Journal of VLSI Circuits and Systems, ISSN: 2582-1458 Vol. 6, No. 2, 2024 (pp. 75 -83)
RESEARCH ARTICLE
WWW.VLSIJOURNAL.COM

Reversible Vedic Direct Flag Divider in Key Generation of RSA Cryptography

Udhayakumar A[1],Ramya K C[2],Vijayakumar P[3],Sheeba Rani S[4], Balamanikandan A[5],Saranya K[6]

[1]*Department of Electronics and Communication Engineering,Hindusthan college of Engineering and Technology, Coimbatore, India.*
[2]*Department of Electrical and Electronics Engineering,Sri Krishna College of Engineering and Technology, Coimbatore,India.*
[3]*School of Electronic Engineering, Vellore Institute of Technology, Chennai,India.*
[4]*Department of Electronics and Communication Engineering,Sri Eshwar College of Engineering, Coimbatore, India.*
[5]*Department of Electronics and Communication Engineering, Mohan Babu University (Erstwhile SreeVidyanikethan Engineering College), Tirupati, India.*
[6]*Department of Electrical and Electronics Engineering, Dr. Mahalingam College of Engineering and Technology Coimbatore, India.*

KEYWORDS:

Reversible Logic, VLSI, Cryptography, Vedic Division, Arithmetic Circuits.

ARTICLE HISTORY:
Received: 09.07.2024
Revised: 12.08.2024
Accepted: 25.09.2024

DOI:
https://doi.org/10.31838/jvcs/07.02.08

Abstract

Reversible logic does not dissipate energy, and information loss never occurs. As a result, this futuristic technology is being applied in many areas requiring minimal energy dissipation. This work focuses on the design of a new Vedic divider circuit and its implementation using reversible gates. The Direct Flag Vedic Division Method (DFVDM) is a novel methodology addressed in this proposed work through reversible logic. We have utilized basic reversible gates in block-level construction and demonstrated that the proposed Reversible Direct Flag Vedic Division Method (RDFVDM) achieves efficiency in quantum parameters, as well as in area, power, and delay. This divider circuit offers several advantages, including fewer garbage outputs and minimal quantum cost. Simulations were conducted using the Cadence Tool. The proposed Vedic divider is compared to existing designs based on reversible structural metrics like garbage outputs, constant inputs, and quantum cost, and the results indicate that RDFVDM outperforms equivalent designs. In terms of energy usage, RDFVDM shows a 19% improvement and exhibits a 5% reduction in quantum cost compared to other state-of-the-art designs.

Author's e-mail and Orcid: udhayakumar.ece@hicet.ac.in, ramyakc@skcet.ac.in, vijayrg-cet@gmail.com, sheebarani.s@sece.ac.in, balamanieee83@gmail.com. ORCID-0000000 223210030, miles2gosaran@gmail.com.

How to cite this article: Udhayakumar A, Ramya KC,Vijayakumar P,Sheeba Rani S, Balamanikandan A,Saranya K. Reversible Vedic Direct Flag Divider in Key Generation of RSA Cryptographic , Journal of VLSI Circuits and System Vol. 6, No. 2, 2024 (pp. 75-83).

ABSTRACT- INDEX TERMS: Direct Flag Vedic Division Method, Reversible Gates, Rivest-Shamir-Adleman Cryptography.

Introduction

Arithmetic dividers are crucial hardware blocks in applications such as digital signal processing, cryptography, and other logical computations. A reversible array divider circuit based on a non-restoring division algorithm has been implemented using k-CNOT gates.[1] This work claims a reduction in the number of garbage outputs and gates. A reversible multiplier designed to reduce quantum parameters is discussed in.[2]. In,[3] double-precision floating-point Vedic dividers are used in Rivest-Shamir-Adleman (RSA) cryptography. A floating-point divider based on the Goldschmidt algorithm, which uses subtraction and floating-point multiplication, is realized. The authors utilized the Nikhilam Sutra and the Parvartya Sutra to reduce time delays. The design of a Red Green Blue to Hue Min Max Difference converter circuit, based on several reversible modules performing addition, subtraction, multiplication, registers, multiplexers, and comparator functions, is used in low-power video processing applications.[4] A scalable reversible binary division circuit that handles floating-point data, exact rounding, and division from single-sided approximations is developed in.[5]

Reversible blocks have been used to design a large divider circuit with components like multiplexers and registers .[6] The work proposed in[7] presents an architecture for

