DESIGN AND ANALYSIS OF QCA CRYPTOGRAPHIC CIRCUITS

Mansi Rana[1], Mr. Ajay Dagar[2]
[1]M.Tech. (ECE), HoD, Electronics & Communicating Engineering, [2]WCTM, Farrukh Nagar, Gurgaon

***Abstract:* In this model, the total capacity of the QCA circuits is divided into two main components, leakage strength and switch power. The power loss is set during clock fluctuations, from low to high or high to low, as a leakage and power loss during the switch period as a switching power. More recently, studies have been conducted to design various QCA structures more efficiently. For example, there are many improved designs for QCA tools logic circuits using exclusive or portals reverse gates and various alternative QCA wiring approaches In addition, much attention has been paid to the design of the memory cell as vital elements in QCA devices, The ring-based QCA methods are a pioneering way to design well with the ambitious goal of promoting traditional CMOS based RAM (SRAM) while the techniques for designing each of these circuits have been established individually, the overall design needs.**

Key word: QCA Tools, CMOS, RAM (SRAM)

I. INTRODUCTION

Over the past decade, high-speed demands for low power consumption and CMOS expansion restrictions have forced scientists to look at alternative emerging technologies [1]. Many techniques, such as the field effects transistors of carbon nanotubes (CNTFETs), quantum automatic transistors (SETs), QCAs, and others have been investigated. QCA is a promising technology that supports a lower transistor model. In nanotechnology, circuits operate with high-speed switching characteristics, extremely high densities, and low power consumption [2], [3] all required for next-generation circuits, especially memory devices. QCA faces challenges related to manufacturing defects, ambient operating conditions, and circuit design, in which we address recent concerns by developing a new approach to degradation and time. The design of efficient bit storage cells plays a pivotal role in the development of QCA technology. They are determined by the logical basic building blocks used, as well as the bonding requirements that are incurred. Structural blocks are determined by the basic logical gate structure. Each QCA cell contains two electrons and four quantum points, and because of the Coulomb interaction between these identical charges, they occupy the points in a diagonal. As a result, the stable polarization of the QCA cell is achieved, as shown in Figure 1 (a). The immediate polarization of the cell is referred to as either 1 or 1, which is encoded to represent a value of 1 and a value of 0 respectively. Meanwhile, connectivity requirements are determined by topology and interactions between cells. A series of QCA cells placed side-by-side capable of spreading the first cell polarization via successive cell reactions to achieve a conductor role in CMOS devices. Figure 1 (b) shows a QCA wire that publishes a binary value of 0. In QCA technology, storage cells do not require an external power source to maintain the current stable polarization. In fact, the clock controls the charge flow in the circuit. The QCA clock consists of four stages around the clock, such as Switch, Hold, Release and Relax, which extend 90 degrees off-track [5], [7]. More recently, the QCA power consumption model has been presented in [6].

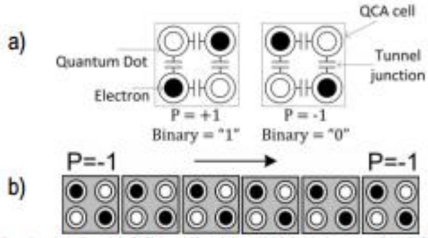


Fig. 1. (a) Basic QCA cell with two binary state (b) QCA standard wire.

In the research literature, a methodology that can achieve any QCA structure has been identified. In order to reduce the number of port numbers necessary to implement the QCA addition, a new design method was introduced to generate signals using the development features of support in a new way. Refers to a new methodology to analyze QCA circuit errors by specific random introduction of potential defects. In [37], a standard method based on the QCA tile was proposed. In this research, a comprehensive methodology of QCA circuit design was proposed. In this method, the analog circuit and the series circuit are connected to two levels of priority blocks (first priority block including MUX and XOR 2:1 gate and a second priority block incorporating a plurality of input multiple gates) After dividing, QCA. These three approaches are called traditional approaches, innovative approaches, and cell-level methods.

