International Journal of Theoretical Physics (2018) 57: 3584–3594
https://doi.org/10.1007/s10773-018-3872-6

Information Confidentiality Using Quantum Spinning, Rotation and Finite State Machine

Hafiz Muhammad Waseem[1] · **Majid Khan**[2]

Received: 25 April 2018 / Accepted: 20 August 2018 / Published online: 6 September 2018

Abstract
Traditional and modern cryptosystems purely rely on mathematics and their algorithms based on fundamental process of factoring large integers into their primes, which is said to be intractable. But this type of cryptography vulnerable to both evolutions in mathematics and development of high computing power which can easily reverse one way functions. Now the requirement is to design a new mechanism whose reverse computation is not possible for any system. The robust security mechanism is necessary. The combination of quantum mechanism and cryptography make it possible to develop such a secure communication systems that utilized different energy spectra for the transmission of information. The combination of quantum mechanics and cryptography gives birth to quantum cryptography. Quantum cryptography is one of the most remarkable application of quantum information theory. To measure the quantum state of any system is not possible without disturbing that system. The facts of quantum mechanics on traditional cryptosystems leads to a new protocol, algorithms and achieving maximum security for systems. The aim of this article is to apply quantum spinning and rotation along with finite state machine to develop an efficient cryptosystems for text encryption and decryption.

Keywords Quantum cryptography · Passive rotation operators · Quantum spinning · Finite state machine

1 Introduction

In regular daily existence, there are numerous circumstances when it is important to hide the actual contents of secret information transmitted over an insecure line of communication. Many traditional cryptosystems were utilized to perform these tasks in order to encrypt the confidential information. However, in a near future all these classical cryptosystems merely

✉ Majid Khan
mk.cfd1@gmail.com

[1] Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan

[2] Department of Applied Mathematics & Statisitcs, Institute of Space Technology, Islamabad, Pakistan

computational secure. The existing classical cryptographic algorithms fundamentally rely on limited computationally development of computer power and mathematical structures. Traditional cryptography experiences key distribution issue, how to convey the key safely between two sets of clients. For quite a long time, it was trusted that the main plausibility to take care of the key dissemination issue was to send some physical medium. With the advancement of technologies, this criterion is obviously unconventional. Moreover, it is even impossible to validate the authentication, integrity and non-repudiation of the transmitted digital contents. Public key cryptography addressed this issue in a quite decent way, yet these algorithms are moderate and cannot be utilized to scramble a lot of information at the same time. Asymmetric key cryptography endures in light of the fact that despite the fact that restricted capacities have not been yet switched with innovative and mathematical advances it is conceivable. The development of quantum cryptography can truly debilitate their security. Previously, there has been a decent arrangement of another cryptographic strategy whose security depends on the principal laws of quantum information science and quantum cryptography. The principle accomplishment is that it can tackle the issue of key distribution. From the reasonable perspective, it is fascinating that quantum cryptography may properly be acknowledged by methods for quantum optics and the optical fiber fills in as a transmission channel [9, 10]. To encode data for instance polarization (disparity, division) or different phases can be utilized. The fundamental principle of quantum mechanism is that the light waves are comprised of a huge number of discrete quanta called photons which are mass less and have energy, momentum and angular momentum called spinning. The spinning of photon conveys the polarization. These photons are unified much like atoms, it simply that they are units of lights [8] .

Photon polarization describes how light photons can have polarized in specific directions. Photon filter with the correct polarization can only detect a polarized photon. The one way characteristics of photons along with the Heisenberg uncertainty principle make quantum cryptography an attractive option to ensure the privacy and defeating eavesdroppers [2]. Some particles, like electrons, neutrinos and quarks have half integer internal angular momentum also called spin . We develop a spinor representation in this paper for spin $1/2$ to give a new direction to cryptography via spinning operators of quantum mechanics [1], [3]– [7]. We have shown here, not only the keys but the message can also be encrypted via this technique. The important aspect of our suggested algorithm is phase information, because phase is used to encrypt and decrypt the keys and message. To achieve maximum security, we use different phases for key and message. To decrypt the message, first we have to decrypt the keys by using phase information and then by using keys with phase information of message to decrypt the message.

