International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Non-Linear Variant of Elliptic Curve Cryptography with Quadratic Residues over Finite Field

Ramachandran S [1], **Sindhu J Kumaar** *[2]

Submitted:11/03/2024 **Revised**: 26/04/2024 **Accepted**: 03/05/2024

Abstract: In the digital world security issues play an important role in data communications over unreliable network. Cryptography is most useful technique for transferring data in secure manner, the data sent is extremely expected to be received by authorized person over the public network. Since the Elliptic curve cryptography is introduced in 1985, elliptic curves have simulated a lot of research works in public key cryptography. At present, several cipher systems have been developed based on the Elliptic Curve Cryptography(ECC) for the purpose of secure data transformation. As security of ECC is related to hardness of discrete logarithm problem on elliptic curve (ECDLP) and there are endless possibilities to create cipher system using ECC we have used elliptic curves in a different way from the way in traditional ECC. In this paper, we have proposed a cipher system, called Quadratic Residue Non- linear Variant to ECC over the finite field F_p to intensify security and privacy

Keywords: *Cryptography, Decryption, Encryption, Functions, Elliptic curve cryptography, Finite field*

1. Introduction

In the modern world, information and communication technology is an essential part of society. As the secured data transmission is the major issue in communication system, cryptography successfully deals almost all security issues in data communication on public network. The reliable communication system means that which provides superior level security in the transmission of personal information and important documents. At present the whole world depends on internet and its applications in every part of life. Every second a sufficient amount of data is interchanged through unsecured channels in internet and it is indispensable to product data from unauthorized usage and harmful attacks.

For most of its history, cryptography is used to conceal military strategies and sensitive diplomatic secrets. Nakamoto. S. Bitcoin [18] has created crypto currency as an application of cryptography with block chain technology. Elliptical Curve Cryptography (ECC) is an encoding technique of data files so that only certain individuals can decode them. Srinivasa Rao O. et al [17] and Scott A. Vansfone [16] have stated that ECC key assures more security than RSA (Rivest R., Shamir A. and Adleman L. algorithm)[10] and DSA (Data Structures and Algorithms) key of the same size. Couvreur C. et al [7] has implemented a fast decryption algorithm for RSA public key cryptosystem. Neal Koblitz [19] has explained about the theory of numbers, algebraic group structure and finite field applications in cryptography. Also Neal Koblitz [1, 5, 12] has interpreted public key cryptosystems with elliptic curves arithmetic over finite fields.

T. El-Gamal [15] has independently developed a public key cryptosystem and a signature scheme based on the discrete logarithm problem. Miller Victor S [2] has expressed cryptographic use of Elliptic curves and proposed a new encryption algorithm, which is similar to Diffie - Hellman key exchange but faster than that. Kenji Koyama. et al [6] has developed a new trap door one-way function (TOF) based on elliptic curves over the Ring Z_n instead of elliptic curves over finite field F_P. A new RSA variant on elliptic curves is proposed by Maher Boudabra. et al [8]. S. Ullah et al [9] have given elaborate work about the challenges, recent advances and future trends on the applications of elliptic curves cryptography. Laiphrakpam Dolendro Sing et al [13] and S. Maria Celestin Vigila et al [14] have proposed elliptic curves cryptosystems for the secure communication of text message using Mathematica. Lawrence C. Washington [20] has given the proof to several theorems on elliptic curves. Hinek M [21] has written about cryptographic variants of RSA and its analysis in detail.

D. Sravana Kumar et al [3] and Lo'ai Tawalbeh et al [4] have mentioned that cryptography plays vital role in each layer of data transmission in the internet and it ensures the data integrity, security and confidentiality. The significant advantage of ECC than RSA is that working in less storage area with smaller key size. ECC is based on the Abelian group concept that it is possible to use the set of F_p rational points defined by an elliptic curve over finite prime field. Security and secrecy level of data communication through ECC is based on the hardness of discrete logarithm problem

[1] *Research Scholar, B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, INDIA*
ORCID ID : 0000-0001-9851-9385

[2] *B.S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, INDIA*
ORCID ID : 0000-0003-2785-9141

(DLP) on elliptic curves. In ECC, the point location on the elliptic curve is used to encrypt and decrypt the message. It is started with the brief introduction of the field “Cryptography”, some basic definitions and properties of elliptic curves in section 3. In Section 4, a new non - linear variant to Elliptic Curve Cryptography is proposed, in addition to that a numerical example is given to support the work.

