Volume 8, Issue 6
December 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Some Efficient and Enhanced Techniques of Ancient Mathematics for Elliptic Curve Cryptography (ECC)

[1]Ankur Kumar, [2]Pratik Gupta and [3]Manoj Kumar

[1,3]Department of Mathematics and Statistics,

Gurukula Kangri Vishwavidyalaya, Haridwar (Uttarakhand) 249404, INDIA

[2]Department of School of Basic Science

Jaipur National University (Jaipur) 302017, INDIA

Email id: [1]ankurgkv99@gmail.com, [2]pratikgupta1810@gmail.com, [3]sdmkg1@gmail.com

ABSTRACT

In this present approach, Some Efficient and Enhanced Techniques of Ancient Mathematics For Elliptic Curve Cryptography (ECC) has been studied, in which, it has been observed that the applications of AIVM Techniques or Sutras decrease the number of multiplications and squares which occur in point doubling and point addition in ECC over the Ring A_4. This paper described the use of AIVM Sutras, Urdhva-Tiryagbhyam for multiplication and Dvandva-Yoga for the square of any number in the ECC over the Ring A_4. The results proved that AIVM based scheme shows better performance in speed, processing time and power consumption of multipliers compared to the conventional method. The coding and synthesis are done in MATLAB for 8-bit and 16-bit multiplications and squares. The results proved that the Vedic Mathematics based scheme shows better performance compared to the conventional method and total delay in computation is reduced by Vedic mathematics Sutras (Urdhva-Tiryagbhyam, Dvandva-Yoga). The effect of some AIVM techniques over ECC was investigated and the obtained results are explained in the form of tables and graphs.

Keywords: *Cryptography, Dvandva-Yoga, Elliptic Curve, Finite Field, Point Addition, Point Doubling, Ring A_4. Urdhva-Tiryagbhyam, Vedic Mathematics.*

1. INTRODUCTION

Elliptic curve cryptography (ECC) is an approach which is based on public-key cryptography. Along the system of a public key cryptography every client or the electronic tools joined in the Network Communication naturally have a couple of keys first one is a public key and other is a private key and a class of numeric operations correlated with keys for doing the various types of cryptographic operation The private key known only by the special client and on the other hand the public key is communicated to all clients which are joints in the communication network [12, 17]. In the core work, we shall discuss the elliptic curves over the ring $A_4 = F_{2^d}[\varepsilon]$ where $\varepsilon^4 = 0$ [1, 5] and we have used some Ancient Indian Vedic Mathematics (AIVM) techniques [9] for the completion of cryptographic operations on these curves. The major congestion that arrangement of the efficiency in ECC operations first is the addition and other is doubling in the schemes which are based on the ECC. In conduct, these operations are found to be very complex and the most time-consuming operations for ECC. It is very well known that the energy efficiency and effective computation methods are the important factors in identifying the performance of any of ECC based algorithm. The performance of an ECC based algorithm can be improved if we are able to reduce its execution time which is basically depending upon the point addition and doubling operations. It is widely known that there exist many simple and time-saving techniques in the form of sixteen Sutras and fourteen sub Sutras of AIVM to compute complex Mathematical manipulations such as multiplication and divisions [9]. In the current approach, we have used Urdhva-Tiryagbhyam multiplication and Dvandva-Yoga technique to speed up the above-mentioned complex computations occurring in the ECC based ring A_4 proposed in. The results show that AIVM based ECC over the ring A_4 can give better performance compared to the conventional methods [9, 13, 14].

2. RELATED WORK

In the last three-decade across the World Vedic Mathematics branch of Mathematics is using so much in the research area. Ancient Indian Vedic Mathematics (AIVM) is based on sixteen Sutras and fourteen sub Sutras. AIVM has a different and unique technique compare to other computational technique for calculations. Kan et al. [2]. purposed in his work in 2012, the Design and implementation of low power multiplier using Vedic multiplication technique involving of small key size in ECC cryptographic system it gives faster implementation and best output. It has been

