IMPLEMENTATION OF AES-S BOX USING QUANTUM DOT CELLULAR AUTOMATA

Arthi K Mahima Kumar K Geethanjali D Hareesha M UG Student, Department of ECE, Narayana Engineering College (Autonomous), Gudur, SPSR Nellore, AP, India
Dr.P Rajasekar Professor, Department of ECE, Narayana Engineering College (Autonomous), Gudur, SPSR Nellore, AP, India :: aarthikannambakam@gmail.com

Abstract: *Quantum Dot Cellular Automata (QCA) represents an emerging technology at the nano technology level. Now a day's many applications of QCA technology are introduced and cryptography can be an interesting application of QCA technology. Substitution Boxes are important components in many modern-day block and stream ciphers. We have implemented a specific 4x4 S Box using QCA technology. Simulation results are obtained from QCA Designer.*
Key words: QCA, SBox, AES, Cryptography, Finite fields

I.INTRODUCTION

The microelectronics technology has tremendously improved the combination, utilization, and the speed during recent a long time through diminishing the element size of semiconductors. In any case, it appears to be that even by diminishing the semiconductor measures, a few issues, for example, power utilization can't be overlooked. Using the QCA innovation for carrying out rationale circuits is one of the methodologies which as well as diminishing the size of rationale circuits and expanding the clock recurrence of these circuits, decreases the force utilization of these circuits. QCA which was first presented by Loaned et.al [1] addresses an arising innovation at the nanotechnology level. QCA cells have quantum specks, in which the situation of electrons will decide the paired degrees of 0 and 1.

Replacement gives a critical part in present day cryptography. For certain applications, the replacements are shaped by basic Boolean capacities (which take a few Boolean sources of info and give a solitary yield thus). The plan of reasonable capacities has gotten huge consideration from cryptographers for quite a long time. Replacement is commonly carried out by replacement boxes (S-Boxes). These capacities have various data sources and different yields. Maybe the most well-known S-Boxes are those of the Information Encryption Standard (DES) [1]. Inside each round of DES, the main commitment to security is made by eight 6-input, 4-yield capacities. These are determined through query tables. The DES calculation has been dependent upon a lot of contention. A lot of this has spun around the specific replacements executed by the eight S-Boxes. The S-Box thought has a firm hold in current cryptography. The new global symmetric key cryptography standard, the High level.

Encryption Standard (AES), likewise utilizes S-Boxes to perform replacements/3/. As a use of QCA innovation, we have carried out a particular 4×4 S Box. The strategy which is utilized to execute the S-Box is the Rationale Based technique. In this strategy, the S-Box is executed by rationale entryways. In the following Area, we will momentarily clarify the Quantum speck Cell Automata. It incorporates the cell presentation, cell-cell coupling, QCA rationale, and QCA timing.

Simulation results of this implementation are obtained from QCADesigner v2.0.3 software (QCADesigner is developed by the ATIPS lab at the University of Calgary in Canada). QCADesigner v2.0.3 features different simulation engines. Throughout this paper, the coherence vector engine is used due to its accurate and detailed evaluation of QCA.

II.LITERATURE SURVEY

The impediments in CMOS innovation, for example, high lithography short channel impacts, and force utilization urged researchers to consider options. Numerous nano innovations were arisen to conquers these constraints, for example, Single Electron Semiconductor Carbon Nanotube Field-Impact Semiconductor Balance FET and Quantum-speck Cell Automata (QCA). QCA innovation was presented interestingly by Loaned et al in 1993 and it is dependability was concentrated in QCA building block is a square shape that has four specks and two electrons. This innovation is assessed exhaustively by QCA relies upon the guideline of electron's repugnance. The memory unit is vital in all electronic circuits.

 Copyright @ 2021 Authors

Planning effective memory units in QCA innovation still in the opposition. The analysts in QCA innovation searching for tracking down a decent circuit with least intricacy (cells and region). This paper presents a novel lock with least intricacy then, at that point utilizes this hook for planning an ideal type of D Flip-Flop with set/reset capacity.

This field presents novel constructions of memory units (D hook and D Flip-Flop) in QCA innovation. The proposed circuits are in ideal structure as far as region and cell checks. The proposed flip lemon can set the yield and reset it. The proposed circuits have more productive than recently distributed in practically all measurements as clarified in examination tables. The yield waveforms show that the proposed structures are liberated from.

