Quantum key distribution by teleportation and unextendible product operator bases

Xiaoxuan Li

Admiral Farragut Academy Tianjin, Tianjin 300042, China

alexandra_xxdd@163.com

Abstract. Quantum teleportation and quantum key distribution (QKD) both play a key role in the application of quantum information processing. They have been widely realized in experiments in the past decades. We construct a multipartite QKD protocol using teleportation by a Greenberger-Horne-Zeilinger entangled state. The latter is a frequently studied family entangled states in theory and experiments. Our protocol shows the security because the loss of any particles does not lead to the loss of information the sender wants to send to the receiver. Further, the classical messages cost in the protocol occur only among some particles. We also apply the unextendible product operator basis (UPOB) by performing them on high dimensional states, which are then teleported to the receiver. We stress that UPOBs are related to quantum nonlocality, which is associated with the local indistinguishability of orthogonal states. Hence our paper may contribute to the novel understanding of quantum nonlocality, as well as related quantum-information tasks such as state and operation discrimination.

Keywords: quantum teleportation, entanglement, key distribution

1. Introduction

In the past decades, quantum teleportation has been investigated by researchers since it was firstly proposed in 1993 [1]. As quantum has no direct counterpart in the classical word, the redesign of the classical communication system model is required to demonstrate the peculiarities of quantum teleportation [2]. During the period of 20 years, researchers have come up with several protocols. Over 10 years ago, an explicit protocol with respect to four-qubit state explained the genuine four-partite analogue to a Bell state [3]. Very recently, researchers' protocol allows to store and retrieve an arbitrary qubit state onto a dual-rail encoded optomechanical quantum memory [4]. Several experiments with great influence have been conducted as well. The experimental quantum teleportation of single-photon qubits from a ground observatory to a satellite was reported [5]. Plus, quantum computing can be realized by teleportation which was proved between light and the vibrations of a nanomechanical resonator [6-8]. In recent years, quantum teleportation has been increasingly popular around the world, and the prevalence of the topic made me, a senior high school student who felt passionately about quantum physics, think a lot about the confidentiality of this technique. The aim of my research is to design an efficient protocol to ensure the safety of quantum teleportation without interfering its result. Thus, in this paper, the process and characteristics of quantum teleportation are mainly investigated based on the information we have got. To be specific, we firstly introduce basic maths and physics to be used in the process of our research, and then we apply those numerical concepts into our topic. We investigate

^{© 2024} The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

quantum measurement thoroughly, considering about No-cloning Theorem, CNOT Gate and different situations when there are only two people communicating and when there are more. Based on various assumptions with different numbers of participants in the communication system, we finally come up with a protocol that ensures not only the safety but also the efficiency of transporting qubit messages innovatively, with least qubits used and no risk of information exposure.

2. Preliminaries

In this section, we briefly introduce the preliminary knowledge used in this paper, such as the matrix calculation, Kronecker product and its calculation in Sec. 2.1, and quantum physics and the entangled state in Sec. 2.2.

2.1. Matrix

Firstly, the calculation of matrices A,B and C of the same size fulfills the associative law of addition, namely (A+B)+C=A+(B+C). The calculation also fulfills the associative law of multiplication, (AB)C=A(BC). When there involves real number in the calculation with matrices, the laws are still fulfilled. We introduce the concept of anti-symmetric determinant. Let $A=(a_{ij})$, $-A=(-a_{ij})$, then A and (-A) are anti-symmetric determinant of each other, with properties A+(-A)=0 and A-B=A+(-B). The identity matrices are also discussed, and all other matrix with the same order is commutative, namely E_m $A_{mn}=A_{mn}E_n=A_{mn}$.

Next, we introduce the unitary matrices U, which fulfills $UU^+ = I$. The set of unitary matrices is closed under the matrix multiplication.

Third, if a square matrix is the same as its transpose, then it is a symmetric matrix. Similarly, if a square matrix is the negative matrix of its transpose, then it is a skew-symmetric matrix.