The rest of the paper is organized as follow. We have added basic definition of finite state machine in Section 2. The derivation of rotation operator is given in Section 3. The proposed quantum spinning and rotations based algorithm illustrate with example and sensitivity analysis are given in Section 4. Finally, conclusion is given in Section 5.

2 Finite State Machine

Finite state automation (FSA) or finite state machines (FSM) are models of behaviors for a system or a complex object, with a limited number of defined modes or conditions, where mode transitions change in circumstances [7].

A DFA (deterministic finite automation) is quintuple $M = (X, \sum, q_0, \wp, F)$, where

X is state of finite sets,
$\sum$ is input symbols of finite set,
q_0 is start state indicated by an arrow $\rightarrow$,
$\wp$ is transition function $\wp : X \times \sum \rightarrow X$, i.e.,, $\wp(q_0, a) = q_i \in X$,
$F \subset X$ is a finite set of final set of final states.

The input symbols can be letters or digits. We say that a string M is accepted by DFA (Deterministic Finite Automaton-self operating machine), if the set of languages accepted by a DFA 'X' is denoted by $L(X)$. In DFA, there is only one transition out of each state on the same input symbol. NDFA (Nondeterministic Finite Automaton) can also be considered here as a mathematical model. In NDFA, we considered here a Moore machine and we use NDFA in our algorithm. In Moore machine, the output depends on the transitions (Fig. 1).

3 Derivation of Rotation Operators

The laws of physics not depend on what axis we choose for our coordinate system (rotational symmetry). If we make an infinitesimal rotation (through and angle $d\phi$) about the$r-$axis, we get the transformed coordinates [5],

$$\begin{aligned} p^{'} &= p - d\phi q, \\ q^{'} &= q + d\phi p. \end{aligned} \tag{1}$$

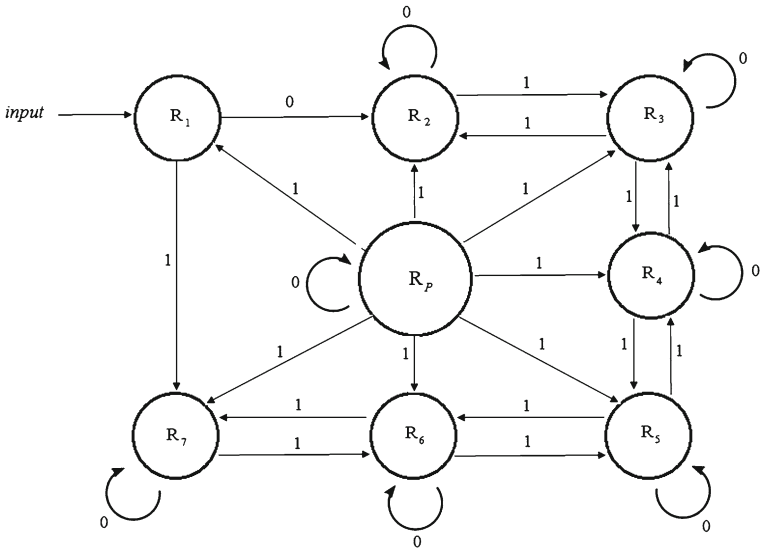

Fig. 1 Finite state machine algorithm

Apply Taylor series on (1) to expand the function.

$$f(p', q') = f(p, q) - \frac{\partial f}{\partial p} d\phi q + \frac{\partial f}{\partial q} d\phi p = \left(1 + \frac{\iota}{\hbar} d\phi S_r\right) f(p, q),$$
$$R_r(d\phi) = \left(1 + \frac{\iota}{\hbar} d\phi S_r\right),$$

where $\hbar$is internal angular momentum. A finite rotation can be made by applying the operator for an infinitesimal rotation over and over. Let $\theta_r = nd\phi$, then

$$R_r(\theta) = \lim_{n\to\infty} \left(1 + \frac{\iota}{\hbar}\frac{\theta}{n} S_r\right)^n = e^{i\theta \frac{S_r}{\hbar}}. \tag{2}$$

