Quantum Stream Cipher

Subjects: Quantum Science & Technology | Computer Science, Information Systems

Contributor: Hirota Osamu

Quantum cryptography includes quantum key distribution (QKD) and quantum stream cipher, but the researchers point out that the latter is expected as the core technology of next-generation communication systems. Various ideas have been proposed for QKD quantum cryptography, but most of them use a single-photon or similar signal. Then, although such technologies are applicable to special situations, these methods still have several difficulties to provide functions that surpass conventional technologies for social systems in the real environment. Thus, the quantum stream cipher has come to be expected as one promising countermeasure, which artificially creates quantum properties using special modulation techniques based on the macroscopic coherent state. In addition, it has the possibility to provide superior security performance than one-time pad cipher.

Keywords: physical cipher ; optical fiber communication ; optical satellite communication ; quantum communication theory

1. General View of Cryptography or Cipher in Social Network Systems

At first, the researchers introduce a comment on a general view of cryptography in their research project. In the recent book [1] and a technical paper [2], S. Tsujii, who is one of the leaders of the cyber security community and industry, explains the current situation of the cyber security community and industry on the current trend of the security technology, as follows. “Quantum computer capable of breaking public key cryptographies, such as RSA or elliptic curve cryptography, that relies on mathematical decipherability due to prime number factorization or discrete logarithm problems, will not be developed within 20 years. Nevertheless, the jeopardy due to the cooperative effect with the development of mathematics remains. Thus, NIST is in the process of selecting candidates for quantum computer-resistant cryptography. The applications of cryptography for confidentiality are categorized into the confidential transmission of data itself and the key delivery or storage for that purpose. Then from the viewpoint of academic methods, they are categorized into mathematical cryptography and quantum cryptography. In the former case, there are two types such as public key cryptography and symmetric key cipher. Public key cryptography has the advantage of securely delivering and storing the initial key for data encryption and transmission. However, its processing speed is slow, so symmetric key cipher is responsible for data encryption. On the other hand, quantum cryptography is a cryptographic technique that uses quantum phenomena to improve security performance. The technique that uses quantum communication to perform the key delivery function of public key cryptography is quantum key distribution (QKD: BB-84 et al.), while the technique that uses quantum communication to perform the cryptographic transmission of data itself is called Y-00 quantum stream cipher (see **Figure 1**). QKD cannot be used to supply keys to One Time Pad cipher, because its data rate is too slow. Y-00 for data encryption is extremely novel in its ability to prevent eavesdroppers from obtaining the ciphertext of the symmetric key cipher. In addition, it is amazing that the strong quantum-ness is created by modulation scheme with multi-ary coherent state signals without any quantum device”.

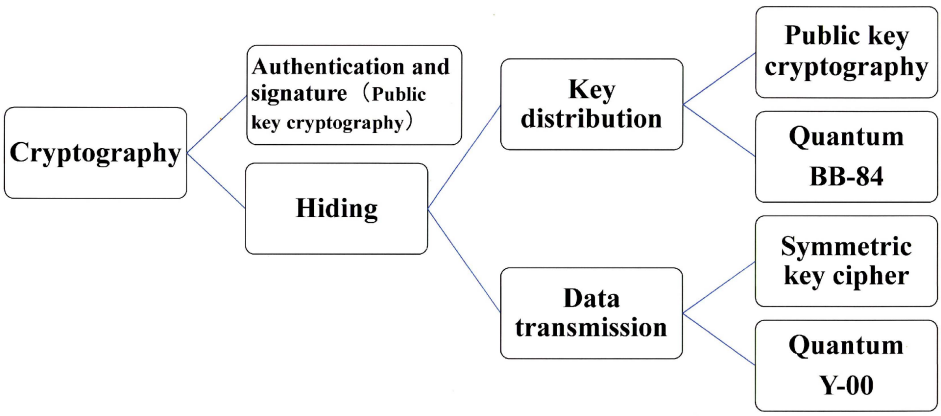

Figure 1. Classification of cryptographic techniques.

Now turn the researchers' focus to quantum cryptography. Both of these quantum technologies are based on designing communication systems to make it difficult for eavesdroppers to steal signals on the communication channels. Such a function to protect the signal itself cannot be realized by mathematical cryptography. As mentioned above, there are two possible system operation methods for these quantum cryptography techniques. One is to use BB-84 quantum key distribution for key delivery and conventional mathematical cryptography for authentication and data encryption. The other is to use Y-00 quantum stream cipher for data encryption and conventional public key cryptography (or quantum computer resistant type) for authentication and key delivery. These quantum cryptography technologies are positioned as technologies to ensure the ultimate security of communication between data center stations, that is of special importance in next-generation 5G and 6G systems. In the following, the researchers will explain the technical contents, applicability to the real world, and development trends.

