Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

DEVELOPMENT OF HIGH SPEED AND LOW POWER 64-BIT APPROXIMATE MULTIPLIER USING SORTING NETWORKING

Appalabattula Ganesh, PG scholar,
Pakki Sridevi, PJoshna Associate Professor
Department of ECE, MIRACLE educational society group of institutions, Bhogapuram, Vizianagaram.India E-mail: ganeshnag02@gmail.com

Abstract

One of the most substantial research areas in the design of VLSI systems is the design of power-efficient, high-speed and small-area datapath logic systems.This paper presents the architecture of a hybrid high speed and low power 64-bit approximate multiplier using sorting networking. A 64-bit multiplier is designed as a case study to show the efficiency of the proposed architecture. This work is implemented in a 0.22 µm CMOS technology using domino logic for most of the sub-circuits. The paper also demonstrates the efficiency of this architecture for higher number of bits. High compression ratio counters and compressors are necessary to speed up the summation.In various digital signal processing units, the summation of multiple operands in parallel forms create a critical path. Her we developed a novel method of fast saturated binary counters and further optimize the (7,3) counter that can perform better in maximum than other designs in delay, based on the sorting network.The sorting network is a powerful parallel hardware system used for data sorting. Any type of number can be sorted if a sorting network can do so for a batch of data whose members are all 1-bit numbers, according to the well-known (0,1) principle. In this work, we exclusively employ it for 1-bit data sorting. The inputs of the counter are asymmetrically divided into two groups and fed into sorting networks to generate reordered sequences, which can be solely represented by one-hot code sequences. Between the reordered sequence and the one-hot code sequence, three special Boolean equations are established, which can significantly simplify the output Boolean expressions of the counter. Using the above method, Similarly, the (15,4) counter is constructed, and it achieves shorter delay, while it significantly consumes less power and area.

Key words:*Fast adder,Multilevel carry skip adder, sorting network.*

1.Introduction

With the increase in usage of portable devices, need for low power is increased greatly. Designers are always giving more importance to power rather than speed, because there is a reliability problem in high performance system. High performance systems often turn hot, and high temperature tends to exacerbate several silicon failure mechanisms Two important characteristics of CMOS logic are high noise immunity and low static power consumption. Since the one transistor of the complementary pair is always turned off. For high density logic functions CMOS logic is best. Pass transistor logic reduces transistor count by eliminating redundant transistors. By reducing transistors we can reduce area and then power. multiplexers are basic logic elements that play a critical role in design and performance of different operations. The critical path involves the summation of several operands, which is frequently utilized in different digital signal processing (DSP) units.The Wallace Tree structure [1], whose performance is the basic multiplier's bottleneck, adds up all the partial products in a basic multiplier circuit.To generate modular multipliers, public-key cryptosystems like RSA and elliptic curve cryptography (ECC) use a significant number multiplier depending on the Toom-Cook [4] or

Karatsuba algorithm [3].These two methods have been the focus of numerous research studies and hardware implementations.Many of the circuit's internal components, as like [5], employ the summation of several operands.In order to speed up large number multiplication and polynomial multiplication, fully homomorphic encryption (FHE), a post-quantum cryptosystem that offers robust security in cloud computing, urgently needs number theoretic transform (NTT) [6].The central processing unit in some high radix [6] NTT implementations is made up of the sum of several operands.

The Wallace tree formand its modified method, the reduced Wallace tree , are the most well-known multiple operands summation techniques. These techniques have logarithmic time consumption because of the reality that they boost up the summing with the usage of full adders as (3, 2) counters. Carry-save structure isthe other name for this kind of form. Since then, numerous papers have examined how to build a faster structure to speed up the summing. The critical idea is to recall extra bits with the same weight as a manner to assemble a counter or compressor with a larger compression ratio than the (3,2) counter. As an illustration, Figure 1 depicts the critical (7,3) counter form collectively with entire adders. By taking into consideration the supply bits amongst neighboring columns, the compressors reduce n rows into 2 rows. The (4,2), (5,2) , and (7,2) compressors—which condense four, five, or seven rows into two rows, respectively—have been discussed in certain papers.However, since they still operate within the framework of complete adders, which uses "XOR" gates as their basic building blocks, it is highly challenging to usage of Venkatachalam and Ko [13], Satish and Paned [14].

1.2. Multilevel carry skip adder

The idea of a simple carry skip adder can be extended for N-bit adder. We assume that the total adder is divided in (N/M) equal-length bypass stages, each of which contains simplify their logical formulations. N rows are condensed into log2 N rows with the resource of the usage of the counters. The counters (4,3, 5, 3, and 6), as well as (7, 3), and (15, 4) [8] have all been discussed in some papers.They tally how many "1"s are there in the inputs. When a counter is saturated, because of this that each one of the "1"s in the inputs are accurately represented in its compressed results, its compression overall performance meets. All of the designs in use an excessive amount of "XOR" gates and are unsaturated. The focus of this essay is saturated counters. For instance, the (7,3) counter is saturated because of the reality a 3-bit price can accurately represent the digits 0 through 7. The counter (6,3) that Fritz and Fam [9] recommended is built using a symmetric stacking construction. Compared to other designs, it is extremely fast, but unsaturated.The saturated (7,3) counter is then created with the resource of the usage of Fritz and Fam using best a MUX on the critical path. The (6:3) counter recommended in is reduced with the resource of the usage of Satish and Pande [10] to a (5:3) counter, and three (5:3) counters are combined to form a (15:4) counter. But this approach is ineffective. In order to rush up multiplication, approximate multipliers are often employed in several error-tolerant domains, consisting of digital photograph processing and finite impulse response (FIR) filters. To attain an estimate multiplier, Manikantta Reddy et al. [11] and Zervakis et al. [12] use approximate booth encoding and partial product perforation. Approximate (4:2) compressors that can be applied in approximate multipliers have been stated with the resource of the

