Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

SHARING OF INFORMATION USING BI-QUTRIT QUANTUM STATES BASED ON BIVARIATE QUANTUM GATES

HARDEEP[1], MANOJ KUMAR[1] and R.K. MISHRA[2]

[1]Department of Mathematics and Statistics, Gurukula Kangri(Deemed to be University), Haridwar (UK), India. Email: hardeeppawariya1994@gmail.com | sdmkg1@gmail.com
[2]Department of Applied Science, G. L. Bajaj Institute of Technology and Management, Greater Noida (Uttar Pradesh), India. Email: rk.mishra@glbitm.org

ABSTRACT:

It is well known that a qubit is a superposition of two orthogonal quantum states while, a qutrit is a superposition of three mutually orthogonal quantum states. It means qutrit is more advantageous than qubit, in carrying information via. quantum based devices. Beside it, higher dimensional quantum states offer many other benefits like increased security, large channel capacity for communication, more efficient quantum operations etc. More generally, qubits in higher dimensions provide intensive in sights in perspective of quantum correlations. Specifically, qutrits are of great importance in quantum information science. Qubits manipulation and controlling were demandable job at first but presently they are commonly used in quantum usage. Now a days it is become more enthralling to study qubit information in higher dimension Hilbert spaces, by raising number of qubits or by increasing the dimension of quantum systems. The present work proposes the sharing of information using bi-qutrit quantum states based on bivariate quantum gates.

Keywords: Quantum Cryptography, Threshold Quantum Secret Sharing, Lagrange Interpolation, Bivariate Operator

1. INTRODUCTION

A scheme in which a secret is distributed into pieces so that each member consists of its own unique piece is called a secret sharing scheme (SSS). SSS is an essential idea of securing information. SS schemes are supreme for hiding secret that is very sensitive and highly important. For example, missile launch codes and joint checking accounts. Here is a complete scenario for joint checking account example. Suppose seven persons want to open a joint checking account. Now, the bank aims to hide all the information of that account for which the bank generates a secret password. For the security of this account, the bank distributes that password among all seven persons so that no less than five persons can access that joint account. This scheme is called (5, 7)-threshold SSS, where 5 is a threshold value. In general, in (t, n)-threshold SSS, the dealer divides the secret into n pieces and allocates them into n participants. Then, any t or more participants can recover the secret, but less than t participants have no information about the secret.

SS plays an important role in preventing secret information from being stolen, erased, or modified. As a result, SS is often used in threshold authentication[1, 2], quantum SS(QSS) protocols [3]-[10], etc. Since 1979, researchers have been studying SSS. Blakely [12] and Shamir [11] separately introduced a SSS in 1979, based on the solution of a system of linear equations and the Lagrange interpolation method (LIM). Quantum Secret Sharing (QSS) is a quantum cryptography extension of SS, and the

Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

difference between SS and QSS is that QSS's security depends on a fundamental property of quantum physics. Quantum information is used in QSS as a cryptographic technique to overcome sharing classical or quantum secrets. That is, the dealer transmits a secret to a set of participants, which may be conventional information or an unknown quantum state, and recovering the secret requires a specific set of participants to cooperate. Hillery et al. [13] introduced the first QSSS in 1999, relying on the Greenberger-Home-Zeilinger (GHZ) state.

Lu et al.[10] introduced one particle with two dimensions QSSS using LIM. Later on, Kumar et al.[18] introduced one particle with three dimensions QSSS based on LIM. These schemes are not based on two particles QSSS. Our scheme uses two particles with three dimensions quantum states for sharing information that means it can carry more information at a time. By comparing it with the existing schemes [13]-[15] that use entangled states, our scheme seems easier to understand and more practicable to implement due to its only dependence on the bi-qutrit and bivariate quantum operation. In our scheme, we have introduced a "two particles with three dimensions quantum state sharing scheme based on LIM & bivariate operator".

2. PRELIMINARIES

This section describes some definitions and conclusions relevant to the qutrit and their mathematical contexts, which are highly useful in understanding our proposed scheme.

