Int. J. Nano Dimens., 9 (4): 336-345, Autumn 2018

ORIGINAL ARTICLE

A novel vedic divider based crypto-hardware for nanocomputing paradigm: An extended perspective

Bandan Kumar Bhoi [1], Neeraj Kumar Misra [2, *], Manoranjan Pradhan [1]

[1]Department of Electronics and Telecommunication, Veer Surendra Sai University of Technology, India

[2]Department of Electronics and Communication Engineering, Bharat Institute of Engineering and Technology, Hyderabad, India

Received 12 March 2018; revised 11 May 2018; accepted 21 May 2018; available online 23 May 2018

Abstract

Restoring and non-restoring divider has become widely applicability in the era of digital computing application due to its computation speed. In this paper, we have proposed the design of divider of different architecture for the computation of Vedic sutra based. The design of divider in the Vedic mode results in high computation throughput due to its replica architecture, where latency is minimized in each of the replica stages. The proposed novel divider based symmetric key crypto-hardware architecture for lightweight embedded devices and the results obtained for this architecture by the analysis using the QCADesigner tool. For the physical environment in QCA computing paradigm are achieved through optimization the architecture of cell by using the robust design computing architecture. For the extended perspective of lower divider to higher divider and to synthesize, target outcomes by using efficient architecture.

Keywords: *Cryptography; Divider; Quantum Dot Cellular Automata; Symmetric Key; Vedic Sutra.*

How to cite this article

Bhoi BK, Misra NK, Pradhan M. A novel vedic divider based crypto-hardware for nanocomputing paradigm: An extended perspective. Int. J. Nano Dimens., 2018; 9 (4): 336-345.

INTRODUCTION

Advances to the integrated circuit in recent sub-micron is more difficult due to the point of miniaturization can present many challenges. Quantum-dot automata (QCA) technology focus on tackling the problem of short channel effect and device density. QCA design provides a more robust, fast computation to the MOS transistor technology and gives a solution at the nanoscale but also offers a new method for computation and information transmission [1-4]. QCA circuits have the major advantage of low power dissipation, lightweight and faster speed of operation. QCA based cryptographic circuits are suitable for lightweight and energy efficient security solutions for mobile and pervasive computing devices. Side Channel Analysis (SCA) attacks based on power analysis have become a significant threat to CMOS based cryptographic circuits [5, 6]. This can be minimized by using QCA based cryptographic circuits because there is no current flow in QCA circuits.

In this work, we develop an extended perspective based divider for the application of crypto-hardware. In this approach, the novel divider is the Vedic framework adopted to optimize the latency in each replica. We have also implemented nanocomputing framework for the physical realization of crypto-hardware.

The rest of the paper is organized as follows: in section 2, we provide a brief background regarding QCA technology. In section 3, we develop the divider architecture. In section 4, the QCA implementation of the proposed crypto hardware is described. Section 5 deals with the result and power consumption analysis of the proposed designs with the earlier designs. The conclusion is presented in section 6.

* Corresponding Author Email: *neeraj.misra@ietlucknow.ac.in*

RELATED WORK

Several studies have reported the design of many cryptography circuits using QCA [7-12]. The work in [7-10] primarily focuses on the Serpent block cipher. A clocked logic is introduced for QCA based cryptographic processors in [11]. Cryptography is broadly classified into two main types. These are symmetric key encryption technique and asymmetric key encryption technique. The authors in [12] have designed a asymmetric key crypto hardware using QCA. To the best of our knowledge, there are no prior works on QCA based symmetric key crypto-hardware with encryption and decryption blocks. Symmetric key cryptography is faster than the Asymmetric cryptography, often by 100 to 1000 times and requirement of storage memory is less as compared to the Asymmetric Key Cryptography [13]. This paper presents a design of symmetric key encryption algorithm using the division algorithm in QCA. However, to date, only two implementations of divider circuits using QCA have been proposed [14, 15], and these are based on restoring and non-restoring division methods. Because of the importance of dividers as an essential arithmetic operation in many computational and processor circuits. In this paper investigates the implementation of a novel QCA divider is proposed. This algorithm describes a simple procedure for carrying out the division using simple multiplications and subtractions. Comparisons show that the new divider is more efficient in terms of latency, complexity and area compared to the previous designs based on restoring and non-restoring architectures [14, 15]. All the proposed architectures are implemented in the QCAD Designer tool [16], resulting in a decrease in gate counts and the level in the QCA design.

QCA BACKGROUND

In this section, we show an overview of QCA logic and established design approached synthesis and target digital logic functions using cells arrangements.

QCA computing logic

QCA was first introduced by Lent et al. in 1993. QCA is a novel emerging technology in which logic states are not stored as voltage levels, but rather as the position of the individual electrons. A QCA cell can be viewed as a set of four 'dots' that are positioned at the corner of the square. A quantum dot is a location of the cell in which a charge can be localized. The cell contains two extra mobile electrons that can quantum mechanically tunnel between the dots. Due to Coulomb repulsion, in the absence of external electrostatic perturbation, the electrons are forced to the corner positions to maximize their separation [17].

