Defeating Eavesdropping with Quantum Illumination

by

Wenbang Xu

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Electrical Engineer

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2012

Author .....
Department of Electrical Engineering and Computer Science
January 17, 2012

Certified by .....
Jeffrey H. Shapiro
Julius A. Stratton Professor of Electrical Engineering
Thesis Supervisor

Accepted by .....
Leslie A. Kolodziejski
Chair, Department Committee on Graduate Theses

Defeating Eavesdropping with Quantum Illumination

by

Wenbang Xu

Submitted to the Department of Electrical Engineering and Computer Science
on January 15, 2012, in partial fulfillment of the
requirements for the degree of
Electrical Engineer

Abstract

Quantum illumination is a paradigm for using entanglement to gain a performance advantage—in comparison with classical-state systems of the same optical power—over lossy, noisy channels that destroy entanglement. Previous work has shown how it can be used to defeat passive eavesdropping on a two-way Alice-to-Bob-to-Alice communication protocol, in which the eavesdropper, Eve, merely listens to Alice and Bob's transmissions. This thesis extends that work in several ways. First, it derives a lower bound on information advantage that Alice enjoys over Eve in the passive eavesdropping scenario. Next, it explores the performance of alternative practical receivers for Alice, as well as various high-order modulation formats for the passive eavesdropping case. Finally, this thesis extends previous analysis to consider how Alice and Bob can minimize their vulnerability to Eve's doing active eavesdropping, i.e., when she injects her own light into the channel.

Thesis Supervisor: Jeffrey H. Shapiro
Title: Julius A. Stratton Professor of Electrical Engineering

Acknowledgments

I truly appreciate my research advisor, Prof. Jeffrey H. Shapiro, for his patience during my research in the quantum communication group. Professor Shapiro always promotes students to explore new and interesting topics. At the same time, he helps them in great detail due to his rigorous background and abundant experience in physics and information theory. His guidance will benefit me in my professional career forever.

I would like to thank Dr. Franco N.C. Wong for setting up my office, answering my questions, and teaching me about experiments. I would especially like to thank Tian Zhong and Dheera Venkatraman for answering some fundamental questions about quantum physics when I joined this group. Discussing the phase-lock experiment platform with Tian was an extremely interesting experience for me. I also thank Prof. Dennis Freeman for giving me the opportunity to teach 6.003, Signals and Systems. This teaching experience has taught me how to actively guide students.

I am grateful for having a great family. My family members—including my wife, Xiuping, Zhang, my brother, Jinbang, Xu and my sisters—are always behind me. Whatever I do, they always support me. When I decided to quit an excellent job and study at MIT, all of them encouraged me to chase my dream and enjoy my life at MIT.

This research was supported by an Office of Naval Research Basic Research Challenge Grant. I would like to thank them for that support.

Contents

List of Figures

Chapter 1

Introduction

Communication is the process by which information is transmitted from one location to another. It is an essential need and a fundamental practice of the world. For example, to discuss a business idea with your friend, you might talk to him face to face, which is a process of interpersonal communication. However, such interpersonal communications is not possible when a long distance separates the communicating parties. To solve the problem of long-distance communication, human beings have invented many communication systems to conquer distance. In ancient times, runners carried messages from one place to another. People lit giant fires on mountain summits or beacon towers, or rang bells to communicate impending attacks. Long-distance communication became much easier, however, with the advent of electromagnetic techniques, such as Morse's development of the telegraph early in the 19th century. Later that century, Maxwell's theory of electromagnetic waves and Hertz's experimental verification relieved the need for wires to carry telegraph signals, leading to Popov and Marconi's invention of the radio-telegraph technique in 1883. At roughly the same time, electromagnetic communication moved beyond the telegraph and into voice communication when Bell patented the telephone in 1876.

The preceding technological advances dramatically improved long-distance communications, but they did not address the fundamental limits on information transmission. Then, in 1948, Claude Shannon published his historic paper "A Mathematical Theory of Communication" [1], establishing the theoretical foundation for classical

communication systems. Since then, technology and theory have advanced together, allowing ubiquitous communications—in the forms of fiber-optic networks, satellite relays, and cellular telephony—to enable the information age in which we now live.

1.1 Classical Communication Theory

Consider a single-user classical communication system whose block diagram is shown in Fig.1-1. Its major blocks consist of the transmitter, whose purpose is to con-

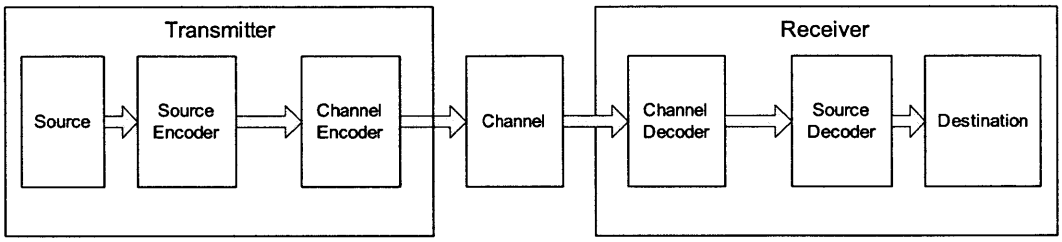

Figure 1-1: Schematic of basic communication system.

vert the information emerging from the source into a form suitable for long-distance transmission through the physical propagation medium contained within the channel, plus a receiver that is needed to retrieve the source information from the signal it collects from the channel's output. Physical limitations in the channel—finite bandwidth, noise, fading, etc.—constrain the capability of the system, and communication theory establishes the ultimate limit on this capability.

Following the source-channel separation theorem, the transmitter employs a source encoder to convert the source content into a minimum redundancy digital form. Encryption may also be applied at this stage, if security against eavesdropping on the channel is desired. The channel encoder then applies channel coding to the source encoder's bit stream to ensure reliable transmission over the channel. The receiver reverses the process used by the transmitter to reproduce the source's information in its original format.

Information theory establishes performance bounds for source coding and channel coding. Consider a discrete memoryless source whose content is a stream of indepen-

dent, identically distributed symbols drawn from an alphabet $A = \{a_m : 1 \leq m \leq M\}$ with probability distribution $\{P_A(a_m) : 1 \leq m \leq M\}$, then the lower bound on the average number of bits needed to represent one symbol is the Shannon entropy of that alphabet

$$H(A) \equiv -\sum_{m=1}^{M} P_A(a_m) \log(P_A(a_m)), \tag{1.1}$$

and the upper bound on the minimum average number of bits needed to represent one symbol is $H(A) + 1$ [1]. This is the simplest form of Shannon's Source Coding Theorem. We can regard the entropy as the expected information content of the alphabet, and coding to the source entropy limit removes the unnecessary redundancy in source's output. Shannon's Noisy Channel Coding Theorem, on the other hand, gives the upper bound on the information that a channel can reliably (without error) transmit per use. For a discrete memoryless channel, this bound is the channel capacity, given by the maximum mutual information [1] between the channel's input ensemble X and its output ensemble Y, namely

$$C = \sup_{P_X} I(X;Y), \tag{1.2}$$

where

$$I(X;Y) \equiv \sum_{y \in Y} \sum_{x \in X} P_{X,Y}(x,y) \log\left(\frac{P_{X,Y}(x,y)}{P_X(x) P_Y(y)}\right). \tag{1.3}$$

In Equation 1.3, $P_X(x)$ is the probability distribution over the channel's input ensemble and $P_{Y|X}(y|x)$ is the channel's transition-probability distribution. The joint distribution of the input and output is given by $P_{X,Y}(x,y) = P_{Y|X}(y|x) P_X(x)$ and the probability distribution for the channel's output is then found from $P_Y(y) = \sum_{x \in X} P_{X,Y}(x,y)$. In essence, the channel encoder adds some controlled redundancy to counteract adverse effects—noise, etc.—in the channel.

