(T, N)-Threshold Quantum State Sharing Scheme Of An Arbitrary One-Qutrit Based On Linear Equation

Manoj Kumar, M. K. Gupta, Sudhanshu Shekhar Dubey, Ajay Kumar

Abstract : In the current research, quantum states sharing are very effective technique to increase the security of a highly sensitive information being transmitted among remote parties. The present work proposes a novel and efficient (t, n)-threshold quantum state sharing scheme which is developed on qutrits using linear equation. Since the proposed scheme has an increased probability of detecting an attacker during the transmission of secret information, therefore the proposed scheme is very efficient and enough secure against PNS attack, intercept and resend attack, and participant attack also that are the possible attacks on the proposed scheme.

Keywords: Quantum cryptography, Unitary transformation, Qutrits, Threshold quantum secret sharing, Linear equation, Quantum key distribution, Quantum state sharing.

1. INTRODUCTION

IN cryptography secret sharing is used to protect an information or a secret in a distributed way such that the echeloned parts called shares, are used to recover the original information. Furthermore the minimum number of shares that are used to recover the information is known as threshold. For example, if our information is a linear curve like straight line and five different points on this linear curve are known by five different persons (in fact no person know more than one point on the curve) then any two points or any two persons are enough to reconstruct the information (linear curve or straight line). Similarly, for quadratic curve information, minimum three points (on the quadratic curve like parabola) or three persons are enough to reconstruct the information (quadratic curve). In general $k+1$ points are enough to reconstruct information involving k degree polynomial curve. Thus k degree polynomial curve information has $k+1$ threshold. More precisely, a secret sharing schemes involves a distribution of a secret by a dealer among $n-$ members in such a way that some authorized members $(k \le n)$ can only cooperate to reconstruct the original secret and rest of the members $(n-k)$ do not know any information about the original secret. It plays a vital role in key distribution, secure multiparty communication etc. The concept of secret sharing was independently first proposed by Shamir [1] and Blakley [2].

Quantum cryptography is an important branch of secure communication which is based on classical Heisenberg's Uncertainty Principle of quantum physics. Motivated by the work of Shamir's [1], Hillery et al.[3] suggested secret sharing scheme based on quantum aspects to achieve the same goal as in the case of classical secret sharing. Quantum secret sharing (QSS) is a vital problem in cryptography and it has been studied extensively [3, 7, 8, 9, 10, 17, 18, 20]. Recently, Qin et al. [15] proposed multi-dimensional quantum state sharing scheme in which they have used quantum Fourier transform to encode a multi-dimensional quantum state into an entanglement state. Their proposed scheme has the virtue that it can be shared the multi-dimensional quantum state without any entanglement measurement. In the mean while Lu et al. [18] proposed threshold quantum secret sharing scheme based on unitary phase shift operation on single qubit. In this scheme they have used decoy photons to prevent eavesdropping. Very recently Chen et al. [19] studied quantum homomorphic encryption scheme which provides the ability to perform calculation on encrypted data without decryption. In this work, we have proposed a (t,n)-threshold quantum state sharing scheme of an arbitrary one – qutrit state based on linear equation. The present paper consists of the seven sections. Section-1 is introductory in nature and it consists of the brief literature review of previous research done on the quantum secret sharing scheme. In section-2, some preliminary results and mathematical background of qutrits are discussed. Section-3 consists of the proposed threshold quantum state sharing scheme of an arbitrary one qutrit state based on linear equation. In section-4 we gave a concrete illustration of the proposed scheme. We described the correctness of the proposed work in section-5 followed by the security analysis in section-6. Finally the last section concludes the present research work.

2. MATHEMATICAL BACKGROUND OF QUTRITS

In this section we shall study some basic definitions and preliminary results which are essential to understand the proposed scheme.

- *Manoj Kumar, Department of Mathematics and Statistics, Gurukul Kangri Vishwavidyalaya, Haridwar-249404(UK), INDIA*
- *Email id: sdmkg1@gmail.com*
- *M. K. Gupta, Department of Mathematics, Chaudhary Charan Singh University, Meerut-250004, INDIA email id: mkgupta2k2@gmail.com*
- *Sudhanshu Shekhar Dubey, Department of Mathematics and Statistics, Gurukul Kangri Vishwavidyalaya, Haridwar-249404(UK), INDIA Email id: sudhanshusdubey@gmail.com*
- *Ajay Kumar, Defence Scientific Information & Documentation, Defence Research & Development Organization, Delhi-110054, INDIA Email id: ajaydesidoc@gmail.com*

2.1 Qutrit: In 2000 Bechmann-Pasquinucci and Peres [21] proposed quantum key distribution (QKD) scheme for three state systems, the so-called qutrits. Infact a qutrit $|\phi\rangle$ can be represented as

$$|\phi\rangle = \alpha\ |0\rangle + \beta\ |1\rangle + \gamma\ |2\rangle \qquad (2.1)$$

where the complex amplitudes α, β, γ of $|\phi\rangle$ satisfy the equality relation

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$$

Here the three states $|0\rangle$, $|1\rangle$, $|2\rangle$ are the orthonormal to each other and constitute the computational bases. A qutrit based QKD systems have the following four mutually unbiased bases.