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

observed that AIVM based ECC gives a better result with uses of small key size than other cryptographic systems. In the current decade, ECC is using because it gives reliability and security ECC is maximally used in security and networking areas because ECC key size is too small. It is using in many devices which have not much storage memory like Smart cards. In the banking sector, ECC makes possible and more secure Smart cards for credit and debit, also electronic tickets and personal registration cards or identification. In the process of encryption and decryption, it is well-explained transforming of an informational into an affine coordinate on the elliptic curve. Nanda and Behera [3] in 2014 proposed the AIVM Sutras based multiplication algorithm Design and Implementation of Urdhva-Tiryagbhyam with the 8×8 bit Vedic Binary Multiplier, this paper shows that AIVM techniques such as Dvandva Yoga to get square of any number and Urdhva-Tiryagbhyam Sutra for computation of n-digits multiplication gives better results comparatively other techniques. Chillali et al. [1] in 2015 purposed ECC over a chain ring of characteristic three this reference explained ECC over the Ring that makes much secure ECC. Anchaliya and Chiranjeevi [14] in 2015 proposed Dvandva Yoga Sutra for Square of a number, Urdhva-Tiryagbhyam Sutra for multiplication, and Dhvajanka Sutra for the division. This paper shows the implementation in ECC by using Vedic Sutra for multiplication of n-digits number and square of a number in point doubling and point addition. The AIVM techniques improve the speed, and time of processing compare to the implementation of other conventional multiplication. Palata et al. [10] have described an Implementation of an efficient multiplier based on AIVM in 2017. This work explained the Implementation of encryption and decryption algorithms in ECC with AIVM Sutras to improve the performance in cryptographic operations. In the above references paper AIVM based ECC gives the best output in faster time execution for a cryptographic system [4, 5, 6, 7, 8, 11, 13, 15].

3. ANCIENT MATHEMATICS

Across India and out of India graph of the research is increasing speedily in the field of AIVM (Ancient Indian Vedic Mathematics) which contain the sixteen Sutras or formulae and fourteen sub Sutras in operations of all branches of Mathematics. In this AIVM section, we will discuss some useful techniques methods first one is Urdhva-Tiryagbhyam and second is Dvandva-Yoga of Ancient Indian Vedic Mathematics which will be used in a later section to improve the performance of ECC based schemes over the Ring A_4 [9].

3.1. Urdhva-Tiryagbhyam

Urdhva-Tiryagbhyam multiplication technique is used for general multiplication [9]. This Sutra directly explains a rule or way in the form of vertically and crosswise which applying on the digits. This Sutra is very useful in all AIVM Sutras, and it has applied in many applications in all kind of branches of mathematical science. In this work, we are explaining this method for two or three-digit numbers. To manipulate this type of issue best Sutra of AIVM Urdhva-Tiryagbhyam technique can be applied and it gives the best results.

Example 3.1. Evaluate 42×26 uging Urdhva-triyaghyam technique.

4×2	$4 \times 6 + 2 \times 2$	2×6
8	28	12
8 + 2	8 + 1	2
10	9	2

= 1092

3.2. Dvandva-Yoga

To calculate the square of any number we can use Dvandva-Yoga (D_Y) algorithm and rule for squaring of binary or decimal numbers from this Sutras is explained as [9, 14]:

- 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 the 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 $2*p_1*r_1+q_1^2$.

4. ELLIPTIC CURVE CRYPTOSYSTEM USING URDVA-TIRYAGHBHYAM AND DVANDVA-YOGA TECHNIQUES

This section shows some arithmetic fundamental of ECC using AIVM Sutras. The elliptic curve is expressed as: $E(a,b)=\left\{ \begin{matrix} (x,y): y^2 = x^3+ax+b \\ and\ 4a^3+27b^2 \neq 0 \end{matrix} \right\} \cup \{O\}$.

