Theoritical Study of Channel Coded Secured Nano Communication Network in QCA Platform.

SUPARBA TAPNA (suparba7@gmail.com)
Durgapur Institute of Advanced Technology and Management https://orcid.org/0000-0003-4025-8404
Kisalaya Chakrabarti
Haldia Institute of Technology
Debarka Mukhopadhyay
Christ University Faculty of Engineering

Research Article

Keywords: Cipher, Quantum Dot Celluar Automata(QCA), Clocking scheme, Mux and Demux with parity, Majority Gate, PRBS, Schrodinger Equation for Quantum Enhancement, Security for Quantum level, n value for Quantized states

Posted Date: June 3rd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1504926/v1

Noname manuscript No.
(will be inserted by the editor)

Theoritical Study of Channel Coded Secured Nano Communication Network in QCA Platform

Suparba Tapna · Kisalaya Chakrabarti · Debarka Mukhopadhyay

the date of receipt and acceptance should be inserted later

Abstract QCA "Quantum Dot-Cellular Automata" is another nano-technology model, that fills in an elective answer for CMOS that have numerous actual cutoff points and heaps of hardware limits. QCA is a semiconductor less innovation as well as data is passed dependent on electron charge and by common electrostatic repugnance among them. QCA has exceptionally higher gadget thickness, quicker exchanging speed timing and very low force utilization. QCA circuits in cryptographic application may assume a significant part. Both unscrambling as well as encryption measure is executed utilizing rationale circuit based on QCA. The research paper depicts fundamental method for creating cipher text in QCA, which may be useful in secure nanocommunication based on QCA.In secured encryption it is finding the realistic way in a secured authentication. The results' execution along with testing is carried out by utilizing QCA Designer-2.0.3 tool.

Keywords Cipher · Quantum Dot Celluar Automata(QCA) · Clocking scheme · Mux and Demux with parity · Majority Gate · PRBS · Schrodinger Equation for Quantum Enhancement · Security for Quantum level · n value for Quantized states

Suparba Tapna
Department of Electronics & Communication Engineering, Durgapur Institute of Advanced Technology and Management, Durgapur,West Bengal, India
Tel.: 9007721804
E-mail: suparba7@gmail.com

Kisalaya Chakrabarti
Department of Electronics & Communication Engineering, Haldia Institute of Technology, Haldia,West Bengal, India Tel.: 8617736215
E-mail: kisalayac@gmail.com

Debarka Mukhopadhyay
Department of Computer Science & Engineering,Faculty of Engineering, CHRIST (Deemed to be University), Bangalore,Karnataka, India Tel.: 8777389550
E-mail: debarka.mukhopadhyay@gmail.com

1 Introduction

QCA is basically the nanotechnology, which could be utilized with the semiconductor-based CMOS system as an elective response. CMOS circuit have issue in their planning as its various segments relies upon one another and furthermore have numerous actual cutoff points [1],[5]. Thus, in CMOS circuit future adaptability is the most concerning issue in light of the fact that no of cells at nanoscale implanted in a solitary chip will increment along with circuit synchronization intricacy will expand much more and limited to few actual wonders. By utilizing QCA, this issue can be tackled as QCA is semiconductor having high thickness, higher timing recurrence along with low force utilization [3],[4].

In time, it is necessary to reduce the size to design a coordinated circuit, for example by increasing the circuit thickness. So we have to switch from semiconductor to semiconductor and QCA provides the opportunity. Electron charges present in the Quantum Dots are transmitted by QCA data irrespective of electrical energy (beat), as in CMOS [8],[9] circuits. In cryptography assumes significant part for addressing the real information into an encoded (non-discernible) from unsecured to secured transformation to get authentic information[12],[13]. This specific article depicts a straightforward method to produce cipher text utilizing QCA. The simulation of the proposed implementation is utilizing QCA Designer-2.0.3[10],[11]. The organization of entire manuscript represent for section 2 is overview of QCA ,section 3 briefly describe abot QCA clocking,section 4 for secure nanocommunication utilizing in QCA.After section 4 we are discussing about PRBS in fifth section and reducing the bit error rate in channel coding in section 6 & results and discussion is represented in section7.The last section is concluding about this research work.

2 QCA Overview

The overall implication is assumed from Quantum Dot Cellular Automata(QCA) perspective. With such a nanotechnological phenomenon are correlated to construct in the finding of this paradigm which is very suitable for the proposed approach and also indicated in this research work in a true manner.

