Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Nanoscale cryptographic architecture design using quantum-dot cellular automata

Bikash DEBNATH[1], Jadav Chandra DAS[1], Debashis DE[†‡2]

[1]*Department of Computer Science and Engineering, Swami Vivekananda Institute of Science and Technology, West Bengal 700145, India*

[2]*Department of Computer Science and Engineering, West Bengal University of Technology, Kolkata 700064, India*

[†]E-mail: dr.debashis.de@gmail.com

Received Aug. 2, 2018; Revision accepted Dec. 8, 2018; Crosschecked July 16, 2019; Published online Aug. 15, 2019

Abstract: Quantum-dot cellular automata (QCA) based on cryptography is a new paradigm in the field of nanotechnology. The overall performance of QCA is high compared to traditional complementary metal-oxide semiconductor (CMOS) technology. To achieve data security during nanocommunication, a cryptography-based application is proposed. The devised circuit encrypts the input data and passes it to an output channel through a nanorouter cum data path selector, where the data is decrypted back to its original form. The results along with theoretical implication prove the accuracy of the circuit. Power dissipation and circuit complexity of the circuit have been analyzed.

Key words: Quantum-dot cellular automata (QCA); Majority gate cryptography; Encryption; Decryption; Nanorouter
https://doi.org/10.1631/FITEE.1800458 **CLC number:** TN91

1 Introduction

Modernization in the field of electronics is directly proportional to the increase in demand of functional performance and device density of a gadget (Lent et al., 1993; Tougaw and Lent, 1994; Orlov et al., 1997; Porod, 1997). Hence, smaller sized gadgets must possess higher functionality. Such functionality requires diminution in circuitry. The very large scale integration (VLSI) industry is shifting towards nanoscale technology. In complementary metal-oxide semiconductor (CMOS) technology, shrinkage of circuit size causes different short channel effects. Because of shrinkage, CMOS predominantly fails to meet the modern requirements. A promising alternative technology is quantum-dot cellular automata (QCA) (Lent and Tougaw, 1997; Porod et al., 1999; Kianpour et al., 2014; Angizi et al., 2015b). This is a transistor-less technology applicable for designing the circuits at the nanoscale level. The advantages of QCA are high-speed computation, low power consumption, and high density design. QCA follows the principle of quantum confinement. The nanometer sized square structure quantum-dot cell consists of four quantum wells and two mobile electrons. Four quantum dots are associated with tunnels. The two electrons can both move between different positions via electron tunneling. They try to occupy the diagonal position which arises due to Coulombic interaction between cells (Pudi and Sridharan, 2015; Das and De, 2017c, 2017d; Ahmadpour and Mosleh, 2018; Heikalabad et al., 2018). The Coulombic interaction between the QCA cells helps achieve the stable position, which represents the binary information.

In the digital world, cryptography (Kahate, 2008) is an important feature since it offers protection and security for the digital data. Cryptography covers mainly three aspects, which are authentication, integrity, and confidentiality. A cryptographic

‡ Corresponding author
ORCID: Debashis DE, https://orcid.org/0000-0002-9688-9806

architecture is proposed in this study. The proposed design consists of an encoder to encrypt the input data stream, a data-path-selector with a nanorouter to transmit the data to the desired output channel, and a decoder to decrypt the previously encrypted input to the output channel. In the proposed design, symmetric key cryptography (Delfs and Knebl, 2015) is used for the encryption and decryption processes.

For secure communication, QCA based nanotechnology is used to build an efficient nanorouter, and obtain the facilities of less power consumption, fewer clock delays, and lower circuit complexity. The major contributions of this study are: (1) a single layer wire crossing in QCA technology for implementing multiplexer (MUX) and demultiplexer (DEMUX); (2) a data path selector that can function as a nanorouter using MUX and DEMUX; (3) cell- and area-efficient design of the XOR gate; (4) codec designed using the proposed XOR gate; (5) a cryptographic nanocommunication architecture using the codec and data path selector; (6) comparison of the proposed XOR, MUX, and DEMUX with the state-of-the-art designs; (7) estimation of power consumption.

2 Related works

In the literature, different works are proposed on router circuits in QCA. Nanocommunication obtained using QCA technology, a router circuit which works as a data path selector circuit, was proposed by Das S and De D (2012). A single channel transfer of data from a different source to the expected destination was achieved. To route to four different destinations while using a single channel, four separate sources were designed. A nanorouter was proposed by Sardinha et al. (2013). The router allows the transmission of data packets. The building block of the proposed nanorouter comprises a crossbar switch, a DEMUX, and a parallel-to-serial converter. The encryption and decryption processes were implemented using QCA based logic circuits reported in Kamaraj et al. (2015). The formulation to generate ciphertext for QCA based secure nanocommunication was demonstrated in Kamaraj et al. (2015). Using the nanorouter circuit proposed in Shah et al. (2011), data from a large number of sources can be routed to their destination using a single path. Thus, the proposed circuit can be used for distributed computing. An efficient QCA layout of MUX and DEMUX circuits has been outlined by some researchers (Mukhopadhyay et al., 2011; Shah et al., 2011; Iqbal et al., 2013).

