QCA BASED SECURE NANOCOMMUNICATION BLOCK CIPHER DESIGN BASED ON ELECTRONIC CODE BOOK

Jadav Chandra Das, Debashis De

Department of Computer Science and Engineering,
West Bengal University of Technology
BF-142, Salt Lake, Sector –I, Kolkata-700064
India
Tel.: +91-8013839069

E-mail: dr.debashis.de@wbut.ac.in

DOI: https://doi.org/10.22452/mjcs.vol31no2.3

ABSTRACT

In nanotechnology, Quantum Dot-Cellular Automata (QCA) is a new paradigm that can serve as an alternative-to CMOS circuits. In comparison to CMOS, QCA has lower device area and faster processing power with an overall low energy consumption. The complexity of cryptographic architecture is a key issue in terms of circuit density and power dissipation.Moreover, security is the major issue in nanocommunication systems. Those issues can be overcome through QCA technology. To date, only few applications of QCA have been explored in the field of cryptography. This paper illustrates the QCA design and implementation of block cipher based on electronic code book (ECB). An encoder circuit, which can function as decoder for ECB is proposed. The design requires only 0.095 μm^2 area and a latency value of 0.75. The circuit dissipates very low energy which is established through calculation of power dissipation. Due to inherent characteristics, side channel attacks like power analysis attack can be prohibited using proposed circuit. The circuit is implemented on QCA Designer platform and the design accuracy is verified via simulation results.

Keywords: QCA, Majority gate, Cipher, Encoder, Decoder, Power dissipation.

1.0 INTRODUCTION

QCA is a nano device for implementing digital circuits at nanoscale level [1-5]. Traditional systems that are based on CMOS technology have various problems such as high power dissipation, low device density, low switching speed and several physical limits [6-7]. Thus, to continue with Moore's law, a new technology, QCA was introduced [7]. QCA may be used as an alternative way out to this problem in near future due to its ultra low energy consumption, high circuit density with high switching speed [8-10]. QCA device is transistor free device where information is accumulated by the cell's polarization and the propagation of information is taking place rather than inter connected wire like in conventional system [10-12]. Cryptography [13] is the method of hiding original data from an unauthenticated person to provide security of the data. Cryptography has a significant role to achieve secure Nanocommunication. In cryptography, block cipher plays most important role to conceal original data at the communication time from the attacker. Besides, QCA can have significant application in designing low power cryptographic architecture at Nano level. This paper illustrates the QCA design and implementation of block cipher based on electronic code book (ECB). An encoder circuit, which can function as decoder for ECB is proposed. The implementation is performed on QCA Designer platform [14] and the design accuracy is verified with simulation results.

The layout of the paper is as follows. In section 2, motivation of the work is portrayed. Section 3 illustrates the background materials for QCA. Section 4 shows the proposed Block Cipher using Electronic Code Book (ECB) in QCA. Section 5 admits the simulation results, circuit complexity and power dissipation and finally section 6 prescribed the conclusion of the work.

2.0 MOTIVATION

Numerous works have already been explored to interpret the design of digital logic circuit in QCA. But the application of QCA in cryptography has not been investigated much yet. The complexity of cryptographic architecture is a key issue in terms of circuit density and power dissipation. Besides, security is the major issue in nanocommunication systems. QCA has inherent resistivity against power analysis attack. Thus in this work, QCA has been considered to design and implement encoder/decoder circuit for ECB.

3.0 BACKGROUND MATERIALS

3.1 QCA Overview

Quantum dots are the basic element for a QCA cell as shown in Fig. 1 [15-19]. The surrounding of dot is an insulating material. The dots are linked via tunnelling wire through which the electron can move between dots. Two basic QCA cell structures are shown in Fig. 1. This structure may be different due to the position of electron in a dot [20-22]. In Fig. 1, P indicates the QCA cell polarization. If P is fixed to -1 then binary '0' is trapped within cell as exposed in Fig. 1(a). If P is fixed to +1 then binary '1' is trapped within the cell as outlined in Fig. 1(b) [17].
The basic QCA logic gate is majority gate (MV) [23-25]. The block diagram of MV and its QCA layout are shown in Fig. 2(a). The output of MV is chosen from the majority of inputs [3, 8-9]. Let the three inputs of MV are P, Q, and R. Then the logic expression for MV can be written as

$$M(P, Q, R) = PQ + QR + RP \quad (1)$$

Now if R is fixed to '0', then MV has the logical AND value of P and Q, as derived in Eq. (2). If R is fixed to '1', then MV has the logical OR value of P and Q, as derived in Eq. (3). The corresponding block diagram is shown in Fig. 2. The result will be same if in place of R, either P or Q is fixed to such values.

$$M(P, Q, 0) = P.Q \quad (2)$$
$$M(P, Q, 1) = P + Q \quad (3)$$

The inversion in QCA is achieved by arranging cells diagonally, i.e., corner touching position from each other [26-28]. Due to this type of placement, the electrostatic interaction causes different polarization to the diagonal cell, as shown in Fig. 3.

