UDC 621.382.3(045)
DOI:10.18372/1990-5548.67.15607

[1]O. S. Melnyk,
[2]A. M. Mykolushko,
[3]A. O. Myshynskyi

NANOCIRCUITS FOR PROTECTION OF THE CIPHER INFORMATION

Faculty of Air Navigation, Electronics & Telecommunications, Nation Aviation University, Kyiv, Ukraine
E-mails: [1]melnyk.olexa@nau.edu.ua ORCID 0000-0003-1072-5526,
[2]andrii.mykolushko@npp.nau.edu.ua ORCID 0000-0002-2767-8255, [3]cyber-shot0@ukr.net

***Abstract*—*While using side-channel attacks, cipher devices was defenseless to power and electromagnetic analysis attacks. These attacks are due to the use of low cost equipment. Currently, most of the cipher circuits are implemented on complementary metal-oxide-semiconductor. The disadvantage is the relationship between the data processing the curcuit to energy consumption. When processing the CMOS transistor logic "1" and the logic "0", through the transistor passes a different volume of current. If don't implement significant counteractions, it will allow another person to decrypt the key of the cipher module. A new logical approach to quantum-dot cellular automata and single-electron transistors is explored. The proposed approach has low power consumption and complicated clocking circuits. In theory and practice of cipher protection one of the key problems is the formation of binary pseudorandom sequences of maximum length of acceptable statistical characteristics. Generators of pseudorandom sequences usually based on linear shift registers with linear feedback. Here expanded the concept of linear shift register, believing that his every category (memory cell) can be in one of the states. Call registers are "generalized linear shift registers".*

Index Terms—Quantum cellular automata; majority gate; single-electron transistors.

I. INTRODUCTION

An example of the analysis attacks [1] is shown in the scheme in Fig. 1. An integral part when constructing block ciphers is power and electromagnetic (EM) side-channels. But energy consumption and EM fields provide almost free access to a large amount of information about the encrypted key. These losses are caused by the current flowing in a cipher circuit. This current is caused by charging or discharging capacitors in CMOS transistors and interconnected wires. The greatest use of Quantum Automata is found in majority gates.

II. PROBLEM STATEMENT

The Quantum-dot Cellular Automata (QCA) devices contain dielectric cells (20x20) nm. Each cell consists of four semiconductor quantum dots of 5 nm in size. Four such points are rosettes in the corners of the cell, which contain two electrons. Their position depends only on a finite set of cell values in the neighborhood of a particular cell [2]. Tunnel connections with potential barriers provides by the isolated cells. Local electric fields control the isolated cells. The fields descend to allow the movement of electrons and rise to prohibit it. Isolated cells can be found in two constituents. Electrons can freely localize at any point in the lower threshold barrier. The emergence of other polarization states is due to an increase in the potential barrier and is required to minimize the energy state of the cell. Charge density of each quantum dots correlate the possibility of a cell in one of the polar state. For calculating of itwe can using the formula:

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

where ρ is charge density every quantum dot of cell.

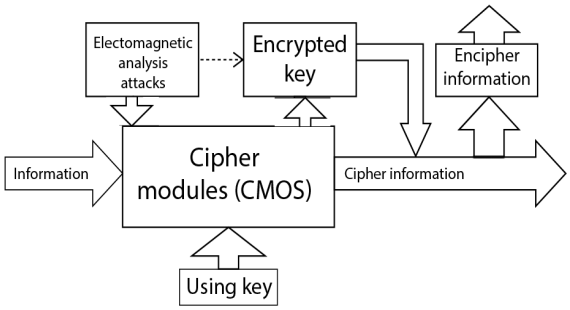


Fig. 1. Principles of side-channel attacks

For data flowing we must place cells close to each others. The allowing of data flowing performed at two cases (45 degree or 90 degree) (Fig. 2), but on practice it is difficult to manufactured nano-cells with different orientation [3]. For build a variouslogic and arithmetic functions must be

constructed a different majority gates. The basic logic gates in QCA are the majority gate (a) and inverter (b) on Fig. 3.

