

Low-Cost Synthesis Approach for Reversible Authenticator Circuits in QCA Environment

Bandan Bhoi¹, Neeraj Kumar Misra^{2*}, Lafifa Jamal³ and Manoranjan Pradhan⁴

^{1,4}Department of Electronics and Telecommunication Engineering, Veer Surendra Sai University of Technology, Burla, India.

²Department of Electronics and Communication Engineering, Bharat Institute of Engineering and Technology, Hyderabad, India.

³Department of Robotics and Mechatronics Engineering, University of Dhaka, Dhaka, Bangladesh.

Received 3 April 2018, Revised 23 December 2018, Accepted 31 December 2018

ABSTRACT

Recently, Quantum-dot Cellular Automata (QCA) based reversible logic circuit has an enormous benefit over CMOS based logic circuit. As a promising technology for Nanoelectronics computing, reversible-QCA has gained more and more attention from researchers around the world. In this paper, a reversible authenticator circuit based on QCA was implemented. This article presents a Nano-authenticator circuit to verify the authenticated and unauthenticated inputs. The proposed QCA designs have been implemented in a different manner from existing designs, which are primarily based on a coplanar design approach. The efficiency of QCA design has been investigated based on parameters such as cell count, area, and latency. Furthermore, missing an additional cell defect of the reversible authenticator has been analyzed, and covers the fault tolerance of 60.41% and 75%, respectively. In addition, the proposed Feynman gate in QCA environment achieves 76.35% area, 12.5% cell count and 95.55% average energy dissipation improvement as compared to the existing layout. Moreover, the new reversible authentication circuit achieves 87.75% cost and 43.54% area improvement in comparison with the previous state-of-art design.

Keywords: Reversible Authentication, Quantum Computing, Minimal, Cellular Automata, Low Cost.

1. INTRODUCTION

Quantum-dot Cellular Automata (QCA) is a nanoscale-based computing paradigm which does not use transistors. QCA circuits are high speed, high-density circuits which consume lower power compared to Complementary Metal-Oxide-Semiconductor (CMOS) logic circuits [1]. CMOS has reached its short channel effect and scaling due to Quantum Mechanical Effect (QME) [2]. Increase in energy dissipation of the CMOS circuit is driven by size and materials. Many Nanocircuits based on QCA has been synthesized for low power and high density [3]. The physical implementation of QCA was first proposed in 1993 and fabricated in 1997 [4]. Energy dissipation is an important factor for the development of digital logic circuit [5].

Nowadays, using advance Nanodevices, the circuits dissipate very low energy. However, as the density of devices increases exponentially, the energy dissipation will play an important role in the next decades. Quantum technology has diverse applications in the domain of Nanoelectronics. Information processing in which there is no loss of data is known as reversible

* Corresponding Author: neeraj.mishra3@gmail.com

computing and the logic gates that execute such task are called quantum logic gates [6]. Reversible and quantum computing are linked to each other because, in quantum technology, all computation must be reversible [7]. Quantum logic information is made of qubit or quantum bit. Digital circuit is constructed from logic gates, whereas quantum computing design is constructed from elemental quantum gates (Controlled-V, Controlled-V+, and CNOT) [8].

This paper aims to synthesis low-cost reversible authenticator based solely on the Feynman Gate (FG). The achievement is based on the comparison of the extracted results with existing works. The achievement of this work is to consider both quantum circuit and physical foreground implementation of authenticator circuit in QCA. Thus, the proposed authenticator layout in QCA improves cost and area, which eventually improves the system reliability of the latest Nanoelectronics devices. While less amount of work for circuit reliability analysis such as a missing cell, additional cell and cell displacement based defect have been available in the literature, there is a lack of robust architecture on their parameters such as complexity, area, and latency. Quantum-dot Cellular Automata Probabilistic (QCAPro) tool is a robust tool which estimates the energy dissipation of QCA Design. In this work, the QCAPro tool was used to calculate the energy estimation results for the proposed reversible authentication circuit. In addition, this study also focuses on understanding the reliability concern in QCA with focus on missing cell defect, additional cell defect, and displacement.

Following are the achievements of the proposed work:

- A low-cost reversible authentication circuit in QCA environment for Nanocomputing application was designed.
- The correct fault pattern of reversible authenticator circuit based on the single and additional missing cell defects in QCA architecture was estimated.
- The energy dissipation parameters of reversible authenticator circuit were estimated.
- The displacement tolerance of reversible authenticator in QCA for loosely and tightly coupled cells was analyzed.
- The displacement tolerance based analysis of loosely coupled cell up to 1nm in the QCA authenticator circuit was applied.
- The cell position success rate of authenticator circuit for tightly coupled cell up to 4.8nm was estimated.

The rest of the paper is arranged as follows. In Section 2, we review the preliminary related to this paper. Section 3, deals with the related work. In Section 4, we implement the Feynman gate in QCA. Framework for authentication matching process is explained in Section 5. Fault detection in authenticator circuit is discussed in Section 6. Energy dissipation is calculated in Section 7. Section 8 deals with the performance parameter analysis. Finally, we conclude the work in Section 9.

2. PRELIMINARIES

Some of the terminologies related to reversible logic and QCA computing are presented in this section. All the terminologies have been reviewed in [9-12].

2.1 Reversible Computing

Definition 2.1: Boolean operation is reversible if every output logic patterns uniquely map to an input logic patterns and vice versa.

Definition 2.2: A reversible network consists of reversible gates and each reversible gate based on Controlled V, Controlled V+, and Controlled NOT. The numbers of elemental quantum gates utilized in the quantum circuit are used for calculation of the quantum cost.

Definition 2.3: A non-reversible Boolean operation $F: \{0,1\}^p \rightarrow \{1,1\}^q$, can also be formed by reversible with the addition of input lines noted as constant input/ ancilla inputs.

Definition 2.4: Toffoli Gate (TG) has three inputs and three outputs. First and second bits are known as control bits that are unchanged by the quantum wire. The third bit is mapped to the control gate. It changes the qubit, if the control bits are fixed to 1, else the qubits are unchanged.

