International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 1 Issue 5 ǁ Sep. 2013 ǁ PP.40-45

Application of Vedic Mathematics In Computer Architecture

Chilton Fernandes[1], Samarth Borkar[2]
[1](*Microelectronics, Goa College of Engineering, Goa University, India)*
[2](*Assistant professor, Goa College of Engineering, Goa University India)*

ABSTRACT*: Vedic mathematics or ancient mathematics is a unique technique of calculations based on 16 sutras. It provides an innovative way of computation of almost all the mathematical operations. In this era of digitization, engineers are working on increase speed of the digital circuits while reducing the size and power consumed. Arithmetic operations are the basic units of all the digital circuitry and hence optimizing these unit increases efficiency of the entire digital design. Unlike conventional mathematics, Vedic math provides different techniques to compute basic arithmetic operations. Vedic math reduces the computational steps required to achieve the result. Designers have implemented many computer architectures based on Vedic math. In this paper we review these architectures as well as several extended work in the area. In addition, we also review several state-of-art applications that take full advantage of such simple ancient Vedic Mathematical technique.*
Keywords - *Nikhilam sutra, RSA algorithm, Urdhva-tiryakbyham, Vedic mathematics, Vedic multiplier*

I. INTRODUCTION

The word "Vedas" which literarily means knowledge has derivational meaning as principle and limitless store-house of all knowledge. The word Veda also refers to the sacred ancient Hindu literature which is divided into four volumes. "Vedic Mathematics" is the name given to the ancient system of mathematics, or, to be precise, a unique technique of calculations based on simple rules and principles, with which any mathematical problem be it arithmetic, algebra, geometry or trigonometry can be solved. The ancient system of Vedic Mathematics was rediscovered between 1911 and 1918 by Sri Bharati Krishna Tirthaji (1884-1960) [1]. Swami Bharati Krishna Tirtha (1884-1960), former Jagadguru Sankaracharya of Puri culled a set of 16 Sutras (aphorisms) and 13 Sub- sutras (corollaries) from the Atharva Veda. He developed methods and techniques for amplifying the principles contained in the aphorisms and their corollaries, and called it Vedic Mathematics. The beauty of Vedic mathematics lies in the fact that it reduces otherwise cumbersome looking calculations in conventional mathematics to very simple ones. This is so because the Vedic formulae are claimed to be based on the natural principles on which the human mind works. This is a very interesting field and presents some effective algorithms which can be applied to various branches of engineering such as computing, VLSI implementation and digital signal processing.

This paper is organized in following sections: Section II provides overview of the Vedic sutras, section III elaborates on the uses of these sutras, performance of Vedic algorithms is analysed in section IV and last section concludes the paper.

II. VEDIC MATHEMATICS SUTRAS

Entire mechanics of Vedic mathematics is based on 16 sutras – formulas and 13 up-sutras meaning – corollaries [2].

Sutras:

1. Ekadhikena Purvena
2. Nikhilam Navatascharamam Dashatah
3. Urdhva-tiryagbhyam
4. Paravartya Yojayet
5. Shunyam Samyasamucchaye
6. Anurupye Sunyamanyat
7. Sankalana vyavakalanabhyam
8. Puranaprranabhyam
9. Calana – Kalanabhyam
10. Yavadunam
11. Vyastisamashtih
12. Sheshanynkena Charmena
13. Sopantyadvayamantyam
14. Ekanyunena Purvena
15. Ginitasamucchayah
16. Gunaksamucchayah

Up-sutras:

1. Anurupyena
2. Shishyate Sheshsamjnah
3. Adyamadye Nantyamantyena
4. Kevalaih Saptakam Gunyat
5. Vestanam
6. Yavadunam Tavadunam
7. Yavadunam Tavadunikutya Varganka ch Yojayet
8. Antyayordhshakepi
9. Antyatoreva

10. Samucchayagunitah
11. Lopanasthapanabhyam
12. Vilokanam
13.Gunitasamucchyah samucchayagunitah

In the field of engineering most of the researcher are using following sutras, we will describe them briefly:

i) Nikhilam navata charanam Dashatah,
ii) Urdhva-tiryakbyham.

