Comment on Quantum Cryptography—Which is More Important, Signal Security, Information Security or Communication Reliability

Zhengjun Cao[1,*], Zhenfu Cao[2]

Abstract. Signal security aims to prevent the adversary from copying communication signals—so it is with quantum cryptography. Information security focuses on preventing the adversary from knowing plaintext or cheating users—so it is with classical cryptography. Communication reliability means that the intended receiver can recover the right communication signals sent by the sender.

In this note, we stress that in the presence of an adversary quantum cryptography can do nothing except for detecting the presence, because the intrusion of adversary has to disturb communication signals so that the intended receiver can not recover the right signals. But classical cryptography works well in the presence of eavesdropping although it cannot detect it. We also remark that in the past decades the functionality of quantum cryptography to detect eavesdropping has been overstated. The plan to build a large quantum photonic network is infeasible.

Keywords. Signal security, information security, communication reliability, quantum communication, eavesdropping, confidentiality, authentication.

1 Communication signals

Communication signals may describe a wide variety of physical phenomena, such as the patterns of variation over time in the source and capacitor voltages in a simple RC circuit, acoustic pressures in a speech and brightness of a picture [15]. Signals are represented mathematically as functions of one or more independent variables. For example, a speech signal can be represented mathematically by acoustic pressure as a function of time and a picture can be represented by brightness as a function of two spatial variables.

Modern communication uses channels to transmit signals. Typical transmission channels [10] include telephone lines, high-frequency radio links, telemetry links, microwave links, satellite links,

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

[2]Software Engineering Institute, East China Normal University, Shanghai, China.

and so on. Typical storage media include semiconductor memories, magnetic tapes, drums, disk files, optical memory units, and so on. Each of these examples is subject to various types of noise disturbances. For example, on a telephone line, the disturbance may come from switching impulse noise, crosstalk from other lines, or lightning. On magnetic tape, surface defects are regarded as a noise disturbance.

2 Communication reliability

In 1948, Shannon [19] proved that reliable communication (the intended receiver can recover the right signals sent by the sender) over a noisy transmission channel can be achieved if one chooses proper encoding and decoding techniques. Here noises are considered to be natural, not artificial (introduced by adversaries). A typical transmission system may be represented by the following Figure 1.

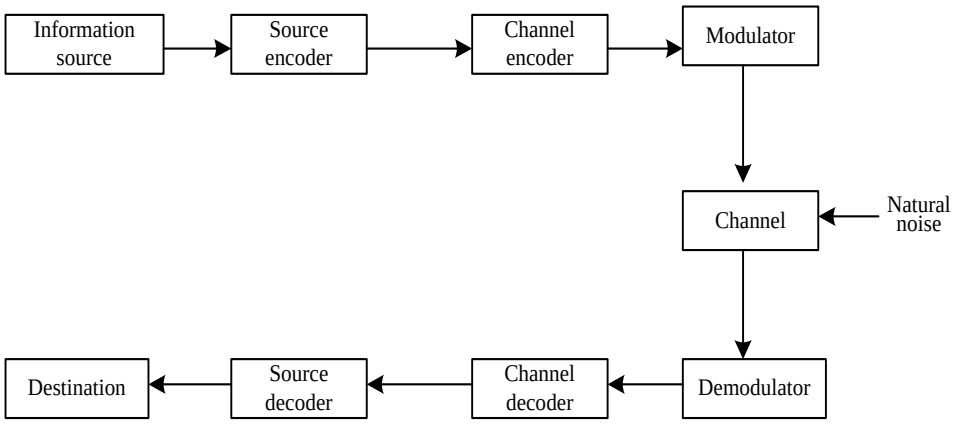

Figure 1: A typical transmission system aims at communication reliability

3 Information security

Information security has many goals according to situations, requirements, attacker's strategies [4], and so on. It focuses mainly on preventing the adversary from knowing plaintext or cheating users. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality and authentication [11].

Basically, one communication system has two essential tasks: communication reliability and information security. Obviously, a system is useless if the intended receiver cannot always recover the right signals. That means communication reliability comes first, not information security, although it has become the focus of our concern. We observed that this principle was so conspicuous that it has been rarely mentioned in literatures and nearly neglected by quantum cryptography

community.

A practical transmission system may be represented by the following Figure 2.

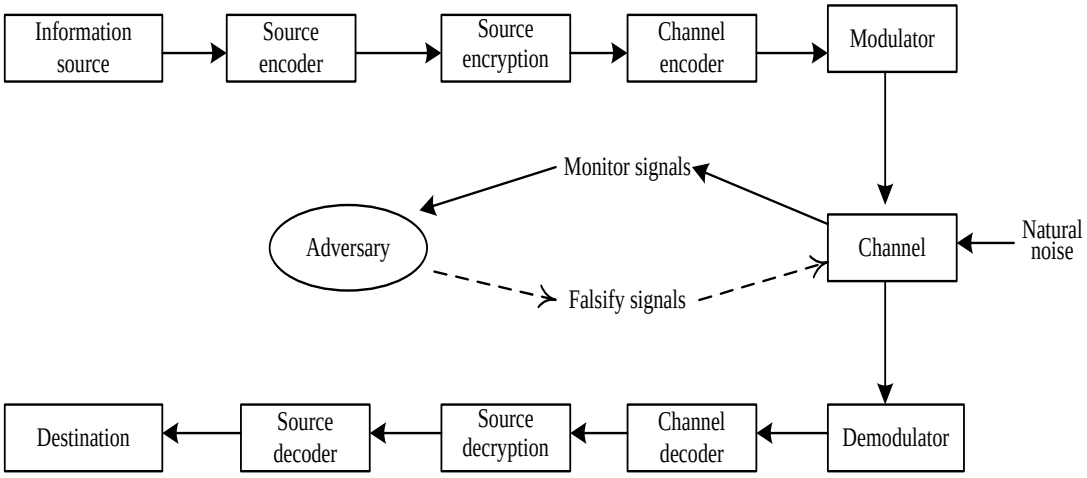

Figure 2: A practical transmission system aims at communication reliability and information security

4 Classical cryptography aims at information security

Classical cryptography aims to prevent the adversary from recovering the embedded information in communication signals or from cheating users. It assumes that an adversary can almost completely eliminate the artificial noises induced by him when he is eavesdropping on transmissions, because electromagnetic signals can be efficiently measured and copied. So, it cannot detect the presence of eavesdropping. But measures are available to prevent the eavesdropper from knowing the embedded information. Encryption which renders data unintelligible is a technique used to keep the content of information from all but those authorized to have it. Traditionally, eavesdropping is viewed as a typical passive attack. It does not reduce the communication reliability.

Instead, active attacks involving some modification of the data stream or the creation of a false stream do greatly reduce or totally ruin the communication reliability. In such case, the artificial noises (falsified signals) are deliberately introduced by adversaries. The intended receiver cannot recover the right signals sent by the sender. But we can protect the receiver from cheating by other techniques, such as digital signature and zero-knowledge proof [11]. Note that it is quite difficult to prevent active attacks absolutely because of various potential physical, software, and network vulnerabilities.

5 Quantum cryptography aims at signal security

In 1984, the work of Bennett and Brassard [2] motivated the research on quantum cryptography, mainly referring to quantum key distribution (QKD) [3, 12–14, 16–18, 21, 22]. The study is based on the fact that nobody can clone an unknown quantum state (No-cloning Theorem).

Quantum cryptography aims to prevent the adversary from copying communication signals. Thus an eavesdropper who tries to intercept the message has to disturb transmitted quantum signals. The sender and the intended receiver can detect eavesdropping by checking the inconsistence of their quantum states in the later public discussion [2].

We here would like to stress that quantum cryptography gains the ability to detect eavesdropping at the expense of communication reliability. Once an adversary gets involved in one quantum communication system (even though he is monitoring), the intended receiver cannot recover the right quantum signals sent by the sender.

We now make a comparison between classical cryptography and quantum cryptography according to attacks launched by an adversary (see Table 1).

	Adversary's attacks		Goals of information security		Communication reliability
Classical cryptography	Monitor signals	**enabled**	Confidentiality	detect the adversary	**Yes**
			enabled	**No**	
	Falsify signals	enabled	Authentication	detect the adversary	No
			enabled	Yes	
Quantum cryptography	Monitor signals	**disenabled**	Confidentiality	detect the adversary	**No**
			enabled	**Yes**	
	Falsify signals	enabled	Authentication	detect the adversary	No
			enabled	Yes	

Table 1: The differences between classical cryptography and quantum cryptography in the presence of adversary

6 Signal security is incompatible with communication reliability in the presence of eavesdropping

If communication signals cannot be copied by the adversary, then he cannot extract the information embedded in the signals. That is to say, signal security inherently implies information security. But this does not mean that signal security is more important than information security. In fact, signal security usually ruins communication reliability in the presence of adversary, i.e., it is not compatible with communication reliability. As for this point, readers can refer to the details of BB84 protocol [2].

The relationships between signal security, information security and communication reliability in the presence of eavesdropping can be described as follows (see Figure 3). It is easy to see that from the practical point of view the integration of information security and communication reliability is more desirable, not the sole signal security.

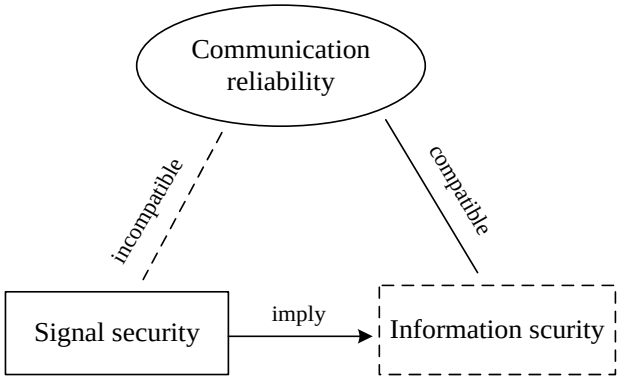

Figure 3: The relationships between signal security, information security and communication reliability in the presence of eavesdropping

In the past decades, the capability of quantum cryptography to prevent an adversary from monitoring quantum signals has been overstated. Meanwhile, the weakness that a quantum communication system cannot support a reliable communication has been rarely discussed. For example, in a recent report [18], the authors claimed that they found a more practical QKD scheme. Taking a close look at the QKD scheme, we find it is just a variation of BB84 protocol [2]. Unlike BB84 protocol in which each bit is encoded in isolation, the new method encodes bits correlatively. Its advantage over the previous works is that an eavesdropper cannot detect a bit without knowing the whole string. Essentially, it proposed a more secure QKD scheme, instead of a more reliable quantum communication system.

7 The threat to classical cryptography might be dissolving

In the past, the threat of Shor's algorithm [20] to classical cryptography, especially to public key cryptography, has been overstated despite the fact that the experimental demonstrations of Shor's algorithm for factoring 15 were falsely claimed and flawed [7]. Amusingly, there are still much quarrelling about what is called a quantum computer.

On May 11, 2011, D-Wave Systems [8] announced the D-Wave One, labeled "the world's first commercially available quantum computer." The company claims this system uses a 128 qubit processor chipset. In early 2012 D-Wave Systems revealed a 512-qubit quantum computer. In January 2014, researchers at UC Berkeley and IBM published a classical model explaining the D-Wave machine's observed behavior, suggesting that it may not be a quantum computer [1]. In May 2014, researchers at D-Wave, Google, USC, Simon Fraser University, and National Research Tomsk Polytechnic University published a paper containing experimental results that demonstrated the presence of entanglement among D-Wave qubits [9].

Historically speaking, Shor's factoring algorithm is the main impetus of developing quantum computers. In some senses, a computer could be called a "quantum computer" only if it is able to factorize large integers by running Shor's factoring algorithm. We believe it is a universally acceptable standard to certify a quantum computer using Shor's factoring algorithm. But it is a pity, D-Wave has no intention to use so-called quantum computers to run Shor's algorithm so as to certify these machines. The increasing evidences suggest that Shor's algorithm might be a false threat [5–7] to modern public key cryptosystems, such as RSA and ElGamal.

8 Conclusion

We think that the study of quantum communication is led astray by some teams or researchers. They ignored that the ultimate goal of setting up a communication system was to provide users with reliable communications. For most communications such as a conventional greeting and a daily conversation, the major problem is reliability, not security. We think it is unreasonable to trade off communication reliability for information security. Naturally speaking, quantum cryptography is putting the cart before the horse. In view of this, we would like to point out that the plan to build a large quantum photonic network is infeasible.

Acknowledgements. This work is supported by the National Natural Science Foundation of China (Project 61303200, 61411146001), and the Shanghai Leading Academic Discipline Project (S30104).

References

[1] T. Albash, et al.: Consistency Tests of Classical and Quantum Models for a Quantum Annealer, http://arxiv.org/abs/1403.4228

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

[3] D. Bouwmeester, et al.: Experimental quantum teleportation. Nature, 390, 575 (1997).

[4] Z.J. Cao: Eavesdropping or Disrupting a Communication - On the Weakness of Quantum Communications. IACR Cryptology ePrint Archive 2013: 474 (2013)

[5] Z.J. Cao and Z.F. Cao: On Shor's Factoring Algorithm with More Registers and the Problem to Certify Quantum Computers. IACR Cryptology ePrint Archive 2014: 721 (2014).

[6] Z.J. Cao, Z.F. Cao and L.H. Liu: Remarks on Quantum Modular Exponentiation and Some Experimental Demonstrations of Shor's Algorithm. IACR Cryptology ePrint Archive 2014: 828 (2014).

[7] Z.J. Cao, Z.F. Cao and L.H. Liu: Comment on Demonstrations of Shor's Algorithm in the Past Decades. IACR Cryptology ePrint Archive 2015: 1207 (2015).

[8] http://en.wikipedia.org/wiki/D-Wave_Systems

[9] T. Lanting, et al.: Entanglement in a Quantum Annealing Processor. Physical Review X 4, 021041 (2014). https://journals.aps.org/prx/pdf/10.1103/PhysRevX.4.021041

[10] S. Lin and D. Costello. Error control coding, fundamentals and applications. Prentice-Hall International, Inc. (1983).

[11] A. Menezes, P. Oorschot and S. Vanstone: Handbook of applied cryptography (1996).

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

[13] C. Nolleke, et al.: Efficient teleportation between remote single-atom quantum memories, Phys.Rev.Lett. 110, 140403 (2013).

[14] S. Olmschenk, et al.: Quantum teleportation between distant matter qubits, Science, 323, 486 (2009).

[15] A. Oppenheim, A. Willsky and S. Nawab. Signals & Systems. Prentice-Hall International, Inc. (1997).

[16] J.W. Pan, et al.: Experimental realization of freely propagating teleported qubits. Nature, 421, 721-725 (2003).

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

[18] T. Sasaki, Y. Yamamoto, M. Koashi: Practical quantum key distribution protocol without monitoring signal disturbance. Nature, 509, 475-478 (2014).

[19] C. Shannon: A mathematical theory of communication, Bell System Technical Journal, 27 (1948).

[20] P. Shor: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26 (5): 1484-1509 (1997).

[21] R. Ursin: Quantum teleportation across the Danube. Nature, 430, 849 (2004).

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