IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

Random Number Generator Design using QCA Logic for FPGA Architecture

Nilima P. Pannase[1], Amol Boke[2]

M.Tech Student, Department of ECE, G.H.R.A.E.T College, Nagpur, India [1]

Asst. Professor, Department of ECE, G.H.R.A.E.T College, Nagpur, India [2]

Abstract: Quantum-dot cellular automata (QCA) are a technology which has the potential of faster speed, smaller size and minimum power consumption compared to transistor based technology. Random number generators (RNGs) are used in variety of applications including Monte Carlo Application Cryptography, Statistical sampling, Game Playing etc .In many hardware implementations it is desirable to optimize performance of the RNGs in terms of speed and area. To be considered as a suitable CMOS substitute, the QCA technology must be able to implement complex real- time applications with affordable complexity. This project describes improved version of RNG using Quantum Dot Cellular Automata Technique to generate wider variety of random number. In the proposed circuit, RNG unit is constructed using a VHDL model of QCA elementary circuits which provides an approach to improve the complexity of RNG.

Keywords: Quantum Dot Cellular Automata (QCA), Random Number Generator (RNG), VHDL, Field Programmable Gate Array (FPGA), Majority Voter Gate (MVG).

I. INTRODUCTION

Present CMOS based technology faces consequences like leakage current, power dissipation, oxide thickness, electron migration in feature size reduction [4]. The CMOS technology is approaching to its fundamental physical limits and, therefore, facing difficulties to generate ICs in nano-scale regimes. In this view the International Technology Roadmap for Semiconductors has proposed several new technologies [1]. Quantum Dot Cellular Automata is one of the emerging nanotechnology. Quantum-dot cellular automata (QCA) were first introduced in 1993 by Lent et al from the University of Notre Dame. Two are the appealing implementations of QCA: molecular QCA built using complex molecules with many oxide-reduction centers[5] and magnetic QCA based on single domain nanomagnets, with only two stable magnetization states[6]. It is predicted that QCA cells of few nanometer size can be fabricated through molecular implementation and can operate at THZ frequency. A QCA based design can be of high device density, very high switching speed and consumes extremely low power. Many QCA circuits have been proposed in the literature, e.g., simple blocks like multiplexers, more complex arithmetic circuits like adders and multipliers, or dividers, sequential circuits like latches, and memories. Most of the circuits that constitute state of the art for QCA are made using QCADesigner, which allows physical placement of individual cells. An alternative approach is the use of a QCA model written using VHDL language [2].

A random number generator (often abbreviated as RNG) is a computational or physical device designed to generate a sequence of numbers or symbols that lack any pattern, i..e appear random. In this paper we propose the design of random number Generator using QCA elementary devices like majority voter gate, QCA wire and QCA inverter considering the physical implementation of QCA technology which is more efficient in speed and area than that of CMOS technology.

II. QCA BACKGROUND

A. QCA Cell

The elementary device in QCA is the QCA cell . QCA is based upon the encoding of binary information in the charge configuration within quantum dot cells .QCA cell is a structure containing multiple quantum-dots. Consider a molecular cell with six dots as shown in Fig. 1(a). Four dots, referred to as “active” dots, form a square. Two “null” dots lie in a plane below the plane of the active dots. With two mobile charges to occupy the dots .Due to coulomb forces the mobile charges repels to maximize their separation. This yields two preferred states in which the mobile charges occupy antipodal active dots. These two states, are used to represent the bits “0” and “1” Fig1 (a).

B. QCA Logical devices

The basis of QCA circuits is intercellular interaction via Coulomb repulsion. Interaction between cells lifts the degeneracy between the 0 and 1 state and determines the state of each cell. Broadside coupling causes neighbouring cells to align .This is the basis for the binary wire Fig. 1(b).Signal inversion can be achieved via diagonal coupling Fig.1(c). The output of a majority gate is determined by the bit which dominates the three inputs Fig. 1(d). One input can be used as a control input to make the majority gate function as a programmable two-input AND-OR gate between the other two inputs.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

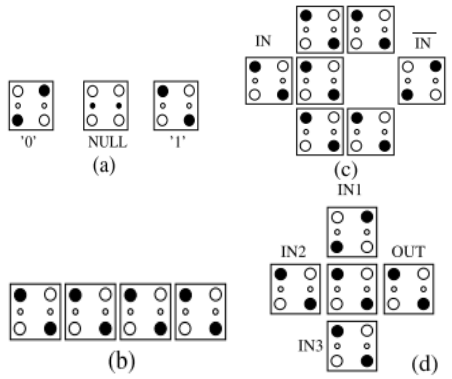

Fig 1. (a) QCA cell containing six dots representing binary '0' '1' and null state (b) QCA wire (c) QCA inverter (d) majority voter gate