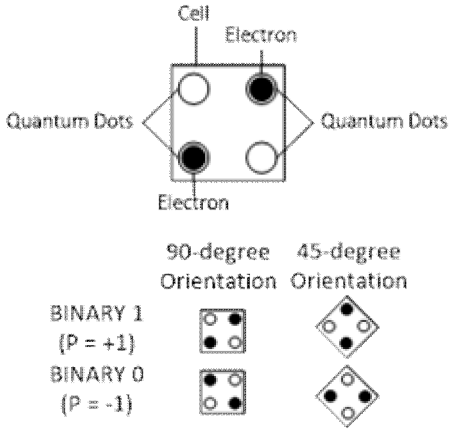
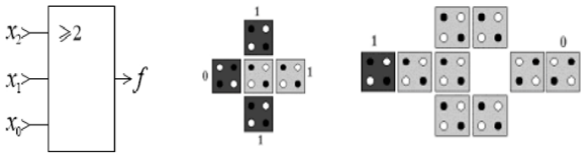


Fig. 2. A single QCA cell and its two possible orientations and polarization ($P = \pm 1$)



a) b)

Fig. 3. 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:

$$f = \text{maj}(x_2, x_1, x_0) = x_2x_1 \vee x_2x_0 \vee x_1x_0. \quad (2)$$

By setting of the polarization any one of the majority gate as logic 1/0, we obtain OR/AND gate respectively:

$$f_{OR} = \text{maj}(x_2, x_1, 1) = x_2 \vee x_1. \quad (3)$$

The quantum-dot cellular automata and single-electron transistors (SET) circuits we introduce in this paper utilize the benefits of low power and data-independent QCA and SET technologies along with sophisticated synchronization circuit, which complicates the creation of power models for ciper engineering implemented in QCA and SET logic.

In theory and practice of cipher protection one of the key problems is the formation of binary pseudorandom sequences of maximum length of acceptable statistical characteristics. Generators of pseudorandom sequences usually based on linear shift registers with linear feedback (Fig. 4). Here expanded the concept of linear shift register, believing that his every category (memory cell) can be in one of the states. Call registers are "generalized linear shift registers".

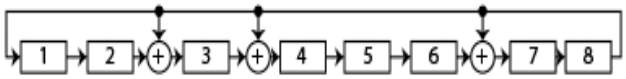


Fig. 4. The block diagram of Galois generator

In theory of Galois fields, which are the foundation of algebra noise immunity coding, cipher and building modern nanoelectronic data transmission systems, the key is the concept of irreducible polynomial of one degree variable

$$f_n(x) = \sum_{i=0}^{n} \alpha_{n-i} x^{n-i}, \alpha_i \in GF(p), \alpha_n = 1,$$

called irreducible over the field, if it does not devide on polynom of smaller degree over the field. In addition to the Galois matrices, we can also introduce Fibonacci matrices over the, which correspond to the Fibonacci shift linear register (Fig. 5).

Fig. 5. The block diagram of the Fibonacci generator

The Fibonacci matrices are mutually unambiguously connected with the Galois matrices by the operator of right-sided transposition. The general form of the Fibonacci (n–1) order matrix:

$$F_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & u_1 \\ 0 & 1 & \cdots & 0 & 0 & u_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & u_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & u_{n-1} \end{pmatrix}. \quad (4)$$

By comparing Galois and Fibonacci generators, it is possible to conclude that the Galois generators are potentially more high-speed than the Fibonacci generators. If Galois generators, the feedback signal from the last trigger enters the corresponding register digits according to the parallel transfer circuit, then in the Fibonacci generators of Fig. 5 feedback signals are successively passed through the chain of circuits XOR, which, if not take special measures.

III. Problem Solution

A. Galois configuration of shift nanoregister with linear feedback

Let consider an example of four-digit linear shift nanoregister with feedback which assignation form first and fourth grade. D-trigger and the gate of XOR (Fig. 6) is the basic elements of sequence nanoregisters with linear feedback.

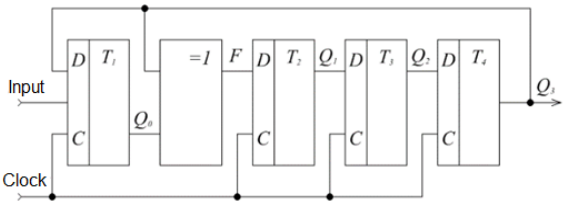


Fig. 6. Block diagram of four-digit shift nanoregister with feedback (Galois configuration)

Period of four-digit shift nanoregister with linear feedback is equal:

$$L = p^n - 1 = 2^4 - 1 = 15. \quad (5)$$

Algebraic form of binary polynomial:

$$f_4(x) = x^4 + x + 1. \quad (6)$$

Feedback function:

$$F(x) = x_4 \oplus x_1 = Q_3 \oplus Q_0. \quad (7)$$

The Table I shows the state of inputs-outputs and value of feedback function F for shift nanoregister with linear feedback.

