

Design of Vedic Multiplier using Quantum Dot Cellular Automata for Cryptographic Applications

B.Shanmugi, Dr. V. Vinoth Thyagarajan, Dr. V. R. Venkata Subramani, Dr. S. Rajaram,
 Thiagarajar College of Engineering, Madurai

bshanmugi968@gmail.com, vvkece@tce.edu, venthiru@tce.edu, rajaram_siva@tce.edu

Abstract—Cryptography has achieved widespread recognition as a secure method of protecting sensitive information. Multiplication is one of the most demanding process in cryptographic algorithms as well as most time consuming. A more efficient and faster multiplier can be utilized to boost the cryptosystems speed. The vedic mathematics makes arithmetic operations easier. There are sixteen algorithms available in vedic mathematics. Vedic polynomial multiplication is performed using Urdhva-Tiryagbyham sutra from vedic mathematics. The speed of multiplication is improved due to parallelism in the nature of the vedic method. The vedic multiplication algorithm enhances the calculation speed by doing concurrent addition and partial product generation. Quantum-dot Cellular Automata (QCA) is a new nano technology trend that is well suited to the construction of high performance and low power integrated circuits. This paper employs a new architecture for a vedic multiplier based on Urdhva-Tiryagbyham sutra. This paper discusses the usage of a vedic multiplier to accomplish finite field multiplication. With the help of QCA Designer tool, the functional simulation of the circuit was verified. In addition, the QCA Designer-E tool is used to calculate the energy dissipation of QCA circuits. The area, latency, and energy dissipation of the vedic multiplier built with QCA technology have all been thoroughly researched. The suggested vedic multiplier provides much higher device density, lower cell count, area and clock delay than existing multipliers cited in the literature.

Index Terms - Cryptography, QCA, Vedic Multiplier.

I. INTRODUCTION

QCA transistor-less technology is increasingly being used as an alternative to CMOS technology. CMOS which targets the miniaturization and tries to reduce the size and at the same time increase the performance and density of the devices. According to Moore's law, the density of components in the integrated circuits doubles every 1.5 years. Though it was reliable for years, now it is reaching the

saturation stage. We cannot miniaturize the device due to various reasons like if more number of devices are packed in same area, the amount of heat generation will increase, if the heat increases that will create lots of problems like reliability issues. Another concern with the shrinking is parasitic capacitance from interconnects, which will have an impact on device performance. These are some limitations we face with CMOS technology, so we have to look for some alternatives.

Algorithms such as Advanced Encryption Standard (AES), an commercial security algorithm [15] used in the aerospace industry and Elliptical Curve Cryptographic algorithm [1] used for mobile applications. In these algorithms multiplication can be performed using vedic multiplier.

In Section II, the terminology of quantum dot cellular automata is presented. In section III, the design for the proposed 4x4 vedic multiplier is presented. In section IV, the results and comparisons are presented and Section V contains the conclusion

PRELIMINARIES

CMOS is approaching its physical boundaries, QCA will serve as a nano scale solution. In general, QCA circuit consist of cells which are arranged in grid like pattern. A QCA cell contains 4 quantum dots and 2 electron tunneling between the four dots. The electrons are allowed to move in vertically upwards or downwards direction through the tunneling junction but the capacitive junction does not allow electron to move horizontally because of this restriction, there are only 2 possibilities in the arrangement of electrons in QCA cell. Due to the coulombic repulsion, the electrons in the QCA cell [9] will tend to localize only at the opposite corners of the cell. A QCA cell and its two possible states are shown in figure

In QCA, the two types of crossovers are coplanar and multilayer crossover. In coplanar crossover, 90 degree cells are placed in one direction and 45 degree cells are placed in other direction so there won't be any glitch or interference

between the data transformation between the two wires and the data will be transferred without any issues. In multilayer crossover, by using different layers we make crossover. This mechanism is very similar to CMOS technology. This layer kind of placement is multiplayer crossover.

