CASCADE BLOCK CIPHER USING BRAIDING/ENTANGLEMENT OF SPIN MATRICES AND BIT ROTATION

D. Sravana Kumar[1], P. Sirisha[2] and CH. Suneetha[3]

[1]Reader in Physics, Dr. V.S. Krishna Government Degree College, Visakhapatnam
[2]Faculty in Mathematics, Indian Maritime University, Visakhapatnam
[3]Assistant Professor in Mathematics, GITAM University, Visakhapatnam

ABSTRACT

Secure communication of the sensitive information in disguised form to the genuine recipient so that an intended recipient alone can remove the disguise and recover the original message is the essence of Cryptography. Encrypting the message two or more times with different encryption techniques and with different keys increases the security levels than the single encryption. A cascade cipher is stronger than the first component. This paper presents multiple encryption schemes using different encryption techniques Braiding/Entanglement of Pauli Spin 3/2 matrices and Rotation of the bits with independent secret keys.

KEYWORDS

Multiple Encryption, Braiding/Entanglement, Rotation of the bits, Encryption and Decryption.

1. INTRODUCTION

As the internet is the basic means of communication nowadays secure transmission of the sensitive information has become a Herculean task. A practical cryptosystem that encrypts the message several times with independent secret keys and with distinct encryption schemes enhances the confidentiality of the message. Multiple encryptions provide better security [1] because even if some of the components of the cipher are broken or some of the secret keys are broken, the confidentiality can still be maintained by the remaining encryptions. Historically, sudden emergence of efficient attacks against the elliptic curve cryptosystem on super singular curves [2, 3] and on prime-field anomalous curves [4] have already reminded us the necessity to do multiple encryptions.

1.1 Pauli Spin 3/2 Matrices

In Quantum Mechanics a very class of dynamical problems arises with central forces. These forces are derivable from a potential that depends on the distance (r) of the moving particle from a fixed point, the origin of the co-ordinate system (O). Since central forces produce no torque about the origin, the angular momentum L = rxp is constant of motion where p is a constant of motion the momentum of the particle. In addition to the dynamical variables x,y,z to describe the

DOI : 10.5121/ijnsa.2016.8205

position of the vector there is another fourth variable σ, called the *spin angular momentum variable* required to describe the dynamical state of fundamental particles. In 1920's, in the study of the spectra of alkali atoms, some troublesome features were observed which could not be explained on the basis of orbital quantum properties [5]. The energy levels corresponding to the n, l and m_l quantum numbers were found to be further split up. Uhlenbeck and Goudsmit [6,7] in 1925 attributed these difficulties due to the fact that the electron has an additional property of intrinsic angular momentum and magnetic momentum. Pauli was the first to propose a non-relativistic wave equation, which takes into account the intrinsic magnetic moment of the electron. To describe the electron spin he used spin ½ , spin 3/2, spin 5/2 matrices. The spin-3/2 matrices are

$$S_x = \frac{1}{2}\begin{bmatrix} 0 & \sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & 2 & 0 \\ 0 & 2 & 0 & \sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{bmatrix} \quad S_y = \frac{1}{2i}\begin{bmatrix} 0 & 0 & 0 & 0 \\ -\sqrt{3} & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -\sqrt{3} & 0 \end{bmatrix} \quad S_z = \frac{1}{2}\begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

1.2 Braiding/Entanglement of Matrices

Entanglement [8] is a term used in quantum theory to describe the way that particles of energy/matter can become *correlated* to predictably interact with each other regardless of how far apart they are. Braiding/Entanglement of matrices is a technique of generating higher order non-singular matrices from simple lower order non-singular matrices.

For example if a = $\begin{bmatrix} a_{11} & a_{12} \\ a_{13} & a_{14} \end{bmatrix}$, b = $\begin{bmatrix} b_{11} & b_{12} \\ b_{13} & b_{14} \end{bmatrix}$, c = $\begin{bmatrix} c_{11} & c_{12} \\ c_{13} & c_{14} \end{bmatrix}$, d = $\begin{bmatrix} d_{11} & d_{12} \\ d_{13} & d_{14} \end{bmatrix}$ are four non-

singular matrices of order 2x2 then these four non-singular matrices are braided/entangled to get higher order 4x4 matrices as

$$A = \begin{bmatrix} a & b \\ d & c \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & b_{11} & b_{12} \\ a_{21} & a_{22} & b_{21} & a_{22} \\ d_{11} & d_{12} & c_{11} & c_{12} \\ d_{21} & d_{22} & c_{21} & c_{22} \end{bmatrix} \quad B = \begin{bmatrix} c & a \\ b & d \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & a_{11} & a_{12} \\ c_{21} & c_{22} & a_{21} & a_{22} \\ b_{11} & b_{12} & d_{11} & d_{12} \\ b_{21} & b_{22} & d_{21} & d_{22} \end{bmatrix}$$