C. Clocking

The signal flow is controlled by clocks. As the main source of them synchronization, a clock plays a key role in the QCA circuit. QCA clock is required in all the circuits to synchronize and control flow of information .that modulates the interdot tunneling barrier of QCA cell. This is accomplished by using four distinct and periodic phases $(0,\frac{\pi}{2},\frac{3\pi}{2},\pi)$ of a reference clock signal as shown in Fig.2 .

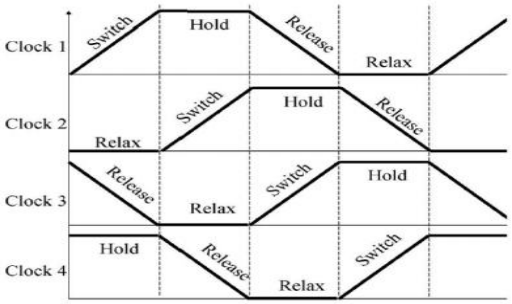

Fig 2 Four clock zones

A QCA circuit is partitioned into a number of clock zones where adjacent clock zones have a π /2 phase shift between them and every fourth clock zone will have the same applied signal. The four phases are Relax, Switch, Hold and Release. During the Relax phase, there is no inter dot barrier and cell remains unpolarized. During Switch phase, the inter dot barrier is slowly raised and cell attains a polarization under the influence of its neighbours. In Hold phase, barriers are high and cell retains its polarity acting as an input to the neighbouring cells. Finally, in the Release phase, barriers are lowered and cell looses its polarity .This clocking mechanism is responsible for inherent pipelined behaviour of QCA and multi bit information transfer through signal latching. A signal is effectively "latched" when one clock zone goes into Hold phase and acts as an input to the subsequent zone.

3. Molecular implementation of QCA

Molecular QCA is built using molecules with few oxide-reduction (redox) sites for charge localization and bridging ligands to provide tunneling among those sites. Redox sites act as quantum dots, able to encode and propagate information. Very low dimensions (1-2nm [9]) and very high switching speeds (1THz [9) could be reached. For molecular QCA, the clock is generated by applying an electrical field perpendicular to the molecular plane. A molecular six-dot cell is illustrated in Fig.3(a). Four active dots are used to represent a bit. Two null dots convey no information. The work in [11] presents a two redox center molecule attached on a Silicon substrate. The quantum dots in the molecule are ferrocene and Ru(dppm)2 groups, while the tunneling junction for the mobile electron is provided by the Carbon-Carbon triple bond. Two molecules form a four-dot QCA cell. For molecular QCA the clocking field can be generated by electrodes "buried" under the molecular layer. These electrodes, referred to as "clocking wires," are raised and lowered in potential sinusoidally to produce the desired clocking field [10] as shown in Fig.3(b).

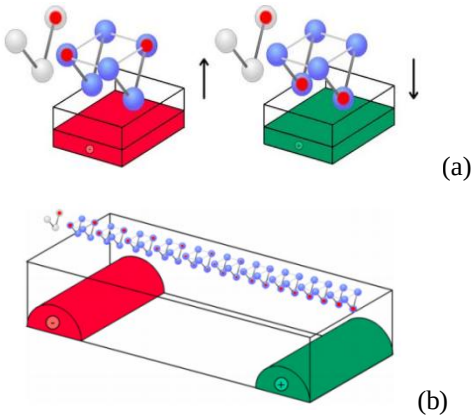

Figure 3 (a) Six dot molecular cell (b) Charged clocking wires are buried beneath an array of molecular QCA cells to activate cell.

The cell may be driven to the null state by charging a conductor buried beneath the cell in the substrate, thereby creating an electric field which repels the mobile charges from (or attracts them to) the null dots. The mobile charge depicted is a pair of electrons. The resulting electric field activates some cells on the substrate while driving others to the null state, thus forming active and null domains.