Basis-1: It is taken as

$$\left.\begin{matrix} |0\rangle \\ |1\rangle \\ |2\rangle \end{matrix}\right\} \qquad (2.2)$$

Basis-2: It can be taken as

$$\left.\begin{aligned} |u\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + |2\rangle\right) \\ |v\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + e^{\frac{2\pi i}{3}}|1\rangle + e^{\frac{4\pi i}{3}}|2\rangle\right) \\ |w\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + e^{\frac{4\pi i}{3}}|1\rangle + e^{\frac{2\pi i}{3}}|2\rangle\right) \end{aligned}\right\} \qquad (2.3)$$

Basis 3: In consists of the following qutrits

$$\left.\begin{aligned} |u'\rangle &= \frac{1}{\sqrt{3}}\left(e^{\frac{2\pi i}{3}}|0\rangle + |1\rangle + |2\rangle\right) \\ |v'\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + e^{\frac{2\pi i}{3}}|1\rangle + |2\rangle\right) \\ |w'\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + e^{\frac{2\pi i}{3}}|2\rangle\right) \end{aligned}\right\} \qquad (2.4)$$

Basis 4: It has the following qutrits

$$\left.\begin{aligned} |u''\rangle &= \frac{1}{\sqrt{3}}\left(e^{\frac{4\pi i}{3}}|0\rangle + |1\rangle + |2\rangle\right) \\ |v''\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + e^{\frac{4\pi i}{3}}|1\rangle + |2\rangle\right) \\ |w''\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + e^{\frac{4\pi i}{3}}|2\rangle\right) \end{aligned}\right\} \qquad (2.5)$$

The sender randomly selects some of the above twelve states and sends them to the receiver after performing an unitary transformation on them.

2.2 Sequence of qutrits : A qutrit sequence denoted by $\{|\phi_k\rangle\}$ is defined as

$$\{|\phi_k\rangle = \alpha_k|0\rangle + \beta_k|1\rangle + \gamma_k|2\rangle\} \qquad (2.6)$$

where $|\alpha_k|^2 + |\beta_k|^2 + |\gamma_k|^2 = 1$ and $k = 1, 2, 3, \ldots, m$.

2.3 Unitary transformation for qutrits : Unitary transformation for one-qutrit state, denoted by $U(\theta)$, is defined as a 3×3 order matrix of the form

$$U(\theta) = \begin{bmatrix} \cos\theta & 0 & -\sin\theta \\ 0 & 1 & 0 \\ \sin\theta & 0 & \cos\theta \end{bmatrix}_{3\times 3} \qquad (2.7)$$

Lemma 2.3.1: If $\theta_1, \theta_2, \ldots, \theta_n \in F$ and $U(\theta)$ is an unitary transformation then for any qutrit $|\phi_k\rangle$, we have

$$U(\theta_1)\cdot U(\theta_2)\cdot \ldots \cdot U(\theta_n)\,|\phi_k\rangle = U(\theta_1 + \theta_2 + \ldots + \theta_n)\,|\phi_k\rangle \ .$$

Proof. First we shall prove the result for θ_1 and θ_2
For this, we have

$$U(\theta_1)\cdot U(\theta_2)|\phi_k\rangle$$

$$= \begin{bmatrix} \cos\theta_1 & 0 & -\sin\theta_1 \\ 0 & 1 & 0 \\ \sin\theta_1 & 0 & \cos\theta_1 \end{bmatrix} \begin{bmatrix} \cos\theta_2 & 0 & -\sin\theta_2 \\ 0 & 1 & 0 \\ \sin\theta_2 & 0 & \cos\theta_2 \end{bmatrix} |\phi_k\rangle$$

$$= \begin{bmatrix} \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 & 0 & -\cos\theta_1\sin\theta_2 - \sin\theta_1\cos\theta_2 \\ 0 & 1 & 0 \\ \sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2 & 0 & -\sin\theta_1\sin\theta_2 + \cos\theta_1\cos\theta_2 \end{bmatrix} |\phi_k\rangle$$

$$= \begin{bmatrix} \cos(\theta_1+\theta_2) & 0 & -\sin(\theta_1+\theta_2) \\ 0 & 1 & 0 \\ \sin(\theta_1+\theta_2) & 0 & \cos(\theta_1+\theta_2) \end{bmatrix} |\phi_k\rangle$$

$$= U(\theta_1 + \theta_2)\,|\phi_k\rangle$$

This shows that result is true for θ_1 and θ_2 .
In a similar manner the result can be generalized for $n-$ variables $\theta_1, \theta_2, \theta_3, \theta_4, \ldots, \theta_n$.

