A Diffie-Hellman Encryption Scheme over Elliptic Curves using Golden Matrices

Ravi Kumar Bora, Sridhar Akiri, VSantosh Kumar

Abstract: In this paper, we proposed Diffie-Hellman encryption scheme based on golden matrices over the elliptic curves. This algorithm works with a bijective function defined as characters of ASCII from the elliptic curve points and the matrix developed the additional personal key, which was obtained from the golden matrices.

Keywords: Diffie-Hellman, decryption, elliptic curves, encryption, golden matrices.

I. INTRODUCTION

In 1976, Diffie and Hellman developed the public key cryptography dependent on the use of two keys one is a personal key and the other a more or less similar public key form user name and password[4]. Most personal key problems have been overcome after the creation of public key cryptography. Public key authentication is the creation of enormous development in the past of cryptography. The main cryptosystem for the public key is Elliptic Curve Cryptography (ECC) that also ensures better safety bit than other public key cryptosystem known today and ECC can utilize significantly shorter key and offer the equal rate of safety as other much larger asymmetric algorithms, thereby reducing processing overhead. Protection of these public key cryptosystems depends on number of computational problems which are well known to perform as one way [2]. The key agreement protocol of Diffie-Hellman is frequently used to safe key replace through unrestricted networks[3].

A. Fibonacci Q_α -matrix

The number theory of Fibonacci determines the prospect of modern utilization for technical outcomes view in last decades [8][12].

The Fibonacci Q_α -matrix was suggested in [10], where

$$Q_\alpha = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad (1)$$

is derive from the recurrence relation of Fibonacci

$G\vartheta'_{l+1} = G\vartheta'_l + G\vartheta'_{l-1.}$ (2)

With $G\vartheta'_1 = G\vartheta'_2 = 1.$ (3)

Later Q_α was extended to $Q_\alpha{}^l$ for integer l [],

$$Q_\alpha{}^l = \begin{pmatrix} G_\vartheta{}'_{l+1} & G_\vartheta{}'_l \\ G_\vartheta{}'_l & G_\vartheta{}'_{l-1} \end{pmatrix}, \ (4)$$

consequently the similarity between $det\ Q_\alpha{}^l$ and the "Cassini formula",

$Det\ Q_\alpha{}^l = G\vartheta'_{l+1}G\vartheta'_{l-1} - G\vartheta'_l{}^2 = (-1)^l.$ (5)

B. The "Golden" Matrices

The "golden" matrices [5] which are the continuous functions of the variable ν being defined by A.P Stakhov with the help of the classical Fibonacci Q_α -matrix and the symmetrical hyperbolic Fibonacci functions, as follows[6][7][9][11].

$$Q_\alpha{}^{2\nu} = \begin{pmatrix} CG_{s_\kappa}(2\nu+1) & SG_{s_\kappa}(2\nu) \\ SG_{s_\kappa}(2\nu) & CG_{s_\kappa}(2\nu-1) \end{pmatrix}, \quad (6)$$

$$Q_\alpha{}^{2\nu+1} = \begin{pmatrix} SG_{s_\kappa}(2\nu+2) & CG_{s_\kappa}(2\nu+1) \\ CG_{s_\kappa}(2\nu+1) & SG_{s_\kappa}(2\nu) \end{pmatrix}. \quad (7)$$

$$where\ \ SG_{s_\kappa}(\nu) = \frac{\tau_\eta{}^\nu - \tau_\eta{}^{-\nu}}{\sqrt{5}}, CG_{s_\kappa}(\nu) = \frac{\tau_\eta{}^\nu + \tau_\eta{}^{-\nu}}{\sqrt{5}}$$

$$and\ \tau_\eta = \frac{1+\sqrt{5}}{2}(the\ Golden\ proportion).$$

The inverse matrices for (6) and (7) are developed by A.P Stakhov [5] for the continuous variable ν as the following form.

