A review on "high speed complex multiplier using Vedic Mathematics: an effective tool"

[1]Mahesh Warang, [2]Anushri Tambe

[1]Dept. of Electronics &Telecommunication VESIT Chembur (Mumbai), India
[2]Dept. of Basic Sciences & Humanities DBIT Kurla(Mumbai), India

Abstract— Vedic mathematics is an amazing system and a unique technique of calculations. Traditionally complex multiplier provides less speed, also in some technical areas tedious computations are involved which are time consuming and it increases hardware complexity. We can resolve all these issues using Vedic mathematics. In this paper we attempt to explore different areas in engineering where we can use Vedic mathematics as an effective tool.

Keywords— Vedic Mathematics, Cryptography, Encryption, Decryption, Time Complexity, Urdhva Tiryagbhyam sutra, FFT

I. INTRODUCTION

The term Vedic Mathematics, is coined by 'Jagadguru Shankaracharya Shri Bharati Krishna Tirthaji for the methods he developed for faster and simpler calculation techniques. His methods are based on 16 sutras from Vedas and 16 upasutras, one each for the main sutras. Swamiji interprets those sutras in various contexts such as addition, multiplication, division, recurring decimals, factorization of polynomials etc. to make them easier. Vedic Mathematics is used all over the world even in higher Engineering Mathematics. It deals with mainly carrying out tedious and cumbersome arithmetical operations [1].

In cryptosystem, encryption of data to be transmitted is always a major concern in wireless communication system. Encryption is important to secure data such that it is received with full integrity at the receiver's end. In case of data encryption and decryption we require large number of calculations [2]. Similarly complex multiplication is of immense importance in Digital Signal Processing (DSP), image processing (IP) and embedded system. To implement hardware module in Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT), Discrete Sine Transformation (DST) and modern broadband communications large number of complex multipliers are required. Hence by using Vedic Mathematics in respective fields one can enhance the speed.

II. URDHVA-TIRYAK SUTRA

Urdhva Tiryagbhyam sutra is the general formula applicable to all cases of multiplication and it is also useful to find division of large number by large number [1]. Urdhva Tiryagbhyam means vertically and crosswise.

Eg.

1)

```
      2  1
    x 2  3
  ----------------------------------
   (2x2) : (2x3+2x1) : (3x1)
     4   :     8     :   3
  Hence, 21x23 = 483
```

2)

```
        2   5   2
      x 2   4   3
-------------------------------------------------------------
(2x2):(2x4 + 5x2):(2x3 + 5x4 + 2x2):(5x3 + 2x4):(2x3)
  4  :    18     :        30        :     23    :  6

        48036
       +132        →Carry
     ------------------------------
        61236
  Hence, 252 x 243 = 61236
```

In general for large numbers we can apply Urdhva Tiryagbhyam sutra in following way:

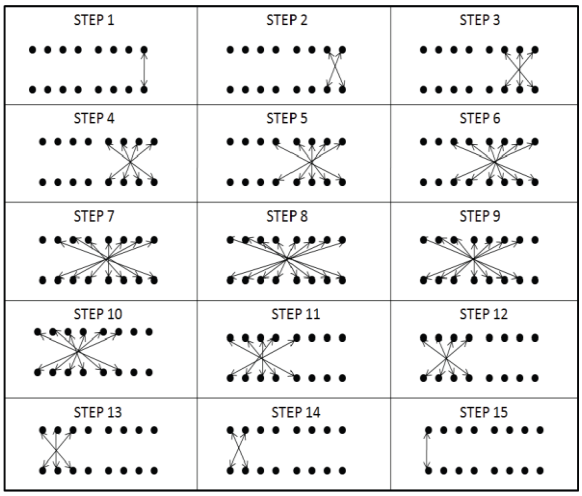

Fig.1 Urdhwa Tiryakbhyam Sutra for multiplication of 8 digit number

III. CRYPTOGRAPHY

In wireless communication encryption of data that is to be transmitted is major concern. This is mainly due to the confidentiality of the data at sender's as well as receiver's end [3]. Cryptography is one such encryption process which is widely used to secure data. It involves encryption of data to be transmitted by means of unique keys for encryption and decryption which are known to authorize person. In recent time several cryptographic algorithms have been discovered giving importance to the problem of vulnerability of the algorithms especially in application which demands high security i.e. for Smartcards, ATM etc [4]. Following algorithms play very important role in cryptography.

A. RSA Algorithm

RSA algorithm is asymmetric key cryptographic algorithm. It is based on mathematical fact that it is easy to find and multiply the large prime numbers together but, it is extremely difficult to factor their product. The public and private keys in RSA are based on very large prime numbers i.e. numbers around 100 to 150 decimal digits [5]. In this situation multiplication and division by conventional method consumes considerable amount of time and hardware for encryption and decryption of data. Hence, to increase computational speed with minimum hardware Vedic Mathematics is useful. The main advantage of Vedic multiplier (Urdhva Tiryagbhyam sutra) is that it calculates the partial products in one single step. By replacing present multiplier architecture by Urdhva Tiryagbhyam sutra along with improved restoring division algorithm saves the time and hardware [6].