TABLE I. STATES OF FUNCTIONS FOR GALOIS NANOREGISTER

Input	**Clock**	Q_0	F	Q_1	Q_2	Q_3
1	1	1	0	0	0	0
0	1	0	1	0	0	0
0	1	0	0	1	0	0
0	1	0	0	0	1	0
0	1	0	0	0	0	1
0	1	1	1	0	0	0
0	1	0	1	1	0	0
0	1	0	0	1	1	0
0	1	0	0	0	1	1
0	1	1	1	0	0	1
0	1	1	0	1	0	0
0	1	0	1	0	1	0
0	1	0	0	1	0	1
0	1	1	1	0	1	0
0	1	0	1	1	0	1
0	1	1	1	1	1	0

Total number of quantum cellular automata shift nanocircuits register (Fig. 7) is: 410. The dimensions of quantum cellular automata (18x18) nm. The distance between the centers of quantum cellular automata is 20 nm. The diameters of quantum islands is 5 nm. Total size of the register are: (960x610) nm.

The Figure 8 shows the results of computer simulation of all waveforms nanoregime Galois configuration, which are fully consistent with its table of signals (Table I).

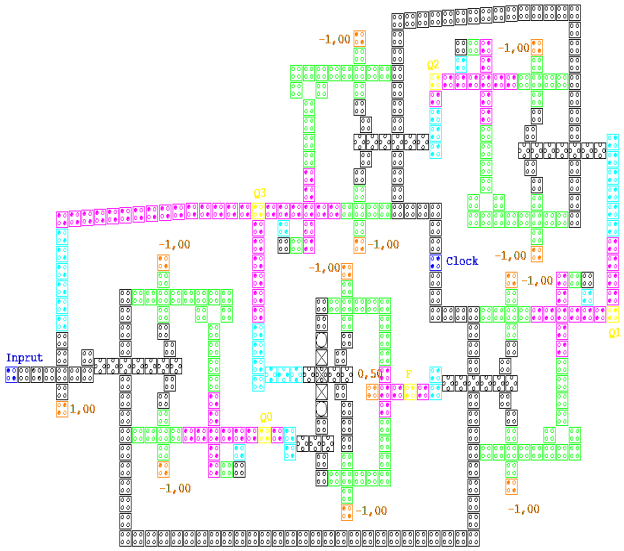


Fig. 7. Circuit of shift nanoregister Galois with linear feedback, which constructed in the environment QCADesinger [4]

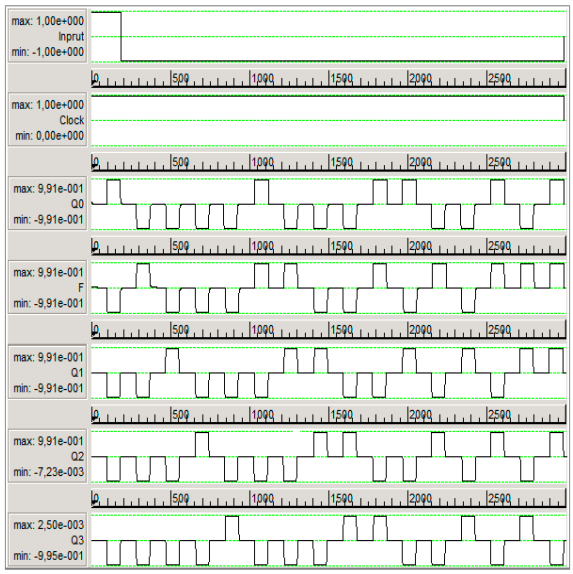


Fig. 8. Waveforms of nanoregister operation (Galois configuration)

B. Fiboncci configuration of shift nanoregister with linear feedback

Let consider a four-digit linear shift nanoregister with linear feedback with a draw from the first and fourth digits of Fig. 9.

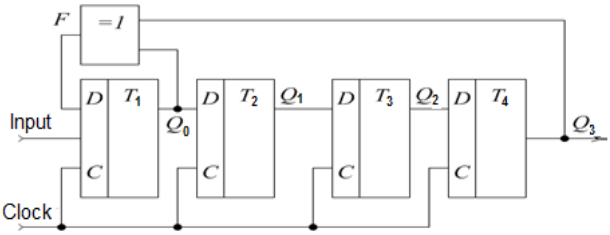


Fig. 9. Block diagram of four-digit shift nanoregister with linear feedback (Fibonacci configuration)

The total number of quantum cellular automata of the shift nanoregister (Fig. 10) is 446. The sizes of quantum cellular automata: (18x18) nm. The distance between the centers of quantum cellular automata is 20 nm. Diameters of quantum islands 5 nm. The total size of the register is: (1400x580) nm. Table II shows the status of inputs – outputs and the value of the feedback function for a four-digit nanoregister shift with Fibonacci configuration.