M bits. The bits are divided in blocks of 4-bits. The diagram of 12-bit adder is shown in Fig. 1.4.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

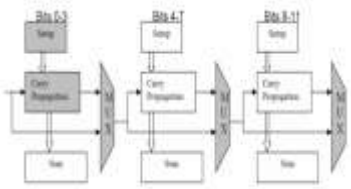
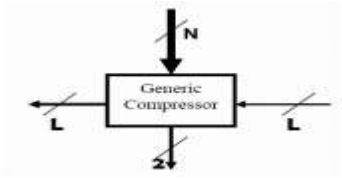


Fig. 1.4: Multilevel Carry skip adder

1.3. Compressors

Compressors are mainlyutilized in multipliers to lessen the operands at the same time asincludingphrases of partial products. A compressor Ci is a combinatorial tool that compresses N enterstrainswith inside thefunctionin to two output strainsi.e., sum and carry. In addition, there are L inputs strains coming to the compressor to exceptionalities. Fig.1.5indicatesaeasy compressor.



.

Fig. 1.5: A generic compressor

1. Existing System:

Because the primaryreason of multi-operand deliver-shop addition or parallel multiplication is to lessen n integers to 2 values, n 2 compressors (or n 2 counters) are usuallyutilized in pc arithmetic. When nicely reproduced, a n 2 compressor is mostly a slice of a circuit that lowers n integers to 2 numbers. The n 2 compressor in slice I of the circuit gets n bits in role I and one or greaterdeliver bits from the locations to the proper, including I - 1 or I - 2.

It generates output bits in locations I and I 1, in addition to one or greaterdeliver bits in better positions, including I 1 or I 2. The 4-2 compressor, which may becarried out with a deliver bit among consecutive slices c1 14 1, is a usually used compression structure. The deliver bit into the toprole is exact as cout, at the same time as the deliver bit from the placement to the proper is exact as cin. The phrases sum and deliver, respectively, also are used to consultthe 2 output bits in locations I and I 1. The 4-2 compressor's outputs are given with inside the following equations, and its reality table is shown in Table 1.

$$Sum = x1 \oplus x2 \oplus x3 \oplus x4 \oplus Cin$$

$$Cout = (x1 \oplus x2)x3 + \overline{(x1 \oplus x2)}x1$$

$$Carry = (x1 \oplus x2 \oplus x3 \oplus x4)Cin + \overline{(x1 \oplus x2 \oplus x3 \oplus x4)}x4.$$

Two full-adder (FA) cells are used to create a 4-2 compressor in the most usual way [8]. The literature has suggested a variety of 4-2 compressor designs. The XOR-XNOR gates, sometimes known as "XOR-XNOR gates," are used in the optimum construction of an exact 4-2 compressor [8]. These gates concurrently produce the XOR and XNOR output signals. Three XORXNOR (often known as XOR) gates, one XOR, and two 2-1 MUXes make up the [8] design. This design's critical path is delayed by 3D, where D is the unitary delay through any design gate.

In 24 of the 32 states, the deliver output in anspecific compressor has the identicalfeebecause theentercin. Thus, this issuehas to be taken into consideration in an expectedlayout. By changing the fee of the alternative8 outputs in Design 1, the deliver is decreased to the integer cin.

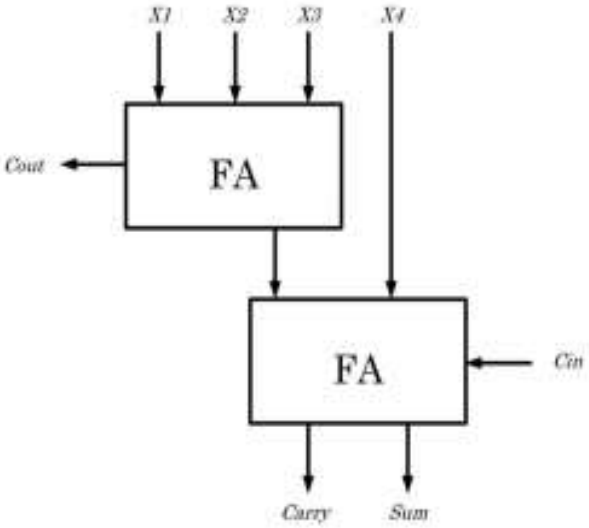


Fig.2.1. Implementation of 4-2 compressors

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

An incorrect price of this signal will result in an output difference price of for the motive that Carry output has the higher weight of a binary bit. For instance, the right output is "010," which equals 2, if the input pattern is "01001" (row 10 of Table 2). The approximation compressor will create the "000" pattern at the output via reducing the supply output to cin (i.e., a price of 0). This awesome disparity may not be acceptable, but it can be made up for or faded via making the cout and sum signals simpler. In particular, the disparity some of the approximate and true outputs further to the complexity are reduced at the same time as sum is simplified to a price of 0 (2d 1/2 of of Table 2). Additionally, producing the approximate sum and the design's normal get rid of is probably sped up withinside the presence of some sum signal errors.

