Continuous-variable measurement-device-independent multipartite quantum communication

Guangqiang He

State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240*, China*

Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou 510006*, China and*

State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai 200062*, China*

Ya-Dong Wu

Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada and

State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240*, China*

In quantum cryptography, to maximize secure transmission distance and remove detector side attacks, physicists use the measurement-device-independent (MDI) method [1], which has been experimentally realized [2]. In MDI quantum key distribution, anyone participating in the quantum communication connects to an untrusted party, who is not a legitimate member in the quantum communication. The secure communication relies on the untrusted party's measurement. So attacks on measurement devices are moved from legitimate members' sides to the untrusted party's side.

In this paper [3], we investigate quantum cryptography with continuous variable (CV). Our protocol utilizes squeezed state of light and homodyne measurement to maximize the secret key rate. Some experiments on CV squeezed states have been done [4, 5], indicating that CV quantum communication based on the squeezed state can be realized.

We design two kinds of CV MDI tripartite quantum communication protocols. One is quantum cryptographic conference (QCC) [6] and the other is quantum secret sharing (QSS) [7]. QCC enables each individual within a specific group to decrypt the encrypted messages published by any group member, whereas nobody outside the group can successfully decrypt the secret messages. QSS enables an authorized group of people to decrypt the secret messages by collaboration, but any unauthorized group of people fails to decrypt the messages.

Both QSS and QCC protocols rely on the post-processed Greenberger-Horne-Zeilinger (GHZ) state. In the entanglement-based (EB) scheme in Fig. 1, three legitimate members in communication, Alice, Bob, and Charlie, are connected with a fourth, untrusted person David. The secure communication relies on David's measurements, which removes any detector side attack in Alice's, Bob's, and Charlie's sides.

We solve the security of both QSS and QCC against two kinds of attacks: one is the entangling cloner attack and the other is the coherent attack. The entangling cloner attack is a practical individual attack, and the coherent attack is the optimal attack Eve can implement.

Fig. 2 shows the independent entangling cloner attack in each channel. Eve owns three independent EPR pairs, i.e., three two-mode squeezed states. He injects one mode of each EPR pair into the channel, through a beam splitter, and stores all the ancillary modes in the quantum memory.

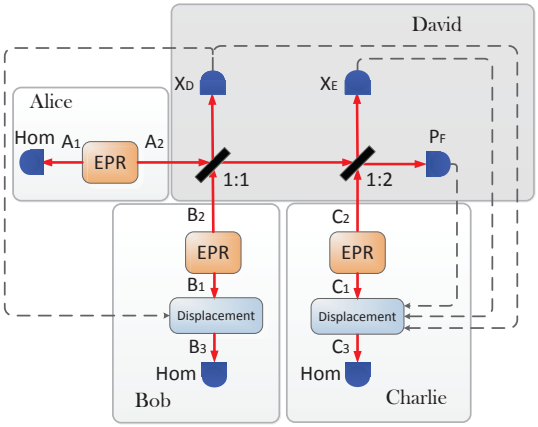

FIG. 1: EB scheme

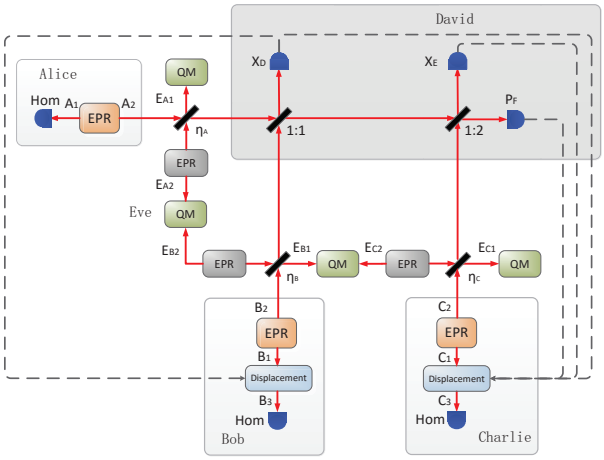

FIG. 2: EB scheme against independent entangling cloner attacks.

Fig. 3 shows a coherent attack in three channels. Eve takes three qumodes out of his globally pure ancillary Gaussian state, and injects them into three channels through beam splitters, respectively. The output states coming out of the beam splitters and the remaining ancillary qumodes are all stored in Eve's quantum memory.

We simulate the security of both QCC and QSS schemes against these two kinds of attacks. The simulation results show that under independent entangling cloner attacks, the total maximal transmission distances can be significantly enlarged when the transmission distances from Alice, Bob and Charlie to David are unbalanced. Under coherent attacks, the maximal transmission distances are markedly reduced. By comparing different coherent attacks, we finally obtain the optimal coherent attacks in QCC and QSS.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grants No. 61475099, No. 61102053, No. 61379153, and No. 61378012), Program of State Key Laboratory of Quantum Optics and Quantum Optics Devices (Grant No. KF201405), and Open Fund of IPOC

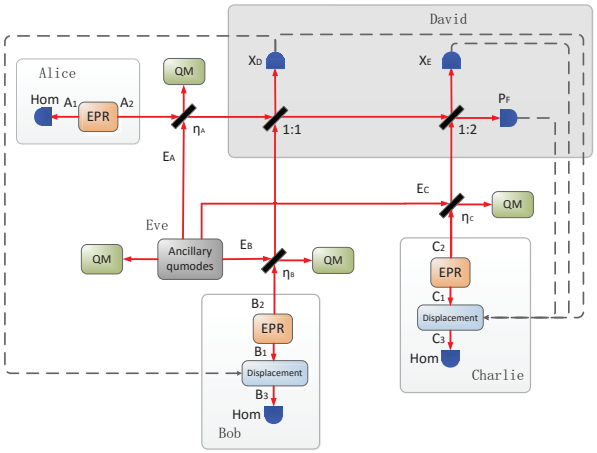

FIG. 3: EB scheme against a coherent attack

(BUPT) (Grant No. IPOC2015B004).

---

[1] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[2] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).

[3] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, Phys. Rev. A **93**, 022325 (2016).

[4] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nat. Commun. **3**, 1083 (2012).

[5] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014).

[6] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).

[7] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).