Example 2.1: Toffoli gate: A 3×3 TG is also CCNOT gate. This gate passes the first two inputs in the output side. In Figure 1, dot is a control point and Ex-OR is a control gate if all the control points are set to 1, then control gate changes the bits.

Example 2.2: Reversible 3×3 Toffoli gate output is $P=A$, $Q=B$, and $R=(AB \oplus C)$. It can generate NAND, OR, AND and NOR on the output node. Reversible Peres gate outputs are $P=A$, $Q=(A \oplus B)$ and $R=(AB \oplus C)$. It can generate AND, NOR, XOR, and NOT. The quantum representation of cascaded reversible Toffoli Gate and Peres Gate is shown in Figure 1

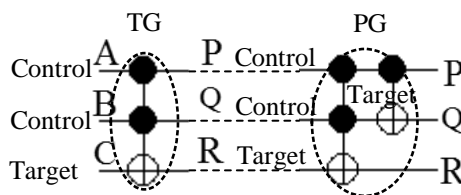
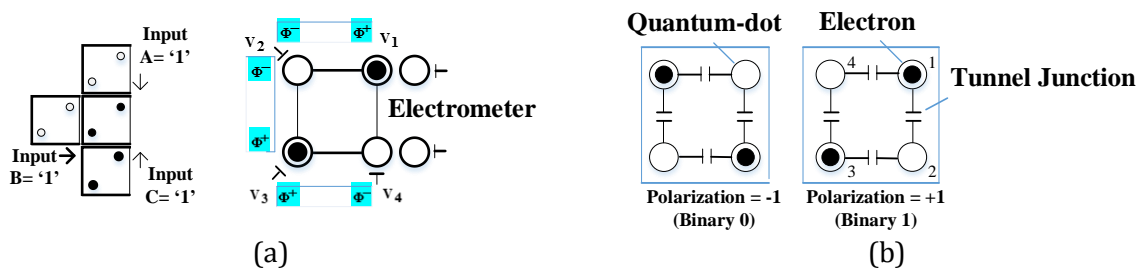


Figure 1. Quantum circuit of TG and PG.

2.2 QCA Computing

The VLSI strategy for circuit design is utilized for CMOS technology. These technologies suffer from high leakage current, limitation of feature size, and scaling limitation [10]. The experimental set-up view of QCA cell is shown in Figure 2a. The QCA technology is one of the newer logic computing with low energy dissipation and high speed. QCA cell is composed of 4 dots with 2 electrons. Two possible polarization states are used, such as $P=+1$ and $P=-1$, for binary 1 and binary 0 respectively, for storing information in the cell (In Figure 2b). Majority gate, fan-out, and inverter design in QCA are depicted in Figures 2c, 2d, and 2e, respectively. QCA design requires a clocking to flow and control the data [11]. The appropriate electric field is required to change the potential barriers [12]. Clock zones activate the data flow computation in a sequential manner [13]. All clocks zones are specified by Switch, Hold, Release and Relax, which is shown in Figure 3. The rotated cells concept in QCA technology is more stable. The advantage of using rotated cells is that wire crossing is possible in the same layer, which requires less area and is more reliable. The rotated and non-rotated cells based wires can cross each other without affecting their logic values in the same plane. If there are no rotated cells in the QCA design, then the crossing of wires can be done using only rotated cells in multilayer. This multilayer crossing leads to more area and less reliability of the design.



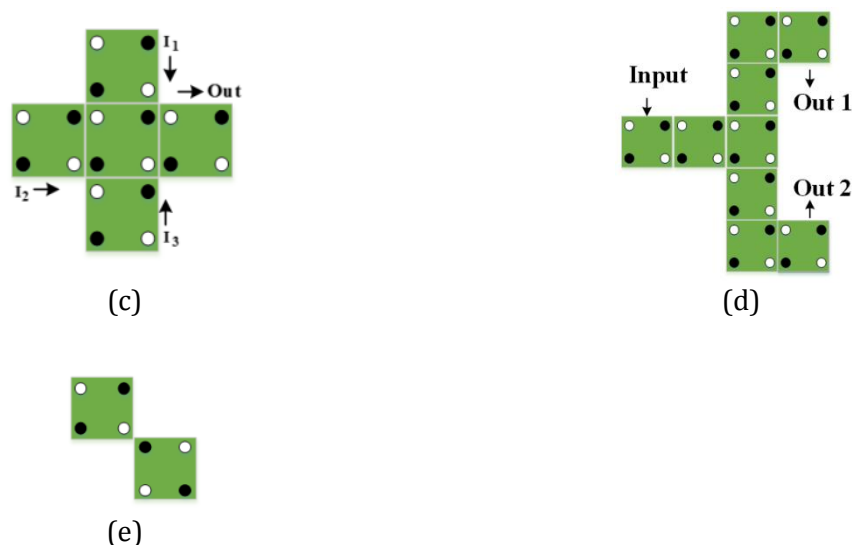


Figure 2. QCA basic: (a) Experimental view of QCA (b) Polarization value in QCA cell (c) Majority gate (d) Fan-out (e) Inverter.

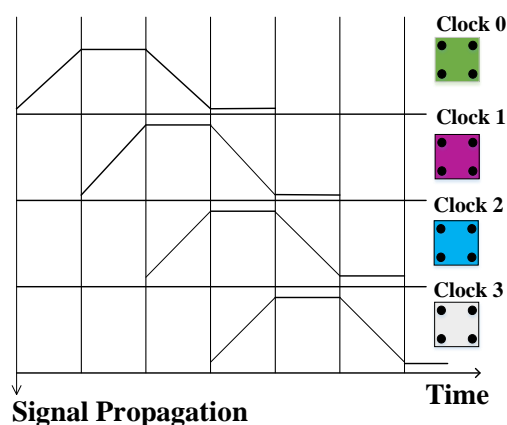


Figure 3. QCA Clocking mechanism.