3 QCA overview

3.1 QCA cell

The structure of a QCA cell (Sen et al., 2014; Das and De, 2016a; Debnath et al., 2018) is a square box containing four quantum dots, charged with two electrons in each QCA cell (Fig. 1). Tunneling of these mobile electrons occurs within the QCA cell. Coulombic interaction creates repulsive tension between electrons, and then the electrons get engaged with the opposite corners of the cell. This gives rise to two polarization states, which are: (1) P=+1 represents logic 1; (2) P=−1 represents logic 0.

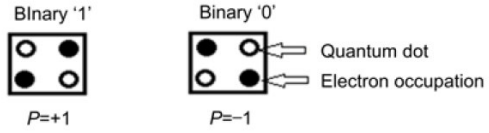

Fig. 1 QCA cells based on polarization

3.2 QCA majority gate

In QCA circuits, the primary logic gate is majority gate (M). The majority logic gate (Angizi et al., 2015a; Das and De, 2017c) consists of five standard cells (Fig. 2). The schematic of the majority gate is displayed in Fig. 2a and the layout in Fig. 2b. There are a majority gate with three inputs, a device cell, and an output. The output depends on the value of the three inputs. If the three inputs of the majority gate are considered to be X, Y, and Z, the expression can be $M(X, Y, Z)=XY+YZ+ZX$. AND or OR gates are formed by adjusting the polarization of the input cells.

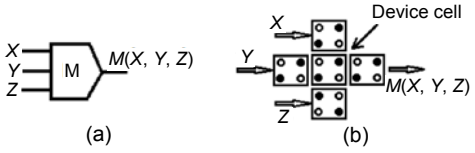

Fig. 2 Majority gate: (a) schematic; (b) QCA layout

When any input X, Y, Z in this equation is fixed to logic 0, this equation will perform as an AND gate

and will be expressed as $M(X, Y, 0)=XY$. If any input is fixed to logic 1, the expression will be expressed as $M(X, Y, 1)=X+Y$, and it will perform as an OR gate.

3.3 QCA inverter

When two standard 90° QCA cells are placed diagonally, they gain opposite polarization and the unit acts as a NOT gate, i.e., inverter (Sayedsalehi et al., 2015; Sridharan and Pudi, 2015). Due to the electrostatic repulsion of cells, a conversion of logic 0 to 1 takes place, and vice versa (Fig. 3).

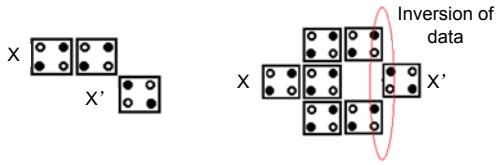

Fig. 3 QCA inverter

3.4 QCA clock zone

Clock signals are required to generate the data flow through QCA circuits (Orlov et al., 2001; Das and De, 2017b; Karkaj and Heikalabad, 2017). The clock signals are shifted in phase by 90° (Fig. 4). The clock signal unlocks the tunnel junctions of the QCA cells. When the clock signal is high, it allows the electrons of the QCA cell to travel through the tunnels from one potential well to another. There are four phases in every cycle, which are described as follows: phase 1 is called the Switch phase, phase 2 is referred to as the Hold phase, phase 3 is known as the Release phase, and phase 4 is known as the Relax phase. The inter-dot barrier during phase 1 is elevated so that the position of electrons within the cell can be altered due to the effect of the cell placed in front of it. Kink energy acts between the cells. In phase 2, the inter-dot barrier is kept high so that the cell remains at its current state. In phase 3, the inter-dot barrier is lowered, and in phase 4, the barrier is made too low, and the cell remains in an unpolarized state.

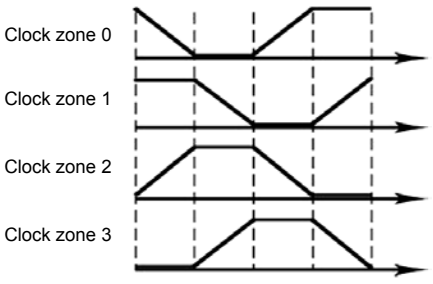

Fig. 4 Different clock zones

4 Proposed cryptographic nanorouter

An organized composition for cryptographic architecture is proposed in this study. In this design, the data required to be transferred is taken from four different input channels. The received data is encoded with an encryption method. Thereafter, the encoded data from the selected input channel is transferred to their target output channel through a data path selector with the nanorouter. In the output channel, the data is decrypted to get back the original message.

4.1 Nanorouter

The block diagram of the proposed design for the data path selector which can act as a router is shown in Fig. 5. It comprises three components, multiplexer (Mukhopadhyay et al., 2011), transmission line, and demultiplexer (Das and De, 2017a). The multiplexer is used to select a particular input from different input lines, and transmit the selected input to the transmission line. The demultiplexer at the receiving end of the transmission line selects the output channel depending on the selected signals, and routes the input data towards it.

