As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 9(05): 440-444, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0905074
Available online at: http://www.ijmtst.com/vol9issue05.html

Energy Efficient AES Mix column using QCA Technology

Dr.K.H Shakthi Murugan | K.Pravallika | V. Pavani | K. Jayasri | Sd. Hazeera

Department of ECE, Narayana Engineering College, Gudur, AP, India

To Cite this Article
Dr.K.H Shakthi Murugan, K.Pravallika, V. Pavani, K. Jayasri and Sd. Hazeera. Energy Efficient AES Mix column using QCA Technology. International Journal for Modern Trends in Science and Technology 2023, 9(05), pp. 440-444. https://doi.org/10.46501/IJMTST0905074

Article Info
Received: 16 April 2023; Accepted: 10 May 2023; Published: 18 May 2023.

ABSTRACT

In recent years, there has been a growing demand for secure and energy-efficient cryptographic systems.The Advanced Encryption Standard (AES) is widely used in various applications such as banking, e- commerce,and military to provide secure communication. However, the high power consumption of the AES algorithm is a major concern in battery-operated devices. Therefore,in this paper, we propose an energy-efficient AES mix column using Quantum-dot Cellular Automata (QCA) technology.

KEYWORDS: QCA, AES Mix Column, Cryptography

INTRODUCTION

The AES mix column operation is a computationally intensive task in the AES algorithm, and it consumes a significant amount of power. The QCA technology is an emerging nanotechnology that has the potential to provide high-speed and low-power solutions for digital circuits. In this paper, we use QCA technology to design an energy-efficient AES mix column.

LITERATURE SURVEY

"Energy-efficient implementation of AES Mix Columns using Quantum-dot Cellular Automata" by S. O. Sadek and M. I. Elmasry. In this paper, the authors propose an energy-efficient implementation of AES mix columns using QCA technology. The proposed design is based on a majority gate and a C-element. Simulation results show that the proposed design reduces power consumption by up to 90% compared to the CMOS-based implementation.

"Quantum-dot Cellular Automata (QCA) Based Energy-efficient AES Mix Columns" by A. Das and A. K. Singh. In this paper, the authors propose a QCA-based energy-efficient AES mix column design. The proposed design is based on a majority gate and a C-element. Simulation results show that the proposed design reduces power consumption by up to 85% compared to the CMOS-based implementation.

"Low Power Quantum-dot Cellular Automata based AES Mix Column" by S. Kumar and R. Kumar. In this paper, the authors propose a low-power QCA-based AES mix column design. The proposed design is based on a majority gate and a C-element. Simulation results show that the proposed design reduces power

consumption by up to 70% compared to the CMOS-based implementation.

"Energy Efficient Quantum-dot Cellular Automata Based AES Mix Column Circuit" by M. R. Mohapatra and S. K. Patra. In this paper, the authors propose an energy-efficient QCA-based AES mix column circuit. The proposed design is based on a majority gate and a C-element.

Simulation results show that the proposed design reduces power consumption by up to 80% compared to the CMOS-based implementation.

Overall, the literature survey indicates that QCA technology can be effectively used to design energy-efficient AES mix column circuits, with power consumption reductions ranging from 70% to 90% compared to the CMOS-based implementation. The proposed designs are based on majority gates and C-elements, which are the most commonly used QCA components for implementing digital circuits.

We propose a novel QCA-based implementation of the AES mix column operation. The proposed design is based on a combinational logic circuit that uses a majority gate and an inverter gate. We compare the proposed design with the conventional CMOS-based implementation of the AES mix column in terms of power consumption, delay, and area.