II. BACKGROUND

QCA Fundamental Concepts

To satisfy this need, we have been invited to many solutions. [1] Using the first method included in the two standard rounds of the QCA cell. As shown in Figure below (A), on a cross serial wire, a single wire is made by standard cells being run by different cell rotation cells. In this case, Alslcan operates independently and does not affect each other. Another way, [8] intersection was introduced in wired logic called. In this way, by looking at the assignment stage outside of 180 degrees, the cell can set the stage of the commentary to allow polarized polarization through the set of diastolic cells. Likewise, switching phase can easily be done at the intersection of all developed cells. Figure below (b) is a complete implementation of this approach. As the minimum and maximum number of cells that need to synchronize such time zones and flows, to acquire accurate work and reduce circuit sensitivity, some of these applications It should be noted that considering the design rule of the agreement matches the QCA concept imposed on the designer. Each time QCA region MUST consist of two cells to maintain its influence over at least the following time periods. If you set all the inputs from the integrated structure of many inputs into the major area of time (in 5 major cells from 3 input majority gate to 5 cells as an example) Synchronization will be achieved by a majority vote. Therefore, the caller says that you must put the following on the output line into the gate after the middle region of the cell. This robust structure guarantees the transfer of highly polarized signals.

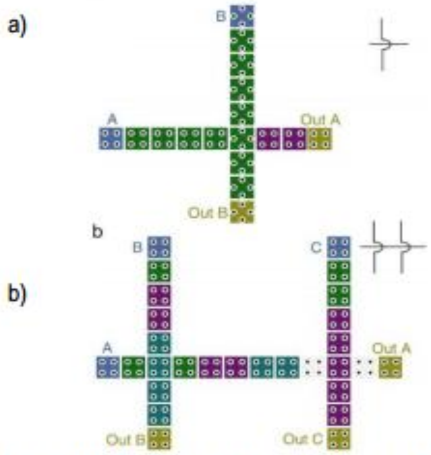


Fig. 3. (a) Coplanar wire-crossing, (b) Logical wire-crossing (Clocking based).

Qca Design Methodology For Designing Efficient Layouts (Sram Cell Case Study)

In this section, a systematic and consistent methodology for designing quantum cell circuits called phase collapse (PPDD) has been proposed. It can be searched for combinations of QCA circuits without losing generality, classified as follows, or harmonics or serial - three priority blocks.

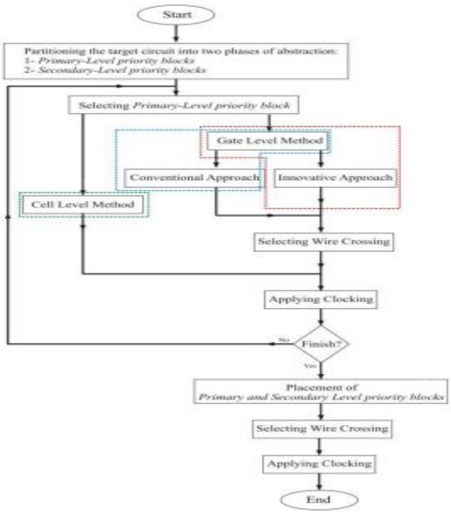
1) In abstract two levels or stages - 2 Input Exclusive - OR Gate or Multiplier Circuits These blocks are created on a regular basis using a number of multiple input multiple gates in interconnected QCAs. Basic priority in its ability to easily implement all complex Almntkiet Basic insight behind the identification of the priority of these logical function blocks directly.

2) Basic portal such as secondary priority block or multi input major gate these blocks play an integral part in providing priority level priority blocks .Figure below shows the proposed design methodology in the form of a flowchart. In the first step, after defining the target circle, divide the logical function into two priority levels of abstraction based on the above concept. QCA random access memory (SRAM) cells are checked as a case study of this study.

Shows a new and improved schematic diagram of a QCA SRAM cell including basic and second level elements for executing cryptographic memory. As block building with initial priority QCA (called rectangle)

1: In this design, in addition to block multiplexer, transmitter

2 Three revenues and a majority of the five blocks of secondary structure QCA priority (called by circle) and three.


Start
Partitioning the target circuit into two phases of abstraction:
1- Primary-Level priority blocks
2- Secondary-Level priority blocks
Selecting Primary-Level priority block
Gate Level Method
Conventional Approach
Innovative Approach
Cell Level Method
Selecting Wire Crossing
Applying Clocking
No
Finish?
Yes
Placement of Primary and Secondary Level priority blocks
Selecting Wire Crossing
Applying Clocking
End

