

Review

Quantum Shannon Information Theory—Design of Communication, Ciphers, and Sensors

Osamu Hirota ^{1,2} 
¹ Quantum ICT Research Institute, Tamagawa University, 6-1-1, Tamagawa-Gakuen, Machida 194-8610, Japan; hirota@lab.tamagawa.ac.jp

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

Abstract

One of the key aspects of Shannon theory is that it provides guidance for designing the most efficient systems, such as minimizing errors and clarifying the limits of coding. This theory has seen great developments in the 50 years since 1948. It has played a vital role in enabling the development of modern ultra-fast, stable, and highly dependable information and communication systems. Shannon theory is supported by statistical communication theories such as detection and estimation theory. The theory of communication systems that transmit Shannon information using quantum media is called quantum Shannon information theory, and research began in the 1960s. The theoretical formulation comparable to conventional Shannon theory has been completed. Its important role is to suggest that application of quantum effects will surpass existing communication performance. It would be meaningless if performance, efficiency, and utility were to deteriorate due to quantum effects, even if a certain new function is given. This paper suggests that there are various limitations to utilizing quantum Shannon information theory to benefit real-world communication systems and presents a theoretical framework for achieving the ultimate goal. Finally, we present the perfect secure cipher that overcomes the Shannon impossibility theorem without degrading communication performance and sensors as an example.

Keywords: quantum technology; secure global optical network; reaction control system



Academic Editor: Sebastian Deffner

Received: 29 September 2025

Revised: 4 November 2025

Accepted: 11 November 2025

Published: 14 November 2025

Citation: Hirota, O. Quantum Shannon Information Theory—Design of Communication, Ciphers, and Sensors. *Entropy* **2025**, *27*, 1158. <https://doi.org/10.3390/e27111158>

Copyright: © 2025 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In the 1970s, while upholding the MIT tradition, R.S. Kennedy and H.A. Haus of MIT shifted communications science toward a research direction that incorporates fundamental theories of communications that take quantum effects into account (Appendix A). Kennedy took the lead in this direction and began nurturing young researchers, which has resulted in research that has had a global impact in a variety of fields. The current boom in quantum information science can be traced back to their leadership.

In this field, theory for systems that transmit conventional information using quantum states is called quantum Shannon information theory. In order to construct such a theory, probability theory is needed to describe quantum mechanical phenomena in an information-theoretic way. It is formulated as quantum probability theory, which has a different mathematical system from conventional probability theory and can faithfully describe quantum mechanical phenomena. For these reasons, it is necessary to build communication theory for the above communication systems based on quantum probability theory. It is called quantum communication theory (or quantum detection and estimation theory) and was developed by Helstrom [1], Holevo [2], Yuen [3], and other researchers.

Like conventional Shannon theory, the construction of quantum Shannon information theory started based on quantum communication theory, the studying of the properties of Shannon mutual information in systems with quantum effects. The most important achievement of the evolution from quantum communication theory to quantum Shannon information theory is the proof of Shannon's second theorem (channel coding theorem) for quantum communication systems. First, Hausladen et al. of the Jozsa group proved it by skillfully using the properties of random coding and quantum measurement on a typical subspace of the Hilbert space spanned by pure signal quantum states for the case where the quantum state communication channel is noiseless [4].

Following from this result, Holevo [5] and Schumacher-Westmoreland [6] proved that the discrete channel capacity of a general quantum channel with noise is given by Holevo information. This is now called the Holevo–Schumacher-Westmoreland theorem.

It is well known that the theorems on the coding limit are the most important ones in the application of information theory among the major theorems in information theory. In particular, the channel coding theorem shows that there exists a coding scheme that is error-free for an infinitely long typical sequence and that the information rate is ultimately equal to the channel capacity.

In response to such a limiting existence theorem, Gallager completed a theory that does not use a typical sequence and gives a limit to the average error probability of code words for a finite-length code system. This allows us to know the limiting characteristics of errors for a finite-length code system for any information rate up to the channel capacity when a channel matrix is given. This is called the theory of reliability functions, and it is well known that it made a major contribution to the process of constructing Shannon theory [7].

Thus, as a natural evolution of research, Holevo's group introduced a reliability function corresponding to quantum communication channels following Gallager's concept [8,9]. In addition, Helstrom, C. Bendjaballa et al. [10–12], and M. Ban et al. [13,14] formulated the cut-off rate of quantum systems. These trials are applications of Gallager theory to quantum systems. Just as Gallager's reliability function theory was effective in analyzing communication systems following classical physics, the quantum reliability function and cut-off rate are also considered to be effective in analyzing communication systems with quantum effects. Based on this perspective, Holevo has completed a unified mathematical foundation for quantum systems [15].

In this paper, we summarize the development from quantum communication theory to quantum Shannon information theory in Sections 2–5 and explain its applications to real-world communication technologies, showing quantum advantage for communication, ciphers, and sensors. The most dramatic result of this theory is the discovery of quantum stream ciphers, which solve the Shannon impossibility theorem for symmetric key ciphers and realize perfectly secure ciphers with short keys.

2. General Quantum Communication Channel Model

In this section, we denote the theoretical structure of general quantum systems and provide an explanation of the mathematical theory of quantum communication channels. In quantum theory for transmission of the information defined by Shannon, Shannon information as a finite set of alphabets is mapped to a quantum state. Therefore, the overall communication channel consists of a quantum state-to-quantum state communication channel and a quantum measurement channel that converts the received quantum state into a classical signal via measurement (Figure 1).

In order to analyze them as information theory, it is necessary to set up a communication channel model. A communication channel that transmits a quantum state onto which the signal is mapped is called a quantum state transmission channel. This channel is described by a completely positive map in the general mathematical sense [15].

Definition 1. Let $\mathcal{A}, \mathcal{B}$ be two $*$ -algebras and $\mathbf{S} \subset \mathcal{A}$ be an operator system. A linear map $\Phi : \mathbf{S} \rightarrow \mathcal{B}$ is called completely positive if $\sum_{i,j=1}^n b_i^* \Phi(a_i^* a_j) b_j \in \mathcal{B}$ is positive for all $n \in \mathbf{N}$ and for all $a_i \in \mathbf{S}, b_i \in \mathcal{B}$. The space of all such maps is denoted by $\text{CP}(\mathbf{S}, \mathcal{B})$.

The key issue is the physical reality of such abstract descriptions. In Shannon theory, a channel is considered noiseless when the relationship between the input and output symbols is injective. From this perspective, it is important that the quantum state carrying Shannon information does not lose its quantum properties along the channel. Fortunately, the following theorem has been shown for real-world channels by Helstrom [16].

Theorem 1 ({Helstrom}). In the transmission of quantum states through an optical communication channel with energy loss, the quantum state that can maintain a pure state is a coherent state which is defined by $\mathbf{a}|\alpha\rangle = \alpha|\alpha\rangle$, where $\mathbf{a}$ is a photon annihilation operator.

This theorem has an affinity with modern communication technology. That is, the maximum capacity of reliable information transmission in general optical channels such as fiber and free space is achieved by a coherent state, considering the channel characteristics, the bandwidth of the light source, and the receiver.

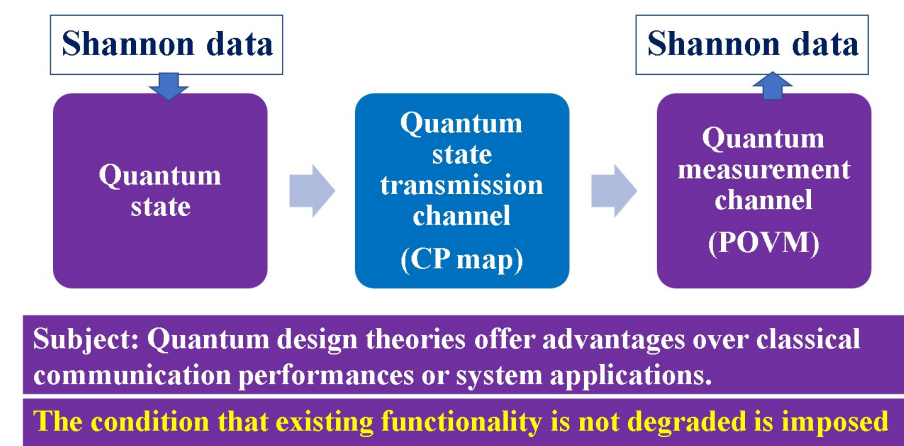


Figure 1. Channel model in quantum Shannon information theory. Shannon information such as digital data or analog signals is transmitted by optical signals with quantum effect governed by a quantum state. The quantum state and quantum measurement determine the communication performance. The existing functionality should not be degraded.

In fact, in optical fiber communication, energy loss is the main issue. When the transmitting quantum state is a coherent state, which is the quantum state of general laser light, it maintains a pure state even if there is any loss, so it is treated as noiseless in the sense of quantum state transmission.

In free-space optical communication, in addition to energy loss, external noise is added, so the quantum state transmission channel becomes a noisier channel (Figure 2). But still, the coherent state provides the maximum capacity, which is discussed in Section 5.

	Optical quantum state transmission channel
Fiber channel	Energy loss, Amplifier noise
Free space channel	Energy loss, Scattering, Turbulence, Back ground noise

Figure 2. Subject of consideration of quantum state transmission channel. The performance requirements for fiber optic communication are 100 Gbit/s to 100 Tbit/s as the transmission speed and a communication distance of 10,000 km. For terrestrial spatial transmission, the speed is 1 Gbit/s to 10 Gbit/s, and the communication distance is about 10 km. There are no quantum states other than coherent states that satisfy these requirements. This is a consequence of Theorem 1.

Remark 1. When a single photon (number state), a squeezed state, quantum entangled states, etc., are used as the transmitter state, energy loss or decoherence transforms these states into a mixed state, and the channel becomes non-injective. Thus, light sources of quantum states with strong quantum properties cannot meet the performance requirements of modern communication, which requires over 100 Gbit/s.

Next, it is necessary to describe the process of identifying the quantum state that has arrived at the receiver. In this quantum measurement process, unavoidable noise due to the most basic observation operation in quantum mechanics appears. If this is modeled as quantum noise, it can be modeled as a quantum measurement communication channel. In other words, unavoidable errors occur in the identification of quantum states, and an optimization problem arises regarding their decision.

This type of model was proposed by Helstrom in 1967 and is called quantum detection and estimation theory [1]. The noise model of the photoelectric conversion process in the receiver of laser optical communication is the simplest physical example of quantum noise. In order to describe this quantum measurement channel, quantum probability theory, which describes the quantum measurement process, is required. Below we briefly present the mathematics of quantum probability as a basis for the following discussion.

3. Mathematical Foundation of Generalized Quantum Measurement and Decision Operator

3.1. Mathematical Formulae of Generalized Quantum Measurement

The mathematical structure of quantum mechanics is given based on the Hilbert space theory constructed by von Neumann. The representation of the quantum measurement process is formulated using the eigen state and eigen value of a self-adjoint operator. This is defined as follows.

Definition 2. Let us assume that the quantum system has the self-adjoint operator as physical observable $\mathbf{T}$ and its quantum state ρ . The Born rule in the standard quantum measurement of the observable is described as follows:

$$\mathbf{T}|x\rangle = x|x\rangle, P(x) = \text{Tr}[\rho|x\rangle\langle x|] \quad (1)$$

where $|x\rangle\langle x|$ is called projection valued measure.

The set of density operator ρ is a convex set, its extreme points being the one-dimensional projection. The corresponding states are called pure. Any measurement

with values in the real number space R_M is described by an affine map of the set of the states (density operator) to the set of probability distributions on R_M .

However, P. Benioff and others have been discussing the mathematical generalization of the projection process to describe the diversity of measurement processes. Finally the generalized quantum measurement process is described in the following form [17].

Definition 3. Let us consider a generalized resolution of identity $\{\mathbf{X}(r); r \in R_M\}$, i.e., the collections of Hermitian operators, satisfying $\sum_{r \in R_M} \mathbf{X}(r) = I, \mathbf{X}(r) \geq 0$. $\text{Tr} \rho \mathbf{X}(r)$ establishes the one-to-one correspondence between affine maps of the set of density operators to the set of probability distributions on R_M and the resolution of identities. In some cases, $\mathbf{X}(r)$ is called the positive operator valued measure (POVM).

This formulation makes it possible to formulate the Born effect in quantum measurements without going through concrete physical quantities (observable).

3.2. Quantum Decision Operator

In quantum communication theory, the POVM is used as the decision operator $\{\Pi_m\}$ by following operational correspondence.

Let us assume the set $\rho_m, m = \{1, 2, 3, \dots, M\}$ of quantum states. The decision result through the quantum measurement is described by a compact set of the decision operator Π_l , with $l = 1, 2, 3, \dots, M$, such that

$$P(l|m) = \text{Tr} \rho_m \Pi_l, \quad m, l = 1, 2, 3, \dots, M \quad (2)$$

$$\sum_{l=1}^M \Pi_l = I, \quad \Pi_l \geq 0 \quad \forall l \quad (3)$$

where I is the identity operator.

Remark 2. The decision operator does not just represent the probability of a quantum measurement process but the probability of error or detection by the receiver's decision. In other words, it must be understood that it involves a decision by the observer [1].

The above remark, from the origins of Helstrom's formulation, is easier to understand if we interpret the quantum decision operator as the generalization of Wald's decision function in a classical system [18].

In classical communication theory, the decision is applied to the given probability function of the variable of the received signal. When one applies the standard quantum measurement, the probability function is given, and the decision function is applied to its probability function as in classical detection theory. However, in the quantum case, the decision operator does not need the explicit probability function of the variable of the received signal. The decision operator directly outputs the probability value of the correctness or incorrectness of the decision without going through the probability function of the measurement process. As an effect of the above fact, the possibility that the discrimination capability of the quantum signal in the quantum measurement process will exceed the discrimination capability by the standard likelihood decision based on standard quantum measurement and its probability function arises. This is equivalent to violating communication-theoretic causality [19,20].

However, this can occur only in the discrete signal set. Its effect disappears in the case of continuous variables. That is, in quantum estimation theory, there is no such quantum advantage. These observations will be discussed in the subsequent sections.

3.3. Decision Operator Based on Entangled Measurement (or Collective Measurement)

As mentioned above, a quantum measurement process is considered a communication channel. In information theory, information is generally transmitted as a code word of length n . When extended to the n -th extension, quantum communication channels need to be treated differently from conventional extension channels.

Let us consider a finite alphabet $\{a_l\}, l = (1, 2, \dots, M)$ with quantum state ρ_l . The code word $\mathbf{k}$ is a combination of the alphabet $\{a_l\}$ with the length n . That is, the input code $\mathbf{k} = (k_1, k_2, \dots, k_i, \dots, k_n)$, and the output is $\mathbf{j} = (j_1, j_2, \dots, j_i, \dots, j_n)$, where i is the order of the sequence in the code, $0 \leq k_i \leq M$, and $0 \leq j_i \leq M$. The compound state $\rho_{\mathbf{k}} = (\rho_{k_1} \otimes \rho_{k_2} \cdots \otimes \rho_{k_n})$ is in a tensor product Hilbert space $H^{\otimes n} = H \otimes \cdots \otimes H$. When the n -th extended signal state is used, the operation of treating a sequence of quantum states of length n as a single quantum state in the n -th extended Hilbert space is called collective or entangled measurement-based decoding. In this case, these structures provide unique performance in quantum Shannon information theory, which will be described in the next section. In cases of individual and entangled measurement, optimizing the decision operator that represents the decision process is an important issue.

4. Structure of Quantum Detection and Estimation Theory

4.1. Quantum Detection Theory

4.1.1. Basic Formula

The appearance of quantum effects in the measurement process of signals and the result of the decision are simultaneously characterized by the quantum decision operator. Thus, the quantum Bayes rule is formulated without going through the likelihood ratio as follows:

$$\bar{P}_e = \min_{\{\Pi\}} \left\{ 1 - \sum_{m=1}^M \xi_m \text{Tr} \rho_m \Pi_m \right\} \quad (4)$$

where the a priori probability must be $(\xi_m > 0, \forall m)$ for admissibility in decision theory. The necessary and sufficient conditions for $\{\Pi_m\}$ are given by Holevo [2] and Yuen [3].