B. Advanced Encryption Standard(AES)

AES is symmetric key cryptographic algorithm. It has higher immunity towards brute-force attack hence it is most preferred method. This algorithm involves several complex operations implemented in Galois Field (GF-2^8) [7]. These complex operations are iterative in nature which in turn disturbs the speed of the encryption system and hence increases the vulnerability. AES algorithm also requires mix columns and inverse mix columns transformation. Galois field multiplication is also required during mix column step which is crucial and power hungry operation causes the computation even more difficult. In order to make this process easier Urdhva Tiryagbhyam Sutra is used. In VLSI / FPGA perspective, Vedic mathematics along with improved architecture for mix columns and its inverse, performs extremely well in terms of speed and occupies less area[3],[8],[9].

IV. FAST FOURIER TRANSFORM

Digital signal processing (DSP) is widely used almost in every engineering technology. DSP needs faster additions and multiplications which are highly important for convolution, Discrete Fourier Transform (DFT), digital filters etc. FFT is one of the fundamental operations that is typically performed in DSP system. It is computationally intensive DSP function widely used in applications such as imaging, instrumentation, wireless communication, software define radio etc. To increase the efficiency in FFT, Urdhva Tiryagbhyam Sutra again plays an important role. Hence reconfigurable FFT designed by Vedic Mathematics has high speed and small area as compared to the conventional FFT. [10]

V. ARRAY OF ARRAY MULTIPLIER

Array of Array multiplier is a derivative of Braun array multiplier which is much suitable for VLSI implementation because of its less space complexity though it shows larger time complexity. On the other hand tree multipliers have time complexity of order log(n) but are less suitable for VLSI implementation; since they show higher space complexity. The main advantage of 'Array of Array' multiplier is its inherent ability to reduce both time and space complexity. Using Vedic multiplication i.e. Urdhva Tiryagbhyam sutra optimization of 16 X 16 'Array of Array' multiplier circuit designed with hierarchical structuring is possible; which results in reduction of average power dissipation and time delay [11].

VI. CONCLUSION

Vedic Mathematics is an effective tool to increase computational speed and efficient method to reduce time complexity. In this paper we have discussed use of only one sutra 'Urdhva Tiryagbhyam sutra'. In future the use of other sutras can also be explored. In this age where speed of the processor is very important, more and more efficient designs for adder and multiplier units are required. Vedic Mathematics can be effectively used

with improved architectures and modern tools for this purpose.

ACKNOWLEDGMENT

We would like to thank Shriprasad Tambe for helping us out for this paper. Also we would like to thank Swami Bharati Krishna Tirthaji for the wonderful mathematics that he created. His sutras will continue to inspire us and several others to explore their applications in modern technologies.

REFERENCES

[1] Jagadguru Swami Sri Bharati Krisna Tirthaji Maharaja, "Vedic Mathematics: Sixteen Simple Mathematical Formulae from the Veda," pp.5-45, Motilal Banarasidas Publishers, Delhi, 2009.

[2] William Stallings, "Cryptography and Network Security: Principles and Practice",3rd ed. Pearson Education, 2002.

[3] Sushma R Huddar, Sudhir Rao Rupanagudi, Ramya Ravi, Shikha Yadav, " Novel Architecture for Inverse Mix Columns for AES using Ancient Vedic Mathematics on FPGA" International Conference on Advances in Computing , communications and Informatics(ICACCI) on. IEEE, 2013.

[4] Knudsen, Lars R., and Matt JB Robshaw, "The Block Cipher Companion", Springer , 2011.

[5] R.Bhaskar, Ganpathi Hegde, P.R. Vaya, "An Efficent Hardware Model for RSA Encryption system using Vedic Mathematics", International Conference on Communication Technology and System Design, Published by Elsevier Ltd. 2011.

[6] Shahina M. Salim, S.A. Lakhotiya, "A Review on Implementation of RSA Cryptosystem Using Ancient Indian Vedic Mathematics", International Journal on Recent and Innovation Trends in Computing and Communication, Vol.3m, Issue1, Jan 2015.

[7] Rachh, Rashmi Ramesh, PV Ananda Mohan, B.S. Anami, "Efficient Implementaion for AES Encryption and Decryption", Circuits, Systems and Signal Processing 31, no. 5 (2012):1765-11785.

[8] Ambika R, C S Mala, S K Pushpa, "FPGA Implementation of AES using Vedic Mathematics ", International Journal of Innovative Research in Science and Engineering(IJIRSE) 2347-3207.

[9] Soumya Sadanandan, Anjali V., "Design of Advanced Encryption Standard using Vedic Mathematics", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Vol.1, Issue 6, July 2014.

[10] Ashish Raman, Anvesh Kumar, R.K. Sarin, "High Speed Reconfigurable FFT Design by Vedic Mathematics", Journal of Computer Science and Engineering, Vol.1, Issue 1, May 2010.

[11] Dr. K.S. Gurumurthy, M.S. Prahalad, "Fast and Power Efficient 16 x 16 Array of Array Multiplier using Vedic Mathematics" unpublished.