UDC 621.382-022.532 (045)

[1]O. S. Melnyk,
[2]D. G. Milke

# NANOCIRCUITS FOR THE CRYPTOGRAPHIC MODULES

Educational & Research Institute of Air Navigation, Nation Aviation University, Kyiv, Ukraine
E-mails: [1]melnyk.ols@gmail.com, [2]i_strong@bigmir.net

***Abstract***— *The possibility of introducing non-emitting nanoscales on the basis of quantum cellular automata has been investigated. It practically neutralizes electromagnetic attacks. The method of protection from external interferences and observations of electromagnetic radiation (attacks) is proposed in the work. The power consumption of cryptographic modules has been reduced by five orders. Secure encryption of cryptographic information is provided..*

**Index Terms**—Quantum cellular automata; majority gate; Gaois configuration; linear shift nanoregister.

## I. Introduction

Power analysis attacks were introduced in [1]. 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 cryptographic 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 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. Problem Statement

### *A Basics of QCA theory*

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]. 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 equation:

$$P = \frac{(p_1 + p_3) - (p_2 + p_4)}{(p_1 + p_3) + (p_2 + p_4)} = \pm 1,$$

where ρi is charge density every quantum dot of cell.

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

### *B Majority Gate and Inverter*

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 deg or 90 deg 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.

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

$$f = \mathrm{maj}(x_0, x_1, x_2) = x_1 x_2 \cup x_0 x_1 \cup x_0 x_2.$$

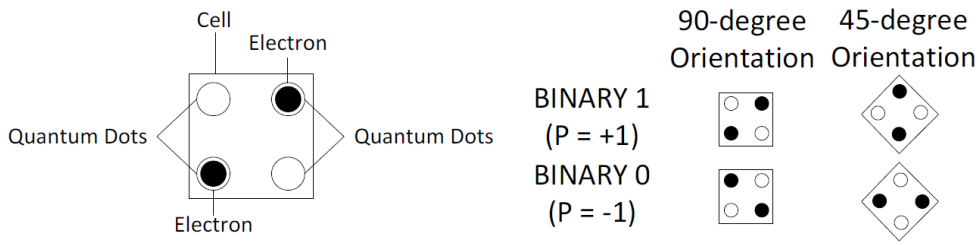
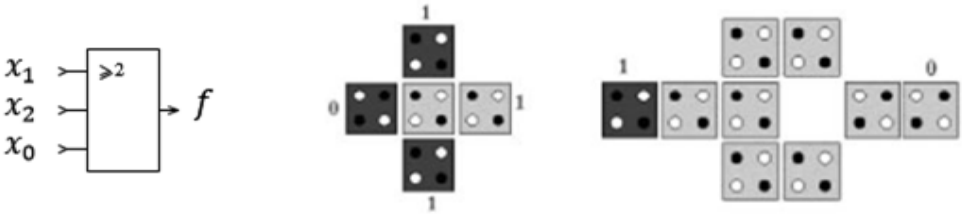



Fig. 1. A single QCA cell and its two possible orientations and polarization ($P = \pm 1$)




a b

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

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

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

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

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

## III. Problem Solution

A power consumption (e.g. the side channel) of a cryptographic 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. Fig. 4 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 cryptographic 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 cryptographic engineering implemented in QCA logic.

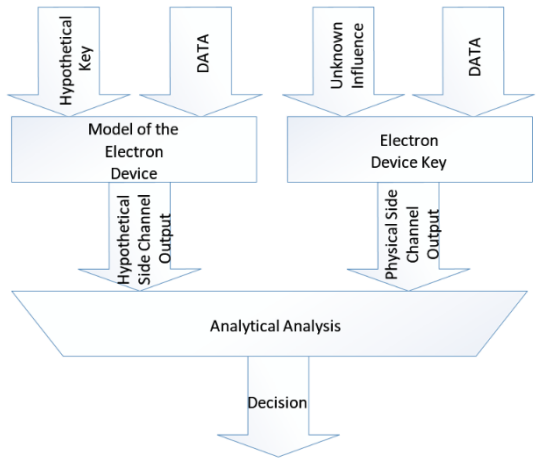



Fig. 3 Principles of side channel attacks

## III. Basic Concepts of Galois Configuration

In theory and practice of cryptographic protection one of the key problems is the formation of binary pseudorandom sequences of maximum length of acceptable statistical characteristics. Generators of pseudorandom sequences implement, usually based on linear shift registers maximum period 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."

The main objective is to develop algorithms generalized matrix Galois and Fibonacci *n*th order over the field, which uniquely determine a structure corresponding generalized *n*-bit linear nano-register shift of the maximum period and forming on the basis of generators of pseudorandom sequences Galois maximum length.

In theory of Galois fields, which are the foundation of algebra noise immunity coding, cryptography and building modern nano-electronic 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.