In this paragraph, we review the definition of Kronecker product and its properties. Let A be a n^*p matrix and B an m^*q matrix. The following matrix is called the Kronecker product/ direct product/ tensor product of A and B.

$$oldsymbol{A} \otimes oldsymbol{B} = \left[egin{array}{cccc} a_{1,1}oldsymbol{B} & a_{1,2}oldsymbol{B} & \cdots & a_{1,p}oldsymbol{B} \ a_{2,1}oldsymbol{B} & a_{2,2}oldsymbol{B} & \cdots & a_{2,p}oldsymbol{B} \ dots & dots & dots & dots & dots \ a_{n,1}oldsymbol{B} & a_{n,2}oldsymbol{B} & \cdots & a_{n,p}oldsymbol{B} \end{array}
ight]$$

From the definition, one can see that $A\otimes B$ would be an mn^*pq matrix. Besides, if $A\otimes B=B\otimes A$, we cannot infer A=B. An example is the identity matrices, $I_2\otimes I_3\neq I_3\otimes I_2$. From the definition, one can see that the calculation of tensor product satisfies the associative law, $(A\otimes B)\otimes C=A\otimes (B\otimes C)$, as well as the multiplicative distribution law, $A\otimes (B+C)=(A\otimes B)+(A\otimes C)$. For scalar $a,a\otimes A=A\otimes a=aA$; for conforming matrices, $(A\otimes B)(C\otimes D)=AC\otimes BD$. The transposed matrix of the tensor product of A and B equals the tensor product of transposed A and transposed A. Also, The A-th power of the tensor product of A and A-th power of A-th power of

2.2. Quantum Physics

Next, we introduce the elementary notations from quantum physics. We refer to the state |x> as an n-dimensional unit vector

$$|x\rangle = \left[\begin{array}{c} a_1 \\ a_2 \\ \dots \\ a_n \end{array} \right]$$

in the sense that

$$< x|x> = [a_1^*, a_2^*, a_3^* \dots a_n^*] \cdot [a_1, a_2, a_3 \dots a_n]^T$$

 $= |a_1|^2 + \dots + |a_n|^2$
 $= a_1 a_1^* + a_2 a_2^* + a_3 a_3^* + \dots + a_n a_n^*$
 $= 1.$

Here, $\langle x| = [a_1^*, a_2^*, a_3^* \dots a_n^*]$ is the conjugate transposition of $|x\rangle$.

In quantum physics and information theory, we refer to a qubit as 2-dimensional unit vector in the Hilbert space $C^{\wedge}2$. The space is spanned by the orthonormal basis |0> and |1>. They fulfil <0|0>=<1|1>=1, and <0|1>=<1|0>=0. Hence if $|x>=\alpha|0>+\beta|1>$, then < x|x>=1. We say that a bipartite state $|\alpha>_{AB}$ in $C^M\otimes C^N$ is a product state if $|\alpha>_{AB}=|x>_A\otimes|y>_B$. It has no entanglement. In contrast, the bipartite entangled state is a bipartite state which is not a product state. To achieve deeper understanding of this concept, the inequation $\frac{(|0,0>+|1,1>)}{\sqrt{2}}\neq |\alpha>\otimes|\beta>$ is required to be verified.

If Left=Right, then $(\frac{\sqrt{2}}{200} \ \frac{\sqrt{2}}{2})^T$ must equals to $(\alpha_0\beta_0\alpha_0\beta_1\alpha_1\beta_0\alpha_1\beta_1)^T$, then there are equation $(0, \alpha_0\beta_0 = \alpha_1\beta_1 = \frac{\sqrt{2}}{2})$ and equation $(0, \alpha_0\beta_1 = \alpha_1\beta_0 = 0)$. From equation $(0, \alpha_0\beta_0, \beta_1)$, thus equation $(0, \alpha_0\beta_0, \beta_1)$.

3. Quantum Teleportation

In this section, we introduce the basics of quantum teleportation. In Sec. 3.1, we introduce the Controlled NOT (CNOT) gates used in teleportation. We further need more quantum measurements, and we introduce them in Sec. 3.2. Using these preliminary knowledge, we introduce the main part of teleportation in Sec. 3.3.