$$Q_\alpha{}^{-2\nu} = \begin{pmatrix} CG_{s_\kappa}(2\nu-1) & -SG_{s_\kappa}(2\nu) \\ -SG_{s_\kappa}(2\nu) & CG_{s_\kappa}(2\nu+1) \end{pmatrix}, \qquad (8)$$

$$Q_\alpha{}^{-(2\nu+1)} = \begin{pmatrix} -SG_{s_\kappa}(2\nu) & CG_{s_\kappa}(2\nu+1) \\ CG_{s_\kappa}(2\nu+1) & -SG_{s_\kappa}(2\nu+2) \end{pmatrix}. \qquad (9)$$

In this paper, we proposed Diffie-Hellman elliptic curve encryption scheme and the secret key has been formed by the matrix, acquired from golden matrices defined by A.P Stakhov[5].

II. PROPOSED ALGORITHM

Romeo needs to deliver the message to Juliet using Diffie-Hellman elliptic curve encryption with the golden matrices. Romeo prefers the elliptic curve $y^2 = x^3 + ux + v$above the field $Z^*_{p.}$ By selecting the point $Q' = (x, y)$ on the elliptic curve and a personal key *'l'*, Romeo has generated the public key β = *'lQ''*.

In this regard, Juliet also has chosen a personal key *'m'* and creates the public key γ = *'mQ''*.

Revised Manuscript Received on December 13, 2019.

***** Correspondence Author

BRavi Kumar,Department of Mathematics,GIS,GITAM (Deemed to be University), Visakhapatnam, INDIA.Email: ravikumarbrk6@gmail.com

Dr. Sridhar Akiri,Department of Mathematics, GIS,GITAM (Deemed to be University), Visakhapatnam, INDIA.Email: akirisridhar@gmail.com

V Santosh Kumar, Department of ECE,GIT,GITAM (Deemed to be University),Visakhapatnam,INDIA.
Email: santoshkumar.velagala@gitam.edu

Table I: The certain pattern of the direct 'golden' matrices $Q_{\alpha}^{2\nu}$:

ν	*0*	*1*	*2*	*3*	*4*	*5*
$Q_{\alpha}^{2\nu}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$	$\begin{pmatrix}2 & 1\\1 & 1\end{pmatrix}$	$\begin{pmatrix}5 & 3\\3 & 2\end{pmatrix}$	$\begin{pmatrix}13 & 8\\8 & 5\end{pmatrix}$	$\begin{pmatrix}34 & 21\\21 & 13\end{pmatrix}$	$\begin{pmatrix}89 & 55\\55 & 34\end{pmatrix}$
$Q_{\alpha}^{-2\nu}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & -1\\-1 & 2\end{pmatrix}$	$\begin{pmatrix}2 & -3\\-3 & 5\end{pmatrix}$	$\begin{pmatrix}5 & -8\\-8 & 13\end{pmatrix}$	$\begin{pmatrix}13 & -21\\-21 & 34\end{pmatrix}$	$\begin{pmatrix}34 & -55\\-55 & 89\end{pmatrix}$

A. Encryption

Romeo selects Juliet's public key $\gamma = mQ'$ and then evaluates $l\gamma = l(mQ')$. He requires sending the message to Juliet, he transforms the text in the elliptic curve points and adopts a point '*þ'*'as the generator of the elliptic curve cyclic group. Let $A' = \{1þ', 2þ', 3þ'\ldots\ldots nþ'\}$ and set B' characters of ASCII. Set h': $A^{'} \rightarrow$ B' as $h'(n\rho') = \grave{a}'_n$, where $n = 1, 2, \ldots.$ and{ $\grave{a}'_{1}, \grave{a}'_{2}, \grave{a}'_{3,\ldots\ldots}$ } are the characters of ASCII which is the first step of protection.