reversible greatest common divisor computation that requires fewer iterations, using a modified binary Greatest Common Divisor (GCD) algorithm. In,[8] a thirty-two-bit divider is designed using the ancient Parvartya Sutra methodology, a general division formula that efficiently divides large numbers concerning delay and power consumption. RSA public key cryptography, used for data encryption, is implemented using the Vedic divider "Dhvajanka" (on the top of the flag) in.[9] Implementing the RSA algorithm for Android message encryption is discussed in,[10] providing insight into validating the suggested approach within RSA crypto techniques. A reversible shift register is used in a new fault-tolerant reversible divider that employs a parallel adder.[12] The use of reversible gates in designing optimal data-path circuits is mentioned in.[13–15] In,[16] RSA cryptography utilizes the Vedic divider with double-precision floating-point division. An adder/subtractor cell and a non-restoring algorithm are used to build an arithmetic serial divider in ,[17]. In,[18] the "Paravartya Yojayet" technique is employed to reduce power consumption and latency in a Vedic divider built using 45 nm technology. The work proposed in[19] implements a programmable frequency divider that uses a binary counter in conjunction with a synchronous counter and an asynchronous reset to convert an input clock of 32 kHz to 1 Hz. A Taylor series expansion is used to construct the reciprocal of the divisor in an approximate binary divider.[20] Low-power signal processing applications use a trade-off between energy and speed to manage accuracy. The binary signed-digit adder, radix complements, and an estimated radix divider are employed to maximize the number of bits, while cell truncation and error compensation improve circuit-level performance and error characteristics.[21] Low power consumption, high speed, and a smaller area are crucial for designing any Very Large Scale Integrated (VLSI) system. Area and speed are often incompatible constraints, so good designs must balance these factors. As a result, high-speed divider architecture is becoming increasingly important. Most existing divider circuits are classified as either restoring or non-restoring, or use Vedic dividers with the Nikhilam Sutra and Parvartya Sutra. The divider circuit is a critical arithmetic unit that involves complex computation and can slow down overall processing. This work introduces a new Vedic Sutra design using blocks of reversible arithmetic circuits, optimizing structural and quantum parameters. The proposed Direct Flag Vedic Division Method (DFVDM) is novel and the first model among the literature on arithmetic divider circuits using basic reversible gates such as the Feynman Gate (FG), Toffoli Gate (TG), and Fredkin Gate (FRG). The Vedic divider is implemented in the RSA cryptographic algorithm to demonstrate the efficiency of the proposed system. Section 2 describes the implementation of RDFVDM in a systematic manner. Section 3 details the block-level implementation of RDFVDM. Section 4 discusses RDFVDM in the context of the Greatest Common Divisor (GCD). Section 5 covers key generation in the RSA cryptographic algorithm. Section 6 elaborates on the simulation results.

Implementation of RDFVDM

The Direct Flag Method is one of the division methodologies in Vedic mathematics that uses shortcuts for dividing any type of number. DFVDM involves four major steps:

Input: Enter the dividend and divisor.

Divide and Flag: Divide the divisor into two halves. Consider the first half as the new divisor and the second half as a flag.

Division Process: Repeat the Divide Multiply Compare Subtract (DMCS) unit N-1 times.

Obtain Results: At each stage of the DMCS unit, obtain the quotient. The remainder is obtained at the end. All blocks in the DFVDM are implemented using reversible gates to achieve the Reversible Direct Flag Vedic Division Method (RDFVDM).

If the Dividend is 1732 and the Divisor is 23 then the below operation illustrates the Figure 1

OPERATION

New divisor= 2 Flag = 3
D3=1; D2=7; D1=3; D0=2

Step1:

Division: D3/New Divisor => 1/2 => Q2=0 & R=1
Multiplication: Q2 x Flag => 0 x 3 = 0
Checking: RD2>0 => 17>0; Condition satisfied
Subtraction: RD2 - 0 = 17 - 0 => 17

Step2:

Division: 17/New Divisor => 17/2 => Q1=8 & R=1
Multiplication: Q1 x Flag => 8 x 3 = 24
Checking: RD1>24 => 13>24; Condition not satisfied
Hence, Q1 - 1 & R + New Divisor => Q1=7 & R=3
Multiplication: Q1 x Flag => 7 x 3 = 21
Checking: RD1>21 => 33>21; Condition satisfied
Subtraction: RD1 - 24 = 33 - 21 => 12

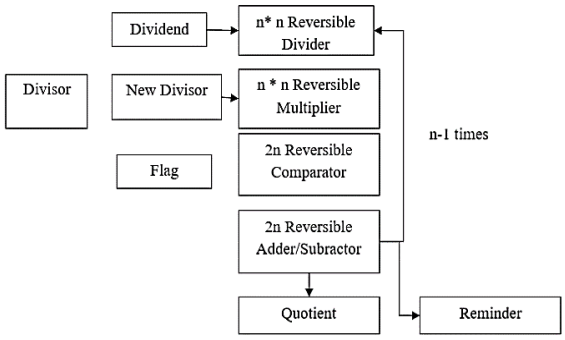

Fig. 1: Dividend and divisor operation

Step3:

Division: 12/New Divisor => 12/2 => Q0=6 & R=0
Multiplication: Q0 x Flag => 6 x 3 = 18
Checking: RD0>18 => 02>24; Condition not satisfied
Hence, Q0 - 1 & R + New Divisor => Q0=5 & R=2
Multiplication: Q0 x Flag => 5 x 3 = 15
Checking: RD0>15 => 22>15; Condition satisfied
Subtraction: RD0 - 15 = 22 - 15 => 7
OUTPUT
Q=086 & R=7

RDFVDM

It can be noted from Figure 1 that the RDFVDM method involves an n*n multiplier, an n*n divider, a 2n-bit comparator, and a 2n-bit adder / subtractor unit. The reversible implementation of the blocks involved is discussed in subsections.