2.1 QCA Cell

The essentials of a four dots of the QCA [4],[16], which can bind an electron within, are presented in Fig. 1(a). Each speck has a burrowing wire that can burrow through each of the four dots, connecting them to each other. Another 2 free electrons were applied to the cell of QCA and as the electrons repel each other, they were placed within QCA in antipodal conditions. There can be two distinct designs of QCA cell, named QCA cell polarization and defined

by P, contingent on this electron situation. As demonstrated in fig1 (b) as well as fig1(c).

P=+1 along with P=-1 demonstrates parallel binary logic such as '1' as well as '0' separately whereas P=0 indicates null cell such that contains no data. [17],[18]

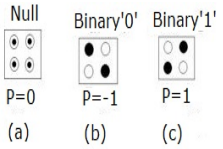

Fig. 1: Cell polarization of different QCA

2.2 Overview of Majority Gate

Majority gate for three i/p is essential rationale entryways utilized in a QCA that monetizes according to the majority gate of the data source[21],[22]. Suppose A, B, C be three contributions to majority gate, at that point rationale work for dominant part entryway may be composed as

$$F(A,B,C) = AB + BC + CA \tag{1}$$

If we fixed its contribution estimation to logic values '0' as well as '1', at that point rationale AND- gate or potentially entryway may be formulated individually [17],[20] composed as:

$$F(A,B,0) = A.B \tag{2}$$

$$F(A,B,1) = A + B \tag{3}$$

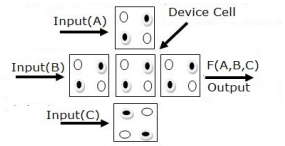

Fig. 2: Realization of majotrity gate for predicted o/p[8]

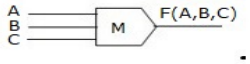

Fig. 3: Realization of majotrity gate for predicted o/p[8]

Table 1: Majority gate truth table

A	B	C	$F(A,B,C)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	1	0	1
1	0	1	1
1	1	0	1
1	1	1	1

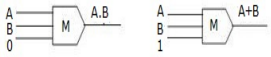

Fig. 4: AND- gate and OR- gate in QCA[8]

2.3 Wire logic in QCA

QCA wire can be formed near setting about QCA cell continuously, whereas data is conveying by electrostatic communication among cells of QCA. These wire assists with conveying data inside a QCA circuit. fig.4 (a) and (b) shows the two unique sorts of QCA wire [18] [21]. The polarization in 90˚ QCA wire stays similar in whole QCA exhibit whereas the polarization in 45˚ QCA wire substitutes in each continuous cell in cluster[**?**],[**?**].

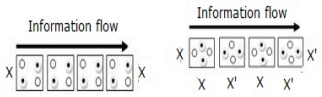

Fig. 5: 90˚ wire and 45˚ wire in QCA[8]

2.4 Inverter circuit in QCA

As given in Fig.5, QCA inverter may be shaped when at 45°point QCA cells sets (corners contacting) as demonstrated in [20],[21]. Because of electrostatic repugnance among cells, "0" and "1" will be the set logic values that can be changed over to "1" as well as "0" separately.

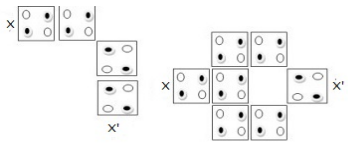

Fig. 6: QCA inverters[8]

3 QCA Clocking

QCA timing has total 4 stage slacking by $\pi/2$ [10],[19] as demonstrated in Fig.6 that makes another way to plan nano-circuit not the same as CMOS circuits [24].

Switch stage—the boundary among QCA cell dabs is increased. The specks are affected through its adjoining electron where electron begins burrowing among dabs. Hence, QCA cell gets energized. Hold stage— Cell's hindrance stays high where electron can't burrow among dots as well as cell keeps up its present statuses (fixed polarization).

Release stage—hindrance among spots are brought down, electron may burrow through specks as well as QCA cell become un-enraptured.

Relax stage—hindrance stay at brought down along with cell stays in un-captivated state.

