ISSN : 2278- 9723
http://dx.doi.org/10.31838/ijccts/07.02.04

Research Article

Quantum-Dot Cellular Automata based Public Key Cryptography

DR. M SANTHI[1],NANDA KUMAR[2],G.UDHAYA KUMAR[3], S.MOHANDOSS[4],R.VENKATASUBRAMANIYAN[5]
12345Saranathan College of Engineering, Trichy, Tamil Nadu, India.

Received: 04.01.19, Revised: 04.02.19, Accepted: 04.03.19

ABSTRACT

In the field of Nanotechnology, Quantum-dot Cellular Automata is a new nascent technology. In order to overcome the CMOS limitations, less area and low power consuming QCA circuits are designed. Cryptography in QCA has been used to provide high data security during transmission. When comparing with symmetric cryptography, Asymmetric cryptography are confidential and authentication. In our paper, we designed a Public key cryptography using RSA algorithm that encrypts and decrypts the data using different keys. We also designed a full adder circuit with less area and latency when compared with previous works. The proposed architecture has been design and tested using QCA Designer tool.

Key words: Quantum-Dot Cellular Automata, Asymmetric, Public key Cryptography, RSA algorithm, Encryption, Decryption.

INTRODUCTION

Several modern electronics has been developed in 21st century to meet the demands in the performance of device. As the demands grows up CMOS technology will be in the state of extension due to limitations in physical size, speed and power consumption. In order to overcome these limitations, VLSI industries has been moved to new emerging technology known as Quantum-Dot Cellular Automata. Quantum dots in the QCA cells have been used to place the two electrons in the electron placeholders diagonally due to repulsive tension. Any data that is to be transmitted to the receiver needs to have high protection, so that no active attacks can happen. Cryptography is used to provide to improve this security. In previously proposed cryptography QCA papers, they have been designed using symmetric key cryptography and serpant cipher model. When we take symmetric cryptography, both the user and the receiver has to use the same key which is has to be transmitted more secretly. When the attacker founds the shared key, the encrypted data can be changed by him. Asymmetric cryptography is used to overcome this problem. In our proposed paper, we designed cryptography for transmitting and receiving the data using Public key cryptography using RSA algorithm where the transmitter and receiver use different keys. The proposed is organised in the order as follows: Section II represents the Overview of the QCA cells, gates and clock zones. Section III represents the related works of QCA cryptography and nano-communicaton. The Public key Cryptography and RSA Algorithm is represented in Section IV and V. The proposed architecture and new full adder design is shown in Section VI and VII. Encryption and Decryption of the proposed algorithm is discussed in Section VIII and IX . Section X shows the comparision with previous works. Finally, Section XI draws the conclusion remarks.

QCA Overview

QCA cell structure is usually a square box which has four places of quantum dots where the charged two electrons are placed diagonally. This diagonal placement of cells is because of electrostatic interaction between the electrons as shown in fig.1. Thus, the electrons in the quantum dots are positioned in opposite corners of the cell. Thus, there are two polarisation states. they are logic'0' (P=-1) and logic'1'(P=+1).

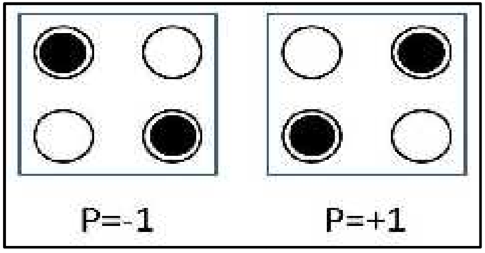

Fig.1: QCA Cells

Majority gate of QCA has three inputs, a device cell and one output. Depending on the three inputs values, output is determined. Among the these inputs one is the selection input.

M(A,B,C)=AB+CA+BC (1)

Depending upon the selection input, Majority gate acts as AND gate or OR gate. M(A,B,0)= AB , if C=0 and M(A,B,1)=A+B if C=1.