Volume 8, Issue 6
December 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

To find the value of $\lambda^2,\, 3x^2$ *and* $\lambda(x_1 - x_3)$ we can use AIVM Sutra Urdhva-Tiryagbhyam in the operations of ECC first is addition and second is doubling:

For Addition, the sum of two points $P+Q$ is R where $P=(x_1,y_1)$, $Q=(x_2,y_2)$ then R will be (x_3,y_3) where x_3, y_3, λ are

$$\begin{bmatrix}(\lambda^2 - x_1 - x_2), \\ (\lambda(x_1 - x_3) - y_1), \\ (y_2 - y_1)/(x_2 - x_1)\end{bmatrix} \text{Respectively.}$$

For doubling, the point doubling of a point $P(x_1y_1)+P(x_1y_1)=2P(x_1y_1)=R(x_3y_3)$ where x_3, y_3, λ are

$$\begin{bmatrix}\lambda^2 - 2x), \\ (\lambda(x - x_1) - y), \\ (3x^2 + a)/2y\end{bmatrix} \text{Respectively.}$$

All these values of point addition and doubling can be determined easily by the help of AIVM useful Sutra.

5. ELLIPTIC CURVES OVER THE RING A4

Explanation: We characterize an elliptic curve over the ring A_4; distinguished $E_{a,b}(A_4)$ as an arc or curve obsessed by such like Weierstrass equation define as [5, 6, 7]:

$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$; In this expression b is invertible and A_4 containing a *and* b.

$$E_{a,b}(A_4) = \left\{ \begin{array}{l} Y^2Z + XYZ = X^3 + aX^2Z + bZ^3 \\ \middle| [\mathrm{X}:\mathrm{Y}:\mathrm{Z}] \in \mathrm{P}_2(\mathrm{A}_4) \end{array} \right\}.$$

- ***Addition of two points in ECC over the Ring A4 [6]:***

If $P_1 = [X_1 : Y_1 : Z_1]$ *and* $P_2 = [X_2 : Y_2 : Z_2]$ *then the Addition of two points* over $E_{a,b}(A_4)$ *is* $P_3 = P_1 + P_2 = [X_3 : Y_3 : Z_3]$ *where*

$$\mathrm{X}_3 = \mathrm{X}_1\mathrm{Y}_2^2\mathrm{Z}_1 + \mathrm{X}_2\mathrm{Y}_1^2\mathrm{Z}_2 + \mathrm{X}_1^2\mathrm{Y}_2\mathrm{Z}_2 + \mathrm{X}_2^2\mathrm{Y}_1\mathrm{Z}_1 + \mathrm{a}\mathrm{X}_1^2\mathrm{X}_2 Z_2 + \mathrm{a}\mathrm{X}_1\mathrm{X}_2^2\mathrm{Z}_1 + \mathrm{b}\mathrm{X}_1\mathrm{Z}_2^2\mathrm{Z}_1 + \mathrm{b}\mathrm{X}_2\mathrm{Z}_1^2\mathrm{Z}_2.$$

$$Y_3 = X_1^2\mathrm{X}_2\mathrm{Y}_2 + \mathrm{X}_1 X_2^2\mathrm{Y}_1 + \mathrm{Y}_1^2\mathrm{Y}_2\mathrm{Z}_2 + \mathrm{Y}_1\mathrm{Y}_2^2\mathrm{Z}_1 + \mathrm{X}_1^2 Y_2 Z_2 + \mathrm{X}_2^2 Y_1 Z_1 + a\mathrm{X}_1^2 Y_2 Z_2 + a\mathrm{X}_2^2 Y_1 Z_1 + a\mathrm{X}_1^2 X_2 Z_2 + aX_1\mathrm{X}_2^2 Z_1 + bY_1 Z_2^2 Z_1 + \mathrm{b}\mathrm{Y}_2 Z_1^2 Z_2 + bX_1 Z_2^2 Z_1 + bX_2 Z_1^2 Z_2.$$

$$Z_3 = X_1^2\mathrm{X}_2 Z_2 + \mathrm{X}_1 X_2^2 \mathrm{Z}_1 + \mathrm{Y}_1^2\mathrm{Z}_2^2 + \mathrm{Y}_2^2\mathrm{Z}_1^2 + \mathrm{X}_1 Y_1 \mathrm{Z}_2^2 + \mathrm{X}_2 Y_2 Z_1^2 + a\mathrm{X}_1^2 Z_2^2 + a\mathrm{X}_2^2 Z_1^2.$$