2. Cryptography

The science of keeping communication private and the study of cyphers which are message sending techniques in disguised form so that only authorized individual can eliminate the disguise and look through the message, called Cryptography. Almost all ciphers in cryptography classified into two types [20], which are Private key cryptography and Public key cryptography, a single key used to encrypt and decrypt in private (symmetric) key cryptography. in the later, encrypting key can be made as public information so that anyone to read the secret messages. The RSA is the most famous one in public key cryptography, which is based on the difficulty of factorizing an integer into two primes. ECC is the best alternative to RSA in public key cryptography, it works with smaller key size compared to key used in RSA and its difficulty based on reaching solution to discrete logarithm problem on elliptic curves

3. Elliptic Curve Cryptography

Elliptic curves have been studied since seventeenth century [8], which has a long and glorious history. Elliptic curves are not ellipses. The elliptic functions, provided by problem of finding arc length of an ellipse and it satisfies the cubic equations. Here cubic curves are called elliptic curves, the most general form of elliptic curves in x and y are $y^2 + ay + b = x^3 + cx^2 + dx + e$. An elliptic curve is a one dimensional abelian group, equipped with a smooth projective group structure which is defined by rational maps. Elliptic curves are valid in any field, but in cryptography only the elliptic curve over finite field with large characteristic is considered. Almost in all applications of ECC, the Weierstrass equation is used, the equation is $y^2 = x^3 + cx + d$, where x, y are variables and the constants c, d are elements in the finite field F_p. Elliptic curve $E_p(c,d)$ is the set of all rational ordered pairs (x, y) which satisfies the equation $y^2 = x^3 + cx + d$, that is, $E_p(c,d) = \{(x.y) : y^2 = x^3 + cx + d\}$. Each rational ordered pair is called rational point (or point) on elliptic curves $E_p(c,d)$ and the order of the elliptic curves is denoted by $\#E_p(c,d)$. If the discriminant $4c^3 + 27d^2 \neq 0$ then $E_p(c,d)$ is non-singular elliptic curve.   Since any line passing through two points on elliptic curve intersects the curve in the third rational point, so that the addition of two different points is defined as the projection of third point about x - axis and adding a point to itself is same manner when the tangent line passing through the point is considered. In the case of vertical line, the addition of two points is point at infinity. The existence of a group law for adding points on the elliptic curve is one the most important property. The set of all rational points together with point at infinity over the finite field forms an abelian group [1], where the binary operations are point addition and point doubling.

3.1. Point Addition and Point Doubling

Let $E(c,d)\colon y^2 = x^3 + cx + d$ be an elliptic curve and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on it. The line through the points P and Q uniquely intersects the elliptic curve in third point R (see Fig. 1). The addition of two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ is $R = (x_3, -y_3)$, $x_3 = m^2 - x_1 - x_2 \; and \; y_3 = m(x_1 - x_3) - y_1$
where slope $m = \frac{y_2 - y_1}{x_2 - x_1} \; if \; P \neq Q$ and $m = \frac{3x_1^2 + A}{2y_1} \; if \; P = Q$. The addition of two different points P and Q is called Point addition (see Fig.1.) and if the point P is added to itself then the addition is called Point doubling (see Fig.1.)

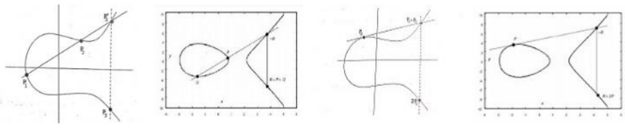

Fig.1. Point addition and Point doubling.