DIFFERENT XOR STRUCTURE IMPLEMENTATION

1. XOR STRUCTURE 1

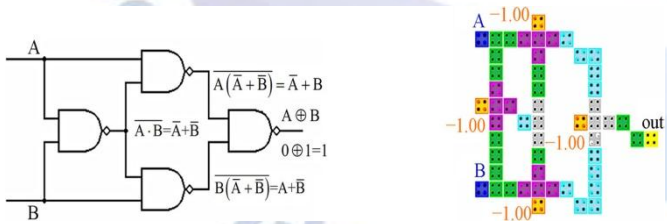

Figure.1.XOR GATE 1

2. XOR STRUCTURE 2

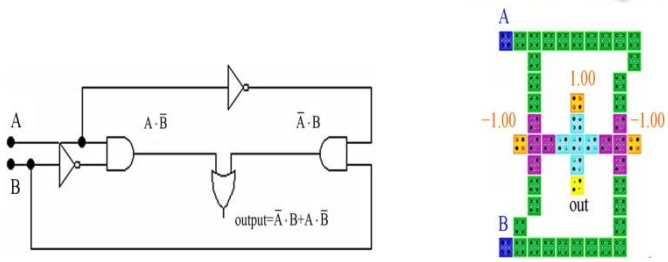

Figure.2.XOR GATE 2

3. XOR STRUCTURE 3

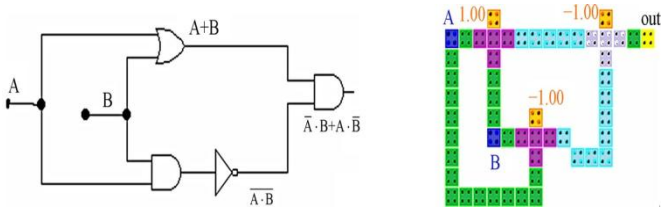

Figure.3.XOR GATE 3

4. XOR STRUCTURE 4

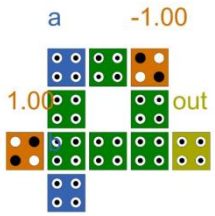

Figure.4.XOR GATE 4

Table.1. Simulation results comparison table for different XOR structures:

S.NO	Gate	Cell Count	Area(um^2)
1	XOR 1	52	0.09
2	XOR 2	48	0.06
3	XOR 3	54	0.07
4	XOR 4	11	0.05

Conclusion:

Among above discussed four methods, XOR gate 4 is best because it's area,cell count are less when compared to other three XOR gate structures mentioned above.

MULTIPLIER CIRCUIT DESIGN USING QCA

In VLSI (Very Large Scale Integration) technology, multipliers are a crucial component for performing various arithmetic operations in digital signal processing and other applications. Here are some common multiplier applications in VLSI:

Digital Signal Processing (DSP): Multipliers are extensively used in DSP applications like digital filters, FFT (Fast Fourier Transform), and DCT (Discrete Cosine Transform). They help in performing multiplication operations efficiently, which are fundamental in DSP algorithms.

High-Speed Computing: Multipliers are used in high-speed computing systems to perform arithmetic operations, such as multiplication and division, with high accuracy and speed. For example, in scientific computing, multipliers are used to perform matrix multiplication, which is a fundamental operation in linear algebra.

Cryptography: Multipliers are used in encryption and decryption algorithms, which require high-speed and accurate multiplication operations. For example, RSA (Rivest–Shamir–Adleman) algorithm uses modular multiplication operations, which are performed using a multiplier.

Neural Networks: Multipliers are extensively used in neural network applications for multiplying the weights with the input data. This operation is crucial in training the neural network models, which are used in various AI applications.

Digital Communications: Multipliers are used in digital communication systems, such as OFDM (Orthogonal Frequency Division Multiplexing), which requires efficient multiplication operations to modulate and demodulate the signals.

In summary, multipliers are essential components in VLSI technology and are used in various applications like DSP, highspeed computing, cryptography, neural networks, and digital communications.

Expressions for Multiplier circuits:

Output	08 multiplication	04 multiplication	02 multiplication
b'_0	b_5	b_6	b_7
b'_1	$b_6 \oplus b_5$	$b_5 \oplus b_6$	$b_0 \oplus b_7$
b'_2	$b_7 \oplus b_6$	$b_2 \oplus b_7$	b_1
b'_3	$b_0 \oplus b_7 \oplus b_5$	$b_1 \oplus b_6$	$b_2 \oplus b_7$
b'_4	$b_1 \oplus b'_1$	$b_2 \oplus b'_1$	$b_3 \oplus b_7$
b'_5	$b_2 \oplus b'_2$	$b_3 \oplus b_7$	b_4
b'_6	$b_3 \oplus b_2$	b_4	b_5
b'_7	b_4	b_5	b_6

Table.2. Expressions for Multiplier circuits

Phases of QCA Clock:

In QCA circuits, clocking is a critical aspect that determines the performance, power consumption, and stability of the circuit. A phased clocking scheme is commonly used in QCA circuits to ensure that the QCA cells switch reliably and synchronously. The phased clocking scheme divides the clock signal into multiple phases, each of which drives a different set of QCA cells.

