ABSTRACT
As the internet is the basic means of communication nowadays, secure transmission of the sensitive information to the genuine recipient has become a Herculean task. Cryptography is an essential tool for protecting information in computer systems. This paper presents a novel encryption scheme using Braiding/Entanglement of Pauli Spin 3/2 matrices.

Keywords
Braiding/Entanglement, Encryption and Decryption

1. INTRODUCTION
Hill cipher was invented in 1929 by Lester S. Hill [1]. It is a famous Polygram and classical ciphering algorithm based on matrix transformation. Hill cipher is a block cipher having diverse advantages such as concealing letter frequency, its simplicity because of using matrix multiplication and inversion for encryption and decryption and high speed. But it is vulnerable to known plain text attacks. Several researchers tried to improve the security of the Hill cipher. The present paper describes a novel encryption algorithm using braiding/entanglement technique with Pauli 3/2 matrices.

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 \( L = r \times p \) is constant of motion where \( p \) is a constant of motion of the particle. In addition to the dynamical variables \( x,y,z \) to describe the position of the vector there is another fourth variable \( \sigma \), 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 [2]. The energy levels corresponding to the \( n, l \) and \( ml \) quantum numbers were found to be further split up. Uhlenbeck and Goudsmit [3,4] 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 \( \frac{1}{2} \), spin 3/2, spin 5/2 matrices. The spin-3/2 matrices are

\[
S_{x} = \frac{1}{2} \begin{pmatrix}
0 & \sqrt{3} & 0 & 0 \\
\sqrt{3} & 0 & 2 & 0 \\
0 & 2 & 0 & \sqrt{3} \\
0 & 0 & \sqrt{3} & 0 \\
\end{pmatrix}
\]

\[
S_{y} = \frac{1}{2} \begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & -\sqrt{3} \\
0 & -\sqrt{3} & 0 & 0 \\
\end{pmatrix}
\]

\[
S_{z} = \frac{1}{2} \begin{pmatrix}
3 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & -1 & 0 \\
0 & 0 & 0 & 3 \\
\end{pmatrix}
\]

1.2 Braiding/Entanglement of Matrices
Entanglement [5] 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 \( a = \begin{pmatrix} a_{11} & a_{12} \\ a_{13} & a_{14} \end{pmatrix} \)

\[
\begin{pmatrix} b_{11} & b_{12} \\ b_{13} & b_{14} \end{pmatrix}, \quad c = \begin{pmatrix} c_{11} & c_{12} \\ c_{13} & c_{14} \end{pmatrix}, \quad d = \begin{pmatrix} d_{11} & d_{12} \\ d_{13} & d_{14} \end{pmatrix}
\]

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

\[
A = \begin{pmatrix} a_{11} & a_{12} & b_{11} & b_{12} \\ a_{21} & a_{22} & b_{21} & b_{22} \\ d_{11} & d_{12} & c_{11} & c_{12} \\ d_{21} & d_{22} & c_{21} & c_{22} \end{pmatrix}
\]

\[
B = \begin{pmatrix} c_{11} & c_{12} & a_{11} & a_{12} \\ c_{21} & c_{22} & a_{21} & a_{22} \\ b_{11} & b_{12} & d_{11} & d_{12} \\ b_{21} & b_{22} & d_{21} & d_{22} \end{pmatrix}
\]
\[ C = \begin{bmatrix} b & c \\ a & d \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & c_{11} & c_{12} \\ b_{21} & b_{22} & c_{21} & c_{22} \\ a_{11} & a_{12} & d_{11} & d_{12} \\ a_{21} & a_{22} & d_{21} & d_{22} \end{bmatrix} \]

\[ D = \begin{bmatrix} c & b \\ a & d \end{bmatrix} = \begin{bmatrix} c_{11} & b_{12} & b_{21} & b_{22} \\ c_{21} & c_{22} & b_{21} & b_{22} \\ a_{11} & a_{12} & d_{11} & d_{12} \\ a_{21} & a_{22} & d_{21} & d_{22} \end{bmatrix} \]

