INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 8, Issue 1 - V8I1-1392)
Available online at: https://www.ijariit.com

Revisiting Vedic math for engineering applications

Himani Kulshreshtha
khimani279@gmail.com
Bharati Vidyapeeth (Deemed to be University), college of engineering, Pune, Maharashtra

ABSTRACT

This paper has been brought up or aimed to represent, show the importance and application of various Vedic algorithms , namely Dhawajanka sutra , Urdhavatriyakbhyam, arunanka into various branches of engineering and science such as computing , VSLI implementation, Real time operations ,Image processing , VLSI implementation of RSA encryption, Cryptography , Network Security , Discrete Fourier transform , Fast Fourier transform, ALU design , Elliptic curve cryptography , AES method cryptography , Digital Signal processing , multiplier and Block convolution.

***Keywords*:** *Dhwajanka Sutra, Urdhavatriyakbyam Sutra, Arunanka Method, Vsli Implemention , Rsa Encryption , Cryptography , Network Security , Discrete Fourier Transform, Fast Fourier Transform, Alu Design , Elliptic Curve Cryptography , Aes Method Cryptography , Digital Signal Processing , Multiplier , , Block Convolution.*

1. INTRODUCTION

Between 1911 and 1918, Sri Bharati Krishna Tirthaji rediscovers Vedic mathematics and its derivational meaning, which is the primordial and limitless storehouse of all knowledge.

Swami Ji chose 16 sutra aphorisms and 13 sub-sutra corollaries from one of the four most popular Vedas, coining the term Vedic mathematic to represent all the approaches and strategies utilized to enrich the concepts in the sutras and sub-sutras.

The entire concept of Vedic equations is based on how the human mind works, allowing them to simplify complex and time-consuming calculations**.**

2. VEDIC MATHEMATICS SUTRAS

SUTRAS:

1. EkadhikenaPurvena
2. NikhilamNavatascharamamDashatah
3. Urdhva –triyagbhyam
4. ParavartyaYojayet**Up-sutras**:
5. ShunyamSamyasamucchaye1. Anurupyena
6. AnurupyeSunyamanyat 2. ShishyateSheshsamjnah
7. Sankalanavyavakalanabhyam3. AdyamadyeNantyamantyena
8. Puranapraanabhyam4. KevalaihSaptakamGunyat
9. Calana- Kalanabhyam 5. Vestanam
10. Yavadunam
11. Vyastisamashtih
12. SheshanynkenaCharmena
13. Sopantyadvayamantyam
14. EkanyunenaPurvena
15. Ginitasamucchayah
16. Gunaksamucchayah

6. YavadunamTavadunam
7. YavadunamTavadunikutyaVargankacgh
8. Anthyayordhshakepi
9. Antyatoreva

3. MATERIALS AND METHODS

RuchiAnchaliya et al. [16] used the Xilinx 13.1 package with the Spartan 3 family and the XC3S400 device to simulate and generate Vedic sutras.Following are the important results:

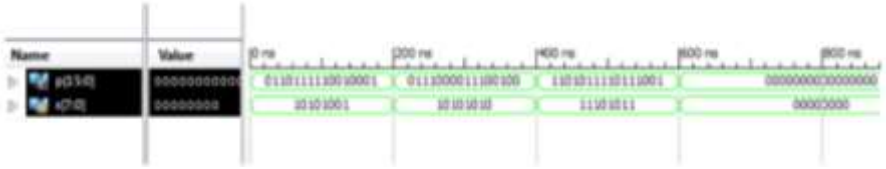


Fig. 1 Simulation result for square of 8-bit binary numbers using Vedic mathematics sutras

For square of a number, total delay has been reduced from 25.380ns (as in normal multiplication) to 15.859ns in case of using Vedic mathematics sutras.

The simulation results of two 8-bit binary numbers are shown below:

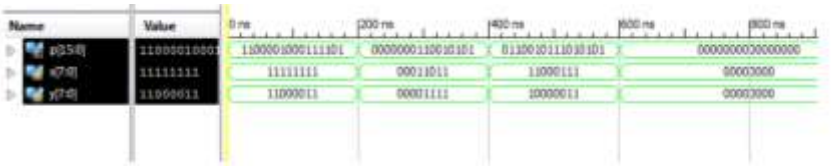


Fig. 2 Simulation result for multiplication of binary number using Vedic mathematics sutras.

Number of slices has also been **reduced** from **72 to 36 out of 4656**. Or multiplication, total delay has been reduced from 25.380ns to 19.868ns with almost same number of slices.