$$C = \begin{bmatrix} b & c \\ a & d \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & c_{11} & c_{12} \\ b_{21} & b_{22} & c_{21} & c_{22} \\ a_{11} & a_{12} & d_{11} & d_{12} \\ a_{21} & a_{22} & d_{21} & d_{22} \end{bmatrix} \quad D = \begin{bmatrix} c & b \\ a & d \end{bmatrix} = \begin{bmatrix} c_{11} & b_{12} & b_{11} & b_{12} \\ c_{21} & c_{22} & b_{21} & b_{22} \\ a_{11} & a_{12} & d_{11} & d_{12} \\ a_{21} & a_{22} & d_{21} & d_{22} \end{bmatrix}$$ and so on.

These matrices are further braided /entangled to get higher order 16x16 matrices like

P = $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ and so on. Non-Singular matrices from the set of these matrices can be selected for the process of encryption/decryption.

1.3 Literature on Golden Matrices

In the last decades the theory of Fibonacci numbers [9, 10] was complemented by the theory of the so-called Fibonacci Q – matrix. Stakhov [11] developed a theory of the golden matrices that are a generalization of the matrix Q^n for continuous domain. He defined the golden matrices in the terms of the symmetrical hyperbolic Fibonacci functions. B.Vellainkann et.al. [12] used non-singular diagonal matrices of higher order, especially induced from quadratic forms in their encryption algorithm. D. Sravana Kumar et.al. [13] proposed encryption technique using Pauli spin ½ matrices. Bibhudendra Acharya et.al. [14] used Hill Cipher for image encryption. Birendra Goswami [15] used matrices in cloud computing. Ayan Mahalanobis [16] used matrices in public key cryptography.

1.4 Rotation of the Bits

The bitwise rotation operation operates on one or more bit patterns of binary numerals at the level of their individual bits. This is used directly at the digital hardware level as well as in microcode, machine code and certain kinds of high level languages. The *bit shifts* are bitwise operations because they operate on the binary representation of an integer instead of its numerical value. In these operations the digits are moved or shifted to the left or right. Registers in a computer processor have a fixed width, so some bits will be *shifted out* of the register at one end, while the same numbers of bits are *shifted in* from the other end and the difference between bit shifts operators lie in how they determine the values of the shifted-in bits.

Example

0	0	0	1	0	1	1	1

When left shifted once gives the number

0	0	1	0	1	1	1	0

When right shifted once gives the number

0	0	0	0	1	0	1	1

Another form of shifting is the *circular shift* or *bit rotation*. In this operation the bits are rotated as if the left and right ends of the register were joined. The value that is shifted in on the right during a left-shift is whatever the value was shifted out on the left, and vice versa. This operation is frequently used in cryptography. Previously Several cryptographers [17,19] used bit rotation of for designing cryptographic algorithm

2. PROPOSED METHOD

The above set of Pauli Spin 3/2 matrices with some elementary transformations are reduced to the matrices

$$b=\begin{bmatrix}0&3&0&0\\3&0&2&0\\0&2&0&3\\0&0&3&0\end{bmatrix}\quad c=\begin{bmatrix}0&-3&0&0\\3&0&-2&0\\0&2&0&-3\\0&0&3&0\end{bmatrix}\quad d=\begin{bmatrix}3&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-3\end{bmatrix}$$

These three matrices derived from Pauli spin 3/2 matrices along with the identity matrix (I_{4x4} = a) are braided or entangled in different possible ways to get a set B of 16 non singular matrices

$$B_0=\begin{bmatrix}a&b\\c&d\end{bmatrix}=\begin{bmatrix}1&0&0&0&0&3&0&0\\0&1&0&0&3&0&2&0\\0&0&1&0&0&2&0&3\\0&0&0&1&0&0&3&0\\0&-3&0&0&3&0&0&0\\3&0&-2&0&0&1&0&0\\0&2&0&-3&0&0&-1&0\\0&0&3&0&0&0&0&-3\end{bmatrix}\quad B_1=\begin{bmatrix}a&d\\b&c\end{bmatrix}=\begin{bmatrix}1&0&0&0&3&0&0&0\\0&1&0&0&0&1&0&0\\0&0&1&0&0&0&-1&0\\0&0&0&1&0&0&0&-3\\0&3&0&0&0&-3&0&0\\3&0&2&0&3&0&-2&0\\0&2&0&3&0&2&0&-3\\0&0&3&0&0&0&3&0\end{bmatrix}$$