QCA operates by the Columbia interaction that connects the state of one cell to the state of the neighbours, unlike the conventional logic circuits in which information is transferred by electrical current. The two-polarization orientation encodes the data, '1' and '0' in QCA. In the binary wire, a signal propagates from the input to the output due to the Columbia interactions between the cells. Due to the presence of even and an odd number of cell arrange by 45° (rotated) cells form a buffer and inverter as shown in Fig. 1b. The inverter is configured by cell arrangement as shown in Fig. 1c. The two basic logic gates in QCA are the majority gate and the inverter. The logic function of majority gate is M (A, B, C) = AB + AC + BC, where A, B and C are three inputs. In a CMOS based system, timing is controlled through a reference signal (i.e., a clock) and is mostly required for sequential circuits. However, timing in QCA is necessary for both combinational and sequential circuits and is accomplished by clocking in four distinct periodic phases [18]. Clocking provides power gains in QCA [19] as well as the control of the information flow between the cells.

The shape of three-input and five-input majority gate, inverter and polarization are drawn in Fig. 1d. The electrostatic repulsion in between the electrons of the primary input cells, the driver cell is polarized and the majority gate performing, subsequently, primary output is shown by the outer cell. Five-input majority gate has fitting in a similar way to the three-input majority gate to generate the Boolean expression of OR, AND. In this way, all the digital designs are based on the majority gate and inverter.

Four Clocking Mechanism: In QCA 4-clocking is considered for information flow. Each group of cells is considered by same clock zone. The picture of a four clock is presented in Fig 1e. There is seen a 90^0 phase-delay from previous clocking zone to next clock as drawn in Fig. 1e. QCA clocking provides signal energy-restoration and timing-synchronization.

EXISTING DIVIDER ARCHITECTURE

The binary division operation is of immense importance in the field of engineering science.

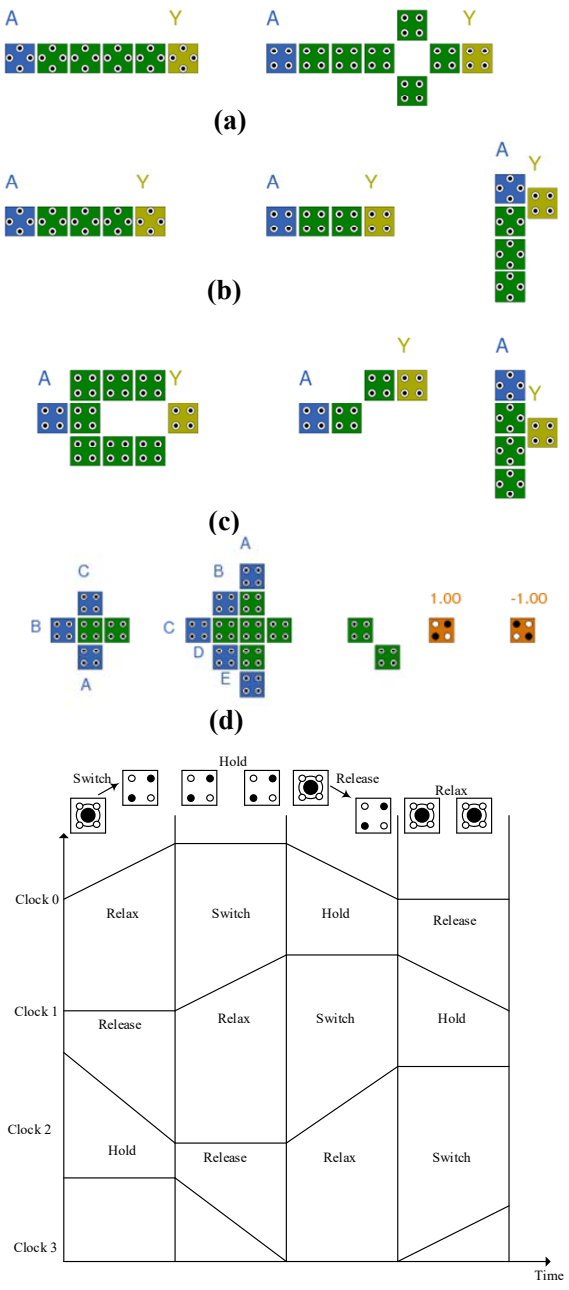

Fig. 1. QCA Design (a) Even number of cell-based wire (b) Odd number of cell-based wire (c) Inverter (d) 3 and 5 input Majority, inverter, and possible polarization (e) Clocking.

