ENCRYPTION OF DATA STREAMS USING PAULI SPINS ½ MATRICES

D. Sravana Kurmar[1,*], CH. Suneetha[2] and A. Chandra Sekhar[3]

[1] Department of Physics, Dr.V S. Krishna Government College, Visakhapatnam, India
skdharanikota@gmail.com

[2] Department of Mathematics, GIT, GITAM University, Visakhapatnam, India
gurukripachs@gitam.edu

[3]Department of Mathematics, GIT, GITAM University, Visakhapatnam, India
acs@gitam.edu

Abstract. Cryptography is the science of transmission and reception of secret messages. In modern times electronic communication has become an essential part of every aspect of human life. Message encryption has become very essential to avoid the threat against possible attacks by hackers during transmission process of the message. All the public key cryptosystems which are known so far are not absolutely secure between the sender and the receiver. In this paper we introduce a new technique of encryption of the message using Pauli Spin ½ matrices, which were named after the great physicist Wolfgang Pauli, that arise in the Pauli's treatment of spin of electrons in Quantum Mechanics.

Key words. Cryptography, Pauli Spin 1/2 matrices, Quantum Mechanics, Entanglement.

1. Introduction

The objective of Cryptography is to ensure secure communications over insecure public channel, so that attackers cannot break or steal the message [12]. The message is converted into an incomprehensible data in the process of encryption. The confidential data is generally encrypted to protect it from attackers, hackers and eavesdroppers [4]. The receiver of the message needs a procedure (algorithm) to retrieve the message from the incomprehensible data he receives. To make the procedure more secure the algorithm is devised so that the retrieval of the message from the encrypted data is possible only for a person holding a private (secret) key. This process is generally referred to as decryption. In the present paper a highly secure symmetric key cryptosystem is proposed using Pauli spin ½ matrices.

1.1 Pauli Spin 1/2 Matrices

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. The energy levels corresponding to the n, l, m_l quantum numbers were found to be further split up. Uhlenbeck and Goudsmit [9,10] in 1925 attributed these difficulties due to the fact that the electron has an additional property of intrinsic angular momentum and magnetic momentum. The magnitude of this intrinsic angular momentum of an electron can be determined by using the formula $\sqrt{\frac{h}{2\pi}\{S(S+1)\}}$ where S is the spin quantum number of electron and h is the Plank's constant. The spin quantum number is measurable value of the spin angular momentum along any direction, which is $\pm\frac{h}{4\pi}$. Pauli was the first to propose a non-relativistic wave equation, which takes into account the intrinsic magnetic moment of the electron. He introduced two wave functions ψ_1 *and* ψ_2 in which one wave function describes a state with one spin orientation, while the other one will describe a state with opposite spin. Pauli suggested that the wave function Ψ

should be chosen in the form of a column matrix $\Psi=\begin{bmatrix}\psi_1\\ \psi_2\end{bmatrix}$ and that the intrinsic magnetic moment of the electron should be put equal to $\mu=-\mu_0\sigma'$, where μ_0 is Bohr magneten[2] and σ' represents three 2×2 Pauli matrices [9, 10]. Pauli Spin ½ matrices are 2×2 complex Hermitian and unitary matrices

$$\sigma'_x=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\quad \sigma'_y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\quad \sigma'_z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

Properties of Pauli matrices:-

- The square of each Pauli matrix is equal to a unit matrix.

  I.e., $\sigma'^2_x=\sigma'^2_y=\sigma'^2_z=I$
- These matrices are mutually anti commutative and

  $\sigma'_x\sigma'_y=-\sigma'_y\sigma'_x=i\sigma'_z$

  $\sigma'_y\sigma'_z=-\sigma'_z\sigma'_y=i\sigma'_x$

  $\sigma'_z\sigma'_x=-\sigma'_x\sigma'_z=i\sigma'_y$

The components of spin angular momenta in terms of these matrices are given by

$S_x=\frac{h}{4\pi}\sigma'_x \qquad S_y=\frac{h}{4\pi}\sigma'_y \qquad S_z=\frac{h}{4\pi}\sigma'_z$ Where S_x, S_y and S_z are operators of components of spin of an electron in x,y,z directions of space coordinates. The square of spin angular momentum S is given by $S^2=S^2_x+S^2_y+S^2_z$