The simulation results for division of up to 9-bit binary number by divisor of up to 5-bit binary numbers are shown below:

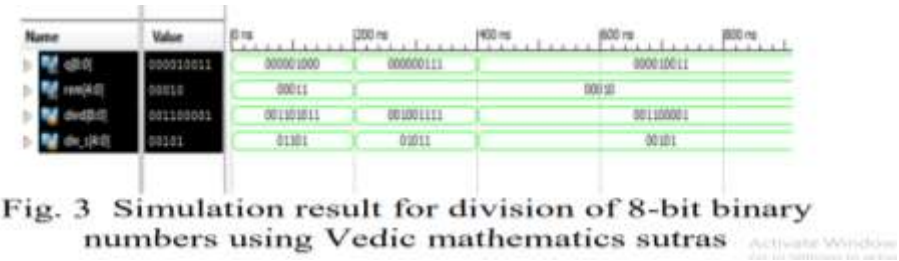


Fig. 3 Simulation result for division of 8-bit binary numbers using Vedic mathematics sutras

For division, **total delay** has been found as **101.503 ns**. **Number of 8-bit and 16-bitadders/subtractors** have also been **reduced** when design in implemented using Vedic Mathematics Sutras.

Nikhilam sutra [29]

The first formula to analyze is nikhilamnavatascharamdashtah which means everything starts with 9 and ends with 10 the algorithm performs best when multiplying numbers with bases of 10 100 and 1000 ie rising powers of 10.

The Nikhilam multiplication technique requires the least amount of mental manual computations, resulting in a reduction in the number of steps in computation, a reduction in space, and a reduction in computation time. The numbers taken can be less or more than the base taken into account. The algorithm's mathematical derivation is shown 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

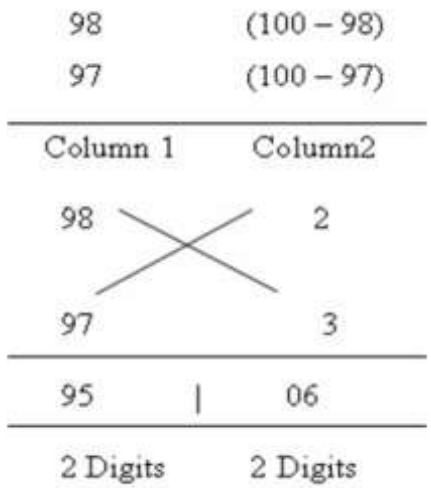


Fig 1: Multiplication using Nikhilam sutra

Result = 98 x 97 = 9506

Nikhilam Sutra for Division [17]
NikhilamNavatashcaramamDashatah sutra in Division is applied when divisor is closer to and slightly lesser than power of 10.

Example: 4382/99

Step1: Split dividend in two parts (quotient and remainder) in such a way remainder to have same digits as that of divisor. Here it is 2.
Dividend: 4382
Divisor: 99

Quotient	**Remainder**
43	**82**

Step 2: Take complement of divisor 01 (100-99=01) .This is called deficiency.
Step 3: Take first digit down as it is

Quotient	Remainder
43	82
4	

Step 4: Multiply the deficiency (01) with first digit (4), shift one place to right and then write below 3 and 8**.**Now add the first column.
Step 5: The above step repeated and add column wise till the number is filled in last column and then added column wise.
Step 6: In few cases it may be possible that remainder is greater than the divisor which is not possible. In this case divide the remainder with the divisor that results in sub quotient and sub-remainder. Add sub-quotient with original quotient and sub-remainder becomes the final remainder.

As in instance of the Vedic approach, the division operation was carried out using multiplication and addition procedures. As we can see, multiplication is a faster and less expensive procedure than division, leads to faster and simpler operation. [15].

Dhawajanka Sutra for division [17]
Dhawajanka Sutra is the upa sutra of vedic mathematics which means ‘on the top of the flag’, is a generalized formula for division. It is based on the formula Urdhva-tiryagbhyam.

Steps of the division are performed in dhawajanka sutra is given below [16]:
Step 1: The divisor and dividend are arranged in the form shown below. Only leftmost digit of divisor is left aside. Dividend is separated in two sections right part consisting number of digits equal to digits in divisor. Divisor is represented by d, dividend by X and quotient by A.
Step 2: Only first digit of dividend is divided by the left out digit, quotient and remainder of this division are noted.
Step 3: During next iteration remainder from previous iteration is used with next digit of dividend. Quotient digits and dividend digits without leftmost digit are multiplied in vertically and crosswise manner. This product is subtracted from number formed by combination of remainder and digit of remainder.
Step 4: Number left after subtraction in step 3 is divided by left out digit of divisor quotient is noted and remainder is prefixed with rest of the digits of dividend.

