# Review on Random Number Generator design using Quantum Dot Cellular Automata

Nilima P. Pannase[1], Amol Boke[2]
[1]*M.Tech Student G.H.R.A.E.T, Nagpur*
[2]*Asst. Professor G.H.R.A.E.T, Nagpur*

***Abstract-*** **Quantum dot cellular automata is a popular nanotechnology which can overcome the limitations of CMOS technology due to its extremely small feature size and ultra low power consumption. In this paper we proposed the design of random number generator using Quantum dot cellular automata technology .In Quantum Dot Cellular Automata the basic elements are simple cells. The cells are used to construct majority voter gate, inverter and wire which are used to realize any complex function. In the given design, random number generator unit is constructed using a VHDL model of QCA elementary circuits which provides an approach to improve the complexity and system throughput of Random Number Generator.**

***Index Terms-*** **Quantum Dot Cellular Automata (QCA), Random Number Generator (RNG), VHDL, Majority voter Gate (MVG)**

## I . INTRODUCTION

Random number generators are key primitive for the variety of applications simulation, game playing, cryptography statistical sampling, evaluation etc. In many applications, it is desirable to optimize performance of the RNGs in terms of speed, area, and power dissipation, while producing high-quality random numbers.

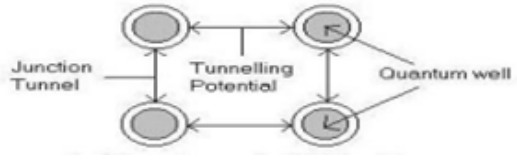
As the size of CMOS transistors keep shrinking, it will eventually hit its limitation. Hence, an alternative device has to be discovered to continually improve the development of electronics devices. Quantum-dot Cellular Automata (QCA) has been seen as a possible alternative to the current CMOS circuits. QCA devices show great promise to be faster and smaller than conventional microelectronic devices, and to operate at a fraction of the power. In this paper we proposes the design of RNG using QCA technology and will compare the different performance parameters with the RNG implemented using QCA technology.

## 1. QUANTUM DOT CELLULAR AUTOMATA (QCA)

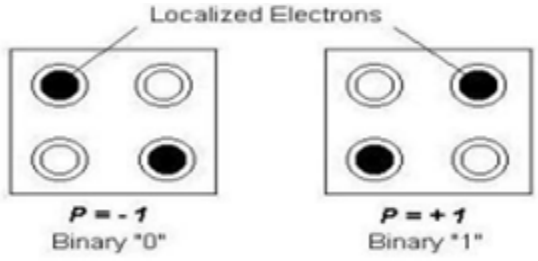
QCA was first proposed by Lent et.al in 1993 and as developed in 1997 [5]. It is expected that QCA plays an important role in nanotechnology research. QCA architecture is based on the coulombic interactions between many identical QCA cells. QCA technology consists of a group of cells which, when combined and arranged in a particular way, are able to perform computational functions. QCA technology transfers information by means of the polarization state of various cells in contrast to traditional computers, which use the flow of electrical current to transfer information. A QCA design provides advantages such as ultra-small factor, low power consumption and high speed clock circuits. QCA clock rate could be in the range of 1-2 THz[7] .

### A. QCA Cell :

QCA is based on the interaction of bi-stable QCA cells constructed from four quantum-dots. A high-level diagram of two polarized QCA cells is shown in Fig. 1. Each cell is constructed from four quantum dots arranged in a square pattern. The cell is charged with two electrons, which are free to tunnel between adjacent dots. These electrons tend to occupy antipodal sites as a result of their mutual electrostatic repulsion. Thus, there exist two equivalent energetically minimal arrangements of the two electrons in the QCA cell as shown in Fig. 1(b). These two arrangements are denoted as cell polarization P = + 1 and P = -1 respectively. By using cell polarization P = +1 to represent logic "1" and P = -1 to represent logic *"0"* ,binary information can be encoded.




(a)Structure of QCA cell




(b) Representing a binary digit with the help of two different polarizations of the localized electron

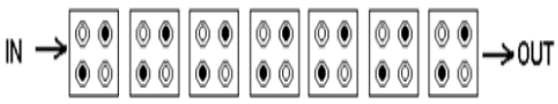
Fig 1 QCA Cell

Arrays of QCA cells can be arranged to perform all logic functions. This is due to the Columbic interactions, which influences the polarization of neighboring cells. QCA architectures have been proposed with potential barriers between the dots that can be controlled and used to clock QCA circuits.