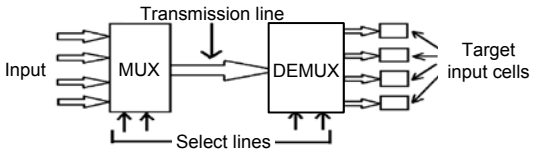

Fig. 5 Overview of the nanorouter

The QCA layout of the proposed nanorouter is illustrated in Fig. 6. IP1, IP2, IP3, and IP4 are the input channels, and *A*, *B*, *C*, and *D* are the output channels. S0 and S1 are the selection lines for the multiplexer, i.e., input path selection bits; S2 and S3 are the selection lines for the demultiplexer, i.e., output path selection bits. The truth table of the circuit is shown in Table 1. The don't care condition is represented by "X." The input selector bits S0 and S1 select data from one of the input channels among IP1, IP2, IP3, and IP4, and pass it to the transmission line;

on the other end, depending on the output channel selection bits S2 and S3, the data present in the transmission line is routed to one of the four output channels *A*, *B*, *C*, and *D*.

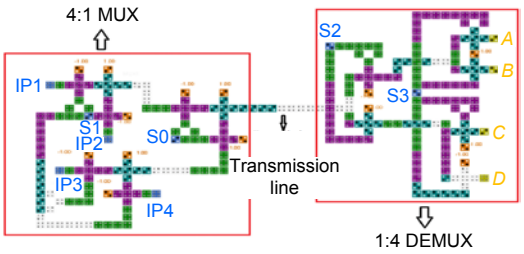

Fig. 6 QCA design of the nanorouter

Table 1 Function table of the nanorouter

Index	Bits for input channels		Bits for output channels		Input data at output channels			
	S0	S1	S2	S3	*A*	*B*	*C*	*D*
1	0	0	0	0	IP1	X	X	X
2	0	0	0	1	X	IP1	X	X
3	0	0	1	0	X	X	IP1	X
4	0	0	1	1	X	X	X	IP1
5	0	1	0	0	IP2	X	X	X
6	0	1	0	1	X	IP2	X	X
7	0	1	1	0	X	X	IP2	X
8	0	1	1	1	X	X	X	IP2
9	1	0	0	0	IP3	X	X	X
10	1	0	0	1	X	IP3	X	X
11	1	0	1	0	X	X	IP3	X
12	1	0	1	1	X	X	X	IP3
13	1	1	0	0	IP4	X	X	X
14	1	1	0	1	X	IP4	X	X
15	1	1	1	0	X	X	IP4	X
16	1	1	1	1	X	X	X	IP4

4.2 Proposed cryptographic architecture

The proposed cryptographic architecture guarantees security. In cryptography (Debnath et al., 2017), the process of conversion of an ordinary text to a ciphertext is called encryption, which in turn is called decryption (Das JC and De D, 2012). In this study we focus on designing a cryptographic architecture with a symmetric key cryptography approach and its implementation in QCA. The architecture is composed of an encoder, a decoder, and a data path selector. The flowchart of the procedure is shown in Fig. 7. The encoder section which contains four inputs and four keys undergoes binary conversion, and thereafter XOR operation is performed within the inputs and keys to obtain the four ciphertexts. Now, two selection lines S0 and S1 determine which ciphertext should be selected from the inputs. Once more, two selection lines S2 and S3 are present for selecting the output lines, i.e., through which output line to transmit the output. The decoding procedure takes place here. The ciphertext will be XOR-ed with the respective keys to obtain the original texts (Fig. 7). In the flowchart, it is shown that when S0 and S1, or S2 and S3, are unable to select any line, the transmission will stop immediately. The block diagram of the proposed cryptographic architecture is shown in Fig. 8.