2.3 QCA Defect

QCA defect has attracted considerable attention in current research for Nanoscale based testing, because of the high possibility of the presence of defects in Nanoscale. These defects are tackled by a testing engineer, which may occur in the chemical synthesis phase. The defect tolerance value usually indicates the reliability percentage of QCA design. Defects can be categorized as cell misalignment, cell displacement, cell missing, extra cell and rotated cells [14]. Some of the QCA defects are described below:

Cell misalignment and displacement-based defect: Each cell in right place structures is shown in Figure 4 (a). Figure 4 (b) and 4 (c) show the QCA defects for the cell incorrectly placed in the position. From the illustration in Figure 4 (b) and 4 (c), it can be said that adjacent cell's distance wrongly placed, the design shows the incorrect logic function.

Cell missing based defect: In Figure 4 (d) cell missing defect have been shown. This kind of defect can be illustrated as when the particular cell position is missing.

Extra cell-based defect: Extra cell makes the design denser because a considerable space is required to place the cell. Also, the functionality of the design is incorrect since the extra cell is randomly found. Figure 4 (e) shows the extra cell model structure.

Drive cell rotated based defect: In Figure 4 (f), the drive cell is rotated. The model structure is incorrectly configured, with drive, and cell rotated. Then, the design results in incorrect functionality.

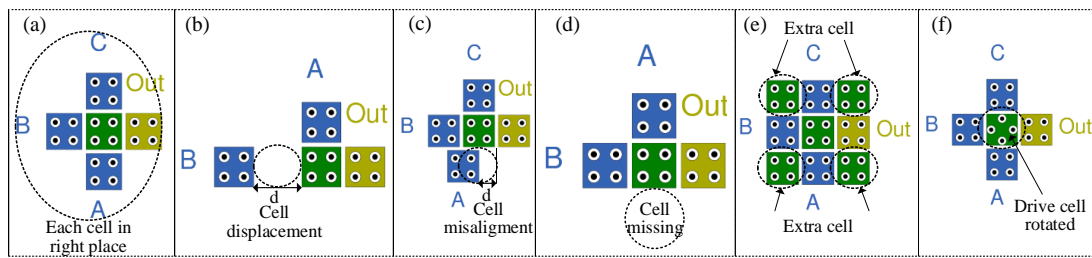


Figure 4. QCA fault (a) no fault in majority gate (b) cell displacement fault (c) cell misalignment fault (d) cell missing fault (e) extra cell fault (f) drive cell rotated fault.

3. RELATED WORK

Due to the advancement in Nanoelectronics technology, high-speed Nanoelectronics circuits are becoming more popular [15]. Parameters of reversible-QCA such as garbage output, quantum cost, complexity, area, and latency are used for optimization of the circuits [16]. However, their testing of Nanocircuit is still a major concern [17]. Missing cell defect, additional cell defect, and displacement cell defect are common faults in QCA terminology. In order to increase the circuit reliability, testing is performed in the proposed authenticator circuit. The authors in [18] have designed data path selector using multiplexer and demultiplexer as an innovative way of path selector. In addition, the design has been implemented in QCA. Three modules such as demultiplexer, crossbar, and parallel-to-serial converter implement the structure of Nano-router [19]. In this work, the proposed design was realized by QCA technology using a four-clock zone scheme.

The existing work in [20] has presented reversible authentication using Fredkin gate. In [20] the quantum cost for authentication using Fredkin and NOT gate have mentioned [6]. In [21], a reversible fingerprint authenticator QCA design was implemented to verify the authentication results. However, no testability features for authentication originated from the state-of-art technology. The existing QCA layout of authenticator requires more cell count, latency and area. By considering all these issues, the proposed design has been optimized in a more efficient way by novel architecture and testability feature. The design, presented in this work, have been implemented by Feynman Gate (FG), which results in low QCA primitives such as area, cell count, and latency. The proposed QCA architecture of authenticator circuit has a less cell count, area, and latency than existing approach while providing the same circuit functionality.

4. REVERSIBLE FEYNMAN GATE (FG)

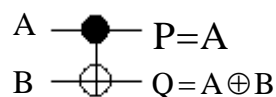


Figure 5. Quantum circuit of FG.

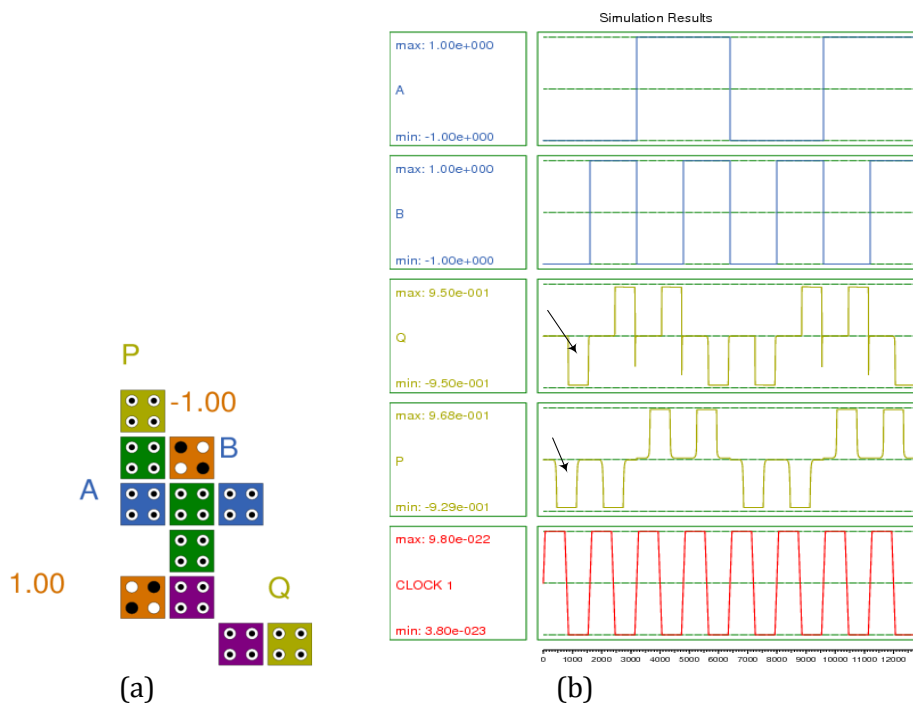


Figure 6. FG: (a) Cell layout (b) Simulation result.