2.1 Nikhilam Sutra

First formula under consideration is Nikhilam Navatascharam Dashtah which means all from 9 and last from 10. The algorithm has its best case in multiplication of numbers, which are nearer to bases of 10, 100, 1000 i.e. increased powers of 10. The procedure of multiplication using the Nikhilam involves minimum mental manual calculations, which in turn will lead to reduced number of steps in computation, reducing the space, saving more time for computation. The numbers taken can be either less or more than the base considered. The mathematical derivation of the algorithm is given below. Consider two n-bit numbers x and y to be multiplied. Then their complements can be represented as x1 = 10n - x and y1 = 10n – y. The product of the two numbers can be given as p = (x, y). Now a factor 102n +10n (x + y) is added and subtracted on the right hand side of the product equation, which is mathematically expressed as shown below.

$p = xy + 102n + 10n (x + y) - 102n - 10n (x + y)$

On simplifying we get,

$p = \{10n (x + y) - 102n\} + \{102n - 10n (x + y) + xy\}$
$= 10n \{(x + y) - 10n\} + \{(10n – x) (10n – y)\}$
$= 10n \{x – y1\} + \{x1\ y1\}$
$= 10n \{y – x1\} + \{x1\ y1\}$

From the above equation we can derive the left hand side of the product as {x – y1} or {y– x1} and the right hand side as (x1.y1) The basic operations involved in the algorithm for a given set of numbers are given below.

Consider 98 x 97

Here the Nearest Base = 100

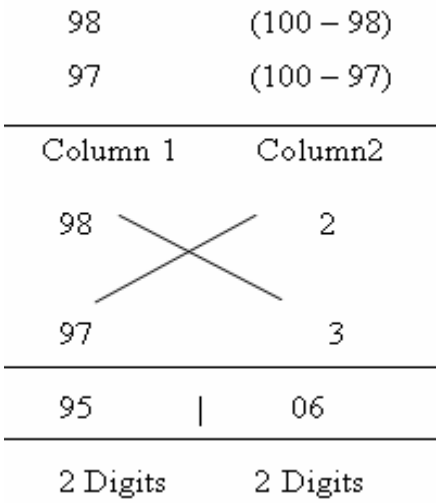

Fig 1: Multiplication using Nikhilam sutra

Result = 98 x 97 = 9506

The Nikhilam Sutra can also be modified for binary arithmetic.

2.2 Urdhava Tiryakbhyam

Urdhava Tiryakbhyam Sutra, which literally means "Vertically and crosswise", is a general multiplication formula applicable to all cases of multiplication. This Sutra highlights parallelism in generation of partial products and their summation as depicted in Fig 2. Consider multiplication of 576x324=186624.

