IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Power and Area Efficient High Speed Squaring Circuit using Vedic Mathematical Techniques

Gumpina Vakula Rani[1], Dr. Bhaskar Reddy[2]

Research Scholar, Rayalaseema University, Kurnool, Andhra Pradesh[1]

Professor and Head, S K University, Ananthapur[2]

Abstract: Vedic Mathematics is an ancient practice which has a unique procedures based on the sixteen Sutras dealing with the different branches of mathematics viz., arithmetic, calculus, algebra, geometry etc. The interest for high speed processing has been growing as an effect of wide computer processing applications. Very efficient math operations are important to accomplish the desired performance in several real-time systems such as Cryptography and Image Processing. Squaring is one of the key arithmetic operations in many applications like finding the transforms or the inverse transforms in signal processing and the development of fast squaring circuit has been a subject of interest over decades. The key requirements for many applications are to reduce the time delay and power consumption for many applications. In this paper, we have proposed power and area efficient fast squaring circuit using Vedic Multiplier and the proposed dsign is compared with the Vedic Multiplier and squaring circuits. The functionality of this circuit is verified and performance evaluation is done using Xilinx ISE design Suite 14.4 on target device xc5vlx20t-2ff363.

Keywords: Vedic Mathematics, Vedic multiplier, Squaring Circuit, Carry Save Adder, Shifter, Combinational Path Delay, Slices, Digital signal processors.

1. INTRODUCTION

Digital signal processors (DSPs) are very important in different disciplines. Fast multiplication and squaring are extremely significant operations in convolution, Fourier transformations and so on. Integer multiplication and squaring play important roles in microprocessors, DSP and other modern electronic machines. Multiplication and Squaring are the fundamental mathematical operations and require considerably more hardware circuitry and execution time than addition and subtraction. A CPU spends a lot of its time for performing numerical computations including multiplications and thus fast arithmetic-coprocessors are required for improving the speed of the PC.

The demand for high speed processing has been increasing as a result of expanding computer and signal processing applications. Highly efficient arithmetic operations are necessary to achieve the desired performance in many real-time systems, cryptography and digital image processing applications. Squaring is one of the key arithmetic operations in many applications like finding the transforms or the inverse transforms in signal processing and the development of fast squaring circuit has been a subject of interest over decades. Reducing the time delay and power consumption are very the essential requirements for many applications.

Squaring is a fairly large block and the amount of circuitry involved is directly proportional to the square of its resolution i.e. a square of size n bits has n^2 bits as an output. For squaring algorithms performed in DSP applications latency and throughput are the two major concerns from the delay perspective. Latency is the real delay of computing a function and measures how long the inputs to a device are stable. The squaring circuit has not only a high delay but also a major source of power dissipation. One of the aim is to minimize the power consumption, it is of incredible interest to reduce the delay by utilizing the different optimization techniques. In this paper, an efficient and high speed squaring circuit using Recursive Vedic Multiplier based on **"**Urdhva Tiryagbhayam**"** is proposed which is faster and elegant when compared to the conventional methods .

This paper is structured as follows. In section 2, related work and the brief introduction to Vedic sutras is presented. Section 3, describes the Methodology, which describes 2x2 Vedic multiplier, basic 2bit squaring unit and 4bit squaring Logic . In section 4, the proposed high speed squaring architecture is presented. In section 5, design analysis and simulation results are presented. Finally, the conclusions are presented in section 6.