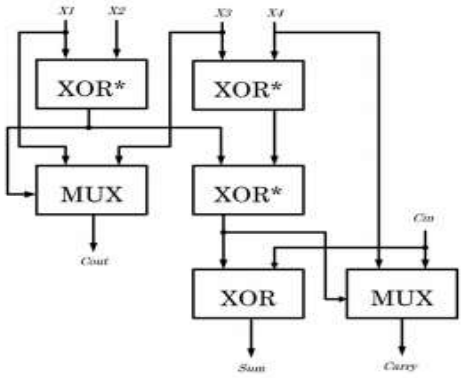


Fig.2.2. Optimized 4-2 compressor

The very last step shouldbring aboutgreater simplification with inside the proposed layout and a discountwith inside theblunders distance suppliedwith the aid of using the approximate deliver and sum. Although the proposed approximate compressor's blunderscharge is expandedwith the aid of using the aforementioned deliver and sum simplifications, its layout complexity and consequentlyenergyintake are drastically reduced. This is made cleanwith the aid of using contrasting (2)-(4) and (five)-. (7). The gate stageshape of the primaryrecommendedlayout demonstrates that the compressor's vitalcourseneverthelessh has a 3-Dput off, making it same to the compressor itself.

2.Proposed System

The vitaldirectionconsists of the summation of numerous operands, that'soften utilised in distinctivevirtualsign processing (DSP) units. The Wallace Tree structure, whose overall performance is the fundamental multiplier's bottleneck, provides up all of the partial merchandise in a fundamental multiplier circuit. A massivevariety multiplier primarily based totallyat the Toom-Cook [4] or Karatsuba algorithm is utilized in public-key cryptosystems like RSA and ECC to create modular multipliers. These techniqueshad been the situation of numerousresearch and hardware implementations. Many additives of the circuit withinside the papers, use the summation of many operands. In order to hurry up massivevariety multiplication and polynomial multiplication, FHE, a post-quantum cryptosystem that givesstrongsafety in cloud computing, urgently desires NTT. The primary processing unit in a fewexcessive radix [6] NTT implementations is made of the sum of numerous operands

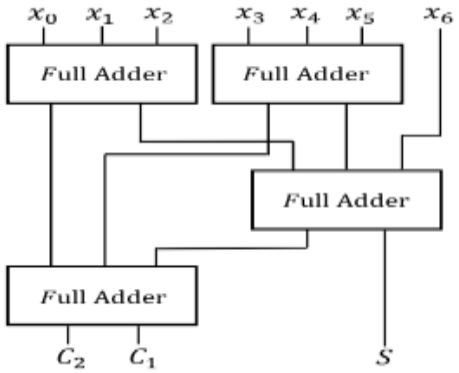


Fig. 3.1. (7,3) counter combined by full adders (7,3) counter mixed through complete adders. The Wallace tree shape and its changed method, the decreased Wallace tree [2], are the maximumfamousmore than oneoperand summation strategies. These strategies have logarithmic time intakedue to the fact they accelerate the summing throughthe usage ofcomplete adders as (3,2) counters. Carry-keepsystems are any othercall for this type ofshape. The essentialconcept is to don't forgetextra bits with the equal weight so one canconstruct a counter or compressor with a

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

bigger compression ratio than the (3,2) counter. For instance, the entireshape of a basic (7,3) counter. By deliberating the deliver bits among neighbouring columns, the compressors lessen n rows into 2 rows. However, on the grounds that they neverthelessperformwithinside the framework of entire adders, which uses "XOR" gates as their essentialconstructing blocks, it's milesespeciallytough to lessen their logical formulations. N rows are condensed into log2 N rows through the counters. The counters (4,3, 5, 3, and 6), as properly as (7, 3), (11), and (15, 4) [12] have all been included in a few studies. They tally how many "1"s there are withinside the inputs. If a counter is saturated, which meansthat every one of the "1"s withinside the inputs are as it should be represented withinside the compressed results, the counter's compression performance reaches the limit. Compared to different designs, it's milesextraordinarily quick, but unsaturated. The saturated (7,3) counter is then created through Fritz and Fam [11] the usage ofonly a MUX at theimportant path.

3.Sorting Network

The sorting network is a powerful parallel hardware system used for data sorting. Any type of number can be sorted if a sorting network can do so for a batch of data whose members are all 1-bit numbers, according to the well-known 0,1 principle. In this work, we exclusively employ it for 1-bit data sorting.

Sorting Network Working Principle

Often employ networks with three and four lanes [14]. Each vertical line represents a sorter, with only 1-bit numbers, two data inputs, and two data outputs. The larger input is always sorted higher than the smaller input. The input sequences for both 4 SN and 3 SN are rearranged with the larger number at the top and the smaller number at the bottom following three layers of sorting.