Then the set

$\mu = \{\grave{a}'_1(æ_1, ý_1), \grave{a}'_2(æ_2, ý_2), \grave{a}'_3(æ_3, ý_3), \grave{a}'_4(æ_4, ý_4), \ldots.\}$(10)

where $\grave{a}'_i \in$ A and $(æ_i, ý_i) \in E$. Alice chooses the initial four points $\grave{a}'_1, \grave{a}'_2, \grave{a}'_3, \grave{a}'_4$ of (10) and arranges in a 2×2-square matrix.

$$\vartheta = \begin{pmatrix} \grave{a}'_1 & \grave{a}'_2 \\ \grave{a}'_3 & \grave{a}'_4 \end{pmatrix}. \qquad (11)$$

The original matrix ϑ can be viewed as a message in which there are 4 factorial i.e. 24 variants permutations from the four points to form the matrix (11). Let us fix the j^{th}permutation by $j = 1, 2, 3\ldots..24$. This is the second four point protection step, $\grave{a}'_1$, $\grave{a}'_2$, $\grave{a}'_3$, $\grave{a}'_4$ which is a permutation$P_j$choice.

Romeo prefers a direct "golden matrices" (6), (7) and then the enciphering matrix by taking the personal key ' $\nu = y_1$', which is the third step of protection of elliptic curve encryption method, based on "golden" matrices.

$$\vartheta \times Q^{2y_1} = \begin{pmatrix} \grave{a}'_1 & \grave{a}'_2 \\ \grave{a}'_3 & \grave{a}'_4 \end{pmatrix} \times \begin{pmatrix} CG_{s_\kappa}(2y_1+1) & SG_{s_\kappa}(2y_1) \\ SG_{s_\kappa}(2y_1) & CG_{s_\kappa}(2y_1-1) \end{pmatrix}$$

$$= \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix}. \qquad (12)$$

where

$$\chi_1 = \grave{a}'_1\, CG_{s_\kappa}(2y_1+1) + \grave{a}'_2\, SG_{s_\kappa}(2y_1), \qquad (13)$$

$$\chi_2 = \grave{a}'_1\, SG_{s_\kappa}(2y_1) + \grave{a}'_2\, CG_{s_\kappa}(2y_1-1), \qquad (14)$$

$$\chi_3 = \grave{a}'_3\, CG_{s_\kappa}(2y_1+1) + \grave{a}'_4\, SG_{s_\kappa}(2y_1), \qquad (15)$$

$$\chi_4 = \grave{a}'_3\, SG_{s_\kappa}(2y_1) + \grave{a}'_4\, CG_{s_\kappa}(2y_1-1). \qquad (16)$$

or

Or

$$\vartheta \times Q^{2y_1+1} = \begin{pmatrix} \grave{a}'_1 & \grave{a}'_2 \\ \grave{a}'_3 & \grave{a}'_4 \end{pmatrix} \times \begin{pmatrix} SG_{s_\kappa}(2y_1+2) & CG_{s_\kappa}(2y_1+1) \\ CG_{s_\kappa}(2y_1+1) & SG_{s_\kappa}(2y_1) \end{pmatrix}$$

$$= \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix}. \qquad (17)$$

Then the encrypted points are,

$\beta = \{\chi_1, \chi_2, \chi_3, \chi_4\}$. (18)

Romeo finally computes $\lambda_i = \chi_i + l(mQ')$ to send the encrypted message λ_i publicly to Juliet.

B. Decryption

To reclaim the plaintext from 'λ_{i}', Juliet has executed the decryption method.

First, Juliet selects his own personal key '*m*' and multiplies with Romeo public key β = 'lQ'', i.e. mlQ' and then finds the inverse of mlQ' i.e. $-mlQ'$ and finally he adds $-mlQ'$ to the encrypted message λi i.e. $\chi_i + lmQ' - lmQ' = \chi_i$.