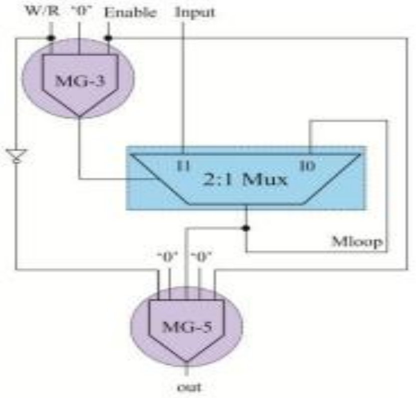


TABLE I
COMPLETE OPERATION OF THE PROPOSED QCA MEMORY CELL

Operation	Enable	W/R	Input	Mloop	out
Write	1 1	1 1	1 0	1 0	0 0
Read	1 1	0 0	x x	0 1	0 1
Idle	0	x	x	Doesn't change	0

A. Gate level Method of PPDD

In this design method, the designer should propose a new gate-level architecture for the initial priority block using multi-input multiple gates and try to implement it exactly. QCA compliance can be defined as a QCA-based majority-based design that ignores the entire existing and / or base structure. After designing the gate level, you can perform two different approaches called traditional and innovative approaches. These methods are described using the dotted line blue and red dotted block in Figure 4. In the conventional method, as described in Section II, the canonical construction of a multi-input majority gate is used. The most striking task of this approach is to achieve the most effective implementation by proper alignment between these gates. Unlike this general design method, regardless of the conventional structure, the PPDD method innovation method can show a new diagram of the basic gate to facilitate circuit implementation. If a 2: 1 multiplex block is given as the primary level block, three alternative architectures are considered at the QCA gate level. In Figure 1, multiplexer 2: 1 is designed using three triple entry gates, as shown in Figure 6 (a), and two AND and OR gates produce the desired output. The last two proposed designs shown in Figures 6 (b) and 6 (c) consist of a multi-input multi-portal, but it can be thought of as a QCA compatible design for a new logical expression I can do it. In the design, as shown in FIG. 6 (b), only one AND gate is connected to the majority decision gate of three inputs. In addition, the design of FIG. 6 (c) of most multi-input gates ignoring the design of the AND-OR base is made.

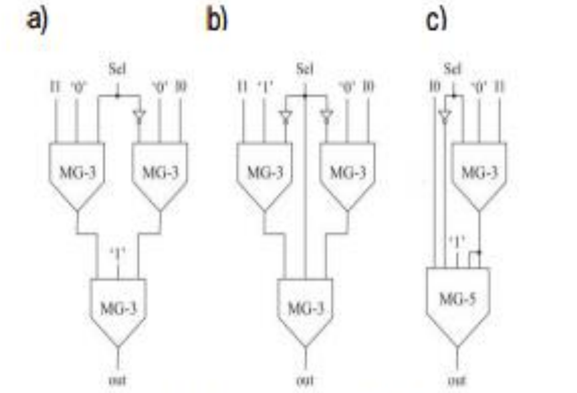


Fig. 6. QCA gate-level designs for *2:1* multiplexer (a) first design using 3 three-input majority gates (b) QCA-compatible design using three-input majority gates (c) alternate QCA-compatible design using three-input and five-input majority gates.

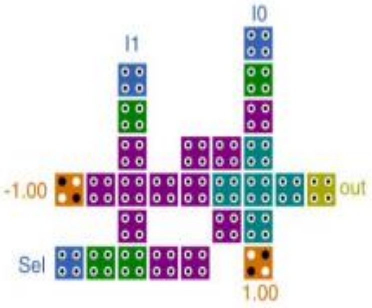


Fig. 7. Proposed QCA layout (M1) of the *2:1* multiplexer employing Gate level method based on the design shown in Fig. 6(c).

According to the flow chart shown in FIG. 4, it is important to select an appropriate wiring intersection for the structural interconnectivity after selecting the appropriate gate level design and the required QCA structure. As shown in Figure 7 for the purpose of reducing the complexity of the circuit, we chose the appropriate connection between the majority of the gates. B. Cell Level PPDD Method In the second design method of PPDD, the first priority block is executed using a new cell order without resorting to the traditional schema of the QCA circuit. The cell level method performs circuit function using clear interaction of the QCA cell. However, this implementation method can take a long time, but the generated layout has superior characteristics compared to the application of the gate level method. In fact, in this way, there is no obligation to use the basic QCA structure to get the correct performance. A comprehensive comparison between QCA 2: 1 multicast and the proposed schema is based on different methods in the second part of this study. We evaluate migration time, number of cells, cross type and area occupation of each circle as an important evaluation scale. In the next step you need to design and implement other priority blocks using the PPDD level or gate level method after enforcing the first phase of the preferential building block at the primary level and applying the organized time recording. By combining the QCA layout of the priority structure with the second priority block, the initial plan of the target circle is determined. Finally, with the proper wiring crossing approach, you need to apply the appropriate clock to the generated layout. The second part of this survey provides a case study to integrate 2: 1 multiplexing units into SRAM memory as the only priority basic building block. Therefore, the cell positions of the first and second blocks can be achieved immediately after the design of the 2: 1 multiplexer.