III. EXISTING RANDOM NUMBER GENERATOR

The Random Number Generator design [3] as shown in Fig. 4 consist of r shift registers and EX-OR unit. In this LUTs are configured as shift registers of variable length, this allows large periods to be achieved, while also improving the rate of mixing within the generator state. The output of r shift registers are mapped into the input of EX-OR gate. The r EX-OR gates generates r bit random number as a output and it is fed as a input to the shift register and continuously generates random numbers at the output of Ex-OR gate. Individual one bit shift registers enable a different solution that allows large periods to be achieved, while also improving the rate of mixing within

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

the generator state. Each of the r shift registers can be assigned some specific length ki<k. .This allows for much more rapid mixing between bits within the state, while still providing necessary conditions for mixing within the state. For n number of state bits in the RNG, the period is given as 2^n-1.

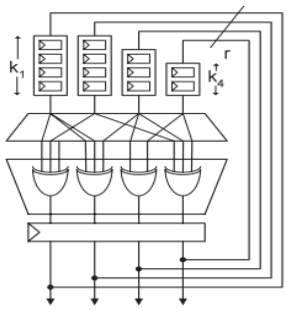

Fig 4 LUT-SR Random Number Generator

IV. PROPOSED RANDOM NUMBER GENERATOR USING QCA FOR FPGA

In this paper we proposed the RNG design [3] using QCA logic on FPGA. The QCA implementation of RNG design achieves faster speed and lower area than CMOS based technology. The main building block of the design are shift register and EX-OR unit In the proposed design shift registers of variable length (4, 6, 8, 10 bits) are used. The variable length of shift registers allows large periods generation.

A shift register, as shown in consists of a chain of cascading flip-flops, where the output of one flip-flop is connected to the input of the next flip-flop. The shift register is unidirectional. The data is shifted one bit position to the right for each clock cycle .To design sequential circuits; the conventional CMOS circuits are not suitable to directly translate into QCA architecture due to the timing constraint of the sequential logic circuits. Therefore, the truth tables of each sequential circuit have been observed and the Boolean equations have been derived for each circuit [8]. From the Boolean equation, the relationship of each variable can be clearly observed and the number of required logic gates can be determined. In the given design D-flip flop is cascaded to design shift register.

The Boolean equation for D flip flop is defined as
$Q_{Dff} = DQ_{t-1}'+DQ_{t-1.}$

The D flip flop is implemented using QCA majority voter gate (MVG) as shown in Fig.5. In QCA cells the shifting of data is transferred using the clock zones assigned to the cells. D flip flop takes one clock cycle to shift the data to the next flip flop.

The shift registers are then designed by cascading the D – flip flop. The output of the four shift registers are mapped into the EX-OR unit. The EX-OR unit consist of four EX-OR gate to generate four bit random number. Each EX-OR gate is 3 input EX-OR gate.

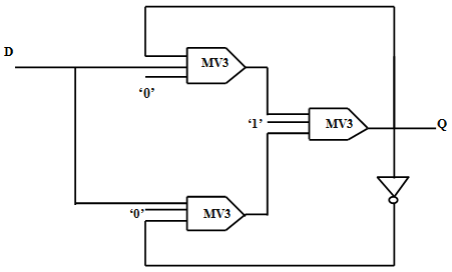

Fig 5 D Flip-flop using QCA

The Boolean expression for EX-OR gate is defined as
F(A,B,C)=ABC+A'B'C+A'BC'+AB'C'
The 3-input EX-OR gate is designed using majority voter gate is as shown in fig 6.

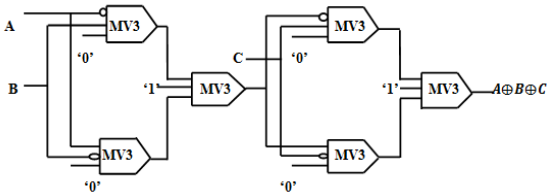

Fig .6 EX-OR flip flop using MVG

The output of the shift registers are mapped into the input of EX-OR gate The EX-OR unit generates the four bit random number. The output of the shift register is fed to the input of shift register for efficient and high quality random number generation. The algorithm for the generation of random number is very simple. A cycle of four bit seed is created through EX-OR gate at the output of RNG. The output of RNG is fed back to shift register to extend the length of shift register. The output of shift register are tapped mapped to the input of EX-OR gate. At the output of EX-OR gate four bit random number is generated continuously.

V. COMPARATIVE STUDY OF MOLECULAR QCA AND CMOS TECHNOLOGY

Comparative study between Physical implementation of Molecular QCA technology and CMOS Technology

1. Area: In molecular QCA, each QCA cell is made up of single molecules of (1-2nm) size. The device integration densities about 900 times more than the current end of CMOS scaling limits, which is not possible in current CMOS technologies. Table show the analysis of Table I. QCA Density Gains over Equivalent CMOS Designs [12].

