UDC 004.94.:621.389.:53.086(045)

COMPUTER DESIGN OF NANOCIRCUITS FOR CRYPTOGRAPHIC ENGINEERING

Oleksandr Melnik, Viktoriia Kozarevych, Dmytrii Khodymchuk

Since the introduction of side-channel attacks, cryptographic devices have been highly susceptible to power and electromagnetic (EM) analysis attacks: because these attacks require only relatively inexpensive equipment's. Most of cryptographic circuits are typically implemented in CMOS. There is a strong dependency between power consumption of circuits implemented based on this logic style and the data that is processed by the circuit. Due to the difference between input and output capacitances of CMOS-transistors, when the transistor switches on and off, different amount of current flows through the transistor and leads to different amount of power consumption when the transistor processes logic a "0" or logic "1". Unless adequate countermeasures are implemented, side channel attacks allow an unauthorized person to reveal the private key of a cryptographic module. Countermeasure a novel logic approach to Quantum-dot Cellular Automata (QCA). The proposed logic takes advantage of low power consumption QCA together with complicated clocking circuits as a paradigm of nanotechnology advances in cryptography engineering.

Keywords: *quantum cellular automata, majority gate, D-type flip-flop, shift nanoregister.*

Actuality of problem

Power analysis attacks were introduced in [1]. In fact, power and 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.

Background

Basics of QCA theory. 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 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 charge density every quantum dot of cell.

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

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 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.

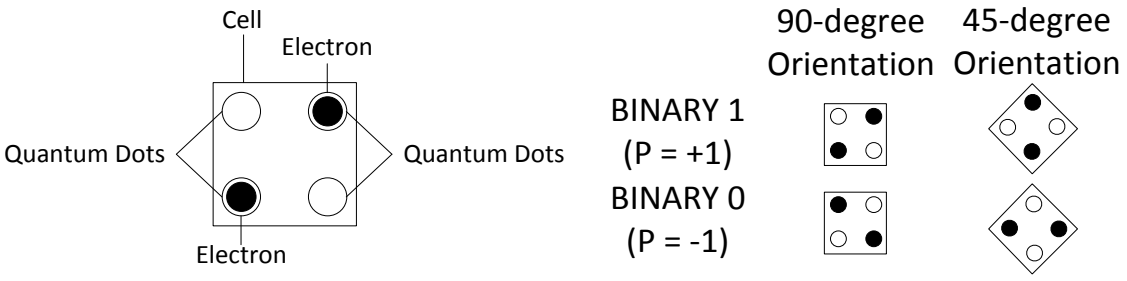
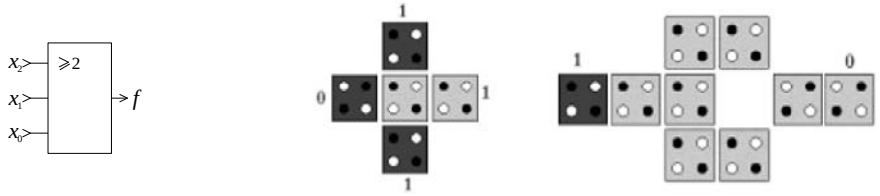


Fig. 1. A single QCA cell and its two possible orientations and polarization ($P = \pm 1$)



a *b*

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

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:

$$f_{AND} = maj(x_2, x_1, 0) = x_2x_1,$$
$$f_{OR} = maj(x_2, x_1, 1) = x_2 \vee x_1.$$

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

Side channel attacks and countermeasures

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.