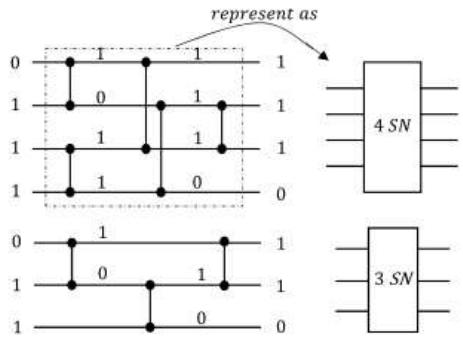


Fig.3.2. Three- and four-way sorting networks

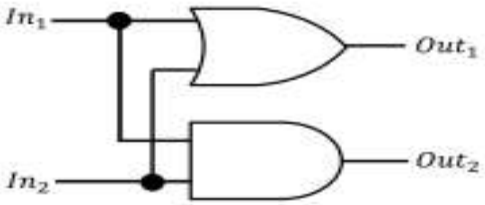


Fig.3.3. Two-input binary sorter

4. SIMULATION RESULTS

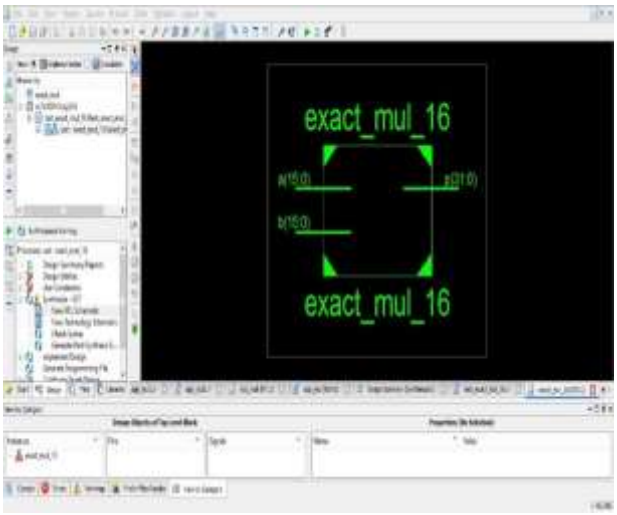


Fig.4.1.Block diagram of the 16-bit exact multiplier

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

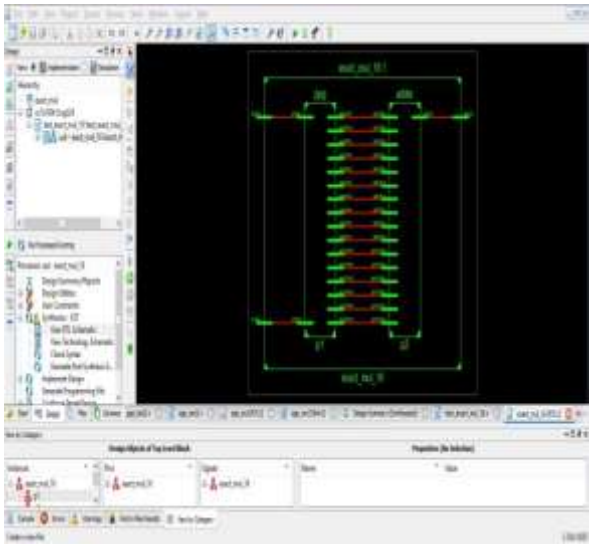


Fig.4.2.RTL Schematic of the 16-bit exact multiplier

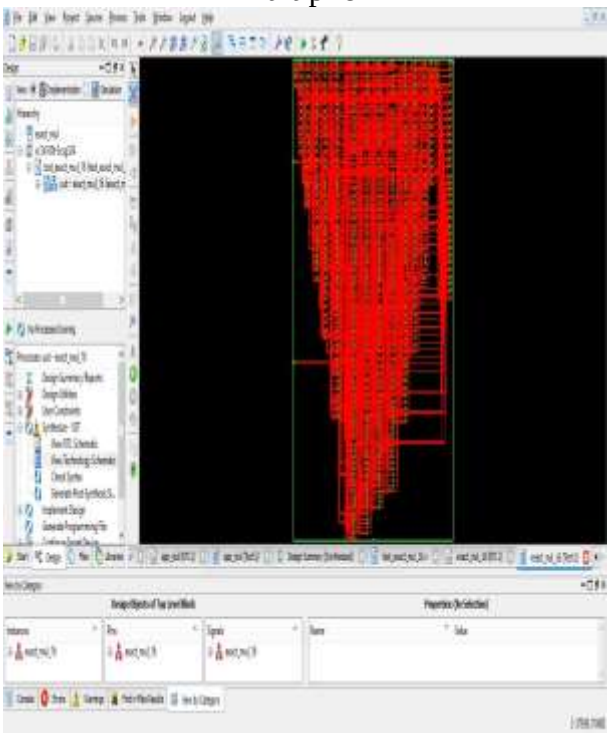


Fig.4.3.Technology Schematic of the 16-bit exact multiplier

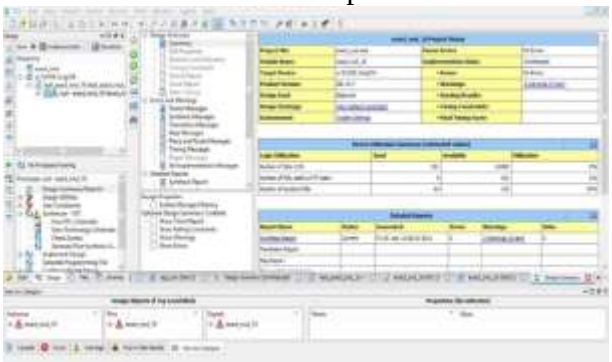


Fig.4.4: Summary Report of the 16-bit exact multiplier

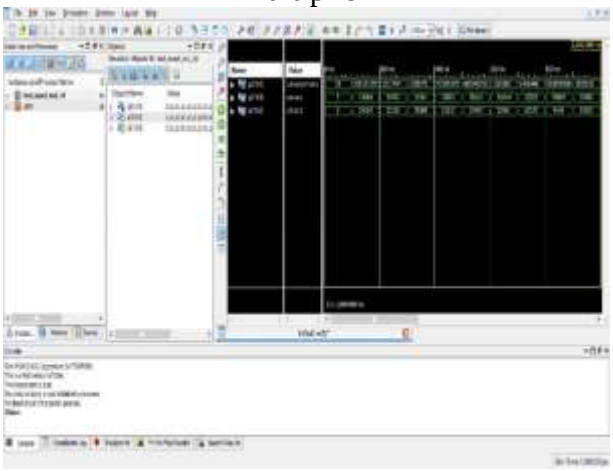


Fig.4.5.Simulation Result of the 16-bit exact multiplier