Algorithm of the addition of two points in ECC over ring A4

Addition of $P_1 = (X_1, Y_1, Z_1)$ **and** $P_2 = (X_2, Y_2, Z_2)$
Input : $P_1 = [X_1 : Y_1 : Z_1]$ *and* $P_2 = [X_2 : Y_2 : Z_2]$, a, b *in ECC over ring* A_4
Output : $P_3 = [X_3 : Y_3 : Z_3] = P_1 + P_2$; *in ECC over ring* A_4.
1. *If* $P_1 = \infty$ *then return* $(X_1 : Y_1 : Z_1)$
2. *If* $P_2 = \infty$ *then return* $(X_2 : Y_2 : Z_2)$
3. $A = X_2 \cdot Y_1$;
4. $B = X_1 \cdot Y_2$;
5. $C = Z_1 \cdot X_2$;
6. $D = Z_2 \cdot X_1$;
7. $E = Z_1 \cdot Y_2$;
8. $F = Z_2 \cdot Y_1$;
9. $G = X_1 \cdot X_2$;
10. $H = Y_1 \cdot Y_2$;
11. $I = Z_1 \cdot Z_2$;
12. $J = D + C$;
13. $K = B \cdot D + A \cdot C$;
14. $L = B \cdot E + A \cdot F$;
15. $X_3 = J[I + aG] + K + L$;
16. $Y_3 = bI[J + M] + K[a+1] + G[N + aJ] + H[F + E]$;

17. $Z_3 = a\left[D^2 + C^2\right] + E\left[E + C\right] + F\left[F + D\right] + G \cdot J;$

18. $Return\left(X_3 : Y_3 : Z_3\right)$

Finally, we can calculate the point $P_3\ (X_3, Y_3, Z_3)$ where

$X_3 = J\left[I + aG\right] + K + L,$

$Y_3 = bI\left[J + M\right] + K\left[a + 1\right] + G\left[N + aJ\right] + H\left[F + E\right]$ and

$Z_3 = a\left[D^2 + C^2\right] + E\left[E + C\right] + F\left[F + D\right] + G \cdot J$

here we can use Urdhva-Tiryagbhyam and Dvandva-Yoga technique to evaluate all values of multiplications and squares.

- ***Doubling of a point in ECC over the Ring A_4 [6]:***

If $P_1 = \left[X_1 : Y_1 : Z_1\right]$ *then the Doubling of a points* over $E_{a,b}\left(A_4\right)$ *is* $P_3 = 2P_1 = \left[X_3 : Y_3 : Z_3\right]$ *where*

$$X_3 = X_1Y_1Y_2^2 + X_2Y_1^2Y_2 + X_2^2Y_1^2 + X_1X_2^2Y_1 + aX_1^2X_2Y_2 + aX_1X_2^2Y_1 + aX_1^2X_2^2 + bX_1Y_1Z_2^2 + bX_2Y_2Z_1^2 + bX_1^2Z_2^2 + bY_1Z_2^2Z_1 + bY_2Z_1^2Z_2 + bX_1Z_2^2Z_1.$$

$$Y_3 = Y_1^2Y_2^2 + X_2Y_1^2Y_2 + aX_1X_2^2Y_1 + a^2X_1^2X_2^2 + bX_1^2X_2Z_2 + bX_1X_2^2Z_1 + bX_1Y_1Z_2^2 + bX_1^2Z_2^2 + abX_2^2Z_1^2 + abX_1^2Z_2^2 + bY_1Z_2^2Z_1 + bX_1Z_2^2Z_1 + abX_1Z_2^2Z_1 + abX_2Z_1^2Z_2 + b^2Z_1^2Z_2^2.$$

$$Z_3 = X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2X_2^2 + X_2Y_1^2Z_2 + X_1^2Y_2Z_2 + aX_1^2Y_2Z_2 + aX_2^2Y_1Z_1 + X_1^2X_2Z_2 + aX_1X_2^2Z_1 + bY_1Z_2^2Z_1 + bY_2Z_1^2Z_2 + bX_1Z_2^2Z_1.$$