Theorem 2 (*{Holevo, Yuen}*). *The necessary and sufficient condition for $\{\Pi_m\}$ on the quantum Bayes rule is given by*

$$\begin{aligned} \Pi_m [\xi_m \rho_m - \xi_l \rho_l] \Pi_l &= 0, \quad \forall l, m \\ \gamma - \xi_l \rho_l &\geq 0, \quad \forall l \\ \gamma &= \sum_l \xi_l \rho_l \Pi_l \end{aligned} \quad (5)$$

On the other hand, following classical detection theory, the quantum minimax rule for a signal system in which the functional with respect to $\{\xi_m\}$ is a convex function is defined as

$$\bar{P}_e = \max_{\{\xi\}} \min_{\{\Pi\}} \left\{ 1 - \sum_{m=1}^M \xi_m \text{Tr} \rho_m \Pi_m \right\} \quad (6)$$

and the necessary and sufficient conditions are as shown below [21].

Theorem 3 (*{Hirota · Ikehara}*). The necessary and sufficient condition for $\{\Pi_m\}$ on the quantum minimax rule is given by

$$\begin{aligned} \text{Tr} \Pi_l \rho_l &= \text{Tr} \Pi_m \rho_m, \quad \forall l, m \\ \Pi_m [\xi_m \rho_m - \xi_l \rho_l] \Pi_l &= 0, \quad \forall l, m \\ \gamma - \xi_l \rho_l &\geq 0, \quad \forall l \\ \gamma &= \sum_l \xi_l \rho_l \Pi_l \end{aligned} \quad (7)$$

For further formulae, please see the references.

4.1.2. Useful Analytical Issues

In general, it is very difficult to find the solutions of the above two quantum detection rules. However, when the signal system satisfies certain conditions or the decision operator can be set in advance, the optimal theory becomes very simple. Some examples of these are described below.

A set of quantum states that conforms to the following definition is particularly convenient.

Definition 4. Let G be a group with an operation $\circ$. The set of quantum state signals is called group covariant if there exist unitary operators $U_k (k \in G)$ such that

$$U_k |\psi_m\rangle = |\psi_{k \circ m}\rangle, \quad \forall m, k \in G \quad (8)$$

It characterizes quantum states $\{|\psi_m\rangle, m \in G\}$ [17].

Let us explain the case of setting a decision operator in advance. Belavkin [22] introduced the following decision operator called square root measurement (SRM).

Definition 5. The decision operator called a square root measurement (SRM) is given by

$$\begin{aligned} \Pi_l &= |\mu_l\rangle\langle\mu_l| \\ |\mu_l\rangle &= \Gamma^{-1/2} |\alpha_l\rangle \\ \Gamma &= \sum_{m=1}^M |\alpha_m\rangle\langle\alpha_m| \end{aligned} \quad (9)$$

where Γ is a Gram operator.

Based on the above formula, the general properties of the quantum Bayes rule and quantum minimax rule based on the above decision operator are given by Ban and Osaki [23,24].

4.1.3. Decision Operator Based on SRM of Entangled Measurement

In the case of the operation of mapping an individual decision to the quantum states corresponding to each slot of a code word, the decision operator and decision probability are given by

$$\begin{aligned} \Pi_{\mathbf{j}} &= \Pi_{j_1} \otimes \Pi_{j_2} \cdots \otimes \Pi_{j_n} \\ P(\mathbf{j}|\mathbf{k}) &= P(j_1|k_1) \times P(j_2|k_2) \times \cdots \times P(j_n|k_n) \end{aligned} \quad (10)$$

where $P(j_l|k_l) = \text{Tr} \rho_{j_l} \Pi_{j_l}$, for $l = \{1, 2, \dots, n\}$. In this case, there is no correlation in the signal decision process.

On the other hand, one can define the decision operator based on the entangled measurement. Let us denote the quantum state of n -th extended quantum state as follows:

$$|\Psi_{\mathbf{k}}\rangle = |\psi_{k_1}\rangle |\psi_{k_2}\rangle \dots |\psi_{k_l}\rangle \dots |\psi_{k_n}\rangle \quad (11)$$

where $k_l = \{1, 2, \dots, M\}, \forall l$. Then we can adopt the square root measurement as follows:

$$\begin{aligned} \Pi_j &= |\Phi_j\rangle\langle\Phi_j|, \\ |\Phi_j\rangle &= \left(\sum_{\mathbf{k}} |\Psi_{\mathbf{k}}\rangle\langle\Psi_{\mathbf{k}}|\right)^{-1/2} |\Psi_j\rangle \\ P(j|\mathbf{k}) &= \text{Tr} \rho_{\mathbf{k}} \Pi_j \end{aligned} \quad (12)$$

where $\rho_{\mathbf{k}} = |\Psi_{\mathbf{k}}\rangle\langle\Psi_{\mathbf{k}}|$. This is called decision operator based on entangled measurement. In this case, in addition to the quantum effects due to the decision action on each alphabet, quantum effects due to entanglement can be expected.

4.1.4. Quantum Advantage in Detection

The performance of optical communications, which is designed using classical communication theory, is determined by the performance of existing receivers such as photon-counting, homodyne, and heterodyne receivers. If the performance of a communication system designed using quantum theory exceeds conventional performance, it is called quantum advantage or quantum gain. The quantum gain characteristics by the quantum decision operator are exemplified below. The concrete advantage of the decision operator based on entangled measurement is discussed in Section 5.

Theorem 4. *If the signal set $\{|\alpha_m\rangle\}$ is covariant, the optimum decision operator is given by the decision operator based on the square root measurement. And the error probability of quantum Bayes and quantum minimax rules for M covariant signals can be given as follows:*

$$\begin{aligned} \bar{P}_e &= 1 - \frac{1}{(M)^2} \left(\sum_{m=1}^M \sqrt{\lambda_m} \right)^2 \\ \lambda_m &= \sum_{k=1}^M \langle \alpha_1 | \alpha_k \rangle u^{-(k-1)m} \end{aligned} \quad (13)$$

where $u = \exp[\pi i / M]$.

Here we show the simplest example. Assuming that the signal system is binary PSK $\rho_1 = |\alpha\rangle\langle\alpha|, \rho_2 = |-\alpha\rangle\langle-\alpha|$ with $\zeta_1 = \zeta_2 = 1/2$, the quantum solution is as follows [1]:

$$\begin{aligned} \bar{P}_e^{opt} &= 1 - (\text{Tr} \rho_1 \Pi_1^{opt} + \text{Tr} \rho_2 \Pi_2^{opt}) \\ &= \frac{1}{2} [1 - \sqrt{1 - |\langle \alpha | -\alpha \rangle|^2}] \\ &\ll \bar{P}_e(\text{Homodyne}) \end{aligned} \quad (14)$$

This is called the Helstrom bound. The decision operator in this case is given as follows:

$$\Pi_1^{opt} = |\omega_1\rangle\langle\omega_1|, \quad \Pi_2^{opt} = |\omega_2\rangle\langle\omega_2| \quad (15)$$

where

$$\begin{aligned}
 |\omega_1\rangle &= \sqrt{\frac{1+\sqrt{1-\kappa^2}}{2(1-\kappa^2)}}|\alpha\rangle \\
 &\quad - \sqrt{\frac{1-\sqrt{1-\kappa^2}}{2(1-\kappa^2)}}|-\alpha\rangle \\
 |\omega_2\rangle &= \sqrt{\frac{1-\sqrt{1-\kappa^2}}{2(1-\kappa^2)}}|\alpha\rangle \\
 &\quad - \sqrt{\frac{1+\sqrt{1-\kappa^2}}{2(1-\kappa^2)}}|-\alpha\rangle
 \end{aligned} \tag{16}$$

where $\kappa = |\langle\alpha|-\alpha\rangle|$.

In the case of a homodyne receiver (classical solution), the measurement operator is

$$\Pi(x) = |x\rangle\langle x|, \quad X_c|x\rangle = x|x\rangle, \quad X_c = \frac{1}{2}(\mathbf{a} + \mathbf{a}^\dagger) \tag{17}$$

The average error probability is given by the likelihood test based on $P(x|\alpha) = \text{Tr}\rho_1\Pi(x)$, $P(x|-\alpha) = \text{Tr}\rho_2\Pi(x)$. It corresponds to the post-measurement procedure. The result does not show quantum advantage.

Separate analysis is required to determine what physical process the quantum optimal solution in Equation (16) corresponds to. An example is the Dolinar receiver [1].

4.2. Quantum Estimation Theory

Quantum estimation theory was also pioneered by Helstrom, Holevo, Personick, and Yuen. Then M.G.A. Paris et al. discussed many aspects of its application [25]. In this section, we show the formulation and discuss a certain problem.

4.2.1. Formulation

When a physical signal parameter is continuous, a set of the quantum states can be treated as a quantum state system corresponding to a continuous signal. Optimization theory goes to quantum estimation from quantum detection theory. Therefore, the decision must deal with a continuous quantity $\{x\}$. So for the density operator $\rho(x)$, the decision is defined as an infinitesimal operator.

$$\begin{aligned}
 \{\Pi_i\} &\rightarrow \{d\Pi(x)\} \\
 P(x_{out}|x_{in}) &= \text{Tr}\rho(x_{in})d\Pi(x_{out})
 \end{aligned} \tag{18}$$

where $x = x_{in} = x_{out}$ for the correct probability. Thus, quantum Bayes estimation can be formulated by replacing the discrete system with an infinitesimal decision operator. In this case, the optimum POVM corresponds to the measurement process of the observable as the parameter. That is, the optimum operator is given by the eigenstate of the operator of the physical observable. Thus, the estimation mechanism will use the maximum likelihood method, just like in classical methods, based on $P(x) = \text{Tr}\rho(x)d\Pi(x)$. Hence, it is easy to understand that it has no quantum advantage in the decision process.

Alternatively, one can adopt the minimum mean square error (MMSE) as the evaluation function. Personick formulated an MMSE estimator which is applicable to the linear filtering of random signal sequences [26]. On the other hand, the Cramér–Rao bound is formulated by Helstrom as follows [1]:

Theorem 5. The estimation bound for a single parameter is given by the following formula:

$$\text{Var}\hat{x} = \text{Tr}\rho(\hat{x} - x)^2 \geq \frac{1}{\text{Tr}\rho(x)L_S^2} \quad (19)$$

where L_S is called the symmetric logarithm derivative and is given by

$$\frac{\partial\rho(x)}{\partial x} = \frac{1}{2}[\rho(x)L_S + L_S\rho(x)] \quad (20)$$

The equality holds in the following case:

$$L_S = k(x)(\hat{x} - x) \quad (21)$$

where $\hat{x}$ is the estimate, $k(x)$ is a function of x , and the estimate operator $\hat{x}$ is given by the operator corresponding to the parameter.

This means that the optimum measurement is the standard quantum measurement and that there is no quantum advantage in the measurement process itself. In addition, there is still a certain difficulty, as discussed in the following.

4.2.2. Example for Coherent-State Signal

In optical communications and optical radar, signals generally have complex amplitudes (quadrature amplitude):

$$\alpha^s = x_c^s + ix_s^s = |\alpha^s| \cos \theta + i|\alpha^s| \sin \theta = \sqrt{N_s}e^{i\theta} \quad (22)$$

Its quantum counterpart is the photon annihilation operator $\mathbf{a} = X_c + iX_s$, where

$$X_c = \frac{1}{2}(\mathbf{a} + \mathbf{a}^\dagger), \quad X_s = \frac{1}{2i}(\mathbf{a} - \mathbf{a}^\dagger) \quad (23)$$

Here X_c and X_s are non-commutative observables. The problem is how to formulate the simultaneous estimation of such non-commutative observables.

(a) Single-parameter estimation

In general, the density operator of an optical field is given as follows:

$$\rho = \frac{1}{\pi N} \int \exp\left\{-\frac{|\alpha - \alpha^s|^2}{N}\right\} |\alpha\rangle \langle \alpha| d^2\alpha \quad (24)$$

where N is background noise energy and α^s is the signal. When we consider the estimation of the single parameter x_c^s of $\alpha^s = x_c^s + ix_s^s$, the solution is given as follows:

$$\frac{\partial\rho}{\partial x_c^s} = \frac{1}{2}(\rho L_S + L_S\rho) \quad (25)$$

$$L_S = \frac{2}{N + 1/2} \left(\frac{\mathbf{a} + \mathbf{a}^\dagger}{2} - x_c^s \right) \quad (26)$$

As a result, we have

$$\hat{x} = X_c = \frac{1}{2}(\mathbf{a} + \mathbf{a}^\dagger), \quad \text{Var}\hat{x}_c = \frac{1}{2}N + \frac{1}{4} \quad (27)$$

where $1/4$ is the effect of quantum noise. The estimate operator $\hat{x}$ indicates a homodyne receiver. Thus, it has no quantum advantage.

(b) Non-commutative parameter estimation

Let us consider the simultaneous estimation of the non-commutative observables X_c and X_s . This is important for the evaluation of optical phase estimation such as

$$\theta = \tan^{-1} \frac{x_s}{x_c} \quad (28)$$

In this case, Theorem 5 does not provide the correct solution for the design of a communication system. The quantum optimum measurement for non-commutative quadrature amplitude can be given by the Yuen–Lax quantum Cramér–Rao bound [27].

Theorem 6. *The estimation bound for complex amplitudes is given by the following formula:*

$$\text{Var}(\hat{\alpha}) \geq \frac{1}{\text{Tr} \rho L_R L_R^\dagger} \quad (29)$$

where the right logarithm derivative L_R is defined by

$$\frac{\partial \rho}{\partial \alpha^s} = L_R^\dagger \rho, \quad L_R = k(\alpha^s)(\mathbf{a} - \alpha^s) \quad (30)$$

where $\mathbf{a}$ is a photon annihilation operator and it corresponds to a heterodyne measurement. Then the bound is given as follows:

$$\text{Var} \hat{\alpha} = N + 1 \quad (31)$$

where $1 = 1/2 + 1/2$ is the simultaneous measurement effect of the non-commutable observables.

If one adopts the separate measurement of the quadrature amplitude by two balanced homodyne receivers, from Theorem 1, the coherent state maintains the coherent state at the output of the half mirror. Here each measurement may adopt Theorem 5.

$$\frac{\partial \rho(x_c^s)}{\partial x_c^s} = \frac{1}{2} [\rho(x_c^s) L_S + L_S \rho(x_c^s)] \quad (32)$$

$$\frac{\partial \rho(x_s^s)}{\partial x_s^s} = \frac{1}{2} [\rho(x_s^s) L_S + L_S \rho(x_s^s)] \quad (33)$$

Each bound is given by

$$\text{Var} \hat{x}_c = \frac{1}{2} N + \frac{1}{4}, \quad \text{Var} \hat{x}_s = \frac{1}{2} N + \frac{1}{4} \quad (34)$$

However, one should not ignore the fact that the signal energy is half at each branch. Thus, the signal-to-noise ratio for the quantum part is

$$\begin{aligned} \text{SNR}(x_c) &= \frac{N_s/2}{1/4} = \frac{N_s}{1/2}, \\ \text{SNR}(x_s) &= \frac{N_s/2}{1/4} = \frac{N_s}{1/2}, \end{aligned} \quad (35)$$

This means that a set of two balanced homodyne receiver systems is equivalent to a heterodyne receiver for the coherent-state signal. Theorem 6 includes the above effect under fixed energy conditions.

Now consider the case where the signals are in a state other than coherent state. In separate measurement of non-commutative parameters, the quantum state is disturbed by a loss of half mirror. Therefore, it is not accurate to evaluate communication performance based on the conventional quantum Cramér–Rao bound only.

4.2.3. Application of Lie Algebra for Non-Commutative Parameters

We have been studying the theory of quantum state control and simultaneous measurement of non-commutative quantities based on Lie algebra. Here we introduce it and its application to the formulation of estimation theory. First, we define the formulation as follows.

