Volume 8, Issue 3
June 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

The Tri-Linear Pairing Map Scheme for Elliptic Curve Cryptography using Vedic Mathematics

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

[1, 2] Department of Mathematics and Statistics,

Gurukula Kangri Vishwavidyalaya, Haridwar (Uttarakhand) 249404, INDIA

[3]School of Basic Science, Jaipur National University Rajasthan, INDIA

E-mail: [1]sdmkg1@gmail.com, [2]ankurgkv99@gmail.com, [3]pratikgupta1810@gmail.com

[2]Corresponding author

ABSTRACT

In this present approach, the tri-linear pairing map scheme for (ECC) elliptic curve cryptography over the algorithms of the Jacobian projective coordinate system using Vedic Mathematics has been studied. This work explained a useful Vedic sutra for multiplication calculation in cryptographic operations. In this paper, we have used Vedic Mathematics Sutra to get minimum steps in the calculation of addition algorithm, doubling algorithm and for improving the speed of processing time in the cryptographic operations, such as point addition, point doubling which occurs in the Elliptic curve tri-linear pairing map scheme. The coding and synthesis are done in MATLAB. 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).

Keywords: *Addition Algorithm, Doubling Algorithm, Dvandva-Yoga, Elliptic Curve Cryptography, Jacobian projective coordinates, Key agreement, Point addition, Point doubling, Tri-linear pairing, Urdhva-Tiryagbhyam.*

1. NTRODUCTION

In the last decade, in a large amount of research work has been achieved on Elliptic Curve Cryptography (ECC) using Vedic Mathematics. Recently, Kumar .M et al. [7, 8] have been explained an ECC scheme of multiparty key exchange with the use of mapping for tri-linear pairing [9]. The major bottlenecks that deal with the efficiency of ECC operations like addition and doubling. In practice, these operations are found to be very complex and the most time-consuming in ECC. It is very well known, the energy efficiency and effective computation methods are the important factors in identifying the performance of any 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 form of sixteen sutras and fourteen sub sutras) in Ancient Indian Vedic Mathematics (AIVM) [10, 11, 12] to compute complex Mathematical manipulations such as multiplication, square and divisions.

In the present paper, we have used some Sutras of Vedic Mathematics to improve the speed in the above-mentioned complex computations occurring in the ECC based tri-linear pairing map scheme proposed in [1, 2, 3, 4, 5]. The results proved that AIVM based scheme shows better performance compared to the conventional method [13, 14]

2. ANCIENT INDIAN VEDIC MATHE-MATICS

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 Jacobian coordinate system [15].

2.1. Urdhva-Tiryagbhyam

Urdhva-Tiryagbhyam multiplication technique is used for general multiplication [15]. This Sutra directly explains away 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. This Sutra is so beneficial because by the use of AIVM technique we get the reduction in multiplications of multi-bits down to one-bits. A Comparison between Vedic multiplier and many others multipliers like Booth and Array multiplier, results show that AIVM based multiplier do not take much time and these multipliers save power, key size, and bits

Volume 8, Issue 3
June 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

comparatively other multipliers. Naturally, by the use of standard or classical method in multiplication we can get results but the number of operations in the classical method is too high almost m^2 operations, for m-bit digit integers so it looks complicated.

Another multiplication method is the Karatsuba method it requires the number of operation is $m^{\log 3}$ for two integers of m-bit. Karatsuba technique (method) gives slow output for a small input in any operations comparatively classical methods of multiplication due to the repetition of overhanging operations. To manipulate this type of issue best Sutra of AIVM Urdhva-Tiryagbhyam technique can be applied and it gives the best results.

2.2. 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 [15] is explained as:

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

3. ELLIPTIC CURVE CRYPTOGRAPHY ARITMETIC

In this section we will through some light on basic nomenclature arithmetic background of ECC.