2. RELATED WORK

The word "Vedic" is derived from the word "veda" which means the store-house of all knowledge. Vedic Mathematics / Ancient Indian Mathematics comprises several simple and unique techniques through which problems associated with different branches of mathematics could be solved very efficiently. This consists of algorithms that can bring down large arithmetic operations to simple mind calculations. Because of that fact the Vedic mathematics approach is totally

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

different and considered very close to the way a human mind works. This system was actually rediscovered from our ancient scriptures during 1911 and 1918 by Sri H. H. Bharati Krishna Tirtha swamiji [1] . "Urdhva Tiryagbhayam" is one of the powerful sutras among 16 sutras of Vedic mathematics, which means 'Vertically and Cross wise'. The idea of using Vedic mathematics for design of multipliers has been discussed in [6-9]. 'Urdhva Tiryagbhyam' Sutra is shown to be an efficient multiplication algorithm as compared to the conventional counterparts. Authors of [11] have also shown the effectiveness of this Sutra to reduce N×N multiplier structure into an efficient 4×4 multiplier structure. However, they have mentioned that 4×4 multiplier section can be implemented using any efficient multiplication algorithm. Recently, a squaring circuit has been reported in the literature [13]. This may be noted that designing Vedic multipliers using array multiplier structures as discussed in above references provide us less delay and, thus, they are treated as high speed multipliers as compared to Booth's algorithm using recorded multipliers and Wallace trees. Later, a high speed squaring circuit for binary numbers is proposed [10] using carry save adders (CSA). CSA is used to perform the doubling. In this proposed architecture, CSA is replaced with Left shifter to perform the doubling. The circuitry required for CSA is complex when compared with the Shifter. The proposed Squaring circuit uses one Vedic multiplier instead of four as in recursive Vedic multiplier for evaluating square of a n-bit binary number.

3. METHODOLOGY

In this section, a complete explanation about the important modules are presented which comprises the circuits of i) 2X2 Vedic Multiplication ii) 2-Bit Squaring and iii) 4-Bit Squaring.

A. 2X2 Vedic Multiplication

The advantage of Vedic Mathematics is that the complex calculations can be solved with simple techniques. The Vedic multiplier using Urdhva Tiryagbhyam sutra of size NXN will produce the 2N-1 partial products of different sizes which when combined forms ($\log_2 N + 1$) partial products. The cross products are obtained by vertical and crosswise operations using the Sutra. Hence the delay is equal to adder delay. Critical path would consist of adders adding the maximum number of bits in cross product. The 2X2 Vedic multiplier is implemented using a two input AND gates and two half-adder as shown in Figure 1. The implemented equations are written as

P0 (1-bit) = A0.B0 .... (1)
P1 (1-bit) = A1.B0 + A0.B1+ C1(P1(1)) ....(2)
P3P2 (2-bits) = A1.B1 + C2(P2(1)) ....(3)
Product = P3P2P1P0 ....(4)

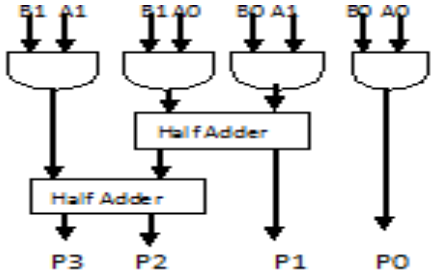


Figure1: 2X2 Vedic Multiplier

B 2-Bit Squaring Operation

The basic squaring circuit can be realized from 2X2 Vedic multiplier as shown in figure 2 [10]. The squaring circuit can be implemented using one half adder and one AND gate instead of two half-adders as shown in Figure 2.

P0 (1-bit) = A0 .....(5)
P1 (1-bit) ='0' .....(6)
P3P2 (2-bits) = A1A0 + A1 .....(7)
Product =P3 P2P1P0 .....(8)

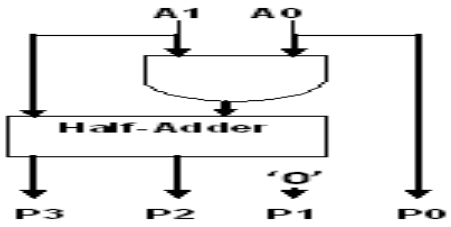


Figure2 : 2 Bit Squaring Circuit

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

C. 4-Bit Squaring Circuit

A 4-bit squaring circuit[10] is implemented using two 2-bit squaring circuits (as shown in Fig.2) and one 2X2 Vedic Multiplier (as displayed in Fig.1) instead of four 2X2 Vedic Multiplier modules used Recursive Vedic Multiplier. The general block diagram of the 4-bit squaring circuit is shown in Figure:3 .

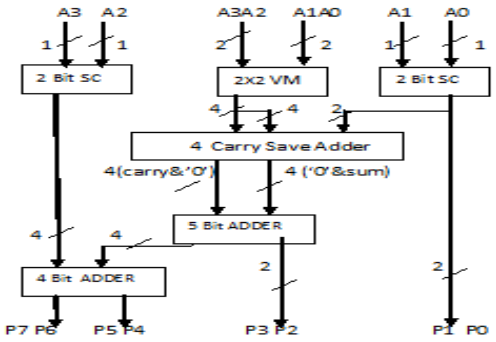


Figure 3: 4 Bit Squaring Circuit

4. PROPOSED HIGH SPEED SQUARING ARCHITECTURE

The proposed high speed 4 bit Squaring circuit is implemented using one 2x2 Vedic multiplier ,two 2 bit squaring circuits, one left shifter instead of Carry Saver Adder to perform the doubling . The circuitry required for CSA is complex when compared with the Shifter. The beauty of Vedic multiplier is that the partial product generation and additions are done concurrently. This in turn reduces the combinational path delay.

1. Algorithm for Proposed for 4 bit Squaring Architecture

Input: 4 bit Binary Number ($A_3A_2A_1A_0$)
Output: Square of 4 bit Binary Number (P7P6P5P4P3P2P1P0).
Step 1: Divide the number ($A_3A_2A_1A_0$) into parts(A_3A_2) & (A_1A_0).
Step 2: Perform the following operations.

a. Square (A_1A_0) using 2 bit Squaring Logic(equations 5 to 8) output is T1(4 bit)
i. P0=T1(0) & P1=T1(1)
b. Multiply (A_3A_2) with (A_1A_0) using Vedic Multiplier (equations 1 to 4)output is T2 (4 bit).
c. Square (A_3A_2) using 2 bit Squaring Logic (equations 5 to 8) output is T3(4 bit).

Step 3: Apply Left Shift operation to T2 output is T4 (5 bit).
Step 4: Add T4 with T1(3..2) output is T5 (6 bit).
P2 = T5(0) & P3 = T5(1)
Step 5: Add T3 with T5 and the output is P7P6P5P4 (4 bit).
Step 6: Print the product P7P6P5P4P3P2P1P0.

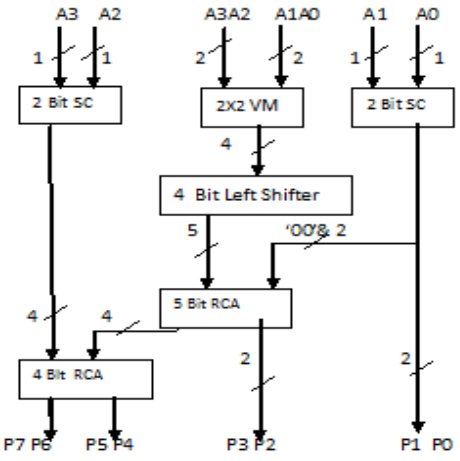


Figure 4: Proposed 4 Bit Squaring Circuit

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Similarly, 8-bit , 16-bit and 32bit squaring circuits are designed and implemented using recursive Vedic multiplier module and squaring circuit modules of 4-bit , 8-bit and 16 bit respectively. The n-bit squaring circuit can be implemented by taking one (n/2)-bit recursive Vedic multiplier module and two (n/2)-bit squaring circuits.
The module level comparison between Vedic multiplier, squaring circuit and proposed squaring circuit is presented in table:1.

Table :1- Module Level Comparison

Bit size	Module Description	VM	SC	PSC
2 bit	AND Gate	4	2	2
	Half Adder	2	1	1
4 bit	2X2 VM	4	1	1
	2 bit SC	-	2	2
	4/5 bit Adders	2	2	2
	4 bit CSA	1	1	-
	4 bit Shifter	-	-	1

5. DESIGN ANALYSIS AND SIMULATION RESULTS

In this work,. 4-bit, 8-bit 16-bit and 32 bit squaring circuits are implemented using Xilinx ISE design Suite 14.4 and ModelSim SE 6.5. in VHDL. The synthesis is done using Xilinx vertx5 FPGA board of device family xc5vlx20t-2ff363. VHDL Coding was done for the functionalities using the structural modelling and the design summary and timing reports are obtained. The results are compared and presented in Table: 2 . Figure : 5 shows the comparison graph of 4 Bit Squaring in terms of i) 4 Input LUT's ii) Number of Slices iii)Number of XOR gates iv) Logic Levels and v) Combinational Path Delay. The comparison graph of 8 Bit , 16 Bit and 32 Bit Squaring are shown in Figures 6, 7 and 8. From the above results, it is clear that the Proposed Squaring Circuit (PSC) is faster than the Recursive Vedic Multiplier (VM) and Squaring Circuit (SC). The proposed architecture has advantages like i) Increase in the speed ii) Decrease in the delay iii) Decrease in the area iv) Decrease in power consumption.

Table:2- Design Summary

	4 Input LUT's			Slices			XOR gates			Logic Levels			Combinational Path Delay		
	VM	**SC**	**PSC**	**VM**	**SC**	**PSC**	**VM**	**SC**	**PSC**	**VM**	**SC**	**PSC**	**VM**	**SC**	**PSC**
4bit	33	6	6	20	5	5	25	18	14	7	3	3	7.154	3.89	3.89
8Bit	134	55	54	53	23	23	125	86	70	15	11	11	12.879	9.878	9.878
16Bit	606	259	219	269	126	106	549	346	298	25	22	18	20.070	18.151	16.280
32Bit	2562	1256	1256	1183	473	454	2293	1338	1210	43	36	36	33.084	29.865	28.192

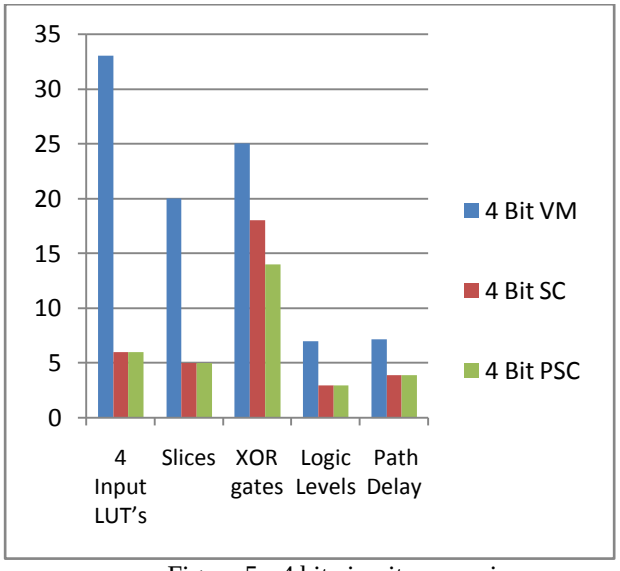


Figure:5 - 4 bit circuit comparison

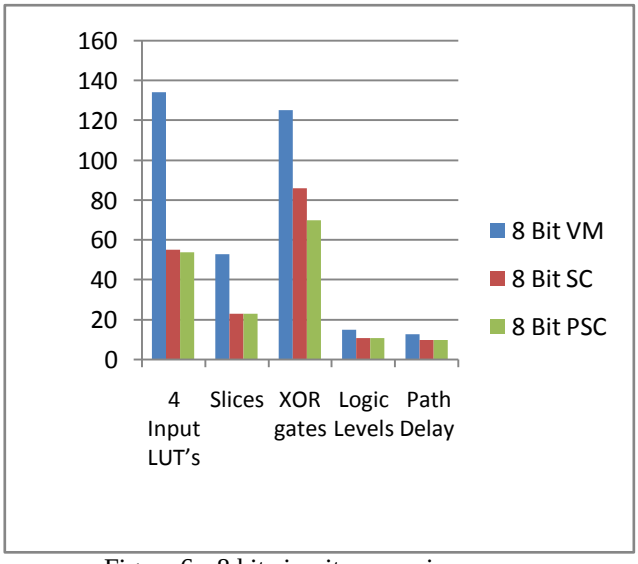


Figure:6 - 8 bit circuit comparison

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

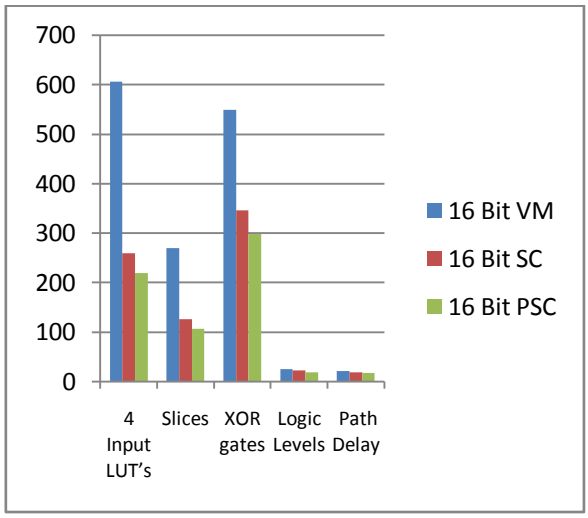


Figure:7 –16 bit circuit comparison

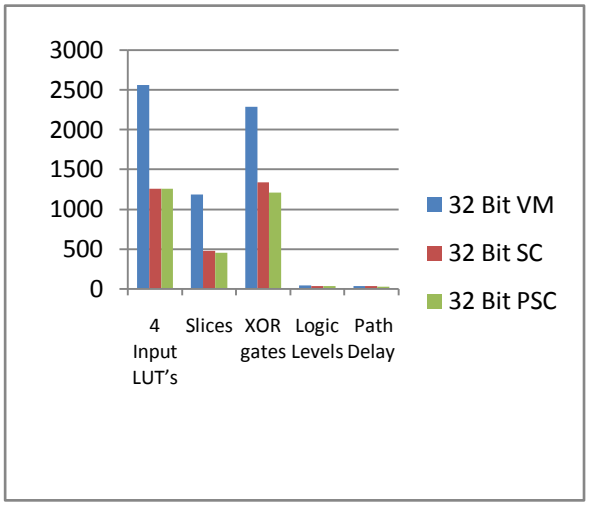


Figure:8 – 32 bit circuit comparison

The following observations are made after comparing the results of the Proposed Squaring Circuit(PSC) with Recursive Vedic Multiplier (VM) of 32-bit number.

- Number of 4 Input LUT's used is reduced by 50.97%
- Number of Slices is reduced by 60.01%
- The Combinational path Delay or critical path delay is reduced by 14.696%
- The number of XOR gates used is reduced by 47.23%.
- Number of logic levels is decreased by 16.27%.

Figures 9 and 10 shows the RTL schematic and Technology Schematic view of 4 Bit Proposed Squaring Circuit(PSC). The Functional Verification of 4 Bit , 8 Bit , 16 Bit and 32 Bit of the proposed Squaring Circuit is presented in the Figure 11.