In most recent couple of many years, the speed up and outstanding scaling in include size have been effectively achieved utilizing lithography-based VLSI innovation. Yet, this pattern faces some genuine difficulties as a result of fundamental constraints of CMOS innovation, for example, short channel impacts, super dainty door oxide, doping changes and costly lithography at nano scale level. QCA is one of the arising advancements that has capacity to supplant the semiconductor-based gadgets at nano scale level. QCA innovation can conquer the limit of regular semiconductor-based innovation. QCA has some high-level highlights like quicker speed, more modest size and lower power utilization in contrast with semiconductor-based innovation.

III. PROPOSED METHOD

In Quantum Cell Automata (QCA), a phone contains four quantum dabs, as schematically appeared in Fig. 1. The quantum specks are appeared as the open circles which address the keeping electronic potential. Every phone is involved by two electrons which are schematically appeared as the strong specks.

In a cell, the electrons are allowed to jump between the individual quantum dots by the mechanism of quantum mechanical tunnelling, but they are not allowed to tunnel between cells. The barriers between cells are assumed sufficient to completely suppress intercellular tunnelling.

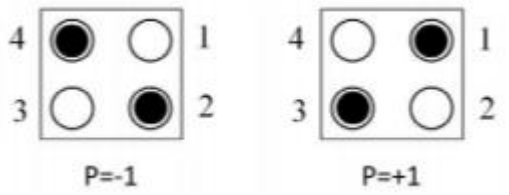

Fig 1. QCA cells and ground states

If they are left alone, they will meet the configuration corresponding to the physical ground state of the cell. It is in an obvious manner that the two electrons will tend to occupy different dots because of the Coulombic force associated with bringing them together in proximity the same dot.

3.1 S Box block diagram

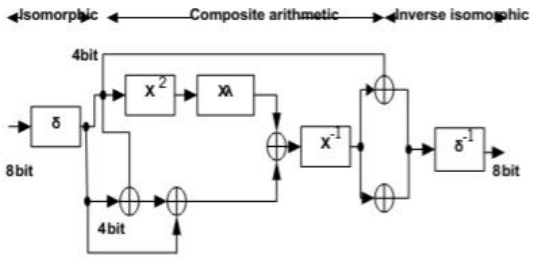

Fig 2 Block diagram of S Box

In cryptography, an S box(substitution box) is a basic component of symmetric key algorithms which performs substitution.fig.2 represent the block diagram for proposed S box. This block diagram contains some blocks those are

 Copyright @ 2021 Authors

3.1.1 XOR gate

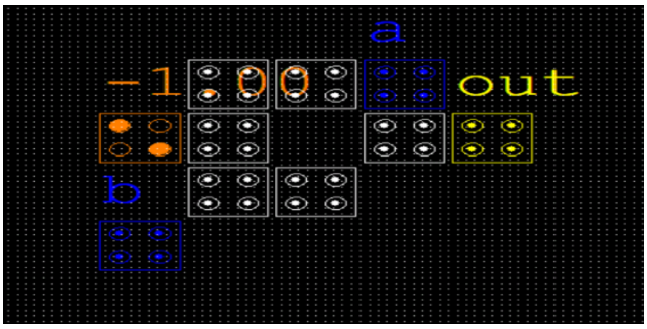

Fig 3. QCA design of XOR gate

In this paper we are implement the S box by using 2 input XOR gates for that we are introducing the following xor gate designed with 10 cells.in this 2 cells are labelled as inputs as A and B another one is labelled as output. Need to provide a polarization value as -1. That's why its represent xor gate .The mathematical equation for xor gate is A⊕B =Y

3.1.2 Proposed Isomorphic Diagram

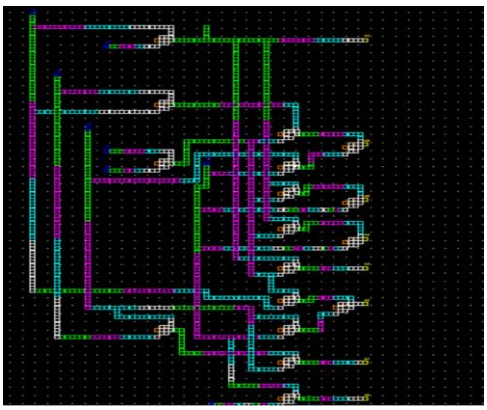

Fig. 4. Isomorphic QCA diagram

Fig.4 represents isomorphic diagram to do isomorphism which is the first block in S box, isomorphism means, in modern algebra, mapping between two sets that preserves binary relationships between elements of the sets. This circuit is designed by using 1354 cells, and also 17 xor gates. The inputs of this circuit is b0 to b7 .