TABLE II. STATES OF FUNCTIONS FOR FIBONACCI NANOREGISTER

Input	Clock	$\bar{Q}_0$	$\bar{Q}_1$	$\bar{Q}_2$	$\bar{Q}_3$	F
1	1	1	0	0	0	0
0	1	0	1	0	0	1
0	1	1	0	1	0	0
0	1	0	1	0	1	1
0	1	1	0	1	0	1
0	1	1	1	0	1	1
0	1	1	1	1	0	0
0	1	0	1	1	1	1
0	1	1	0	1	1	1
0	1	1	1	0	1	0
0	1	0	1	1	0	0
0	1	0	0	1	1	0
0	1	0	0	0	1	1
0	1	1	0	0	0	1
0	1	1	1	0	0	1
0	1	1	1	1	0	1

Figure 10 shows the nanocircuit of linear shift nanoregister with the linear feedback (Fibonacci configurations) and the corresponding waveforms of it on Fig. 11, which confirm its full capacity in accordance with Table II.

The four lower waveforms of the synchronization pulses QCA-nanocircuits power supply, show that the energy consumption for one period is only from $3.8\times10^{-23}J$ to $9.8\times10^{-22}J$. This eliminates the impact of EM attacks. On Figures 12 and 13 shown results of computer designing decoder of cipher information ($4\rightarrow16$).

Single-electron nanotransistior are modern and perspective elemental base for large scale integral circuits, because they provide ultralow power consumption and up high operating frequency range (up to 10 THz) for new functional nanoelectronic devices. Such devices have one or few sub low regions of conduction, which have extremely low capacity. Due to high resulting charging energy of this area, electrical charge within it becomes quantized, this means that by creating certain electrical fields we can induce or terminate tunneling of electrons in quantum dots or otherwise. Such effect, that been called Coulomb blockade, has been used for managing extra low streams of electrons trough out SET (Fig. 14).

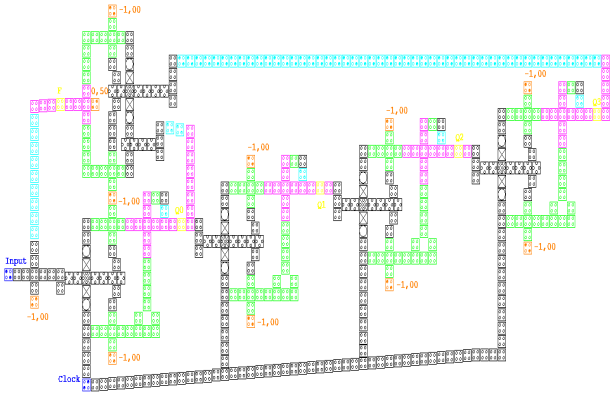


Fig. 10. Circuit of linear shift nanoregister with linear feedback, which is build in QCADesigner environment [4]

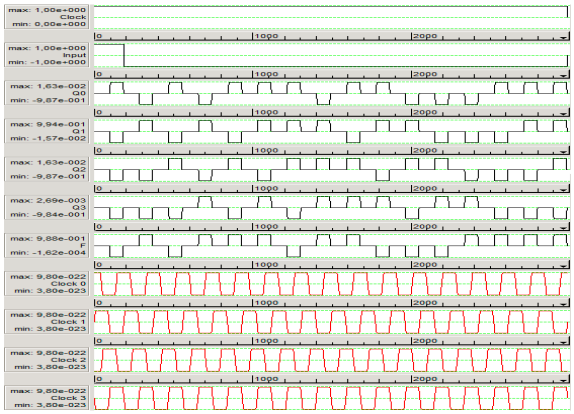


Fig. 11. Waveforms of nanoregister operation (Fibonacci configuration)

