# A LITERATURE SURVEY ON ANCIENT INDIAN VEDIC MATHEMATICS SUTRAS FOR ELLIPTIC CURVE CRYPTOGRAPHY

**Manoj Kumar[1], Ankur Kumar[2]**
[1, 2] Department of Mathematics and Statistics,
Gurukula Kangri Vishwavidyalaya, Haridwar (Uttarakhand) 249404, INDIA
Email id: [1]sdmkg1@gmail.com , [2]ankurgkv99@gmail.com
[2]Corresponding author: Ankur Kumar[2], Email Id: [2]ankurgkv99@gmail.com

***Abstract*—** This survey paper on Ancient Indian Vedic Mathematics (AIVM) sutras for Elliptic Curve Cryptography (ECC) describes some efficient computing techniques of AIVM for ECC. Vedic Mathematics is the ancient methodology of Indian Vedic Mathematics which has unique and best computational sutras for calculations which are based on sixteen sutras and fourteen sub-sutras or formulae. The application of AIVM Sutras save a lot of time and effort in solving the problems as compared to formal methods. This survey, describes useful sutras of AIVM such as, Dvandva-Yoga (DY) Sutra for square of the n-digits number, Urdhva-Tiryagbhyam (UT) Sutra for multiplication of the of n-digits number, Nikhilam Navatashcaramam Dashatah (NND) Sutra for multiplication of n-digits number (base number ten or multiple of number ten) and Dhvajanka sutra is best for any division. In this literature survey, we conclude that, the time consuming can be reduced and hardware complexity can be increased by using AIVM sutras and these sutras or techniques speed up the processing of cryptographic operations such as point addition, point doubling, encryptions and decryptions. The AIVM Sutras have applied in Cryptography such as ElGamal cryptosystem, RSA cryptography, ECC and many more branches of mathematics for best performances. This paper shows a literature survey on ancient Indian Vedic Mathematics sutras for elliptic curve cryptography and motive of this approach is the survey of novel research in the present time and last two decade in the field of cryptography and Vedic Mathematics.

*Keywords— Dvandva-Yoga, Urdhva-Tiryagbhyam, Dhvajanka, Nikhilam Navatashcaramam Dashatah, Vedic Mathematics, Elliptic Curve Cryptography, Point addition, Point doubling.*

## *I. Introduction*

Vedic Mathematics is a great approach and it is so beneficial in all branches of Mathematics. Veda word has come from Sanskrit language and it means 'to know without limits'. Vedic Mathematics is an ancient system of Mathematics existed in India. It is a system of Mathematics consisting of a list of sixteen sutras and fourteen sub-sutras. Vedic Mathematics was reconstructed from the Ancient Indian Vedas by Swami Bharti Krishna Tirthaji Maharaja in the early 20th century (1884-1960). Vedic Mathematics includes mathematical sutras or formulae which can be applied in different branches of mathematics. The conventional mathematical algorithms are simplified and also optimized by using Vedic sutras. The words Sutra is an aphorism or a formula. The word up-sutra is sub-sutra or a corollary. The AIVM Sutras covers almost every useful branch of Mathematics. The application of the AIVM Sutras is completely logical, rational and saves a lot of time and effort in solving the problems, compared to the traditional methods. Vedic sutras can be applied efficiently in calculus, plain, geometry, trigonometry, conic section, elliptic curve cryptography, numerical analysis and many more branches of mathematics, in the mathematical problem it works like magic. From the last decade, the demand of image, digital signals processing, and many computational applications needs faster computation by any processor. In a large number of arithmetic operations like, division, multiplication, square, cube, addition, subtraction is required in cryptographic applications. Number of squares, multiplications, cubes and divisions are the arithmetic operations which require heavy calculations in all mathematical branches. Traditional and conventional methods for doing these operations take so much time in processing. These traditional methods include Array, Booth, Carry Save, Wallace Tree and many more multiplier. Architectures based all these methods are not very efficient in terms of speed, area, and power. AIVM based multipliers involve fewer steps to solve multiplication than traditional multiplication. AIVM sutras help to achieve optimization at all levels of design of digital systems reducing power consumption. Vedic mathematics based multipliers are efficient in terms of speed, power, and area. In this paper, we reviewed various papers in which AIVM sutras used for designing multiplier. The AIVM sutras based multiplication and division calculations can be applied in many computer algorithms and various researches are carried out towards the usage of them. Multiplication and division are the most important operation in cryptography algorithms. Reduced operation and steps in calculations of multiplications, cubes, squares, and divisions will increase the speed of the algorithms. Dvandva-Yoga, Urdhva-Tiryagbhyam, Dhawajanka and Nikhilam Navatashcaramam Dashatah sutra in Vedic mathematics are efficient for square, multiplication and division. The AIVM sutras and sub-sutras are explained in **[8]** as under:

| S. N | AIVM Sutras and sub-sutras | | |
|---|---|---|---|
| | ***NAME OF SUTRAS*** | ***COROLLARY/ SUB-SUTRAS*** | ***MEANING*** |
| 1 | Ekadhikina Purvena | Anurupyena | By one more than the previous one |
| 2 | Nikhilam Navatashcaramam Dashatah (NND) | Sisyate Sesasamjnah | All from 9 and the last from 10 |
| 3 | Urdhva-Tiryagbhyam | Adyamadyenant yamantyena | Vertically and crosswise |