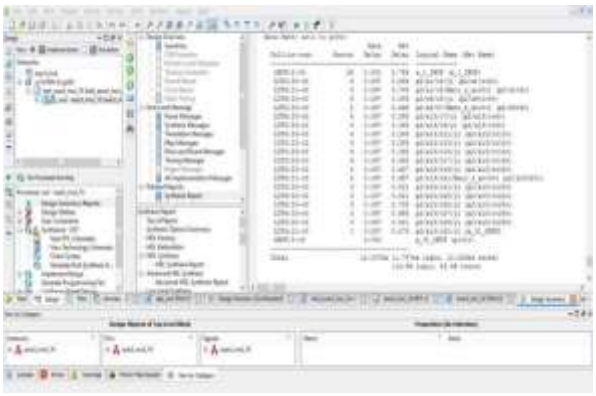


Fig.4.6.Delay Report of the 16-bit exact multiplier

Fig.4.7.Block diagram of the 16-bit approximate multiplier

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

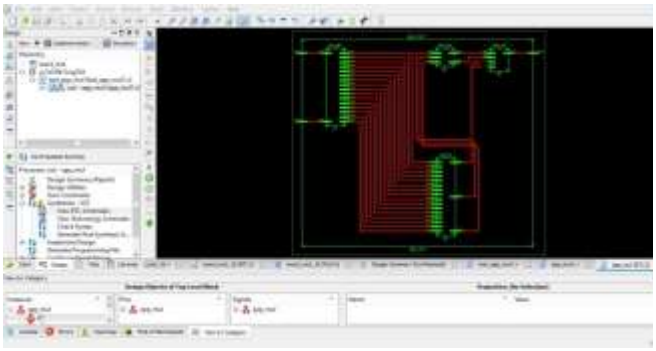


Fig.4.8.RTL Schematic of the 16-bit approximate multiplier

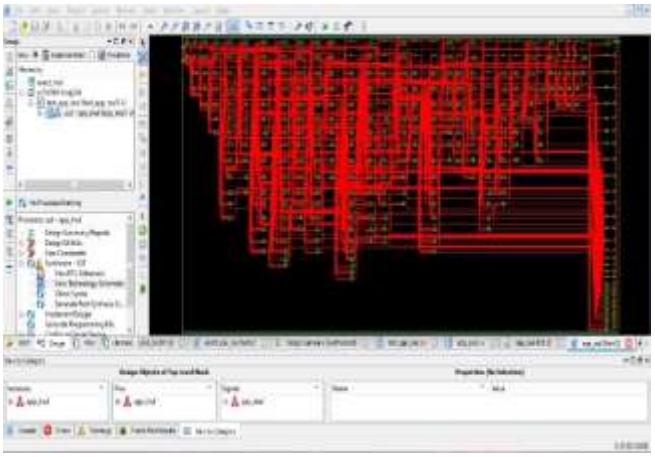


Fig.4.9.Technology Schematic of the 16-bit approximate multiplier

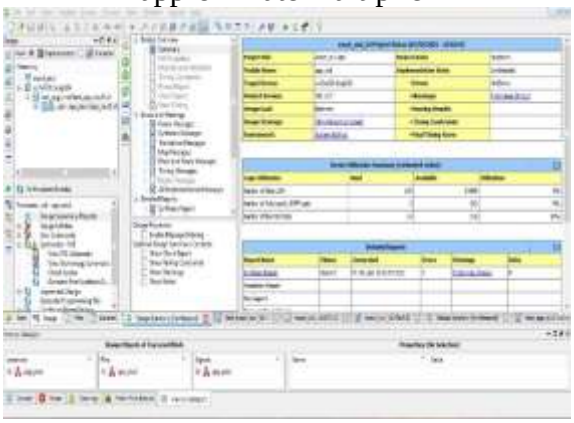


Fig.4.10.Summary Report of the 16-bit approximate multiplier

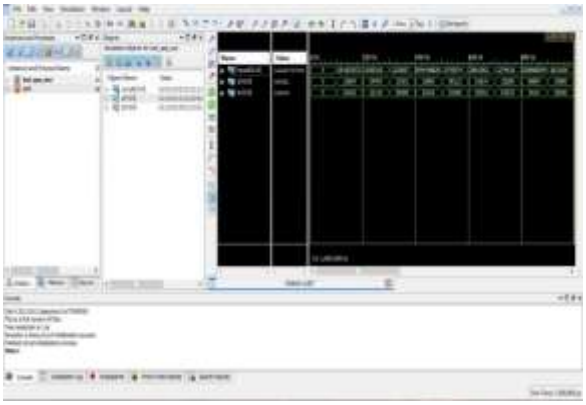


Fig.4.11.Simulation Result of the 16-bit approximate multiplier

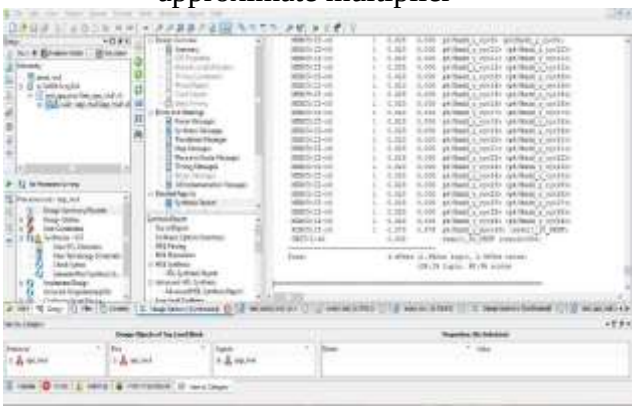
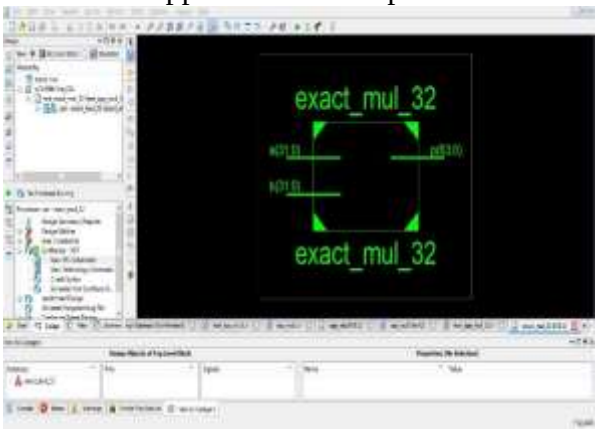
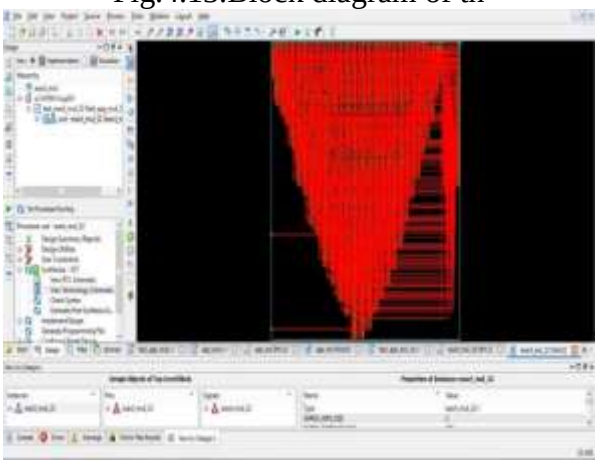


