Design and Simulink Implementation of 128-bit Vedic Multiplier

Gouri G Uppin, Mahesh N. Javalkar

Abstract- In the calculation of real numbers, carry needs to be propagated from the least significant bit (LSB) to the most significant bit (MSB) when binary partial products are added. Thus because of this process, the addition and subtraction after binary multiplications limit the overall speed. Existing vedic multiplication is available for 8bits, 16bits, 32bit and 64 bits, proposed system is for 128bits multiplication and to increased time efficiency, with less consumption of power. Nikhilam Sutra literally means "all from 9 and last from 10". Although it is applicable to all cases of multiplication, it is more efficient when the numbers involved are large. Since it finds out the compliment of the large number from its nearest base to perform the multiplication operation on it, larger is the original number, lesser the complexity of the multiplication. Thus, by using Nikhilam sutra it possible to multiply large numbers which is the limitation in the simple array multipliers. Nikhilam Navatashcaramam Dashatah- All from 9 and the last from 10 From the sixteen sutras available in Vedic mathematics, among them only two sutras are applicable for multiplication operation. They are Urdhva Triyakbhyam Sutra (literally means vertically and cross wise) and Nikhilam Sutra (literally means all from 9 and last from 10).Vedic Mathematics provides some effective algorithms which can be applied to various application fields of engineering. Out of these algorithms former proves to be a faster algorithm and applicable in all cases.

Keywords: Vedic Multiplie (V M), Radix selection unit (RSU), Exponent Determinant (E D), Mean Determinant (MD) Multiplexer (MUX)

I. INTRODUCTION

Vedic mathematics is an ancient system of calculation .This was discovered by Shri Bharati Krishna Tirthaji maharaj. Vedic mathematics is all based on 16 sutras. These sutras apply to and cover almost every branch of mathematics. Vedic Mathematics reduces the complexity in calculations that exist in conventional mathematics. Thus multipliers based on vedic mathematics is one of the most fastest and low power multipliers. The multiplier is fairly a large block of most of the computing systems. The amount of circuitry present is directly proportional to the square of it's resolution .That is, if a multiplier is of the size n bit then n^2 gates. In algorithmic and structural form, lot multiplication techniques have been developed to enhance the efficiency of the multipliers, which helps the reduction of the partial products and/or the methods for their partial products addition. Thus here by using vedic mathematics approach which is totally different and very close to the way a human mind works.

Revised Version Manuscript Received on December 07, 2015.

Gouri G. Uppin, Lecturer, Department of Electronics and Communication Engineering, Maratha Mandal Polytechnic, Belgaum, (Karnataka) India.

Mahesh N. Javalkar, Lecturer, Department of Electronics and Communication Engineering, Maratha Mandal Polytechnic, Belgaum, (Karnataka) India.

In most of the other works ASIC based design like Array multiplier and Booth multiplier etc have been used. In this work a new vedic multiplier structure using "Nikhilam" sutra and a technique like Mat lab with it's simulink implementation is being done. Here The 16 sutras are as follows

1) EKADHIKINA PURVENA - By one more than the previous one
2) NIKHILAM AVATASHCARAMAM DASHATAH- All from 9 and the last from 10
3) URDHVA TIRYAGBHYAM - Vertically and crosswise
4) PARAAVARTYA YOJAYET - Transpose and adjust
5) SHUNYAM SAAMYASAMWUAYE-When the sum is the same that sum is zero
6) (ANURUPYE) SHUNYAMANYAT- If one is in ratio, the other is zero
7) SANKALANA-AVAKALABHYAM-By addition and by subtraction
8) PURANAPURANASYHAM-By the completion or non-completion
9) CHALANA-KALANASYHAM -Differences and Similarities
10) YAAVADUNAM- Whatever the extent of its deficiency
11) VYASHTISAMANSTIH- Part and Whole
12) SHESANYANKENA-The remainders by the last digit
13) SOPAANTYADVAYAMANTYAM- The ultimate and twice the penultimate
14) EKANYUENA PURVENA- By one less than the previous one
15) GUNITASAMEHYAH-The product of the sum is equal to the sum of the product
16) GUNAKASAMCHYAH-The factors of the sum is equal to the sum of the factors