Reversible Adder/Subtractor

The n-bit reversible adder/subtractor comprises one reversible half adder/subtractor (RHA/S) and n-1 reversible full adder/subtractor (RFA/S). Figure 2 shows the block-level implementation of a Reversible 8-bit adder/subtractorwith A and B as inputs and C as the control signal. S_D is the 8-bit output and C_D is the Carry/Difference output. The total quantum cost of the circuit is 76.

Reversible Comparator

The reversible n-bit comparator is made of n-1 single-bit comparator and 1 MSB comparator block. Figure 3 shows the 8-bit comparator with A and B as 8-bit inputs and P, Q and R as the outputs. The most significant bits A7 and

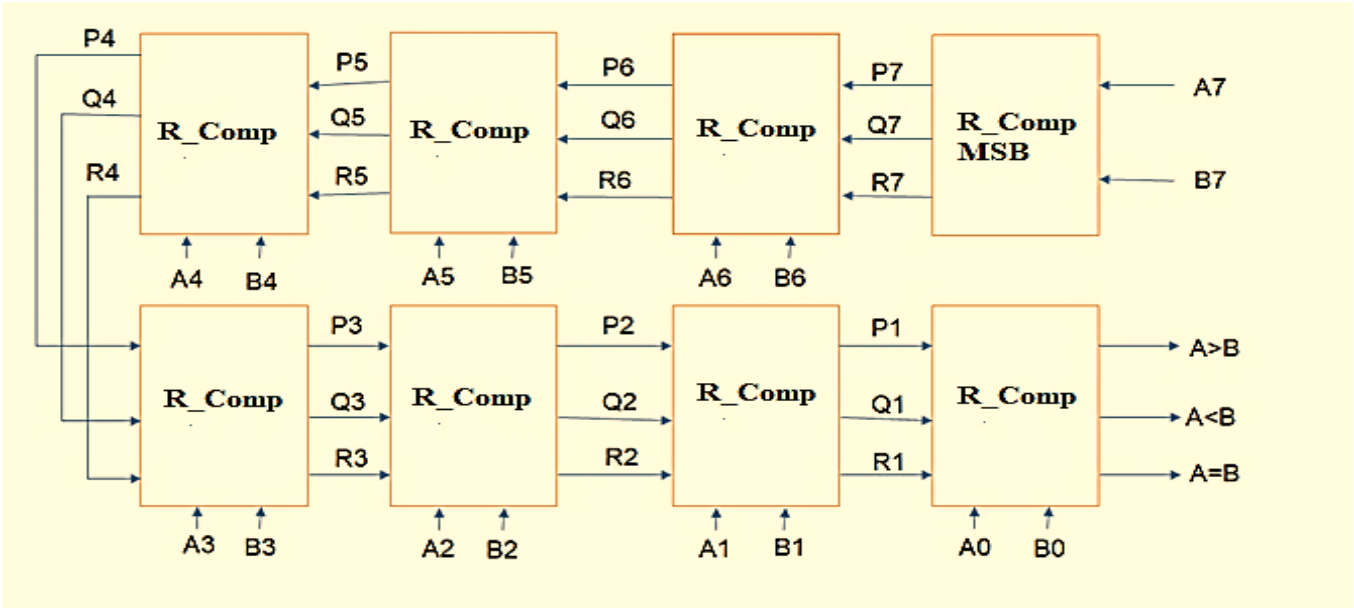

Fig. 2: Reversible 8x8 Adder/Subtractor

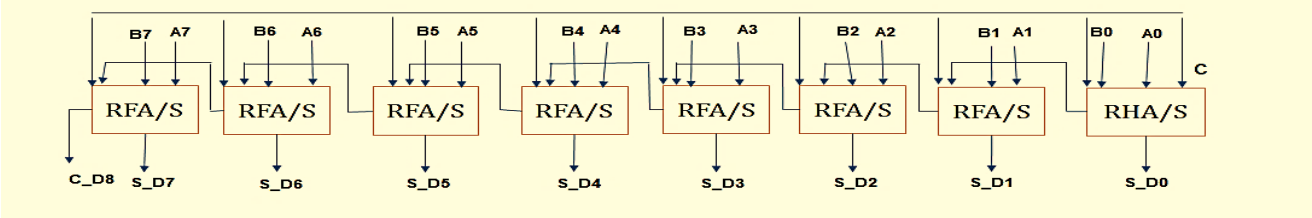

Fig. 3: Reversible 8-bit Comparator

B7 of the inputs are given to the MSB comparator and the remaining inputs are given to the 1-bit comparator. Each comparator gives the comparison result of the corresponding input. The final comparator gives the result of 8-bit inputs. The total quantum cost of the MSB comparator is 11. The quantum cost of the NFT gate is 5. The quantum cost of the NFT Block is 7. The quantum cost of an 8x8 reversible comparator is 179. The number of constant inputs is 33 and the garbage output is 47.