Fig.4.12.Delay Report of the 16-bit approximate multiplier



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

Fig.4.13.Block diagram of th



e 32-bit exact multiplier

Fig.4.14.Technology Schematic of the 32-bit exact multiplier

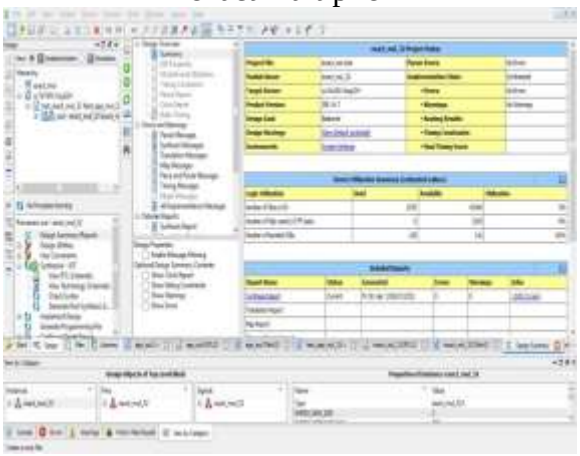


Fig.4.15.Summary Report of the 32-bit exact multiplier

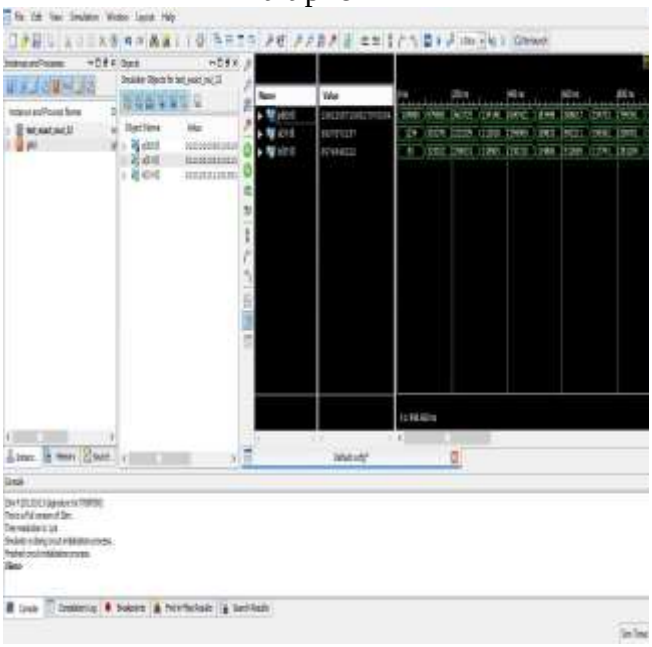


Fig.4.16.Simulation Result of the 32-bit exact multiplier

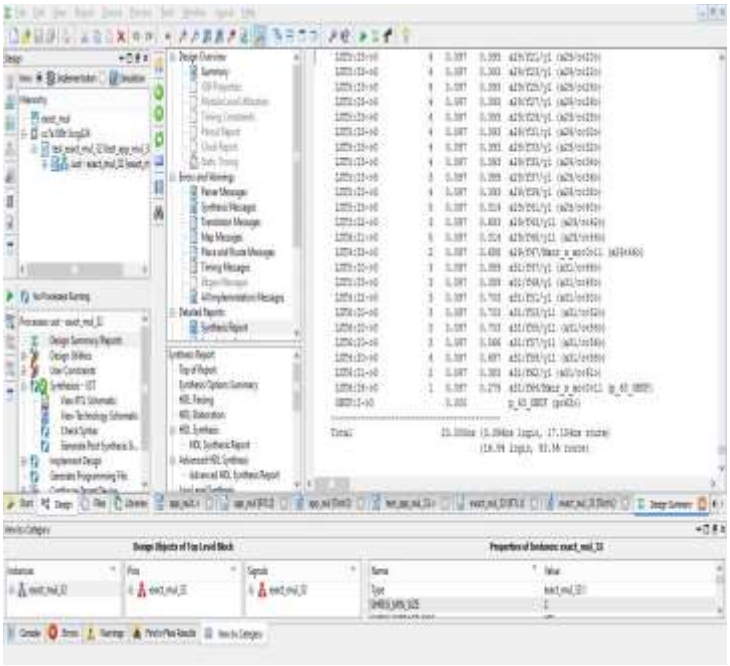


Fig .4.17.Delay Report of the 32-bit exact multiplier

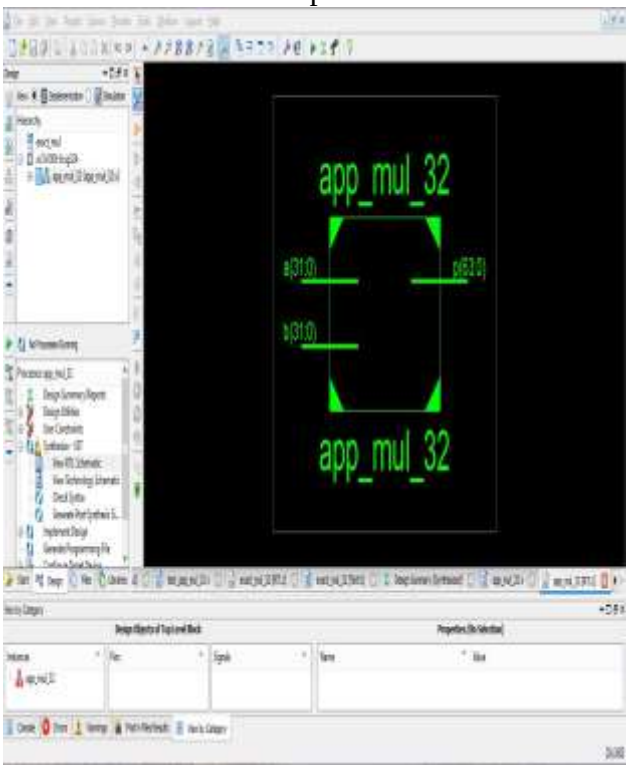


Fig.4.18.Block diagram of the 32-bit approximate multiplier

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

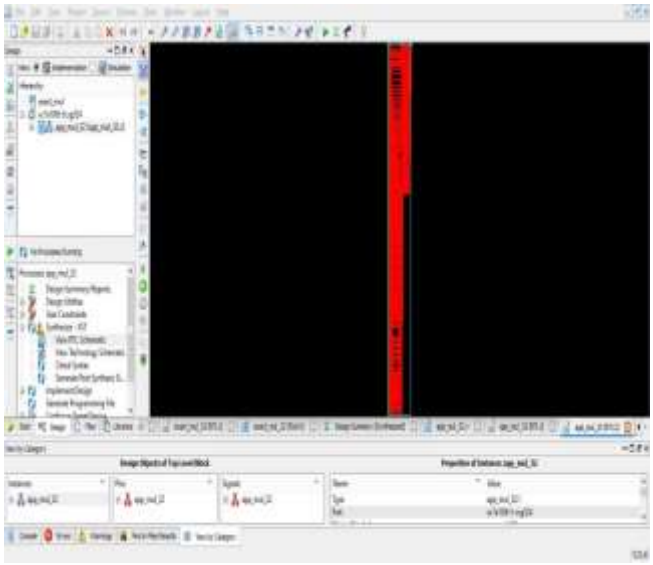


Fig.4.19.RTL Schematic of the 32-bit approximate multiplier

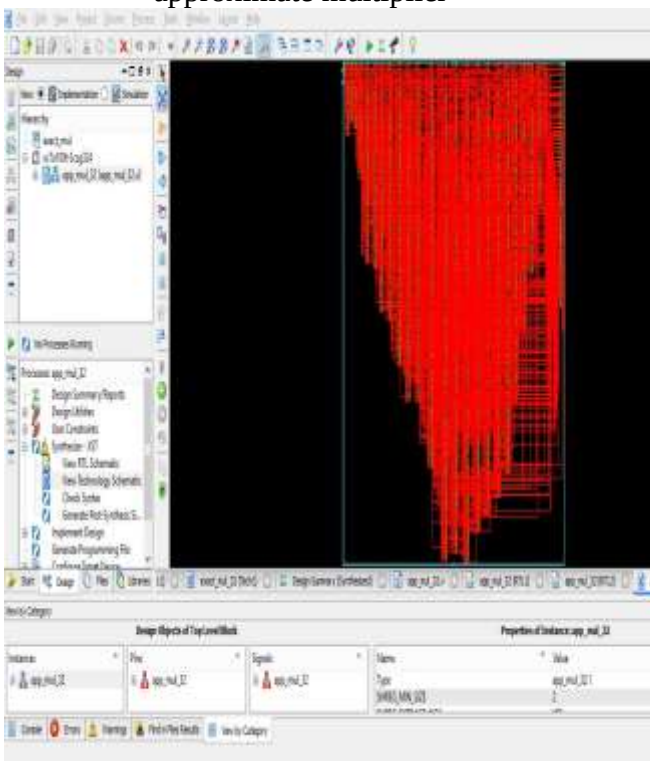


Fig.4.20 .Technology Schematic of the 32-bit approximate multiplier

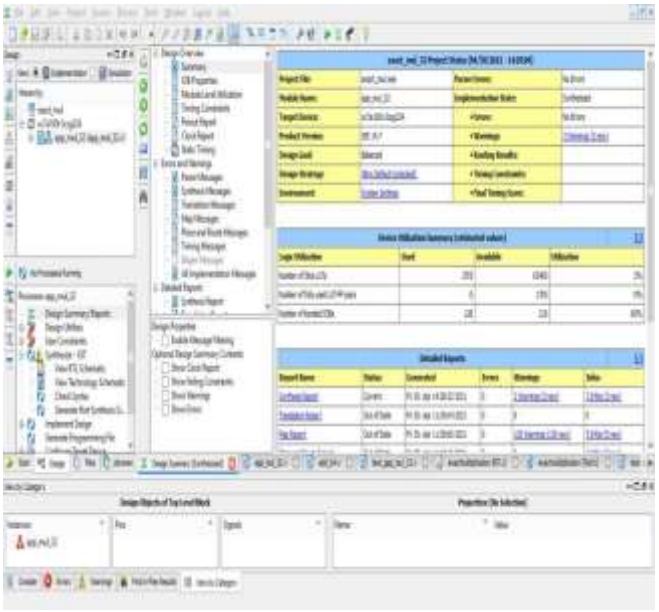


Fig.4.21.Summary Report of the 32-bit approximate multiplier

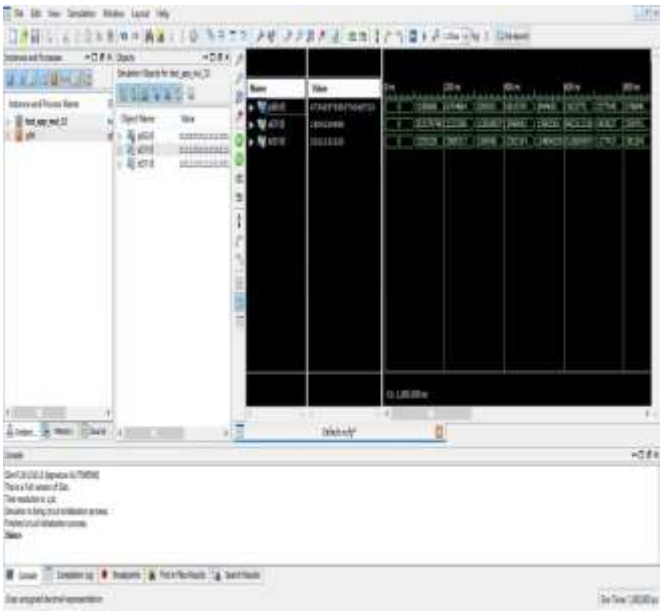


Fig.4.22.Simulation Result of the 32-bit approximate multiplier

5.CONCLUSION

On the premise of the newly offered sorting network-primarily based totally counter layout method, we create the counters (7,3), (15,4), and (31,5). The (7,3) counter consumes much lessenergy and takes up much less room than different designs. The (15,4) counter is extraflexible than in advance designs as it achieves much lessputoffwhilepace is vital and