III. CONCLUSION

In this research, we propose QCA's priority analysis design method (PPDD). In this methodology, after dividing the harmonic and sequential circuit into a primary priority block containing the MUX and XOR 2: 1 interface and a secondary level priority block incorporating a plurality of input multiple gates, each block is used to obtain the desired Priority level to constitute QCA circle.

REFERENCES

[1] P. D. Tougaw and C. S. Lent, "Logical devices implemented using quantum cellular automata," Journal of Applied physics, vol. 75, pp. 1818-1825, 1994.

[2] C. S. Lent and P. D. Tougaw, "A device architecture for computing with quantum dots," Proceedings of the IEEE, vol. 85, pp. 541-557, 1997.

[3] W. Liu, E. E. SwartzlanderJr, and M. O'Neill, Design of Semiconductor QCA Systems: Artech House, 2013.

[4] W. Liu, S. Srivastava, L. Lu, M. O'Neill, and E. E. SwartzlanderJr, "Are QCA cryptographic circuits resistant to power analysis attack?," Nanotechnology, IEEE Transactions on, vol. 11, pp. 1239-1251, 2012.

[5] S. Sheikhfaal, S. Angizi, S. Sarmadi, M. H. Moaiyeri, and S. Sayedsalehi, "Designing efficient QCA logical circuits with power dissipation analysis," Microelectronics Journal, vol. 46, pp. 462-471, 2015.

[6] S. Srivastava, S. Sarkar, and S. Bhanja, "Estimation of upper bound of power dissipation in QCA circuits," Nanotechnology, IEEE Transactions on, vol. 8, pp. 116-127, 2009.

[7] V. Vankamamidi, M. Ottavi, and F. Lombardi, "Two-dimensional schemes for clocking/timing of QCA circuits," Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, vol. 27, pp. 34-44, 2008.

[8] S. Angizi, E. Alkaldy, N. Bagherzadeh, and K.

Navi, "Novel robust single layer wire crossing approach for exclusive or sum of products logic design with quantum-dot cellular automata," Journal of Low Power Electronics, vol. 10, pp. 259-271, 2014.

[9] K. Kim, K. Wu, and R. Karri, "The robust QCA adder designs using composable QCA building blocks," IEEE transactions on computeraided design of integrated circuits and systems, vol. 1, pp. 176-183, 2007.

[10] Hashemi, M. R. Azghadi, and A. Zakerolhosseini, "A novel QCA multiplexer design," in Proceedings of the International Symposium on Telecommunications (IST '08), pp. 692–696, August 2008.

[11] D. Mukhopadhyay and P. Dutta, "Quantum cellular automata based novel unit 2:1 multiplexer," International Journal of Computer Applications, vol. 43, no. 2, pp. 22–25, 2012.

[12] V. C. Teja, S. Polisetti, and S. Kasavajjala, "QCA based multiplexing of 16 arithmetic & logical subsystems-a paradigm for nano computing," in Proceedings of the 3rd IEEE International Conference on Nano/Micro Engineered and Molecular Systems (NEMS '08), pp. 758–763, Sanya, China, January 2008.

[13] M. Askari, M. Taghizadeh, and K. Fardad, "Digital design using quantum-dot cellular automata (A nanotechnology method)," in Proceedings of the International Conference on Computer and Communication Engineering (ICCCE '08), pp. 952–955, May 2008.

[14] A. M. Chabi, S. Sayedsalehi, S. Angizi, and K. Navi, "Efficient QCA Exclusive-or and Multiplexer Circuits Based on a NanoelectronicCompatible Designing Approach," International Scholarly Research Notices, vol. 2014, 2014.

[15] K. Walus, A. Vetteth, G. Jullien, and V. Dimitrov, "RAM design using quantum-dot cellular automata," in NanoTechnology Conference, 2003, pp. 160-163.

[16] M. A. Dehkordi, A. S. Shamsabadi, B. S. Ghahfarokhi, and A. Vafaei, "Novel RAM cell designs based on inherent capabilities of quantum-dot cellular automata," Microelectronics Journal, vol. 42, pp. 701-708, 2011.