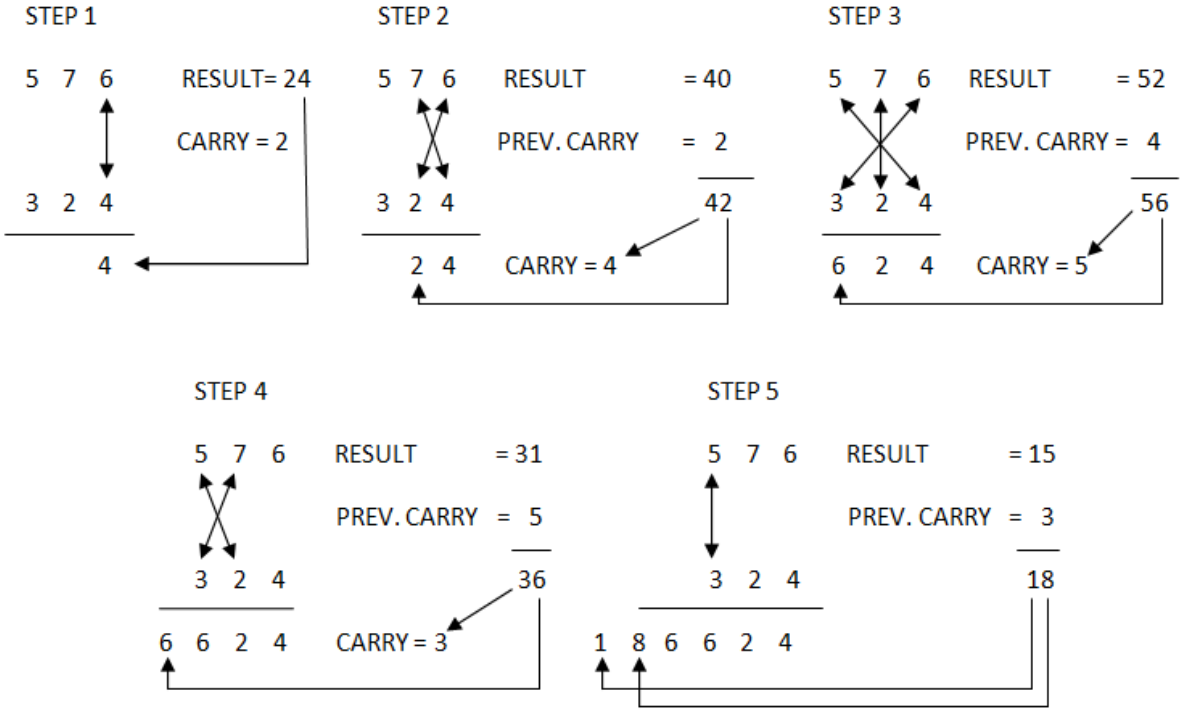

Fig: 2 Illustration of vertically and crosswise multiplication

Alternative method for calculation using Urdhva-Triyakhbhyam sutra is shown in figure 3. Let us consider the multiplication of (5498 × 2314). The numbers to be multiplied are written on two consecutive sides of the square as shown in the figure 1. The square is divided into rows and columns where each row/column corresponds to one of the digit of either a multiplier or a multiplicand. Thus, each digit of the multiplier has a small box common to a digit of the multiplicand. These small boxes are partitioned into two halves by the crosswise lines. Each digit of the multiplier is then independently multiplied with every digit of the multiplicand and the two digit product is written in the common box. All the digits lying on a crosswise dotted line are added to the previous carry. The least significant digit of the obtained number acts as the result digit and the rest as the carry for the next step. Carry for the first step (i.e., the dotted line on the extreme right side) is taken to be zero.

III. Uses of Vedic Sutras

Vedic mathematics is used by several researchers in the field of Digital signal processing, Chip designing, Discrete Fourier Transform , High speed low power VLSI arithmetic and algorithm, RSA encryption system . Most of the researchers have used the Vedic mathematics method such as multiplication, division, squares and cubes in above mention fields.

3.1 Multiplier and squarer architecture

Mathematical operations especially multiplications consumes most of the time of the process in a computer. High speed multiplication is desired in real-time operations and image processing applications. Various multiplier architectures have been developed using various algorithms such as Booth, array multipliers and Wallace tree. All the aforesaid algorithms use the basic conventional method of multiplication. Vedic mathematics provides an innovative method of multiplication. Vedic multiplication reduces computation time by parallel generation of intermediate (Urdhviate) products. Multiplier designed using Urdhva-tiryakbyham sutra of Vedic mathematics is faster than array multiplier and Booth multiplier architecture and is very efficient in silicon area per speed [3, 4, 5]. Another multiplier using Nikhilam sutra of Vedic mathematics shows similar results when compared to the conventional multipliers [6]. Squarer is designed using the "Duplex" D property of the binary numbers and Urdhva-tiryakbyham sutra, is the smallest and fastest as compared to the conventional multipliers [7].