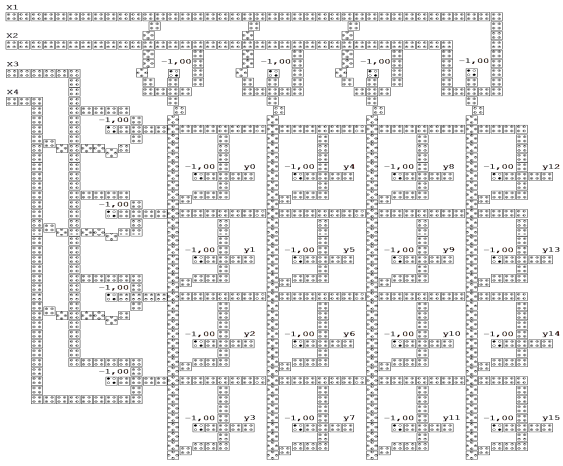


Fig. 12. Circuits of multi-stage (4→16) nanodecoder, which is build in QCADesigner environment [4]

There are two basic methods for modeling single-electron circuits with CAD Simon [5]. One of them is based on the Monte Carlo method and the other on the fundamental equations of solid state physics. The approach of Monte Carlo begins with the calculation of all possible events and probabilities of their existence, and chooses one of the possible events by chance, according to its probability. This operation is repeated many times for the simulation of

displacements of electrons in the nanoscale. Tunneling events are considered as independent and exponentially distributed. For single-electron circuits there is a problem of the effect of the initial, polarization, background charge. Lube impurities and trapped electrons in the substance induce charges on the island, which usually destroy the functioning of single-electron devices. The level of development of technology to date is not able to provide sufficient purity of matter for the construction of single-electronic devices. One impurity atom can completely change the entire behavior of the device. Computer design allows at the present stage to create super-complex devices and devices of single-electronics. These devices have practical applications in cipher modules. For an example below, the results of the computer design of binary to Gray code converter [5] presented. The text or data that the computers or other devices bear is staged by a binary code. The text or data is personified as a sequence of zeroes and ones. Gray codes are essential as they find a plenty of application in analog as well as digital cipher converters. Two adjacent code numbers can be distinguished from each other by just one bit. The single electron device based binary to Gray code converter is shown in the Figs 15, 16 and Table III.