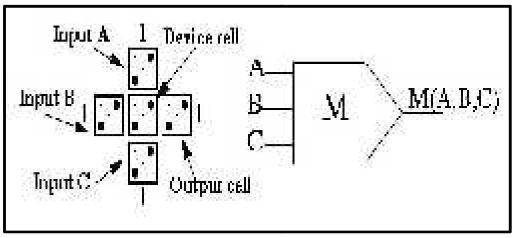

Fig.2: Majority gate

In QCA Inverter Gate, Due to diagonal placement of electrons, it gains opposite polarisation and acts as NOT gate. Replusive tension of the electrons make logic'0' to logic'1' conversion and vice versa.

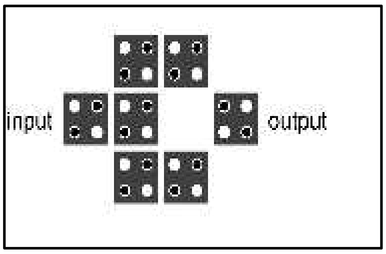

Fig.3: Inverter gate

In QCA wire, information is transferred through a row of QCA cells form one part of the circuit to another because of electrostatic interaction between theQCA cells

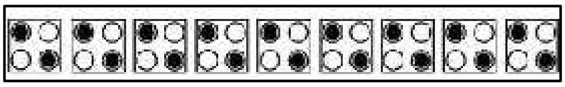

Fig.4: Information flow

Conduction of data flow through the QCA circuits is determined by the clock signals. Clock signals are shifted in phase by 90', so that it unlocks the tunnel junction of the QCA cells. At the switch phase, cell polarisation process takes place and continues till the polarisation of the cell completes. The cell starts retaining its polarization only when it reaches the hold phase of clock pulse. A decrease in polarization of the cell occurs when the clock passes through the release phase. Finally, at the relax phase, the cell is unpolarized.

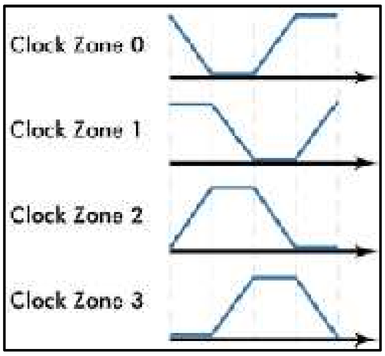

Fig.5: Clock zones

Related Work

In (2), secure QCA cryptographic structure had designed with encryption of the plain with the secrete key and decrypt the cipher text with the same key for any number of bit message. Cipher text was obtained by xoring the plain text with secret key and from that cipher key, plain text was obtained with the same xor operation using the same key. In (10), Secure Nano communication for a image steganography was performed by encoder and decoder circuit using the fayaman gate. Depending upon the size of the pixels, the string was embedded with the image. Single missing cell defect and additional cell defect was used to analysis the QCA circuit defect. In (9), Hamming code and parity checker circuits had been designed for nanocommunication. In (1), Polar encoder circuit is designed at nano-scale level and was performed in single layer to achieve faster speed and also achieved the fault free design by struct-at-fault effect analysis. In (4), Energy estimation was carried out using Hamming distance approach. Each QCA circuit has energy dissipation equal to the dissipated energy by all the logic gates present in a design. In (3), Symmetric key cryptography and LSB technique had been used in the image streganogrpahy. Secrete message was xored with the image and it is embedded with the image processed through encoder and decoder circuit. In (7), With the help of a channel more number of data sources are transmitted and it routed the data to be selected data path with the help of multiplexer and demultiplexer which could provide the connection between the hardware control switches and control memory. In (11), Detection probability of cipher text was reduced by replacing the fixed keys with the random no generator. The design which include xor block, four to sixteen decoder, four-bit counter, two pseudo random number generator block and memory elements. Input streams would be encoded into different patterns in different instance of time for hiding the original data from unauthorized access. In (6), Specific 4x4 substitution box for block cipher and stream cipher had been designed with the help of four bits of input and four bits of output. In (13), 2:1 multiplexer circuit and 1:2 demultiplexer circuit had been used to provide the nanorouter for nanocommunication. Depending upon the selected lines, either of the inputs was transmitted through single transmissionline and received at the respective output. In (14) to (17), they proposed various adder designs with less area and less latency.