This paper presents a new division architecture to perform binary number division. Authors in [14, 15] implemented the non-restoring division architecture in QCA which is the previous best design in QCA. According to Ref. [15], an n-bit divider is formed by n^2 CAS cells. Thus, for a 4-bit division architecture 16 CAS cells and for an 8-bit division architecture 64 CAS cells are needed. A single CAS cell consists of a one-bit full adder and a two-input XOR gate. According to [14] [15], a one-bit full adder is implemented by 3 majority gates, 2 inverters and an XOR gate are implemented by 3 majority gates, 2 inverters in QCA. So to implement a 4 bit non restoring architecture 96 majority gates and 64 inverters needed. Similarly for an 8-bit non restoring division architecture 384 majority

gates and 256 inverters needed. The limitation of non restoring division architecture is that for a n-bit size divisor, 2n-bit size dividend is needed. In majority applications for n bit processor architecture, n-bit dividend and n-bit divisor are needed for division operations. In this paper, we designed a n-bit by n-bit division architecture in QCA which consist of lesser majority gates and inverters compared to n-bit non-restoring division architecture [14, 15].

Proposed division architecture

This paper presents the architecture of a novel division algorithm for binary numbers, which is implemented in QCA. Fig. 2 shows two examples in binary numbers to explain the above process. The steps of an algorithm for binary numbers are explained as follows:

i. Divide A(2) by B(2). Here quotient obtained is 'Q' and Remainder is 'R'.
ii. Append the remainder R to the left of A (1) and form R'A (1)' called C.
iii. Now multiply Q by B(1) called D and subtract the results of this multiplication from value C obtained in step 3.
iv. If the result of the subtraction is equal to or greater than 0, then the result is the final remainder.
v. If the result of the subtraction is less than 0, then decrease the final quotient by 1 and append B(2) to the left of A(1) to form new C.
vi. Multiply the updated quotient 'Q' with the B(1) to form new D.
vii. Subtract D from C to get final Remainder and updated quotient of step 6 is the final quotient 'Q'.

The mathematical modelling of this binary division algorithm is explained below for n number of bits. This model highlights the significant ease of computations and operations. Block diagram of the binary divider for a 4-by-4 bit is shown in Fig. 3.

$$for\ C > D\ and\ i > \left(\frac{n}{2}\right) \rightarrow\ Q = \frac{A(i)}{B(i)}\ ,R = C - D \quad (1)$$

$$for\ C < D\ and\ i > \left(\frac{n}{2}\right)\ \rightarrow Q = \left(\frac{A(i)}{B(i)}\right) - 1 \quad (2)$$

$$C = [A(i)'R1']\,, R1 = remainder\ of A(i)/B(i) \quad (3)$$

$$D = B(i-4) \times \left(\frac{A(i)}{B(i)}\right) \quad (4)$$

$$R = C - D, R = Final\ Remainder \quad (5)$$

Hierarchical design

The proposed method is suitably modified for QCA implementation using the block diagram discussed shown in Fig. 3. This is a block diagram for a simple 4-by-4 bit division that uses a 2-by-2 bit divider, a comparator, two 2 bit multiplier, two 4 bit subtraction blocks and a 2-bit decremented block. Because it is a hierarchical structure, this 4-by-4 bit division block will form the first block of the 8-by-8 bit division. The 8-by-8 bit division block can be built in a similar manner. The advantage of this method is that to carry an 8-by-8 bit division, we will ultimately be using only one 2-by-2 bit division block. Dividers for large word sizes can be implemented simply by adding additional bit slices in an array pattern. Thus, we find that the division circuit can be designed without division.

Design of subcomponents

In this paper, a 4-by-4 bit divider and 8-by-8 divider are implemented in QCA. The basic components for a 4-by-4 bit divider are 2-by-2 bit divider, 2-bit multiplier, 4-bit subtractor, 2 bit decremented block and a 4-bit comparator.

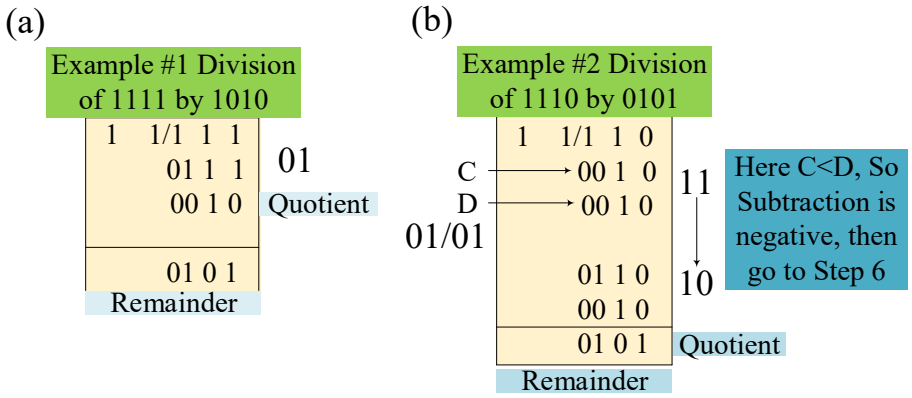

Fig. 2. Division examples (a) 1111 by 1010 (b) 1110 by 0101.

