Eavesdropping or Disrupting a Communication — On the Weakness of Quantum Communications

Zhengjun Cao

Abstract

What is the behavior of an adversary to launch attacks against a communication? The good choice is to eavesdrop the communication such that the communicators can not detect the eavesdropping. The general choice is to disrupt the communication at low cost, say, measuring the transferred quantum signals in the well-known BB84 quantum key distribution protocol. The bad choice is to disrupt it at even high cost, such as severing copper or fiber, if it is necessary. In this note we remark that a quantum communication is very vulnerable to low cost attacks. The plan to build a large quantum photonic network is infeasible.

1 Introduction

In daily life, illegal eavesdropping is everywhere. Should we tolerate eavesdropping or eradicate it?

For a general communication, the first thing we are concerned, is to ensure that the receiver can obtain the proper transmissions. The second thing is to prevent an adversary from recovering plaintext. Classical cryptography assumes that an adversary has complete access to the communications between the sender and receiver. That is, it tolerates eavesdropping. Whereas, quantum cryptography (mainly quantum key distribution) can detect eavesdropping at the expensive of giving up communications.

The advantage that quantum cryptography can prevent an adversary from obtaining any useful information has attracted much attention [1-18]. It was reported that scientists at the Max Planck Institute of Quantum Optics have successfully created the world's first quantum network. Recently, EPSRC has funded a new research which aimed to build the world's biggest quantum photonic network [8]. The news of quantum teleportation hit us one after another. But we here stress the researchers neglect the fact that the fragility of a quantum communication makes it unpractical. Those experiments [9-18] did not show us how to ensure a successful quantum communication in

[0] Department of Mathematics, Shanghai University, Shanghai, China. caozhj@shu.edu.cn

the scenario of having low cost attacks. Compared to a classical communication, in fact, a quantum communication is too weak to resist common passive attacks.

2 Protect a communication from passive attacks or active attacks

People can try various ways to attack a communication (not a cryptographic protocol). Someone not involved in the communication can eavesdrop it. This is called a passive attack because the attacker does not affect the communication. All he can do is to monitor the communication and attempt to gain information. In general, eavesdroppers are assumed to have complete access to the communications between the sender and receiver. Classical cryptographic protocols try to prevent passive attacks from recovering plaintext. They can detect cheating rather than eavesdropping. More precisely, *communicators can accomplish a classical communication in the scenario of having* ***passive*** *attacks.*

Alternatively, an attacker could try to affect the communication to his own advantage. He could pretend to be someone else, introduce new messages, delete existing messages, substitute one message for another, replay old messages, interrupt a communication's channel, or alter stored information in a computer. These are called active attacks [19], because they require active intervention. In general, it is very hard to accomplish a classical communication in the scenario of having active attacks.

In 1984, Bennett and Brassard [20] developed the first quantum cryptographic protocol, BB84 quantum key distribution. The protocol depends on the quantum property that information gain is only possible at the expense of disturbing the signal if two quantum states we are trying to distinguish are not orthogonal. This can be used to detect eavesdropping in quantum key distribution. Notice that *communicators can* ***not*** *accomplish a quantum communication in the scenario of having* ***passive*** *attacks.*

In view of the above difference between a classical communication and a quantum communication, one should ask whether we can efficiently prevent an adversary in real life from launching low cost attacks against a quantum communication. The answer is definitely NO.

The merit that quantum key distribution can detect eavesdropping is heavily advertised in the past decades. Little attention was given to the weakness that a quantum communication is very vulnerable to low cost attacks. Researchers neglected the fact that communicators using a quantum channel can do nothing in the scenario of having passive attacks.

3 Eavesdropping or disrupting a communication

What is the behavior of an adversary to launch attacks against a communication? A passive adversary shall eavesdrop the communication. An active adversary may alter or delete information on an unsecured channel. More explicitly, an adversary has the following choices:

- The good choice is to eavesdrop the communication such that the communicators are not able to detect the eavesdropping.
- The general choice is to disrupt the communication at low cost, say, measuring the transferred quantum signals in the well-known BB84 quantum key distribution protocol.
- The bad choice is to disrupt the communication at even high cost, such as severing copper or fiber, if it is necessary.

In practice, it is reasonable to assume that an adversary has no intention to disrupt a communication if he can eavesdrop the communication such that the communicators can not detect the eavesdropping. To the contrary, an adversary probably disrupt a communication if he is not able to obtain the signals transferred via a communication channel. Based on this premise, we point out that there is a big difference between a classical communication channel and a quantum communication channel if there is an adversary (see Table 1). From the practical point of view, a quantum communication channel is very vulnerable to passive attacks because communicators have to give up communications once eavesdropping happens. More seriously, an adversary who want to disrupt a communication needs only to simply measure the transferred signals over a quantum channel. For a classical channel, however, an adversary has to pay high cost for disrupting a communication, say, severing copper or fiber.