(a) (b)

Fig. 1: Different QCA cell polarization (a) Logic "0", (b) Logic "1"

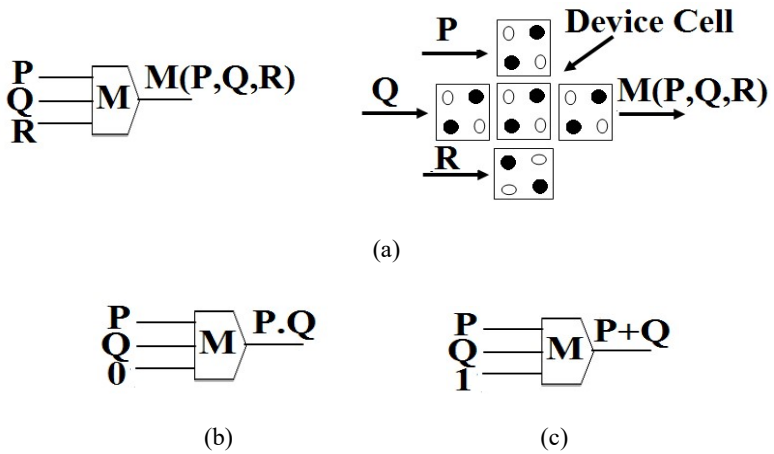


Fig. 2: (a) 3-input MV and its QCA layout, (b) QCA OR-gate, (c) QCA AND-gate

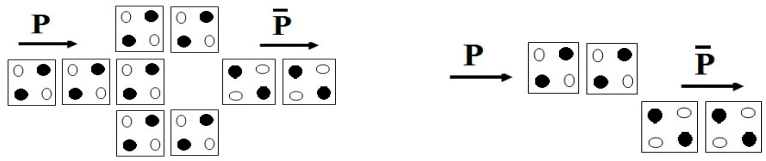


Fig. 3: QCA inverter

3.2 Related Work

The application of QCA in cryptography has been reported by several works [26-31]. In [26], simple stream cipher is designed using QCA XOR-gate whereas in [27], for encoding purpose in GSM, A5/1 stream cipher has been proposed. In [28], the serpent's s-box is studied through QCA. In [29], QCA technique is employed to achieve image steganography through LSB substitution method. In contrast to the work reported in [29], reversible logic has been incorporated in [30] to achieve low power QCA architecture for image Steganography. In [31], it has been shown how correlation and convolution technique can be adopted in QCA to design binary filter for image. But in this paper one more part is accomplished in cryptographic field through QCA.

3.3 Encoding and Decoding with ECB

ECB is the simplest mode of operation for cryptography [13]. In ECB, the incoming plaintext is partitioned into multiple blocks. The size of each block is 64-bit. Each block is then encrypted independently. For all blocks in a message, the same key is used for encryption. The encryption process is shown in Fig. 4. In Fig. 4, PTB1 represent "plain text block 1", PTB2 represent "plain text block 2" and so on. The corresponding decryption process is shown in Fig. 5. In Fig. 5, CTB1 denotes "cipher text block 1", CTB2 denotes "cipher text block 2" and so on. In decoding process, at receiver's end, the plain text is retrieved in reverse order by using the same key as was used for encryption.