The mathematical expression for above diagram is

$b_7=b_5⊕b_7$,
b6=[(b6⊕b7) ⊕(b1⊕b2)] ⊕[b3⊕b4],
b5=b3⊕[(b5⊕b7) ⊕(b1⊕b2) ,
b4=b3⊕[(b5⊕b6)⊕(b1⊕b2)],
b3=(b6⊕b7)⊕(b1⊕b2) ,
b2=[b7⊕(b1⊕b2)] ⊕[b3⊕b4] ,
b1=b4⊕[b4⊕b6],
b0=b0⊕b3

3.1.3 4 bit GF Squarer

Fig 5 shows the 4 bit GF squarer this is designed by using 96 cells .and the inputs are taken as b_0,b_1,b_2,b_3 and outputs are k_0,k_1,k_2,k_3.

The mathematical equations are

$k_0=b_0⊕b1⊕b3$,
k1=b1⊕b2 ,
k2=b2⊕b3,
k3=b3

Copyright @ 2021 Authors

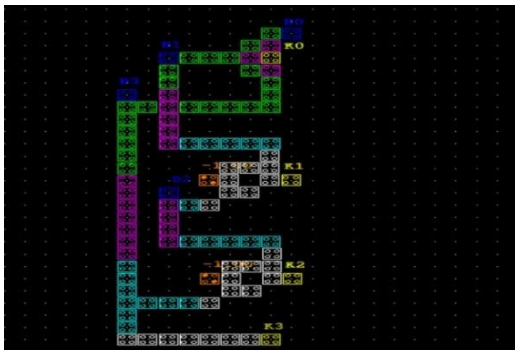

Fig 5. 4 bit GF squarer

3.1.4 GF(2) Multiplication

Fig 6 shows the GF(2) Multiplication it is designed by using 266 cells. And the inputs are taken as b_0, b_1, b_2, b_3 and outputs are k_0,k_1,k_2,k_3.

The mathematical equations are

$k_1=(b_1w_1 \oplus b_0w_1) \oplus (b_1w_0)$

$k_0=b_1w_1 \oplus b_0w_0$.

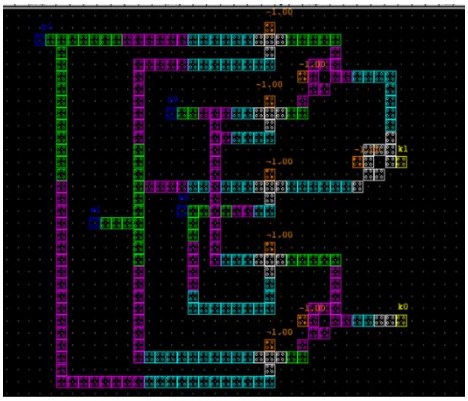

Fig 6: GF(2) Multiplication

3.1.5 Lambda multiplication

Fig.7 shows the lambda multiplication it is designed by using 153 cells. And inputs are taken as b0,b1,b2,b3 and the outputs are k0,k1,k2,k3.

The mathematical equations are

k0=b2,

k1=b3,

k2=b0⊕b1⊕b2⊕b3,

k3=b1⊕b2.