Definition 6. *Algorithm:*

Step 1: Derive the estimation operators for simultaneous estimation of non-commutative quantities based on the symmetric logarithmic differential operator formulae in Equations (32) and (33).

Step 2: Construct a decision operator that expresses simultaneous measurement of non-commuting quantities based on the minimum uncertain state for the two operators obtained.

(a) Construction of decision operator

Definition 7. *An algebra is called a Lie algebra when its multiplication satisfies the following two conditions:*

$$\begin{aligned} [\mathbf{A}, \mathbf{A}] &= 0, \\ [[\mathbf{A}, \mathbf{B}], \mathbf{C}] + [[\mathbf{B}, \mathbf{C}], \mathbf{A}] + [[\mathbf{C}, \mathbf{A}], \mathbf{B}] &= 0 \end{aligned} \quad (36)$$

where $[\]$ is the commutation relation.

An example of its application in quantum mechanics is the Heisenberg–Weyl group: W_1 . The unitary representation of the subgroup of W_1 is

$$\mathbf{T}(\mathbf{g}) = \exp\{is\} \exp\{\alpha \mathbf{a}^\dagger - \alpha^* \mathbf{a}\} \quad (37)$$

where $\mathbf{g}$ is the element of Lie algebra.

Definition 8. *For any element $|\psi\rangle$ of a Hilbert space, the quantum state constructed by the formula*

$$\mathbf{T}(\mathbf{g})|\psi\rangle = |\alpha_\psi\rangle_G \quad (38)$$

is called the generalized coherent state.

Here let us consider non-compact groups in Lie algebras. With respect to Hermite forms, a set that constitutes linear isometric groups is a non-compact group. $SU(1,1)$ is a typical example.

The Lie algebra of $SU(1,1)$ has the following elements: $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_0$. Their commutation relations are

$$\begin{aligned} [\mathbf{K}_1, \mathbf{K}_2] &= -i\mathbf{K}_0, [\mathbf{K}_2, \mathbf{K}_0] = i\mathbf{K}_1 \\ [\mathbf{K}_0, \mathbf{K}_1] &= i\mathbf{K}_2 \end{aligned} \quad (39)$$

Then we define $\mathbf{K}_\pm = \mathbf{K}_1 \pm i\mathbf{K}_2$. The unitary representation of $SU(1,1)$ is given by

$$\mathbf{T}^\tau(\mathbf{g}) = \exp\{\zeta \mathbf{K}_+ - \zeta^* \mathbf{K}_-\} \quad (40)$$

where τ is given by the property of the Casimir operator. The following state is also the generalized coherent state:

$$\mathbf{T}^\tau(\mathbf{g})|\psi\rangle = |\alpha_\tau\rangle_G \quad (41)$$

where $|\alpha_\tau\rangle$ is called a base state. When the above state satisfies the minimum uncertainty relation for two observables, it is called the ideal generalized coherent state.

Here, for the quadrature amplitude, the elements of SU(1,1) are as follows:

$$\begin{aligned} K_+ &= \frac{1}{2} \mathbf{a}^{\dagger 2}, K_- = \frac{1}{2} \mathbf{a}^2, \\ K_0 &= \frac{1}{4} (\mathbf{a} \mathbf{a}^\dagger + \mathbf{a}^\dagger \mathbf{a}) \end{aligned} \quad (42)$$

Then we have

$$\mathbf{T}^\tau(\mathbf{g}) = \exp\left\{\frac{z}{2}(\mathbf{a}^2 - \mathbf{a}^{\dagger 2})\right\} \quad (43)$$

$$\mathbf{T}^\tau(\mathbf{g}) \mathbf{a} \mathbf{T}^{\tau\dagger}(\mathbf{g}) = \mu \mathbf{a} + \nu \mathbf{a}^\dagger \equiv \mathbf{b} \quad (44)$$

$$|\alpha_\tau\rangle = |0\rangle, \quad |\mu|^2 - |\nu|^2 = 1$$

Then the following state is the ideal generalized coherent state:

$$\mathbf{b}|\beta, \mu, \nu\rangle = \beta|\beta, \mu, \nu\rangle \quad (45)$$

$$\mathbf{T}^\tau(\mathbf{g})|0\rangle = |0, \mu, \nu\rangle \quad (46)$$

where $\beta = \mu\alpha + \nu\alpha^* = \bar{x}_c^G + i\bar{x}_s^G$. Equations (45) and (46) give the minimum uncertainty state for x_c and x_s .

Let us define the decision operator as step 1:

$$d\Pi(x_c, x_s) = |\beta, \mu, \nu\rangle\langle\beta, \mu, \nu| \quad (47)$$

This corresponds to the generalized heterodyne receiver [28]. Let us show how to use the above formula in the following.

(b) Estimation bound

Using these formulae, the modified quantum Cramér–Rao bound for the simultaneous estimation of non-commutative parameters of a coherent-state signal without background noise is given by step 2 as follows [28]:

$$\begin{aligned} \text{Var}\hat{x}_c &= \frac{1}{4} + \frac{1}{4}|\mu \pm \nu|^2 \\ \text{Var}\hat{x}_s &= \frac{1}{4} + \frac{1}{4}|\mu \mp \nu|^2 \end{aligned} \quad (48)$$

Then the total minimum bound is

$$\min_{\mu, \nu} (\text{Var}\hat{x}_c + \text{Var}\hat{x}_s) = 1, \quad \mu = 1, \nu = 0 \quad (49)$$

This is equivalent to the Yuen–Lax bound.

4.2.4. Importance of Signal-to-Noise Ratio in Estimation

In general, one should keep the following in mind: The performance of the estimation cannot be evaluated only by the estimation bound. Following communication theory, one needs the concept of the signal-to-noise ratio, which means the operational meaning in the technology.

Let us show an example of the evaluation for a continuous parameter. The squeezed state reduces the quantum noise of one of the quadrature amplitudes, and the purpose is to utilize the signal with that low noise. However, we have the following formulation.

Theorem 7 ({Yuen} [29]). We assume that $\rho = |\beta, \mu_s, \nu_s\rangle\langle\beta, \mu_s, \nu_s|$ as a signal state. Let us define the SNR of this state as follows:

$$SNR = \frac{(\text{Tr}\rho X_c)^2}{\text{Tr}\rho(X_c - \langle X_c \rangle)^2} \quad (50)$$

Under the constraint of the signal energy $\text{Tr}\rho \mathbf{a}^+ \mathbf{a} \leq N_s$, the maximum SNR is given by

$$SNR_{max} = 4N_s(N_s + 1) \quad (51)$$

where

$$\mu_s = \frac{N_s + 1}{\sqrt{2N_s + 1}}, \quad \nu_s = \frac{N_s}{\sqrt{2N_s + 1}} \quad (52)$$

The estimation bound is given by

$$\text{Var}\hat{x}_c = \frac{1}{4}|\mu_s - \nu_s|^2 = \frac{1}{4} \times \frac{1}{2N_s + 1} \quad (53)$$

When the state is a coherent state, $SNR = 4N_s$.

As mentioned above, low noise does not mean good performance. The SNR is the final evaluation for communication technology.

When there is an energy loss ϵ in the channel, the SNR is

$$SNR = \frac{4\epsilon N_s(N_s + 1)}{\epsilon + (1 - \epsilon)(2N_s + 1)} \quad (54)$$

The estimation bound is

$$\text{Var}\hat{x}_c = \frac{\epsilon}{4} \times \frac{1}{2N_s + 1} + \frac{1 - \epsilon}{4} \quad (55)$$

When the loss is large, the above SNR becomes $SNR = 2N_s$, which is worse than the coherent state.

Since evaluations for problems in technology require operational meaning, we emphasize the points to note in “quantum communication theory and quantum mathematical statistics” (Figure 3).

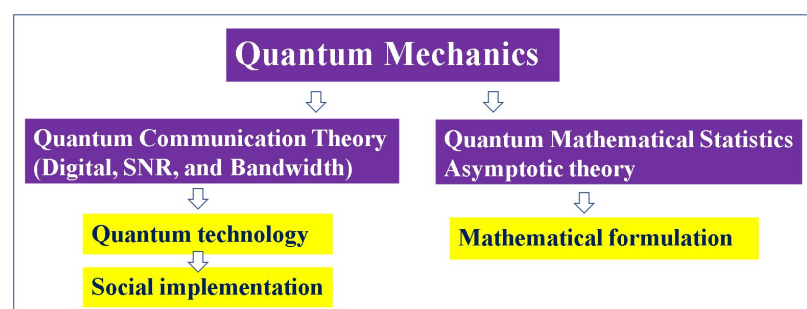


Figure 3. The fundamental concepts of quantum communication theory and quantum mathematical statistics are different, though they have certain similarities. The former has to guarantee operational meaning for quantum communication technology. The latter provides a formulation for statistics, with asymptotic properties, etc., as its main objective. Thus, it does not provide operational meaning. The relationship between the two is the same in classical theory.

5. Quantum Shannon Information Transmission Theory

Shannon theory is a design theory for transmitting signals through noisy communication channels with as few errors as possible. Shannon defined mutual information as the evaluation function, and its maximum value is called the channel capacity. Its operational meaning is the maximum rate (a kind of efficiency) at which errors can be minimized.

In this section, we explain the foundation of design theory for systems in which communication signals are transmitted by optical signals of quantum nature. From Theorem 1, it is necessary to assume a coherent state for quantum design to provide advantages over existing communication capabilities in real-world environments.

5.1. Channel Capacity

5.1.1. Finite, Discrete Alphabet System

Shannon mutual information in the quantum measurement channel is written as follows:

$$J_1(\xi, \Pi) = \sum_{i=1}^M \sum_{j=1}^{M'} \xi_i P(j|i) \ln \left[\frac{P(j|i)}{\sum_k \xi_k P(j|k)} \right] \quad (56)$$

where $P(j|i) = \text{Tr} \rho_i \Pi_j$. The theory of maximization of mutual information is twinned with the above quantum decision theory, and it is denoted as follows:

$$C_1 = \sup_{\xi, \Pi} J_1(\xi, \Pi) \quad (57)$$

Thus, it has the same theoretical structure as the optimal theory for detection theory. As a result, the basic result was derived by Holevo [2] as shown below.

Theorem 8 (*{Holevo}*). *The necessary condition for maximum mutual information with respect to the decision operators for a simple set of states is given as follows:*

$$\begin{aligned} P(j|i) &= \text{Tr} \rho_i \Pi_j \\ \mathbf{F}_j &= \sum_i \xi_i \rho_i \log \left\{ \frac{P(j|i)}{\sum_l \xi_l P(j|l)} \right\} \\ \Pi_j [\mathbf{F}_j - \mathbf{F}_i] \Pi_i &= 0, \forall i, j \end{aligned} \quad (58)$$

where the solution is called accessible information.

On the other hand, there is a problem of Davies in the case of the optimization of mutual information [30]. A partial solution to this is given by [31] under Jozsa's guidance.

We consider the concrete property of the above. Several properties of mutual information were discussed in the serial papers by M. Osaki [32]. As in signal detection theory, the mutual information obtained by the optimal decision operator is greater than that obtained by a classical measurement process. The most useful results are as follows.

Remark 3. *When the signal states are group covariant, the quantum Bayes and minimax decision operators satisfy the above necessary condition for mutual information. In a real environment with large losses or background noise, no quantum state exists that can exceed the mutual information provided by communication based on coherent states.*

Now we still have a difficult problem that is proof of sufficiency. According to Osaki's analysis, the quantum minimax decision operator may provide the maximum mutual information in the practical region such as $|\alpha|^2 \gg 1$ in the set of coherent states.

On the other hand, let us consider the n -th extension of the alphabet and adopt the decision operator based on entangled measurement. Then the following conjecture is imposed:

$$C_1 \leq C_2 \leq \cdots \leq C_n \cdots \leq C_\infty = \lim_{n \rightarrow \infty} \frac{1}{n} C_n \quad (59)$$

Hausladen et al. [4] proved it for the pure-state channel, and Holevo, Schumacher, and Westmoreland proved it for the general states [5,6].

Theorem 9 (*{Holevo · Schumacher · Westmoreland}*). *The upper bound of maximum mutual information and the capacity are given by Holevo information as follows:*

$$C_1 \leq S(\rho_T) - \sum_{i=1}^M \xi_i S(\rho_i) = I_H \quad (60)$$

$$\text{where } \rho_T = \sum_{k=i}^M \xi_i \rho_i,$$

$$\text{Then } C_\infty = C_{\text{Holevo}} = \max_{\xi} I_H \quad (61)$$

where $S(\rho) = -\text{Tr} \rho \log \rho$ is the von Neumann entropy.

The above theorem is the channel capacity formula for a quantum Shannon information transmission system.

Remark 4. *The maximum absolute value of Holevo · Schumacher · Westmoreland (HSW) capacity in a real environment is given by the coherent state.*

The numerical properties of HSW capacity for coherent-state signals have been analyzed by our group [33,34].

5.1.2. Infinite Alphabet System (Continuous)

After the analysis for discrete alphabet systems, the analysis was extended to analog signals with constrained power inputs, among which are channels with additive quantum Gaussian noise. This is the issue of the infinite alphabet scheme. Here we denote a simple result on the final capacity formula of quantum Gaussian channels of free space. According to the quantum Shannon theory established by Holevo and others, the capacity formula of optical quantum communication for free space lossy Gaussian channels is discussed in [35–37].

Theorem 10 (*{Holevo · Sohma · Hirota}*). *The capacity formula of the single-mode quantum lossy Gaussian noise channel is given as follows [36]:*

$$\begin{aligned} C_{\text{Holevo}} &= g(N_s + N_{Th}) - g(N_{Th}) \\ &= (N_s + N_{Th} + 1) \log(N_s + N_{Th} + 1) \\ &\quad - (N_s + N_{Th}) \log(N_s + N_{Th}) \\ &\quad - (N_{Th} + 1) \log(N_{Th} + 1) \\ &\quad + N_{Th} \log N_{Th} \end{aligned} \quad (62)$$

where the above is given by the coherent state; $g(x) = (x + 1) \log(x + 1) - x \log x$, N_s and N_{Th} are average photon numbers of the signal and additive noise at the receiver; and 1 of $(1 + N_{Th})$ means the quantum noise.

The above formula is, in general, greater than the Shannon classical capacity.

$$C_{Shannon} = \log\left(1 + \frac{N_s}{1 + N_{Th}}\right) \quad (63)$$

where the above formula is given by a heterodyne receiver. Thus, the main parameter of capacity in Shannon theory for continuous alphabets is the SNR.

5.1.3. Quantum Advantage in Capacity

Let us discuss quantum advantage. In the transmission system of Shannon information, the quantum advantage for a discrete alphabet is given by

$$C(\text{classical}) \leq C_1 \leq C_H \quad (64)$$

where $C(\text{classical})$ means the capacity for a digital optical fiber communication system designed by conventional communication theory. The above relation of quantum advantages results from the error mitigation effect in the quantum decision mechanism and coding designed by quantum detection theory.

On the other hand, the quantum advantage in the case of infinite alphabets (continuous) is given by

$$C_{Holevo} - C_{Shannon} \geq 0 \quad (65)$$

When the background noise is very large, the quantum advantage disappears.

5.1.4. Implementation Problem

It is important to discuss technologies that will actually realize quantum gain in terms of capacity. The quantum gain for C_1 comes from the effect of the decision operator of a single shot. The quantum gain of C_H comes from both the decision operator based on entangled measurement and coding scheme. Below are some examples of discrete and continuous systems.

(a) Finite, discrete case

The problem, in this case, is an issue of superadditivity of the capacity C_n with respect to n . There are two elements to achieving superadditivity. One is code construction consisting of a sequence of quantum states. The second is a construction of decision operator and its generalization based on entangled measurement; see Equation (12). Many pioneering analyses of the former have already been published, but the latter remains a very difficult problem. Several challenging attempts based on measurement effect have been made [38–41], and some analytical examples based on coding and measurement are given in [42,43].

(b) Continuous case

Generally, quantum gain disappears when the background noise is large or the signal energy is large. Therefore, we discussed how to achieve this when there is no background noise and the received signal is very weak from an ultra-long distance. In this case, it is known that the capacity can be attained by discretization [44].