Algorithm of doubling of a point in ECC over Ring A_4

Doubling of $P_1 = (X_1, Y_1, Z_1)$

Input : $P_1 = \left[X_1 : Y_1 : Z_1\right]$,
a, b in ECC over ring A_4

Output : $P_3 = \left[X_3 : Y_3 : Z_3\right] = 2P_1;$
in ECC over ring A_4

1. *If* $P_1 = \infty$ *then return*$\left(\infty\right)$
2. $A = X_2 \cdot Y_1;$
3. $B = X_1 \cdot Y_2;$
4. $C = Z_1 \cdot X_2;$
5. $D = Z_2 \cdot X_1;$
6. $E = Z_1 \cdot Y_2;$
7. $F = Z_2 \cdot Y_1;$
8. $G = X_1 \cdot X_2;$
9. $H = Y_1 \cdot Y_2;$
10. $I = Z_1 \cdot Z_2;$
11. $J = H + A;$
12. $K = b(F + D);$
13. $L = A + B;$
14. $M = A + aG;$
15. $N = I + C;$
16. $X_3 = G\left[aL + M\right] + K\left[I + D\right] + bE \cdot N + A \cdot J + H \cdot B;$
17. $Y_3 = \left[D + C\right]\left[G + aI\right] + a\left[C^2 + D^2\right] + K\left[I + D\right] + aG \cdot M + H \cdot J + bI^2;$
18. $Z_3 = G\left[L + aC + G + D\right] + E\left[H + bI\right] + aA \cdot C + F \cdot J + I \cdot K;$
19. $Return\left(X_3 : Y_3 : Z_3\right)$

Finally, we can calculate the point $P_3\ (X_3, Y_3, Z_3)$ where

$$X_3 = G\left[aL + M\right] + K\left[I + D\right] + bE \cdot N + A \cdot J + H \cdot B;$$
$$Y_3 = \left[D + C\right]\left[G + aI\right] + a\left[C^2 + D^2\right] + K\left[I + D\right] + aG \cdot M + H \cdot J + bI^2;$$
$$Z_3 = G\left[L + aC + G + D\right] + E\left[H + bI\right] + aA \cdot C + F \cdot J + I \cdot K;$$

Here we can use Urdhva-Tiryagbhyam and Dvandva-Yoga technique to evaluate all values of multiplications and squares.

6. CRYPTOGRAPHIC APPLICATIONS

Volume 8, Issue 6
December 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Let $P \in E_{a,b}(A_4)$ of order τ, we will use the subgroup $< P >$ of $E_{a,b}(A_4)$ to encrypt the message, and we denote $G =< P >$.

- **Coding of elements of *G*.**

We will give a code to each element

$Q = m.P \in G$, where

$m \in \{1, 2 ... \tau\}$,

Let

$$Q = \left[x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : Z \right]$$

Where $x_i, y_i \in F_{2^d}$ *for* $i = 0,1,2,3.$ we set:

If Z=1 then

We code Q as it follows:

$$Q = \left[x_0x_1x_2x_3y_0y_1y_2y_3 : 1 \right]$$

$$Q = \begin{bmatrix} 100010001, 100011111, 100011101, 000011111 \\ 110010001, 100011011, 100010111, 110011111 \\ 101010001, 100010111, 100010101, 100011111 \\ 100110001, 100010011, 100010111, 101011111 \\ 111110001, 111010011, 111110111, \ldots \quad \ldots \quad \ldots \end{bmatrix}$$

Q *has containing* $2^8 = 256$ *elements.*

7. RESULT ANALYSIS

The comparison is based on the number of multiplications and square in point doubling and addition in ECC (Elliptic Curve Cryptography) over the Ring A_4 and VECC (Vedic Mathematics based Elliptic Curve Cryptography) over the Ring A_4. The total arithmetic operations such as multiplication, square are compared in table 1 and 2, which concludes that the number of operations is minimum in table 2 which is based on VECC.