Shannon's theorems provide bounds for the source coding rate and the channel coding rate, but they do not provide practical implementations for approaching these limits. Minimum error-probability detection provides a method to minimize the error probability the receiver achieves given knowledge of the transmitter's encoding

and the channel's transition-probability distribution. Because this thesis will focus on binary phase-shift keying (BPSK), we will limit the present discussion to binary alphabets. Suppose the information symbol before channel transmission is a random variable H, and the information symbol after channel transmission is a random variable Y. The channel is modeled by the conditional probabilities

$$\left\{P_{Y|H}\left(y|H_m\right) : m = 0, 1\right\}, \tag{1.4}$$

and the source by the prior probabilities

$$\begin{aligned} P_H\left(H_0\right) &= p_0 \\ P_H\left(H_1\right) &= p_1. \end{aligned} \tag{1.5}$$

We then find, by means of Bayes' rule, that the posterior distribution for H, given observation $Y = y$, is

$$\begin{aligned} P_{H|Y}\left(H_0|y\right) &= \frac{P_{Y|H}\left(y|H_0\right)p_0}{P_{Y|H}\left(y|H_0\right)p_0 + P_{Y|H}\left(y|H_1\right)p_1} \\ P_{H|Y}\left(H_1|y\right) &= \frac{P_{Y|H}\left(y|H_1\right)p_1}{P_{Y|H}\left(y|H_0\right)p_0 + P_{Y|H}\left(y|H_1\right)p_1}. \end{aligned} \tag{1.6}$$

Error probability is minimized, given $Y = y$, by choosing the message with the higher posterior probability to be the one that is decoded. This rule can be implemented as the likelihood-ratio test

$$L\left(y\right) \equiv \frac{P_{Y|H}\left(y|H_1\right)}{P_{Y|H}\left(y|H_0\right)} \underset{\hat{H}=H_0}{\overset{\hat{H}=H_1}{\gtrless}} \frac{p_0}{p_1}, \tag{1.7}$$

where $\hat{H}$ is the receiver's output.

Error probability is not the only important performance metric for communication systems these days. Security (privacy) has become especially important, because of Internet commerce, military and government networks, and personal communications. Classical cryptography offers two solutions to this problem: private-key and public-key cryptography. The former requires sender and receiver to share a secret

key in advance of engaging in communication. Thus, its difficulty typically lies in distributing and refreshing keys—in a secure manner—between distant users. Public-key cryptography, specifically the RSA system, is the basis for Internet commerce. Its security relies on the presumed difficulty—in a computational complexity sense—of factoring the product of two large prime numbers. However, no proof that this problem is computationally hard exists, and, moreover, it is known that a large quantum computer can attack RSA cryptography.

Shannon addressed the information theory of secure communication in another famous paper "Communication Theory of Secrecy Systems" [2]. A direct result of his work is the security of the One-Time Pad cryptosystem. In such a system, the source's message—expressed as a sequence of bits—called the plaintext is converted into a ciphertext by modulo-2 addition of a sequence of key bits that are independent, identically distributed and equally likely to be 0 or 1. Regardless of the plaintext, the ciphertext is also a sequence of independent, identically distributed bits that are equally likely to be 0 or 1, making them useless to an eavesdropper. However, the intended receiver can retrieve the plaintext from the ciphertext by simple modulo-2 addition of the same key to the ciphertext. The problems with one-time pad cryptography are: (1) reuse of the key renders the system insecure; (2) the key must be as long as the message being sent; and (3) means must be found for secure distribution of the one-time pad key between distant users.

1.2 Quantum Communication

The world, at bottom, is governed by the laws of quantum mechanics that characterize the behavior of atoms and molecules. Most communication systems operate at macroscopic levels for which classical physics suffices. However, high-sensitivity photodetection systems are limited by noise of quantum-mechanical origin, so determining the ultimate limits of optical communication requires constructing information theory in a quantum-mechanical setting. In the narrower context of secure communication, we noted in the preceding section that a large quantum computer will render RSA

cryptography insecure. It is interesting, therefore, to note that quantum mechanics also offers solutions to the problem of secure communication, one of which will be the subject of this thesis. Before introducing that approach, let us briefly describe how quantum mechanics can enable the secure distribution of a one-time pad.

Suppose Alice wishes to establish a one-time pad with Bob over an optical channel despite the presence of an eavesdropper (Eve), who can intercept Alice's transmission in whole or in part. The no-cloning theorem of quantum mechanics [3], which implies that Eve cannot make a perfect copy of the unknown polarization state of a single photon, provides the theoretical foundation for Bennett-Brassard 1984 (BB84) quantum key distribution [4]. In a simple, ideal description of BB84, Alice sends Bob a single photon that is equally likely to be in any of the four polarization qubits: vertical $|\updownarrow\rangle$, horizontal $|\leftrightarrow\rangle$, $+45°$ $|\nearrow\rangle$ and $-45°$ $|\searrow\rangle$. Here we are using Dirac ket notation for these single-photon polarization states, and qubit means quantum bit. $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ are a complete orthonormal basis for the polarization state space of Alice's photons, so too are $|\nearrow\rangle$ and $|\searrow\rangle$. The relationship between these four states is as follows

$$\begin{aligned} |\nearrow\rangle &= \frac{|\leftrightarrow\rangle + |\updownarrow\rangle}{\sqrt{2}} \\ |\searrow\rangle &= \frac{|\leftrightarrow\rangle - |\updownarrow\rangle}{\sqrt{2}} \\ |\leftrightarrow\rangle &= \frac{|\nearrow\rangle + |\searrow\rangle}{\sqrt{2}} \\ |\updownarrow\rangle &= \frac{|\nearrow\rangle - |\searrow\rangle}{\sqrt{2}}. \end{aligned} \tag{1.8}$$

Let us suppose that the Alice-to-Bob connection is, in the absence of Eve, non-depolarizing. Then, from the laws of quantum measurement, we can compute the conditional probabilities for Bob's observations assuming that he randomly chooses to measure the photon he receives in the $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ basis or the $\{|\nearrow\rangle, |\searrow\rangle\}$ basis.

In particular, when Alice and Bob use the same basis, transmission is perfect, i.e.,

$$\begin{aligned}
&\Pr\left(\text{Bob} = |\updownarrow\rangle \,|\text{Alice} = |\updownarrow\rangle\,, \text{Bob uses } \{|\updownarrow\rangle\,, |\leftrightarrow\rangle\} \text{ basis}\right) = 1 \\
&\Pr\left(\text{Bob} = |\leftrightarrow\rangle \,|\text{Alice} = |\leftrightarrow\rangle\,, \text{Bob uses } \{|\updownarrow\rangle\,, |\leftrightarrow\rangle\} \text{ basis}\right) = 1 \\
&\Pr\left(\text{Bob} = |\nearrow\rangle \,|\text{Alice} = |\nearrow\rangle\,, \text{Bob uses } \{|\nearrow\rangle\,, |\searrow\rangle\} \text{ basis}\right) = 1 \\
&\Pr\left(\text{Bob} = |\searrow\rangle \,|\text{Alice} = |\searrow\rangle\,, \text{Bob uses } \{|\nearrow\rangle\,, |\searrow\rangle\} \text{ basis}\right) = 1.
\end{aligned} \tag{1.9}$$

However, when Alice and Bob choose different bases, Bob's outcomes are equally likely, i.e.,

$$\Pr\left(\text{Bob} = |\updownarrow\rangle \,|\text{Alice} = |\nearrow\rangle\,, \text{Bob uses } \{|\updownarrow\rangle\,, |\leftrightarrow\rangle\} \text{ basis}\right) = \frac{1}{2}, \tag{1.10}$$

etc.