$$B_2=\begin{bmatrix}a&c\\b&d\end{bmatrix}=\begin{bmatrix}1&0&0&0&0&-3&0&0\\0&1&0&0&3&0&-2&0\\0&0&1&0&0&2&0&-3\\0&0&0&1&0&0&3&0\\0&3&0&0&3&0&0&0\\3&0&2&0&0&1&0&0\\0&2&0&3&0&0&-1&0\\0&0&3&0&0&0&0&-3\end{bmatrix}\quad B_3=\begin{bmatrix}a&d\\c&b\end{bmatrix}=\begin{bmatrix}1&0&0&0&3&0&0&0\\0&1&0&0&0&1&0&0\\0&0&1&0&0&0&-1&0\\0&0&0&1&0&0&0&-3\\0&-3&0&0&0&3&0&0\\3&0&-2&0&3&0&2&0\\0&2&0&-3&0&2&0&3\\0&0&3&0&0&0&3&0\end{bmatrix}$$

$$B_4=\begin{bmatrix}b&c\\d&a\end{bmatrix}=\begin{bmatrix}0&3&0&0&0&-3&0&0\\3&0&2&0&3&0&-2&0\\0&2&0&3&0&2&0&-3\\0&0&3&0&0&0&3&0\\3&0&0&0&1&0&0&0\\0&1&0&0&0&1&0&0\\0&0&-1&0&0&0&1&0\\0&0&0&-3&0&0&0&1\end{bmatrix}\quad B_5=\begin{bmatrix}b&c\\a&d\end{bmatrix}=\begin{bmatrix}0&3&0&0&0&-3&0&0\\3&0&2&0&3&0&-2&0\\0&2&0&3&0&2&0&-3\\0&0&3&0&0&0&3&0\\1&0&0&0&3&0&0&0\\0&1&0&0&0&1&0&0\\0&0&1&0&0&0&-1&0\\0&0&0&1&0&0&0&-3\end{bmatrix}$$

$$B_6=\begin{bmatrix}b&d\\a&c\end{bmatrix}=\begin{bmatrix}0&3&0&0&3&0&0&0\\3&0&2&0&0&1&0&0\\0&2&0&3&0&0&-1&0\\0&0&3&0&0&0&0&-3\\1&0&0&0&0&-3&0&0\\0&1&0&0&3&0&-2&0\\0&0&1&0&0&2&0&-3\\0&0&0&1&0&0&3&0\end{bmatrix}\quad B_7=\begin{bmatrix}b&a\\d&c\end{bmatrix}=\begin{bmatrix}0&3&0&0&1&0&0&0\\3&0&2&0&0&1&0&0\\0&2&0&3&0&0&1&0\\0&0&3&0&0&0&0&1\\3&0&0&0&0&-3&0&0\\0&1&0&0&3&0&-2&0\\0&0&-1&0&0&2&0&-3\\0&0&0&-3&0&0&3&0\end{bmatrix}$$

$$B_8=\begin{bmatrix} c & d \\ a & b \end{bmatrix}=\begin{bmatrix} 0 & -3 & 0 & 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -3 & 0 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & -3 \\ 1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 \end{bmatrix} B_9=\begin{bmatrix} c & a \\ d & b \end{bmatrix}=\begin{bmatrix} 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & -3 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_A=\begin{bmatrix} c & b \\ a & d \end{bmatrix}=\begin{bmatrix} 0 & -3 & 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & -2 & 0 & 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & -3 & 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -3 \end{bmatrix} B_B=\begin{bmatrix} c & b \\ d & a \end{bmatrix}=\begin{bmatrix} 0 & -3 & 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & -2 & 0 & 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & -3 & 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$B_C=\begin{bmatrix} d & a \\ b & c \end{bmatrix}=\begin{bmatrix} 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \\ 0 & 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 3 & 0 & 2 & 0 & 3 & 0 & -2 & 0 \\ 0 & 2 & 0 & 3 & 0 & 2 & 0 & -3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \end{bmatrix} B_D=\begin{bmatrix} d & a \\ c & b \end{bmatrix}=\begin{bmatrix} 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \\ 0 & -3 & 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & -2 & 0 & 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & -3 & 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_E=\begin{bmatrix} d & b \\ c & a \end{bmatrix}=\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & -3 & 0 & 0 & 3 & 0 \\ 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} B_F=\begin{bmatrix} d & c \\ b & a \end{bmatrix}=\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & -2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & -3 \\ 0 & 0 & 0 & -3 & 0 & 0 & 3 & 0 \\ 0 & 3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Before communicating the messages the sender and the receiver agree upon to use a 16 digit hexadecimal number K which acts as secret key for their communication. The secret key K which is a 16 digit hexadecimal number is divided into two halves K_1 and K_2 having 8 digits each.

$$K = K_1 + K_2.$$

The message is encrypted in two stages. The key for first stage of encryption using braiding/entanglement of Pauli 3/2 matrices technique is K_1 and the key for second stage of encryption using rotation of the bits technique is K_2.

The data to be communicated is divided into blocks of 64 characters each and all the characters are coded to equivalent decimal numbers using ASCII code table and arranged as 8x8 matrices say M_1, M_2, M_3, ……., M_n. The message space always may not be the integral multiples of 64. In such cases the other characters may be filled at random.