If we consider the set of all linear combinations of products of Pauli matrices, it can be represented by an algebra called Pauli algebra, also known as Clifford algebra [7,13] . Here $\sigma'^2_x+\sigma'^2_y+\sigma'^2_z=3I$ where I is the unit matrix. So, the Pauli matrices are involuntary matrices. The determinants and trace of Pauli matrices are -1 and 0 respectively. The eigen values of each Pauli matrix are either +1 or -1. The set of matrices whose elements are Pauli spin ½ matrices and the identity matrix I, forms an orthogonal basis for the complex Hilbert space of all 2x2 matrices. In Quantum mechanics, each Pauli matrix represents an observable describing the spin of a spin ½ particle in the three spatial directions. For a spin ½ particle the spin operator is given by J=h/2 σ', where h is the Plank's constant. The fact that any 2x2 complex Hermitian matrices can be expressed in terms of the identity matrix the Pauli matrices also lead to the Bloch sphere representation of 2×2 mixed states. This can be seen by simply first writing a Hermitian matrix as a real linear combination of {I, σ'_x, σ'_y, σ'_z}

2. Proposed method

Previously encryption processes using Golden Matrices were attempted [11]. In the present paper we use the basic Pauli Spin ½ matrices for the encryption of data streams.

Let $a=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, the identity matrix I

$b=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}=\sigma'_x$

$c=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}=i\,\sigma'_y$

$d=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=\sigma'_z$

We braid/entangle [5] these 2x2 matrices to form the set B of 4x4 non-singular braided matrices. The elements of the set B are formulated as follows.

$$B_{01} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$$

$$B_{02} = \begin{bmatrix} a & b \\ d & c \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{bmatrix}$$

$$B_{03} = \begin{bmatrix} a & c \\ d & b \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$$

$$B_{04} = \begin{bmatrix} b & a \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$$

$$B_{05} = \begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{bmatrix}$$

$$B_{06} = \begin{bmatrix} b & d \\ c & a \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$B_{07} = \begin{bmatrix} c & a \\ b & d \end{bmatrix} = \begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$$

$$B_{08} = \begin{bmatrix} c & d \\ a & b \end{bmatrix} = \begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$B_{09} = \begin{bmatrix} c & d \\ b & a \end{bmatrix} = \begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$B_{10} = \begin{bmatrix} d & b \\ a & c \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$B_{11} = \begin{bmatrix} d & c \\ a & b \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$B_{12} = \begin{bmatrix} d & c \\ b & a \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

This set B of twelve 4x4 non-singular matrices is used to encrypt the message.

3. Algorithm

3.1 Encryption

1. The text message is divided into data streams of 16 characters each. These data streams are coded to the equivalent numerals using the code table given below and the 4X4 message matrix M is obtained.

Code Table:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Null or Space

26

2. Two matrices, say, B_{lm} and B_{no} are selected arbitrarily from the set B of matrices.
3. The product of these two matrices $A = B_{lm} * B_{no}$ is determined. This matrix be called the encoding matrix. The subscripts of the matrices B_{lm}, B_{no} in the order of multiplication i.e. [l m n o] constitutes the private key. This private key is encrypted and sent to the receiver along with the cipher text in public channel. The sender and receiver agree upon a procedure to retrieve private key from the procedure as detailed below.
4. Before communicating the message, the sender and the receiver agree to use a matrix S which is non-singular to encrypt and decrypt the private secret key. The private key [l m n o] is first converted to weighted 8421 BCD code [6]. The 8421 BCD code thus obtained is gray coded [6]. Then it is 8421 decoded and written as 1 × 4 matrix. This 1 × 4 matrix is multiplied with the 4 × 4 matrix S which is already agreed by both the sender and the receiver. This gives 1 ×4 matrix (say K_E). This K_E is the encrypted key and it is sent in public channel.
5. The message matrix M is multiplied with the encoding matrix A raised to some power ‘p’, say.

$$E = M*(A)^p$$

6. E is adjusted to mod 27.

$$C = \text{mod}(E, 27)$$

7. The result along with the power of the encoding matrix A, i.e. ‘p’ is coded to characters using code table and sent to the receiver as the (cipher text C)
8. A matrix I whose elements are integer parts of elements of matrix E when adjusted to mod 27 is sent along with cipher text to the recipient. The elements of matrix I are sent as a string of numerals succeeded by power to which

the matrix A is raised (Say string I). The power of the encoding matrix may be changed for each data stream, depending upon the sensitivity of the data to be communicated.

3.2 Decryption

Before attempting for decryption of the text, the receiver verifies that the code corresponding to the last character in the cipher string is the same as the last numeral in the string I.