Following symbols are used to define elliptic curves [6, 16]

- $GF(p)$ is Galois Field over prime p.
- p is prime number greater than 3.
- a, b is fixed real number.
- (x, y) is point on the elliptic curve E

Using above terminology,

the elliptic curve E defined [6] 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:

$E = \{(x, y) : y^2 = x^3 + ax + b \pmod p$

$and\ 4a^3 + 27b^3 \neq 0 \pmod p).$

3.1. The Elliptic Curve $E(F_p)$ explained as

- 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 $E(F_p)$.
- 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 ar

$$\begin{bmatrix} (\lambda^2 - x_1 - x_2), \\ (\lambda(x_1 - x_3) - y_1), \\ (y_2 - y_1)/(x_2 - x_1) \end{bmatrix}$$ respectively [6].

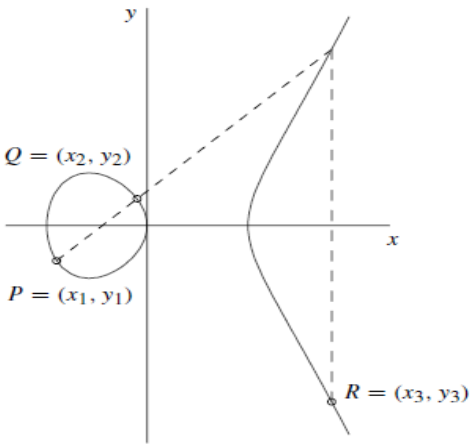

Fig. 1: Addition (P+Q=R) [6]

- 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

$$\begin{bmatrix} \lambda^2 - 2x), \\ (\lambda(x - x_1) - y), \\ (3x^2 + a)/2y \end{bmatrix}$$ respectively [6].

Volume 8, Issue 3
June 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

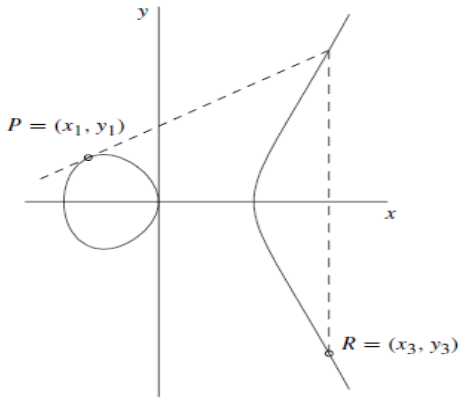

Fig. 2: Doubling (R = 2P) [6]

4. ECC COORDINATE SYSTEM FOR JACOBIAN PROJECTIVE COORDINATE (JPC) SYSTEM

The elliptic curve contains a pair of coordinate systems first is affine and other is projective. For inversion, the affine coordinate system has needed the inversion at the time of doubling and addition of the points, which are so expensive in terms of time, area and speed. We have used the projective plane or coordinate system to remove very demanding operating inversion operation. Elliptic curve operations like addition, doubling needs a fixed number of Square, addition, modular multiplications, shifts, and primary needed fundamental operations. All these kind of operations like, multiplications and squaring depends on the presentation of an elliptic curve for manage the running time in ECC operations [3, 5, 11].

The affine plane $A_F^2 = \{(x, y) \in F \times F\}$ for coordinates (x, y) are mapped to the projective plan $P_F^3 = (X, Y, Z)$ these co-ordinates belongs to $F \times F \times F$. The coordinates (x, y) of the affine plane $A_F^2 = \{(x, y) \in F \times F\}$ are mapped to the coordinates (X,Y,Z) of the projective plane $P_F^3 = \{(X, Y, Z) \in F \times F \times F\}$ with this rule:

$(X, Y, Z) = (x \cdot Z^c, y \cdot Z^d, 1)$ *or* $X = x \cdot Z^c, Y = y \cdot Z^d$.

For JPC system, we take $c = 2$ and $d = 3$, where c, d are integers. For this coordinate system elliptic curve defined as: $E : Y^2 = X^3 + aXZ^4 + bZ^6$.

If two well-defined points $\{P_1, P_2\}$ are $\{(X_1, Y_1, Z_1), (X_2, Y_2, Z_2)\}$ and on the projective plane then $(P_3 = P_1 + P_2)$, $P_3 = (X_3, Y_3, Z_3)$ is known as addition of points and $P_3 = 2P_1 = (X_3, Y_3, Z_3)$ is known as doubling of a point.