2-by-2 bit divider Block

Here 2-by-2 bit divider is designed using truth table and K-map minimization. The corresponding QCA schematic of the 2 by 2-bit divider circuit in QCA is shown in Fig. 4. The Boolean expressions derived for outputs are expressed as below.

$$Q_1 = A_1 B_0 \overline{B}_1 \quad (6)$$

$$Q_0 = A_0 B_0 \overline{B}_1 + A_1 B_1 (A_0 \overline{+} B_0) \quad (7)$$

$$R_1 = A_1 B_0 \overline{A}_0 B_1 \quad (8)$$

$$R_0 = A_0 B_1 (\overline{A}_1 \overline{+} B_0) \quad (9)$$

Two bit multiplier Block

In this paper, a straightforward binary multiplier is used because 2-bit multiplication requires simpler hardware compared to other multiplication algorithms. The algorithm is based on calculating partial products, shifting them to the left and then adding them together. A modified half adder is used in this multiplication architecture. Fig. 5 shows the QCA schematic of half adder and the multiplier for inputs A (i.e., A_1A_0) and B (i.e., B_1B_0). The Boolean expression for this half adder is given below.

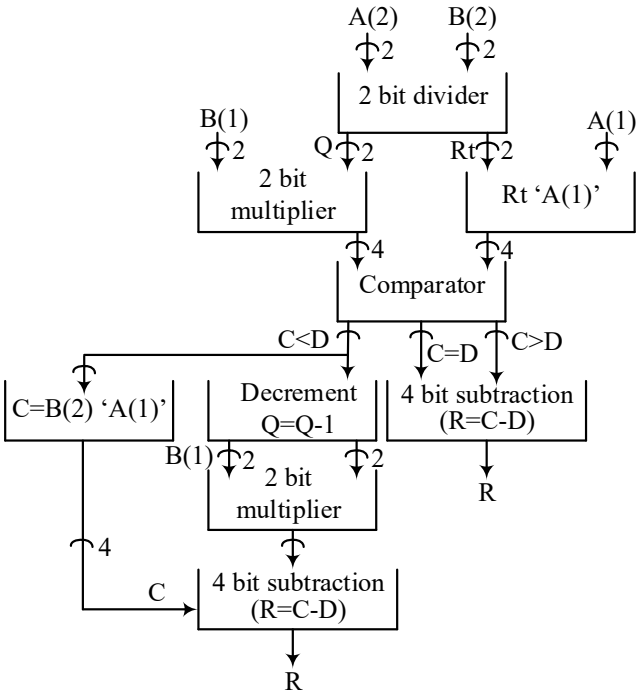

Fig. 3. Block diagram of 4-by-4 proposed binary divider.

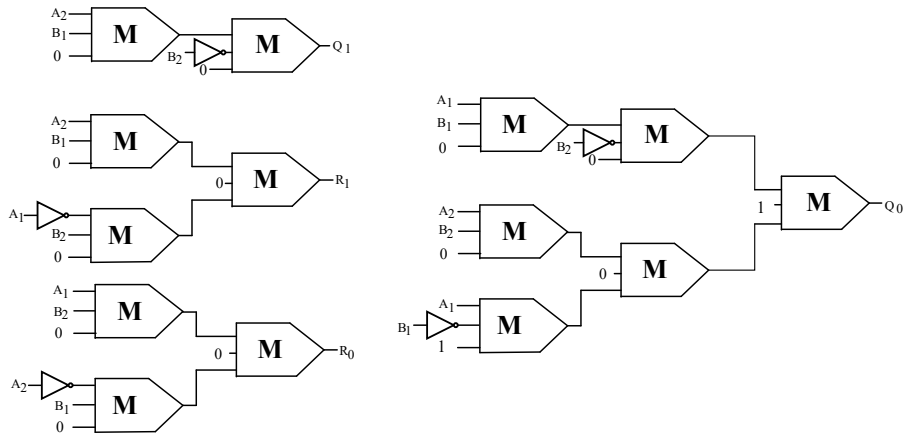

Fig. 4. QCA schematic of 2-by-2 bit divider.

$$Sum = (A + B).\overline{AB} \quad (10)$$

$$Carry = AB \quad (11)$$

Comparator Block

The comparator is a digital circuit that compares two input numbers and generates three outputs. For inputs A and B, then the outputs are A> B, A=B,

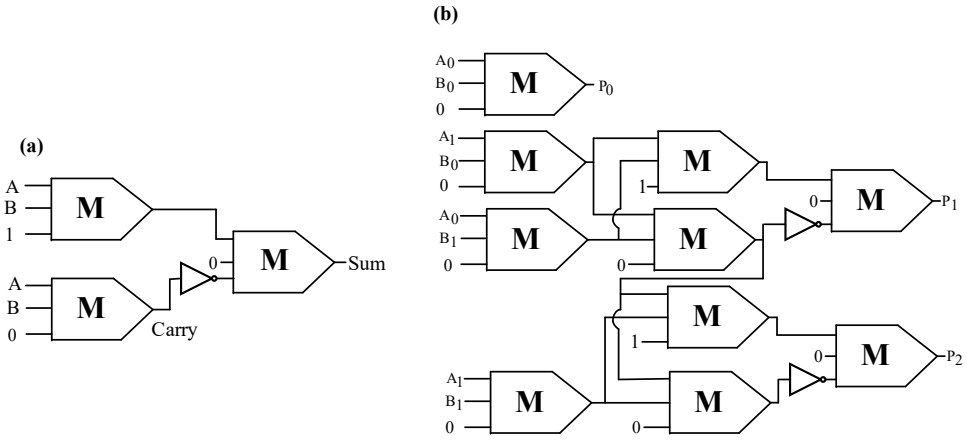

Fig. 5. QCA Schematic (a) Half adder (b) Two-bit multiplier.