5.2. Quantum Reliability Function and Quantum Cut-Off Rate

5.2.1. Reliability Function

The operational meaning of Shannon mutual information is the efficiency of coding and decoding in a noisy channel. The unit is bits/symbol, and it is not the actual amount of information. Reliability functions are introduced to clarify the operational meaning

of Shannon mutual information and channel capacity. Here, we show their quantum equivalents. In general, the reliability function is defined as follows:

$$E_{Q'}(R) = \lim_{n \rightarrow \infty} \sup \frac{1}{n} \ln \frac{1}{P_e} \quad (66)$$

The upper bound of the average error probability of a code of length n is as follows:

$$P_e \leq e^{-nE_{Q'}(R)} \quad (67)$$

We will avoid mathematical details and discuss this in a simplified form.

Theorem 11 (*{Burnashev · Holevo}* [8,9]). *The upper bound on the average error probability of a pure-state code for a quantum channel is given by*

$$\begin{aligned} P_e &\leq 2 \exp \left\{ - \max_{\xi} \max_{0 \leq s \leq 1} n [\mu_Q(\rho_{\xi}, s) - sR] \right\} \\ &\equiv \exp[-nE_Q(R)] \end{aligned} \quad (68)$$

where

$$E_Q(R) = \max_{\xi} \max_{0 \leq s \leq 1} n [\mu_Q(\rho_{\xi}, s) - sR] \quad (69)$$

$$\mu_Q(\rho_{\xi}, s) = -\ln[\text{Tr} \rho_{\xi}^{1+s}], \quad (70)$$

$$\rho_{\xi} = \sum_{j=1}^M \xi_j |\psi_j\rangle\langle\psi_j|$$

where M is the number of symbols.

Now the maximization problem becomes

$$\frac{\partial}{\partial s} [\mu(s, \xi) - sR] = \frac{\partial [\mu(s, \xi)]}{\partial s} - R = 0 \quad (71)$$

$$\frac{\partial \mu(s, \xi)}{\partial s} = \frac{-\text{Tr} \rho_{\xi}^{1+s} \ln \rho_{\xi}}{\text{Tr} \rho_{\xi}^{1+s}} = \frac{-\sum \lambda_j^{1+s} \ln \lambda_j}{\sum \lambda_j^{1+s}} \quad (72)$$

where λ is an eigenvalue of ρ_{ξ} and it is given by the eigenvalue of the following matrix:

$$\begin{bmatrix} \sqrt{\xi_1 \bar{\xi}_1} \langle \psi_1 | \psi_1 \rangle & \cdots & \sqrt{\xi_1 \bar{\xi}_M} \langle \psi_1 | \psi_M \rangle \\ \vdots & \ddots & \vdots \\ \sqrt{\xi_M \bar{\xi}_1} \langle \psi_M | \psi_1 \rangle & \cdots & \sqrt{\xi_M \bar{\xi}_M} \langle \psi_M | \psi_M \rangle \end{bmatrix} \quad (73)$$

The above formula assumes the decision operator based on entangled measurement.

If quantum measurements are individual measurements, the reliability function is given by

$$E_{\text{semi}} = -sR - \ln \sum_{j=1}^{M'} \left(\sum_{i=1}^M \xi_i P(j|i)^{1/1+s} \right)^{1+s} \quad (74)$$

where $P(j|i) = \text{Tr} \rho_i \Pi_j$ and the optimum $\{\Pi\}$ is given by the minimum error probability conditions [10–12]. So this is called semi-quantum reliability function. Ban and Kurokawa clarified the difference between the two definitions [13,14].

5.2.2. Quantum Cut-Off Rate

The quantum cut-off rate is defined from formulation of the quantum reliability function of Burnashev · Holevo in the paper of Figure 4. It is given by [13,14]

Definition 9. The quantum cut-off rate is defined as follows.

$$\begin{aligned} \mathbf{R}_Q &\equiv \max_{\{\xi_i\}} [\mu(\rho_{\xi_i}, s=1)] \\ &= \max_{\{\xi_i\}} \left[-\ln \sum_{i=1}^M \sum_{j=1}^M \xi_i \xi_j |\langle \psi_i | \psi_j \rangle|^2 \right] \\ &= -\ln \left[\min_{\{\xi_i\}} \sum_{i=1}^M \sum_{j=1}^M (\Gamma)_{ij} \xi_i \xi_j \right] \end{aligned} \quad (75)$$

where $(\Gamma)_{ij} = |\langle \psi_i | \psi_j \rangle|^2$.

When the optimization with respect to ξ is performed, we have the following simple form.

Theorem 12 (*{Ban · Kurokawa · Hirota}*). The quantum cut-off rate is given by

$$\mathbf{R}_Q = -\ln \left[\sum_{i=1}^M \sum_{j=1}^M (\Gamma^{-1})_{ij} \right]. \quad (76)$$

under the condition for the optimum values of ξ as follows:

$$\tilde{\xi}_i = \frac{\sum_{j=1}^M (\Gamma^{-1})_{ij}}{\sum_{i=1}^M \sum_{j=1}^M (\Gamma^{-1})_{ij}} > 0 \quad \forall i \quad (77)$$

When the a priori probability is uniform, it becomes

$$\begin{aligned} \mathbf{R}_Q &= \ln \left[\frac{M}{\sum_{j=1}^M |\langle \psi_i | \psi_j \rangle|^2} \right] \\ &= \ln \left[\frac{M}{\langle \psi | \hat{\Phi} | \psi \rangle} \right]. \end{aligned} \quad (78)$$

where $\hat{\Phi} = \sum_{i=1}^M |\psi_i\rangle \langle \psi_i|$.

Thus, the relation between the reliability function and the cut-off rate is given by

$$P_e \leq 2 \exp[-n \mathbf{E}_Q(R)] \leq 2 \exp[-n(\mathbf{R}_Q - R)]. \quad (79)$$

Here let us introduce the definition by Helstrom based on individual measurement.

Definition 10. Here a cut-off rate based on quantum individual measurement is defined as follows:

$$\mathbf{R}_{semi} = \max_{\{\xi_i\}} \max_{\{\hat{\Pi}_i\}} \left(-\ln \sum_{j=1}^{M'} \left[\sum_{i=1}^M \xi_i \sqrt{\text{Tr} \hat{\rho}_i \hat{\Pi}_j} \right]^2 \right) \quad (80)$$

And the upper bound of the above formula is given by

$$\tilde{\mathbf{R}}_{semi} = \max_{\{\xi_i\}} \left[-\ln \sum_{i=1}^M \sum_{j=1}^M (G)_{ij} \xi_i \xi_j \right] \quad (81)$$

where $G_{i,j} = | \langle \psi_i | \psi_j \rangle |$. As a result, we have

$$\mathbf{R}_{semi} \leq \mathbf{R}_Q \leq \mathbf{E}_Q \quad (82)$$

The example will be given in the next section.

In the above, we introduced the special case of the pure state. For the general case, refer to Holevo's paper [9].

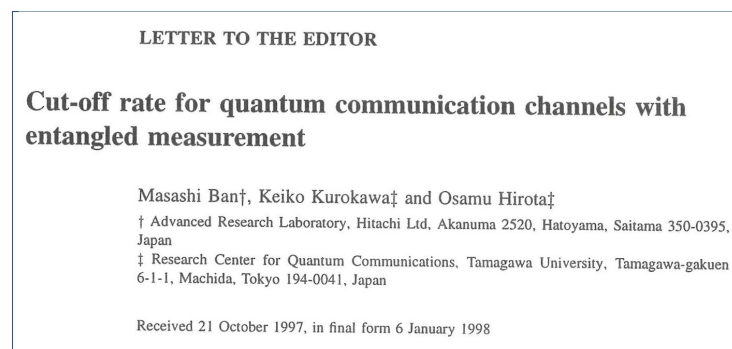


Figure 4. This paper clearly showed the specific structure of definition and effect of cut-off rate of the decision operator based on entangled measurement [13].

6. Examples of Reliability Function and Cut-Off Rate

6.1. Finite, Discrete Alphabet System

Let us show some examples of the reliability function and cut-off rate for the finite alphabet.

6.1.1. Analytical Method

The signal system is set to 3-ary PSK, which is composed of coherent states that enable ultra-high speeds over long distances.

$$|\psi_1\rangle = |\alpha\rangle, \quad |\psi_2\rangle = |\alpha e^{i\frac{2}{3}\pi}\rangle, \quad |\psi_3\rangle = |\alpha e^{-i\frac{2}{3}\pi}\rangle \quad (83)$$

In this case, the modified Gram matrix is as follows:

$$\frac{1}{3} \begin{bmatrix} 1 & K_c + iK_s & K_c - iK_s \\ K_c - iK_s & 1 & K_c + iK_s \\ K_c + iK_s & K_c - iK_s & 1 \end{bmatrix}, \quad (84)$$

The eigenvalues of the above are

$$\begin{aligned} \lambda_1 &= \frac{1 + 2K_c}{3}, \\ \lambda_2 &= \frac{1 - K_c - \sqrt{3}K_s}{3}, \\ \lambda_3 &= \frac{1 - K_c + \sqrt{3}K_s}{3} \end{aligned} \quad (85)$$

where

$$\begin{aligned} K_c &= \exp\left[-\frac{3N_s}{2}\right] \cos\left[\frac{\sqrt{3}N_s}{2}\right], \\ K_s &= \exp\left[-\frac{3N_s}{2}\right] \sin\left[\frac{\sqrt{3}N_s}{2}\right] \end{aligned} \quad (86)$$

where N_s is the average photon number per pulse at the receiver. From these, we can derive the quantum reliability function and quantum cut-off.

On the other hand, if we assume individual measurements, we will adopt individual optimal decisions. In that case, the elements of the communication channel will be as follows:

$$\begin{aligned} P(1|1) &= P(2|2) = P(3|3) \\ &= \frac{1}{9}\{3 + 2\sqrt{\beta_1\beta_2} + \\ &\quad 2\sqrt{\beta_2\beta_3} + 2\sqrt{\beta_3\beta_1}\}, \\ P(1|2) &= P(2|3) = P(3|1), \\ P(1|3) &= P(2|1) = P(3|2), \\ &= \frac{1}{9}\{3 - \sqrt{\beta_1\beta_2} - \\ &\quad \sqrt{\beta_2\beta_3} - \sqrt{\beta_3\beta_1}\} \end{aligned} \quad (87)$$

where

$$\begin{aligned} \beta_1 &= 1 + 2K_c, \\ \beta_2 &= 1 - K_c - \sqrt{3}K_s, \\ \beta_3 &= 1 - K_c + \sqrt{3}K_s \end{aligned} \quad (88)$$

Figure 5 shows a numerical example. The communication system we set up here is intended for deep space communication, where the transmitted signal is sufficiently large and the transmission attenuation is extremely large, resulting in an extremely small received signal.

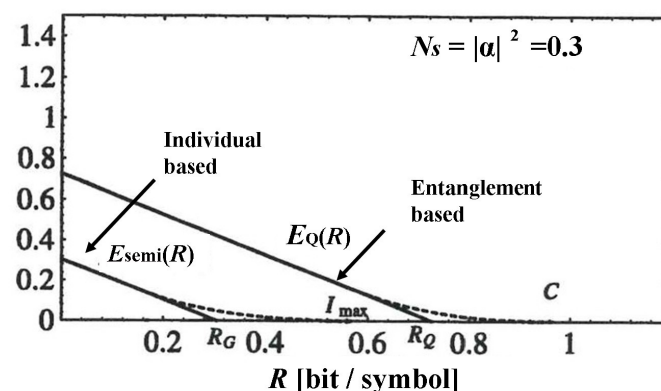


Figure 5. Numerical example of reliability function and cut-off rate for the decision operators based on entangled measurement and individual measurement [45]. This shows the advantage of the reliability functions and cut-off rate based on entangled measurement.

6.1.2. Quantum Advantage of Decision Operator Based on Entangled Measurement

The role of quantum reliability function theory is to show how small the error rate of the transmitted code can be when the transmission rate of code is set. In the design theory of conventional optical communications, classical devices such as heterodynes and energy detectors are used as receivers, and reliability functions are evaluated using classical theory. The question is what benefits the quantum theory introduced here will bring to conventional optical communications. In quantum theory, quantum effects appear in quantum measurements, i.e., at the receiver. From the above theory, individual measurements only reduce the effect of quantum noise on individual signals. On the other hand, entangled measurements can take into account the quantum interference effect among signals due to measurement in addition to the individual quantum effects, thereby further reducing the quantum noise effect and increasing the reliability function and cut-off rate. As a result, when the code error rate is fixed (depending on the application), the code length required to achieve the same error rate can be significantly shortened. See Figure 6.

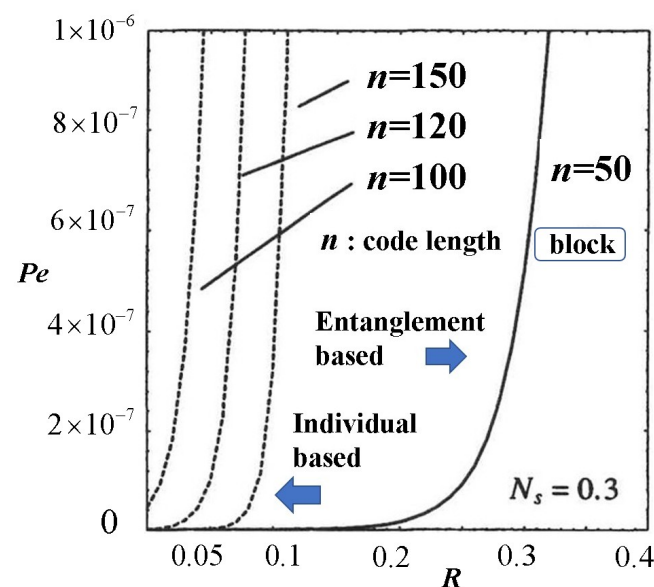


Figure 6. Numerical examples of quantum advantage according to block code length by decision operators based on entangled measurement and individual measurement [45].

6.2. Infinite Alphabet System (Continuous)

6.2.1. Reliability Function

The case of continuous systems with an infinite alphabet was introduced in the paper of Figure 7 [46]. This discussion is extremely important because it can clarify how quantum gain appears, i.e., in comparison with discrete systems.

Let us take the input alphabet A , an arbitrary Borel subset in a finite-dimensional Euclidean space. The input is described by an a priori probability $\zeta(x)$ on A . The energy constraint is posed as follows:

$$\int_A (x - \langle x \rangle)^2 \zeta(x) dx \leq N_s \quad (89)$$

We adopt the product Hilbert space $H^{\otimes n} = H \otimes H \otimes \dots \otimes H$ with the input alphabet n consisting of code words $W = (x_1, x_2, \dots, x_n)$ of length n , and the density operator

$$\rho_W = \rho(x_1) \otimes \dots \otimes \rho(x_2) \otimes \dots \otimes \rho(x_n) \quad (90)$$

We define the set of code of size M that is a sequence $\{W(1), W(2), \dots, W(M)\}$. $\{\Pi_j^c\}$ is a family of decision operators in $H^{\otimes n}$ based on entangled measurement, satisfying $\sum_{j=1}^M \Pi_j^c = I$. The error probability for a code word is $P(k|j) = \text{Tr} \rho_{W(j)} \Pi_k^c$, where $j, k = 1, 2, \dots, M$.

Let us consider the speed of the exponential decay of the error probability when $n \rightarrow \infty$ and $M = e^{nR}$ below the following capacity:

$$C_H = \max_{\mathcal{P}(x)} [\hat{H}(\Lambda[\rho_T(\xi(x))]) - \int \hat{H}(\Lambda[\rho(x)]) \xi(x) dx] \quad (91)$$

Following the Shannon idea of random coding, let us consider the random ensemble of M code words of length n . We have the following theorem [46].