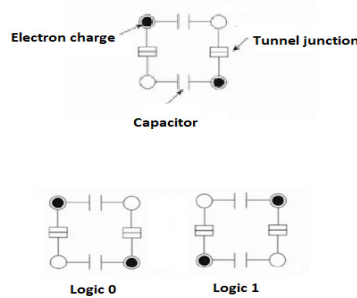


Fig. 1. Two possible states of QCA

II. METHODS AND MODELS

Vedic method of multiplication that differs from regular multiplication. Multiplication can be done with algorithms such as Array multiplier, Booth multiplier, Bit serial Multiplier, Carry save multiplier and Wallace multiplier. [2] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs).

Combinational logic is utilised in the Array multiplier [12] to multiply two binary values. This multiplier executes the product of all bits at once, making it a speedier multiplier. However, it requires a high number of gates, making it inefficient. To add carry to the adder, the bits in the carry save adder are processed one by one. As a result, it is dependent on past carry, which increases the time it takes to execute as the number of bits increases.

In the Wallace tree multiplier [13], three bit signals are delivered to a one bit full adder. The sum of the outputs from these inputs is passed to the higher order state full adder. Due to the speed of the operation, the wallace tree multiplier cannot be laid out.

The bits in the Carry Save Adder are processed one by one to add carry to the adder. As a result, it is dependent on past carry, which lengthens the execution time as the number of bits increases.

A vedic multiplier is presented to alleviate the drawbacks of these existing multipliers. vedic multiplier

reduces the number of stages in the multiplication operation, as well as the computational time. Vedic mathematics simplifies arithmetic procedures. In vedic mathematics, there are sixteen algorithms. The 16 important sutras of vedic mathematics are listed here.

- 1.Ekadhikina purvena
- 2.Nikhilam Navatashcaramam Dshatah
- 3.Urdhva Tiryagbyham
4. Paraavartya Yojayet
- 5.Shunyam Saamasamuccaye
- 6.Shunyamanyat
- 7.Sankala-vyavakalanabhyam
- 8.Puranabyham
- 9.ChalanaKalanabyham
- 10.Yaavadunam
- 11.Vyastisamanstih
- 12.Shesanyankena Charamena
13. Sopaantyadvayamantyam
14. Ekanyunena Purvena
15. Gunitasamuchyah
16. Gunakasamuchyah.

The urdhva-Tiryagbyham sutra from vedic mathematics is used to multiply two binary values. Urdhva means vertical and Tiryagbyham means crosswise. A high speed digit parallel modulo multiplier was designed using Urdhva-Tiryagbyham (UT) sutra. Algorithm 1 shows the steps involved in computation of a 4-bit polynomial multiplier using vedic mathematics. [6] discussed because of various appealing focal points, agreeable correspondences have been broadly viewed as one of the promising systems to enhance throughput and scope execution in remote interchanges.

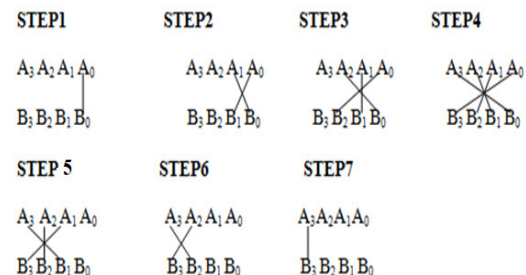


Fig. 2. Illustration of vertical and crosswise multiplication

A_3, A_2, A_1, A_0 are multiplier bits.
 B_3, B_2, B_1, B_0 are multiplicand bits.
 $P_0, P_1, P_2, P_3, P_4, P_5, P_6$ are the output bits.