2.1 Encryption

I stage of Encryption using braiding/entanglement technique of Pauli 3/2 matrices technique with the key K_1 :

From the above set B of non-singular matrices obtained by braiding/entanglement of Pauli 3/2 matrices 8 different matrices are selected whose subscripts are equal to the first, second and so on the eighth digit of the first half part K_1 of the secret key K successively. For example if the secret key K_1 consists of the digits klmnopqr the sender selects the matrices B_k, B_l, B_m, …… B_r. Then the sender computes a matrix which is the product of eight matrices B_k, B_l, B_m, …… B_r successively in the same order called the encoding matrix A. Consider the first data block matrix M_1 which is to be encrypted. It is multiplied with the matrix A and the resulting matrix is adjusted to modulo 256. The resulting matrix when adjusted to Mod 256 is divided into two parts the integer part and the residue part namely I_1 and C_1(Dec).

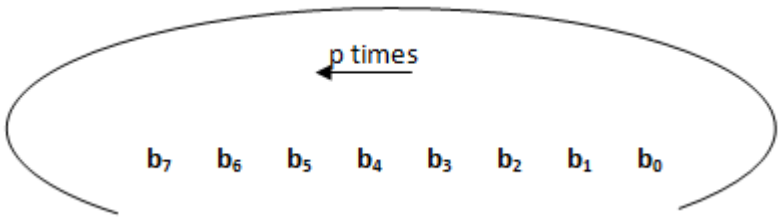
Example : when 1,116 is adjusted to mod 256 the integer part is 4 and the residue part is 92.

$$C_1(\text{Dec}) = (M_1 * A)_{\text{Mod}256}$$

All the elements which are decimal numbers of the matrix C_1(Dec) are converted to 8 bit binary equivalents using ASCII code table which is named as C_1^1(Bin)

II stage of encryption using Rotation of the Bits Technique with secret key K_2 .

The bits each 8 bit binary element of the first row of the matrix C_1^1(Bin) are right rotated the number of times equal to the first hexadecimal digit of the secret key K_2. If the hexadecimal digit exceeds 8 then it is adjusted to mod 8. The bits each 8 bit binary element of the second row are right rotated the number of times equal to the second hexadecimal digit of K_2. Similarly the bits of each 8 bit binary element of third, fourth and so on eighth row are right rotated the number of times equal to the third, fourth and so on eighth hexadecimal digit of the secret key K_2.



Example if the first element of the matrix C_1^1(Bin) is 11001010, the first hexadecimal digit of the secret key K_2 is A. Then A when adjusted to mod 8 is 2. So, the bits of the binary number 11001010 are right rotated 2times.

1	1	0	0	1	0	1	0
0	1	1	0	0	1	0	1
1	0	1	1	0	0	1	0

The resulting binary number is 10110010. After applying the rotation of the bits technique for each element of the matrix C_1^1(Bin) the resulting matrix is C_1^{11}(Bin). Similarly all the other matrices M_2, M_3, ……., M_n are encrypted in the same way to get C_2^{11}(Bin), C_3^{11}(Bin), …….

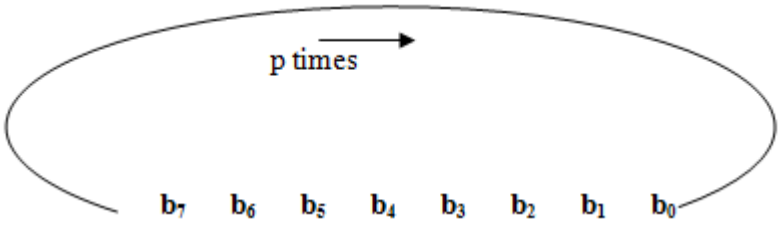
C_n^{11}(Bin). Then all the binary elements the matrices C_1^{11}(Bin), C_2^{11}(Bin), C_3^{11}(Bin), ……. C_n^{11}(Bin) are coded to the text characters using ASCII code table which constitutes the cipher text C. The integer matrices of block matrices M_1 ,M_2, M_3, ……., M_n obtained at I stage of encryption when adjusted to mod 256 are I_1, I_2, …….I_n. These elements are written as string of numbers called the cipher string I. The cipher text C along with the string I are communicated to the receiver in public channel. To provide the authenticity the sender may add an arbitrary decimal number at the end of the string I, the corresponding ASCII character at the end of the cipher text so that the receiver verifies the genuineness.

2.2 Decryption

The receiver decrypts the message using the key K which is agreed upon by both sender and the receiver before communicating the messages. The receiver first divides the key K which is a 16 digit hexadecimal number into two halves K_1 and K_2.