From the 16 sutras available in vedic mathematics, among them only 2 sutras are applicable for multiplication operation. They are,

1) URDHVA TIRYAGBHYAM and
2) NIKHILAM NAVATASHCARAMAM DASHATAH

Vedic mathematics provides some effective algorithms which can be applied to various application fields of engineering." NIKHILAM NAVATASHCARAMAM DASHATAH" formula is used for large number multiplication.

II. IMPLEMENTATION

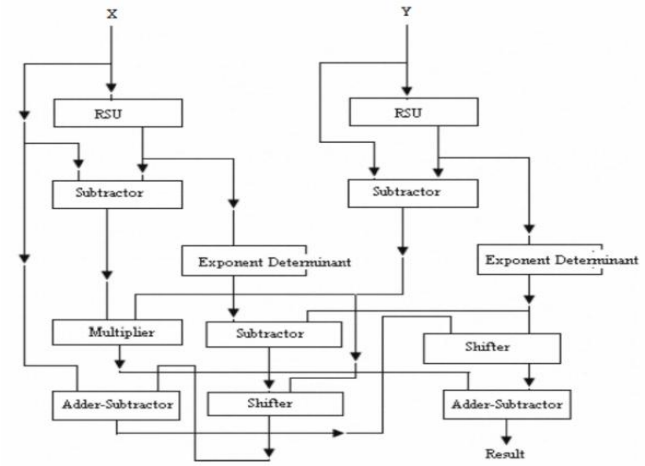


Figure 1 Implementation block diagram

Proposed work is based on Nikhilam Navatascaramam Dasatah. Consider two n bit numbers X and Y. k is the exponents, z1 and z2 of both X and Y respectively. X and Y can be represented as:

$$X = 2^k \pm z_1$$

$$Y = 2^k \pm z_2$$

Assuming product of the number is equals to P.

$$P = X \times Y = (2^k \pm z_1)(2^k \pm z_2)$$

For the fast multiplication using extended rule of the sutra the bases of the multiplicand and the multiplier assuming same, thus the above can be rewritten as

$$P = XY = 2^k(X \pm z_2) \pm z_1 z_2$$

From above equation it is observed that a large number multiplication can easily decomposed into a small number multiplication, addition/subtraction and shifting, leading towards the reduction of hardware cost, propagation delay and power consumption.

Multiplication using "Nikhilam Navatascaramam Dasatah" Sutra:

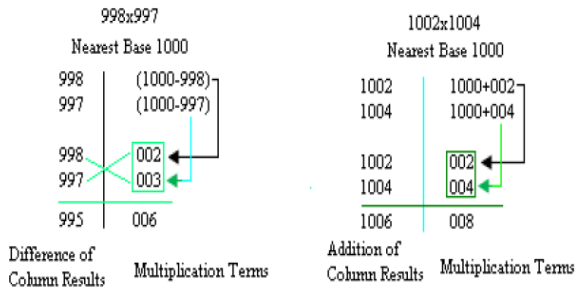


Figure 3.1. Procedure of multiplication using "Nikhilam Navatascaramam Dasatah" Sutra, (a) Numbers are taken below base, (b) Numbers are taken above base.