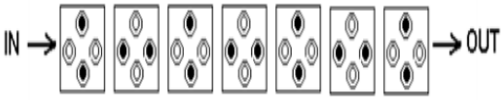
B. QCA Logical Devices :

The fundamental QCA logic devices are the QCA wire, majority gate and inverter.

(a )QCA Wire*:* In a QCA wire, the binary signal propagates from input to output because of the electrostatic interactions between cells. The propagation in a $90^0$ QCA wire is shown in Fig.2. Other than the $90^0$ QCA wire, a $45^0$ QCA wire can also be used. In this case, the propagation of the binary signal alternates between the two polarizations.




(a) QCA wire ($90^0$)




(a) QCA wire ($45^0$)

Fig 2. Information propagation through QCA wires

(b )QCA Inverter: A QCA layout of an inverter circuit is shown in Fig. 3. Cells oriented at $45^0$ to each other take on opposing polarization. This orientation is exploited here to create the inverter shown in this figure

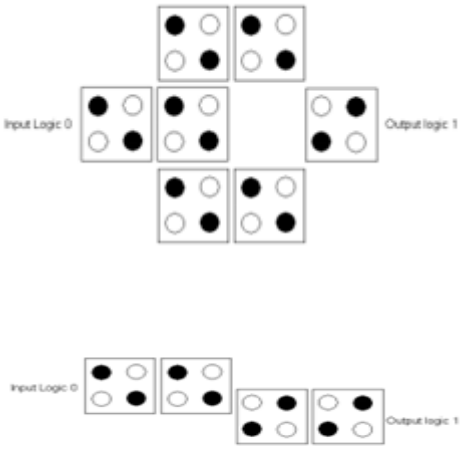


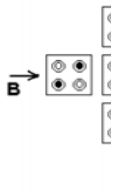

Fig 3. Two different topologies of QCA inverter

(c) QCA Majority voter Gate: The QCA MVG performs a three-input logic function. Assuming the inputs are A ,B and C the logic function of the MVG is

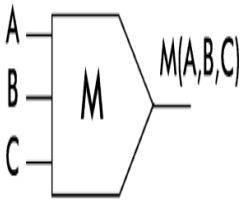
$$M(A,B,C)=AB+BC+AC$$

(a) Truth Table

| A | B | C | MV(A,B,C) |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 |




(b) Cell structure




(c) Representation of Majority voter gate

Fig 4 Majority Voter Gate

## II. LITERATURE REVIEW

David B. Thomas and Wayne Luk [1] implemented LUT optimized (LUT-OPT), LUT – FIFO and LUT –SR random number generator for

FPGA architectures. The LUT-OPT generator uses the absolute minimum resources of one LUT per generated bit, but if we wishes to use all 1024 generated bits it is far less efficient than the LUT-SR-1024, the LUT-FIFO generator can provide very long periods , but requires the use of a block RAM while the FIFO in a LUT-FIFO RNG is usually an expensive block RAM. In new LUT-SR generator LUTs are configured as shift registers. Configuring LUTs as shift registers provides an attractive means of adding more storage bits to a binary linear generator which provides a useful mid-point between the two, with a good balance between resource utilization and good quality .

LDPC decoder implemented by Muhammad Awais, Marco Vacca, Mariagrazia Graziano, Massimo Ruo Roch and Guido Masera [4]using VHDL model of QCA elementary circuit. In VHDL model ,for each clock phase a register is used to model the propagation delay, while ideal wire and gates (majority voters and inverters) with no delay are used to model the logic behavior of the circuit. The performance of LDPC decoder using CMOS and QCA technology are compared on the basis of different parameters like area ,power dissipation which shows that QCA technology can be use to implement applications characterized by very high processing complexity

Lee Ai Lim, Azrul Ghazali, Sarah Chan Tji Yan, Chau Chien Fat [2] implemented Sequential circuits such as gated D latch, RS latch, JK flip-flop, T flip-flop, D flip-flop, 2-bit counter, 4-bit counter, and 4-bit shift register in QCA architecture.These circuit are implemented using MVG and after simulation ,size and no of cells required for this circuit are calculated. It has been shown that area required to implement the given sequential circuit is significantly reduced using QCA.