For any prime $p = 2(mod\ 3)$ and c ∊ F_p, Kenji Koyama. et al [6] have proved that the elliptic curve $E_p(0,d)$: $y^2 = x^3 + d$ is a cyclic group, there are exactly $(p-1)/2$ elements in finite field F_p, such that $x^3 + d$ having quadratic residues, including the point at infinity, the order of $E_p(0,d)$ is $p + 1$, that is, $\#E_p(0,d) = p + 1$. And also proved that for any prime $q = 3(mod\ 4)$, elliptic curve $E_q(c,0)$: $y^2 = x^3 + cx$ is a cyclic group, there are exactly $(q-1)/2$ elements in finite field F_q, such that $x^3 + cx$ having quadratic residues, including the point at infinity, the order of $E_q(c,0)$ is $q + 1$ that is, $\#E_q(c,0) = q + 1$ where, 0 < c < q.   For example, $p = 23 = 2(mod\ 3)$, and $c = 5 \in F_{23}$, the elliptic curve $E_{23}(0,5)$ has 24 points, that is, $E_{23}(0,5) = \{(1,12), (2,6), (3,3),$

$(4,0), (7,7), (10,4), (11,5), (12,13), (14,9), (18,8), (20,1), (22,2),$

$(1,11), (2,17), (3,20), (7,16), (10,19), (11,18), (12,10), (14,14),$

$(18,15), (20,22), (22,21), \mathcal{O}_{23}\}$, where $\mathcal{O}_{23}$ is point at infinity, and the order of $E_{23,}(0,5)$ is 24, that is, $\#E_{23}(0,5) = 24$. This example leads to the proposed work that the construction of a non-linear variant to elliptic curve cryptography with quadratic residues over finite field.

4. Proposed Work

The work non - linear variant to ECC for providing security in data communication. The hyperbola passing through two points on elliptic curve intersects in two more points (see Fig. 2.). For each $x \in F_p$ and $a \in F_p$ such that $x \leq -a$ or $x \geq a$, there are two real values for $y \in F_p$, which satisfy the hyperbola H: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ and the values of are

$$y = \pm \frac{b}{a}\sqrt{x^2 - a^2} \tag{1}$$

With this property it is possible to define the binary operator, called point addition of two different points on the elliptic curve $E_p(c, d)$ in different manner as follow. Let

$$E_p(c, d)\!: \; y^2 = x^3 + cx + d \tag{2}$$

be the elliptic curve with non-singular condition , $4c^3 + 27d^2 \neq 0$. And let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, $P \neq Q$ be two rational points on it. The hyperbola H: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ passing through two points P and Q intersects elliptic curve in two points R' and R $(= -R')$, clearly R', R are different from $P, Q, -P, -Q$ and they are symmetric about x axis (see Fig. 2.). Since the hyperbola H intersects elliptic curve $E_p(c, d)$ in two symmetric points R' and R about x axis. From the equation 2. the positive value of y is obtained by

$$y = \sqrt{x^3 + cx + d} \tag{3}$$

the hyperbola $\boldsymbol{H}$ passing through two points $\boldsymbol{P}$ and $\boldsymbol{Q}$ which intersects the elliptic curve $\boldsymbol{E_p(c, d)}$ at the point $\boldsymbol{R'} = (\boldsymbol{x_3}, \boldsymbol{y_3})$, Reflection of $\boldsymbol{R'}$ across the x- axis is $\boldsymbol{R}$= $(\boldsymbol{x_3}, \boldsymbol{y_3})$ (see Fig. 3. & 4.). The addition of the points $\boldsymbol{P}$ and $\boldsymbol{Q}$ as $\boldsymbol{P} + \boldsymbol{Q} = \boldsymbol{R}$, the coordinate of $\boldsymbol{R}$ is the coordinates combination of $\boldsymbol{P}$ and $\boldsymbol{Q}$.

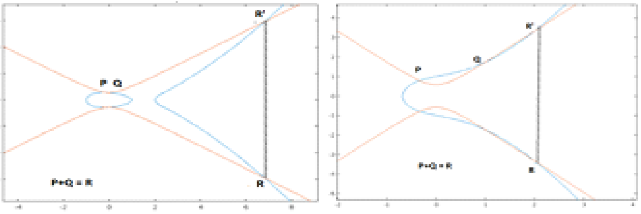

Fig. 2. The Addition of two Point.