3. PROPOSED SCHEME

Suppose $t-$ members say $Mem_{i_1}, Mem_{i_2}, Mem_{i_3}, \ldots, Mem_{i_t}$ $(with\ \ 1 \le i_1 \le i_2 \le i_3 \le \ldots \le i_t \le n)$ out of $n-$ members $Mem_1, Mem_2, Mem_3, \ldots, Mem_n$ request a dealer (which has a qutrit based information $\{|\phi_k\rangle : 1 \le k \le m\}$,
where $|\phi_k\rangle$ is a qutrit as defined in (2.6)) to reconstruct the initial original information $\{|\phi_k\rangle : 1 \le k \le m\}$.

Now to reconstruct the initial original information by $t-$ members, our proposed scheme consists of the following two phases:

3.1 Private Keys Generation Phase

In this phase, dealer generates private keys for each member including itself and then send them to corresponding members. This phase consists of the following steps:

Step 1: Dealer chooses an infinite field F (over the set of real numbers or rational numbers or complex numbers) and generates his/her private key P by randomly choosing $n-$ non zero elements $a_1, a_2, a_3, ..., a_n$ in the field F i.e.

$$P = \{ a_i : 0 \neq a_i \in F \text{ and } 1 \leq i \leq n \}$$

Step 2: For every subset $\{a_{i_1}, a_{i_2}, \dots, a_{i_t}\}$ of P with $1 \leq i_1 \leq i_2 \leq i_3 \leq \dots \leq i_t \leq n$, dealer constructs a $t-$ variable linear equation as:

$$a_{i_1} x_{i_1} + a_{i_2} x_{i_2} + a_{i_3} x_{i_3} + \dots + a_{i_t} x_{i_t} = 1 \qquad (3.1)$$

Step 3: Now dealer determines a solution

$$X_{i_1 i_2 i_3 \dots i_t} = \left(x_{s(i_1)}, x_{s(i_2)}, x_{s(i_3)}, ..., x_{s(i_t)}\right) \qquad (3.2)$$

where $x_{s(i_r)} \neq 0$ for $1 \leq r \leq t$

and $s(i_r) = i_r i_1 i_2 \dots i_{r-1} i_{r+1} i_{r+2} \dots i_t$.

Step 4: Again dealer randomly picks an element $\lambda \neq 0$ in F to yield the private keys P_i $(1 \leq i \leq s)$ of the members as

$$P_i = \left\{ \lambda\, a_i\, x_{i r_1 r_2 \dots r_{t-1}} : i \neq r_1, r_2, ..., r_{t-1} \text{ and } 1 \leq r_1 \leq r_2 \leq r_3 \leq \dots \leq r_{t-1} \leq n \right\}$$

Step 5: Finally dealer transmits P_i to Mem_i through direct quantum secure communication method as described in [22, 24].

3.2 Information Reconstruction Phase

This phase consists of $t-$ loops of which first two loops are explained in details. Rests of the loops are similar to the loop-2.

Loop 1: This loop involving dealer and Mem_{i_1}, consists of the following steps:

1. Dealer applies unitary transformation $U(\theta^{(0)})$ on every element of qutrit sequence $\{|\phi_k\rangle\}$ to get a new transformed qutrit sequence $\left\{ \left|\phi_k^0\right\rangle \equiv U(\theta^{(0)}) |\phi_k\rangle \right\}$, where $\theta^{(0)} = 2\pi - \lambda$ and $U(\theta)$ is an unitary transformation as defined by (2.7) in section-2.
2. Next dealer adds the some decoy qutrits(randomly picked from the bases (2.2) to (2.5) into the sequence $\left\{ \left|\phi_k^0\right\rangle \right\}$ to get a new sequence $\left\{ \left|\psi_k^0\right\rangle \right\}$ involving decoy qutrits.
3. After noting the place of every decoy qutrit, dealer sends the sequence $\left\{ \left|\psi_k^0\right\rangle \right\}$ to Mem_{i_1}.
4. After the Mem_{i_1}'s corroboration of accepting the qutrit sequence $\left\{ \left|\psi_k^0\right\rangle \right\}$, dealer divulged the places and related measuring bases (2.2) to (2.5) of the decoy qutrits.
5. After estimating decoy qutrits of $\left\{ \left|\psi_k^0\right\rangle \right\}$ in related bases (2.2) to (2.5), Mem_{i_1} publicizes his/her estimated results.
6. Dealer measures the error probability by juxtaposing the estimated results of Mem_{i_1} with the qutrit sequence $\left\{ \left|\phi_k^0\right\rangle \right\}$.
7. If the error ratio is smaller than the threshold value then dealer divulged that the process is completed securely, otherwise dealer requests Mem_{i_1} to give up the sequence $\left\{ \left|\psi_k^0\right\rangle \right\}$ and initiates a new qutrit sequence.
8. After securely received sequence $\left\{ \left|\psi_k^0\right\rangle \right\}$, Mem_{i_1} isolates the decoy qutrits from it to get the initial transformed sequence $\left\{ \left|\phi_k^0\right\rangle \right\}$.