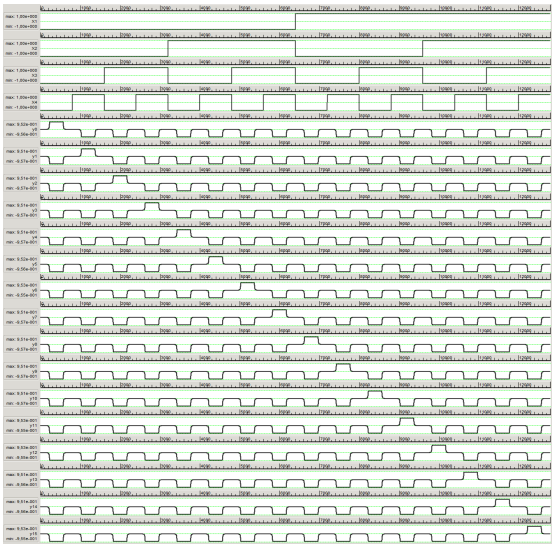


Fig.13. Waveforms of multi-stage (4→16) nanodecoder

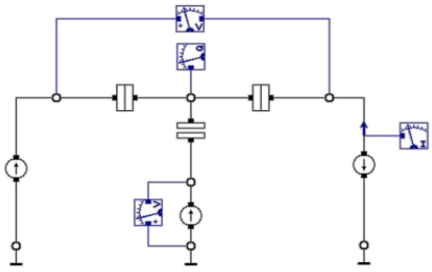


Fig. 14. Model SET on workstation of Simon

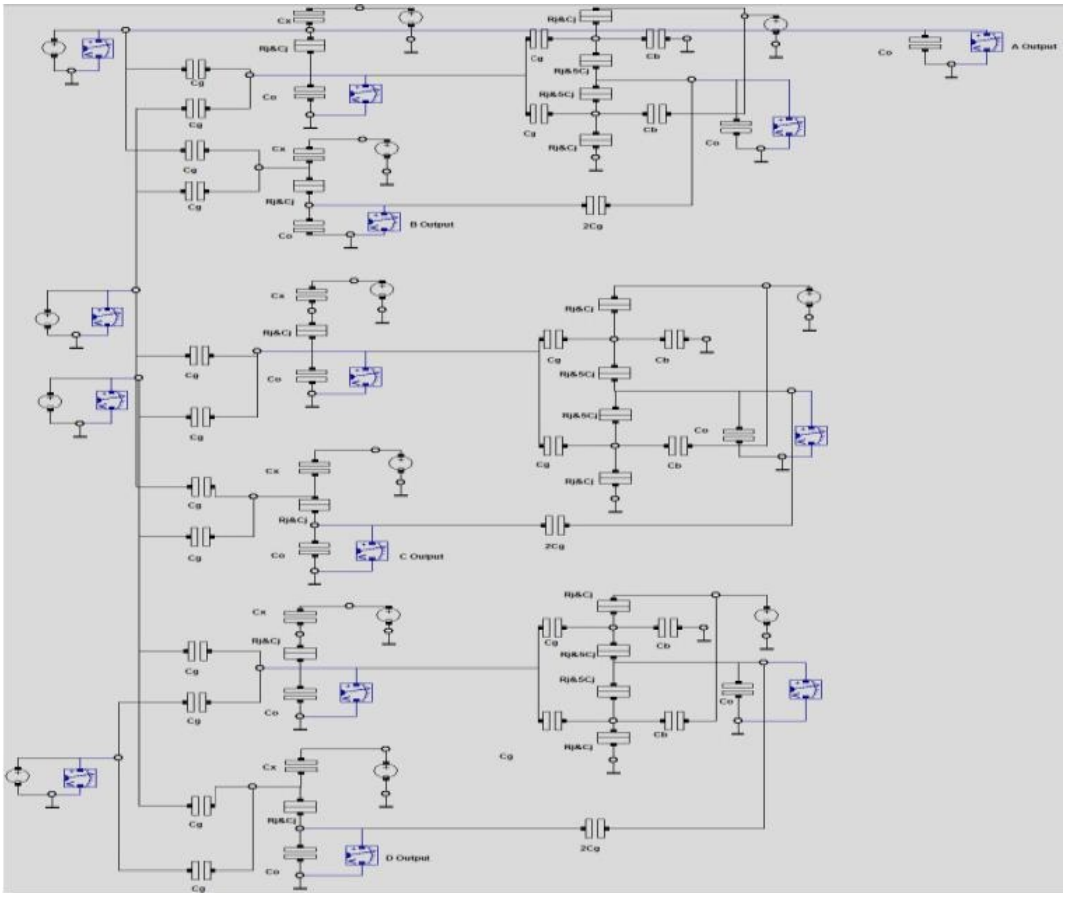


Fig. 15. Single electron device based binary to Gray code converter

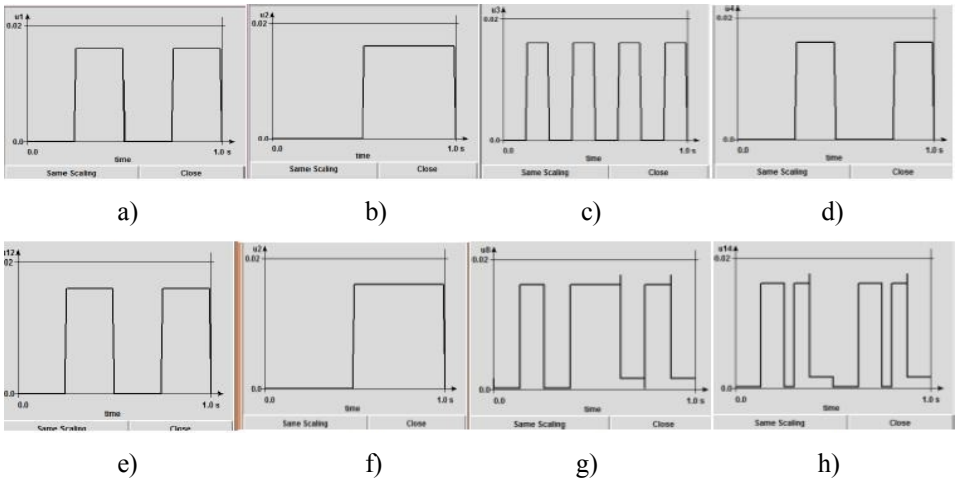


Fig. 16. Simulation results of binary to Gray code converter: input waveform *W* (a); input waveform *X* (b); input waveform *Y* (c); input waveform *Z* (d); output waveform *A* (e); output waveform *B* (f); output waveform *C* (g); output waveform *D* (h)

