UDC 004.056-022.513.2 (045)

O.S. Melnyk, D.G. Milke, Y.V. Poliakov
(National Aviation University, Ukraine)

Nanocircuit for protection of the cryptographic information

While using side-channel attacks, cryptographic devices was defenseless to power and electromagnetic(EM) analysis attacks. These attacks are due to the use of low cost equipment. Currently, most of the cryptographic schemes are implemented on CMOS. A new logical approach to Quantum-dot Cellular Automata (QCA) and Single-Electron Transistors (SET) is explored. The proposed approach has low power consumption and complicated clocking circuits.

Side channel attacks

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 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 cryptographic 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 choice schemes.

Backgrounds

The 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 2 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 three 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 it we can using the formula:

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

where is charge density every quantum dot of cell.

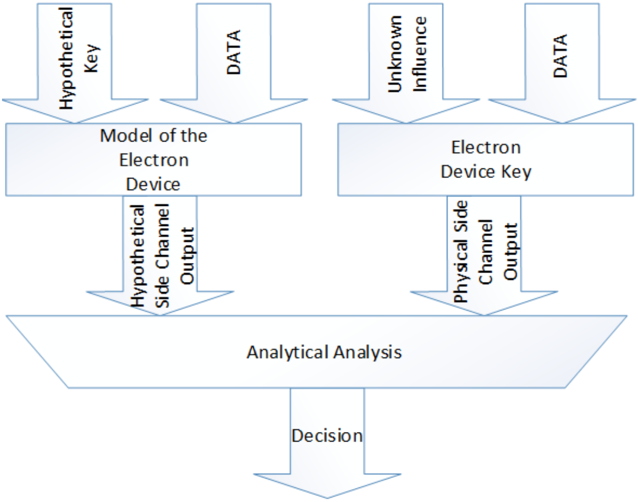

Hypothetical Key
DATA
Unknown Influence
DATA
Model of the Electron Device
Electron Device Key
Hypothetical Side Channel Output
Physical Side Channel Output
Analytical Analysis
Decision

Fig. 1. Principles of side channel attacks

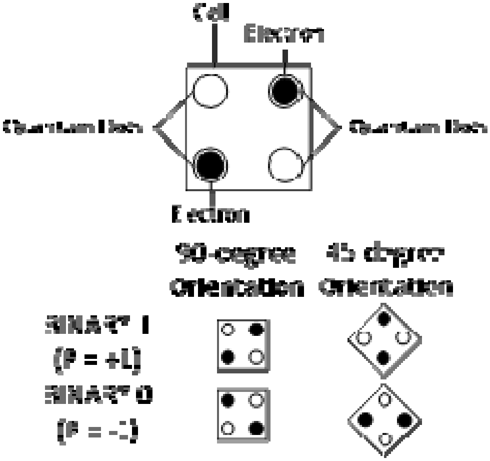
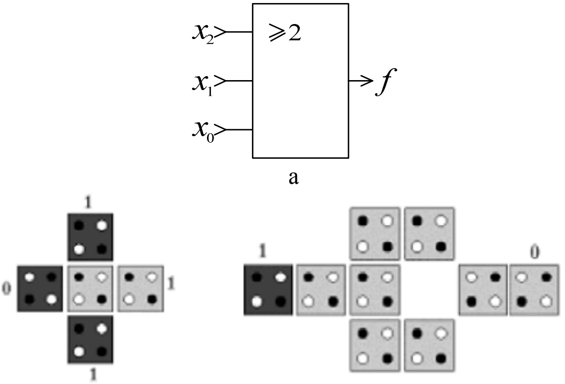


Fig. 2. A single QCA cell and its two possible orientations and polarization (P= 1)

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), but on practice it is difficult to manufactured nano-cells with different orientation [3].

For build a various arithmetic and logic functions must be constructed a different majority gates. The basic logic gates in QCA are the majority gate (a) and inverter (b) on Fig. 2.



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 x2, x1 and x0 is

$$f = maj(x_2, x_1, x_0) = x_2x_1 \vee x_2x_0 \vee x_1x_0 \, .$$

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

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

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

The QCA and SET circuit 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 cryptographic engineering implemented in QCA and SET logic.

Conclusion

The threat to cryptographic 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 cryptographic modules based on QCA technology. The basic logic is implemented on the D triggers with the signal 'clock'. This is due to the development of nanotechnology in solving problems with the protection of information and the development of a safe cryptographic 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. O.Melnyk, V.Kozarevych, D.Khodymchuk. Computer design of nanocircuits for cryptography engineering. // Ukrainian Information Security Research Journal. Volume 18, №1, january-march 2016, – pp.16- 20.

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

4. O.Melnyk, D.Milke, D.Khodymchuk. Nanocircuits for the cryptograpic modules // Electronics and control systems. Vol.51, №1, 2017, – pp.78- 82