Public Key Cryptography

The key which is used to encrypt the data by any user is known as public key which will be distributed to the user whose going to send the data to the receiver. With the help of receivers public key the data is encrypted and send to the receiver. The receiver will decrypt the data with the help of private key. Both these keys are generated from the receiver end, where the private key is kept secret and public key is share between the user.

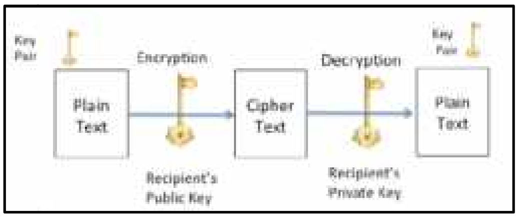

Fig.6: Public key Cryptography

RSA Algorithm

RSA algorithm is used to provide security when the data is sent over the network which is widely used in Public key cryptography. For encryption, either of the public key or the private key can be used and other key which has not been used in encryption is used for decryption. This algorithm is also used in software like browser and in many protocols like Secure Shell, S/MIME.

Steps in RSA Algorithm

Step 1: Select two prime number (q & p)
Step2: Calculate n=p*q
Step3: Calculate Euler's Totient function φ(pq) = φ(p)φ(q)
Step4: Select the value of e that is relatively prime to φ(pq) and e< φ(pq)
Step5: Calculate the value of d, e*d= 1 mod φ(pq)
Step6: The resulting keys are
Public key PU={e,n}
Private key PR={d,n}
Step7: the message should be M< n
Encryption (cipher text) C= M^e mod n
Decryption (Plain text) M=C^d mod n

Proposed Architecture

In this paper we design the architecture which is capable of encrypting and decrypting the 4 bit data. We took p=2 and q=5 and selected e=3 and calculated d=7. Thus the resulting keys are PU={3,10}, PR={7,10}. For encrypting the data(M<10), C=M^3 mod 10 and for decrypting D=C^7 mod 10.

New Adder Design

Full Adder is the digital logical circuit which performs addition of three 1-bit input binary numbers to produce two 1-bit output binary number. One output is the Sum of three inputs and other is the Carry.

$$Sum=A\oplus B\oplus Cin$$

$$Cout=AB+ACin+BCin$$

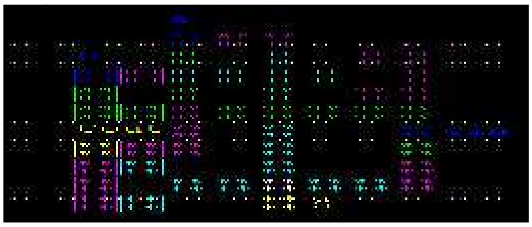

Fig.7: Proposed Adder Design

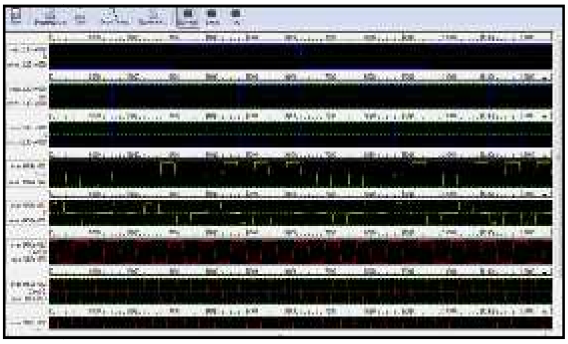

Fig.8: Simulation Result of FA

Encryption

Converting the original information with the help of key into unreadable form is called the cipher text. In determining the Cipher text, we need to perform multiplication of the same message data and have to find the reaminder when divided by n. As we do multiplication , it will be very hard to perform 8 bit multiplication. So we reduced the 1st 4bit mulitiplication result again to 4bits instead of 8bit for effective performance. For reducing the 8 bit to 4 bit we used the concept of BCD adder and other gate operations.