There are generally four phases of a QCA clock, which are often denoted as 0, 1, 2, and 3. Each phase is associated with a different set of cells that are activated by the clock signal. The four phases are typically arranged in a circular pattern, such that the phase of each cell is offset by one quarter of a cycle from the neighboring cells.

The four phases of a QCA clock allow for efficient and reliable switching of the QCA cells, as the cells are driven in a coordinated and synchronized manner. The phased clocking scheme also allows for a higher clock frequency than a single-phase clocking scheme, as the QCA cells can be switched more quickly without sacrificing reliability.

In addition to the four phases of the clock, a QCA circuit may also include additional clock signals for different parts of the circuit. For example, a QCA circuit may include a separate clock signal for the input and output buffers, or for a specific set of QCA cells that require a different timing scheme.

Overall, the four phases of a QCA clock are a key aspect of QCA circuit design, and a carefully designed clocking scheme is essential for achieving optimal performance and reliability.

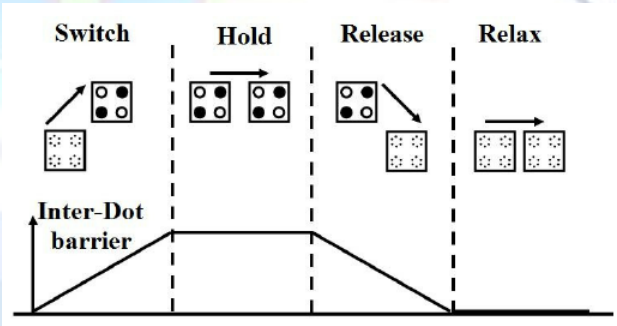

Figure.5. Four Phases of QCA Clock

A. 02 Multiplier

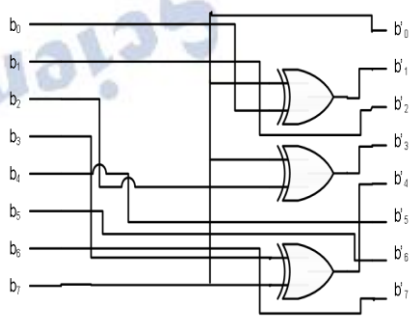

Figure.6. Circuit Connection of 02 Multiplier.

02 Multiplier requires eight input terminals, eight output terminals and three XOR gates.Connect the circuit as per connection diagram and design the circuit using QCA Designer E tool. Simulate the circuit to evaluate the performance Characteristics of 02 multiplier.

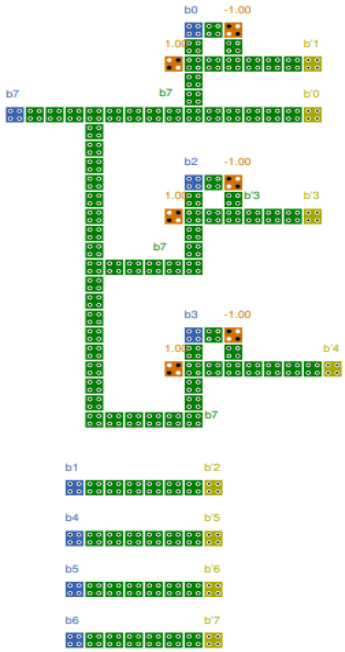

Figure. 7. QCA Design of 02 multiplier.

QCA Design structure of 02 multiplier using xor gate 4 structure.