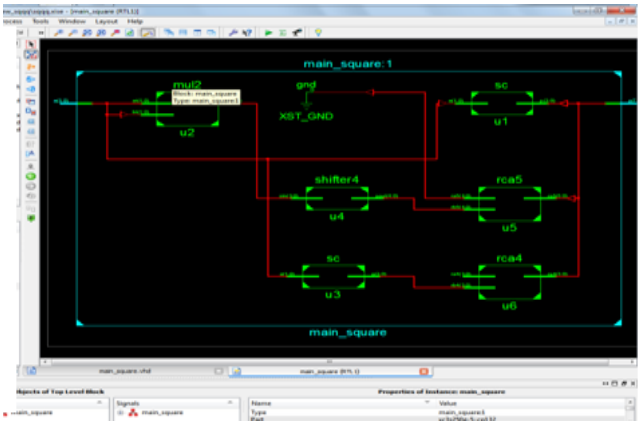


Figure 9: :RTL Schematic-1 of PSC

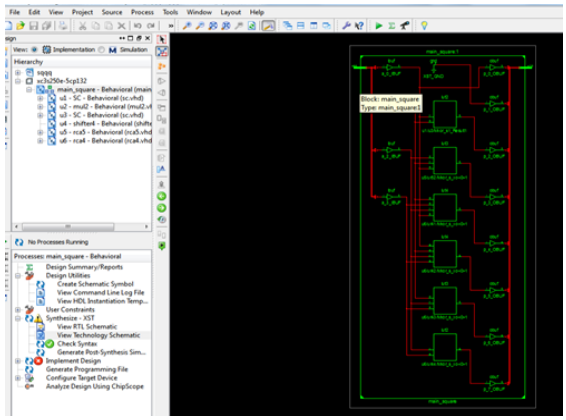
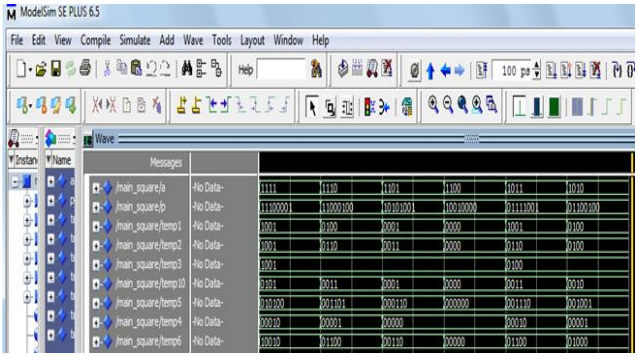
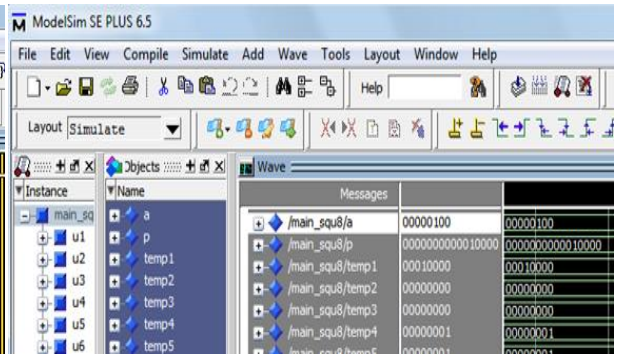


Figure 10: Technology Schematic of PSC



a) 4 Bit

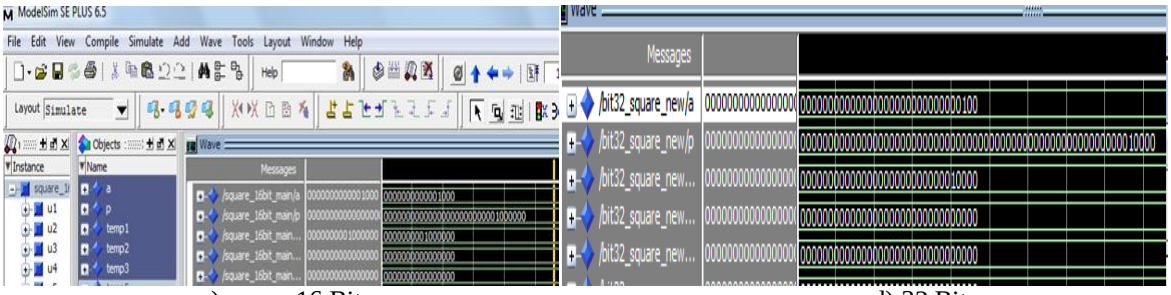


b) 8 Bit

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017



c) 16 Bit d) 32 Bit

Figure 11: Functional Verification of a) 4 Bit b) 8 Bit c) 16 Bit and d) 32 Bit respectively of the proposed Squaring Circuit