ISSN (ONLINE): 2454-9762

ISSN (PRINT): 2454-9762

Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering

(IJARMATE)

Vol. 8, Issue 7, July 2022

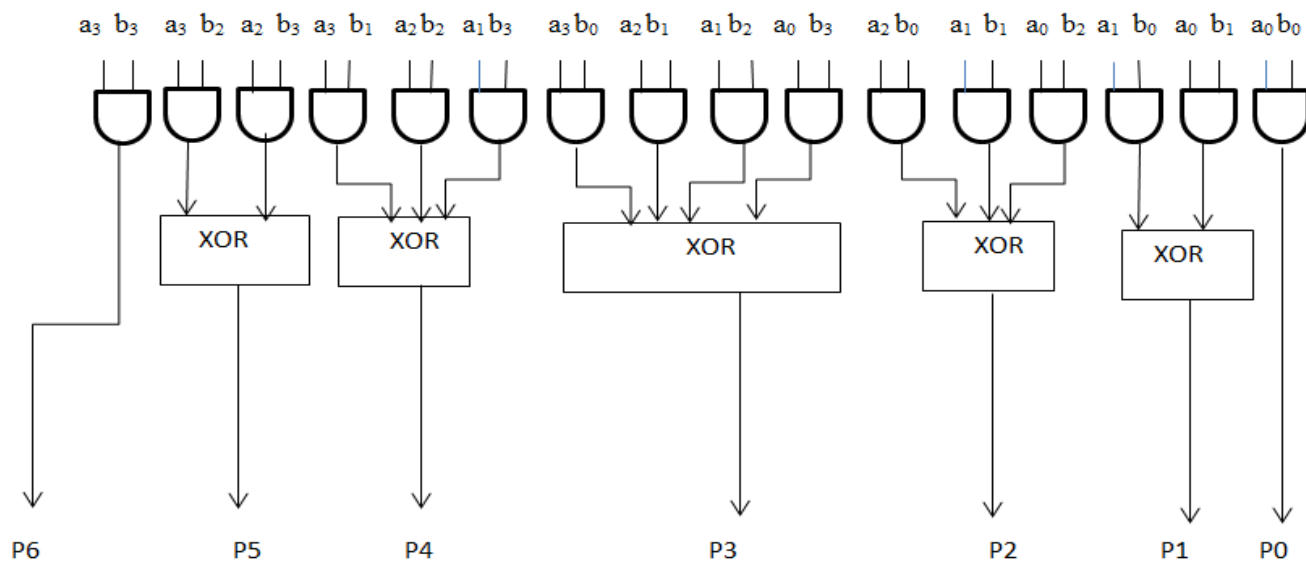


Fig. 3. Proposed 4-bit Vedic Multiplier

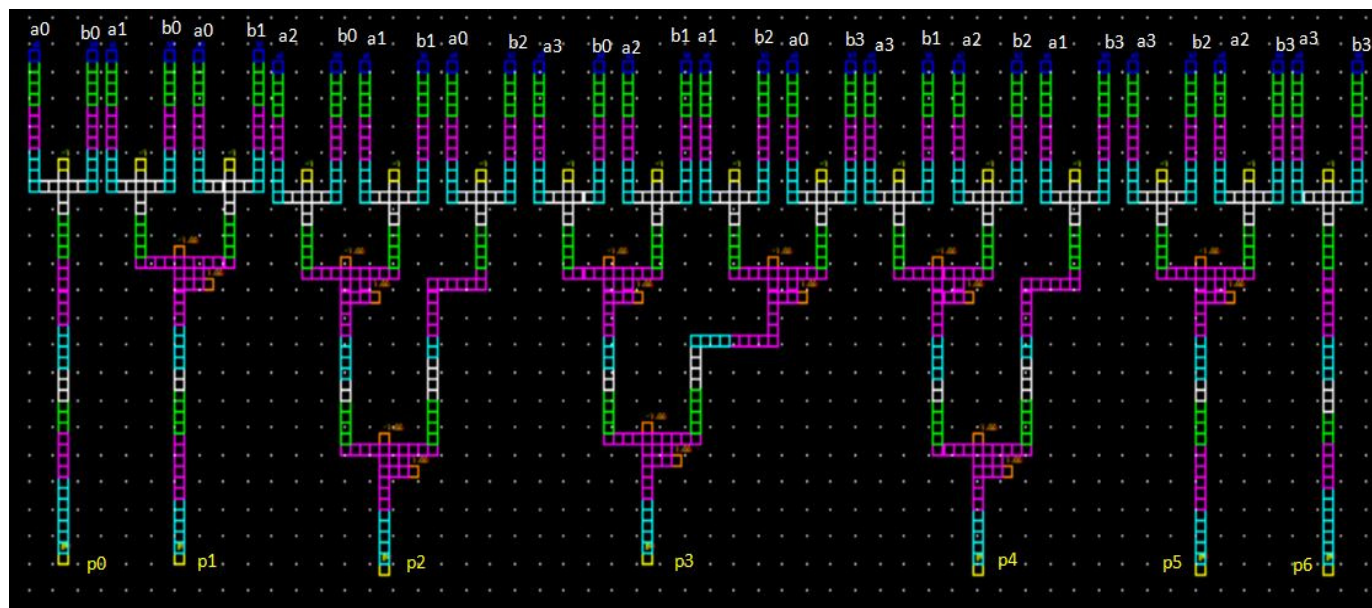



Fig. 4.QCA Layout design for proposed 4x4 Vedic Multiplier

IV.RESULTS AND DISCUSSION

With the help of the QCA designer tool, the circuits functional simulation is verified. For the simulation we have taken the input A3A2A1A0[1011] and B3B2B1B0[10001] and we are getting output as P6P5P4P3P2P1P0[1010011] which indicates the layout is correct and properly working. By applying default parameters of bistable approximation the logic gates can be simulated with below listed parameters.

 Bistable Options

Number Of Samples:	12800
Convergence Tolerance:	0.001000
Radius of Effect [nm]:	65.000000
Relative Permittivity:	12.900000
Clock High:	9.800000e-022
Clock Low:	3.800000e-023
Clock Shift:	0.000000e+000
Clock Amplitude Factor:	2.000000
Layer Separation:	11.500000
Maximum Iterations Per Sample:	1000
<input type="checkbox"/> Randomize Simulation Order	
<input checked="" type="checkbox"/> Animate	



 Cancel  OK

Fig. 5. Simulation parameters

[8] discussed that Helpful correspondence is developing as a standout amongst the most encouraging procedures in remote systems by reason of giving spatial differing qualities pick up. The transfer hub (RN) assumes a key part in agreeable correspondences, and RN choice may generously influence the execution pick up in a system with helpful media get to control (MAC).