If we make an infinitesimal rotation about the $q-$axis, we get the transformed coordinates

$$p^{'} = p - d\phi r$$
$$r^{'} = r + d\phi p \tag{3}$$

Apply Taylor series on (3) to expand the function given below

$$f(p^{'}, r^{'}) = f(p, r) - \frac{\partial f}{\partial p} d\phi r + \frac{\partial f}{\partial r} d\phi p = \left(1 + \frac{\iota}{\hbar} d\phi S_q\right) f(p, r),$$
$$R_q(d\phi) = \left(1 + \frac{\iota}{\hbar} d\phi S_q\right).$$

A finite rotation can be made by applying the operator for an infinitesimal rotation over and over. Let $\theta_q = nd\phi$, then

$$R_q(\theta) = \lim_{n\to\infty} \left(1 + \frac{\iota}{\hbar}\frac{\theta}{n} S_q\right)^n = e^{i\theta \frac{S_q}{\hbar}}. \tag{4}$$

If we make an infinitesimal rotation about the $p-$axis, we get the transformed coordinates

$$q^{'} = q - d\phi r,$$
$$r^{'} = r + d\phi q. \tag{5}$$

Apply Taylor series on (5) to expand the function.

$$f(q^{'}, r^{'}) = f(q, r) - \frac{\partial f}{\partial q} d\phi r + \frac{\partial f}{\partial r} d\phi q = \left(1 + \frac{\iota}{\hbar} d\phi S_p\right) f(q, r),$$
$$R_p(d\phi) = \left(1 + \frac{\iota}{\hbar} d\phi S_p\right).$$

A finite rotation can be made by applying the operator for an infinitesimal rotation over and over. Let $\theta_p = nd\phi$, then

$$R_p(\theta) = \lim_{n\to\infty} \left(1 + \frac{\iota}{\hbar}\frac{\theta}{n} S_p\right)^n = e^{i\theta \frac{S_p}{\hbar}}. \tag{6}$$

3.1 Derive Spin $\frac{1}{2}$ Operators

We use eigenstates of S_r as the basis states [6]

$$\begin{aligned} X_+ &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \\ X_- &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \\ S_r\ X_\pm &= \pm\frac{\hbar}{2} X_\pm, \\ S_r &= \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

It must be diagonal, since the basis states are eigenvectors of the matrix. Now to perform the raising and lowering operators [6], we have

$$\begin{aligned} S_+ X_- &= \overset{S_+ X_+ = 0,}{\sqrt{s(s+1) - m(m+1)}}\hbar X_+ = \hbar X_+, \\ S_+ &= \hbar\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \\ S_- X_- &= 0, \\ S_- X_+ &= \sqrt{s(s+1) - m(m-1)}\hbar X_- = \hbar X_-, \\ S_- &= \hbar\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

Now we can calculate S_p and S_q.

$$S_p = \frac{1}{2}(S_+ + S_-) = \frac{\hbar}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{7}$$

$$S_q = \frac{1}{2\iota}(S_+ - S_-) = \frac{\hbar}{2\iota}\begin{pmatrix} 0 & -\iota \\ \iota & 0 \end{pmatrix}. \tag{8}$$

The Pauli spin matrices are defined as [4],

$$S_i = \frac{\hbar}{2}\sigma_i. \tag{9}$$

Compare (7)-(8) and (9) with (10) to get σ (Pauli matrices).

$$\begin{aligned} \sigma_p &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ \sigma_q &= \begin{pmatrix} 0 & -\iota \\ \iota & 0 \end{pmatrix}, \\ \sigma_r &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned} \tag{10}$$