After decryption, the recovered points has been arranged in 2×2 matrices,

$$\sigma = \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix}. \quad (19)$$

Now Juliet multiplies the recovered points with the inverse of golden matrix which is a personal key.

$$\sigma \times Q^{-2y_1} = \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix} \times \begin{pmatrix} CG_{s_\kappa}(2y_1-1) & -SG_{s_\kappa}(2y_1) \\ -SG_{s_\kappa}(2y_1) & CG_{s_\kappa}(2y_1+1) \end{pmatrix}$$

$$= \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix}, \qquad (20)$$

where

$$p_{11} = \chi_1 CG_{s_\kappa}(2y_1-1) - \chi_2 SG_{s_\kappa}(2y_1), \qquad (21)$$

$$p_{12} = -\chi_1 SG_{s_\kappa}(2y_1) + \chi_2 CG_{s_\kappa}(2y_1+1), \qquad (22)$$

$$p_{21} = \chi_3 CG_{s_\kappa}(2y_1-1) - \chi_4 SG_{s_\kappa}(2y_1), \qquad (23)$$

$$p_{22} = -\chi_3 SG_{s_\kappa}(2y_1) + \chi_4 CG_{s_\kappa}(2y_1-1). \qquad (24)$$

By replacing $\chi_1, \chi_2, \chi_3, \chi_4$ in the above expressions we get.

$$\begin{aligned} p_{11} &= [\grave{a}'_1\, CG_{s_\kappa}(2y_1+1) + \grave{a}'_2\, SG_{s_\kappa}(2y_1)]CG_{s_\kappa}(2y_1-1) \;- \\ &\quad [\grave{a}'_1\, SG_{s_\kappa}(2y_1) + \grave{a}'_2\, CG_{s_\kappa}(2y_1-1)]SG_{s_\kappa}(2y_1) \\ &= \grave{a}'_1\, CG_{s_\kappa}(2y_1+1)\, CG_{s_\kappa}(2y_1-1) + \\ &\quad \grave{a}'_2\, SG_{s_\kappa}(2y_1)\, CG_{s_\kappa}(2y_1-1) - \grave{a}'_1\, SG_{s_\kappa}(2y_1)\, SG_{s_\kappa}(2y_1) \\ &\quad - \grave{a}'_2\, CG_{s_\kappa}(2y_1-1) SG_{s_\kappa}(2y_1) \\ &= \grave{a}'_1\{CG_{s_\kappa}(2y_1+1)\, CG_{s_\kappa}(2y_1-1) - \{SG_{s_\kappa}(2y_1)\}^2. \quad (25) \end{aligned}$$

Using the fundamental identity [6] the decrypted point is,

$$p_{11} = \grave{a}'_1, \qquad (26)$$

$$p_{12} = \grave{a}'_2, \qquad (27)$$

$p_{21} = \grave{a}'_3$, (28)

$p_{22} = \grave{a}'_4$. (29)

The decrypted points are,

$$\begin{pmatrix} \grave{a}'_1 & \grave{a}'_2 \\ \grave{a}'_3 & \grave{a}'_4 \end{pmatrix} = \vartheta. \quad (30)$$

Juliet recovers the plaintext through the decrypted points on the elliptic curve by using the inverse procedure over characters of ASCII.

III. Example

Romeo requires sending the message to Juliet using Diffie-Hellman elliptic curve encryption with the golden matrices. Romeo prefers the elliptic curve $y^2 = x^3 - 4$above the field Z*$_{271}$.

Elliptic curve points are

E={O,(1,57),(1,214),(2,2),(2,269),(5,11),........................……

………………………......………...

...................................,(264,174), (269,114), (269,157)}.

There are 271 points on the elliptic curve,which is a prime and each point is a generator of the chosen elliptic curve E[1]*[13]*.