| S. N | AIVM Sutras and sub-sutras | | |
|---|---|---|---|
| | *NAME OF SUTRAS* | *COROLLARY/ SUB-SUTRAS* | *MEANING* |
| 4 | Paraavartya Yojayet | Kevalaih Saptakam Gunyat | Transpose and adjust |
| 5 | Shunyam Saamyasamuccaye | Vestanam | When the sum is the same that sum is zero |
| 6 | Anurupye or Shunyamanyat | Yavadunam Tavadunam | If one is in ratio, the other is zero |
| 7 | Sankalana-Vyavakalanabhyam | Yavadunam Tavadunikritya Varga Yojayet | By addition and by subtraction |
| 8 | Puranapuranabyham | Antyayordashake'pi | By the completion or non-completion |
| 9 | Chalana-Kalanabyham | Antyayoreva | Differences and Similarities |
| 10 | Yaavadunam | Samuccayagunitah | Whatever the extent of its deficiency |
| 11 | Vyashtisamanstih | Lopanasthapanabhyam | Part and Whole |
| 12 | Shesanyankena Charamena | Vilokanam | The remainders by the last digit |
| 13 | Sopaantyadvayamantyam | Gunitasamuccayah Samuccayagunitah | Gunitasamuccayah Samuccayagunitah |
| 14 | Ekanyunena Purvena | Dhvajanka | By one less than the previous one |
| 15 | Gunitasamuchyah | Dvandva-Yoga | The product of the sum is equal to the sum of the product |
| 16 | Gunakasamuchyah | Adyam Antyam Madhyam | The factors of the sum is equal to the sum of the factors |

**Table (1). AIVM Sutras and sub-sutras**

### *A. Dvandva-Yoga*

For squaring by the Dvandva-Yoga, any binary or decimal number, a purposeful architectonics can rise up its performance and best output than other architecture's multiplier. Using Dvandva-Yoga $(D_Y)$ algorithm and rule for squaring of binary or decimal numbers from the AIVM Sutras is explained as **[8]**:

- To calculate Dvandva-Yoga $(D_Y)$ of a number which contains single digit Dvandva-Yoga expressed that it is the square of that number, Dvandva-Yoga of $p_1$ is $p^2$.
- To calculate Dvandva-Yoga $(D_Y)$ of a number which contains two digits, Dvandva Yoga expressed that, it's double the multiplication of both digits of that number, Dvandva-Yoga of $p_1q_1$ is $2 * p_1 * q_1$.
- To calculate Dvandva-Yoga $(D_Y)$ of numbers which contain three digits, Dvandva-Yoga expressed that, it's got double the product of first and third number and gives the square of that number which is placed in the middle, Dvandva-Yoga of $p_1q_1r_1$ is $2 * p_1 * r_1 + q_1^2$.

**Example (1). Square of six-bit binary number (101101) by Dvandva-Yoga Sutra.**

STEP 1: $D_Y(1) = 1*1 = 1$
STEP 2: $D_Y(10) = 10*1*0 = 00$
STEP 3: $D_Y(101) = 10*1*1+0*0 = 10$
STEP 4: $D_Y(1011) = 10*1*1+10*1*0 = 010$
STEP 5: $D_Y(10110) = 10*1*0+10*0*1+1*1 = 001$
STEP 6: $D_Y(101101) = 10*1*1+10*0*0+10*1*1 = 100$
STEP 7: $D_Y(01101) = 10*0*1+10*1*0+1*1 = 001$
STEP 8: $D_Y(1101) = 10*1*1+10*1*0 = 010$
STEP 9: $D_Y(101) = 10*1*1+0*0 = 10$
STEP10: $D_Y(01) = 10*0*1 = 00$
STEP11: $D_Y(1) = 1*1 = 1$
Answer is 1/00/10/010/001/100/001/010/10/00/1
=1111101001

**Example (2). Square of five-bit decimal number (12345) by Dvandva-Yoga Sutra.**

STEP1: $D_Y(5) = 5^2 = 25$
STEP 2: $D_Y(45) = 2(4\times5) = 40$
STEP 3: $D_Y(345) = 2(3\times5) + 4^2 = 46$
STEP 4: $D_Y(2345) = 2(2\times5) + 2(3\times4) = 44$
STEP 5: $D_Y(12345) = 2(1\times5) + 2(2\times4) + 3^2 = 35$
STEP6: $D_Y(1234) = 2\times(1\times4) + 2(2\times3) = 20$
STEP 7: $D_Y(123) = 2(1\times3) + 2^2 = 10$
STEP 8: $D_Y(12) = 2(1\times2) = 4$
STEP 9: $D_Y(1) = 1^2 = 1$
Answer is 152399025.

### **B.** *Urdhva-Tiryagbhyam*

The Sutras of Ancient Indian Vedic Mathematics (AIVM) is using enormously in the research area of Mathematics. For multiplication we have used AIVM sutra, Urdhva-Tiryagbhyam which gives the best output in the operations of ECC. This Sutra reduces bits and steps in multiplication and saves much time in encryption and decryption of ECC. Compression between AIVM based multiplier, name is Urdhva-Tiryagbhyam and other multipliers, name is Booth, Array and many more, we observed that AIVM multiplier has not much delay and save time and power in the ECC operations, Naturally by the use of standard or classical method in multiplication we can get results but number of operation in classical method is too high almost operations for m bit digit integers so it looks complicated. Another multiplication method is the Karatsuba method [5] it requires the number of operation is for two integers of m-bit. So this is a complicated method of multiplication and other is Karatsuba technique (method) gives slow output for a small input in any operations comparatively classical technique (methods) of multiplication due to the repetition of overhanging operations. To manipulate this type of issue best sutra of AIVM

Urdhva-Tiryagbhyam technique for multiplications can be applied and get the best result easily **[8]**.