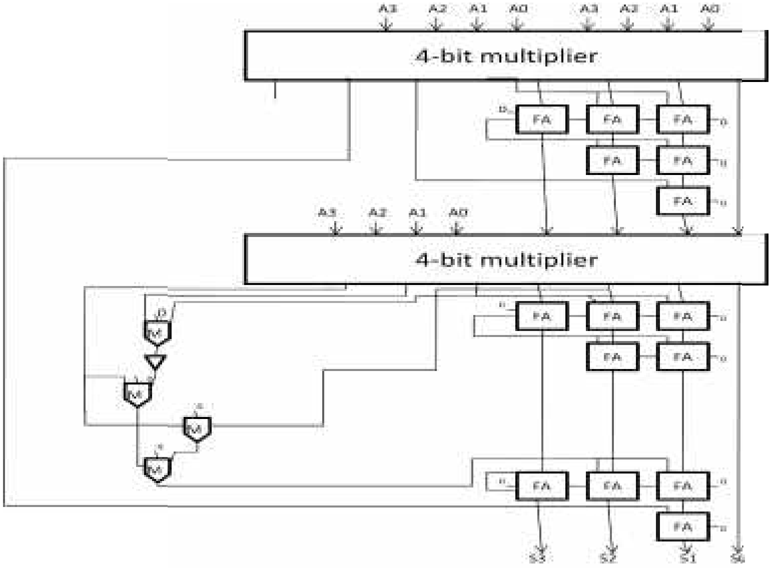

Fig.9: Encryption Architecture

In this above figure, we multiple 4 bit of a message with the same message using 4-bit multiplier and we get output as 8 bit. Then we convert the 8 bit product value to 4-bit value using the full adders. At first p4th postion value is added to p1 and p2, then the carry is added to p3. If there is any carry produced during addition with p3, the add the carry value to p1 and p2. P6th value is added to resulting p1 to make the reduced 4-bit message value. The resultant 4-bit value is again multiplied with 4bit message to perform multiplication. In order to the converting 8 bits to 4 bits we used Majority gates. From the first multiplication p6 value is taken and added to the second bit position from LSB of the second multiplier. Finally we obtained 4-bit value as the encrypted message.

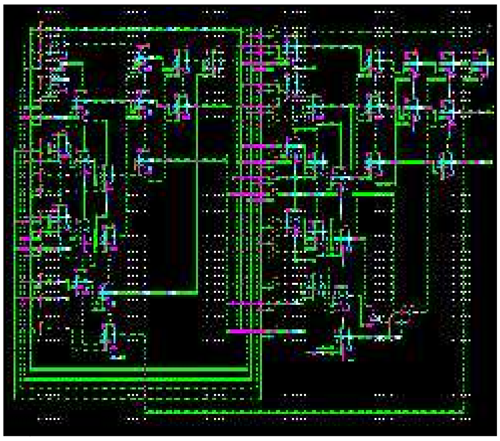

Fig.10: QCA Design for Encryption

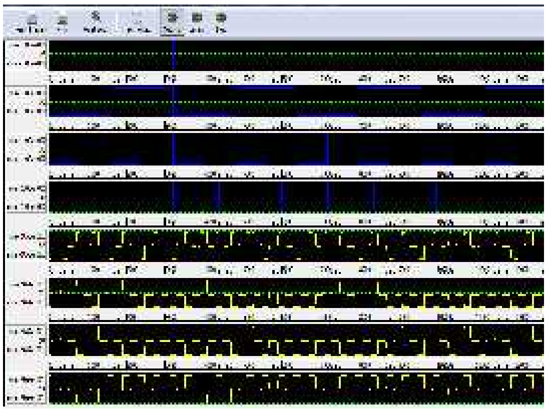

Fig.11: Encryption Simulation Results

Decryption

Retrieving the original data from the unreadable form is called as the plain text. In our proposed decryption we had to do 7 times multiplication. This makes the design too complex and very hard to construct. So we reduced the structure to 3times of multiplication with use of more gate operations.