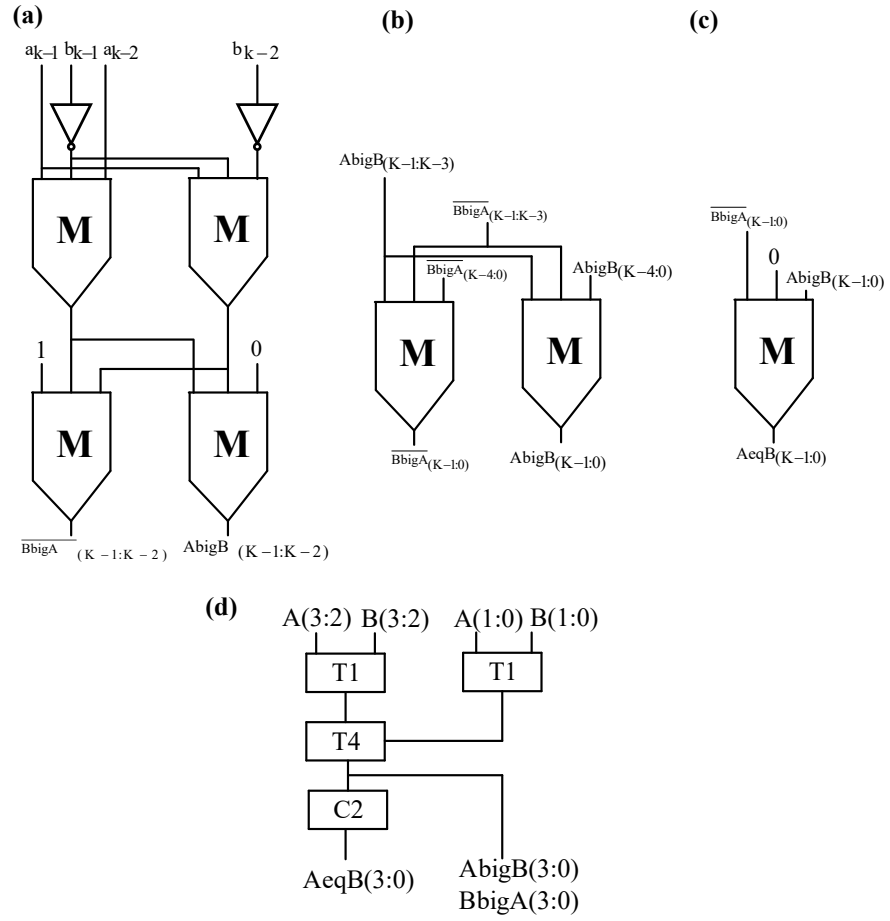

Fig. 6. QCA schematic of 4 bit comparator [20] (a) T1 (b)T4 (c) C2 (d) Final comparator.

and A<B. In this paper for the 4-bit division, a 4-bit comparator [20] is used for 8-bit division and the 8-bit comparator is used [20]. QCA schematic of the 4-bit comparator [20] is shown in Fig. 6.

Four bit Subtractor Block

In this paper, 4-bit subtractor is used in the final divider circuit. Because subtraction of two operands is equal to the addition of one operand with the 2's complement of the other operand, the 1-bit adder is the basic component of the subtractor block. The block diagram of the subtractor and the QCA schematic diagram of one bit modified full adder [14] are shown in Fig. 7.

Two bit Decremented block

In this paper, a two-bit decremented block is used that decreases the given two-bit input number by 1. To implement this, 2-bit subtractor is used.

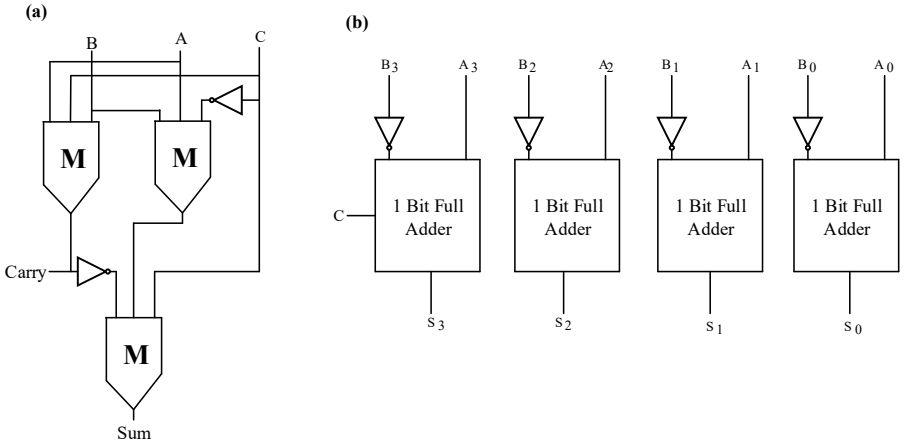

Fig. 7. (a) QCA schematic of Modified full adder [14] (b) Block diagram of 4-bit subtractor.