Loop 2: This loop involving Mem_{i_1} and Mem_{i_2}, consists of the following steps:

1. Mem_{i_1} applies unitary transformation $U(\theta^{(1)})$ on every element of qutrit sequence $\left\{ \left|\phi_k^0\right\rangle \right\}$ to get a new transformed qutrit sequence $\left\{ \left|\phi_k^1\right\rangle \equiv U(\theta^{(1)}) \left|\phi_k^0\right\rangle \right\}$ where $\theta^{(1)} = \lambda \cdot a_{i_1} x_{i_1 i_2 \dots i_t}$ is chosen by Mem_{i_1} from his/her private key P_{i_1}.
2. Next Mem_{i_1} adds the some decoy qutrits(randomly picked from the bases (2.2) to (2.5) into the sequence $\left\{ \left|\phi_k^1\right\rangle \right\}$ to get a new sequence $\left\{ \left|\psi_k^1\right\rangle \right\}$ involving decoy qutrits.
3. After noting the place of every decoy qutrit, dealer sends the sequence $\left\{ \left|\psi_k^1\right\rangle \right\}$ to Mem_{i_2}.
4. After the Mem_{i_2}'s corroboration of accepting the qutrit sequence $\left\{ \left|\psi_k^1\right\rangle \right\}$, Mem_{i_1} divulged the places and related measuring bases (2.2) to (2.5) of the decoy qutrits.
5. After estimating decoy qutrits of $\left\{ \left|\psi_k^1\right\rangle \right\}$ in related bases (2.2) to (2.5), Mem_{i_2} publicizes his/her estimated results.
6. Mem_{i_1} measure the error probability by juxtaposing the estimated results of Mem_{i_2} with the qutrit sequence $\left\{ \left|\phi_k^1\right\rangle \right\}$.
7. If the error ratio is smaller than the threshold value then Mem_{i_1} divulged that the process is completed securely, otherwise Mem_{i_1} requests Mem_{i_2} to give up the sequence $\left\{ \left|\psi_k^1\right\rangle \right\}$ and initiates a new qutrit sequence.
8. After securely received sequence $\left\{ \left|\psi_k^1\right\rangle \right\}$, Mem_{i_2} removes the decoy qutrits from it to get the initial transformed sequence $\left\{ \left|\phi_k^1\right\rangle \right\}$.

Loop 3: This loop involves Mem_{i_2} and Mem_{i_3}, and so on the other loops. The last $t-$ loop involves $Mem_{i_{t-1}}$ and Mem_{i_t}. In this

$t-$ loop, after securely received $\left\{\left|\psi_k^{t-1}\right\rangle\right\}$, Mem_{i_t} removes the decoy qutrits from it and obtained the transformed sequence $\left\{\left|\phi_k^{t-1}\right\rangle\right\}$.

Finally, after choosing $\theta^{(t)} = \lambda \cdot a_{i_t} x_{i_t i_1 i_2 \dots i_{t-1}}$ from his/her private key P_{i_t}, Mem_{i_t} can reconstruct the initial qutrit sequence $\{|\phi_k\rangle\}$ by applying the unitary transformation $U(\theta^{(t)})$ on every qutrit of the sequence $\left\{\left|\phi_k^{t-1}\right\rangle\right\}$ i.e.

$$|\phi_k\rangle = U(\theta^{(t)})\left|\phi_k^{t-1}\right\rangle.$$

4. CORRECTNESS OF THE PROPOSED SCHEME

We have claimed at the end of the reconstruction phase in previous section that the initial qutrit sequence $\{|\phi_k\rangle\}$ can be reconstructed by applying the unitary transform $U(\theta^{(t)})$ on $\left\{\left|\phi_k^{t-1}\right\rangle\right\}$ i.e.

$$|\phi_k\rangle = U(\theta^{(t)})\left|\phi_k^{t-1}\right\rangle \qquad (4.1)$$

Here we shall prove our above assertion (4.1) as follows:

Since $X_{i_1 i_2 \dots i_t} = \left(x_{i_1 i_2 \dots i_t}, x_{i_2 i_1 i_3 \dots i_t}, \dots, x_{i_t i_1 i_2 \dots i_{t-1}}\right)$ is a solution of the linear equation (3.1), therefore we have

$$a_{i_1} x_{i_1 i_2 \dots i_t} + a_{i_2} x_{i_2 i_1 i_3 \dots i_t} + \dots + a_{i_t} x_{i_t i_1 i_2 \dots i_{t-1}} = 1 \qquad (4.2)$$

Also the transformed qutrit sequences obtained in the successive loops of reconstruction phase are respectively given by

$$\left|\phi_k^0\right\rangle = U(\theta^{(0)})|\phi_k\rangle \qquad \text{(in loop-1)}$$

$$\left|\phi_k^1\right\rangle = U(\theta^{(1)})|\phi_k\rangle \qquad \text{(in loop-2)}$$

$$\dots$$

$$\dots$$

$$\left|\phi_k^{t-1}\right\rangle = U(\theta^{(t-1)})\left|\phi_k^{t-2}\right\rangle \qquad \text{(in loop-t)}$$