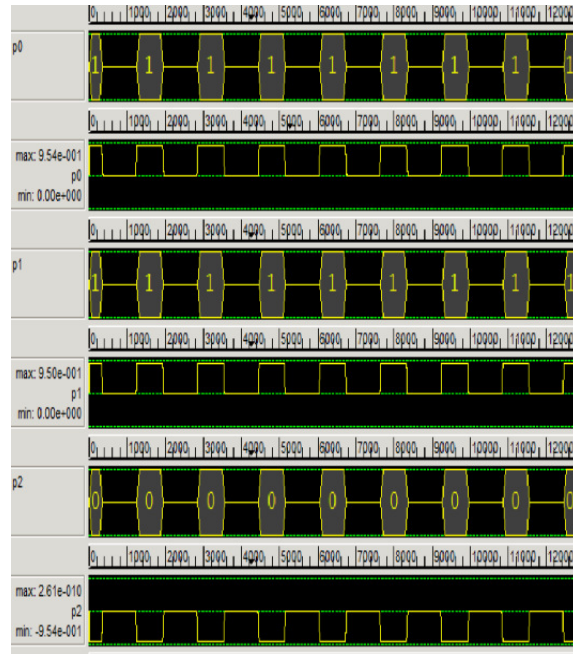


Fig. 6. Simulation result for proposed 4x4 Vedic multiplier

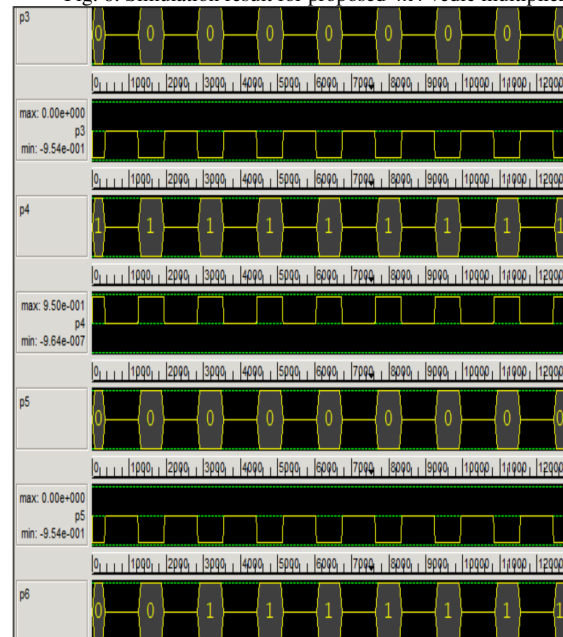


Fig. 7. Simulation result for proposed 4x4 Vedic Multiplier

TABLE-I
 COMPARISON OF PROPOSED MULTIPLIER WITH THE EXISTING MULTIPLIER

Circuit	Cell count	Area (μm^2)	Crossover
4x4 Array Multiplier [12]	3738	6.02	Multilayer
4x4 Dadda Multiplier [13]	3384	7.51	Coplanar
4x4 Wallace Multiplier [13]	3295	7.39	Coplanar
4x4 Vedic Multiplier [5]	1955	2.25	Multilayer
4x4 Vedic Multiplier[18]	1726	1.74	Multilayer
Proposed 4x4 Vedic Multiplier	1010	1.12	Multilayer

E_bath_total (E_{btx})	E_clk_total (E_{ctx})	E_Error_total (E_{etx})	Total energy dissipation Sum_bath (S_b)	Average energy dissipation Avg_bath (A_b)
2.9495 e-003	1.3387 e-003	-2.0543 e-004	3.86 e-002eV	3.51 e-003eV
3.2811 e-003	1.0256 e-003	-2.4216 e-004		
3.2199 e-003	1.0708 e-003	-2.3549 e-004		
2.6607 e-003	1.8839 e-003	-1.7272 e-004		
3.2191 e-003	1.0696 e-003	-2.3540 e-004		
3.9718 e-003	2.6178 e-004	-3.1968 e-004		
3.9220 e-003	2.1743 e-004	-3.1403 e-004		
3.8234 e-003	5.2745 e-004	-3.0318 e-004		
3.6376 e-003	5.3010 e-004	-2.8258 e-004		
3.9706 e-003	2.2009 e-004	-3.1945 e-004		
3.9178 e-003	2.6618 e-004	-3.1374 e-004		

TABLE-II
 ENERGY DISSIPATION ANALYSIS OF PROPOSED 4X4 VEDIC MULTIPLIER

The energy dissipation is calculated using QCA Designer-E with the coherence vector simulation engine. Energy dissipation occurs due to loss of information. The energy dissipated by the loss of a single bit of information can be expressed by

$$\text{Dissipated Energy} = K_B T \times \log_e 2$$

where ,

K_B is Boltzmann's constant ($K_B = 1.3807 \times 10^{-23} \text{ J K}^{-1}$)
 T is the absolute temperature.

E_clk_total (E_{ctx}) is the total energy transferred (Ect1, Ect2, Ect3,...) between the quantum cells.

E_Error_total (E_{etx}) is the summation of each error (Eet1, Eet2, Eet3,...) of the cell for every clock.

Total energy dissipation is the sum of all E_bath energies. For the proposed vedic multiplier sum_bath is 3.86 e-002eV. The average energy dissipation is the average of all E_bath energies. For the proposed vedic multiplier avg_bath is 3.51 e-003eV.