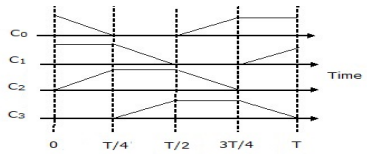

Fig. 7: Four phase clocking[2]

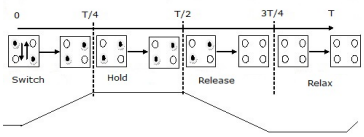

Fig. 8: QCA operation during one clock phase [2]

4 Secure Nanocommunication using QCA

Secure communication is very much important for data privacy. Now a days it is also implicated more authenticated way to consider for sharing some information in between sender and receiver. In this proposed technique is relevant the actual phenomenon for considering the same kind of assumption through channel coding in a nano communication network.

4.1 Cryptography

Cryptography is an encoding (changing) strategy where message from clear structure to non-meaningful structure to give security from an unauthorized access [14],[15].

4.2 QCA Encryption and QCA Decryption

Encryption is a way of converting a regular instant message into an unrecognizable code, and decryption is the reverse cycle of changing the code into an instant message, as shown in Figure 9.[12]

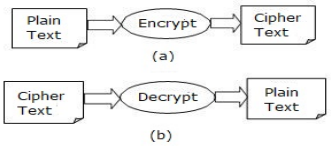

Fig. 9: Encryption System and Decryption System

4.3 QCA Plain Text and QCA Cipher Text

Generic content is a message that can be received by the sender, recipients, and others with access to the content. Then, using the appropriate scheme to construct the generic content, the subsequent message is called the ciphertext.

4.4 Stream Cipher and Block Cipher

The plain text should be possible in symmetrical key cryptography in two basic ways – stream code as well as square code [14],[15]. Each byte is then scratched with the key in the current figure and plain content is encrypted on block figure in a square of bytes, all with the key shown in Figure 10.

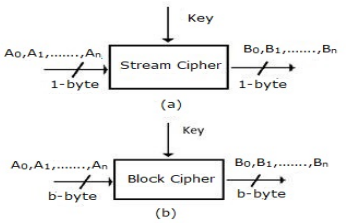

Fig. 10: QCA Stream cipher and QCA Block cipher

4.5 QCA Encryption and Decryptyion in Stream Ciphers

Suppose plain text, ciphertext along with stream key comprises singular pieces, such as $(A_i, B_i, K_i \in 0, 1)$.At that point structure [15] the meaning of encryption as well as decoding capacity may be composed as

Encryption:

$$B_i = EK_i(A_i) \equiv B_i + K_i \mid 2 \mid \tag{4}$$

Unscrambling:

$$A_i = DK_i(B_i) \equiv A_i + K_i \mid 2 \mid \tag{5}$$

The relating outline is appeared in Figure 11.

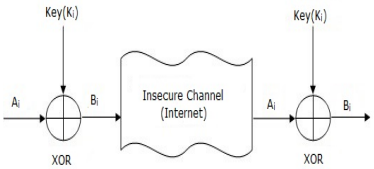

Fig. 11: Encryption and Decryption using Stream Ciphers

In reality encryption as well as decoding capacity are coherently similar [15] as demonstrated below

$DK_i(B_i) \equiv A_i + K_i \mid 2 \mid \equiv (A_i + K_i \mid 2 \mid) + K_i \mid 2 \mid$[From articulation1] $\equiv A_i + K_i \mid 2 \mid + K_i \mid 2 \mid \equiv A_i + 2K_i \mid 2 \mid \equiv A_i + 0 \mid 2 \mid A_i \mid 2 \mid Q.E.D$

Now, the articulation estimation $(2K_i \mid 2 \mid)$ is consistently zero as

$(0 \mid 2 \mid) \equiv 2$. Now, If $K_i = 0$ then

$2K_i = 2 \cdot 0 \equiv (0 \mid 2 \mid)$.

Also, on the off chance that

$K_i = 1, 2K_i \doteq 21 \doteq 2 \equiv (0 \mid 2 \mid)$.

Throughout encryption as well as decoding cycle to create figure text and plain content individually, XOR coherent activity is utilized as in light of the fact that the activity $B_i \doteq EK_i(A_i) \equiv X_i + S_i \mid 2 \mid$ generate yield, which is identical to XOR yield entryway activity as demonstrated in table 2 and 3.

Table 2: Encryption operation truth table

A_i	K_i	$B_i \equiv A_i + K_i \mid 2 \mid$
0	0	0
0	1	1
1	0	1
1	1	0

Table 3: Truth table of xor operation

Ai	Ki	Bi
0	0	0
0	1	1
1	0	1
1	1	0

The first single material is without question created from plain text as seen in Figure 12, since XOR operation is reversible.