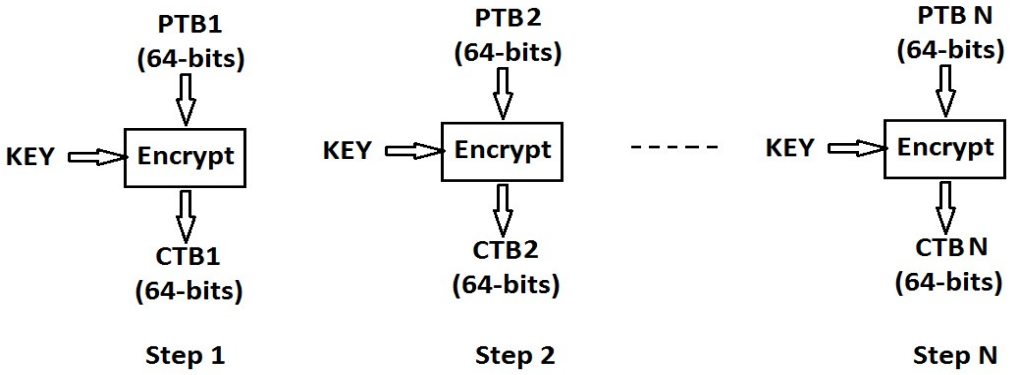


Fig. 4: Encoding process in ECB

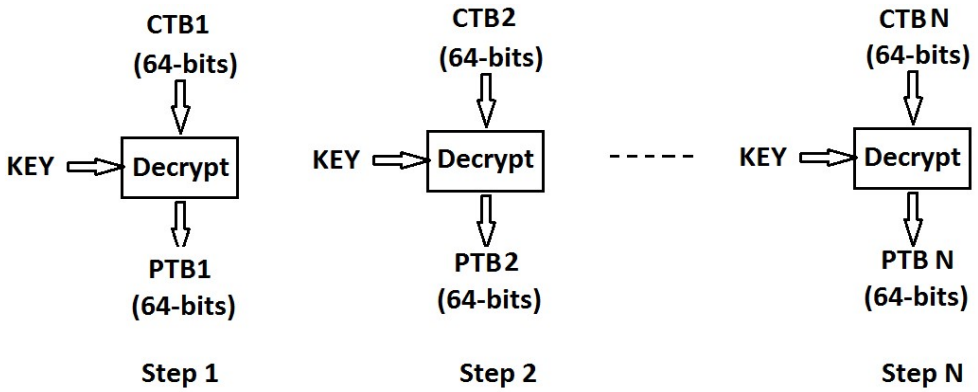


Fig. 5: Decoding process in ECB

3.4 Theoretical Example of Encoding and Decoding with ECB

1. A plain text and symmetric key as shown in Fig. 6 and Fig. 7 are considered for encoding.

JADAV AND DEBASHIS

Fig. 6: Input plain text

01001001

Fig. 7: Input key bits

2. The plain text as shown in Fig. 6 is then divided into plain text blocks (PTBs) of 64-bit each as shown in Fig. 8.

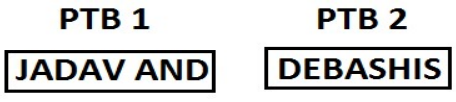


Fig. 8: Blocks of input plain text

3. The characters of each PTB are converted into ASCII value as reflected in Fig. 9.

Fig. 9: ASCII value representation of Fig. 8

4. The ASCII value of each character of Fig. 9 is translated into binary number as given in Fig. 10.

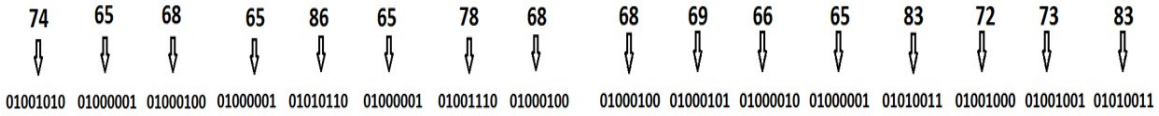


Fig. 10: Binary representation of ASCII value of Fig. 9

5. Now to perform encoding, the binary value of each character of the first PTB and the binary value of each character of the second PTB are then transmitted as a byte stream through the channels "PTB1" and "PTB2"of proposed ECB encoder/decoder as shown in Fig. 20. The key bits are transmitted through channel "KEY" of Fig. 20. The outputs of this ECB encoder/decoder are the encoded byte stream corresponding to input byte stream as shown in Fig. 11.

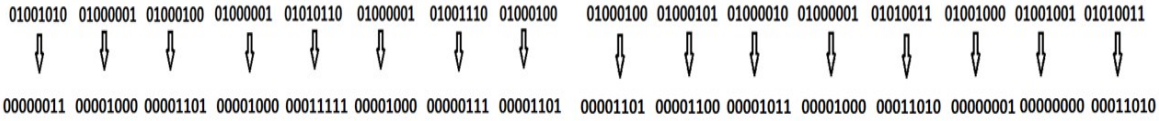


Fig. 11: Encoded byte stream of input byte stream of Fig. 10

6. Encoded byte streams are converted to ASCII value as shown in Fig. 12.

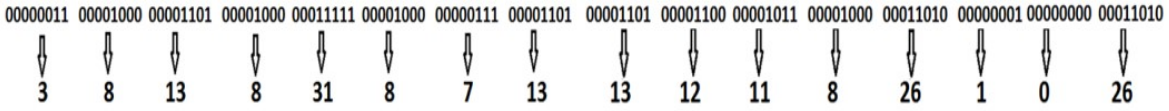


Fig. 12: ASCII value of encoded byte stream

7. Again characters are obtained from each ASCII value to generate the cipher text, as shown in Fig. 13.

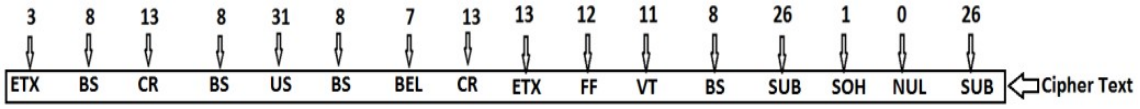


Fig. 13: Encoded character corresponding to ASCII value of Fig. 12

8. Now at decoder section, each character of the encoded text as shown in Fig. 13 is transformed into ASCII value. The result is shown in Fig. 14.