Because of the no-cloning theorem, and Alice and Bob's randomly choosing bases, it is impossible for Eve to perfectly intercept Alice's photon without disturbing the polarization state that Bob will see when he and Alice use the same basis. Thus, after Alice has sent a long sequence of photons to Bob, Bob uses an insecure classical channel to inform Alice of his basis choices, Alice then tells Bob via this same classical channel, for which photons she used the same basis. At this point, Alice and Bob use their classical channel to exchange checksums to determine the locations of and correct errors in the bit values ($|\updownarrow\rangle = 0$, $|\leftrightarrow\rangle = 1$ for the $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ basis, and $|\nearrow\rangle = 0$, $|\searrow\rangle = 1$ for the $\{|\nearrow\rangle, |\searrow\rangle\}$ basis.) when they used the same basis. Attributing all such errors to Eve's intrusion, they can either abort the the protocol—if that intrusion is too severe—or, if not, employ the technique of privacy amplification to reduce Eve's information about a final distilled key to an inconsequential level.

Quantum key distribution, based on the BB84 protocol and other techniques, is a vigorously pursued research area at this time. This thesis, however, will be concerned with an alternative quantum-based approach to secure information transmission, one that is based on another fundamental quantum property—entanglement—instead of the no-cloning theorem. The approach goes by the name quantum illumination, and its purpose is to transmit message information at high data rates, not just to

distribute a one-time pad key. The quantum illumination communication protocol is shown schematically in Fig.1-2. Alice transmits the signal beam from a continuous-wave spontaneous parametric downconversion (SPDC) source to Bob over a lossy channel with transmissivity $\kappa \ll 1$, while retaining the idler beam (without loss) for subsequent joint measurement with what she will receive from Bob. Each T-sec-long transmission from Alice comprises $M = WT \gg 1$ signal-idler mode pairs with average photon number $N_S \ll 1$ per mode, where W is the source's phase-matching bandwidth. Bob, for his part, applies BPSK modulation (bit value k equally likely to be zero or one) to each T-sec-long interval of the light he receives from Alice. Then he amplifies that modulated light—with a phase-insensitive amplifier of gain G_B and amplified spontaneous emission noise N_B photons per mode—and sends the resulting beam back to Alice over the same transmissivity-κ channel. Alice then makes a joint return-beam/idler-beam measurement to obtain Bob's bit sequence. She does this with the optical parametric amplifier (OPA) receiver from [5]. It has been shown [6]

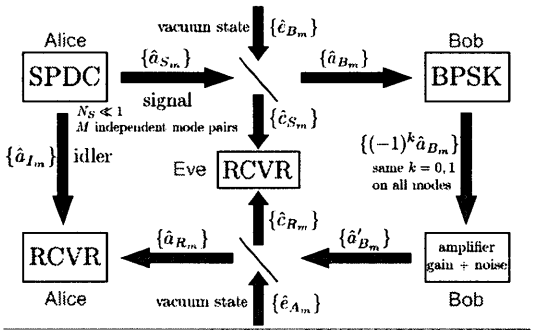

Figure 1-2: Schematic of quantum-illumination two-way communication protocol—showing modal annihilation operators—with passive-eavesdropper Eve receiving all the light that does not reach its intended destination. The annihilation operator notation for the optical modes will be explained in Chapter 3.

that 50 Mbit/s Bob-to-Alice communication with error probability less than 5.1×10^{-7} is possible, in principle, using this receiver for $N_S = 0.004$, $G_B = 10^4$ and $N_B = 10^4$ when $\kappa = 0.1$. In contrast, suppose Eve (via passive eavesdropping) collects all of Alice's light that does not reach Bob and all of Bob's light that does not reach Alice. Then, if she builds an optimum quantum receiver, whose realization is as yet unknown, her error probability for decoding Bob's BPSK bit has been shown [6] to

lie between 0.28 and 0.46. Moreover, this occurs despite Eve's receiving 9 times the amount of Alice's transmitted light that Bob does, and 9 times the amount of Bob's transmitted light that Alice does. Even more surprising, this performance advantage occurs *because* Alice's signal and idler are entangled even though the idler she has retained is *not* entangled with the light she gets from Bob, viz., propagation loss and amplified spontaneous emission (ASE) noise make the two-way channel entanglement breaking.

1.3 Thesis Structure

In this thesis we will extend and generalize the prior work on quantum illumination for secure communication in several ways. First, for the passive eavesdropping scenario examined in [6], we will bound the extra information that Alice receives, in comparison with what Eve gets, to provide a more complete picture of this protocol's immunity to passive eavesdropping when BPSK modulation is employed and Alice uses an OPA receiver. Then we investigate alternatives to the OPA receiver, seeking one whose performance approaches the quantum-optimum error exponent set by the quantum Chernoff bound. Finally, we examine M-ary modulation, with $M \geq 2$, seeking to increase the data rate of the quantum illumination protocol with constant bandwidth.

It was already recognized in [6] that the greatest vulnerability of the Fig.1-2 configuration occurs when Eve performs active eavesdropping, i.e., when she injects her own light into Bob's system and detects some of the modulated, amplified version of that injected light to determine Bob's message bits. Although suggestions were made in [6] for minimizing Alice and Bob's vulnerability to active eavesdropping, no analysis of those suggestions was reported therein. That analysis constitutes a significant portion of this thesis.

The remainder of the thesis is organized as follows. In Chapter 2, we provide background material on quantum optics, the SPDC source, and quantum detection theory that is essential for the work that will follow. In Chapter 3, we focus on the passive eavesdropping attack. In Chapter 4, we treat three versions of active

eavesdropping, and Alice and Bob's tools to counteract them. Finally, in Chapter 5, we summarize our results and give some suggestions for future work.

Chapter 2

Background Material

The dynamical variables in classical physics take on real-number values, whereas the corresponding quantum-mechanical versions of these dynamical variables are Hermitian operators on a Hilbert space of states. The most important difference between numbers and operators is the commutation property. In classical mathematics, multiplication of real numbers is commutative

$$z_1 z_2 = z_2 z_1 : \forall z_1, z_2 \in R. \tag{2.1}$$

However, if $\widehat{O_1}$ and $\widehat{O_2}$ are Hermitian operators, they need not commute viz., in general we have that

$$\widehat{O_1}\widehat{O_2} \neq \widehat{O_2}\widehat{O_1}. \tag{2.2}$$

In this chapter, we provide some background material that is necessary to understand the work to be presented in this thesis. First, we introduce electromagnetic field modes, including relevant operators and states, and we discuss the behavior of optical amplifiers and the statistics of different photodetection modalities. Then, we discuss the difference between classical states and nonclassical states, and present the state of SPDC light. Finally, we consider minimum error-probability discrimination between two density operators.

2.1 Electromagnetic Field Modes

Let us begin from classical electromagnetism. The fundamental equations governing electromagnetic wave propagation in free space are [7]—[10]: Gauss's law

$$\nabla \cdot \varepsilon_0 \overrightarrow{E} = 0, \tag{2.3}$$

Gauss's law for magnetism

$$\nabla \cdot \mu_0 \overrightarrow{H} = 0, \tag{2.4}$$

Faraday's law

$$\nabla \times \vec{E} = -\frac{\partial \left(\mu_0 \overrightarrow{H}\right)}{\partial t}, \tag{2.5}$$

and Ampere's law

$$\nabla \times \vec{H} = \frac{\partial \left(\varepsilon_0 \overrightarrow{E}\right)}{\partial t}. \tag{2.6}$$