## III. PROPOSED WORK

This paper focuses the comparative study of Random number generator proposed by David B. Thomas and Wayne Luk[1] using CMOS technology and proposed circuit using QCA. In LUT-SR RNG [1] for FPGA implementation LUTS are configured as shift register to provide random bits to EX-OR unit and resulting EX-ORing of input bits efficiently generates random Numbers.

Studies shows that any combinational and sequential circuit can be designed using QCA building block majority voter gate, inverter and wire with minimum complexities in comparison with current transistor based Technology. Flip flops and EX-OR gate which are the key components of RNG can be implemented using QCA. M. Kianpour and R. Sabbaghi-Nadooshan[5] implemented a new 2-input and 3-input XOR gate (exclusive OR gate) based on QCA with the minimum delay, area and complexities. Sequential circuits like flip flops, latches ,counters , shift register ,counter can be efficiently implemented by majority gate from the Boolean equation of the respective digital circuit[2] .The proposed design offers better performance characteristics in terms of speed and area than that of RNG implemented using CMOS technology. It can be further modified to improve the randomness of the Random numbers.

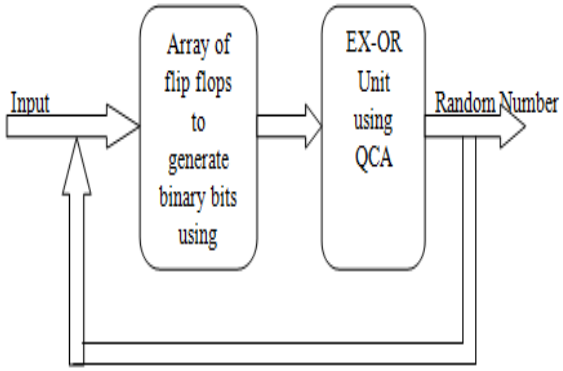



Fig 5. Block Diagram

## IV. CONCLUSION

We will design and simulate the LUT-SR optimized RNG using CMOS and proposed design using QCA in VHDL language with the help of Xilinx tool .As QCA offers faster speed, smaller size, and lower power consumption than transistor-based technology , comparative study of both the designs will show that proposed design offers faster speed , low power consumption and less area for the QCA based RNG.

## REFERENCES

[1] David B. Thomas ,Wayne Luk-The LUT-SR Family Of Random Number Generators For FPGA Architectures *IEEE Transactions On Very Large Integration (VLSI) System 1063–8210/ © 2012 IEEE*

[2] Lee Ai Lim, Azrul Ghazali, Sarah Chan Tji Yan, Chau Chien Fat- Sequential ckt

Design Using Quantum Dot Cellular Automata. *978-1-4673-3119-7/12 ©2012 IEEE*

[3] Jonathan M. Comer, Juan C. Cerda, Chris D. Martinez, and David H. K. Hoe -Random Number Generators using Cellular Automata Implemented on FPGAs *978-1-4577-1493-1/12 ©2012 IEEE*

[4] Muhammad Awais, Marco Vacca, Mariagrazia Graziano Massimo Ruo Roch, and Guido Masera -Quantum Dot Cellular Automata Check Node Implementation for LDPC Decoders *IEEE Transactions On Nanotechnology, Vol. 12, No. 3, May 2013*

[5] M. Kianpour, R. Sabbaghi-Nadooshan -Novel Design of n-bit Controllable Inverter by Quantum-dot Cellular Automata *Int. J. Nanosci. Nanotechnol., Vol. 10, No. 2, June 2014*

[6] R.Nithiyanandham ,S. Charles Lekonard, U.Duraisamy ,V.P. Ahmeed Faheem, V.M Navaneethakrishnan-Adder Design Using QCA Technique with Area Delay Efficient *IJIRSET.2015.0403071*

[7] Abner Luis Panho Marciano, Andre B. Oliveira ,Jose Augusto Miranda Nacif , Omar P. Vilela Neto. -An efficient FPGA implementation in quantum-dot cellular automata *978-1-4799-1132-5/13 ©2013 IEEE*

[8] Rumi Zhang, Konrad Walus, Wei Wang, and Graham A. Jullien-A Method of Majority Logic Reduction for Quantum Cellular Automata *IEEE Transactions On Nanotechnology, Vol. 3, No. 4, December 2004*

.