

Digest of Quantum Stream Cipher based on Holevo-Yuen Theory

Masaki SOHMA¹, Osamu HIROTA^{1,2}

1. Quantum ICT Research Institute, Tamagawa University
6-1-1, Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

2. Research and Development Initiative, Chuo University,
1-13-27, Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

E-mail: sohma@eng.tamagawa.ac.jp, hirotat@lab.tamagawa.ac.jp

Abstract—So far, quantum key distribution (QKD) has been the main subject in the field of quantum cryptography, but that is not quantum cryptographic communication, it is only the ability to send keys for cryptographic purposes. To complete cryptographic communication, a technique for encrypting data is necessary, and the conventional cryptographic technique of mathematical symmetric key cipher or One Time Pad (OTP) is adopted in the discussion so far. However, OTP is not the ultimate cipher for data encryption, because it does not satisfy security conditions in the modern cryptology. Around 2000, a new quantum stream cipher was proposed as a technique to challenge the possibility of overcoming drawbacks of OTP in practical use. Recently, we have published some review papers on it in *Entropy* (Open access journal) [1], and others [2,3]. This paper introduces an overview and a back ground of our paper that is entitled Quantum stream cipher based on Holevo-Yuen theory.

I. GENERAL VIEW OF CRYPTOGRAPHY OR CIPHER IN SOCIAL NETWORK SYSTEMS

Around 2000, the government and communication service providers have imposed the conditions shown in Fig. 1 on the development for future telecommunications security technology. Then Y-00 quantum stream cipher was proposed as a cryptographic technique that satisfies these conditions and is currently undergoing commercialization.

In the recent Book [4] and a technical paper [5], 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 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 (see Appendix [A]). 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

Requirement to Cryptographic Communication in Commercial Use

The first is a system that guarantees maximum security while retaining the communication capabilities of current optical communications.

The second is to provide performance that cannot be achieved with current cryptography theory on symmetric key cipher. For example, the Shannon limit of the cryptology is broken.

Principle for security

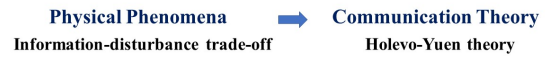


Fig. 1. Basic requirements of performance to new technologies

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. But 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 Fig. 2). 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.”

Let’s now turn our 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

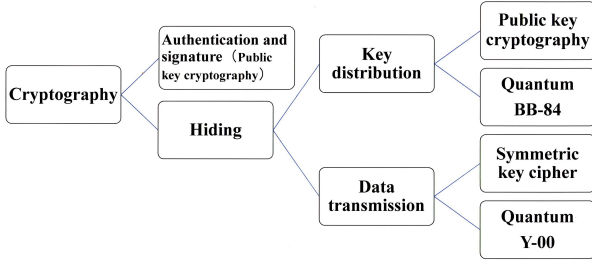


Fig. 2. Classification of cryptographic techniques

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, we will explain the technical contents, applicability to the real world, and development trends.

II. CURRENT STATUS OF QUANTUM COMMUNICATION SECURITY TECHNOLOGY

A. Quantum cryptography

As introduced in the above section, there are two quantum cryptography techniques. Let us give their brief introduction below.

(1) Quantum Key Distribution

BB-84 quantum key distribution (QKD) was proposed by C. H. Bennett and G. Brassard in 1984. It is a protocol to share a secret key sequence by using photon communication, that is guaranteed to be quantum nature. Since the photons used in this protocol are weak light, the transmission speed and distance are limited. In addition, many of the sequence of photons that carry information are lost due to attenuation effects in the transmission line, and the sequence of photons that reaches the receiver is also subject to errors due to noise effects. So the operation involves discarding the majority of the received bit sequence. Therefore, data itself cannot be sent, only random numbers can be sent. Thus only the delivery of the secret key for symmetric key cipher is possible. This is why it is called QKD. Recently, many newspapers have reported that several R & D groups can provide the commercial systems of QKD. The transmission speed is the order of 100 Kbit/sec, and transmission length is below 100 Km. The