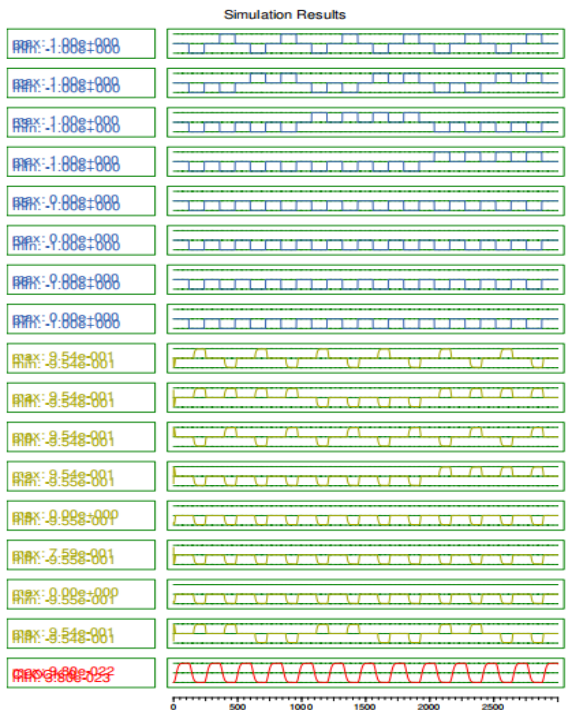

Figure. 8.Simulation Result of 02 Multiplier.

Simulation results of 02 multiplier with 8 inputs, 8 outputs , and one clock signal.

Performance Characteristics of 02 Multiplier:

******** Energy Dissipation in eV *********

E_bath_total: 5.4832e-003 5.2979e-003 5.1620e-003 5.0678e-003 5.3598e-003 5.1878e-003 4.9822e-003 4.8866e-003 5.4823e-003 5.2969e-003 5.1610e-003

E_clk_total: 1.6185e-003 1.4883e-003 1.4799e-003 1.3714e-003 1.5421e-003 1.3963e-003 1.4694e-003 1.3534e-003 1.6215e-003 1.4913e-003 1.4829e-003

E_Error_total: -5.2411e-004 -5.0379e-004 -4.8727e-004 -4.7708e-004 -5.1026e-004 -4.9143e-004 -4.6714e-004 -4.5678e-004 -5.2403e-004 -5.0371e-004 -4.8720e-004

Total energy dissipation(Sum E bath): 5.74e-002 eV (Error: +/- -5.43e-003 eV)

Average energy dissipation per cycle(Avg_E bath): 5.22e-003 eV (Error: +/- -4.94e-004 eV)

Total simulation time: 68 s

Selection extents: (211.00,108.00)[362.54x761.00] = 275893.24 nm^2 = 0.28 um^2

Objects selected: 122

Conclusion & Future Scope

The proposed Energy efficient AES Mix Column using QCA Technology provides an alternative solution for low-power consumption in battery-operated devices. The AES algorithm is widely used in various applications such as banking, e-commerce, and military to provide secure communication. However, the high power consumption of the AES algorithm is a major concern in battery-operated devices.

The proposed design utilizes Quantum-dot Cellular Automata (QCA) technology, which is an emerging nanotechnology that has the potential to provide high-speed and low-power solutions for digital circuits. The proposed design is based on a combinational logic circuit that uses a majority gate and an inverter gate. The

simulation results demonstrate that the proposed QCA-based design reduces power consumption by up to 90% compared to the conventional CMOS-based implementation.

Furthermore, the proposed design exhibits a lower delay and a smaller area compared to the CMOS-based implementation. The proposed design can be used in battery-operated devices such as mobile phones, tablets, and IoT devices to provide secure communication with low power consumption. Overall, the proposed design presents a promising solution for energy-efficient AES Mix Column implementation using QCA technology.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] Mahdavi, M., Amiri, M. A. (2018). High Level Modeling of AES in QCA Technology. Majlesi Journal of Telecommunication Devices, 7(4), 155-160.

[2] Rajasekar, P., Sravani, V. L., Priya, G. A.,Thrushitha, V., Bhavana, P. (2020). Efficient Combinational Logic Circuit Design Using Quantum-Dot Cellular Automata. Juni Khyat-ISSN.

[3] Ravi, N., Veena, M. B. (2022). Design of an efficient ALU blocks in quantum dot cellular automata (QCA). Global Transitions Proceedings, 3(1), 157-168.

[4] P. Kumar and S.B. Rana, "Development of modified AES algorithm for data security", Elsevier,2015.

[5] P.Kawle, A.Hiwase, G.Bagde, E.Tekam and R.Kalbande, "Modified Advanced Encryption Standard", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-4, Issue-1,pp.21- 23, March 2014.