Technology	Length	Width	Area	Density Gain
CMOS (0.07 μ)	29.8 μm	45.5 μm	1356.1 μm^2	N/A
CMOS (0.05 μ)	32.5 μm	21.3 μm	692.3 μm^2	N/A
QCA ("conventional")	28.1 μm	2.7 μm	75.9 μm^2	17.8 (0.07 μ) / 9.1 (0.05 μ)
QCA ("molecular")	2.81 μm	0.27 μm	7.6 μm^2	1787 (0.07 μ) / 912 (0.05 μ)

Table I. QCA Density Gains over Equivalent CMOS Designs

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

This section concludes with some projections from the Technology Roadmap for Nanoelectronics for the year 2006 and 2012 [1]. These are summarized below in Table II.

Benchmark	2006	2012
Feature size	2 nm	10 nm
No. of devices	4	10^6
Circuit speed	10 kHz	100 GHz
Events / chip / s	$4\ 10^4$	10^{14}
Power supply, V_{dd}	0.1 mV	0.1 mV
Power dissipation	1 pW (excluding cooling)	n/A
Temperature	4 K	4 K

Table II. Projections for QCA in various benchmark

2. Speed: The physical implementation of QCA offers high operating frequency in THz range.

3. Power Delay Product: The power delay-product can be considered a quality measure for a switching device as it is simply a measure of the energy consumed by a gate per switching event. A graph of the PDP for various technologies and where QCA would fit into this mix appears below in Fig.7. As one can see, the PDP for QCA is well below that of any other technology

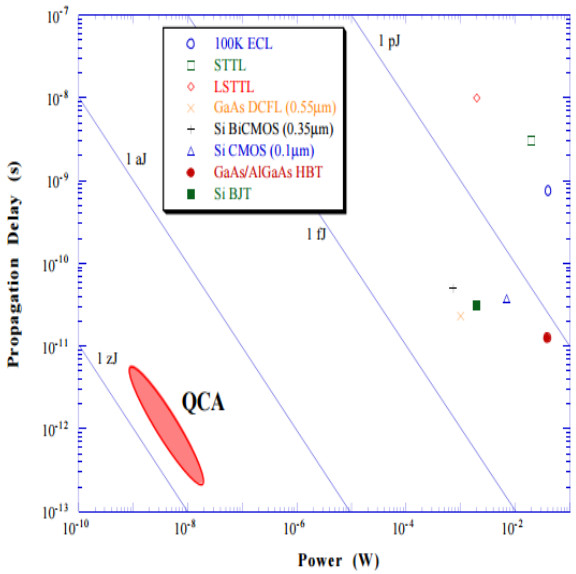

Fig.7 The power-delay-product for QCA and other technologies

VI. SIMULATION RESULT

The proposed RNG using QCA circuit is simulated using Xilinx on Spartan 6. The simulation results show that high quality of random number is generated due to variable length of shift register. Fig 8 shows the RTL schematic and RNG output is shown in Fig 9. Output [3:0] shows the four bit random number generated at the output of EX-OR gate.