V. CONCLUSION

The design and simulation of a QCA based 4 bit Vedic multiplier for cryptographic applications is presented in this paper. QCA Designer bistable simulation was used to examine the operation of the proposed 4x4 vedic multiplier. The design is efficient that it contains fewer cells, uses few clock phases and has significantly shorter wire length, resulting in trouble free operation at higher temperature. When compared to prior works [5][12][13][14], the proposed vedic multiplier has an advantage in terms of cell number and area. The achieved 4 bit vedic multiplier has reduced cell count by 41% when compared with the previous designs. Data loss is a major issue in the development of computer paradigms. The data loss problem can be solved using reversible computation. In future, the reversible design of vedic multiplier will be designed using reversible gates.

VI. REFERENCES

- [1] Rina Maria, V. Anitha, "Light Weight Asymmetric Cryptographic Algorithm for Financial Transactions through Mobile Application", International Journal of Computer Applications, 2017.
- [2] Christo Ananth, M.Danya Priyadarshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254).
- [3] Ashvin Chudasama, Trailokya Nath Sasamal, Jyoti Yadav, "An efficient design of Vedic multiplier using ripple carry adder in Quantum-dot Cellular Automata", Elsevier-Computers and Electrical Engineering, volume-65, pp-527-542, 2018.
- [4] Christo Ananth, Dr.S. Selvakani, K. Vasumathi, "An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing", Journal of Advanced Research in Dynamical and Control Systems, 15-Special Issue, December 2017, pp: 787-792
- [5] Chudasama, A, Sasamal T.N., "Implementation of 4x4 Vedic Multiplier using Carry Save Adder in Quantum-Dot Cellular Automata", In Proceedings of the 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 1260–1264, 2016.
- [6] Christo Ananth, Dr. G. Arul Dalton, Dr.S.Selvakani, "An Efficient Cooperative Media Access Control Based Relay Node Selection In Wireless Networks", International Journal of Pure and Applied Mathematics, Volume 118, No. 5, 2018,(659-668).
- [7] Hari Kishore K, Fazal Noorbasha, Katta Sandeep, D. N. V. Bhupesh, SK. Khadar Imran, K. Sowmya, "Linear convolution using UT Vedic multiplier", International Journal of Engineering & Technology, 7(2.8),409-412,2018.
- [8] Christo Ananth, Joy Winston.J., "SPLITTING ALGORITHM BASED RELAY NODE SELECTION IN WIRELESS NETWORKS", Revista de la Facultad de Agronomía, Volume 34, No. 1, 2018,(162-169).
- [9] John Timler and Criag S. Lent, "Power gain and dissipation in Quantum-dot Cellular Automata", Journal of Applied Physics, 2002.
- [10] S.Karthikeyan and M.Jagadeeswari, "Performance improvement of elliptic curve cryptography system using low power, high speed 16x16 Vedic multiplier based on reversible logic", Journal of ambient intelligence and humanized computing, pp.1-10, 2020.
- [11] Kavitha S, Narasimha Kaulgud, "Quantum dot cellular automata (QCA) design for the realization of basic logic gates", International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECOT),2017.
- [12] Kim S.W, "Design of Parallel Multipliers and Dividers in QCA", UT Electronic Theses and Dissertations, University of Texas, May 2011.
- [13] Kim S.W, Swartzlander E.E," Parallel Multipliers for Quantum-Dot Cellular Automata", In Proceedings of the IEEE Nanotechnology Materials and Devices Conference, pp. 68–72, June 2009.
- [14] Nuriddin Safoev and Jun-Cheol Jeon," Design and Evaluation of Cell Interaction Based Vedic Multiplier Using Quantum-Dot Cellular Automata", Department of Computer Engineering, Kumoh National Institute of Technology, 2020.
- [15] M.Senthil Kumar and Dr.S.Rajalakshmi, "High Efficient Modified MixColumns in Advanced Encryption Standard using Vedic Multiplier", 2 nd International Conference on Current Trends in Engineering and Technology ICCTET,2014.