These are traceless Hermitian matrices, and $\sigma_p^2 = \sigma_q^2 = \sigma_r^2 = I$ (identity) [1]. Now put (10) in (2), (4) and (6) to get rotation operators with respect to σ.

$$\begin{aligned} R_p(\theta) &= e^{i\frac{\theta}{2}\sigma_p}, \\ R_q(\theta) &= e^{i\frac{\theta}{2}\sigma_q}, \\ R_r(\theta) &= e^{i\frac{\theta}{2}\sigma_r}, \end{aligned} \tag{11}$$

$$e^{i\frac{\theta}{2}\sigma_j} = \sum_{n=0}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!}\sigma_j^n. \tag{12}$$

Now deriving the rotation operators of (11) with the help of (12) [6].

$$R_p(\theta) = e^{i\frac{\theta}{2}\sigma_p} = \begin{pmatrix} \sum\limits_{n=0,2,4,\ldots}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} & \sum\limits_{n=1,3,5,\ldots}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} \\ \sum\limits_{n=1,3,5,\ldots}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} & \sum\limits_{n=0,2,4,\ldots}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} & \iota\sin\frac{\theta}{2} \\ \iota\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{13}$$

$$R_q(\theta) = e^{i\frac{\theta}{2}\sigma_q} = \begin{pmatrix} \sum\limits_{n=0,2,4,\ldots}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} & -\iota \\ \iota & \sum\limits_{n=1,3,5,\ldots}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} \end{pmatrix} \begin{pmatrix} \sum\limits_{n=1,3,5,\ldots}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} \\ \sum\limits_{n=0,2,4,\ldots}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{14}$$

$$R_r(\theta) = e^{i\frac{\theta}{2}\sigma_r} = \begin{pmatrix} \sum\limits_{n=0}^{\infty} \frac{\left(i\frac{\theta}{2}\right)^n}{n!} & 0 \\ 0 & \sum\limits_{n=0}^{\infty} \frac{\left(-i\frac{\theta}{2}\right)^n}{n!} \end{pmatrix} = \begin{pmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{pmatrix}. \tag{15}$$

4 Proposed Algorithm

We have derived the rotation operators around p, q and r axis. By using the results, we encrypt the key and message by following algorithm. We ignore the imaginary numbers and used real axis for calculations.

$$\begin{aligned} a &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, \\ b &= \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} = R_p(\theta), \\ c &= \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} = R_q(\theta), \\ d &= \begin{pmatrix} e^{\frac{\theta}{2}} & 0 \\ 0 & e^{-\frac{\theta}{2}} \end{pmatrix} = R_r(\theta). \end{aligned} \tag{16}$$

Let entangle 2×2 matrices of (16) to form the set A of 4×4 entangle matrices. The elements of the set A are:

$$A_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & 1 & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \\ \cos\frac{\theta}{2} & \sin\frac{\theta}{2} & e^{\frac{\theta}{2}} & 0 \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} & 0 & e^{-\frac{\theta}{2}} \end{bmatrix}$$

$$A_2 = \begin{bmatrix} a & b \\ d & c \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & 1 & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \\ e^{\frac{\theta}{2}} & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & e^{-\frac{\theta}{2}} & -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix},$$

$$A_3 = \begin{bmatrix} a & d \\ b & c \end{bmatrix} = \begin{bmatrix} 1 & 0 & e^{\frac{\theta}{2}} & 0 \\ 0 & 1 & 0 & e^{-\frac{\theta}{2}} \\ \cos\frac{\theta}{2} & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix},$$

$$A_4 = \begin{bmatrix} a & d \\ c & b \end{bmatrix} = \begin{bmatrix} 1 & 0 & e^{\frac{\theta}{2}} & 0 \\ 0 & 1 & 0 & e^{-\frac{\theta}{2}} \\ \cos\frac{\theta}{2} & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix},$$