In the synthesize of the authenticator, the FG was utilized as the building block. It maps bijective maps of inputs to outputs as (A, B) to $(A, A \oplus B)$. The quantum circuit of the FG is shown in Figure 5. The FG in QCA layout uses eleven cell count and obtained the output Q after 0.5 clock cycle delay. Figure 6 presents the layout and simulation results of FG. Bistable-approximation simulation engine was selected to simulate the FG layout result presents in Figure 6b. To measure the effectiveness of layout in QCA, the existing layout in [20, 21] was considered. Table 1 presents the comparative results based on QCA primitives such as number of the inverters, number of majority gates, cell count, area and latency. The proposed authentication circuit in QCA only uses two clock zones. The QCA layout consumes only 11 cells, $0.0174\mu\text{m}^2$ area, and 0.5 latency. Table 1 shows the comparative results based on the proposed design and existing designs.

Table 1 New cell layout of utilizing gate in authentication against prior cell layout

Cell layout	Majority	Inverter	Complexity	Cell area	Total Area (μm^2)	Latency
Proposed	1	1	11	0.0035	0.0174	0.5
[20]	3	2	37	0.0148	0.0352	0.75
[21]	6	2	88	0.035	0.098	0.75
% improvement w.r.to [20]		50%	70.27%	76.35%	50.56%	33.33%
% improvement w.r.to [21]		50%	87.5%	90%	82.24%	33.33%

5. THE FRAMEWORK OF PROPOSED AUTHENTICATOR

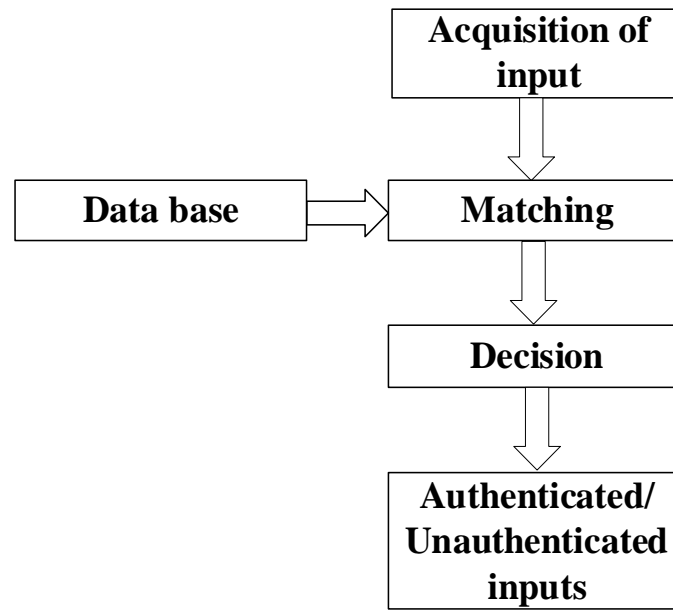


Figure 7. Block diagram of a typical authenticated verification system.

Authenticator matching is a system that determines the acquisition of inputs with a store input accumulated in the database [21]. A complete block diagram of the authenticator matching system is shown in Figure 7. In the authenticator matching system, the database is obtained in the user collection phase. After that, the matching process takes place through the acquisition of inputs. Such inputs must be processed in a matching block. After the processing of the inputs, the decision block will be utilized with the template database. Finally, a result is obtained with the logic bits to ensure the authenticity of the inputs.

5.1 Proposed Design and Simulation Results

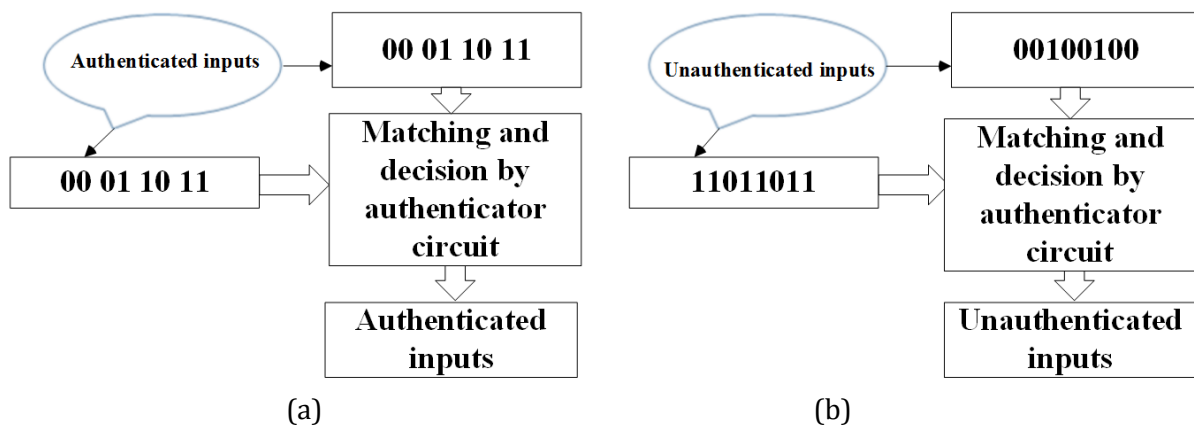


Figure 8. Working of authentication process: (a) authenticated inputs (b) unauthenticated inputs.

The proposed circuit is based on the reversible logic gates. Reversible FG and NOT gates are utilized for the authentication circuit. Reversible FG is used and inputs are assigned to find the authenticated output. The complete block diagram of this authentication approach is presented in Figure 8.

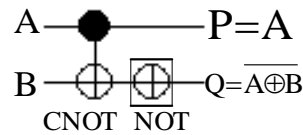


Figure 9. Synthesis of authenticator circuit with FG and NOT gate.

For the synthesis of the authenticator circuit, FG and NOT gates are utilized. The building block of the authenticator circuit based on FG and NOT gate is shown in Figure 9. The output of the authenticator logic circuit is obtained by the second output. It is analyzed that this circuit requires an only two quantum cost.