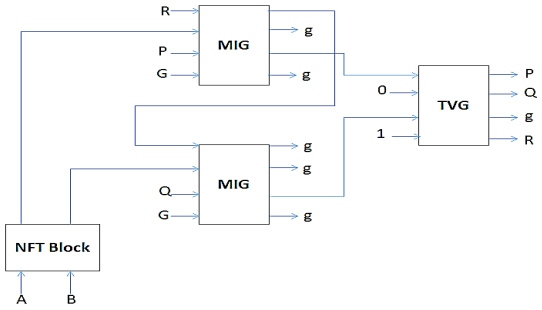

Fig. 4: Reversible 1-bit Comparator (R_Comp)

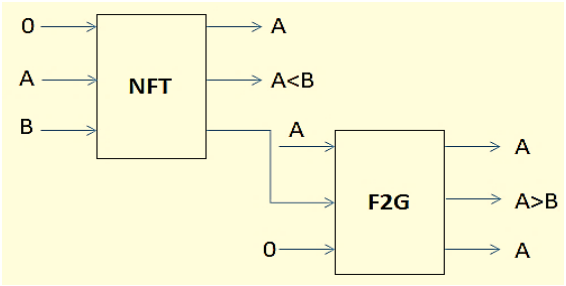

Fig. 5: Reversible NFT Block

Figure 4 shows the block diagram of single-bit comparator R_Comp. It employs one NFT Block, 2 MIG gates and one TVG gate. In Figure 4 A and B are the inputs. The outputs of the NFT blocks are connected to MIG gates. P, Q and R at the input of the MIG gates are the outputs of the previous block. P from the MSB comparator is given to the first MIG gate to produce A>B and Q from the MSB comparator is given to the second MIG gate to produce A<B. The third outputs of both MIG gates are given to the TVG gate to produce A=B. P, Q and R at the outputs are the outputs of the 1-bit comparator. The quantum cost of the TVG gate is 3. The number of constant inputs is four. The number of garbage signals is six which are represented by g.The NFT Block shown in Figure 5 is used to compare the next significant bits with A and B as the inputs to the NFT block. The NFT Block comprises one NFT gate and one F2G gate. NFT block produces output A<B and F2G gate produces output A>B. The quantum cost of the NFT gate is 5. The quantum cost of the NFT Block is 7. This block has two constant inputs which are set as 0. The numbers of garbage outputs are 3 which are denoted by A.

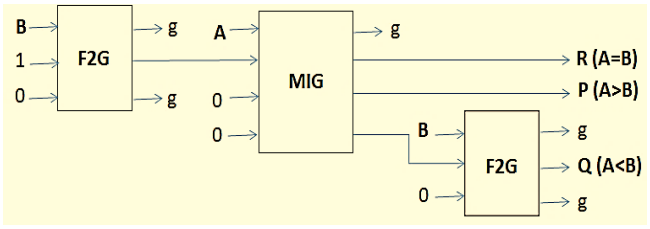

Fig. 6: Reversible MSB Comparator (R_Comp MSB)

The MSB Comparator takes the most significant bit for comparison. The construction of the MSB comparator shown in Figure 6 requires two F2G gates and one MIG gate. A and B are the inputs. P, Q and R are the outputs. B is the input to the first F2G gate and it produces an inverted output B'. A and B' are the inputs to the MIG gate which produces R (A=B) and P(A>B). The last output of the MIG gate is given to another F2G gate to produce Q(A<B). P, Q and R are the inputs to the reversible 1-bit comparator. The quantum cost of the F2G gate is 2 and the MIG gate is 7. The F2G gate is called the Double Feynman gate. The total quantum cost of the MSB comparator is 11. There are four constant inputs used here which are set as 0. The number of garbage outputs is 5. The garbage outputs are represented by g.[7]

Reversible Multiplier

The Urdhva Tiryak Sutra-based multiplier, shown in Figure 7, utilizes crossed and vertical operations. This method

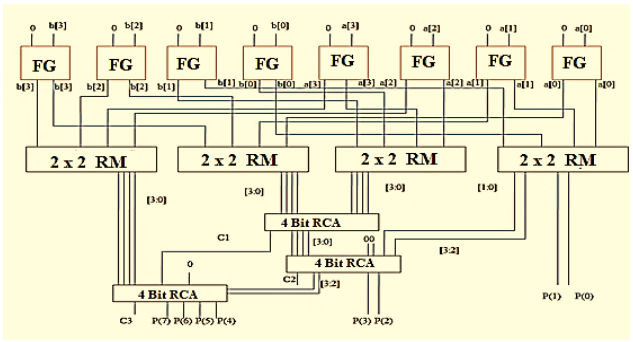

Fig. 7: Reversible 4x4 Vedic Multiplier

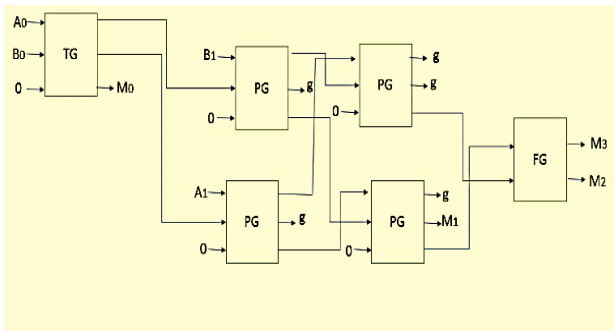

Fig. 8: Reversible 2x2 Reversible Multiplier (RM)

performs partial product generation and addition simultaneously, which speeds up the multiplication process.