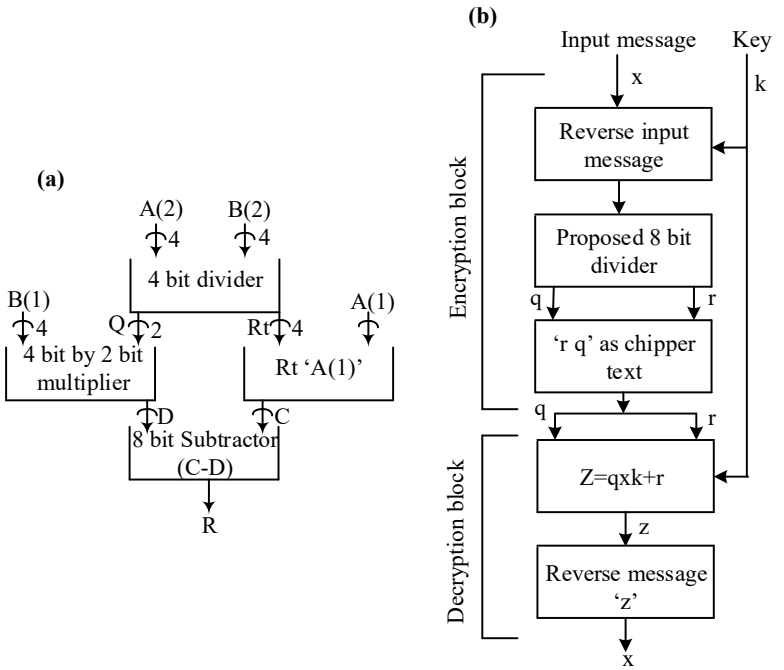

Fig. 8. (a) 8-bit divider block diagram (b) Algorithm of proposed crypto-hardware.

Proposed divider implementation

QCA layout of the proposed 4-bit divider is implemented using the components described in section 3.3. Other than these components four extra 2-to-1 multiplexers and two number of two input AND gates are used. Here the multiplexers are used to select one 4-bit remainder from two remainder values as shown in Fig. 8 of the proposed divider. Here select inputs of multiplexers are the output of the comparator. Similarly AND gates are used to select the final quotient which is the output of decremented block. Using proposed 4-bit divider block a novel 8-by-8 bit divider is designed and implemented. To design an 8-by-8 bit divider steps 6 to 8 of section 3.1 are not required. The block diagram is shown in Fig. 8. This divider is further used to design the proposed novel crypto-hardware.

PROPOSED CRYPTO-HARDWARE

This paper presents a design of symmetric key cryptography architecture using division algorithm. Here a novel encryption block and a decryption block are designed using QCA technology. Mathematically, cryptosystem is defined as a 5-tuple (M, K, E, C, D), where M is the set of characters used in plain texts, K is the set of keys, C is the set of cipher texts, E: M x K -> C is the set of enciphering functions, D: C x K -> M is the set of deciphering functions. The Keyspace K is the set of all possible keys. A brute-force approach for key recovery is called an Exhaustive Key Search. The number of possible keys $|K|$ must be large enough to make an exhaustive key search attack infeasible. For the secure transmission of data, we must design functions E and D such that E and D are inverse functions of each other. The E must not be easily identifiable to a third party. In a symmetric key cryptography, a single key is used for both encryption and decryption. It can be either stream ciphers or block ciphers. Stream ciphers operate on a single bit at a time and implement some form of feedback mechanism so that the key is constantly changing, whereas in the block cipher scheme, it encrypts one block of data at a time using the same key on each block. This paper describes a crypto-hardware based on a block cipher scheme where input key is fixed. But it can be suitably modified to a stream cipher scheme by designing of a feedback mechanism for a Key generation.

Algorithm of Proposed Crypto-Hardware

In this section, a more general algorithm is presented using the division algorithm on a set of positive integers. Given any positive integer x and y, there exist unique positive Integers q and r such that x = qy + r and 0 <r < y. The quotient and remainder, which are unique integers are the basic components used in division Algorithm based crypto-hardware. The algorithm is shown in Fig. 8b. This paper describes both encryption and decryption blocks in QCA. The proposed 8-bit divider implements encryption block and Decryption block is implemented by a 4-bit multiplier and an 8-bit adder circuit. QCA layout of proposed crypto-hardware is shown in Fig. 9.