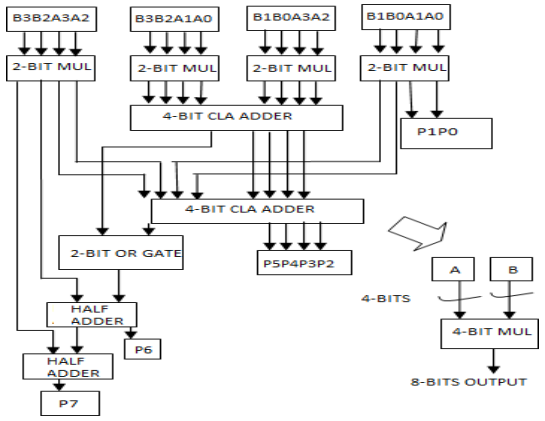


**Figure. (1): The design of 4-bit multiplier [[16]**

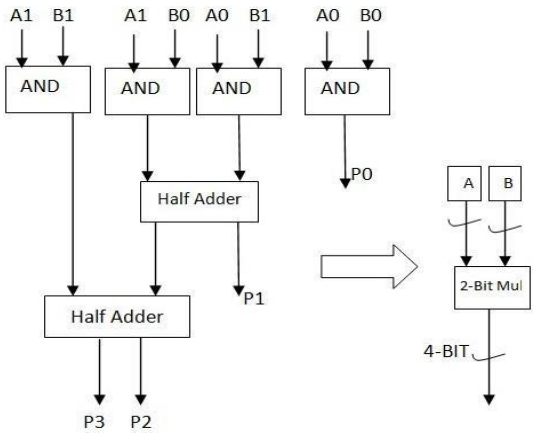


**Figure. (2): The design of 2-bit multiplier [16]**

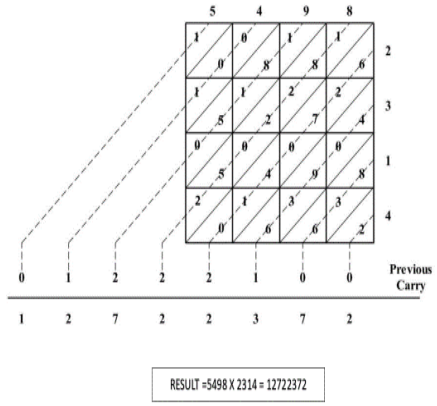


**Figure (3). 4-bit binary multiplication [16]**

*C. Nikhilam-Navatashcaramam Dashatah*

Nikhilam Sutra in Vedic Mathematics can be used as shortcuts to multiply numbers, divide numbers in faster approach. In English, it is translated as All from 9 and last from 10[9] i.e. subtract last digit from 10 and rest of digits from 9. Multiplication using Nikhilam Sutra is used when numbers are closer to the power of 10 i.e. 10, 100, 1000, etc. The procedure is as follows:

- Numbers are below the base number.
- Numbers are above the base number.
- One number is above the base and the other number is below it.
- Numbers are not near the base number, but are near a multiple of the base number, like 20, 30, 50,250,600, etc. Numbers near different bases like multiplier is near to different **[8]**.

*Types of NND Sutras***:**

- This type of Nikhilam Sutra can be applied when numbers slightly* less than power of 10 (10, 100, 1000, etc.).

$$Formula\ used: (x-a)(x-b) = x(x-a-b) + ab$$

- Numbers slightly* greater than power of 10 (10, 100, 1000, etc.).

$$Formula\ used: (x+a)(x+b) = x(x+a+b) + ab$$

- Numbers closer to* & present on either side of power of 10 (10, 100, 1000, etc.). This type of Nikhilam will require understanding of 2.

*Formulas used :-*

- $(x+a)(x-b) = x(x+a-b) - ab$
- $(x-a)(x+b) = x(x-a+b) - ab.$

*Examples of Binary Multiplications by NND sutra are below:*

| | Integer | Base Difference |
|---|---|---|
| **Multiplicand** | 107 | 100-107= -7 |
| **Multiplier** | 109 | 100-109= -9 |
| **Computation** | 107-(-9)=(109-(-7))=116 | (-7)x(-9)=63 |
| | 116 | 63 |
| **Result** | 11663 | |

**Table (2). Decimal Multiplication of 107 * 109**

| | Integer | Base Difference |
|---|---|---|
| **Multiplicand** | 11 | 11-10= 1 |
| **Multiplier** | 11 | 11-10= 1 |
| **Computation** | 11+1=100 | (1)x(1)=1 |
| | 100 | 1 |
| **Result** | 1001 | |

**Table (3). Binary Multiplication of 11*11**

| | Integer | Base Difference |
|---|---|---|
| **Multiplicand** | 101 | 101-100= 1 |
| **Multiplier** | 110 | 110-100= 10 |
| **Computation** | 101+10=111 | (10)x(1)=10 |
| | 111 | 10 |
| **Result** | 11110 | |

**Table (4). Binary Multiplication of 101*110**

*D. Dhvajanka Sutra for Division*

The Sutra, Dhvajanka is the sub-sutra of AIVM sutras which express that 'on the top of the flag', is an observed technique for division. It is stand on the Urdhva-Tiryagbhyam sutra. The six steps of Dhvajanka sutra is disposed down **[8]**:

1. The dividend and divisor are fix up in the form displayed down. Single leftmost digit or figure of divisor is left separately. Dividend is marked in a pair of part, first is right part which recognize number of figures equal to digits in divisor. Divisor, dividend, and quotient is represented by symbol d, 'X' and 'A' respectively.
2. Only first figure or digit of dividend is divided by the left out digit, remainder and quotient of this division are noted.
3. During next iteration remainder from one-time past iteration is used with next figure (digit) of dividend. Quotient figures and dividend figures without leftmost figure are multiplied in vertically and crosswise aspect. This product is subtracted from number formed by combination of remainder and figure of remainder.
4. Number left after subtraction in step three is divided by left out figure of divisor quotient is notable and remainder is prefixed with rest of the figures of dividend.
5. This procedure is move ahead till look-alike number of quotient figures equal to the figures in left part of dividend is collected.
6. Remainder is collected by subtraction of right part of dividend prefixed by last remainder and cross multiplication of quotient and divisor. This sutra gives same results or output whether applied to small or large divisors.

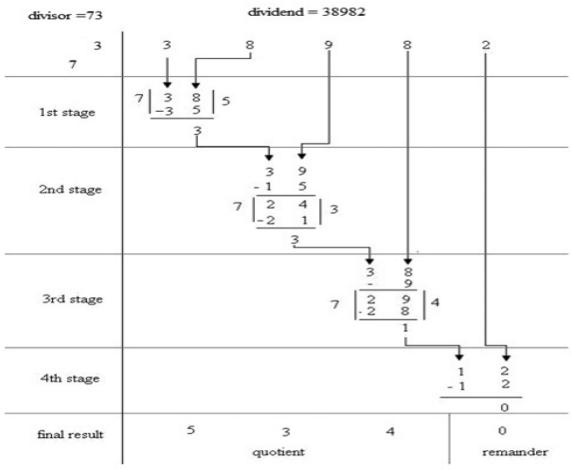


**Figure (4). Dhvajanka sutra for division [14]**

## II. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is public key cryptography in which each device or user taking part in the communication usually a couple of keys, first is a public key and other is a private key and for cryptographic operations, a well-set of operations correlated with the keys. A private key can be used only by the particular user and public key can be used by the all user who took part in the communication and also, in this section, we will through some light on basic nomenclature arithmetic background of ECC. Following symbols are used to define elliptic curves **[5, 6, 22]**:

- $GF(p)$ is Galois Field over prime $p$.
- $p$ is a prime number greater than three.
- $a, b$ is fixed real number.
- $(x, y)$ is the point on the elliptic curve $E$

Using the above terminology, the elliptic curve $E$ defined [11] as the set order pair $(x, y)$ on the curve $y^2 = x^3 + ax + b \pmod p$ pleasing the discernment equation $4a^3 + 27b^3 \neq 0 \pmod p$.

Set-theoretically an elliptic curve can be represented as:

$$E = \{(x, y) : y^2 = x^3 + ax + b \pmod p \; and \; 4a^3 + 27b^3 \neq 0 \pmod p\}.$$

The elliptic curve $E(F_p)$ explained as **[7]:**

- The additive identity property explained as: $P + O = O + P$ where $P$ belongs to $E(F_p)$.
- The additive inverse property explained as: $(x, y) + (x, -y) = O$ where $(x, y)$ belongs to $E(F_p)$.
- The sum of two distinct points $P + Q$ is $R$ where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ is $R$ $(x_3, y_3)$ in this where $x_3, y_3, \lambda$ are $\{(\lambda^2 - x_1 - x_2), (\lambda(x_1 - x_3) - y_1), (y_2 - y_1)/(x_2 - x_1)\}$ respectively.
- Thre point doubling of a point $P(x_1 y_1)$ is $R(x_3 y_3)$ in this where $x_3, y_3, \lambda$ are $\{(\lambda^2 - 2x_1), (\lambda(x_1 - x_3) - y_1), (3x_1^2 + a)/2y_1\}$ respecti vely.