2.1 Qutrit Quantum state [18]**:** A qutrit quantum state $|\Phi\rangle$is defined as

$$|\Phi\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle + \alpha_3|2\rangle \quad (2.1)$$

where α_i, for i = 1, 2, 3, are scalars (real or complex) and holds the following identity

$$\sum_{i=1}^{9} |\alpha_i|^2 = 1.$$

2.2 Bi-Qutrit quantum state: A bi-qutrit quantum state $|T\rangle$is defined as

$$|T\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|02\rangle + \alpha_4|10\rangle + \alpha_5|11\rangle + \alpha_6|12\rangle + \alpha_7|20\rangle + \alpha_8|21\rangle + \alpha_9|22\rangle \quad (2.2)$$

where α_i, for i = 1, 2, . . . , 9, are scalars and holds the following identity

$$\sum_{i=1}^{9} |\alpha_i|^2 = 1.$$

2.3 Sequence of bi-qutrit quantum states: A sequence of bi-qutrit quantum states $\{|Tq\rangle\}$ is defined as

$$\{Tq : Tq = \alpha_{1q}|00\rangle + \alpha_{2q}|01\rangle + \alpha_{3q}|02\rangle + \alpha_{4q}|10\rangle + \alpha_{5q}|11\rangle + \alpha_{6q}|12\rangle + \alpha_{7q}|20\rangle + \alpha_{8q}|21\rangle + \alpha_{9q}|22\rangle,\ 1 \le q \le m\} \quad (2.3)$$

Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

where α_{iq}, for i = 1, 2, . . . , 9, are scalars and holds the following identity

$$\sum_{i=1}^{9} |\alpha_{iq}|^2 = 1, \text{ for } q=1,2,...,m.$$

2.4 Quantum operation for bi-qutrit quantum state: The quantum operation denoted by U(θ, φ) for the bi-qutrit quantum state |T⟩ is defined as

U(θ, φ) = cos(θ) [|00⟩⟨00| + |01⟩⟨01| + |02⟩⟨02| + |10⟩⟨10|] + sin(θ) [|01⟩⟨00| + |02⟩⟨10| − |00⟩⟨01| − |10⟩⟨02|] + cos(2φ) [|12⟩⟨12| + |20⟩⟨20| + |21⟩⟨21| + |20⟩⟨20|] + sin(2φ) [|20⟩⟨12| + |21⟩⟨22| − |12⟩⟨20| − |22⟩⟨21|] + $e^{-2i\varphi}$|11⟩⟨11|

where θ and φ are two parameters.

2.5 Dealer: A reliable party that divides secret information into parts and distributes these parts among n−members who want to share confidential information.

2.6 Decoy particles: The decoy photons are some fake 2−qutrit quantum states that are generated at random by the dealer and introduced into a sequence of 2−qutrit quantum states during the transmission of secret information between members to ensure the confidential information's security.

2.7 Lagrange's interpolation method [18]**:** For a given set of (n+1) points, say (x_i, h_i), i = 0, 1, 2, . . . , n, we can generate the Lagrange's interpolation polynomial h(x) with degree n as follows:

$$h(x) = \sum_{i=0}^{n} h(x_i) \prod_{r=0, r\neq 1}^{n} \frac{x - x_r}{x_i - x_r} = b_0 + b_1 x + \cdots + b_n x^n$$

where $h_i = h(x_i)$ and b_0, b_1, . . . , b_n are constant coefficients of h(x) which have taken from

the finite field F_p, where p is a given prime number.

In our present scheme, the secret value S is formed by the following presumption that

S = h(0) = b_0.

Lemma 2.1. [18] Suppose U(θ_1, φ_1), U(θ_2, ϕ_2), . . . , U(θ_n, ϕ_n) are n−bivaraite quantum operation. After applying these bivaraite quantum operation on a bi-qutrit quantum state |T⟩then U holds the following relation

U(θ_1, ϕ_1)U(θ_2, ϕ_2). . . U(θ_n, ϕ_n)|T⟩ = U(θ_1 + θ_2 + . . . + θ_n, ϕ_1 + ϕ_2 + . . . + ϕ_n)|T⟩. (2.4)

Lemma 2.2. [18] If in a Shamir's (t, n) − threshold SSS, dealer distributes the secret shares(x_r, h_r) with r = 1, 2, . . . , l, t ≤ l ≤ n to the members M_r, then secret S = h(0) can be recovered with the collaboration of all lmembers, by the following expression

Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

$$S = h(0) = \sum_{r=1}^{l} L_r h_r \,(mod\ p),$$

where

$$L_r h_r = \left[\left(\prod_{\omega=1,\omega\neq 1}^{l} \frac{x_\omega}{x_\omega - x_r}\right) h_r\right] mod\ p \quad (2.5)$$

and h(x) is the Lagrange interpolation polynomial of degree (l − 1) generated by l points(x_r, h_r) with r = 1, 2, . . . , l.