Introducing the vector potential $\overrightarrow{A}(\overrightarrow{r}, t)$, and working with the Coulomb gauge, i.e., $\nabla \cdot \overrightarrow{A} = 0$, we can get the 3-D vector wave equation [7]—[10] from Equations (2.3)—(2.6),

$$\nabla^2 \overrightarrow{A}(\overrightarrow{r}, t) - \frac{1}{c^2} \frac{\partial^2 \overrightarrow{A}(\overrightarrow{r}, t)}{\partial^2 t} = 0, \tag{2.7}$$

where $c = 1/\sqrt{\mu_0 \varepsilon_0}$ is the speed of light. Equation (2.7) has monochromatic plane-wave solutions, i.e.,

$$\vec{A}(\vec{r}, t) = \overrightarrow{A_0} e^{-j\left(\omega t - \vec{k} \cdot \vec{r}\right)} + \overrightarrow{A_0}^* e^{j\left(\omega t - \vec{k} \cdot \vec{r}\right)}, \tag{2.8}$$

where $\vec{k} \cdot \vec{k} = \omega^2/c^2$ with $\vec{k}$ having real-valued cartesian components, is a frequency-ω plane wave propagating in the $\vec{k}$ direction. The two terms here are complex conjugates, to ensure that $\vec{A}(\vec{r}, t)$ is real valued. Confining the field in a $L \times L \times L$ unit cube, with periodic boundary conditions, we can further get the general solution to

the vector wave equation [7]

$$\vec{A}(\vec{r},t) = \frac{1}{2\sqrt{\varepsilon_0 L^3}} \sum_{\vec{l},\sigma} q_{\vec{l},\sigma} e^{-j\left(\omega_{\vec{l}} t - \vec{k}_{\vec{l}} \cdot \vec{r}\right)} \vec{e}_{\vec{l},\sigma} + c.c., \tag{2.9}$$

where *c.c.* denotes complex conjugate, $\vec{k}_{\vec{l}} = \frac{2\pi}{L}[l_x, l_y, l_z]^T$ for integers (l_x, l_y, l_z), and $\vec{e}_{\vec{l},\sigma}$, for $\sigma = 0, 1$, is a pair of orthogonal unit vectors that are also orthogonal to $\vec{k}_{\vec{l}}$.

Equation (2.9) expresses the vector potential as a sum of orthogonal plane-wave modes whose time-domain complex amplitudes $q_{\vec{l},\sigma} e^{-j\omega_{\vec{l}} t}$ perform simple harmonic motion, i.e., they behave like classical harmonic oscillators. At this point, the transition to the quantized electromagnetic field is made more convenient by replacing $q_{\vec{l},\sigma}$ with the dimensionless quantity $a_{\vec{l},\sigma} = \sqrt{\frac{\omega_{\vec{l}}}{2\hbar}} q_{\vec{l},\sigma}$. The classical electric field is then found from

$$\vec{E}(\vec{r},t) = -\frac{\partial \vec{A}(\vec{r},t)}{\partial t} \tag{2.10}$$

to be [7]

$$\vec{E}(\vec{r},t) = \sum_{\vec{l},\sigma} j\sqrt{\frac{\hbar\omega_{\vec{l}}}{2\varepsilon_0 L^3}} a_{\vec{l},\sigma} e^{-j\left(\omega_{\vec{l}} t - \vec{k}_{\vec{l}} \cdot \vec{r}\right)} \vec{e}_{\vec{l},\sigma} + c.c. \tag{2.11}$$

Each individual mode can be quantized by treating it as a harmonic oscillator. As a result, the quantized version of the electric field is

$$\widehat{\vec{E}}(\vec{r},t) = \sum_{\vec{l},\sigma} j\sqrt{\frac{\hbar\omega_{\vec{l}}}{2\varepsilon_0 L^3}} \hat{a}_{\vec{l},\sigma} e^{-j\left(\omega_{\vec{l}} t - \vec{k}_{\vec{l}} \cdot \vec{r}\right)} \vec{e}_{\vec{l},\sigma} + h.c., \tag{2.12}$$

where $\hat{a}_{\vec{l},\sigma}$ is the photon annihilation operator of the $\vec{l},\sigma$ mode and *h.c.* denotes Hermitian conjugate.

For the purpose of this thesis, it suffices to work with a simplified quantum field description that follows from assuming only a single polarization state of a narrowband frequency range for $+z$-going spatial modes is excited. Then, suppressing the spatial

dependence, converting the field to $\sqrt{\text{photons/s}}$ units, we can write [7]

$$\hat{E}(t) = \sum_{n=-\infty}^{\infty} \frac{\hat{a}_n}{\sqrt{T}} e^{-j(\omega_0 + 2\pi n/T)t}, \quad 0 \leq t \leq T \tag{2.13}$$

for the positive-frequency field operator, around the center frequency ω_0, over a measurement time interval $0 \leq t \leq T$. The adjoint (Hermitian conjugate) of $\hat{E}(t)$ is

$$\hat{E}^+(t) = \sum_{n=-\infty}^{\infty} \frac{\hat{a}_n^+}{\sqrt{T}} e^{-j(\omega_0 + 2\pi n/T)t}, \quad 0 \leq t \leq T, \tag{2.14}$$

where $\hat{a}_n^+$ is the photon creation operator of the nth temporal mode in the field.

2.2 Operators and States

Annihilation and creation operators play key roles in quantum optics. They do not commute, i.e.,

$$\left[\widehat{a}, \widehat{a}^+\right] = 1. \tag{2.15}$$

Associated with $\hat{a}$ and $\hat{a}^+$ is the number operator,

$$\widehat{N} = \widehat{a}^+ \widehat{a}. \tag{2.16}$$

Also of importance are the quadrature operators, which are defined as follows

$$\begin{aligned} \widehat{a_1} &= \frac{\widehat{a} + \widehat{a}^+}{2} \\ \widehat{a_2} &= \frac{\widehat{a} - \widehat{a}^+}{2j}. \end{aligned} \tag{2.17}$$

Operators and states of the modes together determine the statistics of the output of quantum system. We now discuss some states we use in the thesis. First, consider the number state $|n\rangle$. The annihilation operator reduces the number of the photons in the field by one, and the mathematical relationship between the annihilation operator

and the number state is [11] [12]

$$\widehat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,. \tag{2.18}$$

On the other hand, the creation operator increases the number of the photons in the field by one, so applying the creation operator to the number state $|n\rangle$ transforms it into $|n+1\rangle$, namely

$$\widehat{a}^{+}\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,. \tag{2.19}$$

Combining these two formulas, we can get

$$\widehat{N}\,|n\rangle = \widehat{a}^{+}\widehat{a}\,|n\rangle = \sqrt{n}\widehat{a}^{+}\,|n-1\rangle = n\,|n\rangle\,. \tag{2.20}$$

From this equation, we can conclude that the number states are the eigenstates of the number operator. If we perform the number-operator measurement on a field which is in a number state, we get a deterministic outcome equal to the number of the photons in that state.

The annihilation operator is not Hermitian, hence it need not have eigenstates. However, in 1963 Glauber showed that such eigenstates—which he called coherent state—do exist [13]; he was awarded the Nobel Prize in physics for his work on coherent states and their properties in October 2005. The coherent-state eigenstate relation is

$$\widehat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{2.21}$$

where α is any complex number. Because the set of the number states forms an orthonormal basis, we can express the coherent states in the number-state basis as

$$|\alpha\rangle = \sum_{n=0}^{\infty} \frac{\alpha^{n} e^{-|\alpha|^{2}/2}}{\sqrt{n!}}\,|n\rangle\,. \tag{2.22}$$

An important property of the coherent states is that they are not orthogonal, and

the inner product between two coherent states is [11] [14]

$$\langle\alpha|\beta\rangle = \exp\left(-|\alpha|^2/2 - |\beta|^2/2 + \alpha^*\beta\right), \tag{2.23}$$

Nevertheless, they form a basis for the mode's state space, albeit one that is over-complete. In particular, the coherent states resolve the identity operator $\hat{I}$ as follows,

$$\int |\alpha\rangle \langle\alpha| \frac{d^2\alpha}{\pi} = \widehat{I}. \tag{2.24}$$