Step 5: This process is continued till same number of quotient digits equal to digits in left part of dividend is obtained.
Step 6: Remainder is obtained by subtraction of right part of dividend prefixed by last remainder and cross multiplication of quotient and divisor.

This sutra produces same results whether applied to large or small divisors.

UrdhavaTiryakbhyam [29]
UrdhavaTiryakbhyam 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.

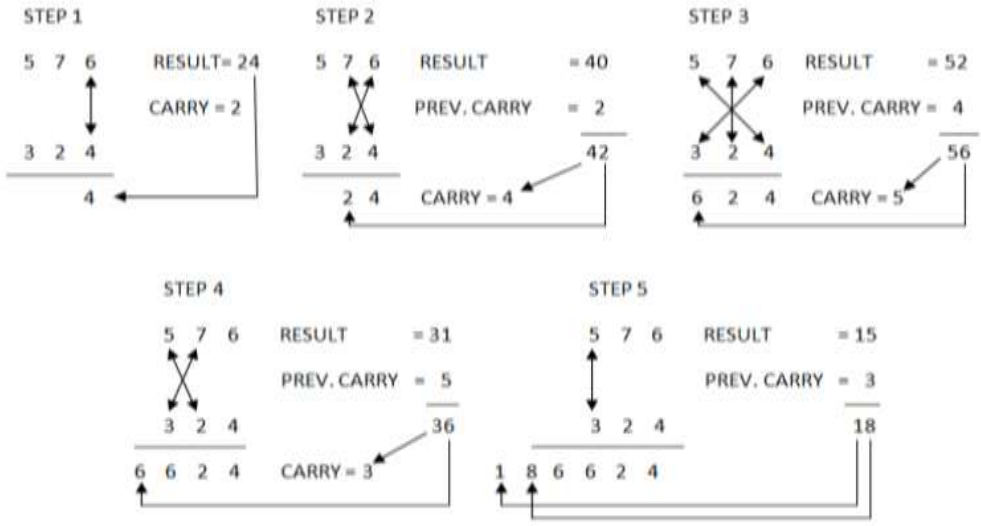


Fig: 2 Illustration of vertically and crosswise multiplication

4. MULTIPLIER AND SQUARER ARCHITECTURE

Mathematical operations, particularly multiplications, take up the majority of the time in a computing. In real-time operations and image processing applications, high-speed multiplication is essential.

Various multiplier structures have been created using methods like Booth, array multipliers, and Wallace trees. All of the abovementioned approaches utilize the basic multiplication approach. Multiplication is done in a distinctive manner in Vedic mathematics.

Vedic multiplication greatly reduces computation time by creating intermediate (Urdhviate) products in parallel. The Urdhva-tiryakbyham sutra of Vedic mathematics is used to develop a multiplier which is faster than array multipliers and Booth multipliers in terms of silicon area per speed [1, 2,3]. When compared to conventional multipliers, another multiplier centered on the Nikhilam sutra of Vedic mathematics yields similar results [4].

Because it is created utilising the unique combination of the duplex d feature of binary digits and the urdhva-tiryakbyham sutra, squarer is the tiniest and shortest multiplier comparison to usual multipliers [5].

Around 2009, Tiwariet. al[41] described a multiplier design based on the nikhilamnavatascaramamdasatah sutras, however he did not include the multiplication hardware. Saha et.al [42] recently released a multiplier for specific types multiplier layout of the same grounds based on the very same logic as the nikhilamnavatascaramamdasatah sutra, but he did not spread his work to general purpose multiplier design.

P.Saha et al. [40] describe a transistor level version (ASIC) of a Vedic Mathematics oriented 32-bit multiplier for super fast reduced power processor. He formulated the mathematics for constructing the 32-bit multiplier architecture at the transistor level with two specific aims in mind: I Ease and modularity multiplications for VLSI implementations, and ii) Carry propagation elimination for quick adds and subtractions. He used Vedic mathematics and a (NN) bit multiplier algorithm to transform one small number multiplication, one addition/subtraction, and shifting operations into one small number multiplication, addition/subtraction, and shifting operations. For small number multiplication, he employed the "Urdhva-tiryakbyham" approach, and for creating the entire (NN) bit multiplier, he used the "NikhilamNavatascaramamDasatah" and "Urdhva-tiryakbyham" methodology.