3.1. CNOT Gates

In this section, the concept of CNOT is firstly introduced. It performs qubit reversal conditionally, and it is self-inversed, which means that after using CNOT twice, the result is the input value itself. This can be expressed as followed:

$$(a,b) \to (a,a \oplus b) \to (a,a \oplus (a \oplus b)) = (a,b)\{0,1\}$$
 Given qubits $|\psi>=\alpha|0>+\beta|1>$ and $|\psi+>=\frac{1}{\sqrt{2}}(|0\ 1>+|1\ 0>),$ CNOT $(H\otimes I)|0\ 1>=$

 $|\psi+\rangle$. This can be demonstrated as following:

$$\begin{split} \text{Left} &= \text{CNOT } H |0> \otimes |1> \\ &= \text{CNOT } \frac{1}{\sqrt{2}} (|0>+|1>) |1> \\ &= \text{CNOT } \frac{1}{\sqrt{2}} (|0\>1>+|1\>1>) \\ &= \frac{1}{\sqrt{2}} (|0\>0\oplus1>+|1\>1\oplus1>) \\ &= \frac{1}{\sqrt{2}} (|0\>1>+|1\>0>) = |\psi+>. \end{split}$$

3.2. Quantum Measurement

Now, Alice wants to transport a particle, namely the message qubit $|\psi\rangle=\alpha|0>+\beta|1>$ to Bob. The particle can be transported by copying if it is a classical particle; while it is not realizable through this way if it is a qubit. To achieve the goal, Alice and Bob must share a bell state of the qubit, $|\psi\rangle=\frac{1}{\sqrt{2}}(|01>+|10>)$, which is also at an entangled state and cannot be written in form of $|\alpha>\otimes|\beta>$. In other words, the measurement of Alice's would affect Bob, and different choices of Alice's result in different states of the qubit Bob receives. At the first place, Alice wants to conduct the measurement on $|\psi\rangle=\alpha|0>+\beta|1>$, but that would collapse the qubit into 0 or 1. In mathematical language, the measure of Alice's can be stated as M, and

$$(M \otimes I)|\psi^{+}\rangle = \frac{1}{\sqrt{2}}(M|0\rangle \otimes |1\rangle + M|1\rangle \otimes |0\rangle) = |\alpha\rangle$$

$$M0 = |0\rangle < 0|, |\alpha\rangle = \frac{1}{\sqrt{2}}|01\rangle;$$

$$M1 = |1\rangle < 1|, |\alpha\rangle = \frac{1}{\sqrt{2}}|10\rangle.$$

The choice of A0 would result in B1, and the choice of A1 would result in B0.

3.3. Main Part of Teleportation

Instead of the first choice, Alice decides to conduct the measurement on the bell operator bases. Alice have 4 bell operator bases:

$$|0 \ 0> = \frac{1}{\sqrt{2}}(|\varphi^{+}> + |\varphi^{-}>)$$

$$|1 \ 1> = \frac{1}{\sqrt{2}}(|\varphi^{+}> - |\varphi^{-}>)$$

$$|0 \ 1> = \frac{1}{\sqrt{2}}(|\psi^{+}> + |\psi^{-}>)$$

$$|1 \ 0> = \frac{1}{\sqrt{2}}(|\psi^{+}> - |\psi^{-}>)$$

The sum of the 4 bases is I_4 , and it is a POVM (positive operator-valued measurement). The completeness relation is:

$$\{Mj^+Mj\}$$
, SUM $(j=1 \sim k)Mj^+Mj=1$.

Now, ρ is a density matrix:

$$\rho = (|\psi > \otimes |\psi^{+} >) (< \psi | \otimes < \psi^{+}|)$$

After measurement there is ρ_i of probability of ρ to be δ_i :

$$\rho \to (\operatorname{Mj} \rho M j^+) / \operatorname{Tr} (M j \rho M j^+) = \delta_j$$

In other words, ρ can be transformed into $\delta_1, \delta_2, \delta_3, \delta_4 \ldots$. The probability of turning into any δ can be calculated, while it is impossible to know which δ would appear actually. Because Alice would do the bell measurement above, there is $\frac{1}{4}$ of possibility for her to get one of the four states, $|\psi^+>,|\psi^->,|\varphi^+>$ and $|\varphi^->$. If Alice conduct the transformation $(H\otimes I)$ CNOT before the measurement, $|\varphi^+>$ would be transformed to $|0\ 0\rangle, |\psi^+>$ to $|0\ 1>, |\varphi^->$ to $|1\ 0>$ and $|\psi>$ to $|1\ 1>$. The whole state can be expressed as:

$$\frac{1}{2}|0 \ 1 > (\alpha|0 > +\beta|1 >) + \frac{1}{2}|1 \ 1 > (\alpha|0 > -\beta|1 >)$$

$$+ \frac{1}{2}|0 \ 0 > (\alpha|1 > +\beta|0 >)$$

$$+ \frac{1}{2}|1 \ 0 > (\alpha|1 > -\beta|0 >)$$

Which is to say, if Alice has result of 00, Bob's particle would collapse into $\alpha|1>+\beta|0>$. Similarly, the result of 01,10 and 11 each matches the collapse of $\alpha|0>+\beta|1>$, $\alpha|1>-\beta|0>$ and $\alpha|0>-\beta|1>$.

Based on the result of Alice's that Bob receive, Bob is able to determine his own method of transformation to use in order to transform whatever he gets in to the original $|\psi>$. When Alice has the measurement result 01, Bob can receive the qubit $|\psi>$. When Alice has the measurement result 11, Bob has $\alpha|0>-\beta|1>$, and Bob can multiply a matrix $(1\ 0/0-1)$, called $U=\sigma_z$, to the original state, and the result would be $\alpha|0>+\beta|1>$. When Alice has the measurement result 00, Bob has $\alpha|1>+\beta|0>$, and Bob can multiply a matrix $(0\ 1/1\ 0)$ called $U=\sigma_x$, and the result would also be $\alpha|0>+\beta|1>$. Lastly, when Alice has the measurement result 10, what Bob receive is $\alpha|1>-\beta|0>$, and Bob should multiply a matrix of $(0\ 1/-1\ 0)$ called $U=i\sigma_y$ and $\alpha|0>+\beta|1>$ would appear as expected. Fig. ?? demonstrates the process described.

Thus, despite of result of measurement of Alice's, Bob can always have a way to receive the qubit. The important thing is the operation he does depends on the measurement base Alice has. Therefore, the result of Alice's measurement must be told to Bob honestly in the one-way classical communication. Plus, the final state of the first qubit measured after teleportation is $|\psi> <\psi|$.

4. Results

In this section we introduce the step of our research to design our own protocol based on the quantum key distribution (QKD). In Sec. 4.1, we introduce the concept of QKD and how its can be interpreted when there are three people involved in the system.

4.1. Tripartite Quantum Key Distribution (QKD)

Now, assume Alice wants to achieve an one-to-two quantum teleportation to Bob and Charlie. The 3 people are in one entangled state. The involvment of the third party turns the state of the particle into $|GHZ>_{ABC}$, as well as $\frac{1}{\sqrt{2}}(|000>+|111>)_{ABC}$.

Similar to what has been done on $|\psi>$ previously, the whole state of Alice's particle after measured can be expressed as

$$\frac{1}{2}|\psi^{+}\rangle(\alpha|00\rangle + \beta|11\rangle)_{BC} + \frac{1}{2}|\psi^{-}\rangle(\alpha|00\rangle - \beta|11\rangle)_{BC} + \frac{1}{2}|\varphi^{+}\rangle(\alpha|11\rangle + \beta|00\rangle)_{BC} + \frac{1}{2}|\varphi^{-}\rangle(\alpha|11\rangle - \beta|00\rangle)_{BC}$$

Under this circumstance, Bob and Charlie still have to conduct transformation based on the result of measurement they receive from Alice. The square matrix that Bob conducts is U, and the square matrix that Charlie conducts is V. The overall conduction is therefore $U \otimes V$.