By selecting the point Q = *(132, 248)* on the elliptic curve and a personal key '*l' = 78,* Romeo has generated the public key *β = 'lQ' = 78(132, 248) = (153, 151).* In this regard Juliet also has chosen a personal key *'m' = 92* and creates the public key *γ = 'mQ'= 92(132, 248) = (58, 157).*

A. Encryption

Romeo selects Juliet's public key *γ = 'mQ'= (58,157)*and he evaluates *lγ = l(mQ)= 78(58, 157) = (133,95).*Romeo requires sending the message *'LOVE'* to Juliet. He transforms the text in to the points on the elliptic curve $y^2 = x^3 - 4$ and chooses a point *ρ = (68, 136)* which is the generator of the cyclic group of E. By using characters of ASCII, the uppercase letter have been converted into points then,

L → 76(68,136) = (163, 200),
O → 79(68,136) = (194, 141),
V→ 65(68,136) = (15, 98),
E → 69(68,136) = (150, 49).

The converted points are
µ = {(163, 200), (194, 141), (15, 98), (150, 49)}.

Romeo creates 2×2 matrix with the converted point's i.e.

$$\vartheta = \begin{pmatrix} (163,\ 200) & (194, 141) \\ (15, 98) & (150,\ 49) \end{pmatrix}.$$

Romeo has chosen a direct "golden matrix" (6) for enciphering matrix by taking the personal key '$y_1 = 5$' (table 1.1), $Q^{10} = \begin{pmatrix} 89 & 55 \\ 55 & 34 \end{pmatrix}.$

Romeo creates 2×2 matrix with the converted point's i.e.

$$\vartheta = \begin{pmatrix} (163,\ 200) & (194, 141) \\ (15, 98) & (150,\ 49) \end{pmatrix}.$$

Romeo has chosen a direct "golden matrix" (6) for enciphering matrix by taking the personal key '$y_1 = 5$' (Table 1.1), $Q^{10} = \begin{pmatrix} 89 & 55 \\ 55 & 34 \end{pmatrix}$

and enciphering matrix,

$$\vartheta \times Q^{10} = \begin{pmatrix} (163,\ 200) & (194, 141) \\ (15, 98) & (150,\ 49) \end{pmatrix} \times \begin{pmatrix} 89 & 55 \\ 55 & 34 \end{pmatrix}$$
$$= \begin{pmatrix} (26,162) & (246,38) \\ (106,77) & (170,120) \end{pmatrix}.$$

The points are,
ξ = *{(26, 162), (246, 38), (106, 77), (170, 120)}.*

Romeo finally evaluates $\lambda_i = \chi_i + l(mQ)$.

$\lambda_1 = (26,162) + (133, 95) = (179, 220),$
$\lambda_2 = (246, 38) + (133, 95) = (2, 2),$
$\lambda_3 = (106, 77) + (133, 95) = (183, 233),$
$\lambda_4 = (170, 120) + (133, 95) = (32, 171).$

The encrypted points are
δ = {(179, 220), (2, 2), (183, 233), (32, 171)}.

Romeo sends the encrypted message in the form of points publicly to Juliet.

B. Decryption

To reclaim the plaintext 'LOVE' from 'λ_i', Juliet has executed the decryption method.

Juliet selects his own personal key *'m = 92'* and multiplies with the Romeo public key i.e. *92(153, 151) = (133, 95)* and then finds the inverse of *(133, 95) i.e. (133, 176*) to the encrypted message *λi* i.e. *(179, 220) + (133, 176) = (26, 162).* Then she got the decrypted point $\chi_1 = (26, 162)$.

In the same manner, the decrypted points are
$\chi_2 = (246, 38)$, $\chi_3 = (106, 77)$,$\chi_4 = (170, 120)$.