Remark: It is noticeable that in Shamir's secret sharing scheme, the dealer keeps the point(0, h_0) private as it consists of the secret information S = h_0i.e. the point (0, h_0) is not distributed to any of the members.

Corollary 2.3. [18] If in Lemma-2.2, the secret S is recovered by the relation

$S = h(0) = \sum_{r=1}^{l} L_r h_r \,(mod\ p)$ with$L_r h_r = \left[\left(\prod_{\omega=1,\omega\neq 1}^{l} \frac{x_\omega}{x_\omega - x_r}\right) h_r\right] mod\ p,$

then$\sum_{r=1}^{l} L_r h_r = N_p + S$, where N is a positive integer.

3 PROPOSED SCHEME

The proposed method involves (t, n) −threshold bi-qutrit quantum state sharing. This scheme shares the secret key using Shamir's technique, then rebuilds the original information using bivariate quantum operator and Lagrange's interpolation formula on a sequence of bi-qutrit quantum states. Suppose at least t−members out of n, say {M_1, M_2, . , M_t} with1 ≤ t ≤ n, request to a dealer which has bi-qutrit quantum information {T_q : 1 ≤ q ≤ m}as given by (2.3) to restore the original secret information |T_q⟩. This section is divided into three parts, which are discussed below:

3.1 Key Distribution Phase: First of all, the dealer allocates the private keys to each member using the following steps:

1) Dealer selects an arbitrary polynomial of degree t − 1 over field F_p of cardinality p, under addition modulo p such that
$$h(x) = [c_0 + c_1 x + \cdots + c_{t-1} x^{t-1}] mod\ p,$$
Where c_0 = S = h(0) < p (p is the cardinality of the field F_p) is the value of secret and (c_1, c_2, . . . , c_{i-1}) ∈ F_p.
2) Dealer chooses the public key x_k(∈ F_p) of the member M_k for k = 1, 2, . . . , n, in such a way that x_k, x_v∈ F_p with x_k≠ x_v for k≠v.
3) Dealer finds each share h(x_k) to corresponding shareholder M_k for k = 1, 2, . . . , n and sends h(x_k) to the each member M_k through quantum direct secure communication[16,17].

3.2 Sharing of quantum states phase: In this phase, the dealer wants to divide the original information into n members, as discussed below:

1) Firstly, the dealer selects a random sequence {|Tq⟩} defined by equation (2.3).
2) For the sharing of secret information |Tq⟩ among the participants, dealer prepares some random decoy particles from the following basis

Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

$$\mu = \{|0\rangle, |1\rangle, |2\rangle\}$$

$$\upsilon = \left\{\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \frac{1}{\sqrt{3}}\left(|0\rangle + e^{\frac{2\pi i}{3}}|1\rangle, +|2\rangle\right), \frac{1}{\sqrt{3}}\left(|0\rangle + e^{\frac{4\pi i}{3}}|1\rangle + e^{\frac{2\pi i}{3}}|2\rangle\right)\right\}$$

3) Now, the dealer performs his bivariate phase operator U(θ_0, φ_0) on each quantum states of sequence |Tq⟩, then we get a new sequence of 2−qutrit quantum states as

$$\{|T_q^0\rangle: |T_q^0\rangle = \alpha_{1q}\cos(\theta_0) - \alpha_{2q}\sin(\theta_0))|00\rangle + (\alpha_{1q}\sin(\theta_0) + \alpha_{2q}\cos(\theta_0))|01\rangle + (\alpha_{3q}\cos(\theta_0) + \alpha_{4q}\sin(\theta_0))|02\rangle + (-\alpha_{3q}\sin(\theta_0) + \alpha_{4q}\cos(\theta_0))|10\rangle + \alpha_{3q}e^{-2i\varphi_0}|11\rangle + (\alpha_{6q}\cos(2\varphi_0) - \alpha_{7q}\sin(2\varphi_0))|12\rangle + (\alpha_{6q}\sin(2\varphi_0) + \alpha_{7q}\cos(2\varphi_0))|20\rangle + (\alpha_{8q}\cos(2\varphi_0) + \alpha_{9q}\sin(2\varphi_0))|21\rangle + (-\alpha_{8q}\sin(2\varphi_0) + \alpha_{9q}\cos(2\varphi_0))|22\rangle\}$$

where$(\theta_0, \varphi_0) = (\frac{-2\pi S}{p}, \frac{\pi S}{p})$ and S is the secret value.