The construction of the 2-bit Vedic multiplier is shown in Figure 8. The 2-bit Vedic multiplier consists of one Toffoli gate, four Peres gates, and one Feynman gate. The inputs, A and B, are each 2 bits wide, and the output, M, is 4 bits wide. The quantum cost of the Toffoli gate is 5, and the quantum cost of the 2-bit Vedic multiplier is 22.[2] This circuit has 5 constant inputs, all set to 0, and 5 garbage signals, and denoted by g. The 4-bit RCA (Ripple Carry Adder) includes one Peres gate and three HNG gates. The inputs, A and B, are each 3 bits wide, and the output, S, is 4 bits wide, with C as the carry output. The quantum cost of the HNG gate is 6, and the quantum cost of the 4-bit RCA is 22. It has 4 constant inputs, all set to 0. The PG gate contributes one garbage output, while each HNG gate contributes two garbage outputs, leading to a total of 7 garbage outputs for the reversible 4-bit RCA. The construction of this circuit is shown in Figure 9.

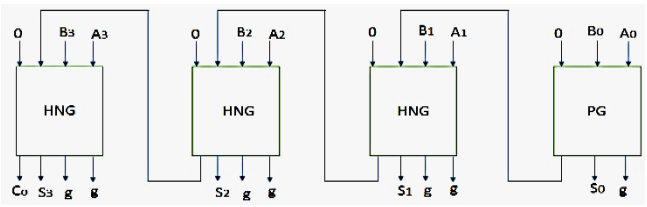

Fig. 9: Reversible 4-bit RCA

Reversible Divider

Non-restoring division is less complex than restoring division because it involves simpler operations such as addition and subtraction. The division method used in RDFVDM, as described by Lamjed Touil et al. [4], employs this technique. This method includes an 8-bit reversible adder/subtractor, with the reversible adder/subtractor being 5 bits in size. In this method, the divisor is 4 bits and the dividend is 8 bits. Initially A is assigned to be zero. At each level A and Q gets shifted to left. When the MSB bit of A is 1, Addition operation is done and when MSB bit of A is 0, Subtraction takes place. Q0 is assigned with the value 0 when MSB bit of A is 1 and vice versa. The process gets repeated until count becomes 0. At the end, if A<0, addition is done and if A>0 the process gets stopped.

Reversible non-restoring division.

INPUTS

Dividend = 1732 Divisor = 23
OPERATION
New divisor= 2 Flag = 3
D3=1; D2=7; D1=3; D0=2

Step1:

Division: D3/New Divisor => 1/2 => Q2=0 & R=1
Multiplication: Q2 x Flag => 0 x 3 = 0
Checking: RD2>0 => 17>0; Condition satisfied0
Subtraction: RD2 - 0 = 17 - 0 => 17

Step2:

Division: 17/New Divisor => 17/2 => Q1=8 & R=1
Multiplication: Q1 x Flag => 8 x 3 = 24
Checking: RD1>24 => 13>24; Condition not satisfied
Hence, Q1 - 1 & R + New Divisor => Q1=7 & R=3
Multiplication: Q1 x Flag => 7 x 3 = 21
Checking: RD1>21 => 33>21; Condition satisfied
Subtraction: RD1 - 24 = 33 - 21 => 12

Step3:

Division: 12/New Divisor => 12/2 => Q0=6 & R=0
Multiplication: Q0 x Flag => 6 x 3 = 18
Checking: RD0>18 => 02>24; Condition not satisfied
Hence, Q0 - 1 & R + New Divisor => Q0=5 & R=2
Multiplication: Q0 x Flag => 5 x 3 = 15
Checking: RD0>15 => 22>15; Condition satisfied
Subtraction: RD0 - 15 = 22 - 15 => 7

OUTPUT

Q=086 & R=7

The quantum cost of one 5-bit Reversible Adder/ subtractor is 46. The total quantum cost of the circuit is 305. Constant input is 40.

RDFVDM in RSA Algorithm.

RSA involves a public key and a private key. The public key can be used to encrypt messages that can be decrypted with the private key.

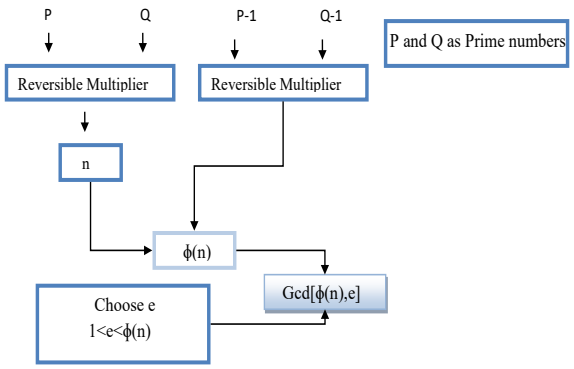

Fig. 10: Key Generation for RSA Cryptographic Algorithm

The keys for the RSA algorithm are generated as illustrated in Figure 11. Initially, n = p x q calculated, where n serves as the modulus for both the public key and the private key.Next, compute ϕ (n) = (p-1) x (q-1). Then select an integer e such that 1<e<ϕ(n) and gcd (ϕ((n))=1 where e is used as the public key exponent. Calculate d=e-1 mod ϕ (n), where d is kept as the private key exponent.