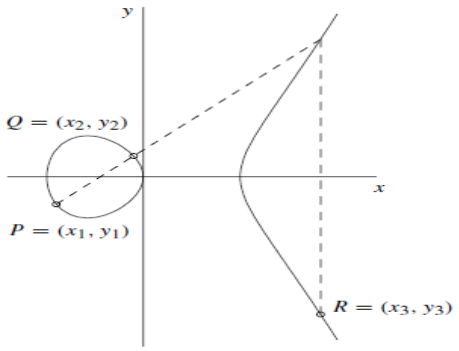


**Figure (5). Addition (R = P+Q) [7]**

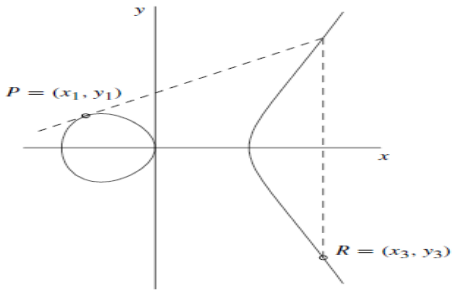


**Figure (6). Doubling (R = 2P) [7]**

## III. RELATED WORK

In this section, we will discuss the review or survey done by researchers on the AIVM sutras for ECC or cryptographic applications. J. Muthukuru and B. Sathyanarayana **[7]** in 2012, have proposed in his survey of ECC implementation for the smart card and it is observed that the performance of ECC based work gives better result than DSA and RSA in term of low memory, smaller key size, timing consumption and low power. In this survey paper, he comparing ECC with PKC schemes, measured performance of public-key algorithms and also ECC implementation details on the smart card. K. Verma and H. Agarwal **[11]** in 2013, have explained in his survey of ECC with various methods and it is observed that ECC based devises do not require much storage, power, memory, and bandwidth than other public key systems (PKS). In 2013, R. Markan and G. Kaur **[15]** have proposed in his survey on ECC techniques of encryption that the ECC provides greater security and more efficiency in performance than other public key techniques. S. Agarwal and V. K. Magraiya **[17]** in 2014 have explained in his review on Vedic Mathematics Multiplier that Urdhva-Tiryagbhyam and Nikhilam sutras of Vedic Mathematics improve the computational skill of the researchers and results gives the best output in term of speed and accuracy. In 2014, S. Jain and V.S. Jagtap **[19]** described in his survey on Ancient Indian Vedic Mathematics (AIVM) in computers processing that Urdhva-Tiryagbhyam and Nikhilam sutras of AIVM require less power, time and give faster results and they survey of various designed multipliers using AIVM. In 2014, also by C. Thomas et al **[4]** determined in his survey on the different algorithm for ECC that, the ECC with Karatsuba Multiplier gives high speed, minimum area (save 51 %), minimum time (save 46 %) and reduce the number of the clock cycle in the hardware implementation of algorithms. K. M. Gaikwad and M. S. Chavan **[9]** in 2015 considered in his review paper that the AIVM sutras can be used for fast signal processing and results give an improvement in speed reduction in consumption of power, area, and complexity, etc. S. M. Salim and N. N. Mandaogade **[20]** in 2015 intended in his review that implementation of RSA (Rivest, Shamir, Adleman) cryptography using AIVM sutras. They explained in his review paper about the time variation and cost variation in cryptographic operations to maintaining the integrity of data or information. In 2016, M. Warang and A. Tambe **[12]** proposed in his that high-speed complex multiplier with AIVM sutras is an effective tool and AIVM is so effective a tool it helps to reduce so much time and increase computational speed. In this approach, they have explained the use of Urdhva-Tiryagbhyam sutra for multiplications in cryptographic operations. A survey of cryptography and ECC by S. D. Pinagle **[18]** in 2016 in which well described cryptography and ECC with defining the model problem for prime curves and implementation of the result by 'C' programming. A review of AIVM sutras by S. Shembalkar **[21]** in 2017, they explained sixteen sutras of AIVM such as Urdhva-Tiryagbhyam, Nikhilam, and Dvandva-Yoga so on and the result is seen to be faster processing in speed and fewer areas in circuits. A review of AIVM sutras for ECC with VLSI design by A. Singh and N. Gupta **[3]** in 2017, they proposed in his paper, that the VLSI design based on AIVM sutras give better speed and so high power efficiency. A survey on squaring using AIVM sutra like, Yavadunam, Dvandva-Yoga, and Ekadhikina-Purvena by A. Deepa and C. M. Marimuthu **[1]** in 2018. They explained squaring by AIVM sutras for digital signals and cryptographic operations and results show excellent performance in processing and reduce the delay. An analysis of AIVM based cryptography algorithms by A. Lisha and T. Monoth **[2]** in 2018, they proposed about performance analysis of AIVM sutras based algorithms and results show these algorithms save processing time and hardware resources.

## IV. SURVEY OUTCOMES

After the search, we collect the data and seems that a lot of work done by the researchers in the past decade as figure (10) depicts that conferences and workshops are done in a good number, to encourage the research persons in the area of ECC (Elliptic Curve Cryptography) using AIVM (Ancient Indian Vedic Mathematics) Sutras there were numerous of organizations which conduct these workshops and conferences to boost the research, and came to know the problems and their solutions which found by the different researchers. The most significant sources which conduct workshops and conferences are AIVM based ECC from where we collect more than 50 papers on different topics. In this stream, as we searched different papers and came to know that all these methods and techniques proposed by the number of authors based on theory problems no practical problem came into light, but in the past decade industries played an excellent role in this area, which gave a real platform to the researchers, where they face the actual problem and find their solution in term of methods and techniques in some cryptographic operation studies done by some authors.

| Years / Publications | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Conferences | 0 | 2 | 1 | 3 | 2 | 2 | 3 | 4 | 2 | 3 | 5 | 6 | 7 | 6 | 5 | 4 | 2 | 57 |
| Symposium | 0 | 1 | 0 | 1 | 0 | 1 | 2 | 2 | 2 | 2 | 3 | 2 | 3 | 1 | 1 | 2 | 1 | 24 |
| Workshop | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 2 | 3 | 1 | 2 | 2 | 1 | 28 |
| Papers (ECC &AIVM) | 3 | 6 | 6 | 4 | 5 | 6 | 12 | 10 | 14 | 12 | 12 | 10 | 12 | 11 | 10 | 12 | 15 | 160 |
| Journals | 3 | 5 | 4 | 2 | 3 | 3 | 5 | 4 | 6 | 3 | 4 | 5 | 6 | 5 | 5 | 7 | 6 | 76 |
| Total | 6 | 15 | 13 | 11 | 11 | 13 | 24 | 22 | 26 | 22 | 27 | 25 | 31 | 24 | 23 | 27 | 25 | --- |