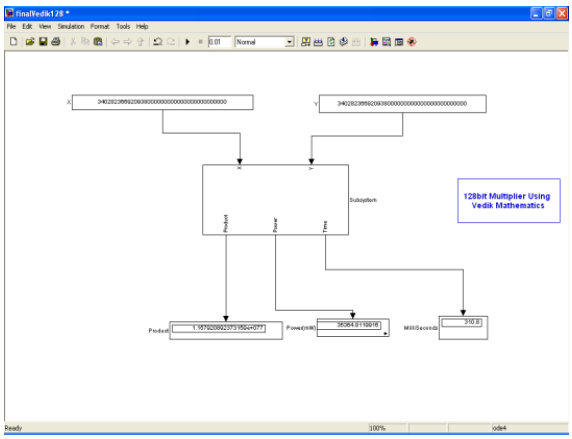
As shown in Figure 1, we write the multiplier and the multiplicand in two rows followed by the differences/addition of each of them from the chosen base. We can now write two columns of numbers, one consisting of the numbers to be multiplied (Column 1) and the other consisting of their compliments (Column 2). The product also consists of two parts which are demarcated/ incremented by a vertical line for the purpose of illustration.

The right hand side (RHS) of the product can be obtained by simply multiplying the numbers of the Column 2 (2×3 = 6 or 2×4=8). The left hand side (LHS) of the product can be found by cross subtraction or addition the second number of Column 2 from the first number of Column 1 or vice versa, i.e., 998-003 = 995 or 997-002 = 995 and 1002+004=1006 or 1004+002=1006. The final result is obtained by concatenating RHS and LHS (Answer = 995006 or 1006008).

6.1 Table of maximum bit and its multiplied output value:

Bits	Max Value	X * Y
4	15	225
8	255	65025
16	65535	4294836225
32	4294967295	1.84467E+19
64	18446744073709600000	3.40282E+38
128	340282366920938000000000000000000000	1.15792E+77

Output for 128*128 bits vedic multiplication



6.2 Table showing COMPARSION of simple array multiplier and vedic multiplier

	Simple Array Multiplier		Vedic Multiplier	
Bits	Time (msec)	Power (mW)	Time (msec)	Power (mW)
4	1.436	6.586	0.065	0.38
8	1.429	10.92	0.074	0.736
16	9.436	142	0.055	1.109
32	_	_	312.7	9382
64	_	_	312.5	18285
128	_	_	310.8	36364

6.3 Table of comparasion for bit length Vs time

Bits	Array Multiplier (mSec)	Vedik Multiplier (mSec)
4 bit	1.436	0.065
8 bit	1.429	0.074
16 bit	9.436	0.055

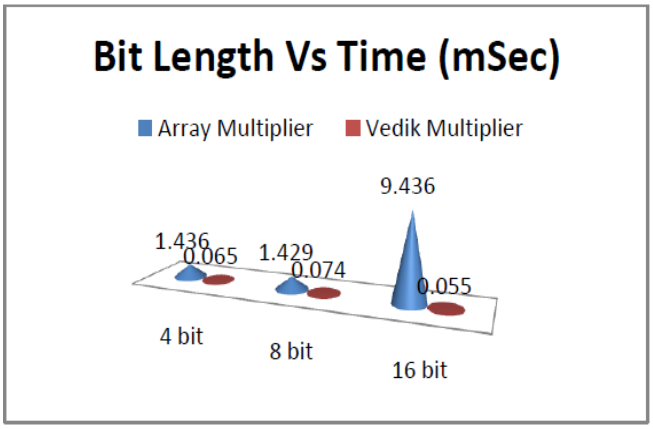


Fig 6.1: Bit length Vs Time(msec)

Table of comparasion for bit length Vs power

Bits	Array Multiplier (mWatts)	Vedik Multiplier (mWatts)
4 bit	6.586	0.38
8 bit	10.92	0.736
16 bit	142	1.109