The RSA algorithm illustrated requires an n x n multiplier, n x n subtractor, n x n comparator, n x n divider, and n x n GCD. For an 8-bit implementation the quantum cost, constant input, and garbage output of the RSA algorithm is 1276,293,311 respectively. If P and Q are 5 and 7 and let “e” be 23 then the Private key will be {23, 35} and the public key will be {1}. If P and Q are 11 and 19 and let “e” be 166 then the Private Key will be {167,209} and the public key will be {13}. The GCD of two numbers is the largest number that divides both. Figure 12 depicts the GCD block diagram. The CD is designed using the proposed RDFVDM.

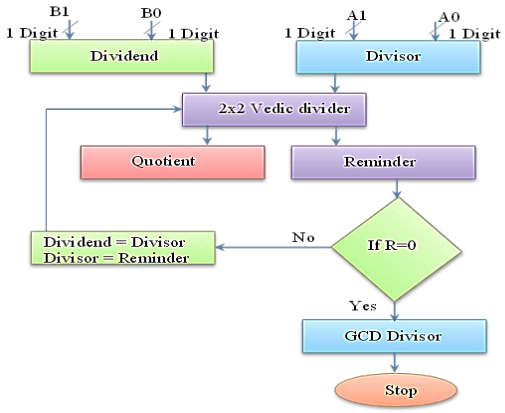

Fig. 11: Block-level implementation of GCD

Results and Discussion

The inputs in Figure 12 are dividend (aa, ab) = 01000010 and divisor (nd, fl) = 00010010, with the outputs being: q (quotient) = 0011 and r (remainder) = 00000110.

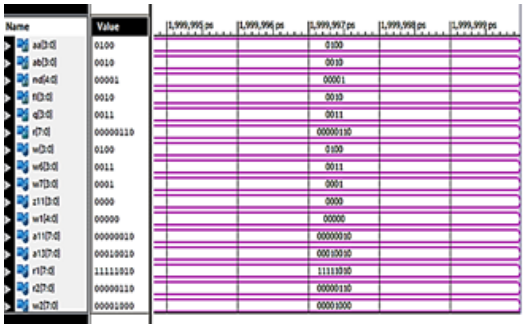

Fig. 12: Simulation waveform of 2-digit Vedic division

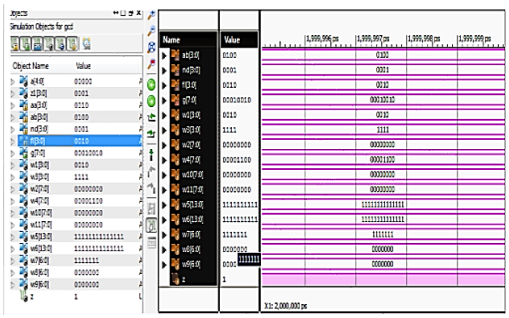

Figure 13 Simulation waveform of 2-digit GCD

In Figure 13, the inputs are 1 (aa, ab) = 00100100 and 2 (ND, Fl) = 00010010, with the corresponding GCD output being: g (GCD) = 00010010. Figure 14 shows the output of the RSA algorithm with the following inputs: p = 0101, q = 0111, and e = 00100011. The public key (e, n) is (00100011, 00110101), and the private key (d) is 1.

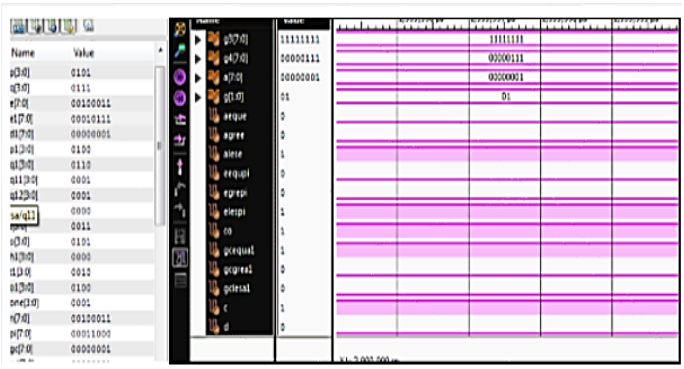

Fig. 14: Simulation waveform of RSA algorithm

Structural Parameters

The proposed architectures and their counterparts were designed using structural Verilog HDL and synthesized using the Cadence Encounter tool with 90nm ASIC PDK Technology and a 1.8V power supply. The ASIC parameter results for the 2-digit Vedic divider are shown in Table 1. From the results in Table 1, it can be explicitly seen that the area and delay are almost the same across designs in,[6], [1], [3], [5], and, [12], with a minimal improvement of around 1.6% compared to the best existing designs. However, power and energy consumption are significantly reduced by approximately 16% and 17%, respectively, demonstrating the efficiency of reversible gates.