6. CONCLUSION

The execution of the proposed Squaring system turned out to be efficient in terms of area, power and speed. Because of its systematic and parallel arrangement, it can be implemented at the chip level. For the performance evaluation 4-bit, 8-bit 16-bit and 32 bit squaring circuits were considered in order to validate and substantiate the theoretical conclusions with simulation results.

From the experimental outcomes, we find that there is an improvement in combinational path delay of the proposed strategy. Even with respect to the number of input-output buffers required for implementation of the functionality, the proposed method provides considerable savings. An optimal solution with respect to combinational path delay is achieved by the reduction in the logic levels and subsequently lesser resource utilization when mapped onto a technology target.

The present approach is highly innovative and guarantees improved performance which is apparent from results achieved from the different cases (4-bit, 8-bit, 16-bit and 32-bit) considered for the study. Finally, it is concluded that the current method is highly innovative and elegant and gives a brilliant platform for future work.

REFERENCES

[1] Maharaja, J.S.S.B.K.T., "Vedic mathematics," Motilal Banarsidass Publishers Pvt. Ltd, Delhi, 2009.
[2] Booth, A.D., "A signed binary multiplication technique," Quarterly Journal of Mechanics and Applied Mathematics, vol. 4, pt. 2, pp. 236– 240, 1951.
[3] Vedic Mathematics [Online]. Available: http://www.hinduism.co.za/ vedic.htm.
[4] B. Parhami, "Computer Arithmetic Algorithms and Hardware Architectures," 2nd ed, Oxford University Press, New York, 2010.
[5] Kai Hwang, "Computer Arithmetic: Principles, Architecture and Design," New York: John Wiley & Sons, 1979.
[6] S. Akhter,, "VHDL implementation of Fast NxN Multiplier Based on Vedic Mathematics," Proc. of IEEE Conference, pp.472-475, 2007.
[7] P.D. Chidgupkar, and M.T. Karad, "The Implementation of Vedic Algorithms in Digital Signal Processing," Global Journal of Engng. Educ., vol.8 , pp.153-158, 2004.
[8] H.S. Dhillon, and A. Mitra, "A Reduced-Bit Multiplication Algorithm for Digital Arithmetic," International Journal of Computational and Mathematical Sciences, pp.64-69, 2008,
[9] P. Mehta, and D. Gawali, "Conventional versus Vedic Mathematical Method for Hardware Implementation of a Multiplier," Proc. Int Conf. on Advances in Computing, Control, and Telecommunication Technologies, Trivandrum, Kerala, India, pp.640-642, 2009.
[10] Kabiraj Sethi and Rutuparna Panda " An Improved Squaring Circuit for Binary Numbers" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.2, 2012.
[11] H. Thapliyal and M. B. Srinivas, "High Speed Efficient N×N Bit Parallel Hierarchical Overlay Multiplier Architecture Based on Ancient Indian Vedic Mathematics," Enformatika Trans., vol. 2, pp. 225–228, Dec. 2004.
[12] 'Xilinx ISE User Manual', Xilinx Inc, USA, 2007
[13] Prabha S., Kasliwal, B.P. Patil and D.K. Gautam, "Performance Evaluation of Squaring Operation by Vedic Mathematics", IETE Journal of Research, vol.57, Issue 1, Jan-Feb 2011
[14] P.K.Srimani and J.Vakula Rani "Implementation of Vedic Mathematical Algorithms to Elliptic Curve Encryption "Natioanl Level Congerence, IISc, Bangalore 2006.