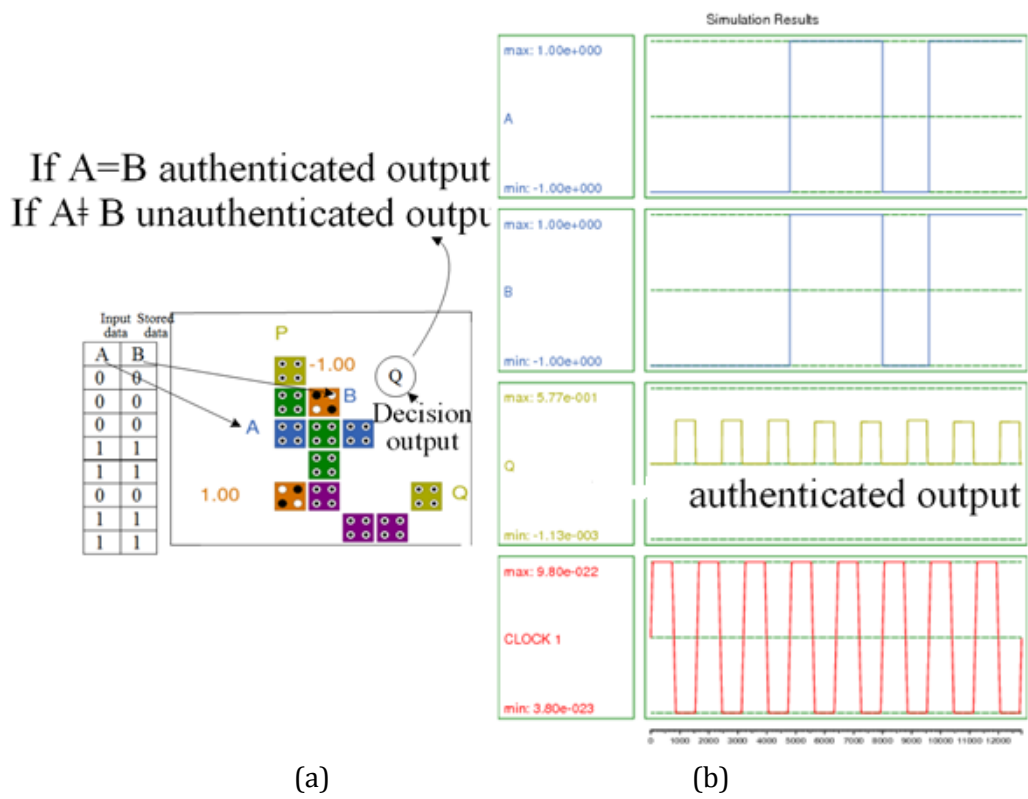
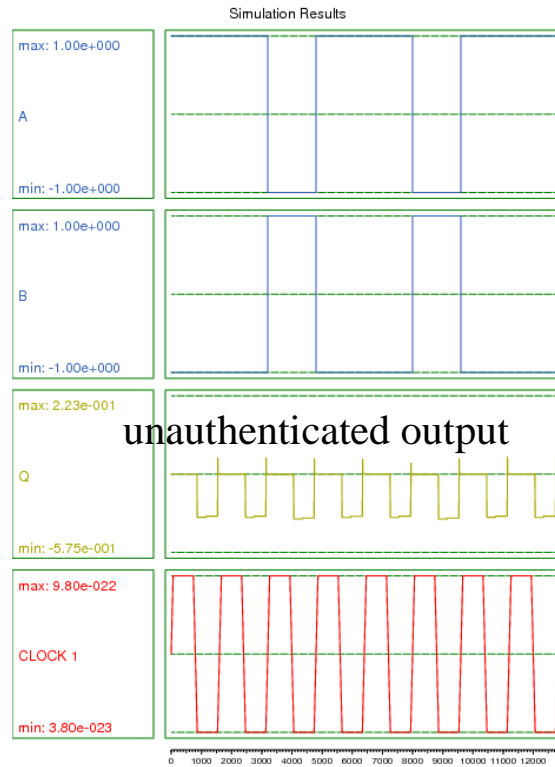
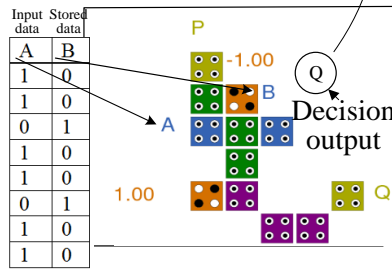


Figure 10. Authenticator Output: (a) Cell layout of authenticator circuit (b) Simulation result of the authenticator circuit based on inputs A(00011011) and B(00011011).

If $A=B$ authenticated output
 If $A \neq B$ unauthenticated output



(a)

(b)

Figure 11. Unauthenticator Output: (a) Cell layout of authenticator circuit (b) Simulation result of the unauthenticated circuit based on inputs A(11011011) and B(00100100).

Authenticator based on reversible gates has been implemented in QCA by using one inverter (INV 1) and proposed Feynman gate in Figure 10(a). The authenticator design consists of 12 cells covering the footprint area of $0.12\mu\text{m}^2$. Simulation setting of the Bistable engine was used to simulate the authenticator design. The authenticator circuit based on input A(00011011) and stored data B(00011011) is shown in Figure 10(b). The other input A(11011011) and stored data B(00100100) generate the unauthenticated output in a binary form as shown in Figure 11(a) and 11(b). The Q output is used to present the unauthenticated output. The two examples are pointed in random cases and the test outputs represent the authenticated and unauthenticated logic of the QCA design based on the FG and inverter gate. Authenticated and unauthenticated inputs for the proposed circuits were analyzed, and the inputs patterns in two cases were considered. The first case takes the input A as 11011011 and matches the stored data B i.e. 11011011. In simulation result, Q output is 11111111. If there is no '0' bit in Q, then A is authenticated input. Figure 10(b) shows the results under inputs 11011011 and stored data 00100100. This QCA level circuit is presented in Figure 11(a). The unauthenticated outputs are presented by simulation results of Figure 11(b). In simulation result, Q is 00000000. If any bit is '0' in Q value then input A is considered as unauthenticated. In this case, A is unauthenticated input.