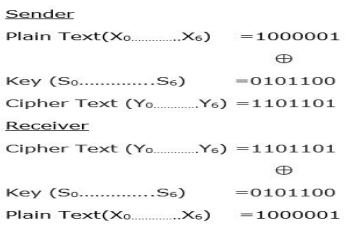

Fig. 12: Example of Encryption and Decryption

The expression 3 & 4 were rewritten from the XOR-gate truth table as in Table 2.

$$B_i = EK_i(A_i) = A_i \oplus K_i = A_i\bar{K}_i + \bar{A}_iK_i \tag{6}$$

$$A_i = DK_i(B_i) = B_i \oplus K_i = B_i\bar{K}_i + \bar{B}_iK_i \tag{7}$$

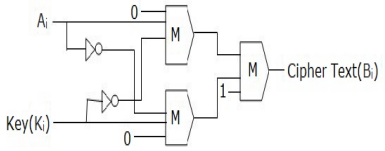

Fig. 13: Cipher Text generation schematic in QCA

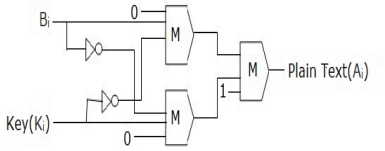

Fig. 14: Plain Text generation schematic in QCA

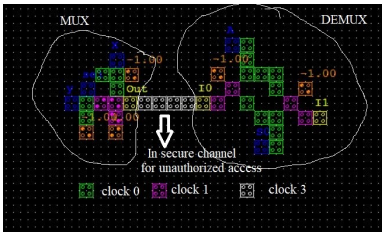

Fig. 15: Encoder and Decoder circuit in QCA with MUX and DEMUX application

The outline shown in Figure 13 and Figure 14. The relevant layout in QCA is shown in Figure 15.

And below is an expansion of the related majority gate expression:

$$B_i = F(F(A_i, \bar{K}_i, 0), F(\bar{A}_i, K_i, 0), 1) \tag{8}$$

$$A_i = F(F(B_i, \bar{K}_i, 0), F(\bar{B}_i, K_i, 0), 1) \tag{9}$$

In Figure 15 we are assuming for symmetric key cryptography, the above depiction relies the several plain to one cipher text and in case of decoder the several cipher text to one plain text for assuming as a mux and demux is encryption and decryption symmetric sequence cryptography.

4.6 Proposed Work for secure network Channel

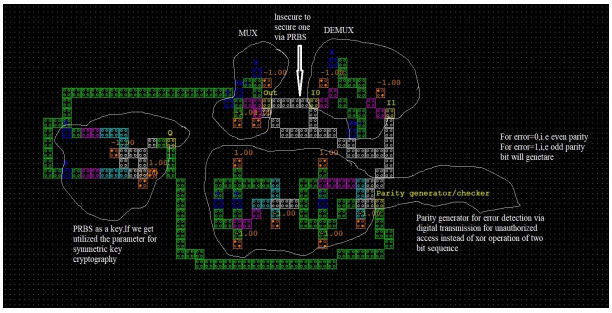

Fig. 16: QCA nanocommunication with Channel Coding

So Nano communication is more secure, so we need to recommend Nano network with channel-encrypted pseudo-binary sequence generator for Crypto network in model prediction. It is generally used to in advanced correspondence frameworks to shield the computerized data from commotion and obstruction and diminish the quantity of bit errors & is generally refined by specifically redundant bits into the sent data stream.

5 Pseudorandon Binary Sequence(PRBS) Generator

We are proposing 1 bit PRBS generator to implicate this finding & application for insecure channel to secure one channel coding. Here the following figure illustrates Pseudo Random Binary Sequence generator circuit.It has applied the concept in case of QCA nanocommunication for cryptographic application which is utilized as a key that automatically changes for every kind of simulation & also increases the possibility to protect against unauthorised access from encryption & decryption in this secure nanocommunication network.

The Figure 17 depicts that we have to realize for fixed sequence 5 “zeros” & 3 “ones”(i,e 8 bit as 01001100) but position will change as of pseudorandom sequence for PRBS generator in the output waveform and have a major role in QCA nanocommunication network for channel coding application.

