ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.7, 5217–5223
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.7.89

A SECURE DIFFIE-HELLMAN ENCRYPTION SCHEME OVER ELLIPTIC CURVES USING GOLDEN MATRICES

RAVI KUMAR BORA[1], S. ASHOK KUMAR, L. KISHORE KUMAR, AND N. SURENDRA

ABSTRACT. In this paper, we proposed a secured Diffie-Hellman encryption scheme over the elliptic curves based on golden matrices. This algorithm works with a bijective function defined from the points on the elliptic curve to ASCII characters. The additional private key has been generated by the matrix, obtained from golden matrices.

1. 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 [1–3]. 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 [7, 8]. Elliptic Curve Cryptography (ECC) is one of the main crypto systems for public key that also ensures better safety bit than other public key crypto system 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 [4, 5]. Protection of these public key crypto systems depends on number of computational problems which are well known to

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68P25.

Key words and phrases. Diffie-Hellman, golden matrices, elliptic curves, encryption, decryption.

perform as one way. The key agreement protocol of Diffie-Hellman is often used to secure key exchange through public networks [6].

2. Fibonacci Q_α -Matrix

The number theory of Fibonacci determines the prospect of modern utilization for technical outcomes view in last decades [10, 17]. The Fibonacci Q_α matrix was suggested in [14], where

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

is derive from the recurrence relation of Fibonacci
$G_{\vartheta' l+1} = G_{\vartheta' l} + G_{\vartheta' l-1}$ with $G_{\vartheta' 1} = G_{\vartheta' 2} = 1$. Later Q_α was extended to $Q_{\alpha'}$ for integer l [14]

$$Q^l_{\alpha'} = \begin{pmatrix} G_{\vartheta' l+1} & G_{\vartheta' l} \\ G_{\vartheta' l} & G_{\vartheta' l-1} \end{pmatrix}.$$

Consequently the similarity between det $Q^l_{\alpha'}$ and the "Cassini formula",
Det $Q^l_{\alpha'} = G_{\vartheta' l+1} G_{\vartheta' l-1} - G^2_{\vartheta' l} = (-1)^l$.

3. The "Golden" Matrices

The "golden" matrices [9] which are the continuous functions of the variable being defined by A.P Stakhov with the help of the classical Fibonacci Q_α -matrix and the symmetrical hyperbolic Fibonacci functions, as follows: see [13, 15, 16]

$$Q^{2v}_\alpha = \begin{pmatrix} CG_{s_k}(2v+1) & G_{s_k}(2v) \\ G_{s_k}(2v) & CG_{s_k}(2v-1) \end{pmatrix} \tag{3.1}$$

$$Q^{2v+1}_\alpha = \begin{pmatrix} SG_{s_k}(2v+2) & CG_{s_k}(2v+1) \\ CG_{s_k}(2v+1) & SG_{s_k}(2v) \end{pmatrix}, \tag{3.2}$$

where $SG_{s_k}(v) = \dfrac{\tau^\nu_\eta - \tau^{-\nu}_\eta}{\sqrt{5}}$, $CG_{s_k}(v) = \dfrac{\tau^\nu_\eta + \tau^{-\nu}_\eta}{\sqrt{5}}$ and $\tau_\eta = \dfrac{1+\sqrt{5}}{2}$ (the Golden proportion).

The inverse matrices for (3.1) and (3.2) are developed by A.P Stakhov [9] for the continuous variable ν as the following form [11, 12].

$$Q_{\alpha}^{-2v} = \begin{pmatrix} CG_{s_k}(2v-1) & -SG_{s_k}(2v) \\ -SG_{s_k}(2v) & CG_{s_k}(2v+1) \end{pmatrix}$$

$$Q_{\alpha}^{-(2v+1)} = \begin{pmatrix} -SG_{s_k}(2v) & CG_{s_k}(2v+1) \\ CG_{s_k}(2v+1) & -SG_{s_k}(2v+2) \end{pmatrix}.$$

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 [9].

4. Proposed Algorithm

Romeo needs to send the message to Julia using Diffie-Hellman elliptic curve encryption by using the golden matrices. Romeo prefers the elliptic curve $y^2 = x^3 + ux + v$ over the field Z_p. By selecting the point $Q^{'} = (x, y)$ on the elliptic curve and a private key 'l', Romeo has generated the public key $\beta = lQ^{'}$. In this regard, Julia also has chosen a private key 'm' and generates the public key $\gamma = mQ^{'}$.

