Measurement-Device-Independent Quantum Key Distribution based on GHZ-Entangled-State

Ximing Hua¹,a, Min Hu¹,b and Banghong Guo¹, 2, 3,c*

¹Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou, 510006, China

²College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China

³Key Laboratory of Quantum Information, University of Science and Technology of China, Chinese Academy of Sciences, Hefei 230026, China

ABSTRACT

Quantum key distribution is the core technology of quantum communication. In 2012, the Measurement-Device-independent quantum key distribution protocol proposed by Lo et al., referred to as MDI-QKD protocol, can effectively resist detector attacks from eavesdroppers. However, the traditional MDI-QKD only supports two parties, which can no longer meet the actual needs in the era of rapid development of communication technology. Therefore, multi-party quantum key distribution has become one of the current hot spots. This paper proposes a multi-user measurement device-independent QKD method based on the GHZ entanglement state. The GHZ entanglement source is used as the quantum relay, which solves the multi-party communication and greatly improves the safe communication distance.

Keywords: Multi-party quantum communication, QKD, MDI-QKD, GHZ entangled state, polarization

1. INTRODUCTION

Quantum key distribution (QKD) is one of the important fields of quantum cryptography, which security is based on quantum mechanics and information theory rather than computation complexity. In 1984, Bennett and Brassard⁴ proposed the first QKD protocol named BB84 protocol. However, due to the difference between the realistic system and the theoretical system, there are various loopholes in the realistic system, and the eavesdropper (Eve) can attack the QKD process through these loopholes. Therefore, some investigator focus on finding a way to resist the attack. In 2012, Lo et al.[⁵] proposed a measurement-device-independent quantum key distribution protocol, referred to as MDI-QKD protocol, which can well prevent attacks on measurement devices. It means that the measurement device can be unreliable.

The traditional QKD protocol has only two communicating parties, we always called Alice and Bob. With the development of quantum communication, the quantum key distribution between the two parties can no longer meet the

---

⁴ cming_hua@163.com
⁵ hm555@yeah.net
⁶ guobangh@163.com
current needs. The multi-party quantum key distribution has broken through the limited of single-channel communication and makes quantum communication authentically practical. In 2015, Fu Yao et al.\cite{3} proposed a multi-party MDI-QKD protocol, and they use the GHZ entangled state in post-selection, and Zhu et al.\cite{4} proposed a multi-user MDI-QKD method based on W entangled state. Multi-party quantum key distribution can be used for multi-party quantum communication, so that multiple users can have a unified key at the same time for multi-party simultaneous confidential communication.

Therefore, we proposes a multi-user MDI QKD scheme based on GHZ entangled state. We will introduce the protocol in Section 2, and compare with other protocol in Section 3 and Section 4.

2. MULTI-USER MEASUREMENT-DEVICE-INDEPENDENT QKD PROTOCOL

We propose a multi-user measurement device-independent QKD protocol based on GHZ entangled state. Its design is divided into three parts: user terminal, measuring terminal, and GHZ entanglement source, as shown in Figure 1.

![Diagram of Multi-User Measurement-Device-Independent QKD Protocol](https://example.com/fig1.png)

Figure 1: The protocol includes user terminal, measurement terminal, GHZ entanglement source. At the user terminal, we use an attenuated light source as a single photon source. The structure of the measurement terminal is the same as the original MDI-QKD protocol, including a BS, two PBSs, and four single photon detectors. The GHZ entanglement source can send GHZ entangled states with different numbers of particles (equal to the number of users) following the number of users.
Our protocol mainly includes five procedures:

Step0: Single photon and GHZ entangled state preparation. It means each user terminal sends single photons through a single photon source and GHZ entangled source to prepare GHZ entangled particles. Under practical conditions, users using the attenuated light source as a single-photon source.

Step1: Send particles through the quantum channel. The single photon particles and GHZ entangled states particles are transmitted to the measurement part through a quantum channel between sources and measurement devices.

Step2: Single photon interferes with GHZ entangled state. The single photon provided by each users and the GHZ entangled state provided by GHZ entangled source (because it is a multi-user communication system, the number of particles contained in each GHZ entangled state is equal to the number of users.) interfere at the measurement part, at the same time, it performs Bell state measurement (the measurement principle of the bell state in this method is the same as that of the BELL state measurement in MDI-QKD).

Step3: Getting the raw key. We successfully get the raw key only if the multiple users send the same polarization state (The coding method will be changed according to the preparation of the GHZ entangled state, which will be further explained in Section 3).

Step4: Post-processing. Classical post-processing is used generate the secure keys same as other QKD protocols, such as error correction, privacy amplification, et al.

3. GHZ ENTANGLED STATE

The GHZ (Greenberger-Horne-Zeilinger) state is a multi-quantum entangled state proposed by Greenberger et al. in 1989. It is a commonly used entangled state used in multi-party quantum communication. For an n-particle GHZ entangled state, it usually has n forms, we usually describe them as:

\[
\begin{align*}
|\varphi>_1 &= \frac{1}{\sqrt{2}}(|H>|H>|H>...|H>\pm|V>|V>|V>...|V>) \\
|\varphi>_2 &= \frac{1}{\sqrt{2}}(|H>|V>|H>...|H>\pm|V>|H>|V>...|V>) \\
&\vdots \\
|\varphi>_n &= \frac{1}{\sqrt{2}}(|H>|H>|H>...|V>\pm|V>|V>|V>...|H>)
\end{align*}
\]

Each form of GHZ entangled state will randomly collapse into two kinds of particles after measurement. Take \(|\varphi>_1\) as an example, after measurement, the GHZ entangled state \(|\varphi>_1\) will randomly collapse into

\[
|\varphi>_{1a} = |H>|H>|H>...|H> \quad \text{or} \quad |\varphi>_{1b} = |V>|V>|V>...|V>.
\]

However, in our protocol, the type of particle that each form of n-particle GHZ entangled state will collapse into after measurement has nothing to do with the coding method, which is related to the form of GHZ entangled state. We also take \(|\varphi>_1\) as an example, if we choose \(|\varphi>_1\) as the form of GHZ entangled state, we coding only if all users send
the same polarization state single photon, it means that all measurement device will have same phenomenon. If we choose $|\varphi>_{2}$ as the form of GHZ entangled state, we coding only if except the second user all users send the same polarization state single photon while the second user sends the orthogonal polarization state single photon. It means that except the second measurement device, all measurement device will have same phenomenon.

4. DISCUSSION AND CONCLUSION

MDI-QKD is widely used because it can resist all attacks on the measurement system, it means that the measurement system can be untrusted. However, the ordinary MDI-QKD has synchronization problems due to two-photon interference. Although the two parties jointly send a single photon to the measurement system, it does not actually increase the communication distance\[^5\]. In our multi-party MDI-QKD protocol we proposed the GHZ entanglement source actually plays the role of a quantum relay, so it can extend the communication distance in addition to multi-party communication based on the original MDI-QKD protocol.

In this paper, we propose a multi-party quantum key distribution method, we realizing multi-party communication through a GHZ entangled state sending. Meanwhile, the GHZ entangled state sending is a quantum repeater. So the communication distance is greatly increased and surpassing the secret-key capacity (SKC) bound of an optical quantum channel. However, there are still many problems have to be solved. For example, since the coding of this protocol requires the single-photon polarization state sent by all users to reach a relatively fixed requirement, the coding rate will be lower.

ACKNOWLEDGMENTS

This work was supported in part by the Key R&D Program of Guangdong province (Grant No. 2018B030325002).

REFERENCES

[1] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," Theoretical Computer Science 560, 7-11 (2014).
[2] Lo, H. K. and Curty, M. and Qi B., "Measurement-Device-Independent Quantum Key Distribution," Physical Review Letters 108(13), 130503 (2012).
[3] Fu, Y. and Yin H. L. and Chen, T. Y. and Chen, Z. B., "Long-Distance Measurement-Device-Independent Multiparty Quantum Communication," Physical Review Letters 114(09), 090501 (2015).
[4] Zhu, C. H. and Xu F. H. and Pei, C. X., "W-state Analyzer and Multi-party Measurement-device-independent Quantum Key Distribution," Scientific Reports 5, 17449 (2015).
[5] Lucamarini, M. and Yuan, Z. L. and Dynes, J. F. and Shields, A. J., "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature 557, 400-403 (2018).