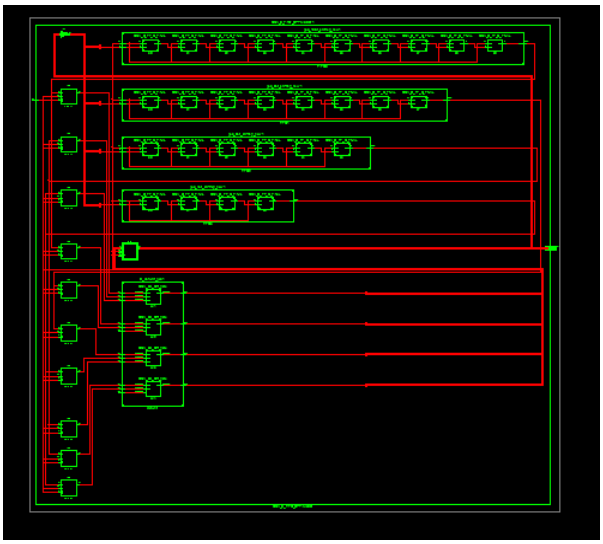

Fig.8 RTL schematic of RNG using QCA Logic

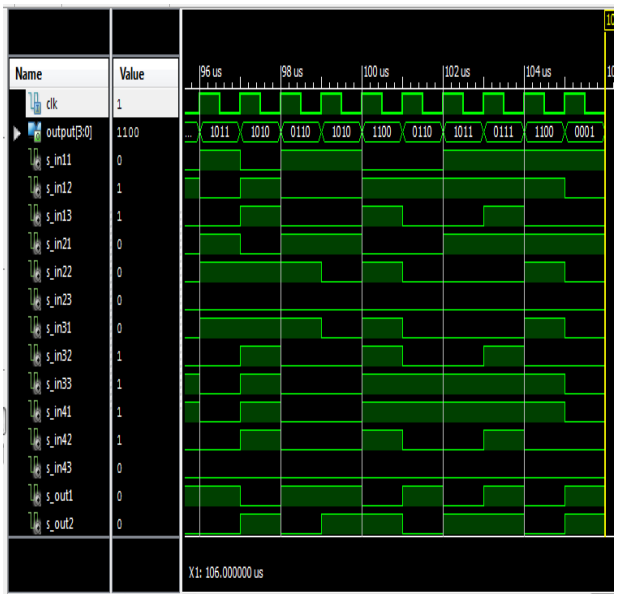

Fig. 9 RNG output

The simulation results after the synthesis of design is discussed below.
Speed: 442.478MHz
Delay: 4.162ns
Device Utilization Summary:

Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	12	18224	0%
Number of Slice LUTs	12	9112	0%
Number of fully used LUT-FF pairs	8	16	50%
Number of bonded IOBs	5	232	2%
Number of BUFG/BUFGCTRLs	1	16	6%

Fig. 10 Device Utilization Summary

DOI 10.17148/IJARCCE.2016.5785

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

VII. CONCLUSION

QCA is one of the emerging nano-technologies in computing paradigm. As it is not possible to scale CMOS beyond a certain limit, QCA technology provides alternative approach to improve the performance parameters in terms of speed and area of the design. The VHDL model of QCA elementary circuit provides simpler approach to design complex circuit for FPGA architecture to check the functionality of circuit for QCA technology.

REFERENCES

[1] International Technology Roadmap for Semiconductors (ITRS), http://www.itrs.net, 2007.
[2] 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
[3] David B. Thomas, Wayne Luk "The LUT-SR Family Of Random Number Generators For FPGA Architectures" IEETransactions On Very Large Integration (VLSI) System 1063–8210/ © 2012 IEEE
[4] Manisha G. Waje , Pravin Dakhole " Design and Simulation of Single Layered Logic Generator Block using Quantum Dot Cellular Automata" 2015 International Conference on Pervasive Computing (ICPC)
[5] Y. Lu and C. Lent, "Theoretical study of molecular quantum dot Cellular automata," in Proc. 10th Int. Comput. Electron.Abstracts.worksh Oct.2004 pp118-119
[6] M. Niemier, G. Bernstein, G. Csaba, A. Dingler, X. Hu, S. Kurtz, S. Liu, J. Nahas, W. Porod, M. Siddiq, and E. Varga, "Nanomagnet logic: Progress toward system-level integration," J. Phys.: Condens.Matter, vol. 23, p. 34, Nov. 2011
[7] R.Nithiyanandham, S.Charles Lekonard, U.Duraisamy, V.P.Ahmeed Faheem, V.M Navaneethakrishnan "Adder Design Using QCA Technique with Area Delay Efficient" International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 3, March 2015
[8] Sequential Circuit Design using Quantum-Dot Cellular Automata (QCA) Lee Ai Lim, Azrul Ghazali, Sarah Chan Tji Yan, Chau Chien Fat Center of Micro and Nano Engineering, College of Engineering,
Universiti Tenaga Nasional Kajang, Selangor, Malaysia
[9] Y. Lu, M. Liu, and C. Lent, "Molecular electronics - from structure to circuit dynamics," in Nanotechnology, 2006. IEEE-NANO 2006. Sixth IEEE Conference on, vol. 1, june 2006, pp. 62 – 65
[10] Enrique P. Blair · Eric Yost · Craig S. Lent "Power dissipation in clocking wires for clocked molecular quantum-dot cellular automata"J Comput Electron DOI 10.1007/s10825-009-0304-0
[11] Y. Lu and C. Lent, "Theoretical study of molecular quantum dot cellular automata," in Proc. 10th Int. Comput. Electron. Abstracts. Worksh., Oct. 2004, pp. 118–119.
[12] S.Kishor Krishna KumarQCA Binary Adder Implementation on FPGAIOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 2, Ver. II (Mar - Apr.2015), PP 81-89