1. To obtain the private key from encrypted private key K_E, the receiver multiplies K_E with inverse of the matrix S. Then the elements of resulting 1 × 4 matrix are 8421 BCD encoded and Gray decoded. Finally the result is 8421 BCD decoded to get private key.
2. Using the private key [l m n o] the receiver selects the matrices B_{lm} and B_{no} from the set of matrices B. He computes the product of these to matrices $A = B_{lm} * B_{no}$. This matrix is encoding matrix used by the sender of the message.
3. The cipher text is coded to numerals using the code table. The last numeral is the power to which encoding matrix was raised during encryption. The numerals corresponding to cipher text are arranged in the form of a 4X4 matrix (cipher matrix C), excluding the last numeral.
4. The string I received along with the cipher text in public channel is converted to matrix I, excluding the last numeral. The elements of matrix I are multiplied with 27 and added to the cipher matrix.

$$D = 27*I + C \quad \text{(or)}$$
$$D_{ij} = 27I_{ij} + C_{ij}$$

Where D_{ij}, I_{ij} and C_{ij} are the elements of matrices D, I and C respectively.

5. The matrix D is multiplied with the inverse of the encoding matrix A raised to the power 'p'.

$$M = D*[\text{inv}(A)]^p$$

6. The numeral message M is decoded to text characters using the code table.

4. Example

4.1 Encryption

Suppose Alice wants to send the message CONGRATULATIONS to Bob. She converts this message to a numerical message using the code table.

1. The text is message in the present example has 15 characters. So null or space is taken as the sixteenth character.
Numerical message = [2 14 13 6 17 0 19 20 11 0 19 8 14 13 18 26]
This numerical message is used to form the message matrix M.

$$M = \begin{bmatrix} 2 & 14 & 13 & 6 \\ 17 & 0 & 19 & 20 \\ 11 & 0 & 19 & 8 \\ 14 & 13 & 18 & 0 \end{bmatrix}$$

2. Two matrices B_{12} and B_{09} are selected at random from the set B of matrices.
3. The product of these matrices $A = B_{12} * B_{09}$ is determined.

$$A = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}$$

This matrix be called encoding matrix. The subscripts of these matrices arranged in the order of multiplication [1 2 0 9] constitute the private key K (say).

K= [1 2 0 9]

4. Suppose the sender and receiver agree upon to use a matrix S which is non-singular

$$S = \begin{bmatrix} 2 & 3 & 4 & 1 \\ 1 & 1 & 2 & 1 \\ 3 & 3 & 3 & 1 \\ 1 & 2 & 3 & 1 \end{bmatrix}$$

K is 8421 BCD encoded to get K_1.

K_1 = [0001 0010 0000 1001]

K_1 is gray coded to get K_2

K_2= [0001 1011 0000 1101]

K_2 is 8421 BCD decoded to get K3

K_3 = [1 11 0 13].

K_3 is multiplied with S to get encrypted key K_E

$K_E = K_3 * S = [1\ 11\ 0\ 13] \begin{bmatrix} 2 & 3 & 4 & 1 \\ 1 & 1 & 2 & 1 \\ 3 & 3 & 3 & 1 \\ 1 & 2 & 3 & 1 \end{bmatrix}$ = [26 40 65 25] which is sent to the receiver as encrypted private key in public channel.

5. The message matrix M is multiplied with the encoding matrix A raised to the power 5.

$$E = M * A^5 = \begin{bmatrix} -144 & 496 & 368 & 112 \\ -288 & 352 & 256 & 896 \\ 0 & 256 & 352 & 608 \\ -144 & 272 & 720 & 304 \end{bmatrix}$$

6. E is adjusted to mod 27.

$$C = \text{mod}(E, 27) = \begin{bmatrix} 18 & 10 & 17 & 4 \\ 9 & 1 & 13 & 5 \\ 0 & 13 & 1 & 14 \\ 18 & 2 & 18 & 7 \end{bmatrix}$$

7. The result along with the power of matrix is coded to text using code table and sent as cipher text to Bob. This corresponds to **SKREJBNFANBOSCSHF**. In this cipher text string the last character F is the text code corresponding to numeral 5 i.e. power to which encoding matrix is raised.