Using the above relations, Lemma 2.3.1 together with the right hand side of (4.1), we obtained

$$U(\theta^{(t)})\left|\phi_k^{(t-1)}\right\rangle \quad |\phi_k\rangle$$

$$= U(\theta^{(t)})U(\theta^{(t-1)})\dots U(\theta^{(1)})U(\theta^{(0)})\,|\phi_k\rangle$$

$$= U(\theta^{(t)} + \theta^{(t-1)} + \dots + \theta^{(1)} + \theta^{(0)})\,|\phi_k\rangle$$

(Using Lemma 2.3.1)

$$= U\big(\lambda \cdot a_{i_t} x_{i_t i_1 \dots i_{t-1}} + \lambda \cdot a_{i_{t-1}} x_{i_{t-1} i_1 \dots i_{t-2} i_t} + \dots$$

$$+ \lambda \cdot a_{i_1} x_{i_1 i_2 \dots i_t} + (2\pi - \lambda)\big)|\phi_k\rangle$$

$$= U\big(\lambda[\,a_{i_t} x_{i_t i_1 \dots i_{t-1}} + a_{i_{t-1}} x_{i_{t-1} i_1 \dots i_{t-2} i_t} + \dots$$

$$+ a_{i_1} x_{i_1 i_2 \dots i_t}\,] + [\,2\pi - \lambda\,]\big)|\phi_k\rangle$$

$$= U(\lambda + (2\pi - \lambda))\,|\phi_k\rangle \qquad \text{(Using (4.1))}$$

$$= U(2\pi)\,|\phi_k\rangle$$

$$= \begin{bmatrix} \cos 2\pi & 0 & -\sin 2\pi \\ 0 & 1 & 0 \\ \sin 2\pi & 0 & \cos 2\pi \end{bmatrix} |\phi_k\rangle$$

$$= I_{3\times 3}\,|\phi_k\rangle$$

$$= |\phi_k\rangle$$

where $I_{3\times 3}$ is an identity matrix of order 3×3.

This proves the correctness of our proposed scheme.

5. A CONCRETE ILLUSTRATION OF THE PROPOSED SCHEME

In this section we have illustrated a concrete example in support to our proposed scheme.

Suppose a $(3,5)$-threshold quantum state sharing scheme is implemented over the field F of complex numbers.

Here we have taken $t = 3$ and $n = 5$.

Phase-1: Private Key Generation Phase

This phase is accomplished in the following steps:

1. Dealer randomly picks $a_1 = 2$, $a_2 = 4$, $a_3 = 5$, $a_4 = 8$ and $a_5 = 10$ to yield his/her private key $P = \{a_1, a_2, a_3, a_4, a_5\}$.

2. For every subset $\{a_{i_1}, a_{i_2}, a_{i_3}\}$ of P with $1 \le i_1 \le i_2 \le i_3 \le 5$, dealer constructs a 3-variable linear equation as:

$$a_{i_1} x_{i_1} + a_{i_2} x_{i_2} + a_{i_3} x_{i_3} = 1 \qquad (5.1)$$

3. Now dealer determines a solution of the above equation (5.1) as

$$X_{i_1 i_2 i_3} = \left(x_{s(i_1)}, x_{s(i_2)}, x_{s(i_3)}\right)$$

where $x_{s(i_r)} \neq 0$ for $r = 1, 2, 3$ and

$$s(i_r) = i_r i_1 i_2 \dots i_{r-1} i_{r+1} i_{r+2} \dots i_3.$$

For $i_1 = 1, i_2 = 2, i_3 = 4$, dealer determines

$$X_{124} = (x_{124}, x_{214}, x_{412}) = \left(1 - i, 2i, \frac{-1 - 6i}{8}\right).$$

For $i_1 = 1, i_2 = 2, i_3 = 5$, dealer determines

$$X_{125} = (x_{125}, x_{215}, x_{512}) = \left(1 - 3i, 1 + i, \frac{-5 + 2i}{10}\right).$$

For $i_1 = 1, i_2 = 3, i_3 = 4$, dealer determines

$$X_{134} = (x_{134}, x_{314}, x3) = \left(\frac{1 - 29i}{2}, i, 3i\right).$$

For $i_1 = 1, i_2 = 3, i_3 = 5$, dealer determines

$$X_{135} = (x_{135}, x_{315}, x_{513}) = \left(1-5i, 1-2i, \frac{-3-2i}{5}\right).$$

For $i_1 = 1, i_2 = 4, i_3 = 5$, dealer determines

$$X_{145} = (x_{145}, x_{415}, x_{514}) = \left(2i, \frac{-9-34i}{8}, 1+3i\right).$$

For $i_1 = 2, i_2 = 3, i_3 = 4$, dealer determines

$$X_{234} = (x_{234}, x_{324}, x_{423}) = \left(-3i, 2-i, \frac{-9+17i}{8}\right).$$

For $i_1 = 1, i_2 = 4, i_3 = 5$, dealer determines

$$X_{145} = (x_{145}, x_{415}, x_{514}) = \left(2i, \frac{-9-34i}{8}, 1+3i\right).$$

For $i_1 = 2, i_2 = 3, i_3 = 4$, dealer determines

$$X_{234} = (x_{234}, x_{324}, x_{423}) = \left(-3i, 2-i, \frac{-9+17i}{8}\right).$$