2. Feature of Quantum Stream Cipher

In the near future, optical networks will move toward even higher speeds, but the Y-00 quantum stream cipher can solve technical requirement from the real world.

2.1. Basic Scheme

As explained in the previous section, the quantum stream cipher is expected to accelerate advanced application in future communication systems. The reason for this is that this scheme can utilize ordinary optical communication devices and is compatible with existing communication systems. In its design, optical communication, quantum theory, and cryptography are effectively integrated. Therefore, it is also called “Y-00 optical communication quantum cryptography” in implementation studies. Pioneering research on practical experiment for this system has been reported by Northwestern University [3][4], Tamagawa University [5], and Hitachi Ltd. [6]. Theories of system design for the basic system have been given by Nair and others [7][8][9][10].

Let the researchers explain the principle of Y-00 quantum stream cipher. First, the Y-00 protocol starts by specifying the signal system that use the transmission medium. The actual signal to be transmitted is selected in terms of amplitude or intensity, phase, quadrature amplitude, etc., having coherent state $|\alpha\rangle$

in quantum optics. Then, the design is made accordingly. Depending on the type of signal to be used, it is called ISK:Y-00, PSK:Y-00, QAM:Y-00, etc.

Here, one communication base consisting of various binary signals is randomly selected for each data slot. Then, a binary data is transmitted by using the communication base selected. Thus, ultra-multi-valued signals appear to be transmitted on the channel. The eavesdropper has to receive the ultra-multi-valued signal, because they do not know which communication base was selected.

2.2. Progress in Security Theory

The BB-84 protocol is a key delivery technique for securely sharing secret key sequences (random numbers). The Y-00 protocol is a symmetric key stream cipher technique for cryptographically transmitting data. As mentioned above, both quantum cryptography techniques enhance security by preventing eavesdroppers from taking the exact signal on the communication channel. The models that explains the principle of such physical technology is called the “basic model”. It is this basic model that can be found in textbooks for beginners.

Let the researchers start with a QKD, such as BB-84. If the basic model of the BB-84 protocol is implemented in a real optical fiber communication system, then it can be eavesdropped. Therefore, in order to guarantee security even in systems with noise and energy loss, a technique that combines error correction and privacy amplification (universal hashing) was proposed, and then a theoretical discussion of security assurance became possible. That is, in 2000, P. Shor, et al. [11] proposed a mathematical security theory for BB-84 on an abstract mathematical model called the Shor model, which was later improved by R. Renner [12]. In brief, the security of the BB-84 protocol is evaluated by quantifying quantum trace distance of the two density operators to the ideal random sequence and the random sequence shared by the real system. This is the current standard theory for the security of QKD. It is very difficult to realize a real system that the quantum trace distance is sufficiently small.

On the other hand, from the beginning, the Y-00 protocol can consider the effects of non-ideal communication systems. As mentioned at the above section, the selection of communication base of the Y-00 protocol is encrypted by conventional mathematical cipher. The Y-00 quantum ciphertext, which is an optical signal, is emitted as the transmission signal. So,

the ciphertext of the mathematical symmetric key cipher that an eavesdropper needs to decipher corresponds to the Y-00 quantum ciphertext. However, since the set of ultra-multi-valued signals, which is Y-00 quantum ciphertext, are a non-orthogonal quantum state ensemble, their received signals are inaccurate due to errors caused by quantum noise. Therefore, the discussion based on the computational security of the mathematical cryptographic part of Y-00 mechanism to be attacked is replaced by the problem of combination of information theoretic analysis and computational analysis. However, the researchers should emphasize that the discussion with infinite number or asymptotic theory are not their concern, because their concern is a physical system under practical situation. For example, if an attacker needs circuits of the number of the size of the universe to perform the brute-force attack, the system is unbreakable. Or, if an attacker needs 100 years to collect the ciphertext for trying the cryptoanalysis, it is also impractical and unbreakable.

3. Concrete Applications of Quantum Stream Cipher

As mentioned above, the Y-00 quantum stream cipher has not yet reached its ideal performance, but in practical use, it has achieved a high level of security that cannot be achieved with conventional techniques, and it can be said that the ciphers are now at a level where they can be introduced to the market. To date, the development of transceiver for the Y-00 quantum stream cipher has been funded by the university president's discretionary fund, as well as external funds from the Ministry of Education, Science and Technology (MEXT), and the Defense Acquisition Agency (DEA). Here, the researchers introduce examples of the use case of the Y-00 quantum stream cipher.