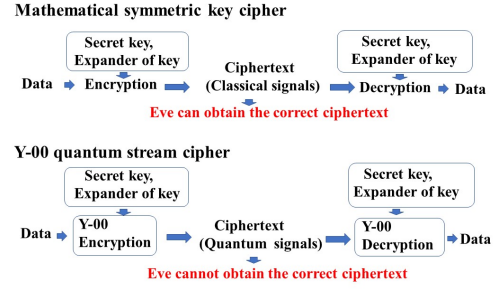


Fig. 3. Principle of operation of Y-00 quantum stream cipher. The expander of key in the both cases means PRNG that is employed in the conventional cipher system. Classical signal means that they have distinguishability, and quantum signal means impossible to distinguish them precisely. Y-00 Encryption is the function of converting a classical signal into a quantum signal. It is also called quantum modulation.

satellite system is one of the solutions to cope with the distance. But the transmission speed is so small. In any case, if one tries to increase the transmission speed, there is a trade-off and one has to shorten the relay interval. Since the maximum transmission speed is about a megabit, it is difficult to supply keys to the One Time Pad cipher for data after key delivery, and it is likely to be limited to supplying initial keys (secret keys) for AES and others (See Appendix [B]).

(2) Quantum Stream Cipher

Y-00 quantum stream cipher is a protocol for physical symmetric key cipher proposed by H.P. Yuen of Northwestern University in the DARPA project (2000) [6]. The details are explained in the next section, but a simple concept is presented here.

This technique is characterized by the fact that it does not allow the physical signals consisting of the mathematical random generator and information data to be obtained without error. In this scheme, the ciphertext in Y-00 circuit system of the mathematical cipher consisting of the generator and data, which is the target of the eavesdropper, is described by $y = \alpha_i(X, f_g(K_s), R_p)$. Then, we design the system such that the ciphertext $y = \alpha_i(X, f_g(K_s), R_p)$ is mapped into ensemble of coherent state $|\Psi(X, K_s, R_p)\rangle$ with the quantumness based on Holevo–Yuen theory [7,8,9]. This is called Y-00 signal which corresponds to ciphertext on the Hilbert space. Thus, the ciphertext as the classical signal is protected by the quantumness. Let us describe it shortly. Although ordinary laser light of high power is used as the transmission signal, signals on the communication channel can be made to have very strong quantum properties in the sense of quantum detection theory. This is Y-00 principle [6]. That is, a large number of physical binary light communication base is prepared to transmit electric binary data, and the binary data is transmitted by using

one communication base which is randomly selected from many communication bases by a mathematical cipher. Let M be the number of the base. The optical signals on the communication channel become ultra-multiple-valued signals ($2M = 4096$ or more values are common) against the eavesdropper without the knowledge of communication base. At this time, strong quantum nature in the signal ensemble appears even if the one signal is in high power light, when it is constructed by such ultra-multiple-valued. In other words, this method means that the quantum nature in the sense of quantum detection theory is created artificially by modulation schemes, so that it does not require light with strong physical quantum nature such as photon. The Y-00 signals of the length m (number of slot) are described as follows:

$$\begin{aligned} &|\Psi(X, K_s, R_p)\rangle = |\alpha_i(X, f_g(K_s), R_p)\rangle_1 \\ &\otimes |\alpha_j(X, f_g(K_s), R_p)\rangle_2 \dots \dots \\ &\otimes |\alpha_k(X, f_g(K_s), R_p)\rangle_m \end{aligned} \quad (1)$$

where $|\alpha_i(X, f_g(K_s), R_p)\rangle$ is coherent state with amplitude $\alpha(\cdot)$, $i, j, k = 1, 2, 3, \dots, 2M$, X is plaintext, $f_g(K_s)$ is a mathematical pseudo random function of secret key K_s , and R_p is additional randomization. The set of these coherent states is designed to be strong non-orthogonal property, even if each amplitude of the signals is $|\alpha_k(X, f_g(K_s), R_p)| \gg 1$.

A legitimate receiver with the knowledge for communication base to which the data is sent can ignore the quantum nature of the data, because it is a binary transmission by high power signal. That is, he can receive the data of error-free. On the other hand, an eavesdropper, who does not know the information of communication base, must receive a sequence of a ultra-multi-valued optical signal that consists of non-orthogonal quantum states of Eq(1). The quantum noise generated by quantum measurement based on Holevo-Yuen theory on quantum detection masks the received signal, resulting in errors. Thus, even if the eavesdropper tries to record the ciphertext, the masking effect of the quantum noise makes it impossible to accurately recover the ciphertext. This fact is a novel function in the cryptology. Fig 3 shows the scheme of Y-00 protocol. And Fig 4 shows the experimental demonstration of the advantage creation principle of security based on Holevo-Yuen theory.