- JPC system with $c = 2$ and $d = 3$, addition of point P_1 and P_2 is $P_3 = (X_3, Y_3, Z_3)$ where,

$$X_3 = (Y_2 Z_1^3 - Y_1 Z_2^3)^2 - (X_1 Z_2^2 + X_2 Z_1^2)(X_2 Z_1^2 - X_1 Z_2^2)^2$$

$$Y_3 = ((Y_2 Z_1^3 - Y_1 Z_2^3)(2X_1 Z_2^2 + X_2 Z_1^2) - Y_1 Z_2^3 (X_2 Z_1^2 - X_1 Z_2^2)) - (Y_2 Z_1^3 - Y_1 Z_2^3)^3 \text{ and .}$$

$$Z_3 = (X_2 Z_1^2 - X_1 Z_2^2) Z_2 Z_1$$

- JPC system with $c = 2$ and $d = 3$, doubling of a point P_1 is $P_3 = (X_3, Y_3, Z_3)$ where,

$$X_3 = (3X_1^2 + aZ_1^4)^2 - 8X_1 Y_1^2$$

$$Y_3 = 12X_1 Y_1^2 (3X_1^2 + aZ_1^4) - (3X_1^2 + aZ_1^4)^3 - 8Y_1^4$$

and $Z_3 = 2Z_1 Y_1$.

4.1. Addition Algorithm of JPC System

We assume $x_2 \cdot Z_2^2 = X_2$ *and* $y_2 \cdot Z_2^3 = Y_2$

Input : $P_1 = (X_1, Y_1, Z_1), and\ P_2 = (X_2, Y_2, Z_2)$

Output : $P_3 = P_1 + P_2 = (X_3, Y_3, Z_3)$

1. $A = X_1$
2. $B = x_2 \cdot Z_1^2$
3. $C = A - B$
4. $D = Y_1$
5. $E = y_2 \cdot Z_1^3$
6. $F = D - E$
7. $G = A + B$
8. $H = D + E$
9. $I = G \cdot C^2 - 2X_3$
10. $X_3 = F^2 - G \cdot C^2$
11. $Y_3 = \dfrac{(I \cdot F - H \cdot C^2)}{2}$
12. $Z_3 = Z_1 \cdot C$
13. $Return(P_3 = X_3, Y_3, Z_3)$

Finally, we can calculate the point P_3 where (X_3, Y_3, Z_3) is $\left((F^2 - G \cdot C^2), (I \cdot F - H \cdot C^2)/2, Z_1 \cdot C\right)$ respectively. Here we can use Urdhva-Tiryagbhyam and Dvandva-Yoga technique to evaluate

$x_2 \cdot Z_1^2$, $y_2 \cdot Z_1^3$, $Z_1 \cdot C$, F^2, $G \cdot C^2$, $I \cdot F$ and $H \cdot C^2$

Volume 8, Issue 3
June 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

4.2. Doubling Algorithm of JPC System

Input : $P_1 = (X_1, Y_1, Z_1),\ a$

Output : $P_3 = (X_3, Y_3, Z_3) = 2P_1$

1. $A = 3X_1^2 + a \cdot Z_1^4$

2. $B = 4X_1 \cdot Y_1^2$
3. $C = 8Y_1^4$

4. $X_3 = A^2 - 2B$
5. $Y_3 = A \cdot (B - X_3) - C$

6. $Z_3 = 2Y_1 \cdot Z_1$

7. $Return\,(P_3 = X_3,\ Y_3,\ Z_3)$

Finally, we can calculate $(P_3(X_3, Y_3, Z_3) = 2P_1)$ where

$X_3 = A^2 - 2B$, $Y_3 = A \cdot (B - X_3) - C$ and $Z_3 = 2Y_1 \cdot Z_1$. Here we can use Urdhva-Tiryagbhyam and Dvandva-Yoga technique to evaluate $x_2 \cdot Z_1^2$, $y_2 \cdot Z_1^3$, $Z_1 \cdot C$, F^2, $G \cdot C^2$, $I \cdot F$ and $H \cdot C^2$.