4) Next, the dealer adds some decoy particles randomly picked from the bases {μ, v} into the sequence {$|T_q^0\rangle$}for detecting spy.
5) After noting the place of every decoy particle, the dealer transmits the sequence to any of the participants, say M_i, 1 ≤ *i* ≤ n. The dealer proclaims the place of decoy photons and requests M_i to detect these photons according to their basis in {μ, v} after confirming that M_i has obtained the sequence. M_i presents the outcomes of his measurements. By comparing the measured results to the original states, the dealer can establish the error rate.
6) If threshold value is less than the error rate, the sender instructs M_i to stop the procedure and begin a new procedure. Otherwise, the procedure will be continued.

The quantum state sequence has been dispersed across *n* members due to the preceding steps, and any t of these n can collaborate to recover the original sequence.

3.3 Recovery Phase: Members {M_1, M_2, . . . , M_t} must first complete the following steps in order to recover the sequence of 2−qutrit quantum states.

1) By removing the decoy particles, M_1 extracts the sequence {$|T_q^0\rangle$} from the received sequence. Now, M_1 calculates$L_1 h(x_1) = \left[\left(\prod_{\omega=2}^{t}\frac{x_\omega}{x_\omega - x_1}\right)h(x_1)\right] mod\ p$with the help of his share and LIM, and then performs bivariate operator U(θ_1, φ_1)on each quantum state of sequence{$|T_q^0\rangle$}, where $(\theta_0, \varphi_0) = (\frac{2\pi L_1 h(x_1)}{p}, \frac{-\pi L_1 h(x_1)}{p})$.Then, we get a new transformed sequence{$|T_q^1\rangle$}, where $|T_q^1\rangle = U(\theta_1, \varphi_1)|T_q^0\rangle$. After that M_1transmits{$|T_q^1\rangle$} to M_2.
2) Now, M_2 calculates$L_2 h(x_2) = \left[\left(\prod_{\omega=1,\omega\neq 2}^{t}\frac{x_\omega}{x_\omega - x_2}\right)h(x_2)\right] mod\ p$with the help of hisshare and LIM, and then performs bivariate operator U(θ_2, φ_2)on each quantum state of sequence{$|T_q^1\rangle$}, where $(\theta_2, \varphi_2) = (\frac{2\pi L_2 h(x_2)}{p}, \frac{-\pi L_2 h(x_2)}{p})$.Then, we geta new transformed sequence{$|T_q^2\rangle$}, where $|T_q^2\rangle = U(\theta_2, \varphi_2)|T_q^1\rangle$. After that M_2transmits{$|T_q^2\rangle$} to M_2.

Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

3) Each remaining member, M_r; r = 3, 4, ..., t, now repeats the process as M_2 does in step 2. After the last member M_t completes his bivariate operation $U(\theta_t, \varphi_t)$, $(\theta_t, \varphi_t) = (\frac{2\pi L_t\, h(x_t)}{p}, \frac{-\pi L_t\, h(x_t)}{p})$, we get

$$(\theta_t, \varphi_t) = U(\theta_t, \varphi_t)U(\theta_{t-1}, \varphi_{t-1})U(\theta_{t-2}, \varphi_{t-2}) \dots U(\theta_2, \varphi_2)U(\theta_1, \varphi_1)|T_q^0\rangle$$
$$= U(\theta_t, \varphi_t)U(\theta_{t-1}, \varphi_{t-1})U(\theta_{t-2}, \varphi_{t-2}) \dots U(\theta_2, \varphi_2)U(\theta_1, \varphi_1)U(\theta_0, \varphi_0)|T_q^0\rangle$$
$$= U(\theta_t + \theta_{t-1} + \theta_{t-2} + \cdots + \theta_1 + \theta_0, \varphi_t + \varphi_{t-1} + \varphi_{t-2} + \cdots + \varphi_1 + \varphi_0)|T_q\rangle$$
$$= U\left(\frac{2\pi}{p}\left(\sum_{r=1}^{t} L_r\, h_r - S\right), -\frac{\pi}{p}\left(\sum_{r=1}^{t} L_r\, h_r - S\right)|T_q\rangle\right)$$
$$= U\left(\frac{2\pi}{p}(N_p + S - S), -\frac{\pi}{p}(N_p + S - S)|T_q\rangle\right) \qquad (N \in Z)$$
$$= U(2\pi N, -\pi N)|T_q\rangle \qquad (N \in Z)$$
$$= |T_q\rangle$$