8. A matrix whose elements are integer parts of elements of matrix E when adjusted to mod 27 is sent along with cipher text to Bob. The elements of this matrix are sent as a string of numerals succeeded by power to which the matrix A is raised.

$$I = \begin{bmatrix} -6 & 18 & 13 & 4 \\ -11 & 13 & 9 & 33 \\ 0 & 9 & 13 & 22 \\ -6 & 10 & 26 & 11 \end{bmatrix}$$

String I = [-6 18 13 4 -11 13 9 33 0 9 13 22 -6 10 26 11 5]

4.2 Decryption

Before attempting for the decryption Bob verifies that the code corresponding to the last character in the cipher text and the last numeral in the key are one and the same. Then Bob starts the decryption process. The last numeral in the key is the power to which the decrypting matrix is to be raised.

1.K_E = [26 40 65 25]

$$K_5 = K_E * \text{inv}(S) = [26\ 40\ 65\ 25] \begin{bmatrix} 1 & 1 & 0 & -2 \\ -2 & -2 & 1 & 3 \\ 2 & 1 & -1 & -2 \\ -3 & 0 & 1 & 3 \end{bmatrix} = [1\ 11\ 0\ 13]$$

K_5 is 8421 BCD encoded to get K_6

K_6 =[0001 1011 0000 1101]

K_6 is gray decoded to get K_7

K_7 =[0001 0010 0000 1001]

Finally it is 8421 BCD decoded to get the decrypted key K

K=[1 2 0 9]

2. Using the secret key Bob selects the matrices B_{12} and B_{09} from the set B of matrices. He computes the product of these two matrices A= B_{12}*B_{09} in the correct order.

$$A = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{bmatrix}$$

3. The cipher text **SKREJBNFANBOSCSHF** is coded to numerals using the code table. The last numeral corresponds to the power to which the inverse of encoding matrix A is to be raised.

Cipher = [18 10 17 4 9 1 13 5 0 13 1 14 18 2 18 7 5]

$$\text{Cipher matrix C} = \begin{bmatrix} 18 & 10 & 17 & 4 \\ 9 & 1 & 13 & 5 \\ 0 & 13 & 1 & 14 \\ 18 & 2 & 18 & 7 \end{bmatrix}$$

The inverse of encoding matrix A is to be raised to power 5 to decrypt the text.

4. The string I received along with the cipher text in public channel is converted to matrix I, excluding the last numeral.

String I is [-6 18 13 4 -11 13 9 33 0 9 13 22 -6 10 26 11 5]

$$I = \begin{bmatrix} -6 & 18 & 13 & 4 \\ -11 & 13 & 9 & 33 \\ 0 & 9 & 13 & 22 \\ -6 & 10 & 26 & 11 \end{bmatrix}$$

Matrix D = 27*I + C is computed.

$$D = \begin{bmatrix} -144 & 496 & 368 & 112 \\ -288 & 352 & 256 & 896 \\ 0 & 256 & 352 & 608 \\ -144 & 272 & 720 & 304 \end{bmatrix}$$

6. Message matrix is obtained by multiplying D with inverse of encoding matrix A raised to the power 5.

$$M = \begin{bmatrix} 2 & 14 & 13 & 6 \\ 17 & 0 & 19 & 20 \\ 11 & 0 & 19 & 8 \\ 14 & 13 & 18 & 0 \end{bmatrix}$$

6. The numeral message is decoded to text characters using the code table. This message matrix is equivalent to the text message CONGRATULATIONS.

5. Security Analysis

Several types of active and passive attacks [1,2,3,8,14] such as 1) known plaintexts attacks 2) Chosen plaintexts attacks 3) cipher text only attacks 4) chosen cipher text attacks are possible on the cipher text.

It is very difficult for passive and active attackers to decipher the cipher texts generated using the procedure described in this paper. For example in the message CONGRATULATIONS the characters O, N, A, T are repeated twice. But in the cipher text SKREJBNFANBOSCSHF, O is mapped to K and S, N is mapped to R and C, A is mapped to B and N and T is mapped to N and B. In the cipher text the character S appears thrice. But in the message no character is appearing three times.

The encryption process can be made more authentic and secure by adopting the following methods.

1) Using $M^1 = M+S \pmod{27}$ in place of M during encryption and retrieving
$M = M^1-S \pmod{27}$ during the decryption. Here the matrix S is the same matrix which is described in the encryption algorithm at step 4. The communicating parties should take care while choosing S, such that each element in S is less than 27.

2) The communication can be made more secure by selecting different keys for different data streams depending on the sensitivity of the message. Suppose that the entire message is divided into 'n' data streams of 16 characters each. The communication is made such that the encrypted key sent with m^{th} cipher stream corresponds to $[(m+p) \pmod{n}]^{th}$ cipher stream. Here p is the power of encoding matrix chosen at step 5 of encryption algorithm.