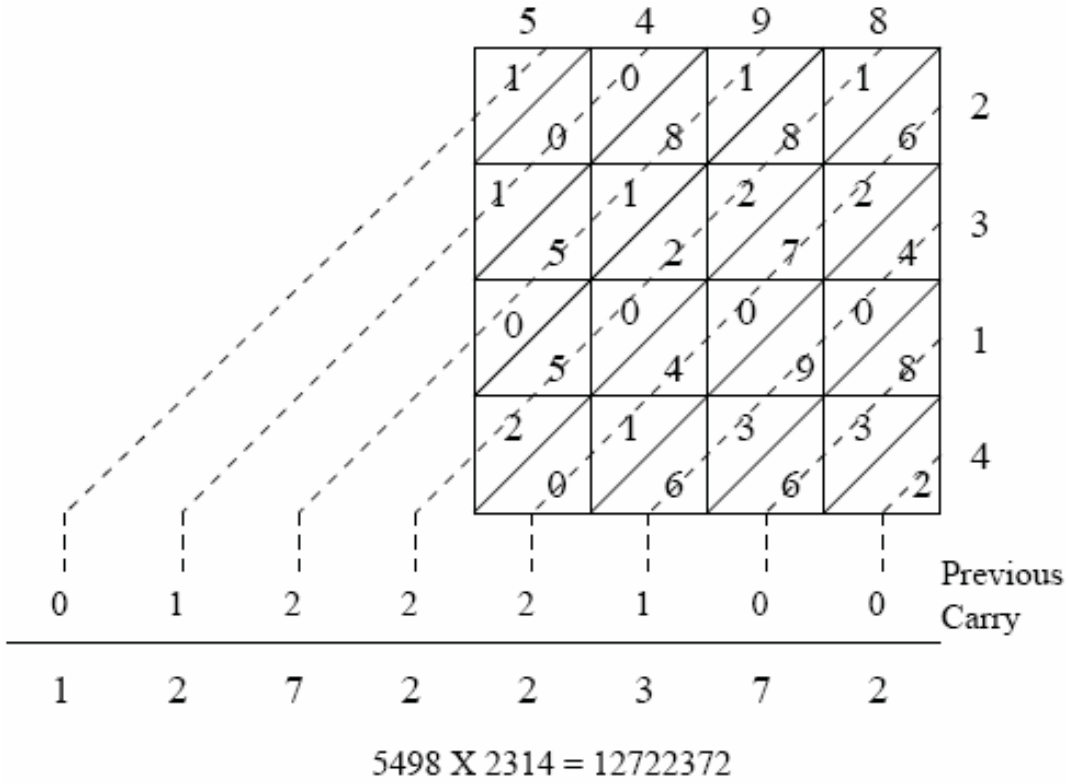

Fig 3: Alternative way of multiplication by Urdhva tiryakbhyam Sutra

3.2 VLSI Implementation of RSA encryption

RSA is an algorithm for public-key cryptography for network security. One of the most time consuming processes in RSA algorithm is computing a^b mod n where 'a' is the text and (b, n) is the public key. Dhvanjanka sutra is used in RSA encryption and decryption algorithm. RSA implemented using the overlay hierarchical multiplier architecture and division architecture using Dhvajanka sutra of Vedic mathematics reduces computation time and reduces delay greatly as compared to the RSA implemented using traditional multipliers and division algorithms [8, 9].

3.3 Discrete Fourier Transform

There are many algorithms for finding DFT. But now a day's only VON-NEUMAN architectural implementation of classical method is found to be used in digital computers. Kulkarni analyses and compares the Implementation of Discrete Fourier Transform algorithm by existing and by Vedic mathematics techniques [10]. He suggested that architectural level changes in the entire computation system to accommodate the Vedic Mathematics method increases the overall efficiency of DFT procedure.

3.4 FFT Implementation

A fast Fourier transform (FFT) is an algorithm to compute the discrete Fourier transform (DFT) and it's inverse. FFT is widely used in wireless communication imaging etc. Implementation of FFT requires large number of complex multiplications and complex additions, so to make this process rapid and simple it's necessary for a multiplier to be fast and power efficient. Vedic mathematics is an efficient method of multiplication.

Nidhi Mittal and Abhijeet Kumar implemented FFT using "Vertically and crosswise" algorithm of Vedic maths and suggested that Vedic mathematics reduces the complex number multiplications and additions from N2 to N/2log2N and Nlog2N respectively and conclude that Vedic method is faster than the array multiplier architecture [11, 12, 13].

3.5 ALU Design

Arithmetic and logic unit is at the heart of the digital circuits. Due to the complexity of the operations that needs to be performed nowadays by the processor, the demand for sharing the load by many special purpose processors is increased. Hence the speed, size and power efficiency of the ALU becomes important factors when designing an ALU. Use of Vedic mathematics for multiplication strikes a difference in actual process and hence

reduces size and power. Anvesh kumar used Urdhva tiryakbhyam Sutra of Vedic mathematics to build a power efficient multiplier in the coprocessor [14]. The advantages of Vedic multipliers are increase in speed, decrease in delay, decrease in power consumption and decrease in area occupancy. It is stated that this Vedic coprocessor is more efficient than the conventional one.

3.6 Elliptic curve cryptography

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Like the RSA, EEC is also a public key encryption. The most important equation that needs to be solved in ECC curve equations are $y2+xy=x3+ax2+b$ (Weierstrass equation in GF(2m)) and $y2=x3+ax+b$ (Weierstrass equation in GF(p)). The major time consuming arithmetic operations operation in ECC are point additions and doubling as exponentiation operations like square, cube and fourth power occur in these operations. Thapliyal *et.al* proposed a novel square and fourth power computation using Vedic mathematics algorithm [16]. A considerable input in the point addition and doubling has been observed when implemented using proposed techniques for exponentiation.