**Table (5). Research work published in different years (2003-2019)**

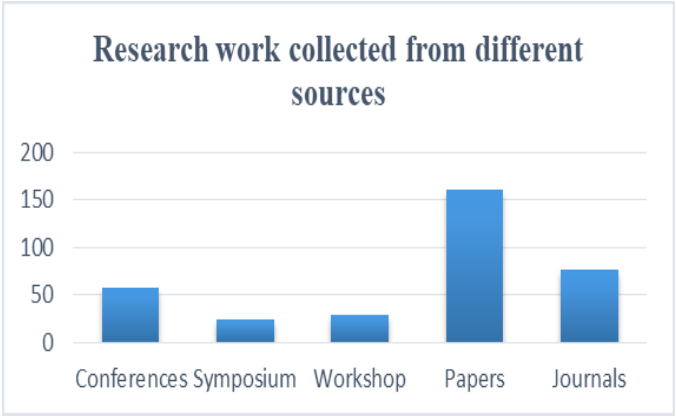


**Figure (7). Research work data collection from different sources**

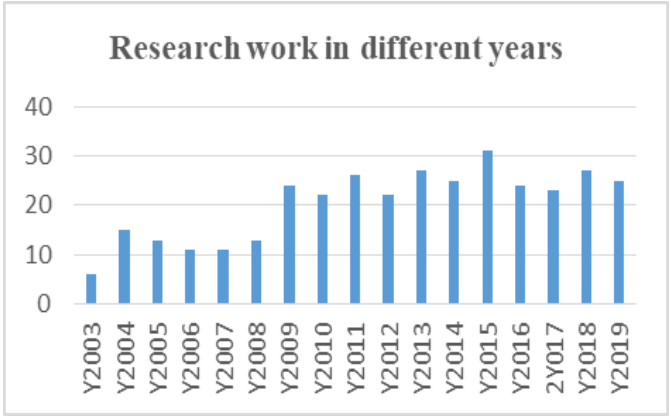


**Figure (8). Research work in different years**

Table (6) Clearly represent that more than 45 conferences conducted in the past 17 years and the frequency of these conferences increase in past 10 years where the authors presented their work (methods, techniques, and tools) in ECC (Elliptic Curve Cryptography) with AIVM (Ancient Indian Vedic Mathematics) Sutras, some authors provided new techniques of AIVM for ECC and some apply existed method to solve the problem which presented ECC workshops conducted in this direction, provide a better platform to the researchers and industrial persons to understand the concept of ECC and AIVM, with the using AIVM methods and techniques, a security-based system can increase their security, reliability, management, testability and decrease the processing time and area of cryptographic operations. Also, unravel solutions for ECC operations and gave researchers new directions for the cryptographic system in the same work.

***A.*** *Survey on different designed multiplier using AIVM sutras*

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

| S. NO. | Authors | Paper Title | Features | Language or Tool | Sutras From AIVM | Publishers | Year |
|---|---|---|---|---|---|---|---|
| 1 | H.D Tiwari et al. | Multiplier design based on ancient Indian Vedic Mathematics | Faster multiplier and square architecture, delay and design area less. | ALTERA Cyclone–II FPGA | Urdhva-Tiryagbhyam, and Nikhilam | IEEE | 2008 |
| 2 | M. Ramalatha et al. | High Speed Energy Efficient ALU Design using Vedic Multiplication Techniques | Parallel generation of intermediate products | Simulations result by Xilinx | Urdhva-Tiryagbhyam | IEEE | 2009 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | Devika Jain et al. | AIVM Based Multiply Accumulate Unit | Binary number multiplication, Realized easily on silicon due to regular and parallel structure. | VHDL and Xilinx | Urdhva-Tiryagbhyam | IEEE | 2011 |
| 4 | Shylashree.N and V. Sridhar | Efficient Implementation of Scalar Multiplication for Elliptic Curve Cryptography using Ancient Indian Vedic Mathematics over GF(p) | Efficient in terms of area and speed | Xilinx 9.1i with Virtex-5 | Multiplications and squaring is done using Vedic Mathematics, | IJCA | 2012 |
| 5 | Akhalesh K. Itawadiya et al. | Design a DSP Operations using Vedic Mathematics | Vedic mathematics based DSP requires less processing time than inbuilt MATLAB functions, Gives better result. | Matlab | Urdhva-Tiryagbhyam | IEEE | 2013 |
| 6 | Sushma R. Huddar et al. | Novel Architecture for Inverse Mix Columns for AES using Ancient Vedic Mathematics on FPGA | Low on-chip area and high speed | Xilinx | Urdhva-Tiryagbhyam, Advanced Encryption Standard (AES) | IEEE | 2013 |
| 7 | R.Thamil Chelvan and S.Roobini priy | Implementation of fixed and floating point division using Dhvajanka sutra | Used in division of RSA encryption/decryption, efficient in terms of area and speed. | VHDL and FPGA synthesis using Xilinx Library | Dhvajanka Sutra | IJVES | 2013 |
| 8 | Diganta Sengupt et al. | A New Paradigm In Fast BCD Division Using Ancient Indian Vedic Mathematics Sutras | The computation time required by the Vedic Division Algorithm is approximately constant irrespective of the size of the dividend. | 32 bit Operating System having Intel Pentium Dual CPU E2180 @2.00 GHz and 0.99 GB DDR2 RAM | Nikhilam and Parvartya sutra | ICCSEA | 2013 |
| 9 | Surabhi Jain et al. | Binary Division Algorithm and High Speed Deconvolution Algorithm (Based on AIVM | Applied for calculating deconvolution, reduced time delay and complexity. | VHDL and Xilinx ISE | Nikhilam, Parvarty Sutra | IEEE | 2014 |
| 10 | Pallavi. B | High Speed FPGA Based Dual Field Elliptic Curve Cryptography using Mixed Coordinate | In order to speed up the time required for multiplication | Xilinx platform | Karatsuba multiplier | IJERT | 2014 |
| 11 | Prokash Barman and Banani | An Efficient Elliptic Curve Cryptography | Efficient in view of less operational steps and | --- | Nikhilam Navatascharamam | The | 2015 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Saha | Arithmetic Using Nikhilam Multiplication | smaller multiplications | | Deshatah | IJES | |
| 12 | M. Jotheeshkumar and S. HemaChitr | Verilog Implementation of Optimized Elliptic Curve Crypto Processor for FPGA platform and its Performance analysis | Processor yields a good result in both area and timing | Xilinx ISE 14.2 | Karatsuba multiplier | IJTET | 2016 |
| 13 | Rina Maria and V. Anitha | Light Weight Asymmetric Cryptographic Algorithm for Financial Transactions through Mobile Application | Consumes less resources in terms of delay and power. | Matlab | Urdhva-Tiryagbhyam | IJCA | 2017 |
| 14 | Leelavathi G et al. | Design of RSA Processor and Field Arithmetic of ECC with Vedic Multipliers for Nodes in Wireless Sensor Network | Performance in speed and memory usage | Spartan 3 FPGA | Urdhva-Tiryagbhyam and Nikhilam | IOSR-JVSP | 2018 |
| 15 | R Dhanupriya and G.V. Subbareddy | High speed multiplier using Nikhilam Sutra algorithm of Vedic mathematics | Investigation the rationale size, region and power utilization | Xilinx 13.2 | Nikhilam Navatascharamam Deshatah | IJMTE | 2019 |