The most important property of finite extended Galois fields, which is generated by irreducible polynomial, it is that for any nonzero element it should be the opposite element such that $g \cdot g^{-1}(\mathrm{mod}\, f_n)=1$ formulated condition holds if is the number simple. It follows that the Galois field characteristic, both simple and advanced, should be a simple number.

## IV. Sinthesis of Linear shift nano-Register with Galois Configuration for Cryptography

Let consider an example of four-digit linear nano-register of shift with feedback which assignation form first and fourth grade (Fig. 4).

D-trigger (Fig. 5) and the gate of XOR (Fig. 6) is the basic elements of sequence nano-registers with linear feedback.

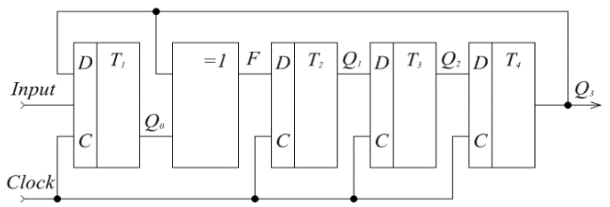
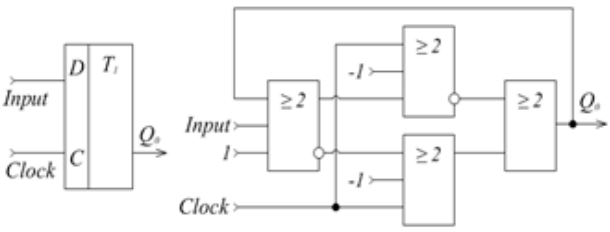


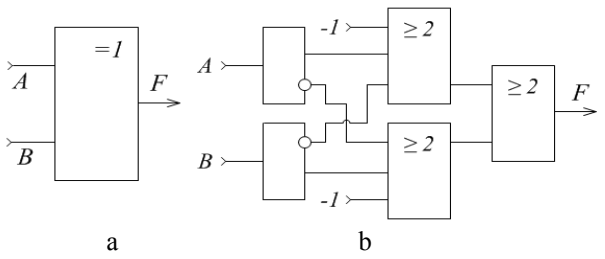

Fig. 4. Block diagram of shift nano-register with feedback (Galois configuration)

D-trigger (Fig. 5) and the gate of XOR (Fig. 6) is the basic elements of sequence nano-registers with linear feedback.




a b

Fig. 5. Block diagram of D-trigger (a) on majority elements (b)




a b

Fig. 6. Block diagram of XOR (a) on majority elements (b)

## V. Simulation results

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

$$L=p^n-1=2^4-1=15.$$

Algebraic form of binary polynomial:

$$f_4(x)=x^4+x+1..$$

Feedback function:

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

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

Table I

State of outputs and inputs of shift nano-registers with Galois configuration

| 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 |

Results of the automated designing linear shift nano-register with Galois configuration shown in Figs 7 and 8.

Total number of quantum cellular automata shift nano-circuits register 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.

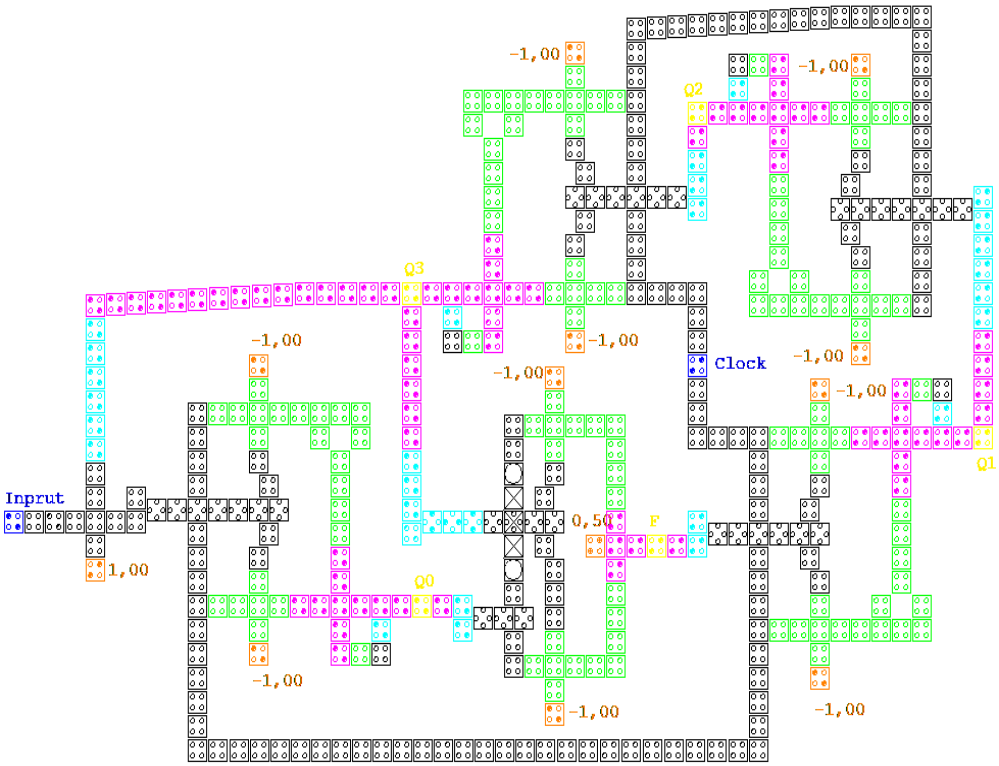



Fig. 7. Circuit of linear shift nano-register with feedback, which constructed in the environment QCADesinger