The implementation results for a 2-digit GCD are shown in Table 2. It can be noted from Table 2 that power consumption is reduced by around 19%, and area reduction is about 3% compared to the best existing designs, specifically in [6]. The ASIC parameters of the proposed and existing RSA algorithms are shown in Table 3. The area of the proposed RSA algorithm is 6266, and the power consumption is 3,159,842.00 nW. Additionally, it can be noted from Table 2

Table.1 Area Power and Delay results of 2 Digit Vedic divider

Parameter	RDFVDM based Design	[6]	[1]	[3]	[5]	[12]
Area (nm^2)	2774	2823	2890	2918	3164	3121
Power (nW)	227567.348	272579.77	303912.2	311117.2	321312.2	342491.2
Delay (ps)	11199	11387	11660	11706	12087	12656
Energy(mW*ns)	2548.522	3103.857	3543.614	3641.936	3883.674	4328.352
Area Delay Product(ns*nm^2)	31066.026	32145.501	33697.400	34158.108	38243.268	39499.376

Table 2: Area Power and Delay results of 2 Digit GCD

Parameter	RDFVDM based Design	[6]	[1]	[3]	[5]	[12]
Area(nm^2)	2854	2945	3099	3124	4241	4623
Power (nW)	235274.608	291333.77	313298.2	323432.2	333098.2	399844.2
Delay (ps)	11948	11987	12891	12993	15196	16669
Energy(mW*ns)	2807780	3493012	4038750	4196739	5060268	6659266
Area Delay Product (ns*nm^2)	34099	35301	39949	40590	64446	77060

Table 3: Area Power and Delay results of RSA algorithm

Parameter	Proposed	[6]	[3]	[5]	[12]
Area(nm^2)	6266	6890	11313	9905	11905
Power (nW)	3159.842	3826.667	7626	5455.646	7455.646
Delay (ps)	6957	7100	9974	13218.3	15988.08
Energy(mW*ns)	21983020.8	27169336	76061724	72114365.5	119201464.7
Area Delay Product(μs*nm^2)	43592.562	48919	112835.9	130927.262	190338.0924

Table 4: Quantum comparison of proposed and existing methods of Vedic Divider

Quantum Parameters	RDFVDM	[6]	[5]	[12]
QC	432	454	605	660
CI	104	103	97	102
GO	87	89	113	114

that power and energy consumption are reduced by around 19%. Furthermore, an area reduction of about 9% is observed compared to the best design in.[6] Reversible logic offers several advantages in the design of the Vedic divider circuit, including reduced energy dissipation and no information loss.

Quantum Parameters

The quantum parameter comparison between the proposed and existing methods is shown in Table 4. The quantum cost of the proposed method is 432, whereas the quantum costs of the existing methods in [5], [6], and [12] are 605, 454, and 660, respectively. The proposed method shows an improvement of 40% compared to ,[5] 5.09% compared to,[6] and 52.77% compared to.[12] The constant inputs of the proposed method are 104, while those of the existing methods in,[5], [6], and [12] are 97, 103, and 103, respectively. The garbage output of the

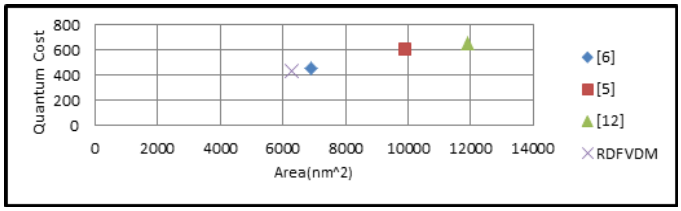

Fig. 15: Plot of QC against area of RDFVDM design against prior algorithms

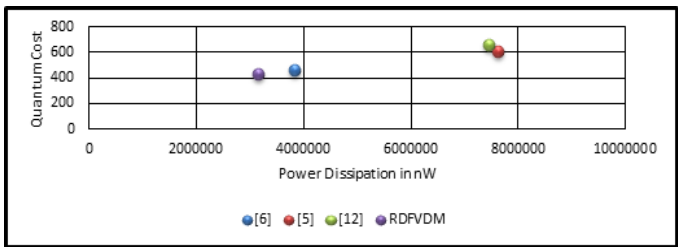

Fig. 16: The plot of QC against the power of RDFVDM design against prior algorithms

proposed method is 87, compared to 113, 89, and 114 for the existing methods in, [5], [6], and, [12] respectively. The proposed method shows an improvement of 21.89% compared to,[5] 2.3% compared to,[6] and 31.03% compared to.[12]. The quantum cost vs. area plot of the proposed and prior designs is shown in Figure 16. As seen in Figure 16, the proposed design exhibits both lower quantum cost and lower area compared to other designs.

Conclusion

Different dividers have been developed, but the RDFVDM (Reversible **Direct Flag** Vedic Divider Multiplier) has lower power consumption compared to a regular divider. By combining decimal logic with ancient Vedic arithmetic, energy consumption is reduced, as is the area used in the RDFVDM design. Current developments in cryptography use a power analysis technique known as differential power analysis to break encryption keys. To counter these types of attacks, reversible logic, which dissipates less energy, is preferred. In terms of area and delay, the proposed RDFVDM implementation outperforms the existing literature. It excels in energy consumption, reducing it by approximately 26% compared to other works. Furthermore, the implementation of the RSA cryptographic algorithm shows that with quantum cost and the number of constant inputs and garbage outputs of 1276, 293, and 311 respectively, it is more efficient in quantum parameters.