playshigher in ADP and PDP whilelocation or strength are vital. The (31,5) counter has a shorter latency than different designs. When includedright into asixteen-bit or 32-bit multiplier, they carry outhigher in most ADP and PDP than whileincluded into different counter designs. Exact/approximate (4:2) compressors also arerecommendedprimarily based totally on a sorting network. They carry outhigher in PDP and ADP while embedded in an approximate multiplier with eight bits, sixteen bits, or 32 bits.

REFERENCES

1. Wallace, C. S. (1964). A suggestion for a fast multiplier. IEEE Transactions on electronic Computers, (1), 14-17.
2. Waters, R. S., &Swartzlander, E. E. (2010). A reduced complexity wallace multiplier reduction. IEEE transactions on Computers, 59(8), 1134-1137.
3. Montgomery, P. L. (2005). Five, six, and seven-term Karatsuba-like formulae. IEEE Transactions on Computers, 54(3), 362-369.
4. Ding, J., Li, S., & Gu, Z. (2018). High-speed ECC processor over NIST prime fields applied with Toom–Cook multiplication. IEEE Transactions on Circuits and Systems I: Regular Papers, 66(3), 1003-1016.
5. Liu, R., & Li, S. (2019). A design and implementation of Montgomery modular multiplier. In 2019 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-4). IEEE.
6. Wang, W., Huang, X., Emmart, N., & Weems, C. (2013). VLSI design of a large-number multiplier for fully homomorphic encryption. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 22(9), 1879-1887.
7. Asif, S., & Kong, Y. (2015). Analysis of different architectures of counter based Wallace multipliers. In 2015 Tenth International Conference on Computer Engineering & Systems (ICCES) (pp. 139-144). IEEE.