the hyperbola H: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ can be re written as

$$y^2 = \frac{b^2}{a^2}(x^2 - a^2) \tag{4}$$

Combining the equations (2) and (4) we have a cubic polynomial equation

$$x^3 - \frac{b^2}{a^2}\, x^2 + cx + b^2 + d = 0 \tag{5}$$

There are three roots for cubic polynomial equation in which at least one of them is real, if the roots are x_1, x_2, x_3, equation 3. gives the values y_1, y_2 , y_3 of y corresponding to x_1, x_2, x_3. By the properties of roots of polynomial, sum and product of the roots are $x_1 + x_2 + x_3 = \frac{b^2}{a^2}$ and $x_1 x_2 x_3 = -b^2 - d$ respectively, so that

$$x_3 = \frac{b^2}{a^2} - x_1 - x_2 \tag{6}$$

Since x_1 and x_2 are roots, the points P, Q are in $E_p(c, d)$ and H, the equation 3. gives third point $R' = (x_3\,, y_3)$. The y-coordinate of R' is obtained as follow, the points P and Q are on hyperbola H, the two equations are obtained

$$\frac{{x_1}^2}{a^2} - \frac{{y_1}^2}{b^2} = 1 \tag{7}$$

$$\frac{{x_2}^2}{a^2} - \frac{{y_2}^2}{b^2} = 1 \tag{8}$$

By solving equations 7. & 8. using Cramer's rule, values of a and b are obtained from the equations

$$\frac{1}{a^2} = \frac{\begin{vmatrix} 1 & -{y_1}^2 \\ 1 & -{y_2}^2 \end{vmatrix}}{\begin{vmatrix} {x_1}^2 & -{y_1}^2 \\ {x_2}^2 & -{y_2}^2 \end{vmatrix}} \tag{9}$$

and

$$\frac{1}{b^2} = \frac{\begin{vmatrix} {x_1}^2 & 1 \\ {x_2}^2 & 1 \end{vmatrix}}{\begin{vmatrix} {x_1}^2 & -{y_1}^2 \\ {x_2}^2 & -{y_2}^2 \end{vmatrix}} \tag{10}$$

Equations 9. & 10. implies that

$$\frac{b^2}{a^2} = \frac{\begin{vmatrix} 1 & -{y_1}^2 \\ 1 & -{y_2}^2 \end{vmatrix}}{\begin{vmatrix} {x_1}^2 & 1 \\ {x_2}^2 & 1 \end{vmatrix}} \tag{11}$$

The point $R' = (x_3\,, y_3)$ in terms of x_1 and x_2 is given by the equations

$$x_3 = \frac{\begin{vmatrix} 1 & -{y_1}^2 \\ 1 & -{y_2}^2 \end{vmatrix}}{\begin{vmatrix} {x_1}^2 & 1 \\ {x_2}^2 & 1 \end{vmatrix}} - x_1 - x_2 \tag{12}$$

and

$$y_3 = \sqrt{{x_3}^3 + cx_3 + d} \tag{13}$$

Hence the point addition of two different points P and Q in this work is defined as $P + Q = R$, where. $R = (x_3\,, -y_3)$. And adding a point to itself (Point Doubling) is as in the work of Koblitz Neal. et al [1], that is, for any point $P = Q = (x_0, y_0)$, $P + Q = R$ (see Fig. 3.) where $R = (x_3\,, -y_3)$ and

$$x_3 = \left(\frac{3{x_0}^2 + c}{2y_0}\right)^2 - 2x_0 \tag{14}$$

$$y_3 = -y_0 + \left(\frac{3{x_0}^2 + c}{2y_0}\right)(x_0 - x_3) \tag{15}$$

and the gradient of the tangent at $P = (x_0, y_0)$ is

$m = \frac{3{x_0}^2+c}{2y_0}$; $y_0 \neq 0$

(16)

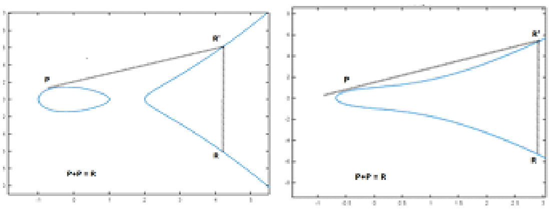

Fig. 3. Adding a point to itself.

Suppose $x_1 = x_2$ but $y_1 \neq y_2$. Then the line passing through P and Q is a vertical line. Since every vertical line passes through the point at infinity $\mathcal{O} = [0:1:0]$ and also on E. thus the line intersects E at this point. Reflecting this point across the x- axis gives the point [0:-1:0]= [0:1:0]. Therefore $P + Q = \mathcal{O}$, P $+ \mathcal{O} = P$ and $\mathcal{O} + \mathcal{O} = \mathcal{O}$. Point at infinity $\mathcal{O}$ acts as additive identity.

