Overview of Quantum Information Technology in Satellite Networks

Yuan Gao[1,3,a], Hong Ao[1,b], Quan Zhou[1,c], Weigui Zhou[1,d] and Yi Li[2,e,*]

[1]Xichang Satellite Launch Center, Sichuan, China

[2] The High School Affiliated to Renmin University of China, Beijing, China

[3] China Defense Science and Technology Information Center, Beijing, China

[a]yuangao08@gmail.com, [b]aohong76@aliyun.com, [c]zhouquanxslc@foxmail.com, [d]wgzhou@nudt.edu.cn, [e]liyi@rdfz.cn, *Corresponding Author

Keywords: Quantum, Information Network, Satellite Network, Cooperation

Abstract. Quantum theory of information science from germination and now has nearly 30 years of history, mainly includes three aspects: (1) quantum communication can be achieved theoretically unconditionally secure transmission of information; (2) quantum computing with ultra-fast computing power; (3) quantum precision measurement. This article will present situation of quantum information science research three points summary and comparison, and gives the academician reviews, has great significance for the future development direction of quantum technology.

Introduction

Properly speaking, quantum communication should be called quantum cryptography, the main emphasis is the confidentiality of communication rather than communication process itself. The four kinds of quantum communication polarization state of light: horizontal, vertical, positive and negative 45 degrees to 45 degrees to load single-photon transmission, and then generates a key according to some sort of agreement. In this process, if an eavesdropper eavesdropping, there are several possible scenarios: one is that the eavesdropper photon "is divided into two halves", leaving half their own hands, the other half sent off. But quantum is indivisible, so this cannot be done; the second case is an identical copy of an eavesdropper photon. Due to the unknown quantum state cannot be accurately cloned copy would inevitably introduce noise, by checking the noise, in theory, have proved will be able to discover the presence of an eavesdropper. It is because quantum indivisible and cannot clone properties, can guarantee the security key in principle, if combined with one-time pad means, it is possible to achieve secure communication encrypted content cannot be deciphered. In fact, the security of confidential communications as early as 1949 by the nose Zu Xiangnong modern information theory proved: If the key is randomly generated key and the same length as the plaintext, the key is not reusable, that information cannot decipher encrypted of. In 2009, some scholars theoretically proved that as long as the establishment of causality, the security of quantum key distribution is strictly proved. So far, a physics principle of causality is strongest. Quantum key distribution security by the basic principles of physics guaranteed.

Security in Quantum Information Delivery

At present, there are a lot of teams in this respect, a more in-depth work. 2012, China in Hefei to build an experimental network covering 6000 square kilometers, basically to meet the security needs of ten thousand users key distribution, and on a small scale piloted. From 2012, China began to build a highly secured communication based on quantum communication security system, Beijing has invested in permanent operation for the 18th National Congress of the Communist Party of China in 2012 and September 3, 2015 Chinese People's Anti-Japanese War victory Day parade provides important information security.

Limited to the level of technology, the technology is currently only available in metropolitan, coverage is relatively small, and it cannot extend directly to the WAN applications. In order to further

expand the network application, China has undertaken a number of new jobs, such as in the trunk with the help of trusted, ensuring each relay node security situation, and build a large-scale communications backbone project. Thus, the transmitter and receiver are better security issues get resolved. Currently, the security of quantum key distribution is well established.

Currently China University of Technology in cooperation with the relevant units at the end of 2016 to complete the construction of stage one thousand kilometers, "the Beijing-Shanghai trunk" to promote the application of information security in the areas of finance, defense, government and so on.

Free Space Quantum Communication

Although the optical system can be used for quantum communication and quantum computing, quantum field but really want is scalable, large-scale light amount of information processing. In quantum communication inside, because the signal cannot be amplified as the traditional image signal, in the optical fiber transmission to 100 km, the signal basically had a serious decay. If the 1000 kilometers of fiber, the loss will probably reach 200dB, even if the repetition frequency of the light source and 10GHz ideal detector uses an average of every 100 years only 0.3 photon transmission, transmission distance is severely limited. The probability of entanglement sources lead to exponential growth in the consumption of resources, efficiency is greatly limited. This problem can be solved by free-space quantum communication, to overcome losses in the fiber channel inside, and free-space quantum communication technology precisely laid the foundation of innovative satellite communication technologies. Because the whole atmosphere is equivalent to about 10 km vertical ground atmosphere outside the vacuum, 80% of the light signals can penetrate the atmosphere to the ground, and there will be no attenuation of outer space. Quantum communication between heaven and earth, can extend the communication range to the world.

In 2004, China carried out to explore the free-space quantum communication work, has in 2005 and 2010 proved that photons penetrate the atmosphere in the state will not be disturbed. In 2012, China successfully in Qinghai Lake made a one hundred kilometers Experiment: This experiment with the loss of one hundred kilometers on day one thousand kilometers to the loss of almost the same proven quantum communication is possible in the high loss of satellite-ground link. 2013, to verify the feasibility of quantum communication in satellite attitude motion, the analog high-speed movement of the satellite, random vibration and high loss channel. All experiments show that the quantum communication between the satellite and the ground is possible. Now supported by Chinese Academy of Sciences, the country is implementing quantum science experimental satellite pilot projects, we are now in the development stage. The satellite is expected to launch in the first half of 2016, after successfully into orbit, it will be to achieve national's first international high-speed satellite-ground quantum communication. If you do MAN fiber, satellite terrestrial fiber optic network to connect to the formation of a wide area network, we can build earth integrated WAN quantum communication networks.