The eigenstates of the quadrature operator $\hat{a}_1$, $|\alpha_1\rangle$, are other states we will use in the thesis because of their connection with homodyne detection. The properties of $|\alpha_1\rangle$ are the following

$$\widehat{a_1}\,|\alpha_1\rangle = \alpha_1\,|\alpha_1\rangle\,, \text{for } \alpha_1 \text{ real} \tag{2.25}$$

$$\langle\alpha_1|\alpha_1'\rangle = \delta\left(\alpha_1 - \alpha_1'\right), \tag{2.26}$$

$$\int |\alpha_1\rangle \langle\alpha_1| d\alpha_1 = \widehat{I}. \tag{2.27}$$

The number states $|n\rangle$, coherent states $|\alpha\rangle$, and quadrature eigenstates $|\alpha_1\rangle$ are all pure states. Although these states are useful to describe the quantum field, they are not enough, as most quantum fields are not in pure states. Instead, they are typically in mixed states, i.e., probabilistic mixtures of pure states. Mixed states are characterized by the density operator $\widehat{\rho}$. If a quantum field is in a pure state, $|\psi\rangle$, its density operator is $\widehat{\rho} = |\psi\rangle \langle\psi|$, which satisfies [15]

$$\begin{aligned} \mathrm{tr}\left(\widehat{\rho}\right) &= 1, \\ \mathrm{tr}\left(\widehat{\rho}^2\right) &= 1, \end{aligned} \tag{2.28}$$

where tr denotes trace. However, if the quantum field is in a mixed state, e.g, $\widehat{\rho} = \sum_n P_n |\psi_n\rangle \langle\psi_n|$, where $\{P_n\}$ is a probability distribution, then we find

$$\begin{aligned} \mathrm{tr}\left(\widehat{\rho}\right) &= 1, \\ \mathrm{tr}\left(\widehat{\rho}^2\right) &< 1. \end{aligned} \tag{2.29}$$

Our work on quantum illumination will necessarily deal with mixed states.

2.3 Photodetection Statistics

Having discussed the operators and the states of quantum fields, we now turn to the relevant photodetection statistics. We first consider direct detection, whose schematic is shown in Fig.2-1 [16] [17]. If a single-mode quantum field $\widehat{E}(t) = \frac{\widehat{a}e^{-j\omega t}}{\sqrt{T}}$, for $0 \leq t \leq T$ illuminates an ideal direct-direction system, it produces a stream of photocurrent impulses. The total number of these impulses, over the time interval $0 \leq t \leq T$, is the detector's photocount output N, which takes on nonnegative integer values $n = 0, 1, 2, \cdots$. The probabilities to get each individual outcome are [16]

$$\Pr\left(N = n | \text{state} = \widehat{\rho}\right) = \langle n | \widehat{\rho} | n \rangle . \tag{2.30}$$

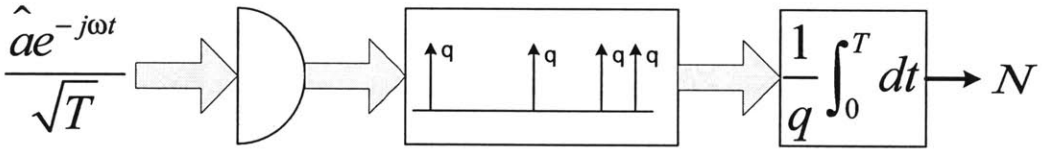

Figure 2-1: Schematic of idealized direct detection, q is the electron charge.

The structure of homodyne detection, shown in Fig.2-2, is more complicated than that of direct detection [16]. In homodyne detection the single-mode field to be de-

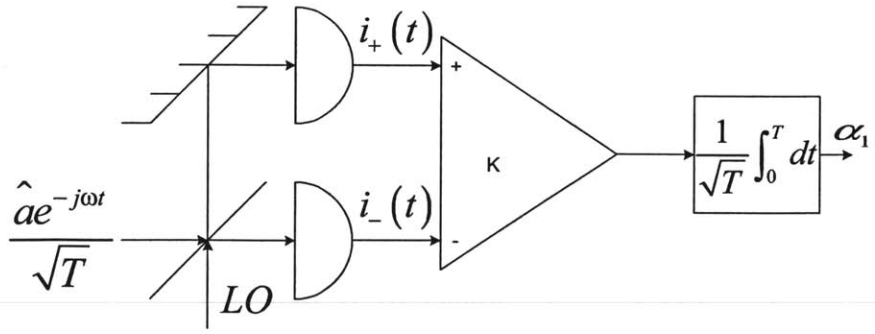

Figure 2-2: Schematic of idealized homodyne detection.

tected is mixed with a strong coherent-state local oscillator on a 50-50 beam splitter. The outputs from this beam splitter are photodetected and subtracted in a differential amplifier. After integration over the measurement interval, and appropriate normalization, the output of the system is a real-valued random variable, α_1, whose probability density function is [16]

$$p(\alpha_1|\text{state} = \widehat{\rho}) = \langle \alpha_1 | \widehat{\rho} | \alpha_1 \rangle , \tag{2.31}$$

when the local oscillator's phase has been chosen to measure the real quadrature of $\widehat{a}$.

Heterodyne detection, shown in Fig.2-3 [16], introduces an intermediate frequency, i.e., a radio-frequency offset between the single-mode field to be measured and the strong coherent-state local oscillator.

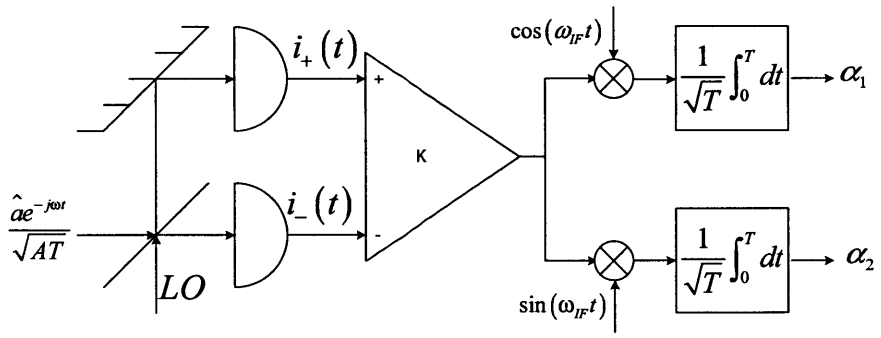

Figure 2-3: Schematic of idealized heterodyne detection.

Heterodyne detection allows both quadratures of the input field to be sensed. However, $\widehat{a}_1$ and $\widehat{a}_2$ do not commute, so they cannot be simultaneously measured in the observable paradigm of quantum mechanics. Heterodyne detection realizes the positive operator-valued measurement (POVM) associated with the coherent states $|\alpha\rangle$. In particular, the complex-valued random variable, $\alpha = \alpha_1 + j\alpha_2$, constructed from the normalized, quadrature-demodulated outputs shown in Fig.2-3, has probability density function [16]

$$p(\alpha|\text{state} = \widehat{\rho}) = \frac{\langle \alpha | \widehat{\rho} | \alpha \rangle}{\pi}. \tag{2.32}$$

2.4 Optical Amplifiers

The quantum-illumination system for secure communication makes use of phase-insensitive and phase-sensitive optical amplifiers. Bob uses the former in his terminal, and Alice uses the two-mode version of the latter in her receiver. The quantum single mode input-output relation for a phase-insensitive optical amplifier is

$$\widehat{a}_O = \sqrt{G}\widehat{a}_I + \sqrt{G-1}\widehat{e}^+, \tag{2.33}$$

where $\widehat{a}_O$ is the annihilation operator of the output mode, $\widehat{a}_I$ is the annihilation operator of the input mode, $\widehat{e}^+$ is the creation operator of an amplified spontaneous emission (ASE) noise mode, and $G > 1$ is the amplifier's gain. Lowest noise operation of this amplifier occurs when the $\widehat{e}$ mode is in its vacuum state.

In a two-mode phase-sensitive amplifier (an optical parametric amplifier), with signal and reference modes at the input and output, the input-output relation is

$$\begin{aligned} \hat{a}_{S_O} &= \sqrt{G}\hat{a}_{S_I} + \sqrt{G-1}\hat{a}^+_{R_I} \\ \hat{a}_{R_O} &= \sqrt{G}\hat{a}_{R_I} + \sqrt{G-1}\hat{a}^+_{S_I}, \end{aligned} \tag{2.34}$$

where $G > 1$ is the gain.