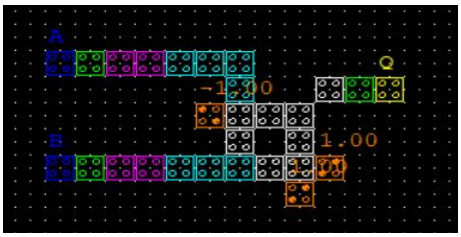

Fig. 17: PRBS generaor[Blue are denotes two inputs ,Yellow represents output, Green for clock 0,Pink for clock1,Indigo for clock 2 & white for clock 3]

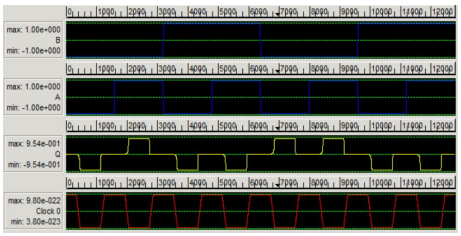

Fig. 18: Output waveform of PRBS generator

6 How to reduce bit error rate in channel coding application

The methodology that can be received to lessen the bit error rate is to decrease the transmission capacity. Lower levels of commotion will be achieved and subsequently the sign to clamor proportion will improve. Again this outcomes in a decrease of the information throughput attainable. Since we need to fundamentally presented as 8 digit of sequence, So here in phenomenon the bit error rate is diminished in 10^8 bit/sec. Channel coding is used to work on signal quality and reduce the bit error rate (BER). The use of a channel coding scheme is to recover from errors that occur during transmission on the respective channel. In the respective setting, the receiver side BER can be affected by channel jitter, impedance, torsion, bit timing issues, limitations, remote multipath interference, etc. The BER can be improved by choosing a strong signal strength (unless it causes crosstalk and more partial errors), choosing a slow and strong tuning plane or a stream encoding plane, and applying the channel coding management, for example, repeat forward error correction codes. Transmit BER is the number of incorrectly recognized parts before error correction, separated by the number of full motion bits (counting of repeated error codes). The BER data, roughly equivalent to the integral error probability, is the number of decoded bits that still have errors after the error changes, separated by the total number of decoded bits (the payload). Usually, the transmission BER is larger than the data BER. The BER data are affected by the strength of the forward error correction (FEC) code.

7 Schrodinger Equation for Quantum Enhancement security level to optimized quantized states

Burrowing electrons have double wave molecule property. Every electron molecule, while traveling through the passage, carries on the collectively of waves as proposed by deBroglies speculation on related waves [12],[13]. As indicated by this theory this gathering of waves is the only superposition of a few monochromatic waves with identical plentifulness and stage however imperceptibly with varied frequency [14],[15]. Let the superposition condition of an electron burrowing between the spots the a way be ψ (a). Fourier change communicates the superposition

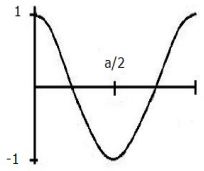

Fig. 19: QCA cell in 2D representation [20]

an electron's state (a),

$$\psi(a) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \phi(s) e^{i(sa)}\, ds \tag{10}$$

where the adequacy of the superposition wave is represented by ψ (s). k = $\frac{2\pi}{\lambda}$ is the wave spread speed,the wavelength is denoted by λ and $i = \sqrt{-1}$. The trademark bend of an electron wave is illustrated by Figure 19 while moving through channels [19]. At whatever point electron is confined, it is situating at a = 0 and $e^{i(sa)} = 1$ achieved this value. It implies electron influxes with varied frequencies meddle valuably and no motions are announced. Henceforth ψ(a) achieves top at a = 0 with varying upsides of a, the segments of $e^{i(sa)}$ are inserted in Equation 10. In this way bringing about motions and the worth of ψ(a) is acquired. At $\frac{a}{2}$, $e^{i(sa)}$ accomplishes least worth and trademark bend accomplishes the negative pinnacle. At the point when 'a' develops starting here, the

worth of $e^{i(sa)}$ likewise develops bringing about development of ψ(a).