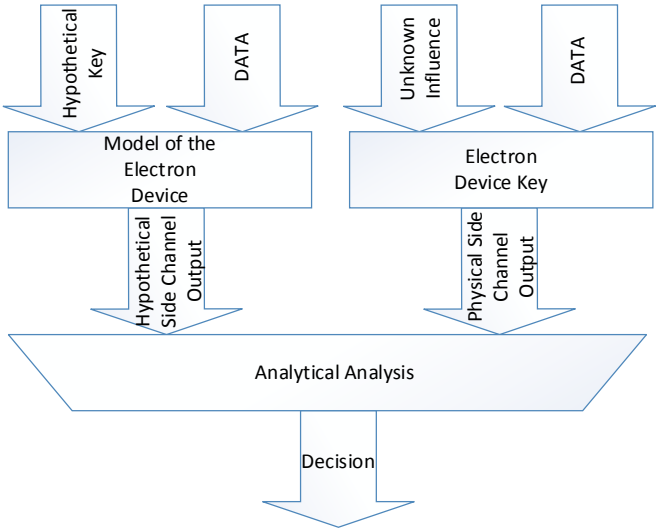


Fig. 3. Principles of side channel attacks

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.

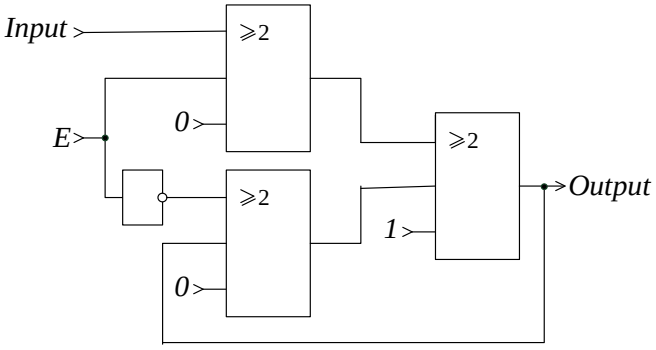


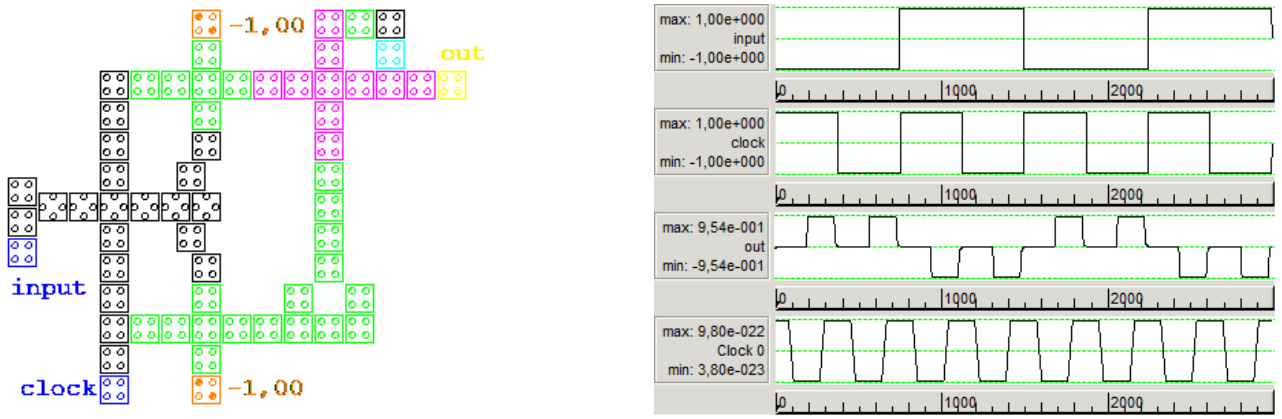
Fig. 4. Structure of a D-latch

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. 5, a. Logic equation in the bulean majority bases D-type flip-flop for states Q_t and Q_{t-1} are as follows:

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

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

where C and D – pulse synchronization codes and cryptographic information.



a b

Fig. 5. QCA D-type nanoflip-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. 5, b).

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

Registers are built from synchronous flip-flop circuit that are sequentially connected, so output signal from the previous flip-flop entries the information input of the next flip-flop. All flip-flops are managed by the general signal of synchronization. In shift registers any two-level flip-flops (types RS, D, JK) can be used. But all of them work in a D-type flip-flop mode.

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 cryptographic 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 cryptography code to parallel show of Fig. 6.