Table 1: cost for disrupting communications

	classical communication	quantum communication
cost of disruption	high (active attack)	low (passive attack)

4 For a classical communication, eavesdropping $\neq$ disrupting

The main strength of classical cryptography is to keep the plaintext (or the key, or both) secret from adversaries. Adversaries are assumed to have complete access to the communications between the sender and receiver. We here always assume that eavesdropping a classical communication does not imply disrupting it.

A classical channel is robust because it is able to ensure normal communications even if there exists an eavesdropper. In nature, the security of a classical communication using classical cryptographic protocols is based on intellectual intractability.

5 For a quantum communication, eavesdropping = disrupting

Quantum cryptography makes use of the natural uncertainty of quantum world. With it, you can create a communication channel where it is impossible to eavesdrop without disturbing the transmission over it. Of course, communicators have to give up a quantum communication once eavesdropping takes place, because eavesdropping a quantum communication does imply disrupting it. As for this property, we refer to the well-known BB84 protocol.

A quantum channel is too fragile to resist any physical attacks. It is not able to ensure normal communications if there exists an eavesdropper. In nature, the security of a quantum communication using quantum cryptographic protocols is based on physical intractability.

6 Conclusion

The functionality of a quantum communication channel, in some sense, is just like that of invisible ink. A quantum channel could be referred to as inmeasurable channel. We think it is impossible to ensure us absolute information security as claimed. The plan to build a large quantum photonic network is infeasible.

References

[1] Bennett C.H., et al.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys.Rev.Lett. 70, 1895-1899 (1993)

[2] Jennewein T., et al.: Quantum Cryptography with Entangled Photons. Phys.Rev.Lett. 84, 4729-4732 (2000).

[3] Kim Y.H., et al.: Quantum teleportation of a polarization state with a complete bell state measurement. Phys.Rev.Lett. 86, 1370 (2001).

[4] Riebe M., et al.: Deterministic Quantum Teleportation with Atoms. Nature 429, 734-737 (2004)

[5] Lee, Noriyuki, et al.: Teleportation of Nonclassical Wave Packets of Light. Science 332 (6027): 330-333. Retrieved 2011-04-26.

[6] Rideout D., et al.: Fundamental quantum optics experiments conceivable with satellitesreaching relativistic distances and velocities. Class. Quantum Grav. 29 224011 (2012)

[7] Nolleke C., et al.: Efficient Teleportation Between Remote Single-Atom Quantum Memories, Phys.Rev.Lett. 110, 140403 (2013)

[8] Walmsley I.A.: Building Large Quantum States out of Light, EPSRC Reference: EP/K034480/1. http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/K034480/1

[9] Mattle K., et al.: Dense Coding in Experimental Quantum Communication. Phys.Rev.Lett. 76, 4656-59 (1996)

[10] Bouwmeester D., et al.: Experimental Quantum Teleportation. Nature, 390, 575 (1997)

[11] Boschi D., et al.: Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. Phys.Rev.Lett. 80, 6, 1121 (1998)

[12] Pan J.W., et al.: Experimental Realization of Freely Propagating Teleported Qubits. Nature 421, 721-725 (2003)

[13] Ursin R.: Quantum teleportation across the Danube. Nature, 430, 849 (2004). Retrieved 2010-05-22.

[14] Peng C.Z., et al.: Experimental free-space distribution of entangled photon pairs over 13Km towards satellite-based global quantum communication. Phys.Rev.Lett. 94, 150501 (2005)

[15] Olmschenk S., et al.: Quantum Teleportation between Distant Matter Qubits, Science 323, 486 (2009)

[16] Jin X.M.: Experimental free-space quantum teleportation. Nature Photonics, 4, 376-381 (2010)

[17] Ma X.S., et al.: Quantum teleportation over 143 kilometres using active feed-forward. Nature, 489,269-273 (2012)

[18] Yin J., et al.: Quantum teleportation and entanglement distribution over 100-kilometre free-space channels, Nature, 488,185-188(2012)

[19] Menezes A., Oorschot P., Vanstone S.: Handbook of Applied Cryptography. CRC Press (1996)

[20] Bennett C., Brassard G.: Quantum cryptography:Public key distribution and coin tossing, Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, Los Alamitos, CA), pp. 175-179 (1984)