B. Comparison of services based on each quantum cryptosystem

QKD and Y-00 are about 40 and 20 years old, respectively, since they were invented. At the time of their invention, the principle models of both quantum cryptography technologies were not very attractive in terms of security and communication performance. But nowadays, the systems and security assurance technologies of both technologies have evolved dramatically. Based on the results, business models for security services using these

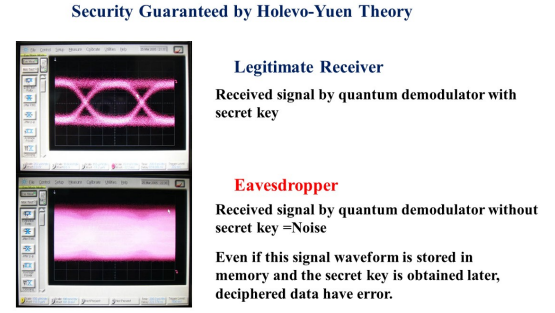


Fig. 4. Experimental demonstration of advantage creation based on Holevo-Yuen theory. Quantum ciphertext for eavesdropper consists of $2M$ densely packed non-orthogonal quantum coherent state signals. As a result, Holevo-Yuen theory guarantees that an eavesdropper cannot receive the correct ciphertext, or cannot copy the ciphertext.

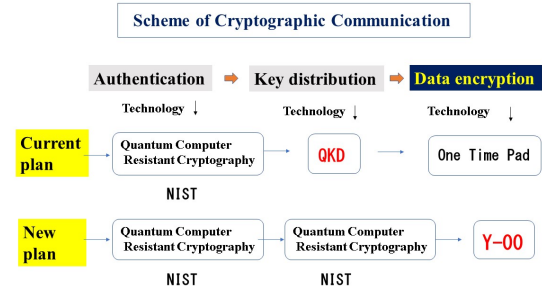


Fig. 5. Two types of quantum cryptographic communication schemes

quantum cryptography technologies have been proposed. Fig.5 shows the cryptography communication scheme based on two types of quantum cryptographies, and Fig.6 shows the current status of the system performance.

III. FEATURE OF QUANTUM STREAM CIPHER

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

System Performance					
	System		Specifications		
	Key delivery	Data encryption	Security	Distance	Rate
Existing Services	RSA, DH, etc	AES, RC-4, etc	Computational guarantee	Unlimited	10 Gbit/sec
Toshiba, NEC (L-1)	QKD	One Time Pad	OTP: ITS against Ciphertext only attack	10km ~ 100km	10 Kbit/sec ~ 10 Mbit/sec
Tamagawa University, Hitachi (L-1)	Quantum computer resistant Public key	Y-00	Y-00: ITS against Ciphertext only attack Non-malleability	1,000km ~ 10,000km	1 Gbit/sec ~ 100 Gbit/sec

Fig. 6. Comparison of product capabilities for two types of quantum cryptography services

there are few introductions to this technology, we describe the details of this technology at the following.

A. Basic Scheme

As explained in the previous section, the quantum stream cipher is expected to accelerate advanced application in the future communication system. 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 researches on practical experiment for this system have been reported by Northwestern University [10,11], Tamagawa University-Panasonic [12], and Hitachi Ltd [13]. Theories of system design for the basic system have been given by Nair and others [14,15,16,17].

Let us explain the principle of Y-00 quantum stream cipher. First, Y-00 protocol starts by specifying the signal system that use as 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 as ISK:Y-00, PSK:Y-00, QAM:Y-00, etc.

Here, one communication base consisting of various binary signals is randomly selected by PRNG (or AES) in 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 she does not which communication base was selected.

B. 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 are called the "basic model". It is this basic model that can be found in textbooks for beginners.

Let us start with QKD such as BB-84. If the basic model of the BB-84 protocol is implemented in a real optical fiber communication system, 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 proposed a mathematical security theory for BB-84 on an abstract mathematical model called the Shor model, which was later improved by R. Renner. 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, Y-00 protocol can consider the effects of non-ideal communication systems. As mentioned at the above section, the selection of communication base of Y-00 protocol is encrypted by conventional mathematical cipher. 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 Y-00 quantum ciphertext. However, since the set of ultra-multi-valued signals, which is Y-00 quantum ciphertext, are non-orthogonal quantum state ensemble, her 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, we should emphasize that the discussion with infinite number or asymptotic theory are not our concern, because our concern is a physical system under practical situation. For example, if attacker needs circuits of number of the size of the universe to perform the brute-force attack, the system is unbreakable. Or, if attacker needs 100 years to collect the ciphertext for trying the crypto-analysis, it is also unbreakable.

C. Randomization technology for quantitative security performance (*Errata of the original paper [1]*)

In the early days when Y-00 was invented, the model was used so called the basic model, and it just explained the principle. In order to achieve sufficient quantitative security, the randomization technique described here is necessary. In the above criteria, Y-00 scheme has a potential to improve quantitative security by additional randomization technology, because all physical parameters are finite. In this point of view, we have developed a new concept such as "quantum noise diffusion technology"[18,19]. In addition, several randomizations based on Yuen's idea [6] have been discussed [20].

"Although we have, at present, no general theory on randomization, using these techniques, it is expected to have security performance that cannot be achieved by conventional cipher. One of them is a special relation between secret key and data (plaintext). That is, under

the condition of $H(X_n | C_n^B, K_s) = 0$, one can expect the following security performance”:

$$H(X_n | C_n^E, K_s) \neq 0 \quad (2)$$

for certain finite $n > |K_s|$. n is the length of the plaintext, C_n^B means the ciphertext for Bob (signal received by Bob), and C_n^E means the ciphertext for Eve (signal received by Eve). This is an amazing capability, and one that cannot be achieved even with any conventional cipher including OTP (see Appendix [C]). In this way, we can say that Y-00 quantum stream cipher has ability to provide security that exceeds the performance of conventional cryptography while maintaining the capabilities of ordinary optical communication.

IV. CONCRETE APPLICATIONS OF QUANTUM STREAM CIPHER

As mentioned above, Y-00 quantum stream ciphers has not yet reached their ideal performance, but in practical use, they have achieved a high level of security that cannot be achieved with conventional techniques, and it can be said that they are now at a level where they can be introduced to the market.

Since quantum stream cipher is a physical cipher, it requires a dedicated transmitter and receiver. So far, principle models for commercial purposes have been developed at Northwestern University, Tamagawa University, Panasonic, and Hitachi, Ltd. Fig.7 shows the transceivers of each research institute. The communication speed is 1 Gbit/sec to 10 Gbit/sec and the communication distance is 100 km to 1,000 km. Using these transceivers, operational tests were conducted in a real optical communication network. Here, we introduce examples of the use case of Y-00 quantum stream cipher.

A. Optical Fiber Communication

Large amounts of important data are instantaneously exchanged on the communication lines between data centers that various data is accumulated. It is important from the viewpoint of system protection to eliminate the risk that the data is copied in its entirety from communication channel. We believe that Y-00 quantum stream cipher is the best technology for this purpose. 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/sec to 10 Gbit/sec have already been realized, and by wavelength division multiplexing, 100 Gbit/sec system has been tested. Also, communication distances of 1,000 km to 10,000 km have been demonstrated. In off-line experiments, 10 Tbit/sec has been demonstrated. In general, a dedicated line such as dark fiber is required. If we want to apply this technology to network function,

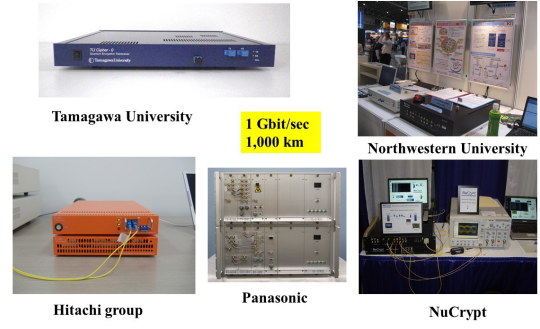


Fig. 7. Commercial Y-00 Transceiver for 1 Gbit/sec optical Ethernet. This can be mass produced.

we 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, we have successfully demonstrated the feasibility of using Y-00 transceiver in testbed optical switching systems. Furthermore, the references [21-28] show the recent activities of the experimental research group at Tamagawa University towards practical application to the real world.

B. Optical Satellite Communication

Y-00 quantum stream cipher, which was developed for fiber-optic communications, can also be applied to satellite communications. In satellite communication applications, rate of operation is an important factor because communication performance depends on 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. We are currently analyzing the performance of the system in such cases at 10 Gbps operation [29].

C. Optical Communication from Base at 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. We 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.

V. CONCLUSION

The current optical network was not laid out in a planned manner, but was configured by extending the

Examples of research reports on Y-00 from the People's Republic of China

- **Army Engineering University of PLA, China**
IEEE Photonics J. 12(4), 7904114 (2020).
Opt. Commun. 461, 125151 (2020).
Opt. Express 25 (10), 10947 (2017).
Quant. Inf. Process. 16(8), 189 (2017).
- **Beijing University of Post and Telecommunications, China**
Opt. Fiber Technol. 52, 101939 (2019).
Opt. Commun. 445, 29 (2019).
OECC Technical Digest, 5D1-3 (2018).
- **Huazhong University of Science and Technology, China**
IEEE Access 8, 63585 (2020).

Fig. 8. Research activities on Y-00 quantum stream cipher in China

existing communication lines for adapting the demand. In the future, the configuration and specifications of the optical network will be determined following to new urban planning. An actual example is the Smart City that Toyota Motor Corporation et al have disclosed as a future plan. Many ideas are also being discussed in other organizations. Recently, NTT has announced a future network concept so called IOWN. In these systems, the security of the all optical network with ultra-high speed is also important issue. The group of QKD and the group of Y-00 are promoting their respective technologies. Y-00 quantum stream cipher is a technology that can realize the specification of high speed and long communication distance. In addition, the signals of Y-00 cipher with ultra-multiple valued scheme for coherent state signal, so called quantum modulation, can have stronger quantum properties than QKD in the sense of quantum detection theory. So, the security is protected by many quantum no-go theorems. Although it is difficult to make an accurate prediction, there is a good chance that such a new technology will be used in the future. In view of the situation described in this paper, Y-00 quantum stream cipher will contribute to real world application of quantum technology for Society 5.0, and new business development can be expected. Finally, we would like to introduce that Chinese research institutes have recently been actively working on Y-00 quantum stream cipher. Fig.8 shows a list of academic papers on their activities [30-37]. It is expected that many research institutes will participate in this technological development.

EXPLANATION OF SYMBOLS

Here we give the explanation on the several symbols.

(a) Conventional cipher:

X is plaintext; $\{0, 1\}$, K_s is secret key, $f(K_s)$ is running key; $\{0, 1\}$, C is conventional ciphertext; $\{0, 1\}$.

(b) Y-00 quantum stream cipher:

X is plaintext; $\{0, 1\}$, K_s is secret key, $f(K_s)$ is running key by PRNG; $\{0, 1\}$, Y-00 running key is $f(K_s) \mapsto f_g(K_s)$; $\{1, 2, 3, \dots, M\}$, Y-00 ciphertext in the circuit is $y = \alpha_i(X, f_g(K_s), R_p)$; $\{1, 2, 3, \dots, 2M\}$, Y-00 signal is $|\alpha_i(X, f_g(K_s), R_p)\rangle$. Quantum ciphertext, C_n^B is ciphertext received by Bob; $\{0, 1\}$, C_n^E is ciphertext; $\{0, 1\}$ for Eve transformed from M -ary received signal, R_p is additional randomization.

APPENDIX

[A] QUANTUM COMPUTER AND QUANTUM COMPUTER-RESISTANT CRYPTOGRAPHY

It is difficult to predict the realization of a quantum computer capable of cryptanalysis. It has been discovered in our recent paper [38] that a new type of error so called nonlinear error or bust error occurs in general quantum computer. Therein, an error probability for single qubit increases depending on number of qubits in the system. These nonlinear errors and bust errors are caused by the recurrence effect due to quantum correlation or the collective decoherence, and by cosmic ray. They give a serious damage to scalable quantum computer, and give serious degradations of the capability of quantum computer. In addition, a number of previously unknown and extremely difficult problems in the development for an error correctable quantum computer have been reported. Thus, the capability of a real quantum computer is strictly limited and that the current cryptography is not subject to the danger posed by current quantum computers. However, we believe that the ideal quantum computer will be realized in the future. So, one should develop quantum computer-resistant cryptosystems based on mathematical analysis, or by physical cipher on the assumption that an ideal quantum computer or new mathematical discovery can be realized in the future.

Recently, J. P. Mattsson, B. Smeets, and E. Thormarker [39] have provided an excellent survey for the NIST quantum computer-resistant cryptography standardization effort, the migration to quantum-resistant public-key cryptography, and the relevance of QKD as a complement to conventional cryptography. In particular, these algorithms of quantum-resistant public-key cryptography can execute completely in software on classical computers, in contrast to e.g., QKD which requires very expensive custom hardware. For functions of authentication, signature, and key distribution, such capability provided by software is the most important in the real world application.

[B] POSITION OF SECURITY SYSTEM BASED ON QKD IN PRACTICAL APPLICATIONS

To complete full quantum secure communication systems, at present, we are challenged to cope with the following problems, discussing a new type of QKD.

Recently, NSA [40], NCSC [41] and ANSSI [42] announced the international stance on QKD. They have

a negative view of QKD, because the communication performance of QKD based on weak signal is not enough for applications to the real situation. Let us denote their comments in the following, respectively.

A. NSA (USA)

(a) NSA does not recommend the usage of QKD for securing the transmission of data in National Security Systems (NSS)

(b) QKD utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology. Quantum cryptography uses the same physics principles and similar technology to communicate over a dedicated communications link. Published theories suggest that physics allows QKD to detect the presence of an eavesdropper, a feature not provided in standard cryptography.

QKD and similar quantum cryptography vendors and the media occasionally state bold claims based on theory e.g., that this technology offers guaranteed security based on the laws of physics. Communications needs and security requirements physically conflict in the use of QKD, and the engineering required to balance these fundamental issues has extremely low tolerance for error. Thus, security of QKD is highly implementation dependent rather than assured by laws of physics.

Technical limitations

- (1) Quantum key distribution is only a partial solution.
- (2) Quantum key distribution requires special purpose equipment.
- (3) Quantum key distribution increases infrastructure costs and insider threat risks.
- (4) Securing and validating quantum key distribution is a significant challenge.
- (5) Quantum key distribution increases the risk of denial of service.

For all of these reasons, NSA does not support the usage of QKD to protect communications in National Security Systems, and does not anticipate certifying or approving any QKD security products for usage by NSS customers unless these limitations are overcome.

B. NCSC (UK)

Given the specialized hardware requirements of QKD over classical cryptographic key agreement mechanisms and the requirement for authentication in all use cases, the NCSC does not endorse the use of QKD for any government or military applications, and cautions against sole reliance on QKD for business critical networks, especially in Critical National Infrastructure sectors. In addition, we advise that any other organizations considering the use of QKD as a key agreement mechanism ensure

that robust quantum-safe cryptographic mechanisms for authentication are implemented alongside them. NCSC advice is that the best mitigation against the threat of quantum computers is quantum safe cryptography. Our white paper on quantum-safe cryptography is available on the NCSC website. The NCSC design principles for high assurance systems, which set out the basis under which products and systems should be designed to resist elevated threats, is also available

C. ANSSI (The French National Agency for the Security of Information Systems)

Quantum Key Distribution (QKD) presents itself as a technology functionally equivalent to common asymmetric key agreement schemes that are used in nearly all secure communication protocols over the Internet or in private networks. The defining characteristic of QKD is its alleged superior secrecy guarantee that would justify its use for high security applications. However, deployment constraints specific to QKD hinder large-scale deployments with high practical security. Furthermore, new threats on existing cryptography, and in particular the emergence of universal quantum computers, can be countered without resorting to QKD, in a way that ensures the future of secure communications. Although QKD can be used in a variety of niche applications, it is therefore not to be considered as the next step for secure communications

[C] DRAWBACK OF ONE TIME PAD CIPHER

OTP is extremely inefficient for the encryption of data, because it requires key sequence as same as data sequence. However, it has the following benefit:

(1) Ciphertext only attack on data

Since the secret key : K_s is a perfect random number, the ciphertext : C is also a perfect random number. Therefore, obtaining the ciphertext gives no information about the plaintext : X . So one has $H(X|C) = H(X)$. At this point, it is called perfect information-theoretic security or unconditional security.

(2) Known plaintext attack on key

In OTP, if the length of the known plaintext is $|X| = N$, then the key of the same length N can be known for sure by obtaining a ciphertext N of the same length. However, since the key sequence is completely random, subsequent key sequences cannot be predicted.

On the other hand, it has the following drawback:

(1) Falsification attack

If Eve obtains the correct ciphertext, and she can invert 0 and 1, and resend. Then 1 and 0 of the data are inverted. As an example, if the data is yes or no, the falsification will be successful. So OTP is not secure against falsification attacks [43].

(2) Partial known plaintext attack on data

If a plaintext sequence has a correlation (e.g., a word), then the possibility of identifying a word arises through a brute force search with a partial known plaintext attack [44]. These are some examples of the fact that OTP does not satisfy the security requirements of modern cryptology.

REFERENCES

- [1] Sohma, M.; Hirota, O. Quantum stream cipher based on Holey-Yuen theory, *Entropy* **2022**, *24*, 667.
- [2] Hirota, O.; Sohma, M. Development of cryptographic technology (Y-00 quantum stream cipher) indispensable for industrial infrastructure in the Society 5.0 era, *Optical and Electro-Optical Engineering Contact*, **2022**, vol-60, no-1, pp29-36.
- [3] Sohma, M.; Hirota, O. Y-00 quantum stream cipher to promote quantum technology innovation and its application to optical satellite communications - Beyond One Time Pad cipher-, *Optical Alliance*, **2022**, vol-33, no-8.
- [4] Tsujii, S. *The Fight against Fakes*; Kotoni Publishing Co.: Chiba Prefecture, Japan, **2021**.
- [5] Hirota, O.; Tsujii, S. Quantum noise analysis for quantum computer. IEICE of Japan, Technical Report on Information theory, **2021**, *121*, no-96, IT2021-20, pp28-33.
- [6] Yuen, H.P. KCQ : Keyed communication in quantum noise. *arXiv* **2003**, arXiv:0311061.
- [7] Holevo, A.S. Statistical decision theory for quantum systems. *J. Multivar. Anal.* **1973**, *3*, 337.
- [8] Yuen, H.P.; Kennedy, R.S.; Lax, M. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inf. Theory* **1975**, *21*, 125-134.
- [9] Hirota, O.; Ikehara, S. Minimax strategy in the quantum detection theory and its application to optical communications. *Trans. IEICE Jpn.* **1982**, *65E*, 627.
- [10] Borbosa, G.A.; Corndorf, E.; Kumar, P.; Yuen, H.P. Secure communication using mesoscopic coherent states. *Phys. Rev. Lett.* **2003**, *90*, 227901.
- [11] Kanter, G.S.; Reilly, D.; Smith, N. Practical physical layer encryption: The marriage of optical noise with traditional cryptography. *IEEE Commun. Mag.* **2009**, *47*, 74-81.
- [12] 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.
- [13] 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.
- [14] Nair, R.; Yuen, H.P.; Corndorf, E.; Kumar, P. Quantum noise randomized ciphers. *Phys. Rev. A* **2006**, *74*, 052309.
- [15] Hirota, O.; Kurosawa, K. Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol. *Quantum Inf. Process.* **2007**, *6*, 81-91.
- [16] Hirota, O. Practical security analysis of quantum stream cipher by Yuen protocol. *Phys. Rev. A* **2007**, *76*, 032307.
- [17] Yuen, H.P. Key generation: Foundation and new quantum approach. *IEEE Sel. Top. Quant. Electron.* **2009**, *15*, 1630-1645.
- [18] Yuen, H.P.; Nair, R.; Corndorf, E.; Kanter, G.S.; Kumar, P. On the security of $\alpha\eta$ response to some attacks on quantum-based cryptographic protocols. *Quantum Inf. Comput.* **2006**, *6*, 561-582.
- [19] Hirota, O.; Sohma, M.; Kawanishi, K. Quantum noise randomized stream cipher: Y-00. *Jpn. J. Opt.* **2010**, *39*, 17.
- [20] Kato, K.; Hirota, O. Quantum stream cipher part IV, Effects of the deliberate signal randomization and deliberate error randomization. In Proceedings of the SPIE Conference on Quantum Communications and Quantum Imaging IV, San Diego, CA, USA, **2006**, August; Volume 6305.
- [21] 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.
- [22] 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.
- [23] Tanizawa, K.; Futami, F. 14 power of 2 intensity-level 10-Gbaud Y-00 quantum stream cipher enabled by coarse-to-fine modulation. *IEEE Photonics Technol. Lett.* **2018**, *30*, 1987-1990.
- [24] Tanizawa, K.; Futami, F. Digital coherent PSK Y-00 quantum stream cipher with 217 randomized phase levels. *Opt. Express* **2019**, *27*, 1071-1079.
- [25] 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.
- [26] 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.
- [27] 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.
- [28] Tanizawa, K.; Futami, F. Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system. *Opt. Express* **2021**, *29*, 10451-10464.
- [29] Hirota, O.; Kato, K.; Sohma, M. Application of Y-00 quantum stream cipher to satellite communication-Mathematical model of weather disturbance-, IEICE of Japan, Technical Report on Information theory, **2022**, *121*, no-327, IT2021-54, 143-148.
- [30] Chen, Y.; Jiao, H.; Zhou, H.; Zheng, J.; Pu, T. Security analysis of QAM quantum noise randomized cipher system. *IEEE Photonics J.* **2020**, *12*, 7904114.
- [31] Tan, Y.; Pu, T.; Zhou, H.; Zheng, J.; Su, G. Performance analysis of physical layer security in ISK quantum noise randomized cipher based on wiretap channel. *Opt. Commun.* **2020**, *461*, 125151.
- [32] Jiao, H.; Pu, T.; Zheng, J.; Xiang, P.; Fang, T. Physical layer security analysis of a quantum noise randomized cipher based on the wire tap channel model. *Opt. Express* **2017**, *25*, 10947.
- [33] Jiao, H.; Pu, T.; Zheng, J.; Xiang, P.; Fang, T.; Zhu, H. Physical-layer security analysis of PSK quantum-noise randomized cipher in optically amplified links. *Quant. Inf. Process.* **2017**, *16*, 189.
- [34] Zhang, M.; Li, Y.; Song, H.; Wang, B.; Zhao, Y.; Zhang, J. Security Analysis of Quantum Noise Stream Cipher under Fast Correlation Attack. In *Optical Fiber Communication Conference (OFC) 2021*; Dong, P., et al., Eds.; OSA Technical Digest Optical Society of America: **2021**; paper Th1A.5.
- [35] Yang, X.; Zhang, J.; Li, Y.; Zhao, Y.; Zhang, H. DFTs-OFDM based quantum noise stream cipher system. *Opt. Commun.* **2019**, *445*, 29.
- [36] Yang, X.; Zhang, J.; Li, Y.; Gao, G.; Zhang, H. *Single Carrier QAM/QNSC and PSK/QNSC Transmission Systems with Bit Resolution Limited DACs*; OECC Technical Digest, **2018**; paper 5D1-3.
- [37] Yu, Q.; Wang, Y.; Li, D.; Song, H.; Fu, Y.; Jiang, X.; Huang, L.; Cheng, M.; Liu, D.; Deng, L. Secure 100 Gb/s IMDD Transmission Over 100 km SSMF Enabled by Quantum Noise Stream Cipher and Sparse RLS-Volterra Equalizer. *IEEE Access* **2020**, *8*, 63585.
- [38] Hirota, O. Introduction to semi-classical analysis for digital errors of qubit in quantum processor. *Entropy* **2021**, *23*, 1577.
- [39] Mattsson, J.P.; Smeets, B.; Thormarker, E. Quantum-Resistant Cryptography. *arXiv* **2021**, arXiv:2112.00399.
- [40] NSA, Quantum computing and post-quantum cryptography FAQs, National security agency central security service, Aug. **2020**. <https://www.quantum.gov/nsa-updates-faq-on-post-quantum-cybersecurity/?msclkid=525975f1cdce11eca34ea2e9f2b11545>. Why Quantum Key Distribution (QKD) is impractical. <https://crypto.stackexchange.com/questions/93830/why-quantum-key-distribution-qkd-is-impractical>.
- [41] NCSC, Quantum security technologies, **2020** <https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies>.
- [42] ANSSI, Should Quantum Key Distribution be Used for Secure Communications? **2020**

<https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications>.

- [43] Imai, H. Theory of information, codes, and Cryptography, Lecture series of IEICE of Japan, Corona Publishing Co. LTD, **2004**.
- [44] Tsuchiya, H. A study of attack against Vernum cipher, Report of graduation research at Tamagawa University, **2002**.