$$A_5 = \begin{bmatrix} a & c \\ d & b \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & 1 & -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \\ e^{\frac{\theta}{2}} & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & e^{-\frac{\theta}{2}} & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$A_6 = \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & 1 & -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \\ \cos\frac{\theta}{2} & \sin\frac{\theta}{2} & e^{\frac{\theta}{2}} & 0 \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} & 0 & e^{-\frac{\theta}{2}} \end{bmatrix},$$

$$A_7 = \begin{bmatrix} b & a \\ c & d \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} & 1 & 0 \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} & 0 & 1 \\ \cos\frac{\theta}{2} & \sin\frac{\theta}{2} & e^{\frac{\theta}{2}} & 0 \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} & 0 & e^{-\frac{\theta}{2}} \end{bmatrix},$$

$$A_8 = \begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} & 1 & 0 \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} & 0 & 1 \\ e^{\frac{\theta}{2}} & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & e^{-\frac{\theta}{2}} & -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix},$$

$$\vdots$$

$$A_{24} = \begin{bmatrix} d & b \\ a & c \end{bmatrix} = \begin{bmatrix} e^{\frac{\theta}{2}} & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & e^{-\frac{\theta}{2}} & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \\ 1 & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & 1 & -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}.$$

4.1 Encryption

1. Define the phase for defined rotation matrices (known to sender and receiver only),
2. Convert the message into numeric vector of order $4 \times n$, say M,
3. Define finite state machine,
4. Decide a key for secret communication,
5. Convert they key into binary,
6. Start with left most bit for encryption of message with rotation matrices and add one by one the key bits towards right and convert to decimal at each step and *mod* the key to 24. Round of encryption depends on key length,
7. Convert the numeric matrix into alphabets at each step to get different ciphers,
8. Finally, cipher alphabets received by using the full length of the key, say M_c.

4.2 Decryption

1. Enter the phase where the message was encrypted,
2. Convert alphabetical cipher message into numeric matrix of order $4 \times n$, say M_c,
3. Enter the key for which the message encrypted and convert it into binary,
4. Now start with full length key under *mod* 24 and operate the cipher with inverse rotation matrices and then subtract 1 by 1 bit from right side under *mod* 24 to operate with rotation matrices,
5. The final numeric vector obtained by performing the inverse rotation matrix of left most bit with previous cipher,
6. Convert the numeric matrix into alphabetical vector to get original message.

4.3 Example

Let us consider a message *'INCOMPREHENSIBLE'* to be encrypted and decrypted at phase $\theta = 320°$ with key 59.

$$M = INCOMPREHENSIBLE = \begin{bmatrix} 8 & 13 & 2 & 14 \\ 12 & 15 & 17 & 4 \\ 7 & 4 & 13 & 18 \\ 8 & 1 & 11 & 4 \end{bmatrix}.$$

4.3.1 Finite State Machine

The mathematical expression of finite state machine which will be used in our proposed algorithm is given below

$$q_{k+1} = q_k \times \left[R_{(\text{sec ret code in decimal form mod } 24)}\right]^{output\ q_{k+1}\ state}.$$

4.3.2 Encryption

The following components are basic requirement for the encryption of plain text *'INCOMPREHENSIBLE'* (see Table 1).

We are now utilizing the fundamental components which are selected in Table 1, by transforming the plaintext into a ciphertext. A comprehensive procedure of our proposed encryption algorithm is given in Table 2.

Table 1 Basic components for encryption of proposed algorithm

Phase	Encryption key					
	Decimal form	Binary form	Rounds	Binary input	Decimal input	Key matrix
320	59	111011	1	1	1	A_1
			2	11	3	A_3
			3	111	7	A_7
			4	1110	14	A_{14}
			5	11101	5	A_5
			6	111011	11	A_{11}

4.3.3 Decryption

The decryption is an inverse process of encryption to transform the ciphertext into a plaintext. The fundamental steps in decryption of information in proposed algorithm are same but apply in a reverse way (see Tables 3 and 4).