3.1. Optical Fiber Communication

Large amounts of important data are instantaneously exchanged on the communication lines between data centers where various data are accumulated. It is important from the viewpoint of system protection to eliminate the risk that the data are copied in their entirety from the communication channel. The researchers believe that the Y-00 quantum stream cipher is the best technology for this purpose (see **Figure 2**). On the other hand, this technology can be used for optical amplifier relay system. Hence, it can apply to the current optical communication systems. Transceivers capable of cryptographic transmission at speeds from one Gbit/s to 10 Gbit/s have already been realized, and by wavelength division multiplexing, a 100 Gbit/s system has been tested. Furthermore, communication distances of 1000 km–10,000 km have been demonstrated. In offline experiments, 10 Tbit/s has been demonstrated. In general, a dedicated line such as dark fiber is required. If the researchers want to apply this technology to network function, then the researchers need the optical switching technology developed by the National Institute of Advanced Industrial Science and Technology (AIST). Thus, in collaboration with AIST and other organizations, the researchers have successfully demonstrated the feasibility of using the Y-00 transceiver in testbed optical switching systems. Furthermore, **Figure 3** shows the recent activities of the experimental research group at Tamagawa University towards practical application to the real world [13][14][15][16][17][18][19][20].

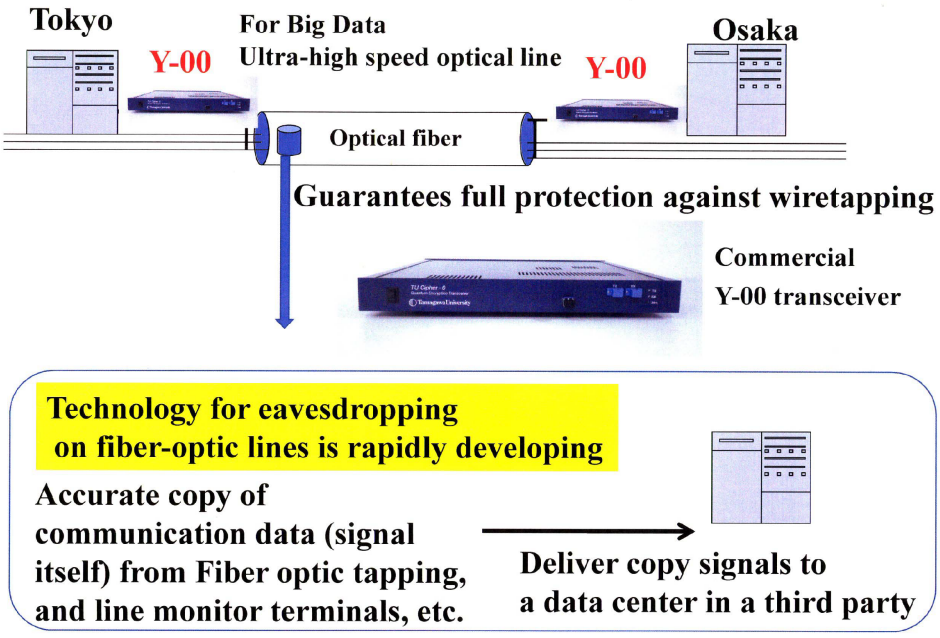

Figure 2. Application to data center communication security (protection against eavesdropping, tampering, and virus injection from communication lines). Commercial transceiver is for 1 Git/s optical ethernet. This can be mass produced.

F.Futami:
***Optics Express*, vol-25, no-26, 33338, 2017**
***IEEE/OSA Journal of Lightwave Technology*, vol. 38, no. 10, pp. 2773-2780, May. 2020.**

K.Tanizawa:
***IEEE Photonics Technology Letters*, vol. 30, no. 22, pp. 1987-1990, Nov.2018.**
***Optics Express*, vol. 27, iss. 18, pp. 25357-25363, Sep. 2019.**
***Optics Express*, vol. 27, iss. 2, pp. 1071-1079, Jan. 2019.**
***Optics Express*, vol. 29, iss. 4, pp. 5658-5664, Feb. 2021.**
***Optics Express*, vol. 29, iss. 7, pp. 10451-10464, Mar. 2021.**
***IEEE/OSA Journal of Lightwave Technology*, vol. 38, no. 16, pp. 4244-4249, Aug. 2020.**

Figure 3. Recent activities of experiment of Y-00 quantum stream cipher at Tamagawa University.

3.2. Optical Satellite Communication

The Y-00 quantum stream cipher, which was developed for fiber-optic communications, can also be applied to satellite communications. In satellite communication applications, the rate of operation is an important factor because communication performance depends on the weather conditions. With QKD, it is difficult to keep communications up and running except on clear-air nights. In the case of Y-00, communication by any satellite system can be almost ensured when the weather is clear. In case of bad weather, the effects of atmospheric turbulence and scattering phenomena need to be considered. The researchers are currently analyzing the performance of the system in such cases at 10 Gbps operation [21].

3.3. Optical Communication from Base on the Moon to Earth

The Japanese government has initiated a study to increase the user transmission rate of optical space communications from 1.8 Gbps to more than 10 Gbps. Furthermore, in the future, the government aims to achieve higher transmission rates in ultra-long-distance communications required for lunar and planetary exploration. This plan is called LUCAS. The researchers have started to design for an implementation of 1 Gbps communication system at a transmission distance of 380,000 km between the Moon and the Earth using the high-speed performance of the Y-00 quantum stream cipher.

References

1. Tsujii, S. The Fight against Fakes; Kotoni Publishing Co.: Chiba Prefecture, Japan, 2021.
2. Hirota, O.; Tsujii, S. Quantum noise analysis for quantum computer. IEICE Jpn. Tech. Rep. Inf. Theory 2021, 121, 28–33.
3. Borbosa, G.A.; Corndorf, E.; Kumar, P.; Yuen, H.P. Secure communication using mesoscopic coherent states. Phys. Rev. Lett. 2003, 90, 227901.
4. Kanter, G.S.; Reillly, D.; Smith, N. Practical physical layer encryption:The marriage of optical noise with traditional cryptography. IEEE Commun. Mag. 2009, 47, 74–81.
5. Hirota, O.; Sohma, M.; Fuse, M.; Kato, K. Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme. Phys. Rev. A 2005, 72, 022335.
6. Ohhata, K.; Hirota, O.; Honda, M.; Akutsu, S.; Doi, Y.; Harasawa, K.; Yamashita, K. 10 Gbit/s optical transceiver using the Yuen 2000 encryption protocol. IEEE. J. Lightw. Technol. 2010, 28, 2714–2723.
7. Nair, R.; Yuen, H.P.; Corndolf, E.; Kumar, P. Quantum noise randomized ciphers. Phys. Rev. A 2006, 74, 052309.
8. Hirota, O.; Kurosawa, K. Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol. Quantum Inf. Process. 2007, 6, 81–91.
9. Hirota, O. Practical security analysis of quantum stream cipher by Yuen protocol. Phys. Rev. A 2007, 76, 032307.

10. Yuen, H.P. Key generation: Foundation and new quantum approach. IEEE Sel. Top. Quant. Electron. 2009, 15, 1630–1645.
11. Shor, P.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 2000, 85, 441.
12. Renner, R. Security of quantum key distribution. Int. J. Quantum Inf. 2008, 6, 1.
13. Futami, F.; Guan, K.; Gripp, J.; Kato, K.; Tanizawa, K.; Chandrasekhar, S.; Winzer, P.J. Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM. Opt. Express 2017, 25, 33338.
14. Futami, F.; Tanizawa, K.; Kato, K. Y-00 quantum-noise randomized stream cipher using intensity modulation signals for physical layer security of optical communications. IEEE/OSA J. Lightw. Technol. 2020, 38, 2773–2780.
15. Tanizawa, K.; Futami, F. 214 intensity-level 10-Gbaud Y-00 quantum stream cipher enabled by coarse-to-fine modulation. IEEE Photonics Technol. Lett. 2018, 30, 1987–1990.
16. Tanizawa, K.; Futami, F. Digital coherent PSK Y-00 quantum stream cipher with 217 randomized phase levels. Opt. Express 2019, 27, 1071–1079.
17. Tanizawa, K.; Futami, F. Single channel 48-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF. Opt. Express 2019, 27, 25357–25363.
18. Tanizawa, K.; Futami, F. Quantum noise-assisted coherent radio-over-fiber cipher system for secure optical fronthaul and microwave wireless links. IEEE/OSA J. Lightw. Technol. 2020, 38, 4244–4249.
19. Chen, X.; Tanizawa, K.; Winzer, P.; Dong, P.; Cho, J.; Futami, F.; Kato, K.; Melikyan, A.; Kim, K.W. Experimental demonstration of 4,294,967,296-QAM based Y-00 quantum stream cipher template carrying 160-Gb/s 16-QAM signals. Opt. Express 2021, 29, 5658–5664.
20. Tanizawa, K.; Futami, F. Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system. Opt. Express 2021, 29, 10451–10464.
21. Hirota, O.; Kato, K.; Sohma, M. Application of Y-00 quantum stream cipher to satellite communication-Mathematical model of weather disturbance. IEICE Jpn. Tech. Rep. Inf. Theory 2022, 121, 143–148.