I stage of Decryption using Rotation of the Bits technique with key K_2:

The receiver after receiving the cipher text C and cipher string I verifies that the character corresponding to the last decimal of the string of integers I is same as the last character of the cipher or not. Then the receiver first divides the cipher text into 64 characters each and converts all the characters to 8 bit binary numbers using ASCII code table and writes as 8x8 matrices say D_1^{11}(Bin), D_2^{11}(Bin), D_3^{11}(Bin), ……. D_n^{11}(Bin). Consider the first cipher block matrix D_1^{11}(Bin). The bits of each element of the first row of the matrix D_1^{11}(Bin)are left rotated the number of times equal to the first hexadecimal digit of the key K_2.



For example the first binary element of the matrix D_1^{11}(Bin) is 11001010 and the first hexadecimal digit of the key K_2 is 2. Then the bits are left rotated 2 times

1	0	1	1	0	0	1	0
0	1	1	0	0	1	0	1
1	1	0	0	1	0	1	0

The bits of each element of the second row of the matrix D_1^{11}(Bin) are left rotated the number of times equal to the second hexadecimal digit of the matrix K_2. Similarly the bits of each element of third, fourth and so on eighth row of the matrix D_1^{11}(Bin) are left rotated the number of times equal to the third, fourth and so on eighth digit of the key K_2. After employing rotation of the bits technique for all the elements of the matrix C_1^{Bin} the resulting matrix is named as D_1^1(Bin) . Then all the elements of the matrix D_1^1(Bin) which are 8 bit binary numbers are converted to decimal equivalents using ASCII code table which is the matrix D_1^1(Dec)

II stage of Decryption using the entanglement of Pauli 3/2 matrices technique with the key K_1:

The cipher string I excluding the last digit is divided into blocks of 64 numbers each. Then all the 64 numbers of each block are written as 8x8 matrices

$I_1, I_2, \ldots\ldots I_n$. Consider the string I_1. Every element of the matrix I_1 is multiplied with 256 and added to the corresponding element of the matrix D_1^1(Dec) which is obtained in I stage of decryption to get the matrix D_1^{11}(Dec).

$$D_1^{11}(Dec)= 256*I_1 + D_1^1(Dec)$$

Now the receiver selects the 8 non-singular matrices form the set B of the above braided matrices whose subscripts are same as the first digit, second digit and so on eighth digit of the key K_1. Then the receiver computes the encoding matrix A which is the product of all the eight matrices successively in the same order. Then the matrix D_1^{11}(Dec) is multiplied with the inverse of the encoding matrix A to get the first message block matrix M_1.

$$M_1 = D_1^{11}(Dec)*Inv(A)$$

In a similar way all the other cipher block matrices D_2^{11}(Bin), D_3^{11}(Bin), ……. D_n^{11}(Bin) are decrypted in two stages to get the message block M_2, M_3, ……., M_n. Then all the decimal elements of each matrix M_1, M_2, M_3, ……., M_n are coded to the text characters using the ASCII code table which is the original message.

3. EXAMPLE

If two communicating parties Alice and Bob want to communicate the messages first they agree upon to use the secret key

K= 4A8E05B9B23D1E74

The key K is divided into two parts $K_1$and K_2

K_1= 4A8E05B9

K_2= B23D1E74

3.1 Encryption

Suppose Alice wants to communicate the message **CONGRATULATIONS,** she encrypts the message in two stages using braiding/entanglement technique of Pauli 3/2 matrices with the key K_1 and rotation of the bits technique with the key K_2. All the text characters of the message are converted to the decimal numbers using ASCII code table and writes as 8x8 matrixes say M. Since the message consists only 15 characters the other characters may be filled at random.

$$M = \begin{bmatrix} 67 & 79 & 78 & 71 & 82 & 65 & 84 & 85 \\ 76 & 65 & 84 & 73 & 79 & 78 & 83 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \end{bmatrix}$$

I stage of Encryption using braiding/entanglement of Pauli 3/2 matrices technique with the key K_1 = 4A8E05B9:

Alice selects 8 matrices from the above set B of non singular matrices whose subscripts are successively the digits of the key K_1 and computes the product of 8 matrices which is the encoding matrix A

$$A = B_4 * B_A * B_8 * B_E * B_0 * B_5 * B_B * B_9 =$$

$$\begin{bmatrix} 7056 & -5856 & -9528 & 6264 & -2160 & 10704 & -1128 & 3096 \\ -6768 & -6928 & 27304 & 18744 & -11568 & 2560 & -27512 & 10440 \\ 29592 & -17000 & -34384 & 9552 & -10680 & 28952 & -1984 & 9936 \\ -7848 & -4920 & 29280 & 11664 & -3240 & -2760 & -17184 & 6336 \\ -5040 & 8592 & 8424 & 2952 & -9792 & -3600 & -11832 & 4824 \\ 2160 & -5152 & -776 & 6072 & -3072 & 4000 & -4664 & 1080 \\ 2520 & 4184 & -12464 & -5376 & -264 & -1496 & 6880 & -4032 \\ -15480 & 12168 & 8256 & -2016 & -1800 & -18744 & -114 & -11520 \end{bmatrix}$$