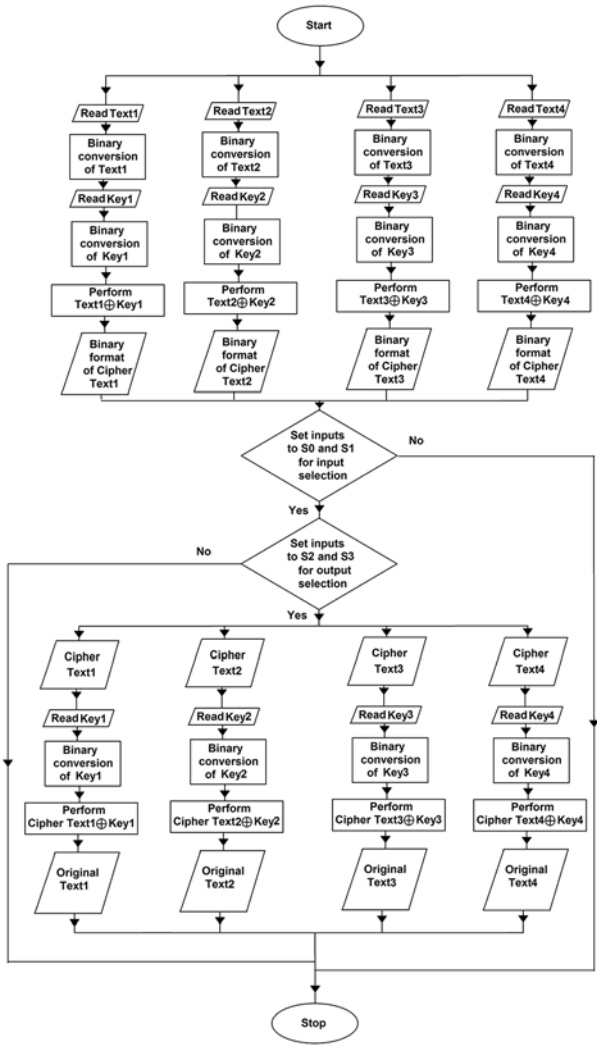

Fig. 7 QCA flowchart of the encryption, transmission, and decryption procedures

The component of each part of the architecture (Fig. 8) is depicted in Fig. 9. It is seen that the codec is made up with four 2-input XOR gates. The nano-router circuit has three 2-input multiplexer (Mardiris and Karafyllidis, 2010) and three 2-input demultiplexer circuits.

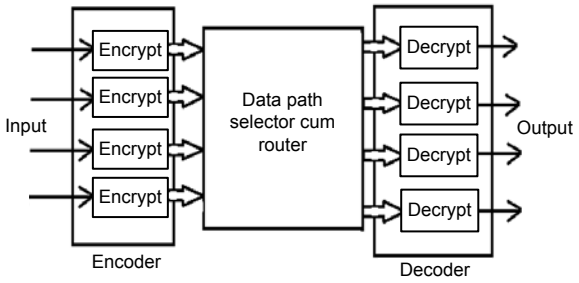

Fig. 8 Block diagram of the proposed cryptographic architecture

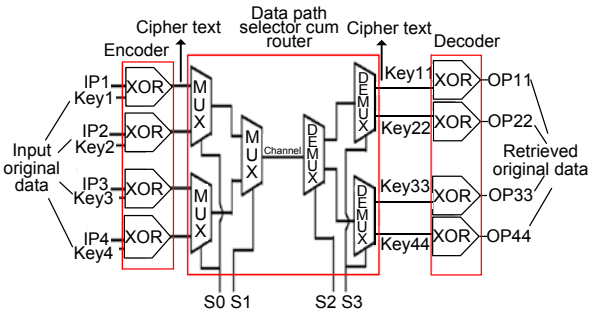

Fig 9 Schematic of the proposed cryptographic architecture

IP1, IP2, IP3, and IP4 are the inputs, encrypted using keys KEY1, KEY2, KEY3, and KEY4, respectively. The encrypted data acts as the input for the next level. Among the encrypted data, specific data is selected using the selection lines S1 and S0 of the multiplexer. Then the data achieved from the selected channel is passed to the output channel and to the demultiplexer. Based on the control signals S2 and S3 of the demultiplexer, the encrypted data reaches the decoder circuit. At the decoder, the encrypted data is decrypted back to the original message using keys KEY11, KEY22, KEY33, and KEY44. The decrypted data will channel out through output channels OP11, OP22, OP33, and OP44. Note that the keys at the encoder section, KEY1, KEY2, KEY3, and KEY4, are symmetric to the keys at the decoder section, KEY11, KEY22, KEY33, and KEY44, respectively. Since no one other than the intended receiver has knowledge about the key to decrypt the encrypted information, no one else can decrypt it. The QCA layout of the proposed cryptographic architecture (Fig. 10) is designed using QCADesigner 2.0.3 (Walus et al., 2004).

5 Results

The simulation results for the proposed design are shown in Fig. 11. When the values of selection

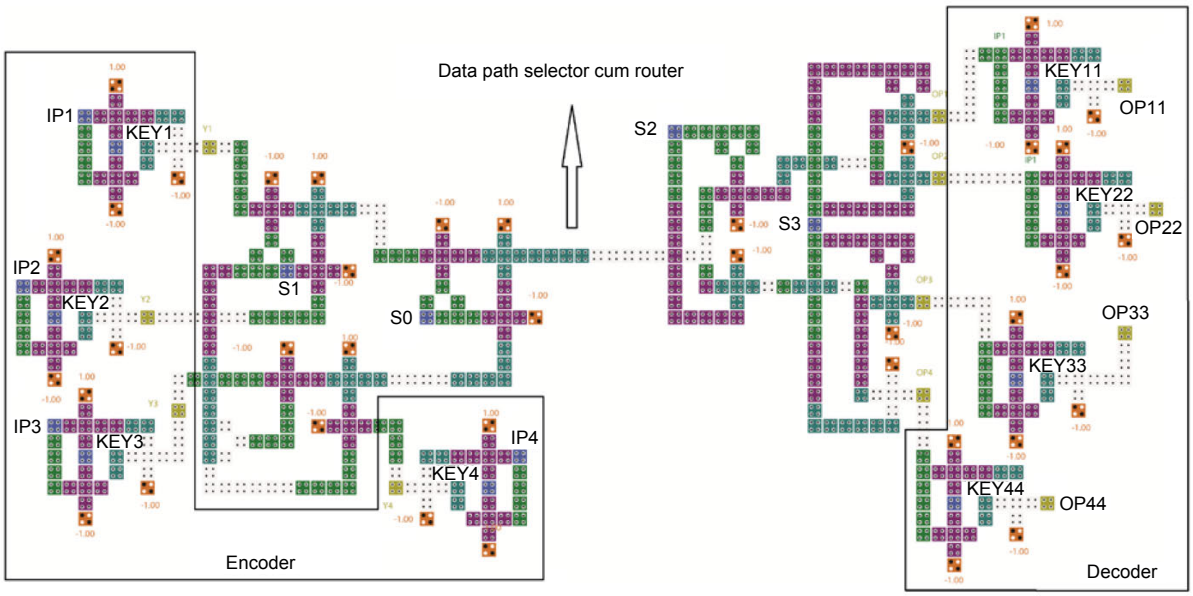

Fig. 10 QCA design of the proposed cryptographic architecture

lines S0, S1, S2, and S3 are 1, 1, 0, and 0, respectively (Table 1), the data from input channel IP4 will be transmitted to the first output channel, and in this case, it is OP11. From Fig. 11, it is observed that the data at output channel OP11 is the same as that at input channel IP4, which is 11110000, so it can be claimed that the circuit is working perfectly.

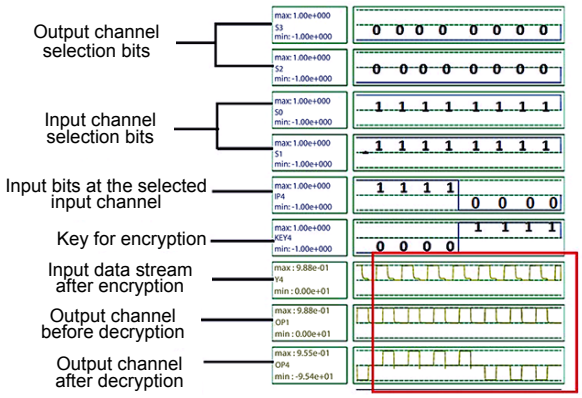

Fig. 11 Simulation results of the cryptographic architecture

5.1 Complexity of the proposed cryptographic architecture

The design complexity of the proposed QCA-based nanorouter is displayed in Table 2. The complexity is measured in terms of the number of MVs, cell count, area, and clocking zone. To construct the proposed design XOR gate, 4:1 MUX and 4:1 DEMUX are required; their circuit complexity is also calculated. The circuit cost of the proposed circuit along with its components is calculated (Table 3).

5.2 Complexity analysis of the nanorouter and its components

The proposed nanorouter and its components are compared with those of the existing designs. The comparative analysis of the proposed nanorouter with the state-of-the-art designs is illustrated in Table 4. The corresponding comparative analysis is illustrated in Table 5. The corresponding comparative analysis of the proposed MUX with the state-of-the-art designs is illustrated in Table 6. The corresponding comparative analysis of the proposed DEMUX with the state-of -the-art designs is given in Table 7.

Table 3 Circuit cost of the proposed QCA circuit

Cryptographic architecture	Circuit cost*
XOR gate	0.0400
4:1 MUX	0.6125
1:4 DEMUX	0.5500
Full circuit	34.4850

* Circuit cost=total area×latency^2

Table 4 Comparative analysis with the existing nanorouter in the literature

Reference	Number of cells	Area (μm^2)	Latency (clock cycle)
Das S and De D (2012)	419	0.54	3.00
Sardinha et al. (2013)	4026	13.81	12.00
This paper	293	0.53	3.75

Table 5 Comparison of the proposed XOR gate with the XOR gates in the literature

Reference	Number of cells	Area (μm^2)	Latency (clock cycle)
Das and De (2016a)	55	0.90	2.0
Sen et al. (2014)	54	0.70	2.0
Das and De (2016b)	35	0.04	1.0
Balali et al. (2017)	14	0.01	0.5
This paper	30	0.04	1.0

Table 6 Comparison of the proposed 4:1 MUX with 4:1 MUX gates in the literature

Reference	Number of cells	Area (μm^2)	Latency (clock cycle)
Mardiris and Karafyllidis (2010)	215	0.25	1.50
Mukhopadhyay et al. (2011)	166	0.27	1.00
Rashidi and Rezai (2017)	107	0.17	1.25
Rashidi et al. (2016)	107	0.15	1.00
This paper	135	0.20	1.75

Table 2 Complexity of the cryptographic architecture and its components

QCA circuit	Number of MVs and inverters	Cell count	Total area (μm^2)	Cell area (μm^2)	Area usage (%)	Latency (clock cycle)
XOR gate	3 MVs, 1 inverter	30	0.04	0.009	22.5	1.00
4:1 MUX	9 MVs, 3 inverters	135	0.20	0.043	21.5	1.75
1:4 DEMUX	6 MVs, 3 inverters	150	0.18	0.048	26.7	1.75
Cryptographic architecture	39 MVs, 14 inverters	581	1.14	0.188	16.5	5.50

Table 7 Comparison of the proposed 1:4 DEMUX with the 1:4 DEMUX gates in the literature

Reference	Number of cells	Area (μm^2)	Latency (clock cycle)
Shah et al. (2011)	217	0.60	2.00
Iqbal et al. (2013)	188	0.22	2.00
This paper	150	0.18	1.75

All the tables show that the proposed QCA circuits have lower cell count, smaller device area, and less latency compared to the state-of-the-art designs.

5.3 Power dissipation analysis of the proposed cryptographic architecture

Power dissipation (PD) of the QCA circuit depends on the Hamming distance (HD) (Liu et al., 2012) of the majority gates and inverters used in a circuit. For different sets of inputs, the Hamming distances of the respective majority gates and inverters of the proposed XOR gate, 2:1 MUX, and 1:2 DEMUX are shown in Tables 8–10 at tunneling energy γ=0.25E_k, and the total power consumption is calculated. The 4:1 MUX and 1:4 DEMUX consumptions of power are calculated from Tables 9 and 10, respectively, and the values along with the total power consumption of the proposed nanorouter circuit are shown in Table 11. The designed nanorouter consists of eight XOR gates, one 4:1 MUX, and one 1:4 DEMUX (Fig. 8). Similarly, power is calculated and tabulated in Table 11. The PD at different tunneling energy values of the proposed nanorouter is further displayed in Fig. 12.

Table 11 Power dissipation of the proposed cryptographic architecture and its components at different tunneling energy levels

Proposed QCA design	Power dissipation (meV)			
	γ=0.25E_k	γ=0.5E_k	γ=0.75E_k	γ=E_k
XOR gate	32.3	38.4	46.7	56.2
4:1 MUX	96.9	115.2	140.1	168.6
1:4 DEMUX	11.7	29.1	51.9	77.7
Cryptographic architecture	367.0	451.5	565.6	695.9

Table 8 Power dissipation (PD) of the XOR gate (γ=0.25E_k)

Input	MV1	HD	PD (meV)	MV2	HD	PD (meV)	INV1	HD	PD (meV)	MV3	HD	PD (meV)	Total PD (meV)
00	100	0	0.8	000	0	0.8	0	0	0.8	001	1	2.3	4.7
01	101	0	0.8	001	0	0.8	0	0	0.8	011	1	2.3	4.7
10	110	0	0.8	010	0	0.8	0	0	0.8	011	1	2.3	4.7
11	111	0	0.8	011	0	0.8	1	1	28.4	010	1	2.3	32.3

Table 9 Power dissipation (PD) of the designed 2:1 MUX (γ=0.25E_k)

Input	MV1	HD	PD (meV)	MV2	HD	PD (meV)	INV1	HD	PD (meV)	MV3	HD	PD (meV)	Total PD (meV)
000	010	1	2.3	000	0	0.8	0	0	0.8	100	0	0.8	4.7
001	010	1	2.3	001	0	0.8	0	0	0.8	100	0	25.3	4.7
010	011	1	2.3	000	0	0.8	0	0	0.8	110	0	2.3	4.7
011	011	1	0.8	001	0	0.8	0	0	0.8	110	0	2.3	4.7
100	000	1	2.3	010	0	0.8	1	1	28.4	100	0	0.8	32.3
101	000	1	2.3	011	0	0.8	0	0	0.8	101	0	0.8	4.7
110	001	1	2.3	010	0	0.8	0	0	0.8	100	0	0.8	4.7
111	001	1	2.3	011	0	0.8	0	0	0.8	101	0	0.8	4.7

Table 10 Power dissipation (PD) of the designed 1:2 DEMUX (γ=0.25E_k)

Input	MV1	HD	PD (meV)	MV2	HD	PD (meV)	INV1	HD	PD (meV)	Total PD (meV)
00	010	1	2.3	000	0	0.8	0	0	0.8	3.9
01	011	1	2.3	001	0	0.8	0	0	0.8	3.9
10	000	1	2.3	010	0	0.8	1	0	0.8	3.9
11	001	1	2.3	011	0	0.8	1	0	0.8	3.9

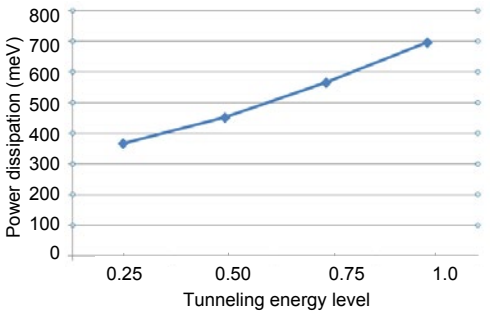

Fig. 12 Power dissipation of the proposed cryptographic architecture at different tunneling energy levels

6 Conclusions

Cryptographic devices can be victimized by a side-channel attack. The proposed design enables to obtain a secure QCA-based cryptographic module, as QCA circuits are resistant against power analysis attack. The codec proposed in this study can encrypt and decrypt 8-bit message using 8-bit key. However, it is applicable to a message of any length. The proposed XOR, MUX, DEMUX, and nanorouter outperform the state-of-the-art designs. Future implementation of cryptographic algorithms for QCA-based secure nanocommunication systems can be achieved using the proposed circuit.