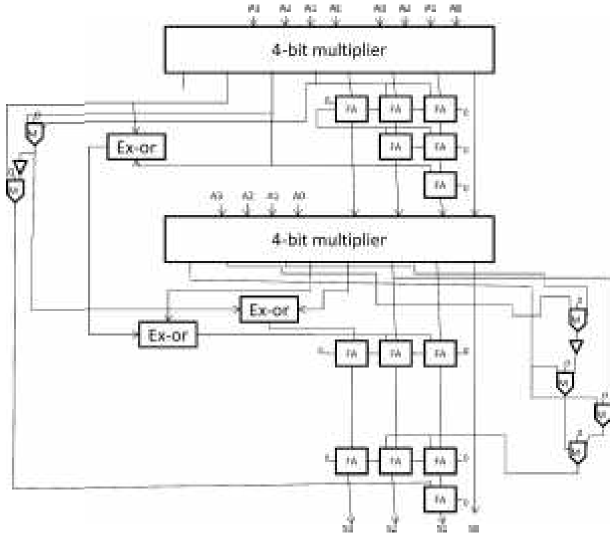

Fig.12: Decryption Architecture

From the below figure, encrypted 4-bit message is multiplied twice using the 4-bit multiplier to produce the 8-bit product value. Here the same encryption operation is performed. In addition to that majority gate and ex-or gates perform the effective operation in reducing the 7times multiplication. After executing the mentioned operations as per the architecture , we can retrieve the original message.

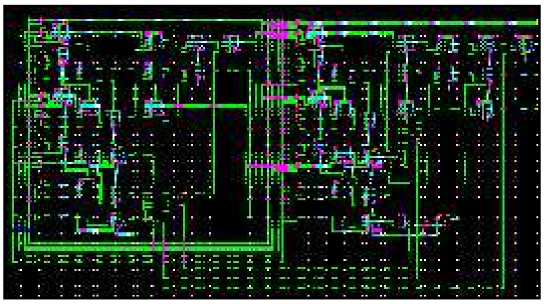

Fig.13: QCA Design for Decryption

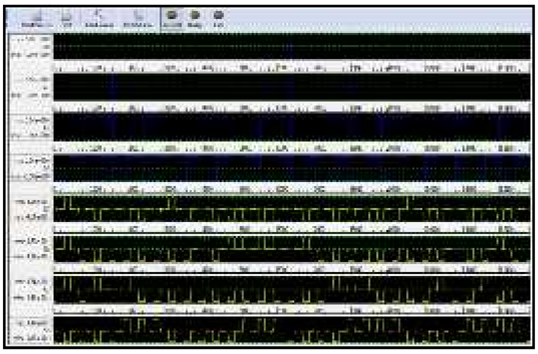

Fig.14: Decryption Simulation Results

Comparsion Results

With the help of QCA Designer tool we designed the Encryption and Decryption architecture using full adders which is designed with less no of cells is shown fig.10& fig.13 . The simulation results of the designes are shown in fig.11 & fig,14.The cost value was determined by the following equation:

$$\text{Cost} = \text{Area} * \text{Latency}^2$$

where Area is the size of the design in um^2 and Latency is the number of clock cycles.

Table 1: Comparison of QCA FAs

QCA FA	Cells	Area (μ m^2)	Latency	Layer Type	Cost
(16)	96	0.1	2	-	0.4
(15)	79	0.064	1	Multiple	0.064
(17)	69	0.07	1	Coplanar	0.07
(14)	59	0.043	1	Coplanar	0.043
new	49	0.04	1	Coplanar	0.04

From the table.1, The proposed Full Adder design is decreased in area by 150% ,60% ,75%,7.5% when comparing with previously designed FA in (16),(15),(17) and (14).