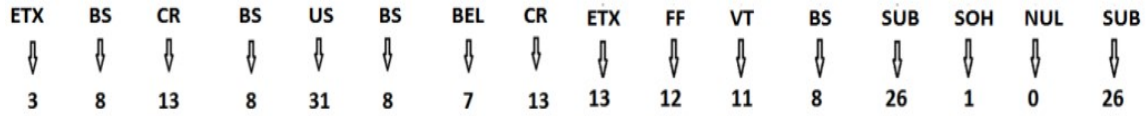


Fig. 14: ASCII value of character of cipher text

9. The ASCII value of each character is then converted into ASCII value as reflected in Fig. 15.

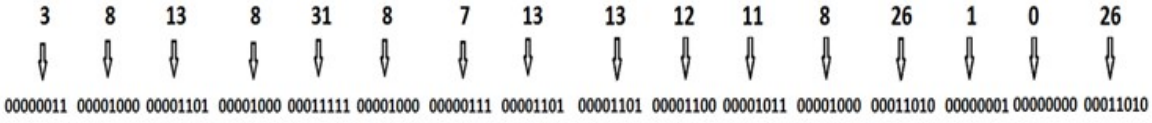


Fig. 15: Binary representation of ASCII value of Fig. 14

10. To decode the encoded bits as shown in Fig. 15, those encoded bits are then transmitted as a byte stream through the channels of ECB encoder/decoder as shown in Fig. 20. The key bits are transmitted through channel "KEY" of Fig. 20. The outputs of this ECB encoder/decoder are the decoded byte stream corresponding to encoded byte stream as shown in Fig. 16.

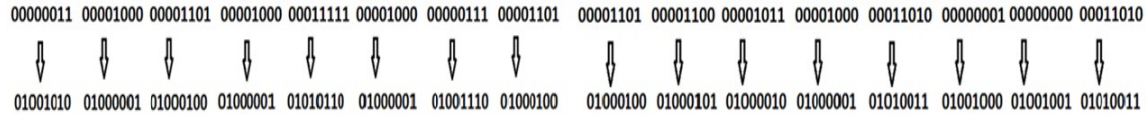


Fig. 16: Decoded byte stream of input byte stream of Fig. 15

11. The decoded byte streams are then converted to its corresponding ASCII value as shown in Fig. 17.

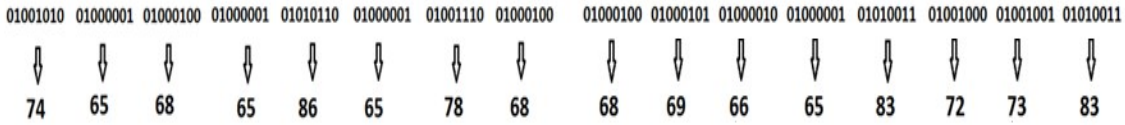


Fig. 17: ASCII value of decoded byte stream

12. Then from this the ASCII values, the original text is obtained as shown in Fig. 18.

Fig. 18: Decoded Alphabet Corresponding to ASCII value of Fig. 17

4.0 PROPOSED ECB ENCODER/DECODER CIRCUIT

Algorithm 1 shows the encoding process in ECB. In the first step, the plain text is disturbed into blocks of 64-bit each. In the second step, each such block is again divided into blocks of 8-bit each. In the third step, each bit of such 8-bit block is XOR-ed with the secret key. In the fourth step, each XOR-ed bit is merged into a blocks of 8-bit length. In the next step, all those 8-bit blocks are merged to produce 64-bit cipher text block. In final step, all the 64-bit cipher blocks are again merged to generate the cipher text.

Algorithm 1 Encoding process in ECB

Input: Plain text, Secret key
Output: Cipher text

1. Divide plain text into blocks of 64-bit each
2. Again divide each such block of 64-bit into blocks of 8-bit each
3. XOR-ed each bit of such block of 8-bit with the secret key
4. Merge each XOR-ed bit to form block of 8-bit
5. Merge each such block of 8it to produce 64-bit block
6. Again merge all the 64-bit blocks to obtain cipher text

Algorithm 2 shows the decoding process in ECB. In the first step, the cipher text is sub-divided into blocks of 64-bit each. In the second step, each such block is again divided into blocks of 8-bit each. In the third step, each bit of such 8-bit block is XOR-ed with the secret key. In the fourth step, each XOR-ed bit is merged to form blocks of 8-bit each. In the next step, each such 8-bit block is merged to produce 64-bit plain text block. In final step, all the 64-bit plain text blocks are again merged to generate the original plain text.

Algorithm 2 Decoding process in ECB

Input: Cipher text, Secret key
Output: Plain text

1. Divide cipher text into blocks of 64-bit each
2. Again divide each such block of 64-bit into blocks of 8-bit each
3. XOR-ed each bit of such block of 8-bit with the secret key
4. Merge each XOR-ed bit to form block of 8-bit
5. Merge each such block of 8it to produce 64-bit block
6. Again merge all the 64-bit blocks to obtain original plain text

The truth table of XOR-gate and proposed ECB encoder/decoder circuit is shown in table 1 and table 2, respectively. The truth table of ECB encoder/decoder circuit is derived based on theoretical example as discussed in section 3.4. In table 2, the blue colored portion represents the input output values for PTB 1 and the green colored portion signifies the input output values for PTB 2.