4.1. **Encryption.** Romeo prefers selects Julia's public key $\gamma = mQ^{'}$ and then evaluates $l\gamma = l(mQ^{'})$. He chooses a point 'R' on the elliptic curve E, where k is the x-coordinate of 'R', $1 \leq k \leq p-2$ and compute $k(lmQ^{'})$. He needs sending the message to Julia, he transforms the message into points on the elliptic curve and chooses a point '$P^{'}$' which is a generator of the cyclic group of the elliptic curve. Let$A^{'} = \{1p^{'}, 2p^{'}, 3p^{'}, \cdots, np^{'}\}$ and set $B^{'}$ characters of ASCII. Set $h^{'}$: $A^{'} \to B^{'}$ as $h^{'}(n\rho^{'})$ = $\grave{a}^{'}n$ where $n = 1, 2, \ldots$ which is the first step of protection. Then the set:

$$\mu = \{\grave{a}^{'}{}_1(\acute{x}_1, \acute{y}_1), \grave{a}^{'}{}_2(\acute{x}_2, \acute{y}_2), \grave{a}^{'}{}_3(\acute{x}_3, \acute{y}_3), \grave{a}^{'}{}_4(\acute{x}_4, \acute{y}_4) \ldots \grave{a}^{'}{}_i(\acute{x}_i, \acute{y}_i)\} \tag{4.1}$$

where $\grave{a}^{'}{}_i \in A$ and $(\acute{x}_i, \acute{y}_i) \in E$. Alice chooses the initial four points $\grave{a}^{'}{}_1, \grave{a}^{'}{}_2, \grave{a}^{'}{}_3, \grave{a}^{'}{}_4$ of (4.1) and arranges in a 2×2 square matrix.

$$\vartheta = \begin{pmatrix} \grave{a}^{'}{}_1 & \grave{a}^{'}{}_2 \\ \grave{a}^{'}{}_3 & \grave{a}^{'}{}_4 \end{pmatrix}. \tag{4.2}$$

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 (4.2). Let us fix the j^{th} permutation by $j = 1, 2, 3.....24$. 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" (3.1), (3.2) 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.

$$\vartheta \times Q^{2y_1} = \begin{pmatrix} \grave{a'}_1 & \grave{a'}_2 \\ \grave{a'}_3 & \grave{a'}_4 \end{pmatrix} \times \begin{pmatrix} CG_{s_k}(2y_1+1) & SG_{s_k}(2y_1) \\ SG_{s_k}(2y_1) & CG_{s_k}(2y_1-1) \end{pmatrix} = \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix},$$

where

$$\begin{aligned} \chi_1 &= \grave{a'}_1 CG_{s_k}(2y_1+1) + \grave{a'}_2 SG_{s_k}(2y_1) \\ \chi_2 &= \grave{a'}_1 SG_{s_k}(2y_1) + \grave{a'}_2 CG_{s_k}(2y_1-1) \\ \chi_3 &= \grave{a'}_3 CG_{s_k}(2y_1+1) + \grave{a'}_4 SG_{s_k}(2y_1) \\ \chi_4 &= \grave{a'}_3 SG_{s_k}(2y_1) + \grave{a'}_4 CG_{s_k}(2y_1-1) \end{aligned}$$

or

$$\vartheta \times Q^{2y_1+1} = \begin{pmatrix} \grave{a'}_1 & \grave{a'}_2 \\ \grave{a'}_3 & \grave{a'}_4 \end{pmatrix} \times \begin{pmatrix} SG_{s_k}(2y_1+2) & CG_{s_k}(2y_1+1) \\ CG_{s_k}(2y_1+1) & SG_{s_k}(2y_1) \end{pmatrix} = \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix}.$$

Then the encrypted points are $\beta = \{\chi_1, \chi_2, \chi_3, \chi_4\}$. Romeo finally computes $\lambda_i = \chi_i + K(lmQ)$ and $R + lmQ$ to send the encrypted message $(\lambda_i, R + lmQ)$ publicly to Julia.

4.2. **Decryption.** To reclaim the plaintext from λ_i Julia has executed the decryption method. First, Julia selects his own private key 'm' and multiplies with Romeo public key $\beta =' lQ^{'}$' i.e. $mlQ^{'}$ then finds the inverse of $mlQ^{'}$ i.e. $-mlQ^{'}$ and adds $-mlQ^{'}$ to the second part of the message i.e. $R + lmQ^{'} - lmQ^{'} = R.$ She computes $k(lmQ^{'})$ where k is the x-coordinate of R and evaluates the inverse element of $k(lmQ^{'})$ is - $k(lmQ^{'})$. She adds $-k(lmQ^{'})$ to the first part of the message χ_i+ $k(lmQ^{'}) - k(lmQ^{'}) = \chi_i$.

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

$$\sigma = \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix}.$$

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

$$\sigma \times Q^{2y_1} = \begin{pmatrix} \chi_1 & \chi_2 \\ \chi_3 & \chi_4 \end{pmatrix} \times \begin{pmatrix} CG_{s_k}(2y_1-1) & -SG_{s_k}(2y_1) \\ -SG_{s_k}(2y_1) & CG_{s_k}(2y_1+1) \end{pmatrix} = \begin{pmatrix} P_{11} & P_{12} \\ P_{13} & P_{14} \end{pmatrix},$$

$$\begin{aligned} P_{11} &= \chi_1 CG_{s_k}(2y_1-1) - \chi_2 SG_{s_k}(2y_1) \\ P_{12} &= -\chi_1 SG_{s_k}(2y_1) + \chi_2 CG_{s_k}(2y_1+1) \\ P_{21} &= \chi_3 CG_{s_k}(2y_1-1) - \chi_4 SG_{s_k}(2y_1) \\ P_{22} &= -\chi_3 SG_{s_k}(2y_1) + \chi_4 CG_{s_k}(2y_1-1)\,. \end{aligned}$$

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

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

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

$$\begin{aligned} P_{11} &= \grave{a}'_1 \\ P_{12} &= \grave{a}'_2 \\ P_{21} &= \grave{a}'_3 \\ P_{22} &= \grave{a}'_4\,. \end{aligned}$$

The decrypted points are,

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

Julia recovers the plain text through the decrypted points on the elliptic curve by using the inverse procedure over characters of ASCII.

5. CONCLUSION

In this paper, a secure Diffie-Hellman encryption scheme is developed by framing a bijective function from the points on the elliptic curve to characters of ASCII. Choose the point R in the elliptic curve and the x- coordinate of R is secret key k it is difficult known by any attack. The additional private key has been generated using the matrix obtained from golden matrices. This will make it more difficult for an attacker to break the scheme.

REFERENCES

[1] W. DIFFIE, M. HELLMAN: *New directions in cryptography*, IEEE Transactions on Information Theory, **22** (1976), 644–654.

[2] M. E. HELLMAN: *A Cryptanalytic time-memory trade off*, IEEE Transactions on Information Theory, **26**(4) (1980), 401–406.

[3] W. DIFFIE, P. C. VAN OORSCHOT, M. J. WIENER: *Authentication and Authenticated Key Exchanges*, Designs, Codes and Cryptography Kluwer Academic Publishers, **2**(2) (1992), 107–125.

[4] N. KOBLITZ: *Hyper Elliptic Cryptosystem*, International Journal of Cryptography, **1** (1989), 139–150.

[5] N. KOBLITZ: *Elliptic curve Cryptosystems*, Mathematics of computation, **48** (1987), 203–209.

[6] N. KOBLITZ: *A course in number theory and cryptography*, Springer-Verlag New York Inc., 1987.

[7] D. H. VANSTONE: *A text book of Guide to elliptic curve Cryptography*, 1965.

[8] W. STALLINGS: *Cryptography and network security principles and practices*, Fourth edition, Pearson education, South Asis, 2007.

[9] A. P. STAKHOV: *The "golden" matrices and a new kind of cryptography*, Chaos, Solutions and Fractals, **32** (2001), 1138–1146.

[10] V. E. HOGGAT: *Fibonacci and Lucas numbers*, Palo Alto, CA: Houghton-Mifflin, 1969.

[11] A. P. STAKHOV: *Codes of the golden proportion*, Moscow: Radio and Communications, 1984. (in Russian)

[12] A. P. STAKHOV: *The golden section in the measurement theory*, Comput Math Appl, **17**(4-6) (1984), 613–638.

[13] A. P. STAKHOV, I. S. TKACHENKO: *Hyperbolic Fibonacci trigonometry*, Rep Ukr Acad Sci, **208**(7) (1993), 9–14. (in Russian).

[14] A. P. STAKHOV: *A generalization of the Fibonacci Q-matrix*, Rep Nat Acad Sci Ukraine, **9** 1999), 46-99.

[15] A. P. STAKHOV: *The golden section and modern harmony mathematics Applications of Fibonacci numbers*, 7 Kluwer Academic Publishers, 1998.

[16] A. P. STAKHOV, B. ROZIN: *On a new class of hyperbolic function*, Chaos, Solutions Fractals, **23** (2004), 379–89.

[17] S. VAJDA: *Fibonacci and Lucas numbers and the golden section Theory and applications*, Ellis Harwood limited, 1989.

DEPARTMENT OF MATHEMATICS
GIS, GITAM UNIVERSITY
VISAKHAPATNAM, INDIA
E-mail address: ravikumarbrk6@gmail.com

DEPARTMENT OF MATHEMATICS
GVP COLLEGE FOR DEGREE AND P.G COURSES(A)
VISAKHAPATNAM, INDIA
E-mail address: saiashok.84@gmail.com

DEPARTMENT OF MATHEMATICS
GVP COLLEGE FOR DEGREE AND P.G COURSES(A)
VISAKHAPATNAM, INDIA
E-mail address: lkishorekumar@gvpcdpgc.edu.in

DEPARTMENT OF MATHEMATICS
GVP COLLEGE FOR DEGREE AND P.G COURSES(A)
VISAKHAPATNAM,INDIA
E-mail address: nsurendra@gvpcdpgc.edu.in