5. ECDH KEY AGREEMENT SCHEME USING VEDIC TRI-LINEAR PAIRING MAP

A tri-linear pairing map using ECC [13] is given by:

$f^{n_1}{}_{a,b,c} : E[n_1] \times E[n_1] \times E[n_1] \rightarrow E[n_1]$,

where

$f^{n_1}{}_{a,b,c}(P,Q,R) = [\alpha_1(\beta_2\gamma_3 - \beta_3\gamma_2) + \beta_1(\alpha_3\gamma_2 - \alpha_2\gamma_3)$, here
$+\gamma_1(\alpha_2\beta_3 - \alpha_3\beta_2)].(aU + bV + cW)$

$\beta_2\gamma_3, \beta_3\gamma_2, \alpha_1(\beta_2\gamma_3 - \beta_3\gamma_2), \alpha_3\gamma_2, \alpha_2\gamma_3,$
$\beta_1(\alpha_3\gamma_2 - \alpha_2\gamma_3),\ \alpha_2\beta_3,\ a_3b_2$ and $\gamma_1(\alpha_2\beta_3 - \alpha_3\beta_2)$

Can be calculated by Urdhva-Tiryagbhyam technique.

The key compliance program system of EC Diffie Hellman it have followings three phases can be described as:

Phase-1: Is the key generation

- Alice (A) carries secret integer α, Bob (B) carries β and Carol (C) carries γ randomly where $\alpha, \beta, \gamma \in (1, s-1)$.
- $\alpha P, \beta P, \gamma P$ Computed and broadcasted the above values by them respectively.Now the system have these public values $(P, Q, R, \alpha P, \beta P, \gamma P, f^s_{a,b,c})$.

Phase-2: Is transmission

- 'A' measure $S_A = \alpha.\beta P.\gamma P = \alpha\beta\gamma P$ (because $P \in E[n_1]$) and $f^s{}_{a,b,c}(\alpha P, Q, R)$ she sends $h(S_A) f^s{}_{a,b,c}(\alpha P, Q, R)$ to 'B' and 'C'.
- 'B' measure $S_B = \beta.\alpha P.\gamma P = \alpha\beta\gamma P$ and $f^s{}_{a,b,c}(\beta P, Q, R)$. He sends $h(S_B) f^s{}_{a,b,c}(\beta P, Q, R)$ to 'A' and 'C'.
- C' measure $S_C = \gamma.\alpha P.\beta P = \alpha\beta\gamma P$ and $f^s{}_{a,b,c}(\gamma P, Q, R)$. He sends $h(S_C) f^s{}_{a,b,c}(\gamma P, Q, R)$ to 'A' and 'B'.

It is obvious that $S_A = S_B = S_C = \alpha\beta\gamma P = S_{ABC}$ (say).

Here $\alpha.\beta$, $\alpha\beta.\gamma$, $\beta.\alpha$, $\beta\alpha.\gamma$, $\gamma.\alpha$ and $\gamma\alpha.\beta$ can be figured by the use of AIVM Sutra Urdhva-Tiryagbhyam and Dvandva-Yoga.

Phase-3: Certification of Secret Share Key (SSK)

- 'A' accept
  $I_A = h(S_B) f^s{}_{a,b,c}(\beta P, Q, R) \square h(S_C) f^s{}_{a,b,c}(\gamma P, Q, R)$
  By bi-linearity of pairing $f^s{}_{a,b,c}$. After accept $I_A = h(S_{ABC})\beta\gamma f^s{}_{a,b,c}(P, Q, R)$. 'A' measure $h(S_A)^{-1} (\mathrm{mod}\, s)$ to access SSK $K_A = ah(S_A)^{-1} I_A$.

- Next 'B' accept
  $I_B = h(S_A) f^s{}_{a,b,c}(\alpha P, Q, R) \square h(S_C) f^s{}_{a,b,c}(\gamma P, Q, R)$
  $= h(S_{ABC})\alpha\gamma f^s{}_{a,b,c}(P, Q, R)$
  To access SSK, 'B' $h(S_B)^{-1} (\mathrm{mod}\, s)$ and measure his SSK as $K_B = \beta h(S_B)^{-1} I_B$.