Compliance with ethics guidelines

Bikash DEBNATH, Jadav Chandra DAS, and Debashis DE declare that they have no conflict of interest.

References

Ahmadpour SS, Mosleh M, 2018. A novel fault-tolerant multiplexer in quantum-dot cellular automata technology. *J Supercomput*, 74(9):4696-4716. https://doi.org/10.1007/s11227-018-2464-9

Angizi S, Sarmadi S, Sayedsalehi S, et al., 2015a. Design and evaluation of new majority gate-based RAM cell in quantum-dot cellular automata. *Microelectr J*, 46(1): 43-51. https://doi.org/10.1016/j.mejo.2014.10.003

Angizi S, Moaiyeri MH, Farrokhi S, et al., 2015b. Designing quantum-dot cellular automata counters with energy consumption analysis. *Microprocess Microsyst*, 39(7): 512-520. https://doi.org/10.1016/j.micpro.2015.07.011

Balali M, Rezai A, Balali H, et al., 2017. Towards coplanar quantum-dot cellular automata adders based on efficient three-input XOR gate. *Results Phys*, 7:1389-1395. https://doi.org/10.1016/j.rinp.2017.04.005

Das JC, De D, 2012. Quantum dot-cellular automata based cipher text design for nano-communication. Proc Int Conf on Radar, Communication and Computing, p.224-229. https://doi.org/10.1109/ICRCC.2012.6450583

Das JC, De D, 2016a. Novel low power reversible binary incrementer design using quantum-dot cellular automata. *Microprocess Microsyst*, 42:10-23. https://doi.org/10.1016/j.micpro.2015.12.004

Das JC, De D, 2016b. Quantum-dot cellular automata based reversible low power parity generator and parity checker design for nanocommunication. *Front Inform Technol Electron Eng*, 17(3):224-236. https://doi.org/10.1631/FITEE.1500079

Das JC, De D, 2017a. Circuit switching with quantum-dot cellular automata. *Nano Commun Netw*, 14:16-28. https://doi.org/10.1016/j.nancom.2017.09.002

Das JC, De D, 2017b. Nanocommunication network design using QCA reversible crossbar switch. *Nano Commun Netw*, 13:20-33

Das JC, De D, 2017c. Reversible binary subtractor design using quantum dot-cellular automata. *Front Inform Technol Electron Eng*, 18(9):1416-1429. https://doi.org/10.1631/FITEE.1600999

Das JC, De D, 2017d. Operational efficiency of novel SISO shift register under thermal randomness in quantum-dot cellular automata design. *Microsyst Technol*, 23(9):4155-4168. https://doi.org/10.1007/s00542-016-3085-y

Das S, De D, 2012. Nanocommunication using QCA: a data path selector cum router for efficient channel utilization. Proc Int Conf on Radar, Communication and Computing, p.43-47. https://doi.org/10.1109/ICRCC.2012.6450545

Debnath B, Das JC, De D, 2017. Reversible logic-based image steganography using quantum dot cellular automata for secure nanocommunication. *IET Circ Dev Syst*, 11(1):58-67. https://doi.org/10.1049/iet-cds.2015.0245

Debnath B, Das JC, De D, 2018. Design of image steganographic architecture using quantum-dot cellular automata for secure nanocommunication networks. *Nano Commun Netw*, 15:41-58. https://doi.org/10.1016/j.nancom.2017.11.001

Delfs H, Knebl H, 2015. Symmetric-key cryptography. In: Delfs H, Knebl H (Eds.), Introduction to Cryptography. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-47974-2_2

Heikalabad SR, Asfestani MN, Hosseinzadeh M, 2018. A full adder structure without cross-wiring in quantum-dot cellular automata with energy dissipation analysis. *J Supercomput*, 74(5):1994-2005. https://doi.org/10.1007/s11227-017-2206-4

Iqbal J, Khanday FA, Shah NA, 2013. Design of quantum-dot cellular automata (QCA) based modular 2^n-1-2^n MUX-DEMUX. Proc IMPACT, p.189-193. https://doi.org/10.1109/MSPCT.2013.6782116

Kahate A, 2008. Cryptography and Network Security. Tata McGraw Hill Education, India.

Kamaraj A, Marichamy P, Abinaya M, 2015. Design of reversible logic based area efficient multilayer architecture router in QCA. *Int J Appl Eng Res*, 10(1):140-144.

Karkaj ET, Heikalabad SR, 2017. Binary to gray and gray to binary converter in quantum-dot cellular automata. *Optik*, 130:981-989. https://doi.org/10.1016/j.ijleo.2016.11.087

Kianpour M, Sabbaghi-Nadooshan R, Navi K, 2014. A novel design of 8-bit adder/subtractor by quantum-dot cellular automata. *J Comput Syst Sci*, 80(7):1404-1414. https://doi.org/10.1016/j.jcss.2014.04.012

Lent CS, Tougaw PD, 1997. A device architecture for computing with quantum dots. *Proc IEEE*, 85(4):541-557. https://doi.org/10.1109/5.573740

Lent CS, Tougaw PD, Porod W, et al., 1993. Quantum cellular automata. *Nanotechnology*, 4(1):49-57. https://doi.org/10.1088/0957-4484/4/1/004

Liu WQ, Srivastava S, Lu L, et al., 2012. Are QCA cryptographic circuits resistant to power analysis attack? *IEEE Trans Nanotechnol*, 11(6):1239-1251. https://doi.org/10.1109/TNANO.2012.2222663

Mardiris VA, Karafyllidis IG, 2010. Design and simulation of modular 2^n to 1 quantum-dot cellular automata (QCA) multiplexers. *Int J Circ Theory Appl*, 38(8):771-785. https://doi.org/10.1002/cta.595

Mukhopadhyay D, Dinda S, Dutta P, 2011. Designing and implementation of quantum cellular automata 2:1 multiplexer circuit. *Int J Comput Appl*, 25(1):21-24. https://doi.org/10.5120/2996-4026

Orlov AO, Bernstein AGH, Lent CS, et al., 1997. Realization of a functional cell for quantum-dot cellular automata. *Science*, 277(5328):928-930. https://doi.org/10.1126/science.277.5328.928

Orlov AO, Kummamuru R, Ramasubramaniam R, et al., 2001. Clocked quantum-dot cellular automata devices: experimental studies. Proc 1st IEEE Conf on Nanotechnology, p.425-430. https://doi.org/10.1109/NANO.2001.966460

Porod W, 1997. Quantum-dot devices and quantum-dot cellular automata. *J Franklin Inst*, 334(5-6):1147-1175. https://doi.org/10.1016/S0016-0032(97)00041-0

Porod W, Lent C, Bernstein GH, et al., 1999. Quantum-dot cellular automata: computing with coupled quantum dots. *Int J Electron*, 86(5):549-590. https://doi.org/10.1080/002072199133265

Pudi V, Sridharan K, 2015. A bit-serial pipelined architecture for high-performance DHT computation in quantum-dot cellular automata. *IEEE Trans Very Large Scale Integr (VLSI) Syst*, 23(10):2352-2356. https://doi.org/10.1109/TVLSI.2014.2363519

Rashidi H, Rezai A, 2017. Design of novel efficient multiplexer architecture for quantum-dot cellular automata. *J Nano Electron Phys*, 9(1):01012. https://doi.org/10.21272/jnep.9(1).01012

Rashidi H, Rezai A, Soltany S, 2016. High-performance multiplexer architecture for quantum-dot cellular automata. *J Comput Electron*, 15(3):968-981. https://doi.org/10.1007/s10825-016-0832-3

Sardinha LHB, Costa AMM, Neto OPV, et al., 2013. Nanorouter: a quantum-dot cellular automata design. *IEEE J Sel Areas Commun*, 31(12):825-834. https://doi.org/10.1109/JSAC.2013.SUP2.12130015

Sayedsalehi S, Azghadi MR, Angizi S, et al., 2015. Restoring and non-restoring array divider designs in quantum-dot cellular automata. *Inform Sci*, 311:86-101. https://doi.org/10.1016/j.ins.2015.03.030

Sen B, Dutta M, Sikdar BK, 2014. Efficient design of parity preserving logic in quantum-dot cellular automata targeting enhanced scalability in testing. *Microelectr J*, 45(2):239-248. https://doi.org/10.1016/j.mejo.2013.11.008

Shah NA, Khanday FA, Bangi ZA, et al., 2011. Design of quantum-dot cellular automata (QCA) based modular 1 to 2^n demultiplexers. *In J Nanotechnol Appl*, 5(1):47-58. https://doi.org/10.1109/MSPCT.2013.6782116

Sridharan K, Pudi V, 2015. Design of Arithmetic Circuits in Quantum Dot Cellular Automata Nanotechnology. Springer, Cham, Germany. https://doi.org/10.1007/978-3-319-16688-9

Tougaw PD, Lent CS, 1994. Logical devices implemented using quantum cellular automata. *J Appl Phys*, 75(3): 1818-1825. https://doi.org/10.1063/1.356375

Walus K, Dysart TJ, Jullien GA, et al., 2004. QCADesigner: a rapid design and simulation tool for quantum-dot cellular automata. *IEEE Trans Nanotechnol*, 3(1):26-31. https://doi.org/10.1109/TNANO.2003.820815