2.5 Classical versus Nonclassical States

The photodetection schemes in Section 2.3 treated photodetection statistics from quantum theory. In many cases, however, quantitatively identical results can be obtained from semiclassical photodetection, in which the light field is taken to be a classical electromagnetic wave and the fundamental photodetection noise source is the shot noise associated with the discreteness of the electron charge. States of the quantized electromagnetic field whose direct detection, homodyne detection, and heterodyne detection statistics can be correctly obtained from semiclassical theory are said to be classical states of the field.

Nonclassical states demonstrate some unique signatures in one or more of these

photodetection paradigms that cannot be explained by semiclassical photodetection theory. Density operators of the classical states have proper P-representations [16]

$$\widehat{\rho} = \int P(\alpha, \alpha^*) |\alpha\rangle \langle\alpha| \, d^2\alpha, \tag{2.35}$$

where $P(\alpha, \alpha^*)$ is a classical probability density function, i.e., $P(\alpha, \alpha^*) \geqslant 0$, and $\int P(\alpha, \alpha^*) \, d^2\alpha = 1$. A nonclassical state has a density operator that cannot be represented by Equation (2.35) with $P(\alpha, \alpha^*)$ being a classical probability density function. Important nonclassical signatures include sub-Poissonian distributions in direct detection and sub shot-noise quadrature variance in homodyne detection.

Squeezed vacuum states demonstrate the sub-shot-noise quadrature variance nonclassical signature. Squeeze operators are defined as follows

$$\widehat{S}(\xi) \equiv \exp\left[\frac{1}{2}\left(\xi^* \widehat{a}^2 - \xi \widehat{a}^{+2}\right)\right], \tag{2.36}$$

where $\xi = re^{i\theta}$. The major properties of the squeezed operators are [18]—[20]

$$\begin{aligned} \hat{S}^+(\xi) &= \hat{S}^{-1}(\xi) = \hat{S}(-\xi) \\ \hat{S}^+(\xi)\, \hat{a} \hat{S}(\xi) &= \hat{a} \cosh(r) - \hat{a}^+ e^{i\theta} \sinh(r) \\ \hat{S}(\xi)\, \hat{a} \hat{S}^+(\xi) &= \hat{a} \cosh(r) + \hat{a}^+ e^{i\theta} \sinh(r). \end{aligned} \tag{2.37}$$

The squeezed vacuum state, $|\xi, 0\rangle$, is defined by

$$|\xi, 0\rangle \equiv \widehat{S}(\xi) |0\rangle. \tag{2.38}$$

From Equations (2.36)—(2.38), we can derive the variance of the first quadrature of the squeezed vacuum state for $\theta = 0$,

$$\langle\xi, 0| \, \Delta\widehat{a}_1^2 \, |\xi, 0\rangle = \frac{1}{4} e^{-2r}. \tag{2.39}$$

From this result, we see that $r > 0$ makes this a sub-shot-noise quadrature noise,

because $\xi = 0$ makes $|\xi, 0\rangle$ the vacuum state, whose quadrature variance of 1/4 matches the semiclassical theory's shot-noise level.

2.6 Spontaneous Parametric Downconversion

One of the major methods to generate nonclassical light is the spontaneous parametric downconversion (SPDC) process. Frequency-degenerate SPDC generates squeezed vacuum state light, whereas the nondegenerate SPDC produces the two-mode squeezed vacuum state light [21]. In this thesis, we call two-mode squeezed vacuum state light SPDC light. Two-mode squeezed operator is

$$\hat{S}(\xi) \equiv \exp\left[\frac{1}{2}\left(\xi^* \hat{a}\hat{b} - \xi \hat{a}^+ \hat{b}^+\right)\right], \tag{2.40}$$

where $\hat{a}$ is the annihilation operator for the first mode and the $\hat{b}$ is the annihilation operator for the second mode. Its properties are

$$\begin{aligned} \hat{S}(\xi)\,\hat{a}\hat{S}^+(\xi) &= \hat{a}\cosh(r) + \hat{b}^+ e^{i\theta}\sinh(r) \\ \hat{S}(\xi)\,\hat{b}\hat{S}^+(\xi) &= \hat{b}\cosh(r) + \hat{a}^+ e^{i\theta}\sinh(r). \end{aligned} \tag{2.41}$$

The two-mode squeezed vacuum state is

$$\hat{S}(\xi)\,|0\rangle_a\,|0\rangle_b\,, \tag{2.42}$$

where $|0\rangle_a$ and $|0\rangle_b$ are the vacuum states of the $\hat{a}$ and $\hat{b}$ modes.

Another representation of the two-mode squeezed vacuum state can be given in the number state basis [22]

$$|\psi\rangle_{a,b} = \sum_{n=0}^{\infty} \sqrt{\frac{N^n}{(N+1)^{n+1}}}\,|n\rangle_a\,|n\rangle_b\,, \tag{2.43}$$

where $N = \sinh^2(r)$ is the average number of photons in the $\hat{a}$ and $\hat{b}$ modes, and $\theta = 0$ is assumed. Tracing out the other modes, we can get the density operator for

each individual mode [22]

$$\begin{aligned}\hat{\rho}_a &= \mathrm{tr}_b\left(\hat{\rho}_{ab}\right) = \mathrm{tr}_b\left(|\psi\rangle_{a,b}\langle\psi|\right) = \sum_{n=0}^{\infty} \frac{N^n}{(N+1)^{n+1}} |n\rangle_a\langle n| \\ \hat{\rho}_b &= \mathrm{tr}_a\left(\hat{\rho}_{ab}\right) = \mathrm{tr}_a\left(|\psi\rangle_{a,b}\langle\psi|\right) = \sum_{n=0}^{\infty} \frac{N^n}{(N+1)^{n+1}} |n\rangle_b\langle n|\end{aligned} \tag{2.44}$$

Thus, although the two-mode squeezed vacuum state is a pure state, each individual mode is in a mixed state, which is a signature of the two-mode state's being entangled.

2.7 Minimum Error-Probability Detection

Minimum error probability detection is a much more difficult problem for quantum measurement than it is for classical observations. Fortunately, there is an exact theoretical solution for the binary quantum case, the Helstrom bound. Suppose we want to distinguish between two states, $\widehat{\rho}_0$ and $\widehat{\rho}_1$, with minimum error probability. We need to choose a quantum measurement whose outcome will be the minimum error-probability decision. Let the prior probabilities for this decision problem be

$$\begin{aligned}\mathbf{Pr}\left(\hat{\rho} = \hat{\rho}_0\right) &= \pi_0 \\ \mathbf{Pr}\left(\hat{\rho} = \hat{\rho}_1\right) &= \pi_1.\end{aligned} \tag{2.45}$$

We want a POVM, $\left\{\widehat{M}_0, \widehat{M}_1\right\}$ with $\widehat{M}_0 + \widehat{M}_1 = \widehat{I}$, $\widehat{M}_0 \geqslant 0$, and $\widehat{M}_1 \geqslant 0$, that minimizes the resulting error probability when this measurement is performed, i.e., it minimizes [23] [24]

$$\mathbf{Pr}\left(\text{error}\right) = \pi_0 \mathrm{tr}\left(\hat{M}_1\hat{\rho}_0\right) + \pi_1 \mathrm{tr}\left(\hat{M}_0\hat{\rho}_1\right). \tag{2.46}$$

To minimize the error probability, we convert Equation (2.46) to

$$\mathbf{Pr}\left(\text{error}\right) = \pi_1 - \mathrm{tr}\left(\hat{M}_1\left(\pi_1\hat{\rho}_1 - \pi_0\hat{\rho}_0\right)\right) \tag{2.47}$$

From Equation (2.47), it is apparent that $\widehat{M}_1$ should be the projection operator onto the positive eigenvalue subspace of $(\pi_1\hat{\rho}_1 - \pi_0\hat{\rho}_0)$—and $\widehat{M}_0$ will then be the projection onto the nonpositive eigenvalue subspace of $(\pi_1\hat{\rho}_1 - \pi_0\hat{\rho}_0)$—to minimize the error probability. The resulting minimum error probability is [23] [24]

$$\min \Pr(\text{error}) = \frac{1}{2}\left(1 - \sum_n \alpha_n^{(+)}\right), \tag{2.48}$$

where $\left\{\alpha_n^{(+)}\right\}$ are the positive eigenvalues of $(\pi_1\hat{\rho}_1 - \pi_0\hat{\rho}_0)$.