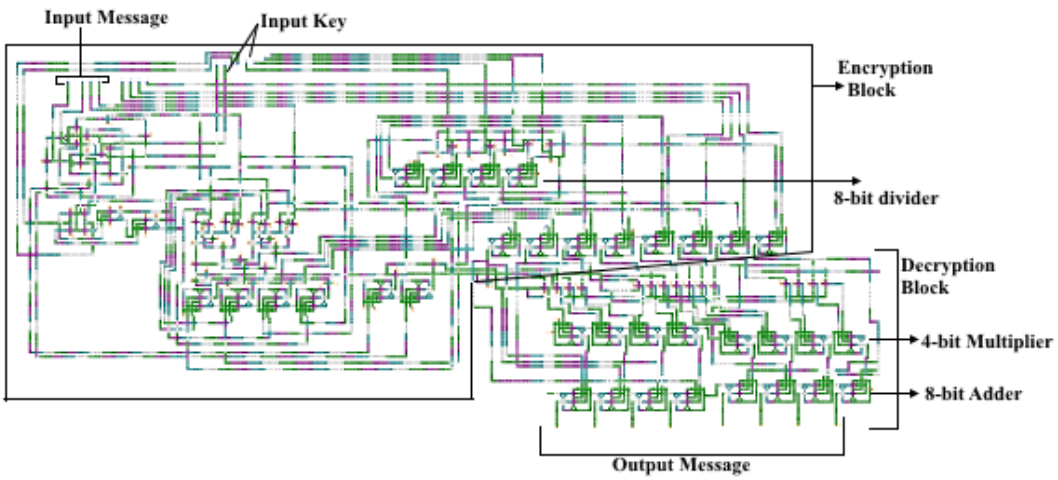

Fig. 9. QCA layout of Proposed Crypto-hardware.

RESULT ANALYSIS

In this section, we presented the all the subcomponents and the proposed divider in QCADesigner v2.0.3 tool [16]. The simulation was performed using the bistable approximation engine [17]. The parameters of the simulation are such as cell size of 18 nm, quantum dots in the cell have a diameter of 5 nm, adjacent cells are placed with a center to center distance of 20 nm, the number of samples is 12800, convergence tolerance is 0.001, effective radius is 65 nm, relative permittivity is 12.9, clock high is 9.8×10^{-22}, clock low is 3.8×10^{-23}, clock amplitude factor is 1, layer separation is 11.5, maximum iteration per sample is 100 [20]. The proposed crypto-hardware QCA layout is verified using exhaustive testing.

Case Study

In this section, we will discuss a case study to verify the operation of the proposed cryptographic architecture. In this case study, we shall illustrate the encryption and decryption process for a string *s*. Let *s* = "Wiley". Write ASCII code in binary for each character. The binary code for s will be "01010111 01101001 01101100 01100101 01111001".

Encryption Process

Here proposed division algorithm is applied to each character in binary code. Table 1 shows the application of encryption process for k = $(01010101)_b$. Thus, the encrypted text *y* for "Wiley" is "0100000010010000010100110110000010100010101001100100101". Here the length of plain text s is 40 and that of encrypted text is 50 bits long.

Decryption Process

Here encrypted text y will read from right to left. For each of the 10-bit sequence, we take rightmost 2 bits as q and left most 8 bits as r. Then form z = qk + r. This z is same as n. Then reversing digits in z, we get original string x. Consider rightmost 10 bits from string y. It is (0100100101). Here r = (01001001) and q = (10000), then w = q * k + r = (10011110). Reversing digits of *w,* original binary string (01111001) will be obtained, i.e., character 'y'. In this way, the process will be applied to all the group of 10 characters at a time to obtain original string "Wiley". Simulation result of the above case study is shown in Fig. 10.

It is divided into two parts for a clear view of the results because there is a delay of $20^{3}/_{4}$ clocks

Table 1. Encryption Process for the Characters in the String "Wiley".

Character	Binary (x)	*n* = Reverse (x)	q	r	y= encrypted n (r`q')
W	01010111	11101010	10	01000000	0100000010
i	01101001	10010110	01	01000001	0100000101
l	01101100	00110110	00	00110110	0011011000
e	01100101	10100110	01	01010001	0101000101
y	01111001	10011110	01	01001001	0100100101

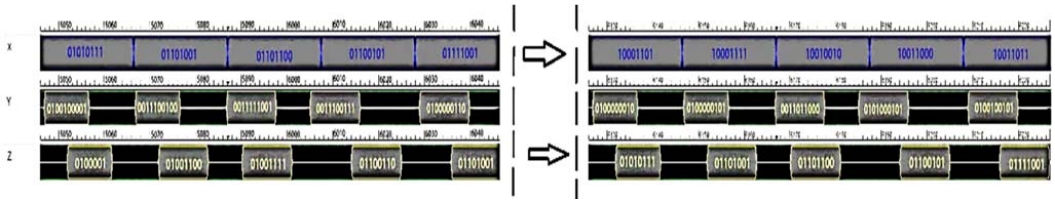

Fig. 10. Simulation result of case study example.

Table 2. Brief review and comparison table of the proposed designs.