Theorem 13 (*{Holevo}*). Let us define $P_e(M = e^{nR}, n)$ as the minimum error probability with respect to coding and the decision operator. Here we introduce the reliability function as follows:

$$\mathbf{E}(R) = \lim_{n \rightarrow \infty} \sup \frac{1}{n} \log \frac{1}{P_e(e^{nR}, n)} \quad (92)$$

The lower bound of the reliability function is given by

$$\mathbf{E}(R) \geq \max\{\mathbf{E}_{Q_r}(R), \mathbf{E}_{Q_{ex}}(R)\} \quad (93)$$

where Q_r and Q_{ex} mean the random coding bound and expurgated bound, respectively. They are

$$\mathbf{E}_{Q_r}(R) = \max_{0 \leq s \leq 1} (\max_{0 \leq p} \max_{\xi} \mu(\xi, s, p) - sR) \quad (94)$$

$$\mathbf{E}_{Q_{ex}}(R) = \max_{1 \leq s} (\max_{0 \leq p} \max_{\xi} \tilde{\mu}(\xi, s, p) - sR) \quad (95)$$

where

$$\begin{aligned} \mu(\xi, s, p) &= -\log \text{Tr} \left(\int e^{p[f(x)-E]} \rho(x) \xi(x) \right)^{1+s} \\ \tilde{\mu}(\xi, s, p) &= -s \log \int \int e^{p[f(x)+f(y)-2E]} \\ &\quad \times (\text{Tr} \sqrt{\rho(x)} \sqrt{\rho(y)})^{1/s} \xi(x) \xi(y) \end{aligned} \quad (96)$$

where f is a function satisfying the condition for the central limit theorem for a random variable $f(x_k)$

$$\int f(x)^2 \xi(x) < E \quad (97)$$

This corresponds to the energy constraint.

The above equations are primitive formulae of quantum reliability function theory [46].

6.2.2. Cut-Off Rate

In general, it is difficult to obtain the reliability function. Therefore, it is useful to define and calculate the cut-off rate in the same way as in the discrete system. It is given by the following relation:

$$\mathbf{R}_Q = \max_{0 \leq p} \max_{\xi} \mu(\xi, 1, p) \quad (98)$$

where s is fixed to 1.

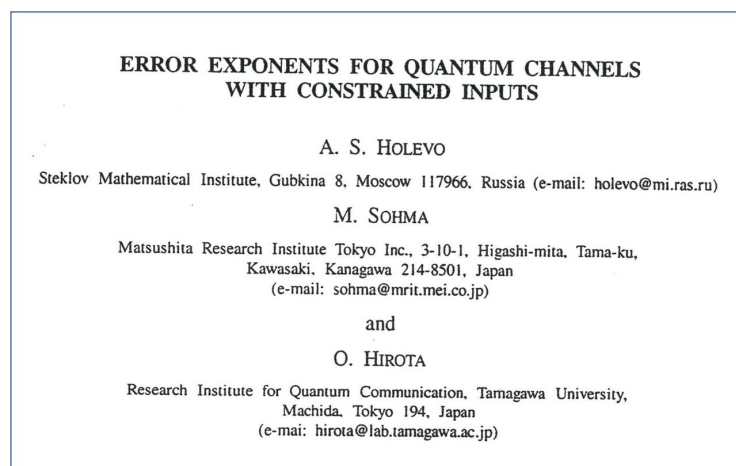


Figure 7. This paper provides the first rigorous definition of reliability function and cut-off rate for infinite alphabet systems under the energy constraint [46]. Especially, the concrete form of quantum cut-off rate is given.

6.2.3. Example of Cut-Off Rate for Gaussian Channel

In real communication, the only useful quantum states of continuous quantities are coherent states. Let us assume that the coherent-state alphabet is disturbed by Gaussian noise.

$$\rho_0 = \frac{1}{\lambda + 1/2} \sum_{n_p} \left(\frac{\lambda - 1/2}{\lambda + 1/2} \right)^{n_p} |n_p\rangle \langle n_p| \quad (99)$$

Even in this case, it is difficult to obtain an exact formula for the reliability function. However, we have the exact solution of the cut-off rate as follows:

$$\mathbf{R}_Q = 2 \left(\frac{N_{sc}}{2g} + 1 - \mathcal{D}(N_{sc}/g) \right) + \log \mathcal{D}(N_{sc}/g) \quad (100)$$

where $\mathcal{D}(N_{sc}) = (1 + \sqrt{N_{sc}^2 + 1})/2$, N_{sc} is the energy of the code word, and $g = \lambda g_{1/2}(\lambda)$, with

$$g_{1/2}(t) = \frac{1}{2t} \times \frac{(t + 1/2)^{1/2} + (t - 1/2)^{1/2}}{(t + 1/2)^{1/2} - (t - 1/2)^{1/2}} \quad (101)$$

In this case, the quantum gain is only the entangled effect of the decision process, i.e., the double quantum gain disappears as in the discrete system.

6.3. Importance of Cut-Off Rate and Quantum Advantage

According to reliability function theory, when the rate exceeds the cut-off rate and enters the capacity region, an extremely long code length is required to achieve a sufficiently small error rate. This means increased communication delays and has come to be seen as the biggest drawback of modern communication technology. Therefore, rather than achieving capacity, a coding technique that minimizes code length in the cut-off rate region is essential. Based on the theory in this section, it is preferable to utilize the effect of entangled measurement to shorten code length rather than increase capacity. This is because the amount of information that can be transmitted (bit/s) can be increased by orders of magnitude with optical communication. Therefore, there is no longer any need to forcefully achieve channel capacity, which is efficiency. Rather, delay is the major issue.

In other words, we can point out the following: The primary requirements of modern communication systems are low latency and ultra-high speed. This is because communication systems are fundamentally bidirectional. The challenge for the former lies in shortening the code length, while the latter depends on bandwidth characteristics. Since

channel capacity is merely a matter of efficiency, if sufficient bandwidth is available, there is no need to pursue channel capacity. Channel capacity becomes a concern only in inherently unidirectional communication scenarios, such as deep space. Quantum systems, being based on optical communication, have ample bandwidth. However, shortening the code length remains a challenge. Therefore, as pointed out here, it is desirable to develop techniques for shortening code length based on the cut-off rate. Further details will be discussed in the following paper.

7. Discovery of a Cipher That Breaks the Shannon Impossibility Theorem

In the previous section, applications of quantum effects to the modern optical communications were considered for achieving high-performance communication based on quantum Shannon theory.

In this section and the sections that follow, we introduce applications of quantum Shannon theory to several technologies, such as cipher and radar. In the case of ciphers, to achieve information-theoretic security for symmetric key ciphers, it is necessary to realize a mechanism that can hide not only data but also secret keys by using quantum noise. This can consist of modulation and demodulation technologies based on the above theories (Figure 8). In this section, we will introduce the basic concept.

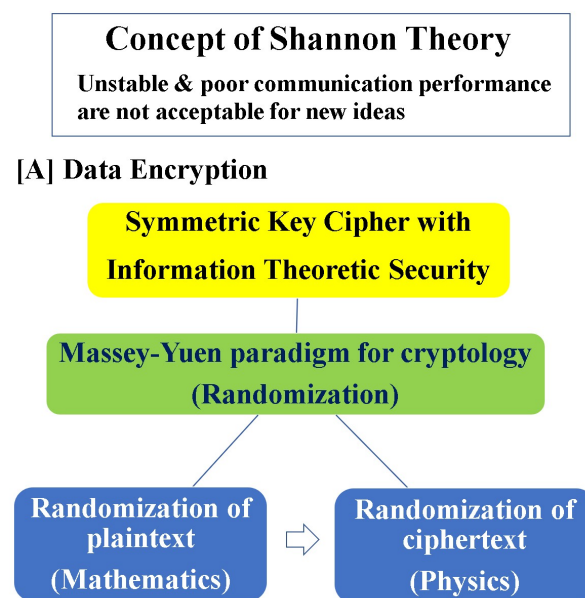


Figure 8. Basic scenario in the Shannon concept for cryptology. One can obtain the drastic quantum advantage in physical encryption based on the quantum modulation–demodulation protocol.

7.1. New Principle for Ciphers

First of all, we will introduce the application of quantum Shannon theory to the design of ciphers. This is the most exciting application of quantum information science, as it promises to completely outperform conventional functionality in the real world.

There are several no-go theorems in quantum mechanics. Quantum Shannon theory can be considered a theory for designing optimal communication systems that utilize these.

The most important application is to solve the Shannon impossibility theorem, which limits the security of classical cryptography. The Shannon impossibility theorem is given as follows.

Theorem 14 ({Shannon}). *The information-theoretic security of a symmetric key cipher is limited by the Shannon entropy of the key.*

$$H(X|Y) \leq H(K_S) \quad (102)$$

where X is the message, K_S is the shared secret key, and Y is the ciphertext received by an eavesdropper. The perfect secure cipher is only given by a one-time pad cipher.

The principle proposed to break the above theorem is the KCQ principle (keyed communication in quantum noise). It was disclosed as a white paper in 2000 and made public in 2003 [47].

Principle 1 ({Yuen}). *The non-orthogonality of a set of signal states can be increased by randomization due to a secret key. One can create a differentiation in reception performance such that the performance of the receiver with a key to randomized quantum states is superior to that of the receiver without the key. That is,*

$$\bar{P}_e^B(\text{with} - \text{key}) \ll \bar{P}_e^E(\text{without} - \text{key}) \quad (103)$$

$$C^B(\text{with} - \text{key}) > C^E(\text{without} - \text{key}) \quad (104)$$

where $\bar{P}_e$ and C are the error performance of signal detection and the capacity, respectively. The indexes B and E mean Bob and Eve. These inequalities are called advantage creation based on KCQ.

Yuen's main focus was quantum key distribution (QKD) as an application of his own principle. I introduced Yuen's concept for lifting the Shannon impossibility theorem of symmetric key ciphers based on the above principle in 2004 (Figure 9) [48]. Since then, our collaborative research has brought various important advances [49–51]. In the following, we show a survey of how to apply quantum communication theory to realize a cipher based on KCQ. Its main concept is to use quantum modulation as encryption.

General Theory of Information Transfer and Combination (April, 2004)

Room: Pentagon - QUANTUM INFORMATION
Jozef Gruska (Brno): "Quantum information processing primitives"
Philippe Jorrand (Grenoble): "Toward minimal resources for universal measurement-based quantum Turing machines"
Anna Sanpera (Hannover): "Witnessing entanglement"
Osamu Hirota (Tokyo): "Secure quantum communication protocol based on quantum communication theory"
- Coffee Break -
Alexander S. Holevo (Moscow): "An exactly solvable model related to the additivity problem for quantum channels"
Andreas Winter (Bristol): "Identification via quantum channels"
Philippe Blanchard (Bielefeld): "Quantum random walk and piecewise deterministic evolutions"
Armin Uhlmann (Leipzig): "On rank two channels"

Figure 9. Program of the Conference on General theory of Information Transfer and Combination held at the Center for Interdisciplinary Research, Bielefeld University, organized by Prof. Rudolf Ahlswede.

7.2. Optical Quantum Modulation as Encryption Based on the New Principle

In this section, we will explain the model of the encryption–decryption scheme by optical quantum modulation–demodulation and clarify the principle behind the appearance of quantum noise effects to hide the data and the shared secret key. We mainly deal with quantum stream ciphers and quantum block cipher formats.

(a) Quantum stream cipher

The first example of ciphers designed according to this principle is the quantum stream cipher. For detailed diagrams of the structure, see references [49–51].

Let us denote the protocol, where the data (plaintext) is a sequence of binary signals:

- (i) The sender prepares a big number ($M \gg 1$) of communication bases $\{|\alpha_m\rangle, |-\alpha_m\rangle\}$ consisting of two non-orthogonal states (coherent state with high power) such as

$$\{|\alpha_1\rangle, |-\alpha_1\rangle\}, \dots, \{|\alpha_M\rangle, |-\alpha_M\rangle\} \quad (105)$$

where $m = \{1, 2, 3, \dots, M\}$. One of them is selected by using a pseudorandom number generator (PRNG) with a secret key.

- (ii) The sender then transmits binary data using the selected binary communication basis.

$$0 \text{ or } 1 \rightarrow \text{Mapper} \rightarrow |\alpha_m\rangle \text{ or } |-\alpha_m\rangle \quad (106)$$

where *Mapper* is the random mapping function due to the same PRNG (see [51]).

- (iii) A receiver who has the same pseudorandom number with the key can identify the communication basis, so they always receive binary signals with small error, because the signal amplitude of binary coherent states is large enough.

A receiver who does not have the key must identify the quantum states of $2M$ that make up the many communication bases, which increases the error. The reason is that the discrimination error of a multi-quantum state is larger than that of a binary quantum state according to quantum detection theory.

The designer of this cipher could use this error to completely erase the information on the secret key and pseudorandom number structure shared by the sender and receiver, optimizing the scheme based on quantum Shannon theory (see reference [51] for the specific protocol and structure).

As a result, the ciphertext for the eavesdropper is completely masked by quantum error, and it becomes possible to break the Shannon limit (Shannon impossible theorem), which determines the limitation of information-theoretic security of symmetric key ciphers. That is,

$$H(X|Y^{E_q}) \gg H(K_S) \quad (107)$$

where Y^{E_q} is the ciphertext received by the eavesdropper.

Shannon's focus was only on ciphertext-only attacks, but in modern times, it is necessary to deal with known-plaintext attacks. For this reason, the following evaluation method has been established [52]. The quantitative evaluation of information-theoretic security is evaluated by the unicity distance for known-plaintext attacks.

Definition 11. The unicity distance of known-plaintext attacks for quantum stream ciphers is defined as follows:

$$n_1^Q : H(K_S | X_{n_1^Q}, Y_{n_1^Q}^{E_q}) = 0 \quad (108)$$

It is the minimum value of the ciphertext sequence required for an eavesdropper to be able to guess the key. Then it is given by the following theorem [52].

Theorem 15 (*{Yuen · Nair}*). The lower bound of the generalized unicity distance for KPA is given as follows:

$$n_1^Q \geq \frac{|K_S|}{C_1^E}, \quad C_1^E = \max_{\{\Pi^E\}} I(K^R; Y^{E_q}) \quad (109)$$

where C_1^E is the maximum amount of mutual information (accessible information) for the eavesdropper's measurement from a set of quantum states with K^R (running key sequence) as a variable. C_1^E can be replaced with Holevo capacity.

However, the original idea did not guarantee sufficient security against known-plaintext attacks. In 2007, we solved that problem. That is, one can attain $C_1^E \rightarrow 0$ by generalized randomization [53] (see reference [51] for the detailed concept). In other words, while the one-time pad requires a secret key of the same length as the message, this mechanism can encrypt any message in an information-theoretically secure manner using only a short secret key of a few hundred bits.

As a result, these quantum stream ciphers can provide the encryption system with 100 Gbit/s $\sim$ 10 Tbit/s over a communication distance of 1000 km $\sim$ 10,000 km, guaranteeing information-theoretic security. More details are provided in Section 7.3.

(b) Quantum block cipher

We can consider the block cipher form based on the new principle. Quantum versions of classical block ciphers are called quantum block ciphers. Here we introduce the encryption theory for the quantum block cipher using unitary transformation by Sohma [54,55], which is also a scheme of quantum modulation.

First, let us consider M -ary coherent state composed by M blocks of coherent states as follows:

$$|\Phi\rangle = |\alpha_1\rangle |\alpha_2\rangle |\alpha_3\rangle \dots |\alpha_M\rangle \quad (110)$$

We consider an operator $\mathbf{V}$ that extends the Heisenberg commutation relation for self-adjoint operators on Hilbert spaces to the Weyl–Segal commutation relation.