IV. Performance Analyses of Vedic Algorithms

Various parameters are recommended by researchers to evaluate the performance of Vedic Maths algorithm. Researchers suggested many parameters few of them are: Time, Delay, Power and Number of slices. The comparison of Delay (ns) factor for multiplication implemented in different algorithms between Conventional and Vedic way is shown in Table 1 [15].

V. Conclusion

Vedic mathematics formulae can be used in various algorithms in different computer applications. Various parameters are considered for comparisons of different algorithms. It is concluded that the computer architectures designed using Vedic mathematics are proved to better the conventional architecture in terms of computation speed, power utilisation and silicon area. Various algorithm based on Vedic maths proved to have faster speed, less power and lesser area. The results obtained are also verified on various FPGAs. Further improvement can be done by reducing the delay caused by propagation of the carry generated from the intermediate products in the multipliers.

Sr. No.	Implemented in	Conventional		Vedic	
		8 bit	16 bit	8 bit	16 bit
01	VLSI Implementation of High Performance RSA Algorithm	31.241	57.973	26.081	54.973
02	High Speed Energy Efficient ALU Design	31.029	46.811	15.418	22.604
3	An Efficient Method of Elliptic Curve Encryption (for square)	30.370	60.646	15.193	23.600
4	An Efficient Method of Elliptic Curve Encryption (for point doubling)	604.861	1327.809	542.325	1207.677

Table 1: Comparisons of different architecture using Vedic and conventional way

REFERENCES

[1] Website: http://www.vedicmaths.org/introduction/what-is-vedic-mathematics

[2] Website: http://vedamu.org/PageViewerToC.aspx?ID=148372&DivisionId=1795

[3] Poornima M, Shivaraj Kumar Patil, "Implementation of Multiplier using Vedic Algorithm", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013.

[4] ShamainAkhter, "VHDL Implementation of Fast NxN Multiplier based on Vedic Mathematics", Jaypee Institute of Information Technology University, Noida, 201307op, India, IEEE 2007

[5] H. Thapliyal and M. B. Srinivas, "High Speed Efficient N by N Bit Parallel Hierarchical Overlay Multiplier Architecture Based", pp. 225-228, Dec. 2004.

[6] D. Kishore Kumar, A. Rajakumari, "Modified Architecture of Vedic Multiplier for High speed applications", International Journal of Engineering Research and Technology (IJERT), ISSN: 2278-0181, vol. 1 Issue 6, August 2012.

[7] Himanshu Thapliyal, Hamid R Arabnia, "A time-area-power efficient multiplier and square architecture based on ancient Indian Vedic mathematics"

[8] Himanshu Thapliyal and M.B Srinivas "VLSI Implementation of RSA Encryption System Using Ancient Indian Vedic Mathematics" Proceedings of International Conference on Security Management, 2005.
[9] R. Tamil Chelvan, S. Roobini Priya, "Implementation of fixed and floating point division Dhvajanka sutra" International journal of VLSI and embedded Systems-IJVES, ISSN:2249-6556, Vol 04, Issue 02: March-April 2013.
[10] Mr.Shripad Kulkarni " Discrete Fourier Transform by Vedic Mathematics".
[11] Ashish Raman, Anvesh Kumar, R.K.Sarin, "High Speed Reconfigurable FFT Design by Vedic Mathematics", journal of Computer Science and Engineering, vol.1, pp 59-63 May 2010.
[12] Anvesh Kumar, Ashish Raman, "Small Area Reconfigurable FFT Design by Vedic Mathematics", vol 5, IEEE pp 836-838, 2010.
[13] Nidhi Mittal, Abhijeet Kumar "Hardware Implementation of FFT using vertically and Crosswise Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 35– No.1, December 2011.
[14] Anvesh Kumar, Ashish Raman, "Low Power ALU Design by Ancient Mathematics", vol 5, IEEE pp 862-865, 2010
[15] Dr.S.M.Khairnar, Ms. Sheetal Kapade, Mr.Naresh Ghorpade, "Vedic Mathematics-The Cosmic Software For Implementation Of Fast Algorithms"
[16] H. Thapliyal and M. B. Srinivas, "An Efficient Method of Elliptic Curve Encryption Using Ancient Indian Vedic Mathematics", Proc. IEEE MIDWEST symp.Circuits and systems, pp. 826{829, Cincinnati, Aug. 2005.