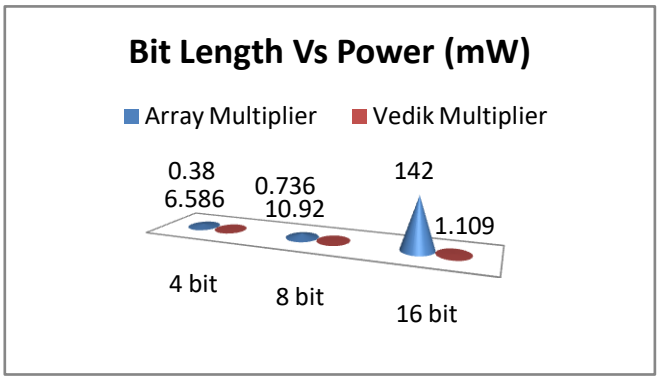


Fig 6.2: Bit length Vs Power (mwatts)

6.4 Table of comparison for bit Vs Time

Bits	Time (mS)
4 bit	0.065
8 bit	0.074
16 bit	0.055
32 bit	312.7
64 bit	312.5
128 bit	310.8

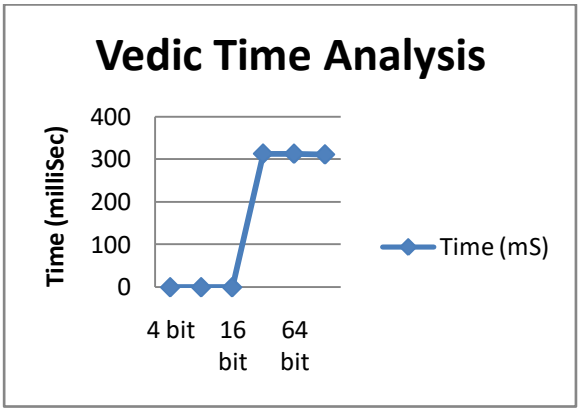


Fig 6.3: Vedic time analysis Bit length Vs Time (ms)

6.5 Table of comparasion for bit Vs Average power Time

Bits	AvgPower (mW)
4 bit	5.846153846
8 bit	9.945945946
16 bit	20.16363636
32 bit	30.00319795
64 bit	58.512
128 bit	117.001287

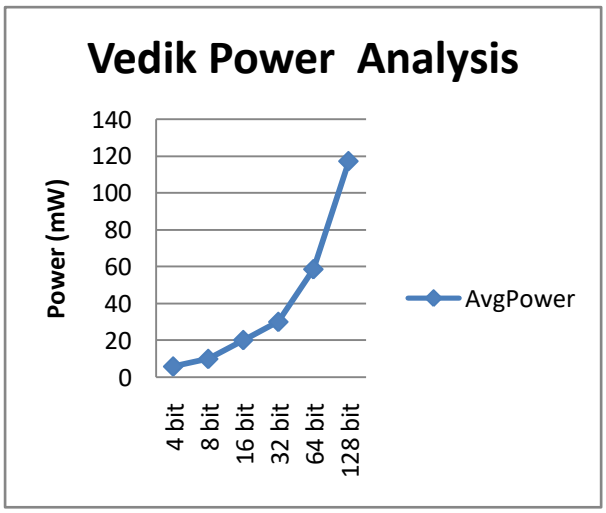


Fig 6.4: Vedic power analysis Bit length Vs Power (mW)

III. CONCLUSION

After the comparision of simple array multiplier and vedic multiplier with respect to time and power consumption, it is found that vedic multiplier is much better than array multiplier. Also, vedic multiplier allows to make large number multiplication, which is not possible with array multiplier. It can be concluded that Vedic Multiplier is superior in all respect like speed, delay, complexity, power .However Array Multiplier requires more power consumption and more time for process. Ancient Indian Vedic Mathematics gives efficient algorithms or formulae for multiplication which increase the speed of devices. Nikhilam sutra, is general mathematical formula and equally works the best.

Applicable to all cases of multiplication. Also, the architecture based on this sutra is seen to be similar to the popular array multiplier where an array of adders is required to arrive at the final product.

FUTURE SCOPE

This work can be extended to make large number divisions using Vedic mathematics. As Vedic mathematics improves the computation skills of the learners in a large area of problems, ensuring both speed and accuracy.