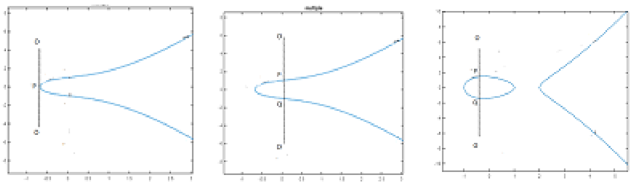

Fig. 4. Adding two vertical points.

4.1. Nature of Addition

Addition of two different points $P = (x_1, y_1)$ and $Q = (x_1, y_1)$ is $R = (x_3, -y_3)$, since $R = (x_3, -y_3)$ is a point on the hyperbola H, it satisfies H, that is, $\frac{{x_3}^2}{a^2} - \frac{{y_3}^2}{b^2} = 1$, which implies that $y_3 = \pm\frac{b}{a}\sqrt{{x_3}^2 - a^2}$, y_3 is rational number if and only if ${x_3}^2 - a^2 \geq 0$, so that $x_3 \leq -a$ or $x_3 \geq a$. The eccentricity of hyperbola is $e = 1 + \frac{b^2}{a^2}$.

4.2. Group Law

The binary operators *point addition* (adding two different points) and *point doubling* (adding a point to itself) on the set of rational points as follow. If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two points on elliptic curve $E(c, d)$ then the point addition is defined as

(i) If $x_1 \neq x_2$ then $P + Q = R$,
where $R = (x_3, -y_3)$, $x_3 = \lambda - x_1 - x_2$, $y_3 = \sqrt{{x_3}^3 + cx_3 + d}$ and $\lambda = \frac{b^2}{a^2} = \frac{\begin{vmatrix} 1 & -{y_1}^2 \\ 1 & -{y_2}^2 \end{vmatrix}}{\begin{vmatrix} {x_1}^2 & 1 \\ {x_2}^2 & 1 \end{vmatrix}}$

(ii) If $x_1 = x_2$ but $y_1 \neq y_2$ then $P + Q = \mathcal{O}$

(iii) If $P = Q$ that is $x_1 = x_2 = x_0$ and $y_1 = y_2 = y_0 \neq 0$ then $P + Q = R$ where $R = (x_3, -y_3)$, $x_3 = \lambda^2 - 2x_0$, $y_3 = -y_0 + \lambda(x_0 - x_3)$ and $\lambda = \frac{3{x_0}^2+c}{2y_0}$

(iv) If P $= Q$ and $y_0 = 0$ then $P + Q = \mathcal{O}$. Moreover P $+ \mathcal{O} = P$ for all points P on $E(c, d)$

5. Example

Let $E(c, d) : y^2 = x^3 + cx + d$ be an elliptic curve with coefficients from F_p, the set of all rational points on elliptic curve $E(c, d)$ over finite field F_p is denoted by $E(F_p) = \{(x, y) : y^2 - x^3 - cx - d = 0, \ x, \ y \in F_p\} \cup \{\mathcal{O}\}$ where $\mathcal{O}$ is point at infinity. The set $E(F_p)$ with above binary operator is a group in the finite field F_p. Consider the elliptic curve $E(1,1)$: $y^2 = x^3 + x + 1$ over the finite field F_5. Maher Boudabra. et al [8]. has explained that direct computation to find the set of all rational points on the elliptic curve $E(F_5) = \{(0, \pm1), (2, \pm1), (3, \pm1), (4, \pm2)\} \cup \{\mathcal{O}\}$, for example, if x=0 then $E(1,1) : y^2 = 1 \ (mod \ 5)$ implies $y = \pm1$, two points$(0, \pm1)$ are obtained, similarly if $x = 2$ then $E(1,1) : y^2 = 8 + 2 + 1 = 1 \ (mod \ 5)$ implies $y = \pm1$, got two points $(2, \pm1)$. Thus $E(F_5)$ is an abelian group and $\#E(1,1) = 9$ over the finite field F_5.