Spice spectre was being used to calculate system performance like propagation delay, dynamic leakage power, and dynamic switching power consumption of the proposed model using 90 nm standard CMOS technology, and the results have been compared to other models such as Wallace Tree Multiplier (WTM) [3], Modified Booth Array (MBA) [4], Baugh Wooley Multiplier (BWM) [5], and Row Bypassing and Parallel Architecture (RBPA) [6]. According to the calculations, the (3232) bit multiplier has a propagation latency of only 1.06 seconds and costs 132 uW dynamic switching power.

5. VLSI IMPLEMENTATION OF RSA ENCRYPTION

RSA is a public-key cryptographic technique for network security. Computing a b mod n, where 'a' is the content and (b, n) is the public key, is one of most time-consuming stages in the RSA algorithm. In the RSA encryption and decryption algorithm, the Dhvanjanka sutra is incorporated.

When compared to RSA done using conventional multipliers and division methodologies, RSA built utilising overlay hierarchical multiplier architecture and division structure using Dhvajanka sutra of Vedic mathematics dramatically reduces processing time and delay. [8,9]

In public key cryptography, the RSA public key cryptosystem is a popular approach. RSA is the most secure top quality algorithm for network security.

R G Kaduskar [18] offers a new RSA algorithm structure based on vedic mathematics. The nikhilam and arunankavedic mathematics division techniques are used to create a new architecture for the RSA algorithm. Applying modular exponentiation operations in very large integer integers takes a long time. For these kind of computations in RSA systems, the researcher proposes using vedic mathematics. When Sutras were employed for computations, it was found to be more effective as compared to basic architectural implementation.

R Bhaskar et al. [19] increased the RSA encryption system's computation time via using vedic mathematics as well as a better restoring division approach. They used the UrdhvaTiryagbhyam sutra, which is a Vedic multiplication shortcut. For encryption / decryption, key generation takes a very long time and requires a great deal of hardware. The vedic multiplier accelerates computing speed while reducing hardware requirements.

Greeshma Liz Jose et al. [20] compared the performance of vedic multiplication and division algorithms against conventional multiplication and division algorithms based on speed, power, and area. The RSA encryption and decryption mechanism is then implemented using vedic techniques. The vedic RSA allowed RSA hardware to operate at the same speed as its software counterparts.

R ThamilChelvan et al. [21] propose using the Dhavajanka sutra in vedic mathematics for division operations to develop the RSA encryption/decryption algorithm. While comparison to multipliers and division algorithms, the RSA circuitry has shorter timing delay when performing the vedic division technique. In terms of area/speed, it is also effective.

Because of its mathematical complexity, the RSA algorithm only lags behind in regards of encryption speed. A multiplier based on vedic mathematics is utilised to boost the speed. The hardware is also quite complicated. In order to make it work with digital gear, it had to be modified. Instead of using the decimal number system, Dhanashri R Kadu et al.[22] applied the urdhvaTiryakbhyam sutra to multiply binary numbers. The goal of Shahina M. Salim's planned study is to develop and implement the RSA cryptosystem in order to increase speed, area reduction, and throughput. [17]

JainathNasreen.P and EmyRamola.P used VHDL to create a 16-bit RSA block cypher system in their paper [31, 32]. The entire procedure is divided into three parts: key generation, encryption, and decryption. The goal of the key generation stage is to generate a pair of cryptographic keys, whereupon the private key is distributed to the receiver via various key distribution algorithms. The suggested system model minimizes the memory consumption and overhead associated with key generation. At the receiver's end, the encrypted text can be decoded using the RSA secret key. They reached the conclusion that the suggested design outperforms the current one in all of the metrics studied.

Synopsis' Design Vision tool was used to obtain the analysis results. For a 16-bit input, the relevant works all feasible random numbers and stores these in memory. Prime numbers were identified and stored in a FIFO memory from the created random numbers. For encryption, the first two prime numbers in the FIFO are chosen. However, by validating for primality and selecting two prime numbers simultaneously when the random numbers are being created, the suggested architecture avoids the requirement for memories. The production also comes to a halt when the machine identifies two prime numbers.