The message matrix M is multiplied with A and all the elements are adjusted to mod 256. The resulting matrix when adjusted to Mod 256 is divided into two parts the integer part and the residue part namely I and C_1(Dec).

$$C_1(\text{Dec}) = (M_1 * A)_{\text{Mod}256} = \begin{bmatrix} 240 & 64 & 56 & 232 & 112 & 80 & 232 & 8 \\ 144 & 0 & 192 & 240 & 128 & 80 & 240 & 96 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \end{bmatrix}$$

$$I = \begin{bmatrix} 1218 & -3358 & 4729 & 13622 & -12889 & 4795 & -16921 & 5488 \\ 4986 & -5854 & 976 & 13734 & -12374 & 8795 & -15740 & 7077 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \end{bmatrix}$$

All the elements which are decimal numbers of the matrix C_1(Dec) are converted to 8 bit binary equivalents using ASCII code table which is named as C_1^{1}(Bin)

C_1^{1}(Bin)=

$$\begin{bmatrix} 11110000 & 01000000 & 00111000 & 11101000 & 01110000 & 01010000 & 11101000 & 00001000 \\ 10010000 & 00000000 & 11000000 & 11110000 & 10000000 & 01010000 & 11110000 & 01100000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \end{bmatrix}$$

II stage of encryption using Rotation of the Bits Technique using secret key
K_2= B23D1E74

Since the first digit of the key K_2 is B. It is equivalent to 3 when adjusted to mod 8. So, the bits of each 8 bit binary element of the first row of C_1^{1}(Bin) are right rotated 3 times. Since the second digit of K_2 is 2 then the bits of each 8 bit binary element of the second row of C_1^{1}(Bin) are right rotated 2 times. The right rotation operation on each element of third, fourth and so on eighth row is performed 3times, 5 times and so on 4 times. The resulting matrix is named as C_1^{11}(Bin)

C_1^{11}(Bin)=

$$\begin{bmatrix} 00011110 & 00001000 & 00000111 & 00011101 & 00001110 & 00001010 & 00011101 & 00000001 \\ 001000100 & 00000000 & 00110000 & 00111100 & 00100000 & 00010100 & 00111100 & 00011000 \\ 00010100 & 00010000 & 00000100 & 00000100 & 00010100 & 00011000 & 00011000 & 00010000 \\ 00000101 & 00000100 & 00000001 & 00000001 & 00000101 & 00000110 & 00000110 & 00000100 \\ 01010000 & 01000000 & 00010000 & 00010000 & 01010000 & 01100000 & 01100000 & 01000000 \\ 10000010 & 00000010 & 10000000 & 10000000 & 10000010 & 00000011 & 00000011 & 00000010 \\ 01000001 & 00000001 & 01000000 & 01000000 & 01000001 & 10000001 & 10000001 & 00000001 \\ 00001010 & 00001000 & 00000010 & 00000010 & 00001010 & 00001100 & 00001100 & 00001000 \end{bmatrix}$$

Then all the elements which are 8 bit binary elements of the matrix C_1^{11}(Bin) are coded to the text characters using ASCII code table which constitutes the cipher text

RS BS BEL GS SO LF GS SOH $ NUL 0 < (SPACE) DC4 < CAN DC4 DLE EOT EOT DC4 CAN CAN DLE ENQ EOT SOH SOH ENQ ACK ACK EOT P @ DLE DLE P ` ` @ , STX € € , ETX ETX STX A SOH @ @ A Ü Ü SOH LF BS STX STX LF FF FF BS ?

The string of integers obtained in I stage of encryption when adjusted to mod 256 are
1218, -3358, 4729, 13622,-12889, 4795,-16921, 5488, 4986,-5854, 976, 13734,-12374,
8795,-15740,7077,1112,-2680,2895, 8599,-7651,3524,-10345,3622,1112,-2680,2895, 8599,-7651,3524,-10345,3622,1112,-2680,2895,8599,-7651,3524,-10345,3622,1112,-2680,2895,
8599,-7651, 3524,-10345,3622,1112,-2680,2895,8599,-7651,3524,-10345,
3622, 1112, -2680, 2895, 8599,-7651, 3524,-10345, 3622, 63.

Alice added number "63" at the end of the string I and the corresponding ASCII character "?" at the end of the cipher text C to authenticate the message and communicates the cipher text along with the cipher string I to Bob in public channel.

3.2 Decryption

Bob after receiving the cipher text and the string of integers I verifies whether the last character of the cipher text is same as the corresponding character of last decimal number of the string of integers I or not. Then he starts decrypting the message in two different stages using rotation of the bits technique and braiding/entanglement technique of Pauli 3/2 matrices with the keys K_2 and K_1.