APPLICATIONS

1) RSA (cryptosystem): RSA is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers.
2) Fundamental operation squaring: Finding the square root of a number is the inverse operation of squaring that number. Remember, the square of a number is that number times itself.
3) Cubing: This process involves multiplying a number three times, thus the result is achieved. Therefore a multiplier can be used for this process also.
4) Linear equation: A linear equation is an algebraic equation in which each term is either a constant or the product of a constant and a single variable. Linear equations can have one or more variables.

REFERENCES

1. Prabir Saha·, Arindam Banerjee··, Partha Bhattacharyya·, Anup Dandapat , High Speed ASIC Design of Complex Multiplier Using Vedic Mathematics ,Proceeding of the 2011 IEEE Students' Technology Symposium 14-16 January, 2011, lIT Kharagpur.
2. Saha, Banerjee, Dandapat, Bhattacharyya, vedic mathematics based 32-bit multiplier design for high speed low power processors , international journal on smart sensing and intelligent systems vol. 4, no. 2, june 2011.
3. Manoranjan Pradhan,Rutuparna Panda,Sushanta Kumar Sahu, 16 Speed Comparison of 16x16 Vedic Multipliers International Journal of Computer Applications (0975 – 8887) Volume 21– No.6, May 2011.
4. Tom´as Lang and Alberto Nannarelli , Combined Radix-10 and Radix-16 Division Unit, 978-1-4244-2110-7-2007 IEEE.
5. Badal sharma, Design and hardware implementation of 128-bit vedic multiplier , volume 1, issue v, june 2013 international journal for advance research in engineering and technology.
6. R.Priya and J.Senthil Kumar, Implementation and comparison of vedic multiplier using area efficient CSLA architectures. Volume 73, no.10,july 2013.international journal of computer application.
7. G.Ganesh Kumar , V. Charishma, Design of high speed vedic multiplier using vedic mathematics techniques. Volume 2, march 2012.
8. Poornima M, Shivaraj Kumar Patil, Shivukumar , Shridhar K P , Sanjay H , Implementation of Multiplier using Vedic Algorithm, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013
9. Poornima M, Shivaraj Kumar Patil, Shivukumar , Shridhar K P ,sanjay "Implementation of Multiplier using Vedic Algorithm
10. Kripa Mathew, S.Asha Latha, T.Ravi, E.Logashanmugam, proposed " Design and Analysis of an Array Multiplier Using an Area Efficient Full Adder Cell in 32nm CMOS Technology"
11. N. Ravi, A.Satish, Dr.T.Jayachandra Prasad and Dr.T.Subba Rao proposed "A New Design for Array Multiplier with Trade off in Power and Area".

AUTHOR PROFILE

Gouri G. Uppin was born in Belgaum , Karnataka , India in 1974 . She received the B.E. degree in Electronics and Communication Engineering from Karnataka University Dharwad (KUD) , Dharwad , India . Further she received M.Tech degree from Visvesvaraya Technological University (VTU), Belgaum, India, in VLSI Design and Embedded Systems course . She is currently working as Selection Grade Lecturer in the department of Electronics and Communication Engineering , Maratha Mandal Polytechnic , Belgaum , India . She has 19 years of teaching experience . Her area of interest includes Microcontroller , VLSI Design techniques, Microprocessor , MAT programming and Computer Networking.

Mahesh N. Javalkar was born in Belgaum , Karnataka , India in 1971 . He received the B.E. degree in Electronics and Communication Engineering from Karnataka University Dharwad (KUD) , Dharwad , India . Further he received M.Tech degree from Visvesvaraya Technological University (VTU) , Belgaum , India, in VLSI Design and Embedded Systems course . He is currently working as Selection Grade Lecturer in the department of Electronics and Communication Engineering , Maratha Mandal Polytechnic , Belgaum , India . He has 17 years of teaching experience . His area of interest includes Microprocessors , ARM Microcontrollers , VLSI Design techniques and Computer Networking .