For our quantum illumination communication protocol we will need error-probability results for optimum quantum reception when M independent, identically distributed mode pairs are observed, each of which then has density operator $\widehat{\rho}_0$ or $\widehat{\rho}_1$, so that the overall density operator is then $\widehat{\rho}_0^{\otimes M}$ or $\widehat{\rho}_1^{\otimes M}$. Moreover, because these will be mixed-state density operators, a direct evaluation of the $\left\{\alpha_n^{(+)}\right\}$ is prohibitively difficult. However, the quantum Chernoff bound,

$$\Pr(\text{error}) \leq \frac{1}{2}\exp(-M\epsilon), \tag{2.49}$$

where $\epsilon = \min_{0\leq t\leq 1}\left(\text{tr}\left(\widehat{\rho}_0^t\widehat{\rho}_1^{1-t}\right)\right)$, comes to the rescue, because it is known that this bound is exponentially tight, i.e.,

$$\lim_{M\to\infty}\frac{\ln(2\Pr(\text{error}))}{M} = \epsilon \tag{2.50}$$

Chapter 3

Passive Eavesdropping

In passive eavesdropping, Eve just listens to the Alice-to-Bob channel and the Bob-to-Alice channel, but she does not inject her own light into these two channels. Although we assume that Eve collects all photons that were not received by Alice and Bob, which account for 90% of the total photons on the two channels when the channel has transmissivity $\kappa = 0.1$, she gets almost no information from such photons.

3.1 Passive Attack Communication Protocol

The quantum illumination communication protocol is shown schematically in Fig.3-1. Alice transmits the signal beam from a continuous-wave SPDC source to Bob over a lossy channel with transmissivity $\kappa \ll 1$, while retaining the idler beam (without loss) for subsequent joint measurement with what she will receive from Bob. Each T-sec-long transmission from Alice comprises $M = WT \gg 1$ signal-idler mode pairs with average photon number $N_S \ll 1$ per mode, where W is the source's phase-matching bandwidth. Bob, for his part, applies BPSK modulation (bit value k equally likely to be zero or one) to each T-sec-long interval of the light he receives from Alice. Then he amplifies that modulated light—with a phase-insensitive amplifier of gain G_B and amplified spontaneous emission noise N_B photons per mode—and sends the resulting beam back to Alice over the same transmissivity-κ channel. Alice then makes a joint return-beam/idler-beam measurement to obtain Bob's bit sequence. She does this

with the OPA receiver from [5], which, unlike the Alice's optimum quantum receiver, has an explicit hardware realization.

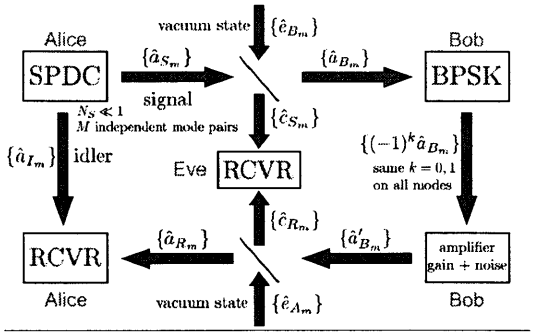

Figure 3-1: Schematic of quantum-illumination two-way communication protocol—showing modal annihilation operators—with passive-eavesdropper Eve receiving all the light that does not reach its intended destination.

Analysis of this communication protocol requires a quantum treatment, because the SPDC source's signal and idler outputs are entangled. For continuous-wave operation, the output beams comprise a collection of M independent, identically distributed mode pairs with annihilation operators $\{\,\hat{a}_{S_m}, \hat{a}_{I_m} : 1 \leq m \leq M\,\}$. Hence their joint density operator is

$$\hat{\rho}_{SI} = \bigotimes_{m=1}^{M} \hat{\rho}_{S_m I_m}, \tag{3.1}$$

where $\hat{\rho}_{S_m I_m}$, the state of the $\hat{a}_{S_m}$, $\hat{a}_{I_m}$ mode pair, is a zero-mean, maximally entangled Gaussian state whose Wigner-distribution covariance matrix is [6]

$$\mathbf{\Lambda}_{SI} = \frac{1}{4} \begin{bmatrix} S & 0 & C_q & 0 \\ 0 & S & 0 & -C_q \\ C_q & 0 & S & 0 \\ 0 & -C_q & 0 & S \end{bmatrix}, \tag{3.2}$$

where $S \equiv 2N_S + 1$ and $C_q \equiv 2\sqrt{N_S(N_S+1)}$.

The channel from Alice to Bob is purely lossy, so the modal annihilation operators

of the light beam that Bob receives are

$$\hat{a}_{B_m} = \sqrt{\kappa}\,\hat{a}_{S_m} + \sqrt{1-\kappa}\,\hat{e}_{B_m}, \text{ for } 1 \leq m \leq M, \tag{3.3}$$

where the $\{\hat{e}_{B_m}\}$ are in their vacuum states. Bob first modulates the light he has received with a BPSK information bit k that is equally likely to be 0 or 1. He then amplifies the modulated light with a phase-insensitive amplifier whose gain is G_B, leading to the following modal annihilation operators at the amplifier's output,

$$\hat{a}'_{B_m} = (-1)^k\sqrt{G_B}\,\hat{a}_{B_M} + \sqrt{G_B-1}\,\hat{a}^\dagger_{N_m}, \text{ for } 1 \leq m \leq M, \tag{3.4}$$

where $\{\hat{a}_{N_m}\}$ are in thermal states with $\langle \hat{a}_{N_m}\hat{a}^\dagger_{N_m}\rangle = N_B/(G_B-1) \geq 1$. Finally, Bob transmits the amplified modulated light back to Alice through the Bob-to-Alice channel, i.e., the same purely lossy channel as the Alice-to-Bob channel, so that the modal annihilation operators of the light beam Alice receives are

$$\hat{a}_{R_m} = \sqrt{\kappa}\,\hat{a}'_{B_m} + \sqrt{1-\kappa}\,\hat{e}_{A_m}, \text{ for } 1 \leq m \leq M, \tag{3.5}$$

where the $\{\hat{e}_{A_m}\}$ are in their vacuum states. Combining these formulas, $\hat{a}_{R_m}$ is found to satisfy

$$\hat{a}_{R_m} = (-1)^k\sqrt{G_B}\kappa\hat{a}_{S_m} + (-1)^k\sqrt{G_B}\sqrt{\kappa}\sqrt{1-\kappa}\hat{e}_{B_m} + \sqrt{G_B-1}\sqrt{\kappa}\hat{a}^\dagger_{N_m} + \sqrt{1-\kappa}\hat{e}_{A_m}. \tag{3.6}$$

Because $\{\hat{a}_{S_m}, \hat{a}_{I_m}, \hat{e}_{B_m}, \hat{e}_{A_m}, \hat{a}_{N_m}\}$ are in a zero-mean jointly Gaussian state, and because the transformation in (3.6) is linear, we know that $\{\hat{a}_{R_m}, \hat{a}_{I_m}\}$ are in zero-mean jointly Gaussian state when k is known. It is easily shown that this joint state is the tensor product of M independent, identically-distributed (iid) zero-mean, jointly Gaussian mode-pair states characterized by the Wigner-distribution covariance

matrix

$$\mathbf{\Lambda}_{RI}^{(k)} = \frac{1}{4}\begin{bmatrix} A & 0 & (-1)^k C_a & 0 \\ 0 & A & 0 & (-1)^{k+1} C_a \\ (-1)^k C_a & 0 & S & 0 \\ 0 & (-1)^{k+1} C_a & 0 & S \end{bmatrix}, \tag{3.7}$$

where $A \equiv 2\kappa^2 G_B N_S + 2\kappa N_B + 1$ and $C_a \equiv \kappa\sqrt{G_B}\, C_q$.