Table 2 Encryption process of proposed algorithm

Cipher	Cipher matrix	Cipher message
C_1	$(A_1 \times M) = \begin{bmatrix} 3 & 9 & 17 & 22 \\ 6 & 15 & 9 & 4 \\ 15 & 13 & 17 & 24 \\ 2 & 6 & 20 & 13 \end{bmatrix}$	$DJRWGPJEPNRYCGUN$
C_2	$(A_7 \times C_2) = \begin{bmatrix} 0 & 17 & 23 & 14 \\ 15 & 1 & 1 & 24 \\ 19 & 13 & 3 & 17 \\ 17 & 24 & 7 & 13 \end{bmatrix}$	$LTXRIMUSECLCUIUN$
C_3	$(A_7 \times C_2) = \begin{bmatrix} 0 & 17 & 23 & 14 \\ 15 & 1 & 1 & 24 \\ 19 & 13 & 3 & 17 \\ 17 & 24 & 7 & 13 \end{bmatrix}$	$ARXOPBBYTNDRRYHN$
C_4	$(A_{14} \times C_3) = \begin{bmatrix} 17 & 16 & 0 & 3 \\ 1 & 24 & 0 & 11 \\ 18 & 6 & 14 & 14 \\ 18 & 0 & 21 & 5 \end{bmatrix}$	$RQADBYALSGOOSAVF$
C_5	$(A_5 \times C_4) = \begin{bmatrix} 13 & 1 & 7 & 21 \\ 12 & 25 & 15 & 4 \\ 3 & 17 & 25 & 3 \\ 15 & 9 & 8 & 20 \end{bmatrix}$	$NBHVMZPEDRZDPJIU$
C_6	$(A_{11} \times C_5) = \begin{bmatrix} 7 & 1 & 7 & 13 \\ 17 & 10 & 14 & 6 \\ 18 & 17 & 1 & 19 \\ 1 & 4 & 20 & 4 \end{bmatrix}$	$HBHNRKOGSRBTBEUE$

Table 3 Basic components for decryption of proposed algorithm

Phase	Encryption key					
	Decimal form	Binary form	Rounds	Input binary	Input decimal	Key matrix
320	59	111011	1	111011	11	A_{11}
			2	11101	5	A_5
			3	11101	14	A_{14}
			4	111	7	A_7
			5	11	3	A_3
			6	1	1	A_1

4.4 Sensitivity Analysis

We have applied, our designed algorithm on different texts in which some texts shown in Table 5. By changing the phase, key or both lead to change the cipher. The beauty and versatility of designed algorithm is to change any term (either key or phase) lead to change

Table 4 Decryption process of proposed algorithm

Cipher	Cipher matrix	Cipher message
C_5	$\left(A_{11}^{-1} \times C_6\right) = \begin{bmatrix} 13 & 1 & 7 & 21 \\ 12 & 25 & 15 & 4 \\ 3 & 17 & 25 & 3 \\ 15 & 9 & 8 & 20 \end{bmatrix}$	$NBHVMZPEDRZDPJIU$
C_4	$\left(A_5^{-1} \times C_5\right) = \begin{bmatrix} 17 & 16 & 0 & 3 \\ 1 & 24 & 0 & 11 \\ 18 & 6 & 14 & 14 \\ 18 & 0 & 21 & 5 \end{bmatrix}$	$RQADBYALSGOOSAVF$
C_3	$\left(A_{14}^{-1} \times C_4\right) = \begin{bmatrix} 0 & 17 & 23 & 14 \\ 15 & 1 & 1 & 24 \\ 19 & 13 & 3 & 17 \\ 17 & 24 & 7 & 13 \end{bmatrix}$	$ARXOPBBYTNDRRYHN$
C_2	$\left(A_7^{-1} \times C_3\right) = \begin{bmatrix} 11 & 19 & 23 & 17 \\ 8 & 12 & 20 & 18 \\ 4 & 2 & 11 & 2 \\ 20 & 8 & 20 & 13 \end{bmatrix}$	$LTXRIMUSECLCUIUN$
C_1	$\left(A_3^{-1} \times C_2\right) = \begin{bmatrix} 3 & 9 & 17 & 22 \\ 6 & 15 & 9 & 4 \\ 15 & 13 & 17 & 24 \\ 2 & 6 & 20 & 13 \end{bmatrix}$	$DJRWGPJEPNRYCGUN$
M	$\left(A_1^{-1} \times C_1\right) = \begin{bmatrix} 8 & 13 & 2 & 14 \\ 12 & 15 & 17 & 4 \\ 7 & 4 & 13 & 18 \\ 8 & 1 & 11 & 4 \end{bmatrix}$	$INCOMPREHENSIBLE$