In table 3 and 4 we observed that running time process using Vedic Mathematics takes 70% (app.) less time than running time process using Conventional Methods for four bits, eight bits, and sixteen bits. The arithmetic operations in ECC over the Ring A_4 for point addition and point are compared in fig.3 which also conclude that the number operations are minimum in the purposed results. Where **M** (Number of multiplications), **S** (Number of Squares), **T** (Total number of Arithmetic Operations)]

ECC over Ring A4	M	S	T
Point addition	56	34	90
Point doubling	74	52	126

Table 1: Number of operations needed in addition and doubling of points in ECC over Ring A4.

ECC over Ring A4	M	S	T
Point addition	25	2	27
Point doubling	23	3	26

Table 2: Number of operations needed in addition and doubling of points in VECC over Ring A4.

8 Bits Running Time	Running Time Processed using Conventional Methods	Running Time Processed using Vedic Mathematics Sutras	Average of Reducing Time
Point Addition	0.01109 app. (s)	0.0025012 app. (s)	77.2803%
Point Doubling	0.01048 app. (s)	0.0030219 app. (s)	71.1643%

Table 3. Synthesis results of point addition and point doubling

16 Bits Running Time	Running Time Processed using Conventional Methods	Running Time Processed using Vedic Mathematics Sutras	Average of Reducing Time
Point Addition	0.010888 app. (s)	0.0020361 app. (s)	81.26464%
Point Doubling	0.011017 app. (s)	0.0024856 app. (s)	77.4386%

Table 4. Synthesis results of point addition and point doubling

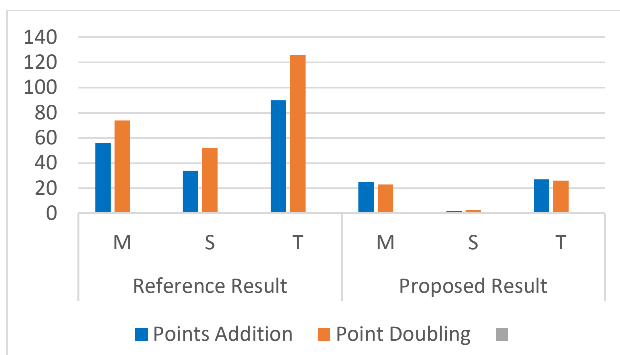

Fig. 3: Comparing the arithmetic operations in ECC over the Ring A4 for point addition and point doubling

8. CONCLUSION

In this approach, we have analyzed the ECC (Elliptic Curves Cryptography) over the Ring $A_4 = F_{2^d}[\varepsilon]$ where $\varepsilon^4 = 0$, and the coding over the EC (Elliptic Curve) $E_{a,b}(A_4)$ well established. There are mainly two useful operations elaborated in ECC over the Ring $A_4 = F_{2^d}[\varepsilon]$

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

first one is the addition and other is doubling. In these major operations, all multiplications and squares are calculated by AIVM Sutras to push forward the all scalar multiplications. Our approach described the squaring of an n-digit number and multiplications in point doubling and addition. The AIVM techniques based multiplications give best performance and results than the arithmetical multiplication. AIVM technique provides a minimum manipulation in the operations of ECC such as, point addition other is point doubling which are the major parts of ECC to manage the keys of encryption and decryption process.

This approach is effectual in the terms of processing time, speed, time of key generation, key size, strength, and as well as area. Various Ancient Indian Vedic Mathematics sutras discussed above have been implemented in MATLAB and are synthesized and simulated using MATLAB. The code is written for the square of 4 bit, 8 bit, and 16-bit binary number, multiplication of two 8-bit, and 16-bit binary numbers. For cryptographic operations (point addition, point doubling) using Vedic Mathematics, the Average of Reducing Time is 70% (approx.) less than conventional methods.

Future work of the AIVM based ECC will be improved all cryptographic-based security system, such as IP Security, e-mail, e-commerce, internet banking, secure communications, and information system.