For $i_1 = 2, i_2 = 3, i_3 = 5$, dealer determines

$$X_{235} = (x_{235}, x_{325}, x_{523}) = \left(\frac{-9-55i}{4}, 2-i, -5i\right).$$

For $i_1 = 2, i_2 = 4, i_3 = 5$, dealer determines

$$X_{245} = (x_{245}, x_{425}, x_{524}) = \left(2-i, 1+i, \frac{-15-4i}{10}\right).$$

For $i_1 = 3, i_2 = 4, i_3 = 5$, dealer determines

$$X_{345} = (x_{345}, x_{435}, x_{534}) = \left(\frac{1+52i}{5}, i, -6i\right)$$

4. Again dealer randomly picks an element $\lambda = 1+2i$ in F to yield the private keys P_i, $(1 \le i \le 5)$ of the five members as

$$P_i = \left\{\lambda\, a_i\, x_{ir_1r_2} : i \ne r_1, r_2 \text{ and } 1 \le r_1 \le r_2 \le 5\right\} \quad \text{i.e.}$$

$$P_1 = \{\lambda a_1 x_{123}, \lambda a_1 x_{124}, \lambda a_1 x_{125}, \lambda a_1 x_{134}, \lambda a_1 x_{135}, \lambda a_1 x_{145}\}$$

$$= \{-4+2i, 6+2i, 14-2i, 59-27i, -18+14i, -8+4i\}$$

$$P_2 = \{\lambda a_2 x_{213}, \lambda a_2 x_{214}, \lambda a_2 x_{215}, \lambda a_2 x_{234}, \lambda a_2 x_{235}, \lambda a_2 x_{245}\}$$

$$= \{-8+4i, -16, -4+12i, 24-12i, 101-73i, 16+12i\}$$

$$P_3 = \{\lambda a_3 x_{312}, \lambda a_3 x_{314}, \lambda a_3 x_{315}, \lambda a_3 x_{324}, \lambda a_3 x_{325}, \lambda a_3 x_{345}\}$$

$$= \{13-4i, -4+5i, 25, 20+15i, 20+15i, -103+54i\}$$

$$P_4 = \{\lambda a_4 x_{412}, \lambda a_4 x_{413}, \lambda a_4 x_{415}, \lambda a_4 x_{423}, \lambda a_4 x_{425}, \lambda a_4 x_{435}\}$$

$$= \{11-8i, -48+24i, 59-52i, -43-i, -8+24i, -16+8i\}$$

$$P_5 = \{\lambda a_5 x_{512}, \lambda a_5 x_{513}, \lambda a_5 x_{514}, \lambda a_5 x_{523}, \lambda a_5 x_{524}, \lambda a_5 x_{534}\}$$

$$= \{-9-8i, -6-12i, -50+50i, 100-50i, -7-34i, 120-60i\}$$

5. Finally dealer respectively transmits P_1, P_2, P_3, P_4, P_5 to Mem_1 , Mem_2 , Mem_3 , Mem_4 , Mem_5 through direct quantum secure communication method as described in [22,24].

Phase-2: Information Reconstruction Phase

Now suppose three members Mem_2 , Mem_4 and Mem_5 request dealer to reconstruct the initial qutrit based sequence $\{|\phi_k\rangle\}$. Then, from their private keys P and P_2, P_4, P_5 , dealer and three members respectively pick $\theta^{(0)}$ and $\theta^{(2)}$, $\theta^{(4)}$, $\theta^{(5)}$ as

$\theta^{(0)} = 2\pi - (1+2i)$ and $\theta^{(2)} = \lambda a_2 x_{245} = 16+12i$,

$\theta^{(4)} = \lambda a_4 X_{425} = -8+24i$, $\theta^{(5)} = \lambda a_5 X_{524} = -7-34i$.

Finally, dealer and three members Mem_2 , Mem_4 and Mem_5 respectively use unitary transform $U(\theta^{(0)})$ and $U(\theta^{(2)})$, $U(\theta^{(4)})$, $U(\theta^{(5)})$ to rebuild the $|\phi_k\rangle$ as

$$U(\theta^{(5)})U(\theta^{(4)})U(\theta^{(2)})U(\theta^{(0)})|\phi_k\rangle = U(\theta^{(5)}+\theta^{(4)}+\theta^{(2)}+\theta^{(0)})|\phi_k\rangle$$

$$= U((-7-34i)+(-8+24i)+(16+12i)+[2\pi-(1+2i)])|\phi_k\rangle$$

$$= U(2\pi)|\phi_k\rangle$$

$$= \begin{bmatrix} \cos 2\pi & 0 & -\sin 2\pi \\ 0 & 1 & 0 \\ \sin 2\pi & 0 & \cos 2\pi \end{bmatrix}|\phi_k\rangle$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}|\phi_k\rangle$$

$$= |\phi_k\rangle$$

6. SECURITY ANALYSIS

In this section we will study the security of our proposed scheme which may involve the following possible attacks as under described.