- Lastly 'C' accept
  $I_C = h(S_A) f^s{}_{a,b,c}(\alpha P, Q, R) \square h(S_B) f^s{}_{a,b,c}(\beta P, Q, R)$
  $= h(S_{ABC}) abf^s{}_{a,b,c}(P, Q, R)$

  To access SSK 'C' determined $h(S_C)^{-1} (\mathrm{mod}\, s)$ and accesses his SSK as $K_C = \gamma h(S_C)^{-1} I_C$.

  It can be freely analyzing that $K_A = K_B = K_C = \alpha\beta\gamma f^s{}_{a,b,c}(P, Q, R) = K$ (say).

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

6. RESULT ANALYSIS AND COMPARISONS

There are following analyses of using AIVM in ECC, which are graphically explained in Fig.4. The Comparison between Size of Key and total processing time for RSA, ECC and VECC (Vedic Mathematics based ECC) in Fig.4. This complete graph shows that the encryption with the help of VECC display regular state feedback and considering that, the RSA has epidemic feedback for the processing time. The fig.4 displays approximately a steady state feedback for a different kind of equation of parabolic irrespective size of the key.

The VECC have needed very low time in the comparison of ECC and RSA. VECC plays the best role for the environment, when the power of processing, bandwidth, and space in storage are so limited. VECC gives speed and that speed gives the best advantages in the term of small key size and time in system processing. And the hand, the comparison is based on the number of arithmetic operations in the point doubling and point addition in JPC system over ECC (Elliptic Curve Cryptography) and VECC (Vedic Mathematics based Elliptic Curve Cryptography).

The total arithmetic operations such as multiplication, square are compared in table 1 and 2, which concludes that the numbers of arithmetic operations are less then to table 2 which is based on VECC. The arithmetic operations in ECC for point addition and point doubling are compared in fig.3 which also concludes that the numbers of arithmetic operations are less then to the purposed results. In table 3, 4, and 5 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.

Where, **M** is Number of multiplications**, S** is Number of Squares**, C** is Number of cube, $\mathbf{P_4}$ is Number of fourth power, **T** is Total number of Arithmetic Operations**.**

ECC (Prime Field)	M	S	C	P_4	T
Point addition	22	12	8	0	40
Point doubling	7	6	1	4	18

Table 1: Number of operations needed in addition and doubling of points in JPC System over ECC

ECC (Prime Field)	M	S	C	P_4	T
Point addition	6	3	1	0	10
Point doubling	4	3	0	2	09

Table 2: Number of operations needed in addition and doubling of points in JPC System over VECC.

4 Bits Running Time	Running Time Processed using Conventional Methods	Running Time Processed using Vedic Mathematics Sutras	Average of Reducing Time
Point Addition	0.010809 app. (s)	0.0026362 app. (s)	75.6114%
Point Doubling	0.0097559 app. (s)	0.0024454 app. (s)	74.9337%

Table 3. Synthesis results of point addition and point doubling

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 4. 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	Averageof 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 5. Synthesis results of point addition and point doubling

Volume 8, Issue 3
June 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

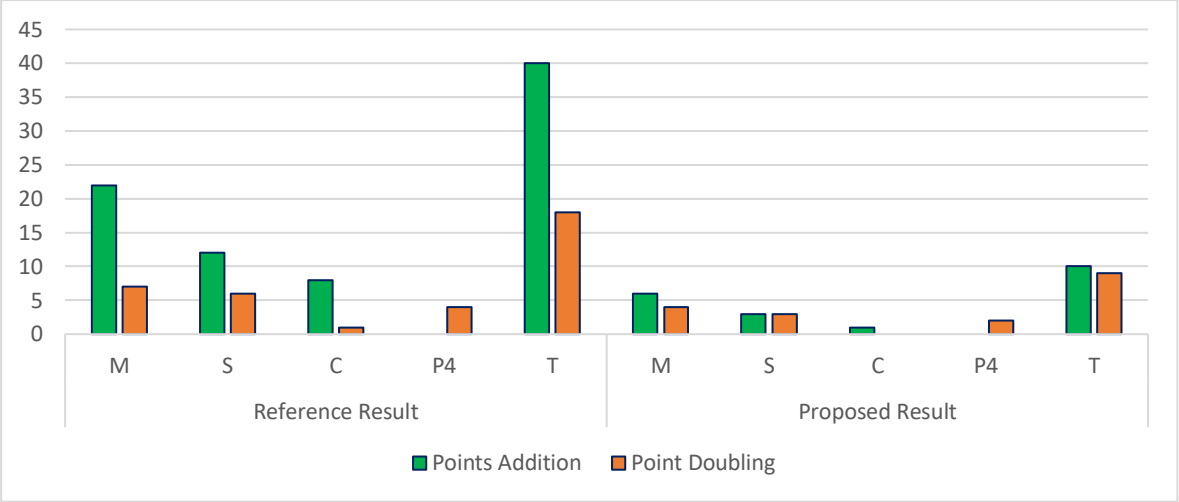

Fig. 3: Comparing the arithmetic operations in Point Addition and Point Doubling JPC system

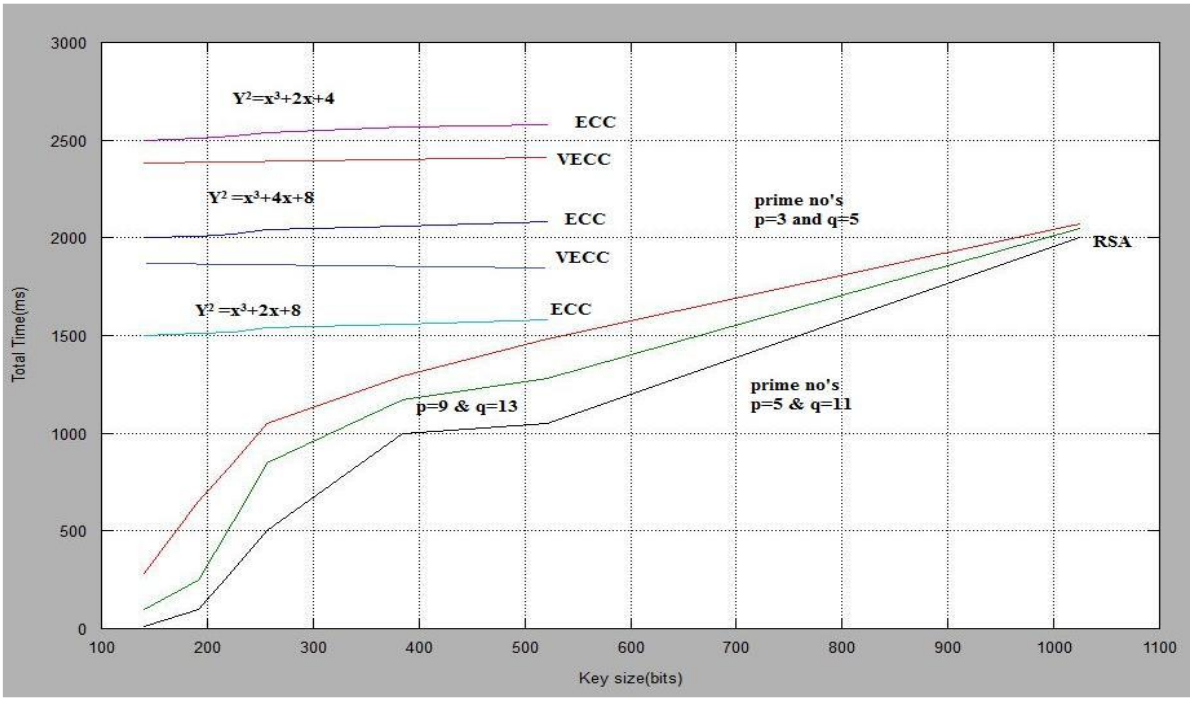

Fig.4: Comparison between Size of Key and total processing time for RSA, ECC and VECC (Vedic Mathematics based ECC)

7. CONCLUSION

This approach gives high security with the key which is too small in size. The Vedic based ECC performance is exceeding than the other cryptography for, example, El-Gamal, RSA and others. The speed of cryptographic operations (point addition and doubling) is found to be quicker. The work well displays the enhanced performance of AIVM based ECC, in the term of small size of the key, minimum time to develop the key and the full time which is required in processing. To be achieved better efficiency in storage space, processing power, power consumption or bandwidth are studded in the large-scale.