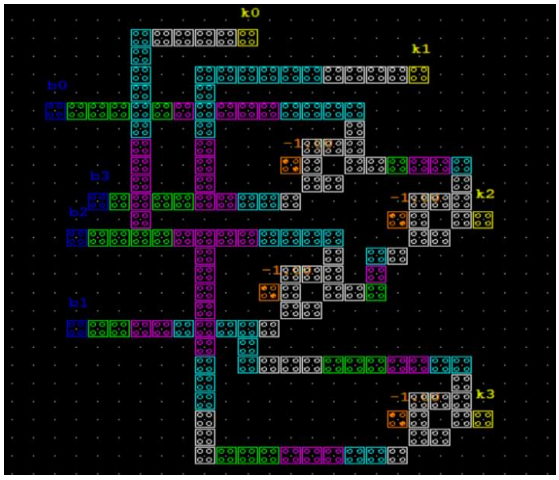

Fig 7:Lambda Multiplication

Copyright @ 2021 Authors

3.1.6 GF Pi Multiplier

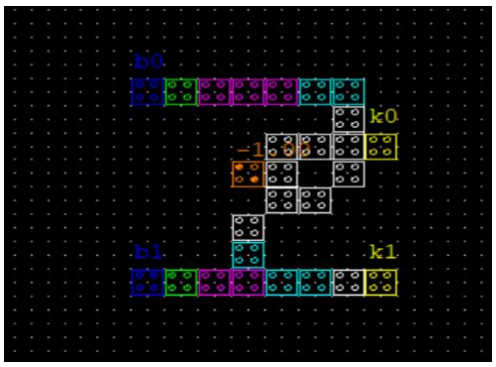

Fig.8 GF Φ Multiplier

Fig 8 shows the GF Φ multiplier it is designed by using 27 cells and the inputs are taken as b0,b1 and the outputs are taken as k0,k1.

The mathematical equations are

$$k0=b0 \oplus b1,$$
$$k1=b1.$$

3.1.7 GF Multiplicative inverse partial product module

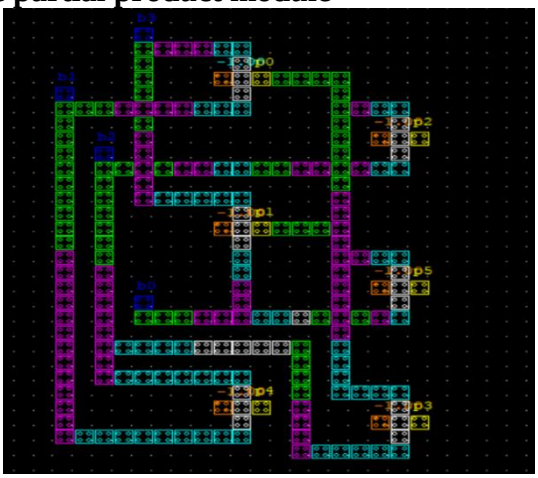

Fig 9 GF Multiplicative inverse partial product module

Fig 9 shows the GF multiplicative inverse partial product module it is designed by using 207 cells.and the inputs are taken as b0,b1,b2,b3 and the outputs are taken as k0,k1,k2,k3.

The mathematical equations are

$$k2=b1b3b2$$
$$k1=b1b3b0$$
$$k0=b1b2$$
$$k3=b1b2b3$$

IV. RESULT AND DISCUSSIONS

Table IV. Result and Discussion

Sites of design	Number of QCA cells	Number of gates	Area nm^2
Isomorphic diagram	1354	17	3389364.00
4-bit GF squarer	96	3	104222.24
GF(2) Multiplications	266	8	425063.0
Lambda multiplication	153	2	180684.0
GF Pi multiplier	27	1	24964.00
GF multiplicative inverse partial product module	207	6	227333.96
XOR gate	10	1	11574.00
S Box	2113	38	4182520.00

Copyright @ 2021 Authors

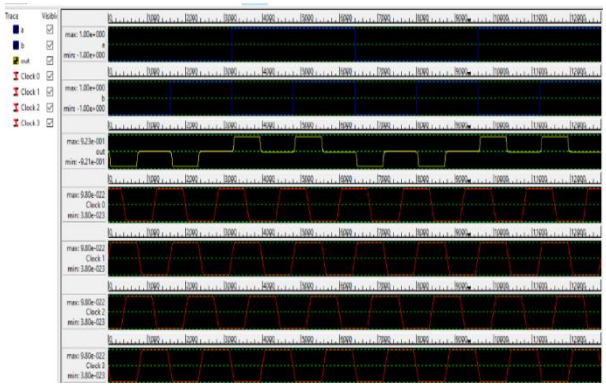

Fig 10 XOR gate

Consider the output the output it is implemented by using the QCA cells and illustrated in fig.10 the inputs are applied through the binary wires.