[17] S. Hashemi and K. Navi, "New robust QCA D flip flop and memory structures," Microelectronics Journal, vol. 43, pp. 929-940, 2012.

[18] S. Angizi, K. Navi, S. Sayedsalehi, and A. H. Navin, "Efficient quantum dot cellular automata memory architectures based on the new wiringapproach," Journal of Computational and Theoretical Nanoscience, vol. 11, pp. 2318-2328, 2014.

[19] S. Angizi, S. Sarmadi, S. Sayedsalehi, and K. Navi, "Design and evaluation of new majority gate-based RAM cell in quantum-dot cellular automata," Microelectronics Journal, vol. 46, pp. 43-51, 2015.

[20] M. Kianpour and R. Sabbaghi-Nadooshan, "A Novel Quantum-Dot Cellular Automata X-bit x 32-bit SRAM" Very Large Scale Integration (VLSI) Systems, IEEE Transactions On , In press.

[21] C. Shin, N. Damrongplasit, X. Sun, Y. Tsukamoto, B. Nikoli´c, and T.-J. K. Liu, "Performance and yield benefits of quasi-planar bulk CMOS technology for 6-T SRAM at the 22-nm node," IEEE Trans. Electron Devices, vol. 58, no. 7, pp. 1846–1854, Jul. 2011.

[22] V. Vankamamidi, M. Ottavi, and F. Lombardi, "A line-based parallel memory for QCA implementation," Nanotechnology, IEEE Transactions on, vol. 4, pp. 690-698, 2005.

[23] M. A. Tehrani, F. Safaei, M. H. Moaiyeri, and K. Navi, "Design and implementation of multistage interconnection networks using quantumdot cellular automata," Microelectronics Journal, vol. 42, pp. 913-922, 2011.

[24] A. Fijany and B. N. Toomarian, "New design for quantum dots cellular automata to obtain fault tolerant logic gates," Journal of nanoparticle Research, vol. 3, pp. 27-37, 2001.

[25] A. Imre, G. Csaba, L. Ji, A. Orlov, G. Bernstein, and W. Porod, "Majority logic gate for magnetic quantum-dot cellular automata," Science, vol. 311, pp. 205-208, 2006.

[26] H. Balijepalli, and M. Niamat. Design of a nanoscale Quantum-dot Cellular Automata Configurable Logic Block for FPGAs.Circuits and Systems (MWSCAS), 2012 IEEE 55th International Midwest Symposium on, (2012) 5-8 Aug.

[27] M. Kianpour, and R. Sabbaghi-Nadooshan. A conventional design for CLB implementation of a FPGA in Quantum-dot Cellular Automata (QCA).Nanoscale Architectures (NANOARCH), 2012 IEEE/ACM International Symposium on, (2012) 4-6 July.

[28] V. A. Mardiris, and I. G. Karafyllidis. Design and simulation of modular 2 n to 1 quantum-dot cellular automata (QCA) multiplexers. Int. J. Circ. Theor. Appl. 38, 771 (2010).

[29] C. Nagendra, R. Owens, and M. Irwin, "Power-delay characteristics of CMOS adders," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 2, pp. 377–381, 1994.

[30] A. Chandrakasan, S. Sheng, and R. Brodersen, "Low-power CMOS digital design," IEEE J. Solid-State Circuits, vol. 27, pp. 473–484, 1992.

[31] V. Pudi and K. Sridharan, "Low complexity design of ripple carry and Brent-Kung adders in QCA," IEEE Trans. Nanotechnol., vol. 11, pp. 105–119, 2012.

[32] L. Lu, W. Liu, M. O'Neill, and E. E. Swartzlander, "QCA systolic array design," Computers, IEEE Transactions on, vol. 62, pp. 548-560, 2013.

[33] D. Y. Feinstein and M. A. Thornton, "ESOP transformation to majority gates for quantum-dot cellular automata logic synthesis," in Proc. of the Reed-Muller Workshop (RMW), 2007, pp. 43-50.

[34] G. Cocorullo, P. Corsonello, F. Frustaci, and S.

Perri, "Design of efficient QCA multiplexers," International Journal of Circuit Theory and Applications, 2015.

[35] S. Perri and P. Corsonello, "New methodology for the design of efficient binary addition circuits in QCA," Nanotechnology, IEEE Transactions on, vol. 11, pp. 1192-1200, 2012.