Theorem 16. From the Stone–von Neumann theorem, we can construct the following formula. The quantum characteristic function $\mathbf{G}(\mathbf{z})$ for the class of quantum Gaussian state is given as follows:

$$\begin{aligned} \mathbf{G}(\mathbf{z}) &= \text{Tr} \mathbf{U} |\Phi\rangle \langle \Phi| \mathbf{U}^\dagger \mathbf{V}(\mathbf{z}) \\ &= \text{Tr} |\Phi\rangle \langle \Phi| \mathbf{V}(\mathcal{L}^T \mathbf{z}) \end{aligned} \quad (111)$$

where T means transpose and where

$$\mathbf{V}(\mathbf{z}) = \exp\{i\mathbf{R}^T \mathbf{z}\} \quad (112)$$

$$\mathbf{R} = [(\mathbf{q}_1, \mathbf{p}_1), \dots, (\mathbf{q}_M, \mathbf{p}_M)]^T \quad (113)$$

and where $(\mathbf{q}_i, \mathbf{p}_i)$ are the canonical conjugate operators. Then $\mathcal{L}$ in Equation (111) is called a symplectic matrix, and it is given by

$$\mathcal{L} = \begin{pmatrix} r_{11}e^{i\theta_{11}} & \dots & r_{1M}e^{i\theta_{1M}} \\ r_{21}e^{i\theta_{21}} & \dots & r_{2M}e^{i\theta_{2M}} \\ \vdots & \dots & \vdots \\ r_{M1}e^{i\theta_{M1}} & \dots & r_{MM}e^{i\theta_{MM}} \end{pmatrix} \quad (114)$$

$\mathbf{U}$ in Equation (111) is called the unitary operator associated with symplectic transformation $\mathcal{L}$, and the following apply:

- (i) A set of $\mathcal{L}(r_{i,j}, \theta_{i,j})$ with different elements is prepared.
- (ii) One $\mathcal{L}$ is selected from the set using a pseudorandom sequence with the secret key K_S .
- (iii) A quantum ciphertext is generated by a unitary transformation associated with the selected $\mathcal{L}$ as follows.

Here let us denote a vector of complex amplitudes α of coherent state by

$$\vec{\alpha}_{in} = (\alpha_1, \alpha_2, \dots, \alpha_M) \quad (115)$$

then we have the following relation:

$$\vec{\alpha}_{out} = \mathcal{L}\vec{\alpha}_{in} = (\alpha_1^{out}, \alpha_2^{out}, \dots, \alpha_M^{out}) \quad (116)$$

As a result, the unitary transformation for the coherent-state sequence is given as follows:

$$\mathbf{U}|\Phi\rangle = |\Phi_{out}\rangle = |\alpha_1^{out}\rangle |\alpha_2^{out}\rangle \dots |\alpha_M^{out}\rangle \quad (117)$$

Thus, randomization of complex amplitudes through $\mathcal{L}$ converts the basic codes of coherent states into quantum ciphertext with arbitrary complex amplitude by $\mathbf{U}$. When $r_{i,j} = 1, \forall i, j$, the above is called phase randomization.

On the other hand, Bob's decryption procedure involves applying the inverse $\mathbf{U}^{-1}$ of a pseudorandomly selected unitary transformation to the quantum ciphertext by using the same pseudorandom numbers. As a result, a receiver with the key can always receive the basic quantum state code signal before the randomization. For a more detailed explanation, see the study in [56].

7.3. Social Implementation

7.3.1. Development of Transceiver for Quantum Stream Cipher

Finally, we will explain the development status of transceivers for practical use of the above encryption. Figure 10 shows the history of the development of the transceiver. In 2002, a handmade prototype was developed, and communication experiments were successfully conducted at 125 Mbps. Subsequently, with the cooperation of Panasonic and Hitachi, a two-way prototype transceiver was developed. Currently, the development of a commercial transceiver for standard quantum stream ciphers has been completed, and we are now in the phase of improving it to generalized quantum stream ciphers with several randomizations.

On the other hand, P. Kumar and his group at Northwestern University independently developed the world's first high-performance transceiver of quantum stream ciphers in 2002, 2003, and 2009 [57–59]. They also demonstrated it for applications in aircraft communication.

7.3.2. Application to Global Optical Network of 100 Gbit/s of Quantum Stream Cipher

When developing new capabilities in cryptography, it is unacceptable to degrade conventional communication performance. To avoid deterioration of communication characteristics, the application of the coherent state, which is the miraculous quantum state, is essential. The cryptographic techniques introduced in this section do not degrade communication characteristics.

This encryption device can be operated without changing the structure of the current global optical network system with optical amplifier repeaters. In other words, encryption of ultra-high-speed optical communications can be completed simply by replacing the current optical transceivers with quantum stream transceivers.

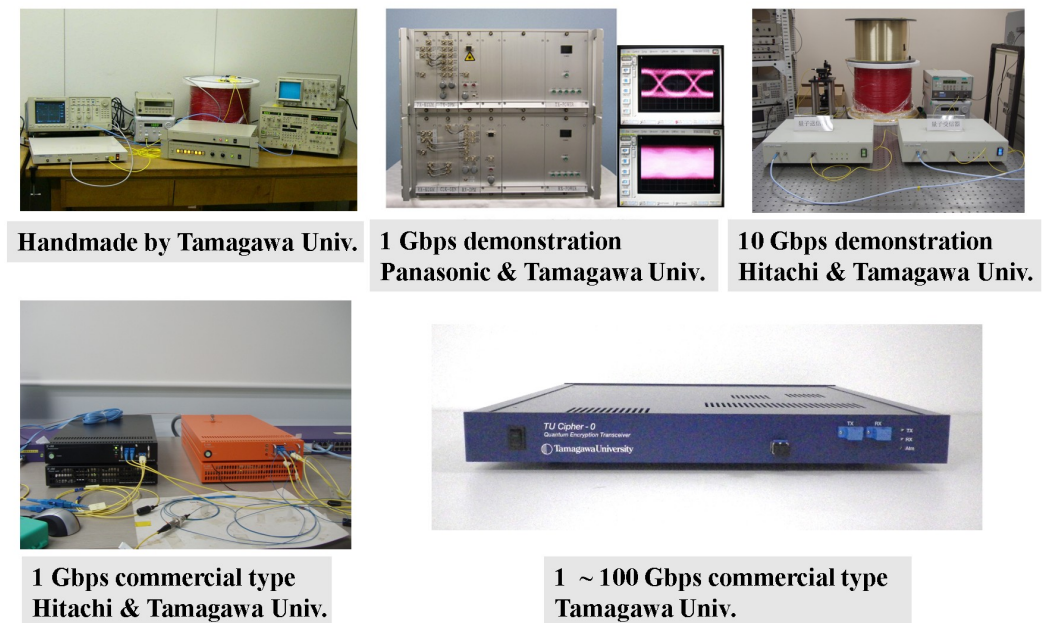


Figure 10. History of the development of quantum stream cipher communication devices, which enable encrypted communication of arbitrary ultra-high-speed binary data with randomized coherent-state signals without delay. Setup is complete by simply replacing the optical transceiver currently in use with the above.

Key distribution for the upper layers of the network utilizes quantum-resistant or PQC, and after key sharing, it can be instantly replaced with a new key using a quantum stream cipher. Thus, we recommend that global network applications in the real world follow the scheme shown in Figure 11. That is, the best solution for defense against today's urgent cyber attacks is to implement a combined scheme of the quantum-resistant public key cryptography as recommended by the NIST and quantum stream ciphers to protect data [60,61]. Much research and development are being carried out towards these goals [62–66].

[B] Authentication and Key Establishment

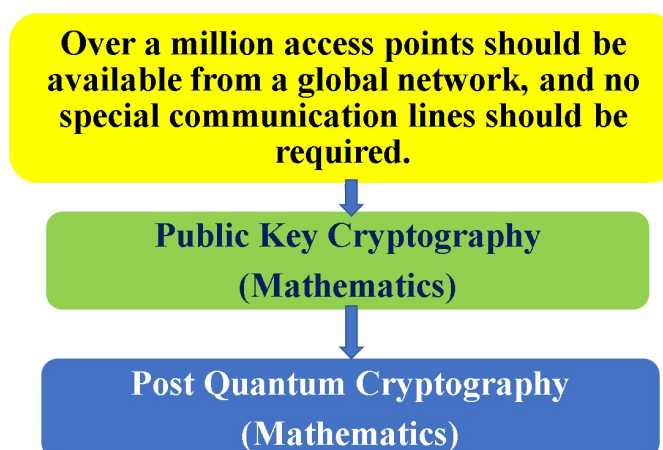


Figure 11. Key distribution and authentication require strong conditions on utility for global networks. After key establishment, the key is exchanged for a new one by using the information-theoretically secure symmetric key cipher described above. It is also safe even if the correct key is leaked after the encrypted communication.

On the other hand, the threat of eavesdropping from undersea cables will become extremely important. This is because in undersea communication networks that are approximately 10,000 km long, signals are transmitted from light to light via optical amplifiers. Furthermore, technology has been established to eavesdrop on optical signals from optical amplifier repeaters.

The quantum stream cipher is expected to be a technology that can address this issue, and preliminary experiments have already been carried out [67]. In such systems, keys are pre-installed, and no key distribution is required.

7.3.3. Business for Quantum Stream Cipher Service

Commercialization of quantum stream cipher transceivers and their application systems began in the United States in 2025. Services that meet customer needs will be available within a few years.

8. Sensor Applications Beyond the Standard Quantum Limit

8.1. Bell State Based on Entangled Coherent State

In general, the Bell states consist of four orthogonal states. However, the four entangled states based on non-orthogonal states are called quasi-Bell states. As a specific example, we present the following states based on coherent states:

$$\begin{cases} |\Psi_1\rangle &= h_1(|\alpha\rangle_A|\alpha\rangle_B + |-\alpha\rangle_A|-\alpha\rangle_B) \\ |\Psi_2\rangle &= h_2(|\alpha\rangle_A|\alpha\rangle_B - |-\alpha\rangle_A|-\alpha\rangle_B) \\ |\Psi_3\rangle &= h_3(|\alpha\rangle_A|-\alpha\rangle_B + |-\alpha\rangle_A|\alpha\rangle_B) \\ |\Psi_4\rangle &= h_4(|\alpha\rangle_A|-\alpha\rangle_B - |-\alpha\rangle_A|\alpha\rangle_B) \end{cases} \quad (118)$$

where $\{h_i\}$ are constants for normalization, i.e., $h_1 = h_3 = 1/\sqrt{2(1+\kappa^2)}$, $h_2 = h_4 = 1/\sqrt{2(1-\kappa^2)}$; $\langle\alpha|-\alpha\rangle = \kappa$; and $\langle-\alpha|\alpha\rangle = \kappa^*$.

Some of these quasi-Bell states are not orthogonal to each other. Here, if $\kappa = \kappa^*$, then their Gram matrix becomes very simple, as follows:

$$G = \begin{pmatrix} 1 & 0 & D & 0 \\ 0 & 1 & 0 & 0 \\ D & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (119)$$

where $D = \frac{2\kappa}{1+\kappa^2}$. Let us employ the entanglement of formation as the degree of entanglement. The degrees of entanglement for quasi-Bell states becomes

$$\begin{aligned} E(|\Psi_1\rangle) &= E(|\Psi_3\rangle) \\ &= -\frac{1+C_{13}}{2} \log \frac{1+C_{13}}{2} - \frac{1-C_{13}}{2} \log \frac{1-C_{13}}{2} \end{aligned} \quad (120)$$

where $C_{ij} = |\langle\Psi_i|\Psi_j\rangle|$, and we have the special property of $E(|\Psi_2\rangle) = E(|\Psi_4\rangle) = 1$ [68]. Thus $|\Psi_2\rangle$ and $|\Psi_4\rangle$ have the perfect entanglement.

These physical properties and the mechanisms of teleportation were elucidated by S.J. van Enk [69].

8.2. Quantum Reading Scheme

The term of quantum reading as a sensor was pioneered by Pirandola [70] (Appendix B). We will employ the PSK scheme such that the memory on the classical disk consists of the flat and concave areas, which correspond to “0” and “1”, respectively. This type of memory was invented in the beginning of the 1980s, employing a gas laser with high coherence as

the light source. Later, its scheme was replaced with a laser diode with high coherence in which the decision scheme consists of the effect of reflection wave injection in laser diodes [71].

For the quantum version of such kind of sensor, one can describe the phase shift by an unitary operator as follows:

$$U(\theta) = \exp(-\theta a^\dagger a) \quad (121)$$

where a and $a^\dagger$ are the annihilation and creation operators for bosonic systems, respectively. Here, the phase factor θ is set to between 0 and 2π .

The reading method in the current PSK scheme is to illuminate the laser light (coherent state) on a disk and to read the phase difference. That is, the signal states of light to discriminate are

$$|\alpha(0)\rangle = I|\alpha\rangle \quad (122)$$

$$|\alpha(1)\rangle = U(\theta)|\alpha\rangle \quad (123)$$

where I is the identity operator.

8.3. Error-Free Sensor Applicable to Reaction Control

Let us introduce an application of the quasi-Bell state in reaction control systems [72]. Here we restrict the problem to binary detection. So detection targets are two quantum states. Since the phase difference will be π , the problem is to read the phase shift π from the steady state or input state.

The coherent states are prepared in the current classical memory, and the target signal model becomes

$$|\alpha(0)\rangle = I|\alpha\rangle = |\alpha\rangle \quad (124)$$

$$|\alpha(1)\rangle = U(\theta = \pi)|\alpha\rangle = |-\alpha\rangle \quad (125)$$

If one employs a conventional homodyne receiver to discriminate the above quantum states, the limitation is imposed by the so-called quantum shot noise limit. This is the standard quantum limit in modern information technology.

However, in general, it is reasonable to employ a quantum optimum receiver in order to overcome the standard quantum measurement which is achieved by a homodyne receiver. In this case, from Equation (14), the limitation depends on the inner product between the two quantum states. For example, the inner product of two coherent states is

$$\langle\alpha|-\alpha\rangle = \exp(-2|\alpha|^2) \quad (126)$$

Let us assume that the $|\Psi_2\rangle$ of quasi-Bell states in Equation (118) is employed as the light source and the B mode illuminates a memory disk. The reflection effect $U_B(\theta)$ operates in B mode, so the channel model is

$$\epsilon_{A\otimes B} = I_A \otimes U_B(\pi) \quad (127)$$

Then, the target states become

$$\begin{aligned} |\Psi_2(0)\rangle &= h_2(|\alpha\rangle_A |\alpha\rangle_B - |-\alpha\rangle_A |-\alpha\rangle_B) \\ |\Psi_2(1)\rangle &= \epsilon_{A\otimes B} h_2(|\alpha\rangle_A |\alpha\rangle_B - |-\alpha\rangle_A |-\alpha\rangle_B) \\ &= h_2(|\alpha\rangle_A |-\alpha\rangle_B - |-\alpha\rangle_A |\alpha\rangle_B) \end{aligned} \quad (128)$$

Thus, the input state $|\Psi_2(0)\rangle = |\Psi_2\rangle$ is changed to $|\Psi_2(1)\rangle = |\Psi_4\rangle$. The inner product between the above two entangled coherent states in the quasi-Bell state is

$$\langle\Psi_2(0)|\Psi_2(1)\rangle = 0 \quad (129)$$

That is, the inner product becomes zero, and it is independent of the energy of the light source. This is a property of the quasi-Bell state. To check this special property, one can examine the different phase shift as follows:

$$|\langle\Psi_2(0)|I_A \otimes U_B(\theta)|\Psi_2(0)\rangle| > 0 \quad (130)$$

where $\theta \neq \pi$.

Finally, let us employ the quantum optimum receiver for the binary pure state of two modes. The ultimate detection performance of systems with the coherent state and homodyne, coherent state and quantum receiver, and quasi-Bell state and quantum receiver are given as

$$\bar{P}_e(C) = \bar{P}_e(\text{Homodyne}) \quad (131)$$

$$\bar{P}_e(Q1) = \frac{1}{2}[1 - \sqrt{1 - 4\xi_0\xi_1 e^{-4|\alpha|^2}}] \quad (132)$$

$$\bar{P}_e(Q2) = 0 \quad (133)$$

respectively. Thus, one can see that the property of the quasi-Bell state provides an attractive improvement, and this property can be obtained only by the combination of the nonclassical state and the quantum optimum receiver. Although there are many nonclassical states, almost all are not changed from the input state to the orthogonal state to the original input state just by reflection. So we interpret that such effectiveness of the quasi-Bell state comes from the special phenomena of entanglement based on non-orthogonal states, which is a feature of quasi-Bell states.