Table 1: Truth table of XOR gate

Input		**Output**
A	B	F
0	0	0
0	1	1
1	0	1
1	1	0

Table 2: Truth table of proposed ECB encoder/decoder

Input	Output
Binary Representation	Binary Representation
0100 1010	0000 0011
0100 0001	0000 1000
0100 0100	0000 1101
0100 0001	0000 1000
0101 0110	0001 1111
0100 0001	0000 1000
0100 1110	0000 0111
0100 0100	0000 1101
0100 0100	0000 1101
0100 0101	0000 1100
0100 0010	0000 1011
0100 0001	0000 1000
0101 0011	0001 1010
0100 1000	0000 0001
0100 1001	0000 0000
0101 0011	0001 1010

Table 2 shows that only two XOR gates are required to perform encoding as well as decoding with ECB. Thus, cascading two QCA XOR-gate, the encoder/decoder circuit for ECB has been designed as shown in Fig. 19. The equivalent QCA layout is shown in Fig. 20.

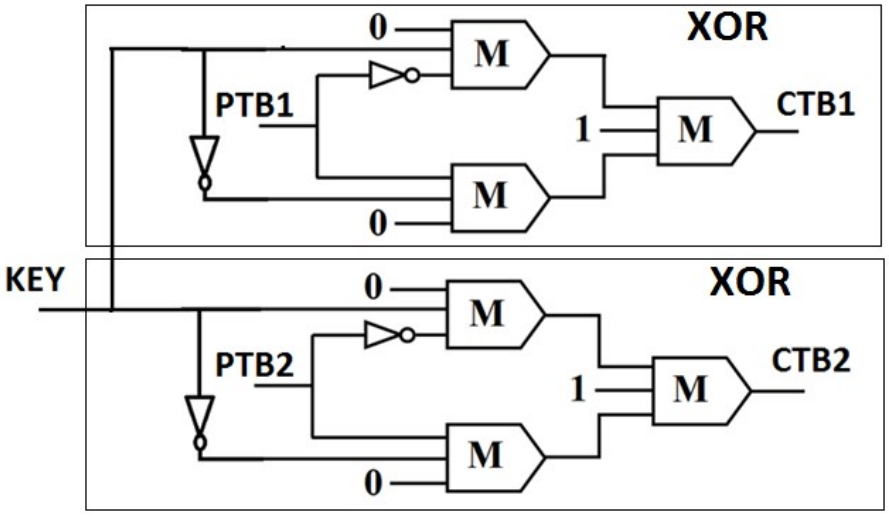


Fig. 19: QCA schematic of ECB encoder/decoder

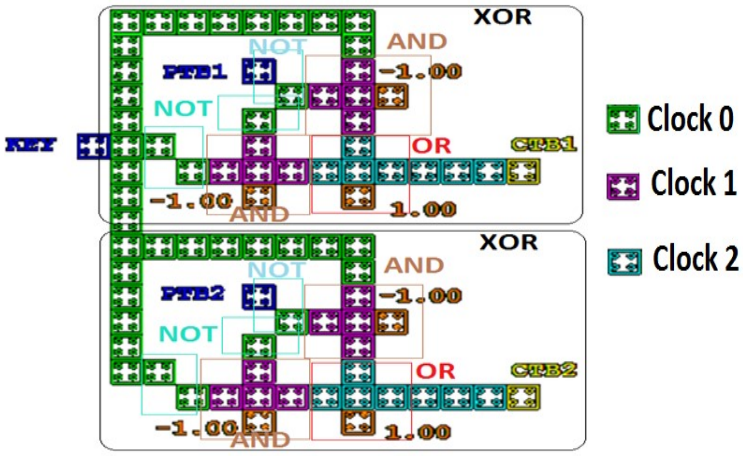


Fig. 20: QCA schematic of ECB encoder/decoder

5.0 RESULT AND DISCUSSIONS

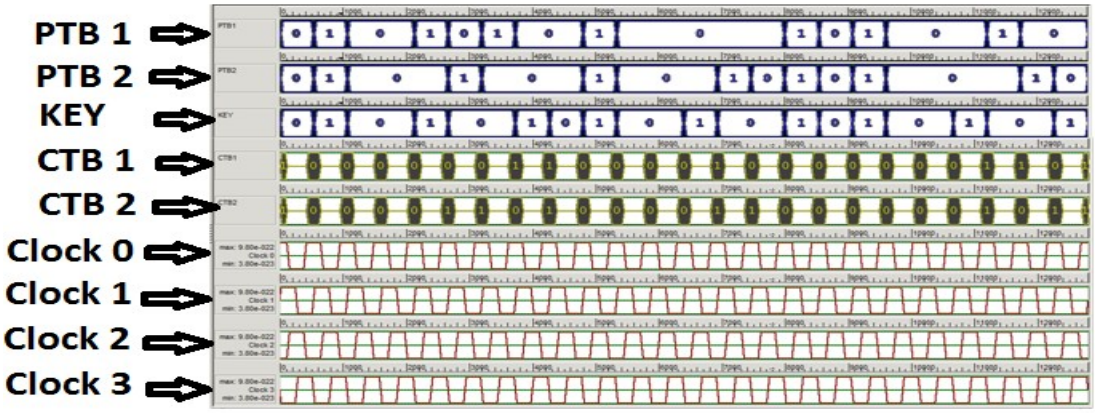
The circuit is implementation on QCA Designer tool [14]. QCA Designer is a Bi-stable simulation engine. The simulation parameters are as follows: Dot diameter 5nm, Cell width 20nm and Cell height 20nm, Radius of effect 65.00nm, Tolerance of convergence 0.0010, Number of samples 12800, Relative permittivity 12.900, Clock amplitude factor 2.0000, Clock low 3.80000e-23J, Clock high 9.80000e-22J, Layer separation 11.50000nm and Maximum iterations/sample 12000.