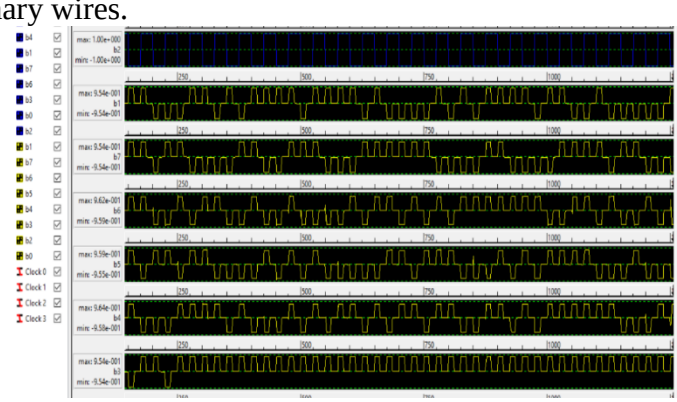

Fig 11: Isomorphic QCA diagram

Consider the output it is implemented using QCA cells and illustrated in fig.11 the inputs are applied through the binary wires. Each term of function is composed of two or three gates which are used as xor gate.an exhaustive simulation result also accomplished for b0 t0 b7 output and simulation result will be shown in fig.11.

The “0011001010111101”pattern in b0 which corresponds to the values of inputs from 0 to F ,can be seen in fig.

The “1101100011001110” pattern in b1, “0110111111111111” patterns in b3, “1100101100100100” pattern in b4, “100111101000101” pattern in b5,

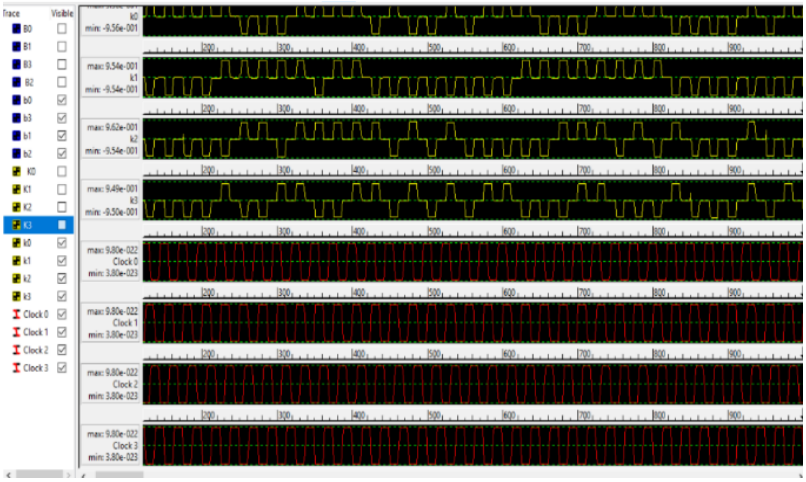

Fig 12. 4-bit GF squarer

Consider the output it is implemented using QCA cells and illustrated in fig.3.1.3 the inputs are applied through the binary wires. Each term of function is composed of two or three gates which are used

Copyright @ 2021 Authors

as xor gate.an exhaustive simulation result also accomplished for b0 t0 b7 output and simulation result will be shown in fig.12.

The “1111000111100011”pattern in k0 which corresponds to the values of inputs from 0 to F ,can be seen in fig.The “1101100011001110” pattern in k1, “0000011011111101” patterns in k2, “0001001100110101” pattern in k3.