REFERENCES

[1] A. Chillali, M.H. Hassib, M.A. Elomary, "*Elliptic curves over a chain ring of characteristic 3*", Journal of Taibah University for Science, Vol.**9** Issue.**3**, pp.**276-287**, **2015.**

[2] A. Kan he, S.K. Das, A.K. Singh, "*Design and implementation of low power multiplier using Vedic multiplication technique",* International Journal of Computer Science and Communication, Vol.**3,** Issue.**1**, pp.**131-132**, **2012.**

[3] A. Nanda, S. Behera "*Design and Implementation of Urdhva-Tiryagbhyam Based Fast* 8×8 *Vedic Binary Multiplier",* International Journal of Engineering Research & Technology, Vol.**3**, Issue.**3**, pp.**1856-1859**, **2014.**

[4] A. Pawar, A.K. Sahu, G.R. Sinha, "*Implementation of High-Speed Vedic Multiplier"* International Journal of Innovative Research in Advanced Engineering, Vol.**1, Issue10**, pp.**396-401**, **2014.**

[5] A. Tadmori, A. Chillali and M. Ziane, "*Coding over elliptic curves in the ring of characteristic two",* International Journal of Applied Mathematics and Informatics, Vol.**8**, pp.**65-67**, **2014.**

[6] A. Tadmori, A. Chillali and M. Ziane., "*Elliptic Curve over Ring A_4"*, Applied Mathematics Science, Vol.**9**, pp.**1721-1733**, **2015.**

[7] A. Tadmori, A. Chillali and M. Ziane., "*Normal Form of the elliptic curves over the finite ring"*, Journal of Mathematics and System Science, Vol.**4**, pp.**194-196**, **2014.**

[8] G. Sameer, M. Sumana and S. Kumar, "*Novel High-Speed Vedic Mathematics Multiplier using Compressors"* International Journal of Advanced Technology and Innovative Research, Vol.**7**, Issue.**2**, pp.**0244-0248**, **2015**.

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

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

[11] M. Poornima, S. K. Patil, S. Kumar, K. P. Shridhar and H. Sanjay, "*Implementation of multiplier using Vedic algorithm"*, International Journal of Innovative Technology and Exploring Engineering, Vol.**2**, Issue **6**, pp.**219-223**, **2013**.

[12] N. Koblitz, "*Elliptic Curve Cryptosystem"*, Journal of Mathematics Computation, Vol.**48,** Issue.**177**, pp.**203-209**, **1987**.

[13] N. Shylashree, D. V. N. 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, Vol.**49**, Issue.**7**, pp.**0975-8887**, **2012**.

[14] R. Anchalya, G. Chiranjeevi N., S. Kulkarni, "*Efficient Computing Techniques using Vedic Mathematics Sutras, International Journal of Innovative Research in Electrical",* Electronic Instrumentation and control engineering, Vol.**3**, Issue**5**, pp.**24-27**, **2015**.

[15] S. M. Salim and S. A. Lakhotiya, "*Implementation of RSA Cryptosystem Using Ancient Indian Vedic Mathematics"* International Journal of Science and Research, Vol.**4**, Issue.**5**, pp.**3221-3230**, **2015**.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

[16] S. Sadanandan and V.Anjali, "*Design of advanced encryption standard using Vedic Mathematics"* International Journal of Innovative Research in Advanced Engineering, Vol.**1**, Issue.**6**, pp.**322-325**, **2014**.

[17] W. Stallings, "*Cryptography and Network Security: Principals and Practices*" Prentice-Hall, **India**, 2003.

AUTHOR PROFILES

Mr Ankur Kumar is working as a Research Scholar in the Department of Mathematics and Statistics, at Gurukula Kangri Vishwavidyalaya, Haridwar (Uttarakhand) 249404, INDIA and he is having 3 years of Teaching and Research experience. His research areas are Cryptography, Elliptic Curve Cryptography and Vedic Mathematics. He has been published more than 6 research papers in reputed national and international Journals.

Dr Pratik Gupta is working as an assistant professor in the department of school of science Jaipur National University (Jaipur) INDIA and he is having more than 10 research papers and two years of Academic Teaching Experience. Areas of interest are Cryptography and Network Security.

Dr Manoj Kumar is working as an assistant professor in the Department of Mathematics and Statistics, Gurukul Kangri Vishwavidyalaya, Haridwar, Uttarakhand (India). His research areas are Elliptic Curve Cryptography, Quantum Cryptography and Approximation Theory. He has been published more than 20 research papers in reputed national and international Journals.