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**


**2. PROPOSED METHOD**

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

\[ b = \begin{bmatrix} 0 & 3 & 0 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 \end{bmatrix} \]

\[ c = \begin{bmatrix} 0 & -3 & 0 & 0 \\ 3 & 0 & -2 & 0 \\ 0 & 2 & 0 & -3 \\ 0 & 0 & 3 & 0 \end{bmatrix} \]

\[ d = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -3 \end{bmatrix} \]

These three matrices which were derived from Pauli spin 3/2 matrices along with the identity matrix (1x4 = 1) are braided or entangled in different possible ways to get a set \( B \) of 16 non singular matrices.

\[ B_{01} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 \end{bmatrix} \]

\[ B_{02} = \begin{bmatrix} a & d \\ b & c \end{bmatrix} = \begin{bmatrix} 0 & 3 & 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 3 & 0 & 0 \end{bmatrix} \]

\[ B_{03} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & -3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 \end{bmatrix} \]

\[ B_{04} = \begin{bmatrix} a & d \\ c & b \end{bmatrix} = \begin{bmatrix} 0 & 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 3 & 0 & 2 & 0 & 3 & 0 & -2 & 0 \\ -3 & 0 & 0 & 0 & 3 & 0 & 0 \end{bmatrix} \]

\[ B_{05} = \begin{bmatrix} b & c \\ d & a \end{bmatrix} = \begin{bmatrix} 0 & 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 3 & 0 & 2 & 0 & 3 & 0 & -2 & 0 \\ 0 & 2 & 0 & 3 & 0 & 2 & 0 & -3 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \]

\[ B_{06} = \begin{bmatrix} b & c \\ a & d \end{bmatrix} = \begin{bmatrix} 0 & 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 2 & 0 & 3 & 0 & 2 & 0 & -3 \\ 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 \end{bmatrix} \]
The Subscript \( lm \) of the first matrix, the power \( pq \) to which it is raised and the subscript \( no \) of the second matrix, the power \( rs \) to which it is raised are selected at random. Then the product of these two matrices raised to the powers \( pq, rs \) is computed which is represented as the encoding matrix \( \Lambda \).

\[
\Lambda = B_{lm}^{pq} \ast B_{no}^{rs}
\]

The Subscript \( lm \) of the first matrix, the power \( pq \) to which it is raised and the subscript \( no \) of the second matrix, the power \( rs \) to which it is raised successively constitute the secret key. The sender also encrypts the secret key and communicates to the receiver in a public channel.

Step 3: The message matrix \( M \) is multiplied with the encoded sender also encrypts the secret key and communicates to the receiver in a public channel.

\[
E = M \times A_t \text{ then it is adjusted to mod 256}
\]

\[
C = \text{mod}(E, 256)
\]
Step 4: All the elements of the matrix C along with the power ‘t’ are coded to the text characters using the ASCII code table which is the cipher text C.

The integer parts of the matrix E when adjusted to mod 256 is named as the integer matrix I.

Example: when 1,116 is adjusted to mod 256 the integer part is 4 and the residue part is 92. All the elements of the integer matrix I along with the power to which the matrix A is raised are written successively as a string of numbers called the cipher string I. The cipher text C along with the cipher string I are communicated to the receiver in public channel.

2.2 Encryption of the secret key
Before communicating the message, the sender and the receiver agree upon to use a non-singular 8x8 matrix S to encrypt and decrypt the secret key. The secret key [l m p q n o r s] is first converted to weighted 8421 BCD code. The 8421 BCD code thus obtained is gray coded. Then it is 8421 BCD decoded and written as 1 x 8 matrix. This 1 x 8 matrix is multiplied with the 8x8 matrix S to obtain the 1x8 matrix KE. This KE is the encrypted secret key and it is sent in public channel to the receiver.