As expressed before, a clock signal is the energy provider to the electrons for changing their state. We accept that between spot channels are encountering infinite V(a) potential energy in the positive a direction. At that point time, autonomous Schrodinger wave condition is,

$$\frac{p^2\psi(a)}{da^2} + \frac{2m}{\hbar^2}(En - V(a))\psi(a) = 0 \tag{11}$$

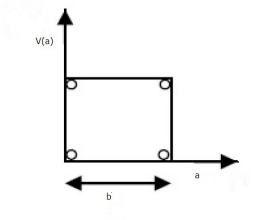

Fig. 20: Characteristic Curve [20]

where electron mass is denoted by m, decreased plank constant by $\hbar$ [23],[24], In finite arrangement of discrete energy levels is expressed by E_n relating to all conceivable non-negative basic upsides of n. whereas the quantum number is given by n. Condition 12 can be diminished to

$$E_n = \frac{n^2\pi^2\hbar^2}{2mp^2} + V(a) \tag{12}$$

where p is the atomic cell measurement [19]. Whenever voltage is given to the atom as V volt with C intersection capacitance at that point, articulation will be produced as [16],

$$\frac{n^2\pi^2\hbar^2}{2mp^2} + V(a) = \frac{1}{2}CV^2 \tag{13}$$

This articulation will help to compute the working RMS voltage of the framework.

To compare two quantum numbers n_1 and n_2, we need two discrete states i,e. E_{n1} and E_{n2}. The electron may travel starting with one energy state then onto the next if the whole or contrast of quantum no. is an even number[19].To move from this condition to the ground, we must discover the nth quantum number, the energy is transmitted by a cell between 3.85×10^{-3} eV to $10^{-4}eV$. This change is communicated as,

$$\Delta E = E_n - E_1 = \frac{\pi^2\hbar^2}{mb^2}(n^2 - 1) \tag{14}$$

producing framework needs to emanate energy in the reach between 3.85×10^{-3} eV to $10^{-4}eV$. Considering most reduced energy esteem i.e., 3.85×10^{-3} eV to be equivalent to ΔE in Equation 15,the connection between cell measurement (p) and quantum no. (n) is given as

$$n^2 - 1 = 16.24 \times 10^{41}p^2 \tag{15}$$

Now, the most elevated energy radiation that is 10^{-4} eV is being taken into account and comparing it to ΔE_n in Equation 16, the connection between subatomic cell measurement (p) and quantum no. (n) is given as

$$n^2 - 1 = 2.59 \times 10^{42} p^2 \tag{16}$$

A cautious investigation of Figure 20 outcomes that at at 2 V_{rms} working voltage as well as a temperature of 1000 K the phones accomplish a component of 10 nm believing the expected energy of an electron to be 4.2×10^{-20} Joules and the value of C will be 200 atto-farad. If atomic cell measurement is viewed as 10 nm, for the most minimal degree of radiation, Equation 15 creates the worth of n to be 290. On the off chance that we apply a similar technique in Equation 16 for the most elevated restriction of radiation, the value of n will be 298, with 1300 ° C updated temparature value at a voltage of 2.81 V_{rms} for a solitary atomic cell,Equation 16 should be written as,

$$\nu_2 = \frac{\pi \hbar}{2mp^2}(n^2 - 1) \tag{17}$$

where ν_2 is radiation frequency.

Equation 16 produces the corollary that $\nu_2 = 1,015 \times 10^{15}$Hz has a value of n=298 and d=10 nm and $\nu_2 = 9,612 \times 10^{14}$Hz with n= 290 and d = 10 nm ranges from 1×10^{15}Hz to 10^{15}Hz, the repeat range of the existing frame. The above calculations are for a subatomic cell. The intensity of the radiant energy for N subatomic cells arranged in a course is recorded in the range of $3.85 \times 10^3 \times$N to 10^4 times N..We have also shown the variation of potential energy in different states of quantum level. It is illustrated in Figure 21 and Figure 22 calculated from the open source[24].

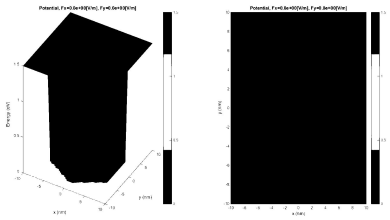

Fig. 21: 1st Quantum states potential energy in 2D representation

Here we have computed the different condition for n value approaches in a Tabular formation.It also have analysed in Table 4.