5.1 Design Accuracy of Proposed ECB Encoder/Decoder Circuit

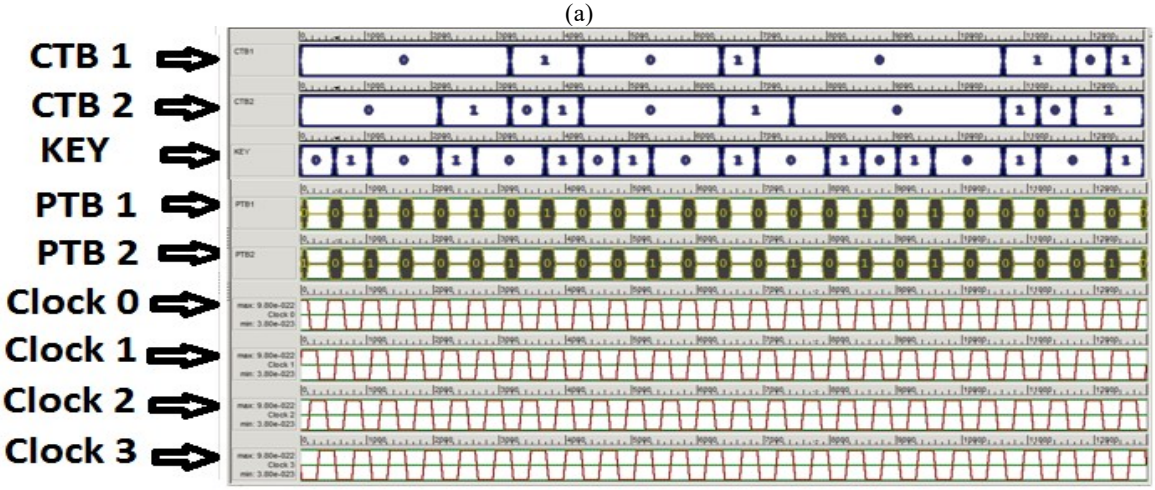
a. Fig. 21(a) and Fig. 21(b) portrayed the simulation results for encoding and decoding through proposed encoder/decoder circuit. Figure 21(a) shows that during encoding process when the value of input PTB1=0, PTB2=0 and key=0 then the output will be CTB1=0 and CTB2=0. When the value of input PTB1=1, PTB2=1 and key=1 then the output will be CTB1=0 and CTB2=0 and so on.

b. Figure 21(b) shows that during decoding process when the value of input CTB1=0, CTB2=0 and key=0 then the output will be PTB1=0 and PTB2=0. When the value of input CTB1=0, CTB2=0 and key=1 then the output will be PTB1=1 and PTB2=1 and so on.

c. These results are evaluated with the truth table 2. The comparison reflects that the all the designed circuit works efficiently. For evaluation, 8-bit sequence, i.e., one byte of the data of plain text is applied as an input value to the proposed ECB encoder/decoder circuit.



(a)



(b)

Fig. 21: Simulation result of proposed ECB encoder/decoder (a) encoding process, (b) decoding process

5.2 Complexity of Proposed ECB Encoder/Decoder Circuit

The proposed ECB encoder/decoder requires only 0.095 μm^2 areas, 6 majority gates, 6 inverters, 80 QCA cells and 3 clock zones as exposed in table 3.