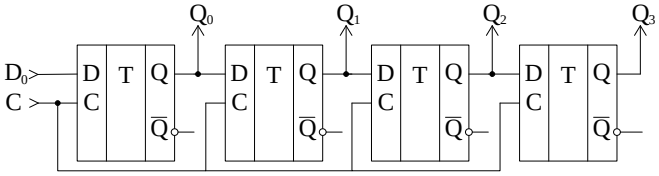


Fig. 6. Serial D-type flip-flop register

Simulation results

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

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

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

$$Q_0 = maj(C, D, 0), maj(\overline{C}, D, -1), 1),$$

$$maj(maj(C, Q_0, -1), maj(\overline{C}, Q_0, -1), 1) \to Q_1 \text{ and so on.}$$

The states of all outputs for shift register show in table 1.

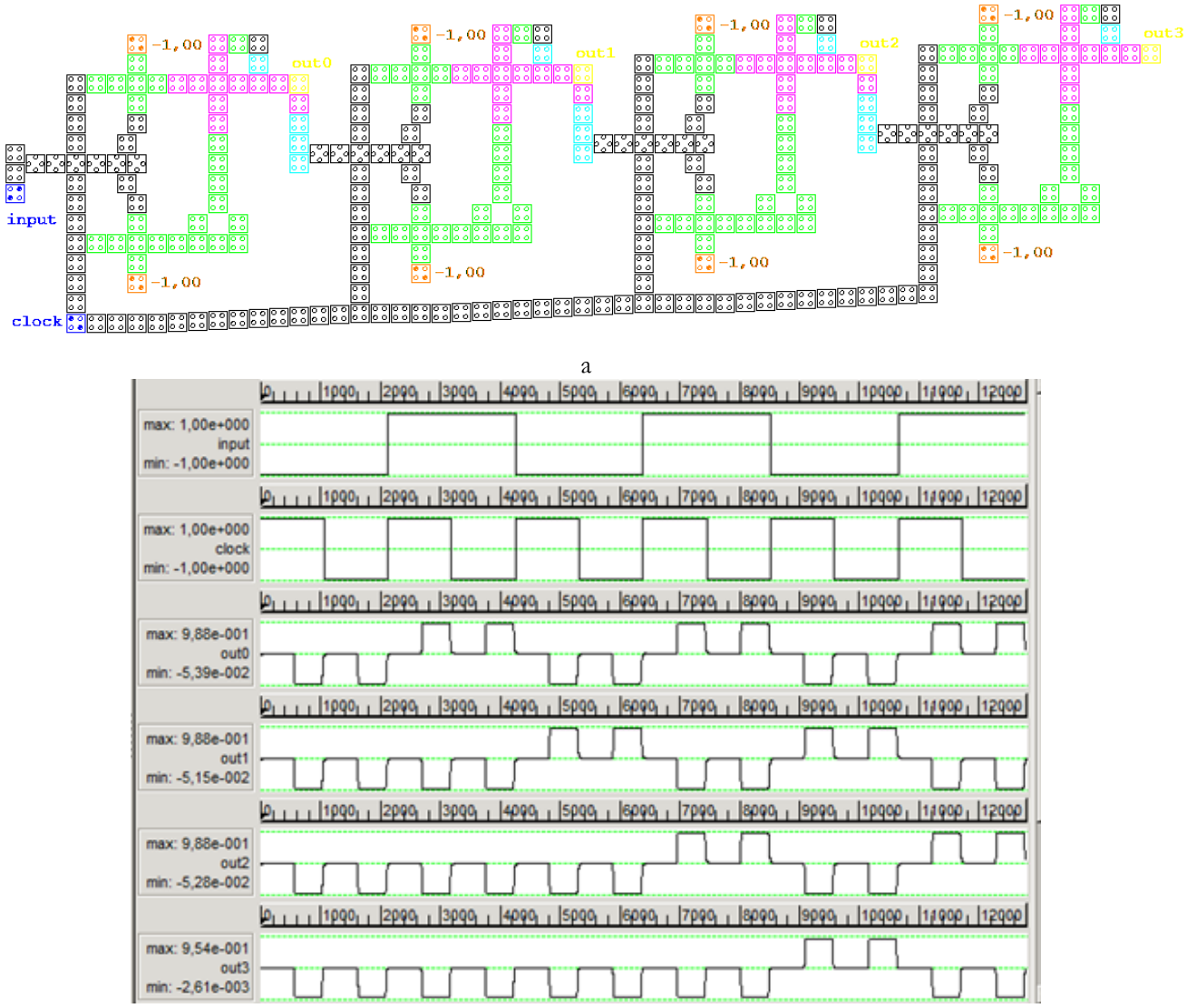
Table 1

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

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 500 nm x 1760 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. 5, b).