First Bob converts the cipher text to equivalent 8 bit binary numbers using ASCII code table. Then he writes all the 64 binary numbers as 8x8 matrix which is named as D_1^{11}(Bin)

D_1^{11}(Bin)=

$$\begin{bmatrix} 00011110 & 00001000 & 00000111 & 00011101 & 00001110 & 00001010 & 00011101 & 00000001 \\ 001000100 & 00000000 & 00110000 & 00111100 & 00100000 & 00010100 & 00111100 & 00011000 \\ 00010100 & 00010000 & 00000100 & 00000100 & 00010100 & 00011000 & 00011000 & 00010000 \\ 00000101 & 00000100 & 00000001 & 00000001 & 00000101 & 00000110 & 00000110 & 00000100 \\ 01010000 & 01000000 & 00010000 & 00010000 & 01010000 & 01100000 & 01100000 & 01000000 \\ 10000010 & 00000010 & 10000000 & 10000000 & 10000010 & 00000011 & 00000011 & 00000010 \\ 01000001 & 00000001 & 01000000 & 01000000 & 01000001 & 10000001 & 10000001 & 00000001 \\ 00001010 & 00001000 & 00000010 & 00000010 & 00001010 & 00001100 & 00001100 & 00001000 \end{bmatrix}$$

I stage of Decryption using bit rotation operation with the key K_2:

Since the first digit of the key K_2 is B. It is equivalent to 3 when adjusted to mod 8. So, the bits of each 8 bit binary element of the first row of D_1^{11}(Bin) are left rotated 3 times. Since the second digit of K_2 is 2 then the bits of each 8 bit binary element of the second row are left rotated 2 times. The left rotation operation on each element of third, fourth and so on eighth row is performed 3times, 5 times and so on 4 times. The resulting matrix is named as D_1^1(Bin)

D_1^1(Bin)=

$$\begin{bmatrix} 11110000 & 01000000 & 00111000 & 11101000 & 01110000 & 01010000 & 11101000 & 00001000 \\ 10010000 & 00000000 & 11000000 & 11110000 & 10000000 & 01010000 & 11110000 & 01100000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \\ 10100000 & 10000000 & 00100000 & 00100000 & 10100000 & 11000000 & 11000000 & 10000000 \end{bmatrix}$$

Then all the elements of D_1^1(Bin) are coded to equivalent decimal numbers using ASCII code table which is D_1^1(Dec)

$$D_1^1(Dec) = \begin{bmatrix} 240 & 64 & 56 & 232 & 112 & 80 & 232 & 8 \\ 144 & 0 & 192 & 240 & 128 & 80 & 240 & 96 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \\ 160 & 128 & 32 & 32 & 160 & 192 & 192 & 128 \end{bmatrix}$$

II stage of decryption using braiding /entanglement of Pauli 3/2 matrices with the key K_1:
Bob writes the numbers in the cipher string I of as 8x8 matrix excluding the last number which is the matrix I

$$I = \begin{bmatrix} 1218 & -3358 & 4729 & 13622 & -12889 & 4795 & -16921 & 5488 \\ 4986 & -5854 & 976 & 13734 & -12374 & 8795 & -15740 & 7077 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \\ 1112 & -2680 & 2895 & 8599 & -7651 & 3524 & -10345 & 3622 \end{bmatrix}$$

Each element of the matrix I is multiplied with 256 and added to the corresponding element of the matrix D_1^1(Dec) which is the matrix D_1^{11}(Dec)

$D_1^{11}(Dec) =$

$$\begin{bmatrix} 312048 & -859584 & 1210680 & 3487464 & -3299472 & 1227600 & -4331544 & 1404936 \\ 1276560 & -1498624 & 250048 & 3516144 & -3167616 & 2251600 & -4029200 & 1811808 \\ 284832 & -685952 & 741152 & 2201376 & -1958496 & 902336 & -2648128 & 927360 \\ 284832 & -685952 & 741152 & 2201376 & -1958496 & 902336 & -2648128 & 927360 \\ 284832 & -685952 & 741152 & 2201376 & -1958496 & 902336 & -2648128 & 927360 \\ 284832 & -685952 & 741152 & 2201376 & -1958496 & 902336 & -2648128 & 927360 \\ 284832 & -685952 & 741152 & 2201376 & -1958496 & 902336 & -2648128 & 927360 \\ 284832 & -685952 & 741152 & 2201376 & -1958496 & 902336 & -2648128 & 927360 \end{bmatrix}$$

Then the resulting matrix $D_1^{11}(Dec)$ is multiplied with the inverse of the encoding matrix A which gives the original message matrix M.

$$M = D_1^{11}(Dec) * Inv(A)$$

$$M = \begin{bmatrix} 67 & 79 & 78 & 71 & 82 & 65 & 84 & 85 \\ 76 & 65 & 84 & 73 & 79 & 78 & 83 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \end{bmatrix}$$