The paper published by HimanshuThapliyal and M.B Srinivas [6] , proposed the hardware implementation of RSA encryption/decryption algorithm using the algorithms of Ancient Indian Vedic Mathematics that have been modified to improve performance. The recently proposed hierarchical overlay multiplier architecture is used in the RSA circuitry for multiplication operation. Due to its parallel and regular structure the proposed architecture can be easily laid out onsilicon chip and can work at high speed without increasing the clock frequency. It has the advantage that as the number of bits increases its gate delay and area increase very slowly as compared to RSA circuitry employing traditional multipliers and division algorithm.[32]

Modular Multiplication and Exponentiation Architectures for Fast RSA Cryptosystem,Based on Digit Serial Computation ,the paper published by Gustavo D. Sutter, Jean-Pierre Deschamps, and José Luis Imaña[33,32], in their paper, they optimized the Montgomery's multiplication and proposed architectures to perform the least significant bit first and the most significant bit first algorithms. The developed architecture has the following distinctive characteristics: 1) use of digit serial approach for Montgomery multiplication. 2) Conversion of the CSA representation of intermediate multiplication using carry–skip addition. This allowed the critical path to be reduced, albeit with a small-area speed penalty; and 3) precompute the quotient value in Montgomery's iteration in order to speed up the operating frequency. And they concluded that,CSA was used to perform large word-length additions in conjunction with quotient precomputation and digit serial computation. Another characteristic of the proposed architecture was the use of binary representation for intermediate exponentiation results and the use of efficient carry–skip addition at the end of a

Montgomery's multiplication. For fair comparison, the circuits were implemented in Virtex 2 and Virtex 5 FPGA devices and in a 0.18-µm ASIC-technologies, presenting in all technologies the best results. A technological observation is that the Xilinx Virtex 5implementation (65 nm) achieves throughput similar to a 0.18-µm ASIC technology and almost doubles the data rate of a Virtex 2 technologies (0.15 µm).

The paper proposed by K.Z. Pekmestzi, N.K. Moshopoulos [34,32], in their paper a new implementation of a Montgomery multiplier is presented, which is based on the direct approach achieving higher performance than any other realization. The circuit is modified in an elegant way in order to implement both the modular multiplication and squaring in a bitinterleaved form. The modular exponentiation requires approximately 2n2 clock cycles with the minimum hardware complexity, reported so far. The proposed design is approximately 2 and 3 times more efficient than respectively. Compared to their circuit's performance is about 20% higher. This is due to the direct implementation of the Montgomery algorithm, which yields a decrease of the circuit's complexity, equal to 19 gates per bit.

A hardware version of the RSA using the Montgomery's algorithm with systolic arrays has been proposed by Ali ZiyaAlkar, RemziyeSonmez [35,32], where they use systolic arrays, to speed up the modular multiplication and squaring, bit level systolic arrays are used with the Montgomery's modular multiplication algorithm to constitute the core of modular exponentiation operation. The squaring systolic structure is also performed in parallel with the systolic multiplication in the modular exponentiation. The novel idea in their paper was to use the systolic array cells with increased performance of up to 20% and use them in a single row organization. The final RSA design is configurable and can operate both for encryption and decryption. The results are obtained at the high-level synthesis stage and show the highest possible clock rate that can be achieved.

Dhanashri R. Kadu et.al [32] proposed a novel efficient technique for data security using the RSA lacks in encryption speed because of its mathematical calculation and to prevent this, theUrdhvatiryakbhyam sutra which is the most efficient sutra, giving minimum delay for multiplication of all types of numbers, either small or large and it eliminates unwanted multiplication steps as compared to conventional multiplication. In the paper the RSA algorithm using vedic mathematics was the prototype using VHDL and its analysis had the base on the FPGA.

6. 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. [29]

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 arraymultiplier architecture [9, 10, 11].

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 hencereduces size and power.

Anveshkumar used Urdhvatiryakbhyam Sutra of Vedic mathematics to build a power efficient multiplier in the coprocessor [12]. 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 conventisonal one.

M. Ramalatha [39] used Urdhvatiryakbhyam Sutra of Vedic mathematics to builda high speed power efficient multiplier in the co-processor. It also showed the same results that are more efficient.

7. 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 [14]. A considerable input in the point addition and doubling has been observed when implemented using proposed techniques for exponentiation.
Scalar multiplication in point addition and point doubling in ECC is the most time consuming process. Prokash Barman et al. [27] used vedic sutra for scalar multiplication. By comparing the conventional multipliers they found that the functional speed of ECC

arithmetic increased by using vedic multiplier. Shylashree.N, D et al. [28] proposed a high speed ECC using vedic mathematics. They found that proposedvedic multiplication is six times faster than the other methods previously used when applied in point doubling.

AES method of cryptography [17]

One of the crucial mathematical operations performed during AES is the mix column steps in AES. Computation of mix columns and its inverse is considered to be even more difficult task. UrdhavaTiryakbhyam sutra of vedic mathematics is used in proposed architecture for mix columns and its inverse. The architecture performs better when compared with conventional AES in terms of area.