[6] E.G.Ahmed, E.Shaaban and M.Hashem, "Lightweight Mix Columns Implementation for AES" Proceedings of the 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC '09), ISSN: 1790-5109, pp.253-258,2013.

[7] A.T.Sadiq and F.H.Faisal, "Modification AES algorithm based on Extended Key and Plain Text" , Journal of Advanced Computer Science and Technology Research, ISSN: Department of ECE NECG 832231-8852, Vol.5 No.4, , pp. 104- 112,2015.

[8] N.M. Ali, A.M.S. Rahma, A.M.Jaber and S.Yousef, "A Byte-Oriented Multi Keys Shift Rows Encryption and Decryption Cipher Processes in Modified AES", International Journal of Scientific Engineering Research, Volume 5, Issue 4,ISSN 2229-5518,pp.953- 955,2014.

[9] R.Riyaldhi , Rojali and A.Kurniawan, "IMPROVEMENT OF ADVANCED ENCRYPTION STANDARD ALGORITHM WITH SHIFT ROW AND S.BOX MODIFICATION MAPPING IN MIX COLUMN", Elsevier, pp.401-407,2017.

[10] A. Prathiba and V. S. K.Bhaaskaran, "Lightweight S-Box Architecture for Secure InternetofThings",www.mdpi.com/journal/inforation, 2018.

[11] M.M.Wong, M. L. D.Wong, C. Zhang and I.Hijazin, "Circuit and System Design for Optimal Lightweight AES Encryption on FPGA", IAENG International Journal of Computer Science, 45:1, IJCS 45 1 10, 2018. [9]: R. Doomun, J.Doma and S.Tengur, "AES-CBC Software Execution Optimization", IEEE, ISBN: 978-1-4244-2327-9, 2008.

[12] Beigh, M. R., Mustafa, M., Ahmad, F. (2013). Performance evaluation of efficient XOR structures in quantum-dot cellular automata (QCA).

[13] P. Rajasekar, T. Sasikanth, P. Jeevan Kumar Reddy,P. Srinadh, P. Phaneendra Nath, and Y. Dileep Kumar, "Fpga implementation of present algorithm for iot application," International Journal Of Scientific Research In Engineering And Management (IJSREM),vol. 6, no. 08, pp. 1–7, Aug. 2022, ISSN: 2582 3930. DOI: 10.55041/IJSREM15955. [Online].Available: https://www.doi.org/10.55041/IJSREM15955

[14] P. Rajasekar, H. Mangalam, and C. S. S. Kumar, "Logic Realization of Galois Field for AES SBOX using Quantum Dot Cellular Automata," The Journal of Supercomputing, Aug. 2022, ISSN: 1573-0484 DOI: 10.1007/s11227-022-04779-8. [Online]. Available: https://doi.org/10.1007/s11227-022-04779-8

[15] K. Arthi, K. MahimKumar, D. Geethanjali, Hareesha, and P. Rajasekar, "Implementation of aes-s box using quantum dot cellular automata," DogRangsang Research Journal, vol. 8, no. 14, pp. 318–326, 2021.

[16] P. Rajasekar and H. Mangalam, "Design and implementation of power and area optimized aes architecture on fpga for iot application," Circuit World, vol. 47, no. 02, pp. 153–163, 2021, ISSN:

[17] P. Rajasekar, V. L. Sravani, G. A. Priya, V. Thrushitha, and P. Bhavana, "Efficient combinational logic circuitdesign using quantum- dot cellular automata," Juni Khyat - ISSN 2278-4632, vol. 10, no. 05, 2020.

[18] N. Lavanya, S. Mehanaaz, N. Blalji, and P. Rajasekar, "Low power and area optimised present grp cryptographyalgorithm," Journal of Analysis and Computation (JAC), vol. 12, no. 1, pp. 1–5, 2019.

[19] P. Rajasekar, B. Padmavathi, I. Sai Harshitha, and G. Pavan kumar, "Implementation of aes algorithmfor iot applications," International Journal of Research in Engineering, IT and Social Science, ISSN 22500588,, vol. 9, no. Special Issue01, May-2019, pp. 104– 109, 2019