6. DEFECT ANALYSIS OF THE PROPOSED AUTHENTICATOR QCA LAYOUT

6.1 Missing and Additional Cell Defects in Proposed QCA Architecture

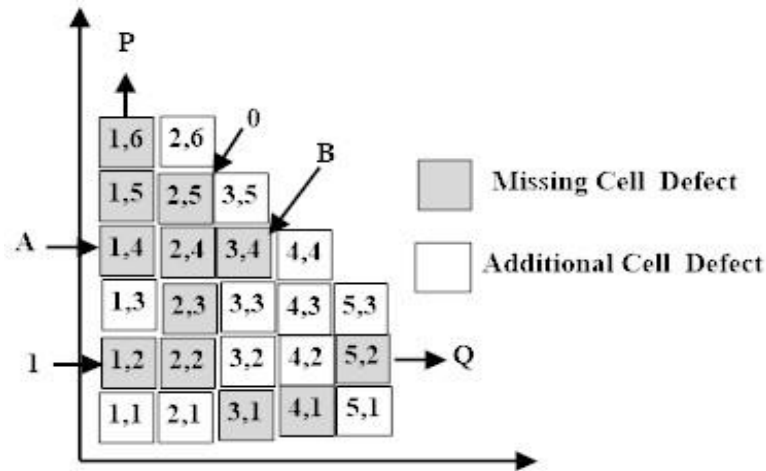


Figure 12. Cell deposition defects of reversible authentication circuit.

The missing and additional cell defects of faulty FG are depicted in Figure 12 where all cells are numbered according to the coordinates. Missing cell defects are possible for all 12 numbers of cells for the proposed QCA authenticated circuit. Similarly, 12 numbers of additional cell defects are possible in the proposed layout. The functionality of the circuit is verified in presence of all possible missing and additional cell defects in QCA Designer tool. The results are summarized in Table 2 and Table 3. In both tables, the first column specifies the input test vectors for A and B. On the other hand, only Q output is considered for fault tolerance analysis because it is the decision output of the proposed layout of the authenticator. In Table 2, the value of Q is specified for all possible missing cell faults from column no. 2 to 12. Similarly, in Table 3, Q outputs are given for all additional cell-based defects. In both tables, the last column indicates the correct patterns out of total patterns in presence of faults. The average correct patterns for missing cell defects are 60.41%, whereas it is 75% for additional cell defects. The average fault tolerance value is 67.70% (i.e. $(60.41\% + 75\%) / 2$) in presence of these defects. Therefore, under single missing cell and additional cell defects, the probability of having the correct decision output for the proposed authenticator is 67.70%.

Table 2 Fault tolerant analysis of missing cell defects

A B	(1,2)	(1,4)	(1,5)	(1,6)	(2,2)	(2,3)	(2,4)	(2,5)	(3,1)	(3,4)	(4,1)	(5,2)	correct patterns
0 0	0	1	1	1	0	1	1	1	0	1	0	0	7/12 = 58.33%
0 1	0	1	0	0	0	1	1	1	0	1	0	0	7/12 = 58.33%
1 0	0	1	0	0	1	1	1	1	0	1	0	0	6/12 = 50%
1 1	1	1	1	1	1	1	1	1	0	1	0	0	9/12 = 75%

Avg. =60.41%

Table 3 Fault tolerant analysis of additional cell defects

A B	(1,1)	(1,3)	(2,1)	(2,6)	(3,2)	(3,3)	(3,5)	(4,2)	(4,3)	(4,4)	(5,1)	(5,3)	correct patterns
0 0	1	1	0	1	0	1	1	0	1	1	0	1	8/12 = 75%
0 1	0	1	0	0	0	1	0	1	0	0	1	0	8/12 = 75%
1 0	0	1	0	0	0	1	0	1	0	0	1	0	8/12 = 75%
1 1	1	1	0	1	0	1	1	0	1	1	0	1	8/12 = 75%

Avg. =75%

6.2 Displacement Tolerance for the Proposed Authenticator

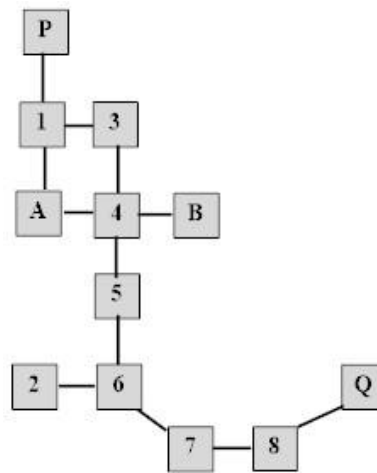


Figure 13. Representation of Authenticator layout with nodes.

Besides missing cells and additional cells, the relative position of cells or cells displacement also has some impact on the structure. Therefore, the fault tolerance of the displacement of cells from its original position plays a vital role in the fabrication of error-free circuits. For the analysis of displacement behaviour, the layout is described by using nodes as shown in Figure 13. The cells shown in the Figure are divided into two categories based on the connection with the driver cell, i.e. loosely and tightly coupled cells. A cell is called loosely coupled if it is connected to one or two cells, similarly if a cell is connected to more than two numbers of cells is known as tightly coupled. The tightly coupled cells have a greater influence on the circuit than do loosely coupled cells. The maximum displacement of the cells in all directions beyond which the circuit will not perform correctly is reported in Table 4. In Table 4, displacement fault-tolerance is measured for Q output. The average value of cell displacement fault-tolerance of loosely coupled cells is 1nm. This value is 4.8nm for tightly coupled cells.

Table 4 Displacement tolerance of cells of the authenticator

Cell position (nm)	Success rate	Loosely coupled cell								
		3	A	2	5	7	8	B	Q	Avg.
		0.8nm	1.6nm	0nm	0.3nm	0.2nm	1.3nm	0.2nm	3.6nm	1nm

Cell position (nm)	Success rate	Tightly coupled cell			
		1	4	6	Avg.
		14nm	0.5nm	0nm	4.8nm

7. ENERGY DISSIPATION ANALYSIS IN DIFFERENT TUNNELING LEVELS OF ENERGY

In order to measure the energy dissipation of new authentication circuits, QCAPro tool was used to estimate the energy dissipations parameters. The energy dissipations parameters and the thermal map were obtained by QCAPro tool after the successful simulation of QCA design. The energy dissipation parameters are obtained for selection of energy level at a temperature of 2K, as presented in Table 5. Further, the extracted parameters such as Avg. Switching Energy diss., Avg. Energy diss. of circuit, Avg. Leakage Energy diss. at three levels of tunnelling energy such as $0.5E_k$, $1E_k$, and $1.5E_k$ of the proposed design and existing designs are presented in Table 5. As per the Table 5, it is shown that the newly authentication design dissipate 80.32% less Avg. Switching Energy diss., 75.80% Avg. Energy diss. of the circuit, and 63.32% Avg. Leakage Energy diss. at $0.5E_k$. It is proved that we have attained an optimal value of power dissipation. It ensures that the proposed design achieves the low lost Nanocircuits feature.