TABLE III. CONVERTING BINARY CODE TO GRAY CODE

i	***W*(b)**	***X*(c)**	***Y*(d)**	***Z*(e)**	*i*	***A*(f)**	***B*(g)**	***C*(h)**	***D*(i)**
0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	0	0	0	1
2	0	0	1	0	2	0	0	1	1
3	0	0	1	1	3	0	0	1	0
4	0	1	0	0	4	0	1	1	0
5	0	1	0	1	5	0	1	1	1
6	0	1	1	0	6	0	1	0	1
7	0	1	1	1	7	0	1	0	0
8	1	0	0	0	8	1	1	0	0
9	1	0	0	1	9	1	1	0	1
10	1	0	1	0	10	1	1	1	1
11	1	0	1	1	11	1	1	1	0
12	1	1	0	0	12	1	0	1	0
13	1	1	0	1	13	1	0	1	1
14	1	1	1	0	14	1	0	0	1
15	1	1	1	1	15	1	0	0	0

IV. CONCLUSION

The threat to cipher modules is side channel attacks. Because these attacks are due to the use of low cost equipment. In this work a new approach is presented for implementation of quantum cipher modules based on QCA and SET technologies. The basic logic is implemented on the *D*-triggers with the signal 'clock' with ultra-low energy consumption~ $5 \cdot 10^{-22}$ J. This is due to the development of nanotechnology in solving problems with the protection of information and the development of a safe cipher shift nanoregister, nanodecoder and Gray converter.

REFERENCES

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

[2] C. Lent and P. Tougaw, "Devices architecture for Computing with Quantum Dots." *Proc. IEEE – 1998*, vol. 10, no. 3, 1998, pp. 73–83.

[3] O. S. Melnyk and D. G. Milke, "Nanocircuits for the Cryptography Moduls," *Electronic and Control Systems,* no. 1(51), pp. 78–83, 2017. https://doi.org/10.18372/1990-5548.51.11697

[4] K. Walus, "QCADesiner: A Rapid Design and Simulation. Toll to QCAD II," *Int. Journal of Nanotech. and Appl.*, no. 1, pp. 1–7, 2005.

[5] Banani Talukdar, Dr. P. C. Pradhan and Amit Agarwal, "Design of different digital circuits using single electron devices," *Advances in Materials Science and Engineering: An International Journal (MSEJ)*, vol. 3, no. 1, March 2. https://doi.org/10.5121/msej.2016.3102

Received January 05, 2021

Melnyk Oleksandr. orcid.org/0000-0003-1072-5526. Candidate of Science (Engineering). Associate Professor.
Department of Electronics, Robotics, Monitoring and IoT Technologies, Faculty of Air Navigation, Electronics & Telecommunications, National Aviation University, Kyiv, Ukraine.
Education: Kiev Polytechnic Institute, Kyiv, Ukraine, (1971).
Research area: Nanoelectronics, Computer aided designe of nanoelectronic circuits, Simulation of single-electron circuit.
Publications: 154.
E-mail: melnyk_olexa@nau.edu.ua

Mykolushko Andriy. orcid.org/0000-0002-2767-8255. Assistant.
Department of Electronics, Robotics, Monitoring and IoT Technologies, Faculty of Air Navigation, Electronics & Telecommunications, National Aviation University, Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine.
Research area: Computer-aided design.
Publications: 20.
E-mail: andrii.mykolushko@npp.nau.edu.ua

Myshynskyi Arsen. Student.
Department of Electronics, Robotics, Monitoring and IoT Technologies, Educational & Research Institute of Air Navigation, National Aviation University, Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine.
Research area: Nanoelectronics.
Publications: 1.
E-mail: cyber-shot0@ukr.net

О. С. Мельник, А. М. Миколушко, А. О. Мишинський. Наносхеми для захисту інформаційного шифрування

Розглянуто вплив атак по побічним каналам, за якого пристрої шифрування беззахисні перед атаками силового і електромагнітного аналізу. Ці атаки обумовлені використанням недорогого обладнання. В даний час більшість схем шифрування реалізується на комплементарної структурі метал-оксид-напівпровідник. Недоліком є співвідношення між споживаною енергією і обробкою даних. При обробці КМОН-транзистором логічної «1» і логічного «0», через транзистор протікає струм різної величини. Якщо не реалізувати істотні протидії, це дозволить сторонній людині розшифрувати ключ модуля шифрування. Досліджено новий логічний підхід до точкових коміркових автоматів і одноелектронних транзисторів. Запропонований підхід відрізняється низьким енергоспоживанням і складними схемами тактування. В теорії і практиці захисту шифрів однією з ключових проблем є формування двійкових псевдовипадкових послідовностей максимальної довжини з прийнятними статистичними характеристиками. Генератори псевдовипадкових послідовностей зазвичай засновані на регістрах зсуву з лінійним зворотним зв'язком. Розширено поняття лінійного регістра зсуву, вважаючи, що кожна його комірка пам'яті може перебувати в одному зі станів. Регістри викликів – це «узагальнені лінійні регістри зсуву».