**Table (6). Survey of Different Multiplier Design Using AIVM sutras**

***B.*** *Survey of performance analysis of various cryptography using AIVM sutras*

| S. No | Author Names | Name of Cryptographic algorithms used | Computational Complexity |
|---|---|---|---|
| 1 | R. G. Kaduskar et.al | RSA | Efficient in Time |
| 2 | R. Bhaskar et.al | RSA | Improve computation speed and efficient in hardware |
| 3 | Greeshma Liz Jose et.al | RSA | Efficient in Terms of speed and Area |
| 4 | Kadu R Dhanashri | RSA | Reduce complexity, execution time, power etc. |
| 5 | Thamil Chelvan R et.al | RSA | Efficient in time, speed and area |
| 6 | Shahina M. Salim et.al | RSA | Efficient in time and area, space, speed |
| 7 | Soumya Sadanandan et.al | AES | Efficient in performance and use less area |
| 8 | Shrita G et al | AES | Area efficient and high speed |

| | | | |
|---|---|---|---|
| 9 | Suresh Kavuri et al | AES | Perform well in terms of speed and occupies less area |
| 10 | L. Anjali | AES | Efficient in terms of area and hardware Resources |
| 11 | Prokash Barman et al | ECC | Increase speed of arithmetic in ECC |
| 12 | N.D. Shylashree et al | ECC | Increase Speed of scalar multiplication. |
| 13 | M. Jotheeshkumar and S. HemaChitr | ECC | Decrease area and timing |
| 14 | Rina Maria and V. Anitha | ECC | Consumes less resources in terms of delay and power. |
| 15 | R. Dhanupriya and G V Subbareddy | ECC | Investigation the rationale size, region and power utilization |
| 16 | Pallavi. B | ECC | In order to speed up the time required for multiplication |

**Table (8). Performance Analysis of AIVM Sutras based Algorithms**

### *C. Survey of comparison between Vedic multiplier and other conventional multipliers*

| S. No | Parameter | Array Multiplier | Wallace Tree Multiplier | Booth's Multiplier | Vedic Multiplier |
|---|---|---|---|---|---|
| 1 | Operation Speed | Less | High | Highest | Most High |
| 2 | Time Delay | More | Medium | Less | Much Less |
| 3 | Area | Maximum area because it uses a large number of Adders | Medium area because Wallace Tree used to reduce Operands | Minimum area because no of adder is small | Much minimum area |
| 4 | Complexity | Less complex | More complex | Most complex | Much less complex |
| 5 | Power Consumption | Most | More | Less | Much less |
| 6 | FPGA implementation | Less efficient | Not efficient | Most efficient | Most efficient |

**Table (9). Comparison between Vedic Multiplier and other conventional Multipliers**

Table 9. Clearly shows that Vedic Multiplier gives best results in the term of operational speed, time delay, complexity, area, power consumption and, FPGA implementation in the comparison of other conventional Multipliers.

## V. CONCLUSION

In this work, we studied about 200 research papers, 60 conferences, 30 workshops approximately. Almost 120 papers are related to AIVM sutras for ECC and useful for our survey as well as queries presented above. In this survey, we have surveyed the tools and AIVM sutras which are used in the last 17 years of research papers by authors. In this paper, we tried to show, that how much work has been done in the field of ECC with AIVM sutras so far and what still not to be done. In this survey paper, we conclude that AIVM sutras based multipliers are giving best results comparison than the other conventional multipliers.

