

# Encryptions of Data Streams using Pauli Spin $\frac{1}{2}$ Matrices and Finite State Machine

B. Krishna Gandhi  
Professor J.N.T.U(H) C.E  
Hyderabad India

A. Chandra Sekhar  
GITAM university  
Vishakapattanam, India

S. Sri Lakshmi  
Lecturer J.N.T.U(A)  
C.E.Anantapur India

## ABSTRACT

Cryptography is the science of transmission and reception of secret messages. Recently 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. Finite state machines (FSM), also known as finite state automation (FSA), at their simplest, are models of the behaviors of a system or a complex object, with a limited number of defined conditions or modes, where mode transitions change with circumstance. In the present paper, new cryptographic scheme is proposed using finite state machine and Pauli spins  $\frac{1}{2}$  matrices.

## Keywords

Moore Machine, key, recurrence relation, cryptography Pauli Spin  $\frac{1}{2}$  matrices, Quantum Mechanics, Entanglement .

## 1. INTRODUCTION

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security but rather on set of techniques. Cryptography plays a fundamental role in securing communication.[6]

Cryptography referred almost exclusively to encryption, the process of converting ordinary information (plain text) into unintelligible gibberish (cipher text). Decryption is the reverse, moving from unintelligible cipher text to plain text. A cipher is a pair of algorithms, which perform this encryption and the reversing decryption. The detailed operation of cipher is controlled both by the algorithm and, in each instance, by a key. This is a secret parameter (known only to the communicants) for a specific message exchange context. Cryptography can be defined as the study of mathematical techniques related to the security of transmission and storage of information. Cryptography was concerned solely with message confidentiality (i.e., encryption) conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message).

### 1.1 Finite State Machines

Automata theory is a key to software for verifying systems of all types that have a finite number of distinct states, such as communication protocols or protocol for secure exchange of information. Finite state machines (FSM), also known as finite state automation (FSA) , at their simplest ,are models of

the behaviors of a system or a complex object, with a limited number of defined conditions or modes, where mode transitions change with circumstance.

Finite state machines consist of four main elements:

1. States which define behavior and may produce actions.
2. State transitions which are movement from one state to another.
3. Rules or conditions which must be met to allow a state transition.
4. Input events which are either externally or internally generated, which may possibly trigger rules and lead to state transitions.

A finite state machine must have an initial state which provides a starting point, and a current state which remembers the product of the last state transition. Received input events act as triggers, which cause an evaluation of some kind of the rules that govern the transitions from the current state to other states. The best way to visualize a FSM is to think of it as a flow chart or a directed graph of states.

In Moore Machine every of finite state machine has a fixed output. [5][7] Mathematically Moore machine is a six- tuple machine and is defined as

$$M = (Q, \Sigma, \Delta, \delta, \lambda', q_0)$$

$Q$  : A nonempty finite set of state in Moore machine

$\Sigma$  : A nonempty finite set of inputs.

$\Delta$  : A nonempty finite set of outputs.

$\delta$  : It is a transition function which takes two arguments one is input state and another is input symbol. The out put of this function is a single state.

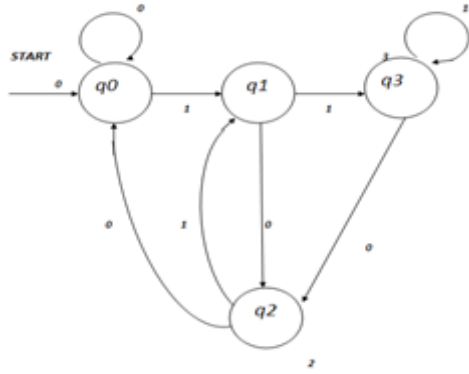
$\lambda'$  : Is a mapping function which maps  $Q \times \Sigma$  to  $\Delta$ , giving the output associated with each transition.

$q_0$  : is the initial state of  $Q$

Moore machine can also be represented by transition table, as well as transition diagram.

In the present paper consider Moore machine which calculates the residue mod 4

**Fig 1 Moore machines which calculates residue mod 4**



## 1.2 Pauli Spin 1/2 Matrices

In the present paper we use the basic Pauli spin 1/2 matrices for the encryption of data streams [3]

The pauli spin matrices are set of three 2x2 complex matrices  $\sigma_1, \sigma_2$  and  $\sigma_3$  which are Hermitian and unitary matrices represents the intrinsic angular momentum components of spin 1/2 particles in quantum mechanics.

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2. PROPOSED ALGORITHM

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.[1][2][4]

Code table

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26
Null or Space 27												

### 2.1 Algorithm

#### Encryption

Step 1

Let P be a square matrix of order 4, is the plain text.

Step 2

Select secret key in binary form and a finite state machine.

Step 3

Define cipher text at q(i+1)th state

Cipher text at q(i+1)th state = cipher text at q(i)th state \*

$[B_{\text{secret code in decimal form mod 12}}]_{\text{out put at q(i+1)th state.}}$

Step 4

Send this cipher text to the receiver.