9. Conclusions

This paper explains the development of quantum communication theory and its link to Shannon information transmission theory. In particular, it shows how quantum gain appears in the performance of functions such as communications designed using these theories. While quantum applications are currently being actively discussed, new mechanisms that sacrifice some of the conventional performance when applying quantum properties cannot be applied to real-world situations. In other words, quantum communication using qubits, etc., is not suitable for social implementation, because such schemes cannot maintain the current communication capabilities. In addition, we explained that improving delay characteristics (latency) is essential to communication systems in the 21st century. Therefore, it is essential to advantageously apply quantum effects to modern optical communications, which have the highest performance for communication functions. The theory introduced here has been shown to be compatible with such system design. In particular, the quantum stream cipher, as shown in Figure 12, when compared with conventional technology, is expected to provide new possibilities.

Finally, Appendices B–D discuss paths for future development. In conclusion, readers of this paper will be able to understand the structure of the design principles of ultra-high-speed communication, quantum stream ciphers, and quantum sensors.

	Shannon-Massey type	Wire tap channel type	Quantum stream cipher
Countermeasure	Randomization of plaintext	Coding of plaintext	Randomization of ciphertext of Eve
Technology	Homophonic substitution	Wire tap coding, COSET coding	Quantum noise diffusion
Effect	Increase source entropy	Disable Eve's decoding ability	Reduce Eve's accessible information and capacity

Figure 12. Comparison of the characteristics of the conventional information-theoretic cipher and the quantum stream cipher. Quantum stream ciphers evolved from forms of Shannon-Massey ciphers.

Funding: This research received no external funding.

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

Appendix A. Towards Social Implementation of Quantum Technology

As telecommunications and microwave communications have evolved into optical communications, a major shift is occurring in communications theory, which governs their design. In general, there are three fundamental aspects of communications: the amount of information transmitted (bits/s), error characteristics (reliability), and communication distance. Currently, the delay characteristic (latency) is also essential. So far, it was considered acceptable to sacrifice the delay characteristic in order to improve these three fundamental characteristics. In particular, for error-correcting codes, a longer code length was not considered a major issue. On the other hand, there has been a noticeable trend of moving away from technical theory towards abstract theory.

To prevent this trend from being carried over into quantum communication theory, Kennedy–Haus proposed training researchers with a careful focus on balancing the roles of mathematics, physics, and electronics (Figure A1). Currently, quantum Shannon information theory has been developed as a result of this research, and communication technologies that apply quantum effects based on this theory are being implemented in society.

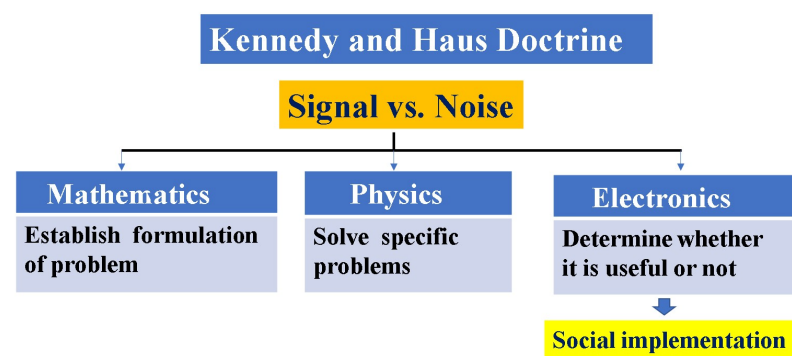


Figure A1. Fundamental concepts for advancing research into utilizing quantum effects for the advancement of communications in the real world.

Appendix B. Towards Further Development of Theory

We will introduce the challenges and notable contributions to further development of quantum communication theory in three fields.

(1) Mathematics

Entropy, POVM, and its related formulae are simply measures, and their operational meaning is, in general, guaranteed separately by various theorems. Any arbitrary interpretation of the above measures in physics and mathematics is meaningless. A typical example is the Shannon entropy. It first acquires meaning through the source and channel coding theorem.

In the following, we present contributions to further developments regarding the operational meaning of measures introduced in quantum theory:

· Holevo-Umegaki

The von Neumann entropy is given operational meaning as the maximum value of Shannon capacity through the HSW theorem. On the other hand, the Umegaki relative entropy [73] has operational meaning in the field of quantum Shannon theory as a derivative of Holevo theory.

The need for a mathematical generalization of the quantum measurement process was emphasized by Umegaki and others. Then P. Benioff, C.W. Helstrom, and H.P. Yuen emphasized the operational meaning of the POVM, which was proposed as a mathematical generalization. Finally the formulation of the POVM for quantum communication theory was systematized by Holevo, following the concept of decision operator interpretation by Helstrom. Their operational meaning forms the basis of quantum communication theory.

· Davies-Ozawa

E. Davies has published a book that provides an overview of the mathematical background of the quantum measurement process [74]. Then he defined the concept of instrument as follows.

Definition A1. Let Ω be a set with a σ -field $\mathcal{F}$. Then one can define the POVM on Ω to be a map $\mathcal{E}: \mathcal{F} \rightarrow \mathcal{L}^+(V)$.

If the POVM satisfies the condition

$$\text{Tr}[\mathcal{E}(\Omega)\rho] = \text{Tr}[\rho], \quad \forall \rho \in V \quad (\text{A1})$$

then it is called an “instrument”.

M. Ozawa [75–77] took the debate between Yuen and Caves in the theory of gravitational wave detection as an opportunity to develop Davies’s instrument theory to a high level, including “Ozawa’s representation theorem”. It is expected that his results will help to clarify operational meaning through the theory of gravitational wave detection in the future.

· Belavkin

V.P. Belavkin formulated the mathematical foundation for extending classical linear and nonlinear filtering theory to quantum systems [78,79]. For example, he has developed quantum versions of Kalman–Bucy-type linear filters and Bellman equations for control systems with feedback. The mathematical basis for this is “quantum stochastic calculus in Fock space and stochastic equation”.

$$\begin{aligned} |d\psi_t\rangle &= \frac{1}{i\hbar} H(u_t) |\psi_t\rangle dt \\ &- \frac{1}{2} \sum_{\alpha} [L_{\alpha}^{\dagger} L_{\alpha} - 2\lambda_{\alpha}(t) L_{\alpha} + \lambda_{\alpha}^2(t)] |\psi_t\rangle dt \\ &+ \sum_{\alpha} [L_{\alpha} - \lambda_{\alpha}(t)] |\psi_t\rangle dW_{\alpha}(t) \end{aligned} \quad (\text{A2})$$

The main results may provide a theory of optimal estimation of quantum measurements, which is essential to future development of quantum control theory.

In sum, new mathematical research with operational meaning will provide the impetus for further development of quantum Shannon theory.

(2) Physics

Glauber's coherent-state theory opened up the field of quantum optics. Yuen pioneered the theory of two-photon coherent states to control the uncertainty relation between quadrature amplitudes [80]. This opened up new technological possibilities for the controllability of quantum states of light. Currently, these are being developed in various fields as squeezed states.

Meanwhile, the theory of entanglement of quantum states mentioned above was proposed by Sanders [81]. Its operational meaning was explored through theories by van Enk [69] and others, and applications were opened up. Furthermore, P. Grangier [82] and H. Jeong [83,84] made significant contributions to the analysis of physical properties and experimental development.

(3) Detection and estimation theory

In this section, we introduce several extensions of quantum detection and estimation for communication theory.

· Eldar

In the field of electrical signal processing, squared error is sometimes used to evaluate the error. Eldar introduced squared error evaluation for finite alphabets as a system evaluation for quantum signal processing [85]. The evaluation measure is given as follows:

$$\Delta = \sum_{i=1}^M \langle e_i | e_i \rangle, \quad |e_i\rangle = |\psi_i\rangle - |\mu_i\rangle \quad (\text{A3})$$

Eldar has formulated an optimum theory by considering quantum states to be signal vectors. Thus, she has assumed pure-state ensembles $\{|\psi_i\rangle\}$ and sought a POVM $\Pi_i = |\mu_i\rangle\langle\mu_i|$ consisting of rank-one positive operators with measurement vectors that minimize the sum of the squared norms of the error vectors. However, the challenge is to clarify the meaning of the POVM, which is the solution.

· Chefles and Barnnet

Chefles and Barnnet formulated an optimum theory of "Unambiguous decision" [86]. This combines error-free discrimination with a certain fraction of inconclusive results. They showed that there is a necessary and sufficient condition for the existence of unambiguous measurements for distinguishing between M quantum states.

· Pirandola

Pirandola proposed a new detection concept in quantum detection theory that is called "quantum reading" [70]. Quantum reading is defined as the use of input quantum resources (such as entanglement) and output quantum measurements to enhance the retrieval of classical information stored in the cells of a memory.

His idea developed into quantum channel discrimination (QCD) [87]. QCD is a very general problem where an ensemble of quantum channels is prepared in a black box and they need to be discriminated.

Several generalizations of unambiguous decision and channel discrimination have been developed by K. Nakahira [88–90].

· Personick

Personick is a pioneer in research on the specific structure of modulation and demodulation based on quantum estimation [26]. Fundamentally, estimation theory deals

with analog signals. Therefore, the evaluation function is the minimum mean square error, as follows:

$$\min_{\mathbf{X}} \mathcal{C}(\mathbf{X}) = \int \xi(s) [\text{Tr} \rho(s)(\mathbf{X}(ds) - sI)]^2 ds \quad (\text{A4})$$

He found the optimum condition for the above problem and his work led to filter theory. The review was given by Helstrom and Kennedy [91].

R.O. Harger and his group attempted to develop a quantum linear filter using Perseus's theory [92]. These operational meanings are clear and provide a basis for further development of estimation theory.

Appendix C. Quantum Shannon Information Transmission Theory

Since the publication of Shannon theory, research on the construction of fundamental theories and their applications has expanded into an extremely broad field. The true essence of this theory lies in coding theory. However, research in the second half of the 20th century focused on abstract theories and mathematical research into unrealizable asymptotics, to which Shannon himself was not favorable. Coding techniques are used in actual communication technology, but delay (latency) issues as their greatest drawback have become a serious problem in the 21st century.

Rather than theories that achieve communication capacity, there is growing demand for theories that can keep code lengths below a certain level when the rate is fixed below the cut-off rate.

Meanwhile, this type of research into quantum systems remains limited to asymptotic discussions that stick to old styles. This is inherently useless. Twenty-first century communications are moving towards the realization of ultra-high-speed, low-latency communication systems. Research by the quantum information community must meet these demands.

Considering such a situation, the development of reliability function theory is appropriate. Dalai's work [93] deserves great recognition. He provided the fundamentals of random coding, sphere-packing, and expurgation. Kato [94] analyzed specific examples of coherent-state signals in real-world ultra-high-speed communications and clearly demonstrated their properties based on Dalai's theory. Code constructions that take into account the properties of specific quantum states have already been considered [95].

We recommend the following books to help you learn these basic theories in interdisciplinary fields [96–103].

1. R.L. Stratonovich, *Theory of information and its value*.
2. R.G. Gallager, *Principle of digital communication*.
3. G.C. Papen and R. Blahut, *Lightwave communications*.
4. J. Perina, *Quantum statistics of linear and nonlinear optical phenomena*.
5. I.B. Djordjevic, *Quantum communication, quantum networks and quantum sensing*.
6. G. Cariolaro, *Quantum communications*.
7. L. Cohen, H.V. Poor, and M.O. Scully, *Classical, semiclassical and quantum noise*.
8. M. Ohya and D. Petz, *Quantum entropy and its use*.

Appendix D. Towards the Development of Quantum Ciphers for Global Optical Networks

Generally, the characteristics of cryptography are evaluated based on many factors, including security, scalability, implementation characteristics, latency characteristics, cost, and compatibility with real-world systems. Unless a balance among these factors is maintained, social implementation is impossible.

When evaluating the characteristics of physical cryptography, communication characteristics are particularly important. Therefore, using single photons or quantum entanglement is impractical.

Future physical cryptography that utilizes quantum properties must prioritize protecting the data used in today's ultra-high-speed optical communications. To achieve this, the quantum stream cipher, which can encrypt data while maintaining ultra-high speeds, would be the best solution. This is because it follows the trend of modern cryptography represented by Massey and others [104–107] and provides new security features.

References

1. Helstrom, C.W. *Quantum Detection and Estimation Theory*; Academic Press: Cambridge, MA, USA, 1976.
2. Holevo, A.S. Statistical decision theory for quantum systems. *J. Multivar. Anal.* **1973**, *3*, 337. [\[CrossRef\]](#)
3. 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. [\[CrossRef\]](#)
4. Hausladen, P.; Jozsa, R.; Schumacher, B.; Westmoreland, M.; Wootters, W. Classical information capacity of a quantum channel. *Phys. Rev. A* **1996**, *54*, 1869. [\[CrossRef\]](#) [\[PubMed\]](#)
5. Holevo, A.S. The capacity of the quantum channel with general signal state. *IEEE Trans. Inf. Theory* **1998**, *1*, 269. [\[CrossRef\]](#)
6. Schumacher, B.; Westmoreland, M. Sending classical information via noisy quantum channels. *Physical. Rev. A* **1997**, *56*, 131. [\[CrossRef\]](#)
7. Gallager, R.G. *Information Theory and Reliable Communication*; Wileys: Hoboken, NJ, USA, 1968.
8. Burnashev, M.V.; Holevo, A.S. On reliability function of quantum communication channel. *Probl. Peredachi Inform.* **1988**, *34*, 1–13.
9. Holevo, A.S. Reliability function of general classical-quantum channel. *IEEE Trans. Inf. Theory* **2000**, *46*, 2256. [\[CrossRef\]](#)
10. Helstrom, C.W.; Charbit, M.; Bendjaballah, C. Cut off rate performance for phase shift keying modulated coherent state. *Opt. Commun.* **1987**, *64*, 253. [\[CrossRef\]](#)
11. Bendjaballah, C.; Charbit, M. Quantum communication with coherent states. *IEEE Trans. Inf. Theory* **1989**, *35*, 1114. [\[CrossRef\]](#)
12. Charbit, M.; Bendjaballah, C.; Helstrom, C.W. Cut off rate for the M-ary PSK modulation channel with optimal quantum detection. *IEEE Trans. Inf. Theory* **1989**, *35*, 1131. [\[CrossRef\]](#)
13. Ban, M.; Kurokawa, K.; Hirota, O. Cut-off rate for quantum communication channels with entangled measurement. *Quantum Semiclass Opt.* **1998**, *10*, L7–L12. [\[CrossRef\]](#)
14. Ban, M.; Kurokawa, K.; Hirota, O. Cut-off rate performance of quantum communication channels with symmetric signal states. *J. Opt. B Quantum Semiclass Opt.* **1999**, *1*, 206–218. [\[CrossRef\]](#)
15. Holevo, A.S. *Quantum Systems, Channels, Information*, 2nd ed.; De Gruyter: Berlin, Germany, 2019.
16. Helstrom, C.W. The conversion of a pure state into a statistical mixture by the linear quantum channel. *Opt. Commun.* **1981**, *37*, 175–177. [\[CrossRef\]](#)
17. Holevo, A.S. *Probabilistic and Statistical Aspects of Quantum Theory*; North-Holland Publishing: Amsterdam, The Netherlands, 1982.
18. Wald, A. *Statistical Decision Function*; Wileys: Hoboken, NJ, USA, 1950.
19. Fuchs, C.A. Notes on a Paulian Idea: Foundational, Historical, Anecdotal and Forward-Looking Thoughts on the Quantum. *arXiv* **2001**, arXiv:quant-ph/0105039. [\[CrossRef\]](#)
20. Hirota, O. Non-causality and quantum communication theory. *Tamagawa Univ. Res. Rev.* **1995**, *1*, 1.
21. Hirota, O.; Ikehara, S. Minimax strategy in the quantum detection theory and its application to optical communications. *Trans. IEICE Jpn.* **1982**, *65E*, 627.
22. Belavkin, V.P. Optimal multiple quantum statistical hypothesis testing. *Stochastics* **1975**, *1*, 315–345. [\[CrossRef\]](#)
23. 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. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Ban, M.; Kurokawa, K.; Momose, R.; Hirota, O. Quantum measurements for discrimination among symmetric quantum states and parameter estimation. *Int. J. Theor. Phys.* **1997**, *36*, 1269. [\[CrossRef\]](#)
25. Paris, M.G.A. Quantum estimation for quantum technology. *Int. J. Quantum Inf.* **2009**, *7*, 125. [\[CrossRef\]](#)
26. Personick, S.D. Application of quantum estimation theory to analog communication over quantum channels. *IEEE Trans. Inf. Theory* **1971**, *17*, 234. [\[CrossRef\]](#)
27. Yuen, H.P.; Lax, M. Multiple-parameter quantum estimation and measurement of non-self adjoint observables. *IEEE Trans. Inf. Theory* **1973**, *19*, 740–750. [\[CrossRef\]](#)
28. Hirota, O. Generalized quantum measurement process and its application to quantum communication theory. *Trans. IECE Jpn.* **1977**, *60A*, 701–708.
29. Yuen, H.P. States that give the maximum signal to quantum noise ratio for a fixed energy. *Phys. Lett.* **1976**, *56A*, 105. [\[CrossRef\]](#)