### ACKNOWLEDGMENT

I would like to thank J. S. S. B. K. Tirthaji for giving Sixteen Simple Sutras, Mr. Ashish Saini, Mr. Satveer, & Mr. Satendra Kumar, Research Scholar, Department of Computer Science, Gurukula Kangri Vishwavidyalaya, Haridwar (Uttarakhand) 249404, INDIA for supporting me in this research work.

## REFERENCES

[1] A. Deepa and C. N. Marimuthu., "Squaring using Vedic Mathematics and its architectures: a survey", International Journal of Intellectual Advancements and Research in Engineering Computations, 6(1), 214-218, (2018).

[2] A. Lisha and T. Monoth., "Anaysis of cryptography algoritms based on Vedic Mathematics", International Journal of Applied Engineering Research, 13(3), 68-72, (2018).

[3] A. Singh and N. Gupta., "Vedic Mathematics for VLSI: A Review" International Journal of Engineering Science & Research Technology, 6(3), 194-206, (2017).

[4] C. Thomas, G. Sheela and P. K. Saranya., "A Survey on Various Algorithm Used for Elliptic Curve Cyrptography", 5(6), 7296-7301, (2014).

[5] D. Hankerson, Menzes A. and Vanstone S., Guide to Elliptic Curve Cryptography, Springer-Verlag, New York, 2004.

[6] J. Menezes, "*Elliptic Curve Public Key Cryptosystems*", Kluwer Academic Publishers, Springer, (1993).

[7] J. Muthukuru and B. Sathyanarayan., "A Survey of Elliptic Curve Cryptography Implementation for Efficient Smart Card Processing", Global Journal of Computer Science and Technology, 12 (1), 7-12, 2012.

[8] J. S. S. B. K. Tirthaji., Vedic Mathematics or Sixteen Simple Sutras from Vedas, Motilal Bhandaridas, Varanasi, India, (1986).

[9] K. M. Gaikwad and M. S. Chavan., "Vedic Mathematics for Digital Signal Processing Operations: A Review", International Journal of Computer Applications, 131(8), 10-14, (2015).

[10] K. N. Palata, V. K. Nadar, J. S. Jethawa , T. J. Surwadkar , R. S. Deshmukh., "Implementation of an Efficient Multiplier based on Vedic Mathematics", International Research Journal of Engineering and Technology, 4(4), 494-497, (2017).

[11] K. Verma and H. Agarwal., "A Survey on Elliptical Curve Cryptography in Different Methods", International Journal of Advanced Research in Computer Science, 4(4), 101-105, (2013).

[12] M. Warang and A. Tambe., "A review on high speed complex multiplier using Vedic Mathematics: an effective tool". International Journal of Advance Electrical Electronics Engineering, 5(1), 26-28, (2016).

[13] M.C. Sudep, B.M and Sharath, V. Mahendra., "Design and FPGA implementation of high speed Vedic multiplier", International Journal of Computer Applications, 90 (16), 6-9, 2014.

[14] P. Saha, D. Kumar, P. Bhattacharyya, A. Dandapat.,"Vedic division methodology for high-speed very large scale integration applications", The Journal of Engineering, 2014(2),51-59, (2013).

[15] R. Markan and G. Kaur., "Literature Survey on Elliptic Curve Encryption Techniques". International Journal of Advanced Research in Computer Science and Software Engineering, 3(9), 906-908, (2013).

[16] R.K. Bathija, S. Sarkar, R. Sahu, and R.S. Meena., "Low Power High Speed 16x16 bit Multiplier using Vedic Mathematics", International Journal of Computer Applications,59(6), 41-44, (2012).

[17] S. Agrawal and V. K. Magraiya., "A Review of Vedic Multiplier", Journal of Multidisciplinary Science and Technology, 1(5), 142-144, (2014).

[18] S. D. Pinagle., "A Survey of Trends in Cryptography and Curve Cryptography", International Journal of Scientific Research and Education, 4(50), 5294-5301, (2016).

[19] S. Jain and V. S. Jagtap., "Vedic Mathematics in Computer: A Survey", International Journal of Computer Science and Information Technologies, 5(6), 7458-7459, (2014).

[20] S. M. Salim and N. N. Mandaogade, "A Review on Implementation of RSA Cryptosystem Using Ancient Vedic Mathematics", 5(5), 280-282, (2018).

[21] S. Shembalkar, S. Dhole T. Yadav, and P. Thakre., "Vedic Mathematics Sutra- A Review", International Conference on Recent Trends in Engineering Science and Technology, 5(1), 148-155, (2017).

[22] W. Stallings, "*Cryptography and Network Security: Principals and Practices*" Prentice Hall, Incdia, (2003).

## BIOGRAPHIES

**Dr. Manoj Kumar** is an Assistant Professor in the Department of mathematics and Statistics, at Gurukula Kangri Vishwavidyalaya, Haridwar (Uttrakhand) 249404, INDIA and he is having more than 15 research paper and 15 years of Academic Teaching Experience. Areas of interest are Cryptography, Quantum Cryptography, Approximation Theory and Vedic Mathematics.

**Mr. Ankur Kumar** is a Research Scholar in the Department of mathematics and Statistics, at Gurukula Kangri Vishwavidyalaya, Haridwar (Uttrakhand) 249404, INDIA. Areas of interest are Cryptography, Vedic Mathematic.