryption," *Scientific works of VNTU*, no. 1, pp. 1–9, 2011. [in Ukraine].

[6] E. Brier, Th. Peyrin and J. Stern, *BPS: a format-preserving encryption proposal*, 11 p. Resource access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/bps/bps-spec.pdf.

[7] M. Bellare, Ph. Rogaway and T. Spies, "The FFX Mode of Operation for Format-Preserving Encryption," Draft 1.1. February 20, 2010, 18 p. Resource access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM documents/proposedmodes/ffx/ffx-spec.pdf.

[8] O. V. Dmytryshyn and V. A. Luzhetskyi, "The mode of controlled coupling of encrypted text blocks," *Visnyk VPI*, Vinnytsia, Vinnytsia National University Publishing House, no. 1, pp. 34–36, 2009. [in Ukraine].

[9] V. A. Luzhetskyi and O. V. Dmytryshyn, "Procedures for developing keys for block ciphers based on arithmetic operations by modulo," *Information technologies and computer engineering*, Vinnytsia, Vinnytsia National University Publishing House, no. 2, pp. 69–74, 2009. [in Ukraine].

[10] I. D. Gorbenko, G. M. Gulak and others, "Analysis of the properties of block symmetric encryption algorithms (based on the results of the international NESIE project)," *Radiotechnique: Vseukr. interdisciplinary scientific and technical Sat.*, Kharkiv: KHNURE, no. 141, pp. 7–24, 2005. [in Ukraine].

Received May 14, 2023

Melnyk Oleksandr. ORCID 0000-0003-1072-5526. Candidate of Sciences (Engineering). Associated Professor.
Department of Electronics, Robotics, Monitoring & IoT Technologies, National Aviation University, Kyiv, Ukraine.
Education: Kyiv Polytechnic Institute, Kyiv, Ukraine, (1971).
Research interests: Modeling micro- and nanoelectronics devices, computer-aided designe, solid-states electronics.
Publications: more than 170 papers.
E-mail: oleksandr.melnyk@npp.nau.edu.ua

Kozarevych Viktoriia. ORCID 0000-0002-4380-0927. Senior Lecturer.
Department of Electronics, Robotics, Monitoring & IoT Technologies, National Aviation University, Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine, (2007).
Research interests: Computer-aided design, single-electron circuits, solid-states electronics.
Publications: 34.
E-mail: viktoriia.kozarevych@npp.nau.edu.ua

О. С. Мельник, В. О. Козаревич. Автоматизоване моделювання шифрувальних нанопристроїв

У статті реалізовано метод автоматизованого моделювання та проектування нових невипромінюючих наноелектронних шифрувальних модулів. Наразі криптографічне обладнання практично не захищене від електромагнітних атак і дешифрування інформації, оскільки створене по застарілій комплементарній мікротехнології метал-окисел-напівпровідник. Для підвищення безвідмовної роботи шифрувальних пристроїв в статті використана система автоматизованого проектування нанопристроїв на базі квантових коміркових автоматів з використанням мажоритарних принципів їх функціонування. Автоматизоване моделювання довело, що енергія випромінювання розроблених нанопристроїв не перевищує $3{,}8\times10^{-23}$ Дж. Тому безпілотні апарати, обладнані розробленими нанопристроями, повністю захищені від електромагнітних атак. Результати автоматизованого моделювання та верифікації за допомогою системи комп'ютерного проектування QCADesigne повністю підтвердили ефективність запровадження одноелектронних нанопристроїв в криптографічні пристрої безпілотних комплексів. В роботі досліджено можливість запровадження невипромінюючих наносхем на базі квантових коміркових автоматів, що практично нейтралізує електромагнітні атаки.

Ключові слова: квантовий комірковий автомат; мажоритарний елемент; D-тригер; нанорегістр зсуву.

Мельник Олександр Степанович. ORCID 0000-0003-1072-5526. Кандидат технічних наук. Доцент.
Кафедра електроніки, робототехніки, моніторингу та технологій Інтернету речей, Національний авіаційний університет, Київ, Україна.
Освіта: Київський політехнічний інститут, Київ, Україна, (1971).
Напрям наукової діяльності: моделювання пристроїв мікро- та наноелектроніки, автоматизоване проектування, твердотільна електроніка.
Кількість публікацій: більше 170 наукових робіт.
E-mail: oleksandr.melnyk@npp.nau.edu.ua

Козаревич Вікторія Олександрівна. ORCID 0000-0002-4380-0927. Старший викладач.
Кафедра електроніки, робототехніки, моніторингу та технологій Інтернету речей, Національний авіаційний університет, Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна, (2007).
Напрям наукової діяльності: системи автоматизованого проектування, одноелектронні схеми, твердотільна електроніка.
Кількість публікацій: 34.
E-mail: viktoriia.kozarevych@npp.nau.edu.ua