30. Davies, E.B. Information and quantum measurement. *IEEE Trans. Inf. Theory* **1978**, *24*, 596. [\[CrossRef\]](#)
31. Sasaki, M.; Barnett, S.M.; Jozsa, R.; Osaki, M.; Hirota, O. Accessible information and optimum strategies for real symmetrical quantum sources. *Phys. Rev. A* **1999**, *59*, 3325. [\[CrossRef\]](#)
32. Osaki, M.; Hirota, O.; Ban, M. The maximum mutual information without coding for binary quantum states. *J. Mod. Opt.* **1998**, *45*, 269. [\[CrossRef\]](#)
33. Sasaki, M.; Kato, K.; Izutsu, M.; Hirota, O. Quantum channels showing superadditivity in classical capacity. *Phys. Rev. A* **1998**, *58*, 146. [\[CrossRef\]](#)
34. Kato, K.; Osaki, M.; Hirota, O. Derivation of classical capacity of quantum channel for discrete information source. *Phys. Lett. A* **1999**, *251*, 157. [\[CrossRef\]](#)
35. Holevo, A.S.; Sohma, M.; Hirota, O. Capacity of quantum Gaussian channels. *Phys. Rev. A* **1999**, *59*, 1820. [\[CrossRef\]](#)
36. Sohma, M.; Hirota, O. Information capacity formula of quantum optical channels. *Recent Res. Dev. Opt.* **2001**, *1*, 145.
37. Giovanenetti, V.; Guha, S.; Lloyd, S.; Maccone, L.; Shapiro, J.H.; Yuen, H.P. Classical capacity of lossy Bosonic channels: Exact solution quantum Gaussian channels. *Phys. Rev. Lett.* **2004**, *92*, 027902. [\[CrossRef\]](#)
38. Buck, J.R.; van Enk, S.J.; Fuchs, C.A. Experimental proposal for achieving superadditive communication capacities with a binary quantum alphabet. *Phys. Rev. A* **2000**, *61*, 032309. [\[CrossRef\]](#)
39. Lloyd, S.; Giobannetti, V.; Maccone, L. Sequential projective measurements for channel decoding. *Phys. Rev. Lett.* **2011**, *106*, 250501. [\[CrossRef\]](#)
40. Guha, S. Structured optical receivers to attain super-additive capacity and the Holevo limit. *Phys. Rev. Lett.* **2011**, *106*, 240502. [\[CrossRef\]](#) [\[PubMed\]](#)
41. Chung, H.W.; Guha, S.; Zheng, L. Capacity of optical communications over a lossy Bosonic channel with a receiver employing the most general coherent electro-optic feedback control. *Phys. Rev. A* **2017**, *96*, 012320. [\[CrossRef\]](#)
42. Hirota, O. A foundation of quantum channels with super additiveness for Shannon information. *Appl. Algebra Eng. Commun. Comput.* **2000**, *10*, 401–423. [\[CrossRef\]](#)
43. Chung, H.W.; Guha, S.; Zheng, L. Super additivity of Quantum Channel Coding Rate with Finite Block length Quantum Measurements. *IEEE Trans. Inf. Theory* **2016**, *62*, 5938. [\[CrossRef\]](#)
44. Sohma, M.; Hirota, O. Binary discretization for quantum continuous channels. *Phys. Rev. A* **2000**, *62*, 52312. [\[CrossRef\]](#)
45. Kurokawa, K.; Hirota, O. Property of quantum reliability function and its applications to several quantum signals. *Electron. Commun. Jpn.* **2001**, *84 Pt 3*, 31. [\[CrossRef\]](#)
46. Holevo, A.S.; Sohma, M.; Hirota, O. Error exponents for quantum channels with constrained inputs. *Rep. Math. Phys.* **2000**, *46*, 343. [\[CrossRef\]](#)
47. Yuen, H.P. KCQ: A new approach to quantum cryptography I. General principles and key generation. *arXiv* **2003**, arXiv:quant-ph/0311061. [\[CrossRef\]](#)
48. Hirota, O. Secure quantum communication protocol based on quantum communication theory. In Proceedings of the General Theory of Information Transfer and Combination, Bielefeld, Germany, 15 September 2004.
49. Sohma, M.; Hirota, O. Quantum stream cipher based on Holevo-Yuen theory; part I. *Entropy* **2022**, *24*, 667. [\[CrossRef\]](#) [\[PubMed\]](#)
50. Hirota, O.; Sohma, M. Quantum stream cipher based on Holevo-Yuen theory: Part II. *Entropy* **2024**, *26*, 983. [\[CrossRef\]](#)
51. Hirota, O. Design of quantum stream cipher—Part I; Lifting the Shannon impossibility theorem. *arXiv* **2025**, arXiv:2025.14872v1. [\[CrossRef\]](#)
52. Nair, R.; Yuen, H.P.; Corndolf, E.; Kumar, P. Quantum noise randomized ciphers. *Phys. Rev. A* **2006**, *74*, 052309. [\[CrossRef\]](#)
53. Hirota, O.; Kurosawa, K. Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol. *Quantum Inf. Process.* **2007**, *6*, 81–91. [\[CrossRef\]](#)
54. Sohma, M.; Hirota, O. Coherent Pulse Position Modulation Quantum Cipher Supported by Secret Key. *Bull. Quantum ICT Res. Inst. Tamagawa Univ.* **2011**, *1*, 15–19. Available online: <https://www.tamagawa.jp/research/quantum/bulletin/2011.html> (accessed on 1 July 2020).
55. Sohma, M.; Hirota, O. Masking property of quantum random cipher with phase mask encryption. *Quantum Inf. Process.* **2014**, *13*, 2221–2240. [\[CrossRef\]](#)
56. Hirota, O. Quantum stream cipher and quantum block cipher—The Era of 100 Gbit/sec real-time encryption-. *arXiv* **2025**, arXiv:2504.17240.
57. Borbosa, G.A.; Corndolf, E.; Kumar, P.; Yuen, H.P. Secure communication using coherent state. In *Proceedings of QCMC-2002*; Shapiro, J.H., Hirota, O., Eds.; Rinton Press: Princeton, NJ, USA, 2002.
58. Borbosa, G.A.; Corndorf, E.; Kumar, P.; Yuen, H.P. Secure communication using mesoscopic coherent states. *Phys. Rev. Lett.* **2003**, *90*, 227901. [\[CrossRef\]](#)
59. Kanter, G.S.; Reilly, D.; Smith, N. Practical physical layer encryption: The marriage of optical noise with traditional cryptography. *IEEE Commun. Magazijn* **2009**, *47*, 74–81. [\[CrossRef\]](#)

60. Futami, F.; Tanizawa, K.; Kato, K. Field Trial of Y-00 Quantum Stream Cipher System with Functions of Authentication and Key Distribution by Post-Quantum Cryptography. In Proceedings of the 2022 IEICE Japan Society Conference, Tokyo, Japan, 29 November–1 December 2022.
61. Kato, K.; Futami, F.; Tanizawa, K. Quantum-enhanced secure-link architecture with quantum stream cipher Y-00 and post-quantum cryptography: Basic structure and experiment. In Proceedings of the Proceedings Volume 12692, Quantum Communications and Quantum Imaging XXI, San Diego, CA, USA, 20–22 August 2023.
62. Futami, F.; Tanizawa, K.; Kato, K. Transmission of Y-00 Quantum Noise Stream Cipher with Quantum Deliberate Signal Randomization over Field-Installed Fiber. *Bull. Quantum ICT Res. Inst. Tamagawa Univ.* **2023**, *13*, 23–25. Available online: <https://www.tamagawa.jp/research/quantum/bulletin/2023.html> (accessed on 10 March 2024).
63. 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](#)]
64. 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](#)]
65. Luo, H.; Zhang, Z.; Dai, L.; Zhong, Y.Q.; Deng, L.; Liu, D.; Dai, X.; Gao, X.; Cheng, M. Device-compatible ultra-high-order quantum noise stream cipher based on delta-sigma modulator and optical chaos. *Nat. Commun. Eng.* **2024**, *3*, 27. [[CrossRef](#)]
66. Li, Z.Y.; Zhang, Y.K.; Pang, H.Y.; Luo, Q.S.; Zhang, X.; Tao, Z.Y.; Fan, Y.X. Quantum noise stream cipher based on optical digital to analog conversion. *Opt. Quantum Electron.* **2025**, *57*, 95. [[CrossRef](#)]
67. Tanizawa, K.; Futami, F. Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system. *Opt. Express* **2021**, *29*, 10451–10464. [[CrossRef](#)]
68. Hirota, O.; Sasaki, M. Entangled state based on nonorthogonal state. In *Quantum Communication, Computing, and Measurement 3*; Tombesi, P., Hirota, O., Eds.; Springer: Boston, MA, USA, 2001; pp. 359–366.
69. van Enk, S.J.; Hirota, O. Entangled coherent states: Teleportation and decoherence. *Phys. Rev. A* **2001**, *64*, 022313. [[CrossRef](#)]
70. Pirandola, S. Quantum reading of a classical digital memory. *Phys. Rev. Lett.* **2011**, *106*, 090504. [[CrossRef](#)]
71. Hirota, O.; Suematsu, Y. Noise properties of injection lasers due to reflected waves. *IEEE J. Quantum Electron.* **1979**, *15*, 142. [[CrossRef](#)]
72. Hirota, O. Error free quantum reading by quasi Bell state of entangled coherent states. *Quantum Meas. Quantum Metrol* **2017**, *4*, 70.
73. Umegaki, H. Conditional expectation in an operator algebra, VI (entropy and information). *Kodai Math. Sem. Rep.* **1962**, *14*, 59. [[CrossRef](#)]
74. Davies, E.B. *Quantum Theory of Open Systems*; Academic Press: Cambridge, MA, USA, 1976.
75. Ozawa, M. Quantum measuring processes of continuous observables. *J. Math. Phys.* **1984**, *25*, 79. [[CrossRef](#)]
76. Ozawa, M. Measurement breaking the standard quantum limit for free mass position. *Phys. Rev. Lett.* **1988**, *60*, 385. [[CrossRef](#)] [[PubMed](#)]
77. Ozawa, M. Quantum measurement theory for systems with finite dimensional state spaces. *arXiv* **2021**, arXiv:2110.03219. [[CrossRef](#)]
78. Belavkin, V.P. *Quantum Stochastics and Information*; World Scientific: Singapore, 2006.
79. Belavkin, V.P.; Hirota, O.; Hudson, R.L. *Quantum Communications and Measurement*; Plenum Press (Springer): New York, NY, USA, 1995.
80. Yuen, H.P. Two-photon coherent state of the radiation fields. *Phys. Rev. A* **1976**, *13*, 2226–2243. [[CrossRef](#)]
81. Sanders, B.C. Entangled coherent state. *Phys. Rev. A* **1992**, *46*, 2966. [[CrossRef](#)]
82. Ourjoumtsev, A.; Ferreyrol, F.; Tualle-Brouiri, R.; Grangier, P. Preparation of non-local superposition of quasi-classical light state. *Nat. Phys.* **2009**, *5*, 189. [[CrossRef](#)]
83. Jeong, H.; Kim, M.S.; Lee, J. Quantum information processing for a coherent superposition state via a mixed entangled coherent channel. *Phys. Rev. A* **2001**, *64*, 052308.
84. Park, K.; Jeong, H. Entangled coherent states versus entangled photon pairs for practical quantum-information processing. *Phys. Rev. A* **2010**, *86*, 062325. [[CrossRef](#)]
85. Eldar, Y.C.; Forney, G.D., Jr. On quantum detection and the square-root measurement. *IEEE Trans. Inf. Theory* **2001**, *47*, 858–872. [[CrossRef](#)]
86. Chefles, A.; Barnett, S.M. Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A* **1998**, *250*, 223–229. [[CrossRef](#)]
87. Pirandola, S.; Lupo, C.; Giovannetti, V.; Mancini, S.; Braunstein, S.L. Quantum reading capacity. *New J. Phys.* **2011**, *13*, 113012. [[CrossRef](#)]
88. Nakahira, K.; Kato, K.; Usuda, T. Minimax strategy in quantum signal detection with inconclusive results. *Phys. Rev. A* **2013**, *88*, 032314. [[CrossRef](#)]

89. Nakahira, K.; Kato, K.; Usuda, T. Generalized quantum state discrimination problems. *Phys. Rev. A* **2015**, *91*, 052304. [[CrossRef](#)]
90. Nakahira, K.; Kato, K. Generalized quantum process discrimination problems. *Phys. Rev. A* **2021**, *103*, 062606. [[CrossRef](#)]
91. Helstrom, C.W.; Kennedy, R.S. Noncommuting observables in quantum detection and estimation theory. *IEEE Trans. Inf. Theory* **1974**, *20*, 16. [[CrossRef](#)]
92. Baras, J.S.; Hargar, R.O.; Park, Y.H. Quantum mechanical linear filtering of random signal sequence. *IEEE Trans. Inf. Theory* **1976**, *22*, 59. [[CrossRef](#)]
93. Dalai, M. Lower bounds on the probability of error for classical and classical-quantum channels. *IEEE Trans. Inf. Theory* **2013**, *59*, 8027. [[CrossRef](#)]
94. Kato, K. A note on the reliability function for M-ary PSK coherent state signal. *Bull. Quantum ICT Res. Inst. Tamagawa Univ.* **2018**, *1*, 21.
95. 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](#)]
96. Stratonovich, R.L. *Theory of Information and Its Value*; Springer: Berlin/Heidelberg, Germany, 2020.
97. Gallager, R.G. *Principle of Digital Communication*; Cambridge University Press: Cambridge, UK, 2008.
98. Papen, G.C.; Blahut, R.E. *Lightwave Communications*; Cambridge University Press: Cambridge, UK, 2019.
99. Perina, J. *Quantum Statistics of Linear and Nonlinear Optical Phenomena*; D.Reidel Publishing Company: Dordrecht, The Netherlands, 1984.
100. Djordjevic, I.B. *Quantum Communication, Quantum Networks and Quantum Sensing*; Academic Press: Cambridge, MA, USA, 2022.
101. Cariolaro, G. *Quantum Communications*; Springer: Berlin/Heidelberg, Germany, 2015.
102. Cohen, L.; Poor, H.V.; Scully, M.O. (Eds.) *Classical, Semiclassical and Quantum Noise*; Springer: Berlin/Heidelberg, Germany, 2012.
103. Ohya, M.; Petz, D. *Quantum Entropy and Its Use*; Springer: Berlin/Heidelberg, Germany, 1993.
104. Massey, J. *Contemporary Cryptology—An Introduction*; Simmons, G.J., Ed.; IEEE Press: Piscataway, NJ, USA, 1992.
105. Blahut, R.E. *Cryptography and Secure Communication*; Cambridge University Press: Cambridge, UK, 2014.
106. Welsh, D. *Codes and Cryptography*; Oxford Science Publications: Oxford, UK, 1988.
107. National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Standardization. 2020. Available online: <https://csrc.nist.gov/projects/post-quantum-cryptography> (accessed on 15 April 2021).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.