Hence, any tparticipants can recover the original sequence $|T_q\rangle$.

4. CORRECTNESS OF THE PROPOSED SCHEME

First, dealer applies their bivariate quantum operation, say$U(\theta_0, \varphi_0)$and after that all t−participants applies their corresponding bivariate phase operations, say,$U(\theta_1, \varphi_1)$, $U(\theta_2, \varphi_2)$, … $U(\theta_t, \varphi_t)$, on original sequence of bi-qutrit quantum state$|T_q\rangle$, then it becomes$|T_q^t\rangle$, which is given by

$$|T_q^t\rangle = U(\theta_t, \varphi_t)U(\theta_{t-1}, \varphi_{t-1}) \dots (\theta_2, \varphi_2)(\theta_1, \varphi_1)(\theta_0, \varphi_0)|T_q\rangle \qquad (2.6)$$

By using Lemma-2.1, equation (2.6) can be written as

$$|T_q^t\rangle = U(\theta_t + \theta_{t-1} + \cdots + \theta_1 + \theta_0, \varphi_t + \varphi_{t-1} + \cdots + \varphi_1 + \varphi_0)|T_q\rangle \qquad (2.7)$$

Now, substitute the values of (θ_k, φ_k), with k = 0, 1, . . . , t, in (2.7) and add up all the innerterms in U, we get

$$|T_q^t\rangle = U\left(\frac{2\pi}{p}(\textstyle\sum_{r=1}^{t} L_r\, h_r - S), -\frac{\pi}{p}(\sum_{r=1}^{t} L_r\, h_r - S)\right)|T_q\rangle. \qquad (2.8)$$

Now with the help of Corollary-2.3 and definition of bivariate operator in equation (2.8), we get the initial secret information as

$$|T_q^t\rangle = |T_q\rangle$$

This proves the correctness of the proposed scheme for bi-qutrit quantum state sharing.

Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

5. CONCRETE ILLUSTRATION OF THE PROPOSED SCHEME

We will justify our proposed schemes with the help of the following example consisting of a (5, 7) −threshold QSS scheme over the finite field F_{13}. In this example, we have t = 5,n = 7 and p = 13.

5.1. Key Distribution Phase: This phase completes in the following steps:

1) Dealer chooses a random polynomial $h(x) = 11 + 2x + 3x^2 + x^3 + 4x^4$ of degree four over F_{13}, with the secret information s = 11 = h(0).

2) Dealer chooses the public key $x_k = k + 3$ for participant M_k, k = 1, 2, 3, 4, 5, 6, 7.Then, dealer calculates $h_k$using the polynomial $h(x) = 11 + 2x + 3x^2 + x^3 + 4x^4$ with the relation $h_k = h(x_k)$, as follows:
   $h_1 = h(x_1 = 4) = 1155(\text{mod}13) = 11$, $h_2 = h(x_2 = 5) = 2721(\text{mod}13) = 4$,
   $h_3 = h(x_3 = 6) = 5531(\text{mod}13) = 6$, $h_4 = h(x_4 = 7) = 10119(\text{mod}13) = 5$,
   $h_5 = h(x_5 = 8) = 17115(\text{mod}13) = 7$, $h_6 = h(x_6 = 9) = 27245(\text{mod}13) = 10$,
   $h_7 = h(x_7 = 10) = 41331(\text{mod}13) = 4$.
3) Finally, dealer use the quantum secure direct communication methods of [16, 17] to distribute the shares $h_1 = 11$, $h_2 = 4$, $h_3 = 6$, $h_4 = 5$, $h_5 = 7$, $h_6 = 10$ and $h_7 = 4$ to the participants M_1, M_2, M_3, M_4, M_5, M_6 and M_7 respectively.