Shrita G et al. [24] have also proposed a novel method for the mix column and inverse mix columns operation in AES cryptography. They found that by implementing the proposed system is efficient in terms of speed and area.

Kavuri Suresh et al. [27] in their paper proposed an architecture using vedic mathematics for performing mix and inverse mix column computation in AES. They achieved 100% area efficiency and a two times increase in speed by the novel algorithm, in comparison with two other popular implementations of the same.

Anjali L[26] in her paper presents a low area, cost effective AES cipher for encryption /decryption using a 128 bit iterative architecture. In this work, the amount of hardware resources has been optimized with respect to various proposed designs on alternative platforms.

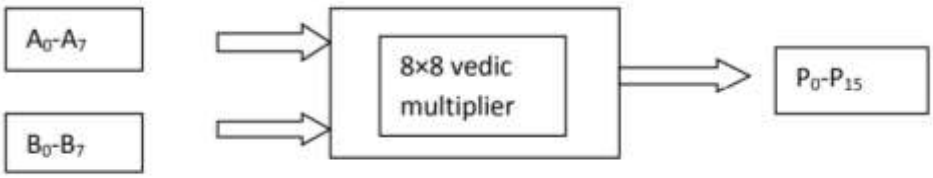
Digital Signal Processing [36]

Digital Signal processing is a technology that is present in almost every engineering discipline. It is also the fastest growing technology of the century and hence it possesses tremendous challenges to the engineering community. Faster addition and multiplication are of extreme importance in DSP for Convolution, DFT and Digital filters .The core computing process is always a multiplication routine and hence DSP engineers are constantly looking for new algorithms and hardware to implement them. The methods in Vedic Mathematics are complementary directly and easy. Mr. MangeshKarad and Mr. Chidgupkar [37s] highlight the use of multiplication process based on vedic algorithms and implemented on 8085 and 8086 microprocessors. Use of Vedic algorithms shows appreciable saving of processing time**.**

The modern multipliers process a drawback of speed in their multiplier design. The mode of multiplication operation takes more time as the number of implicates increases. Thus designing a processor for High speed multiplication is of great concern.Finite Impulse Response filters normally called as a convolution filter includes a multiplier in it. Both FIR and IIR filters can be designed using the Vedic method.The time comparison is done between Vedic method and conventional method in MATLAB Domain. The computation time taken by Vedic method is compared with the inbuilt function MATLAB. Later, the computation time is implemented by using Graphical UserInterface (GUI).GUI is a tool in Matlab and it acts as a mode of interaction between the user and the system. The results show that the UrdhwaTiryagbyam sutra reduces the execution time as compared to the inbuilt function of MATLAB. [43]

8. VEDIC MULTIPLIER

Multiplier with the use of Vedic multiplication is called as vedic multiplier. The method applied here is UrdhwaTiryagyam method. A simple block diagram below shows the 8×8 multiplier.



8. BLOCK CONVOLUTION

In DSP applications convolution with very long sequence is often required. To compute convolution of long sequence overlap add method (OLA) and overlap solve method (OLS) can be considered which are well knownefficient schemes for high order filtering.

Hanumantharaju M. C., Jayalakshami H.[38] proposed a high performance and area efficient architecture for FPGA implementation of block convolution. By using vertically and crosswise structure of vedic mathematics new multiplier architecture is developed and embedded it into OLA and OLS methods for improved efficiency. The result shows that the proposed vedic multiplier architecture achieves a significantimprovement in performance over the traditional multiplier architectures. If the bits in the number are continuously increased to N by N (N is any number) bits then Vedic Mathematics architecture shows greatest advantage as compare to other architectures of the multipliers over gate delays and regularity of structure.

9. RESULTS AND DISCUSSION

Various parameters are recommended by researchers to evaluate the performance of VedicMath 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 betweenConventional and Vedic way is shown in Table 1 [13].