#### Decryption

Decrypt the cipher text using the key and the key matrices B.

### 2.2 Example

Let the secret key be 22(10110)

$$P = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix}$$

Let the finite state machine be the Moore machine which calculates the residue mod4

For mathematical computations, in this paper we use mod (61).

Table 1.2 Example

S.No	input in the binary form	input in decimal form mod 12	present state	output	key matrix	cipher text
1	1	1	$q_1$	1	$B_{01}$	$\begin{bmatrix} 5 & -1 & 5 & -3 \\ 13 & -1 & 13 & -3 \\ 21 & -1 & 21 & -3 \\ 29 & -1 & 29 & -3 \end{bmatrix}$
2	0	2	$q_2$	2	$B_{02}$	$\begin{bmatrix} 11 & 2 & 3 & 9 \\ 35 & 2 & 11 & 17 \\ 59 & 2 & 19 & 25 \\ 22 & 2 & 27 & 33 \end{bmatrix}$
3	1	5	$q_1$	1	$B_{05}$	$\begin{bmatrix} 5 & 2 & 20 & -1 \\ 13 & 18 & 52 & -9 \\ 21 & 34 & 23 & -17 \\ 29 & -11 & 55 & -25 \end{bmatrix}$
4	1	11	$q_3$	3	$B_{11}$	$\begin{bmatrix} 38 & -42 & -6 & -14 \\ 25 & 0 & 10 & -1 \\ 12 & -19 & 26 & -49 \\ 60 & -38 & -19 & -36 \end{bmatrix}$
5	0	10	$q_2$	2	$B_{10}$	$\begin{bmatrix} -24 & 16 & 11 & 27 \\ 34 & 16 & 14 & 36 \\ -30 & 16 & -44 & 40 \\ -33 & 16 & 20 & 54 \end{bmatrix}$

Then the cipher text is

$$\begin{bmatrix} -24 & 16 & 11 & 27 \\ 34 & 16 & 14 & 36 \\ -30 & 16 & -44 & 40 \\ -33 & 16 & 20 & 54 \end{bmatrix}$$

### 2.3 Security analysis

To extract the original information, it is very difficult due to the chosen finite state machine and the pauli spin  $\frac{1}{2}$  matrices.

Brute force attack on key is also difficult due to the increase in key size.

Table 2.2 Security analysis

S.No	Name of the attack	Possibility of the attack	Remarks
1	Cipher text attack	Very difficult	Due to the secret key, chosen finite state machine and the operation matrix multiplication.
2	Known plain text attack	Not easy	Due to the chosen finite state machine and the operation matrix multiplication.
3	Chosen plain text attack	Difficult	Due to the chosen finite state machine and the operation matrix multiplication.
4	Adaptive chosen plain text attack	Difficult	Due to the chosen finite state machine and the operation matrix multiplication.
5	Chosen cipher text attack	Very difficult	Due to the secret key, chosen finite state machine and the operation matrix multiplication.
6	Adaptive chosen cipher text attack	Very difficult	Due to the secret key, chosen finite state machine and the operation matrix multiplication.

### 3. CONCLUSIONS

A robust implementation of the secure data management is critical to the message transformation. In the present paper a scalable cryptographic scheme to enhance the message protection is presented based on finite state machines and the operation matrix multiplication. Secrecy is maintained at three levels, the secret key, the chosen finite state machine, and the Pauli spin  $\frac{1}{2}$  matrixes. The obtained cipher text becomes quite difficult to break or to extract the original information even if the algorithm is known. Therefore a more reliable cryptosystem can be realized with a single secret key.

### 4 REFERENCES

- [1] B.Krishna Gandhi, .A.Chandra Sekhar, S.Srilakshmi (September 2011) "Cryptographic scheme for digital signals using finite state machine" international journal of computer applications.
- [2] A.Chandra Sekhar,D.Sravana Kumar and CH.Suneetha, "Encryption of Data Streams using Boolean Matrices, Proceedings of International conference on challenges and application of Mathematics in Technology ed. By S.Chakravaty(Advanced Research series, Macmillan Publishers India Ltd., 2010),pp.523-531.
- [3] D.Sravana Kumar, CH.Suneetha and A.Chandra Sekhar " Encryption of Data Streams using Pauli spins  $\frac{1}{2}$  matrices" International journal of Engineering Science and Technology Vol . 2(6), 2010, 2020-2028.
- [4] A.P.Stakhov " The Golden matrices and a new kind of cryptography" chaos, solutions and Fractals 32(2007) pp1138-1146.
- [5] Adesh K.Pandey. reprint 2009, "An introduction to automata theory and formal languages 'S.K.Kararia & sons. New Delhi.
- [6] A.Menezed, P.Van Oorschot and S.Vanstone Hand book of Applied Cryptography e-Book.
- [7] John E.Hopcroft, Rajeev Motwain, Jeffrey D.Ulman. " Introduction to automata theory,language,and computation" Vanstone3<sup>rd</sup> impression,2007 CRC Press., Dorling Kindersley (India) Pvt.Ltd.