5.2. Sharing of Quantum State Phase: In this phase, firstly dealer performs his bivariate operation $U(\theta_0, \varphi_0)$, $(\theta_0, \varphi_0) = \left(\frac{-2\pi S}{p}, \frac{\pi S}{p}\right) = \left(\frac{-22\pi}{13}, \frac{11\pi}{13}\right)$, on the bi-qutrit sequence $|Tq\rangle$. Then, he distributes the sequence into n members as we did in section (3.2).

5.3. Recovery Phase: Suppose M_1, M_2, M_4, M_6, and M_7wish to recover the secret information $|Tq\rangle$. For this, participants M_1, M_2, M_4, M_6, and M_7respectively calculate $L_1h(x_1)$,$L_2h(x_2)$, $L_4h(x_4)$, $L_6h(x_6)$ and $L_7h(x_7)$ using LIM as follow:

$$L_1h(x_1) = \left[\left(\prod_{\omega=2}^{t} \frac{x_\omega}{x_\omega - x_1}\right) h(x_1)\right] mod\ 13 = 8,$$

$$L_2h(x_2) = \left[\left(\prod_{\omega=1,\omega\neq 2}^{t} \frac{x_\omega}{x_\omega - x_2}\right) h(x_2)\right] mod\ 13 = 8,$$

$$L_4h(x_4) = \left[\left(\prod_{\omega=1,\omega\neq 4}^{t} \frac{x_\omega}{x_\omega - x_4}\right) h(x_4)\right] mod\ 13 = 3,$$

$$L_6h(x_6) = \left[\left(\prod_{\omega=1,\omega\neq 6}^{t} \frac{x_\omega}{x_\omega - x_6}\right) h(x_6)\right] mod\ 13 = 1,$$

$$L_7h(x_7) = \left[\left(\prod_{\omega=1,\omega\neq 7}^{t} \frac{x_\omega}{x_\omega - x_7}\right) h(x_7)\right] mod\ 13 = 4.$$

Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

Therefore,

$$(\theta_1, \varphi_1) = \left(\frac{2\pi L_1 h(x_1)}{p}, \frac{-\pi L_1 h(x_1)}{p}\right) = \left(\frac{16\pi}{13}, \frac{-8\pi}{13}\right)$$

$$(\theta_2, \varphi_2) = \left(\frac{2\pi L_2 h(x_2)}{p}, \frac{-\pi L_2 h(x_2)}{p}\right) = \left(\frac{16\pi}{13}, \frac{-8\pi}{13}\right)$$

$$(\theta_4, \varphi_4) = \left(\frac{2\pi L_4 h(x_4)}{p}, \frac{-\pi L_4 h(x_4)}{p}\right) = \left(\frac{6\pi}{13}, \frac{-3\pi}{13}\right)$$

$$(\theta_6, \varphi_6) = \left(\frac{2\pi L_6 h(x_6)}{p}, \frac{-\pi L_6 h(x_6)}{p}\right) = \left(\frac{2\pi}{13}, \frac{-\pi}{13}\right)$$

$$(\theta_7, \varphi_7) = \left(\frac{2\pi L_7 h(x_7)}{p}, \frac{-\pi L_7 h(x_7)}{p}\right) = \left(\frac{8\pi}{13}, \frac{-4\pi}{13}\right)$$

Now, M_1, M_2, M_4, M_6, and M_7 performs their corresponding bivariate operations on $|T_q^0\rangle$. Then, we get

$$|T_q^5\rangle = U(\theta_7, \varphi_7)U(\theta_6, \varphi_6)U(\theta_4, \varphi_4)U(\theta_2, \varphi_2)U(\theta_1, \varphi_1)|T_q^0\rangle$$

$$= U(\theta_7, \varphi_7)U(\theta_6, \varphi_6)U(\theta_4, \varphi_4)U(\theta_2, \varphi_2)U(\theta_1, \varphi_1)U(\theta_0, \varphi_0)|T_q\rangle$$

$$= U(\theta_7 + \theta_6 + \theta_4 + \theta_2 + \theta_1 + \theta_0, \varphi_7 + \varphi_6 + \varphi_4 + \varphi_2 + \varphi_1 + \varphi_0)|T_q\rangle$$