10. CONCLUSIONS

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 utilization and silicon area. Various algorithm based on Vedic math 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

11. ANALYSIS OF COMPUTATIONAL COMPLEXITY OF ALGORITHMS BASED ON VEDIC MATHEMATICS.

To evaluate the performance of vedic mathematics algorithms researchers recommended various parameters such as time, delay, power and number of slices. Here we analysed computational complexity of algorithms using vedic mathematics proposed by different researchers are given in table 2:

Sr. No.	Author/Title of the paper.	Name of the cryptographic Algorithm used.	Computational complexity.
1.	R G Kaduskar et.al [18]	RSA	Efficient in time.
2.	R Bhaskar et.al [19]	RSA	Improve computation speed and efficient in hardware.
3.	Greeshma Liz Jose et.al [20]	RSA	Efficient in terms of speed and area.
4.	R Kadu et.al [22]	RSA	Reduce complexity, execution time, power etc
5.	ThamilChelvan R et.al.[21]	RSA	Efficient in time, speed and area.
6.	Shahina M. Salim et.al.[23]	RSA	Efficient in time and area
7.	SoumyaSadanandan et.al. [30]	AES	Efficient in performance and use less area.
8.	Shrita G et al.[24]	AES	Area efficient and high Speed.
9.	Suresh Kavuri et al.[27]	AES	Perform well in terms of speed and occupies less area.
10.	Anjali.L[26]	AES	Efficient in terms of area and hardware resources.

11.	Prokash Barman et al.[27]	ECC	Increase speed of arithmetic in ECC.
12.	Shylashree.N, D et al. [28]	ECC	Increase Speed of scalar multiplication.

12. CONCLUSION

In this paper, we did a comparative analysis of various researches carried out to use vedic sutras in computer algorithms with a special focus to All the researchers recommend the use of vedic shortcuts in algorithms to save hardware resources and processing time.

13. REFERENCES

[1] 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.

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

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

[4] 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.

[5] HimanshuThapliyal, Hamid R Arabnia, "A time-area-power efficient multiplier and square architecture based on ancient Indian Vedic mathematics".

[6] HimanshuThapliyal and M.B Srinivas "VLSI Implementation of RSA Encryption System Using Ancient Indian Vedic Mathematics" Proceedings of International Conference on Security Management, 2005.

[7] R. Tamil Chelvan, S. RoobiniPriya, "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.

[8] Mr.ShripadKulkarni" Discrete Fourier Transform by Vedic Mathematics".

[9] 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.

[10] Anvesh Kumar, Ashish Raman, "Small Area Reconfigurable FFT Design by Vedic Mathematics", vol 5, IEEE pp 836-838, 2010.

[11] 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.

[12] Anvesh Kumar, Ashish Raman, "Low Power ALU Design by Ancient Mathematics", vol 5, IEEE pp 862-865, 2010.

[13] Dr.S.M.Khairnar, Ms. SheetalKapade, Mr.NareshGhorpade, "Vedic Mathematics-The Cosmic Software For Implementation Of Fast Algorithms".

[14] 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.

[15] Diganta Sengupta, Mahamuda Sultana, AtalChaudhuri, "Vedivision– A Fast BCD Division Algorithm Facilitated By Vedic Mathematics", International Journal of Computer Science & Information Technology (IJCSIT, Vol 5(4), August 2013.

[16] AnchaliyaRuchi.,Chiranjeevi G .N., and SubhasKulkarni, "Efficient Computing Technique using Vedic Mathematics Sutra", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering 3(5), pp. 24-27.

[17] Lisha A, Thomas Monoth, "Analysis of cryptographic Algorithms Based on Vedic Mathematics", International Journal of Applied Engineering Research,ISSN 0973-4562 Volume 13, Number 3 (2018).

[18] R G Kaduskar , "A New Architecture for RSA Algorithm using Vedic Mathematics", 2011 Fourth International Conference on Emerging Trends in Engineering & Technology , pp.233-237.

[19] R Bhaskar, GanapathiHegde and P R Vaya, "An Efficient Model for RSA Encryption System Using Vedic Mathematics ", International Conference on Communication Technology and System Design 2011, pp.124-128.

[20] Greeshma Liz Jose, Sani John., "VLSI Implentation of Vedic Mathematics and Its Application in RSA Cryptosystem", IJIRD Vol 2(10),October 2013.

[21] R Thamil Chelvan, S RoobiniPriya, "Implementation of Fixed and Floating Point Division using Dhavajanka Sutra", International Journal of VLSI and Embedded Systems-IJVES, Vol 4(2),March-April 2013.

[22] Dhanashri R Kadu and Dr.G P Dhok.,"A Novel Efficient Technique For Data Security using Vedic Mathematics", International Journal of Application or Innovation In Engineering &Managemant(IJAIEM), Vol 4(5),May 2015.

[23] Shahina M. Salim, Sonal A. Lakhotiya.," Implementation of RSA Cryptosystem Using Ancient Indian Vedic mathematics", International Journal of Science and Research (IJSR), Volume 4 (5), May 2015, pp3221-3230.

[24] Shrita G and Basavaraj S M, "A Novel Architecture for Inverse Mix Operation in AES using Vedic Mathematics", International Journal of engineering & Research technology January 2015.