Table 3: Complexity of ECB encoder/decoder circuit

Proposed QCA Circuit	#MV	# QCA Cell	Total Area (μm^2)	Cell Area (μm^2)	Area Usage (%)	Latency
ECB Encoder/Decoder	6 MVs and 6 inverters	80	0.095	0.032	33.61	0.75

5.3 Power Dissipation of Proposed ECB Encoder/Decoder Circuit

The power dissipation by proposed ECB encoder/decoder circuit has been derived in this section. During estimation, hamming distance of each QCA logic gates and different tunnelling energy (γ) has been considered [3, 32-33]. Hamming distance to each MV of proposed ECB encoder/decoder circuit (Fig. 20) is 2. For inverter, hamming

distance 1 is considered. The dissipated energy for proposed ECB encoder/decoder circuit can be derived by the equation as shown in Eq. (4).

$$P_{total} = \Sigma P_{maj} + \Sigma P_{inverter} \quad (4)$$

Where γ indicates the tunneling energy, P_{total} is the total dissipated energy, P_{maj} depicts the dissipated energy by individual MVs and $P_{inverte}$ represents the dissipated energy by individual inverters. E_k is the kink energy. The power dissipated by the proposed circuit at temperature (*T)* 2.0K and different value of γ is exposed in table 4. The proposed design has very low power dissipation. Thus side channel attacks through power analysis attack can be prohibited using proposed circuit [32].

Table 4: Power Dissipation of ECB encoder/decoder circuit in different tunnelling energy

QCA Circuit	**Power Dissipation**			
	$\gamma = 0.25E_k$	$\gamma = 0.5E_k$	$\gamma = 0.75E_k$	$\gamma = 1.0E_k$
ECB Encoder/Decoder	322.2 meV	330.0 meV	343.8 meV	360.0 meV

6.0 CONCLUSION

The simulation result specifies the truthfulness of the circuit. The circuit dissipates very low energy which is established through calculation of power dissipation. Due to inherent characteristics, side channel attacks like power analysis attack can be prohibited using proposed circuit. The proposed design can be used to turn out more powerful encoder/decoder circuit to encrypt message and to ensure secure nanocommunication. For simplicity, a simple text of three words is used to evaluate the proposed work and at each time, one byte of data from the plain text is considered as an input to the proposed circuit. But this encoder/decoder circuit can also works on higher bits.

ACKNOWLEDGEMENTS

The authors are grateful to The University Grants Commission (UGC), India, for providing with the grant for accomplishment of the project entitled "Study of Quantum Dot Cellular Automata for Designing Circuits and Implementing them for High Speed and Low Power Fault Tolerant Computing" under the UGC Major Project File No. 41-631/2012(SR) and DST FIST Project File No. SR/FST/ETI-296/2011.

REFERENCES

[1] V. Pudi and K. Sridharan, "A Bit-Serial Pipelined Architecture for High-Performance DHT Computation in Quantum-Dot Cellular Automata", *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, Vol. 23, No. 10, October 2015, pp. 2352-2356.

[2] R. Farazkish and F. Khodaparast, "Design and characterization of a new fault-tolerant full-adder for quantum-dot cellular automata", *Microprocessors and Microsystems*, Vol. 39, No. 6, August 2015, pp. 426-433.

[3] S. Sheikhfaal, S. Angizi, Sarmadi, S., Moaiyeri, M.H., and Sayedsalehi, S., "Designing efficient QCA logical circuits with power dissipation analysis", *Microelectronics Journal*, Vol. 46, No. 6, June 2015, pp. 462-471.

[4] J. C. Das and D. De, "Novel Low Power Reversible Binary Incrementer Design Using Quantum-Dot Cellular Automata", *Microprocessors and Microsystems*, Vol. 42, May 2016, pp. 10-23.

[5] J. C. Das and D. De, "Operational Efficiency of Novel SISO Shift Register Under Thermal Randomness in Quantum-Dot Cellular Automata Design", *Microsystem Technologies*, July 2016. doi: 10.1007/s00542-016-3085-y.

[6] C. S. Lent and Tougaw, P. D., "A Device Architecture for Computing with Quantum Dots", *Proceeding IEEE*, Vol. 85, No.4, April 1997, pp.541-557.

[7] C. S. Lent, P. D. Tougaw, W. Porod, and G.H. Bernstein, "Quantum cellular automata", *Nanotechnology*, Vol. 4, No. 1, July 1993, pp. 49–57.

[8] J. C. Das and D. De, "Quantum Dot-Cellular Automata Based Reversible Low Power Parity Generator and Parity Checker Design for Nanocommunication", *Frontiers of Information Technology and Electronic Engineering*, Vol. 17, No. 3, March 2016, pp. 224-236.

[9] S. Angizi, M. H. Moaiyeri, S. Farrokhi, Navi, and K. Bagherzadeh, N., "Designing quantum dot cellular automata counters with energy consumption analysis", *Microprocessors and Microsystems*, Vol. 39, No. 7, October 2015, pp. 512-520.

[10] K. Walus et al., "Quantum Cellular Automata adders", *in Proceedings of the IEEE Nanotechnology conference*, Vol. 3, December 2003, pp. 461-464.

[11] S. K. Lakshmi, G. Rajakumar, and A. G. Saminathan "Design and Analysis of Sequential Circuits Using Nanotechnology Based Quantum Dot Cellular Automata", *Journal of Nanoelectronics and Optoelectronics*, Vol. 10, No. 5, October 2015, pp. 601-610.

[12] J. C. Das and D. De, "Novel Low Power Reversible Encoder Design Using Quantum-Dot Cellular Automata". *Journal of Nanoelectronics and Optoelectronics*, Vol. 11, No. 4, August 2016, pp. 450-458.