8 Results and Discussions

The circuit was executed and imitated using the Bistable QCA Designer2.0.3 game engine [10], yield came after the second control span as shown in Figure 13 and confirmed using the pinboard. sole reason. Figure 13 shows the end of the encoder when $K_i = 0$, $A_i = 1$ then $A_i = 0$ and $B_i = 1$, $K_i = 1$ then

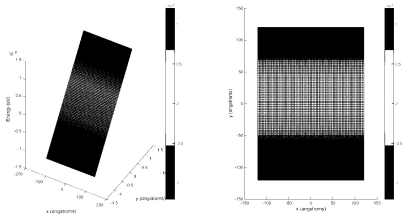

Fig. 22: 2nd Quantum states potential energy in 2D representation

Table 4: Comparative study of different n value approaches in the state of Quantum level

Theoritical Assumption	Expression	Energy	Value of Quantum number
Quantum Enhancement Security for Quantum number & cell dimension[Existing] [20]	$n^2 - 1 = 13.29 \times 10^{21} p^2$	5×10^{-3} ev to $10^{-4} ev$	116
Quantum Enhancement Security for Quantum number & molecular cell dimension[Existing][20]	$n^2 - 1 = 2.66 \times 10^{22} p^2$	$10^{-4} ev$	162
Quantum Enhancement Security for Quantum number & cell dimension[Proposed]	$n^2 - 1 = 16.24 \times 10^{41} p^2$	3.85×10^{-3} ev to $10^{-4} ev$	290
Quantum Enhancement Security for Quantum number & molecular cell dimension[Proposed]	$n^2 - 1 = 2.59 \times 10^{42} p^2$	$10^{-4} ev$	298

$B_i = 1$, etc as shown by the green circle. At the end of decoder when $K_i = 0$, $B_i = 1$ then $A_i = 1$ and $K_i = 1$, $B_i = 1$, then $A_i = 0$, etc as indicated by the blue mark. Attached limits used to estimate determineable: impact radius 65.00 nm, Clock high 9.8×10^{22}J, 1,000 maximum iterations, 12,800 times test, 12,900 Relative License, 5 nm Spot Distance, 20 nm Cell Size, and 20 nm Cell Width.

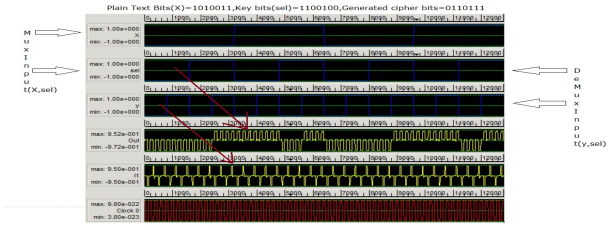

Fig. 23: Encoder and Decoder circuit simulation result in QCA

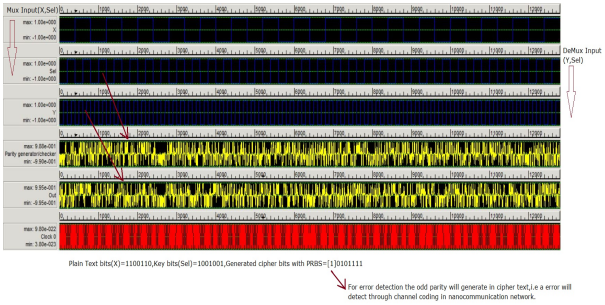

Fig. 24: Simulation result of QCA naoncommunication with Channel Coding

Table 5: Encoder(MUX) and decoder(DEMUX) circuit description

QCA Mux and Demux	No.of Majority gate used	No. of Cells	Area	Delay
1	6 MG and 3 inverters	40	$324nm^2$	3 clock cycles

2.0000 is set to the clock crest factor, 11.50000 nm is set to layer separation, 0.001000 convergence tolerance and 3.8×10^{23}J lower clock.

Table 6: Circuit for nano-communication in QCA with channel coding description

QCA Mux and Demux with Parity Generator	Majority gate used	Cells No.	Area utilized	Circuit delay
1	14 MG and 4 inverters	221	$0.42nm^2$	4 clock cycles

9 Conclusions

Due to the creation of side-channel attacks, crypto utility can be exploited to the extent of brute force and electromagnetic forensic attacks. With that, since QCA has extremely low force usage and extremely fast time rates, the proposed circuit can be a guiding principle for creating a secure QCA encryption module instead of one. normal size. Encryption as well as decryption is done on a 7 bit message using a 7 bit key, but it can very well be done on any length of message bit as well as key material using a offer. The circuit now requires only 3 MVs, 42 cells, 3 clock regions, 2 inverters, as well as 36,000 nm^2 regions for the decoder and encoder. For such a view, we have shown more secure encryption in this cryptographic approach in QCA. This indicates and improves more

secure authentication through channel encryption in nanocommunication networks with Pseudo-Randomn Binary Sequence (PRBS). Future performance of cryptographic calculations for a secure nano-matching framework based on QCA can be performed using this proposed circuit.