Table 5 Sensitivity analysis of proposed algorithm

Message	*Phase*	*Key*	*Final ciphertext*
INCOMPREHENSIBLE	320°	59	*HBHNRKOGSRBTBEUE*
INCOMPREHENSIBLE	280°	59	*KHPEHHJIRVHJJSOK*
INCOMPREHENSIBLE	320°	63	*TCUKNRRTKMEYCGNG*
ELECTROMAGNETISM	150°	37	*OLDLEMZVNDVFDRPI*
ELECTROMAGNETISM	220°	37	*HUPFMCEMQNHLXGKT*

the cipher and it is not possible to retrieve the plaintext exactly. The reverse process of this scheme by knowing the key is not possible because phase θ has infinite points.

5 Conclusion

The efficiency of designed algorithm test on texts, by changing the phase only 0.010 lead to change the cipher. Both parties can do secure data transmission with limited key space in very short time and can encrypt/ decrypt data character by character in defined range of phases. The above results of plain texts have different ciphers clarified that by changing either key or phase to get different results. We can create million of ciphers by changing phases of one original plain text. In this paper, the algorithm refers symmetric cryptography. The described algorithm refers to half spinning, so the points in between $-720°$to$720°$ are infinite and possible combinations of rotation matrices are 24!. It is not possible for any machine to store infinite points in each of 24! matrices. All of these rotation matrices become the identity matrix for rotations through 720° and are minus the identity for rotations through 360°. The purpose of using FSM is to enhance the security.

Acknowledgments One of the authors Dr. Majid Khan is highly thankful to Vice Chancellor Engineer Imran Rahman, Institute of Space Technology, Islamabad Pakistan, for providing a decent atmosphere for research and development.

References

1. Wheeler, N.: Spin Matrices for Arbitrary Spin. Reed College Physics Department, Portland (2000)
2. Aditya, J., Shankar Rao, P.: Quantum cryptography, Proceedings of computer society of India (2005)
3. Man, P.P.: Wigner active and passive rotation matrices applied to NMR tensor. Concepts Magn. Reson. Part A **45A**(1), 26 (2017)
4. Zwiebach, B.: Spin one-half, bras, kets and operators, MIT Physics Department (2013)
5. Drakos, N., Moore, R.: Quantum Physics, Derive the expression for rotation operator (1996)
6. Drakos, N., Moore, R.: Quantum Physics Spin 1/2 and Derive Spin 1/2 rotation matrices and operators (1996)
7. Kumar, R., Sekhar, C.: An ElGamal encryption scheme of Pauli spin 1/2 matrices and finite machines. International Journal of Mechatronics Electrical and Computer Technology **5**(18), 2577–2584 (2015)
8. Rubya, T., Prema Latha, N., Sangeetha, B.: A survey on recent security trends using quantum cryptography. International Journal on Computer Science and Engineering **02**(09), 3038–3042 (2010)
9. Buchmann, J., Braun, J., Demirel, D., Geihs, M.: Quantum cryptography: a view from classical cryptography. Quantum Sci Technol. **2**, 1–4 (2017)
10. Lopes, M., Sarwade, N.: Cryptography from quantum mechanical viewpoint. International Journal on Cryptography and Information Security **4**(2), 13–25 (2014)