Conclusion

As there is an increase in the side channel attacks, cryptography devices can be victimized. The proposed circuit is used in providing secure QCA Cryptography module than the previously proposed QCA modules. The encryption and decryption of the 4-bit message is performed here but it can be done for any message bits. Future implementation of QCA based cryptography algorithms can be achieved by using this proposed circuit.

References

1. Das, J. C., & De, D. (2018). "QCA based design of Polar encoder circuit for nano communication network". Nano Communication Networks, 18, 82–92.
2. Das, J. C., & De, D. (2012). "Quantum Dot-Cellular Automata based cipher text design for nano-communication". International Conference on Radar, Communication and Computing (ICRCC).
3. Debnath, B., Das, J. C., & De, D. (2018). "Design of image steganographic architecture using quantum-dot cellular automata for secure nanocommunication networks". Nano-Communication Networks, 15, 41–58.
4. Weiqiang Liu, Srivastava, S., Liang Lu, O'Neill, M., & Swartzlander, E. E. (2012)." Are QCA cryptographic circuit resistant to power analysis attack?", IEEE Transactions on Nanotechnology, 11(6), 1239–1251.
5. Weiqiang Liu, Srivastava, S., Liang Lu, O'Neill, M., & Swartzlander, E. E. (2013). "Power analysis attack of QCA circuits: A case study of the Serpent cipher". IEEE International Symposium on Circuits and Systems (ISCAS2013).
6. Amiri, M. A., Mahdavi, M., & Mirzakuchaki, S. (2010)." Logic based on QCA realization of a 4x4 S-boxes". 2010 International Conference on Computer Applications and Industrial Electronics.
7. Soumyadip Das and Debashis De (2012). "Nanocommunication using QCA: A data path selector cum router for the efficient channel utilization". 2012 International Conference on Radar, Communication and Computing (ICRCC).
8. D. S. Silva, L. H. B. Sardinha, M. A. M. Vieira, L. F. M. Vieira and O. P. V. Neto, "Robust Serial Nanocommunication With QCA," IEEE Transactions on Nano-technology, vol. 14, no. 3, pp. 464-472, May 2015.
9. Das, J. C., De, D., & Sadhu, T. (2016)." A novel low power nano-scale reversible decoder using quantum-dot cellular automata for nano-communication". 2016 3rd International Conference on Devices, Circuits and Systems (ICDCS).
10. Debnath, B., Das, J. C., & De, D. (2017)." Reversible logic based on image steganography using quantum dot cellular automata for secure nano-communication" . IET Circuits, Devices & Systems, 11(1), 58–67.
11. Purkayastha, T., De, D., & Das, K. (2016). "A novel pseudo random number generator based cryptographic architecture using quantum-dot cellular automata. Microprocessors and Microsystems", 45, 32–44.
12. Das, J. C., & De, D. (2017). "Nanocommunication network design using QCA reversible crossbar switch". Nano Communication Networks, 13, 20–33.
13. Ahmad, F. (2018). "An optimal design of QCA based 2 n:1/1:2 n multiplexer/demultiplexer and its efficient digital logic realization". Microprocessors and Microsystems, 56, 64–75.
14. D. Abedi, G. Jaberipur and M. Sangsefidi, "Coplanar Full Adder in Quantum-Dot Cellular Automata via Clock-Zone-Based Crossover," in IEEE Transactions on Nanotechnology, vol. 14, no. 3, pp. 497-504, May 2015.
15. V.pudi and K.Sridharan, " Low Complexity design of ripple carry and Brent-kung adders in QCA", IEEE Trans.Nanotechnology, vol. 11, no. 1, pp. 105-119, Jan.2012
16. Mohammadyan, S., Angizi, S., & Navi, K. (2015). "New fully single layer QCA full-adder cell based on feedback model". International Journal of High Performance Systems Architecture, 5(4), 202.
17. Kianpour, M., Sabbaghi-Nadooshan, R., and Navi, K.: "A novel design of 8-bit adder/subtractor by quantum-dot cellular automata", J. Comput. Syst. Sci., 2014, 80, (7), pp. 1404–1414