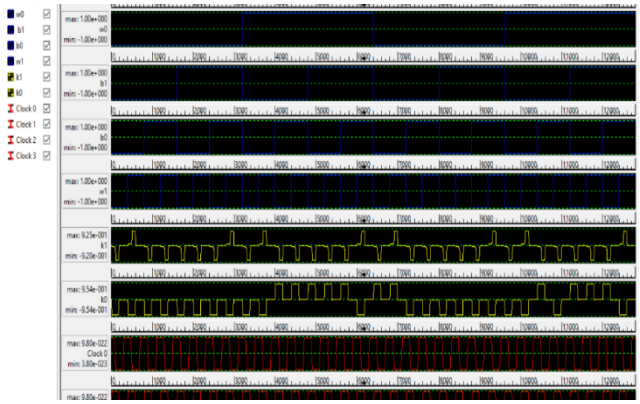

Fig 13. Lambda multiplication

Consider the output it is implemented using QCA cells and illustrated in fig.3.1.4 the inputs are applied through the binary wires. Each term of function is composed of two or three gates which are used as xor gate.an exhaustive simulation result also accomplished for b0 t0 b7 output and simulation result will be shown in fig.14 .The “0000000011111011”pattern in k0 which corresponds to the values of inputs from 0 to F ,can be seen in fig.The “1000010101111101” pattern in k1.

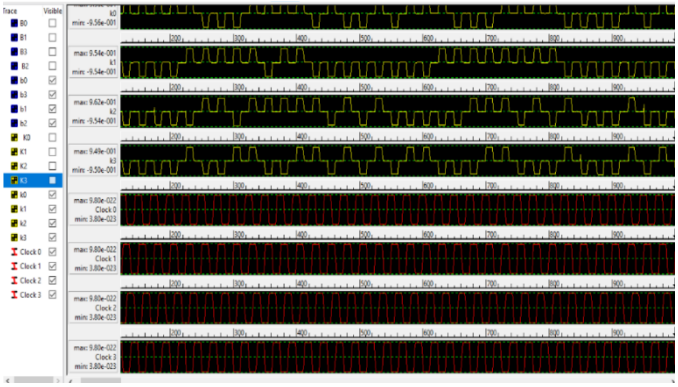

Fig 14: GF Pi multiplier

Consider the output it is implemented using QCA cells and illustrated in fig.14 the inputs are applied through the binary wires. Each term of function is composed of two or three gates which are used as xor gate.an exhaustive simulation result also accomplished for b0 t0 b7 output and simulation result will be shown in fig.15.

The “1111000111100011”pattern in k0 which corresponds to the values of inputs from 0 to F ,can be seen in fig.The “1101100011001110” pattern in k1, “0000011011111101” patterns in k2, “0001001100110101” pattern in k3.

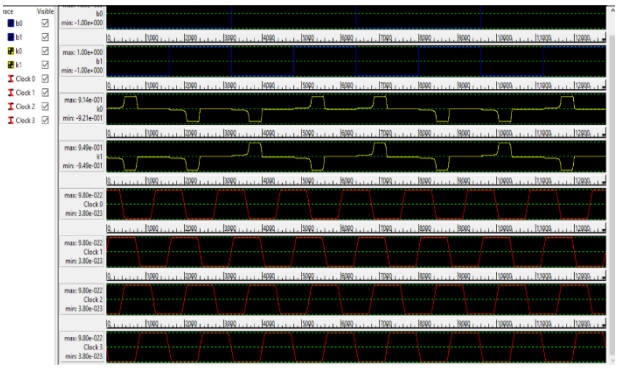

Fig.15. GF multiplicative inverse partial product module

Copyright @ 2021 Authors

Consider the output it is implemented using QCA cells and illustrated in fig.3.1.4 the inputs are applied through the binary wires. Each term of function is composed of two or three gates which are used as xor gate.an exhaustive simulation result also accomplished for b0 t0 b7 output and simulation result will be shown in fig.15

The “0000000011111011”pattern in k0 which corresponds to the values of inputs from 0 to F ,can be seen in fig.The “1000010101111101” pattern in k1.

Fig.16 Results of 3.1.7

Consider the output it is implemented using QCA cells and illustrated in fig.3.1.3 the inputs are applied through the binary wires. Each term of function is composed of two or three gates which are used as xor gate.an exhaustive simulation result also accomplished for b0 t0 b7 output and simulation result will be shown in fig.3.1.3.

The “1111000111100011”pattern in k0 which corresponds to the values of inputs from 0 to F ,can be seen in fig.The “1101100011001110” pattern in k1, “000001101111101” patterns in k2, “0001001100110101” pattern in k3.

V. CONCLUSSION

We have implemented a specific AES S Box using QCA technology. Generally, QCA should in the form of reversible logic gates and normal gate .so, we are designing this for the first time. Normally these exits only a combinational circuit in qca design. due to this reason, it is not implemented as specific application oriented form till now, so to reduce this drawback, we are the people come forward and designed this for the first time .in this we are taking encryption application .s box is small tool according to an encryption process so, we select this and executed in this paper we select the best xor gate for implementation of s box.