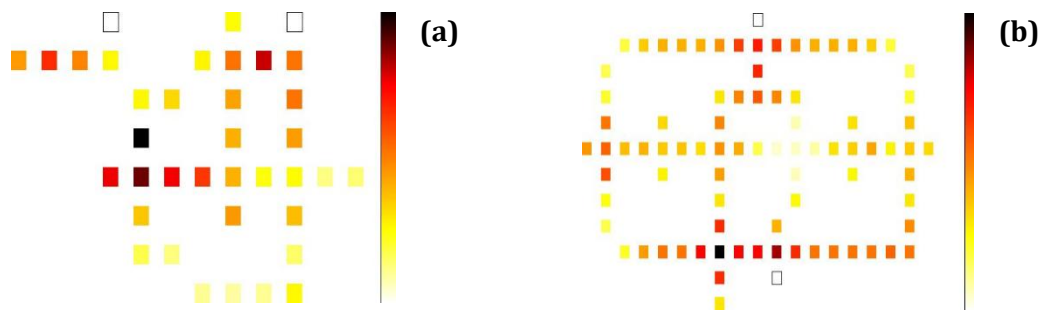


Figure 14. Power dissipation map for the existing QCA architecture with $0.5E_k$ (a) Authentication circuit #1 in [20] (b) Authentication circuit #2 in [21].

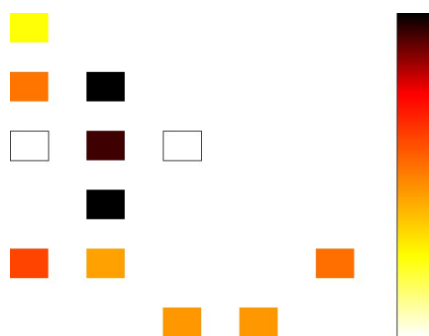


Figure 15. Power dissipation map for the proposed QCA authentication with $0.5E_k$.

Table 5 Energy dissipation analysis of authentication circuit in different tunneling levels of energy

Design	Avg Switching Energy diss. (meV)			Avg Energy diss. (meV)			Avg Leakage Energy diss. (meV)		
	0.5E _k	1E _k	1.5E _k	0.5E _k	1E _k	1.5E _k	0.5E _k	1E _k	1.5E _k
Proposed	0.0055 5	0.0046 0	0.0038 5	0.0105 3	0.0167 1	0.0234 6	0.0049 8	0.0121 1	0.0196 1
[20]	0.0282 1	0.0238 6	0.0199 6	0.0417 9	0.0614 0	0.0842 1	0.0135 8	0.0375 4	0.0642 6
[21]	0.1258 5	0.1108 6	0.0960 3	0.1503 3	0.1857 9	0.2310 9	0.0244 8	0.0749 3	0.1350 6
% Improvement w.r.to [20]	80.32	80.72	80.71	75.80	72.78	72.14	63.32	67.74	69.22
% Improvement w.r.to [21]	95.55	95.85	95.99	92.99	91.10	89.88	79.65	83.79	85.48

In the dissipation map of existing authentication circuit in [20, 21], the lighter cells dissipate less energy and darker cells dissipate higher energy, which is shown in Figures. 14 and 15. These thermal maps were obtained after the simulation of QCA design by the QCAPro tool. The energy dissipation parameters of the existing QCA authentication [20, 21] and proposed circuit in with 0.5E_k is shown in Table 5. The power dissipation map of the proposed authentication is measured in standard tunnelling energy levels at 0.5E_k. According to Figure 15, it is observed that the presented authentication thermal have fewer darker cells (3 cells out of 12) to ensure less energy dissipation.

8. PERFORMANCE PARAMETER COMPARISON

Performance comparison is a key parameter to check the synthesis of the circuit. The implemented design in [20] requires six quantum cost. Existing design based on Fredkin and inverter gate introduces delay as per the counting of the quantum gate in the quantum circuit. According to the comparison Table 6, the new design for the authenticator circuit utilizes FG, which has less cell count, area, and latency as compared to the state-of-art designs. The proposed design of reversible authentication in QCA framework benefits from a low cost related to QCA. It is worth studying that low latency corresponds to less cell count and crossover. The comparison of the new and prior circuit can be evaluated easily with the support of performance analysis of authenticator circuit in Table 6. From Table 6, it is clear that the proposed design latency, total area, cell area are 33.33%, 74.61%, and 88.48% respectively, as compared to the existing design in [20, 21]. Therefore, after comparing all the existing designs in [20, 21], it is noticeable that the performance of proposed authenticator QCA layout with a feature in QCA primitives gives the cost-efficient approach. To determine the overall performance of the authenticator designs, the $Cost=Latency^2 \times Total\ area$ is also shown in Table 6 below.