6.1 Intercept-and-resend attack: If an attacker intercepts some qutrits sent by dealer or any other member Mem_i and resends an altered sequence $\left\{\left|\psi_k^{\,i}\right\rangle\right\}$ with forged qutrits to any other member Mem_j or dealer, then the attacker definitely cause some mistakes owing to his/her full ignorance of the places, measuring bases and estimated results of the decoy qutrits, because the inserted decoy qutrits of the authorized sequence $\left\{\left|\psi_k^{\,i}\right\rangle\right\}$ are randomly picked from the bases (2.2) to (2.5). Since the probability of an attacker selects the incorrect basis from the four mutually unbiased bases $\{|0\rangle, |1\rangle, |2\rangle\}$, $\{|u\rangle, |v\rangle, |w\rangle\}$, $\{|u'\rangle, |v'\rangle, |w'\rangle\}$ and $\{|u''\rangle, |v''\rangle, |w''\rangle\}$ is $75\,\%$, therefore the probability an intercepted photon yields an error in the key string is $75\,\% \times 75\,\% = \frac{9}{16}$. In this case attacker will be exposed with the probability $1-\left(\frac{7}{16}\right)^m$ which will converge to 1 when transmitted sequence $\left\{\left|\psi_k^{\,i}\right\rangle\right\}$ involves a sufficiently large number of qutrits. This shows that our proposed scheme is secure against intercept-and-resend attack. It is evident that the detected probability $1-\left(\frac{7}{16}\right)^m$, of an attacker, converges to

1 more rapidly than the detected probability $1-\left(\frac{3}{4}\right)^m$, of an attacker, in case of qubits. This implies that an attacker in our proposed scheme will be detected more rapidly than the existing scheme in literature.

6.2 Photon number splitting (PNS) attack: In practice most of the implementors use very low level laser pulses to send the quantum states. Actually these laser pulses endue a very small number of photons which are distributed in a Poisson fashion. In fact, most laser pulses spilt no photons; some laser pulses endue a single photon and a few laser pulses spilt more than one photons. In the case, laser pulses spilt more than one photons, an attacker can gather the extra photons and send the remnant single photon to the receiver. This causes the photon number splitting (PNS) attack. Generally, attacker collects these extra photons in a quantum memory until the receiver discovers the rest single photon and the sender divulges the measuring bases $\{|0\rangle,|1\rangle,|2\rangle\}$, $\{|u\rangle,|v\rangle,|w\rangle\}$, $\{|u'\rangle,|v'\rangle,|w'\rangle\}$ and $\{|u''\rangle,|v''\rangle,|w''\rangle\}$. In the meantime, attacker can estimate his/her qutrits in the accurate basis and procured secret information without preluding detectable errors. As we have discussed in previous intercept and resend attack that the attacker detecting probability $1-\left(\frac{7}{16}\right)^m$ of the proposed scheme, more rapidly converges to 1, it means our proposed scheme has very negligible probability for PNS attack. Furthermore, PNS attack can also be interdicted for the proposed scheme if the scheme implementors use the security methods introduced in [25].

6.3 Participants attack: It is well known that a quantum secret sharing scheme is secure against any outside attacker if it is secure against a dishonest participant. Further, a dishonest participant can intercept other participant's particles to transmit forged particles and pilfer the secret information through measuring the aider particles. As discussed above, it is evident from the intercept and resend attack, and PNS attack that neither outside eavesdropper nor dishonest participant can filch the secret information from the transmitted particles because the transmitted particles in our proposed quantum state sharing scheme are conserved by the decoy qutrits which are randomly picked from the four mutually unbiased bases $\{|0\rangle,|1\rangle,|2\rangle\}$, $\{|u\rangle,|v\rangle,|w\rangle\}$, $\{|u'\rangle,|v'\rangle,|w'\rangle\}$ and $\{|u''\rangle,|v''\rangle,|w''\rangle\}$. This implies that the dishonest participant has a very negligible probability of stealing the secret information. Thus proposed scheme is more secure against participants attack also.

7. CONCLUSION

Security analysis of the proposed qutrit state sharing scheme shows that the probability expression $1-\left(\frac{7}{16}\right)^m$ of detecting an attacker, more rapidly converges to 1 for sufficiently large value of m. This is due to the four mutually unbiased bases $\{|0\rangle,|1\rangle,|2\rangle\}$, $\{|u\rangle,|v\rangle,|w\rangle\}$, $\{|u'\rangle,|v'\rangle,|w'\rangle\}$ and $\{|u''\rangle,|v''\rangle,|w''\rangle\}$ endow less opportunity for an attacker to make forgery on transmitted particles during quantum state sharing phase. It means our proposed scheme can give much perfect security compare to existing schemes. Furthermore, proposed scheme is efficient and enough secure against PNS attack, intercept and resend attack, and participant attack also that are the possible attacks on the proposed (t,n)-threshold quantum state sharing scheme. Proposed schemes may be ideal for storing information that are highly sensitive and highly important viz. encryption keys, missile launch codes and numbered bank accounts. The proposed (t,n)-threshold quantum state sharing scheme may be profitable in cloud computing environments where key is distributed over many servers by threshold secret sharing mechanism. The key is then reconstructed when needed. The proposed scheme may also be suggested for sensor networks where the links are liable to be tapped by sending the data in shares which makes the task of the attacker harder. The security in such environments can be made greater by continuous changing of the way the shares are constructed.