Quantum Relay in Spatial Networks

Since the satellite launch cost is relatively high, so the cost-ground solutions, namely the so-called quantum repeater technology has been proposed to solve the long-distance transmission relay problem by quantum. Quantum relay requires three technologies: quantum entanglement swapping, quantum entanglement purification and storage. These techniques can be combined to solve resource depletion and photon number probability bring consumption. Quantum repeaters can also produce more light deterministic entanglement, which itself can also be used for quantum computing and quantum simulation.

In 2008, China in the international arena for the first time a demonstration of quantum repeater node. In early 2016 the quantum storage have relatively good progress, has been able to meet the

needs of quantum repeater 600 km, but the current technology can only be achieved in Chengdu in a lab environment, to practical take some time.

On this basis, to achieve effective quantum computing and simulations need to be introduced Hamiltonian, so that these particles interacting together. However, the coupling between the photons is very weak, even if the encounter in space and almost no interaction. March 2016, China successfully captured about a few thousand atoms, it laid the foundation for the development of quantum repeater technology. In the light inside the lattice, so that the interference by the middle of one optical lattices decreased by two optical lattice tunneling can produce entanglement between atoms. After generating entanglement, we can put near the pairwise atom tunneling once again, to produce atomic entangled in the chain. At present, China has been able to generate entanglement in the two between two atoms, is expected within 10 years will produce entangled 50 atoms, but also by the action of analog electronic interaction between atoms and atoms in the electromagnetic field, with controllable way to achieve quantum simulator special sense.

Summary

China quantum communication technology has reached the world's top level, leading the United States and Europe. July 2016, the world's first quantum communication security Link "the Beijing-Shanghai route," will be built. Meanwhile, China has independently developed the world's first "quantum science experimental satellite" also launch soon.

In fact, in the country "Thirteen Five" plan proposed earlier released, quantum communication has become one of the major science and technology projects. Currently, China's metropolitan quantum cryptography technology has matured, it is possible to reach the commercial level, the future once more to achieve technological breakthroughs, and the market will be broader. Of course, from a military sense, quantum technology also has a very high potential military applications.

In short, the maturity of quantum information technology, the 21st century will bring the information technology revolution. China remained the same level with foreign countries in basic research and promote the industrialization of quantum communication, even in some areas has been the leading American and European countries. Civilian aspects of spending huge sums in some cities to establish a quantum communication network, and in early 2015 to achieve the electronic banking information files encrypted transmission between the city; the military aspects into engineering universal need three to five years. Review of researchers in the field of quantum communication for many years to pay, we can see that China is quietly rising in this area. Faced with the imminent disruptive technology revolution, China is not only a "follower", should seize the opportunity, seize the opportunity, truly achieve leapfrog development, scientific and technological progress to make quantum leader.

Acknowledgement

This work is funded by China's 973 project under grant of 2012CB316002 and China's 863 project under grant of 2013AA013603, 2012AA011402, National Natural Science Foundation of China(61201192), The Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2012D02); International Science and Technology Cooperation Program(2012DFG12010); National S & T Major Project (2013ZX03001024-004) ,Operation Agreement Between Tsinghua University and Ericsson, Qualcomm Innovation Fellowship, whose funding support is gratefully acknowledgment. The author would also like to thank all the reviewers, their suggestions help improve the work a lot.

References

[1] 10 Bar-On A, Dinur I, Dunkelman O, et al. Cryptanalysis of SP networks with partial non-linear layers. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 315–342

[2] Sun S W, Hu L, Wang P, et al. Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 158–178

[3] Emami S, Ling S, Nikoli04 I, et al. Low probability differentials and the cryptanalysis of full-round CLEFIA-128. In:Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 141–157

[4] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: an ultra-lightweight block cipher. In: Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2007. 450–466

[5] Wu W L, Zhang L. LBlock: a lightweight block cipher. In: Applied Cryptography and Network Security. Berlin: Springer, 2011. 327–344

[6] Borghoff J, Canteaut A, G¨uneysu T, et al. PRINCE-a low-latency block cipher for pervasive computing applications.In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2012. 208–225

[7] Albrecht M R, Benedikt D, Kavun E B, et al. Block ciphers-focus on the linear layer (feat. PRIDE). In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 57–76

[8] Gilbert H. A simplified representation of AES. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014.200–222

[9] Papakonstantinou P A, Yang G. Cryptography with streaming algorithms. In: Advances in Cryptology CRYPTO.Berlin: Springer, 2014. 55–70

[10] Banegas G. Attacks in stream ciphers: a survey. http://eprint.iacr.org/2014/677.pdf

[11] A˙ gren M, L¨ondahl C, Hell M, et al. A survey on fast correlation attacks. Cryptogr Commun, 2012, 4: 173–202

[12] Hell M, Johansson T, Brynielsson L. An overview of distinguishing attacks on stream ciphers. cryptogr commun, 2009, 1: 71–94

[13] Knellwolf S, Meier W. High order differential attacks on stream ciphers. Cryptogr Commun, 2012, 4: 203–215

[14] Dinur I, Shamir A. Applying cube attacks to stream ciphers in realistic scenarios. Cryptogr Commun, 2012, 4:217–232