Then all the decimal elements of the matrix M are coded to the text characters using ASCII code table which is the original message **CONGRATULATIONS.**

4. CRYPTANALYSIS AND CONCLUSIONS

Folk theorem [18] states that a cascade of ciphers is at least as difficult to break as any of its component ciphers. The enemy cannot exploit information about the plaintext statistics. If the ciphers commute, then a cascade is difficult to break. In the cascade cipher presented in this paper the message is encrypted in two stages using two different encryption algorithms with two different keys. So, the cipher is powerful and improves the security. The original message CONGRATULATIONS contains 15 characters. Here the alphabets O,N,A,T are repeated twice. But no character in the first 15 of the cipher is repeated. Besides that the original message contains only 15 characters but the size of the block here is 64. So, the remaining characters are the dummy characters which may be selected at random. Here same dummy character "." is selected to fill the remaining characters. But, the same characters in the plain text are mapped to different characters in the cipher. This shields the cipher against the security implications like chosen plain text attacks, chosen cipher text attacks, linear cryptanalysis, mono-alphabetic cryptanalysis. Even though the original message contains less than 64 characters the other characters are filled at random. This is the reason that the proposed cascade block cipher

presented in this paper is less prone to timing attacks because the time required to encipher of decipher is same for all the data blocks. Here the message is encrypted in two different stages using braiding/ entanglement technique with key K_1, bit rotation technique with the key K_2 . Security levels of the cipher can be further enhanced by encrypting the already encrypted message in two more stages using braiding/entanglement technique with the key K_2 and the bit rotation technique with key K_1.

REFERENCES

[1] S. Even and O. Goldreich. On the Power of Cascade Ciphers. ACM Trans. Comp. Systems 3: 108–116 (1985)

[2] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to lgarithms in a finite field. IEEE Trans. on Information Theory, 39:1639–1646, 1993.

[3] R. Merkle and M. Hellman. On the security of multiple encryption. Communications of the ACM, 24(7):465–467, 1981.

[4] N. Smart. The discrete logarithm problems on elliptic curves of trace one. Journal of Cryptology, 12:193–196, 1999.

[5] Jaeger G, "Entanglement, information, and the interpretation of quantum mechanics", Heildelberg 2009: Springer, ISBN 978-3-540-92127-1.

[6] Richard Liboff, "Introductory quantum mechanics, IV Edition, Addison Wesley, 2002

[7] J. J. Sakurai, "Modern quantum mechanics", Addidon Wesley, 1985

[8] Steward EG ,"Quantum mechanics: its early development and the road to entanglement", 2008,Imperial College Press. ISBN 978-1860949784.

[9] Gould HW., "A history of the Fibonacci Q-matrix and a higher-dimensional problem, the Fibonacci quart." 1981(19),250-7.

[10] Hoggat VE., "Fibonacci and Lucas numbers", Palo Alto, CA: Houghton-Mifflin, 1969

[11] Stakhov A.P. , "The golden matrices and a new kind of cryptography", Chaos, Solutions and Fractals, 2006

[12] B.Vellainkannan, Dr. V. Mohan, V. Gnanaraj "A Note on the application of Quadratic forms in Coding Theory with a note on Security", International Journal Computer Tech. Applications Vol 1(1) 78-87.

[13] D.Sravana Kumar, CH. Suneetha ,A. Chandrasekhar "Encryption of Data Streams using Pauli Spin ½ matrices", International Journal of Engineering Science and Research, Vol. 2(6), 2010, 2020-2028.

[14] Bibhudendra Acharya , Saroj Kumar Panigrahy, Sarat Kumar Patra , and Ganapati Panda, "Image Encryption using Advanced Hill cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[15] Birendra Goswami, Dr.S.N.Singh "Enhancing Security in Cloud computing using Public Key Cryptography with Matrices" International Journal of Engineering Research and Applications Vol. 2, Issue 4, July-August 2012, pp.339-344 339.

[16] Ayan Mahalanobis, "Are Matrices Useful in Public-Key Cryptography?" International Mathematical Forum, Vol. 8, 2013, no. 39, 1939 - 1953 HIKARI Ltd, www.m-hikari.com http://dx.doi.org/10.12988/imf.2013.310187

[17] D.Sravana Kumar, CH. Suneetha and A. Chandrasekhar, "A Block Cipher using Rotations and Logical Operations", International Journal of Computer Science Issues, Vol. 8, Issue 6, No. 1, Nov 2011.

[18] U. Maurer and J. Massey. Cascade Ciphers: the Importance of Being First. J. Crypto 6(1): 55–61 (1993).

[19] Shipra Rathore, Nilmani Verma "A Novel Visual Cryptography Scheme Using Bit Rotation and Blowfish Algorithm", International Journal of Scientific Research Engineering & Technology, Volume 3 Issue 1, April 2014