Circuit	Complexity	Area	Latency
4-bit non restoring divider [14]	5124 cells	9.99 μm^2	$15^{1}/_{4}$ clocks
4 bit non restoring divider [15]	6865 cells	10.95 μm^2	$47^{1}/_{4}$ clocks
4 bit proposed divider	4570 cells	9.92 μm^2	$14^{1}/_{4}$ clocks
8 bit proposed divider	7212 cells	13.42 μm^2	$17^{1}/_{2}$clocks
Proposed crypto hardware	3485 cells	25.80 μm^2	$20^{3}/_{4}$clocks

cycle between the inputs and outputs. Here, the outputs obtained in the right-hand side part of simulation results are the inputs of the left-hand side part. Table 2 shows the cell complexity, area and delay of proposed designs.

CONCLUSION

In this paper, we analyze Vedic divider in QCA as an extended approach. We focus on submodules comparator, and divider embedded into Vedic divider architecture. We present the robust computing strategy of possible crypto-hardware implementation using single layer synthesis approaches and under metrics to evaluate the circuit. We show that crypto-hardware of divider created using QCA cell and high speed against throughput minimize, which has significant benefits compared to all ASIC based crypto-hardware circuits. As the design size increases, the proposed design will show more improvements compared to other designs in terms of area, and latency. The proposed circuit can be modified to any bit size by the proposed division algorithm for advanced security level.

CONFLICT OF INTEREST

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

REFERENCES

1. Tougaw P. D., Lent C. S., (1994), Logical devices implemented using quantum cellular automata. *J. Appl. Phys.* 75: 1818-1825.
2. Bhoi B., Misra N. K., Pradhan M., (2017), Design and evaluation of an efficient parity-preserving reversible QCA gate with online testability. *Cogent Eng.* 4: 1416888-1416892.
3. Amarel S., Cooke G., Winder R. O., (1964), Majority gate networks. *IEEE. Transac. Elec. Comput. EC.* 13: 4-13.
4. Bhoi B. K., Misra N. K., Pradhan M., (2018), Design of conservative gate and their novel application in median filtering in emerging QCA nanocircuit. *In Proceedings of the Second International Conference on Computational Intelligence and Informatics* (pp. 131-141). Springer, Singapore.
5. Kocher P., (1996), Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other Systems. Proc. of the *16th Annual International Cryptology Conference on Advances in Cryptology*. 104-113.
6. Kelsey J., Schneier B., Wagner D., Hall C., (2000), Side channel cryptanalysis of product Ciphers. *J. Comp. Security.* 8: 141-158.
7. Liu W., Neill M., Swartzlander E. E., (2012), Are QCA cryptographic circuits resistant to power analysis attack. *J. IEEE Transact. Nanotech.* 11: 1239-1251.
8. Amiri M. A., Mahdavi M., Mirzakuchaki S., (2010), Logic-based QCA implementation of a 4× 4 S-Box. *IEEE Conf. Comp. Applic. Indust. Electron.* 415-420.
9. Rahimi E., Nejad S. M., (2009), Secure clocked QCA logic for implementation of quantum cryptographic processors. *In Appl. Electron. AE 2009 IEEE.* 217-220.
10. Amiri M. A., Amin M., Mahdavi M., Atani R. E., Mirzakuchaki S., (2009), QCA implementation of serpent block cipher. *In Advances in Circuits, Electronics and Micro-electronics CENICS'09.* 16-19.
11. Das J. C., De D., (2012), Quantum dot-cellular automata based cipher text design for nano-communication. *In Radar, Communication and Computing (ICRCC' 12). Int. Conf. IEEE.* 224-229.
12. Purkayastha T., De D., Das K., (2016), A novel pseudo random number generator based cryptographic architecture using quantum-dot cellular automata. *J. Microprocess. Microsys.* 45: 32-44.
13. Forouzan B. A., (2007), Cryptography Network Security. Tata McGraw-Hill.
14. Sayedselehi S., Azghadi M. R., Angizi S., Navi K., (2015), Restoring and non-restoring array divider designs in quantum-dot cellular automata. *Inform. Sci.* 311: 86-101.
15. Cui H., Cai L., Yang X., Feng C., Qin T., (2014), Design of non-restoring binary array divider in quantum-dot cellular automata. *IET Micro & Nano Lett.* 9: 464-467.
16. Walus K., Dysart T. J., Jullien G. A., Budiman R. A., (2004), QCADesigner: A rapid design and simulation tool for quantum-dot cellular automata. *IEEE Transact. Nanotechnol.* 3: 26-31.
17. Lent C. S., Tougaw P. D., Porod W., Bernstein G. H., (1993), Quantum cellular automata. *Nanotechnol.* 4: 49-57.
18. Sen N. K., Wairya B., Bhoi S., (2017), Testable novel parity-preserving reversible gate and low-cost quantum decoder design in 1D molecular-QCA. *J. Circuits. Sys. Comput.* 26: 1750145-1750145.
19. Lent C. S., Isaksen B., (2003), Clocked molecular quantum-dot cellular automata. *IEEE Transact. Elect. Dev.* 50: 1890-1895.
20. Perri S., Corsonello P., Cocorullo G., (2013), Design of efficient binary comparators in quantum-dot cellular automata. *IEEE Transact. Nanotech.*13: 192-202.