References

[1] S Rakshit, S Mondal, A Chakraborty, A Sarkar, D K Kole Synthesis of Reversible Array Divider Circuit, (2019) pp701-707.

[2] Zahra Ariafar and Mohammad Mosleh, 'Effective Designs of Reversible Vedic Multiplier', International Journal of Theoretical Physics (2019) 58:2556–2574.

[3] Ramadevi Vemula and K Manjunatha Chari, 'A review on various divider circuit designs in VLSI', Conference on Signal Processing and Communication Engineering Systems (SPACES), 2018.

[4] LamjedTouil and BouraouiOuni, 'Design of hardware RGB to HMMD converter based on reversible logic', IET Image Process., 2017, Vol. 11 Iss. 8, pp. 646-655.

[5] Hafiz Md, HasanBabu, MdSolaiman Mia, Design of a compact reversible fault tolerant division circuit, Microelectronic J (2016), vol. 51, pp. 15-29.

[6] Sadulla, Shaik. "Next-Generation Semiconductor Devices: Breakthroughs in Materials and Applications." *Progress in Electronics and Communication Engineering* 1.1 (2024): 13-18.

[7] H V Jayashree, SkandaKotethota and V K Agrawal, 'Reversible circuit design for GCD computation in cryptography algorithms', Int. J. Circ. Theor. Appl. (2016).

[8] Siba K P and Arati S, 'A Novel Vedic Divider Architecture with Reduced Delay for VLSI Applications', International Journal of Computer Applications, (2015) Vol. 120, No.17, pp.0975 – 8887.

[9] Jyotinnayeesubudhi and C Karthick, 'Implementation of Vedic divider on RSA cryptosystem', International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015.

[10] Huseyin Bodur and Resul Kara, 'Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application', 3rd International Symposium on Innovative Technologies in Engineering and Science, June 2015.

[11] Jayashree H. V, V K Agarwal, P Venkatasree Charan, and A M Chirag Kariappa, 'Design of Fault Tolerant n bit Reversible Comparator for optimization of Garbage and Ancilla bits', Proceedings of International Conference on Circuits, Communication, Control and Computing, (2014) pp-21-22.

[12] P. B, B. A, J. S, A. K. N, and S. K, "Exact Computing Multiplier Design using 5-to-3 Counters for Image Processing," International Journal of Electrical and Electronics Research, vol. 12, no. 2, pp. 435-442, Apr. 2024, doi: 10.37391/ijeer.120215.

[13] Faraz D and Majid H. 'A novel nanometric fault tolerant reversible divider', International Journal of the Physical Sciences Vol. 6, No.24, (2011), pp. 5671-5681.

[14]H G Rangaraju, U. Venugopal, K N Muralidhara and K B Raja, 'Low Power Reversible Parallel Binary Adder/Subtractor', International Journal of VLSI Design & Communication Systems, 1.3(2010), pp-23-34.

[15] H. Thapliyal and M. B. Srinivas, "Novel Reversible Multiplier Architecture Using Reversible TSG Gate," IEEE International Conference on Computer Systems and Applications, 2006, Dubai, United Arab Emirates, 2006, pp. 100-103.

[16] R. Landauer, Irreversibility and heat generation in the computational process, IBM J. Res. Dev. 5 (1961) 183-191.

[17] Soorya, B., S. Sweetline Shamini, and K. Sangeetha. "VLSI implementation of lossless video compression technique using New cross diamond search algorithm." *International Journal of communication and computer Technologies* 5.1 (2017): 27-31.

[18] R. Mishra, An efficient VLSI architecture for a serial divider, Devices for Integrated Circuit (DevIC), 2017, pp. 482-486.

[19] Ramadevi V, Manjunatha K, Design, and implementation of 64-bit divider using 45 nm CMOS technology, International Journal of Pure and Applied Mathematics, Vol 118 No. 5 2018, 293-301.

[20] D. Tomic, J. Mikulic, G. Schatzberger, J. Fellner and A. Baric, "Programmable low-frequency divider in 180nm CMOS technology," 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2020, pp. 89-92.

[21] Jackson Melchert, Setareh Behroozi, Jingjie Li, and Younghyun Kim. SAADI-EC: A Quality-Configurable Approximate Divider for Energy Efficiency. IEEE Trans.Very Large Scale Integr. Syst. 27, 11 (Nov. 2019), pp.2680–2692.

[22]Saranya, Mrs K., Priya, Ms N., Priyadharshini, Ms M., Vedhanivetha, Ms. D., & Lukman, Mr. B. Urdhva Tiryak Sutra Based Ancient Multiplication in Reversible Logic Circuits. In International Journal of Innovative Technology and Exploring Engineering Vol. 9, Issue 5, (2020). pp. 685–697. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP. https://doi.org/10.35940/ijitee.e2130.039520.

[23] A.Balamanikandan and K. Krishnamoorthi, "Low area ASIC implementation of LUT–CLA–QTL architecture for cryptography applications," Wireless Networks, vol. 26, no. 4, pp. 2681–2693, May 2019, doi: 10.1007/s11276-019-02017-3.