5.1. Point Addition for two different points $\mathbf{P_1}$ and $\mathbf{Q_1}$

Let $P_1 = (0, 1)$ and $Q_1 = (2\ ,1)$ be two points in $E(F_5)$, Here $x_1 = 0$, $x_2 = 2$, $y_1 = 1$, and $y_2 = 1$, using group law (i), the value of $\lambda = \frac{\begin{vmatrix} 1 & -{y_1}^2 \\ 1 & -{y_2}^2 \end{vmatrix}}{\begin{vmatrix} {x_1}^2 & 1 \\ ,{x_2}^2 & 1 \end{vmatrix}} = \frac{\begin{vmatrix} 1 & -1 \\ 1 & -1 \end{vmatrix}}{\begin{vmatrix} 0 & 1 \\ 4 & 1 \end{vmatrix}} = 0 \ (mod \ 5)$, $x_3 = 0 - 0 - 2 = -2 = 3(mod \ 5)$ and $y_3 = \sqrt{3^3 + 3 + 1} = 1 \ (mod \ 5)$, thus $R_1 = (x_3, -y_3) = (3, -1) = (3, 4)(mod \ 5)$. Hence $P_1 + Q_1 = R_1$, that is $(0, 1) + (2\ ,1) = (3, 4)$. And let $P_2 = (2, 1)$ and $Q_2 = (4, 2)$ be another two points, then $\frac{b^2}{a^2} = \frac{\begin{vmatrix} 1 & -1 \\ 1 & -4 \end{vmatrix}}{\begin{vmatrix} 4 & 1 \\ 16 & 1 \end{vmatrix}} = 4$, $x_3 = -2 = 3$ and $y_3 = 1$, thus $P_2 + Q_2 = R_2 = (3, \ -1) = (3, 4)$.

5.2. Point doubling for single point $\mathbf{P_1}$

Let $P_1 = (0, 1)$, For finding $2P_1$ and $3P_1$, here $x_0 = 0$, $y_0 = 1$, Using group law (iii), $\lambda = \frac{3{x_0}^2+c}{2y_0} = \frac{1}{2}\lambda^2 = \left(\frac{1}{2}\right)^2 = \frac{1}{4} = \frac{16}{4} = 4(mod \ 5)$, $x_3 = \lambda^2 - 2x_0 = 4$ and $y_3 = -y_0 + \lambda(x_0 - x_3) = -1 + 4(0 - 4) = -17 = -2 = 3 \ mod \ (5)$, therefore $2P_1 = (x_3, -y_3) = (4, -3) = (4, 2)$. Similarly $3 \ P_1 = (2, 4)$ and $4P_1 = (3, \ 4)$. It can easily be proved that $E(F_5)$ is a group, in particular which is a cyclic group with generator P_1, that is $E(F_5) =< P_1 >$.

6. Conclusion

Using elliptic curves, in this work, a new public key cryptographic technique is proposed, which is a non-linear variant to ECC. The operator point addition is defined in different way with the property that every hyperbola passes through any two points on elliptic curve intersects the elliptic curve in another two different points, which are symmetrical points about x –axis. An example has been given for the elliptic curves having $(p-1)/2$ quadratic residue elements to support the cryptosystem. Also proposed cryptosystem is demonstrated with an example. Public key cryptosystems are increasingly being used by organizations and ECC is a central part of database management. Since security is an important component in the communication system, proposed cryptosystem would be a better alternative to ECC for providing high level security in data transmission. And this technique assures the cipher text more confused. In future, comparative study of proposed cryptosystem NLECC (Non-Linear Elliptic Curve Cryptography) with ECC will be carried out, also advantages and disadvantages will be studied while using this technique in Diffie - Hellman Key Exchange and El Gamal Public Key Encryption algorithm.

Acknowledgements

The author Ramachandran S is very much indebted to the management of *Raak* College of Engineering and Technology, Pondicherry. for continuous support to do the research work in the field of cryptography, and very grateful to Mrs. R. Dhanalakshmi, Manager, Agriculture market committee, Sethiathoppu, Tamil Nadu. for the moral support and encouragement.