REFERENCES

[1] A. Shamir, "How to share a secret," Communication of the ACM, vol. 22, no. 11, 612-613, 1979.

[2] G. R. Blakley, "Safeguardimng cryptographic keys," In Proc. Of AFIPS National Computer conference, New York, 48, 313-317, 1979.

[3] M. Hillery, V. Buzek and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A, vol. 59, no. 3, 1999.

[4] L. Pang and Y. Wang, A new $(t,n)-$ multi secret sharing scheme based on Shamir"s secret sharing, Applied mathematics and computation, vol. 167, no. 2, 840-848, 2005.

[5] F. Deng, X. Li, C Li., P. Zhou and H.Y. Zhou, "Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pair," Phys. Rev. A, vol. 72, no. 4, 2005.

[6] F. Deng, X. Li, C. Li, P. Zhou and H.Y. Zhou, "Quantum state sharing of an arbitrary two-qubit state with two photon entanglement and Bell-state measurements," Eur. Physical J.D., Atomic , Mol., Opt. Plasma Phys., vol. 39, no. 3, 459-464, 2006.

[7] L. Han, Y. Liu, H. Yuan, and Z. Zhang, "Efficient multiparty-to-multiparty quantum secret sharing via continuous variable operations," Chin. Phys. Lett., vol. 24, no. 12, 3312-3315, 2007.

[8] T. Gao, F.L. Yan and Y.C. Li, "Quantum secret sharing between m-party and n-party with six states," Sci. China G, Phys., Mech. Astron., vol. 52, no. 8, 1191-1202, 2009.

[9] W. Wang and H. Cao, "An improvement multiparty quantum secret sharing with Bell states and Bell measurement," Int. J. Theor. Phys., vol. 52, no. 6, 2099-2011, 2013.

[10] C. Liao, C. Yang and T. Hwang, "Dynamic quantum secret sharing scheme based on GHZ state," Quantum Inf. Process., vol. 13, no. 8, 1907-1916, 2014.

[11] H. Qin and Y. Dal, "d- dimensional quantum state sharing with adversary structure," Quantum Inf. Process., vol. 15, no. 4, 1689-1701, 2016.[12] Y.G. Yang, Y.W. Teng, H.P. Chai and Q.Y. Wen, "Verifiable quantum $(k,n)-$ threshold secret key sharing," Int. J. Theor. Phys., vol. 50, no. 3, 792-798, 2011.

[12] Y.G. Yang, X. Jia, H.Y. Wang and H. Zhang, "Verifiable quantum $(k,n)-$ threshold secret sharing," Quantum Inf. Process, vol. 11, no. 6, 1619-1625, 2012.[14] J.Y. Peng, M. Bai and Z.W. Mo, "Biderectional quantum states sharing," Int. J. Theor. Phys., vol. 55, no. 5, 2481-2489, 2016.
[13] H. Qin, R. Tso, Y. Dai, "Multi-dimensional quantum state sharing based on quantum Fourier transform," Quantum Inf. Process., vol. 17, no. 48, 2018.
[14] A. Shamsoshoara, "Overview of Blakley secret sharing scheme," 2019. https://arxiv.org/pdf/1901.02802.pdf
[15] H. Qin, X. Zhu and Y. Dai, "$(t,n)-$ Threshold quantum secret sharing using the phase shift operation," Quantum Inf. Process., vol. 14, no. 8, 2997-3004, 2015.
[16] C. Lu, F. Miao, K. Meng, "Threshold quantum secret sharing based on single qubit," Quantum Inf. Process, vol. 17, no. 64, 1-13, 2018.
[17] X.- B. Chen, Y. - R. Sun, G. Xu, Y.- X. Yan, "Quantum homomorphic encryption scheme with flexible number of evaluator based $(k,n)-$ threshold quantum state sharing," Information Sciences, 501, 172-181, 2019.
[18] M. Kumar, "A verifiable threshold quantum secret sharing scheme using interpolation method," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 7, 42-47, 2017.
[19] H. Bechmann-Pasquinucci and A. Peres, "Quantum cryptography with $3-$ state systems," Physical Review Letters 85, 3313, 2000.
[20] F. G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," Phys. Rev. A, vol. 69, no. 5, 2004.
[21] D. Costa, N.G. De Almeida and C.J. Villas-Boas, "Secure quantum communication using classical correlated channel," Quantum Inf. Process., vol. 15, no. 10, 4303-4311, 2016.
[22] S. Mi, T. Wang, G. Jin and C. Wang, "High capacity quantum secure direct communication with orbital angular momentum of photons," IEEE Photon. J., vol. 7, no. 5, 2015.
[23] D. Gottesman, H-K Lo , N Lutekenhaus and J. Preskill, "Security of quantum key distribution with imperfect diveces," Quantum Information and Computation, vol. 4, no. 5, 325-360, 2004.