VI. REFERENCES

1. Lent, C. S., Tougaw, P. D., Porod, W., & Bernstein, G. H. (1993). Quantum cellular automata. Nanotechnology, 4(1), 49.
2. Laajimi, R., Ajimi, A., Touil, L., & Bahar, A. N. (2017). A novel design for XOR gate used for quantum-dot cellular automata (QCA) to create a revolution in nanotechnology structure. International Journal of Advanced Computer Science and Applications, 8(10), 279-287
3. Mohammad Amin Amiri, Sattar Mizakuchaki, Modesh Mahdevi,(2010) “Logic based QCA implementation of 4x4 S box ,
4. Ali H.Majeed,Shamin Zainal,Essam Alkaldy, “Quantum dot cellular automata,2019.
5. Chaves, J. F., Ribeiro, M. A., Silva, L. M., de Assis, L. M., Torres, M. S., & Neto, O. P. V. (2018). Energy efficient QCA circuits design: simulating and analyzing partially reversible pipelines. Journal of Computational Electronics, 17(1), 479-489.
6. Subash Kumar C S., & Gopalakrishnan, V. (2015). Modified Synchronous Reference Frame based Harmonic Extraction for Shunt Active Filter. International Journal of Power Electronics and Drive Systems, 6(4).

 Copyright @ 2021 Authors

7. P.Rajasekar, H Mangalam, "Design and implementation of power and area optimized AES architecture on FPGA for IoT application", Circuit World, ISSN 0305-6120 Vol. 47 No. 2, pp. 153-163 https://doi.org/10.1108/CW-04-2019-0039
8. Ramanand Jaiswal,Trailokya Nath Sasamal,Efficient design of exclusive or gate using 5 input majority gate in QCA.
9. P.Rajasekar,V. Lakshmi Sravani, G. Anjani Priya, V. Thrushitha, P. Bhavana,,Efficient Combinational Logic Circuit Design Using Quantum- Dot Cellular Automata, Juni Khyat - ISSN 2278-4632VOL-10 ISSUE-5 NO. 1 MAY 2020.
10. P.Rajasekar,V. Lakshmi Sravani, G. Anjani Priya, V. Thrushitha, P. Bhavana,(2020), Efficient Combinational Logic Circuit Design Using Quantum- Dot Cellular Automata, Juni Khyat - ISSN 2278-4632VOL-10 ISSUE-5 NO. 1 MAY 2020
11. P.Rajasekar, CS SubashKumar, "Implementation of Low Power Null Conventional Logic Function for Configuration Logic Block", Wireless personal communication, Springer, ISSN 0929-6212.
12. Dr.P.Rajasekar, B.V.Padmavathi, I.Sai Harshitha,G.Pavan kumar, Implementation of AES Algorithm for IOT Applications, International Journal of Research in Engineering, IT and Social Science, ISSN 2250-0588, Volume 09, Special Issue 1, May 2019, Page 104-109.
13. Penchalaiah P, Rajasekar P, Srinivas Viswanth V and Ramesh Reddy (2020), "An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence For Highly Secure Data", International Journal of Future Generation Communication And Networking, ISSN/eISSN 2233-7857/2207-9645, 30 Jun 2020, vol. 13, no.2 , pp. 1-10, 10.33832/ijfgcn.2020.13.2.01
14. "Mehta, U., & Dhare, V. (2017). Quantum-dot Cellular Automata (QCA): A Survey. arXiv preprint arXiv:1711.08153.
15. P.Rajasekar, & H.Mangalam Design of Low Power Optimized MixColumn/Inverse MixColumn Architecture for AES", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 2 (2016) pp 922-926
16. P.Rajasekar & H.Mangalam " Design and Implementation of Low Power Multistage AES S Box", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 19 (2015) pp 40535-40540
17. M.Shanthini, P.Rajasekar and H.Mangalam ,"Design of low power S-Box in Architecture Level using GF", International Journal of Engineering Research and General Science Volume 2, Issue 3, April-May 2014

 Copyright @ 2021 Authors