$$= U\left(\frac{8\pi}{13} + \frac{2\pi}{13} + \frac{6\pi}{13} + \frac{16\pi}{13} + \frac{16\pi}{13} - \frac{22\pi}{13}, -\frac{4\pi}{13} - \frac{\pi}{13} - \frac{3\pi}{13} - \frac{8\pi}{13} - \frac{8\pi}{13} + \frac{11\pi}{13}\right)|T_q\rangle$$

$$= U(2\pi, -\pi)|T_q\rangle$$

$$= |T_q\rangle$$

Hence, 5 out of 7 participants can recover the initial information.

6. SECURITY ANALYSIS

The decoy particles are utilized in our protocol to detect eavesdropping. Therefore, when a spy tries to get transmitted information by mounting an “intercept and resend” attack, then only quantum sequence intercepted by him but not the sequence states, and is, therefore, unable to resend an exact copy of the sequence because of the quantum no-cloning theorem and the Heisenberg uncertainty principle. Furthermore, because the spy is unaware of the decoy particles’ positions and states, the attack will lead to an increased error rate. Therefore, the attack will be detected with the probability $1 - \left(\frac{5}{9}\right)^k$ [19], where *k* is the number of decoy particles. For a very large k, the probability converges to 1. There is another famous attack, “entangle-and-measure,” which may be taken by a spy. Still, because of the decoy particles, he will not obtain any relevant information regarding the secret.

Xi'an ShiyouDaxueXuebao (ZiranKexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

Another famous attack is the “participant attack”. In this attack, any number of participants fewer than *t* may attempt to steal information, but they will fail to reconstruct the dealer’s phase value$(\theta_0, \varphi_0) = \left(\frac{-2\pi S}{p}, \frac{\pi S}{p}\right)$. Hence, they are unable to obtain any information regarding quantum states.

7. COMPARISION

Our proposed method is based on the sharing of bi-qutrit quantum states. Due to their wide Hilbert space, bi-qutrits may be more efficient than qubits in quantum information processing, such as quantum key distribution in the involvement of various eavesdroppers. They provide benefits such as better security in a diversity of quantum computation protocols, increased communication range for quantum communication, innovative fundamental quantum mechanics tests, and more effective quantum gates. Also, increasing the number of qutrits leads to the carrying of a large amount of information.

Most of the existing schemes based on qubit quantum states[2, 3, 7, 9, 10], in comparison our scheme is based on bi-qutrit. As a result, unlike qubits, our approach is made up of high-dimensional quantum states. Because of its high-dimensional nature, bi-qutrit provides a larger Hilbert space to process and store information, which can reduce circuit complexity, simplify experimental setup, and improve algorithm performance. Although the advantages of the bi-qutrit system in numerous applications and the potential for future growth are significant, this system gets less prominence than standard qubit-based quantum mechanics. Our technique can transfer quantum information by combining Lagrange interpolation with a quantum bivariate phase shift operation, whereas schemes [20, 21] can only transfer classical information.

The main difference between Xiao’s scheme [21] and our scheme is that it can only transfer classical information, but do not share the quantum state. Because of non-entanglement quantum state sharing, our technique becomes more feasible and easier to implement. Because of the higher dimension of bi-qutrit quantum states, they enable heightened sensitivity in quantum image processing schemes, they can improve the efficiency levels of biological compounds, they provide richer assets for quantum simulation, they result in higher increased efficiency in quantum data processing and clock synchronization, and they can be useful in quantum measurement applications. As bi-qutrit has a huge Hilbert space, it provides a number of advantages, ranging from enhanced capacity and noise resistance to unique fundamental research opportunities in quantum physics.

8. CONCLUSION

A bi-qutrit based scheme is proposed for sharing information via. quantum channels. Compared to a qubit (superposition of two orthogonal quantum states), a qutrit has

ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

large number of quantum states (superposition of three pairwise orthogonal quantum states) and is, therefore, beneficial in encoding and carrying more quantum information. It has been observed in literature that a qutrit is helpful in encoding more information because it has a larger Hilbert Space compared to a qubit. Also, increasing the number of qutrit results in the carrying much information. The present work proposes “the sharing of information using bi-qutrit quantum states based on bivariate quantum gates”.