[13] A. Kahate, *Cryptography and Network Security*, Tata McGraw-Hill Education, Inc., 2003.

[14] K. Walus, T. J. Dysart, G. Jullien, and Budiman, R., "QCA Designer: A rapid design and simulation tool for quantum-dot cellular automata", *IEEE Transactions on Nanotechnology*, Vol. 3, No. 1, March 2004, pp. 26-31.

[15] J. C. Das and D. De, "Reversible Comparator Design using Quantum Dot-Cellular Automata", *IETE Journal of Research*, Vol. 62, No. 3, July 2016, pp. 323-330.

[16] J. C. Das and D. De, "Optimized Design of Reversible Gates in Quantum Dot-Cellular Automata: A Review", *Reviews in Theoretical Science*, Vol. 4, No. 3, September 2016, pp. 279–286.

[17] K. Das and D. De, "Characterization, Test and Logic Synthesis of Novel Conservative & Reversible Logic Gates for QCA". *International Journal of Nanoscience*, Vol. 9, No. 3, June 2010, pp. 201-214.

[18] J. C. Das and D. De, "Reversible Binary to Grey and Grey to Binary Code Converter using QCA", *IETE Journal of Research*, Vol. 61, No. 3, May 2015, pp. 223-229.

[19] J. C. Das and D. De, "User Authentication Based on Quantum-Dot Cellular Automata Using Reversible Logic for Secure Nanocommunication", *Arabian Journal for Science and Engineering*, Vol. 41, No. 3, March 2016, pp. 773-784.

[20] M. Kianpour and R. Sabbaghi-Nadooshan, "A conventional design and simulation for CLB implementation of an FPGA quantum-dot cellular automata", *Microprocessors and Microsystems*, Vol. 38, No. 8, November 2014, pp. 1046–1062.

[21] S. R. Kassa and R. K. Nagaria, "A novel design of quantum dot cellular automata 5-input majority gate with some physical proofs", *Journal of Computational Electronics*, Vol. 15, No. 1, March 2016, pp. 324-334.

[22] J. C. Das, T. Purkayastha, and D. De., "Reversible Nano-Router Using QCA for Nanocommunication", *Nanomaterials and Energy*, Vol. 5, No. 1, January 2016, pp. 28–42.

[23] J. C. Das and D. De, "Reversible Half-Adder Design Using Quantum Dot-Cellular Automata", *Quantum Matter*, Vol. 5, No. 4, August 2016, pp. 476-491.

[24] J. C. Das, Debnath, B., and D. De, "Area Efficient Low Power Scan Flip-Flop Design Based on Quantum-Dot Cellular Automata", *Advances in Industrial Engineering and Managagement*, Vol. 1, No. 1, 2016, pp. 157-164.

[25] J. C. Das and D. De, "Shannon's Expansion Theorem Based Multiplexer Synthesis Using QCA", *Nanomaterials and Energy*, Vol. 5, No. 1, January 2016, pp. 53–60.

[26] J. C. Das and D. De, "Quantum Dot Cellular Automata Based Cipher Text Design for Nano Communication", in *Proceedings of the Int. Conference on Raddar,Communication and Computing*, *India*, IEEE, 2012, pp.343-348.

[27] M. A. Amiri, A. Mirzakuchaki, and Mahdavi, M. "A5/1 Implementation in Quantum Cellular Automata", *Nanoscience and Nanotechnology*, Vol. 1, No. 2 , January 2011, pp. 58-63.

[28] M. A. Amiri, S. Mirzakuchaki, M. Mahdavi, and N.K. Darav, "Serpent Implementation in Quantum Cellular Automata", *Nanoscience and Nanotechnology*, Vol. 1, No. 1, April 2011, pp. 1-7.

[29] J. C. Das, Debnath, B., and D. De, "Image Steganography using Quantum dot Cellular Automata", *Quantum Matter*, Vol. 4, No. 5, October 2015, pp. 504-517.

[30] B. Debnath, J. Das, and B. Debnath, "Reversible Logic Based Image Steganography Using QCA for Secure Nanocommunication", *IET Circuits Devices and Systems*, March 2016, doi:10.1049/iet-cds.2015.0245.

[31] B. Debnath, J. C. Das, and D. De., "Correlation and convolution for binary image filter using QCA", *Nanomaterials and Energy*, Vol. 5, No. 1, June 2016, pp. 61–70.

[32] W. Liu, S. Srivastava, L. Lu, and E.E. Swartzlander Jr., "Are QCA Cryptographic Circuits Resistant to Power Analysis Attack?", *IEEE transactions on nanotechnology*, Vol. 11, No. 6, October 2012, pp. 1239-1251.

[33] S. Srivastava, S. Sudeep, and B. Sanjukta, "Estimation of upper bound of power dissipation in QCA circuits". *IEEE trans. on nanotechnol.*, Vol. 8, No. 1, September 2009, pp. 116-127.