After decryption, the recovered points have been arranged in 2×2 matrix.

$$\sigma = \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix} = \begin{pmatrix} (26, 162) & (246, 38) \\ (106, 77) & (170, 120) \end{pmatrix}.$$

Now, Juliet multiplies the recovered points with the inverse of the golden matrix (8) and by using the table (1.1).

$$\sigma \times Q^{-10} = \begin{pmatrix} (26,162) & (246,38) \\ (106,77) & (170,120) \end{pmatrix} \times \begin{pmatrix} 34 & -55 \\ -55 & 89 \end{pmatrix},$$
$$= \begin{pmatrix} (163,\ 200) & (194, 141) \\ (15, 98) & (150,\ 49) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Then Juliet retrieves the message as:

$a_1 = (163, 200) \rightarrow L$
$a_2 = (194, 141) \rightarrow O$
$a_3 = (15, 98) \rightarrow V$
$a_4 = (150, 49) \rightarrow E$

Ultimately, Juliet receives the message "LOVE" from Romeo.

IV. CONCLUSION

In this paper, Diffie-Hellman encryption scheme is developed by framing a bijective function from the points on the elliptic curve to characters of ASCII. The additional personal key has been generated with the matrix obtained from golden matrices. This algorithm is more secure over the elliptic curves.

REFERENCES

1. ApostolTM "*Introductiontoanalyticnumbertheory*".NewYork:Springer-Verlag, 1976.
2. Darrel Hancott Vanstone, *A text book of Guide to elliptic curve Cryptography*, 1965.
3. Diffie W, van Oorschot, P. C., Wiener, M. J. (1992), "*Authentication and Authenticated Key Exchanges*", Designs, Codes and Cryptography Kluwer Academic Publishers 2 (2): 107–125.
4. Hellman M.E., "A Cryptanalytic time-memory trade off". IEEE Transactions on InformationTheory26(4):401-406,1980.M. Young, *The* Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.
5. Stakhov AP. "The ''golden'' matrices and a new kind of cryptography", Chaos, Solutions and Fractals 32 (2007) pp1138–1146.
6. Hoggat VE. Fibonacci and Lucas numbers. Palo Alto, CA: Houghton-Mifflin; 1969.
7. Stakhov AP. *Codes of the golden proportion*. Moscow: Radio and Communications; 1984[in Russian].
8. Stakhov AP. *The golden section in the measurement theory*. Comput Math Appl 1989; 17(4–6):613–38.
9. Stakhov AP, Tkachenko IS. *Hyperbolic Fibonacci trigonometry*. Rep Ukr Acad Sci 1993; 208(7):9–14 [in Russian].
10. Stakhov OP.*A generalization of the Fibonacci Q-matrix*. Rep Nat Acad Sci Ukraine1999 (9):46-9.
11. Stakhov AP. *The golden section and modern harmony mathematics. Applications of Fibonacci numbers*, 7. Kluwer Academic Publishers; pages 393–99, 1998.
12. Stakhov A, Rozin B. *On a new class of hyperbolic function*. Chaos, Solitons & Fractals 2004; 23:379–89.
13. B. Ravi Kumar, A. Chandra Sekhar, G. Appala Naidu, "A Diffie –Hellman key exchange for self encryption over points on the Elliptic Curve Cryptography" Journal of Information and Computing Science, Volume12 (2), pages 083-087, 2017.

AUTHORS PROFILE

Ravi Kumar Bora obtained his Masters Degree in Applied Mathematics from Andhra University Visakhapatnam, India in 2003. He received his Ph.D from Andhra University Visakhapatnam, India in 2019. His research areas include Number theory and Cryptography and image processing.

Sridhar Akiri obtained his Masters Degree in OR & SQC from SKU PG Centre, Kurnool, India in 2001. He received his Ph.D degree from Sri Krishna Devaraya University, Anantapur, India in 2012. His research areas include Reliability Theory and Cryptography.

V Santosh Kumar obtained his M.Tech. in R&M from Andhra University Visakhapatnam, India 2006. He is pursuing Ph.D in the area of Antennas in Department of ECE GITAM University, Visakhapatnam. His areas of interest are Signal processing, Antennas and Cryptography.

Retrieval Number: B10411292S319/2019©BEIESP
DOI: 10.35940/ijitee.B1041.1292S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication