entropy

Special Issue Reprint

Quantum Communication, Quantum Radar, and Quantum Cipher

Edited by
Osamu Hirota

www.mdpi.com/journal/entropy

MDPI

Quantum Communication, Quantum Radar, and Quantum Cipher

Quantum Communication, Quantum Radar, and Quantum Cipher

Editor

Osamu Hirota

MDPI

Basel • Beijing • Wuhan • Barcelona • Belgrade • Novi Sad • Cluj • Manchester

Editor
Osamu Hirota
Quantum ICT Research
Institute
Tamagawa University
Tokyo, Japan

Editorial Office
MDPI
St. Alban-Anlage 66
4052 Basel, Switzerland

This is a reprint of articles from the Special Issue published online in the open access journal *Entropy* (ISSN 1099-4300) (available at: https://www.mdpi.com/journal/entropy/special_issues/quantum_commu_radar).

For citation purposes, cite each article independently as indicated on the article page online and as indicated below:

Lastname, A.A.; Lastname, B.B. Article Title. *Journal Name* **Year**, *Volume Number*, Page Range.

ISBN 978-3-0365-8560-4 (Hbk)
ISBN 978-3-0365-8561-1 (PDF)
doi.org/10.3390/books978-3-0365-8561-1

Contents

About the Editor

Osamu Hirota

Osamu Hirota, Ph.D., is Professor Emeritus at the Quantum ICT Research Institute of Tamagawa University and Research Professor at the Research and Development Initiative of Chuo University. His research focusses on studying quantum communication theory and quantum noise analysis of quantum computers. He has received the following prizes and awards: The Takayanagi Kenjiro Research Encouragement Prize (1986), Telecom System Technology Prize (1987), Quantum Information Science Award (2002), and Telecom Advanced Tech. Center, President Prize (2022). He obtained a PhD in Physical Electronics (1981) from the Tokyo Institute of Technology.

Preface

Quantum information science has become established as a basic science thanks to the contributions of many pioneers, and the time has now come to seek practical applications based on applied research. Until now, discussions have been based on microscopic qubits to discuss the principle possibilities. However, in order to make quantum information science applicable to the real world, it is necessary to change direction to focus on engineering technology based on macroscopic qubits. If this is achieved, quantum communication will further expand the possibilities of ultrahigh-speed optical communication, quantum radar will enable the feasibility of all-weather sensors, and macroscopic quantum cryptography will contribute to enhancing the security of the physical layer of current optical networks. In addition, decoherence properties of quantum processors are clarified toward scaling for real applications of quantum technology. The purpose of this Special Issue is to consolidate and publish the latest research trends by researchers who are conducting research toward the above goals. It consists of invited papers, original papers, short reviews, and proposals for the future prospects in this field.

Osamu Hirota
Editor

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

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

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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".

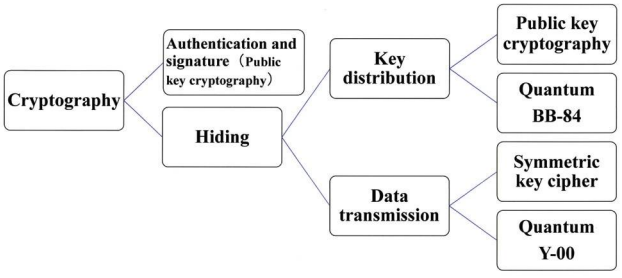


Figure 1. Classification of cryptographic techniques.

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 $|\Psi(X, K_s, R_p)>$ 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:

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

where $|\alpha_i(X, f_g(K_s), R_p)>$ 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.

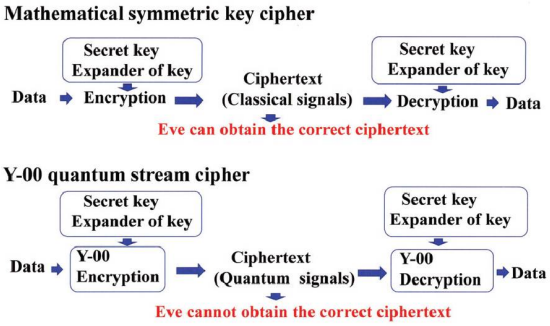


Figure 2. Principle of operation of Y-00 quantum stream cipher. Classical signal means that they have distinguishability, and quantum signal means it is impossible to distinguish them precisely. Y-00 encryption is the function of converting a classical signal into a quantum signal. It is also called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

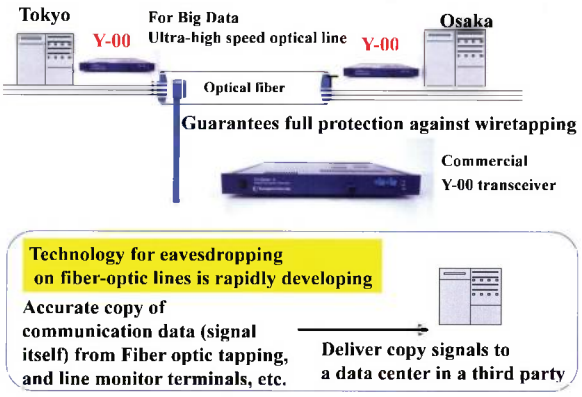


Figure 4. Application to data center communication security (protection against eavesdropping, tampering, and virus injection from communication lines). Commercial transceiver is for 1 Git/s optical ethernet. This can be mass produced.

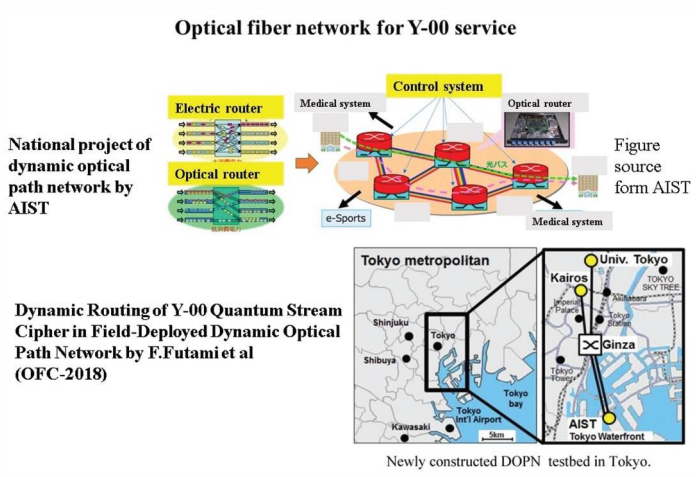


Figure 5. Scheme of optical network by dynamic path and experimental demonstration of service of the Y-00 quantum stream cipher by Tamagawa University and AIST in Tokyo Bay Coastal area.

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 $-M/2 \leq h \leq M/2$.

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]

entropy

MDPI

Article

On the Classical Capacity of General Quantum Gaussian Measurement

Alexander Holevo

Steklov Mathematical Institute, RAS, 119991 Moscow, Russia; holevo@mi-ras.ru

Abstract: In this paper, we consider the classical capacity problem for Gaussian measurement channels. We establish Gaussianity of the average state of the optimal ensemble in the general case and discuss the Hypothesis of Gaussian Maximizers concerning the structure of the ensemble. Then, we consider the case of one mode in detail, including the dual problem of accessible information of a Gaussian ensemble. Our findings are relevant to practical situations in quantum communications where the receiver is Gaussian (say, a general-dyne detection) and concatenation of the Gaussian channel and the receiver can be considered as one Gaussian measurement channel. Our efforts in this and preceding papers are then aimed at establishing full Gaussianity of the optimal ensemble (usually taken as an assumption) in such schemes.

Keywords: Gaussian measurement channel; classical capacity; Gaussian ensemble; accessible information; Gaussian maximizer

Citation: Holevo, A. On the Classical Capacity of General Quantum Gaussian Measurement. *Entropy* **2021**, *23*, 377. https://doi.org/10.3390/e23030377

Academic Editor: Osamu Hirota

Received: 2 March 2021
Accepted: 19 March 2021
Published: 21 March 2021

1. Introduction

From the viewpoint of information theory, measurements are hybrid communication channels that transform input quantum states into classical output data. As such, they are described by the classical information capacity which is the most fundamental quantity characterizing their ultimate information-processing performance [1–4]. Channels with continuous output, such as bosonic Gaussian measurements, do not admit direct embedding into properly quantum channels and, hence, require separate treatment. In particular, their output entropy is the Shannon differential entropy, instead of the quantum entropy, which completely changes the pattern of the capacity formulas. The classical capacity of multimode Gaussian measurement channels was computed in Reference [5] under so-called threshold condition (which includes phase-insensitive or gauge covariant channels as a special case [6]). The essence of this condition is that it reduces the classical capacity problem to the minimum output differential entropy problem solved in Reference [7] (in the context of quantum Gaussian channels, a similar condition was introduced and studied in References [8,9]; also see references therein).

In this paper, we approach the classical capacity problem for Gaussian measurement channels without imposing any kind of threshold condition. In particular, in the framework of quantum communication, this means that both (noisy) heterodyne and (noisy/noiseless) homodyne measurements [10,11] are treated from a common viewpoint. We prove Gaussianity of the average state of the optimal ensemble in general and discuss the Hypothesis of Gaussian Maximizers (HGM) concerning the structure of the ensemble. The proof uses the approach of the paper of Wolf, Giedke, and Cirac [12] applied to the convex closure of the output differential entropy. Then, we discuss the case of one mode in detail, including the dual problem of accessible information of a Gaussian ensemble.

In quantum communications, there are several studies of the classical capacity in the transmission scheme where not only the Gaussian channel but also the receiver is fixed, and the optimization is performed over certain set of the input ensembles (see References [10,13–15] and references therein). These studies are practically important in view of greater complexity of the optimal receiver in the Quantum Channel Coding (HSW)

theorem (see, e.g., Reference [16]). Our findings are relevant to such a situation where the receiver is Gaussian and concatenation of the channel and the receiver can be considered as one Gaussian measurement channel. Our efforts in this and preceding papers are then aimed at establishing full Gaussianity of the optimal ensemble (usually taken as a key assumption) in such schemes.

2. The Measurement Channel and Its Classical Capacity

An *ensemble* $\mathcal{E} = \{\pi(dx), \rho(x)\}$ consists of probability measure $\pi(dx)$ on a standard measurable space $\mathcal{X}$ and a measurable family of density operators (quantum states) $x \to \rho(x)$ on the Hilbert space $\mathcal{H}$ of the quantum system. The *average state* of the ensemble is the barycenter of this measure:

$$\bar{\rho}_{\mathcal{E}} = \int_{\mathcal{X}} \rho(x)\, \pi(dx),$$

the integral existing in the strong sense in the Banach space of trace-class operators on $\mathcal{H}$.

Let $M = \{M(dy)\}$ be an observable (POVM) on $\mathcal{H}$ with the outcome standard measurable space $\mathcal{Y}$. There exists a $\sigma-$finite measure $\mu(dy)$ such that, for any density operator ρ, the probability measure $\mathrm{Tr}\rho M(dy)$ is absolutely continuous w.r.t. $\mu(dy)$, thus having the probability density $p_\rho(y)$ (one can take $\mu(dy) = \mathrm{Tr}\rho_0 M(dy)$, where ρ_0 is a nondegenerate density operator). The affine map $M : \rho \to p_\rho(\cdot)$ will be called the *measurement channel*.

The joint probability distribution of x, y on $\mathcal{X} \times \mathcal{Y}$ is uniquely defined by the relation

$$P(A \times B) = \int_A \pi(dx) \mathrm{Tr}\, \rho(x) M(B) = \int_A \int_B p_{\rho(x)}(y)\, \pi(dx)\mu(dy),$$

where A is an arbitrary Borel subset of $\mathcal{X}$, and B is that of $\mathcal{Y}$. The classical Shannon information between x, y is equal to

$$I(\mathcal{E}, M) = \int \int \pi(dx)\mu(dy) p_{\rho(x)}(y) \log \frac{p_{\rho(x)}(y)}{p_{\bar{\rho}_{\mathcal{E}}}(y)}.$$

In what follows, we will consider POVMs having (uniformly) bounded operator density, $M(dy) = m(y)\mu(dy)$, with $\|m(y)\| \leq b$, so that the probability densities $p_\rho(y) = \mathrm{Tr}\,\rho m(y)$ are uniformly bounded, $0 \leq p_\rho(y) \leq b$. (The probability densities corresponding to Gaussian observables we will be dealing with possess this property). Moreover, without loss of generality [6] we can assume $b = 1$. Then, the output differential entropy

$$h_M(\rho) = -\int p_\rho(y) \log\, p_\rho(y) \mu(dy) \tag{1}$$

is well defined with values in $[0, +\infty]$ (see Reference [6] for the details). The output differential entropy is concave lower semicontinuous (w.r.t. trace norm) functional of a density operator ρ. The concavity follows from the fact that the function $p \to -p \log p$, $p \in [0, 1]$ is concave. Lower semicontinuity follows by an application of the Fatou-Lebesgue lemma from the fact that this function is nonnegative, continuous, and $\left|p_\rho(y) - p_\sigma(y)\right| \leq \|\rho - \sigma\|_1$.

Next, we define the *convex closure of the output differential entropy* (1):

$$e_M(\rho) = \inf_{\mathcal{E}:\bar{\rho}_{\mathcal{E}}=\rho} \int h_M(\rho(x))\pi(dx), \tag{2}$$

which is the "measurement channel analog" of the convex closure of the output entropy for a quantum channel [17].

Lemma 1. *The functional $e_M(\rho)$ is convex, lower semicontinuous and strongly superadditive:*

$$e_{M_1 \otimes M_2}(\rho_{12}) \geq e_{M_1}(\rho_1) + e_{M_2}(\rho_2). \tag{3}$$

As it is well known, the property (3) along with the definition (2) imply *additivity*: if $\rho_{12} = \rho_1 \otimes \rho_2$ then

$$e_{M_1 \otimes M_2}(\rho_{12}) = e_{M_1}(\rho_1) + e_{M_2}(\rho_2). \tag{4}$$

Proof. The lower semicontinuity follows from the similar property of the output differential entropy much in the same way as in the case of quantum channels, treated in Reference [17], Proposition 4; also see Reference [18], Proposition 1.

Let us prove strong superadditivity. Let

$$\rho_{12} = \int \rho_{12}(x)\pi(dx) \tag{5}$$

be a decomposition of a density operator ρ_{12} on $\mathcal{H}_1 \otimes \mathcal{H}_2$, then

$$\begin{aligned} & p_{M_1 \otimes M_2}(y_1, y_2|x) \\ = \; & \operatorname{Tr} \rho_{12}(x)[m_1(y_1) \otimes m_2(y_2)] \\ = \; & \operatorname{Tr} \rho_1(x)\, m_1(y_1) \operatorname{Tr} \rho_2(y_1, x)\, m_2(y_2) \\ = \; & p_{M_1}(y_1|x)\, p_{M_2}(y_2|y_1, x), \end{aligned}$$

where $\rho_1(x) = \operatorname{Tr}_2 \rho_{12}(x), \rho_2(y_1, x) = \frac{\operatorname{Tr}_1 \rho_{12}(x)[m_1(y_1) \otimes I_2]}{\operatorname{Tr} \rho_{12}(x)[m_1(y_1) \otimes I_2]}$, so that

$$\operatorname{Tr} \rho_{12}(x)[m_1(y_1) \otimes I_2] = \operatorname{Tr} \rho_1(x)\, m_1(y_1) = p_{M_1}(y_1|x),$$

and $\rho_2 = \int \int \rho_2(y_1, x) p_{M_1}(y_1|x)\pi(dx)\mu_1(dy_1)$ while $\rho_1 = \int \rho_1(x)\pi(dx)$. It follows that:

$$\begin{aligned} h(Y_1, Y_2|X) \; \equiv \; & \int h_{M_1 \otimes M_2}(\rho_{12}(x))\pi(dx) \\ = \; & \int h_{M_1}(\rho_1(x))\pi(dx) \\ + \; & \int \int h_{M_2}(\rho_2(y_1, x)) p_{M_1}(y_1|x)\pi(dx)\mu_1(dy_1) \\ = \; & h(Y_1|X) + h(Y_2|Y_1, X), \end{aligned}$$

and, whence taking the infimum over decompositions (5), we obtain (3). □

Let H be a Hamiltonian in the Hilbert space $\mathcal{H}$ of the quantum system, E a positive number. Then, the *energy-constrained classical capacity* of the channel M is equal to

$$C(M, H, E) = \sup_{\mathcal{E}: \operatorname{Tr} \bar{\rho}_{\mathcal{E}} H \leq E} I(\mathcal{E}, M), \tag{6}$$

where maximization is over the input ensembles of states $\mathcal{E}$ satisfying the energy constraint $\operatorname{Tr} \bar{\rho}_{\mathcal{E}} H \leq E$, as shown in Reference [5], proposition 1.

If $h_M(\bar{\rho}_{\mathcal{E}}) < +\infty$, then

$$I(\mathcal{E}, M) = h_M(\bar{\rho}_{\mathcal{E}}) - \int h_M(\rho(x))\pi(dx). \tag{7}$$

Note that the measurement channel is entanglement-breaking [16]; hence, its classical capacity is additive and is given by the one-shot expression (6). By using (7), (2), we obtain

$$C(M, H, E) = \sup_{\rho: \operatorname{Tr} \rho H \leq E} [h_M(\rho) - e_M(\rho)]. \tag{8}$$

3. Gaussian Maximizers for Multimode Bosonic Gaussian Observable

Consider now multimode bosonic Gaussian system with the quadratic Hamiltonian $H = R\epsilon R^t$, where $\epsilon > 0$ is the energy matrix, and $R = [q_1, p_1, \ldots, q_s, p_s]$ is the row vector of the bosonic position-momentum observables, satisfying the canonical commutation relation

$$[R^t, R] = i\Delta I, \quad \Delta = \operatorname{diag}\Big[\underbrace{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}}_{1,\ldots,s}\Big],$$

(see, e.g., References [11,16]). This describes quantization of a linear classical system with s degrees of freedom, such as finite number of physically relevant electromagnetic modes on the receiver's aperture in quantum optics.

From now on, we will consider only states with finite second moments. By $\mathfrak{S}(\alpha)$, we denote the set of all states ρ with the fixed correlation matrix

$$\alpha = \operatorname{Re} \operatorname{Tr} R^t \rho R.$$

For *centered* states (i.e., states with vanishing first moments), the covariance matrix and the matrix of second moments coincide. We denote by ρ_α centered Gaussian state with the correlation matrix $\alpha \geq \pm i/2\Delta$. For states $\rho \in \mathfrak{S}(\alpha)$, we have $h_M(\rho) \leq h_M(\rho_\alpha) < +\infty$, by the maximum entropy principle.

The energy constraint reduces to

$$\operatorname{Sp} \alpha\, \epsilon \leq E. \tag{9}$$

(We denote Sp trace of $s \times s$-matrices as distinct from trace of operators on $\mathcal{H}$.)

For a fixed correlation matrix α, we will study the *α-constrained* capacity

$$C(M;\alpha) = \sup_{\mathcal{E}:\bar{\rho}_{\mathcal{E}} \in \mathfrak{S}(\alpha)} I(\mathcal{E}, M) = \sup_{\rho \in \mathfrak{S}(\alpha)} [h_M(\rho) - e_M(\rho)]. \tag{10}$$

With the Hamiltonian $H = R\epsilon R^t$, the *energy-constrained classical capacity* of observable M is

$$C(M; H, E) = \sup_{\alpha: \operatorname{Sp} \alpha\epsilon \leq E} C(M;\alpha).$$

We will be interested in the approximate position-momentum measurement (observable, POVM)

$$M(d^{2s}z) = D(z)\rho_\beta D(z)^* \frac{d^{2s}z}{(2\pi)^s} \tag{11}$$

where $\bar{\rho}_\beta$ is centered Gaussian density operator with the covariance matrix β and

$$D(z) = \exp i \sum_{j=1}^{s} (y_j q_j - x_j p_j), \quad z = \begin{bmatrix} x_1, y_1, & \ldots, & x_s, y_s \end{bmatrix}^t \in \mathbb{R}^{2s}$$

are the unitary displacement operators. Thus, $\mu(dz) = \frac{d^{2s}z}{(2\pi)^s}$ and the operator-valued density of POVM (11) is $m(z) = D(z)\rho_\beta D(z)^*$. In quantum optics, some authors [11,19] call such measurements (noisy) general-dyne detections.

In what follows, we will consider n independent copies of our bosonic system on the Hilbert space $\mathcal{H}^{\otimes n}$. We will supply all the quantities related to $k-$th copy ($k = 1, \ldots, n$) with upper index $^{(k)}$, and we will use tilde to denote quantities related to the whole collection on n copies. Thus,

$$\tilde{z} = \begin{bmatrix} z^{(1)} \\ \ldots \\ z^{(n)} \end{bmatrix}, \quad D(\tilde{z}) = D(z^{(1)}) \otimes \cdots \otimes D(z^{(n)})$$

and

$$M^{\otimes n}(d\tilde{z}) = \tilde{m}(\tilde{z})\tilde{\mu}(d\tilde{z}) = \left[m(z^{(1)}) \otimes \cdots \otimes m(z^{(n)})\right] \mu(dz^{(1)}) \ldots \mu(dz^{(n)}).$$

Lemma 2. *Let $O = [O_{kl}]_{k,l=1,\ldots,n}$ be a real orthogonal $n \times n$—matrix and U—the unitary operator on $\mathcal{H}^{\otimes n}$ implementing the linear symplectic transformation*

$$\tilde{R} = \left[\begin{array}{ccc} R^{(1)}, & \ldots, & R^{(n)} \end{array} \right] \to \tilde{R}\, O,$$

so that

$$U^* D(\tilde{z}) U = D(O\,\tilde{z}). \tag{12}$$

Then, for any state $\tilde{\rho}$ on $\mathcal{H}^{\otimes n}$,

$$e_{M^{\otimes n}}(\tilde{\rho}) = e_{M^{\otimes n}}(U\tilde{\rho}U^*). \tag{13}$$

Proof. The covariance matrix $\tilde{\beta}$ of $\rho_\beta^{\otimes n}$ is block-diagonal, $\tilde{\beta} = [\delta_{kl}\beta]_{k,l=1,\ldots,n}$; hence, $O^t\tilde{\beta}O = \tilde{\beta}$. Thus, we have $U^*\rho_{\tilde{\beta}}^{\otimes n}U = \rho_{\tilde{\beta}}^{\otimes n}$, and taking into account (12),

$$U^*\tilde{m}(\tilde{z})U = D(O\,\tilde{z})\rho_{\tilde{\beta}}^{\otimes n} D(O\,\tilde{z})^* = \tilde{m}(O\tilde{z}).$$

Therefore, for any state $\tilde{\sigma}$ on $\mathcal{H}^{\otimes n}$, the output probability density of the measurement channel $\tilde{M} = M^{\otimes n}$ corresponding to the input state $U\tilde{\sigma}U^*$ is

$$p_{U\tilde{\sigma}U^*}(\tilde{z}) = \mathrm{Tr}\,(U\tilde{\sigma}U^*)\tilde{m}(\tilde{z}) = \mathrm{Tr}\,\tilde{\sigma}\tilde{m}(O\tilde{z}) = p_{\tilde{\sigma}}(O\tilde{z}). \tag{14}$$

Hence, by using orthogonal invariance of the Lebesgue measure,

$$h_{M^{\otimes n}}(U\tilde{\sigma}U^*) = h_{M^{\otimes n}}(\tilde{\sigma}).$$

If $\tilde{\rho} = \int_{\mathcal{X}} \tilde{\rho}(x)\,\pi(dx)$, then $U\tilde{\rho}U^* = \int_{\mathcal{X}} (U\tilde{\rho}(x)\,U^*)\pi(dx)$, and taking $\tilde{\sigma} = \tilde{\rho}(x)$ in the previous formula, we deduce

$$\int_{\mathcal{X}} h_{M^{\otimes n}}(U\tilde{\rho}(x)U^*)\pi(dx) = \int_{\mathcal{X}} h_{M^{\otimes n}}(\tilde{\rho}(x))\pi(dx);$$

hence, (13) follows. □

Lemma 3. *Let M be the Gaussian measurement (11). For any state ρ with finite second moments, $e_M(\rho) \geq e_M(\rho_\alpha)$, where α is the covariance matrix of ρ.*

Proof. The proof follows the pattern of Lemma 1 from the paper of Wolf, Giedke, and Cirac [12]. Without loss of generality, we can assume that ρ is centered. We have

$$e_M(\rho) \overset{(1)}{=} \frac{1}{n} e_{M^{\otimes n}}(\rho^{\otimes n}) \overset{(2)}{=} \frac{1}{n} e_{M^{\otimes n}}(\tilde{\rho}) \overset{(3)}{\geq} \frac{1}{n}\sum_{k=1}^{n} e_M(\tilde{\rho}^{(k)}), \tag{15}$$

where $\tilde{\rho} = U\rho^{\otimes n}U^*$ with symplectic unitary U in $\mathcal{H}^{\otimes n}$, corresponding to an orthogonal matrix O as in Lemma 2, and $\tilde{\rho}^{(k)}$ is the k—th partial state of $\tilde{\rho}$.

Step (1) follows from the additivity (4). Step (2) follows from lemma 2, and step (3) follows from the superadditivity of e_M (Lemma 1). The final step of the proof,

$$\liminf_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} e_M(\tilde{\rho}^{(k)}) \geq e_M(\rho_\alpha), \tag{16}$$

uses ingeniously constructed U from Reference [12] and lower semicontinuity of e_M (Lemma 1). Namely, $n = 2^m$, and U corresponds via (12) to the following special orthogonal matrix

$$O = [O_{kl}|_{k,l=1,\ldots,n} = H^{\otimes m}, \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Every row of the $n \times n-$matrix O, except the first one which has all the elements 1, has $n/2 = 2^{m-1}$ elements equal to 1 and $n/2$ elements equal to -1. Then, the quantum characteristic function of the states $\tilde{\rho}^{(k)}, k = 2, \ldots, n$ is equal to $\phi(z/\sqrt{n})^{n/2}\phi(-z/\sqrt{n})^{n/2}$, where $\phi(z)$ is the quantum characteristic function of the state ρ. This allows to apply Quantum Central Limit Theorem [20] to show that $\tilde{\rho}^{(k)} \to \rho_\alpha$ as $n \to \infty$, in a uniform way, implying (16); see Reference [12] for details. □

Theorem 1. *The optimizing density operator ρ in (10) is the (centered) Gaussian density operator ρ_α :*

$$C(M;\alpha) = h_M(\rho_\alpha) - e_M(\rho_\alpha), \tag{17}$$

and, hence,

$$C(M,H,E) = \max_{\alpha:\mathrm{Sp}\,\alpha \leq E} C(M;\alpha) = \max_{\alpha:\mathrm{Sp}\,\alpha \leq E} [h_M(\rho_\alpha) - e_M(\rho_\alpha)]. \tag{18}$$

Proof. Lemma 3 implies that, for any ρ with finite second moments, $e_M(\rho) \geq e_M(\rho_\alpha)$, where α is the covariance matrix of ρ. On the other hand, by the maximum entropy principle, $h_M(\rho) \leq h_M(\rho_\alpha)$. Hence, (17) is maximized by a Gaussian density operator. □

Remark 1. *The proof of Lemma 2 and, hence, of Theorem 1 can be extended to a general Gaussian observable M in the sense of Reference [16,21], defined via operator-valued characteristic function of the form*

$$\phi_M(w) = \exp\left(i\,R\,Kw - \frac{1}{2}w^t\gamma w\right), \tag{19}$$

where K is a scaling matrix, γ is the measurement noise covariance matrix, and $\gamma \geq \pm\frac{i}{2}K^t\Delta K$. Then, the Fourier transform of the measurement probability density $p_\rho(z)$ is equal to $\mathrm{Tr}\,\rho\phi_M(w)$, and one can use this function to obtain generalization of the relation (14) for the measurement probability densities. The case (11) corresponds to the type 1 Gaussian observable [21] with $K = I_{2s}, \gamma = \beta$. However, (19) also includes type 2 and 3 observables (noisy and noiseless multimode homodyning), in which case K is a projection onto an isotropic subspace of Z (i.e., one on which the symplectic form Δ vanish.)

Remark 2. *Theorem 1 establishes Gaussianity of the average state of the optimal ensemble for a general Gaussian measurement channel. However, Gaussian average state can appear in a non-Gaussian ensemble. An immediate example is thermal state represented as a mixture of the Fock states with geometric distribution. Thus, Theorem 1 does not necessarily imply full Gaussianity of the optimal ensemble as formulated in the following conjecture.*

Hypothesis of Gaussian Maximizers (HGM). *Let M be an arbitrary Gaussian measurement channel. Then, there exists an optimal Gaussian ensemble for the convex closure of the output differential entropy (2) with Gaussian ρ and, hence, for the energy-constrained classical capacity (6) of the channel M. More explicitly, the ensemble consists of (properly squeezed) coherent states with the displacement parameter having Gaussian probability distribution.*

For Gaussian measurement channels of the type 1 (essentially of the form (11), see Reference [21] for complete classification) and Gaussian states ρ_α satisfying the "threshold condition" , we have

$$e_M(\rho_\alpha) = \min_\rho h_M(\rho), \tag{20}$$

with the minimum attained on a squeezed coherent state, which implies the validity of the HGM and an efficient computation of $C(M, H, E)$; see Reference [5]. On the other hand, the problem remains open in the case where the "threshold condition" is violated, and in particular, for all Gaussian measurement channels of the type 2 (noisy homodyning), with the generic example of the energy-constrained approximate measurement of the position $[q_1, \ldots, q_s]$ subject to Gaussian noise (see Reference [22], where the entanglement-assisted capacity of such a measurement was computed). In the following section, we will touch upon the HGM in this case for one mode system.

4. Gaussian Measurements in One Mode

Our framework in this section will be one bosonic mode described by the canonical position and momentum operators q, p . We recall that

$$D(x,y) = \exp i(yq - xp), \quad x, y \in \mathbb{R}$$

are the unitary displacement operators.

We will be interested in the observable

$$M(dxdy) = D(x,y)\rho_\beta D(x,y)^* \frac{dxdy}{2\pi}, \tag{21}$$

where ρ_β is centered Gaussian density operator with the covariance matrix

$$\beta = \begin{bmatrix} \beta_q & 0 \\ 0 & \beta_p \end{bmatrix}; \quad \beta_q\beta_p \geq \frac{1}{4}. \tag{22}$$

Let ρ_α be a centered Gaussian density operator with the covariance matrix

$$\alpha = \begin{bmatrix} \alpha_q & 0 \\ 0 & \alpha_p \end{bmatrix}. \tag{23}$$

The problem is, to compute $e_M(\rho_\alpha)$ and, hence, the classical capacity $C(M, H, E)$ for the oscillator Hamiltonian $H = \frac{1}{2}(q^2 + p^2)$ (as shown in the Appendix of Reference [22], we can restrict to Gaussian states ρ_α with the diagonal covariance matrix in this case). The energy constraint (9) takes the form

$$\alpha_q + \alpha_p \leq 2E. \tag{24}$$

The measurement channel corresponding to POVM (21) acts on the centered Gaussian state ρ_α by the formula

$$\begin{aligned} M \quad &: \quad \rho_\alpha \to p_{\rho_\alpha}(x,y) \\ &= \quad \frac{1}{\sqrt{2\pi(\alpha_q + \beta_q)(\alpha_p + \beta_p)}} \exp\left[-\frac{x^2}{2(\alpha_q + \beta_q)} - \frac{y^2}{2(\alpha_p + \beta_p)}\right], \end{aligned} \tag{25}$$

so that

$$h_M(\rho_\alpha) = \frac{1}{2}\log(\alpha_q + \beta_q)(\alpha_p + \beta_p) + c. \tag{26}$$

In this expression, c is a fixed constant depending on the normalization of the underlying measure μ in (1). It does not enter the information quantities which are differences of the two differential entropies.

Assuming validity of the HGM, we will optimize over ensembles of squeezed coherent states

$$\rho_{x,y} = D(x,y)\,\rho_\Lambda D(x,y)^*, \quad (x,y) \in \mathbb{R}^2,$$

where ρ_Λ is centered Gaussian state with correlation matrix $\Lambda = \begin{bmatrix} \delta & 0 \\ 0 & 1/(4\delta) \end{bmatrix}$, and the vector (x,y) has centered Gaussian distribution with covariance matrix $\begin{bmatrix} \gamma_q & 0 \\ 0 & \gamma_p \end{bmatrix}$. Then, the average state $\bar{\rho}_\mathcal{E}$ of the ensemble is centered Gaussian ρ_α with the covariance matrix (23), where

$$\alpha_q = \gamma_q + \delta, \quad \alpha_p = \gamma_p + 1/(4\delta);$$

hence,

$$\frac{1}{4\alpha_p} \le \delta \le \alpha_q. \tag{27}$$

For this ensemble,

$$\int h_M(\rho_{x,y})\pi(dx\,dy) = h_M(\rho_\Lambda) = \frac{1}{2}\log(\delta+\beta_q)\,(1/(4\delta)+\beta_p) + c.$$

Then, the hypothetical value:

$$e_M(\rho_\alpha) = \min_{1/(4\alpha_p)\le\delta\le\alpha_q} \frac{1}{2}\log(\delta+\beta_q)\,(1/(4\delta)+\beta_p) + c. \tag{28}$$

The derivative of the minimized expression vanishes for $\delta = \frac{1}{2}\sqrt{\frac{\beta_q}{\beta_p}}$. Thus, depending on the position of this value with respect to the interval (27), we obtain three possibilities):

Here, the column C corresponds to the case where the "threshold condition" holds, implying (20). Then the full validity of the HGM in much more general multimode situation was established in Reference [5]. All the quantities in this column, as well as the value of $C(M,H,E)$ in the central column of Table 2, were obtained in that paper as an example. On the other hand, the HGM remains open in the cases of mutually symmetric columns L and R (for the derivation of the quantities in column L of Tables 1 and 2 see Appendix A).

Table 1. The three parameter ranges.

range	L: $\frac{1}{2}\sqrt{\frac{\beta_q}{\beta_p}} < \frac{1}{4\alpha_p}$	C: $\frac{1}{4\alpha_p} \le \frac{1}{2}\sqrt{\frac{\beta_q}{\beta_p}} \le \alpha_q$	R: $\alpha_q < \frac{1}{2}\sqrt{\frac{\beta_q}{\beta_p}}$
HGM	open	valid	open
δ_{opt}	$1/(4\alpha_p)$	$\frac{1}{2}\sqrt{\frac{\beta_q}{\beta_p}}$	α_q
$e_M(\rho_\alpha) - c$	$\frac{1}{2}\log\left[\left(\frac{1}{4\alpha_p}+\beta_q\right)\times(\alpha_p+\beta_p)\right]$	$\log\left(\sqrt{\beta_q\beta_p}+1/2\right)$	$\frac{1}{2}\log\left[\left(\frac{1}{4\alpha_q}+\beta_p\right)\times(\alpha_q+\beta_q)\right]$
$C(M;\alpha)$	$\frac{1}{2}\log\frac{\alpha_q+\beta_q}{\frac{1}{4\alpha_p}+\beta_q}$	$\frac{1}{2}\log\frac{(\alpha_q+\beta_q)(\alpha_p+\beta_p)}{\left(\sqrt{\beta_q\beta_p}+1/2\right)^2}$	$\frac{1}{2}\log\frac{\alpha_p+\beta_p}{\frac{1}{4\alpha_q}+\beta_p}$

Maximizing $C(M;\alpha)$ over α_q, α_p which satisfy the energy constraint (24) (with the equality): $\alpha_q + \alpha_p = 2E$, we obtain $C(M,H,E)$ depending on the signal energy E and the measurement noise variances β_q, β_p :

Table 2. The values of the capacity $C(M,H,E)$.

L: HGM Open	C: HGM Valid [5]	R: HGM Open
$\beta_q \le \beta_p; E < E(\beta_p,\beta_q)$	$E \ge E(\beta_p,\beta_q) \vee E(\beta_q,\beta_p)$	$\beta_p \le \beta_q; E < E(\beta_q,\beta_p)$
$\log\left(\frac{\sqrt{1+8E\beta_q+4\beta_q^2}-1}{2\beta_q}\right)$	$\log\left(\frac{E+(\beta_q+\beta_p)/2}{\sqrt{\beta_q\beta_p}+1/2}\right)$	$\log\left(\frac{\sqrt{1+8E\beta_p+4\beta_p^2}-1}{2\beta_p}\right)$

where we introduced the "energy threshold function"

$$E(\beta_1,\beta_2) = \frac{1}{2}\left(\beta_1 - \beta_2 + \sqrt{\frac{\beta_1}{\beta_2}}\right).$$

In the gauge invariant case when $\beta_q = \beta_p = \beta$, the threshold condition amounts to $E \ge 1/2$, which is fulfilled by definition, and the capacity formula gives the expression $\log\left(\frac{E+\beta}{\beta+1/2}\right)$ equivalent to one obtained in Hall's 1994 paper [13].

Let us stress that, opposite to column C, the values of $C(M,H,E)$ in the L and R columns are hypothetic, conditional upon validity of the HGM. Looking into the left column, one can see that $C(M;\alpha)$ and $C(M,H,E)$ do not depend at all on β_p. Thus, we can let the variance of the momentum p measurement noise $\beta_p \to +\infty$, and, in fact, set $\beta_p = +\infty$, which is equivalent to the approximate measurement only of the position q described by POVM

$$M(dx) = \exp\left[-\frac{(q-x)^2}{2\beta_q}\right]\frac{dx}{\sqrt{2\pi\beta_q}} = D(x,0)\mathrm{e}^{-q^2/2\beta_q}D(x,0)^*\frac{dx}{\sqrt{2\pi\beta_q}}, \tag{29}$$

which belongs to type 2 according to the classification of Reference [21]. In other words, one makes the "classical" measurement of the observable

$$X = q + \xi, \quad \xi \sim \mathcal{N}(0,\beta_q),$$

with the quantum energy constraint $\mathrm{Tr}\,\rho(q^2+p^2) \le 2E$.

The measurement channel corresponding to POVM (29) acts on the centered Gaussian state ρ_α by the formula

$$M : \rho_\alpha \to p_{\rho_\alpha}(x) = \frac{1}{\sqrt{2\pi(\alpha_q+\beta_q)}}\exp\left[-\frac{x^2}{2(\alpha_q+\beta_q)}\right]. \tag{30}$$

In this case, we have

$$h_M(\rho_\alpha) = \frac{1}{2}\log(\alpha_q+\beta_q) + c, \tag{31}$$

$$e_M(\rho_\alpha) = \frac{1}{2}\log(1/(4\alpha_p)+\beta_q) + c, \tag{32}$$

which differ from the values in the case of finite $\beta_p \to +\infty$ by the absence of the factor $(\alpha_p+\beta_p)$ under the logarithms, while the difference $C(M;\alpha) = h_M(\rho_\alpha) - e_M(\rho_\alpha)$ and the capacity $C(M,H,E)$ have the same expressions as in that case (column L).

For $\beta_q = 0$ (sharp position measurement, type 3 of Reference [21]), the HGM is valid with

$$C(M,H,E) = \log 2E.$$

This follows from the general upper bound (Figure 1)

$$C(M,H,E) \leq \log\left(1+\frac{E-1/2}{\beta_q+1/2}\right) = \log\left(\frac{2(E+\beta_q)}{1+2\beta_q}\right) \tag{33}$$

for $\beta_q \geq 0$ (Equation (28) in Reference [23]; also see Equation (5.39) in Reference [10]).

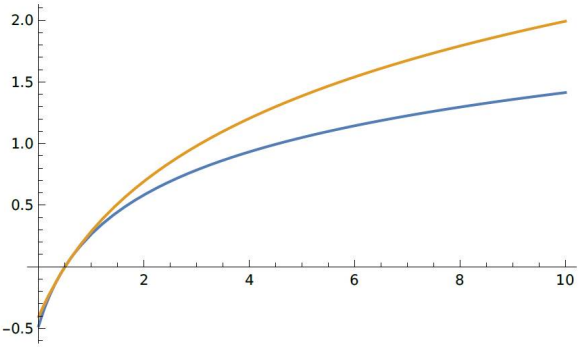


Figure 1. (color online) The Gaussian classical capacity (A6) and the upper bound (33) ($\beta = 1$).

5. The Dual Problem: Accessible Information

Let us sketch here *ensemble-observable duality* [1,2,4] (see Reference [6] for details of mathematically rigorous description in the infinite dimensional case).

Let $\mathcal{E} = \{\pi(dx), \rho(x)\}$ be an ensemble, $\mu(dy)$ a $\sigma-$finite measure and $M = \{M(dy)\}$ an observable having operator density $m(y) = M(dy)/\mu(dy)$ with values in the algebra of bounded operators in $\mathcal{H}$. The dual pair ensemble-observable $\{\mathcal{E}', M'\}$ is defined by the relations

$$\mathcal{E}': \quad \pi'(dy) = \operatorname{Tr}\bar{\rho}_{\mathcal{E}}\, M(dy), \quad \rho'(y) = \frac{\bar{\rho}_{\mathcal{E}}^{1/2} m(y) \bar{\rho}_{\mathcal{E}}^{1/2}}{\operatorname{Tr}\bar{\rho}_{\mathcal{E}}\, m(y)}; \tag{34}$$

$$M': \quad M'(dx) = \bar{\rho}_{\mathcal{E}}^{-1/2} \rho(x) \bar{\rho}_{\mathcal{E}}^{-1/2} \pi(dx). \tag{35}$$

Then, the average states of both ensembles coincide

$$\bar{\rho}_{\mathcal{E}} = \bar{\rho}_{\mathcal{E}'} \tag{36}$$

and the joint distribution of x, y is the same for both pairs $(\mathcal{E}, M)$ and $(\mathcal{E}', M')$ so that

$$I(\mathcal{E}, M) = I(\mathcal{E}', M'). \tag{37}$$

Moreover,

$$\sup_{M} I(\mathcal{E}, M) = \sup_{\mathcal{E}': \bar{\rho}_{\mathcal{E}'} = \bar{\rho}_{\mathcal{E}}} I(\mathcal{E}', M'), \tag{38}$$

where the supremum in the right-hand side is taken over all ensembles $\mathcal{E}'$ satisfying the condition $\rho_{\mathcal{E}'} = \rho_{\mathcal{E}}$. It can be shown (Reference [6], Proposition 4), that the supremum in the lefthand side remains the same if it is taken over *all* observables M (not only of the special kind with the density we started with), and then it is called the *accessible information* $A(\mathcal{E})$ of the ensemble $\mathcal{E}$. Thus,

$$A(\mathcal{E}) = \sup_{\mathcal{E}': \bar{\rho}_{\mathcal{E}'} = \bar{\rho}_{\mathcal{E}}} I(\mathcal{E}', M').$$

Since the application of the duality to the pair $\{\mathcal{E}', M'\}$ results in the initial pair $\{\mathcal{E}, M\}$, we also have

$$A(\mathcal{E}') = \sup_{M'} I(\mathcal{E}', M') = \sup_{\mathcal{E}:\bar{\rho}_{\mathcal{E}}=\rho_{\mathcal{E}'}} I(\mathcal{E}, M).$$

Coming to the case of bosonic mode, we fix the Gaussian state ρ_α and restrict to ensembles $\mathcal{E}$ with $\bar{\rho}_{\mathcal{E}} = \rho_\alpha$. Let M be the measurement channel corresponding to POVM (21). Then, according to formulas (34), the dual ensemble $\mathcal{E}' = \{p'(x,y),\ \rho'(x,y)\}$, where $p'(x,y)$ is the Gaussian probability density (25) and

$$\rho'(x,y) = \left[p'(x,y)\right]^{-1} \sqrt{\rho_\alpha} D(x,y) \rho_\beta D(x,y)^* \sqrt{\rho_\alpha}.$$

By using the formula for $\sqrt{\rho_1}\rho_2\sqrt{\rho_1}$, where ρ_1, ρ_2 are Gaussian operators (see Reference [24] and also Corollary in the Appendix of Reference [25]), we obtain

$$\rho'(x,y) = D(x',y')\rho_{\alpha'}D(x',y')^* = \rho_{\alpha'}(x',y'),$$

where

$$\alpha' = \alpha - \gamma', \quad \gamma' = \kappa(\alpha+\beta)^{-1}\kappa, \quad \begin{bmatrix} x' \\ y' \end{bmatrix} = \kappa(\alpha+\beta)^{-1}\begin{bmatrix} x \\ y \end{bmatrix}, \tag{39}$$

and

$$\kappa = \sqrt{I + (2\alpha\Delta^{-1})^{-2}}\,\alpha = \alpha\sqrt{I + (2\Delta^{-1}\alpha)^{-2}}. \tag{40}$$

Since $\begin{bmatrix} x & y \end{bmatrix}^t \sim \mathcal{N}(0, \alpha+\beta)$, then, from second and third equations in (39), we obtain $\begin{bmatrix} x' & y' \end{bmatrix}^t \sim \mathcal{N}(0, \kappa(\alpha+\beta)^{-1}\kappa) = \mathcal{N}(0,\gamma')$. By denoting $p_{\gamma'}(x',y')$, the density of this normal distribution, we can equivalently rewrite the ensemble $\mathcal{E}'$ as $\mathcal{E}' = \{p_{\gamma'}(x',y'),\ \rho_{\alpha'}(x',y')\}$ with the average state ρ_α, $\alpha = \alpha' + \gamma'$. Then, HGM is equivalent to the statement

$$A(\mathcal{E}') = C(M;\alpha),$$

where the values of $C(M;\alpha)$ are given in Table 1; however, they should be reexpressed in terms of the ensemble parameters γ', α'. In Reference [25], we treated the case C in multimode situation, establishing that the optimal measurement is Gaussian, and described it. Here, we will discuss the case L (R is similar) and show that, for large β_p (including $\beta_p = +\infty$), the HGM is equivalent to the following: the value of the accessible information

$$A(\mathcal{E}') = C(M;\alpha) = \frac{1}{2}\log\frac{\alpha_q+\beta_q}{\frac{1}{4\alpha_p}+\beta_q} \tag{41}$$

is attained on the sharp position measurement $M'_0(d\xi) = |\xi\rangle\langle\xi|d\xi$ (in fact, this refers to the whole domain L: $\frac{1}{2}\sqrt{\frac{\beta_q}{\beta_p}} < \frac{1}{4\alpha_p}$, which, however, has rather cumbersome description in the new variables γ', α', cf. Reference [25]).

In the one mode case we are considering, the matrix α is given by (23), β – by (22), and $\Delta = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, so that $\left(2\Delta^{-1}\alpha\right)^2 = -\left(4\alpha_q\alpha_p\right)I$. Computations according to (39) and (40) give

$$\alpha' = \begin{bmatrix} \alpha'_q & 0 \\ 0 & \alpha'_p \end{bmatrix} = \begin{bmatrix} \frac{\alpha_q\left(\beta_q + 1/\left(4\alpha_p\right)\right)}{\alpha_q+\beta_q} & 0 \\ 0 & \frac{\alpha_p\left(\beta_p + 1/\left(4\alpha_q\right)\right)}{\alpha_p+\beta_p} \end{bmatrix}. \tag{42}$$

But under the sharp position measurement $M'_0(d\xi) = |\xi\rangle\langle\xi|d\xi$, one has (in the formulas below, $p(\xi) = \mathcal{N}(m,\alpha)$ means that $p(\xi)$ is Gaussian probability density with mean m and variance α):

$$p(\xi|x',y') = \langle\xi|\,\rho_{\alpha'}(x',y')|\xi\rangle = \mathcal{N}(x',\alpha'_q),$$

while $\langle\xi|\,\rho_\alpha|\xi\rangle = \mathcal{N}(0,\alpha_q)$ (note that $\rho_{\mathcal{E}'} = \rho_{\mathcal{E}} = \rho_\alpha$), and

$$\begin{aligned} I(\mathcal{E}', M_0') &= \frac{1}{2}\Big[\log\big(\alpha_q' + \gamma_q'\big) - \log\alpha_q'\Big] \\ &= \frac{1}{2}\left[\log\alpha_q - \log\frac{\alpha_q(\beta_q + 1/4\alpha_p)}{(\alpha_q + \beta_q)}\right] \\ &= \frac{1}{2}\log\frac{(\alpha_q + \beta_q)}{(\beta_q + 1/4\alpha_p)}, \end{aligned} \tag{43}$$

which is identical to the expression in (41).

In the case of the position measurement channel M corresponding to POVM (29) ($\beta_p = +\infty$), we have $\alpha_p' = \alpha_p$; otherwise, the argument is essentially the same. Thus, we obtain that the HGM concerning $e_M(\rho)$ in case L is equivalent to the following:

The accessible information of a Gaussian ensemble $\mathcal{E}' = \{p'(x),\ \rho'(x)\}$, *where*

$$p'(x) = \mathcal{N}(0,\gamma_q'), \quad \rho'(x) = D(x,0)\rho_{\alpha'}D(x,0)^*,$$

is given by the expression (43) and attained on the sharp position measurement $M_0'(dx) = |\xi\rangle\langle\xi|d\xi$.

6. Discussion

In this paper, we investigated the classical capacity problem for Gaussian measurement channels. We established Gaussianity of the average state of the optimal ensemble in full generality and discussed the Hypothesis of Gaussian Maximizers concerning the detailed structure of the ensemble. Gaussian systems form the backbone of information theory with continuous variables, both in the classical and in the quantum case. Starting from them, other, non-linear models can be constructed and investigated. Therefore, the quantum Gaussian models must be studied exhaustively. Despite the progress made, there are still intriguing gaps along this way. A major problem remains the proof (or refutation) of the hypothesis of Gaussian optimizers for various entropy characteristics of quantum Gaussian systems and channels. So far, the proof of this hypothesis in special cases required tricky and special constructions, such as in the path-breaking paper [7] concerning gauge-covariant channels, or in Section 3 of the present work concerning general Gaussian measurement channels. It seems plausible that quantum Gaussian systems may have some as yet undiscovered structural property, from which a proof of this hypothesis in its maximum generality would follow in a natural way.

Funding: This work was performed at the Steklov International Mathematical Center and supported by the Ministry of Science and Higher Education of the Russian Federation (agreement no. 075-15-2019-1614).

Acknowledgments: The author is grateful to M. J. W. Hall for sending a copy of his paper [13], and to M. E. Shirokov for the comments improving the presentation.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A. Case L in Tables 1 and 2

By taking the Gaussian ensemble parameters in (28) as

$$\delta = 1/(4\alpha_p), \quad \gamma_p = 0, \quad \gamma_q = \alpha_q - 1/(4\alpha_p), \tag{A1}$$

we get the hypothetic value

$$e_M(\rho_\alpha) = \frac{1}{2}\log\left(\frac{1}{4\alpha_p} + \beta_q\right)(\alpha_p + \beta_p) + c, \tag{A2}$$

hence taking into account (26),

$$C_{Gauss}(M;\alpha) = h_M(\rho_\alpha) - e_M(\rho_\alpha) = \frac{1}{2}\log\frac{\alpha_q+\beta_q}{\frac{1}{4\alpha_p}+\beta_q}. \tag{A3}$$

The Gaussian constrained capacity is

$$\begin{aligned} C_{Gauss}(M,H,E) &= \max_{\alpha_q+\alpha_q\leq 2E}\frac{1}{2}\left[\log(\alpha_q+\beta_q) - \log(1/(4\alpha_p)+\beta_q)\right] \\ &= \max_{\alpha_p}\frac{1}{2}\left[\log(2E-\alpha_p+\beta_q) - \log(1/(4\alpha_p)+\beta_q)\right], \end{aligned} \tag{A4}$$

where, in the second line, we took the maximal value $\alpha_q = 2E - \alpha_p$. Differentiating, we obtain the equation for the optimal value α_p:

$$4\beta_q\alpha_p^2 + 2\alpha_p - (2E+\beta_q) = 0,$$

the positive solution of which is

$$\alpha_p = \frac{1}{4\beta_q}\left(\sqrt{1+8E\beta_q+4\beta_q^2}-1\right), \tag{A5}$$

whence

$$C_{Gauss}(M,H,E) = \log\left(\frac{\sqrt{1+8E\beta_q+4\beta_q^2}-1}{2\beta_q}\right). \tag{A6}$$

The parameters of the optimal Gaussian ensemble are obtained by substituting the value (A5) into (A1) with $\alpha_q = 2E - \alpha_p$.

The above derivation concerns the measurement (21) ($\beta_p < \infty$). The case of the measurement (29) ($\beta_p = +\infty$) is treated similarly, with (A2), (26) replaced by (32), (31). Notably, in this case, the expression (A6) coincides with the one obtained in Reference [13] by optimizing the information from applying sharp position measurement to noisy optimally squeezed states (the author is indebted to M. J. W. Hall for this observation).

References

1. Hall, M.J.W. Quantum information and correlation bounds. *Phys. Rev. A* **1997**, *55*, 1050–2947. [CrossRef]
2. Dall'Arno, M.; D'Ariano, G.M.; Sacchi, M.F. Informational power of quantum measurements. *Phys. Rev. A* **2011**, *83*, 062304. [CrossRef]
3. Oreshkov, O.; Calsamiglia, J.; Munoz-Tapia, R.; Bagan, E. Optimal signal states for quantum detectors. *New J. Phys.* **2011**, *13*, 073032. [CrossRef]
4. Holevo, A.S. Information capacity of quantum observable. *Probl. Inform. Transm.* **2012**, *48*, 1–10. [CrossRef]
5. Holevo, A.S.; Kuznetsova, A.A. Information capacity of continuous variable measurement channel. *J. Phys. A Math. Theor.* **2020**, *53*, 175304. [CrossRef]
6. Holevo, A.S. Gaussian maximizers for quantum Gaussian observables and ensembles. *IEEE Trans. Inform. Theory* **2020**, *66*, 5634–5641. [CrossRef]
7. Giovannetti, V.; Holevo, A.S.; Mari, A. Majorization and additivity for multimode bosonic Gaussian channels. *Theor. Math. Phys.* **2015**, *182*, 284–293. [CrossRef]
8. Schäfer, J.; Karpov, E.; Garćia-Patrón, R.; Pilyavets, O.V.; Cerf, N.J. Equivalence Relations for the Classical Capacity of Single-Mode Gaussian Quantum Channels. *Phys. Rev. Lett.* **2013**, *111*, 030503. [CrossRef]
9. Holevo, A.S. On the constrained classical capacity of infinite-dimensional covariant channels. *J. Math. Phys.* **2016**, *57*, 15203. [CrossRef]
10. Caves, C.M.; Drummond, P.D. Quantum limits on bosonic communication rates. *Rev. Mod. Phys.* **1994**, *68*, 481–537. [CrossRef]
11. Serafini, A. *Quantum Continuous Variables: A Primer of Theoretical Methods*; CRC Press: Boca Raton, FL, USA, 2017.
12. Wolf, M.M.; Giedke, G.; Cirac, J.I. Extremality of Gaussian quantum states. *Phys. Rev. Lett.* **2006**, *96*, 080502. [CrossRef] [PubMed]
13. Hall, M.J.W. Gaussian noise and quantum optical communication. *Phys. Rev. A* **1994**, *50*, 3295–3303. [CrossRef] [PubMed]
14. Takeoka, M.; Guha, S. Capacity of optical communication in loss and noise with general Gaussian receivers. *Phys. Rev. A* **2014**, *89*, 042309. [CrossRef]

15. Lee, J.; Ji, S.W.; Park, J.; Nha, H. Gaussian benchmark for optical communication aiming towards ultimate capacity. *Phys. Rev. A* **2016**, *93*, 050302. [CrossRef]
16. Holevo, A.S. *Quantum Systems, Channels, Information: A Mathematical Introduction*, 2nd ed.; De Gruyter: Berlin, Germany; Boston, MA, USA, 2019.
17. Shirokov, M.E. On entropic quantities related to the classical capacity of infinite dimensional quantum channels. *Theor. Probab. Appl.* **2007**, *52*, 250–276. [CrossRef]
18. Shirokov, M.E. On properties of the space of quantum states and their application to the construction of entanglement monotones. *Izv. Math.* **2010**, *74*, 849–882. [CrossRef]
19. Wiseman, H.M.; Milburn, G.J. *Quantum Measurement and Control*; Cambridge University Press: New York, NY, USA, 2010.
20. Cushen, C.D.; Hudson, R.L. A quantum mechanical central limit theorem. *J. Appl. Prob.* **1971**, *8*, 454–469. [CrossRef]
21. Holevo, A.S. The structure of general quantum Gaussian observable. *arXiv* **2020**, arXiv:2007.02340.
22. Holevo, A.S.; Yashin, V.I. Maximum information gain of approximate quantum position measurement. *Quantum Inf. Process.* **2021**, *20*, 97. [CrossRef]
23. Hall, M.J.W. Information exclusion principle for complementary observables. *Phys. Rev. Lett.* **1995**, *74*, 3307. [CrossRef] [PubMed]
24. Lami, L.; Das, S.; Wilde, M.M. Approximate reversal of quantum Gaussian dynamics. *J. Phys. A* **2018** *51*, 125301. [CrossRef]
25. Holevo, A.S. Accessible information of a general quantum Gaussian ensemble. *arXiv* **2021**, arXiv:2102.01981.

entropy

MDPI

Article

Simplification of the Gram Matrix Eigenvalue Problem for Quadrature Amplitude Modulation Signals

Ryusuke Miyazaki [1], Tiancheng Wang [1,2,*] and Tsuyoshi Sasaki Usuda [1,*]

[1] Graduate School of Information Science and Technology, Aichi Prefectural University, Nagakute 480-1198, Aichi, Japan; im201011@cis.aichi-pu.ac.jp
[2] Faculty of Engineering, Kanagawa University, Yokohama 221-8686, Kanagawa, Japan
* Correspondence: wang@kanagawa-u.ac.jp (T.W.); usuda@ist.aichi-pu.ac.jp (T.S.U.)

Abstract: In quantum information science, it is very important to solve the eigenvalue problem of the Gram matrix for quantum signals. This allows various quantities to be calculated, such as the error probability, mutual information, channel capacity, and the upper and lower bounds of the reliability function. Solving the eigenvalue problem also provides a matrix representation of quantum signals, which is useful for simulating quantum systems. In the case of symmetric signals, analytic solutions to the eigenvalue problem of the Gram matrix have been obtained, and efficient computations are possible. However, for asymmetric signals, there is no analytic solution and universal numerical algorithms that must be used, rendering the computations inefficient. Recently, we have shown that, for asymmetric signals such as amplitude-shift keying coherent-state signals, the Gram matrix eigenvalue problem can be simplified by exploiting its partial symmetry. In this paper, we clarify a method for simplifying the eigenvalue problem of the Gram matrix for quadrature amplitude modulation (QAM) signals, which are extremely important for applications in quantum communication and quantum ciphers. The results presented in this paper are applicable to ordinary QAM signals as well as modified QAM signals, which enhance the security of quantum cryptography.

Keywords: quantum communication; quantum cipher; quadrature amplitude modulation (QAM); coherent state; Gram matrix; square-root measurement (SRM)

Citation: Miyazaki, R.; Wang, T.; Usuda, T.S. Simplification of Gram Matrix Eigenvalue Problem for Quadrature Amplitude Modulation Signals. *Entropy* **2022**, *24*, 544. https://doi.org/10.3390/e24040544

Academic Editor: Osamu Hirota

Received: 21 March 2022
Accepted: 11 April 2022
Published: 13 April 2022

1. Introduction

The efficient computations and evaluations of quantities such as the error probability, mutual information, channel capacity, and reliability function are extremely important in quantum communication, quantum radar, and quantum cipher systems [1–5]. The computation of these quantities is essential not only for evaluating the reliability of quantum communication and the sensitivity of quantum radar but also for guaranteeing the security of quantum cryptography. In particular, because the security of a quantum stream cipher relies on the difference between the quantum optimum receiving capabilities of the legitimate receiver and the eavesdropper, it is essential to evaluate the optimum quantum receiver performance of the eavesdropper to guarantee security [6,7]. In quantum stream ciphers, the number of signals usually runs to several hundreds or thousands [8,9]. However, recent experiments have shown that some cases may contain millions or even billions of signals [10,11].

The eigenvalues and eigenvectors of the Gram matrix are very useful for computing various quantities that evaluate system performance. By solving the eigenvalue problem of the Gram matrix and finding its square root, the channel matrix given by the so-called square-root measurement (SRM) [12–16] can be computed. This implies that the error probability and mutual information using SRM can be directly calculated. SRM is asymptotically optimal for any quantum state signals with respect to minimizing the error probability, and

it is used in the proof of the quantum channel coding theorem [14]. Moreover, SRM is strictly optimal for symmetric pure-state signals with uniform *a priori* probabilities [12–15,17–19]. Actually, SRM is also strictly optimal for some asymmetric pure-state signals with not necessarily uniform *a priori* probabilities [20]. As each component of the square root of the Gram matrix corresponds to the inner product of a signal quantum state and a measurement state of the SRM, a matrix representation of the signal quantum state can be obtained when the signal quantum states are linearly independent [21]. This representation is known to be useful for analyzing quantum systems (e.g., [21]). Furthermore, even if the quantum state is a vector in an infinite-dimensional Hilbert space, such as a coherent state or squeezed state, the matrix form allows numerical calculations to be performed because it provides a representation in a finite-dimensional subspace (e.g., [22]). Because the Gram matrix is a matrix representation of the density operator of the quantum information source, the Holevo capacity [14] and the upper and lower bounds of the reliability function [23,24] can be directly calculated by using its eigenvalues.

In general, the Gram matrix is $M \times M$ for M-ary pure-state signals. Therefore, if we use a universal numerical algorithm to compute the eigenvalues and eigenvectors of the Gram matrix, the computation is hard when M is large. However, if the signals are symmetric, the analytic solutions of the Gram matrix eigenvalues and eigenvectors can be obtained by using well-known operations in linear algebra. In addition, by using the character [25] of a group, analytic solutions [26] can be obtained for narrow-sense group covariant signals [27], which are a generalization of symmetric signals. Narrow-sense group covariant signals are important in applications such as phase-shift keying (PSK) coherent-state signals and coded symmetric signals. Unfortunately, however, several important asymmetric signals are not narrow-sense group covariant, such as amplitude-shift keying (ASK) coherent-state signals and quadrature amplitude modulation (QAM) coherent-state signals [27]. QAM coherent-state signals are extremely important for quantum communication [28] and quantum ciphers [29]; moreover, QAM signals almost achieve the quantum channel capacity under energy constraints [30].

Recently, we showed that the eigenvalue problem of the Gram matrix can be simplified by using its partial symmetry for ASK coherent-state signals and amplitude-modulated phase-modulated (AMPM) signals, which belong to a class of asymmetric signals [31–33]. In this paper, we show that the eigenvalue problem of the Gram matrix can also be simplified by using its partial symmetry for QAM signals, which are more important for applications than ASK and AMPM signals. The method in this paper is applicable to ordinary QAM signals as well as modified QAM signals, which enhance the security of quantum stream ciphers [29]. Note that the signals considered in this paper belong to a class of asymmetric signals defined in Ref. [20], where the class is referred to as "the multiple constellations of geometrical uniform symmetry (GUS) state". The results of this paper are closely related to Ref. [20].

The remainder of this paper is organized as follows. In Section 2, we introduce some preliminaries and basic theory. First, we define quantum signals and measurements, and then we explain various quantities such as the error probability, mutual information, and Holevo capacity. Next, we introduce the Gram matrix, SRM, and symmetric signals, which are the subject of this paper. In Section 3, we present the main results. For the eigenvalue problem of the Gram matrix of $M = 4m$ QAM signals, we show that the size of the problem can be reduced by using the partial symmetry of the signals. In Section 4, we show examples for the simplest case of $m = 2$ and provide specific forms of eigenvalues and eigenvectors for the smaller matrices than the Gram matrix. In Section 5, we provide numerical experiments as examples of applications for the main result. Finally, in Section 6, we summarize the conclusions to this study.

2. Basic Theory

2.1. Quantum Signals and Measurements

Let $\mathcal{H}$ be the Hilbert space of a quantum system. The set of M-ary pure-state signals is represented by the following:

$$\mathcal{S} = \{|\psi_i\rangle \in \mathcal{H} \mid i = 1, 2, \ldots, M\}, \tag{1}$$

where $\langle\psi_i|\psi_i\rangle = 1$. Let ξ_i be the *a priori* probability of state $|\psi_i\rangle$. Then, the pair $(\mathcal{S}, \xi)$ is referred to as a quantum information source or a quantum ensemble.

In general, a quantum measurement is mathematically described by a positive operator-valued measure (POVM). The POVM is described as follows:

$$\Pi = \{\hat{\Pi}_j \mid j = 1, 2, \ldots, M\}, \tag{2}$$

where $\hat{\Pi}$ is a Hermitian operator on $\mathcal{H}$ satisfying the following.

$$\hat{\Pi} \geq 0, \quad \sum_{j=1}^{M} \hat{\Pi} = \hat{I}.$$

Here, $\hat{I}$ is the identity operator on $\mathcal{H}$. Although POVM is a mathematical representation of a quantum measurement, it may be called a quantum measurement. The conditional probability that the result j is obtained when performing the measurement Π on quantum state $|\psi_i\rangle$ is as follows.

$$P(j|i) = \mathrm{Tr}\left(|\psi_i\rangle\langle\psi_i|\hat{\Pi}_j\right). \tag{3}$$

2.2. Error Probability, Mutual Information, and Holevo Capacity

Suppose we measure the quantum information source $(\mathcal{S}, \xi)$ by a POVM Π. Using Equation (3), the average error probability is defined as follows:

$$P_{\mathrm{e}} = \sum_{i=1}^{M} \xi_i \sum_{j \neq i} P(j|i) = 1 - \sum_{i=1}^{M} \xi_i P(i|i), \tag{4}$$

which is also simply called the error probability. Then, the following is the case:

$$P_{\mathrm{e}}^{(\mathrm{opt})} = \min_{\Pi} P_{\mathrm{e}} \tag{5}$$

and it is referred to as the minimum error probability and the set Π that attains $P_{\mathrm{e}}^{(\mathrm{opt})}$ is called the optimum POVM. The mutual information is defined as follows:

$$I(\mathcal{S}, \xi) = \sum_{i=1}^{M} \xi_i \sum_{j=1}^{M} P(j|i) \log_2 \left[\frac{P(j|i)}{\sum_{k=1}^{M} \xi_k P(j|k)} \right], \tag{6}$$

and its maximization with respect to quantum measurements is the following:

$$I_{\mathrm{acc}} = \max_{\Pi} I(\mathcal{S}, \xi), \tag{7}$$

which is called accessible information. For $(\mathcal{S}, \xi)$, the following is the case:

$$\hat{\rho} = \sum_{i=1}^{M} \xi_i |\psi_i\rangle\langle\psi_i| \tag{8}$$

and it is called the density operator of the quantum information source. Using the density operator, we define von Neumann entropy as follows.

$$\chi(\xi) = -\mathrm{Tr}(\hat{\rho}\log_2\hat{\rho}). \tag{9}$$

When the signals are pure states, the maximization of $\chi(\xi)$ with respect to ξ is the so-called Holevo capacity.

$$C = \max_{\xi} \chi(\xi). \tag{10}$$

Let λ_j be the eigenvalues of $\hat{\rho}$ corresponding to the ξ that attains C. Then, the Holevo capacity can be calculated as follows.

$$C = -\sum_j \lambda_j \log_2 \lambda_j. \tag{11}$$

The error probability and mutual information and their optimal values are calculated using the conditional probability (3), while the Holevo capacity uses the density operator (8) of the quantum information source.

2.3. Gram Matrix

For an M-ary pure-state signal set $S = \{|\psi_i\rangle \mid i = 1, 2, \ldots, M\}$, the Gram matrix Γ is defined as follows.

$$\Gamma = \begin{bmatrix} \langle\psi_1|\psi_1\rangle & \langle\psi_1|\psi_2\rangle & \cdots & \langle\psi_1|\psi_M\rangle \\ \langle\psi_2|\psi_1\rangle & \langle\psi_2|\psi_2\rangle & \cdots & \langle\psi_2|\psi_M\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle\psi_M|\psi_1\rangle & \langle\psi_M|\psi_2\rangle & \cdots & \langle\psi_M|\psi_M\rangle \end{bmatrix}. \tag{12}$$

The Gram matrix is an $M \times M$ matrix in which the (i, j)-th element is the inner product $\langle\psi_i|\psi_j\rangle$ between quantum state signals (Note that the Gram matrix is sometimes defined by using the inner products between weighted quantum state signals [20,34]). By definition, the Gram matrix is Hermitian; moreover, it is non-negative [35]. Because the norm of the quantum state vector is unity, so are all diagonal components of the Gram matrix, and the sum of the diagonal components is M. The Gram matrix is very useful in the theoretical treatment of M-ary pure-state signal systems. First, for a quantum information source $(S, \{\frac{1}{M}\})$ for which its *a priori* probabilities are uniform, $\frac{1}{M}\Gamma$ is a matrix representation of its density operator. That is, $\hat{\rho}$ and $\frac{1}{M}\Gamma$ are isomorphic.

$$\hat{\rho} \cong \frac{1}{M}\Gamma. \tag{13}$$

In this case, the eigenvalues of the Gram matrix and those of the density operator are identical, and the von Neumann entropy can be calculated using the eigenvalues of the Gram matrix. For symmetric signals, the Holevo capacity can be calculated directly from the eigenvalues of the Gram matrix, because the Holevo capacity is attained with uniform *a priori* probabilities [36]. A similar statement can be made for the upper and lower bounds of the quantum reliability function [37,38]. Furthermore, the Gram matrix is closely related to the theory of SRM, as described below.

2.4. Square-Root Measurement

The SRM is a quantum measurement defined using the quantum states that are being transmitted. For a set of M-ary pure-state signals $S = \{|\psi_i\rangle \mid i = 1, 2, \ldots, M\}$, the POVM of the SRM $\{\hat{\Pi}_j^{(\mathrm{SRM})} \mid j = 1, 2, \ldots, M\}$ is defined as follows:

$$\hat{\Pi}_j^{(\mathrm{SRM})} = |\mu_j\rangle\langle\mu_j|, \tag{14}$$

$$|\mu_j\rangle = \hat{\Psi}^{-\frac{1}{2}}|\psi_j\rangle, \tag{15}$$

$$\hat{\Psi} = \sum_{i=1}^{M} |\psi_i\rangle\langle\psi_i|, \tag{16}$$

where vector $|\mu_j\rangle$ is the measurement state or measurement quantum state (e.g., [4]). For linearly independent signal systems, the set of measurement quantum states $\{|\mu_j\rangle\}$ is an orthonormal system and is an orthonormal basis of the space spanned by signal quantum states [34]. Although SRM appeared in papers in the 1970s (e.g., Belavkin [12] and earlier papers by Holevo), the name SRM has only been used since 1996, when Hausladen et al. presented the quantum channel coding theorem [14]. They proved that the inner product between quantum states $|\psi_i\rangle$ and $|\mu_j\rangle$ in Equation (15) is equal to the (i, j)-th element of the square root of the Gram matrix, Γ, and called this the "square-root" measurement. Specifically, they showed the following.

$$\langle\psi_i|\mu_j\rangle = \left(\Gamma^{\frac{1}{2}}\right)_{i,j}. \tag{17}$$

The existence of $\Gamma^{\frac{1}{2}}$ is always guaranteed because the Gram matrix is non-negative and Hermitian, as mentioned above. Therefore, Equation (17) denotes a component of the matrix representation of the signal quantum state $|\psi_i\rangle$ using the orthonormal basis $\{|\mu_j\rangle\}$. Thus, as the signal quantum state can be represented in matrix form based on the square-root of the Gram matrix, computing $\Gamma^{\frac{1}{2}}$ is very useful for simulating systems such as quantum communication, quantum radar, and quantum ciphers. From Equation (3), we have the following.

$$\begin{aligned} P(j|i) &= \mathrm{Tr}\left(|\psi_i\rangle\langle\psi_i|\hat{\Pi}_j^{(\mathrm{SRM})}\right) = \mathrm{Tr}\left(|\psi_i\rangle\langle\psi_i|\mu_j\rangle\langle\mu_j|\right) \\ &= |\langle\psi_i|\mu_j\rangle|^2 = \left|\left(\Gamma^{\frac{1}{2}}\right)_{i,j}\right|^2. \end{aligned} \tag{18}$$

Because the matrix in which the (i, j)-th elements are equal to $P(j|i)$ is the channel matrix and obtaining $P(j|i)$ allows the error probability and mutual information to be calculated using Equations (4) and (6). Therefore, if the square root of the Gram matrix can be computed efficiently, it is easy to compute the error probability and mutual information when SRM is applied. In general, the square root of a matrix can be computed using its eigenvalues and eigenvectors. Thus, being able to efficiently compute the eigenvalues and eigenvectors of a Gram matrix is extremely important.

2.5. Coherent-State Signals

Coherent states are the most fundamental optical quantum states used in macroscopic quantum communication or quantum ciphers. They are the stable states of light that can be realized by an ideal laser. The coherent state $|\alpha\rangle$ with the complex amplitude α is given by the following:

$$|\alpha\rangle = \exp\left(-\frac{|\alpha|^2}{2}\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{19}$$

where $|n\rangle$ is the photon number state, and n is the number of photons. The inner product between two coherent states $|\alpha\rangle$ and $|\beta\rangle$ is as follows:

$$\langle\alpha|\beta\rangle = \exp\left(\alpha^*\beta - \frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}\right), \tag{20}$$

where * denotes complex conjugation. If α and β are both real numbers, the value of $\langle\alpha|\beta\rangle$ is real. In this paper, we assume that the signal quantum state is a coherent state.

Note that the coherent state is completely characterized by its complex amplitude α, as shown in Equation (19). A complex number α is graphically described by a point on the complex plane, and so a coherent state signal is also described by a point on the complex plane. In this case, the complex plane is often called the phase plane.

2.6. Symmetric Signals

In the field of quantum information science, Davies defined a group covariant signal [39] with symmetry corresponding to the symmetry of the group, which is sometimes simply called a symmetric signal. Although Davies' definition of group covariant signals applies to a broader class of signals than the pure-state signals treated in this paper, we adopt the following narrow definition of group covariant signals [27], which is applicable only to simpler pure-state signals.

Definition 1 (Narrow-sense group covariant signals [27]). *Let $(G;\circ)$ be a finite group with the operation $\circ$. A set $\{|\psi_i\rangle|i \in G\}$ of quantum state signals is called (narrow-sense) group covariant with respect to the group $(G;\circ)$ if the following is the case:*

$$\forall i,k \in G,\ \exists\hat{U}_k,\ \hat{U}_k|\psi_i\rangle = |\psi_{k\circ i}\rangle, \tag{21}$$

where $\hat{U}_k$ is a unitary operator.

Narrow-sense group covariant signals have the following necessary and sufficient conditions.

Proposition 1 (Necessary and sufficient conditions for narrow-sense group covariant signals [27]). *A set of quantum state signals $\{|\psi_i\rangle|i \in G\}$ is narrow-sense group covariant with respect to $(G;\circ)$ if and only if the following is the case.*

$$\forall i,j,k \in G,\ \langle\psi_{k\circ i}|\psi_{k\circ j}\rangle = \langle\psi_i|\psi_j\rangle. \tag{22}$$

From this proposition, we can easily show that signals such as arbitrary binary pure-state signals and arbitrary M-ary PSK coherent-state signals are narrow-sense group covariant. In addition, for narrow-sense group covariant signals, analytic solutions for the eigenvalues and eigenvectors of the Gram matrix have been presented, indicating that narrow-sense group covariant signals are very useful for communication and cipher systems. In this study, we apply this knowledge to QAM signals that are not group-covariant.

3. Eigenvalues and Eigenvectors of $M = 4m$-ary QAM Signals and Their Gram Matrix

In this section, we consider the eigenvalues and eigenvectors of the Gram matrix corresponding to $M = 4m$-ary QAM signals. First, $M = 4m$-ary QAM signals are defined and the corresponding Gram matrix is explained. Next, we state that the Gram matrix can be block-partitioned and clarify that it has the structure of the sum of tensor products. Finally, we show that the scale of the computation can be reduced.

3.1. 4m-ary QAM Signals

This subsection describes the $4m$-ary QAM signals treated in this paper. QAM is a major modulation scheme used in digital communication, such as for coherent optical

communication [40], and QAM signals are important for applications in quantum technologies such as quantum communication and quantum ciphers. Ordinary QAM signals are placed in a square lattice on the phase plane. As an example, Figure 1a shows the signal constellation of 256QAM on the phase plane. In quantum ciphers, modified QAM signals in which signals near the origin are removed have been proposed for higher security [29]. As an example, Figure 1b shows the signal constellation of the modified 156QAM on the phase plane. For 256QAM signals, the number of signals is $M = 4m = 256$ and $m = 64 = 8^2$, while for modified 156QAM signals, it is $M = 4m = 156$ and $m = 39$.

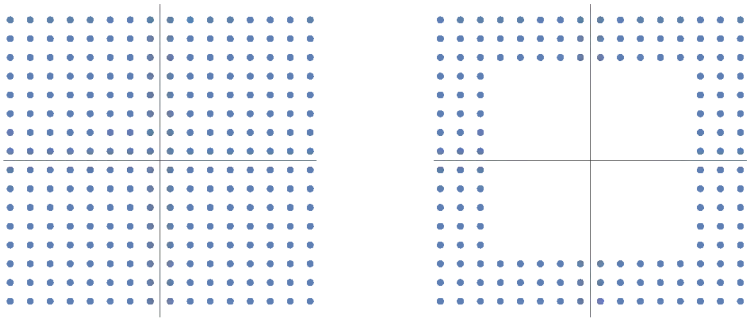


Figure 1. Examples of QAM signals presented in [29]. (**a**) 256QAM. (**b**) Modified 156QAM.

In this paper, we consider the signals defined below, which include both the ordinary QAM of Figure 1a and the modified QAM of Figure 1b, and we call them QAM signals.

Definition 2 (4m-ary QAM Signals). *Let $\{\beta_1, \beta_2, \ldots, \beta_m\}$ be any m-ary set of complex amplitudes for which its arguments lie in the range $0 < \varphi < \frac{\pi}{2}$. That is, the complex amplitudes correspond to points in the first quadrant. Here, $\beta_k \neq 0$ $(k = 1, 2, \ldots, m)$ and $\beta_k \neq \beta_{k'}$ $(k \neq k')$ are assumed. For each β_k, let $\alpha_k^{(1)} = \beta_k$, $\alpha_k^{(2)} = \mathbf{i}\beta_k$, $\alpha_k^{(3)} = -\beta_k$, and $\alpha_k^{(4)} = -\mathbf{i}\beta_k$, where $\mathbf{i} = \sqrt{-1}$. Then, we call the following set of coherent states "4m-ary QAM coherent-state signals" (4m-ary QAM signals for short):*

$$\mathcal{S} = \bigcup_{k=1}^{m} \mathcal{S}_k, \tag{23}$$

where $\mathcal{S}_k$ are sets of coherent states defined as follows.

$$\mathcal{S}_k = \{|\alpha_k^{(i)}\rangle \mid i = 1, 2, 3, 4\}. \tag{24}$$

The rotation operator [4] that rotates the phase by an angle θ in the phase plane is represented as follows:

$$\hat{U}(\theta) = \exp\left[\mathbf{i}\theta \hat{a}^\dagger \hat{a}\right], \tag{25}$$

where $\hat{a}$ and $\hat{a}^\dagger$ are photon annihilation and creation operators, respectively. Rewriting $\hat{U}(\theta = \frac{\pi}{2})$ as simply $\hat{U}$, $\mathcal{S}_k$ becomes the following.

$$\mathcal{S}_k = \left\{|\alpha_k^{(i)}\rangle, \hat{U}|\alpha_k^{(1)}\rangle, \hat{U}^2|\alpha_k^{(i)}\rangle, \hat{U}^3|\alpha_k^{(i)}\rangle\right\} = \left\{|\beta_k\rangle, \hat{U}|\beta_k\rangle, \hat{U}^2|\beta_k\rangle, \hat{U}^3|\beta_k\rangle\right\}. \tag{26}$$

Here, we have the following.

$$\hat{U}^4 = \hat{U}^0 = \hat{I}. \tag{27}$$

The $4m$-ary QAM signals defined above obviously include both ordinary QAM signals (e.g., Figure 1a) and modified QAM signals (e.g., Figure 1b). Although $4m$-ary QAM signals are not symmetric signals, each subset $\mathcal{S}_k$ is symmetric, group covariant, and geometrical uniform symmetric (GUS). Moreover, we should mention that $4m$-ary QAM signals in Definition 2 satisfy the definition of the multiple constellations of GUS state [20], which is a particularization of the concept of compound geometrical uniform (CGU) states [41]. Hence, $4m$-ary QAM signals are practical examples of the multiple constellations of GUS state and CGU states. The following results are also applicable when considering non-coherent states $|\psi_k\rangle$, such as squeezed states, instead of $|\beta_k\rangle$ in Equation (26).

3.2. Gram Matrix of 4m-ary QAM Signals

As shown in Equation (23), $4m$-ary QAM signals are partitioned into m subsets $\mathcal{S}_k$ $(k = 1, 2, \ldots, m)$. Let $\Gamma_{k,l}^{(4)}$ be the 4×4 matrix for which its entries are the inner product between two signals, where one of the two signals is chosen from the subset $\mathcal{S}_k$, and the other is chosen from the subset $\mathcal{S}_l$. Then, the Gram matrix of the $4m$-ary QAM signals can be represented in block-partitioned form as follows.

$$\Gamma = \begin{bmatrix} \Gamma_{1,1}^{(4)} & \Gamma_{1,2}^{(4)} & \cdots & \Gamma_{1,m}^{(4)} \\ \Gamma_{2,1}^{(4)} & \Gamma_{2,2}^{(4)} & \cdots & \Gamma_{2,m}^{(4)} \\ \vdots & \vdots & \ddots & \vdots \\ \Gamma_{m,1}^{(4)} & \Gamma_{m,2}^{(4)} & \cdots & \Gamma_{m,m}^{(4)} \end{bmatrix}. \tag{28}$$

From Equation (26), the (i, j)-th element of $\Gamma_{k,l}^{(4)}$ is as follows.

$$\left(\Gamma_{k,l}^{(4)}\right)_{i,j} = \langle \alpha_k^{(1)} | \left(\hat{U}^{i-1}\right)^{\dagger} \hat{U}^{j-1} | \alpha_l^{(1)} \rangle = \langle \alpha_k^{(1)} | \hat{U}^{j-i} | \alpha_l^{(1)} \rangle = \langle \beta_k | \hat{U}^{j-i} | \beta_l \rangle. \tag{29}$$

This implies that $\Gamma_{k,l}^{(4)}$ is cyclic.

Denoting the components of the first row of $\Gamma_{k,l}^{(4)}$ as $a_{k,l}$, $b_{k,l}$, $c_{k,l}$ and $d_{k,l}$, the submatrix $\Gamma_{k,l}^{(4)}$ is described as follows:

$$\Gamma_{k,l}^{(4)} = \begin{bmatrix} a_{k,l} & b_{k,l} & c_{k,l} & d_{k,l} \\ d_{k,l} & a_{k,l} & b_{k,l} & c_{k,l} \\ c_{k,l} & d_{k,l} & a_{k,l} & b_{k,l} \\ b_{k,l} & c_{k,l} & d_{k,l} & a_{k,l} \end{bmatrix}, \tag{30}$$

where the following is the case.

$$\begin{aligned} a_{k,l} &= \langle \beta_k | \beta_l \rangle, \\ b_{k,l} &= \langle \beta_k | \hat{U} | \beta_l \rangle = \langle \beta_k | \mathbf{i} \beta_l \rangle, \\ c_{k,l} &= \langle \beta_k | \hat{U}^2 | \beta_l \rangle = \langle \beta_k | -\beta_l \rangle, \\ d_{k,l} &= \langle \beta_k | \hat{U}^3 | \beta_l \rangle = \langle \beta_k | -\mathbf{i} \beta_l \rangle. \end{aligned}$$

3.3. Decomposition of Submatrices

Here, we consider the common properties of each $\Gamma_{k,l}^{(4)}$ by performing a spectral decomposition of each submatrix $\Gamma_{k,l}^{(4)}$ introduced in the previous section. Because $\Gamma_{k,l}^{(4)}$

is cyclic according to Equation (30), the analytic expressions of its eigenvalues $\lambda_i^{(k,l)}$ and eigenvectors $\boldsymbol{\lambda_i}$ $(i = 1, 2, 3, 4)$ are well known. The expressions are as follows.

$$\begin{aligned}
\lambda_1^{(k,l)} &= a_{k,l} + b_{k,l} + c_{k,l} + d_{k,l}, \\
\lambda_2^{(k,l)} &= a_{k,l} - b_{k,l} + c_{k,l} - d_{k,l}, \\
\lambda_3^{(k,l)} &= a_{k,l} + \mathbf{i}b_{k,l} - c_{k,l} - \mathbf{i}d_{k,l}, \\
\lambda_4^{(k,l)} &= a_{k,l} - \mathbf{i}b_{k,l} - c_{k,l} + \mathbf{i}d_{k,l},
\end{aligned}$$

$$\boldsymbol{\lambda_1} = \frac{1}{2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}, \boldsymbol{\lambda_2} = \frac{1}{2}\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix}, \boldsymbol{\lambda_3} = \frac{1}{2}\begin{bmatrix}1\\\mathbf{i}\\-1\\-\mathbf{i}\end{bmatrix}, \boldsymbol{\lambda_4} = \frac{1}{2}\begin{bmatrix}1\\-\mathbf{i}\\-1\\\mathbf{i}\end{bmatrix}.$$

As eigenvectors $\{\boldsymbol{\lambda_1}, \boldsymbol{\lambda_2}, \boldsymbol{\lambda_3}, \boldsymbol{\lambda_4}\}$ are orthonormal, $\Gamma_{k,l}^{(4)}$ can be spectrally decomposed as follows:

$$\Gamma_{k,l}^{(4)} = \sum_{i=1}^{4} \lambda_i^{(k,l)} \boldsymbol{\lambda_i} \boldsymbol{\lambda_i}^{\mathrm{H}}, \tag{31}$$

where $\boldsymbol{\lambda_i}^{\mathrm{H}}$ denotes the conjugate transpose of $\boldsymbol{\lambda_i}$.

3.4. Decomposition of Gram Matrix

In this subsection, we decompose the Gram matrix Γ into a sum of tensor products using the spectral decomposition of submatrices $\Gamma_{k,l}^{(4)}$. All $\Gamma_{k,l}^{(4)}$ have common eigenvectors independent of k and l. Substituting Equation (31) into Equation (28), we obtain the following:

$$\begin{aligned}
\Gamma &= \begin{bmatrix}
\Gamma_{1,1}^{(4)} & \Gamma_{1,2}^{(4)} & \cdots & \Gamma_{1,m}^{(4)} \\
\Gamma_{2,1}^{(4)} & \Gamma_{2,2}^{(4)} & \cdots & \Gamma_{2,m}^{(4)} \\
\vdots & \vdots & \ddots & \vdots \\
\Gamma_{m,1}^{(4)} & \Gamma_{m,2}^{(4)} & \cdots & \Gamma_{m,m}^{(4)}
\end{bmatrix} \\
&= \sum_{i=1}^{4} \begin{bmatrix}
\lambda_i^{(1,1)} & \lambda_i^{(1,2)} & \cdots & \lambda_i^{(1,m)} \\
\lambda_i^{(2,1)} & \lambda_i^{(2,2)} & \cdots & \lambda_i^{(2,m)} \\
\vdots & \vdots & \ddots & \vdots \\
\lambda_i^{(m,1)} & \lambda_i^{(m,2)} & \cdots & \lambda_i^{(m,m)}
\end{bmatrix} \otimes \boldsymbol{\lambda_i} \boldsymbol{\lambda_i}^{\mathrm{H}} \\
&= \sum_{i=1}^{4} A_i \otimes \boldsymbol{\lambda_i} \boldsymbol{\lambda_i}^{\mathrm{H}},
\end{aligned} \tag{32}$$

where the following is the case.

$$A_i = \begin{bmatrix}
\lambda_i^{(1,1)} & \lambda_i^{(1,2)} & \cdots & \lambda_i^{(1,m)} \\
\lambda_i^{(2,1)} & \lambda_i^{(2,2)} & \cdots & \lambda_i^{(2,m)} \\
\vdots & \vdots & \ddots & \vdots \\
\lambda_i^{(m,1)} & \lambda_i^{(m,2)} & \cdots & \lambda_i^{(m,m)}
\end{bmatrix}. \tag{33}$$

In the following, we show that each matrix A_i consisting of the eigenvalues of $\Gamma^{(4)}_{k,l}$ is Hermitian. As Γ is the Gram matrix (and is therefore Hermitian), its submatrices satisfy the following.

$$\left(\Gamma^{(4)}_{k,l}\right)^{\mathrm{H}} = \Gamma^{(4)}_{l,k}. \tag{34}$$

From Equation (31), we have the following:

$$\left(\Gamma^{(4)}_{k,l}\right)^{\mathrm{H}} = \sum_{i=1}^{4} \left(\lambda_i^{(k,l)}\right)^* \boldsymbol{\lambda_i}\boldsymbol{\lambda_i}^{\mathrm{H}} \tag{35}$$

and from Equation (34), it coincides with the following.

$$\Gamma^{(4)}_{l,k} = \sum_{i=1}^{4} \lambda_i^{(l,k)} \boldsymbol{\lambda_i}\boldsymbol{\lambda_i}^{\mathrm{H}}. \tag{36}$$

Thus, we have

$$\left(\lambda_i^{(k,l)}\right)^* = \lambda_i^{(l,k)}. \tag{37}$$

Hence, all A_i of Equation (33) are Hermitian.

$$A_i{}^{\mathrm{H}} = A_i, \quad i \in \{1,2,3,4\}. \tag{38}$$

Therefore, each A_i is spectrally decomposable. Let $a_j^{(i)}$ and $\boldsymbol{a_j^{(i)}}$ be the eigenvalues and corresponding orthonormalized eigenvectors of A_i. Then, the spectral decomposition form of A_i is as follows.

$$A_i = \sum_{j=1}^{m} a_j^{(i)} \boldsymbol{a_j^{(i)}} \boldsymbol{a_j^{(i)}}^{\mathrm{H}}. \tag{39}$$

Substituting this into Equation (32), we obtain the following.

$$\Gamma = \sum_{i=1}^{4} \sum_{j=1}^{m} a_j^{(i)} \boldsymbol{a_j^{(i)}} \boldsymbol{a_j^{(i)}}^{\mathrm{H}} \otimes \boldsymbol{\lambda_i}\boldsymbol{\lambda_i}^{\mathrm{H}}. \tag{40}$$

3.5. Eigenvalues and Eigenvectors of Gram Matrix

In this subsection, we derive the eigenvalues and eigenvectors from the decomposition form (40) of the Gram matrix Γ. Because both $\left\{\boldsymbol{a_j^{(i)}}\right\}$ and $\{\boldsymbol{\lambda_i}\}$ are orthonormal, we have the following:

$$\Gamma\left(\boldsymbol{a_j^{(i)}} \otimes \boldsymbol{\lambda_i}\right) = a_j^{(i)}\left(\boldsymbol{a_j^{(i)}} \otimes \boldsymbol{\lambda_i}\right) \qquad (j = 1, \ldots, m,\ i = 1,2,3,4),$$

and the eigenvalues and eigenvectors of the Gram matrix Γ of $M = 4m$-ary QAM signals are listed in Table 1.

Therefore, to compute the eigenvalues and eigenvectors of the $4m \times 4m$ matrix Γ, it is sufficient to consider the eigenvalue problem of the smaller matrices A_i $(i = 1,2,3,4)$.

3.6. Relation of the Results in the Relevant Literature

In this subsection, we consider the relation between the results in this paper and those in Ref. [20]. As examples of the multiple constellations of GUS state, the new signals were introduced [20]. They are called a double quantum binary phase shift keying (BPSK) and a double quantum pulse position modulation (PPM). As mentioned in Section 3.1, $4m$-ary

QAM signals also belong to the class of the multiple constellations of GUS state. The signals are not new, but they are rather traditional, and they are well known to be useful. Therefore, it is worth noticing that the results in Ref. [20] are also applicable to $4m$-ary QAM signals. The most significant result is the optimality of SRM. That is, SRM can be an optimal measurement for $4m$-ary QAM signals with certain *a priori* probabilities. Furthermore, various results had been obtained in Ref. [20] while they had shown the optimality of SRM. They provided the block-partitioned form of the Gram matrix and showed that each submatrix is diagonalizable by the Fourier matrix. These results correspond to the results in Sections 3.2 and 3.3. Then, they considered a transformation of the matrix block-partitioned by diagonal submatrices into a block diagonal matrix. This result is closely related to the result in Section 3.4. Although they had not mentioned the eigenvalues and eigenvectors, one may connect their discussion for the square-root of the Gram matrix to the results in this section. We would like to emphasize here a reduction in computational costs, whereas they did not explicitly state a reduction.

Table 1. Eigenvalues and eigenvectors of Γ $(j = 1, \ldots, m)$.

Eigenvalues	Eigenvectors
$a_j^{(1)}$	$\boldsymbol{a}_j^{(1)} \otimes \boldsymbol{\lambda}_1$
$a_j^{(2)}$	$\boldsymbol{a}_j^{(2)} \otimes \boldsymbol{\lambda}_2$
$a_j^{(3)}$	$\boldsymbol{a}_j^{(3)} \otimes \boldsymbol{\lambda}_3$
$a_j^{(4)}$	$\boldsymbol{a}_j^{(4)} \otimes \boldsymbol{\lambda}_4$

4. Examples for the Case of $m = 2$

Here, we consider the simplest case of $m = 2$ as examples.

4.1. Submatrices A_i

From Equation (33), each A_i consists of the eigenvalues $\lambda_i^{(k,l)}$ of $\Gamma_{(k,l)}^{(4)}$. Since $\lambda_j^{(k,l)}$ is a weighted sum of the inner products $\langle\beta_k|\beta_l\rangle, \langle\beta_k|\mathrm{i}\beta_l\rangle, \langle\beta_k| - \beta_l\rangle$, and $\langle\beta_k| - \mathrm{i}\beta_l\rangle$, it is convenient to describe the forms of the inner product for coherent states by using Equation (20):

$$\langle\alpha| \pm |\beta\rangle = e^{\pm\alpha^*\beta} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \quad \langle\alpha| \pm |\mathrm{i}\beta\rangle = e^{\pm\mathrm{i}\alpha^*\beta} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}},$$

where we set $\alpha = \beta_k$ and $\beta = \beta_l$. Using the above forms, we have the following:

$$\begin{aligned}
\lambda_1^{(k,l)} &= \langle\alpha|\beta\rangle + \langle\alpha|\mathrm{i}\beta\rangle + \langle\alpha| - \beta\rangle + \langle\alpha| - \mathrm{i}\beta\rangle \\
&= \left(e^{\alpha^*\beta} + e^{\mathrm{i}\alpha^*\beta} + e^{-\alpha^*\beta} + e^{-\mathrm{i}\alpha^*\beta}\right) e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}} \qquad (41) \\
&= 2\{\cosh(\alpha^*\beta) + \cos(\alpha^*\beta)\} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \\
\lambda_2^{(k,l)} &= \langle\alpha|\beta\rangle - \langle\alpha|\mathrm{i}\beta\rangle + \langle\alpha| - \beta\rangle - \langle\alpha| - \mathrm{i}\beta\rangle \\
&= 2\{\cosh(\alpha^*\beta) - \cos(\alpha^*\beta)\} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \qquad (42) \\
\lambda_3^{(k,l)} &= \langle\alpha|\beta\rangle + \mathrm{i}\langle\alpha|\mathrm{i}\beta\rangle - \langle\alpha| - \beta\rangle - \mathrm{i}\langle\alpha| - \mathrm{i}\beta\rangle \\
&= 2\{\sinh(\alpha^*\beta) - \sin(\alpha^*\beta)\} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \qquad (43) \\
\lambda_4^{(k,l)} &= \langle\alpha|\beta\rangle - \mathrm{i}\langle\alpha|\mathrm{i}\beta\rangle - \langle\alpha| - \beta\rangle + \mathrm{i}\langle\alpha| - \mathrm{i}\beta\rangle \\
&= 2\{\sinh(\alpha^*\beta) + \sin(\alpha^*\beta)\} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \qquad (44)
\end{aligned}$$

where we write the following.

$$\frac{e^x + e^{-x}}{2} = \cosh(x), \quad \frac{e^{\mathrm{i}x} + e^{-\mathrm{i}x}}{2} = \cos(x),$$
$$\frac{e^x - e^{-x}}{2} = \sinh(x), \quad \frac{e^{\mathrm{i}x} - e^{-\mathrm{i}x}}{2\mathrm{i}} = \sin(x).$$

From Equations (41)–(44), we obtain for the case of $m = 2$:

$$A_1 = \begin{bmatrix} \cosh(|\beta_1|^2) + \cos(|\beta_1|^2) & \cosh(\beta_1^*\beta_2) + \cos(\beta_1^*\beta_2) \\ \cosh(\beta_2^*\beta_1) + \cos(\beta_2^*\beta_1) & \cosh(|\beta_2|^2) + \cos(|\beta_2|^2) \end{bmatrix} \circ (2\mathrm{X}), \tag{45}$$

$$A_2 = \begin{bmatrix} \cosh(|\beta_1|^2) - \cos(|\beta_1|^2) & \cosh(\beta_1^*\beta_2) - \cos(\beta_1^*\beta_2) \\ \cosh(\beta_2^*\beta_1) - \cos(\beta_2^*\beta_1) & \cosh(|\beta_2|^2) - \cos(|\beta_2|^2) \end{bmatrix} \circ (2\mathrm{X}), \tag{46}$$

$$A_3 = \begin{bmatrix} \sinh(|\beta_1|^2) - \sin(|\beta_1|^2) & \sinh(\beta_1^*\beta_2) - \sin(\beta_1^*\beta_2) \\ \sinh(\beta_2^*\beta_1) - \sin(\beta_2^*\beta_1) & \sinh(|\beta_2|^2) - \sin(|\beta_2|^2) \end{bmatrix} \circ (2\mathrm{X}), \tag{47}$$

$$A_4 = \begin{bmatrix} \sinh(|\beta_1|^2) + \sin(|\beta_1|^2) & \sinh(\beta_1^*\beta_2) + \sin(\beta_1^*\beta_2) \\ \sinh(\beta_2^*\beta_1) + \sin(\beta_2^*\beta_1) & \sinh(|\beta_2|^2) + \sin(|\beta_2|^2) \end{bmatrix} \circ (2\mathrm{X}), \tag{48}$$

where $\circ$ denotes the Hadamard product, and the following is the case.

$$\mathrm{X} = \begin{bmatrix} e^{-|\beta_1|^2} & e^{-\frac{|\beta_1|^2}{2} - \frac{|\beta_2|^2}{2}} \\ e^{-\frac{|\beta_1|^2}{2} - \frac{|\beta_2|^2}{2}} & e^{-|\beta_2|^2} \end{bmatrix}. \tag{49}$$

The remaining task is to calculate the eigenvalues and eigenvectors of the 2×2 matrices $A_1 \sim A_4$. Although it is possible to calculate eigenvalues and eigenvectors of a 2×2 matrix, the general form may be slightly complicated. In the following, we consider simple two cases.

4.2. Case of $|\beta_1| = |\beta_2| = \gamma$

This case corresponds to phase-mismatching PSK signals. The signals are similar to the double quantum BPSK with a misalignment or a systematic bias error in the angle defining one of the two constellations [20]. Note that the number of signals is different. In this case, from the following:

$$\mathrm{X} = \begin{bmatrix} e^{-\gamma^2} & e^{-\gamma^2} \\ e^{-\gamma^2} & e^{-\gamma^2} \end{bmatrix},$$

"$\circ(2\mathrm{X})$" in Equations (45)–(48) becomes simply a scalar product "$\times(2e^{-\gamma^2})$". Therefore, each A_i has the following form:

$$\begin{bmatrix} a & b \\ b^* & a \end{bmatrix},$$

where a is a real number and b is a complex number. The eigenvalues and the corresponding orthonormal eigenvectors of the above form are the following:

$$a \pm |b|, \quad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \pm e^{-\mathrm{i}\mu} \end{bmatrix}, \tag{50}$$

where $\mu = \arg(b)$. Therefore, the eigenvalues of A_i are as follows:

$$a_1^{(1)} = 2e^{-\gamma^2}\Big\{\cosh(\gamma^2) + \cos(\gamma^2) + |\cosh(\delta) + \cos(\delta)|\Big\}, \tag{51}$$

$$a_2^{(1)} = 2e^{-\gamma^2}\Big\{\cosh(\gamma^2) + \cos(\gamma^2) - |\cosh(\delta) + \cos(\delta)|\Big\}, \tag{52}$$

$$a_1^{(2)} = 2e^{-\gamma^2}\Big\{\cosh(\gamma^2) - \cos(\gamma^2) + |\cosh(\delta) - \cos(\delta)|\Big\}, \tag{53}$$

$$a_2^{(2)} = 2e^{-\gamma^2}\Big\{\cosh(\gamma^2) - \cos(\gamma^2) - |\cosh(\delta) - \cos(\delta)|\Big\}, \tag{54}$$

$$a_1^{(3)} = 2e^{-\gamma^2}\Big\{\sinh(\gamma^2) - \sin(\gamma^2) + |\sinh(\delta) - \sin(\delta)|\Big\}, \tag{55}$$

$$a_2^{(3)} = 2e^{-\gamma^2}\Big\{\sinh(\gamma^2) - \sin(\gamma^2) - |\sinh(\delta) - \sin(\delta)|\Big\}, \tag{56}$$

$$a_1^{(4)} = 2e^{-\gamma^2}\Big\{\sinh(\gamma^2) + \sin(\gamma^2) + |\sinh(\delta) + \sin(\delta)|\Big\}, \tag{57}$$

$$a_2^{(4)} = 2e^{-\gamma^2}\Big\{\sinh(\gamma^2) + \sin(\gamma^2) - |\sinh(\delta) + \sin(\delta)|\Big\}, \tag{58}$$

where we set $\beta_1 = \gamma e^{\nu_1}, \beta_2 = \gamma e^{\nu_2}, \beta_1^* \beta_2 = \gamma^2 e^{\mathbf{i}(\nu_2 - \nu_1)} = \delta$.

The eigenvectors of A_i are as follows:

$$\boldsymbol{a}_1^{(i)} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ e^{-\mathbf{i}\mu_i} \end{bmatrix}, \qquad \boldsymbol{a}_2^{(i)} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -e^{-\mathbf{i}\mu_i} \end{bmatrix}, \quad (i = 1, 2, 3, 4) \tag{59}$$

where the following is the case.

$$\mu_1 = \arg(\cosh(\delta) + \cos(\delta)), \quad \mu_2 = \arg(\cosh(\delta) - \cos(\delta)),$$
$$\mu_3 = \arg(\sinh(\delta) - \sin(\delta)), \quad \mu_4 = \arg(\sinh(\delta) + \sin(\delta)).$$

4.3. Case of $\arg(\beta_1) = \arg(\beta_2) = \nu$

The signals in this case are similar to the four-pulse amplitude modulation (PAM) [20]. Note that the number of signals is eight in this case, but four for the 4-PAM. In this case, the form of A_i is as follows:

$$\begin{bmatrix} a & b \\ b & c \end{bmatrix}, \tag{60}$$

where a, b, and c are real numbers. The eigenvalues of the matrix with this form are as follows:

$$\frac{1}{2}\left(a + c \pm \sqrt{(a-c)^2 + 4b^2}\right), \tag{61}$$

and the corresponding orthogonal eigenvectors are the following.

$$\begin{bmatrix} a - c \pm \sqrt{(a-c)^2 + 4b^2} \\ 2b \end{bmatrix}. \tag{62}$$

We obtain the orthonormal eigenvectors by normalizing them. Using the above equations, we can obtain the explicit forms of $a_1^{(1)} \sim a_2^{(4)}$ and $\boldsymbol{a}_1^{(1)} \sim \boldsymbol{a}_2^{(4)}$ as the same manner in Section 4.2.

5. Numerical Experiments

Here, we provide numerical experiments as examples of application for the results in Section 3. We consider 16QAM signals (the case of $m = 4$) in this section. Set $\beta_1 = (1 + \mathbf{i})\alpha$,

$\beta_2 = (3+\mathbf{i})\alpha, \beta_3 = (3+3\mathbf{i})\alpha, \beta_4 = (1+3\mathbf{i})\alpha$. The average number of photons of 16QAM coherent-state signals is as follows:

$$\frac{1}{4}\left(|(1+\mathbf{i})\alpha|^2 + |(3+\mathbf{i})\alpha|^2 + |(3+3\mathbf{i})\alpha|^2 + |(1+3\mathbf{i})\alpha|^2\right) = 10|\alpha|^2,$$

and it is proportional to $|\alpha|^2$. Hence, in the following, we show numerical results of some quantities with respect to $|\alpha|^2$.

5.1. Von Neumann Entropy

First, we consider the von Neumann entropy, which is calculated by using eigenvalues of the Gram matrix. Since the Holevo capacity is the maximization of the von Neumann entropy with respect to *a priori* probabilities, the von Neumann entropy is a lower bound on the capacity. Let $\hat{\rho}$ be the density operator of 16QAM signals. Then, the von Neumann entropy (9) is calculated by the eigenvalues of $\hat{\rho}$ as follows.

$$\chi = -\sum_{j=1}^{16} \lambda_j \log_2 \lambda_j.$$

Each λ_j is equal to an eigenvalue of $\frac{1}{16}\Gamma$ from Equation (13). According to the results in Section 3, the following is the case:

$$\begin{aligned}\chi &= -\sum_{i=1}^{4}\sum_{j=1}^{4}\left(\frac{1}{16}a_j^{(i)}\right)\log_2\left(\frac{1}{16}a_j^{(i)}\right) = -\frac{1}{16}\sum_{i=1}^{4}\sum_{j=1}^{4} a_j^{(i)}\left(\log_2 a_j^{(i)} - \log_2 16\right)\\ &= 4 - \frac{1}{16}\sum_{i=1}^{4}\sum_{j=1}^{4} a_j^{(i)}\log_2 a_j^{(i)},\end{aligned}$$

where $a_j^{(i)}$ are eigenvalues of the matrices A_i described in Section 3, and we numerically calculate $a_j^{(i)}$. Note that we only need numerical calculation of eigenvalues for smaller matrices A_i than the original Gram matrix Γ.

Figure 2 shows the von Neumann entropy of 16QAM signals with respect to $|\alpha|^2$. The blue line is drawn by using the results in Section 3, while the red dots are plotted by using direct calculation of eigenvalues for the Gram matrix. From Figure 2, we can confirm that both results are identical.

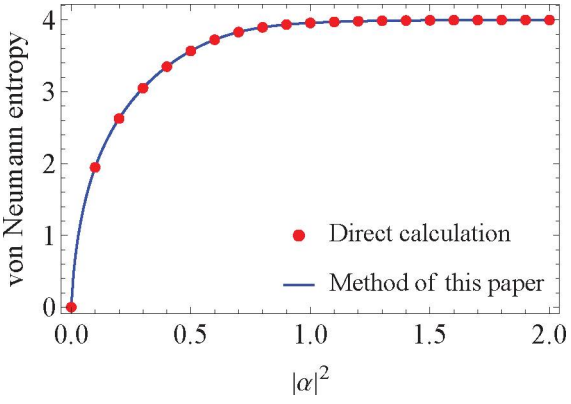


Figure 2. von Neumann entropy of 16QAM signals with respect to $|\alpha|^2$. The blue line is drawn by using the results in Section 3, while the red dots are plotted by using direct calculation of eigenvalues for the Gram matrix.

5.2. Error Probability

Now, we consider the error probability by using the SRM. To compute the error probability, both eigenvalues and eigenvectors of the Gram matrix are needed. As explained in Section 2, the error probability is as follows.

$$P_{\mathrm{e}} = 1 - \frac{1}{16}\sum_{i=1}^{16} P(i|i) = 1 - \frac{1}{16}\sum_{i=1}^{16}\left|\left(\Gamma^{\frac{1}{2}}\right)_{i,i}\right|^2.$$

From Equation (40), we have the following.

$$\Gamma^{\frac{1}{2}} = \sum_{i=1}^{4}\sum_{j=1}^{4}\sqrt{a_j^{(i)}}\,\boldsymbol{a}_j^{(i)}\boldsymbol{a}_j^{(i)\mathrm{H}} \otimes \boldsymbol{\lambda}_i\boldsymbol{\lambda}_i^{\mathrm{H}}.$$

Then, numerically calculating the eigenvalues $a_j^{(i)}$ and the eigenvectors $\boldsymbol{a}_j^{(i)}$ for matrices A_i, and substituting them into the above equation, we obtain the error probability.

Figure 3 shows the error probability of 16QAM signals with respect to $|\alpha|^2$. The blue line and the red dots have the same meaning as in Figure 2. From Figure 3, we can confirm that both results are identical.

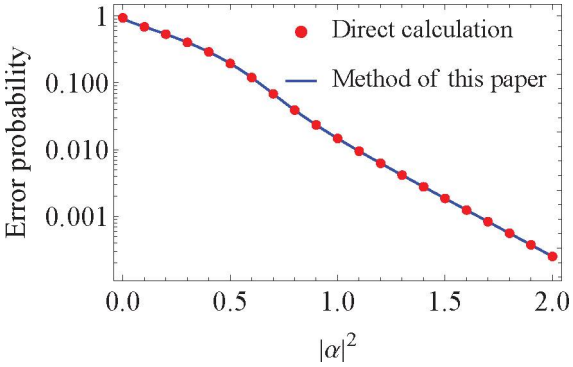


Figure 3. Error probability of 16QAM signals with respect to $|\alpha|^2$. The blue line is drawn by using the results in Section 3, while the red dots are plotted by using direct calculation of the matrix square-root for the Gram matrix.

6. Conclusions

In this paper, we have described the simplification of the Gram matrix eigenvalue problem for QAM coherent-state signals and shown that the scale of the computation can be reduced. As explained in Section 2, by solving the eigenvalue problem of the Gram matrix, it is possible to calculate quantities such as the error probability, mutual information, Holevo capacity, and the upper and lower bounds of the reliability function, which are important for evaluating the performance of quantum communication, quantum radar, and the security of quantum cryptography. The QAM signals treated in this study are very versatile, being applicable not only to ordinary QAM signals but also to any signals generated by rotation in the first quadrant of the phase plane. The quantum state used is typically but not necessarily the coherent state. In fact, the QAM signals defined in this paper belong to the class of the multiple constellations of GUS [20] and CGU states [41]. Therefore, the results in the literature are also applicable to QAM signals. Moreover, some results in Ref. [20] are closely related to the results in this paper, as explained in Section 3.6.

The most significant challenge for the future is the further simplification of the eigenvalue problem of the Gram matrix. For this purpose, the regularity of the signal constellation in the first quadrant of the phase plane should be taken into account. Therefore, carefully determining the order of signals in the first quadrant is important, even if they are

the same signals. Another challenge is to apply the methods of this study to actual problems, whereas we have shown simple examples for 16QAM. For this purpose, the combined use of numerical algorithms (e.g., [42]) for the matrix calculations should be considered.

Author Contributions: Conceptualization, T.S.U.; methodology, R.M.; validation, T.W.; formal analysis, R.M.; investigation, R.M.; writing—original draft preparation, R.M.; writing—review and editing, T.W. and T.S.U.; supervision, T.S.U.; project administration, T.S.U.; funding acquisition T.W. and T.S.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by JSPS KAKENHI (grant number JP20K20397, JP20H00581, and JP21K04064) and research grants from the Marubun Research Promotion Foundation and the Nitto Foundation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank S. Takahira and M. Yoshida for valuable discussions during this and previous research studies. We thank Stuart Jenkinson, PhD, from Edanz (https://jp.edanz.com/ac, accessed on 12 April 2022) for editing a draft of this manuscript.

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

Abbreviations

The following abbreviations are used in this manuscript:

SRM	Square-root measurement;
PSK	Phase shift keying;
ASK	Amplitude shift keying;
QAM	Quadrature amplitude modulation;
AMPM	Amplitude-modulated phase-modulated;
POVM	Positive operator-valued measure.

References

1. Helstrom, C.W. Detection theory and quantum mechanics. *Inform. Control* **1967**, *10*, 254–291. [CrossRef]
2. Holevo, A.S. Statistical decision theory for quantum systems. *J. Multivar. Anal.* **1973**, *3*, 337–394. [CrossRef]
3. Yuen, H.P.; Kennedy, R.S.; Lax, M. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inform. Theory* **1975**, *21*, 125–134. [CrossRef]
4. Helstrom, C.W. *Quantum Detection and Estimation Theory*; Academic Press: New York, NY, USA, 1976.
5. Hirota, O.; Ikehara, S. Minimax strategy in the quantum detection theory and its application to optical communication. *Trans. IECE* **1982**, *65*, 627–633.
6. Yuen, H.P. KCQ: A new approach to quantum cryptography I. General principles and key generation. *arXiv* **2004**, arXiv:quant-ph/0311061.
7. Yuen, H.P. Key generation: Foundations and a new quantum approach. *IEEE J. Sel. Top. Quantum Electron.* **2009**, *15*, 1630–1645. [CrossRef]
8. Corndorf, E.; Liang, C.; Kanter, G.S.; Kumar, P.; Yuen, H.P. Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks. *Phys. Rev. A* **2005**, *71*, 062326. [CrossRef]
9. 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]
10. Tanizawa, K.; Futami, F. Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels. *Opt. Express* **2019**, *27*, 1071–1079. [CrossRef]
11. 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]
12. Belavkin, V.P. Optimal multiple quantum statistical hypothesis testing. *Stochastics* **1975**, *1*, 315–345. [CrossRef]
13. Belavkin, V.P. Optimal distinction of non-orthogonal quantum signals. *Radio Eng. Electron. Phys.* **1975**, *20*, 39–47.
14. Hausladen, P.; Jozsa, R.; Schumacher, B.; Westmoreland, M.; Wootters, W.K. Classical information capacity of a quantum channel. *Phys. Rev. A* **1996**, *54*, 1869–1876. [CrossRef] [PubMed]

15. Eldar, Y.C.; Forney, G.D., Jr. On quantum detection and the square-root measurement. *IEEE Trans. Inform. Theory* **2001**, *47*, 858–872. [CrossRef]
16. Kato, K.; Hirota, O. Square-root measurement for quantum symmetric mixed state signals. *IEEE Trans. Inform. Theory* **2003**, *49*, 3312–3317. [CrossRef]
17. 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]
18. Usuda, T.S.; Takumi, I.; Hata, M.; Hirota, O. Minimum error detection of classical linear code sending through a quantum channel. *Phys. Lett. A* **1999**, *256*, 104–108. [CrossRef]
19. Usuda, T.S.; Usami, S.; Takumi, I.; Hata, M. Superadditivity in capacity of quantum channel for q-ary linearly dependent real symmetric-state signals. *Phys. Lett. A* **2002**, *305*, 125–134. [CrossRef]
20. Dalla Pozza, N.; Pierobon, G. Optimality of square-root measurements in quantum state discrimination. *Phys. Rev. A* **2015**, *91*, 042334. [CrossRef]
21. Osaki, M.; Usuda, T.S.; Hirota, O. Group covariant detection for a three-phase shift keyed signal. *Phys. Lett. A* **1998**, *245*, 189–196. [CrossRef]
22. Takeuchi, H.; Yamaguchi, S.; Usuda, T.S. Entanglement-assisted classical communication using quasi Bell states. In Proceedings of the 1st International Workshop on Entangled Coherent State and Its Application to Quantum Information Science—Towards Macroscopic Quantum Communications, Tokyo, Japan, 26–28 November 2012; pp. 115–119.
23. Burnashev, M.V.; Holevo, A.S. On reliability function of quantum communication channel. *Probl. Peredachi Inform.* **1998**, *34*, 1–13.
24. Dalai, M. Lower bounds on the probability of error for classical and classical-quantum channels. *IEEE Trans. Inform. Theory* **2013**, *59*, 8027–8056. [CrossRef]
25. Isaacs, I.M. *Character Theory of Finite Groups*; Academic Press: New York, NY, USA; London, UK, 1976.
26. Usuda, T.S.; Shiromoto, K. Analytical expression of s-th power of Gram matrix for group covariant signals and its application. In *Quantum Communication, Measurement and Computing (QCMC), AIP Conference Proceedings*; American Institute of Physics: New York, NY, USA, 2011; Volume 1363, pp. 97–100.
27. Usuda, T.S.; Takumi, I. Group covariant signals in quantum information theory. In *Quantum Communication, Computing, and Measurement 2*; Plenum Press: New York, NY, USA, 2000; pp. 37–42.
28. Kato, K.; Osaki, M.; Sasaki, M.; Hirota, O. Quantum detection and mutual information for QAM and PSK signals. *IEEE Trans. Commun.* **1999**, *47*, 248–254. [CrossRef]
29. Kato, K.; Hirota, O. Quantum quadrature amplitude modulation system and its applicability to coherent-state quantum cryptography. In Proceedings of the SPIE, Quantum Communications and Quantum Imaging III, San Diego, CA, USA, 31 July 2005; Volume 5893.
30. Ishida, Y.; Kato, K.; Usuda, T.S. Capacity of attenuated channel with discrete-valued input. In Proceedings of the 8th International Conference on Quantum Communication, Measurement and Computing, Tsukuba, Japan, 28 November–3 December 2006; NICT Press: Tokyo, Japan, 2007; pp. 323–326.
31. Miyazaki, R.; Yoshida, M.; Usuda, T.S. Simplification of calculation of channel matrix for 2m-ary ASK coherent-state signals. In Proceedings of the 2019 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, Nagoya, Japan, 9–10 September 2019; No. F5-4. (In Japanese)
32. Miyazaki, R.; Yoshida, M.; Wang, T.; Usuda, T.S. Simplification of the calculation of the channel matrix for AMPM coherent-state signals. In Proceedings of the 2020 International Symposium on Information Theory and Its Applications (ISITA2020), Hawai'i, HI, USA, 24–27 October 2020; pp. 121–125.
33. Miyazaki, R.; Yoshida, M.; Wang, T.; Takahira, S.; Usuda, T.S. Simplification of calculation of channel matrix for non-symmetric signals. *IEICE Trans. Commun.* **2022**, *J105-B*, 74–87. (In Japanese)
34. Sasaki, M.; Kato, K.; Izutsu, M.; Hirota, O. Quantum channels showing superadditivity in classical capacity. *Phys. Rev. A* **1998**, *58*, 146–158. [CrossRef]
35. Horn, R.A.; Jonson, C.R. *Matrix Analysis*; Cambridge University Press: Cambridge, UK, 1985.
36. Kato, K.; Osaki, M.; Hirota, O. Derivation of classical capacity of quantum channel for discrete information source. *Phys. Lett. A* **1999**, *251*, 157–163. [CrossRef]
37. Kato, K. Error exponents of quantum communication system with M-ary PSK coherent state signal. *Tamagawa Univ. Quantum ICT Res. Inst. Bull.* **2011**, *1*, 33–40.
38. Kato, K. A note on the reliability function for M-ary PSK coherent state signal. *Tamagawa Univ. Quantum ICT Res. Inst. Bull.* **2018**, *8*, 21–25.
39. Davies, E.B. Information and quantum measurement. *IEEE Trans. Inform. Theory* **1978**, *IT-24*, 596–599. [CrossRef]
40. Kikuchi, K. Digital coherent optical communication systems: Digital coherent optical communication systems. *IEICE Electron. Express* **2011**, *8*, 1642–1662. [CrossRef]
41. Eldar, Y.C.; Megretski, A.; Verghese, G. Optimal detection of symmetric mixed quantum states. *IEEE Trans. Inform. Theory* **2004**, *50*, 1198–1207. [CrossRef]
42. Mizuno, S.; Moriizumi, Y.; Usuda, T.S.; Sogabe, T. An initial guess of Newton's method for the matrix square root based on a sphere constrained optimization problem. *JSIAM Lett.* **2016**, *8*, 17–20. [CrossRef]

entropy

MDPI

Article

Error Performance of Amplitude Shift Keying-Type Asymmetric Quantum Communication Systems

Tiancheng Wang [1,2,*] and Tsuyoshi Sasaki Usuda [2,*]

[1] Faculty of Engineering, Kanagawa University, Yokohama 221-8686, Kanagawa, Japan
[2] Graduate School of Information Science and Technology, Aichi Prefectural University, Nagakute 480-1198, Aichi, Japan
* Correspondence: wang@kanagawa-u.ac.jp (T.W.); usuda@ist.aichi-pu.ac.jp (T.S.U.)

Abstract: We propose an amplitude shift keying-type asymmetric quantum communication (AQC) system that uses an entangled state. As a first step toward development of this system, we evaluated and considered the communication performance of the proposed receiver when applied to the AQC system using a two-mode squeezed vacuum state (TSVS), the maximum quasi-Bell state, and the non-maximum quasi-Bell state, along with an asymmetric classical communication (ACC) system using the coherent state. Specifically, we derived an analytical expression for the error probability of the AQC system using the quasi-Bell state. Comparison of the error probabilities of the ACC system and the AQC systems when using the TSVS and the quasi-Bell state shows that the AQC system using the quasi-Bell state offers a clear performance advantage under specific conditions. Additionally, it was clarified that there are cases where the universal lower bound on the error probability for the AQC system was almost achieved when using the quasi-Bell state, unlike the case in which the TSVS was used.

Keywords: entanglement; quasi-Bell state; asymmetric communication system; error performance

Citation: Wang, T.; Usuda, T.S. Error Performance of Amplitude Shift Keying-Type Asymmetric Quantum Communication Systems. *Entropy* **2022**, *24*, 708. https://doi.org/10.3390/e24050708

Academic Editor: Osamu Hirota

Received: 18 March 2022
Accepted: 11 May 2022
Published: 16 May 2022

1. Introduction

Entanglement [1] is an important phenomenon for quantum protocols. Entanglement is a nonlocal correlation that works with multiple quantum systems. This correlation can be maintained regardless of the distance between these multiple quantum systems. The quantum cryptographic protocol called E91 [2], quantum superdense coding [3], and quantum teleportation [4], which were all proposed in the 1990s, are well known as quantum communication protocols that apply entanglement. In addition, quantum illumination [5] and quantum reading [6], which are quantum metrology protocols based on entanglement and were proposed around 2010, have also been attracting increasing attention in recent years.

Many of the quantum communication protocols described above that use entanglement belong to the class of symmetric communication systems. Symmetric communication systems have the same transmission capability, regardless of the direction of communication. In contrast, asymmetric communication systems have different transmission capabilities that depend on the direction of communication (e.g., [7,8]). The differences in transmission capability in this case are caused by the differences between the physical resources that can be used on the two sides of the communication process. However, as far as we know, there are no asymmetric communication systems which essentially utilize quantum mechanical phenomena such as entanglement. With this in mind, we define the following: asymmetric systems using quantum and classical communication protocols are called asymmetric quantum communication (AQC) systems and asymmetric classical communication (ACC) systems, respectively. In this paper, we consider the quantum communication protocols with entanglement. Typical examples of ACC systems include terrestrial-to-satellite communications, communication between a mobile device and a cellular base station, and communication between an Internet of Things (IoT) device and an IoT base station. For example, in an IoT-based ACC system, there is a major difference

between the transmission capabilities of a small battery-driven IoT device—where the battery is replaced once every few years and the microprocessor unit can only perform simple calculation processes—and that of a base station with an abundant power supply and high processing capacity. In this work, the side with the low transmission capability, e.g., satellites, mobile phones, and IoT devices, is called Alice, and the side with the high transmission capability, e.g., ground base stations, mobile phone base stations, and IoT base stations, is called Bob. Taking an IoT-based ACC system as an example, the usage scenario of that is considered as a simple model in this paper follows: (1) Bob (the IoT base station) tells Alice (the IoT device) whether to sense the physical environment; (2) if yes, Alice senses the physical environment and transmits the corresponding data to Bob. In general, information leakage is prone to occur in the channel of (2), and the system must perform some communication protocols, such as lightweight cryptography. One of the security problems for the asymmetric communication system can be described as follows: the low processing capacity struggles to always provide a high security level for the data transmitted from such an IoT device, because the frequency of upgrading the device may be low and the development of code breaking technique is fast. We aimed to develop a new AQC system to improve the reliability and security of communications from Alice to Bob, and also to reduce Alice's energy costs by introducing entanglement into the asymmetric communication system. This paper represents the first step in this research.

To develop the required AQC system, it will be necessary to clarify the effects of deterioration of the quantum effects in the various channels with respect to the entangled state. Reference [9] dealt with the quantum channel discrimination problem using beam splitters with reflectivities of R_0 and $R_1 (0 \leq R_0 < R_1 \leq 1)$. In this channel model, a quantum state source (i.e., a light source) produces an entangled state, and these two modes are labeled S (signal mode: mode S) and A (ancilla mode: mode A). Light corresponding to mode S is directed toward one beam splitter with a reflectivity of either R_0 or R_1; the subsequently reflected light is then collected using a detector. The other beam, which corresponds to mode A, is sent to the detector directly. The detector then distinguishes the two channels that correspond to R_0 and R_1 by performing optimum quantum measurements (i.e., joint measurements) of the two light beams. In reference [9], the Einstein–Podolsky–Rosen (EPR) state, which consists of the m-fold tensor product of the two-mode squeezed vacuum state (TSVS) [10], was used as the light source, and the performance with regard to the error probability when using the EPR state was evaluated using its upper bound, which is defined by the Chernoff bound [11], and the lower bound, which is defined by the fidelity. As a result, it was found that the lower bound on the error probability when using the EPR state may almost reach the universal lower bound. In fact, if we consider that the communication system is used in such a manner that Alice operates the two beam splitters to transmit binary information to Bob based on differences in reflectivity (i.e., the differences in the amplitudes of the reflected light beams when subjected to different energy attenuation levels), the model in reference [9] would be an amplitude shift keying (ASK)-type AQC system. Therefore, it can be said that the work in this paper uses the same model for a different purpose to that of reference [9].

When considering aspects of the communication performance, it is necessary to perform instantaneous performance evaluations, but not using the Chernoff bound that corresponds to the case in which m-shot optical pulses are applied; instead, the error probability when a one-shot optical pulse is used here. In this case, the TSVS, i.e., the EPR state when $m = 1$, is considered, rather than the EPR state. In addition, there is a quasi-Bell state [12] that is constructed using nonorthogonal quantum states such as coherent states, but it becomes the maximum entangled state (maximum quasi-Bell state). It has been shown that the attenuation resistance of this state is strong, depending on application protocols, and it has been studied actively (e.g., [13,14]) since the publication of reference [12]. In addition, study of the application of a quasi-Bell state that is not the maximum entangled state (i.e., a non-maximum quasi-Bell state) has advanced, and it has been reported that the non-maximum quasi-Bell state is superior to the maximum quasi-Bell state for use in certain protocols, such as quantum teleportation [15]. In particular, it was recently clarified

that the quasi-Bell state is superior to both the TSVS and conventional laser radar in terms of its performance for quantum illumination with attenuation (i.e., the model used in this paper with $R_0 = 0$) [16–19].

Based on the discussion above, we aim to clarify Bob's communication performance based on the error probability criterion as a first step toward development of an ASK-type AQC system (hereinafter referred to simply as the AQC system). Specifically, by using the Schrödinger picture to describe the time evolution of both the quasi-Bell state and the TSVS, we evaluate and compare the error probabilities that occur when using these states, and thus consider the basic characteristics, i.e., the error performance, of the AQC system. We also compare these results with the error probability characteristics of an ACC system which was constructed using a coherent state source and an optimum classical measurement approach, along with the universal lower bound on the error probability when the use of any multimode quantum state is allowed. As the main results of this analysis, we derive an analytical expression for the error probability of the AQC system when using the quasi-Bell state. Then, by investigating the numerical characteristics of the system using this analytical expression with various reflectivities and the average number of photons, we demonstrate that the AQC system using the quasi-Bell state is not only always superior to the ACC system, but also is asymptotically superior to the same AQC system using the TSVS. Additionally, in contrast to reference [9], which shows that using the EPR state asymptotically outperforms using the coherent state, this paper shows that the ACC system asymptotically outperforms the AQC system when using the TSVS. Finally, we show that the AQC system using the quasi-Bell state may almost reach the universal lower bound on the error probability, unlike the AQC system using the TSVS.

The rest of this paper is organized as follows. Section 2 describes the TSVS, the quasi-Bell state, and the ACC system. Section 3 describes the model of the AQC system when using the entangled states, and also provides a description of Bob's received quantum states in the AQC system. Section 4 presents an analytical expression for the error probability of the AQC system when using the quasi-Bell state. In Section 5, by using the analytical expression obtained in Section 4, the system error performance is given and is compared numerically with the error probabilities of both the ACC system and the AQC system when using the TSVS and the universal lower bound on the error probability.

2. Basic Theory

2.1. Quantum State

The state of a quantum system (i.e., the quantum state ρ) is expressed using a density operator. This density operator is a nonnegative Hermitian operator on Hilbert space and satisfies

$$\rho \geq 0, \ \mathrm{Tr}\,\rho = 1. \tag{1}$$

Originally, ρ was called the density operator of the quantum state, but it has become customary for ρ also to be called a quantum state.

2.2. Photon Number State

The most typical quantum state of light is the photon number state $|n\rangle$, which represents a state in which the number of photons is n, and it forms the following orthonormal basis:

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = \mathbb{I}, \langle n|m\rangle = \delta_{mn}, \tag{2}$$

where $\mathbb{I}$ is the identity operator on Hilbert space, and δ_{mn} is the Kronecker delta.

2.3. Coherent State

This paper considers a quasi-Bell state that has been constructed using coherent states that are nonorthogonal quantum states. The coherent state is known as the most

fundamental quantum state of light, and this state is very important because it can be realized approximately using laser light. The coherent state is expressed as

$$|\alpha\rangle = \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} e^{-\frac{1}{2}|\alpha|^2} |n\rangle, \tag{3}$$

where α is the complex amplitude of the coherent state, and the average number of photons of the state is $\langle n \rangle_{\mathrm{Coh}} = |\alpha|^2$.

The inner product of the two coherent states corresponding to the amplitudes α and β is

$$\langle \alpha | \beta \rangle = e^{\alpha^* \beta - \frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}. \tag{4}$$

If both α and β are real numbers, then the value of $\langle \alpha | \beta \rangle$ is also a real number. In addition, the coherent state that is reflected from a beam splitter with reflectivity R is subjected to energy attenuation, causing it to become another coherent state, represented by $|\sqrt{R}\alpha\rangle$.

2.4. Quasi-Bell State

The quasi-Bell state [12] is an entangled state that is constructed using nonorthogonal quantum states but has maximum entanglement. The two modes of the quasi-Bell state can be labeled S and A. In this paper, we use two coherent states as the nonorthogonal quantum states, where the coherent states with amplitudes α and β are denoted by $|\alpha\rangle$ and $|\beta\rangle$. The quasi-Bell states are represented as the quantum states of the composite system SA as follows:

$$|\Psi_1\rangle_{\mathrm{SA}} = h_1(|\alpha\rangle_{\mathrm{S}}|\beta\rangle_{\mathrm{A}} + |-\alpha\rangle_{\mathrm{S}}|-\beta\rangle_{\mathrm{A}}), \tag{5}$$

$$|\Psi_2\rangle_{\mathrm{SA}} = h_2(|\alpha\rangle_{\mathrm{S}}|\beta\rangle_{\mathrm{A}} - |-\alpha\rangle_{\mathrm{S}}|-\beta\rangle_{\mathrm{A}}), \tag{6}$$

$$|\Psi_3\rangle_{\mathrm{SA}} = h_3(|\alpha\rangle_{\mathrm{S}}|-\beta\rangle_{\mathrm{A}} + |-\alpha\rangle_{\mathrm{S}}|\beta\rangle_{\mathrm{A}}), \tag{7}$$

$$|\Psi_4\rangle_{\mathrm{SA}} = h_4(|\alpha\rangle_{\mathrm{S}}|-\beta\rangle_{\mathrm{A}} - |-\alpha\rangle_{\mathrm{S}}|\beta\rangle_{\mathrm{A}}), \tag{8}$$

where

$$h_1 = h_3 = \frac{1}{\sqrt{2(1+\kappa_{\mathrm{S}}\kappa_{\mathrm{A}})}}, \tag{9}$$

$$h_2 = h_4 = \frac{1}{\sqrt{2(1-\kappa_{\mathrm{S}}\kappa_{\mathrm{A}})}}, \tag{10}$$

$$\kappa_{\mathrm{S}} = \langle \alpha | -\alpha \rangle = \langle -\alpha | \alpha \rangle = e^{-2|\alpha|^2}, \tag{11}$$

$$\kappa_{\mathrm{A}} = \langle \beta | -\beta \rangle = \langle -\beta | \beta \rangle = e^{-2|\beta|^2}, \tag{12}$$

and α and β are nonnegative real numbers.

$|\Psi_2\rangle_{\mathrm{SA}}$ has the maximum entanglement, and the amount of entanglement is 1 ebit when $\alpha = \beta$. Therefore, we treat $|\Psi_2\rangle_{\mathrm{SA}}$ with $\alpha = \beta$ as the maximum quasi-Bell state in this paper. The average number of photons in mode S is $\langle n \rangle_{\mathrm{Max}} = |\alpha|^2 \coth(2|\alpha|^2)$, and the minimum average number of photons is 0.5 because $\langle n \rangle_{\mathrm{Max}} \to 0.5$ when $\alpha \to 0$. Additionally, we treat $|\Psi_1\rangle_{\mathrm{SA}}$ with $\alpha = \beta$ as the non-maximum quasi-Bell state in this paper. Note that the amount of entanglement in this case is smaller than 1 ebit. The average number of photons in mode S is $\langle n \rangle_{\mathrm{NonMax}} = |\alpha|^2 \tanh(2|\alpha|^2)$, and the minimum average number of photons is 0 because $\langle n \rangle_{\mathrm{NonMax}} \to 0$ when $\alpha \to 0$.

2.5. TSVS

In reference [9], an m-fold tensor product of the following TSVS was used as an EPR state:

$$|\psi\rangle_{\mathrm{SA}} = \sum_{n=0}^{\infty} \sqrt{\frac{N_{\mathrm{S}}^{n}}{(N_{\mathrm{S}}+1)^{n+1}}} |n\rangle_{\mathrm{S}} |n\rangle_{\mathrm{A}}, \tag{13}$$

where $\langle n \rangle_{\mathrm{TSVS}} = N_{\mathrm{S}}$ represents the average number of photons in mode S. In this paper, we set $m = 1$ and analyze the TSVS.

The TSVS is one of the most important entangled states and has been discussed in numerous studies as a basic quantum state in both quantum illumination [20] and quantum reading [6] protocols. In particular, the amount of entanglement of the TSVS, which is given by

$$E_{\mathrm{TSVS}} = (N_{\mathrm{S}}+1)\log_2(N_{\mathrm{S}}+1) - N_{\mathrm{S}}\log_2 N_{\mathrm{S}}, \tag{14}$$

can exceed 1 ebit. A larger average number of photons causes a greater amount of entanglement because $\lim_{N_{\mathrm{S}}\to\infty} E_{\mathrm{TSVS}} = \infty$.

2.6. Asymmetric Classical Communication

In this paper, we also compare the proposed system with an ACC system that has no mode A—mode A can be considered to be the vacuum state $|0\rangle_{\mathrm{A}}$ in an AQC system without entanglement. Here, the coherent state $|\alpha\rangle$ is prepared by Bob as the light source and is directed toward one of the two beam splitters operated by Alice. By switching the two beam splitters with their reflectivities of R_0 and $R_1 (R_0 < R_1)$, Alice encodes binary information using the different reflectivities. The reflected light collected by Bob thus becomes the binary coherent state signal $\{|\sqrt{R_0}\alpha\rangle, |\sqrt{R_1}\alpha\rangle\}$, and this can be considered to be an ASK modulation scheme. Assuming that the binary signal has equal *a priori* probabilities and that the measurement in Bob's detector, which we call an optimum classical receiver, is a homodyne measurement, the error probability for Bob is then given as follows:

$$P_{\mathrm{e}}^{(\mathrm{Hom})} = \frac{1}{2}\left\{1 + \mathrm{erf}\left(\frac{\sqrt{R_0}|\alpha|^2 - \sqrt{R_1}|\alpha|^2}{\sqrt{2}}\right)\right\}. \tag{15}$$

3. Model of an ASK-Type AQC System

In this section, we describe the model of the AQC system that is constructed using the entangled states and the description of Bob's received quantum states in the AQC system.

A diagram of the model of the AQC system using the entangled state is shown in Figure 1. Binary information is sent from Alice to Bob. The dashed and solid arrows in the figure represent mode S and mode A of the entangled state, respectively. The AQC system protocol is given as follows:

Protocol of an AQC system (Figure 1).

1. Bob (receiver) inputs the light corresponding to mode A directly into their detector.
2. Bob radiates the light corresponding to mode S toward one of the two beam splitters operated by Alice (sender); Alice then switches the two beam splitters with reflectivities of R_0 and R_1 $(R_0 < R_1)$ to encode the binary information.
3. The subsequently reflected light with reflectivity of either R_0 or R_1 is then collected by Bob's detector.
4. Bob decodes the binary information received at their detector by performing an optimum quantum measurement, i.e., a joint measurement of both light beams.

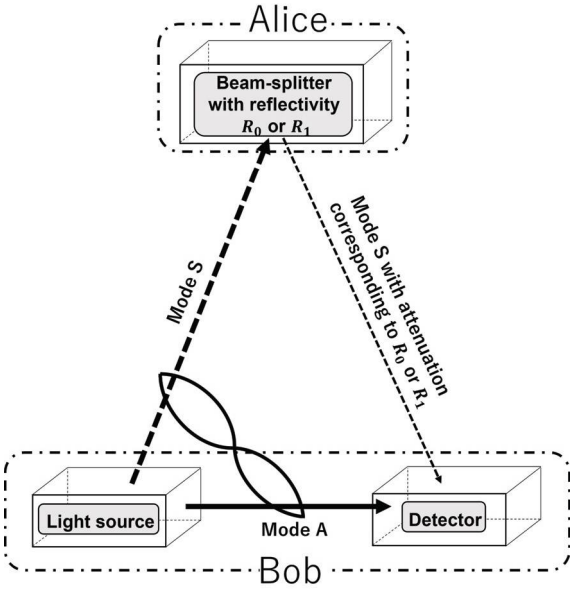


Figure 1. Protocol of an amplitude shift keying-type asymmetric quantum communication system.

In this paper, we use the same model for a different purpose than that of reference [9], and therefore must first clarify the differences in this case when compared with the basic characteristics presented in [9]. We focus on investigation of Bob's error performance as the basic characteristic of the ASK-type AQC system. In addition, the AQC system is characterized as an "ASK-type" system because Alice encodes information using different reflectivities, i.e., the differences in the amplitude of the reflected light corresponding to mode S.

3.1. Description of Received Quantum State

In this section, we describe the received quantum state corresponding to each entangled state. However, based on consideration of the prospect of the discussion, we analyze the quasi-Bell state using a Stinespring representation, and analyze the TSVS using a Kraus representation. Note that the light that corresponds to mode A is assumed to pass through an ideal channel because it is propagating inside Bob.

3.1.1. Quasi-Bell State with Stinespring Representation

When a Stinespring representation is used, the loss incurred by an attenuated channel can be expressed using the interaction with the vacuum field as an environment mode E. In other words, the unitary evolution of the composite system SE can be described by applying the unitary operator $\mathbb{U}_{\mathrm{SE}}^{(\eta)}$ to the SE, where the results represent the interaction between modes S and E:

$$\mathbb{U}_{\mathrm{SE}}^{(\eta)}|\alpha\rangle_{\mathrm{S}}|0\rangle_{\mathrm{E}} = |\sqrt{\eta}\alpha\rangle_{\mathrm{S}}|\sqrt{1-\eta}\alpha\rangle_{\mathrm{E}}, \tag{16}$$

$$\mathbb{U}_{\mathrm{SE}}^{(\eta)}|-\alpha\rangle_{\mathrm{S}}|0\rangle_{\mathrm{E}} = |-\sqrt{\eta}\alpha\rangle_{\mathrm{S}}|-\sqrt{1-\eta}\alpha\rangle_{\mathrm{E}}, \tag{17}$$

where η is the energy transmissivity. The reduced state of the composite system SAE on SA, i.e., the received quantum state, can be acquired by performing a partial trace over mode E, because only the composite system SA is actually measured by the detector.

For the case where $\mathrm{b} \in \{0,1\}$, we now consider the received quantum states $\Psi_{\mathrm{SA}}^{(\mathrm{b})}$ when the binary information that was recorded using the reflectivities R_{b} is denoted by "0" and "1". Suppose that the transmitted quantum state at the light source is the maximum quasi-Bell state. Then, the received quantum state $\Psi_{\mathrm{SA}}^{(\mathrm{b})}$ can be represented by

$$\Psi_{\mathrm{SA}}^{(\mathrm{b})} = \mathrm{Tr}_{\mathrm{E}}\left\{ \left(\mathbb{U}_{\mathrm{SE}}^{(R_{\mathrm{b}})} \otimes \mathbb{I}_{\mathrm{A}} \right) \left(|\Psi_2\rangle_{\mathrm{SA}} \langle \Psi_2| \otimes |0\rangle_{\mathrm{E}} \langle 0| \right) \left(\mathbb{U}_{\mathrm{SE}}^{(R_{\mathrm{b}})} \otimes \mathbb{I}_{\mathrm{A}} \right)^{\dagger} \right\}. \tag{18}$$

The same supposition can be applied to the non-maximum quasi-Bell state.

3.1.2. TSVS with Kraus Representation

In the TSVS case, a Kraus representation is used to express the attenuation channel. This Kraus representation allows us to describe the relationship between the transmitted and received quantum states, and can be expressed without use of an external system, unlike the Stinespring representation. If the transmitted and received quantum states are $\rho^{(\mathrm{in})}$ and $\rho^{(\mathrm{out})}$, respectively, then the Kraus representation of the attenuation channel is given as follows:

$$\rho^{(\mathrm{out})} = \sum_{k=0}^{\infty} \mathbb{E}_k^{(\eta)} \rho^{(\mathrm{in})} \mathbb{E}_k^{(\eta)\dagger}, \tag{19}$$

where

$$\mathbb{E}_k^{(\eta)} = \sum_n \sqrt{\binom{n}{k}} \sqrt{\eta^{n-k}(1-\eta)^k} |n-k\rangle\langle n| \tag{20}$$

is the Kraus operator [21] for the attenuation channel with respect to the energy transmissivity η.

For the case where $\mathrm{b} \in \{0,1\}$, we now consider the received quantum states $\psi_{\mathrm{SA}}^{(\mathrm{b})}$ when the binary information recorded using the reflectivities R_{b} is denoted by "0" and "1". The received quantum state $\psi_{\mathrm{SA}}^{(\mathrm{b})}$ can then be represented by

$$\psi_{\mathrm{SA}}^{(\mathrm{b})} = \sum_{k=0}^{\infty} \left\{ \left(\mathbb{E}_k^{(R_{\mathrm{b}})} \right)_{\mathrm{S}} \otimes \mathbb{I}_{\mathrm{A}} \right\} |\psi\rangle_{\mathrm{SA}} \langle \psi| \left\{ \left(\mathbb{E}_k^{(R_{\mathrm{b}})} \right)_{\mathrm{S}} \otimes \mathbb{I}_{\mathrm{A}} \right\}^{\dagger}. \tag{21}$$

3.2. Error Probability Determined by Optimum Quantum Measurement

The error probability is an important performance evaluation index for communication systems. In this paper, it is assumed that Bob has no information about the *a priori* probabilities $\xi_{\mathrm{b}} \in \{\xi_0, \xi_1\}$ that correspond to the binary information $\mathrm{b} \in \{0,1\}$. If the *a priori* probabilities of the quantum states are unknown, it is known that use of the Bayes decision criterion with equal *a priori* probabilities under the quantum minimax criterion is the optimum approach from quantum detection theory [22]. If we suppose that the received quantum states are $\rho_{\mathrm{SA}}^{(0)}$ and $\rho_{\mathrm{SA}}^{(1)}$, and that the corresponding *a priori* probabilities are equal, i.e., $\xi_0 = \xi_1 = 1/2$, then the error probability given by the optimum quantum measurement [23] is

$$P_{\mathrm{e}} = \frac{1}{2}\left(1 - \sum_{\lambda_i > 0} \lambda_i\right), \tag{22}$$

where $\{\lambda_i\}$ are the eigenvalues of $\rho_{\mathrm{SA}}^{(0)} - \rho_{\mathrm{SA}}^{(1)}$.

4. Derivation of Analytical Expression for the Error Probability of the Quasi-Bell State

In this section, we derive an analytical expression for the error probability of the AQC system when using the quasi-Bell state. As an example of the quasi-Bell state, we consider

the case where the maximum quasi-Bell state is used. To calculate the error probability of given by Equation (22), it is necessary to obtain eigenvalues for the difference between the two received quantum states $\Psi_{\mathrm{SA}}^{(0)} - \Psi_{\mathrm{SA}}^{(1)}$. The coherent state is represented using either an infinite dimensional vector or an infinite matrix (i.e., the density operator). The maximum quasi-Bell state used here is constructed from the coherent states, and its density operator is thus infinite. The eigenvalues of $\Psi_{\mathrm{SA}}^{(0)} - \Psi_{\mathrm{SA}}^{(1)}$ also take the form of an infinite matrix and are generally difficult to calculate. However, in this paper, we find that the received quantum states $\Psi_{\mathrm{SA}}^{(0)}$ and $\Psi_{\mathrm{SA}}^{(1)}$ can be represented by an 8×8 matrix when a special orthonormal basis is used. Additionally, by deriving the eigenvalues for the 8×8 matrix of $\Psi_{\mathrm{SA}}^{(0)} - \Psi_{\mathrm{SA}}^{(1)}$, we can also derive an analytical expression for the error probability of the AQC system using the quasi-Bell state.

There are four steps that must be considered in the derivation of this analytical expression. Each step is explained individually below.

4.1. Step 1: Representation of the Received Quantum States by an 8×8 *Matrix*

First, if we focus on mode A in the received quantum states $\Psi_{\mathrm{SA}}^{(0)}$ and $\Psi_{\mathrm{SA}}^{(1)}$, we can see that the mode is constructed using the two coherent states $\{|\pm\alpha\rangle_{\mathrm{A}}\}$. In the two-dimensional subspace of a Hilbert space that is spanned by $\{|\pm\alpha\rangle\}$, the orthonormal basis $\{|\omega_0\rangle, |\omega_1\rangle\}$ used in references [24,25] is the measurement state of the square-root measurement (SRM) [26], which is often applied to the representation of the numerical vector of the quasi-Bell state and to the representation of its density operator. It is known that this approach improves the prospects of the discussion (e.g., [27]). The SRM for $\{|\pm\alpha\rangle_{\mathrm{A}}\}$ is an optimum quantum measurement that minimizes the error probability, and use of these measurement states means that $\{|\pm\alpha\rangle_{\mathrm{A}}\}$ can be expressed as:

$$|\pm\alpha\rangle_{\mathrm{A}} = \frac{1}{\varepsilon_+ - \varepsilon_-}\left(\sqrt{\varepsilon_\pm}|\omega_0\rangle_{\mathrm{A}} - \sqrt{\varepsilon_\mp}|\omega_1\rangle_{\mathrm{A}}\right). \tag{23}$$

Therefore, $\{|\pm\alpha\rangle_{\mathrm{A}}\}$ can be represented by a two-dimensional vector, as follows:

$$|\pm\alpha\rangle_{\mathrm{A}} = \frac{1}{\varepsilon_+ - \varepsilon_-}\begin{bmatrix} \sqrt{\varepsilon_\pm} \\ -\sqrt{\varepsilon_\mp} \end{bmatrix}, \tag{24}$$

where $\kappa_{\mathrm{A}} = \kappa_{\mathrm{S}} =: \kappa$ and $\varepsilon_\pm$ is given as follows:

$$\varepsilon_\pm = \frac{1 \pm \sqrt{1-\kappa^2}}{2(1-\kappa^2)}. \tag{25}$$

Next, if we focus on mode A in the received quantum states $\Psi_{\mathrm{SA}}^{(0)}$ and $\Psi_{\mathrm{SA}}^{(1)}$, we can see that the mode is constructed using the following four coherent states: $\{|-\sqrt{R_1}\alpha\rangle_{\mathrm{S}}, |-\sqrt{R_0}\alpha\rangle_{\mathrm{S}}, |\sqrt{R_0}\alpha\rangle_{\mathrm{S}}, |\sqrt{R_1}\alpha\rangle_{\mathrm{S}}\} (=: \{|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle\})$. In the four-dimensional subspace of a Hilbert space that is spanned by these coherent states, we also consider the measurement state of the SRM to be an orthonormal basis. The representation of a four-dimensional vector of these coherent states in the four-dimensional subspace can be obtained immediately from the square root of their Gram matrix. In general, the Gram matrix for $\{|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle\}$ is constructed as follows [28]:

$$\begin{bmatrix} \langle\alpha_0|\alpha_0\rangle & \langle\alpha_0|\alpha_1\rangle & \langle\alpha_0|\alpha_2\rangle & \langle\alpha_0|\alpha_3\rangle \\ \langle\alpha_1|\alpha_0\rangle & \langle\alpha_1|\alpha_1\rangle & \langle\alpha_1|\alpha_2\rangle & \langle\alpha_1|\alpha_3\rangle \\ \langle\alpha_2|\alpha_0\rangle & \langle\alpha_2|\alpha_1\rangle & \langle\alpha_2|\alpha_2\rangle & \langle\alpha_2|\alpha_3\rangle \\ \langle\alpha_3|\alpha_0\rangle & \langle\alpha_3|\alpha_1\rangle & \langle\alpha_3|\alpha_2\rangle & \langle\alpha_3|\alpha_3\rangle \end{bmatrix} = \begin{bmatrix} 1 & b & c & d \\ b & 1 & a & c \\ c & a & 1 & b \\ d & c & b & 1 \end{bmatrix}, \tag{26}$$

where

$$a = \mathrm{e}^{-2R_0|\alpha|^2}, \quad b = \mathrm{e}^{\sqrt{R_0R_1}|\alpha|^2 - \frac{1}{2}|\alpha|^2(R_0+R_1)},$$

$$c = \mathrm{e}^{-\sqrt{R_0 R_1}|\alpha|^2 - \frac{1}{2}|\alpha|^2(R_0+R_1)}, \quad d = \mathrm{e}^{-2R_1|\alpha|^2}. \tag{27}$$

However, because the representation of the square root of the Gram matrix is complicated, the method described in references [29–31] is applied in this paper. In references [29–31], the order of these coherent states was rearranged to be $\{|-\sqrt{R_0}\alpha\rangle_S, |\sqrt{R_0}\alpha\rangle_S, |-\sqrt{R_1}\alpha\rangle_S, |\sqrt{R_1}\alpha\rangle_S (=: \{|\alpha'_0\rangle, |\alpha'_1\rangle, |\alpha'_2\rangle, |\alpha'_3\rangle)\}$ to take advantage of the partial symmetry of the coherent state signal, and the Gram matrix Γ then became as follows:

$$\Gamma = \begin{bmatrix} \langle\alpha'_0|\alpha'_0\rangle & \langle\alpha'_0|\alpha'_1\rangle & \langle\alpha'_0|\alpha'_2\rangle & \langle\alpha'_0|\alpha'_3\rangle \\ \langle\alpha'_1|\alpha'_0\rangle & \langle\alpha'_1|\alpha'_1\rangle & \langle\alpha'_1|\alpha'_2\rangle & \langle\alpha'_1|\alpha'_3\rangle \\ \langle\alpha'_2|\alpha'_0\rangle & \langle\alpha'_2|\alpha'_1\rangle & \langle\alpha'_2|\alpha'_2\rangle & \langle\alpha'_2|\alpha'_3\rangle \\ \langle\alpha'_3|\alpha'_0\rangle & \langle\alpha'_3|\alpha'_1\rangle & \langle\alpha'_3|\alpha'_2\rangle & \langle\alpha'_3|\alpha'_3\rangle \end{bmatrix} = \begin{bmatrix} 1 & a & b & c \\ a & 1 & c & b \\ b & c & 1 & d \\ c & b & d & 1 \end{bmatrix}. \tag{28}$$

Through observation of Γ, we found that it can be divided into four blocks using a 2×2 real symmetric matrix with the common structure of

$$M^{(2)}(u,v) = \begin{bmatrix} u & v \\ v & u \end{bmatrix}. \tag{29}$$

The eigenvalues and corresponding orthonormal eigenvectors of $M^{(2)}(u,v)$ are given by

$$x_1 = u + v, \quad x_2 = u - v \tag{30}$$

and

$$|x_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |x_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}, \tag{31}$$

respectively (Although $|x_1\rangle$ and $|x_2\rangle$ are not vectors in the Hilbert space of a quantum system, and in fact are numerical vectors, we use Dirac's notation for convenience). We then obtain the spectral decomposition form of $M^{(2)}(u,v)$, which is expressed as

$$M^{(2)}(u,v) = (u+v)|x_1\rangle\langle x_1| + (u-v)|x_2\rangle\langle x_2|. \tag{32}$$

Using $M^{(2)}(u,v)$, Γ can then be divided into blocks, as follows:

$$\Gamma = \begin{bmatrix} M^{(2)}(1,a) & M^{(2)}(b,c) \\ M^{(2)}(b,c) & M^{(2)}(1,d) \end{bmatrix}. \tag{33}$$

By substituting the spectral decomposition form into the equation above, we obtain

$$\Gamma = M^{(+)} \otimes |x_1\rangle\langle x_1| + M^{(-)} \otimes |x_2\rangle\langle x_2|, \tag{34}$$

where

$$M^{(+)} = \begin{bmatrix} 1+a & b+c \\ b+c & 1+d \end{bmatrix}, \quad M^{(-)} = \begin{bmatrix} 1-a & b-c \\ b-c & 1-d \end{bmatrix}. \tag{35}$$

Both $M^{(+)}$ and $M^{(-)}$ have the common structure of

$$M^{(\pm)} = \begin{bmatrix} p & q \\ q & r \end{bmatrix}, \tag{36}$$

and the eigenvalues $\lambda_\pm(p,q,r)$ and the corresponding orthonormal eigenvectors $|\lambda_\pm(p,q,r)\rangle$ of this structure can be expressed as:

$$\lambda_\pm(p,q,r) = \frac{1}{2}\left(p + r \pm \sqrt{(p-r)^2 + 4q^2}\right) \tag{37}$$

and

$$|\lambda_{\pm}(p,q,r)\rangle = \frac{|\lambda'_{\pm}(p,q,r)\rangle}{\sqrt{\langle\lambda'_{\pm}(p,q,r)|\lambda'_{\pm}(p,q,r)\rangle}}, \tag{38}$$

respectively, where

$$|\lambda'_{\pm}(p,q,r)\rangle = \begin{bmatrix} p-r\pm\sqrt{(p-r)^2+4q^2} \\ 2q \end{bmatrix}. \tag{39}$$

Based on the derivation above, the analytical expressions for the eigenvalues $\{\lambda_i\}$ and the corresponding orthonormal eigenvectors $\{\lambda_i\}$ of Γ can be expressed as

$$\lambda_1 = \lambda_+(1+a,b+c,1+d), \tag{40}$$
$$\lambda_2 = \lambda_-(1+a,b+c,1+d), \tag{41}$$
$$\lambda_3 = \lambda_+(1-a,b-c,1-d), \tag{42}$$
$$\lambda_4 = \lambda_-(1-a,b-c,1-d) \tag{43}$$

and

$$|\lambda_1\rangle = |\lambda_+(1+a,b+c,1+d)\rangle \otimes |x_1\rangle, \tag{44}$$
$$|\lambda_2\rangle = |\lambda_-(1+a,b+c,1+d)\rangle \otimes |x_1\rangle, \tag{45}$$
$$|\lambda_3\rangle = |\lambda_+(1-a,b-c,1-d)\rangle \otimes |x_2\rangle, \tag{46}$$
$$|\lambda_4\rangle = |\lambda_-(1-a,b-c,1-d)\rangle \otimes |x_2\rangle, \tag{47}$$

respectively. Therefore, the spectral decomposition form of Γ is given as follows:

$$\Gamma = \sum_{i=1}^{4} \lambda_i |\lambda_i\rangle\langle\lambda_i|. \tag{48}$$

Here, $\{|\lambda_i\rangle\}$ forms an orthonormal basis, which means that the square root of the Gram matrix, $\Gamma^{\frac{1}{2}}$, can be derived immediately as:

$$\Gamma^{\frac{1}{2}} = \sum_{i=1}^{4} \sqrt{\lambda_i}|\lambda_i\rangle\langle\lambda_i| = \begin{bmatrix} \gamma_{11}^{(+)} & \gamma_{11}^{(-)} & \gamma_{13}^{(+)} & \gamma_{13}^{(-)} \\ \gamma_{11}^{(-)} & \gamma_{11}^{(+)} & \gamma_{13}^{(-)} & \gamma_{13}^{(+)} \\ \gamma_{13}^{(+)} & \gamma_{13}^{(-)} & \gamma_{33}^{(+)} & \gamma_{33}^{(-)} \\ \gamma_{13}^{(-)} & \gamma_{13}^{(+)} & \gamma_{33}^{(-)} & \gamma_{33}^{(+)} \end{bmatrix}, \tag{49}$$

where each element of the 4×4 matrix $\Gamma^{\frac{1}{2}}$ can be obtained directly via substitution of Equations (40)–(47) into $\sum_{i=1}^{4}\sqrt{\lambda_i}|\lambda_i\rangle\langle\lambda_i|$. See Appendix A for details. The four-dimensional vector representation of $\{|-\sqrt{R_0}\alpha\rangle_S, |\sqrt{R_0}\alpha\rangle_S, |-\sqrt{R_1}\alpha\rangle_S, |\sqrt{R_1}\alpha\rangle_S\}$ is given as follows:

$$|-\sqrt{R_0}\alpha\rangle_S = \begin{bmatrix} \gamma_{11}^{(+)} \\ \gamma_{11}^{(-)} \\ \gamma_{13}^{(+)} \\ \gamma_{13}^{(-)} \end{bmatrix}, \quad |\sqrt{R_0}\alpha\rangle_S = \begin{bmatrix} \gamma_{11}^{(-)} \\ \gamma_{11}^{(+)} \\ \gamma_{13}^{(-)} \\ \gamma_{13}^{(+)} \end{bmatrix},$$
$$|-\sqrt{R_1}\alpha\rangle_S = \begin{bmatrix} \gamma_{13}^{(+)} \\ \gamma_{13}^{(-)} \\ \gamma_{33}^{(+)} \\ \gamma_{33}^{(-)} \end{bmatrix}, \quad |\sqrt{R_1}\alpha\rangle_S = \begin{bmatrix} \gamma_{13}^{(-)} \\ \gamma_{13}^{(+)} \\ \gamma_{33}^{(-)} \\ \gamma_{33}^{(+)} \end{bmatrix}. \tag{50}$$

Finally, by substituting Equations (24) and (50) into Equation (18), we obtain

$$\begin{aligned}\Psi_{\mathrm{SA}}^{(\mathrm{b})} &= \mathrm{Tr}_{\mathrm{E}}\left\{\left(\mathbb{U}_{\mathrm{SE}}^{(R_{\mathrm{b}})}\otimes\mathbb{I}_{\mathrm{A}}\right)\left(|\Psi_2\rangle_{\mathrm{SA}}\langle\Psi_2|\otimes|0\rangle_{\mathrm{E}}\langle 0|\right)\left(\mathbb{U}_{\mathrm{SE}}^{(R_{\mathrm{b}})}\otimes\mathbb{I}_{\mathrm{A}}\right)^{\dagger}\right\}\\ &= h_2^2\Big(|\sqrt{R_{\mathrm{b}}}\alpha\rangle_{\mathrm{S}}\langle\sqrt{R_{\mathrm{b}}}\alpha|\otimes|\alpha\rangle_{\mathrm{A}}\langle\alpha| - L_{\mathrm{b}}|\sqrt{R_{\mathrm{b}}}\alpha\rangle_{\mathrm{S}}\langle-\sqrt{R_{\mathrm{b}}}\alpha|\otimes|\alpha\rangle_{\mathrm{A}}\langle-\alpha|\\ &\quad -L_{\mathrm{b}}|-\sqrt{R_{\mathrm{b}}}\alpha\rangle_{\mathrm{S}}\langle\sqrt{R_{\mathrm{b}}}\alpha|\otimes|-\alpha\rangle_{\mathrm{A}}\langle\alpha| + |-\sqrt{R_{\mathrm{b}}}\alpha\rangle_{\mathrm{S}}\langle-\sqrt{R_{\mathrm{b}}}\alpha|\otimes|-\alpha\rangle_{\mathrm{A}}\langle-\alpha|\Big),\end{aligned} \tag{51}$$

where $L_{\mathrm{b}} = \mathrm{e}^{-2(1-R_{\mathrm{b}})|\alpha|^2}$, and by taking the difference between the two received quantum states, $\Psi_{\mathrm{SA}}^{(0)} - \Psi_{\mathrm{SA}}^{(1)} (=: U)$, we then obtain an 8×8 matrix that can be expressed as:

$$U = \Psi_{\mathrm{SA}}^{(0)} - \Psi_{\mathrm{SA}}^{(1)} = \begin{bmatrix} A & B & C & D & G & H & I & J \\ B & E & F & C & K & L & M & N \\ C & F & E & B & N & M & L & K \\ D & C & B & A & J & I & H & G \\ G & K & N & J & O & P & Q & R \\ H & L & M & I & P & S & T & Q \\ I & M & L & H & Q & T & S & P \\ J & N & K & G & R & Q & P & O \end{bmatrix}. \tag{52}$$

The 8×8 matrix U is a real symmetric matrix, and each element of this matrix can be obtained directly by substituting Equations (24) and (50) into Equation (52) and then taking the difference between $\Psi_{\mathrm{SA}}^{(0)}$ and $\Psi_{\mathrm{SA}}^{(1)}$. See Appendix B for details of this procedure.

4.2. Step 2: Similar Transformation of 8×8 Matrix

Next, we consider the derivation of the eigenvalues of the 8×8 real symmetric matrix U. In this paper, we derive the eigenvalues for the 8×8 real symmetry matrix U by using its symmetrical structure, although there is no general solution for the eigenvalues of a square matrix with an order of five or more because of the Abel–Ruffini theorem. To use the symmetrical structure of U, we must first convert U into a more tractable form.

When the eigenvalues of U and U' become equal when U is converted into $V^{-1}UV := U'$ using a regular matrix V; this is known as similarity transformation. Here, if such a similarity transformation of U is performed using the regular matrix

$$V = V^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \tag{53}$$

we then obtain the matrix U' after the similarity transformation as follows:

$$U' = V^{-1}UV = \begin{bmatrix} A & D & C & B & I & H & G & J \\ D & A & B & C & H & I & J & G \\ C & B & E & F & L & M & N & K \\ B & C & F & E & M & L & K & N \\ I & H & L & M & S & T & Q & P \\ H & I & M & L & T & S & P & Q \\ G & J & N & K & Q & P & O & R \\ J & G & K & N & P & Q & R & O \end{bmatrix}. \tag{54}$$

4.3. Step 3: Spectral Decomposition Form of the 8×8 *Matrix*

Through observation of U', we see that this matrix can be divided into 16 blocks using the 2×2 real symmetric matrix (29). We perform a spectral decomposition operation on U' in the same manner as Equation (34), and we then obtain

$$U' = U^{(+)} \otimes |x_1\rangle\langle x_1| + U^{(-)} \otimes |x_2\rangle\langle x_2|, \tag{55}$$

where

$$\begin{aligned} U^{(+)} &= \begin{bmatrix} A+D & C+B & I+H & G+J \\ C+B & E+F & L+M & N+K \\ I+H & L+M & S+T & Q+P \\ G+J & N+K & Q+P & O+R \end{bmatrix}, \\ U^{(-)} &= \begin{bmatrix} A-D & C-B & I-H & G-J \\ C-B & E-F & L-M & N-K \\ I-H & L-M & S-T & Q-P \\ G-J & N-K & Q-P & O-R \end{bmatrix} \end{aligned} \tag{56}$$

are also real symmetric matrices. Let the eigenvalues and eigenvectors of $U^{(+)}$ and $U^{(-)}$ be written as $\{\tau_i^{(+)}\}$, $\{\tau_i^{(-)}\}$ and $\{|\tau_i^{(+)}\rangle\}$, $\{|\tau_i^{(-)}\rangle\}$, respectively; then, we obtain:

$$U^{(+)} = \sum_{i=1}^{4} \tau_i^{(+)} |\tau_i^{(+)}\rangle\langle\tau_i^{(+)}|, \quad U^{(-)} = \sum_{i=1}^{4} \tau_i^{(-)} |\tau_i^{(-)}\rangle\langle\tau_i^{(-)}|, \tag{57}$$

because any real symmetric matrix can be spectrally decomposed. Substitution of these expressions into U' allows the spectral decomposition form of U' to be expressed as

$$U' = \sum_{i=1}^{4} \tau_i^{(+)} |\tau_i^{(+)}\rangle\langle\tau_i^{(+)}| \otimes |x_1\rangle\langle x_1| + \sum_{i=1}^{4} \tau_i^{(-)} |\tau_i^{(-)}\rangle\langle\tau_i^{(-)}| \otimes |x_2\rangle\langle x_2|, \tag{58}$$

where the eigenvalues of U' are given as follows:

$$\tau_i^{(+)}, \quad \tau_i^{(-)}, \quad i = \{1, 2, 3, 4\}. \tag{59}$$

4.4. Step 4: Eigenvalues of 4×4 *Matrix*

To determine the eigenvalues given by Equation (59), we must find the eigenvalues $\{\tau_i^{(+)}\}$ and $\{\tau_i^{(-)}\}$ of the 4×4 real symmetric matrices $U^{(+)}$ and $U^{(-)}$. All these eigenvalues must be real numbers because $U^{(+)}$ and $U^{(-)}$ are real symmetric matrices. The eigenvalues for $U^{(+)}$ and $U^{(-)}$ can be derived as follows.

The eigenvalues $\{\tau_i^{(+)}\}$ for the 4×4 real symmetric matrix $U^{(+)}$ are the solutions to the eigenvalue equation $\det(U^{(+)} - \tau_i^{(+)}\mathrm{I}) = 0$, where I is the identity matrix. We have

$$\det(U^{(+)} - \tau_i^{(+)}\mathrm{I}) = \tau_i^{(+)^2}\left(\tau_i^{(+)^2} + \mathcal{A}\tau_i^{(+)} + \mathcal{B}\right) = 0, \tag{60}$$

where $U_{ij}^{(+)}$ is element (i, j) of $U^{(+)}$, and

$$\begin{aligned}\mathcal{A} &= -U_{11}^{(+)} - U_{22}^{(+)} - U_{33}^{(+)} - U_{44}^{(+)} \\ &= -\frac{(L_0+1)(a\kappa-1)+(1+L_1)(1-d\kappa)}{2(\kappa^2-1)}, \end{aligned} \tag{61}$$

$$\begin{aligned}\mathcal{B} &= -U_{12}^{(+)^2} - U_{13}^{(+)^2} - U_{14}^{(+)^2} + U_{11}^{(+)}U_{22}^{(+)} - U_{23}^{(+)^2} - U_{24}^{(+)^2} + U_{11}^{(+)}U_{33}^{(+)} \\ &\quad + U_{22}^{(+)}U_{33}^{(+)} - U_{34}^{(+)^2} + U_{11}^{(+)}U_{44}^{(+)} + U_{22}^{(+)}U_{44}^{(+)} + U_{33}^{(+)}U_{44}^{(+)} \\ &= -\frac{(L_0+1)(L_1+1)\{(a\kappa-1)(d\kappa-1)-(b-c\kappa)^2\}}{4(\kappa^2-1)^2}. \end{aligned} \tag{62}$$

We confirm directly that two of the eigenvalues $\{\tau_i^{(+)}\}$ are 0, and let $\tau_3^{(+)} = \tau_4^{(+)} = 0$. To determine the signs of the other eigenvalues $\tau_1^{(+)}$ and $\tau_2^{(+)}$ for $\tau_i^{(+)^2} + \mathcal{A}\tau_i^{(+)} + \mathcal{B} = 0$, we prove that $\tau_1^{(+)}\tau_2^{(+)} = \mathcal{B} < 0$ (see Appendix C for this proof), and we then know that these two eigenvalues have opposite signs: $\tau_1^{(+)} = \frac{-\mathcal{A}+\sqrt{\mathcal{A}^2-4\mathcal{B}}}{2} > 0$, and $\tau_2^{(+)} = \frac{-\mathcal{A}-\sqrt{\mathcal{A}^2-4\mathcal{B}}}{2} < 0$. Note that the corresponding eigenvalues $\{\tau_i^{(-)}\}$ for $U^{(-)}$ can be obtained in the same manner.

4.5. Derivation of Analytical Expression

The eigenvalues $\{\tau_i^{(+)}\} \cup \{\tau_i^{(-)}\}$ of U' (i.e., U) that were obtained from the analysis above can be substituted into Equation (22). Here, it can be confirmed that $\tau_1^{(+)}, \tau_1^{(-)} > 0$, and thus the error probability $P_{\mathrm{e}}^{(\mathrm{Max})}$ of the AQC system when using the maximum quasi-Bell state is finally given as follows:

$$P_{\mathrm{e}}^{(\mathrm{Max})} = \frac{1}{2}\left\{1 - \frac{1}{2}\left(\sqrt{\Lambda_{\mathrm{M}}^{(+)^2} - 4\Xi_{\mathrm{M}}^{(+)}} - \Lambda_{\mathrm{M}}^{(+)}\right) - \frac{1}{2}\left(\sqrt{\Lambda_{\mathrm{M}}^{(-)^2} - 4\Xi_{\mathrm{M}}^{(-)}} - \Lambda_{\mathrm{M}}^{(-)}\right)\right\}, \tag{63}$$

$$\Lambda_{\mathrm{M}}^{(\pm)} = -\frac{(L_0 \pm 1)(a\kappa \mp 1) + (1 \pm L_1)(1 \mp d\kappa)}{2(\kappa^2-1)}, \tag{64}$$

$$\Xi_{\mathrm{M}}^{(\pm)} = -\frac{(L_0 \pm 1)(L_1 \pm 1)\{(a\kappa \mp 1)(d\kappa \mp 1) - (b \mp c\kappa)^2\}}{4(\kappa^2-1)^2}. \tag{65}$$

The error probability $P_{\mathrm{e}}^{(\mathrm{NonMax})}$ for the AQC system when using the non-maximum quasi-Bell state can also be obtained using steps 1 to 4 as per the case for the maximum quasi-Bell state. As a result, the corresponding probability is given by:

$$P_{\mathrm{e}}^{(\mathrm{NonMax})} = \frac{1}{2}\left\{1 - \frac{1}{2}\left(\sqrt{\Lambda_{\mathrm{N}}^{(+)^2} - 4\Xi_{\mathrm{N}}^{(+)}} - \Lambda_{\mathrm{N}}^{(+)}\right) - \frac{1}{2}\left(\sqrt{\Lambda_{\mathrm{N}}^{(-)^2} - 4\Xi_{\mathrm{N}}^{(-)}} - \Lambda_{\mathrm{N}}^{(-)}\right)\right\}, \tag{66}$$

$$\Lambda_{\mathrm{N}}^{(\pm)} = -\frac{(L_0 \mp 1)(a\kappa \mp 1) - (1 \mp L_1)(1 \mp d\kappa)}{2(\kappa^2+1)}, \tag{67}$$

$$\Xi_{\mathrm{N}}^{(\pm)} = -\frac{(L_0 \mp 1)(L_1 \mp 1)\{(a\kappa \mp 1)(d\kappa \mp 1) - (b \mp c\kappa)^2\}}{4(\kappa^2+1)^2}, \tag{68}$$

where

$$\begin{aligned} &a = \mathrm{e}^{-2R_0|\alpha|^2}, \quad b = \mathrm{e}^{\sqrt{R_0R_1}|\alpha|^2 - \frac{1}{2}|\alpha|^2(R_0+R_1)}, \quad c = \mathrm{e}^{-\sqrt{R_0R_1}|\alpha|^2 - \frac{1}{2}|\alpha|^2(R_0+R_1)}, \\ &d = \mathrm{e}^{-2R_1|\alpha|^2}, \quad \kappa = \mathrm{e}^{-2|\alpha|^2}, \quad L_0 = \mathrm{e}^{-2(1-R_0)|\alpha|^2}, \quad L_1 = \mathrm{e}^{-2(1-R_1)|\alpha|^2}. \end{aligned} \tag{69}$$

5. Error Performance

In this section, we present the results that were obtained numerically when using the error probability (15) for the ACC system and the analytical expression for the error probabilities (63) and (66) for the AQC system when using the quasi-Bell states. When

using the TSVS, the calculation of the error probability $P_{\mathrm{e}}^{(\mathrm{TSVS})}$ in the case in which the average number of photons is small ($\langle n \rangle_{\mathrm{TSVS}} \leq 5$) is performed based on the conventional numerical calculation method, i.e., using an equation that approximates Equation (13) to a finite value of n. In other words, as described in references [32,33], the calculation should be performed after suitable truncation of the Hilbert space by taking both the average number of photons and the order of the error probability into consideration. However, in the case where the average number of photons is large (i.e., $\langle n \rangle_{\mathrm{TSVS}} > 5$), it is difficult to treat the eigenvalue problem in Equation (22) numerically because the dimensions of the received quantum state (i.e., its density operator) are large. Therefore, the AQC system's performance is evaluated using the upper bound $P_{\mathrm{UB}}^{(\mathrm{TSVS})}$ and the lower bound $P_{\mathrm{LB}}^{(\mathrm{TSVS})}$ on the error probability $P_{\mathrm{e}}^{(\mathrm{TSVS})}$ given in reference [9] when the TSVS is used, as follows:

$$P_{\mathrm{LB}}^{(\mathrm{TSVS})} = \frac{1}{2}\left[1 - \sqrt{1 - \left\{\left(1 - \sqrt{R_0 R_1} - \sqrt{(1-R_0)(1-R_1)}\right) N_{\mathrm{S}} + 1\right\}^{-2}}\right], \tag{70}$$

$$P_{\mathrm{UB}}^{(\mathrm{TSVS})} = \begin{cases} \frac{1}{2}\left\{\left(1 - \sqrt{R_0}\right) N_{\mathrm{S}} + 1\right\}^{-2} & (R_1 = 1) \\ \frac{1}{2}\left(\Sigma \sigma^z - \Theta \theta^z\right)^{-1} & (R_1 \neq 1) \end{cases}, \tag{71}$$

where

$$\sigma = \frac{(1-R_0)N_{\mathrm{S}} + 1}{(1-R_1)N_{\mathrm{S}} + 1}, \tag{72}$$

$$\theta = \frac{1-R_0}{1-R_1}, \tag{73}$$

$$\Sigma = \frac{\left\{\left(1 - \sqrt{R_0 R_1}\right) N_{\mathrm{S}} + 1\right\}^2}{(1-R_0)N_{\mathrm{S}} + 1}, \tag{74}$$

$$\Theta = (1-R_1)N_{\mathrm{S}}, \tag{75}$$

$$z = \begin{cases} 0 & \left((\Sigma - \Theta)^{-2}(\ln \theta^{\Theta} - \ln \sigma^{\Sigma}) \geq 0\right) \\ 1 & \left((\Sigma - \Theta)^{-2}(\ln \theta^{\Theta} - \ln \sigma^{\Sigma}) < 0\right) \end{cases}. \tag{76}$$

This paper also provides a comparison with the universal lower bound $P_{\mathrm{U-LB}}$ on error probability given in reference [9] when the use of any multimode pure input state is permitted, as follows:

$$P_{\mathrm{U-LB}} = \frac{1}{2}\left\{1 - \sqrt{1 - \left(\sqrt{R_0 R_1} + \sqrt{(1-R_0)(1-R_1)}\right)^{2N_{\mathrm{S}}'}}\right\}, \tag{77}$$

where $\langle n \rangle_{\mathrm{U-LB}} = N_{\mathrm{S}}'$ is the average number of photons in mode S.

5.1. Performance Comparison of Use of Maximum and Non-Maximum Quasi-Bell States

Figure 2 plots the error probabilities for the AQC system versus the reflectivities R_0 and R_1 ($R_0 < R_1$), which are changed from 0 to 1 when the transmitted average number of photons in the maximum and non-maximum quasi-Bell states is fixed at $\langle n \rangle_{\mathrm{Max}} = \langle n \rangle_{\mathrm{NonMax}} = 1$. The error probability when the maximum quasi-Bell state is used is represented by the green curved surface, and the error probability when the non-maximum quasi-Bell state is used is represented by the orange curved surface.

Figure 2 shows that the error probability $P_{\mathrm{e}}^{(\mathrm{Max})}$ when the maximum quasi-Bell state is used tends to decrease when $R_1 - R_0$ increases. In particular, the figure shows reasonable results that confirm that the maximum error probability is achieved when $R_0 \approx R_1$, and that the minimum error probability is achieved when $R_0 = 0$ and $R_1 = 1$. Comparison of the error probabilities of the AQC system when using the maximum and non-maximum

quasi-Bell states shows that the maximum quasi-Bell state is superior in most cases, but there is no significant difference between the two cases. Furthermore, use of the maximum quasi-Bell state does not always provide superior results, because the AQC system using the non-maximum quasi-Bell state is superior to the corresponding system using the maximum quasi-Bell state in the extreme case in which $R_1 - R_0$ is very small and $R_0 \approx 1$ or $R_0 \approx 0$. The details can be seen in Figure 3 regarding the contour plot of the ratio, $P_e^{(\mathrm{NonMax})}/P_e^{(\mathrm{Max})}$, of the error probability when using the non-maximum state to that when using the maximum quasi-Bell state. Figure 3 shows that the ratio is between 1 and 1.1 in most cases, but the ratio may be less than 1 in the extreme case.

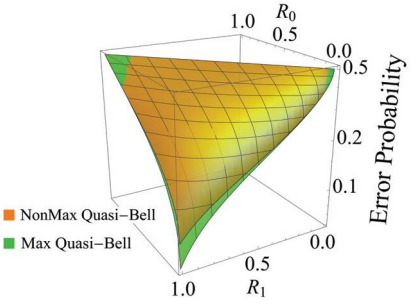


Figure 2. Error probability characteristics with respect to the reflectivities $\{R_0, R_1\}$ when using the maximum quasi-Bell state (green curved surface) and the non-maximum quasi-Bell state (orange curved surface). The average number of photons is fixed at 1.

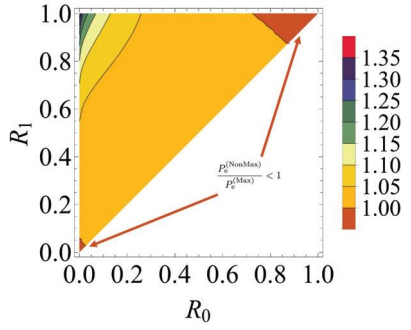


Figure 3. Contour plot of the ratio of the error probability when using the non-maximum quasi-Bell state ($P_e^{(\mathrm{NonMax})}$) to that when using the maximum quasi-Bell state ($P_e^{(\mathrm{Max})}$). The average number of photons is fixed at 1.

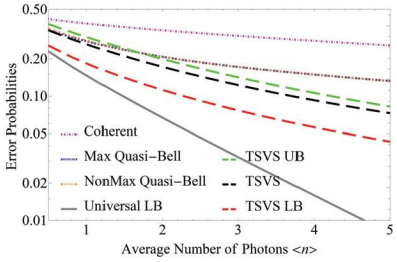
Actually, there are several studies comparing the performance between the maximum and non-maximum quasi-Bell states, such as quantum teleportation [15], quantum superdense coding [34], quantum reading [33], and quantum illumination [18,19]. Reference [15] showed that the non-maximum quasi-Bell state offers an advantage over the maximum quasi-Bell state at small coherent amplitudes, and may offer more resistance to attenuation than the maximum quasi-Bell state. References [18,19,33,34] showed that the non-maximum quasi-Bell state offers more resistance to attenuation and phase noise than the maximum quasi-Bell state, in some special cases, and the result of this paper is one more piece of evidence in terms of that. That evidence also reveals a fact that the maximum quasi-Bell state offers better performance than the non-maximum quasi-Bell state in ideal cases, such as cases with large coherent amplitudes or environments without noise, but the opposite may be true in some unideal cases. Therefore, for some applications using the quasi-Bell state at small coherent amplitudes or environments with noise, the non-maximum quasi-Bell state which offers more resistance to noise may play an important role. We must be careful not to

dismiss the value of using the non-maximum quasi-Bell state, although the reason in terms of its superiority has not yet been elucidated. We consider the issue to be an interesting topic that has value as a future subject.

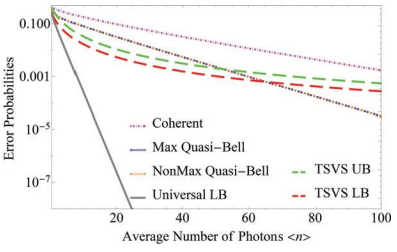
5.2. Performance Comparison Using Each Quantum State

Figure 4a,c,e,g shows the error probabilities obtained when the average number of photons $\langle n \rangle (:= \langle n \rangle_{\mathrm{U-LB}} = \langle n \rangle_{\mathrm{TSVS}} = \langle n \rangle_{\mathrm{Max}} = \langle n \rangle_{\mathrm{NonMax}} = \langle n \rangle_{\mathrm{Coh}})$, which is regarded as the signal energy, is varied from 0.5 to 5 for the AQC system when using the TSVS, the maximum quasi-Bell state, and the non-maximum quasi-Bell state, and the ACC system using the coherent state, for which the reflectivities $\{R_0, R_1\}$ were fixed at $\{0.5, 1\}$, $\{0.3, 0.6\}$, $\{0.2, 0.8\}$, and $\{0, 0.3\}$, respectively. The pink chain line represents the error probability $P_{\mathrm{e}}^{(\mathrm{Hom})}$ for the ACC system, and the blue and orange dotted lines represent the error probabilities $P_{\mathrm{e}}^{(\mathrm{Max})}$ and $P_{\mathrm{e}}^{(\mathrm{NonMax})}$ for the AQC system when using the maximum and non-maximum quasi-Bell states, respectively. The black dashed line represents the error probability $P_{\mathrm{e}}^{(\mathrm{TSVS})}$ for the AQC system when using the TSVS, and the green and red dashed lines represent the upper bound $P_{\mathrm{UB}}^{(\mathrm{TSVS})}$ and the lower bound $P_{\mathrm{LB}}^{(\mathrm{TSVS})}$, respectively, for $P_{\mathrm{e}}^{(\mathrm{TSVS})}$. The gray solid line represents the universal lower bound on the error probability, $P_{\mathrm{U-LB}}$. The horizontal axis represents the average number of photons, and the vertical axis represents the error probability in each case. The minimum average number of photons that can be considered is 0.5 because the minimum average number of photons in the maximum quasi-Bell state is $\langle n \rangle_{\mathrm{Max}} = 0.5$, and cases smaller than that are not defined. If the average number of photons is greater than 5, it then becomes difficult to calculate the error probability $P_{\mathrm{e}}^{(\mathrm{TSVS})}$; therefore, only the upper bound $P_{\mathrm{UB}}^{(\mathrm{TSVS})}$ and the lower bound $P_{\mathrm{LB}}^{(\mathrm{TSVS})}$ are used for the evaluation of this probability. Figure 4b,d,f,h shows the error performances corresponding to those shown in Figure 4a,c,e,g, respectively, when the average number of photons $\langle n \rangle$ is increased from 0.5 to 100.

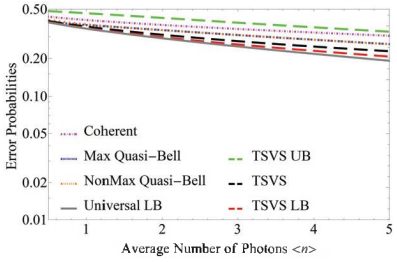
These figures confirm that the AQC system using the quasi-Bell state always maintains a clear performance advantage over the ACC system, despite increases in the average number of photons $\langle n \rangle$. Although the error probability of the AQC system when using the quasi-Bell state is similar to that of the ACC system, in that it decreases exponentially in tandem with the increase in $\langle n \rangle$, the AQC system can achieve the same error probability when using only half of the average number of photons used by the ACC system. Conversely, Figure 4b,d,f,h shows the error probability for the AQC system using the TSVS approaches that of the ACC system with increasing $\langle n \rangle$. In particular, as shown in Figure 4f, the ACC system provides superior performance to the AQC system using the TSVS when $\langle n \rangle > 35$. Figure 4g,h shows that the performance of the ACC system exceeds that of the AQC system using the TSVS when the average number of photons is smaller, i.e., when $\langle n \rangle \approx 5$. This is contrary to the results presented in reference [9], which indicated that the performance obtained when using the m-shot EPR state exceeds that of the coherent state as the average number of photons increases, and this performance is considered to be a characteristic unique to the one-shot pulse case. Consideration of these figures together with Figure 4b,d shows that the ACC system exceeds the performance of the AQC system using the TSVS with smaller average number of photons when R_0 is small or when $R_1 - R_0$ is large. Otherwise, the latter system can maintain its performance superiority over the former within the range of the small average number of photons. In addition, as shown in Figure 4f, the AQC system using the quasi-Bell state demonstrates superior performance to the same system using the TSVS when $\langle n \rangle > 10$. Figure 4g,h shows that the AQC system using the quasi-Bell state has an error probability that is the same as or lower than that of the system using the TSVS. Consideration of these figures together with Figure 4b,d shows that the performance of the AQC system using the quasi-Bell state exceeds that of the system using the TSVS with smaller average number of photons when R_0 is small or when $R_1 - R_0$ is large. Otherwise, the former system requires a larger average number of photons to surpass the performance of the latter.



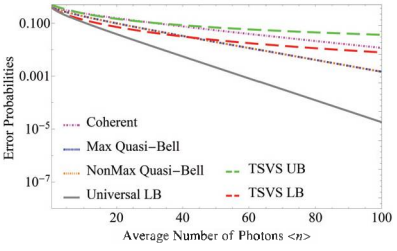
(**a**) $R_0 = 0.5$, $R_1 = 1$, $\langle n \rangle \leq 5$.



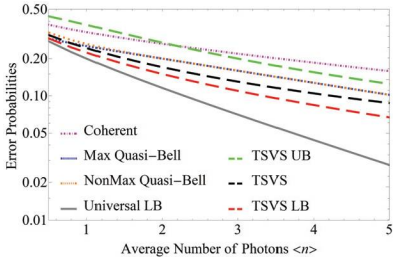
(**b**) $R_0 = 0.5$, $R_1 = 1$, $\langle n \rangle \leq 100$.



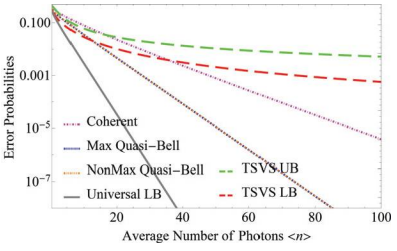
(**c**) $R_0 = 0.3$, $R_1 = 0.6$, $\langle n \rangle \leq 5$.



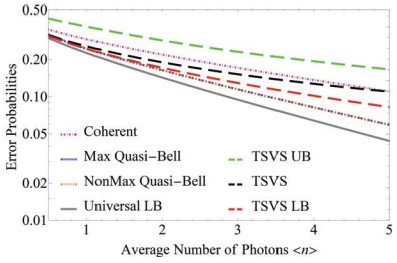
(**d**) $R_0 = 0.3$, $R_1 = 0.6$, $\langle n \rangle \leq 100$.



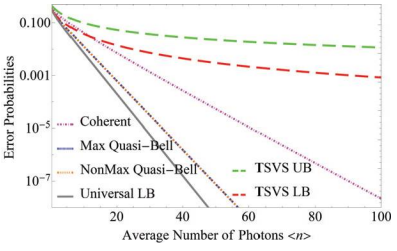
(**e**) $R_0 = 0.2$, $R_1 = 0.8$, $\langle n \rangle \leq 5$.



(**f**) $R_0 = 0.2$, $R_1 = 0.8$, $\langle n \rangle \leq 100$.



(**g**) $R_0 = 0$, $R_1 = 0.3$, $\langle n \rangle \leq 5$.



(**h**) $R_0 = 0$, $R_1 = 0.3$, $\langle n \rangle \leq 100$.

Figure 4. Error probabilities with respect to the average number of photons $\langle n \rangle$ when using the coherent state (denoted by Coherent), the maximum quasi-Bell state (denoted by Max Quasi-Bell), the non-maximum quasi-Bell state (denoted by NonMax Quasi-Bell), and the two-mode squeezed vacuum state (denoted by TSVS) with reflectivities $\{R_0, R_1\} = \{0.5, 1\}, \{0.3, 0.6\}, \{0.2, 0.8\}, \{0, 0.3\}$. $\langle n \rangle$ ranges up to either 5 or 100. Universal LB, TSVS UB, and TSVS LB present the universal lower bound on the error probability, the upper bound on the error probability for the TSVS case, and the lower bound on the error probability for the TSVS case, respectively.

5.3. Performance Comparison with Universal Lower Bound

Finally, we consider a performance comparison with the universal lower bound on the error probability. For example, when the average number of photons is small, the AQC system using the TSVS almost reaches the universal lower bound, as illustrated in Figure 4c. However, as Figure 4d shows, the gap between the lower bound on the error probability for the TSVS and the universal lower bound increases when the average number of photons increases. This differs from the results reported in reference [9], which stated that when the m-shot EPR state is used, the universal lower bound is almost always reached, and this is considered to be a characteristic unique to the one-shot pulse case. The characteristics of Figure 4b,f,h become more outstanding and the gap between the lower bound on the error probability for the TSVS and the universal lower bound increases rapidly as the average number of photons increases. In addition, Figure 4b shows that gap between the error probability for the AQC system using the quasi-Bell state and the universal lower bound may also increase rapidly in the same manner as the TSVS. However, Figure 4f shows that the error probability of the AQC system using the quasi-Bell state differs from that of the system using the TSVS in that the gap with respect to the universal lower bound only increases slowly as the average number of photons increases. Furthermore, as shown in Figure 4h, the error probability for the AQC system using the quasi-Bell state almost reaches the universal lower bound even when the average number of photons increases in the case where both R_0 and R_1 are small.

To see these details of this characteristics in greater detail, Figure 5 shows the error performance when $\{R_0, R_1\} = \{0, 0.08\}, \{0, 0.03\}$ in addition to that when $\{R_0, R_1\} = \{0, 0.3\}$. As shown in Figure 5, R_0 is fixed at 0, and as R_1 decreases, the error probability for the AQC system using the quasi-Bell state becomes closer to the universal lower bound. To clearly demonstrate the trend of the gap between the error probability when using the quasi-Bell state and the universal lower bound, Figure 6 shows the ratio $P_{\mathrm{U-LB}}/P_{\mathrm{e}}^{(\mathrm{Max})}$ with respect to R_1 when fixing R_0 at 0. (Note the special case where the maximum quasi-Bell state becomes a Bell state when $\langle n \rangle_{\mathrm{Max}} = 0.5$ [13].) As is evident in Figure 6, the ratio approaches 1 as R_1 decreases in spite of increasing $\langle n \rangle$. This performance characteristic makes it possible to use the quasi-Bell state to almost reach the universal lower bound in the AQC system, even if severe attenuation—where energy attenuation in the channel can be considered to be included in R_1—occurs in an ultra-long distance channel. (If energy attenuation associated with energy transmissivity η occurs in the channel, then just substitute ηR_{b} into R_{b} in the results. For an example, Figure 4c expresses the error performance when $R_0 = 0.3$, $R_1 = 0.6$, and $\eta = 1$; and when $R_0 = 0.5$, $R_1 = 0.75$, and $\eta = 0.8$.)

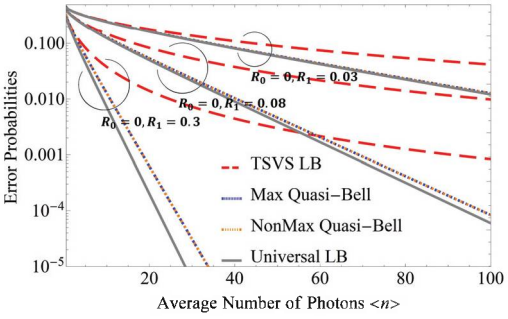


Figure 5. Error probabilities with respect to the average number of photons $\langle n \rangle$ when using the maximum quasi-Bell state (denoted by Max Quasi-Bell), the non-maximum quasi-Bell state (denoted by NonMax Quasi-Bell), and the two-mode squeezed vacuum state (denoted by TSVS) with reflectivities of $\{R_0, R_1\} = \{0, 0.3\}, \{0, 0.08\}, \{0, 0.03\}$. $\langle n \rangle$ ranges up to 100. Universal LB and TSVS LB represent the universal lower bound on the error probability and the lower bound on the error probability for TSVS, respectively.

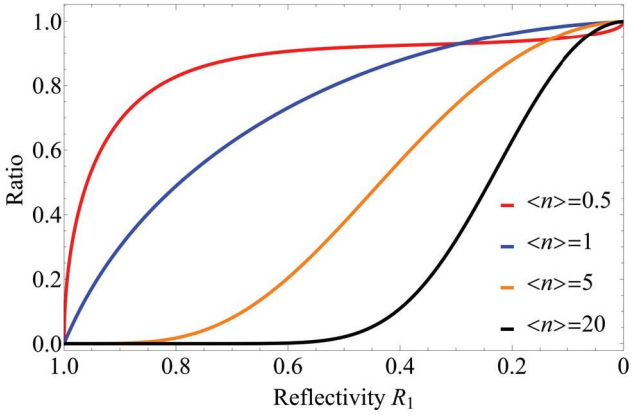


Figure 6. Ratio of the universal lower bound on the error probability to the error probability when using the maximum quasi-Bell state with respect to reflectivity R_1, where R_0 is fixed at 0.

6. Conclusions

In this paper, we have proposed an ASK-type AQC system as a step toward development of a new asymmetric communication system. In this AQC system, Bob, who has a high transmission capability, transmits one of the entangled light beams, which acts as a communication medium, to Alice, who has a low transmission capability; Alice operates on the light beam to encode the information that she wants to send to Bob, and then sends the light beam back to Bob. Bob then decodes the information received from Alice by performing an optimum quantum measurement (i.e., a joint measurement) of the other entangled light beam and the light beam that returned from Alice.

As a first step toward evaluation of the system performance, we focused on the communication performance from Alice to Bob, and investigated the basic performance characteristics based on the error probability criterion. First, using the quasi-Bell state as the light source, we derived an analytical expression for the error probability by using an 8×8 matrix representation to express the density operators of the two received quantum states affected by the reflectivities $\{R_0, R_1\}$, which corresponded to the binary information that Alice wants to send. Then, using this analytical expression, we compared the superior performances of the AQC systems using the TSVS, the maximum quasi-Bell state, and the non-maximum quasi-Bell state with that of the asymmetric classical communication (ACC) system in terms of their error probabilities. As a result, it was clarified that the error probabilities of the AQC systems using the maximum and non-maximum quasi-Bell states differed only slightly. In addition, the error probability of the AQC system using the quasi-Bell state is always lower than that of the ACC system, regardless of the reflectivity setting, and the AQC system using the quasi-Bell state also shows a clear performance advantage over the system using the TSVS when a sufficiently large average number of photons is used. In fact, as described in Section 2, when the average number of photons is large, the amount of entanglement of the TSVS is overwhelmingly greater than that of the quasi-Bell state, but the results in this paper show that the performance of the AQC system using the quasi-Bell state is overwhelmingly better than that of the same system using the TSVS. Therefore, the performance of the AQC system should be determined by selecting a type of entangled state that is suitable for the system, rather than by considering the amount of entanglement. The conclusion above is strengthened by the fact that the performance of the ACC system surpassed that of the AQC system using the TSVS when the average number of photons was sufficiently large. What causes quasi-Bell state to work better than the TSVS? Unfortunately, as far as we know, there are no studies in terms of the comparison between the quasi-Bell state and the TSVS, except for references [18,19], although the reason for the superiority of the quasi-Bell state and some related potential properties of that have not been elucidated. These studies also reveal the fact that there

are some entanglement-based systems or protocols that require a suitable entangled state rather than a large amount of entanglement to improve its performance. Additionally, we believe the advantage of the quasi-Bell state over the TSVS comes from the robustness of coherent states against attenuation. However, a perfect explanation is not yet available. We consider the issue to be a very challenging topic that has value as a future subject. Getting back to the main topic, when R_0 is small or when $R_1 - R_0$ is large, the AQC system using the quasi-Bell states shows a clear advantage when only a small average number of photons is used. In particular, when $R_0 = 0$, the AQC system using the quasi-Bell state has the same or a lower error probability than the corresponding system using the TSVS. However, when $R_1 = 1$, a large average number of photons is required to enable the AQC system using the quasi-Bell state to exceed the performance of the system using the TSVS. Finally, we compared the error probability for the AQC system using the quasi-Bell state, the lower bound on the error probability for the AQC system using the TSVS, and the universal lower bound on the error probability, and found that performance closer to the universal lower bound was achieved using the quasi-Bell state when compared with the system with TSVS in the case when R_0 and R_1 are very small. As a result, it is expected that the AQC system using the quasi-Bell state will be applicable even in ultra-long distance channels, in which severe attenuation can occur.

In this paper, we evaluated the performance based on the error probability results for the AQC system and clarified the basic performance characteristics. In fact, if an eavesdropper Eve was present between Alice and Bob, one of the simplest attack methods for Eve would be to intercept the light corresponding to mode S, which is reflected from Alice. However, Eve cannot access the light corresponding to mode A, which remains inside Bob, and thus there would be a difference in reception performance between Eve and Bob. This reception performance difference creates the security of the AQC system. In addition, the AQC system discussed in this paper is expected to have various security applications, e.g., quantum cryptographic conferencing [35]. Future work will include security evaluation of this system, including the case of information leakage when an eavesdropper is present, and security enhancement for this system by performing some quantum communication protocols.

Author Contributions: Conceptualization, T.W. and T.S.U.; software, T.W.; validation, T.W. and T.S.U.; formal analysis, T.W.; investigation, T.W.; data curation, T.W.; writing—original draft preparation, T.W.; writing—review and editing, T.W. and T.S.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by JSPS KAKENHI, grant numbers JP20K20397, JP20H00581, and JP21K04064.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research was funded by the Marubun Research Promotion Foundation and The Nitto Foundation. The authors would like to thank S. Takahira for valuable discussions during this and previous research. We thank David MacDonald from Edanz (https://jp.edanz.com/ac, accessed 12 May 2022) for editing a draft of this manuscript.

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

Abbreviations

The following abbreviations are used in this manuscript:

AQC	Asymmetric quantum communication
ACC	Asymmetric classical communication
IoT	Internet of Things
EPR state	Einstein–Podolsky–Rosen state
TSVS	Two-mode squeezed vacuum state
ASK	Amplitude shift keying
Max Quasi-Bell	Maximum quasi-Bell state
NonMax Quasi-Bell	Non-maximum quasi-Bell state
Coherent	Coherent state
LB	Lower bound
UB	Upper bound
U-LB or Universal LB	Universal lower bound

Appendix A

The elements $\{\gamma_{11}^{(\pm)}, \gamma_{13}^{(\pm)}, \gamma_{33}^{(\pm)}\}$ of Γ_2^1 are given as follows:

$$\gamma_{11}^{(\pm)} = \sum_{i=0}^{1} \frac{\sqrt{(-1)^i e_+ + a + d + 2}\{(-1)^i e_+ + a - d\}^2}{2\sqrt{2}\left[\{(-1)^i e_+ + a - d\}^2 + 4(b+c)^2\right]} \pm \sum_{j=0}^{1} \frac{\sqrt{(-1)^j e_- - a - d + 2}\{(-1)^j e_- - a + d\}^2}{2\sqrt{2}\left[\{(-1)^j e_- - a + d\}^2 + 4(b-c)^2\right]}, \tag{A1}$$

$$\gamma_{13}^{(\pm)} = \sum_{i=0}^{1} \frac{(b+c)\sqrt{(-1)^i e_+ + a + d + 2}\{(-1)^i e_+ + a - d\}}{\sqrt{2}\left[\{(-1)^i e_+ + a - d\}^2 + 4(b+c)^2\right]} \pm \sum_{j=0}^{1} \frac{(b-c)\sqrt{(-1)^j e_- - a - d + 2}\{(-1)^j e_- - a + d\}}{\sqrt{2}\left[\{(-1)^j e_- - a + d\}^2 + 4(b-c)^2\right]}, \tag{A2}$$

$$\gamma_{33}^{(\pm)} = \sum_{i=0}^{1} \frac{\sqrt{2}(b+c)^2\sqrt{(-1)^i e_+ + a + d + 2}}{\{(-1)^i e_+ + a - d\}^2 + 4(b+c)^2} \pm \sum_{j=0}^{1} \frac{\sqrt{2}(b-c)^2\sqrt{(-1)^j e_- - a - d + 2}}{\{(-1)^j e_- - a + d\}^2 + 4(b-c)^2}, \tag{A3}$$

$$e_\pm = \sqrt{(\pm a \mp d)^2 + 4(b \pm c)^2}. \tag{A4}$$

Appendix B

The elements $\{A, \ldots, T\}$ of U are given as follows:

$$A = \sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\left(\gamma_{13}^{(-)}\gamma_{13}^{(+)}L_1 - \gamma_{11}^{(-)}\gamma_{11}^{(+)}L_0\right) + \frac{1}{2}\varepsilon_+(\gamma_{11}^{(-)} - \gamma_{13}^{(-)})(\gamma_{11}^{(-)} + \gamma_{13}^{(-)}) + \frac{1}{2}\varepsilon_-(\gamma_{11}^{(+)} - \gamma_{13}^{(+)})(\gamma_{11}^{(+)} + \gamma_{13}^{(+)}), \tag{A5}$$

$$B = \frac{1}{2}\left\{\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\left(-\gamma_{11}^{(-)^2} - \gamma_{11}^{(+)^2} + \gamma_{13}^{(-)^2} + \gamma_{13}^{(+)^2}\right) + (\varepsilon_- + \varepsilon_+)\left(\gamma_{11}^{(-)}\gamma_{11}^{(+)}L_0 - \gamma_{13}^{(-)}\gamma_{13}^{(+)}L_1\right)\right\}, \tag{A6}$$

$$C = \frac{1}{2}\left[\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\left\{L_1\left(\gamma_{13}^{(-)^2} + \gamma_{13}^{(+)^2}\right) - L_0\left(\gamma_{11}^{(-)^2} + \gamma_{11}^{(+)^2}\right)\right\} + (\varepsilon_- + \varepsilon_+)(\gamma_{11}^{(-)}\gamma_{11}^{(+)} - \gamma_{13}^{(-)}\gamma_{13}^{(+)})\right], \tag{A7}$$

$$D = \frac{1}{2}L_0\left(\gamma_{11}^{(-)^2}\varepsilon_+ + \gamma_{11}^{(+)^2}\varepsilon_-\right) + \sqrt{\varepsilon_-}\sqrt{\varepsilon_+}(\gamma_{13}^{(-)}\gamma_{13}^{(+)} - \gamma_{11}^{(-)}\gamma_{11}^{(+)})$$

$$-\frac{1}{2}L_1\left(\gamma_{13}^{(-)^2}\varepsilon_+ + \gamma_{13}^{(+)^2}\varepsilon_-\right), \tag{A8}$$

$$E = \sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\left(\gamma_{13}^{(-)}\gamma_{13}^{(+)}L_1 - \gamma_{11}^{(-)}\gamma_{11}^{(+)}L_0\right) + \frac{1}{2}\varepsilon_-(\gamma_{11}^{(-)} - \gamma_{13}^{(-)})(\gamma_{11}^{(-)} + \gamma_{13}^{(-)}) + \frac{1}{2}\varepsilon_+(\gamma_{11}^{(+)} - \gamma_{13}^{(+)})(\gamma_{11}^{(+)} + \gamma_{13}^{(+)}), \tag{A9}$$

$$F = \frac{1}{2}L_0\left(\gamma_{11}^{(-)^2}\varepsilon_- + \gamma_{11}^{(+)^2}\varepsilon_+\right) + \sqrt{\varepsilon_-}\sqrt{\varepsilon_+}(\gamma_{13}^{(-)}\gamma_{13}^{(+)} - \gamma_{11}^{(-)}\gamma_{11}^{(+)}) - \frac{1}{2}L_1\left(\gamma_{13}^{(-)^2}\varepsilon_- + \gamma_{13}^{(+)^2}\varepsilon_+\right), \tag{A10}$$

$$G = \frac{1}{2}\Big[\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\Big\{L_1(\gamma_{13}^{(-)}\gamma_{33}^{(+)} + \gamma_{13}^{(+)}\gamma_{33}^{(-)}) - L_0(\gamma_{11}^{(-)}\gamma_{13}^{(+)} + \gamma_{11}^{(+)}\gamma_{13}^{(-)})\Big\} + \gamma_{13}^{(-)}\varepsilon_+(\gamma_{11}^{(-)} - \gamma_{33}^{(-)}) + \gamma_{13}^{(+)}\varepsilon_-(\gamma_{11}^{(+)} - \gamma_{33}^{(+)})\Big], \tag{A11}$$

$$H = \frac{1}{2}\Big\{\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}(-\gamma_{11}^{(-)}\gamma_{13}^{(-)} - \gamma_{11}^{(+)}\gamma_{13}^{(+)} + \gamma_{13}^{(-)}\gamma_{33}^{(-)} + \gamma_{13}^{(+)}\gamma_{33}^{(+)}) + L_0(\gamma_{11}^{(-)}\gamma_{13}^{(+)}\varepsilon_+ + \gamma_{11}^{(+)}\gamma_{13}^{(-)}\varepsilon_-) - L_1(\gamma_{13}^{(-)}\gamma_{33}^{(+)}\varepsilon_+ + \gamma_{13}^{(+)}\gamma_{33}^{(-)}\varepsilon_-)\Big\}, \tag{A12}$$

$$I = \frac{1}{2}\Big[\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\Big\{L_1(\gamma_{13}^{(-)}\gamma_{33}^{(-)} + \gamma_{13}^{(+)}\gamma_{33}^{(+)}) - L_0(\gamma_{11}^{(-)}\gamma_{13}^{(-)} + \gamma_{11}^{(+)}\gamma_{13}^{(+)})\Big\} + \gamma_{11}^{(-)}\gamma_{13}^{(+)}\varepsilon_+ + \gamma_{11}^{(+)}\gamma_{13}^{(-)}\varepsilon_- - \gamma_{13}^{(-)}\gamma_{33}^{(+)}\varepsilon_+ - \gamma_{13}^{(+)}\gamma_{33}^{(-)}\varepsilon_-\Big], \tag{A13}$$

$$J = \frac{1}{2}\Big\{\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}(-\gamma_{11}^{(-)}\gamma_{13}^{(+)} - \gamma_{11}^{(+)}\gamma_{13}^{(-)} + \gamma_{13}^{(-)}\gamma_{33}^{(+)} + \gamma_{13}^{(+)}\gamma_{33}^{(-)}) + L_0(\gamma_{11}^{(-)}\gamma_{13}^{(-)}\varepsilon_+ + \gamma_{11}^{(+)}\gamma_{13}^{(+)}\varepsilon_-) - L_1(\gamma_{13}^{(-)}\gamma_{33}^{(-)}\varepsilon_+ + \gamma_{13}^{(+)}\gamma_{33}^{(+)}\varepsilon_-)\Big\}, \tag{A14}$$

$$K = \frac{1}{2}\Big\{\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}(-\gamma_{11}^{(-)}\gamma_{13}^{(-)} - \gamma_{11}^{(+)}\gamma_{13}^{(+)} + \gamma_{13}^{(-)}\gamma_{33}^{(-)} + \gamma_{13}^{(+)}\gamma_{33}^{(+)}) + L_0(\gamma_{11}^{(-)}\gamma_{13}^{(+)}\varepsilon_- + \gamma_{11}^{(+)}\gamma_{13}^{(-)}\varepsilon_+) - L_1(\gamma_{13}^{(-)}\gamma_{33}^{(+)}\varepsilon_- + \gamma_{13}^{(+)}\gamma_{33}^{(-)}\varepsilon_+)\Big\}, \tag{A15}$$

$$L = \frac{1}{2}\Big[\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\Big\{L_1(\gamma_{13}^{(-)}\gamma_{33}^{(+)} + \gamma_{13}^{(+)}\gamma_{33}^{(-)}) - L_0(\gamma_{11}^{(-)}\gamma_{13}^{(+)} + \gamma_{11}^{(+)}\gamma_{13}^{(-)})\Big\} + \gamma_{13}^{(-)}\varepsilon_-(\gamma_{11}^{(-)} - \gamma_{33}^{(-)}) + \gamma_{13}^{(+)}\varepsilon_+(\gamma_{11}^{(+)} - \gamma_{33}^{(+)})\Big], \tag{A16}$$

$$M = \frac{1}{2}\Big\{\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}(-\gamma_{11}^{(-)}\gamma_{13}^{(+)} - \gamma_{11}^{(+)}\gamma_{13}^{(-)} + \gamma_{13}^{(-)}\gamma_{33}^{(+)} + \gamma_{13}^{(+)}\gamma_{33}^{(-)}) + L_0(\gamma_{11}^{(-)}\gamma_{13}^{(-)}\varepsilon_- + \gamma_{11}^{(+)}\gamma_{13}^{(+)}\varepsilon_+) - L_1(\gamma_{13}^{(-)}\gamma_{33}^{(-)}\varepsilon_- + \gamma_{13}^{(+)}\gamma_{33}^{(+)}\varepsilon_+)\Big\}, \tag{A17}$$

$$N = \frac{1}{2}\Big[\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\Big\{L_1(\gamma_{13}^{(-)}\gamma_{33}^{(-)} + \gamma_{13}^{(+)}\gamma_{33}^{(+)}) - L_0(\gamma_{11}^{(-)}\gamma_{13}^{(-)} + \gamma_{11}^{(+)}\gamma_{13}^{(+)})\Big\} + \gamma_{11}^{(-)}\gamma_{13}^{(+)}\varepsilon_- + \gamma_{11}^{(+)}\gamma_{13}^{(-)}\varepsilon_+ - \gamma_{13}^{(-)}\gamma_{33}^{(+)}\varepsilon_- - \gamma_{13}^{(+)}\gamma_{33}^{(-)}\varepsilon_+\Big], \tag{A18}$$

$$O = \sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\left(\gamma_{33}^{(-)}\gamma_{33}^{(+)}L_1 - \gamma_{13}^{(-)}\gamma_{13}^{(+)}L_0\right) + \frac{1}{2}\varepsilon_+(\gamma_{13}^{(-)} - \gamma_{33}^{(-)})(\gamma_{13}^{(-)} + \gamma_{33}^{(-)}) + \frac{1}{2}\varepsilon_-(\gamma_{13}^{(+)} - \gamma_{33}^{(+)})(\gamma_{13}^{(+)} + \gamma_{33}^{(+)}), \tag{A19}$$

$$P = \frac{1}{2}\Big\{\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\left(-\gamma_{13}^{(-)^2} - \gamma_{13}^{(+)^2} + \gamma_{33}^{(-)^2} + \gamma_{33}^{(+)^2}\right) + (\varepsilon_- + \varepsilon_+)\left(\gamma_{13}^{(-)}\gamma_{13}^{(+)}L_0 - \gamma_{33}^{(-)}\gamma_{33}^{(+)}L_1\right)\Big\}, \tag{A20}$$

$$Q = \frac{1}{2}\left[\sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\left\{L_1\left(\gamma_{33}^{(-)^2} + \gamma_{33}^{(+)^2}\right) - L_0\left(\gamma_{13}^{(-)^2} + \gamma_{13}^{(+)^2}\right)\right\} + (\varepsilon_- + \varepsilon_+)(\gamma_{13}^{(-)}\gamma_{13}^{(+)} - \gamma_{33}^{(-)}\gamma_{33}^{(+)})\right], \tag{A21}$$

$$R = \frac{1}{2}L_0\left(\gamma_{13}^{(-)^2}\varepsilon_+ + \gamma_{13}^{(+)^2}\varepsilon_-\right) + \sqrt{\varepsilon_-}\sqrt{\varepsilon_+}(\gamma_{33}^{(-)}\gamma_{33}^{(+)} - \gamma_{13}^{(-)}\gamma_{13}^{(+)})$$

$$-\frac{1}{2}L_1\left(\gamma_{33}^{(-)^2}\varepsilon_+ + \gamma_{33}^{(+)^2}\varepsilon_-\right), \tag{A22}$$

$$S = \sqrt{\varepsilon_-}\sqrt{\varepsilon_+}\left(\gamma_{33}^{(-)}\gamma_{33}^{(+)}L_1 - \gamma_{13}^{(-)}\gamma_{13}^{(+)}L_0\right) + \frac{1}{2}\varepsilon_-(\gamma_{13}^{(-)} - \gamma_{33}^{(-)})(\gamma_{13}^{(-)} + \gamma_{33}^{(-)}) + \frac{1}{2}\varepsilon_+(\gamma_{13}^{(+)} - \gamma_{33}^{(+)})(\gamma_{13}^{(+)} + \gamma_{33}^{(+)}), \tag{A23}$$

$$T = \frac{1}{2}L_0\left(\gamma_{13}^{(-)^2}\varepsilon_- + \gamma_{13}^{(+)^2}\varepsilon_+\right) + \sqrt{\varepsilon_-}\sqrt{\varepsilon_+}(\gamma_{33}^{(-)}\gamma_{33}^{(+)} - \gamma_{13}^{(-)}\gamma_{13}^{(+)}) - \frac{1}{2}L_1\left(\gamma_{33}^{(-)^2}\varepsilon_- + \gamma_{33}^{(+)^2}\varepsilon_+\right). \tag{A24}$$

Appendix C

The proof that $\mathcal{B} < 0$ is presented as follows:

Proof. To prove that $\mathcal{B} = -\frac{(L_0+1)(L_1+1)\{(a\kappa-1)(d\kappa-1)-(b-c\kappa)^2\}}{4(\kappa^2-1)^2} < 0$, it is necessary to prove that

$$(a\kappa - 1)(d\kappa - 1) - (b - c\kappa)^2 > 0, \tag{A25}$$

because $-\frac{(L_0+1)(L_1+1)}{4(\kappa^2-1)^2} < 0$. This inequality can be rewritten as follows using a hyperbolic function:

$$-2e^{-|\alpha|^2(2+R_0+R_1)}W > 0, \tag{A26}$$

where

$$W = \cosh\left\{|\alpha|^2(R_0-R_1)\right\} - \cosh\left\{|\alpha|^2(2+R_0+R_1)\right\} - 1 + \cosh\left\{2|\alpha|^2(1+\sqrt{R_0R_1})\right\}. \tag{A27}$$

We then rewrite W using a sum-to-product formula and we then obtain

$$W = 2\sinh\left\{|\alpha|^2(1+R_0)\right\}\sinh\left\{-|\alpha|^2(1+R_1)\right\} + 2\sinh^2\left\{|\alpha|^2(1+\sqrt{R_0R_1})\right\}. \tag{A28}$$

The first term on the right-hand side (RHS) is negative, and the second term on the RHS is positive because $0 \leq R_0 < R_1 \leq 1$. Furthermore, the absolute value of the first term is greater than that of the second term because $(1+R_0)(1+R_1) > (1+\sqrt{R_0R_1})^2$, and sinh is odd and increases monotonically. Therefore, $W < 0$, and thus $\mathcal{B} < 0$. □

References

1. Einstein, A.; Podolsky, B.; Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **1935**, *47*, 777–780. [CrossRef]
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *14*, 661–663. [CrossRef] [PubMed]
3. Bennett, C.H.; Wiesner, S.J. Communication via 1- and 2-particle operators on Einstein–Podolsky-Rosen states. *Phys. Rev. Lett.* **1992**, *69*, 2881–2884. [CrossRef] [PubMed]
4. Bennett, C.H.; Brassard, G.; Crépeau, C.; Jozsa, R.; Peres, A.; Wootters, W.K. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky-Rosen channels. *Phys. Rev. Lett.* **1993**, *70*, 1895–1899. [CrossRef]
5. Lloyd, S. Enhanced sensitivity of photodetection via quantum illumination. *Phys. Rev. Lett.* **2008**, *321*, 1463–1465. [CrossRef]
6. Pirandola, S. Quantum reading of a classical digital memory. *Phys. Rev. Lett.* **2011**, *106*, 090504. [CrossRef]
7. Acharya, S.; Alonso, R.; Franklin, M.; Zdonik, S. Broadcast disks: data management for asymmetric communication environments. *ACM SIGMOD Record* **1995**, *24*, 199–210. [CrossRef]
8. Adler, M.; Maggs, B.M. Protocols for asymmetric communication channels. In Proceedings of the 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), Palo Alto, CA, USA, 8–11 November 1998.
9. Nair, R. Discriminating quantum-optical beam-splitter channels with number-diagonal signal states: Applications to quantum reading and target detection. *Phys. Rev. A* **2011**, *84*, 032312. [CrossRef]
10. Schumaker, B.L.; Caves, C.M. New formalism for two-photon quantum optics. II. Mathematical foundation and compact notation. *Phys. Rev. A* **1985**, *31*, 3093–3111. [CrossRef]
11. Audenaert, K.M.R.; Calsamiglia, J.; Munoz-Tapia, R.; Bagan, E.; Masanes, L.; Acin, A.; Verstraete, F. The quantum Chernoff bound. *Phys. Rev. Lett.* **2007**, *98*, 160501. [CrossRef]

12. Hirota, O.; Sasaki, M. Entangled state based on nonorthogonal state. In Quantum Communication, Computing, and Measurement 3. In Proceedings of the Fifth International Conference on Quantum Communication, Measurement and Computing (QCM&C-Y2K), Capri, Italy, 3–7 July 2000; Hirota, T., Ed.; Springer: New York, NY, USA, 2001.
13. van Enk, S.J.; Hirota, O. Entangled coherent states: Teleportation and decoherence. *Phys. Rev. A* **2001**, *64*, 022313. [CrossRef]
14. Hirota, O. Error free quantum reading by quasi Bell state of entangled coherent states. *Quantum Meas. Quantum Metrol.* **2017**, *4*, 70–73. [CrossRef]
15. Prakash, H.; Mishra, M.K. Teleportation of superposed coherent states using nonmaximally entangled resources. *J. Opt. Soc. Am. B* **2012**, *29*, 2915–2923. [CrossRef]
16. Yamauchi, J.; Ishikawa, K.; Takahashi, Y.; Wang, T.; Usuda, T.S. On dependence of entangled states for quantum illumination with attenuation. In Proceedings of the 2019 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, Nagoya, Japan, 9–10 September 2019; No. F5-5. (In Japanese)
17. Yamauchi, J.; Takahashi, Y.; Wang, T.; Usuda, T.S. Quantum illumination using quasi-Bell states. In Proceedings of the 2020 International Symposium on Information Theory and Its Applications (ISITA2020), Kapolei, HI, USA, 24–27 October 2020; No. A06-03; pp. 116–120.
18. Wang, T.; Usuda, T.S. Exact solution of error probability for quantum illumination with attenuation using quasi-Bell state. In Proceedings of the 20th Asian Quantum Information Science Conference (AQIS2020), Sydney, Australia, 7–9 December 2020; No. 095; pp. 135–136.
19. Wang, T.; Takahira, S.; Usuda, T.S. Error probabilities of quantum illumination with attenuation using maximum and non-maximum quasi-Bell states. *IEEJ Trans. Electron. Inf. Syst.* **2022**, *142*, 151–161. (In Japanese) [CrossRef]
20. Tan, S.H.; Erkmen, B.I.; Giovannetti, V.; Guha, S.; Lloyd, S.; Maccone, L.; Pirandola, S.; Shapiro, J.H. Quantum illumination with Gaussian states. *Phys. Rev. Lett.* **2008**, *101*, 253601. [CrossRef]
21. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2000.
22. Hirota, O.; Ikehara, S. Minimax strategy in the quantum detection theory and its application to optical communication. *IEICE Trans.* **1982**, *E65*, 627–633.
23. Helstrom, C.W. *Quantum Detection and Estimation Theory*; Academic Press: New York, NY, USA, 1976.
24. Osaki, M.; Ban, M.; Hirota, O. Derivation and physical interpretation of the optimum detection operators for coherent-state signals. *Phys. Rev. A* **1996**, *54*, 1691–1701. [CrossRef]
25. Sasaki, M.; Hirota, O. Two examples of measurement processes illustrating Helstrom's optimum decision bound. *Phys. Lett. A* **1996**, *210*, 21–25. [CrossRef]
26. Hausladen, P.; Jozsa, R.; Schumacher, B.; Westmoreland, M.; Wootters, W.K. Classical information capacity of a quantum channel. *Phys. Rev. A* **1996**, *54*, 1869–1876. [CrossRef]
27. Takeuchi, H.; Yamaguchi, S.; Usuda, T.S. Entanglement-assisted classical communication using quasi Bell states. In Proceedings of the 1st International Workshop on Entangled Coherent State and Its Application to Quantum Information Science—Towards Macroscopic Quantum Communications, Tokyo, Japan, 26–28 November 2012; No. 16; pp. 115–119.
28. Kato, K. Quantum detection of quaternary amplitude-shift keying coherent state signal. *Tamagawa Univ. Quantum ICT Res. Inst. Bull.* **2016**, *6*, 9–24.
29. Miyazaki, R.; Yoshida, M.; Usuda, T.S. Simplification of calculation of channel matrix for 2m-ary ASK coherent-state signals. In Proceedings of the 2019 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, Nagoya, Japan, 9–10 September 2019; No. F5-4. (In Japanese)
30. Miyazaki, R.; Yoshida, M.; Wang, T.; Usuda, T.S. Simplification of the calculation of the channel matrix for AMPM coherent-state signals. In Proceedings of the 2020 International Symposium on Information Theory and Its Applications (ISITA2020), Kapolei, HI, USA, 24–27 October 2020; No. A06-04; pp. 121–125.
31. Miyazaki, R.; Yoshida, M.; Wang, T.; Takahira, S.; Usuda, T.S. Simplification of calculation of channel matrix for non-symmetric signals. *IEICE Trans. Commun.* **2022**, *J105-B*, 74–87. (In Japanese)
32. Olivares, S.; Cialdi, S.; Castelli, F.; Paris, M.G.A. Homodyne detection as a near-optimum receiver for phase-shift-keyed binary communication in the presence of phase diffusion. *Phys. Rev. A* **2013**, *87*, 050303. [CrossRef]
33. Ishikawa, K.; Wang, T.; Usuda, T.S. Comparison of performances on quantum reading in non-symmetric loss using maximum and non-maximum quasi-Bell states. *IEEJ Trans. Electron. Inf. Syst.* **2020**, *140*, 1328–1335. (In Japanese) [CrossRef]
34. Yamaguchi, S.; Takeuchi, H.; Usuda, T.S. Property of a capacity of quantum channel assisted by a non-maximum quasi-Bell state. In Proceedings of the 2012 Tokai-Section Joint Conferrence on Electircal and Related Engineering, Toyohashi, Japan, 24–25 September 2012; No. O1-5. (In Japanese)
35. Fu, Y.; Yin, H.-L.; Chen, T.-Y.; Chen, Z.-B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **2015**, *114*, 090501. [CrossRef] [PubMed]

entropy

MDPI

Article

Non-Orthogonality Measure for a Collection of Pure Quantum States

Kentaro Kato

Quantum ICT Research Institute, Tamagawa University, 6-1-1 Tamagawagakuen, Machida 194-8610, Tokyo, Japan; kkatop@lab.tamagawa.ac.jp

Abstract: Modern optical communication technology can realize a large-scale multilevel (or M-ary) optical signal. Investigating the quantum mechanical nature of such a large-scale M-ary optical signal is essential for a unified understanding of quantum information science and optical communication technology. This article focuses on the quantum-mechanical non-orthogonality for a collection of pure quantum states and proposes a non-orthogonality index based on the least squares error criterion in quantum detection theory. First, we define the index for linearly independent signals, and the proposed index is analyzed through numerical simulations. Next, the index is applied to a highly large-scale M-ary phase-shift keying (PSK) coherent state signal. Furthermore, the index is compared with the capacity of the pure state channel with the PSK signal. As a result, it is shown that a highly large-scale M-ary PSK coherent state signal exhibits a quantum nature even when the signal transmission power is very high. Thus, the theoretical characterization of a highly large-scale M-ary coherent state signal based on the proposed index will be the first step toward a better understanding of cutting-edge optical communication technologies such as the quantum stream cipher Y00.

Keywords: quantum communications; quantum cryptography; quantum states; non-orthogonality; least squares error; M-ary optical signal

Citation: Kato, K. Non-Orthogonality Measure for a Collection of Pure Quantum States. *Entropy* **2022**, *24*, 581. https://doi.org/10.3390/e24050581

Academic Editor: Giuseppe Vallone

Received: 3 March 2022
Accepted: 15 April 2022
Published: 21 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

In 1967–1968, Helstrom achieved a breakthrough in optical communication theory by providing a new framework with a complete quantum mechanical description of optical signals and receivers [1–3]. In addition, he successfully demonstrated the quantum limit of detection error for binary optical signals based on the Bayes and Neyman–Pearson criteria developed in the classical detection theory (e.g., [4,5]). After Helstrom's work, Yuen et al. investigated the conditions for the optimal quantum detection of general quantum states based on a linear programming method [6,7]. Furthermore, Holevo investigated the existence problem for optimal quantum detection and demonstrated the necessary and sufficient conditions for the optimal quantum detection of general quantum states [8]. These pioneering scientists opened up the field of quantum detection theory. Quantum detection theory has since been extensively developed and is a key theory for unifying quantum information science and optical communication technology.

In quantum detection theory, optical signals are mathematically expressed as quantum states of light. For pure states, error-free quantum detection is only allowed when the states are orthogonal to each other. This is a significant result of quantum detection theory. A similar result is observed from the no-cloning theorem [9–11]. The no-cloning theorem claims that perfect cloning is possible within a collection of quantum states if and only if the quantum states are orthogonal.

Recent development in experimental studies on the quantum stream cipher Y00 demonstrates that highly large-scale multilevel (or M-ary [12–14]) optical signals can be realized using advanced technologies in optical communications [15,16]. Therefore, the theoretical characterization of a large-scale collection of coherent states is essential for a unified understanding of quantum information science and optical communication technology.

Coherent states are non-orthogonal, and a collection of coherent states forms a linearly independent set. Hence, the case of linearly independent pure states is of particular interest. A collection of pure states can be almost orthogonal, moderately non-orthogonal, or almost identical states. Therefore, a quantitative measure of the degree of non-orthogonality of each collection is needed for a detailed analysis. In the case of binary pure states, the degree of non-orthogonality is usually measured through the modulus of the inner product between the two states. However, no method to quantify the degree of non-orthogonality of a collection of more than three quantum states has been developed. Therefore, this study aims to develop a quantitative measure for the non-orthogonality of a collection of many states.

For this aim, we propose an index to evaluate the non-orthogonality of a collection of linearly independent pure states based on the least squares error (LSE) criterion in quantum detection theory. We summarize the LSE criterion in Section 2 and define a non-orthogonality index in Section 3. The proposed index is analyzed through numerical simulations with randomly generated vectors in Section 4. Then, the index is applied to the M-ary phase-shift keying (PSK) coherent state signal in Section 5. Further, the capacity of a pure state channel with the PSK signal is analyzed to understand the operational meaning of the index in the same section. Finally, we give conclusions in Section 6.

2. LSE Criterion in Quantum Detection Theory

Let $S = \{|\psi_m\rangle : 1 \le m \le M\}$ be a collection of M linearly independent pure quantum states, where each state is normalized, $\||\psi_m\rangle\| = 1$. Then, the squared error $E(S, \beta)$ for S by adapting an orthonormal basis $\beta = \{|v_m\rangle : 1 \le m \le M\}$ in vector space $\mathcal{V}$ spanned by S as a measurement basis is defined as follows.

$$E(S, \beta) = \frac{1}{M} \sum_{m=1}^{M} \langle e_m | e_m \rangle, \tag{1}$$

where $|e_m\rangle = |\psi_m\rangle - |v_m\rangle$. This expression can be arranged into the following form:

$$E(S, \beta) = \frac{1}{M} \sum_{m=1}^{M} \||e_m\rangle\|^2 = \frac{1}{M} \sum_{m=1}^{M} \||\psi_m\rangle - |v_m\rangle\|^2. \tag{2}$$

Then, the least squares error (LSE) is defined as

$$E^\circ(S) = \min_{\beta} E(S, \beta) = E(S, \beta^\circ). \tag{3}$$

A constructive manner can find the optimal basis β° from past studies as follows.

Theorem 1 ([17,18]). *For $S = \{|\psi_m\rangle : 1 \le m \le M\}$ of linearly independent pure quantum states, the optimal basis $\beta^\circ = \{|v_m^\circ\rangle : 1 \le m \le M\}$ for the LSE is given by*

$$|v_m^\circ\rangle = \hat{G}^{-1/2} |\psi_m\rangle, \qquad \text{with} \quad \hat{G} = \sum_{m=1}^{M} |\psi_m\rangle\langle\psi_m|. \tag{4}$$

This basis β° is known as the square-root measurement [19–22]. Then, the LSE can be written as

$$E^\circ(S) = E(S, \beta^\circ) = \frac{1}{M} \sum_{m=1}^{M} \left(1 - \sqrt{\lambda_m}\right)^2, \tag{5}$$

where λ_m is the eigenvalue of the Gram matrix

$$\mathbf{G} = \begin{bmatrix} \langle\psi_1|\psi_1\rangle & \langle\psi_1|\psi_2\rangle & \cdots & \langle\psi_1|\psi_M\rangle \\ \langle\psi_2|\psi_1\rangle & \langle\psi_2|\psi_2\rangle & \cdots & \langle\psi_2|\psi_M\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle\psi_M|\psi_1\rangle & \langle\psi_M|\psi_2\rangle & \cdots & \langle\psi_M|\psi_M\rangle \end{bmatrix}. \tag{6}$$

3. Non-Orthogonality Measure Based on LSE

3.1. Maximum and Minimum of LSE

Suppose that S consists of orthonormal vectors. Hence, $\mathbf{G}$ of S is the identity matrix of size M. Moreover, the optimal basis β° is identical to S. Therefore, $E^\circ(S) = 0$. From definition (1), $E(S, \beta) \geq 0$. Thus, the minimum value of $E^\circ(S)$ is zero.

$E^\circ(S)$ is the solution to the minimization problem of $E(S, \beta)$ with respect to β for given S. However, the maximum of $E^\circ(S)$ for S has not been discussed. As mentioned above, the minimum value is attained when S consists of orthogonal vectors. Hence, we suppose that the other extreme case, where S consists of almost identical vectors, will provide the maximum value. Therefore, we assume that each vector in S is close to the barycenter $|\text{barycenter}\rangle$ for β°. That is,

$$|\psi_m\rangle \sim |\text{barycenter}\rangle = \frac{1}{\sqrt{M}} \sum_{\ell=1}^{M} |v_\ell^\circ\rangle,$$

and, hence, $|e_m\rangle \sim |\text{barycenter}\rangle - |v_m^\circ\rangle$. This implies

$$E^\circ(S) \sim 2\left(1 - \frac{1}{\sqrt{M}}\right).$$

To give a clear description, we use Equation (5). Applying a simple inequality on the square root ($\sum \sqrt{\cdot} \geq \sqrt{\sum \cdot}$), we have

$$E^\circ(S) = 2\left\{1 - \frac{1}{M} \sum_{m=1}^{M} \sqrt{\lambda_m}\right\} \leq 2\left\{1 - \frac{1}{M}\sqrt{\sum_{m=1}^{M} \lambda_m}\right\} = 2\left(1 - \frac{1}{\sqrt{M}}\right). \tag{7}$$

Thus, $2(1 - 1/\sqrt{M})$ is an upper bound of $E^\circ(S)$ for linearly independent S.

According to Eldar and Forney [18], the LSE for linearly dependent S is given by $E^\circ(S) = 2\left[1 - (1/M)\sum_{i=1}^{r} \sqrt{\lambda_i}\right]$, where r is the rank of $\mathbf{G}$ and λ_i is the nonzero eigenvalue of $\mathbf{G}$. From the convexity of the square root and the inequality used in Equation (7), we have $2(1 - \sqrt{r/M}) \leq E^\circ(S) \leq 2(1 - 1/\sqrt{M})$ for linearly dependent S. If all the vectors in S are identical, then $r = 1$ and $\lambda_1 = M$. Therefore, the upper bound $2(1 - 1/\sqrt{M})$ can be attained by the case that all the vectors in S are identical. Thus, the quantity $2(1 - 1/\sqrt{M})$ can be regarded as the maximum of $E^\circ(S)$ if the identical vector case is allowed. Furthermore, a simple calculation derives the inequality $X_r(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_r) \geq X_{r-1}(\lambda_1 + \lambda_2, \lambda_3, \ldots, \lambda_r)$, where $X_r(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_r) = \sum_{i=1}^{r} \sqrt{\lambda_i}$ for $2 \leq r \leq M$. Therefore, we have

$$2\left(1 - \frac{1}{M} X_r(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_r)\right) \leq 2\left(1 - \frac{1}{M} X_{r-1}(\lambda_1 + \lambda_2, \lambda_3, \ldots, \lambda_r)\right). \tag{8}$$

The orthonormal states and the identical state case attain the minimum and maximum values of LSE, respectively. That is, the smallest rank $r = 1$ case gives the maximum, and the full rank $r = M$ case provides the minimum. The inequality above supports this fact. A lower rank has a higher non-orthogonality and vice versa.

3.2. A Non-Orthogonality Index of a Collection of Pure State Signals

The range of $E^{\circ}(S)$ is given by

$$0 \leq E^{\circ}(S) \leq 2\left(1 - \frac{1}{\sqrt{M}}\right) \leq 2. \tag{9}$$

Hence, we define the non-orthogonality index (NOI), which is a new measure of the non-orthogonality of a collection of linearly independent pure states, as follows:

$$NOI(S) \equiv \frac{1}{2\left(1 - 1/\sqrt{M}\right)} E^{\circ}(S), \tag{10}$$

where $0 \leq NOI(S) \leq 1$. The vectors in S are almost orthogonal to each other when $NOI(S)$ is approximately equal to 0. Conversely, all vectors in S are almost identical when $NOI(S)$ is approximately equal to 1.

4. Numerical Simulations

4.1. Binary Case

For $S = \{|\psi_1\rangle, |\psi_2\rangle\}$,

$$NOI(S) = \frac{2 - \sqrt{1 - |\kappa|} - \sqrt{1 + |\kappa|}}{2 - \sqrt{2}}, \tag{11}$$

where the inner product $\kappa = \langle\psi_1|\psi_2\rangle$. $NOI(S) = 0$ when $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal ($\kappa = 0$), and $NOI(S) = 1$ when $|\psi_1\rangle = |\psi_2\rangle$ ($\kappa = 1$). From Equation (11), we have

$$|\kappa| = \frac{1}{2}(2 - t)\sqrt{t(4 - t)}, \quad t = (2 - \sqrt{2})NOI(S). \tag{12}$$

The minimum average probability of the quantum detection error is given by $P_e = (1 - \sqrt{1 - |\kappa|^2})/2$ [23], where we assume that the states are equiprobable. Moreover, the capacity for a binary pure state channel, $b \to |\psi_b\rangle$ ($b = 1, 2$), is given by $C = -\mu_+ \log_2 \mu_+ - \mu_- \log_2 \mu_-$, where $\mu_\pm = (1 \pm |\kappa|)/2$ [24]. Figure 1 illustrates the plot of these quantities versus $NOI(S)$ instead of the modulus of the inner product $|\kappa|$. The error probability P_e is nearly proportional to $NOI(S)$, and the capacity C monotonically decreases with respect to $NOI(S)$.

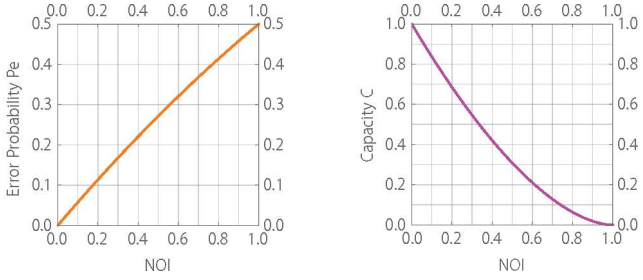


Figure 1. Binary case. **(left)** Minimum error probability P_e vs. $NOI(S)$. **(right)** Capacity C vs. $NOI(S)$.

4.2. Numerical Simulation I: (Condition-Free)

A simple computer simulation was performed to verify the property $0 \leq NOI(0) \leq 1$. In this simulation, M normalized complex vectors, $|\psi_m\rangle = |r_m\rangle \in \mathbb{C}^M$, are randomly generated, and $NOI(S)$ is computed if $S = \{|\psi_m\rangle : 1 \leq m \leq M\}$ is linearly independent. This procedure was repeated 1000 times for each M, where $M = 4, 8, 16, 32, 64, 128, 256$. No exceptional values of $NOI(S)$ were observed in this simulation.

4.3. Numerical Simulation II: (Almost Orthogonal Case)

A simulation for the case of almost orthogonal quantum states was performed to see how $NOI(S)$ approaches zero.

Let $\beta^\bullet = \{|v_1^\bullet\rangle, \ldots, |v_M^\bullet\rangle\}$ be the standard basis for $\mathbb{C}^M$. For each m, a normalized vector $|r_m\rangle \in \mathbb{C}^M$ is randomly generated and the state vector is set to $|\psi'_m\rangle = \mathcal{N}(|v_m^\bullet\rangle + \tilde{\delta}|r_m\rangle)$, where $\mathcal{N}$ is a normalization factor and $\tilde{\delta}$ is a small positive number. When $S' = \{|\psi'_1\rangle, \ldots, |\psi'_M\rangle\}$ is linearly independent, $NOI(S')$ and $\delta = \max\{\delta_1, \ldots, \delta_M\}$ are evaluated, where $\delta_m = \||\psi'_m\rangle - |v_m^\bullet\rangle\|$. This procedure was repeated 200 times for each $\tilde{\delta}$, where $\tilde{\delta}$ was chosen from 0.001 to 0.3 with step 0.001. Hence, the total number of trials was 60000 for each M, where $M = 8, 16, 32, 64, 128, 256$.

Figure 2 illustrates the graph of $NOI(S')$ versus δ for each M. The overall trend of the figures is that $NOI(S')$ almost depends on δ^2, which reflects the definition of δ_m. We observed that the variance of $NOI(S')$, which means the dispersion of values at each δ, decreases and the typical value of $NOI(S')$ approaches zero when δ approaches zero. Conversely, the smallest value in each δ leaves from the floor line of $NOI(S) = 0$ and the variance of $NOI(S')$ increases when δ increases.

Comparing the figures, the variance of $NOI(S')$ shrinks as M increases. The transition from $NOI(S) = 0$ to $NOI(S) = 1$ in a figure is related to the change in the rank of $\mathbf{G}$. Each graph shows only the case of linearly independent S, namely the case of $r = M$. Taken together with Equation (8), one may infer that the boundary of the plotted points means a borderline of whether the randomly generated vector set is linearly independent or not. Based on this thought, the variance in each δ shows the existing range of linearly independent S. Hence, we conjecture that the range of possible values of the NOI for linearly independent sets becomes relatively smaller when M increases.

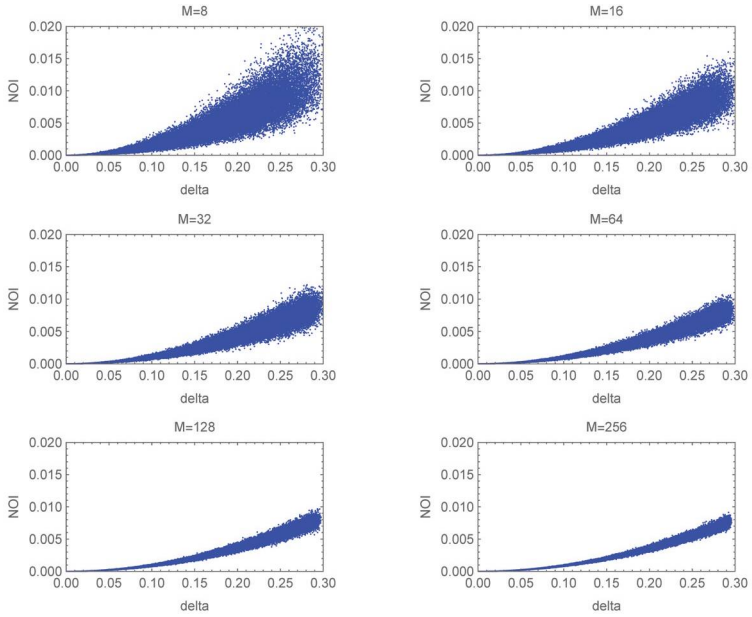


Figure 2. $NOI(S')$ vs. δ for almost orthogonal cases.

4.4. Numerical Simulation III: (Almost Identical Case)

A simulation for the case that the quantum states are almost identical was performed to see how $NOI(S)$ approaches one.

Let $|c\rangle = (1/\sqrt{M}, \ldots, 1/\sqrt{M}) \in \mathbb{C}^M$. For each m, a normalized vector $|r_m\rangle \in \mathbb{C}^M$ is randomly generated and the state vector is set to $|\psi'_m\rangle = \mathcal{N}(|c\rangle + \tilde{\epsilon}|r_m\rangle)$, where $\mathcal{N}$ is

a normalization factor and $\bar{\epsilon}$ is a small positive number. When $S' = \{|\psi'_1\rangle, \ldots, |\psi'_M\rangle\}$ is linearly independent, $NOI(S')$ and $\epsilon = \max\{\epsilon_1, \ldots, \epsilon_M\}$ are evaluated, where $\epsilon_m = \||\psi'_m - c\|$. This procedure was repeated 200 times for each $\bar{\epsilon}$, where $\bar{\epsilon}$ was chosen from 0.001 to 0.3 with step 0.001. Hence, the total number of trials was 60,000 for each M, where $M = 8, 16, 32, 64, 128, 256$.

Figure 3 illustrates the graph of $NOI(S')$ versus ϵ. The overall trend of the figures is that $NOI(S')$ is linear for ϵ. In each figure, the variance of $NOI(S')$ decreases, and the typical value of $NOI(S')$ approaches one as ϵ approaches zero. Conversely, the largest value leaves from the ceiling line of $NOI(S) = 1$ and the variance of $NOI(S')$ increases when ϵ increases. Comparing the figures, the variance of $NOI(S')$ shrinks as M increases, as in the almost orthogonal case.

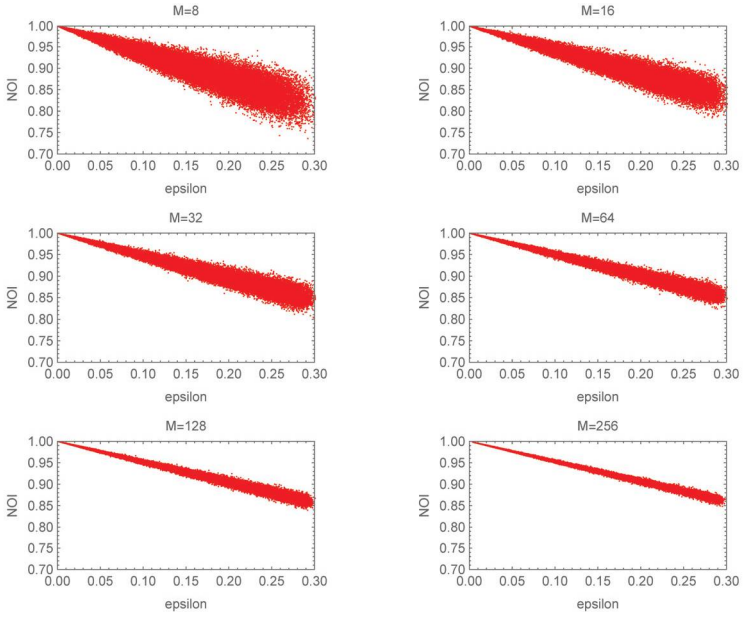


Figure 3. $NOI(S)$ vs. ϵ for almost identical cases.

5. An Application of the Proposed Technique

Let us consider the case of an M-ary PSK coherent state signal as a practical application of the index. As for the M-ary PSK coherent state signal, many researchers have studied it in various ways. The performance of the optimal quantum receiver for the PSK signals has been well studied (e.g., [25–28]). The closed-form expression of the capacity of the pure state channel with the PSK signal was derived in Ref. [29]. The reliability function of the pure state channel with the PSK signal at a high information rate was analyzed in Ref. [30]. Furthermore, an experiment utilizing the 2^{17}-ary (131072-ary) optical PSK signal was reported in Ref. [15].

An optical signal emitted from a laser can be expressed as a coherent state of light. The coherent state with complex amplitude α [31] is expressed as

$$|\alpha\rangle = \exp[-\frac{|\alpha|^2}{2}] \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{13}$$

where $|n\rangle$ is the number state. The average number of signal photons in the state $|\alpha\rangle$ is given by $\langle n\rangle = |\alpha|^2$. In a communication scenario, the complex amplitude of a coherent

state signal is determined based on the signal modulation format. For an M-ary PSK coherent state signal, S is given by

$$S = \left\{ |\alpha_0 \exp[\frac{2m\pi\jmath}{M}]\rangle : 0 \le m \le M-1 \right\}, \tag{14}$$

where $\jmath = \sqrt{-1}$, and the fundamental amplitude α_0 is assumed to be a positive real number. The M-ary PSK coherent state signal is designed to be symmetric on the constellation diagram. Hence, the average number of signal photons does not depend on the probability distribution $\mathbf{p} = (p_0, \ldots, p_{M-1})$ of the signal. That is,

$$N_S = \sum_{m=0}^{M-1} p_m \left| \alpha_0 \exp[\frac{2m\pi\jmath}{M}] \right|^2 = \alpha_0^2. \tag{15}$$

In order to compute $NOI(S)$ of the M-ary PSK coherent state signal, we use the eigenvalues of $\mathbf{G}$ constructed from S of Equation (14). In this case, the eigenvalues are given as follows.

$$\lambda_m = \sum_{\ell=1}^{M} A_{(1,\ell)} \cos\left[\Theta_{(1,\ell)} - \frac{2\pi}{M} m(\ell-1)\right], \tag{16}$$

where

$$A_{(1,\ell)} = \exp\left[-2|\alpha_0|^2 \sin^2\left[\frac{\pi}{M}(\ell-1)\right]\right], \tag{17}$$

$$\Theta_{(1,\ell)} = |\alpha|^2 \sin\left[\frac{2\pi}{M}(\ell-1)\right]. \tag{18}$$

Figure 4 illustrates the graph of $NOI(S)$ of the M-ary PSK coherent state signal versus $\log_2 M$ (the size of M in bits). Typical values of M are $2^4 = 16$, $2^6 = 64$, $2^8 = 256$, $2^{10} = 1024$, $2^{12} = 4096$, $2^{14} = 16{,}384$, $2^{16} = 65{,}536$, and $2^{17} = 131{,}072$. In this computation, the average number N_s of signal photons was between 10 and 1,000,000 photons. From Figure 4, we observe that $NOI(S)$ increases monotonically for M. This mutual relationship was observed for all values of N_S. The non-orthogonality of the states is one of the fundamental properties of a quantum system. Therefore, Figure 4 shows that the M-ary PSK coherent state signal exhibits a quantum nature for a significantly large number of signal photons when the total number M of the signals is large enough.

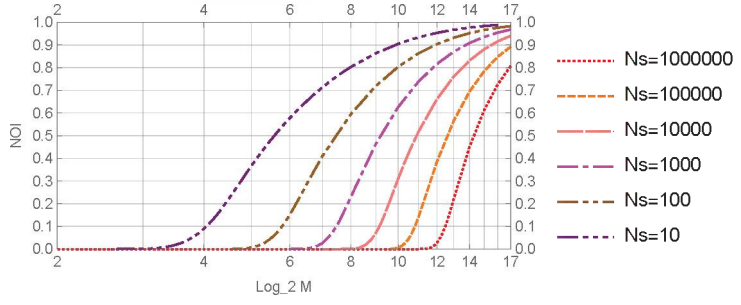


Figure 4. $NOI(S)$ vs. $\log_2 M$ for M-ary PSK coherent state signal.

The capacity of the pure state channel $m \to |\psi_m\rangle$ for the M-ary PSK coherent state signal is analyzed to understand the operational meaning of $NOI(S)$. From Ref. [29], the capacity of this channel is given by

$$C = -\sum_{m=1}^{M} \mu_m \log_2 \mu_m, \quad \mu_m = \frac{\lambda_m}{M}, \tag{19}$$

where λ_m is given by Equation (16), because the optimal signal distribution to achieve the capacity is a uniform distribution $\mathbf{p} = (1/M, \ldots, 1/M)$. Normalized quantity C', which represents the number of Shannon bits per one binary digit of a signal, is obtained by dividing the capacity C by $\log_2 M$. Figure 5 illustrates the graph of the normalized capacity versus $\log_2 M$. From Figures 4 and 5, we observe that the normalized capacity is maximum (or 1) in the region where $NOI(S)$ is almost zero, and the capacity decreases when $NOI(S)$ increases. Thus, $NOI(S)$ effectively detects the trend of the capacity.

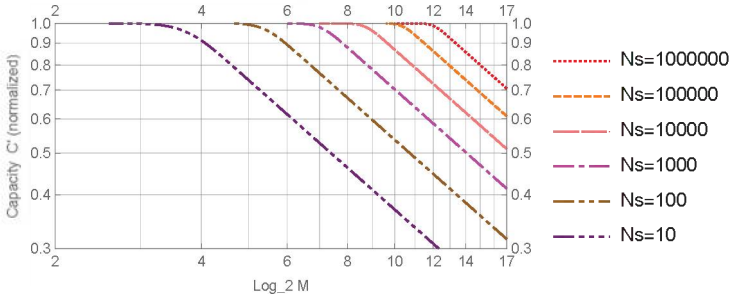


Figure 5. Normalized capacity C' vs. $\log_2 M$ for M-ary PSK coherent state signal.

6. Conclusions

We have proposed a novel index to measure the non-orthogonality of a collection of linearly independent pure states based on the least squares error criterion in quantum detection theory. We call this index the non-orthogonality index (NOI). First, the non-orthogonality index was analyzed using numerical simulations for binary, condition-free, almost orthogonal, and almost identical cases. The index effectively measured the non-orthogonality of a collection of linearly independent signals from the computer simulations. Next, the non-orthogonality index was applied to the M-ary phase-shift keying (PSK) coherent state signal. It was shown that a highly large-scale M-ary PSK coherent state signal exhibits high non-orthogonality when the total number of signals is sufficiently large. Furthermore, the index was compared with the capacity of the pure state channel with the PSK signal. Then, we observed that the proposed index effectively detects the trend of the capacity.

In general, a quantum cryptographic system must use a quantum signal set that is unable to distinguish the signals with small detection error or extract much information for an eavesdropper. A simple method is to use single-photon or very weak coherent states. However, this approach has inherent limitations in transmission speed and distance. On the other hand, the coherent state signal having very high power can behave as an almost non-orthogonal signal if the number of signals is sufficiently large. Thus, using a highly large-scale multilevel coherent state signal can create an advantage for legitimate users against the eavesdropper from quantum signal detection. Quantum stream cipher Y00 is a protocol that uses a sufficient number of high-power coherent state signals. Therefore, we conclude that the characterization of a highly large-scale M-ary coherent state signal based on the non-orthogonality index provides a basis for understanding cutting-edge optical communication technologies such as quantum stream cipher Y00.

This article discussed the non-orthogonality index in the case of linearly independent pure state signals. Therefore, the generalization of the index remains for future work,

which will involve a more precise analysis of linearly dependent cases and the cases of mixed states. In addition, the application to other multilevel coherent state signals such as quadrature amplitude modulation signals will be considered in future work.

Funding: This research was funded under Grant No. JPJ004596 from ATLA, Japan.

Institutional Review Board Statement: Not applicable

Data Availability Statement: All relevant simulation parameters and equations are within the paper. No experimental data was used in this study.

Acknowledgments: The author would like to thank Fumio Futami and Ken Tanizawa of Tamagawa University for their helpful discussions. The author is grateful to Shigeo Tsujii of Chuo University for his encouragement.

Conflicts of Interest: The author declares no conflict of interest associated with this manuscript.

Abbreviations

The following abbreviations are used in this manuscript:

LSE	Least squares error
NOI	Non-orthogonality index
PSK	Phase-shift keying

References

1. Helstrom, C.W. Detection theory and quantum mechanics. *Inf. Control* **1967**, *10*, 254–291. [CrossRef]
2. Helstrom, C.W. Detection theory and quantum mechanics (II). *Inf. Control* **1968**, *13*, 156–171. [CrossRef]
3. Helstrom, C.W. Fundamental limitations on the detectability of electromagnetic signals. *Int. J. Theor. Phys.* **1968**, *1*, 37–50. [CrossRef]
4. Middleton, D. *An Introduction to Statistical Communication Theory*; McGraw-Hill: New York, NY, USA, 1960; pp. 771–1070.
5. Van Trees, H.L. *Detection, Estimation, and Modulation Theory*; Part I; John Wiley and Sons: New York, NY, USA, 1968; pp. 19–165.
6. Yuen, H.P.; Kennedy, R.S.; Lax, M. On optimal quantum receivers for digital signal detection. *Proc. IEEE* **1970**, *58*, 1770–1773. [CrossRef]
7. Yuen, H.P.; Kennedy, R.S.; Lax, M. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inf. Theor.* **1975**, *21*, 125–134. [CrossRef]
8. Holevo, A.S. Statistical decision theory for quantum systems. *J. Multivar. Anal.* **1973**, *3*, 337–394. [CrossRef]
9. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
10. Dieks, D. Communication by EPR devices. *Phys. Lett.* **1982**, *92*, 271–272. [CrossRef]
11. Yuen, H.P. Amplification of quantum states and noiseless photon amplifiers. *Phys. Lett.* **1986**, *113*, 405–407. [CrossRef]
12. Middleton, D.; Van Meter, D. On optimum multiple-alternative detection of signals in noise. *IRE Trans. Inf. Theor.* **1955**, *1*, 1–9. [CrossRef]
13. Gallager, R.G. *Principles of Digital Communication*; Cambridge University Press: New York, NY, USA, 2008; Section 8.4.
14. Papen, G.C.; Blahut, R. E. *Lightwave Communications*; Cambridge University Press: New York, NY, USA, 2019; Chapter 10.
15. Tanizawa, K.; Futami, F. Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels. *Opt. Express* **2019**, *27*, 1071–1079. [CrossRef] [PubMed]
16. 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]
17. Holevo, A.S. On asymptotically optimal hypotheses testing in quantum statistics. *Theor. Probab. Appl.* **1979**, *23*, 411–415. 429–432. [CrossRef]
18. Eldar, Y.C.; Forney, G.D., Jr. On quantum detection and the square-root measurement. *IEEE Trans. Inf. Theor.* **2001**, *47*, 858–872. [CrossRef]
19. Belavkin, V.P. Optimal multiple quantum statistical hypothesis testing. *Stochastics* **1975**, *1*, 315–345. [CrossRef]
20. Hausladen, P.; Wootters, W.K. A "pretty good" measurement for distinguishing quantum states. *J. Mod. Opt.* **1994**, *41*, 2385–2390. [CrossRef]
21. 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]
22. Tyson, J. Error rates of Belavkin weighted quantum measurements and a converse to Holevo's asymptotic optimality theorem. *Phys. Rev. A* **2009**, *79*, 032343. [CrossRef]
23. Helstrom, C.W. *Quantum Detection and Estimation Theory*; Academic Press: New York, NY, USA, 1976; p. 113.

24. Holevo, A.S. *Statistical Structure of Quantum Theory*; Springer: Berlin, Germany, 2001; p. 53.
25. Charbit, M.; Bendjaballah, C.; Helstrom, C.W. Cutoff rate for the *M*-ary PSK modulation channel with optimal quantum detection. *IEEE Trans. Inf. Theor.* **1989**, *35*, 1131–1133. [CrossRef]
26. Kato, K.; Osaki, M.; Sasaki, M.; Hirota, O. Quantum detection and mutual information for QAM and PSK signals. *IEEE Trans. Commun.* **1999**, *47*, 248–254. [CrossRef]
27. Djordjevic, I.B. LDPC-coded *M*-ary PSK optical coherent state quantum communication. *J. Light. Technol.* **2009**, *27*, 494–499. [CrossRef]
28. Cariolaro, G.; Pierobon, G. Performance of quantum data transmission systems in the presence of thermal noise. *IEEE Trans. Commun.* **2010**, *58*, 623–630. [CrossRef]
29. Kato, K.; Osaki, M.; Hirota, O. Derivation of classical capacity of a quantum channel for a discrete information source, *Phys. Lett. A* **1999**, *251*, 157–163. [CrossRef]
30. Kato, K. A Note on the Reliability Function for *M*-ary PSK Coherent State Signal. *Tamagawa Univ. Quant. ICT Res. Inst. Bulletin* **2018**, *8*, 21–25. Available online: https://www.tamagawa.jp/research/quantum/bulletin/pdf/Tamagawa.Vol.8-5.pdf (accessed on 19 April 2022).
31. Glauber, R.J. Coherent and incoherent states of the radiation field. *Phys. Rev.* **1963**, *131*, 2766–2788. [CrossRef]

entropy

MDPI

Article

Detecting a Photon-Number Splitting Attack in Decoy-State Measurement-Device-Independent Quantum Key Distribution via Statistical Hypothesis Testing

Xiaoming Chen [1,2,3], Lei Chen [1,2,*] and Yalong Yan [3]

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Beijing Electronic Science and Technology Institute, Beijing 100070, China
[3] School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230026, China
* Correspondence: chenlei1992@bupt.edu.cn

Abstract: Measurement-device-independent quantum key distribution (MDI-QKD) is innately immune to all detection-side attacks. Due to the limitations of technology, most MDI-QKD protocols use weak coherent photon sources (WCPs), which may suffer from a photon-number splitting (PNS) attack from eavesdroppers. Therefore, the existing MDI-QKD protocols also need the decoy-state method, which can resist PNS attacks very well. However, the existing decoy-state methods do not attend to the existence of PNS attacks, and the secure keys are only generated by single-photon components. In fact, multiphoton pulses can also form secure keys if we can confirm that there is no PNS attack. For simplicity, we only analyze the weaker version of a PNS attack in which a legitimate user's pulse count rate changes significantly after the attack. In this paper, under the null hypothesis of no PNS attack, we first determine whether there is an attack or not by retrieving the missing information of the existing decoy-state MDI-QKD protocols via statistical hypothesis testing, extract a normal distribution statistic, and provide a detection method and the corresponding Type I error probability. If the result is judged to be an attack, we use the existing decoy-state method to estimate the secure key rate. Otherwise, all pulses with the same basis leading to successful Bell state measurement (BSM) events including both single-photon pulses and multiphoton pulses can be used to generate secure keys, and we give the formula of the secure key rate in this case. Finally, based on actual experimental data from other literature, the associated experimental results (e.g., the significance level is 5%) show the correctness of our method.

Keywords: decoy state; measurement-device independent; quantum key distribution; photon number splitting attack; statistical hypothesis testing

Citation: Chen, X.; Chen, L.; Yan, Y. Detecting a Photon-Number Splitting Attack in Decoy-State Measurement-Device-Independent Quantum Key Distribution via Statistical Hypothesis Testing. *Entropy* **2022**, *24*, 1232. https://doi.org/10.3390/e24091232

Academic Editor: Osamu Hirota

Received: 11 July 2022
Accepted: 23 August 2022
Published: 2 September 2022

1. Introduction

Quantum key distribution (QKD) [1–6] is a technique that allows two remote parties (Alice and Bob), to share unconditional secure keys. The unconditional security of the keys are guaranteed by the laws of quantum mechanics [7–10]. The first ideal QKD protocol is BB84-QKD created by Bennett and Brassard [1], which needs a perfect single-photon source and detectors. However, there is always a large gap between ideal and reality. Due to the imperfection of equipment, the implementation of the QKD suffers double attacks from the source side and detection side. On the one hand, at present, perfect single-photon sources are not available, and weak coherent photon sources (WCPs) after phase randomization are often utilized to replace the single-photon sources. While the photon number of the pulses emitted by WCPs may be more than one, an eavesdropper Eve can launch a photon-number splitting (PNS) attack [11–15]. Specially, a weaker version of a PNS attack is one in which Alice's or Bob's pulse count rate changes significantly after the attack [11–14], and the stronger PNS attack means that both Alice's and Bob's pulse count rates remain unchanged after the attack [15]. The difference between these two attacks is the effect on Alice's and

Bob's pulse count rates. Fortunately, the decoy-state method [16–18] proposed later can resist PNS attacks very well.

On the other hand, due to the low detection efficiency of the detectors, Eve can launch attacks against the detectors. Compared with source attacks, there are more attacks from the detection side, such as the detector blinding attack [19,20], dead time attack [21], faked state attack [22,23], and time shift attack [24].People have proposed device-independent quantum key distribution (DI-QKD) [25,26], which can resist all attacks from devices. However, this protocol is highly impractical because it needs close to unity detection efficiency. In 2012, Lo et al. [27] proposed measurement-device-independent quantum key distribution (MDI-QKD), which is also known as the time-inversion version of EPR protocol [28]. In MDI-QKD, Alice and Bob do not need to perform measurement operations, so it can be innately immune to all detection attacks. MDI-QKD combined with the decoy-state method can resist both source attacks and detection attacks; thus, decoy-state MDI-QKD [29–31] is one of the most promising QKD protocols, which can provide unconditional secure keys in practical applications.

However, the secure key rate of the existing decoy-state MDI-QKD is not high [32,33]. The decoy-state method defeats the PNS attack through providing a more accurate method to determine the secure key rate. More specifically, the existing decoy-state method can more closely estimate the lower bound of gain and the upper bound of quantum bit error rate (QBER) of single-photon signals, and then the secure key rate can be calculated by the GLLP formula [34]. In essence, the existing decoy-state method does not care about the existence of a PNS attack, and the secure keys are only generated by single-photon components [35]. However, if we can determine that there is no PNS attack on the channel, multiphoton pulses can also generate secure keys. For simplicity, we only analyze the weaker version of PNS attack in which the legitimate user's pulse count rate changes significantly after the attack. In this case, there is no doubt that using the existing methods to estimate the secure key rate will waste the underlying keys generated from multiphoton pulses and reduce the efficiency.

In this work, under the null hypothesis of no PNS attack H_0, we first retrieve the lost information in the existing decoy-state MDI-QKD, extract a normal distribution statistic, and provide a new method to determine whether there is a PNS attack or not through statistical hypothesis testing. If the result is judged to be an attack, the keys can only be generated from single-photon pulses, and the secure key rate will be estimated by the existing decoy-state method. Otherwise, all pulses with the same basis leading to a successful Bell state measurement (BSM) event including both single-photon pulses and multiphoton pulses can be used to generate keys, and we give the formula of the secure key rate in this case. Furthermore, we use the real experimental data in [36] to verify our method, and the analytical results show that our method is credible (e.g., a significance level of 5%).

The structure of this paper is organized as follows. In Section 2, we briefly review the typical decoy-state MDI-QKD and related notations. In Section 3, we describe our method for detecting the PNS attack in the decoy-state MDI-QKD via statistical hypothesis testing in detail. In Section 4, the correctness of our method is verified with the real experimental data from the existing literature. Finally, we discuss and draw conclusions in Section 5.

2. Three-Intensity Decoy-State MDI-QKD

In this paper, we adopt a typical decoy-state MDI-QKD with polarization encoding [36], which mainly consists of three steps.

(i) Alice generates phase-randomized pulses from WCPs and randomly selects the basis $W \in \{Z, X\}$. That is, $P_Z = P_X = 1/2$, where P_Z and P_X are the probabilities of choosing the Z basis and X basis, respectively. Then Alice uses an intensity modulator to modulate the pulses with three different intensities and sends them to Charlie located in the middle. This three intensities are the intensity of signal state μ_2, the intensity of decoy state μ_1, and the intensity of vacuum state μ_0, respectively. Furthermore, the

corresponding percentages being emitted are P_{μ_2}, P_{μ_1}, and P_{μ_0}, respectively. Obviously, $P_{\mu_2} + P_{\mu_1} + P_{\mu_0} = 1$. At the same time, Bob performs the same procedures as Alice, and the intensities of Bob's pulses are noted as ν_2, ν_1, and ν_0 for the signal state, decoy state, and vacuum state, respectively. Similarly, the corresponding percentages being emitted are P_{ν_2}, P_{ν_1}, and P_{ν_0}, respectively, where $P_{\nu_2} + P_{\nu_1} + P_{\nu_0} = 1$.

(ii) The pulses from Alice and Bob interfere when they reach Charlie. Then Charlie performs a Bell state measurement (BSM) on the interference outcomes and announces the measurement results to Alice and Bob.

(iii) Alice and Bob compare their bases, and determine the secure keys through Charlie's measurement results. Specifically, if Alice and Bob choose the same basis and Charlie has a successful BSM event at the same time, then this part of the pulses can generate keys. It is important to emphasize that the secure keys are only generated from the signal state with Z basis, and the others are used for parameter estimation.

The secure key rate of the decoy-state MDI-QKD [27,36] is given by

$$R \geq q\{P_{11}^{\mu_2\nu_2} Y_{11}^{Z}[1 - H(e_{11}^{X})] - Q_{\mu_2\nu_2}^{Z} f_e H(E_{\mu_2\nu_2}^{Z})\}. \tag{1}$$

In the above equation, $q = P_Z^2 P_{\mu_2} P_{\nu_2}$ is the probability that Alice and Bob both select the Z basis and both modulate the pulse as signal state. $P_{11}^{\mu_2\nu_2} = \mu_2\nu_2 e^{-\mu_2-\nu_2}$ is the probability that the pulses from Alice's signal state and Bob's signal state are both single-photon pulses. Y_{11}^{Z} and e_{11}^{X} are the yield of single-photon state with Z basis and the quantum bit error rate (QBER) of single-photon state with X basis. $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. $Q_{\mu_2\nu_2}^{Z}$ and $E_{\mu_2\nu_2}^{Z}$ are the overall gain and overall QBER of signal state with Z basis, respectively. $f_e > 1$ is the error correction efficiency.

According to [37,38], the overall gain $Q_{\mu_k\nu_l}^{W}$ $(W \in \{X, Z\})$ and the overall QBER $E_{\mu_k\nu_l}^{W}$ $(W \in \{X, Z\})$ can be obtained by the following equations,

$$\begin{aligned} Q_{\mu_k\nu_l}^{X} &= 2y^2[1 + 2y^2 - 4yI_0(x) + I_0(2x)], \\ E_{\mu_k\nu_l}^{X} Q_{\mu_k\nu_l}^{X} &= e_0 Q_{\mu_k\nu_l}^{X} - 2(e_0 - e_d)y^2[I_0(2x) - 1], \\ Q_{\mu_k\nu_l}^{Z} &= Q_C + Q_E, \\ E_{\mu_k\nu_l}^{Z} Q_{\mu_k\nu_l}^{Z} &= e_d Q_C + (1 - e_d) Q_E. \end{aligned} \tag{2}$$

where

$$\begin{aligned} Q_C &= 2(1-p_d)^2 e^{-\mu'/2}[1 - (1-p_d)e^{-\eta_a\mu_k/2}] \times [1 - (1-p_d)e^{-\eta_b\nu_l/2}], \\ Q_E &= 2p_d(1-p_d)^2 e^{-\mu'/2}[I_0(2x) - (1-p_d)e^{-\mu'/2}]. \end{aligned} \tag{3}$$

In the above equations, μ_k and ν_l, $k, l \in \{0, 1, 2\}$, are the intensities of pulses emitted by Alice and Bob, respectively. $I_0(x)$ is the modified Bessel function of the first kind. e_0 is the error rate of background. e_d is the misalignment-error probability. p_d is the dark count rate. η_a and η_b are the transmission efficiencies of Alice and Bob, respectively. In addition,

$$\begin{aligned} x &= \sqrt{\eta_a\mu_k\eta_b\nu_l}/2, \\ y &= (1-p_d)e^{-\mu'/4}, \\ \mu' &= \eta_a\mu_k + \eta_b\nu_l, \\ \eta_a &= \eta_d 10^{-\frac{\delta L_{ac}+\theta}{10}}, \\ \eta_b &= \eta_d 10^{-\frac{\delta L_{bc}+\theta}{10}}, \end{aligned} \tag{4}$$

where η_d is the quantum efficiency of detectors, δ is the loss coefficient measured in dB/km, L_{ac} (L_{bc}) is the distance in km from Alice (Bob) to Charlie, and θ is the insertion loss in Charlie's measurement setup in dB. Without Eve's intervention, based on Equations (2)–(4),

the yield and the QBER of single-photon pulses when Alice and Bob select the same basis X or Z are, respectively, given by

$$\begin{aligned} Y_{11}^X = Y_{11}^Z &= (1-p_d)^2[\frac{\eta_a\eta_b}{2} + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)p_d + 4(1-\eta_a)(1-\eta_b)p_d^2], \\ e_{11}^X Y_{11}^X &= e_0 Y_{11}^X - (e_0 - e_d)(1-p_d)^2\frac{\eta_a\eta_b}{2}, \\ e_{11}^Z Y_{11}^Z &= e_0 Y_{11}^Z - (e_0 - e_d)(1-p_d)^2(1-p_d)\frac{\eta_a\eta_b}{2}. \end{aligned} \tag{5}$$

3. Statistical Hypothesis Testing

In this section, we introduce a new method to detect the PNS attack in the decoy-state MDI-QKD via statistical hypothesis testing. It is important to emphasize that the PNS attacks mentioned here and below refer to the weaker version of PNS attack. Then we analyze the Type I error of the test; that is, mistaking no PNS attack when there is a PNS attack. Generally speaking, our method first puts forward a null hypothesis and alternative hypothesis based on the theory of statistical hypothesis testing. Then, the test statistic is constructed according to the null hypothesis and other conditions. Furthermore, the specific values of the statistics can be obtained by using the parameters and experimental data. After the significance level is given, we can infer whether there is PNS attack in the channel with a certain probability. The details are as follows.

(i) Identify null and alternative hypothesis. Let us consider the hypothesis testing problem of the null hypothesis H_0: there is no PNS attack on the channel and the alternative hypothesis H_1: there is a PNS attack on the channel.

(ii) Construct the test statistic. We need a test statistic to conduct the hypothesis testing. In what follows, the distribution of the test statistic is derived under the null hypothesis H_0. Let us further consider Alice's and Bob's pulses emission process and Charlie's BSM event. When Alice and Bob send pulses with the same basis, the BSM event outcomes at Charlie only include two cases, successful or failed. Therefore, the above process can be regarded as a Bernoulli trial. Note that $Q_{\mu_k\nu_l}^W$ is the probability that Charlie obtains a successful BSM event provided that Alice and Bob emit pulses with the intensities μ_k and ν_l and select the basis W. Suppose the total number of pulses emitted by Alice (Bob) is N_{data}, then the number of pulses is $P_W^2 P_{\mu_k\nu_l} N_{data}$ when Alice's and Bob's intensities with W basis are μ_k and ν_l, respectively. In the above equation, P_W is the probability that Alice (Bob) chooses the $W \in \{X, Z\}$ basis, $P_{\mu_k\nu_l} = P_{\mu_k} P_{\nu_l}$ is the probability that Alice and Bob choose the intensities μ_k and ν_l, respectively. At this point, the number of successful BSM events that Charlie obtained is denoted as $n_{\mu_k\nu_l}^W$. Then, $n_{\mu_k\nu_l}^W$ has the binomial distribution with parameters $(P_W^2 P_{\mu_k\nu_l} N_{data},\ Q_{\mu_k\nu_l}^W)$, for short,

$$n_{\mu_k\nu_l}^W \sim B(P_W^2 P_{\mu_k\nu_l} N_{data},\ Q_{\mu_k\nu_l}^W). \tag{6}$$

According to [36], we find N_{data} is so large (typically $10^{10} \sim 10^{11}$), $Q_{\mu_k\nu_l}^W$ is close to $10^{-8} \sim 10^{-5}$. Generally, the selections of basis and intensity are random. In other words, $P_Z = P_X = 1/2$, $P_{\mu_k} = P_{\nu_l} = 1/3$ where $k, l \in \{0, 1, 2\}$. Thus, we have $P_W^2 P_{\mu_k\nu_l} N_{data} Q_{\mu_k\nu_l}^W > P_W^2 P_{\mu_k\nu_l} N_{data}(1 - Q_{\mu_k\nu_l}^W) \geq 5$. By the law of large numbers and the central limit theorem, when $P_W^2 P_{\mu_k\nu_l} N_{data} Q_{\mu_k\nu_l}^W \geq 5$ and $P_W^2 P_{\mu_k\nu_l} N_{data}(1 - Q_{\mu_k\nu_l}^W) \geq 5$, the binomial distribution with parameters $(P_W^2 P_{\mu_k\nu_l} N_{data},\ Q_{\mu_k\nu_l}^W)$ can be approximately regarded as the normal distribution with mean $P_W^2 P_{\mu_k\nu_l} N_{data} Q_{\mu_k\nu_l}^W$ and variance $P_W^2 P_{\mu_k\nu_l} N_{data}(1 - Q_{\mu_k\nu_l}^W)$, given by

$$n_{\mu_k\nu_l}^W \sim N(P_W^2 P_{\mu_k\nu_l} N_{data} Q_{\mu_k\nu_l}^W,\ P_W^2 P_{\mu_k\nu_l} N_{data}(1 - Q_{\mu_k\nu_l}^W)). \tag{7}$$

After standardization, we obtain a random variable $U^W_{\mu_k\nu_l}$, which obeys the standard normal distribution; that is,

$$U^W_{\mu_k\nu_l} = \frac{n^W_{\mu_k\nu_l} - P^2_W P_{\mu_k\nu_l} N_{data} Q^W_{\mu_k\nu_l}}{\sqrt{P^2_W P_{\mu_k\nu_l} N_{data}(1 - Q^W_{\mu_k\nu_l})}} \sim N(0,1). \tag{8}$$

Considering the additivity of normal distribution, we obtain a random variable involving all possibilities of $U^W_{\mu_k\nu_l}$ where $W \in \{X, Z\}$, $k, l \in \{0, 1, 2\}$, which also obeys the normal distribution. There are eighteen cases of $U^W_{\mu_k\nu_l}$ considering that the pair of intensity is nine cases and the selection of basis is two cases. Note that we only consider the same basis for Alice and Bob, that is, both Z basis or both X basis. After standardization, we obtain a new random variable V that obeys the standard normal distribution, which can be written as

$$V = \frac{1}{\sqrt{18}} \sum_{W\in\{Z,X\},\, k,\, l\in\{0,1,2\}} \frac{n^W_{\mu_k\nu_l} - P^2_W P_{\mu_k\nu_l} N_{data} Q^W_{\mu_k\nu_l}}{\sqrt{P^2_W P_{\mu_k\nu_l} N_{data}(1 - Q^W_{\mu_k\nu_l})}} \sim N(0,1). \tag{9}$$

Furthermore, $\Phi(v)$ is the distribution function of V, given by

$$\Phi(v) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{v} e^{-\frac{t^2}{2}} \mathrm{d}t, \ -\infty < vs. < \infty, \tag{10}$$

where v is the value of V and is just the test statistic that we find.

(iii) Find the value of the test statistic. We set the parameters N_{data}, e_d, e_0, p_d, L_{ac}, L_{bc}, δ, θ, P_Z, P_X, μ_k, ν_l, P_{μ_k}, and P_{ν_l}, where $k, l \in \{0, 1, 2\}$, and we calculate the theoretical value of $Q^W_{\mu_k\nu_l}$ according to Equations (2)–(4). We record $n^W_{\mu_k\nu_l}$ where $k, l \in \{0, 1, 2\}$, $W \in \{X, Z\}$. We substitute the above data into Equation (9) and obtain the value of the test statistic v.

(iv) Choose a significance level. We need to determine a significance level α (typically 0.05) for the test. In terms of the null hypothesis H_0 of the test, we deduce that the test is a two-tailed hypothesis testing. Given α, the rejection region is $|vs.| > v_{[1-\alpha/2]}$ where $v_{[1-\alpha/2]}$ can be obtained by Equation (10). More precisely, the variables $-v_{[1-\alpha/2]}$ and $v_{[1-\alpha/2]}$ refer to the boundary values between the rejection region and the acceptance region for the test. Let the left side of Equation (10) be equal to $\alpha/2$; the upper limit of the integral will be $-v_{[1-\alpha/2]}$. According to the symmetry of the probability density function of normal distribution, $v_{[1-\alpha/2]}$ can be obtained.

(v) Make a decision. Compare the test statistic v with the critical values $v_{[1-\alpha/2]}$ and $-v_{[1-\alpha/2]}$. If $v > v_{[1-\alpha/2]}$ or $v < -v_{[1-\alpha/2]}$, we will reject H_0 and accept H_1. This means that we believe there is a PNS attack on the channel. Otherwise, we fail to reject H_0. That is to say, we consider there is no PNS attack on the channel. Note that the significance level of the test α is just the Type I error probability of the test, namely, the probability of mistaking no PNS attack for having a PNS attack. Let β denote the Type II error probability of the test, to be precise, the probability of mistaking having a PNS attack for no PNS attack. Note that β is usually difficult to solve in most situations. Furthermore, determining the value of β requires more information about the aggression behavior.

If the result is judged to be a PNS attack, the secure key rate in this case can be estimated by Equation (1). Otherwise, all pulses with the Z basis leading to a successful BSM event including both single-photon pulses and multiphoton pulses can be used to generate the keys. Furthermore, the secure key rate formula Equation (1) becomes

$$R \geq qQ^Z_{\mu_2\nu_2}[1 - f_e H(E^Z_{\mu_2\nu_2}) - H(E^Z_{\mu_2\nu_2})]. \tag{11}$$

By comparing Equation (11) with Equation (1), we can easily find the secure key rate has been highly improved when the judgment result is no PNS attack. This is mainly due to the contribution of multiphoton components.

4. Results and Analysis

In the preceding section, we showed the details of our detection method. Now, we move forward to the corresponding experiments based on the aforementioned method and analyze the experimental results. Generally speaking, the real experimental data were substituted into the formulas in Section 3 to verify the correctness of our method. The experimental parameters were from real experiments [36]. Specially, the experimenters in [36] adopted a symmetric scheme; that is, all parameters of Alice and Bob were identical and optimized. The relevant experimental parameters used in [36] and this paper are shown in Table 1.

Table 1. Experimental parameters used in this paper. Data from *Phys. Rev. Lett.* **2014**, *112*, 190503.

$\mu_2(\nu_2)$	$\mu_1(\nu_1)$	$\mu_0(\nu_0)$	$P_{\mu_2}(P_{\nu_2})$	$P_{\mu_1}(P_{\nu_1})$	$P_{\mu_0}(P_{\nu_0})$	$P_Z(P_X)$
0.3	0.1	0.01	0.2	0.45	0.35	0.5
N_{data}	e_d	e_0	p_d	$L_{ac}(L_{bc})$	δ	θ
1.69×10^{11}	0.01	0.5	5×10^{-5}	5	0.2	0.8

Based on the above parameters, we can obtain the values of $Q^W_{\mu_k\nu_l}$, as shown in Table 2. Note that Table 2 in this paper is exactly the same as Table I in the Supplementary Materials of [36]. We record the values of $n^W_{\mu_k\nu_l}$, as shown in Table 3. Note that the data in Table 3 can be deduced from Table I in the Main Text of [36]. According to the above data and Equation (8), all values of $U^W_{\mu_k\nu_l}$ can be obtained, as shown in Table 4.

Table 2. The values of $Q^W_{\mu_k\nu_l}(\times 10^{-4})$ with intensities $\mu_k \in \{\mu_2, \mu_1, \mu_0\}$ and $\nu_l \in \{\nu_2, \nu_1, \nu_0\}$ based on $W \in \{X, Z\}$. Reprinted/adapted with permission from Ref. [36], 2014, American Physical Society.

	Z			X		
ν_l \ μ_k	μ_2	μ_1	μ_0	μ_2	μ_1	μ_0
ν_2	0.4643	0.1596	0.0215	0.9086	0.4074	0.2449
ν_1	0.1596	0.0539	0.0066	0.4074	0.1039	0.0319
ν_0	0.0215	0.0066	0.0007	0.2449	0.0319	0.0012

Table 3. The values of $n^W_{\mu_k\nu_l}(\times 10^4)$ with intensities $\mu_k \in \{\mu_2, \mu_1, \mu_0\}$ and $\nu_l \in \{\nu_2, \nu_1, \nu_0\}$ based on $W \in \{X, Z\}$.

	Z			X		
ν_l \ μ_k	μ_2	μ_1	μ_0	μ_2	μ_1	μ_0
ν_2	787.5	270.4	38.03	1526	692.9	429.3
ν_1	262.0	89.74	11.83	670.9	172.4	52.73
ν_0	36.17	11.32	1.521	415.7	53.57	2.366

Table 4. The values of $U^W_{\mu_k\nu_l}$ with intensities $\mu_k \in \{\mu_2, \mu_1, \mu_0\}$ and $\nu_l \in \{\nu_2, \nu_1, \nu_0\}$ based on $W \in \{X, Z\}$.

	Z			X		
ν_l \ μ_k	μ_2	μ_1	μ_0	μ_2	μ_1	μ_0
ν_2	1.026	0.6174	3.709	2.415	2.512	10.00
ν_1	−7.100	−3.187	4.016	−10.05	−5.452	−3.197
ν_0	−0.3709	1.004	5.438	1.209	−0.9135	4.154

The schematic diagram of statistical hypothesis testing is illustrated in Figure 1. After calculation, we obtained the value of the test statistic $v = 0.236$. Given the significance

level of the test $\alpha = 0.05$, the critical values were $v_{[1-\alpha/2]} = 1.96$ and $-v_{[1-\alpha/2]} = -1.96$. Since $-1.96 < 0.236 < 1.96$, the test statistic did not fall inside the rejection region, and we failed to reject H_0. In other words, we inferred that there was no PNS attack on the channel, and the corresponding Type I error probability was less than 5%. According to [36], there was indeed no PNS attack in the experiment, which verifies the correctness of our method. Thus, both single-photon and multiphoton components can be used to generate keys in this case. At this time, the secure key rate can be estimated through Equation (11).

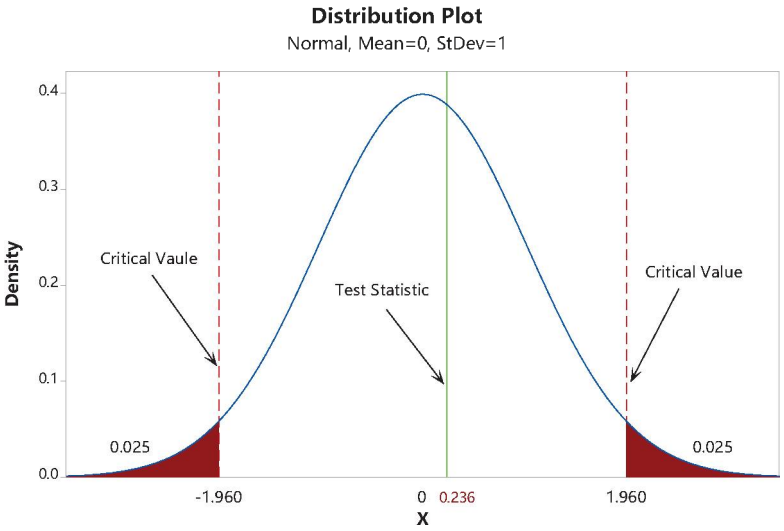


Figure 1. The schematic diagram of statistical hypothesis testing. The value of the test statistic v is 0.236. Given the significance level of the test $\alpha = 0.05$, the critical values are $v_{[1-\alpha/2]} = 1.96$ and $-v_{[1-\alpha/2]} = -1.96$.

5. Conclusions and Discussion

In summary, we first recovered the lost information of the existing decoy-state method when detecting the weaker version of a PNS attack in the decoy-state MDI-QKD and extracted a normal distribution statistic via statistical hypothesis testing. Based on this information, we proposed a new method to detect the weaker version of a PNS attack. Most importantly, the error probability of detection was precisely calculated by our method, and we also gave the calculation. Finally, according to the judgment result, the corresponding secure key rate was provided. In particular, compared with the existing decoy-state MDI-QKD protocols, the secure key rate with our method has been highly improved if the judgment result is no weak PNS attack. Meanwhile, the associated experimental results also verified the correctness of our method.

Nevertheless, all judgment results in this paper were obtained under the condition that the null hypothesis was no weak version of a PNS attack. In other words, we assume that the gain of signal or decoy state will change significantly after the PNS attack. However, we can do nothing about the stronger PNS attack, which retains the gain of signal and decoy state, such as a partial PNS attack [15], because the premise of the derivation no longer holds, and the Type II error probability of our method in this case will be poor even close to unity. For this reason, compared with the existing decoy-state method [29–31] to directly estimate the secure key rate, our method is not ready for practical application now; however, we provide a new direction to improve the secure key rate and efficiency.

Author Contributions: Conceptualization, X.C.; Formal analysis, L.C.; Methodology, L.C.; Writing—original draft, L.C.; Writing—review & editing, Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available within the article.

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

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7. [CrossRef]
2. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
3. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
4. Kraus, B.; Gisin, N.; Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **2005**, *95*, 080501. [CrossRef]
5. Gisin, N.; Thew, R. Quantum communication. *Nat. Photon.* **2007**, *1*, 165. [CrossRef]
6. Duĕk, M.; Lütkenhaus, N.; Hendrych, M. Quantum cryptography. *Prog. Opt.* **2006**, *49*, 381.
7. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802. [CrossRef]
8. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050. [CrossRef]
9. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **2001**, *48*, 351. [CrossRef]
10. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1. [CrossRef]
11. Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **1995**, *51*, 1863. [CrossRef] [PubMed]
12. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330. [CrossRef] [PubMed]
13. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
14. Liu, W.T.; Sun, S.H.; Liang, L.M.; Yuan, J.M. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution. *Phys. Rev. A* **2011**, *83*, 042326. [CrossRef]
15. Liu, D.; Wang, S.; Yin, Z.Q.; Chen, W.; Han, Z.F. The security of decoy state protocol in the partial photon number splitting attack. *Chin. Sci. Bull.* **2013**, *58*, 3859. [CrossRef]
16. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef] [PubMed]
17. Wang, X.B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
18. Lo, H.K.; Ma, X.F.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
19. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2011**, *2*, 349. [CrossRef]
20. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Scarani, V.; Makarov, V.; Kurtsiefer, C. Experimentally Faking the Violation of Bell's Inequalities. *Phys. Rev. Lett.* **2011**, *107*, 170404. [CrossRef]
21. Henning, W.; Harald, K.; Markus, R.; Martin, F.; Sebastian, N.; Harald, W. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. *New J. Phys.* **2004**, *13*, 073024.
22. Makarov, V.; Hjelme, D.R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 5. [CrossRef]
23. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313. [CrossRef]
24. Qi, B.; Fung, C.H.F.; Lo, H.K.; Ma, X.F. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **2007**, *7*, 73. [CrossRef]
25. Antonio, A.; Nicolas, B.; Nicolas, G.; Serge, M.; Stefano, P.; Valerio, S. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501.
26. Stefano, P.; Antonio, A.; Nicolas, B.; Nicolas, G.; Serge, M.; Valerio, S. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **2009**, *11*, 045021.
27. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
28. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 6. [CrossRef]

29. Liang, W.T.; Xue, Q.Y.; Jiao, R.Z. The performance of three-intensity decoy-state measurement-device-independent quantum key distribution. *Quantum Inf. Process.* **2020**, *19*, 165. [CrossRef]
30. Lu, F.Y.; Yin, Z.Q.; Fan-Yuan, G.J.; Wang, R.; Liu, H.; Wang, S.; Chen, W.; He, D.Y.; Huang, W.; Xu, B.J.; et al. Efficient decoy states for the reference-frame-independent measurement-device-independent quantum key distribution. *Phys. Rev. A* **2020**, *101*, 052318. [CrossRef]
31. Jiang, C.; Zhou, F.; Wang, X.B. Four-intensity measurement-device-independent quantum key distribution protocol with modified coherent state sources. *Opt. Express* **2022**, *30*, 7. [CrossRef] [PubMed]
32. Tang, Y.L.; Yin, H.L.; Chen, S.J.; Liu, Y.; Zhang, W.J.; Jiang, X.; Zhang, L.; Wang, J.; You, L.X.; Guan, J.Y.; et al. Measurement-Device-Independent Quantum Key Distribution over 200 km. *Phys. Rev. Lett.* **2014**, *113*, 190501. [CrossRef] [PubMed]
33. Zhou, Y.H.; Yu, Z.W.; Wang, X.B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **2016**, *93*, 042324. [CrossRef]
34. Gottesman, D.; Lo, H.K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325.
35. Ma, X.F.; Fung, C.H.F.; Dupuis, F.; Chen, K.; Tamaki, K.; Lo, H.K. Decoy-state quantum key distribution with two-way classical postprocessing. *Phys. Rev. A* **2006**, *74*, 032330. [CrossRef]
36. Tang, Z.T.; Liao, Z.F.; Xu, F.H.; Qi, B.; Qian, L.; Lo, H.K. Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2014**, *112*, 190503. [CrossRef]
37. Ma, X.F.; Fung, C.H.F.; Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 052305. [CrossRef]
38. Ma, X.F.; Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 062319. [CrossRef]

entropy

MDPI

Review

Introduction to Semi-Classical Analysis for Digital Errors of Qubit in Quantum Processor

Osamu Hirota [1,2,†]

[1] Quantum ICT Research Institute, Tamagawa University, Tokyo 194-8610, Japan; hirota@lab.tamagawa.ac.jp
[2] Reserch and Development Initiative, Chuo University, Tokyo 112-8551, Japan
† Current address: Quantum ICT Research Institute, Tamagawa University, 6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan.

Abstract: In recent years, remarkable progress has been achieved in the development of quantum computers. For further development, it is important to clarify properties of errors by quantum noise and environment noise. However, when the system scale of quantum processors is expanded, it has been pointed out that a new type of quantum error, such as nonlinear error, appears. It is not clear how to handle such new effects in information theory. First of all, one should make the characteristics of the error probability of qubits clear as communication channel error models in information theory. The purpose of this paper is to survey the progress for modeling the quantum noise effects that information theorists are likely to face in the future, to cope with such nontrivial errors mentioned above. This paper explains a channel error model to represent strange properties of error probability due to new quantum noise. By this model, specific examples on the features of error probability caused by, for example, quantum recurrence effects, collective relaxation, and external force, are given. As a result, it is possible to understand the meaning of strange features of error probability that do not exist in classical information theory without going through complex physical phenomena.

Keywords: communication channel error model; nonlinear error; burst error; cosmic ray; quantum Zeno effect

Citation: Hirota, O. Introduction to Semi-Classical Analysis for Digital Errors of Qubit in Quantum Processor. *Entropy* **2021**, *23*, 1577. https://doi.org/10.3390/e23121577

Academic Editor: Rosario Lo Franco

Received: 1 November 2021
Accepted: 23 November 2021
Published: 26 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

When an ideal architecture of quantum processor is available, quantum computers are theoretically predicted to have significantly higher computing power than conventional computers [1]. The Shor's algorithm is a prime example of its appeal, because it will bring the jeopardization of public key cryptography. A few years ago, the standardization of quantum computer-resistant cryptography [2] began in conjunction with the development of the quantum computer. In general, a quantum computer must consist of a combinatorial circuit of large number of quantum processors such as quantum gates and quantum memories. The recent demonstration of quantum transcendence by Google and IBM under the small number of qubits have sparked public interest in the real performance of quantum computers. Many people therefore expect a new prediction law based on the so called threshold theorem [3], that is comparable to Moore's law for classical computers. According to the theorem, the errors in quantum computers can be corrected by several quantum error correcting schemes [4–8], and it will take a similar evolutionary process to the classical computer from the current small-scale quantum computer. However, the situation is not so simple. Furthermore, one should clarify the characteristics of quantum noise from the viewpoint of information theory. In this article, I will demonstrate how to achieve this. I firstly present the most general classification of potential errors by quantum noise. From such a classification, one can see a new kind of error that the error probability of a qubit depends on number of qubits in a quantum processor. This comes from the quantum nature, and has been called "Nonlinear error" [9,10]. I then introduce concrete physical phenomena for such features discussed in physics articles [11–14]. However,

these phenomena are very complicated, and therefore, it is worthwhile to build an error model as an error in the communication channel model that can be understood without the detailed physical phenomena. Based on discoveries of a new type of error in the physics, I give the channel error model of error performance due to new quantum noise effects, and show several examples. This means to clarify properties of error probability, and it does not mean to discuss the concrete error such as bit error, phase error, and so on. This is important because there such strange properties of error probability do not exist in classical information theory [15–17], and such properties are also not taken into account in quantum error correction theory [4–8].

Let us here give the contents in this paper. Section 2 gives a classification of errors due to quantum noise effects in the information theoretic view. Section 3 introduces the basic equations for quantum noise analysis. Section 4 gives a review on physical examples of new quantum errors described in Section 2, which have been discovered recently. Section 5 shows concrete examples of strange features of error probability based on communication channel modeling. This provides a visualization of the strange error phenomena to researchers in information theory. Section 6 gives the error model and its features when the external force comes from the outside of the quantum processors, such as cosmic rays. Section 7 discusses an effect of the Quantum Zeno operation by external forces.

2. Information Theoretic View of Quantum Error

In a real system, the quantum computer operates as a time evolution of quantum states with noise, which brings an error in the digital processing. Therefore, one needs a method to mathematically model digital error due to the physical evolution of quantum states with noise. In this section, I classify the quantum noise effect by physical phenomena and give the corresponding information theoretic representation in order to make it easier for information theorists to participate. Here the information theoretic view of quantum error means to classify properties of error probability.

2.1. Phenomenal Classification of Quantum Noise

The quantum noise we are discussing here refers to the phenomenon of decoherence to quantum states. I list the classification of quantum noise in physics literature [18]:

1. Stochastic Pauli Noise: This corresponds to bit or phase flip errors of a single qubit.
2. Coherent Noise: No decoherence to a quantum state occurs, but it becomes an unintended quantum state.
3. Amplitude Damping: A specific example of decoherence, especially derived from energy loss.
4. Local correlated noise (Markov, non-Markov): This is an extension of Pauli noise, in which several qubits around the errored qubits are correlated to produce the error.
5. Non-local correlated noise (Markov, non-Markov):This has a potential to give an error for every qubit in the system with correlation.
6. The disentanglement noise: When the entanglement is released, it can be regarded as an error. These can be observed in an interaction with the environment, an interaction with other qubits, an imperfect gate, and also leakage, respectively. The details of these physical phenomena have been analyzed in physics. A list of references and a brief description of them are given in Appendix A.

The categorization of such noise for the information theory is important in order to proceed with a system design of the quantum computer. In particular, the effect of correlation based not only quantum but also on classical phenomena in quantum computing may cause a new type of error in the information theoretic view. The necessity of considering the correlated noise in the case of quantum computers is due to the following reasons. In the classical system, the semiconductor elements that make up a bit can be considered to be independent of each other. Next, the noise is additive, and errors in the execution of logical calculations are sufficiently practical to be analyzed only by the stochastic properties of the noise itself. As a result, almost all errors can be considered to be each bit independent

or, if correlated, very local. On the other hand, in a quantum computer, some qubits are combined by quantum correlations such as entanglements, so it may be unique that only some qubits make errors independently.

2.2. Information Theoretic Classification of Quantum Errors

In this subsection, I present an information theoretic classification of errors that occur in quantum computers, which is the main subject of this paper. In information theory, the probability of the occurrence of an error is an important parameter. The detailed nature of the physical phenomena that cause errors is not the main subject. Therefore, the errors due to quantum noise mentioned in the previous section can be modeled based on the characteristics of the error probability, depending on what properties the quantum error has.

2.2.1. Linear Individual Independent Error

Assume that N qubits are prepared. Errors shall occur separately and independently of each qubit. The basic error probability is set as $0 \leq p(error) \leq 1/2$ in the information theory. The worst case is $p(error) = 1/2$. When this probability does not depend on the number of qubits, it is referred to as linear. The single error probability and a basis of T error probability in N qubits are given as follows, respectively:

$$p(error) \equiv \eta_j = \eta^* \quad \forall j \in N \tag{1}$$

$$P_e(T) \propto {\eta^*}^T (1-\eta^*)^{N-T} \tag{2}$$

This is a standard error model in conventional information theory.

2.2.2. Nonlinear Individual Independent Error

Let us assume that N qubits are prepared and that errors occur separately and independently in each qubit. If the error probability of jth qubit depends on the number of qubits, it is referred to as the nonlinear error. It can be defined as follows:

$$p(error) = f(\eta^*, N) \equiv \eta_j(N) \tag{3}$$

where this means that the error probability is a function of a number of qubits N and an error rate η^* when only one qubit is prepared. When the concrete physical phenomena are analyzed, the above may be described as an approximation in some numerical regions for a physical setting as follows:

$$p(error) \sim \eta^* N^\alpha < \frac{1}{2} \tag{4}$$

This is valid for $\eta^* \ll 1$. α is a real number to approximate the representation of the feature of N dependence in the error probability. This nonlinear error is the most serious error in quantum computers. The physical examples will be introduced in Section 4.

2.2.3. Simple Burst Error Due to Correlation Phenomena

Linear Local Correlated and Non-Local Correlated Error

Assume that N qubits are prepared, and the subset T qubits are correlated to each other. Let us assume that one qubit of T qubits decays with the probability η^*, and let us assume that it does not depend on the number of qubits. However, if the T qubits collapse simultaneously due to one qubit decay, it is defined as a simple burst error. It is induced by correlation of neighboring (local) or arbitrary (non-local) qubits of the system. Then, the probability for the simple burst error is simply equal to the probability of one qubit error η^*, as follows:

$$P(burst) = \eta^* \tag{5}$$

This is the most simple description for burst error.

Nonlinear Local or Non-Local Correlated Error

N qubits are prepared. Let us assume that an error occurs in one qubit, ands then the error occurs in the neighborhood or the whole system by correlation. In addition, the probability of the error of a single qubit triggering it depends on the number of qubits, as in Equation (3), and the nonlinear burst probability can be described by

$$P(burst) = \eta_j(N) = f(\eta^*, N) \tag{6}$$

This is called the nonlinear correlated error.

2.2.4. Avalanche Burst Error and Accumulation Error

If one qubit makes an error, and the surrounding qubits make errors one after another based on classical correlation, I name this phenomenon an avalanche burst error. Such an error will be generated in a superconducting quantum computer when cosmic rays are irradiated to the system. Physical examples are discussed in Section 6. When the first error propagates to the next step in an iterative gate operation, or in an iterative calculation, with the assumption that the error accumulates in the quantum circuit, I define these phenomena as a propagation-accumulation error.

3. Basis of Quantum Noise Analysis

A quantum computation mechanism has a structure in which qubits in a QPU quantum processor unit are correlated, and a huge pure quantum state consisting of all qubits is unitarily evolved according to a program using the correlation. In other words, the whole QPU is considered to be monolithic. Therefore, the interaction between the pure state system and the environment, including the vacuum field, will inevitably cause the quantum states that carry information to become undesired quantum states, or to be destroyed. Then, simple bit-flip and phase flip (Pauli-flip type) errors similar to classical systems are rather exceptional, and quantum-specific errors can be the main ones. Therefore, in order to predict the realization of a large scale quantum computing mechanism, it is essential to elucidate the exact features of the noise itself by quantum noise analysis. The following is a starting point for this.

First, let X be a physical quantity representing a quantum bit, and let N_o be the noise operator representing the noise to a quantum bit. Here the interaction between qubits and the interaction between qubits and noise are quite different from the classical system. The analysis of characteristics of these interactions is called quantum noise analysis. The interaction is denoted by the interaction Hamiltonian H_{int}, which consists of X and $\mathcal{N}$. The Hamiltonian of the entire system is

$$H = H_X + H_{\mathcal{N}} + H_{int} \equiv H_0 + H_{int} \tag{7}$$

The quantum state representing the information evolves in time driven by the above Hamiltonian, but depending on the situation, either the Schrödinger equation on the extended Hilbert space or the following Lindblad equation [19]

$$\frac{\partial \rho}{\partial t} = \frac{-i}{\hbar}[H, \rho] + \sum_{n=1}^{N^2-1} (v_n \rho v_n^\dagger - \frac{1}{2}\{v_n^\dagger v_n, \rho\}) \tag{8}$$

is employed, where v_n is a Lindblad-decoherence operator. Currently, this equation is the most frequently utilized.

Assuming an actual general purpose program, further generalization to include measurement systems is needed, not only models of decoherence systems as described in the previous section. As a generalization, a generalized stochastic Schrödinger equation [20] may be applicable. However, it is very hard to handle for calculation. Therefore, I simply employ the semi-classical stochastic differential equation, which is a simplification of the generalized stochastic Schrödinger equation. See Appendix A.

4. Review of Physical Examples of a New Type of Quantum Noise

This section introduces physical examples [11–13] of the error model categorized in Section 2. However, since physical phenomena are so complex, we exclude physical rigor and emphasize the logic that arrives at each error model. That is, the main objective is to show that the strange error characteristics in Section II exist in reality, or rather, that they may be the main noise in a certain type of quantum computers.

4.1. Hutter-Loss Recurrence Effect

Let us consider a model in which a group of qubits combined by quantum correlations, such as surface code, are interacted to the heat bath of a considered environment. There are many physical mechanisms available, such as direct interactions between each qubit and the heat bath, or non-Markovian interactions mediated by the heat bath. However, let us focus on the simplest of phenomena. That is, only bit-flip (σ^x) for X is subject to error, the heat bath is in thermal equilibrium at the onset with the Hamiltonian $H_{\mathcal{N}} = \sum_k \hbar\omega_k a_k^\dagger a_k$. Then the interaction Hamiltonian may be given by

$$H_{int} = \sum_j \sigma_j^x \otimes \sum_{\{k\in\mathbf{k}\}} |k|^r \frac{\lambda}{\sqrt{M}} (e^{ikR_j}\hat{a}_k + e^{-ikR_j}\hat{a}_k^\dagger) \tag{9}$$

R_j means the spatial position of the qubit, M is the total number of modes, $k \in \mathbf{k}$ is the wave number of modes, $r = 0, \pm 1/2$. Next, consider how a given jth qubit evolves as it interacts with the heat bath, where j of R_j is the number of modes. If the initial state of the system is $\rho_S \otimes \rho_{\mathcal{N}}$, then its decoherence evolution is expressed by using the Lindblad equation Equation (8) as follows [13]:

$$\rho_S \longmapsto \Phi_e(\rho_S) = Tr_{\mathcal{N}}\{e^{-iHt}(\rho_S \otimes \rho_{\mathcal{N}})e^{iHt}\} \tag{10}$$

ρ_S is a density operator of all signal systems connected by correlation. Here, the operation in the measurements is added, such as

$$\Psi_\Pi(\sigma) = \sum_{\mathbf{a}} \Pi_{\mathbf{a}} \sigma \Pi_{\mathbf{a}} \tag{11}$$

Then the density operator for jth qubit becomes as follows:

$$\rho_j(t) = Tr_{k\neq j} \circ \Psi_\Pi \circ \Psi_e(\rho_S) = (1 - \eta_j(t,N))\rho_j + \eta_j(t,N)\sigma_j^x \rho_j \sigma_j^x \tag{12}$$

where $\eta_j(t,N)$ is the error probability of the jth single qubit in a population of N qubits. From this formula, for a set with quantum correlations, the influence from all other qubits result in the following properties.

$$\eta_j(t,N+1) = \cos^2(J_{1,N+1})\eta_j(t,N) + \sin^2(J_{1,N+1})(1 - \eta_j(t,N)) \tag{13}$$

where

$$J_{m,n} \sim \lambda^2 \int dk \frac{|k|^{2r}}{\omega_k^2} \times \cos(k(R_m - R_n))(\sin(\omega_k t) - \omega_k t) \tag{14}$$

As a result, Hutter-Loss pointed out [13] that the error probability for jth qubit can be described by

$$p(error) \propto \eta_j(t,N) \equiv f(t,\eta^*,N) \tag{15}$$

The specific form of the dependency of N in the above equation is given by the formulae in Equation (34) based on the semiclassical analysis. Thus, this phenomenon induces a N-dependence of the error probability. Here I refer it as Hutter–Loss effect.

4.2. Collective Decoherence Effect

Here I would like to introduce another example for a new type of quantum noise. In general, one can consider a collective decoherence such as generalized Dicke super radiation. Let N atoms of a two-level system be qubits. Then one can assume more general discussion than the standard assumption that the wavelength of the radiation field is longer than the size of the qubit population in the interaction with the continuous mode field. The system can therefore be in the super radiant region. In general, the Wigner–Weisskopf theory is applied [21], and the interacting Hamiltonian, such as generalized Dicke super radiation, is given as follows:

$$H_{int} = -\sum_{j}\sum_{n}\hbar\kappa_n(\hat{a}_n\sigma(+)_j + \hat{a}_n^{\dagger}\sigma(-)_j) \tag{16}$$

where $\sigma(z)_j = |e\rangle_{jj}\langle e| - |g\rangle_{jj}\langle g|$, $\sigma(+)_j = |e\rangle_{jj}\langle g|$, $\sigma(-)_j = |g\rangle_{jj}\langle e|$. Initially, the qubit system is assumed to be superimposed and the field is a vacuum. The initial state of the two coupled systems is given by

$$|\Psi(t=0)\rangle = \sum_{m=0}^{2^N-1} c_{m,0}|m,0\rangle \tag{17}$$

Here let us show a physical analysis given by Lemberger and Yavus [11,12]. From the Schrödinger equation in the extended Hilbert space of the coupled system, the time evolution is

$$|\Psi(t)\rangle = \sum_{m=0}^{2^N-1} c_{m,0}(t)e^{-i(N_m\omega_a)t}|m,0\rangle + \sum_{n}\sum_{m'}^{2^N-1} c_{m',n}(t)e^{-i(N_{m'}\omega_a+\nu_n)t}|m',1_n\rangle \tag{18}$$

It can be assumed that $N/2+\bar{N}$ are the excited state and $N/2-\bar{N}$ are the ground state among N qubits. $\bar{N}$ is the average number. The equation of motion for the stochastic amplitude of the point of interest in the above equation is given as follows.

$$\frac{dc_{m,0}}{dt} = -(\frac{\Gamma}{2}+\delta\omega)(\frac{N}{2}+\bar{N})(\frac{N}{2}-\bar{N}+1)c_{m,0} \tag{19}$$

where Γ and $\delta\omega$ are the single decay rate and Lam shift, respectively. From the above, the decay of the probability amplitude of the representative point of interest is as follows.

$$|c_{m,0}(t)|^2 \sim |c_{m,0}(t=0)|^2 e^{-(N^2/4)\Gamma t} \tag{20}$$

The above equation is applicable to the majority of stochastic amplitudes for N qubits and it represents a feature of super-radiance. Since super-radiance implies the simultaneous decay of the majority of qubits, one can consider this super-radiance as a cause of error. Lemberger and Yavus analyzed how the decay rate of only certain qubits is affected by other qubits based on the above theory. In order to make the features easier to see, the initial state is set as follows.

$$|\psi(t=0)\rangle = \sum_{m=0}^{2^{N-1}-1} c_{m,0}|g\rangle_j \otimes |m,0\rangle + \sum_{m=0}^{2^{N-1}-1} d_{m,0}|e\rangle_j \otimes |m,0\rangle \tag{21}$$

where m corresponds to an indicater of the quantum state of a qubit of $N-1$ other than jth qubit. If the density operator on the composite space is $\rho = |\psi\rangle\langle\psi|$, then the density

operator of jth qubit is obtained by tracing this density operator over a qubit fraction of $N-1$. The result is

$$\rho_j = \sum_{m=0}^{2^{N-1}-1} |c_{m,0}|^2 |g\rangle_{jj}\langle g| + \sum_{m=0}^{2^{N-1}-1} |d_{m,0}|^2 |e\rangle_{jj}\langle e| + \sum_{m=0}^{2^{N-1}-1} c_{m,0} d^*_{m,0} |g\rangle_{jj}\langle e| + \sum_{m=0}^{2^{N-1}-1} c^*_{m,0} d_{m,0} |e\rangle_{jj}\langle g| \quad (22)$$

In the initial state, if the qubit of j is excited, N qubits radiate at once. On the other hand, if it is on the ground, the qubits of $N-1$ radiate at the same time. As a result,

$$|c_{m,0}(t)|^2 \sim |c_{m,0}(t=0)|^2 e^{-((N-1)^2/4)\Gamma t} \quad (23)$$

$$|d_{m,0}(t)|^2 \sim |d_{m,0}(t=0)|^2 e^{-(N^2/4)\Gamma t} \quad (24)$$

where Γ is a function of η^*. From the above, Lemberger and Yavus [11,12] showed that as the subsection IV A, the error probability of the jth qubit at gate time δt can be described by

$$p(error) = f(\eta^*, N) \sim \frac{1}{2}\Gamma N^2 < \frac{1}{2} \quad (25)$$

The above formula is valid when $\Gamma \ll 1$, because of physical approximation. This phenomenon is non-local. I would like to emphasize that this causes a burst error to the whole system with the same probability as the above equation.

4.3. Leak from Decoherence Free Subspace Due to Collective Decoherence

One can use a decoherence free subspace (DFS) [22] to avoid an error in the system that interacts with a heat bath. The evolution for the traced density operator is given by the Lindblad equation in general. Let the Hilbert space of the system of quantum bits be $\mathcal{H}_S$ and all density operators on it be $D(\mathcal{H}_S)$.

Definition 1. *A decoherence free subspace : $\mathcal{H}_{DFS}$ is a subspace of $\mathcal{H}_S$ in which all density operators $\rho \in D(\mathcal{H}_{DFS})$ defined in that space satisfy the following equation.*

$$\frac{\partial \rho}{\partial t} = \frac{-i}{\hbar}[H, \rho] \quad \forall t \quad (26)$$

In other words, it is equivalent to the absence of the effect of the Lindblad operator in Equation (8). The alternative way of characterizing the DFS is to consider all possible of singlet states

$$|\Psi(j,k)\rangle_{DFS} = \frac{1}{\sqrt{2}}(|e\rangle_j \otimes |g\rangle_k - |g\rangle_j \otimes |e\rangle_k \quad (27)$$

However, Lemberger and Yavus pointed out that there exists a phenomenon of the leak from DFS when collective decoherence occurs [11,12]. The decay rate of the stochastic amplitude at this time is interpreted as the rate at which the system leaks from the decoherence free subspace into a large extended Hilbert space. As a result, the leak probability is regarded as follows.

$$P_{(Leak)}(t) \sim \Gamma \delta t N^2 \quad (28)$$

where $\Gamma \ll 1$. This causes also nonlinear error depending on the number of qubits, and also it gives the burst error.

5. Communication Channel Modeling of Quantum Errors Due to Quantum Correlation

In the former sections, I have introduced new error phenomena due to quantum noise which depend on the number of qubits. Although the main concern in physical analysis

is to discuss the decay rate by interaction with environments, in the discussion of the information theory for error correction, one needs to know the feature of error probability of information by the decay process. Phenomena of quantum decay by quantum noise depending on the number of qubits means the increasing of error probability by a quantum correlation. There is no such phenomenon in the conventional information theory. In this section, I give a model for error phenomena due to the above quantum phenomena by using classical probability. As a result, researchers of information theory can well understand such strange error phenomena in quantum computers.

5.1. Semi-Classical Modeling of Quantum Bit Array Structure

When a group of qubits is placed in a given environment, it was pointed out in the above section that an increase in the number of qubits enhances the error probability of one of its components. Here, I attempt to describe such quantum phenomena using only information theoretic concepts [15–17], leaving out the physical processes. Since our concern is to characterize the error probability, the causes of error such as bit error, phase error, entanglement error, and so on, are not considered. In this case, one can think of a qubit as just a bit, and a model as a two-dimensional arrangement of bits and the interaction of error factors from the environment with the qubits.

Let us assume that i, j are positions of N qubits on the two dimensional surface. Then, let us describe the qubits by the information bit $x_{(m,n)}$ of the spatial position (m, n). And $e_{(m,n)}$ means the error bit for that information bit. So one can employ the following representation:

$$\begin{pmatrix} x_{(1,1)} \bigoplus e_{(1,1)}, \ldots x_{(1,N)} \bigoplus e_{(1,N)} \\ x_{(2,1)} \bigoplus e_{(2,1)}, \ldots x_{(2,N)} \bigoplus e_{(2,N)} \\ \vdots \ldots \\ x_{(N,1)} \bigoplus e_{(N,1)}, \ldots x_{(N,N)} \bigoplus e_{(N,N)} \end{pmatrix} \tag{29}$$

The quantum correlations among qubits are described by the coupling probability $p_{(m^*,n^*),(m,n)} \equiv p_{j,k}$, $j, k \in N$ among error bits in this modeling. Here I emphasize the fact that only the probabilistic nature of the error is an essential factor as the first stage in the information theoretic analysis. Of course, in the design stage of the quantum error correction scheme, one needs more detailed physical characterization. However, this is beyond the scope of this paper. The reason is that if the kind of noise discussed here occurs, consideration of the error correction mechanism loses its meaning.

5.2. Semi-Classical Description of Nonlinear Local Correlated Errors

I discuss here the nonlinear errors due to local quantum correlation. One qubit at center position $x_{(m^*,n^*)}$ in two dimensional space is prepared and several qubits N_{sub} of N are put around the first qubit with quantum mechanical correlation. Let us assume that the decay rate of the center qubit is assumed as η^* when it is a single. If the error probability of the center qubit due to the interaction among other quabits is given by

$$p(error) = f(\eta^*, N_{sub}), \tag{30}$$

then this is the nonlinear error due to local quantum correlation. To verify this feature of error, I deal with the recurrence effect introduced in the section IV A . Let us assume that the Hutter–Loss effect occures in the quantum processor. Hutter–Loss [13], as the first step of the recurrence effect, gave a semi-classical description of error performance for own phenomena on the recurrence effect as follows. The probability of error of the center qubit is $\eta_{m,n} = \eta^*$. Let $N_{sub1} = 5$ be a subset of qubits which are set around the first qubit . Let the latent probability (correlation) of an error-induced in pairwise with the center and one

of four qubits be $0 \leq p_{(m^*,n^*),(m,n)} \equiv p_1^* \leq 1/2$. In this case, the error probability of the center qubit in subset ($N_{sub1} = 5$) is given by the following [13]:

$$\begin{aligned} p(error) &= \eta^* \sum_{q:even} \frac{4!}{q!(4-q)!}(p_1^*)^q(1-p_1^*)^{4-q} \\ &+(1-\eta^*) \sum_{q:odd} \frac{4!}{q!(4-q)!}(p_1^*)^q(1-p_1^*)^{4-q} \\ &= \frac{1}{2} - \frac{1}{2}(1-2\eta^*)(1-2p_1^*)^4 = \frac{1}{2} - \frac{1}{2}(1-2\eta^*)\Lambda_1 \\ &\equiv \eta_1^* \geq \eta^* \end{aligned} \tag{31}$$

where $\Lambda_1 = (1-2p_1^*)^4$. This is an example of the nonlinear error, because it is greater than η^*. This shows that the error is not changed when $p_1^* = 0$. It means that there is no correlation among qubits.

The above is just one step for the scalable system. To understand the recurrence phenomena, let us consider a more complicated structure of correlated qubits in general processors, with an extension of the above formula. Let us add four qubits to the initial five qubits, and let the latent probability (correlation) of an error-induced in pairwise with the center and one of new four qubits be $0 \leq p_2^* \leq 1/2$, respectively, based on operation gate such as control NOT. From the recurrence phenomena, the error probability for the qubit in the center has to employ the initial probability η_1^* given by the Equation (31) instead of η^*. That is, η^* is replaced by η_1^*, and p_1^* is replaced by p_2^* in Equation (31). Then one gets the following

$$\begin{aligned} p(error) &= f(\eta_1^*, N_{sub2}) = \eta_1^* \sum_{q:even} \frac{4!}{q!(4-q)!}(p_2^*)^q(1-p_2^*)^{4-q} \\ &+(1-\eta_1^*) \sum_{q:odd} \frac{4!}{q!(4-q)!}(p_2^*)^q(1-p_2^*)^{4-q} = \frac{1}{2} - \frac{1}{2}(1-2\eta_1^*)(1-2p_2^*)^4 \end{aligned} \tag{32}$$

Here $\Lambda_2 = (1-2p_2^*)^4$. So, the above becomes as follows:

$$p(error) = f(\eta^*, N_{sub2}) = \frac{1}{2} - \frac{1}{2}(1-2\eta^*)\Lambda_1\Lambda_2 \tag{33}$$

Let us repeat the same operation. One needs to replace the initial probability and the latent probability of an error-induced in pairwise in each operation. Finally one gets the following

$$p(error) = f(\eta^*, N_{subK}) = \frac{1}{2} - \frac{1}{2}(1-2\eta^*)\prod_{l=1}^{K}\Lambda_l \tag{34}$$

where $\Lambda_l = (1-2p_l^*)^4$, and $l = \{1, 2, \ldots, K\}$. When one constructs the structure based on the steps of K times, the error probability of each qubit increases with respect to K. This model provides a visualization of the new type of quantum error due to the recurrence effect, and clarifies a curious feature of the nonlinear error. That is, despite the nature of the quantum noise from the environment as being invariant, the probability of its own error increases when qubits are clustered together. As a special case, when K is increased, one has following characteristics:

$$p(error) = f(\eta^*, N_{subK}) = \eta^*, \quad p_l^* = 0 \quad \forall l \tag{35}$$

$$p(error) = \eta_j(N_{subK}) \to \frac{1}{2}, \quad p_l^* \neq 0, K \gg 1 \tag{36}$$

5.3. Semi-Classical Description of Nonlinear Non-Local Correlated Errors

The decoherence by nonlocal correlation among all qubits such as super radiance is alsoa serious phenomena in quantum processors. This phenomenon was explained in Section 4.2. The problem is how to describe such a decoherence based on a communication channel model for information theory. It is known that a qubit can be classically viewed as a radiating dipole at the frequency of the qubit transition. This radiating dipole produces an electric field at the position of the qubit. This electric field interacts with whole qubits and induces unwanted rotation of the qubit state. The decay rate of dephasing by this rotation can be modeled by the Rabi frequency due to the electric field. The value is proportional to the electric field. The Rabi frequency of the j-th qubit affected by all qubits is given by the incoherent sum from each emission of the other qubits.

Here I give a model for nonlinear error and burst error in the case when a qubit at a certain position $x_{(m^*,n^*)}$ of Equation (29) interacts, based on the quantum mechanical method with whole qubits. Let the qubit at $x_{(m^*,n^*)}$ be the jth qubit. Then, $\gamma_{m^*,n^*} \equiv \gamma_j^*$ is the decay rate of the qubit at x_{m^*,n^*} due to an effect of that interaction, and let us assume that N_{super} is the number of qubits in a region of super radiance. Then, the interaction efficiency amongst all the qubits can be described by $0 \leq \nu_{(m^*,n^*),(m,n)} \equiv \nu_{j,k} \leq 1$, where $j,k \in N_{super}$.

The decay rate of the jth qubit due to the interaction between the position x_{m^*,n^*} and all the existing qubits is modeled as the sum of each decay rate from an analogy of Rabi oscillation coupling as follows:

$$\gamma_j(N_{super}) = \sum_{k=1,k\neq j}^{N_{super}} \nu_{j,k}\gamma_j^* \tag{37}$$

Thus, the error probability of jth qubit due to its interaction during Δt is defined as follows:

$$p(error) = \frac{1}{2}(1 - \exp\{-|\gamma_j(N_{super})|^2\}) \quad \forall j \tag{38}$$

As one can see, the above model provides a way to understand the origin of nonlinear effects in the error performance, which depends on the number of qubits. When $\nu_{j,k} = 1, \forall j,k$, it corresponds to the Lembeger–Yavus super radiance decay, which is introduced in Section 4.2. Let us consider the physical counterpart in Section 4.2 of the above equation. The correspondence between γ_j^* and the physical decay rate Γ corresponds to $(\gamma_j^*)^2 = \Gamma$. When $\Gamma \ll 1$ (good quality), and there is no super radiance, the error probability is nearly zero. However, even if $(\gamma_j^*)^2 = \Gamma \ll 1$, when the super radiance occurs, the concrete form of the Equation (42) can be approximated as follows:

$$p(error) \cong \frac{1}{2}\Gamma N_{super}^2 < \frac{1}{2} \tag{39}$$

It is valid for $\Gamma \ll 1$ and for finite N_{super}. This matches the result of the Lembeger–Yavus super radiance decay. On the other hand, when the number of qubits of super radiance is large, or Γ is large, the error probability goes to $1/2$.

In addition, when super radiance occurs, the correlation consists of all the qubits. This fact drives a serious error such as burst error, in which all qubits are destroyed simultaneously with the following probability:

$$P_e(burst) \cong \frac{1}{2}\Gamma N_{super}^2 \tag{40}$$

6. Communication Channel Modeling of Quantum Error Due to External Forces

6.1. Physical Reality of External Force Such as Cosmic Rays

I have been discussing the decay effects of the interaction of a particular qubit with the environment in a quantum processor. On the other hand, a similar error occurs through interaction with external forces by particles coming from outside the systems. These include cosmic ray from space, γ-ray and charged particles from laboratory environments. Occurrence of such a case was pointed out by Vepsalainen et al. [23] in the case of superconducting quantum computers. Here let p_{ex} be the probability that one qubit in the system is hit by an external force. In this case, the error probability in our model Equation (1) for one qubit is modified by replacing the initial error rate η^* as follows:

$$\eta^*_{ex} = \eta^* + p_{ex} \tag{41}$$

When this occurs, a burst error occurs in addition to the above. This phenomenon has been experimentally demonstrated in superconducting quantum computers by Wilen et al. [24]. In this section, let us discuss a model for a burst error by such phenomena.

6.2. Communication Channel Error Model Due to Environment Correlation

In Section 4, I discussed the correlated error by quantum correlation and clarified the formulation of nonlinear error. There are no such phenomena in the classical world. Even if there is no quantum correlation among the qubits, the correlation among the qubits exists in superconducting quantum computers. That is, the charge field of qubits or other parameters may have the potential to generate a correlation, or the environment itself may generate the correlation among qubits. In fact, the discovery of long-range two-qubit correlations has been reported [24,25]. Thus, one has to consider the communication channel model for error propagation of qubits due to classical correlation. Although the physical phenomena of the interaction between qubits and environment are very complicated, let us simplify this situation. Assume that $p_{(k|j)}$ is the conditional probability that qubit k is affected when an error of qubit j is caused by an external force. The total scheme is described on two dimensional constellation of qubits by

$$\begin{pmatrix} p_{(1|1)}, \cdots, p_{(1|N)} \\ p_{(2|1)}, \cdots, p_{(2|N)} \\ \vdots \cdots \\ p_{(N|1)}, \cdots, p_{(N|N)} \end{pmatrix} \tag{42}$$

These conditional probabilities correspond to correlations among electric charge fields of qubits.

Here the burst error caused by external force is described as follows: One of the qubits makes an error due to a collision with an external particle, then the other many qubits make errors in conjunction with that error. Let us deal here with a simple example. If the ripple effect on qubits is the most simple, then the burst probability is given by only conditional probabilities on the j-th qubit as follows:

$$P(burst) = \eta^*_{ex} \prod_{k \neq j} p(k|j) \quad \forall k \quad p(k|j) \neq 0 \tag{43}$$

The other is a chain of errors like a Markov chain, in which the error in the j-th qubit propagates to the i-th qubit, and then the error in the i-th qubit propagates to the k-th qubit, and so on. One can define it as the avalanche burst effect. In this case, the avalanche burst probability can be approximated by

$$P(burst) \sim \eta^*_{ex} p^*(k|j) p^*(l|k) \cdots \tag{44}$$

where $p^*(k|j)$ implies the maximum probability of the transition from j to k. The parameters to control such effects are η^*, and the correlation through the electric field around the superconducting qubit. If the ripple effect is more complex, then one should consider all the qubits in quantum processors to be collapsing. However, the experimental results of error propagation in the reference [23–25] may be analyzed with the above modeling.

In order to reduce such effects, one should design the circuit such that correlations among electric charge fields of qubits in the superconducting quantum computers are eliminated.

7. Communication Channel Modeling of Quantum Error in Operations

If an initial quantum state of a qubit decays to the vacuum state, it becomes an error of the quantum computer. So one can consider the physical protection of the decay of qubits to avoid such errors. The quantum Zeno effect is a typical example of a methodology for keeping a qubits in a normal state [26,27]. The use of this phenomena to stabilize qubits in quantum processors has been proposed by Franson's group [28]. In this section, we analyze the external noise effect for such artificial operations.

7.1. Collapse of Quantum Zeno Effect for Single Qubit

In conventional theory with the ideal environment, the quantum Zeno effect is described by the survival probability of the initial state as follows [26,27]:

$$P(\delta t) = |\langle\psi|e^{-iHt}|\psi\rangle|^2 \approx 1 - (\frac{\delta t}{\tau_z})^2 \tag{45}$$

where $\delta t \ll 1$, H is the total Hamiltoniann of the system and the Zeno time is $\tau_z^2 = \langle\psi|H_{int}^2|\psi\rangle$. Then the survival probability at time t after the Jth measurements is

$$P_{(J)}(t) = P(\delta t)^J \approx [1 - (\frac{\delta t}{\tau_z})^2]^J \tag{46}$$

If one assumes that t is fixed and the time interval $\delta t = t/J$, one has a convenient formula of the above relation as follows:

$$P_{(J)}(t) = P(\delta t)^J \approx 1 - \frac{1}{J}(\frac{t^2}{{\tau_z}^2}) \to 1, \quad 1 \ll J \tag{47}$$

Thus the initial state is kept. This is called the quantum Zeno effect. However, in the general or non ideal environment of quantum computers, it has been pointed out that the quantum Zeno effect may be eliminated.

Since my purpose is to formulate in the sense of information theory, I do not describe the exact physical model. I employ here the stochastic Schrödinger equation discussed by Adler and Diosi ([29], also see Appendix B).

$$d|\Psi\rangle = -iH|\Psi\rangle dt - V_r^2(H - < H >)^2|\Psi\rangle dt + V_r(H - < H >)|\Psi\rangle dW_t \tag{48}$$

where H is the Hamiltonian, $< H > = \langle\Psi|H|\Psi\rangle$. V_r is a parameter governing the strength of an external force. Here one can employ the standard theory of the stochastic processes [30,31]. dW_t is an Itô stochastic differential together with dt, and it obeys the Standard Itô calculus rules as follows:

$$dW_t^2 = dt, \quad dW_t dt = dt^2 = 0 \tag{49}$$

where the Wiener process is

$$W_t = \int_0^t dW_t \tag{50}$$

In Itô calculus, the following formula is used.

$$d(AB) = (A + dA)(B + dB) - AB = (dA)B + AdB + dAdB \tag{51}$$

Thus, the next relation is given.

$$d\exp(bW_t) = \exp(bW_t) < bdW_t + \frac{1}{2}b^2dt > \tag{52}$$

where b is a real number. Then one has

$$d < \exp(bW_t) > = < \exp(bW_t) > \frac{1}{2}b^2dt \tag{53}$$

$$< \exp(bW_t) > = \exp(\frac{1}{2}b^2t) \tag{54}$$

The equation for the density operator $\rho = |\psi\rangle\langle\psi|$ is given by

$$\begin{aligned} d\rho &= (d|\psi\rangle)\langle\psi| + |\psi\rangle d\langle\psi| + d|\psi\rangle d\langle\psi| \\ &= i[\rho, H]dt - V_r^2[H,[H,\rho]]dt + V_r[\rho,[\rho,H]]dW_t \end{aligned} \tag{55}$$

Based on the above equation, the Adler and Diosi gave the following formula [29].

$$P(\delta t) \approx 1 - \frac{1}{\tau_z^2}(V_r^2\delta t + \delta t^2) \tag{56}$$

Let us assume here that t is fixed. One can describe the survival probability at the artificial operations as follows:

$$P_{(J)}(t) = P(\delta t)^J \approx 1 - \{\frac{{V_r}^2}{{\tau_z}^2}t + \frac{1}{J}(\frac{t^2}{{\tau_z}^2})\} \tag{57}$$

The survival probability decreases with respect to t even if one operates any measurement, because the second term is independent of J. Following the above results, one can formulate the system failure probability of the artificial operation to protect the qubits as follows:

$$P_f = 1 - P(\delta t)^J \approx \frac{{V_r}^2}{{\tau_z}^2}t \quad < 1 \tag{58}$$

The above formulae are valid only for $t \ll 1$ in the perturbation approximation in physical analysis. As a result, the failure performance is mainly described by a single parameter V_r. This is very useful for information theorists who are not interested in the detailed physical process.

7.2. Collaps of Quantum Zeno Effect for Qubits with Correlation

Here I discuss the scheme of a system of several qubits with quantum correlation, such as entanglement. In general, when the conventional environment is employed, an entangled state between qubits $j = 1$ and 2 in memory can be protected by applying the Zeno effect in a composite system of qubits and environment. That is, let us consider a series of non selective measurements on the qubits performed at time interval δt. These have the following properties. One is the projection onto the collective ground state $|\phi >_G = |0 >_1 |0 >_2$, and the other is that the measurement cannot distinguish between $|1 >_1 |0 >_2$ and $|0 >_1 |1 >_2$. These measurements disentangle the qubits from the environment at each time δt. The survival probability is given by the same formula Equation (61) of the case of single qubit.

Let us consider the non-ideal environment. I consider the N qubits system with quantum correlation with each other. When one employs a general Zeno effect operation on all the qubits, if the environment for all qubits is the ideal case, one can use the protection scheme of the system. Let us assume that an environment becomes a general or non-ideal environment for a single qubit in N qubits. That is, the stochastic coupling parameter by external force V_r for a certain qubit is non zero. Then, the qubit in the non-ideal environment suffers the same effect as the case of the single qubit, such as in Equation (58).

Hence one cannot deny the possibility that the whole system is destroyed, because all the qubits have quantum correlations. Thus, the system failure probability for the whole system can be evaluated by

$$P_f(Nqubits) \approx \frac{V_r^{*2}}{\tau_z^2} t \quad < 1 \tag{59}$$

This is valid for $t \ll 1$. The concrete value of V_r^* should be determined by the concrete physical analysis, but the physical structure is not so important for the information theory.

8. Conclusions

In this paper, a new type of error performance, the so called nonlinear error, where the error probability for a single qubit depends on the number of qubits in the system, has been discussed. I have shown how to model such strange properties of error probability based on a semi-classical method. Then it has been clarified that nonlinear errors give serious degradations of the capability of quantum computer, by the recurrence effect due to quantum correlation and also by collective decoherence . In order to cope with the quantum errors described in this paper, or to avoid this situation, one method is to further develop the conventional quantum error correction theory based on quantum noise analysis, or to establish a new way to physically suppress such errors [32–34]. Recently, a number of previously unknown and extremely difficult challenges in the development of an error correctable quantum computer have been reported [35–38]. However, I believe that the ideal quantum computer will be realized in the future. I expect that this paper may provide some hints for finding a way toward the ideal quantum computer.

Finally, I would like to point out that it is difficult to predict the realization of a quantum computer capable of cryptanalysis. However, because my results suggest that the capability of a real quantum computer is strictly limited, one can say that the current cryptography is not subject to the danger posed by current quantum computers. However, one should develop quantum computer-resistant cryptosystems based on mathematical analysis [39,40], or by physical cipher on the assumption that an ideal quantum computer or new mathematical discovery can be realized in the future.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A. Physical Research of Decoherence and Disentanglement Phenomena

The decoherence issue is of great significance for the foundations of quantum physics, as well as for problems of practical interest, such as quantum engineering. In the past two decades, it has become increasingly clear that many of the symptoms of classicality can be induced in quantum systems by their environments. Furthermore, issues of disentanglement and quantum discord are the same subjects as decoherence. The fundamental discussions on these physical phenomena have been given by Zurek [41] and Yu et al. [42,43]. The mathematical foundation for such issues belongs to the open system theory in quantum mechanics. The detailed analysis based on the open system theory for recent topics have been given by Lo Franco et al. [44], de Vega et al. [45], Bellomo et al. [46], and Aaronson et al. [47], respectively. Moreover, the experimental justification has been discussed by Rotter et al. [48]. Readers who are interested in the physical problem of decoherence and quantum noise in quantum processing, including quantum computing, can obtain detailed scientific knowledge from the above references.

Appendix B. From Lindblad Equation to Semi-Classical Stochastic Differential Equation

In general, dissipative processes in physical systems are governed by complete positive maps, and dynamical semigroup theory plays an important role. Complete positive maps $\hat{X} \to T(\hat{X})$ is described by a Kraus representation $T(\hat{X}) = \sum A_n \hat{X} A_n$. However, in order to analyze dynamic processes, it is necessary to shift the mathematical system to infinitesimal analysis. The time evolution of a fully positive statistical operator is described by the following Lindblad equation, which is an embodiment of Equation (8).

$$\mathcal{L}\rho = \frac{-i}{\hbar}[H, \rho] + \sum_{n \in N} [v_n \rho v_n^\dagger - \frac{1}{2}\{v_n^\dagger v_n, \rho\}] \tag{A1}$$

The relationship between the $v_n \rho v_n^\dagger$ terms can be understood by identifying v_n : the fast-varying component of A_n with a strength of $(dt)^{1/2}$. This fact may enable us to understand the Lindblad equation in the context of stochastic differential equations [29]. From the standard treatment of quantum noise [31], one can begin by mapping A_n to the following

$$\begin{aligned} A_n &= d_n + u_n dt + v_n dW_t^n \\ A_n^\dagger &= d_n + u_n^\dagger dt + v_n^\dagger dW_t^n \end{aligned} \tag{A2}$$

where d_n is a positive number and, W is the Wiener process. dW_t^n has the following properties from Itô calculus.

$$dW_t^m dW_t^n = c^{mn} dt, \quad dW_t^m dt = 0 \tag{A3}$$

where c is real symmetric covariant matrix, and its diagonal elements are $e^{nm} = 1, \forall n$. Let us consider that the complete positive map is described by

$$\rho \to \rho + d\rho = T(\rho) \tag{A4}$$

The we have the following relation from the above explanations.

$$\begin{aligned} \rho + d\rho &= \sum_{n \in N} (d_n + u_n dt + v_n dW_t^n)\rho(d_n + u_n^\dagger dt + v_n^\dagger dW_t^n) \\ &= \sum_{n \in N} d_n^2 \rho + \sum_{n \in N} d_n (v_n \rho + \rho v_n^\dagger) dW_t^n + (\rho U^\dagger + U\rho + \sum_{n \in N} v_n \rho v_n^\dagger) dt \end{aligned} \tag{A5}$$

where $U = \sum_{n \in N} d_n u_n, \sum d_n^2 = 1$. Then we have the form of the stochastic differential equation as follows:

$$d\rho = \sum_{n \in N} d_n (v_n \rho + \rho v_n^\dagger) dW_t^n + (\rho U^\dagger + U\rho + \sum_{n \in N} v_n \rho v_n^\dagger) dt \tag{A6}$$

When one takes the partial trace with respect to the disturbance, it becomes as follows:

$$dE[\rho] = E[d\rho] = (E[\rho]U^\dagger + UE[\rho] + \sum_{n \in N} v_n E[\rho] v_n^\dagger) dt \tag{A7}$$

This is equivalence to the Lindblad equation as follows:

$$\frac{dE[\rho]}{dt} = \frac{-i}{\hbar}[H, E[\rho]] + \sum_{n \in N} (v_n E[\rho] v_n^\dagger - \frac{1}{2} v_n^\dagger v_n E[\rho] - \frac{1}{2} E[\rho] v_n^\dagger v_n) \tag{A8}$$

where v_n, $v_n^\dagger$ correspond to Lindblad operator.

References

1. National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects*; Grumbling, E., Horowitz, M., Eds.; The National Academies Press: Washington, DC, USA, 2019.

2. National Institute of Standards and Technology. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Processes*; National Institute of Standards and Technology Interagency or Internal Report 8309; NIST: Gaitherburg, MD, USA, 2020.
3. Preskill, J. Sufficient condition on noise correlations for scalable quantum computing. *Quant. Inf. Comput.* **2013**, *13*, 181. [CrossRef]
4. Kempe, J. Approaches to quantum error correcction. *Poincare Semin.* **2005**, *1*, 65–93.
5. Djordjevic, I. *Quantum Information Processing and Quantum Error Correction: An Engineering Approach*; Academic Press: Cambridge, MA, USA, 2012.
6. Bomb, H. An Introduction to Topological Quantum Codes. In *Topological Codes in Quantum Error Correction*; Lidar, D.A., Brun, T.A., Eds.; Cambridge University Press: New York, NY, USA, 2013.
7. Fowler, A.G.; Mariantoni, M.; Martinis, J.M.; Cleland, A.N. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A* **2012**, *86*, 032324. [CrossRef]
8. Fowler, A.G.; Martinis, J.M. Quantifying the effects of local many-qubit errors and nonlocal two-qubit errors on the surface code. *Phys. Rev. A* **2014**, *89*, 101103. [CrossRef]
9. Hirota, O. *Quantum Noise Analysis for Quantum Computer*; IT-2020-17; The IEICE Technical Report on Information Theory at The IEICE of Japan: Tokyo, Japan, 2020; pp. 1–6.
10. Hirota, O. *Basis of Quantum Noise Analysis for Quantum Computers*; Bulletin of Quantum ICT Research Institute at Tamagawa University: Tokyo, Japan, 2020; Volume 10, pp. 1–7.
11. Lemberger, B.; Yavus, D.D. Effect of correlated decay on fault tolerant quantum computation. *Phys. Rev. A* **2017**, *96*, 062337. [CrossRef]
12. Yavus, D.D. Superradiance as a source of collective decoherence in quantum computer. *J. Opt. Soc. Am.* **2014**, *B31*, 2665. [CrossRef]
13. Hutter, A.; Loss, D. Breackdown of surface code error correction due to coupling to a bosonic bath. *Phys Rev. A* **2014**, *89*, 042334. [CrossRef]
14. Staudt, D. The Role of Correlated Noise in Quantum Computing. 2011. Available online: http://arxiv.org/abs/1111.1417 (accessed on 22 November 2021).
15. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; John Wiley and Sons: New York, NY, USA, 2006.
16. Blahut, R.E. *Principles and Practice of Information Theory*; Addison-Wesley: Reading, MA, USA, 1987.
17. Gallager, R.G. *Information Theory and Reliable Communication*; Wiley: New York, NY, USA, 1968.
18. Resch, S.; Karpuzcu, U.R. Benchmarking Quantum Computers and the Impact of Quantum Noise. 2020. Available online: http://arxiv.org/abs/1912.00546v4 (accessed on 22 November 2021).
19. Lindblad, G. On the generators of quantum dynamical semigroups. *Commun. Math. Phys.* **1976**, *17*, 821. [CrossRef]
20. Belavkin, V.P.; Hirota, O.; Hudson, R.L. The World of Quantum Noise and the Fundamental Outout Processes. In *Qauntum Communications and Measurement*; Plenum Press (Springer): New York, NY, USA, 1995.
21. Merzbacher, E. *Quantum Mechanics*; John Wiley: New York, NY, USA, 1970.
22. Karasik, R.; Marzlin, K.; Sanders, B.; Whaley, K. Multiparticle decoherence free subspaces in extended systems. *Phys. Rev. A* **2007**, *76*, 012331. [CrossRef]
23. Vepsalainen, A.P.; Karamlou, A.H.; Orrell, J.L.; Dogra1, A.S.; Loer, B.; Vasconcelos1, F.; Kim, D.K.; Melville, A.J.; Niedzielski, B.M.; Yoder, J.L.; et al. Impact of ionizing radiation on superconducting qubit coherence. *Nature* **2020**, *584*, 551–556. [CrossRef]
24. Wilen, C.D.; Abdullah, S.; Kurinsky, N.A.; Stanford, C.; Cardani, L.; D'Imperio, G.; Tomei, C.; Faoro, L.; Ioffe, L.B.; Liu, C.H.; et al. Correlated charge noise and relaxation errors in superconducting qubits. *Nature* **2021**, *594*, 369–373. [CrossRef]
25. Harper, R.; Flammia, S.T.; Wallman, J.J. Efficient learning of quantum noise. *Nat. Phys.* **2020**, *16*, 1184–1188. [CrossRef]
26. Misra, B.; Sudarshan, E.G. The Zeno's Paradox in Quantum Theory. *J. Math. Phys.* **1977**, *18*, 756. [CrossRef]
27. Itano, W.M.; Heinzen, D.J.; Bollinger, J.J.; Wineland, D. Quantum Zeno effect. *Phys. Rev. A* **1990**, *41*, 2295. [CrossRef] [PubMed]
28. Franson, J.D.; Jacobs, B.C.; Pittman, T.B. Quantum computing using single photons and the Zeno effect. *Phys. Rev.* **2004**, *A70*, 062302. [CrossRef]
29. Adler, S.L. Weisskopf-Wigner decay theory for the energy-driven stochastic Schrodinger equation. *Phys. Rev. D* **2002**, *67*, 025007. [CrossRef]
30. Karatzas, I.; Shreve, S.E. *Brownian Motion and Stochastic Calculus*; Springer: New York, NY, USA, 1998.
31. Gardiner, C.W.; Zoller, P. *Quantum Noise*; Springer: New York, NY, USA, 2000.
32. McEwen, M.; Kafri, D.; Chen, Z.; Atalaya, J.; Satzinger, K.J.; Quintana, C.; V.Klimov, P.; Sank, D.; Gidney, C.; Fowler, A.G.; et al. Removing leakage-induced correlated errors in superconducting quantum error correction. *Nat. Commun.* **2021**, *12*, 1761. [CrossRef] [PubMed]
33. Google, A.I. Exponential suppression of bit or phase flip errors with repetitive error correction. *Nature* **2021**, *595*, 383. [CrossRef]
34. McEwen, M.; Faoro, L.; Arya, K.I.; Dunsworth, A.; Huang, T.; Kim, S.; Burkett, B.; Fowler, A.; Arute, F.; .Bardin, J.C.; et al. Resolving catastrophic error bursts from cosmic rays in large arrays of superconducting qubits. *arXiv* **2021**, arXiv:2104.05219.
35. Dinc, F.; Bran, A.M. Non-Markovian super-superradiance in a linear chain of up to 100 qubits. *Phys. Rev. Res.* **2019**, *1*, 032042(R). [CrossRef]
36. Fang, K.; Liu, Z. No-Go Theorems for Quantum Resource Purification. *Phys. Rev. Lett.* **2020**, *125*, 060405. [CrossRef]
37. Bousba, Y.; Russell, T. No quantum Ramsey theorem for stabilizer codes. *IEEE Trans. Inform. Theory* **2021**, *67*, 408–415. [CrossRef]

38. Asiani, M.; Chai, J.; Whitney, R.; Auffeves, A.; Ng, H. Limitations in quantum computing from resource constraints. *arXiv* **2020**, arXiv:2007.01966.
39. Kan, K.; Une, M. Recent Trends on Research and Development of Quantum Computers and Standardization of Post-Quantum Cryptography. IMES Discussion Paper Series at Bank of Japan 2021, No-2021-E-5. Available online: https://www.imes.boj.or.jp/research/abstracts/english/21-E-05.html (accessed on 22 November 2021).
40. Miyaji, A. Theoretical and practical possibilities of Elliptic curve: From Elliptic curve cryptosystem to post quantum cryptosystems. *IEICE Jpn. Fundam. Rev.* **2021**, *14*, 329–336. [CrossRef]
41. Zurek, W.H. Decoherence, einselection, and the quantum origins of the classical. *Rev. Mod. Phys* **2003**, *75*, 715. [CrossRef]
42. Yu, T.; Eberly, J.H. Sudden death of entanglement. *Science* **2009**, *323*, 598-601. [CrossRef] [PubMed]
43. Yu, T.; Eberly, J.H. Finite-time disentanglement via spontaneous emission. *Phys. Rev. Lett.* **2004**, *93*, 140404. [CrossRef]
44. Lo Franco, R.; Bellomo, B.; Maniscalco, S.; Compagno, G. Dynamics of quantum correlations in two-qubit systems within non-Markovian environments. *Int. J. Mod. Phys.* **2013**, *B 27*, 1345053. [CrossRef]
45. De Vega, I.; Alonso, D. Dynamics of non-Markovian open quantum systems. *Rev. Mod. Phys.* **2017**, *89*, 015001. [CrossRef]
46. Bellomo, B.; Lo Franco, R.; Compagno, G. Non-Markovian effects on the dynamics of entanglement. *Phys. Rev. Lett.* **2007**, *99*, 160502. [CrossRef]
47. Aaronson, B.; Lo Franco, R.; Adesso, G. Comparative investigation of the freezing phenomena for quantum correlations under nondissipative decoherence. *Phys. Rev. A* **2013**, *88*, 012120. [CrossRef]
48. Rotter, I.; Bird, J.P. A review of progress in the physics of open quantum systems: theory and experiment. *Rep. Prog. Phys.* **2015**, *78*, 114001. [CrossRef] [PubMed]

entropy

MDPI

Article

Randomness and Irreversiblity in Quantum Mechanics: A Worked Example for a Statistical Theory

Yves Pomeau and Martine Le Berre *

Laboratoire d'Hydrodynamique, Ladhyx, CNRS UMR 7646, Ecole Polytechnique, 91128 Palaiseau, France; yves.pomeau@gmail.com
* Correspondence: martine.le-berre@u-psud.fr

Abstract: The randomness of some irreversible quantum phenomena is a central question because irreversible phenomena break quantum coherence and thus yield an irreversible loss of information. The case of quantum jumps observed in the fluorescence of a single two-level atom illuminated by a quasi-resonant laser beam is a worked example where statistical interpretations of quantum mechanics still meet some difficulties because the basic equations are fully deterministic and unitary. In such a problem with two different time scales, the atom makes coherent optical Rabi oscillations between the two states, interrupted by random emissions (quasi-instantaneous) of photons where coherence is lost. To describe this system, we already proposed a novel approach, which is completed here. It amounts to putting a probability on the density matrix of the atom and deducing a general "kinetic Kolmogorov-like" equation for the evolution of the probability. In the simple case considered here, the probability only depends on a single variable θ describing the state of the atom, and $p(\theta, t)$ yields the statistical properties of the atom under the joint effects of coherent pumping and random emission of photons. We emphasize that $p(\theta, t)$ allows the description of all possible histories of the atom, as in Everett's many-worlds interpretation of quantum mechanics. This yields solvable equations in the two-level atom case.

Keywords: quantum jumps; irreversibility; fluorescence; Kolmogorov-like model; Everett's interpretation

Citation: Pomeau, Y.; Le Berre, M. Randomness and Irreversiblity in Quantum Mechanics: A Worked Example for a Statistical Theory. *Entropy* **2021**, *23*, 1643. https://doi.org/10.3390/e23121643

Academic Editor: Osamu Hirota

Received: 3 August 2021
Accepted: 26 November 2021
Published: 7 December 2021

1. Introduction

The transition from Newtonian mechanics to quantum mechanics in the early years of the twentieth century has been a major step in the progress of our understanding of the world. This transition was more than a change in equations because it also involved a deep change in our understanding of the limits of human knowledge. It included, from the very beginning, a statistical interpretation of the theory. In other words, quantum mechanics is not fully predictive and cannot be so. The introduction of statistical methods to describe nature was not new, of course. Statistical concepts were introduced in physics to interpret classical (non-quantum) laws as a way to describe complex systems with many degrees of freedom, such as assemblies of many atoms in a macroscopic volume of fluid. The mathematical theory behind the statistical approach in classical physics is ergodic theory because no human being has enough computational power to solve Newton's equations [1] with the initial data (position and velocity) of too many particles. Nowadays, one cannot solve the classical equations of motion of more than a few thousand particles. In classical mechanics, a slightly more subtle point makes it difficult to predict the future from the initial data in the long run. This is related to the ergodic (Ergodic is the term used by Kolmogorov, although the common word is now chaotic or Anosovian if the trajectories are Lyapunov unstable [2]) properties of classical dynamics: a flow is ergodic, chaotic, or Anosovian if a small disturbance or inaccuracy in the initial conditions is amplified in the course of time. This property of ergodicity is very hard to prove for given systems. As far we are aware, this has been proven to be true [3] only for systems of hard spheres making elastic collisions, and the proof is highly non-trivial. In the two examples (many

particles and/or ergodicity of classical dynamics), the statistical method of analysis is just a way to describe systems given the imperfect knowledge of the initial conditions and their overwhelming abundance. On the contrary, quantum mechanics needs, from the very beginning, a statistical interpretation, a point that has raised controversies. To many, it seemed strange to postulate (see later for the precise meaning of this word in this context) a statistical interpretation of a theory that looks to be "deterministic" in the sense that the dynamical equations (Schrödinger or Dirac equations, including the interaction with the electromagnetic (EM) field) look well posed with a unique solution for given initial data. What is called "determinism" is, however, not as well defined as one could believe at first. There is a clearly defined *mathematical* meaning of the concept based on the notion (seemingly first understood by Newton) that, for given initial data (position and velocities of particles moving in vacuo), there is a well-defined future for a dynamical system obeying differential equations of a finite order in time. A superficial view could be that because the equations of non-relativistic quantum mechanics are mathematically "deterministic" and of the first order in time, a complete understanding of the initial data is enough to predict the future. The fallacy of this concept is in the word "complete". Because measurements of the initial conditions are made with quantum devices, there is a *fundamental* uncertainty in the initial conditions due to the limited accuracy of those measurements, a point made by Heisenberg [4]. This is central to our discussion: In the case of the emission of photons by an atom in an excited state, the instant of the emission cannot be predicted from measurements of the initial state of the atom. This fundamental question of the determination of the time of decay of an atom by emission of a photon was answered by Dirac [5] in a masterpiece of science in the context of black-body radiation, which is different from the one devoted to quantum jump statistics for a two-level atom pumped by a laser field treated here.

Note that the word "quantum jump", which is currently used for a single atom that emits photons when submitted to an EM field, may be ambiguous, particularly because the interaction between the atom and the emitted photon has a typical intrinsic time and period of the EM wave involved; therefore, it does not make sense to make statements for times shorter than this "intrinsic" time scale. The wave function of the full system—atom plus photons outside—changes continuously in time because when an atom initially in the excited state emits a photon, the resulting state is made of the atom in its ground state, plus an outgoing photon added to the EM field, and the amplitude of this new state (emitted photon, EM field, plus atom in the ground state) grows continuously from zero. When the initial state of the atom is a superposition of the ground state and of the excited state, it may go through the excited state under the effect of the Rabi oscillations and can then jump back to the ground state by emitting a photon, or the atomic state may follow Rabi oscillations without emitting any photons, with the atomic state evolving as a superposition of the ground and excited states until the next emission of a photon (which could occur only when the atomic state goes through the excited state). In summary, both possibilities (emission of a photon or no emission) exist in different universes in the Everett sense, as explained below.

After the early days of this grand history of the birth of quantum mechanics, a somewhat arcane field of knowledge had to ask whether such a theory with seemingly well-posed dynamical equations (Schrödinger and Dirac equations) has a kind of fundamental statistical interpretation. This is the aim of the present paper, which focuses on a worked problem, the fluorescence of a single atom. In the list of obscure concepts introduced to make the quantum description match the real data, let us quote what is often called the "reduction (or collapse) of the wave packet (or wave function)". Our aim is not to decide on the measure problem in quantum mechanics, which was the object of many debates and is still a controversial topic. However, let us note that the difficulties related to the conservation of the total probability are removed in Everett's theory.

In 1957, Everett introduced [6] a convincing explanation compatible both the idea of reduction of the wave packet and the constraint of unitarity of the evolution, or of conservation of the probability in the statistical interpretation. Everett's idea is that each

outcome of a measurement creates a new universe with a subsequent history consistent with the result of this measurement but disconnected from other universes corresponding each to another outcome of the measurement. This profound idea makes everything consistent at the price of introducing a direction of time. This direction of time plays the same role as the one introduced to explain the arrow of time of thermodynamics; namely, it represents the physical impossibility of reversing the history of a peculiar system. Said otherwise, the statistics introduced by quantum mechanics are there, in principle, to make averages over all universes corresponding to various outcomes of a measurement. As said above, because we are discussing something related to physics and not philosophy, there are consequences of this line of reasoning in the physical and mathematical picture of processes. This relies on definite equations for probability distributions, of which we shall give an example below.

In the case of the fluorescent light emitted by a single atom, the characteristic time associated with a quantum jump is very short, of the order of the laser period [5] and much smaller than the Rabi period. This property allows us to make the Markov approximation leading to our Kolmogorov-like equation for the evolution of the probability distribution of a single variable θ describing the trajectory of the atom.

In Section 2, we present our model equation for the evolution of the single parameter θ controlling the atomic state and derive the statistics of the emission times t_i with and without the pump field. In Section 3, we explain why Everett's theory is useful in interpreting our statistical description of the fluorescence of a single atom.

2. A Model Physical Problem

The spontaneous emission of photons by an assembly of atoms in thermal equilibrium was considered by Einstein [7] and by Dirac [5] as fundamentally random. Einstein used statistics to describe an atom interacting with black-body radiation. In this case, there is a continuous process of excitation of the ground state by the black-body radiation, but practically, this is not a very efficient process compared to the excitation by a resonant monochromatic beam, which we shall consider. Thanks to the progress of experimental atomic physics, in 1986, Hans Dehmelt [8–10] observed the leaping of electrons from one atomic state to another in individual atoms. This sudden transition of a tiny object (such as an electron, ion, molecule, or atom) from one of its discrete energy states to another has been called a quantum jump since Niels Bohr, who put this concept forward for discontinuous events, although Schrödinger (and others) strongly objected to their existence, postulating instead that they are not instantaneous.

Here, we study a simpler case, the emission of light by a two-level atom, an interesting worked example from the point of view of the statistical interpretation of quantum mechanics.

2.1. Towards a Full Statistical Theory of the Emission Process

We shall outline the principles of a statistical treatment that is able to describe both the emission of photons and the optical Rabi oscillations in the case of a single pumped two-level atom, detailed in [11]; then, we shall explain how to derive the probability distribution of the time intervals between two successive photon-emission events. This was based upon the property that, in such an interval, the atom does make unhindered Rabi oscillations, and that the emission of a photon is a phenomenon seen as instantaneous. This is, of course, one basic feature of a Markov process because we consider quick jumps occurring at random with a probability depending on the state of the system and, possibly, on the absolute time. For such a phenomenon, the Kolmogorov equation seems to be the right tool to describe the state of an atom because this kind of equation describes the evolution of the probability distribution of a system under the effects of two processes, one leading to a deterministic dynamics, the other to random quasi-instantaneous events, as just written. Let $\Theta(t)$ be the set of time-dependent parameters changing with time, with the

time derivative $\partial_t \Theta = v(\Theta)$, a function of Θ. In the deterministic phase, the conservative and normalized probability $p(\Theta, t)$ obeys the equation

$$\partial_t p(\Theta, t) + \partial_\Theta (v(\Theta) p(\Theta, t)) = 0, \tag{1}$$

where ∂_t is here and elsewhere for the derivative with respect to time, and ∂_Θ for the derivative with respect to Θ (This is actually a gradient in general because Θ has more than one component, but this only complicates the writing in an unessential way).

Kolmogorov equations add a right-hand side representing instantaneous transitions (or jumps) occurring at random instants of time to this equation, represented by a positive-valued function $\Gamma(\Theta'|\Theta)$. During a small interval of time $\mathrm{d}t$, if the system is in state Θ, it quickly jumps to state Θ' with probability $\Gamma(\Theta'|\Theta)\mathrm{d}t$ so that the Kolmogorov equation describes both the deterministic dynamics and the jump process and reads [12]:

$$\partial_t p(\Theta, t) + \partial_\theta (v(\Theta) p(\Theta, t)) = \int \mathrm{d}\Theta_1 \Gamma(\Theta|\Theta_1) p(\Theta_1, t) - p(\Theta, t) \int \mathrm{d}\Theta' \Gamma(\Theta'|\Theta). \tag{2}$$

In the right-hand side, the first positive term describes the increase in probability of the Θ-state due to jumps from other states to Θ. The second term represents the loss of probability because of jumps from Θ to any other state Θ'. By integration over Θ, one finds that the L^1-norm $\int \mathrm{d}\Theta\, p(\Theta, t)$ is constant (if it converges, as we assume).

Let us now consider a two-level atom whose wave function is of the form

$$\Psi_{at}(t) = \Big(\cos(\theta(t))|g> + ie^{i\omega t} \sin(\theta(t))|e>\Big) e^{i\varphi}, \tag{3}$$

where $\dot{\theta}$, the time derivative of $\theta(t)$, is equal to $\Omega/2$ between two jumps, Ω being the Rabi frequency. The Kolmogorov equation deals explicitly with the probability distribution $p(\theta, t)$ for the atomic state, here indexed by a single variable θ.

In the right-hand side of Equation (2), the probability $\Gamma(\theta; \theta')$ for the atom to make a quantum jump from the state θ towards the state θ' is proportional to $\delta(\sin\theta')$ (where $\delta(.)$ is the Dirac distribution) because any jump lands on $\theta' = 0$ in the interval $[-\pi/2, \pi/2]$, and this probability is proportional to $\gamma \sin^2\theta$ because it comes from the state a_1 with the squared amplitude $\sin^2\theta$, and γ is the emission rate of the atom in the excited state calculated by Dirac [5]. Therefore,

$$\Gamma(\theta|\theta') = \gamma\ \sin^2\theta\ \delta(\sin\theta'). \tag{4}$$

Thus, the Kolmogorov equation for the two-level atom illuminated by a resonant pump field is

$$\frac{\partial p}{\partial t} + \frac{\Omega}{2} \frac{\partial p}{\partial \theta} = \gamma \left(\delta(\sin\theta) \int_{-\pi/2}^{\pi/2} \mathrm{d}\theta'\ p(\theta', t) \sin^2\theta' - p(\theta, t) \sin^2\theta \right), \tag{5}$$

Introducing a probability distribution depending on a continuous variable, θ here, which amounts to putting a probability on the elements of the atomic density matrix, is a way to take into account all possible trajectories emanating from the emission of a single photon, with a new value of the number of photons radiated in any direction at each quantum jump. Average values of a time-dependent quantity that depends on θ can be calculated via the probability distribution $p(\theta, t)$, which is a π-periodic function with a finite jump at $\theta = 0$, but smooth elsewhere. This procedure allows us to deal correctly with the infinite number of possible trajectories, since Boltzmann's genius lies precisely in transforming the classical statistical theory based on unknown initial conditions into statistics for an ensemble of indeterminate trajectories.

We insist that our description of the fluorescence of a single two-level atom goes beyond solving Heisenberg equations (which is impossible anyway without making a strong hypothesis because of the infinite number of degrees of freedom of the EM field).

Here, as in the quantum mechanical frame, the infinite number of degrees of freedom are taken care of because they represent the fast phenomena, which are well approximated in Dirac's calculation of the coefficient γ for the black-body radiation calculus. Moreover, the whole story before and after each rapid event is told here through the balance terms written in the right-hand side of the Kolmogorov equation, which has a built-in conservation law of the total probability at any time, a serious advantage with respect to the quantum treatments using a Lindblad equation [13], which is difficult to handle [14].

Because it is linear, Equation (5) can be solved in a Laplace transform, but the general solution in time requires the inversion of a Laplace transform, which can be done only formally. There are two constraints: (i) The probability $p(\theta,t)$ is positive or zero and (ii) the total probability $\int_{-\pi/2}^{\pi/2} \mathrm{d}\theta\ p(\theta,t)$ is unity at any time, which reflects the unitary evolution of the atomic state (the integral of the square modulus of the wave function is constant and equal to one). It is relatively easy to check that they are fulfilled, since $\int_{-\pi/2}^{\pi/2} \mathrm{d}\theta\ p(\theta,t)$ is constant and $p(\theta,t) \geq 0$ at any positive time if $p(\theta,0) \geq 0$. Solutions in various limits are derived in [11]. The factors $\sin^2\theta$ on the right-hand side are there to take into account that a quantum jump occurs only if the atom is in the excited state, which has probability $\sin^2\theta$. The negative term on the right-hand side is the loss term representing the decrease in the amplitude of the excited state by jumps to the ground state, whereas the positive one is for the increase in the amplitude of the ground state when a jump takes place.

The populations of the two levels, or probabilities for the atom to be in the excited or in the ground state at time t, are, respectively,

$$\rho_1(t) = \int_{-\pi/2}^{\pi/2} \mathrm{d}\theta'\ p(\theta',t)\sin^2\theta'. \tag{6}$$

and

$$\rho_0(t) = \int_{-\pi/2}^{\pi/2} \mathrm{d}\theta'\ p(\theta',t)\cos^2\theta'. \tag{7}$$

Their sum is one, as it should be, if $p(\theta,t)$ is normalized to one.

From (5), one can derive an equation for the time derivative of $\rho_1(t)$ and $\rho_0(t)$ by multiplying (5) by $\sin^2\theta$ and by $\cos^2\theta$ and integrating the result over θ. This gives

$$\dot{\rho}_1 = -\frac{\Omega}{2}\int_{-\pi/2}^{\pi/2} \mathrm{d}\theta'\ \sin^2\theta' \frac{\partial p}{\partial\theta} - \gamma\left(\int_{-\pi/2}^{\pi/2} \mathrm{d}\theta'\ p(\theta',t)\sin^4\theta'\right), \tag{8}$$

and

$$\dot{\rho}_0 = -\frac{\Omega}{2}\int_{-\pi/2}^{\pi/2} \mathrm{d}\theta'\ \cos^2\theta' \frac{\partial p}{\partial\theta} + \gamma\left(\int_{-\pi/2}^{\pi/2} \mathrm{d}\theta'\ p(\theta',t)\sin^4\theta'\right). \tag{9}$$

On the r.h.s of the rate Equations (8) and (9), the first term, proportional to the Rabi frequency Ω, describes the effect of the Rabi oscillations, whereas the second term, proportional to γ, displays the effect of the quantum jumps responsible for the photoemission. Because $p(\theta,t)$ includes both the fluctuations due to the quantum jumps and the streaming term, the right-hand side of (8) and (9) represents the new history beginning at each step. After integration by parts, (8) and (9) become

$$\dot{\rho}_1(t) = -\dot{\rho}_0(t) = \int_{-\pi/2}^{\pi/2} \mathrm{d}\theta\ p(\theta,t)\ (\frac{\Omega}{2}\sin 2\theta - \gamma\sin^4\theta). \tag{10}$$

Note that the set of Equations (8) and (9), or (10), is not closed. It *cannot* be mapped into equations for $\rho_1(t)$ and $\rho_0(t)$ only because their right-hand sides depend on higher momenta of the probability distribution $p(\theta,t)$, momenta that cannot be derived from the knowledge of $\rho_1(t)$ and $\rho_0(t)$. The unclosed form of (8) and (9) is a rather common situation. To name a few cases, the BBGKY hierarchy of non-equilibrium statistical physics makes an infinite set of coupled equations for the distribution functions of systems of interacting (classical) particles [15], where the evolution of the one-body distribution

depends explicitly on the two-body distribution, which depends itself on the three-body distribution, etc. In the theory of fully developed turbulence, for instance, the average value of the velocity depends on the average value of the two-point correlation of the velocity fluctuations, depending itself on the three-point correlations, etc. Fortunately, one can solve the Kolmogorov Equation (5) via an implicit integral equation [11]; then, there is generally no need to manipulate an infinite hierarchy of equations as in those examples.

In the present case, one can say, following Everett, that the probability distribution $p(\theta, t)$ allows one to make averages over the states of the atom in different universes, each being labeled by a value of θ at a given time t. As written above, physical phenomena such as the observation of a quantum state decay measured by emission of a photon are relative to the measurement apparatus that takes place in the universe associated with the observer. At every emission of a photon, a new history begins, represented by the right-hand side of (9). In summary, the creation of new universes at each step defines a Markov process, which can be described by a Kolmogorov statistical picture, and cannot be considered as a deterministic process depending in a simple way on averaged quantities, such as population values.

2.2. Quantum Jump Statistics

To illustrate how one can use the Kolmogorov equation, we derive the time-dependent probability of photo-emission by a single atom, first without any pump field, then in the presence of a resonant laser.

We consider first an isolated atom initially in pure state $\Psi_{at}(0)$ given by (3) with $\theta(0) = \theta_0$. The solution of (5) with $\Omega = 0$ (no pump) and $p(\theta, 0) = \delta(\theta - \theta_0)$ is

$$p(\theta, t) = (1 - q(t))\delta(\theta) + q(t)\delta(\theta - \theta_0) \qquad \text{with} \qquad q(t) = e^{-(\gamma \sin^2 \theta_0)t}. \tag{11}$$

The evolution of the probability that the atom is in the excited state at time t is given by (6), and the emission of a photon occurs randomly in time with a rate:

$$\dot{\rho_1} = -\gamma \sin^2 \theta(t) \rho_1(t). \tag{12}$$

Once the atom "jumps" to its ground state, it cannot emit another photon; then, the emission of a photon, if recorded, is a way to measure the state of the atom. The solution of (12) leads to the population of the excited state

$$\rho_1(t) = \sin^2 \theta_0 e^{-(\gamma \sin^2 \theta_0)t} \tag{13}$$

when taking into account the initial condition, and the photo-emission rate is

$$\dot{\rho_1}(t) = -\gamma \sin^4 \theta_0 e^{-(\gamma \sin^2 \theta_0)t}. \tag{14}$$

The probability of photo-emission in the interval $(0, \infty)$ is the integral of $\dot{\rho_1}$:

$$\int_0^\infty \gamma \sin^4 \theta_0 \, e^{-(\gamma \sin^2 \theta_0)t} dt = \sin^2 \theta_0, \tag{15}$$

which means that the final state of the coupled system of the atom plus the emitted photon field is

$$\Psi(\infty) = \sin \theta_0 |g, 1> + e^{i\phi'} \cos \theta_0 |g, 0> \tag{16}$$

where the indices (1, 0) correspond to the one and zero photon states, respectively. The relation (15) means that if we consider N atoms initially prepared in a given pure state with $\theta(0) = \theta_0$, namely, with total energy $N \sin^2 \theta_0 \, \hbar\omega$, we get, at infinite time, N atoms in the ground state and $N \sin^2 \theta_0$ photons of individual energy $\hbar\omega$. In the final state, only a fraction of them, $N \sin^2 \theta_0$, jump from the excited state to the ground state with the emission of a photon; the others, $N \cos^2 \theta_0$, simply stay in the ground state [16].

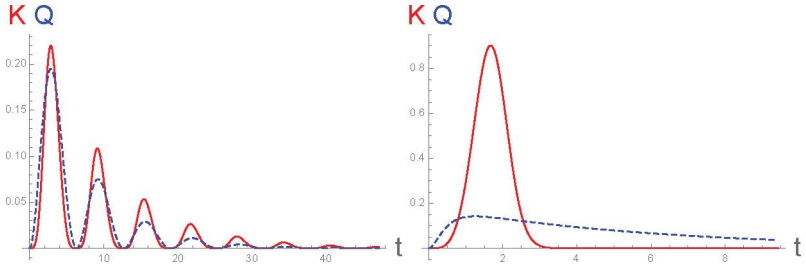
In the case of an atom submitted to a resonant pump field, the atom will emit photons at random times, forming a point process. Here, we assume that the process is Markovian, but more generally, any process with time-dependent history is completely characterized by its conditional intensity function $\lambda(t|\mathcal{H}_t)$, the density of points at time t, where $\mathcal{H}_t$ is the history of the emission activity up to time t, and the time interval probability distribution is given by the relation $\ell(\tau) = \lambda(\tau|\mathcal{H}_\tau)e^{-\int_0^\tau \lambda(t|\mathcal{H}_t)dt}$. In the present Markovian case, the conditional intensity of the point process, which is the probability of emission of a photon at time t, only depends on the value of θ at this time; therefore, one simply has $\ell(\tau) = \lambda(\tau)e^{-\int_0^\tau \lambda(t)dt}$. From (8), we deduce

$$\lambda(t) = \gamma \sin^4 \theta(t). \tag{17}$$

In this relation, the exponent 4 comes from two conditions: One in which the atom is in the excited state, and the other in which it emits a photon, as in (14), which describes an emission without any pump field. With a pump field, in between two successive emission times, the atom undergoes Rabi oscillations with $\theta(t) = \Omega t/2$, assuming that a photon is emitted at time $t = 0$. Therefore, the inter-emission time distribution for an atom driven by a resonant pump is given by the expression [17]:

$$\ell(\tau) = \gamma \sin^4(\frac{\Omega}{2}\tau)\ e^{-\gamma \int_0^\tau \sin^4(\frac{\Omega}{2}t)}, \tag{18}$$

which gives $\int_0^\infty \ell(\tau)d\tau = 1$, as expected. The result is shown in Figure 1 in the two opposite limits of large and small values of the ratio Ω/γ and is compared to the delay function derived in [18,19] (which does not have the standard form expected for a Markovian process). For the case of a strong input field, $\Omega > \gamma$, the two methods approximately agree; see Figure 1a. However, they differ noticeably in the opposite case, which is shown in Figure 1b. For weak laser intensity (or strong damping), the Kolmogorov derivation gives a mean delay between successive photons of order $\tau_K = (\Omega^4\gamma)^{-1/5}$, which decreases slowly as the damping rate γ increases, which seems reasonable. In the same limit, the dressed atom method leads to $\tau_Q = \gamma/\Omega^2$, a time scale much longer than the inverse of γ, and increasing with the damping rate, a result that seems to go against intuition [20].



(**a**) (**b**)

Figure 1. Inter-emission time distribution $\ell(t)$ in two opposite cases: (**a**) for weak and (**b**) for strong dissipative rates (with the respect to the Rabi frequency). The solid red curves are for our Kolmogorov statistical theory (Equation (18)). The dashed blue curves display the delay function deduced in [18,19] for the same values of Ω/γ, which are equal to 3.33 in (**a**) and 1/6 in (**b**).

2.3. Relationship with Planck-Einstein Theory

The above analysis of the spontaneous emission was devoted to an atom (or an ensemble of independent atoms) initially prepared in the pure state

$$\Psi_{at}(t) = \cos(\theta_0)|g> + i\sin(\theta_0)|e> . \tag{19}$$

In this case, the non-diagonal component of the atomic density matrix evolves as

$$\rho_{01}(t) = i\sin(\theta_0)\cos(\theta_0)e^{-\gamma\sin^2\theta_0\, t}. \tag{20}$$

This case—the so-called "coherent case"—displays a rate of emission of photons that is not equal to γ, the line-width of the excited state, but is equal to $\gamma\sin^2\theta_0$. Then, $\rho_1(t)$ depends in a non-trivial way on the atomic state. This points to a potentially interesting feature because the rate decreases when θ decreases; therefore, the atom is maintained in the excited state longer than in the case of black-body radiation, where the decay rate is γ, as was deduced by Planck and Einstein. In the latter case, the atoms are in thermal equilibrium (an incoherent state with $\rho_{10} = 0$), with a probability $(1-p)$ of being in the ground state or p of being in the excited state. At equilibrium, the probability $p_{eq}(\theta)$ is

$$p_{eq}(\theta, 0) = (1-p)\delta(\theta) + p\delta(\theta - \pi/2). \tag{21}$$

Taking expression (21) as an initial condition, the problem reduces to the one treated in Section 2.2 with $\Omega = 0$ and $\theta_0 = \pi/2$. The solution of the Kolmogorov equation is then given by (11), and the non-diagonal component of the atomic density matrix is given by (20). The important point is that the decay rate is equal to the constant γ without the factor $\sin\theta_0^2$ (when taking $\theta_0 = \pi/2$ in these equations), and the non-diagonal components of the density matrix vanish at any time, as expected for an incoherent state.

This permits to understand where the $\sin^2\theta_0$ factor in the decay constant comes from. Let us associate this result with the Dirac expression for γ. In Dirac's calculation, γ is proportional to the square modulus of the excited-state amplitude of the wave function because he considered a problem of evolution in general. From the point of view of Everett's multiple worlds, this amplitude depends on the universe in which the atom evolves. If $\rho_{01} = 0$, one knows that the atom may belong to the set of atoms that are in the excited state with a probability of one, and no reduction factor has to be associated with the decay rate γ. However, if $\rho_{01} \neq 0$, one cannot assume that the atom is in the excited state with a probability of one. Therefore, there is, a priori, a reduction factor (less than 1) to be included in Dirac's formula for the rate γ.

3. Statistical Picture of the Emission of Photons and Everett's Theory

Let us return to the connection of our model with Everett's theory that was presented in the 1950s for quantum physics, which is sometimes considered as philosophical speculation without a connection with real physics. As already mentioned in the introduction, Everett's ideas are useful in understanding the statistical effects observed in fluorescence. One fundamental idea of Everett when applied to the problem of emission of photons by a single atom is that, after each the emission time t_i the trajectory (or universe in Everett's notation) of the system of an atom plus photons splits into two separate trajectories (or universes). One corresponds to the atom plus an emitted photon, which is the universe of the observer; the other one is the trajectory without an emitted photon, with the atom pursuing the Rabi cycles until a photon emission occurs in this universe. Each couple of universes $\{U_{i,1ph}, U_{i,0ph}\}$ is indexed by the emitted photon $\{i\}$, which moves away from the atom at a given time t_i, so that the ensemble of all universes is nothing but an outflow of photons emitted at different instants. The important point is that all of these universes ignore each other, which implies no interference among them, a property justified because the characteristic time associated with a quantum jump is very short, of the order of the period of the atomic motion, which is also the period of the EM waves emitted by the atom in its excited state. This property allows us to make the Markov approximation leading to the Kolmogorov-like Equation (5) presented above and studied in [11]. A 3D schema illustrating a possible set of trajectories coming from successive t_i is drawn in Figure 2 (see the captions) with the aim of illustrating that the various universes do not overlap.

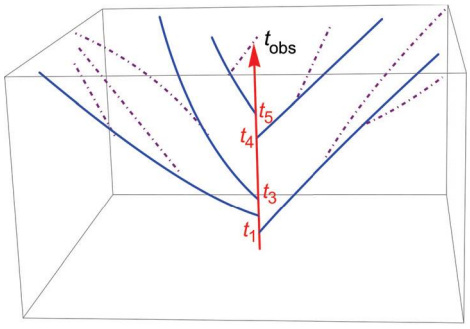


Figure 2. Schema of the possible trajectories of the atom emitting photons at times t_i, $\{i, 1, 5\}$ in the universe of the observer. The vertical red line with the arrow is the trajectory seen by the observer, where the atom makes Rabi oscillations between t_i and t_{i+1}. The solid blue lines stemming from each t_i illustrate the successive splitting of the observer trajectory (universe) into two parts. On the blue trajectory (virtual for the observer), no photon is emitted at t_i, but Rabi oscillations go along until a photon is emitted in this universe. This occurs at the crossing points of the blue curves with the purple dotted–dashed curves. At these crossing points, a virtual "blue trajectory" splits into two parts, one (blue) with an emitted photon and another one (purple) with no photon emitted.

By different universes, one implies two related things. First, the histories of the two universes are a priori different after the emission event. This does not imply a big difference, of course, between the two universes because their initial conditions at the instant of the emission are almost the same but for the absence or presence of a single photon. Secondly, the two universes are separated "mathematically" because their density matrices have no overlap. Therefore, one can define in each universe a density matrix that will evolve in the future without any relationship with the density matrix of the other universe. In the case of fluorescence, what happens in all universes can be described only statistically, the statistics being carried over all universes existing at a given time. This defines a kind of super-statistics because probability distributions are themselves defined over an object with a statistical meaning, namely, the density matrix for the quantum state in the universe under consideration. In the case of a pumped two-level atom, this density matrix depends on the angle θ so that the probability distribution is a probability depending on this single variable only.

Contrary to other theories of fluorescence of a single atom, such a statistical theory has a built-in statistical structure that is, we believe, necessary for describing the randomness of the emission process. Such a randomness is intrinsic to the emission process, represented as successive splitting of one trajectory into two every time a photon is emitted. By attempting to write a dynamical equation for the density matrix describing the emission process, one has to make a kind of average of this density matrix over all possible universes, something that is not physically possible because of the lack of overlap of the density matrices attached to the different universes.

4. Summary and Conclusions

The purpose of this paper was to show first how the view of quantum mechanics as a statistical theory grew from the very beginning of this theory and how things were clarified by Everett's bold idea of multiple universes. We also felt that it was not sufficient to discuss these questions abstractly as points of metaphysics, but as those of physics (although the word "metaphysics" is not from Aristotle, it is here understood in its original meaning by Aristotle, as "just after physics"). This was demonstrated on a model problem with a non-trivial "solution", namely, a model where the statistical analysis needs to be done very carefully even though its mathematics are actually fairly simple. This model also has the interest of being connected with the problems raised first by the founding fathers focused on the interaction of matter and light. We thought that it was instructive to show how

the general concepts of quantum mechanics as a statistical theory work "concretely" in a given case. By "concretely", we mean in a probabilistic mathematical framework using probability distributions and their evolution equation. We hope that this discussion of a specific model brings more light on this difficult subject than a more abstract discussion.

Author Contributions: Writing—original draft, Y.P.; Writing—review & editing, M.L.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: This paper is dedicated to the memory of Jean Ginibre, who played a crucial role in the first developments of the theory outlined there. His whole life was devoted to the study of fundamental problems in theoretical physics with an exigence of rigor and of relevance. We hope that the present work does not deviate from his high standards.

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

References and Notes

1. We reluctantly use the word "equations" here because Newton never wrote down ordinary differential equations of classical mechanics in the modern sense. As is well known, he solved dynamical problems by using elegant geometrical methods instead of what we now call Calculus. For instance, the integral of the solution of the two-body problem with a general spherical potential was replaced by the calculation of areas between curves and two radii.
2. Cornfeld, I.P.; Fomin, S.V.; Sinai, Y.G. *Ergodic Theory*; Springer: New York, NY, USA, 1982.
3. Sinai, Y.G. On the Foundation of the Ergodic Hypothesis for a Dynamical System of Statistical Mechanics. *Sov. Math. Dokl.* **1963**, *4*, 1818–1822.
4. Heisenberg, W. *The Physical Principles of the Quantum Theory*; Dover: New York, NY, USA, 1949.
5. Dirac, P.A.M. The quantum theory of the emission and absorption of radiation. *Proc. R. Soc. A* **1927**, *114*, 243–265.
6. Everett, H. Relative State Formulation of Quantum Mechanics. *Rev. Mod. Phys.* **1957**, *29*, 454–462. [CrossRef]
7. Einstein, A. On the quantum theory of radiation. *Phys. Z.* **1917**, *18*, 121–128.
8. Dehmelt, H.G. Laser fluorescence spectroscopy on Ti+ mono-ion oscillator II. *Bull. Am. Phys. Soc.* **1975**, *20*, 60.
9. Dehmelt, H.G. Monoion oscillator as potential ultimate laser frequency standard. *IEEE Trans. Instrum. Meas.* **1982**, *31*, 83. [CrossRef]
10. Dehmelt, H.G. Quantum jump. *Nature* **1987**, *325*, 581. [CrossRef]
11. Pomeau, Y.; Le Berre, M.; Ginibre, J. Ultimate statistical Physics: Fluorescence of a single atom. *J. Stat. Mech.* **2016**, *26*, 104002. [CrossRef]
12. Probability theory and mathematical statistics. In *Selected Works of A.N. Kolmogorov*; This Book Contains Also Many Works Not Related to Markov Processes, Discrete or Continuous; Springer Science + Business: Dordrecht, The Netherlands, 1992; Volume 2.
13. Lindblad, G. On the generators of quantum dynamical semigroups. *Comm. Math. Phys.* **1976**, *48*, 119–130. [CrossRef]
14. Starting from the Lindblad equation and using the dressed atom formalism, Reynaud, Dalibard and Cohen-Tanoudji reduce the set of infinite coupled equations (for coupled manifolds describing the fluorescent cascade) by the equations for a single manifold in their 1986 paper. Actually, this procedure amounts to truncating the Lindblad equation by suppressing the gain term, $\Gamma S^{-}\sigma S^{+}$, in Equation (2). 1 of their paper. After truncation, the equation displays a nonconservative interaction Hamiltonian in the inter-emission intervals.
15. Résibois, P.; de Leener, M. *Classical Kinetic Theory of Fluids*; Wiley: New York, NY, USA, 1976; Chapter VII-4.
16. We thank C. Cohen-Tannoudji, J. Dalibard, and S. Reynaud for a stimulating discussion that was at the origin of the above derivation.
17. We take the opportunity of this publication to give the right expression of the inter-emission time probability. In our 2016 paper with J.Ginibre, $\sin^2(\frac{\Omega}{2}\tau)$ should be changed into $\sin^4(\frac{\Omega}{2}\tau)$ in the expression of the conditional intensity of the photo-emission point process.
18. Reynaud, S.; Dalibard, J.; Cohen-Tannoudji, C. Photon statistics and quantum jumps: The picture of the dressed atom radiative cascade. *IEEE J. Quant. Electr.* **1986**, *24*, 1395–1402.
19. Cohen-Tannoudji, C.; Dalibard, J. Single-atom laser spectroscopy. Looking for dark periods in fluorescence light. *Europhys. Lett.* **1986**, *1*, 441–448. [CrossRef]
20. In the 1986 paper of Cohen-Tannoudji and Dalibard, the authors interpret $1/\tau_Q$ as the width of the ground state induced by the pump laser. We must also notice that the average number of radiated photons per unit time deduced from the Bloch equations is also of the order γ/Ω^2 in this limit.

entropy

MDPI

Article

A Method to Compute the Schrieffer–Wolff Generator for Analysis of Quantum Memory

Dong-Hwan Kim, Su-Yong Lee *, Yonggi Jo, Duk Y. Kim, Zaeill Kim and Taek Jeong *

Emerging Science and Technology Directorate, Agency for Defense Development, Daejeon 34186, Korea; kiow639@add.re.kr (D.-H.K.); yonggi@add.re.kr (Y.J.); duk0@add.re.kr (D.Y.K.); zkim@add.re.kr (Z.K.)
* Correspondence: suyong2@add.re.kr (S.-Y.L.); jeongt88@add.re.kr (T.J.)

Abstract: Quantum illumination uses entangled light that consists of signal and idler modes to achieve higher detection rate of a low-reflective object in noisy environments. The best performance of quantum illumination can be achieved by measuring the returned signal mode together with the idler mode. Thus, it is necessary to prepare a quantum memory that can keep the idler mode ideal. To send a signal towards a long-distance target, entangled light in the microwave regime is used. There was a recent demonstration of a microwave quantum memory using microwave cavities coupled with a transmon qubit. We propose an ordering of bosonic operators to efficiently compute the Schrieffer–Wolff transformation generator to analyze the quantum memory. Our proposed method is applicable to a wide class of systems described by bosonic operators whose interaction part represents a definite number of transfer in quanta.

Keywords: quantum illumination; transmon-cavity quantum memory; equivalent circuit; Schrieffer–Wolff transformation

Citation: Kim, D.-H.; Lee, S.; Jo, Y.; Kim, D.Y.; Kim, Z.; Jeong, T. A Method to Compute the Schrieffer–Wolff Generator for Analysis of Quantum Memory. *Entropy* **2021**, *23*, 1260. https://doi.org/10.3390/e23101260

Academic Editor: Osamu Hirota

Received: 11 August 2021
Accepted: 23 September 2021
Published: 27 September 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Quantum memories are required to store and retrieve quantum states with high fidelity. To synchronize various events, quantum memories are essential for quantum information networks, including quantum computation [1], quantum communication [2], and quantum illumination [3]. Quantum illumination (QI), a target detection scheme using quantum entangled light with signal and idler modes, has as its objective enhancing the detection rate of a target with low-reflectivity in a highly noisy environment [3]. In QI, the signal mode is sent to the target while the idler mode is retained. Although the noisy environment destroys the entanglement between the signal and idler modes, we can take quantum advantage over the classical limit by jointly measuring the returned signal mode and the idler mode when the signal arrives [4–7]. During this process, it is highly appreciable to keep the idler mode in an ideal quantum memory. This was investigated using various systems, such as a microwave cavity [8], mechanical oscillators [9], or spin ensembles [10,11].

Here, we focus on quantum memories using microwave cavities that can have high-quality factors and allow continuous-variable quantum information processes. By coupling a microwave cavity to a transmon qubit, it is able to write arbitrary states on the cavity and infer information about the cavity [8,12]. It is based on the cross Kerr effect, where the energy gap of neighboring levels of the cavity (transmon qubit) depends on the excitations of the transmon qubit (cavity). The anharmonicity of the transmon qubit gives rise to the cross Kerr effect through coupling of the qubit and cavity [13,14].

In dealing with such systems, it is crucial to understand how the coupling affects the energy structure. The Schrieffer–Wolff transformation computes this shift in energy structure by using a basis change unitary to remove the coupling [15,16]. For multiple bosonic modes containing nonlinear terms, it is complicated to find the exact generator of the unitary for the Schrieffer–Wolff transformation. Here, we propose a systematic approach

to find the generator and compute the energy corrections induced by this transformation. An ordering of operators, which we call computational ordering, greatly simplifies the commutation structure of operators making it suitable in calculating the Schrieffer–Wolff transformation generator.

2. Equivalent Circuit Analysis of a Quantum Memory

The quantum memory demonstrated in Ref. [8] couples two microwave cavities through a transmon qubit. One cavity is used as a memory (storage) to store quantum states and the other cavity is used as a readout port whose response depends on the memory-cavity state through the transmon qubit. Such a system can be described by an equivalent circuit depicted in Figure 1b. Two LC oscillators represent the microwave cavities, while the middle oscillator represents the transmon qubit. The oscillators are labeled as s, t, and r for storage, transmon, and readout, respectively, as in Ref. [8]. The transmon qubit is coupled to both cavities by capacitors. The Hamiltonian describing this system is

$$\frac{\hat{\mathcal{H}}}{\hbar} = \sum_{i=s,t,r} \omega_i \hat{a}_i^\dagger \hat{a}_i - \frac{E_C}{2\hbar} \hat{a}_t^\dagger \hat{a}_t^\dagger \hat{a}_t \hat{a}_t + g_1(\hat{a}_s^\dagger \hat{a}_t + \hat{a}_s \hat{a}_t^\dagger) + g_2(\hat{a}_t^\dagger \hat{a}_r + \hat{a}_t \hat{a}_r^\dagger), \tag{1}$$

where $\hat{a}_s$, $\hat{a}_t$, $\hat{a}_r$ are bosonic annihilation operators corresponding to each oscillator mode. A detailed derivation of this Hamiltonian and expressions of $\omega_s, \omega_t, \ldots$ in terms of L_i, C_i, C_{c1}, C_{c2} $(i = s, t, r)$ are given in Appendix A. We assume that the system is in the dispersive regime, where the couplings g_1 and g_2 are much smaller than the detunings $|\omega_s - \omega_t|$ and $|\omega_t - \omega_r|$.

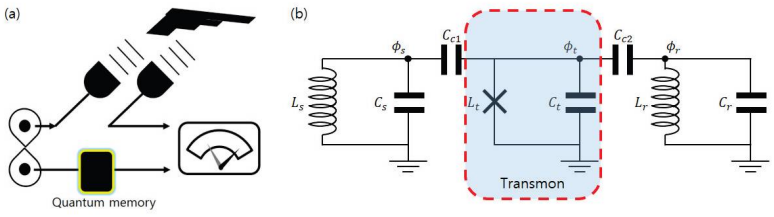


Figure 1. (**a**) Concept of quantum illumination with a quantum memory. (**b**) Equivalent circuit model of quantum memory under consideration. Transmon is coupled to two LC oscillators via capacitors. Symbols with L represent inductances, while symbols with C represent capacitances. ϕ_i at each specified node is flux variable used in Appendix A.

The elimination of capacitive couplings in Equation (1) gives rise to cross Kerr effects among each cavity and the transmon. This is done by diagonalizing the Hamiltonian. There are two ways in achieving this; namely, second-order perturbation and the Schrieffer–Wolff transformation [16]. These methods were previously applied to systems of transmon qubits coupled with LC oscillators in evaluating the energy structure [13,14]. For the Schrieffer–Wolff transformation, one must find an operator $\hat{S}$, the Schrieffer–Wolff generator, which is an off-diagonal operator satisfying a given commutator equation. It is complicated to determine the operator $\hat{S}$ and compute various commutators to obtain the second-order energy corrections. Thus, we introduce a method that simplifies the computation and apply it to Equation (1). After the computation, we truncate the transmon qubit to the lowest two levels to obtain a Jaynes–Cummings-like Hamiltonian [13]. Truncation of the transmon qubit should be done after diagonalization since virtual excitations of the transmon need to be considered.

2.1. Computational Ordering for Schrieffer–Wolff Transformation

We propose an ordering of bosonic operators, which gives direct computation of the Schrieffer–Wolff generator and second-order energy corrections. For a short recall of the Schrieffer–Wolff transformation, let $\hat{\mathcal{H}}$ be the Hamiltonian in interest. We separate the Hamiltonian into diagonal and off-diagonal parts, $\hat{H}_0$, $\hat{V}$ respectively, so $\hat{\mathcal{H}} = \hat{H}_0 + \hat{V}$. The Schrieffer–Wolff generator $\hat{S}$ is defined as the off-diagonal operator which satisfies $[\hat{S}, \hat{H}_0] = -\hat{V}$. Then,

$$e^{\hat{S}}\hat{\mathcal{H}}e^{-\hat{S}} = \hat{H}_0 + \frac{1}{2}[\hat{S}, \hat{V}] + \dots. \tag{2}$$

The energy separations of $\hat{H}_0$ must be larger than $\hat{V}$, so that $\hat{S}$ becomes small and a perturbative approach is applicable [17]. This condition becomes evident when we write down the explicit form of $\hat{S}$ in Equation (5). The second-order energy corrections to $\hat{H}_0$ are given as the diagonal part of $\frac{1}{2}[\hat{S}, \hat{V}]$.

We consider a system of N bosonic modes, where $\hat{a}_i$ is the annihilation operator of the i-th mode and satisfies $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$. We propose an ordering of operators

$$\hat{a}^{\dagger\mathbf{n}} f(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{m}} \tag{3}$$

to efficiently compute the Schrieffer–Wolff transformation generator and second-order energy corrections to $\hat{H}_0$. In Equation (3), $\hat{a}^\dagger\hat{a} = (\hat{a}_1^\dagger\hat{a}_1, \dots, \hat{a}_N^\dagger\hat{a}_N)$, $\mathbf{n} = (n_1, \dots, n_N)$, $\mathbf{m} = (m_1, \dots, m_N)$ are N tuples and $\hat{a}^{\dagger\mathbf{n}} = \hat{a}_1^{\dagger n_1} \dots \hat{a}_N^{\dagger n_N}$, $\hat{a}^{\mathbf{m}} = \hat{a}_1^{m_1} \dots \hat{a}_N^{m_N}$. To ensure that f is unique, we require $\mathbf{n}, \mathbf{m}$ to have disjoint support, i.e., $\mathbf{n} \cdot \mathbf{m} := (n_1 m_1, \dots, n_N m_N) = (0, \dots, 0)$. For example, the operator $\hat{a}_1^\dagger\hat{a}_1^\dagger\hat{a}_1^\dagger\hat{a}_1\hat{a}_1$ will be written as

$$\hat{a}_1^\dagger\hat{a}_1^\dagger\hat{a}_1^\dagger\hat{a}_1\hat{a}_1 = \hat{a}_1^\dagger(\hat{a}_1^\dagger\hat{a}_1\hat{a}_1^\dagger\hat{a}_1 - \hat{a}_1^\dagger\hat{a}_1) = \hat{a}_1^\dagger f(\hat{a}^\dagger\hat{a}),$$
$$f(x_1, \dots, x_N) = x_1^2 - x_1.$$

The main motivation of this ordering is that diagonal operators in the Fock basis correspond to functions defined on $\mathbb{N}_0^N$, with $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$, and functions are in general easier to manipulate than operators. The computational ordering is then equivalent to writing a given operator in terms of number operators as much as possible. Explicit expressions for writing normal-ordered or antinormal-ordered operators in this ordering are given in Appendix B. Note that operators that have $\mathbf{n} = \mathbf{m} = 0$ are exactly the diagonal operators in the Fock basis.

We write the Hamiltonian $\hat{\mathcal{H}}$ in this ordering:

$$\hat{\mathcal{H}} = f(\hat{a}^\dagger\hat{a}) + \sum_{\mathbf{n},\mathbf{m}} \hat{a}^{\dagger\mathbf{n}} g_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{m}}. \tag{4}$$

The sum, here and henceforth, is over all $\mathbf{n}, \mathbf{m}$ satisfying $\mathbf{n} \cdot \mathbf{m} = (0, \dots, 0)$ and $\mathbf{n}, \mathbf{m}$ are not both 0. This automatically splits the Hamiltonian into diagonal and off-diagonal parts. The hermitian condition on $\hat{\mathcal{H}}$ forces f to be real valued and $g_{\mathbf{nm}}^* = g_{\mathbf{mn}}$, z^* being the complex conjugate of z. The main results are

$$\hat{S} = \sum_{\mathbf{n},\mathbf{m}} \hat{a}^{\dagger\mathbf{n}} \frac{g_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})}{f(\hat{a}^\dagger\hat{a} + \mathbf{n}) - f(\hat{a}^\dagger\hat{a} + \mathbf{m})}\hat{a}^{\mathbf{m}}, \tag{5}$$

$$\frac{1}{2}[\hat{S}, \hat{V}]_{(d)} = \sum_{\mathbf{n},\mathbf{m}} \frac{(\hat{a}^\dagger\hat{a})^{\underline{\mathbf{n}}}(\hat{a}^\dagger\hat{a} - \mathbf{n} + \mathbf{m})^{\underline{\mathbf{m}}}|g_{\mathbf{nm}}(\hat{a}^\dagger a - \mathbf{n})|^2}{f(\hat{a}^\dagger\hat{a}) - f(\hat{a}^\dagger\hat{a} - \mathbf{n} + \mathbf{m})}. \tag{6}$$

where $x^{\underline{n}} = x(x-1)\dots(x-n+1)$ is the falling factorial and the falling factorial of tuples is defined element-wise. The subscript $_{(d)}$ means to take the diagonal part, so $\frac{1}{2}[\hat{S}, \hat{V}]_{(d)}$ is the second-order correction to energy. Since $f, g_{\mathbf{nm}}$ are essentially functions defined on $\mathbb{N}_0^N$ as noted before, the computation of Equations (5) and (6) is straightforward. In the end, the original Hamiltonian is transformed via the Schrieffer–Wolff transformation as

$$e^{\hat{S}}\hat{\mathcal{H}}e^{-\hat{S}} = \hat{H}_0 + \frac{1}{2}[\hat{S},\hat{V}]_{(d)} + \cdots = \hat{H}_0 + \hat{H}^{(2)} + \ldots \tag{7}$$

where the omitted terms are off-diagonal terms of second-order in $\hat{V}$ or diagonal terms of third-order in $\hat{V}$. The superscript $^{(2)}$ indicates that the term is second-order in $\hat{V}$.

To obtain the main results Equations (5) and (6), we need a computational lemma.

Lemma 1. *The commutators of $\hat{a}^{\dagger\mathbf{n}}$, $\hat{a}^{\mathbf{m}}$ with $f(\hat{a}^\dagger\hat{a})$ are as follows.*

$$[\hat{a}^{\dagger\mathbf{n}}, f(\hat{a}^\dagger\hat{a})] = \hat{a}^{\dagger\mathbf{n}}(f(\hat{a}^\dagger\hat{a}) - f(\hat{a}^\dagger\hat{a}+\mathbf{n})), \tag{8}$$

$$[\hat{a}^{\mathbf{m}}, f(\hat{a}^\dagger\hat{a})] = (f(\hat{a}^\dagger\hat{a}+\mathbf{m}) - f(\hat{a}^\dagger\hat{a}))\hat{a}^{\mathbf{m}}. \tag{9}$$

Proof. It suffices to check on number states $|\mathbf{k}\rangle = |k_1,\ldots,k_N\rangle$. One can verify

$$\begin{aligned}
[\hat{a}^{\dagger\mathbf{n}}, f(\hat{a}^\dagger\hat{a})]\,|\mathbf{k}\rangle &= \hat{a}^{\dagger\mathbf{n}} f(\hat{a}^\dagger\hat{a})\,|\mathbf{k}\rangle - f(\hat{a}^\dagger\hat{a})\hat{a}^{\dagger\mathbf{n}}\,|\mathbf{k}\rangle \\
&= f(\mathbf{k})\hat{a}^{\dagger\mathbf{n}}\,|\mathbf{k}\rangle - \left(\prod_{i=1}^{N}(k_i+1)^{\overline{n_i}}\right)^{1/2} f(\hat{a}^\dagger\hat{a})\,|\mathbf{k}+\mathbf{n}\rangle \\
&= \left(\prod_{i=1}^{N}(k_i+1)^{\overline{n_i}}\right)^{1/2} (f(\mathbf{k}) - f(\mathbf{k}+\mathbf{n}))\,|\mathbf{k}+\mathbf{n}\rangle \\
&= \hat{a}^{\dagger\mathbf{n}}(f(\mathbf{k}) - f(\mathbf{k}+\mathbf{n}))\,|\mathbf{k}\rangle \\
&= \hat{a}^{\dagger\mathbf{n}}(f(\hat{a}^\dagger\hat{a}) - f(\hat{a}^\dagger\hat{a}+\mathbf{n}))\,|\mathbf{k}\rangle\,.
\end{aligned}$$

Here, $x^{\overline{n}} = x(x+1)\ldots(x+n-1)$ is the rising factorial. The commutator with $\hat{a}^{\mathbf{m}}$ follows from taking the adjoint. □

Now one can compute the commutator of $\hat{S}$ with $\hat{H}_0$. Write $\hat{S}$ as

$$\hat{S} = \sum_{\mathbf{n},\mathbf{m}} \hat{a}^{\dagger\mathbf{n}} h_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{m}}, \tag{10}$$

with $h^*_{\mathbf{nm}} = -h_{\mathbf{mn}}$ so that $\hat{S}$ is antihermitian. Then, one has

$$\begin{aligned}
[\hat{S},\hat{H}_0] &= \sum_{\mathbf{n},\mathbf{m}} [\hat{a}^{\dagger\mathbf{n}} h_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{m}}, \hat{H}_0] \\
&= \sum_{\mathbf{n},\mathbf{m}} \hat{a}^{\dagger\mathbf{n}} h_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})(f(\hat{a}^\dagger\hat{a}+\mathbf{m}) - f(\hat{a}^\dagger\hat{a}+\mathbf{n}))\hat{a}^{\mathbf{m}}.
\end{aligned}$$

The choice of $\hat{S}$ as in Equation (5) yields $[\hat{S},\hat{H}_0] = -\hat{V}$, i.e., we take $h_{\mathbf{nm}}$ as

$$h_{\mathbf{nm}}(\hat{a}^\dagger\hat{a}) = \frac{g_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})}{f(\hat{a}^\dagger\hat{a}+\mathbf{n}) - f(\hat{a}^\dagger\hat{a}+\mathbf{m})}. \tag{11}$$

The conditions on f, $g_{\mathbf{nm}}$ ensure that $h^*_{\mathbf{nm}} = -h_{\mathbf{mn}}$ holds. This is well-defined as long as the diagonal part is nondegenerate, which is true when considering low excitations of transmons.

Using the generator $\hat{S}$ defined as Equation (5), we can compute the correction to energies as the diagonal part of $\frac{1}{2}[\hat{S},\hat{V}]$. The only term in $\hat{V}$ that gives a diagonal contribution with the $\hat{a}^{\dagger\mathbf{n}} h_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{m}}$ term in $\hat{S}$ is $\hat{a}^{\dagger\mathbf{m}} g_{\mathbf{mn}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{n}}$. A pictorial representation of this statement is given in Figure 2. Hence,

$$\frac{1}{2}[\hat{S},\hat{V}]_{(d)} = \frac{1}{2}\sum_{\mathbf{n},\mathbf{m}}[\hat{a}^{\dagger\mathbf{n}}h_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{m}},\hat{a}^{\dagger\mathbf{m}}g_{\mathbf{mn}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{n}}] \tag{12}$$

$$= \frac{1}{2}\sum_{\mathbf{n},\mathbf{m}}\left\{\frac{(\hat{a}^\dagger\hat{a})^{\underline{\mathbf{n}}}(\hat{a}^\dagger\hat{a}-\mathbf{n}+\mathbf{m})^{\underline{\mathbf{m}}}|g_{\mathbf{nm}}(\hat{a}^\dagger a-\mathbf{n})|^2}{f(\hat{a}^\dagger\hat{a})-f(\hat{a}^\dagger\hat{a}-\mathbf{n}+\mathbf{m})}\right. \tag{13}$$

$$\left. + \frac{(\hat{a}^\dagger\hat{a})^{\underline{\mathbf{m}}}(\hat{a}^\dagger\hat{a}+\mathbf{n}-\mathbf{m})^{\underline{\mathbf{n}}}|g_{\mathbf{nm}}(\hat{a}^\dagger a-\mathbf{m})|^2}{f(\hat{a}^\dagger\hat{a})-f(\hat{a}^\dagger\hat{a}+\mathbf{n}-\mathbf{m})}\right\}$$

$$= \sum_{\mathbf{n},\mathbf{m}}\frac{(\hat{a}^\dagger\hat{a})^{\underline{\mathbf{n}}}(\hat{a}^\dagger\hat{a}-\mathbf{n}+\mathbf{m})^{\underline{\mathbf{m}}}|g_{\mathbf{nm}}(\hat{a}^\dagger a-\mathbf{n})|^2}{f(\hat{a}^\dagger\hat{a})-f(\hat{a}^\dagger\hat{a}-\mathbf{n}+\mathbf{m})}. \tag{14}$$

The calculation of the commutator can be done by using Lemma 1 and results in Appendix B. Note that the summand in Equation (13) is symmetric under change of $\mathbf{n}$, $\mathbf{m}$, which leads to Equation (14). This result is equivalent to nondegenerate second-order perturbation energy correction,

$$E_{\mathbf{k}}^{(2)} = \sum_{\mathbf{k}'\neq\mathbf{k}}\frac{|\langle\mathbf{k}'|\hat{V}|\mathbf{k}\rangle|^2}{E_{\mathbf{k}}-E_{\mathbf{k}'}}, \tag{15}$$

computed in our proposed ordering.

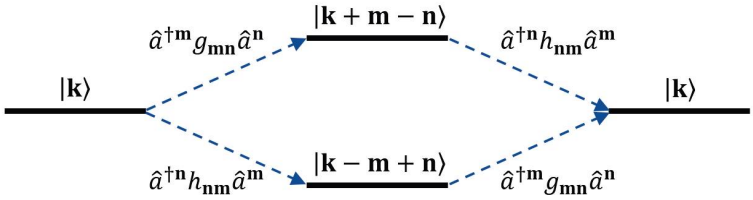


Figure 2. Schematic representation of diagonal terms in the commutator $\frac{1}{2}[\hat{S},\hat{V}]$. The Fock basis state $|\mathbf{k}\rangle$ must end up in $|\mathbf{k}\rangle$ to give a diagonal contribution. For example, in the product $\hat{S}\hat{V}$, the $\hat{a}^{\dagger\mathbf{m}}g_{\mathbf{mn}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{n}}$ term in $\hat{V}$ maps the state $|\mathbf{k}\rangle$ to $|\mathbf{k}+\mathbf{m}-\mathbf{n}\rangle$. The only term in $\hat{S}$ which maps this back to $|\mathbf{k}\rangle$ is $\hat{a}^{\dagger\mathbf{n}}h_{\mathbf{nm}}(\hat{a}^\dagger\hat{a})\hat{a}^{\mathbf{m}}$. This corresponds to the upper-half of the above diagram. The lower-half of the diagram represents the $\hat{V}\hat{S}$ product.

In most cases, interaction terms are of form $\hat{a}_i^\dagger g_{ij}(\hat{a}^\dagger\hat{a})\hat{a}_j$, which represent a single transfer of quantum excitations. If we restrict the interaction to only these terms, our main results Equations (5) and (6) are simplified to

$$\hat{S} = \sum_{i\neq j}\hat{a}_i^\dagger\frac{g_{ij}(\hat{a}^\dagger\hat{a})}{f(\hat{a}^\dagger\hat{a}+e_i)-f(\hat{a}^\dagger\hat{a}+e_j)}\hat{a}_j, \tag{16}$$

$$\frac{1}{2}[\hat{S},\hat{V}]_{(d)} = \sum_{i\neq j}\frac{\hat{a}_i^\dagger\hat{a}_i(\hat{a}_j^\dagger\hat{a}_j+1)|g_{ij}(\hat{a}^\dagger\hat{a}-e_i)|^2}{f(\hat{a}^\dagger\hat{a})-f(\hat{a}^\dagger\hat{a}-e_i+e_j)}, \tag{17}$$

where e_i is the N tuple, which has 1 as its i-th component, and all other elements are 0 and $i,j\in\{1,2,\ldots,N\}$.

2.2. Application to Analyzing the Circuit Hamiltonian

We return to the diagonalization of the circuit Hamiltonian Equation (1). To apply the previous formalism, define functions f, g_{12}, g_{23} as

$$f(n,m,\ell) := \omega_s n+\omega_t m+\omega_r\ell-\frac{E_C}{2\hbar}m(m-1), \tag{18}$$

$$g_{12}(n,m,\ell) = g_{21}(n,m,\ell) := g_1, \tag{19}$$

$$g_{23}(n,m,\ell) = g_{32}(n,m,\ell) := g_2. \tag{20}$$

These functions give a full description of the Hamiltonian Equation (1). n, m, ℓ correspond to $\hat{a}_s^\dagger \hat{a}_s$, $\hat{a}_t^\dagger \hat{a}_t$, $\hat{a}_r^\dagger \hat{a}_r$, respectively. The second-order energy corrections can be directly computed by our main result Equation (17).

$$\begin{aligned}\frac{\hat{H}^{(2)}}{\hbar} &= |g_1|^2\left(\frac{n(m+1)}{f(n,m,\ell)-f(n-1,m+1,\ell)}+\frac{m(n+1)}{f(n,m,\ell)-f(n+1,m-1,\ell)}\right)\\ &\quad+|g_2|^2\left(\frac{m(\ell+1)}{f(n,m,\ell)-f(n,m-1,\ell+1)}+\frac{\ell(m+1)}{f(n,m,\ell)-f(n,m+1,\ell-1)}\right)\end{aligned} \tag{21}$$

$$\begin{aligned}&= |g_1|^2\left(\frac{\hat{a}_s^\dagger\hat{a}_s(\hat{a}_t^\dagger\hat{a}_t+1)}{\Delta_{st}+\hat{a}_t^\dagger\hat{a}_t E_C/\hbar}-\frac{\hat{a}_t^\dagger\hat{a}_t(\hat{a}_s^\dagger\hat{a}_s+1)}{\Delta_{st}+(\hat{a}_t^\dagger\hat{a}_t-1)E_C/\hbar}\right)\\ &\quad+|g_2|^2\left(\frac{\hat{a}_r^\dagger\hat{a}_r(\hat{a}_t^\dagger\hat{a}_t+1)}{\Delta_{rt}+\hat{a}_t^\dagger\hat{a}_t E_C/\hbar}-\frac{\hat{a}_t^\dagger\hat{a}_t(\hat{a}_r^\dagger\hat{a}_r+1)}{\Delta_{rt}+(\hat{a}_t^\dagger\hat{a}_t-1)E_C/\hbar}\right),\end{aligned} \tag{22}$$

with $\Delta_{st} := \omega_s - \omega_t$, $\Delta_{rt} := \omega_r - \omega_t$. To read off shifts in frequency, cross Kerr coefficients, and anharmonicities, we must put Equation (22) in normal order:

$$\frac{\hat{H}^{(2)}}{\hbar} = \delta_s\hat{a}_s^\dagger\hat{a}_s+\delta_t\hat{a}_t^\dagger\hat{a}_t+\delta_r\hat{a}_r^\dagger\hat{a}_r+\frac{\delta_K}{2\hbar}\hat{a}_t^\dagger\hat{a}_t^\dagger\hat{a}_t\hat{a}_t+\chi_{st}\hat{a}_s^\dagger\hat{a}_s\hat{a}_t^\dagger\hat{a}_t+\chi_{rt}\hat{a}_r^\dagger\hat{a}_r\hat{a}_t^\dagger\hat{a}_t+\ldots. \tag{23}$$

Using the result from Equation (A16), the shifts are given as

$$\begin{aligned}\frac{\hat{H}^{(2)}}{\hbar} &= \frac{|g_1|^2}{\Delta_{st}}\hat{a}_s^\dagger\hat{a}_s+\frac{|g_2|^2}{\Delta_{rt}}\hat{a}_r^\dagger\hat{a}_r+\sum_{k=1}^{\infty}\frac{(-1)^k}{E_C}\left(\frac{|g_1|^2}{(\Delta_{st}/E_C)^{\overline{k}}}+\frac{|g_2|^2}{(\Delta_{rt}/E_C)^{\overline{k}}}\right)\hat{a}_t^{\dagger k}\hat{a}_t^k\\ &\quad+\sum_{k=1}^{\infty}\frac{(-1)^k|g_1|^2(k+1)}{E_C(\Delta_{st}/E_C)^{\overline{k+1}}}\hat{a}_s^\dagger\hat{a}_t^{\dagger k}\hat{a}_t^k\hat{a}_s+\sum_{k=1}^{\infty}\frac{(-1)^k|g_2|^2(k+1)}{E_C(\Delta_{rt}/E_C)^{\overline{k+1}}}\hat{a}_r^\dagger\hat{a}_t^{\dagger k}\hat{a}_t^k\hat{a}_r,\end{aligned} \tag{24}$$

where $x^{\overline{n}} = x(x+1)\ldots(x+n-1)$ is the rising factorial and factors of $\hbar$ were omitted in the right-hand side for simplicity. Restoring these factors are done by replacing E_C with $E_C/\hbar$. The shifts in physical quantities are found by simply reading off the coefficients of Equation (24):

$$\delta_s = \frac{|g_1|^2}{\Delta_{st}}, \quad \delta_r = \frac{|g_2|^2}{\Delta_{rt}}, \quad \delta_t = -\frac{|g_1|^2}{\Delta_{st}}-\frac{|g_2|^2}{\Delta_{rt}}, \tag{25}$$

$$\delta_K = \frac{2|g_1|^2E_C}{\Delta_{st}(\Delta_{st}+E_C/\hbar)}+\frac{2|g_2|^2E_C}{\Delta_{rt}(\Delta_{rt}+E_C/\hbar)}, \tag{26}$$

$$\chi_{st} = -\frac{2|g_1|^2E_C/\hbar}{\Delta_{st}(\Delta_{st}+E_C/\hbar)}, \quad \chi_{rt} = -\frac{2|g_2|^2E_C/\hbar}{\Delta_{rt}(\Delta_{rt}+E_C/\hbar)}. \tag{27}$$

Hence, the total transformed Hamiltonian can be written as

$$\begin{aligned}e^{\hat{S}}\frac{\hat{\mathcal{H}}}{\hbar}e^{-\hat{S}} &= \frac{1}{\hbar}\left(\hat{H}_0+\hat{H}^{(2)}+\ldots\right)\\ &= \sum_{i=s,t,r}(\omega_i+\delta_i)\hat{a}_i^\dagger\hat{a}_i-\frac{E_C-\delta_K}{2\hbar}\hat{a}_t^\dagger\hat{a}_t^\dagger\hat{a}_t\hat{a}_t+\chi_{st}\hat{a}_s^\dagger\hat{a}_s\hat{a}_t^\dagger\hat{a}_t+\chi_{rt}\hat{a}_r^\dagger\hat{a}_r\hat{a}_t^\dagger\hat{a}_t+\ldots.\end{aligned} \tag{28}$$

This extends the results using Bogoliubov approach to diagonalize the Hamiltonian of a coupled single LC oscillator and transmon [18] in the sense that the frequency shift of the transmon qubit is the sum of contributions from coupling to each LC oscillator. Such a system is described by a Hamiltonian

$$\hat{\mathcal{H}} = \hbar\omega_1\hat{a}^\dagger\hat{a}+\hbar\omega_2\hat{b}^\dagger\hat{b}-\frac{E_C}{2}\hat{b}^\dagger\hat{b}^\dagger\hat{b}\hat{b}+\hbar g(\hat{a}^\dagger\hat{b}+\hat{a}\hat{b}^\dagger). \tag{29}$$

Elimination of the $\hbar g(\hat{a}^\dagger\hat{b}+\hat{a}\hat{b}^\dagger)$ term gives rise to cross Kerr coefficient between $\hat{a}, \hat{b}$,

$$\chi = -\frac{2|g|^2E_C/\hbar}{\Delta(\Delta+E_C/\hbar)}, \tag{30}$$

where $\Delta := \omega_1 - \omega_2$, which highly resembles the results in Equation (27). Note that there is a sign difference in the definition of Δ compared with that of Ref. [18].

To obtain a form similar to that given in Refs. [13,14], we truncate the transmon Hilbert space to the first two levels. Such truncation is done by replacing $\hat{a}_t^\dagger \hat{a}_t$ with $(\sigma_z + 1)/2$ in Equation (22). The result is

$$\begin{aligned}\frac{\hat{H}^{(2)}}{\hbar} = &\frac{|g_1|^2}{\Delta_{st} + E_C/\hbar}\hat{a}_s^\dagger \hat{a}_s - \left(\frac{|g_1|^2}{\Delta_{st}} + \frac{|g_2|^2}{\Delta_{rt}}\right)\frac{\sigma_z}{2} + \frac{|g_2|^2}{\Delta_{rt} + E_C/\hbar}\hat{a}_r^\dagger \hat{a}_r \\ &- \frac{|g_1|^2 E_C/\hbar}{\Delta_{st}(\Delta_{st} + E_C/\hbar)}\hat{a}_s^\dagger \hat{a}_s \sigma_z - \frac{|g_2|^2 E_C/\hbar}{\Delta_{rt}(\Delta_{rt} + E_C/\hbar)}\hat{a}_r^\dagger \hat{a}_r \sigma_z\end{aligned} \tag{31}$$

up to an overall constant. Again, the contributions from each oscillator-transmon coupling stated in Ref. [13] are added independently. The frequency shifts of LC oscillators seem to be different compared with Equation (25), but this is due to a subtle difference of physical interpretation. The coefficients δ_s, δ_r in Equation (25) are the frequency shifts when the transmon is in the ground state, while the coefficients of $\hat{a}_s^\dagger \hat{a}_s$, $\hat{a}_r^\dagger \hat{a}_r$ in Equation (31) are the average of the frequency shifts when the transmon is in the ground state and excited state. With the $\hat{a}_s^\dagger \hat{a}_s \sigma_z$, $\hat{a}_r^\dagger \hat{a}_r \sigma_z$ terms in consideration, both Equations (22) and (31) give the same energy spectrum when considering up to the first excitation of the transmon.

3. Discussion

We proposed an ordering of bosonic operators to efficiently compute the Schrieffer–Wolff transformation generator and energy corrections. This formalism was applied to a system with a transmon coupled to two different LC oscillators to model a quantum memory and readout device demonstrated in Ref. [8]. We solved the normal ordering problem for an operator that appears in the second-order energy correction, so that shifts in physical parameters such as frequency, anharmonicity, and cross Kerr coefficients can be directly read off from the normal-ordered form.

Our proposed method can be directly applied to systems consisting of LC circuits coupled with multiple transmons, and even to systems that have nonlinear couplings provided that the couplings represent a definite number of excitations or de-excitations in the Fock basis. It is possible to generalize this method to incorporate fermionic operators in this formalism, which can be used to reproduce the results of the original application of Schrieffer–Wolff transformation to the Anderson impurity model as in Appendix C. With such a general method, one can analyze a wide range of time-independent systems.

Quantum illumination, an example of quantum information technology, uses entangled light to achieve higher detection rate of a target with low-reflectivity. The idler mode, a part of the entangled light, should be stored in a quantum memory for ideal operation. Our method was used to analyze a demonstrated quantum memory and can be used to analyze other systems operating in various quantum technologies. For further research, it is required to find methods to store and release the propagating idler mode efficiently [19], leading to applications of quantum memories to quantum illumination.

Author Contributions: D.-H.K. and S.-Y.L. initiated the project. D.-H.K. analyzed the details. Y.J., D.Y.K., Z.K. and T.J. provided guidance. T.J. supervised the whole project. D.-H.K. wrote the manuscript with input from all authors. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by a grant to Defense-Specialized project funded by Defense Acquisition Program Administration and Agency for Defense Development.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Appendix A. Derivation of Hamiltonian from Circuit QED

In this section, we follow the quantization method of Ref. [20] and obtain various physical quantities, such as the normal mode frequency of each oscillator and the couplings of modes in terms of circuit parameters $L_i, C_i, C_{c1}, C_{c2} (i = s, t, r)$. Let ϕ_i be the flux variable at node $i (i = s, t, r)$ as labeled in Figure 1b. The corresponding (linear) Lagrangian for this system is

$$\mathcal{L} = \frac{1}{2}\left(C_s\dot{\phi_s}^2 + C_t\dot{\phi_t}^2 + C_r\dot{\phi_r}^2 + C_{c1}(\dot{\phi_s} - \dot{\phi_t})^2 + C_{c2}(\dot{\phi_t} - \dot{\phi_r})^2 \right) - \frac{1}{2}\left(\frac{\phi_s^2}{L_s} + \frac{\phi_t^2}{L_t} + \frac{\phi_r^2}{L_r} \right) \tag{A1}$$

The conjugate variables are $q_i := \partial\mathcal{L}/\partial\dot{\phi}_i$ and the Hamiltonian $\mathcal{H}$ is

$$\begin{aligned} \mathcal{H} = &\frac{1}{2\overline{C}^3}\begin{bmatrix} q_s & q_t & q_r \end{bmatrix}\begin{bmatrix} \overline{C}_s^2 & C_{c1}(C_r + C_{c2}) & C_{c1}C_{c2} \\ C_{c1}(C_r + C_{c2}) & \overline{C}_t^2 & C_{c2}(C_s + C_{c1}) \\ C_{c1}C_{c2} & C_{c2}(C_s + C_{c1}) & \overline{C}_r^2 \end{bmatrix}\begin{bmatrix} q_s \\ q_t \\ q_r \end{bmatrix} \\ &+ \frac{1}{2}\begin{bmatrix} \phi_s & \phi_t & \phi_r \end{bmatrix}\begin{bmatrix} L_s^{-1} & & \\ & L_t^{-1} & \\ & & L_r^{-1} \end{bmatrix}\begin{bmatrix} \phi_s \\ \phi_t \\ \phi_r \end{bmatrix}, \end{aligned} \tag{A2}$$

$$\begin{aligned} \overline{C}^3 := &C_sC_tC_r + C_sC_tC_{c2} + C_sC_rC_{c1} + C_sC_rC_{c2} + C_tC_rC_{c1} \\ &+ C_sC_{c1}C_{c2} + C_tC_{c1}C_{c2} + C_rC_{c1}C_{c2}, \end{aligned} \tag{A3}$$

$$\overline{C}_s^2 := C_tC_r + C_tC_{c2} + C_rC_{c1} + C_rC_{c2} + C_{c1}C_{c2}, \tag{A4}$$

$$\overline{C}_t^2 := (C_s + C_{c1})(C_r + C_{c2}), \tag{A5}$$

$$\overline{C}_r^2 := C_sC_t + C_sC_{c1} + C_tC_{c1} + C_sC_{c2} + C_{c1}C_{c2}. \tag{A6}$$

Elevating q_i, ϕ_i to canonical operators $\hat{q}_i, \hat{\phi}_i$ with $[\hat{\phi}_i, \hat{q}_j] = i\hbar\delta_{ij}$ and defining creation, annihilation operators as usual gives

$$\begin{aligned} \hat{\mathcal{H}} = &\sum_{i=s,t,r} \hbar\omega_i\hat{a}_i^\dagger\hat{a}_i \\ &- \hbar g_1(\hat{a}_s^\dagger - \hat{a}_s)(\hat{a}_t^\dagger - \hat{a}_t) - \hbar g_2(\hat{a}_t^\dagger - \hat{a}_t)(\hat{a}_r^\dagger - \hat{a}_r) - \hbar g_3(\hat{a}_s^\dagger - \hat{a}_s)(\hat{a}_r^\dagger - \hat{a}_r), \end{aligned} \tag{A7}$$

$$\hat{q}_i := i\left(\frac{\hbar^2\overline{C}^3}{4L_i\overline{C}_i^2}\right)^{1/4}(\hat{a}_i^\dagger - \hat{a}_i),\ \hat{\phi}_i := \left(\frac{\hbar^2 L_i\overline{C}_i^2}{4\overline{C}^3}\right)^{1/4}(\hat{a}_i^\dagger + \hat{a}_i),\ \omega_i^{-2} := L_i\overline{C}^3/\overline{C}_i^2, \tag{A8}$$

$$g_1 := \frac{C_{c1}(C_r + C_{c2})}{4(L_sL_t\overline{C}_s^2\overline{C}_t^2\overline{C}^6)^{1/4}},\ g_2 := \frac{C_{c2}(C_s + C_{c1})}{4(L_tL_r\overline{C}_t^2\overline{C}_r^2\overline{C}^6)^{1/4}},\ g_3 := \frac{C_{c1}C_{c2}}{4(L_sL_r\overline{C}_s^2\overline{C}_r^2\overline{C}^6)^{1/4}}. \tag{A9}$$

Note that in the weak coupling limit $(C_{c1}, C_{c2} \ll C_s, C_t, C_r)$, the eigen frequencies and couplings simplify to

$$\omega_i^{-2} \simeq L_iC_i,\quad g_1 \simeq \frac{C_{c1}}{4(L_sL_tC_s^3C_t^3)^{1/4}},\quad g_2 \simeq \frac{C_{c2}}{4(L_tL_rC_t^3C_r^3)^{1/4}},\quad g_3 \simeq \frac{4g_1g_2}{\omega_t}. \tag{A10}$$

The coupling between $\hat{q}_s, \hat{q}_r$ is off-diagonal of second-order, and hence, give energy corrections of third- and higher-order. Our analysis concerns up to second-order energy corrections, so we dropped this term. If one wants to consider higher-order corrections, then consideration of this coupling is necessary.

The nonlinearity of the transmon is introduced by replacing $\hat{\phi}_t^2/2L_t$ with $-\frac{\Phi_0^2}{L_t}\cos(\frac{\hat{\phi}_t}{\Phi_0})$, where $\Phi_0 = \hbar/2e$ is the flux quantum. Expanding the cosine series up to fourth-order yields

$$\begin{aligned} \frac{\hat{\mathcal{H}}}{\hbar} = &\omega_s\hat{a}_s^\dagger\hat{a}_s + \left(\omega_t - \frac{E_C}{\hbar}\right)\hat{a}_t^\dagger\hat{a}_t + \omega_r\hat{a}_r^\dagger\hat{a}_r \\ &+ g_1(\hat{a}_s^\dagger\hat{a}_t + \hat{a}_s\hat{a}_t^\dagger) + g_2(\hat{a}_t^\dagger\hat{a}_r + \hat{a}_t\hat{a}_r^\dagger) - \frac{E_C}{2\hbar}\hat{a}_t^\dagger\hat{a}_t^\dagger\hat{a}_t\hat{a}_t, \end{aligned} \tag{A11}$$

where $E_C = e^2\overline{C_t^2}/2\overline{C^3}$ is the charging energy of the transmon, which is small compared with $\hbar\omega_t$ in the transmon regime [18]. The correction to ω_t is ignored, while it can be easily recovered in the final results by just replacing ω_t with $\omega_t - E_C/\hbar$. We applied the rotating wave approximation to remove nonresonant terms such as $\hat{a}_s^\dagger\hat{a}_t^\dagger$, $\hat{a}_t^\dagger\hat{a}_t^\dagger\hat{a}_t^\dagger\hat{a}_t$ which represent the creation or destruction of two or more quanta.

Appendix B. Computational Ordering of Normal-Ordered and Antinormal-Ordered Operators

In this section, we give explicit formulas of writing normal-ordered and antinormal-ordered operators in our proposed computational ordering. They extensively use Stirling numbers of the first kind $s(n,k)$, which are the matrix elements of the basis change of monomials x^n and falling factorials $x^{\underline{n}}$ [21] (p. 824).

$$x^{\underline{n}} = \sum_{k=0}^{n} s(n,k)x^k. \tag{A12}$$

The relation of rising factorials and monomials is similar, only differing in sign.

$$x^{\overline{n}} = \sum_{k=0}^{n} (-1)^{n-k}s(n,k)x^k. \tag{A13}$$

Since the matrix elements of our computational ordered operators and normal-, antinormal-ordered operators in the Fock basis involve monomials, falling factorials, rising factorials, respectively, it is obvious that Stirling numbers will appear. The results are stated for a single bosonic operator $\hat{a}$. Extension to several bosonic operators is trivial.

$$\hat{a}^{\dagger n}\hat{a}^m = \begin{cases} \hat{a}^{\dagger n-m}(\hat{a}^\dagger\hat{a})^{\underline{m}} & = \hat{a}^{\dagger n-m}\sum_{k=0}^{m} s(m,k)(\hat{a}^\dagger\hat{a})^k \quad (n \geq m) \\ (\hat{a}^\dagger\hat{a})^{\underline{n}}\,\hat{a}^{m-n} & = \sum_{k=0}^{n} s(n,k)(\hat{a}^\dagger\hat{a})^k\hat{a}^{m-n} \quad (n \leq m) \end{cases}, \tag{A14}$$

$$\hat{a}^m\hat{a}^{\dagger n} = \begin{cases} \hat{a}^{\dagger n-m}(\hat{a}^\dagger\hat{a}+n)^{\underline{m}} & = \hat{a}^{\dagger n-m}\sum_{k=0}^{m} s(m,k)(\hat{a}^\dagger\hat{a}+n)^k \quad (n \geq m) \\ (\hat{a}^\dagger\hat{a}+m)^{\underline{n}}\,\hat{a}^{m-n} & = \sum_{k=0}^{n} s(n,k)(\hat{a}^\dagger\hat{a}+m)^k\hat{a}^{m-n} \quad (n \leq m) \end{cases}. \tag{A15}$$

To read off anharmonicity and cross Kerr coefficients as in Equation (23), one must know how to convert operators in our ordering into normal order. We end this section with showing that

$$\frac{1}{\hat{a}^\dagger\hat{a}+c} = \sum_{k=0}^{\infty}\frac{(-1)^k}{c^{\overline{k+1}}}\hat{a}^{\dagger k}\hat{a}^k = \frac{1}{c} - \frac{\hat{a}^\dagger\hat{a}}{c(c+1)} + \frac{\hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a}}{c(c+1)(c+2)} - \ldots \tag{A16}$$

where c is not a nonpositive integer. This is equivalent to finding α_k such that

$$\frac{1}{n+c} = \sum_{k=0}^{n}\alpha_k n^{\underline{k}}. \tag{A17}$$

Since $(n^{\underline{k}})_{nk}$ is a lower diagonal matrix, its inverse exists. The inverse matrix is easily shown to be the lower diagonal matrix

$$\left(\frac{(-1)^{n+k}}{k!(n-k)!}\right)_{nk}. \tag{A18}$$

Then, the coefficients α_k become

$$\alpha_k = \sum_{n=0}^{k}\frac{(-1)^{n+k}}{n!(k-n)!}\frac{1}{n+c} = \frac{(-1)^k}{k!c}\,{}_2F_1(c,-k;c+1;1) = \frac{(-1)^k}{c^{\overline{k+1}}} \tag{A19}$$

which proves Equation (A16). Here, ${}_2F_1(a,b;c;z)$ is the hypergeometric function [21] (p. 556).

Appendix C. Generalization to Fermionic Operators

In this section, we adapt our formalism to fermionic operators and apply it to the Anderson impurity model. We consider n fermionic modes, described by operators $\{\hat{b}_i, \hat{b}_j^\dagger\} = \delta_{ij}$, $\{\hat{b}_i, \hat{b}_j\} = 0$, $\{\hat{b}_i^\dagger, \hat{b}_j^\dagger\} = 0$, where $\hat{b}_i$ is the annihilation operator of the i-th mode. We write operators in the following order as in Equation (3),

$$\hat{b}_I^\dagger f(\hat{b}^\dagger\hat{b})\hat{b}_J, \tag{A20}$$

where $\hat{b}^\dagger\hat{b} = (\hat{b}_1^\dagger\hat{b}_1, \ldots, \hat{b}_n^\dagger\hat{b}_n)$ is an n tuple and $I = \{i_1, \ldots, i_k\}$, $J = \{j_1, \ldots, j_\ell\}$ are disjoint subsets of $\{1, 2, \ldots, n\}$. The operators are defined as $\hat{b}_I^\dagger = \hat{b}_{i_1}^\dagger \ldots \hat{b}_{i_k}^\dagger$, $\hat{b}_J = \hat{b}_{j_1}^\dagger \ldots \hat{b}_{j_\ell}^\dagger$. We take $i_1 < i_2 < \cdots < i_k$, $j_1 < j_2 < \cdots < j_\ell$ to fix ordering and require I, J be disjoint for the ordering to be unique. Since $\hat{b}_i$ are fermionic operators, f is essentially a function defined on $\{0,1\}^n$ and if $i \in I \cup J$, then f is independent of the i-th variable.

We split the Hamiltonian into diagonal and off-diagonal terms,

$$\hat{\mathcal{H}} = f(\hat{b}^\dagger\hat{b}) + \sum_{I,J} \hat{b}_I^\dagger g_{IJ}(\hat{b}^\dagger\hat{b})\hat{b}_J. \tag{A21}$$

The sum is over all disjoint subsets I, J of $\{1, 2, \ldots, n\}$ where both are not the null set. The hermiticity of $\hat{\mathcal{H}}$ makes f a real valued function and $g_{IJ}^* = g_{JI}$. One then computes the commutator of $\hat{b}_I^\dagger$, $\hat{b}_J$ with $f(\hat{b}^\dagger\hat{b})$:

$$[\hat{b}_I^\dagger, f(\hat{b}^\dagger\hat{b})] = \hat{b}_I^\dagger\{f(I=0) - f(I=1)\}, \tag{A22}$$

$$[\hat{b}_J, f(\hat{b}^\dagger\hat{b})] = \{f(J=1) - f(J=0)\}\hat{b}_J. \tag{A23}$$

Here, $f(I=0)$ is the operator obtained from $f(\hat{b}^\dagger\hat{b})$ by replacing $\hat{b}_i^\dagger\hat{b}_i$ with 0 for all $i \in I$ and other operators are defined similarly. This can be seen from noting that $\hat{b}_I^\dagger f(\hat{b}^\dagger\hat{b}) = \hat{b}_I^\dagger f(I=0)$, $f(\hat{b}^\dagger\hat{b})\hat{b}_I^\dagger = \hat{b}_I^\dagger f(I=1)$ and similar relations hold for $\hat{b}_J$. Hence the commutator $[\hat{b}_I^\dagger h_{IJ}(\hat{b}^\dagger\hat{b})\hat{b}_J, f(\hat{b}^\dagger\hat{b})]$ is

$$[\hat{b}_I^\dagger\, h_{IJ}(\hat{b}^\dagger\hat{b})\, \hat{b}_J, f(\hat{b}^\dagger\hat{b})] = \hat{b}_I^\dagger\, h_{IJ}(\hat{b}^\dagger\hat{b})\{f(I=0,\ J=1) - f(I=1\ J=0)\}\, \hat{b}_J. \tag{A24}$$

Now we take $h_{IJ}(\hat{b}^\dagger\hat{b})$ as follows to ensure $[\hat{S}, \hat{H}_0] = -\hat{V}$:

$$h_{IJ}(\hat{b}^\dagger\hat{b}) := \frac{g_{IJ}(\hat{b}^\dagger\hat{b})}{f(I=1,J=0) - f(I=0,J=1)}, \tag{A25}$$

$$\hat{S} := \sum_{IJ} \hat{b}_I^\dagger\, h_{IJ}(\hat{b}^\dagger\hat{b})\, \hat{b}_J. \tag{A26}$$

h_{IJ} does not have the terms $\hat{b}_i^\dagger\hat{b}_i$ if $i \in I \cup J$.

The diagonal contribution of $\frac{1}{2}[\hat{S}, \hat{V}]$ comes from the terms

$$\begin{aligned}&[\hat{b}_I^\dagger\, h_{IJ}(\hat{b}^\dagger\hat{b})\, \hat{b}_J, \hat{b}_J^\dagger\, g_{IJ}(\hat{b}^\dagger\hat{b})\, \hat{b}_I] \\ &= \frac{(-1)^{s(|I|)+s(|J|)}|g_{IJ}(\hat{b}^\dagger\hat{b})|^2}{f(I=1,\ J=0) - f(I=0,\ J=1)}\Big\{(\hat{b}^\dagger\hat{b})_I(1-\hat{b}^\dagger\hat{b})_J - (1-\hat{b}^\dagger\hat{b})_I(\hat{b}^\dagger\hat{b})_J\Big\}.\end{aligned} \tag{A27}$$

Here $s(n) := \frac{1}{2}n(n-1)$ counts the number of anticommutators needed in ordering products like $\hat{b}_I^\dagger\hat{b}_I$. For $I = \{i_1, \ldots, i_k\}$ with $i_1 < i_2 < \cdots < i_k$, we define $(\hat{b}^\dagger\hat{b})_I := \hat{b}_{i_1}^\dagger\hat{b}_{i_1} \ldots \hat{b}_{i_k}^\dagger\hat{b}_{i_k}$, $(1-\hat{b}^\dagger\hat{b})_I := (1-\hat{b}_{i_1}^\dagger\hat{b}_{i_1}) \ldots (1-\hat{b}_{i_k}^\dagger\hat{b}_{i_k})$. As before, the commutator is symmetric in I,J, so the total diagonal contribution becomes

$$\frac{1}{2}[\hat{S},\hat{V}]_{(d)} = \sum_{IJ}(-1)^{s(|I|)+s(|J|)}\frac{(\hat{b}^\dagger\hat{b})_I(1-\hat{b}^\dagger\hat{b})_J|g_{IJ}(\hat{b}^\dagger\hat{b})|^2}{f(I=1,\ J=0)-f(I=0,\ J=1)}. \tag{A28}$$

We end this appendix with an application to the Anderson impurity model. To simplify equations, we only consider the interaction of one conduction electron $\hat{b}$ and one localized orbital with two spin configurations possible, $\hat{c}_+$, $\hat{c}_-$. Under this simplification, the Hamiltonian reads

$$\hat{\mathcal{H}} = \epsilon\hat{b}^\dagger\hat{b} + \epsilon_c\hat{c}_+^\dagger\hat{c}_+ + \epsilon_c\hat{c}_-^\dagger\hat{c}_- + U\hat{c}_+^\dagger\hat{c}_+\hat{c}_-^\dagger\hat{c}_- + \sum_{s=+,-} V\hat{b}^\dagger\hat{c}_s + V^*\hat{b}\hat{c}_s^\dagger. \tag{A29}$$

U represents the Coulomb repulsion between the two electrons in the same orbital with opposite spin, and V represents the coupling between conduction electrons and the localized orbital. Using $\hat{b}, \hat{c}_+, \hat{c}_-$ as a bias ordering, we define functions

$$f(n,m,\ell) := \epsilon n + \epsilon_c m + \epsilon_c\ell + Um\ell, \tag{A30}$$

$$g_{12}(n,m,\ell) = g_{13}(n,m,\ell) := V. \tag{A31}$$

Then using our result Equation (A26), the transformation generator becomes

$$\hat{S} = \hat{b}^\dagger h_{12}\hat{c}_+ + \hat{b}^\dagger h_{13}\hat{c}_- - \text{H.C.} \tag{A32}$$

$$= \sum_{s=+,-}\hat{b}^\dagger\frac{V}{(\epsilon+\epsilon_c\hat{c}_{-s}^\dagger\hat{c}_{-s}) - (\epsilon_c+\epsilon_c\hat{c}_{-s}^\dagger\hat{c}_{-s}+U\hat{c}_{-s}^\dagger\hat{c}_{-s})}\hat{c}_s - \text{H.C.} \tag{A33}$$

$$= \sum_{s=+,-}\hat{b}^\dagger V\left\{\frac{1}{\epsilon-\epsilon_c} + \left(\frac{1}{\epsilon-\epsilon_c+U} - \frac{1}{\epsilon-\epsilon_c}\right)\hat{c}_{-s}^\dagger\hat{c}_{-s}\right\}\hat{c}_s - \text{H.C.}, \tag{A34}$$

which is the form obtained in Ref. [15].

References

1. Ladd, T.D.; Jelezko, F.; Laflamme, R.; Nakamura, Y.; Monroe, C.; O'Brien, J.L. Quantum computers. *Nature* **2010**, *464*, 45–53. [CrossRef] [PubMed]
2. Bhaskar, M.K.; Riedinger, R.; Machielse, B.; Levonian, D.S.; Nguyen, C.T.; Knall, E.N.; Park, H.; Englund, D.; Loncar, M.; Sukachev, D.D.; et al. Experimental demonstration of memory-enhanced quantum communication. *Nature* **2020**, *580*, 60–66. [CrossRef] [PubMed]
3. Lloyd, S. Enhanced Sensitivity of Photodetection via Quantum Illumination. *Science* **2008**, *321*, 1463–1465. [CrossRef] [PubMed]
4. Tan, S.; Erkmen, B.I.; Giovannetti, V.; Guha, S.; Lloyd, S.; Maccone, L.; Pirandola, S.; Shapiro, J.H. Quantum Illumination with Gaussian States. *Phys. Rev. Lett.* **2008**, *101*, 253601. [CrossRef] [PubMed]
5. Guha, S.; Erkmen, B.I. Gaussian-state quantum-illumination receivers for target detection. *Phys. Rev. A* **2009**, *80*, 052310. [CrossRef]
6. Jo, Y.; Lee, S.; Ihn, Y.S.; Kim, Z.; Lee, S.-Y. Quantum illumination receiver using double homodyne detection. *Phys. Rev. Res.* **2021**, *3*, 013006. [CrossRef]
7. Lee, S.-Y.; Jo, Y.; Jeong, T.; Kim, J.; Kim, D.H.; Kim, D.; Kim, D.Y.; Ihn, Y.S.; Kim, Z. Optimal observables for Gaussian illumination. *arXiv* **2021**, arXiv:2106.12109.
8. Reagor, M.; Pfaff, W.; Axline, C.; Heeres, R.W.; Ofek, N.; Sliwa, K.; Holland, E.; Wang, C.; Blumoff, J.; Chou, K.; et al. Quantum memory with millisecond coherence in circuit QED. *Phys. Rev. B* **2016**, *94*, 014506. [CrossRef]
9. Palomaki, T.A.; Harlow, J.W.; Teufel, J.D.; Simmonds, R.W.; Lehnert, K.W. Coherent state transfer between itinerant microwave fields and a mechanical oscillator. *Nature* **2013**, *495*, 210–214. [CrossRef] [PubMed]
10. Julsgaard, B.; Grezes, C.; Bertet, P.; Molmer, K. Quantum Memory for Microwave Photons in an Inhomogeneously Broadened Spin Ensemble. *Phys. Rev. Lett.* **2013**, *110*, 250503. [CrossRef] [PubMed]
11. Ranjan, V.; O'Sullivan, J.; Albertinale, E.; Albanaese, B.; Chaneliere, T.; Schenkel, T.; Vion, D.; Esteve, D.; Flurin, E.; Morton, J.J.L.; et al. Multimode storage of quantum microwave field in electron spins over 100 ms. *Phys. Rev. Lett.* **2020**, *125*, 210505. [CrossRef]
12. Heeres, R.W.; Vlastakis, B.; Holland, E.; Krastanov, S.; Albert, V.V.; Frunzio, L.; Jiang, L.; Schoelkopf, R.J. Cavity State Manipulation Using Photon-Number Selective Phase Gates. *Phys. Rev. Lett.* **2015**, *115*, 137002. [CrossRef] [PubMed]
13. Koch, J.; Yu, T.M.; Gambetta, J.; Houck, A.A.; Schuster, D.I.; Majer, J.; Blais, A.; Devoret, M.H.; Girvin, S.M.; Schoelkopf, R.J. Charge-insensitive qubit design derived from the Cooper pair box. *Phys. Rev. A* **2007**, *76*, 042319. [CrossRef]
14. Zhu, G.; Ferguson, D.G.; Manucharyan, V.E.; Koch, J. Circuit QED with fluxonium qubits: Theory of the dispersive regime. *Phys. Rev. B* **2013**, *87*, 024510. [CrossRef]
15. Schrieffer, J.R.; Wolff, R.A. Relation between the Anderson and Kondo Hamiltonians. *Phys. Rev.* **1966**, *149*, 491. [CrossRef]

16. Cohen-Tannoudji, C.; Dupont-Roc, J.; Grynberg, G. *Atom-Photon Interactions: Basic Processes and Applications*; Wiley-VCH: Weinheim, Germany, 1998; Chapter B-1.
17. Bravyi, S.; DiVincenzo, D.; Loss, D. Schrieffer–Wolff transformation for quantum many-body systems. *Ann. Phys.* **2011**, *326*, 2793–2826. [CrossRef]
18. Blais, A.; Grimsmo, A.L.; Grivin, S.M.; Wallraff, A. Circuit quantum electrodynamics. *Rev. Mod. Phys.* **2021**, *93*, 025005. [CrossRef]
19. Pfaff, W.; Axline, C.J.; Burkhart, L.D.; Vool, U.; Reinhold, P.; Frunzio, L.; Jiang, L.; Devoret, M.H.; Schoelkopf, R.J. Controlled release of multiphoton quantum states from a microwave cavity memory. *Nat. Phys.* **2017**, *13*, 882–887. [CrossRef]
20. Vool, U.; Devoret, M.H. Introduction to Quantum Electromagnetic Circuits. *Int. J. Circ. Theor. Appl.* **2017**, *45*, 897–934. [CrossRef]
21. Abramowitz, M.; Stegun, I. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. National Bureau of Standards Applied Mathematics Series 55. Tenth Printing*; National Bureau of Standards (NBS): Washington, DC, USA, 1972.

entropy

MDPI

Article

Entanglement-Assisted Joint Monostatic-Bistatic Radars

Ivan B. Djordjevic

Department of Electrical and Computer Engineering, University of Arizona, 1230 E. Speedway Blvd., Tucson, AZ 85721, USA; ivan@email.arizona.edu; Tel.: +1-520-626-5119

Abstract: With the help of entanglement, we can build quantum sensors with sensitivity better than that of classical sensors. In this paper we propose an entanglement assisted (EA) joint monostatic-bistatic quantum radar scheme, which significantly outperforms corresponding conventional radars. The proposed joint monostatic-bistatic quantum radar is composed of two radars, one having both wideband entangled source and EA detector, and the second one with only an EA detector. The optical phase conjugation (OPC) is applied on the transmitter side, while classical coherent detection schemes are applied in both receivers. The joint monostatic-bistatic integrated EA transmitter is proposed suitable for implementation in $LiNbO_3$ technology. The detection probability of the proposed EA joint target detection scheme outperforms significantly corresponding classical, coherent states-based quantum detection, and EA monostatic detection schemes. The proposed EA joint target detection scheme is evaluated by modelling the direct radar return and forward scattering channels as both lossy and noisy Bosonic channels, and assuming that the distribution of entanglement over idler channels is not perfect.

Keywords: entanglement; radars; quantum sensing; quantum radars; entanglement assisted detection

Citation: Djordjevic, I.B. Entanglement-Assisted Joint Monostatic-Bistatic Radars. *Entropy* **2022**, *24*, 756. https://doi.org/10.3390/e24060756

Academic Editor: Osamu Hirota

Received: 5 May 2022
Accepted: 25 May 2022
Published: 26 May 2022

1. Introduction

The entanglement represents a unique quantum information processing (QIP) attribute [1–7] that enables: (1) outperforming classical sensors sensitivity [1,2,5], (2) unconditional security for future communication networks [1,3,5,6], and (3) beating the classical channel capacities [8–10]. Further, the pre-shared entanglement enables distributed quantum sensing [1,7] and secure distributed quantum computing [11].

One of the key motivations behind the quantum target detection studies is to outperform the quantum limit of classical sensors [12]. The quantum radars have several advantages compared to corresponding classical counterparts: improved receiver sensitivity, better detection probability of targets, in particular in a low signal-to-noise ratio (SNR) regime, improved synthetic-aperture radar imaging quality, improved detection through clouds and fog (in particular when microwave photons are used), better resilience to jamming, and higher cross-section (as shown in [12]), to mention few. Moreover, the quantum radar signals are more difficult to detect compared to classical radars. On the other hand, the quantum radars are much more difficult to implement in practice. Recently, two popular quantum radar designs emerged: (i) the quantum radar employing Lloyd's quantum illumination sensing concept [13] and (ii) interferometric quantum radar. For further details on various quantum radars concepts and classification of different quantum radar techniques an interested reader is referred to [14–19].

In this paper, we propose an entanglement assisted (EA) joint monostatic-bistatic quantum radar detection scheme with corresponding operational principle being depicted in Figure 1. The wideband entangled source generates two entangled pair of photons, each pair containing signal and idler photons. The idler photons are kept in the quantum memories of the receivers. Both signal photons are transmitted with the help of corresponding expanding telescopes over noisy, lossy, and atmospheric turbulent channel towards the target. Directly reflected photon is collected by the compressing telescope and detected

by the first radar receiver, while the forward scattered photon is collected by the second compressing telescope and detected by the second radar receiver. The quantum correlation is utilized on receive sides to improve overall target detection probability. Inherent spatial diversity is exploited to improve the overall SNR. Additional description of the proposed joint monostatic-bistatic radar scheme is provided in Section 3.

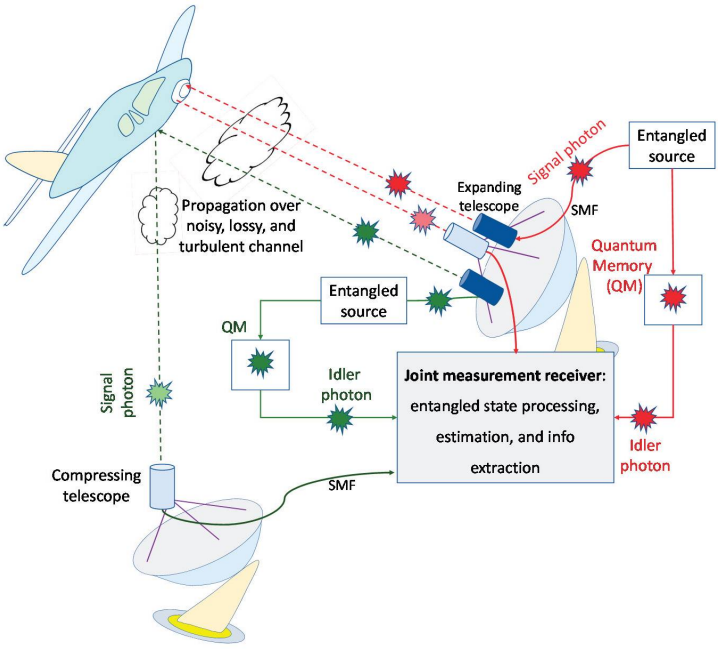


Figure 1. The proposed EA joint monostatic-bistatic quantum radar technique.

To simplify design and at the same time improve the target detection probability we apply the optical phase conjugation (OPC) on the transmitter side rather than the receive side. We propose the joint monostatic-bistatic integrated EA transmitter that is suitable for implementation in $LiNbO_3$ technology. The EA detectors are based on classical coherent detection with idler mode having the same role as the local oscillator (LO) laser signal. We show that the proposed EA joint target detection scheme significantly outperforms coherent states-based quantum detection, EA monostatic, and classical radar counterparts. We further evaluate the proposed EA joint target detection scheme by modelling both directly reflected mode channel and forward scattered mode channel as lossy and noisy Bosonic channels. Finally, we assume that the distribution of entanglement over the idler channels is not perfect.

The paper is organized as follows. The EA monostatic radar concept is introduced in Section 2, which is used as a reference case. The proposed EA joint monostatic-bistatic radar scheme, employing the OPC on the transmitter side and coherent detection on the receiver sides, is described in Section 3. Both directly reflected (return) signal mode and forward scattered signal mode channels are modeled as lossy and noisy Bosonic channels. The idler channels are also modelled as lossy and noisy Bosonic channels. In Section 4 we evaluate the detection probability performances of the proposed EA joint monostatic-bistatic radar target detection scheme and compare it against coherent states-based quantum detection, EA monostatic detection, and classical detection schemes. The relevant concluding remarks are given in the last section (Section 5).

2. Entanglement Assisted Monostatic Radars

In this section, we describe the entanglement assisted monostatic radar target detection scheme, shown in Figure 2, employing the Gaussian states generated through the continuous-wave spontaneous parametric down conversion (SPDC) process. The SPDC-based entangled source represents a broadband source having $D = T_m W$ i.i.d. signal-idler photon pairs, where T_m is the measurement interval and W is the phase-matching SPDC bandwidth. Each signal-idler photons pair, which for monostatic radar are denoted as red photons in Figure 2, is in fact a two-mode squeezed vacuum (TMSV) state whose representation in Fock basis is given by:

$$|\psi\rangle_{s,i} = \frac{1}{\sqrt{N_s+1}} \sum_{n=0}^{\infty} \left(\frac{N_s}{N_s+1}\right)^{n/2} |n\rangle_s |n\rangle_i, \tag{1}$$

where $N_s = \langle \hat{a}_s^\dagger \hat{a}_s \rangle = \langle \hat{a}_i^\dagger \hat{a}_i \rangle$ is the mean photon number per mode, with corresponding signal and idler creation operators being denoted by $\hat{a}_s^\dagger$ and $\hat{a}_i^\dagger$, respectively. The signal-idler entanglement is characterized by the phase-sensitive cross-correlation (PSCC) coefficient, defined as $\langle \hat{a}_s \hat{a}_i \rangle = \sqrt{N_s(N_s+1)}$, which can be considered as the quantum limit.

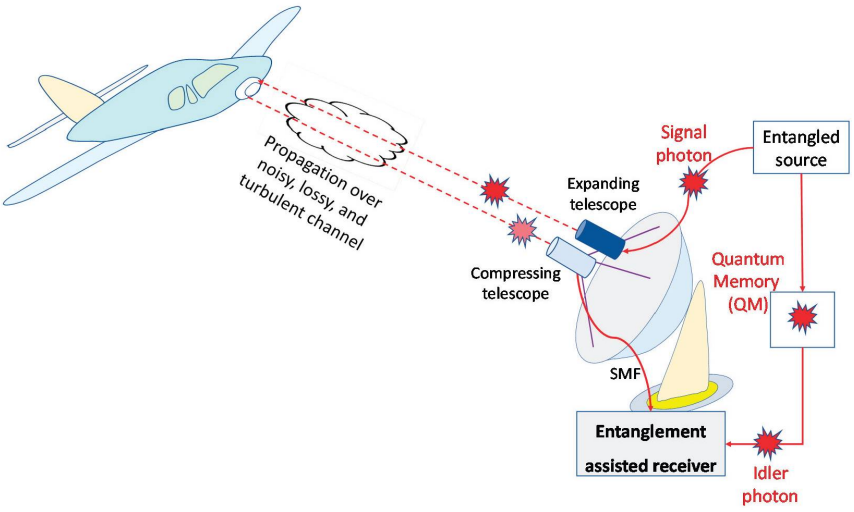


Figure 2. The EA monostatic quantum radar.

The TMSV state represents a pure maximally entangled zero-mean Gaussian state with the following Wigner covariance matrix:

$$\mathbf{\Sigma}_{TMSV} = \begin{bmatrix} (2N_s+1)\mathbf{1} & 2\sqrt{N_s(N_s+1)}\mathbf{Z} \\ 2\sqrt{N_s(N_s+1)}\mathbf{Z} & (2N_s+1)\mathbf{1} \end{bmatrix}, \tag{2}$$

where $\mathbf{Z} = \mathrm{diag}(1, -1)$ denotes the Pauli Z-matrix and $\mathbf{1}$ denotes the identity matrix. Clearly, in the low-brightness regime $N_s << 1$, the PSCC is $\langle \hat{a}_s \hat{a}_i \rangle \approx \sqrt{N_s}$ that is much larger than the corresponding classical limit N_s. As described earlier, by going back to Figure 2, the entangled source is used on the transmitter side to generate quantum correlated signal photon (probe) and idler photon, which serves as a local reference. With the help of the expanding telescope, the signal photon is transmitted over a noisy, lossy, and atmospheric turbulent channel towards the target. The reflected photon (the radar return) is collected by the compressing telescope and detected by the radar's receiver, and the quantum correlation between radar return and retained reference (idler photon) is exploited on receive side to improve the receiver sensitivity. The interaction between the probe (signal) photon and the target can be described by a beam splitter of transmissivity $T^{(r)}$. Therefore, we can model

the radar transmitter-target-radar receiver (directly reflected mode) channel (direct return channel) as a lossy thermal Bosonic channel

$$\hat{a}_{\mathrm{Rx}}^{(r)}(\varphi) = \sqrt{T^{(r)}}e^{-j\varphi^{(r)}}\hat{a}_s + \sqrt{1-T^{(r)}}\hat{a}_b^{(r)}, \tag{3}$$

where $\hat{a}_b^{(r)}$ is a background (thermal) state of the direct return channel with the mean photon number being $\left(1-T^{(r)}\right)\left\langle \hat{a}_b^{(r)\dagger}\hat{a}_b^{(r)}\right\rangle = N_b$. With $\varphi^{(r)}$ we denoted signal-mode phase shift introduced by the target and channel. The idler-mode channel is also modelled as the lossy and noisy Bosonic channel

$$\hat{a}_{\mathrm{Rx,\ idler}} = \sqrt{T^{(i)}}\hat{a}_i + \sqrt{1-T^{(i)}}\hat{a}_b^{(i)}, \tag{4}$$

where $T^{(i)}$ is transmissivity of the idler channel and $\hat{a}_b^{(i)}$ is the annihilation operator of the background (thermal) mode of the idler channel with the mean photon number being $\left(1-T^{(i)}\right)\left\langle \hat{a}_b^{(i)\dagger}\hat{a}_b^{(i)}\right\rangle = N_b^{(i)}$. The radar returned probe and retained reference (stored idler) can be described by the following covariance matrix:

$$\mathbf{\Sigma}_t = \begin{bmatrix} (2N_s+1)\mathbf{1} & 2\sqrt{T^{(r)}T^{(i)}N_s(N_s+1)}\mathbf{Z}\delta_{1t} \\ 2\sqrt{T^{(r)}T^{(i)}N_s(N_s+1)}\mathbf{Z}\delta_{1t} & \left(2N_s^{(r)}+1\right)\mathbf{1} \end{bmatrix}, \tag{5}$$

where $N_s^{(r)} = (T^{(i)}N_s + N_b^{(i)})T^{(r)} + N_b$. We use t to denote the target indicator. In the absence of the target, we have that $t = 0$ and in this case the return signal does not contain probe, just the background noise, and the covariance matrix is diagonal. On the other hand, in the presence of the target, we have that $t = 1$ and antidiagonal terms, representing the quantum correlation between the signal and idler, are non-zero.

The EA monostatic radar receiver may use the optical parametric amplifier (OPA), shown in Figure 3, with a low gain $G - 1 = \varepsilon << 1$, to obtain:

$$\hat{a}^{(r)}\left(\varphi^{(r)}\right) = \sqrt{G}\,\hat{a}_{\mathrm{Rx,\ idler}} + \sqrt{G-1}\,\hat{a}_{\mathrm{Rx}}^{(r)\dagger}\left(\varphi^{(r)}\right) \tag{6}$$

for each signal-idler pair of a given mode. The direct detection of the OPA has the following mean photon number $\overline{N}\left(\varphi^{(r)}\right) = \left\langle [\hat{a}^{(r)}(\varphi^{(r)})]^{\dagger}\hat{a}^{(r)}(\varphi^{(r)})\right\rangle$.

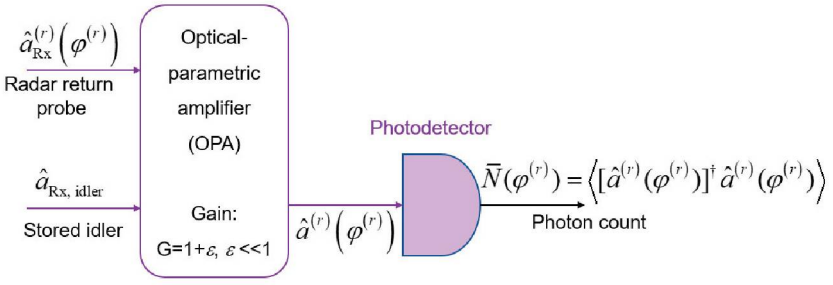


Figure 3. The optical-parametric amplifier (OPA)-based EA target detection receiver.

Zhang et al. have shown in ref. 19 that the OPA-based EA receiver, for ideal distribution of the idler ($T^{(i)} = 1$), provides ≤ 3 dB improvement over corresponding classical receiver. In the presence of experimental imperfections, the improvement was reduced to 1 dB, as shown in [19]. Given that the OPC receiver outperforms the OPA receiver [1,9,10], here we propose an EA joint monostatic-bistatic target detection scheme that employs the OPC on the transmitter side and classical coherent detection on both receiving ends, with details provided in following section.

3. Proposed Entanglement Assisted Joint Monostatic-Bistatic Radar Detection Scheme

In this section, we describe our proposed entanglement assisted joint monostatic-bistatic radar detection concept, shown in Figure 1, which is inspired by our recently proposed EA communication system [10]. The proposed joint monostatic-bistatic integrated ($LiNbO_3$ technology-based) EA transmitter, with transmit side OPC, is provided in Figure 4. The phase modulator or I/Q modulator is optional here. We perform the OPC operation through the difference frequency generation (DFG) process by using the periodically poled $LiNbO_3$ (PPLN) waveguide. In the first PPLN waveguide, the SPDC concept is utilized to generate signal-idler photon pairs, which get separated by the Y-junction. Given that the SPDC is the wideband process, a large number of signal-idler photon pairs are generated so that we use subscript k to denote the kth signal-kth idler photon pair. In the second PPLN, the DFG interaction of the pump photon ω_p and signal photon $\omega_{s,k}$ takes place and the phase-conjugated (PC) photon at radial frequency $\omega_p - \omega_{s,k}$ is generated. We further use the wavelength division demultiplexer to separate the signal/idler photons corresponding to monostatic and bistatic transmitters/receivers, as shown in Figure 1. As an illustrative example, for the strong pump at $\lambda_p = 780$ nm, through the SPDC the following signal-idler pairs can be generated: (1) the idler photon 1 at $\lambda_{i,1} = 1535$ nm—the signal photon 1 at wavelength $\lambda_{s,1} = 1585.8$ nm and (2) the idler photon 2 at $\lambda_{i,2} = 1545$ nm—the signal photon 2 at wavelength $\lambda_{s,2} = 1575.3$ nm. After the OPC PPLN waveguide, the signal photon 1 interacts with the pump photon through DFG to get the PC signal photon at $\lambda_{s,1,PC} = 1/(1/\lambda_p - 1/\lambda_{s,1}) = 1530$ nm, which is the same wavelength as that of the idler photon 1. In a similar fashion, after the OPC PPLN waveguide the signal photon 2 interacts with the pump photon through DFG to get the PC signal photon at $\lambda_{s,2,PC} = 1/(1/\lambda_p - 1/\lambda_{s,2}) = 1545$ nm, representing the same wavelength as that of the idler photon 2. In Figure 4 we use s to denote a signal constellation point imposed by either phase modulator or I/Q modulator. For M-ary PSK s is simply $\exp(j\theta_{mod})$, where $\theta_{mod} \in \{0, 2\pi/M, \ldots, (M-1)\,2\pi/M\}$.

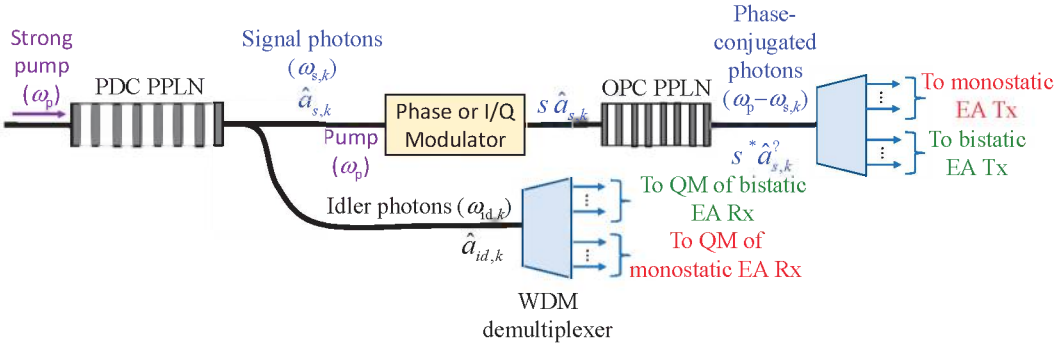


Figure 4. Joint monostatic-bistatic $LiNbO_3$ technology-based integrated EA transmitter with transmit side OPC. PDC: parametric down conversion, OPC: optical phase-conjugation, PPLN: periodically poled $LiNbO_3$ waveguide, QM: quantum memory.

By performing the OPC on the transmitter side, conventional-classical balanced coherent detection receiver can be applied on receive sides of monostatic and bistatic radars (see Figure 1), with one such receiver being provided in Figure 5. Evidently, the OPC radar direct return probe/forward scattered probe and idlers modes are mixed on balanced beam splitter, followed by two photodiodes. The idler mode for each EA detector serves as a local (oscillator) laser signal for the homodyne coherent detection.

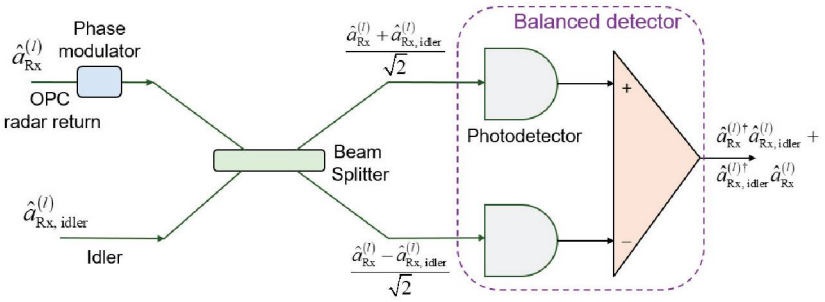


Figure 5. EA homodyne balanced detection receiver corresponding to the direct return/forward scattered components. The phase modulator is used to detect either in-phase or quadrature component of the OPC signal. Photodiode responsivity is set to 1 A/W.

For transmit-side OPC, the direct return channel r/forward scattering channel fs models can be represented by

$$\hat{a}_{Rx,k}^{(l)}\left(\varphi^{(l)}\right) = \sqrt{T^{(l)}}e^{-j\varphi^{(l)}}\hat{a}_{s,k}^{(l)\dagger} + \sqrt{1-T^{(l)}}\hat{a}_{b}^{(l)}, \tag{7}$$

where in the superscript l is used to denote either the direct return channel ($l = r$) or the forward scattering channel ($l = fs$), while subscript k is used to denote the kth signal-idler photon pair. The overall phase $\varphi^{(l)}$ is composed of three components:

$$\varphi^{(l)} = \theta_{\text{mod}} + \vartheta^{(l)} + \phi^{(l)}, \tag{8}$$

where θ_{mod} is the modulation phase (when M-ary PSK is used), while $\vartheta^{(l)}$ denotes the phase-shift introduced by the target. For the direct return probe, given that the distance between the transceiver and target is d, the phase shift introduced by the target will be $\vartheta^{(r)} = 2kd$, with k being the wave number related to the wavelength λ by $k = 2\pi/\lambda$. On the other hand, given that the distance between target and receiver in the forward scattering channel is D, the corresponding phase shift introduced by the target will be $\vartheta^{(fs)} = k(d + D)$. Finally, $\phi^{(l)}$ is the random phase shift introduced by the lth channel. The purpose of the transmit side phase modulator is to impose the sequence on the transmitter side that will be used for estimation of the random phase shift and corresponding cancelation.

The balanced detector (BD) photocurrent operator (assuming that the photodiode responsivity is 1 A/W) for EA detector, shown in Figure 5, is given by:

$$\hat{i}_{BD}^{(l)} = \left(\hat{a}_{Rx}^{(l)}\right)^{\dagger}\hat{a}_{\text{Rx,idler}}^{(l)} + \left(\hat{a}_{\text{Rx,idler}}^{(l)}\right)^{\dagger}\hat{a}_{Rx}^{(l)},\ l \in \{r, fs\} \tag{9}$$

For the receive side phase modulator shift of $\Delta\varphi = 0$ rad (see Figure 5), in the presence of the target, we obtain the following BD photocurrent operator expectation:

$$\left\langle \hat{i}_{BD}^{(l)} \right\rangle = 2\sqrt{T^{(i)}T^{(l)}N_s(N_s+1)}\cos\varphi^{(l)},\ l \in \{r,\ fs\} \tag{10}$$

On the other hand, for the receive side phase modulator shift of $\Delta\varphi = -\pi/2$ rad, in the presence of target, we obtain the following BD photocurrent operator expectation:

$$\left\langle \hat{i}_{BD}^{(l)} \right\rangle = 2\sqrt{T^{(i)}T^{(l)}N_s(N_s+1)}\sin\varphi^{(l)},\ l \in \{r,\ fs\} \tag{11}$$

In order to determine the exact phase-shift and the target range both in-phase and quadrature components are needed.

For the receive side phase modulator shift of $\Delta\varphi = 0$ rad, the variance of the BD photocurrent operator, defined as $\text{Var}\left(\hat{i}_{BD}^{(l)}\right) = \left\langle \left(\hat{i}_{BD}^{(l)}\right)^2 \right\rangle - \left\langle \hat{i}_{BD}^{(l)} \right\rangle^2$, will be:

$$\mathrm{Var}\left(\hat{i}_{BD}^{(l)}\right) = N_i N_s^{(l)} + (N_i+1)\left(N_s^{(l)}+1\right) + 2N_s T^{(l)} T^{(i)} (N_s+1)\left[\cos\left(2\varphi^{(l)}\right) - 2\cos^2\varphi^{(l)}\right], \tag{12}$$

where $N_s^{(l)} = (T^{(i)}N_s + N_b^{(i)})T^{(l)} + N_b^{(l)}$.

In the absence of the target, the BD photocurrent operator expectation is zero, while the corresponding variance is:

$$\mathrm{Var}\left(\hat{i}_{BD,t=0}^{(l)}\right) = N_i N_b^{(l)} + (N_i+1)\left(N_b^{(l)}+1\right) = N_s N_b^{(l)} + (N_s+1)\left(N_b^{(l)}+1\right), \tag{13}$$

where we used the fact that $N_i = N_s$.

Given that in the target detection problem the prior probabilities are not known in advance we need to apply the Neyman-Pearson criterion [20,21]. In Neyman-Pearson criterion we fix the maximum tolerable false alarm probability and maximize the target detection probability.

For the proposed EA joint monostatic-bistatic target detection scheme, the *false alarm (FA) probability* is given by:

$$Q_{FA} = \frac{1}{2}\mathrm{erfc}\left(\frac{t_{sh}}{\sqrt{N_s N_b + (N_s+1)(N_b+1)}}\right), \tag{14}$$

where t_{sh} is the threshold determined from the tolerable FA probability, wherein the complementary error function is given by $\mathrm{erfc}(x) = (2/\sqrt{\pi})\int_x^\infty \exp(-u^2)du$.

Assuming that the equal gain combining (see ref. [22] for more details) is used as the joint detection scheme for two receivers, the target *detection probability* is given by:

$$Q_D = \frac{1}{2}\mathrm{erfc}\left(\frac{t_{sh} - m_v}{\sqrt{V^{(r)} + V^{(fs)}}}\right), \tag{15}$$

where

$$\begin{aligned} m_v &= 2\sqrt{T^{(r)}T^{(i)}N_s(N_s+1)} + 2\sqrt{T^{(fs)}T^{(i)}N_s(N_s+1)}, \\ V^{(r)} &= N_i N_s^{(r)} + (N_i+1)\left(N_s^{(r)}+1\right) - 2T^{(r)}T^{(i)}N_s(N_s+1), \\ V^{(fs)} &= N_i N_s^{(fs)} + (N_i+1)\left(N_s^{(fs)}+1\right) - 2T^{(fs)}T^{(i)}N_s(N_s+1). \end{aligned} \tag{16}$$

4. Illustrative Numerical Results

The referent case will be the monostatic radar in which a coherent state is used to illuminate the target, in the presence of thermal (background) radiation. The density operator, in the presence of thermal radiation, has the following P-representation [1–4,20]:

$$\rho_t = \frac{1}{\pi N_b}\int e^{-\frac{|\alpha-\mu_t|^2}{N_b}}|\alpha\rangle\langle\alpha|d^2\alpha. \tag{17}$$

In the absence of the target ($t = 0$) we have that $\mu_0 = 0$, while in the presence of the target ($t = 1$) $\mu_1 = \mu$. The parameter N_b denotes the average number of thermal (background) photons. The coherent state $|\alpha\rangle$ can be expressed in terms of number states by $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n (\alpha^n/\sqrt{n!})|n\rangle$ and after substitution in (17) we obtain:

$$\rho_0 = \sum_{n=0}^{\infty}(1-v)v^n|n\rangle\langle n|, \quad v = N_b/(N_b+1). \tag{18}$$

The corresponding density matrix in the presence of target is given by (20):

$$\langle n|\rho_1|m\rangle = \begin{cases} (1-v)\sqrt{\frac{n!}{m!}}v^m(\mu^*/N)^{m-n}e^{-(1-v)|\mu|^2}\cdot \\ \qquad L_n^{m-n}\left[-(1-v)^2|\mu|^2/v\right],\ m \geq n \\ \langle m|\rho_k|n\rangle^*,\ m < n \end{cases} \tag{19}$$

where $|\mu\rangle$ denotes the state used to illuminate the target. In (19), we use $L_{deg}^{ord}(\cdot)$ to denote the associated Laguerre polynomials with superscript *ord* and subscript *deg* denoting the order and degree, respectively. For the Neyman-Pearson criterion the optimum strategy will be to determine the eigenvalues η_k and eigenkets $|\eta_k\rangle$ of the operator $\rho_1 - \Lambda\rho_0$ by solving the eigenvalue equation:

$$(\rho_1 - \Lambda\rho_0)|\eta_k\rangle = \eta_k|\eta_k\rangle, \tag{20}$$

in which the parameter Λ is determined from the maximum tolerable FA probability. This problem can be solved numerically.

To reduce receiver complexity, the *Helstrom threshold detector* can be used instead (20), with the corresponding detection operator defined as

$$\Pi_{H.t.} = (N_b + 0.5)^{-1}\left(\hat{a} + \hat{a}^\dagger\right), \tag{21}$$

which is related to the in-phase operator.

By assuming that the idler channels are ideal by setting the corresponding transmissivities to $T^{(I)} = 1$, in Figure 6 we compare the proposed EA joint monostatic-bistatic target detection scheme against various coherent states-based schemes and EA detection scheme for monostatic radar, in terms of detection probability vs. SNR, by setting the average number of background photons to $N_b = 10$, wherein the false alarm probability that can be tolerated is fixed to $Q_{\mathrm{FA}} = 10^{-6}$. For completeness of the presentation, the classical Albersheim's equation-based curves are provided as well for the number of samples set to $N = 1$ and 10 (see [23,24] for the Albersheim's equation details). For the non-classical target detection schemes the SNR is defined by $N_s/(2N_b + 1)$. The coherent states-based detection schemes under study include optimum quantum detector, quantum receiver (Rx) with the random phase, and Helstrom threshold receiver. Evidently, the proposed EA joint (monostatic-bistatic) target detection scheme significantly outperforms various coherent states-based detections schemes, the EA detection scheme for monostatic radar, and the classical target detection.

Given that the SPDC-based entangled source is broadband source in Figure 6 we also study the improvement in SNR that we can get when the number of bosonic modes is increased to $D = 10$. The proposed EA joint target detection scheme significantly outperforms the Helstrom threshold receiver with $D = 10$ modes and classical radar detector for $N = 10$ samples. For the detection probability set to $Q_{\mathrm{D}} = 0.95$ (and false alarm probability fixed to $Q_{\mathrm{FA}} = 10^{-6}$), the EA target detection scheme for $D = 10$ Bosonic modes outperforms the Helstrom detection scheme (for the same number of Bosonic modes) by 6.16 dB, while at the same time outperforming the corresponding classical scheme with $N = 10$ samples by even 11.29 dB. The joint EA scheme for $D = 10$ bosonic modes outperforms the corresponding EA scheme for monostatic radar (also with 10 bosonic modes at $Q_{\mathrm{D}} = 0.95$) by 3.01 dB.

In Figure 7 we evaluate the proposed EA joint detection scheme's detection probability vs. SNR by modelling both the direct return probe and forward scattered probe channels as the bosonic noisy and lossy channels with $N_{\mathrm{b}} = 11$ and transmissivities $T^{(r)} = T^{(fs)} = T$, wherein the corresponding channel models are given by Equation (7). Here we assume the ideal distribution of entanglement over the idler channels ($T^{(i)} = 1$ and $N_b{}^{(i)} = 0$). Clearly, when transmissivities of the direct return probe and forward scattered probe channels are low, the use of single Bosonic mode is not sufficient because the required SNR to achieve high target detection probability is way too high. On the other hand, when the number of bosonic modes is increased to 10, high target detection probabilities can be achieved even

at moderate SNRs (for low channel transmissivities). For $T = 0.05$, the EA joint detector with 10 bosonic modes outperforms EA monostatic radar detector by 3.04 dB at $Q_D = 0.95$.

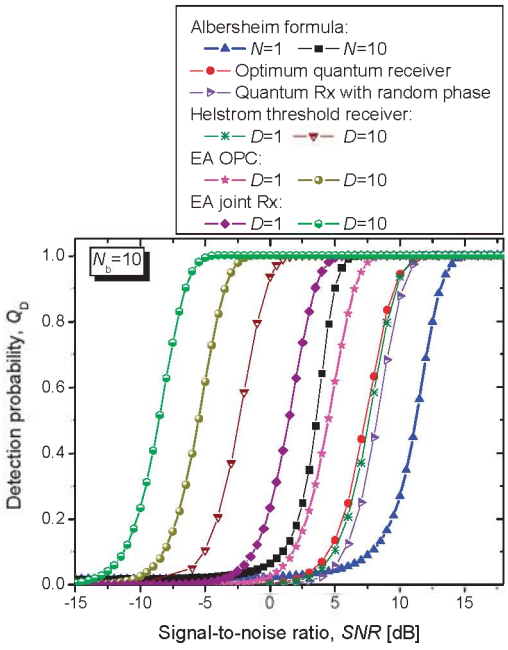


Figure 6. Detection probability vs. SNR [dB] for different radar detection schemes for average number of thermal photons set to $N_b = 10$. The maximum tolerable FA probability is fixed to $Q_{FA} = 10^{-6}$. The monostatic and bistatic idler channels are assumed to be ideal.

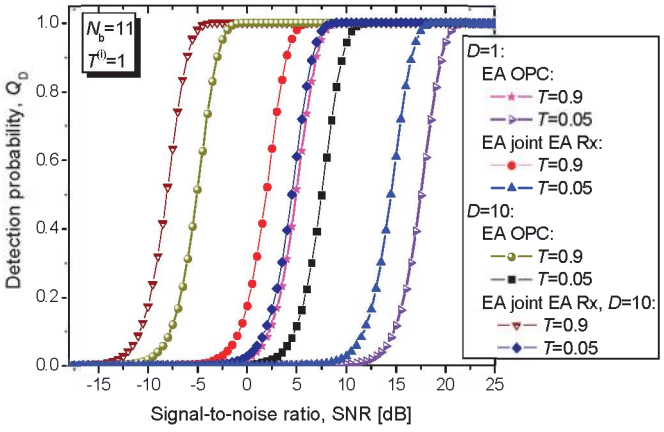


Figure 7. Detection probability vs. SNR [dB] for joint EA scheme for different direct return probe/forward scattered probe bosonic channel transmissivities $T^{(r)} = T^{(fs)} = T$. The maximum tolerable false alarm probability is fixed to $Q_{FA} = 10^{-6}$. The idler channel is assumed to be ideal.

In Figure 8 we evaluate the proposed EA joint detection scheme's detection probability vs. SNR by fixing the direct return probe/forward scattered probe channel transmissivities to $T^{(r)} = T^{(fs)} = T = 0.05$ and varying the transmissivity of the idler channels, wherein the idler channel model is described by Equation (4). Both signal and idler bosonic channels

are under assumption of being noisy with corresponding parameters being $N_b = 12$ and $N_b^{(i)} = 2$, respectively. Obviously, when the idler channel is noisy and lossy the same detection probability is achieved for higher SNR values, compared to the case with perfect distribution of entanglement. To solve for this problem, we can increase the number of bosonic modes, which is not difficult to implement thanks to the wideband nature of the SPDC process.

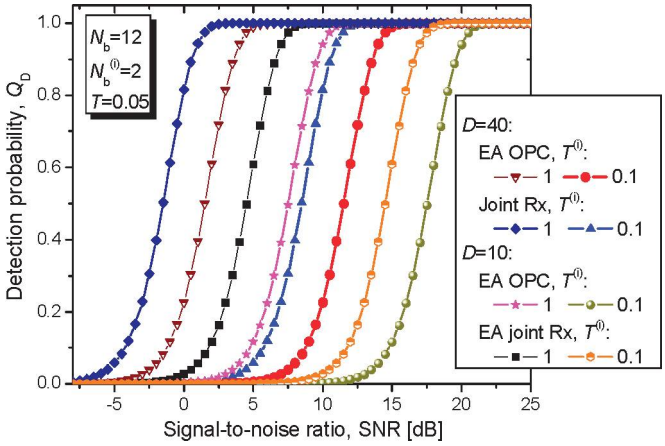


Figure 8. Detection probability vs. SNR [dB] for EA joint detection scheme for different idler channels transmissivities. The direct return probe/forward scattered probe bosonic channel transmissivities are fixed to $T^{(r)} = T^{(fs)} = T = 0.05$. The maximum tolerable false alarm probability is set to $Q_{FA} = 10^{-6}$.

Finally, in Figure 9 we study the proposed EA joint detection scheme's detection probability when the transmissivities of the direct return probe and the forward scattered probe channels are different, while the average number of thermal photons is set to $N_b = 11$. The idler channels are considered identical but lossy and noisy [$T^{(i)} = 0.9$ and $N_b^{(i)} = 0.5$]. The joint EA detection scheme for $T^{(r)} = 0.4$ and $T^{(fs)} = 0.1$ for 10 bosonic modes outperforms the EA detector for monostatic radar with $T^{(r)} = 0.4$ by even 6.49 dB at $Q_D = 0.95$.

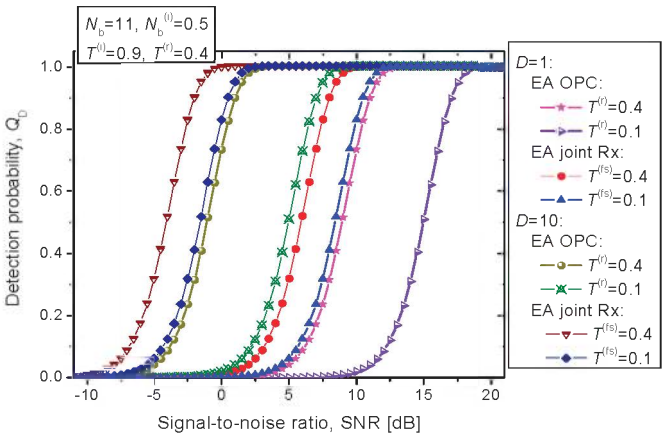


Figure 9. Detection probability vs. SNR [dB] for EA joint detection scheme for fixed idler channels transmissivity $T^{(i)} = 0.9$. The direct return probe channel transmissivity is set to $T^{(r)} = 0.4$, while the forward scattered probe channel transmissivity is varied $T^{(fs)} \in \{0.1, 0.4\}$. The maximum tolerable false alarm probability is fixed to $Q_{FA} = 10^{-6}$.

5. Concluding Remarks

We have proposed the entanglement assisted joint bistatic-monostatic quantum radar detection scheme. The proposed EA joint radar detection scheme employs the optical phase conjugation on the transmitter side and classical coherent detection on both receiver sides.

The proposed EA joint target detection scheme has been evaluated against the coherent states-based quantum detection schemes and EA detection scheme for monostatic radar. We have shown that the detection probability of the proposed EA joint target detection scheme has been significantly better than that of corresponding coherent states-based quantum detection schemes, the classical detection, and EA detection scheme for monostatic radar. The proposed scheme has been also evaluated by assuming the imperfect distribution of entanglement and by modeling the direct return probe and forward scattered probe channels as both lossy and noisy Bosonic channels. The proposed EA joint transmitter, with transmit side OPC, is suitable for implementation in mature $LiNbO_3$ technology. Given that the EA receiver is based on a commercially available balanced coherent detector, the implementation of the proposed joint bistatic-monostatic radar is not far from practical implementation.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Djordjevic, I.B. *Quantum Communication, Quantum Networks, and Quantum Sensing*; Elsevier/Academic Press: London, UK, 2022.
2. Guha, S.; Erkmen, B.I. Gaussian-state quantum-illumination receivers for target detection. *Phys. Rev. A* **2009**, *80*, 052310. [CrossRef]
3. Djordjevic, I.B. *Quantum Information Processing, Quantum Computing, and Quantum Error Correction: An Engineering Approach*, 2nd ed.; Elsevier: London, UK; Academic Press: San Diego, CA, USA, 2021.
4. Cariolaro, G. *Quantum Communications*; Springer International Publishing AG: Cham, Switzerland; Berlin/Heidelberg, Germany, 2015.
5. Djordjevic, I.B. *Physical-Layer Security and Quantum Key Distribution*; Springer International Publishing AG: Cham, Switzerland; Berlin/Heidelberg, Germany, 2019.
6. Liao, S.-K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.-P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43. [CrossRef] [PubMed]
7. Zhang, Z.; Zhuang, Q. Distributed quantum sensing. *Quantum Sci. Technol.* **2021**, *6*, 043001. [CrossRef]
8. Holevo, A.S.; Werner, R.F. Evaluating capacities of Bosonic Gaussian channels. *Phys. Rev. A* **2001**, *63*, 032312. [CrossRef]
9. Shi, H.; Zhang, Z.; Zhuang, Q. Practical route to entanglement-assisted communication over noisy Bosonic channels. *Phys. Rev. Appl.* **2020**, *13*, 034029. [CrossRef]
10. Djordjevic, I.B. On Entanglement Assisted Classical Optical Communication with Transmitter Side Optical Phase-Conjugation. *IEEE Access* **2021**, *9*, 168930–168936. [CrossRef]
11. Childs, A.M. Secure assisted quantum computation. *Quantum Inf. Comput.* **2005**, *5*, 456–466. [CrossRef]
12. Lanzagorta, M. *Quantum Radar*; Morgan and Claypool Publishers: San Rafael, CA, USA, 2012.
13. Lloyd, S. Enhanced Sensitivity of Photodetection via Quantum Illumination. *Science* **2008**, *321*, 1463–1465. [CrossRef] [PubMed]
14. Harris Corporation. *Quantum Sensors Program*; Final Technical Report, AFRL-RI-RS-TR-2009-208; Harris Corporation: Melbourne, FL, USA, 2009.
15. Torromé, R.G.; Bekhti-Winkel, N.B.; Knott, P. Introduction to quantum radar. *arXiv* **2020**, arXiv:2006.14238v3.
16. Shapiro, J.H. The Quantum Illumination Story. *IEEE Aerosp. Electron. Syst. Mag.* **2020**, *35*, 8–20. [CrossRef]
17. Sorelli, G.; Treps, N.; Grosshans, F.; Boust, F. Detecting a target with quantum entanglement. *arXiv* **2021**, arXiv:2005.07116. [CrossRef]
18. Karsa, A.; Spedalieri, G.; Zhuang, Q.; Pirandola, S. Quantum illumination with a generic Gaussian source. *Phys. Rev. Res.* **2020**, *2*, 023414. [CrossRef]
19. Zhang, Z.; Mouradian, S.; Wong, F.N.C.; Shapiro, J.H. Entanglement-enhanced sensing in a lossy and noisy environment. *Phys. Rev. Lett.* **2015**, *114*, 110506. [CrossRef] [PubMed]
20. Helstrom, C.W. *Quantum Detection and Estimation Theory*; Academic Press: New York, NY, USA, 1976.
21. McDonough, R.N.; Whalen, A.D. *Detection of Signals in Noise*, 2nd ed.; Academic Press: San Diego, CA, USA, 1995.

22. Djordjevic, I.B. *Advanced Optical and Wireless Communications Systems*; Springer International Publishing: Cham, Switzerland, 2017.
23. Tufts, D.W.; Cann, A.J. On Albersheim's Detection Equation. *IEEE Trans. Aerosp. Electron. Syst.* **1983**, *AES-19*, 643–646. [CrossRef]
24. Richards, M.A. *Fundamentals of Radar Signal Processing*; McGraw-Hill: New York, NY, USA, 2005.

MDPI
St. Alban-Anlage 66
4052 Basel
Switzerland
www.mdpi.com

Entropy Editorial Office
E-mail: entropy@mdpi.com
www.mdpi.com/journal/entropy

Academic Open
Access Publishing

www.mdpi.com

ISBN 978-3-0365-8561-1