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 square of 4 bit, 8 bit, and 16 bit binary number, multiplication of two 4 bit, 8 bit, and 16 bit binary numbers. For cryptographic operations (point addition, point doubling) using Vedic Mathematics, the Average of Reducing Time is 70% (appx.) 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.

ACKNOWLEDGMENT

We would like to thank Swami Bharati Krishna Tirthaji for the wonderful Ancient Indian Mathematics that he created. His useful sixteen sutras will continue to inspire and helping

us in all branches of mathematics and several others to explore their applications in modern science and technologies. I also wish to acknowledge my sincere gratitude to the entire Gurukula Kangri Vishwavidyalaya, Haridwar (Uttarakhand).

REFERENCES

[1] Anchalya, R., Chiranjeevi, N.G., Kulkarni, S. "Efficient Computing Techniques using Vedic Mathematics Sutras". Electronic Instrumentation and control engineering. 3(5), 24-27, 2015.

[2] Dwivedi, S.P. "An Efficient Multiplication Algorithm Using Nikhilam Method, Data structure and algorithm. Cornell University Library", 2013.

[3] Kanhe, A., Das S.K., Singh A.K. "Design and implementation of low power multiplier using Vedic multiplication technique". International Journal of Computer Science and Communication. 3(1), 131-132, 2012.

[4] Kapse, Y.D., Sarangpure, P.R., Lokhande, K. M. "Review on a Compressor Design and Implementation of Multiplier using Vedic Mathematics". International Journal of Advanced Research in Computer and Communication Engineering. 6(2), 86-90, 2017.

[5] Karatsuba, A., Ofman, Y. "Multiplication of multi-digit numbers by automata", Soviet Physics-Doklady. 7, 595-596, 1963.

[6] Koblitz, N. "Elliptic Curve Cryptosystem". Journal of mathematics computation. 48(177), 203-209, 1987.

[7] Kumar, M., Gupta, P. "Cryptographic schemes based on Elliptic Curve over the Ring $Z_p[i]$." Applied Mathematics. 7(3), 304-312, 2016.

[8] Kumar, M., Gupta, P., Kumar, A. "A Novel and Secure Multi-party Key Exchange Scheme Using Tri-linear Pairing Map Based on Elliptic Curve Cryptography". International Journal of Pure and Applied Mathematics. 116(1), 1-14, 2017.

[9] Manjunath, K.M., Muralidhara, K.N., Chigateri, M.K., Manjuvani, K.M. "An Exhaustive Research Survey on Vedic ALU Design". International Journal of Innovative Research in Computer and Communication Engineering. 4(7), 13027-13034, 2016.

[10] Maria, R., Anitha, V. "Light Weight Asymmetric Cryptographic Algorithm for Financial Transactions through Mobile Application". International Journal of Computer Applications Foundation of Computer Science. N.Y., USA. 170(3), 37-41, 2017.

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

[12] Ramya, D.K., Revathy, R., Hemanandh, S. "Design of Complex Multiplier for FFT implementation using Vedic" Mathematics. International Research Journal of Engineering and Technology. 4(4), 446-449, 2017.

[13] Salim, S.M., Lakhotiya, S.A. "Implementation of RSA Cryptosystem Using Ancient Indian Vedic mathematics". International Journal of Science and Research. 4(5), 3221-3230, 2015.

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

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

[16] Washington L.C. "Elliptic Curves Number Theory and Cryptography", Chapman and Hall/CRC. United Kingdom 2008.

Author Profiles

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 fifteen research papers in reputed national and international Journals.

Mr. Ankur Kumar is a Research Scholar in the Department of Mathematics and Statistics, at Gurukula Kangri Vishwavidyalaya, Haridwar Uttrakhand (India). His research areas are Cryptography, Elliptic Curve Cryptography and Vedic Mathematic. He has been published more than four research papers in reputed national and international Journals.

Dr. Pratik Gupta is working as an assistant professor in the department of school of science at Jaipur National University, Jaipur (India). Areas of interest are Cryptography, and Network Security. He has been published more than five research papers in reputed national and international Journals.