Ключові слова: квантові коміркові автомати; мажоритарний елемент; одноелектронні транзистори.

Мельник Олександр Степанович. orcid.org/0000-0003-1072-5526. Кандидат технічних наук. Доцент.
Кафедра електроніки, робототехніки і технологій моніторингу та інтернету речей, Факультет аеронавігації, електроніки та телекомунікацій, Національний авіаційний університет, Київ, Україна.
Освіта: Київський політехнічний інститут, Київ, Україна, (1971).
Напрям наукової діяльності: наноелектроніка, автоматизовані системи проектування, моделювання одноелектронних схем.
Кількість публікацій: 154.
E-mail: melnyk_olexa@nau.edu.ua

Миколушко Андрій Миколайович. orcid.org/0000-0002-2767-8255. Асистент.
Кафедра електроніки, робототехніки і технологій моніторингу та інтернету речей, Факультет аеронавігації, електроніки та телекомунікацій, Національний авіаційний університет, Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна.
Напрям наукової діяльності: автоматизовані системи проектування
Кількість публікацій: 20.
E-mail: andrii.mykolushko@npp.nau.edu.ua

Мишинський Арсен Олександрович. Студент.
Кафедра електроніки, робототехніки і технологій моніторингу та інтернету речей, Факультет аеронавігації, електроніки та телекомунікацій, Національний авіаційний університет, Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна.

Напрям наукової діяльності: наноелектроніка.
Кількість публікацій: 1.
E-mail: cyber-shot0@ukr.net

А. С. Мельник, А. Н. Миколушко, А. А. Мышинский. Наносхемы для защиты информационного шифрования

Рассмотрено влияние атак по побочным каналам, при котором устройства шифрования беззащитны перед атаками силового и электромагнитного анализа. Эти атаки обусловлены использованием недорогого оборудования. В настоящее время большинство схем шифрования реализуется на комплементарной структуре металл-оксид-полупроводник. Недостатком является соотношение между потребляемой энергией и обработкой данных. При обработке КМОП-транзистором логической «1» и логического «0», через транзистор протекает ток разной величины. Если не реализовать существенные противодействия, это позволит постороннему человеку расшифровать ключ модуля шифрования. Исследован новый логический подход к клеточным автоматам с квантовыми точками и одноэлектронным транзисторам. Предлагаемый подход отличается низким энергопотреблением и сложными схемами тактирования. В теории и практике защиты шифров одной из ключевых проблем является формирование двоичных псевдослучайных последовательностей максимальной длины с приемлемыми статистическими характеристиками. Генераторы псевдослучайных последовательностей обычно основаны на регистрах сдвига с линейной обратной связью. Расширено понятие линейного регистра сдвига, полагая, что каждая его ячейка памяти может находиться в одном из состояний. Регистры вызовов – это «обобщенные линейные регистры сдвига».

Ключевые слова: квантовые клеточные автоматы; мажоритарный элемент; одноэлектронные транзисторы.

Мельник Александр Степанович. orcid.org/0000-0003-1072-5526. Кандидат технических наук. Доцент.
Кафедра электроники, робототехники и технологий мониторинга и интернета вещей, Факультет аэронавигации, электроники и телекоммуникаций, Национальный авиационный университет, Киев, Украина.
Образование: Киевский политехнический институт Киев, Украина, (1971).
Направление научной деятельности: наноэлектроника, автоматизированные системы проектирования, моделирование одноэлектронных схем.
Количество публикаций: 154.
E-mail: melnyk_olexa@nau.edu.ua

Миколушко Андрей Николаевич. orcid.org/0000-0002-2767-8255. Ассистент.
Кафедра электроники, робототехники и технологий мониторинга и интернета вещей, Факультет аэронавигации, электроники и телекоммуникаций, Национальный авиационный университет, Киев, Украина.
Образование: Национальный авиационный университет, Киев, Украина.
Направление научной деятельности: автоматизированные системы проектирования.
Количество публикаций: 20.
E-mail: andrii.mykolushko@npp.nau.edu.ua

Мышинский Арсен Александрович. Студент.
Кафедра электроники, робототехники и технологий мониторинга и интернета вещей, Факультет аэронавигации, электроники и телекоммуникаций, Национальный авиационный университет, Киев, Украина.
Образование: Национальный авиационный университет, Киев, Украина.
Направление научной деятельности: наноэлектроника.
Количество публикаций: 1.
E-mail: cyber-shot0@ukr.net