Author contributions

Ramachandran S: Conceptualization, Writing-Original draft preparation, Visualization **Sindhu J Kumaar:** Investigation, Visualization, Reviewing- Original the draft.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Neal Koblitz, “Elliptic Curve Cryptosystems,” Mathematics of Computation, vol. 48, issue 177, pp. 203–209, January 1987.

[2] S. Miller Victor, "Use of elliptic curves in cryptography," In Advances in Cryptology-CRYPTO'85 Proceedings, Springer Berlin Heidelberg, pp. 417-426. 1985.

[3] D. Sravana Kumar, Ch. Suneetha and A. Chandrasekhar. “ Encryption of Data Using Elliptic Curve Over Finite Fields,” International Journal of Distributed and Parallel Systems (IJDPS), no. 1, vol. 3, January 2012.

[4] Lo’ai Tawalbeh, Moad Mowafi and Walid Aljoby. “Use of Elliptic Curve Cryptography for Multimedia Encryption,” IET Information Security, vol. 7, issue 2, pp. 67–74, 2012.

[5] Koblitz Neal, Alfred Menezes and Scott Vanstone. “The state of elliptic curve cryptography,” In Towards a quarter - century of public key cryptography, Springer US, pp. 103-123, 2000.

[6] K. Koyama, U.M.Maurer, T. Okamoto and S.A. Vanstone, “New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n,” In Annual International Cryptology Conference; Lecture Notes in Computer Science 576, Springer, Berlin/Heidelberg, Germany, pp. 252–266, 1991.

[7] C. Couvreur and J.J. Quisquater, “ Fast Decipherment Algorithm for RSA Public-Key Cryptosystem,” Electron. Lett., vol.18, pp. 905–907, 1982.

[8] Maher Boudabra and Abderrahmane Nitaj, “A New RSA Variant Based on Elliptic Curves,” Cryptography 2023, 7, 37.

[9] S. Ullah, J. Zhen and N. Din et al, “Elliptic Curve Cryptography, Applications, challenges, recent advances, and future trends: A comprehensive survey,” Computer Science Review 47, 2023.

[10] R. Rivest, A. Shamir and L. Adleman, “A Method for Obtaining signatures and public-key cryptosystems,” Commun. ACM, vol. 21, pp. 120–126, 1978.

[11] H.M. Sun, M.E. Wu, W.C. Ting and M.J. Hinek, “Dual RSA and its security analysis,” Digital IEEE Trans. Inf. Theory, vol. 53, 2007.

[12] N. Koblitz, “Elliptic curve cryptosystems,” Math. Comput., Vol. 48, pp. 203–209, 1987.

[13] Laiphrakpam Dolendro Sing and Khumanthem Manglem Singh, “Implementation of Text Encryption using Elliptic Curve Cryptography,” Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015) Procedia Computer Science, vol. 54, pp, 73 - 82, 2015.

[14] S. Maria Celestin Vigila and K. Muneeswaran, “Implementation of Text based Cryptosystem using Elliptic Curve Cryptography,” International Conference on Advanced Computing, IEEE, pp. 82–85, December 2009.

[15] T. El-Gamal, "A public key cryptosystem and a signature scheme based on the discrete logarithm," IEEE Transactions on Information Theory, vol. 31, no. 1, pp. 469-472, 1985.

[16] Scott A. Vansfone, “Elliptic Curve Cryptography-The Answer to Strong, Fast Public-Key Cryptography for Securing Constrained Environments,” Information Security Technical Report, vol. 2, no. 2, pp. 78–87, 1997.

[17] O. Srinivasa Rao and S. Pallam Setty, “Efficient Mapping Methods for Elliptic Curve Cryptography,”

International Journal of Engineering Science and Technology, vol. 2, pp. 3651–3656, 2010.

[18]Nakamoto. S. Bitcoin, “A Peer-to-Peer Electronic Cash System,” 2009, Available online: https://bitcoin.org/bitcoin.pdf.

[19]Neal Koblitz, A Course in Number Theory and Cryptography. Second edition , Springer-Verleg, 1994.

[20]Lawrence C. Washington, Elliptic curves: Number Theory and Cryptography. Second edition, Chapman & Hall/CRC, New York, 2006.

[21]M. Hinek, Cryptanalysis of RSA and its Variants. Cryptography and Network Security Series, Chapman & Hall/CRC Press, Boca Raton, FL, USA, 2009.