2.3 Decryption
The receiver after receiving the cipher text C, cipher string I and the encrypted secret key KE first verifies that the corresponding numeral of the last character of the cipher text C is same as the last numeral in the string I.

2.4 Decryption of the secret key
To obtain the secret key K from the encrypted key KE the receiver multiplies the 1x8 matrix KE with the inverse of the matrix I. The product of these two matrices along with the powers [0 1 0 5 0 2 0 6] constitute the secret key K.

3. Example
Suppose Alice and Bob want to communicate with each other first they agree upon to use a non-singular 8x8 matrix S for encryption and decryption of the secret key.

$$A = B_{10}^{05} \times B_{10}^{06}$$

Step 1: All the characters of the cipher text C are coded to the decimal equivalents using ASCII code table excluding the last numeral and are written as 8x8 matrix say the cipher matrix C. The subscripts of these matrices along with the powers [0 1 0 5 0 2 0 6] constitute the secret key K.

Step 2: Two matrices B01 and B02 are selected at random from the set B of matrices. The product of these two matrices B01 and B02 are raised to the power 05 and 06is the encoding matrix A.

$$A = B_{01}^{05} \times B_{02}^{06} =$$

$$\begin{bmatrix}
1029952 & -252288 & -371808 & -1142208 & 1616736 & -1172176 & -1382976 & 835488 \\
1405056 & -605392 & 225952 & 878888 & 1109688 & 1316704 & -1999712 & -1514304 \\
403552 & -908080 & 505472 & 293952 & 672192 & 151328 & -399776 & -351264 \\
-163584 & 83424 & -94648 & -322400 & -262080 & -496320 & 242368 & 417120 \\
1426176 & -640320 & 511008 & 173176 & 751260 & 2600544 & -2085520 & -2452896 \\
34752 & 25152 & 252627 & 207072 & 8352 & 193632 & 162912 & -138816 \\
406944 & -236736 & 10944 & 21504 & 385344 & 118388 & -350208 & -162144 \\
1893312 & -545568 & -1540608 & -3064320 & 3211488 & -4242624 & -3131040 & 2297952
\end{bmatrix}$$

The receiver multiplies the resulting 8x8 matrix along with the powers [0 1 0 5 0 2 0 6] to the encrypted key KE to get the secret key K.

Step 3: The message matrix M is multiplied with the inverse of the encoding matrix A raised to the power t to get the message matrix M.

$$M = D^{t} \times (A^{-1})$$

Step 4: Then the numerals are coded to the text characters using ASCII code table which is the original message.
All the elements of the matrix C along with the power 3 are coded to the text characters using the ASCII code table which is the cipher text C ° (non breaking space)É @ (space)(Null char) É É É @ (Null char) (Space) @ É É É (Null char) (Space) @ É É É (Null char) (Space) @ É É É (Null char) (Space) @ É É É (Null char) (Space) @ É É É (Null char) (Space) @ É É É (Null char) (Space) @ É É É (Null char) (Space)@ É É É (ETX)

This cipher text C along with the cipher string I whose last number is 3 is communicated to Bob in a public channel.

3.2 Encryption of the secret key
Before communicating the messages Alice and Bob agree upon to use the 8x8 non singular matrix S.

K = [0 1 0 5 0 2 0 6]
K is 8421BCD encoded to get K1.
K1 = [0000 0001 0000 0010 0000 0010 0000 0110]
K1 is gray coded to get k2
K2 = [0000 0001 1000 1011 1000 0011 0000 0101]
K2 is 8421BCD decoded to get K3
K3 = [0 1 8 7 8 3 0 5]
K3 is multiplied with S to get encrypted key KE
KE = [71 77 94 152 98 161 83 81]
KE = [71 77 94 152 98 161 83 81] is sent to Bob as encrypted secret key in a Public channel.

3.3 Decryption
Before attempting for the decryption Bob verifies that the numerical corresponding to the last character in the cipher text C is same as the last numeral in the cipher string I. Bob starts the decryption process as follows.