8. Najafi, A., Mazloom-nezhad, B., & Najafi, A. (2013). Low-power and high-speed 4-2 compressor. In 2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 66-69). IEEE.
9. Najafi, A., Timarchi, S., & Najafi, A. (2014). High-speed energy-efficient 5: 2 compressor. In 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 80-84). IEEE.
10. Asif, S., & Kong, Y. (2015). Design of an algorithmic Wallace multiplier using high speed counters. In 2015 Tenth international conference on computer engineering & systems (ICCES) (pp. 133-138). IEEE.
11. Fritz, C., & Fam, A. T. (2017). Fast binary counters based on symmetric stacking. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 25(10), 2971-2975.
12. Jiang, Q., & Li, S. (2017). A design of manually optimized (15, 4) parallel counter. In 2017 International Conference on Electron Devices and Solid-State Circuits (EDSSC) (pp. 1-2). IEEE.
13. Najafi, M. H., Lilja, D. J., Riedel, M. D., &Bazargan, K. (2018). Low-cost sorting network circuits using unary processing. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 26(8), 1471-1480.
14. Knuth, D. E. (1973). Sorting and Searching: The Art of Computer Progranning. addison-Wesley.
15. Mehta, M., Parmar, V., & Swartzlander Jr, E. E. (1991). High-speed multiplier design using multi-input counter and compressor circuits. In IEEE Symposium on Computer Arithmetic (pp. 43-50).
16. Kim, J., Caire, G., & Molisch, A. F. (2015). Quality-aware streaming and scheduling for device-to-device video delivery. IEEE/ACM Transactions on Networking, 24(4), 2319-2331.