Table 6 Performance comparison analysis of the authenticated circuit

Design	Number of cells	Gate count (Inverter +Maj)	Latency (Clock cycle delay)	Total area in μm^2	Cell area in μm^2	Area usage in %	Cost=Latency ² x Total area
Proposed	12	2+1=3	0.50	0.0231	0.0038	16.45	0.0057
[20]	37	3+3=6	0.75	0.0352	0.0148	42.05	0.0198
[21]	84	6+4=10	0.75	0.0910	0.0330	36.26	0.0511
% Improvement w.r.to [20]	67.56	50	33.33	34.37	74.32	60.87	71.21
% Improvement w.r.to [21]	85.71	70	33.33	74.61	88.48	54.63	88.84

9. CONCLUSION

The important application of authenticator circuit is the information security. In this article, the robust architecture of reversible authenticator was proposed for QCA environment. Total area, latency and cost analysis of new architecture and state-of-art circuits, introduced in this paper, demonstrate that our methodology achieves superior results as far as latency, total area, cell area, and cost are concerned. The article has also presented methods such as missing cell defects, and additional cell defects into a testable Nano-authentication circuit and experimentally presented 60.41% and 75% correct patters. Moreover, the displacement tolerance of the proposed authenticator in QCA was analyzed and found that the tightly coupled cells have a greater influence on the circuit compared to the loosely coupled. The robustness of proposed authenticator circuit in QCA was examined in terms of missing cell defect, additional cell defect, and displacement defect. The proposed Feynman-gate-based synthesis of the authentication circuit consume 75.80% less avg. switching energy dissipation., and 63.32% avg. energy dissipation, compared to its state-of-art designs counterpart. The future direction of this work is to work with the HDL approach for fault testing, which will cover maximum fault tolerance capability based on software simulation and synthesis method [1, 22].

REFERENCES

- [1] Zaid Alwardi, Robert Wille & Rolf Drechsler. "Synthesis of Reversible Circuits Using Conventional Hardware Description Languages." In 2018 IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL), (2018) 97-102.
- [2] Bandan Kumar Bhoi, Neeraj Kumar Misra & Manoranjan Pradhan. "Novel Robust Design for Reversible Code Converters and Binary Incrementer with Quantum-Dot Cellular Automata." In Intelligent Computing and Information and Communication, Springer, Singapore, (2018) 195-205.
- [3] Z Mohammadi & Majid Mohammadi. "Implementing a one-bit reversible full adder using quantum-dot cellular automata." Quantum information processing **13**, 9 (2014) 2127-2147.
- [4] Craig S Lent & P. Douglas Tougaw. "A device architecture for computing with quantum dots." Proceedings of the IEEE **85**, 4 (1997) 541-557.
- [5] JF Chaves, Marco A. Ribeiro, Leandro M. Silva, Leonardo MBC de Assis, Marzo S. Torres & Omar P. Vilela Neto. "Energy efficient QCA circuits design: simulating and analyzing partially reversible pipelines." Journal of Computational Electronics **17**, 1 (2018) 479-489.
- [6] Himanshu Thapliyal, Nagarajan Ranganathan & Saurabh Kotiyal. "Design of testable reversible sequential circuits." IEEE transactions on very large scale integration (VLSI) systems **21**, 7 (2013) 1201-1209.

- [7] Neeraj Kumar Misra, Bibhash Sen & SubodhWairya. "Towards designing efficient reversible binary code converters and a dual-rail checker for emerging nanocircuits." *Journal of Computational Electronics* **16**, 2 (2017) 442-458.
- [8] Hafiz Md. Hasan Babu, Nazir Saleheen, Lafifa Jamal, Sheikh Muhammad Sarwar & Tsutomu Sasao. "Approach to design a compact reversible low power binary comparator." *IET Computers & Digital Techniques* **8**, 3 (2014) 129-139.
- [9] Himanshu Thapliyal & Nagarajan Ranganathan. "Reversible logic-based concurrently testable latches for molecular QCA." *IEEE transactions on nanotechnology* **9**, 1 (2010) 62-69.
- [10] Z Mohammadi, Majid Mohammadi, and Mahdi Hasani. "Designing of testable reversible QCA circuits using a new reversible MUX 2×1 ." (2012) 51-64.
- [11] Bibhash Sen, Manojit Dutta, Mrinal Goswami & Biplab K. Sikdar. "Modular design of testable reversible ALU by QCA multiplexer with increase in programmability." *Microelectronics Journal* **45**, 11 (2014) 1522-1532.
- [12] K Kim, Kaijie Wu & Ramesh Karri. "The robust QCA adder designs using composable QCA building blocks." *IEEE transactions on computer-aided design of integrated circuits and systems* **26**, 1 (2007) 176-183.
- [13] Hennessy, Kevin & Craig S. Lent. "Clocking of molecular quantum-dot cellular automata." *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures Processing, Measurement, and Phenomena* **19**, 5 (2001) 1752-1755.
- [14] Tahoori, Mehdi B., Jing Huang, Mariam Momenzadeh & Fabrizio Lombardi. "Testing of quantum cellular automata." *IEEE Transactions on Nanotechnology* **3**, 4 (2004) 432-442.
- [15] Askari, Mehdi, Maryam Taghizadeh & KhossroFardad. "Digital design using quantum-dot cellular automata (a nanotechnology method)." In *Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on, IEEE, (2008)* 952-955.
- [16] Lafifa Jamal, Md. Masbaul Alam & Hafiz Md Hasan Babu, "An efficient approach to design a reversible control unit of a processor." *Sustainable Computing: Informatics and Systems* **3**, 4 (2013) 286-294.
- [17] Bibhash Sen, Anirban Nag, Asmit De & Biplab K. Sikdar. "Towards the hierarchical design of multilayer QCA logic circuit." *Journal of Computational Science* **11** (2015) 233-244.
- [18] S Das & Debashis De. "Nanocommunication using QCA: a data path selector cum router for efficient channel utilization." In *Radar, Communication and Computing (ICRCC), 2012 International Conference on, IEEE, (2012)* 43-47
- [19] LHB Sardinha, Artur MM Costa, Omar P. Vilela Neto, Luiz FM Vieira & Marcos AM Vieira. "Nanorouter: A quantum-dot cellular automata design." *IEEE Journal on Selected Areas in Communications* **31**, 12 (2013) 825-834.
- [20] B Debnath, Jadav Chandra Das & Debashis De. "Fingerprint authentication using QCA technology." In *Devices for Integrated Circuit (DevIC), IEEE, (2017)* 125-130.
- [21] J.C Das & Debashis De. "User authentication based on quantum-dot cellular automata using reversible logic for secure nanocommunication." *Arabian Journal for Science and Engineering* **41**, 3 (2016) 773-784.
- [22] Mustapha Y Abu bakar, Low Tang Jung, Nordin Zakaria, Ahmed Younes & Abdel-Haleem Abdel-Aty. "Reversible circuit synthesis by genetic programming using dynamic gate libraries." *Quantum Information Processing* **16**, 6 (2017) 160.