a

b

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

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. 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.

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

[4]. *Pakulov N. N.* Mazhoritarnyiy printsip postroeniya nadezhnyih uzlov i ustroystv TsVM / N. N. Pakulov – M.: Sov. radio – 1974.

ЛІТЕРАТУРА

[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.

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

[4]. *Пакулов Н. Н.* Мажоритарный принцип построения надежных узлов и устройств ЦВМ / Н. Н. Пакулов – М.: Сов. радио – 1974.

КОМП'ЮТЕРНЕ ПРОЕКТУВАННЯ СХЕМ ДЛЯ КРИПТОГРАФІЧНОЇ ІНЖЕНЕРІЇ

Традиційне криптографічне обладнання недостатньо захищене від сторонніх втручань та спостережень електромагнітного випромінювання (атак). Більшість існуючих криптографічних схем реалізовані на КМОН-транзисторах, енергоспо-живання яких суттєво залежить від імпульсних характеристик перетворюваної інформації. В режимах комутації логічного "0" або логічної "1" через транзистори проходять істотно різні струми стоку із-за різниці між вхідними та вихідними КМОН-ємностями, які перезаряджаються струмом стоку, виникають різні рівні електромагнітного вип-ромінювання. Це може призводити до розшифровки криптографічної інформації. В роботі досліджується 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.

КОМПЬЮТЕРНОЕ ПРОЕКТИРОВАНИЕ СХЕМ ДЛЯ КРИПТОГРАФИЧЕСКОЙ ИНЖЕНЕРИИ

Традиционное криптографическое оборудование недостаточно защищенное от посторонних вмешательств и наблюдений электромагнитного излучения (атак). Большинство существующих криптографических схем реализованы на КМОП-транзисторах, энергопотребление которых сущес-твенно зависит от импульсных характеристик преобразуемой информации. В режимах коммутации логического "0" или логической "1" через транзисторы проходят разные токи стока из-за разности между входящими и исходящими КМОП-емкостями, которые перезаряжаются током стока, возникают разные уровни электромагнитного излучения. Это может приводить к расшифровке криптографической информации. В работе исследуется возможность внедрения неизлучающих наносхем на базе квантовых сотовых автоматов, что практически нейтрализует электромагнитные атаки.

Ключевые слова: квантовый сотовый автомат, мажоритарный элемент, D-триггер, сдвиговый нанорегистр.

Мельник Олександр Степанович, кандидат технічних наук, доцент, доцент кафедри електроніки Національного авіаційного університету.
E-mail: melnyk.ols@gmail.com

Мельник Александр Степанович, кандидат технических наук, доцент, доцент кафедры электроники Национального авиационного университета.

Melnyk Oleksandr, candidate of technical science, Associate Professor, Associate Professor of De-partment Electronics of National Aviation University.

Козаревич Вікторія Олександрівна, асистент кафедри електроніки Національного авіаційного університету.
E-mail: st-viktoria@yandex.ru

Козаревич Виктория Александровна, асситент кафедры электроники Национального авиационного университета.

Kozarevych Viktoriia, Assistant of Department Electronics of National Aviation University.

Ходимчук Дмитрій Сергійович, студент кафедри електроніки Національного авіаційного університету.
E-mail: hodimchukdmitriy@gmail.com

Ходымчук Дмитрий Сергеевич, студент кафедры электроники Национального авиационного универ-ситета.

Khodymcuk Dmytrii, Student of Department Electronics of National Aviation University.