Fig. 8. Time diagram of nano-register operation

## IV. Conclusion

Side channel attacks seriously threaten cryptographic modules as they can be implemented with relatively inexpensive equipment's. In this work, a new approach to implementation of quantum cryptographic modules via QCA technology has been presented. Matrix of Galois configuration have important properties such as

primitiveness and commutativity, which made it possible to build on its basis a general linear nano-register of maximal period. Galois Generator not very cryptographically strong, but provides performance gains: all XOR operations can be performed by one action. This nano-circuit gives advantages in the hardware implementation.

## REFERENCES

[1] E. Ramini and S. M. Nejad. *Secure clocked QCA logic for implementation of cryptographic processors*. 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.

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

[4] A. Y. Beleckij and A. A. Beleckij, *Gray's conversion*. Monograph in 2 volumes, vol. 1, *Fundamentals of Theory*, Kyiv, NAU, 2007, 506 p. (in Russian).

Received January 21, 2017

**Melnyk Oleksandr**. Candidate of Sciences (Engineering). Associate Professor.
Electronics Department, Educational & Research Institute of Air Navigation, 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: 176.
E-mail: melnyk.ols@gmail.com

**Milke Denis.** Student.
Electronics Department, Educational & Research Institute of Air Navigation, National Aviation University, Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine, (2017).
Research area: Modeling of single-electron circuits.
E-mail: i_strong@bigmir.net

**О. С. Мельник, Д. Г. Мільке. Наносхеми для криптографічних модулів**

Досліджено можливість запровадження невипромінюючих наносхем на базі квантових коміркових автоматів. Це практично нейтралізує електромагнітні атакию. Запропоновано метод захисту від сторонніх втручань та спостережень електромагнітного випромінювання (атак). На п'ять порядків знижено енергоспоживання криптографічних модулів. Забезпечено завадостійке шифрування криптографічної інформації.

**Ключові слова**: квантовий комірковий автомат; мажоритарний елемент; конфігурація Галуа; лінійного нанорегістру зсуву.

**Мельник Олександр Степанович.** Кандидат технічних наук. Доцент.
Кафедра електроніки, Національний авіаційний університет, Київ, Україна.
Освіта: Київський політехнічний інститут, Київ, Україна, (1971).
Напрям наукової діяльності: наноелектроніка, автоматизовані системи проектування, симулювання одноелектронних схем.
Кількість публікацій: 176.
E-mail: melnyk.ols@gmail.com

**Мільке Денис Геннадійович.** Студент.
Кафедра електроніки, Національний авіаційний університет, Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна, (2017).
Напрям наукової діяльності: моделювання одноелектронних схем.
Кількість публікацій: 0.
E-mail: i_strong@bigmir.net

**А. С. Мельник, Д. Г. Мильке. Наносхемы для криптографических модулей**

Исследована возможность введения неизлучающие наносхем на базе квантовых ячеистых автоматов. Это практически нейтрализует электромагнитные атакию. Предложен метод защиты от посторонних вмешательств и наблюдений электромагнитного излучения (атак). На пять порядков снижено энергопотребление криптографических модулей. Обеспечено помехоустойчивое шифрования криптографической информации.

**Ключевые слова**: квантовый сотовый автомат; мажоритарный элемент; конфигурация Галуа; линейный сдвиговый нанорегистр.

**Мельник Александр Степанович.** Кандидат технических наук. Доцент.
Кафедра электроники, Национальный авиационный университет, Киев, Украина.
Образование: Киевский политехнический институт Киев, Украина (1971).
Направление научной деятельности: наноэлектроника, автоматизированные системы проектирования, симулирование одноэлектронных схем.
Количество публикаций: 176.
E-mail: melnyk.ols@gmail.com

**Мильке Денис Геннадиевич.** Студент.
Кафедра электроники, The possibility of introducing non-emitting nanoscales on the basis of quantum cellular automata has been investigated. It virtually neutralizes electromagnetic attacks. The method of protection from external interferences and observations of electromagnetic radiation (attacks) is proposed in the work. The power consumption of cryptographic modules has been reduced by five orders. Secure encryption of cryptographic information is provided.разование: Национальный авиационный университет, Киев, Украина.
Направление научной деятельности: моделирование одноэлектронных схем.
Количество публикаций: 0.
E-mail: i_strong@bigmir.net