References

1. M. Niemer, P. Kogge, Problems in designing with qcas: Layout = timing, Int. J.Circuit Theory Appl 29 (2001) 49–62.
2. S. Umira, R. Qadri, Z. Bangi, M. Banday, G. Bhat, A novel cryptographic design in quantum dot cellular automata (2018) 1–6.
3. C. Lent, P. Tougaw, A device architecture for computing with quantum dots, Vol. 85, 1997, pp. 541–557.
4. B. Debnath, J. Das, D. De, S. Mondal, A. Aumadian, M. Salimi, M. Ferrara, Security analysis with novel image masking based quantum-dot cellular automata information security model, IEEE 8 (2020) 117159–117172.
5. K. Navi, S. Sayedsalehi, R. Farazkish, M. R. Azghadi, Five-input majority gate, a new device for quantum-dot cellular automata, Comput. Theor. Nanoscience 7 (2010) 1546–1553.
6. P. Singh, A. Majumder, B. Chowdhury, R. Singh, N. Mishra, A novel realization of reversible lfsr for its application in cryptography (2015) 601–606.
7. M. Amiri, M. Mahdavi, S. Chaki, Qca implementation of a5/1 stream cipher (2009) 48–51.
8. V. Vankamamidi, M. Ottavi, F. Lombardi, A serial memory by quantumdot cellular automata (qca), IEEE Trans. Computer 57 (2008) 606–618.
9. W. Liu, S. Srivastava, L. Lu, M. O'Neill, E. Swartzlander, Power analysis attack of qca circuits:a case study of the serpent cipher (2013) 2075–2078.
10. A. Cilardo, Exploring the potential of threshold logic for cryptographyrelated operations, IEEE Transactions on Computer 60 (2011) 452–462.
11. W. Liu, S. Srivastava, L. Lu, M. O'Neill, E. Swartzlander, Are qca cryptographic circuits resistant to power analysis attack?, IEEE Transaction on Nanotechnology 11 (2012) 1239–1251.
12. S. Heikalabad, A. Navin, M. Hosseinzadeh, Midpoint memory: A special memory structure for data-oriented models implementation, Journal of Circuits, Systems and Computers 24 (2015) 1550063(1)–1550063(14).
13. K. Datta, D. Mukhopadhyay, P. Dutta, Comprehensive study on the performance comparision of logically reversible and irreversible parity generator and checker designs using two-dimensional two-dot one electron qca, Microsystem Technologies (2017) 1–9doi:10.1007/s00542-017-3445-2.
14. M. Ghosh, D. Mukhopadhyay, P. Dutta, A novel parallel memory design using 2 dot 1 electron qca (2015) 485–490.
15. K. Chakrabarti, Realization of original quantum entanglement state from mixing of four entangled quantum states 863. doi:https://doi.org/10. 1007/978-3-030-34152-712.
16. D. Mukhopadhyay, P. Dutta, A study on energy optimized 4 dot 2 electron two dimensional quantum dot cellular automata logical reversible flip-flops, Microelectronics Journal 46 (2015) 519–530.
17. M. Ghosh, D. Mukhopadhyay, P. Dutta, A 2d 2 dot 1 electron quantum dot cellular automata based logically reversible 2:1 multiplexer (2015) 1–6.
18. D. Mukhopadhyay, P. Dutta, Quantum dot cellular automata based novel unit reversible multiplexer, Advance Science Letters 5 (2012) 1–6.
19. K. Datta, D. Mukhopadhyay, P. Dutta, Comprehensive design and analysis of gray code counters using 2-dimensional 2-dot 1-electron qca, Microsystem Technologies (2018) 1–19doi:0.1007/s00542-018-3818-1.
20. $https://github.com/LaurentNevou/QSchrodinger2DDemo$.
21. G. Bernstein, A. Imre, V.Metlushko, A. Orlov, L. Zhou, L. Ji, G. Csaba, W. Porod, Magnetic qca systems, Microelectron. J 36 (2005) 619–624.

22. M. Amiri, M. Mahdavi, R. Atani, S. Chaki, Qca implementation of serpent block cipher (2009) 16–19.
23. S. Hashemi, K. Navi, New robust qca d ip op andmemory structures, Microelectronics 43 (2012) 929–940.
24. K. Chakrabarti, Is there any spooky action at a distance? 170. doi:https://doi.org/10.1007/978-981-33-4084-865.