When Alice's result of measurement is $\alpha|00>+\beta|11>$, Bob and Charlie can receive the particle directly;

When Alice's result of measurement is $\alpha|00>-\beta|11>, U\otimes V$ must be $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$, and

$$U = \left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array}\right), V = \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right).$$

When Alice's result of measurement is $\alpha|11>+\beta|00>, U\otimes V$ must be $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$, and

$$U = \left(\begin{array}{cc} 0 & 1\\ 1 & 0 \end{array}\right), V = \left(\begin{array}{cc} 0 & 1\\ 1 & 0 \end{array}\right).$$

When Alice's result of measurement is $\alpha|11>-\beta|00>, U\otimes V$ must be $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$, and

$$U = \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right), V = \left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right).$$

In this way, neither Bob nor Charlie receive the completed particle, or they could not send the particle out to anyone else. This example illustrates the security QKD can have.

4.2. UPOB

UPOB (Unextendible product operator basis) is a set of orthogonal product matrices, which is not orthogonal to any given nonzero product matrix at the same time. These bases are significantly important in ensuring the safety of our protocol.

First we have to understand the contents and characteristics of the bases. There are i number of basis M, where

$$i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

Specifically, the bases M_i are

$$\begin{split} M_1 &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}, \quad M_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \\ M_3 &= \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & \omega_3 \\ \omega_3^2 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad M_4 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & \omega_3 \\ \omega_3^2 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \\ M_5 &= \frac{1}{\sqrt{3}} \begin{bmatrix} 0 & 1 \\ \omega_3 & \omega_3^2 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad M_6 = \frac{1}{\sqrt{3}} \begin{bmatrix} 0 & 1 \\ \omega_3^2 & \omega_3 \\ \omega_3 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \\ M_7 &= \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad M_8 = \frac{1}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}, \\ M_9 &= \frac{1}{2} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad M_{10} = \frac{1}{2} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}, \\ M_{11} &= \frac{1}{4} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}. \end{split}$$

These M_i bases are orthogonal as

$$(A^{+} \otimes B^{+}) \cdot (C \otimes D) = A^{+}C \otimes B^{+}D = M_{1}^{+}M_{2}$$

$$M_{1} = A \otimes B_{j}, M_{2} = C \otimes D$$

$$\operatorname{Tr}(M_{1}^{+}M_{2}) = 0$$

$$(\operatorname{Tr} A^{+}C) \cdot (\operatorname{Tr} B^{+}D) = 0$$

$$\operatorname{Tr}(M_{1}^{+}M_{1}) = 0, i \neq j.$$

The result tells us the truth that the information can only be decoded when the systems join together. If they are not, there has been no way to break the qubit mathematically, which ensures the safety of our QKD.

5. Conclusion

We have used the quantum teleportation based on entanglement, to construct tripartite and multipartite quantum key distribution protocols. We showed that the protocols are against classical attacks because the robbery of particles by invaders cannot result in the loss of messages to be sent. Further, in the multipartite protocols, we have shown that the sender does not have to release the measurement results to every receiver, so as to enhance the security of protocols. We also have studied the teleportation of UPOBs using high-dimensional entangled states. An open problem arising from this paper is to investigate whether more UPOBs can be sent via less entanglement and classical communications.

References

- [1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels, Phys.Rev. Lett. 70, 1895 (1993).
- [2] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, When entanglement meets classical communications: Quantum teleportation for the quantum internet, IEEE Trans. Commun. 68, 3808(2020).
- [3] Y. Yeo and W. K. Chua, Teleportation and Dense Coding with Genuine Multipartite Entanglement, Phys. Rev. Lett. 96, 060502 (2006).
- [4] N. Fiaschi, B. Hensen, A. Wallucks, R. Benevides, J. Li, T. P. M. Alegre, and S. Gröblacher, Optomechanical quantum teleportation, Nat. Photon. 15, 817 (2021).
- [5] J.-G. Ren, P. Xu, H.-L. Yong et al., Ground-to-satellite quantum teleportation, Nature (London) 549, 70 (2017).
- [6] G. I. Harris and W. P. Bowen, Quantum teleportation from light to motion, Nat. Photon. 15, 792 (2021).
- [7] T. M. Graham, H. J. Bernstein, T.-C. Wei, M. Junge, and P. G. Kwiat, Superdense teleportation using hyperentangled photons, Nat. Commun. 6, 7185 (2015).
- [8] P. Agrawal and A. Pati, Perfect teleportation and superdense coding with W states, Phys. Rev. A 74, 062320 (2006).