6. Key Space

In the proposed algorithm encoding matrix A is the product of two matrices B_{lm} and B_{no} belonging to the set B. Hence the size of the key space is 12x11 = 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 12 x 11 x ……. x (12+1-q).

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

$\begin{bmatrix} B_{pq} & 0 \\ 0 & B_{rs} \end{bmatrix}$ Or $\begin{bmatrix} B_{pq} & B_{rs} \\ 0 & B_{tu} \end{bmatrix}$ or $\begin{bmatrix} B_{pq} & 0 \\ B_{rs} & B_{tu} \end{bmatrix}$ and so on. With braided matrices of the order 16x16, use of data streams of 256 characters (that form 16x16 message matrices) and ASCII code table will be more practicable and appropriate.

7. **Conclusions**

The proposed algorithm refers to symmetric key cryptography. The level of security is more in the proposed algorithm since it involves the encryption at four levels.

- Selection of the matrices arbitrarily from the set B
- Order of multiplication of the matrices i.e., the sequence of multiplication of the matrices.

- Power of the encrypting matrix
- Key matrix

It is very difficult to obtain secret key from cryptanalysis, because the plaintext is coded using code table, a mod function is used and the power of the encoding matrix is changed for each data stream. The encrypted key can be decrypted by the authenticated receiver. i,e, who knows the matrix S. The procedure can be further improved to make encryption more difficult by selecting more matrices from set B, so that the encrypted matrix is the product of the individual matrices raised to different powers in the specific order $B_{01}^{q}B_{02}^{r}B_{03}^{s}$……where q, r, s,…..$\in$N and this matrix will be used as the encoding matrix raised to some power p$\in$N the set of natural numbers. The proposed algorithm provides high security at relatively low computational difficulty.

8. Acknowledgement

The second author (CHS) is grateful to GITAM University, Visakhapatnam, India for the financial support extended under the minor research project "Encryption for data security using mathematical technique".

9:References

[1] Johannes A. Buchmann, Introduction to Cryptography II Edition, Springer-Verlag, 2001
[2] F. Bauer, Decrypted Secrets, Springer- Verlag, Berlin, 2000
[3] Canetti R. Halevi, S. and Katz, J. Chosen cipher text security from identity-based encryption, Advances in Cryptography-EUROCRYPT 2004, Vol. 3027 of LNCS, Springer-Verlag
[4] A. Chandra Sekhar, Prasad Reddy P.V.G.D, A.S.N. Murthy, B. Krishna Gandhi "Self Encrypting Data Streams Using Graph Structures" IETECH Journal of Advanced Computations, Vol:2 No:1, 2007-2009
[5] A. Chandra Sekhar, D. Sravana Kumar and CH. Suneetha, Encryption of Data streams using Boolean Matrices, proceedings of International Conference on Challenges and Applications of Mathematics in Science and Technology ed. by S. Chakraverty (Advanced Research Series, Macmillan Publishers India Ltd., 2010), pp. 524-531
[6] Donald P. Leach, Albert P. Malvino and Goutam Saha, Digital Principles & Applications, VI Edition, Tata McGraw-Hill Publishing Co. 2006
[7] Michel Planat and Patric Solse "Clifford groups of Quantum gates, BN-pairs and smooth cubic surfaces" Journal of Physics A: Mathematical and theoretical 19th December 2008
[8] Y. Rangel-Romero et al, Comments on How to repair Hill cipher, Zhejiang University Press, co-publisher with Springer-Verlag, 2007
[9] Richard Liboff, Introductory Quantum Mechanics, IV Edition, Addison Wesley, 2002
[10] J. J. Sakurai, Modern Quantum Mechanics, Addidon Wesley, 1985
[11] A.P. Stakhov,"The 'golden' matrices and a new kind of cryptography", Chaos, Solutions and Fractals 32 ((2007) pp1138–1146
[12] D. Stinson, Cryptography, Theory and Practice, CRC Press, Boca Raton Florida, II Edition, 2002
[13] M. Yoshida-Dier olf "Operator algebra for birefringence and mirror reflection" Journal of Optics Communications Volume 203, Issues1-2 March 2002, page 79-85
[14] B. Zhang, H. Wu, D. Feng, F. Bao, Chosen cipher text attack on a new class of self-synchronizing stream ciphers, in progress in cryptology-INDOCRYPT 2004,ed. by A. Canteaut, K. Viswanathan, Lecture Notes in Computer Science, Vol. 3348/2004 (Springer, Berlin, 2004), pp.73-83