entropy

MDPI

Review

Quantum Stream Cipher Based on Holevo–Yuen Theory

Masaki Sohma [†] and Osamu Hirota [*,†]

Quantum ICT Research Institute, Tamagawa University, Tokyo 194-8610, Japan; sohma@eng.tamagawa.ac.jp
* Correspondence: hirota@lab.tamagawa.ac.jp
† These authors contributed equally to this work.

Abstract: In this review paper, we first introduce the basic concept of quantum computer-resistant cryptography, which is the cornerstone of security technology for the network of a new era. Then, we will describe the positioning of mathematical cryptography and quantum cryptography, that are currently being researched and developed. Quantum cryptography includes QKD and quantum stream cipher, but we 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. Finally, we introduce detailed research activity aimed at putting the quantum stream cipher into practical use in social network technology.

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

check for updates

Citation: Sohma, M.; Hirota, O. Quantum Stream Cipher Based on Holevo–Yuen Theory. *Entropy* **2022**, *24*, 667. https://doi.org/10.3390/e24050667

Academic Editor: Rosario Lo Franco

Received: 1 April 2022
Accepted: 5 May 2022
Published: 10 May 2022

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

At first, we introduce a comment on a general view of cryptography in our 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".

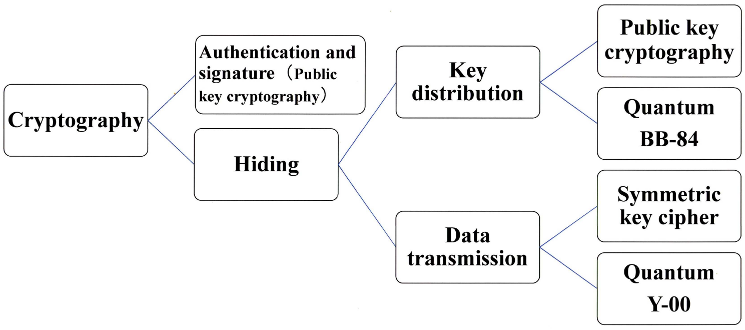


Figure 1. Classification of cryptographic techniques.

Let us 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 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.

2. Current Status of Quantum Communication Security Technology

2.1. 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/s, and transmission length is below 100 km. The satellite system is one of the solutions to cope with the distance. However, the transmission speed is so small. In any case, if one tries to increase the transmission speed, then 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.

(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) [3]. 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, as 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 $\mid \Psi(X, K_s, R_p) >$ with the quantumness based on the Holevo–Yuen theory [4–6]. 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 [7]. This is the Y-00 principle [3]. 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 signal. In other words, this method means that the quantum nature in the sense of quantum detection theory [7] is created artificially by modulation schemes, so that it does not require light with strong physical quantum nature, such as a photon. The Y-00 signals of the length m (number of slot) are described as follows:

$$\begin{aligned} &\mid \Psi(X, K_s, R_p) >=\mid \alpha_i(X, f_g(K_s), R_p) >_1 \\ &\otimes \mid \alpha_j(X, f_g(K_s), R_p) >_2 \ldots\ldots \\ &\otimes \mid \alpha_k(X, f_g(K_s), R_p) >_m \end{aligned} \tag{1}$$

where $\mid \alpha_i(X, f_g(K_s), R_p) >$ is coherent state with amplitude $\alpha(\cdot)$, $i, j, k = 1, 2, 3, \ldots 2M$, 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, one can receive the error-free data. On the other hand, an eavesdropper, who does not know the information of the communication base, must receive a sequence of a ultra-multi-valued optical signal that consists of non-orthogonal quantum states of Equation (1). The quantum noise generated by quantum measurement based on the Holevo–Yuen theory on quantum detection [8–10] 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. Figure 2 shows the scheme of Y-00 principle (Appendix A).

2.2. Comparison of Services Based on Each Quantum Cryptosystem

QKD and Y-00 are about 40 and 20 years old, respectively. 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. However, nowadays, the systems and security assurance technologies of both technologies have evolved dramatically. Based on the results, business models for security services using these quantum cryptography technologies have been proposed. Figure 3 shows the current status.

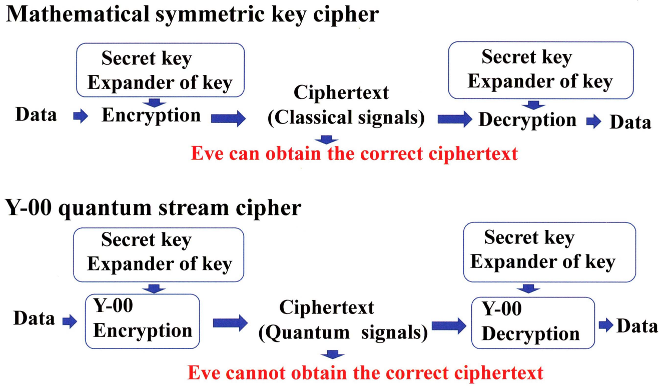
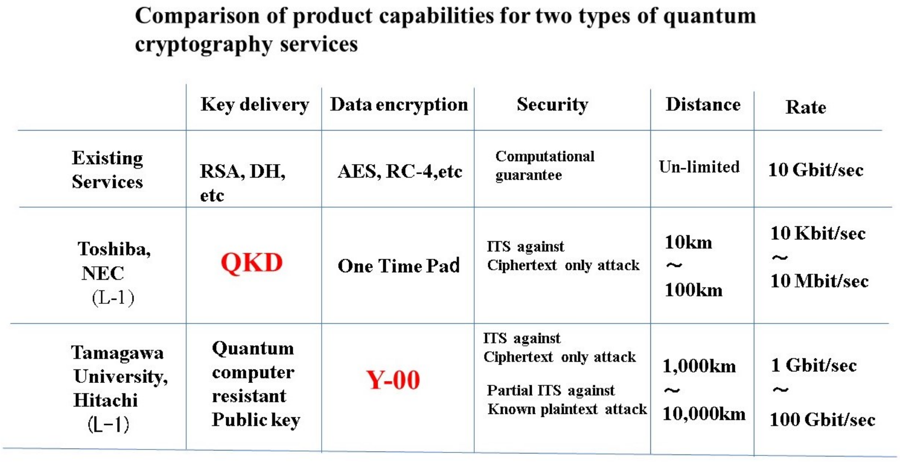


Figure 2. Principle of operation of Y-00 quantum stream cipher. Classical signal means that they have distinguishability, and quantum signal means it is impossible to distinguish them precisely. Y-00 encryption is the function of converting a classical signal into a quantum signal. It is also called quantum modulation.



Comparison of product capabilities for two types of quantum cryptography services

	Key delivery	Data encryption	Security	Distance	Rate
Existing Services	RSA, DH, etc	AES, RC-4,etc	Computational guarantee	Un-limited	10 Gbit/sec
Toshiba, NEC (L-1)	QKD	One Time Pad	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	ITS against Ciphertext only attack Partial ITS against Known plaintext attack	1,000km ~ 10,000km	1 Gbit/sec ~ 100 Gbit/sec

Figure 3. Comparison of product capabilities for two types of quantum cryptography services.

3. 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. Since there are few introductions to this technology, we describe the details of this technology in the following section.

3.1. 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 [8,9], Tamagawa University [10], and Hitachi Ltd. [11]. Theories of system design for the basic system have been given by Nair and others [12–15].

Let us 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.

3.2. 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 us 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. [16] proposed a mathematical security theory for BB-84 on an abstract mathematical model called the Shor model, which was later improved by R. Renner [17]. 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, 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 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.

4. Survey of the Mathematical Security Analysis

4.1. The Main Story of Security

In the conventional symmetric key cipher, we have

$$H(C \mid X, f(K_s)) = 0 \tag{2}$$

where X is plaintext, K_s is secret key, $f(K_s)$ corresponds to running key and $|f(K_s)| \gg |K_s|$, and C is ciphertext. However, in physical cipher system, the eavesdropper cannot do anything without obtaining the ciphertext from the physical signal. In the case of the Y-00 scheme, the eavesdropper has no other way but to observe the non-orthogonal signal, because the Y-00 signals corresponding to the ciphertext in the symmetric key cipher are an ensemble of non-orthogonal quantum states. Thus, the ciphertext that the eavesdropper can obtain are randomized by its quantum nature for any quantum processing by several quantum no-go theorems developed by Holevo and Yuen. This result means that the ciphertext cannot be determined correctly, even if the eavesdropper obtains the secret key K_s and the plaintext X. That is,

$$H(C \mid X, f(K_s)) \neq 0 \tag{3}$$

This is the definition of so called "Random Cipher". Thus, Y-00 scheme is a typical example of the random cipher. Here, let us describe the security evaluation in the practical setting based on two issues.

(i) The first issue:

The first issue was raised by the community of cryptology. The question of the cryptocommunity is how to formulate the error or correct estimation of ciphertext based on closeness between the sequence of ciphertext from the Y-00 signals received by the eavesdropper and a true random number sequence. Let us consider a quantum trace distance between density operators on the tensor product Hilbert space that corresponds to the ideal random sequence and the random sequence received by the eavesdropper. It can be denoted by following form, based on the Holevo–Yuen theory on quantum detection:

$$\Delta_q = \max_{\Pi} Tr\Pi(\sum_y p(y)\rho^y_{C^I C^E} - \rho_{C^I} \otimes \rho_{C^E}) \tag{4}$$
$$\Pi : POVM$$

In this case, C^I is the ideal ciphertext , and C^E is the output of the Eve's receiver. Then, ρ_{C^I} corresponds to the density operator for ideal randomness, and that of Eve is ρ_{C^E} which depends on the randomization based on quantum noise effect and the artificial scheme designed in the Y-00 scheme.

Closeness of the ciphertext sequence of the eavesdropper to a true random number based on the above equation is evaluated as follows [18]:

Theorem 1. *Trace distance is bounded by Holevo information, as follows:*

$$\Delta_q^2 \leq B\chi(\epsilon) \tag{5}$$

where B is a constant depending on the definition of relative entropy, and $\chi(\epsilon)$ is Holevo information from the channel to the eavesdropper.

$$\chi(\epsilon) = S(\rho_{C^E}) - \sum_y p(y)S(\rho^y_{C^E}) \tag{6}$$

where $\mathcal{S}(\rho)$ is the von Neumann entropy. The above Holevo information is a decrease function by the appropriate randomization technique under the fixed M.
Next, the probability that an eavesdropper can estimate the ciphertext $y = \alpha_k(X, f_g(K_s), R_p)$ of Y-00 quantum stream cipher is given as follows. Let Δ_q be the trace distance of the quantum density operators between an actual protocol and the ideal one. Then the average guessing probability for ciphertext of Y-00 cipher is bounded as follows:

$$\frac{1}{N} \leq P_{guess} \leq \frac{1}{N} + \Delta_q \leq \frac{1}{N} + \sqrt{B\chi(\epsilon)} \tag{7}$$

where $N = 2^{|C_y|}$. $|C_y|$ is the length of binary sequence converted from 2M-ary signal with the length m (number of slot). Thus, the guessing probability for the ciphertext $y = \alpha_k(X, f_g(K_s), R_p)$ is controlled by Holevo information. In conclusion, under the fixed number of N, one can try to design the randomization technique such that $\chi(\epsilon) \to 0$, and $P_{guess} \to 1/N$. Indeed, the Y-00 scheme provides this situation under ciphertext-only attack.

(ii) The second issue:

The next issue is information-theoretic security analysis for symmetric key cipher. In general security analysis for the symmetric key cipher, we have three problems—ciphertext-only attack (COA), statistical attack (SA), and known-plaintext attack (KPA), respectively.

The main issue is that, assess to that information-theoretic security (ITS) can be guaranteed depending on how much ciphertext under COA (or plaintext at KPA) an eavesdropper obtains. Shannon gave the following inequality for general mathematical symmetric key ciphers under ciphertext-only attack:

$$H(X|C) \leq H(K_s) \tag{8}$$

This is called the Shannon limit. Thus, one has the following property under KPA for the conventional additive stream cipher.

$$H(K_s \mid X_{n=|K_s|}, C_{n=|K_s|}) = 0 \tag{9}$$

where $X_{n=|K_s|}, C_{n=|K_s|}$ mean plaintext and ciphertext of the length $n = |K_s|$, respectively.

A random physical cipher, such as the Y-00 scheme, may break the above relation. We describe the story of the theory in the following. Here, in the Y-00 scheme, the following is guaranteed:

$$H(X \mid C^B, f(K_s)) = 0 \tag{10}$$

where C^B is the ciphertext received by a legitimate receiver. From here, we discuss the new potential of Y-00 scheme. In the case of a ciphertext-only attack, from Equation (3), this system provides the ability to break the Shannon limit in the cryptology as follows [19,20]:

$$H(K_s) \leq H(X_n|C_n^E) \tag{11}$$

where X_n, C_n^E mean the plaintext sequence and ciphertext sequence of the length n received by the eavesdropper, respectively. We emphasize that C_n^E is different of the original ciphertext created by Y-00 mechanism.

Let us consider statistical attack and the known-plaintext attack. Here, the security evaluation is given by the quantum unicity distance [12,19] under the Holevo–Yuen theory on quantum detection [4–6], as follows:

$$n_0 \quad : \quad H(K_s \mid C_{n_0}^E) = 0 \tag{12}$$

$$n_1 \quad : \quad H(K_s \mid X_{n_1}, C_{n_1}^E) = 0 \tag{13}$$

where n_0 and n_1 are the unicity distances for ciphertext-only attack and known-plaintext attack, respectively. These mean the number of observations needed to find the secret key with and without known plaintext in the sense of information theoretic security. For exceeded number of n_0 and n_1 , it still provides the algorithm independent computational security.

The formulae of the unicity distance for the concrete Y-00 scheme were given by Nair et al. [12]. Let us compare Equations (9) and (13). If the Y-00 scheme can provide

$$n_1 \gg |K_s|, \tag{14}$$

then the Y-00 scheme has the great advantage in comparison with the conventional cipher technology. For more rigorous analysis, we have the following criteria proposed by Yuen.

$$W(n) = \max_{C^E} \max_{K_s \in K_{C^E}} P(K_s|C_n^E) \tag{15}$$

Thus, it is possible to evaluate the security of this cipher quantitatively. This is a very significant feature in the history of cryptography.

4.2. Randomization Technology

In the early days when Y-00 was invented, the model used was the so-called basic model, and it just explained the principle. In order to achieve sufficient quantitative security, the randomization technique described here is necessary. In the criteria of cryptography by Shannon, such as Equations (12) and (13), the Y-00 scheme has a potential to have excellent quantitative security by additional randomization technology.

In this point of view, we have developed a new concept such as "quantum noise diffusion technology" [13,14]. In addition, several randomizations based on Yuen's idea [3] have been discussed [21]. Using these techniques, it is expected to have security against known-plaintext attacks on key that cannot be achieved by a conventional cipher, as follows:

$$H(X_n \mid C_n^E, K_s) \neq 0 \tag{16}$$

for certain finite $n = n_2 > |K_s|$ under the condition Equation (10). This means that one cannot pin-down the data under the finite length of ciphertext with error even if the secret key is provided to the attacker after they have received the Y-00 signals by their instruments [19,20]. This comes from the fact that the ciphertext for attacker is not correct ciphertext. This is called advantage creation based on receivers with key and without key.

This is an amazing capability, and this cannot be achieved even with "One Time Pad Cipher". However, as the pointed out in the above, these security of abilities are limited to "**finite**" n_1, and n_2 in principle, and these depend on the randomization technique. The general quantitative evaluation for the concrete randomization is still an open question. In this way, we can say that the Y-00 quantum stream cipher has the ability to provide security that exceeds the performance of conventional cryptography while maintaining the capabilities of ordinary optical communication. To date, there have been several criticisms of the security of the Y-00 principle, but one can see that they all turn out to be based on misunderstandings of the structure and claim of the Y-00 principle.

5. 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, we introduce examples of the use case of the Y-00 quantum stream cipher.

5.1. 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. We believe that the Y-00 quantum stream cipher is the best technology for this purpose (see Figure 4). 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 we want to apply this technology to network function, then 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 the Y-00 transceiver in testbed optical switching systems (see

Figure 5). Furthermore, Figure 6 shows the recent activities of the experimental research group at Tamagawa University towards practical application to the real world [22–29].

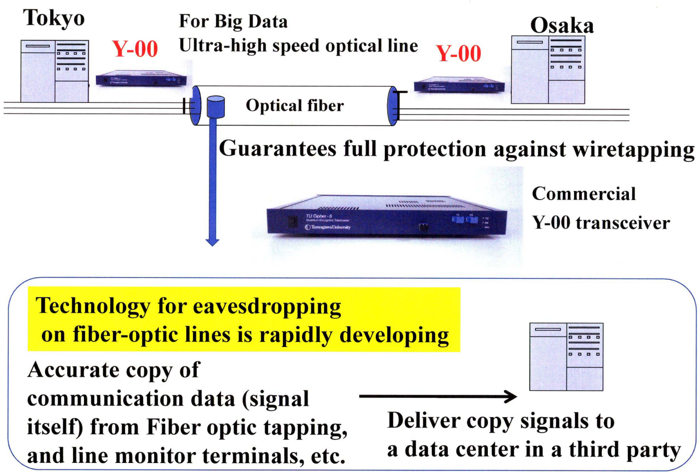
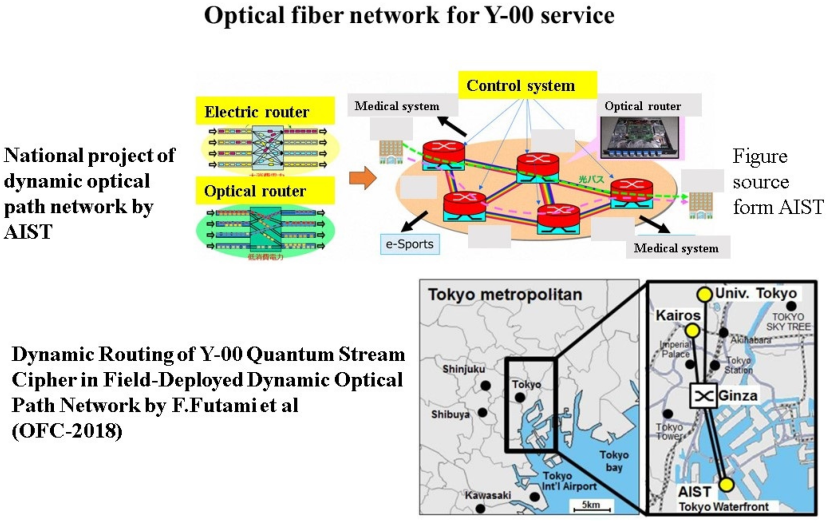
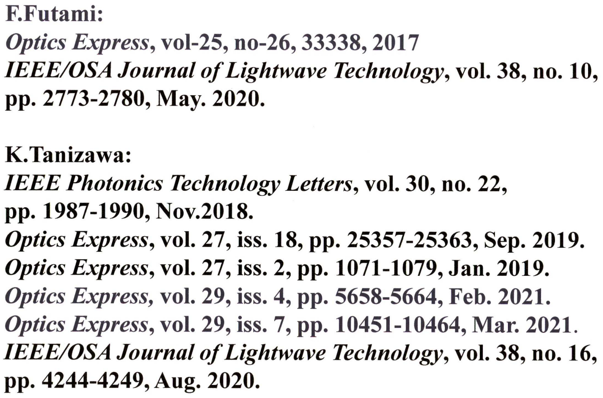

Tokyo
Y-00
For Big Data
Ultra-high speed optical line
Y-00
Osaka
Optical fiber
Guarantees full protection against wiretapping
Commercial
Y-00 transceiver
Technology for eavesdropping
on fiber-optic lines is rapidly developing
Accurate copy of
communication data (signal
itself) from Fiber optic tapping,
and line monitor terminals, etc.
Deliver copy signals to
a data center in a third party

Figure 4. 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.



Newly constructed DOPN testbed in Tokyo.

Figure 5. Scheme of optical network by dynamic path and experimental demonstration of service of the Y-00 quantum stream cipher by Tamagawa University and AIST in Tokyo Bay Coastal area.



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

5.2. *Optical Satellite Communication*

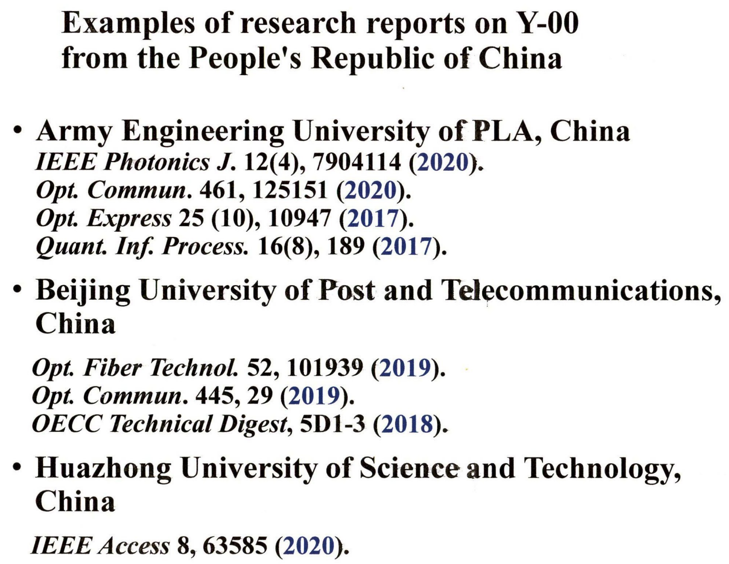
The Y-00 quantum stream cipher, which was developed for fiber-optic communications, can also be applied to satellite communications. In satellite communication applications, the rate of operation is an important factor because communication performance depends on the weather conditions. With QKD, it 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. We are currently analyzing the performance of the system in such cases at 10 Gbps operation [30].

5.3. *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. 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.

6. Future Outlook and Conclusions

The current optical network was not laid out in a planned manner, but was configured by extending the 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. However, recently, NSA and others announced the international stance on QKD [31]. They have a negative view of QKD, because the communication performance of QKD based on weak signal is not sufficient for applications to real situations. So, we do not employ QKD for key distribution of the initial key of Y-00, as shown in Figure 3 (Appendix B).



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).**

Figure 7. Research activities on the Y-00 quantum stream cipher in China.

On the other hand, the 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 (Appendix C). 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, the Y-00 quantum stream cipher will contribute to real-world applications of quantum technology for Society 5.0, and new business development can be expected. Finally, we would like to note that Chinese research institutes have recently been actively working on Y-00 quantum stream cipher. Figure 7 shows a list of academic papers on their activities [32–39]. It is expected that many research institutes will participate in this technological development.

Author Contributions: Conceptualization, M.S. and O.H.; methodology, M.S. and O.H.; validation, M.S. and O.H.; formal analysis, M.S. and O.H.; investigation, M.S. and O.H.; writing—original draft preparation, O.H.; writing—review and editing, M.S. and O.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research recieved no external funding.

Acknowledgments: We are grateful to F. Futami, K. Tanizawa on experimental research, K. Nakahira, K. Kato and T. S. Usuda for discussions on theory.

Conflicts of Interest: The authors declare no conflict of interest.

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 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 of PRNG; $\{0,1\}$,
Y-00 running key is $f(K_s) \mapsto f_g(K_s)$; $\{1,2,3,\ldots M\}$,
Y-00 ciphertext is $y = \alpha_i(X, f_g(K_s), R_p)$; $\{1,2,3,\ldots 2M\}$,
R_p is additional randomization,
Y-00 signal (quantum) is$| \alpha_i(X, f_g(K_s), R_p) >$,
C_y is binary representation of Y-00 ciphertext;$\{0,1\}$,
C^E is ciphertext received by eavesdropper; $\{1,2,3,\ldots 2M\}$, C^I is the true random sequence.

Appendix A. Simple Explanation of Y-00 Principle

Here, we introduce the mathematical formulation of the Y-00 principle. Let us define signals. The information is binary, 0 or 1. Bit symbols $i = 0, 1$ are transmitted by many kinds of coherent state signals indexed by j. Here, j means the jth communication base in $j \in \mathcal{M}$. Then, we have the following signal ensemble:

$$\begin{aligned} &\rho(i,j) = |\alpha(i,j)\rangle\langle\alpha(i,j)|, \\ &i = 0,1, \quad j = 1,2,3,\ldots,M \end{aligned} \tag{A1}$$

where $\alpha(i,j)$ is a complex amplitude of coherent state, and the total number of signals becomes $2M$. It is important that we here set the following signal (see references [1,5–7]):
(1) Signal setting-A

$$\langle\alpha(0,j)|\alpha(1,j)\rangle = \eta \ll 1, \forall j \tag{A2}$$

(2) Signal setting-B
Even if $\langle\alpha(0,j)|\alpha(1,j)\rangle = \eta \ll 1, \forall j$, we can arrange the signal configuration as follows:

$$\langle\alpha(k = M/2)|\alpha(k = M/2) \pm h\rangle \cong 1 \tag{A3}$$

where $-M/2 \le h \le M/2$.

The communication channel for the legitimate user having the knowledge of j becomes the binary channel. That is, the signal is $|\alpha(0,j)\rangle$ or $|\alpha(1,j)\rangle, \forall j$. Let $\Pi(i_{out}) = \{\Pi(0), \Pi(1)\}$ be the POVM for the binary detection. The conditional probability of the legitimate receiver is given as follows:

$$P(i_{out} \neq i) = Tr|\alpha(i)\rangle\langle\alpha(i)|\Pi(i_{out}) \cong 0, \forall j \tag{A4}$$

where $i = 0, 1$, $i_{out} = 0, 1$. On the other hand, when one does not know the j, the channel becomes the binary vs. $2M$. That is, the input signals are $|\alpha(0,j)\rangle$ or $|\alpha(1,j)\rangle$, and the output signals are $2M$ coherent states $\{|\alpha(i,j)\rangle\}$. Let $\{\Pi(k)\}, k = 1, 2, 3, \ldots, 2M$ be the POVM for $2M$ signal detection, where k is the combination of i and j. The average correct probability of the eavesdropper is given by the Holevo–Yuen theory as follows:

$$P_{correct}(k) = \max_{\Pi(k)} \sum_{k} P(k) Tr|\alpha(k)\rangle\langle\alpha(k)|\Pi(k) \cong \frac{1}{2M} \tag{A5}$$

Here, we give more simple explanation how the data (plaintext) is protected under the ciphertext-only attack. Let us consider the accessible information. From signal setting A, the channel with the knowledge on j is based on Equations (A2) and (A4) as follows:

$$P(i|i_{out}) \cong \delta_{i,i_{out}} \tag{A6}$$

Thus, the accessible information on the data (plaintext) to the ensemble $\{\rho(i,j)\}$ with the knowledge on j is

$$I(X,Y)_{A,B} = H(X) - H(X|Y) \cong H(X) = 1 \tag{A7}$$

The channel without the knowledge on j is based on Eq(A-21) as follows:

$$P(i = 0|k) \cong \frac{1}{2} - \epsilon_k, \quad P(i = 1|k) \cong \frac{1}{2} + \epsilon_k \tag{A8}$$

where $\epsilon_k \sim 0$. Thus, the accessible information on the data (plaintext) of the eavesdropper is

$$I(X,Y)_{A,E} = H(X) - H(X|Y) \sim 0 \tag{A9}$$

The difference between $I(X,Y)_{A,B}$ and $I(X,Y)_{A,E}$ is called the advantage creation by the knowledge on j. This is a core of the Y-00 principle.

Appendix B. Quantum Computer and Quantum-Computer-Resistant Cryptography

It is difficult to predict the realization of a quantum computer capable of cryptoanalysis. It was discovered in our recent paper [40] 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 cause serious damage to scalable quantum computers, and cause serious degradation to the capability of the 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 [41–44]. 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 [45] 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 quantum key distribution 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., quantum key distribution, which requires very expensive custom hardware. For functions of authentication, signature, and key distribution, such capability provided by software is very important in real-world applications.

Appendix C. Advanced Quantum Detection and Estimation Theory

The development of modern optical communications has been remarkable and its communication abilities are providing its benefits to all regions of the globe. Any communication technology must assume the current performance of optical communication when one intends to provide new functions in communication technology. It is not acceptable to sacrifice this communication ability in order to provide new functions. The communication distance and speed required by the real world cannot be achieved except in a conventional light source. One of the reasons for this is that laser light as a light source has a very stable quantum property called coherent state. The Y-00 quantum stream cipher is the most typical technology to provide a new feature of security to ordinary optical communications having a coherent state. Its basic technology is to use the quantum communication theory [4,5,46] in order to enhance the quantumness of the signal ensemble under high power coherent state signal. Further development along this concept is expected in the future. In particular, the theories of M. Ban [47], S. van Enk [48], S. Pirandola [49,50], M. G. A. Paris [51], and others will contribute to the development of generalized Y-00, and others. In fact, attempts have been made to integrate these theories as a no-go theorem [52–55].

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. Yuen, H.P. KCQ: Keyed communication in quantum noise. *arXiv* **2003**, arXiv:0311061.
4. Holevo, A.S. Statistical decision theory for quantum systems. *J. Multivar. Anal.* **1973**, *3*, 337–394. [CrossRef]
5. 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. [CrossRef]
6. Hirota, O.; Ikehara, S. Minimax strategy in the quantum detection theory and its application to optical communications. *Trans. IEICE Jpn.* **1982**, *65E*, 627.
7. Kato, K. Non-orthogonality measures for a collection of pure quantum states. *Entropy* **2022**, *24*, 581. [CrossRef]
8. Borbosa, G.A.; Corndorf, E.; Kumar, P.; Yuen, H.P. Secure communication using mesoscopic coherent states. *Phys. Rev. Lett.* **2003**, *90*, 227901. [CrossRef]
9. 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. [CrossRef]
10. 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. [CrossRef]
11. 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. [CrossRef]
12. Nair, R.; Yuen, H.P.; Corndolf, E.; Kumar, P. Quantum noise randomized ciphers. *Phys. Rev. A* **2006**, *74*, 052309. [CrossRef]
13. Hirota, O.; Kurosawa, K. Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol. *Quantum Inf. Process.* **2007**, *6*, 81–91. [CrossRef]
14. Hirota, O. Practical security analysis of quantum stream cipher by Yuen protocol. *Phys. Rev. A* **2007**, *76*, 032307. [CrossRef]
15. Yuen, H.P. Key generation: Foundation and new quantum approach. *IEEE Sel. Top. Quant. Electron.* **2009**, *15*, 1630–1645. [CrossRef]
16. Shor, P.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
17. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1. [CrossRef]
18. Hirota, O. Application of quantum Pinsker inequality to quantum communications. *arXiv* **2020**, arXiv:2005.04553.
19. 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.
20. Hirota, O.; Sohma, M.; Kawanishi, K. Quantum noise randamized stream cipher:Y-00. *Jpn. J. Opt.* **2010**, *39*, 17.
21. 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 Communciations and Quantum Imaging IV, San Diego, CA, USA, 13–17 August 2006; Volume 6305.

22. 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. [CrossRef]
23. 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. [CrossRef]
24. Tanizawa, K.; Futami, F. 2^{14} intensity-level 10-Gbaud Y-00 quantum stream cipher enabled by coarse-to-fine modulation. *IEEE Photonics Technol. Lett.* **2018**, *30*, 1987–1990. [CrossRef]
25. Tanizawa, K.; Futami, F. Digital coherent PSK Y-00 quantum stream cipher with 217 randomized phase levels. *Opt. Express* **2019**, *27*, 1071–1079. [CrossRef] [PubMed]
26. 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. [CrossRef] [PubMed]
27. 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. [CrossRef]
28. 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. [CrossRef] [PubMed]
29. Tanizawa, K.; Futami, F. Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system. *Opt. Express* **2021**, *29*, 10451–10464. [CrossRef]
30. 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.
31. NSA. Quantum Computing and Post-Quantum Cryptography FAQs, National Security Agency Central Security Service. 2021. Available online: https://www.quantum.gov/nsa-updates-faq-on-post-quantum-cybersecurity/?msclkid=525975f1cdce11eca34ea2e9f2b11545 (accessed on 1 March 2022).
32. 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. [CrossRef]
33. 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. [CrossRef]
34. 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. [CrossRef] [PubMed]
35. 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. [CrossRef]
36. 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*; Optical Society of America: Washington, DC, USA, 2021.
37. Yang, X.; Zhang, J.; Li, Y.; Zhao, Y.; Zhang, H. DFTs-OFDM based quantum noise stream cipher system. *Opt. Commun.* **2019**, *445*, 29. [CrossRef]
38. 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, 5D1-3; OECC: Camden, AR, USA, 2018.
39. 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. [CrossRef]
40. Hirota, O. Introduction to semi-classical analysis for digital errors of qubit in quantum prosessor. *Entropy* **2021**, *23*, 1577. [CrossRef] [PubMed]
41. Dinc, F.; Bran, A.M. Non-Markovian super-superradiance in a linear chain of up to 100 qubits. *Phys Rev. Res.* **2019**, *1*, 032042. [CrossRef]
42. Fang, K.; Liu, Z. No-Go Theorems for Quantum Resource Purification. *Phys. Rev. Lett.* **2020**, *125*, 060405. [CrossRef]
43. Bousba, Y.; Russell, T. No quantum Ramsey theorem for stabilizer codes. *IEEE Trans. Inform. Theory* **2021**, *67*, 408–415. [CrossRef]
44. Asiani, M.; Chai, J.; Whitney, R.; Auffeves, A.; Ng, H. Limitations in quantum computing from resource constraints. *arXiv* **2020**, arXiv:2007.01966.
45. Mattsson, J.P.; Smeets, B.; Thormarker, E. Quantum-Resistant Cryptography. *arXiv* **2021**, arXiv:2112.00399.
46. Helstrom, C.W. *Quantum Detection and Estimation Theory*; Academic Press: New York, NY, USA, 1976.
47. Ban, M.; Kurokawa, K.; Momose, R.; Hirota, O. Optimum measurements for discrimination among symmetric quantum states and parameter estimation. *Int. J. Theor. Phys.* **1997**, *36*, 1269–1288. [CrossRef]
48. van Enk, S.J. Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography. *Phys. Rev. A* **2002**, *66*, 042313. [CrossRef]
49. Pirandola, S. Quantum reading of a classical digital memory. *Phys. Rev. Lett.* **2011**, *106*, 090504. [CrossRef] [PubMed]
50. Pirandola, S.; Lupo, C.; Giovannetti, V.; Mancini, S.; Braunstein, S.L. Quantum reading capacity. *New J. Phys.* **2011**, *13*, 113012. [CrossRef]
51. Paris, M.G.A. Quantum estimation for quantum technology. *Int. J. Quantum Inf.* **2009**, *7*, 125. [CrossRef]
52. Nakahira, K.; Kato, K.; Usuda, T. Minimax strategy in quantum signal detection with inconclusive results. *Phys. Rev. A* **2013**, *88*, 032314. [CrossRef]

53. Nakahira, K.; Kato, K.; Usuda, T. Generalized quantum state discrimination problems. *Phys. Rev. A* **2015**, *91*, 052304. [CrossRef]
54. Nakahria, K.; Usuda, T.; Kato, K. Finding Optimal Solutions for Generalized Quantum State Discrimination Problems. *IEEE Trans. Inf. Theory* **2017**, *63*, 7845. [CrossRef]
55. Nakahira, K.; Kato, K. Generalized quantum process discrimination problems. *Phys. Rev. A* **2021**, *103*, 062606. [CrossRef]