REFERENCES

[1] Zhang, X., 2009. One-way quantum identity authentication based on public key. Chinese Science Bulletin, 54(12), pp.2018-2021.
[2] Qin, H., Zhu, X. and Dai, Y., 2015. (t, n) Threshold quantum secret sharing using the phase shift operation, Quantum Information Processing, 14(8), 2997-3004. https://doi.org/10.1007/ s11128-015-1037-6
[3] Yang, Y.G., Teng, Y.W., Chai, H.P. and Wen, Q.Y., 2011. Verifiable quantum (k, n)-threshold secret key sharing, International Journal of Theoretical Physics, 50(3), 792-798. https://doi.org/10.1007/ s10773-010-0616-7
[4] Qin, H., Tso, R. and Dai, Y., 2018. Multi-dimensional quantum state sharing based on quantum Fourier transform, Quantum Information Processing, 17(3), 1-12. https://doi.org/10.1007/ s11128-018-1827-8.
[5] Hao, C. and Wenping, M., 2017. (t, n) Threshold quantum state sharing scheme based on linear equations and unitary operation, IEEE Photonics Journal, 9(1), 1-7. https://doi.org/10.1109/JPHOT.2017. 2657232
[6] Cleve, R., Gottesman, D. and Lo, H.K., 1999. How to share a quantum secret. Physical Review Letters, 83(3), p.648.
[7] Deng, F.G., Li, X.H., Li, C.Y., Zhou, P. and Zhou, H.Y., 2006. Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements. The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics, 39(3), pp.459-464.
[8] Gao, T., Yan, F. and Li, Y., 2009. Quantum secret sharing between m-party and n-party with six states. Science in China Series G: Physics, Mechanics and Astronomy, 52(8), pp.1191-1202.
[9] Liao, C.H., Yang, C.W. and Hwang, T., 2014. Dynamic quantum secret sharing protocol based on GHZ state. Quantum information processing, 13(8), pp.1907-1916.
[10] Lu, C., Miao, F., Meng, K. and Yu, Y., 2018. Threshold quantum secret sharing based on single qubit. Quantum Information Processing, 17(3), pp.1-13.
[11] Shamir, A., 1979. How to share a secret. Communications of the ACM, 22(11), pp.612-613.
[12] Blakley, G.R., 1979, December. Safeguarding cryptographic keys. In Managing Requirements Knowledge, International Workshop on (pp. 313-313). IEEE Computer Society.
[13] Hillery, M., Buˆzek, V. and Berthiaume, A., 1999. Quantum secret sharing. Physical Review A, 59(3), p.1829.
[14] Karlsson, A., Koashi, M. and Imoto, N., 1999. Quantum entanglement for secret sharing and secret splitting. Physical Review A, 59(1), p.162.
[15] Gottesman, D., 2000. Theory of quantum secret sharing. Physical Review A, 61(4), p.042311.
[16] Qing-Yu, C. and Bai-Wen, L., 2004. Deterministic secure communication without using entanglement. Chinese Physics Letters, 21(4), p.601.
[17] Deng, F.G. and Long, G.L., 2004. Secure direct communication with a quantum one-time pad. Physical Review A, 69(5), p.052319.
[18] Kumar, M., Gupta, M.K., Mishra, R.K., Dubey, S.S., Kumar, A. and Hardeep, 2020. Security Analysis of a Threshold Quantum State Sharing Scheme of an Arbitrary Single-Qutrit Based on

ISSN:1673-064X
E-Publication:Online Open Access
Vol: 64 Issue 12 | 2021
DOI 10.17605/OSF.IO/A49EJ

Lagrange Interpolation Method, Proceedings of ETCCS 2020. https://doi.org/10.1007/978-981-15-7804-5

[19] Qin, H. and Dai, Y., 2017. Dynamic quantum secret sharing by using d-dimensional GHZ state, Quantum information processing, 16(3), 64. https://doi.org/10.1007/s11128-017-1525-y

[20] Yang, W., Huang, L., Shi, R. and He, L., 2013. Secret sharing based on quantum Fourier transform. Quantum information processing, 12(7), 2465-2474.

[21] Xiao, H. and Gao, J., 2013. Multi-party d-level quantum secret sharing scheme. International Journal of Theoretical Physics, 52(6), pp.2075-2082.