Decryption of the secret key KE
KE = [71 77 94 152 98 161 83 81]
K0 = KE * Inv(s)= [0 1 8 7 8 3 0 5]
K1 is 8421 BCD encoded to get K2
K2 = [0000 0001 1000 0011 1000 0011 0000 0101]
K2 is gray decoded to get k1
K1 = [0000 0001 0000 0010 0000 0010 0000 0101]
Finally it is 8421 BCD decoded to get decrypted key K
K2 = [0 1 0 5 0 2 0 6]

Step 1: Using the secret key Bob selects the matrices B01 and B02 from the set of B of matrices. He computes the product of these two matrices raised to the power 05 and 06 in the correct order.

\[ A = B_{05} \times B_{06} = \]

\[
\begin{bmatrix}
1029952 & 252288 & -371800 & -1142208 & 1616736 & -1712736 & -1382976 & 835488 \\
1405056 & -603392 & 229952 & 878688 & 1109856 & 1136704 & -1999712 & -1514304 \\
603552 & -90880 & 505472 & 279352 & 672192 & 151328 & -399776 & -331284 \\
-163584 & 83424 & 94656 & -322496 & -26208 & -496320 & 242976 & 417210 \\
-142676 & -640220 & 511008 & 1737560 & 753120 & 2600544 & -2051520 & -2452896 \\
34752 & 25152 & 252672 & 207072 & 8352 & 193632 & 162912 & -138816 \\
406944 & -226736 & 10944 & 21504 & 383544 & 118368 & -530208 & -61244 \\
118364 & -545568 & 1540608 & -3064320 & 3211448 & -4242624 & -3131040 & 2297952 \\
\end{bmatrix}
\]

Step 2: The cipher text C excluding the last character is coded to the decimal numbers using ASCII code table and all the numbers are written as 8x8 matrix, the cipher matrix C.

Step 3: The string I of integers received along with the cipher text in public is converted to 8x8 matrix I excluding the last numeral.

D=256*1+C is computed

Step 4: The matrix D is multiplied with the inverse of encoding matrix A raised to the power 3 to get the matrix M.

\[
M = D \times Inv[A^3] =
\]

\[
\begin{bmatrix}
67 & 79 & 78 & 71 & 82 & 65 & 84 & 85 \\
76 & 65 & 84 & 73 & 79 & 78 & 83 & 46 \\
46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\
46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\
46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\
46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\
46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\
46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\
\end{bmatrix}
\]

All the elements are coded to text characters using the ASCII code table which is the original message CONGRATULATIONS.

4. CRYPTOANALYSIS AND CONCLUSIONS
The original message contains only 15 characters but the size of the block here is 64. So, the remaining characters are dummy which may be selected at random. Here same dummy character \( \ast \) is selected to fill the remaining characters. But, in the cipher the same character is mapped to different characters. This shields the cipher against the security implications like chosen plain text attacks, chosen cipher text attacks, linear cryptanalysis and mono-alphabetic cryptanalysis. In the proposed algorithm encoding matrix A is the product of two matrices Blm and Bno belonging to the set B. Hence the size of the key [13] space is 16x15 = 132. If we alter the algorithm such that A is the product of \( q \) matrices belonging to the set B, then the size of the key space will be \( 16 \times 15 \times \ldots \times (16+1-l) \). The size of key space can be increased by braiding the elements of the set B to form 16x16 non-singular matrices of the type

\[
\begin{bmatrix}
B_{pq} & 0 & B_{rs} & B_{ln} \\
0 & B_{rs} & B_{ln} & \end{bmatrix}
\]

and so on.

The encrypted secret key can be decrypted only by the authenticated receiver. i.e., who knows the matrix S. The procedure can be further improved to enhance the security level by selecting more matrices from the set B of matrices and raising each matrix to the power \( f(i,j) \) where the function \( f(i,j) \) is confidential between the communicating parties. So, the encryption algorithm presented here provides high level of security at relatively low computational overhead.

5. REFERENCES