[25] Kavuri Suresh and Jagadish Reddy," Implementation of AES algorithm using UrdhwaTiryakbhyam Sutra and Galois field", International Journals and Magazine of Engineering, Technology, Management and Research, Volumn 2 (7) July 2015 pp. 1545-1550.

[26] Anjali.L ," An Efficient Hardware FPGA Implementation of AES-128 Cryptosystem Using Vedic Multiplier and Non LFSR", International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 3(5), August 2014.pp.842-846.

[27] Prokash Barman, BananiSaha,"An Efficient Elliptic curve Cryptography Arithmetic Using NikilamMultiplication".,The International Journal of Engineering and Science. Vol4(4). Pp.45-50,2015.

[28] Shylashree.N, D. VenkataNarayana Reddy and V. Sridhar," Efficient Implementation of Scalar Multiplication for Elliptic Curve Cryptography using Ancient Indian Vedic Mathematics over GF (p)", International Journal of Computer Applications Volume 49(7), July 2012.pp.46-50 .
[29] Chilton Fernandes, Samarth Borkar, "Application of Vedic Mathematics In Computer Architecture", International Journal of Research in Engineering and Science (IJRES) ,ISSN (Online): 2320-9364, ISSN (Print): 2320-9356, Sep. 2013.
[30] Soumya Sadanandan, Anjali," Design of advanced encryption standard using Vedic Mathematics",International Journal of Innovative Research in Advanced Engineering (IJIRAE) Vol 1 (6), July 2014.
[31] Jainath Nasreen.P, Emy Ramola.P , A Novel Architecture for VLSI Implementation of RSA Cryptosystem , 2012 IEEE.
[32] Dhanashri R. Kadu , Dr.G.P.Dhok, "A NOVEL EFFIECIENT TECHNIQUE FOR DATA SECURITY USING VEDIC MATHEMATICS", International Journal of Application or Innovation in Engineering & Management (IJAIEM),ISSN 2319 – 4847,Volume 4, Issue 5, May 2015.
[33] Gustavo D. Sutter, Jean-Pierre Deschamps, and José Luis Imaña, Modular Multiplication and Exponentiation Architectures for Fast RSA Cryptosystem,Based on Digit Serial Computation, IEEE Transactions on industrial electronics, VOL. 58, NO. 7, JULY 2011
K.Z. Pekmestzi*, N.K. Moshopoulos, A bit-interleaved systolic architecture for a high-speed RSA system 19,October 2001.
[34] Ali ZiyaAlkar, RemziyeSonmez, A hardware version of the RSA using the Montgomery's algorithm with systolic arrays, 2004.
[35] Dr.S.M.Khairnar,Ms. Sheetal Kapade, Mr.Naresh Ghorpade, "VEDIC MATHEMATICS-THE COSMIC SOFTWARE FOR IMPLEMENTATION OF FAST ALGORITHMS".
[36] P. D. Chidgupkar and M. T. Karad, "The Implementation of Vedic Algorithms in Digital Signal Processing", Global J. of Engg. Edu., Vol.8, No. 2, pp. 153-158, 2004.
[37] Hanumantharaju M. C., Jayalakshami H., Renuka R, Ravishankar M., "High Speed Block Convolution using Ancient IndianVedic Mathematics", Proceedings of International Conference on Computational Intelligence and Multimedia Applications, 2007.
[38] M. Ramalatha, K. Deena Dayalan, P. Dharani, " High Speed Energy Efficient ALU Design using Vedic Multiplication Techniques" ACTEA, IEEE pp 600-603.
[39] P.Saha, A. Banerjee, A. Dandapat, P. 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.
[40] H. D. Tiwari, G. Gankhuyag, C. M. Kim, and Y. B. Cho, "Multiplier design based on ancient Indian Vedic Mathematics," Proc. IEEE International SoC Design Conference, pp. 65-68, Nov. 24-25, 2008.
[41] P. Saha, A. Banerjee, P. Bhattacharyya, and A. Dandapat, "High Speed ASIC Design of Complex Multiplier Using Vedic Mathematics", Proc. (Abstract) IEEE TechSym 2011, pp. 38-38,Jan 14-16.
[42] Kavita.H.Dharmannavar , Mrs.Dharmambal , "THE APPLICATION OF VEDIC MATHEMATICS FOR HIGH SPEED MULTIPLIER IN FIR FILTER DESIGN", International Journal of Engineering Research and General Science Volume 3, Issue 3, Part-2 , May-June, 2015 ISSN 2091-2730.