Assuming Eve receives all photons that Alice and Bob miss in the communication process, we have that Eve collects M iid mode pairs whose annihilation operators, $\{\, \hat{c}_{S_m}, \hat{c}_{R_m} : 1 \le m \le M \,\}$, satisfy

$$\hat{c}_{S_m} = \sqrt{1-\kappa}\,\hat{a}_{S_m} - \sqrt{\kappa}\,\hat{e}_{B_m} \tag{3.8}$$

$$\hat{c}_{R_m} = \sqrt{1-\kappa}\,\hat{a}'_{B_m} - \sqrt{\kappa}\,\hat{e}_{A_m}. \tag{3.9}$$

The joint state for each mode pair Eve receives is again zero-mean and jointly Gaussian given k, but its Wigner-distribution covariance matrix is

$$\mathbf{\Lambda}_{c_S c_R}^{(k)} = \frac{1}{4}\begin{bmatrix} D & 0 & (-1)^k C_e & 0 \\ 0 & D & 0 & (-1)^k C_e \\ (-1)^k C_e & 0 & E & 0 \\ 0 & (-1)^k C_e & 0 & E \end{bmatrix}, \tag{3.10}$$

where $D \equiv 2(1-\kappa)N_S + 1$, $C_e \equiv 2(1-\kappa)\sqrt{\kappa G_B}\, N_S$, and $E \equiv 2(1-\kappa)\kappa G_B N_S + 2(1-\kappa)N_B + 1$.

We will allow Eve to use the optimum (minimum error-probability) quantum receiver for deciding whether Bob's bit was 0 or 1, even though no known physical implementation is available for this receiver. On the other hand, we will only allow Alice to use the OPA receiver, which is a sub-optimum approach, whose realization is known. In both cases, we shall employ error-probability bounds, because—at least for Eve—the exact performance is too difficult to compute.

Specifically, for the minimum error-probability decision between M iid mode pairs

with each mode pair having either density operator $\hat{\rho}^{(0)}$ or $\hat{\rho}^{(1)}$, we have the upper bound

$$\Pr(e) \leq \frac{1}{2} e^{-M \max_{0 \leq s \leq 1} \mathcal{E}(s)}, \tag{3.11}$$

and the lower bound

$$\Pr(e) \geq \frac{1}{2}\left(1 - \sqrt{1 - e^{-2M\mathcal{E}(1/2)}}\right), \tag{3.12}$$

where $\mathcal{E}(s) \equiv -\ln\left(\mathrm{tr}[(\hat{\rho}^{(0)})^s (\hat{\rho}^{(1)})^{1-s}]\right)$.

Equation (3.11) is the quantum Chernoff bound [23], which is known to be exponentially tight. Its $s = \frac{1}{2}$ version

$$\Pr(e) \leq \frac{1}{2} e^{-M\mathcal{E}(1/2)}, \tag{3.13}$$

is known as the Bhattacharyya bound, and is generally loose but often more convenient, especially if analytical results are desired. When $\hat{\rho}^{(0)}$ and $\hat{\rho}^{(1)}$ are Gaussian states, Pirandola and Lloyd [25] have shown how to compute these bounds in terms of the symplectic decompositions of $\hat{\rho}^{(0)}$ and $\hat{\rho}^{(1)}$.

The interesting operating regime for the quantum illumination communication protocol is when $\kappa \ll 1$, $N_S \ll 1$, and $N_B \gg 1$, i.e., lossy propagation, low-brightness source, and high-brightness noise. Here it has been shown [6] that $s = \frac{1}{2}$ maximizes the error exponents for Alice and Eve's optimum quantum receivers with

$$\Pr(e)_{\text{Alice}} \leqslant \frac{1}{2} e^{-4M\kappa G_B N_S / N_B}, \tag{3.14}$$

and

$$\Pr(e)_{\text{Eve}} \leqslant \frac{1}{2} e^{-4M\kappa(1-\kappa) G_B N_S^2 / N_B}. \tag{3.15}$$

Because $N_S \ll 1$, there is an enormous disparity—in favor of Alice—in these bounds. However, we will only allow Alice to use a realizable receiver, in which she

uses an OPA to obtain modes with annihilation operators

$$\hat{a}'_m = \sqrt{G_A}\,\hat{a}_{I_M} + \sqrt{G_A - 1}\,\hat{a}^\dagger_{R_m}, \text{ for } 1 \leq m \leq M, \tag{3.16}$$

and then makes a minimum error-probability decision based on the photon-counting measurement $\sum_{m=1}^{M} \hat{a}'^\dagger_m \hat{a}'_m$ with $G_A = 1 + N_S/\sqrt{\kappa N_B}$. As a result, the Bhattacharyya bound on her receiver's performance is

$$\Pr(e)_{\text{Alice}} \leqslant \frac{\exp(-2M\kappa G_B N_S/N_B)}{2}, \tag{3.17}$$

which is only 3 dB inferior in error exponent to the optimum quantum receiver, and still better than Eve's receiver performance.

Figure 3-2 shows the immunity that this protocol offers to passive eavesdropping, viz., it plots upper and lower bounds on the error probability of Eve's optimum quantum receiver when she collects all of Alice's light that does not reach Bob and all of Bob's light that does not reach Alice. Also included are upper bounds on Alice's error probabilities with her optimum quantum receiver and her OPA receiver. With $W = 1\,\text{THz}$, $T = 20\,\text{ns}$ and the remaining parameters as shown in the figure, Bob can communicate to Alice at 50 Mbit/s with an OPA receiver at an error probability less than 5.1×10^{-7}, while Eve's optimum quantum receiver has an error probability bounded between 0.28 and 0.46. Neglecting all other losses, the $\kappa = 0.1$ transmissivity between Alice and Bob corresponds to this communication being carried out over 50 km of low-loss (0.2 dB/km) fiber.

3.2 Information Disparity between Alice and Eve

Mutual information is another important specification of the receiver, as it indicates how much information the receiver can get per channel use. As discussed in the previous section, Alice's error probability is much smaller than Eve's. Intuitively, we expect the mutual information between Alice and Bob to be much higher than that between Eve and Bob. However, as Alice's and Eve's receivers operate in different

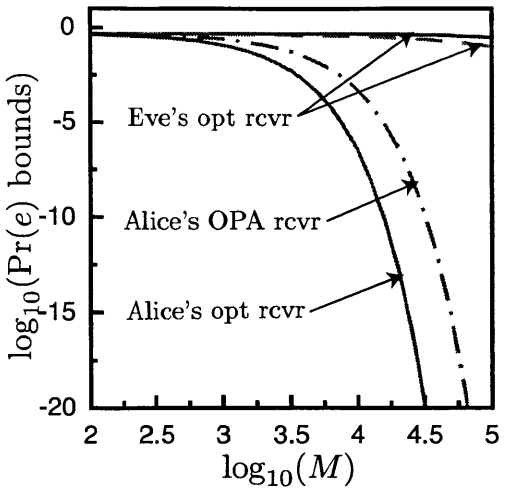

Figure 3-2: Error-probability bounds for $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$. Solid curves: Chernoff upper bounds for Alice and Eve's optimum quantum receivers. Dashed curve: error-probability lower bound for Eve's optimum quantum receiver. Dot-dashed curve: Bhattacharyya upper bound for Alice's OPA receiver.

regimes, the computation of these two mutual informations is different.

In particular, we can say that the secure information that Alice receives per channel use equals her Shannon information with Bob minus Eve's Holevo information with Bob.

As we focus on Alice's OPA receiver, whose implementation is known, we calculate the Shannon information for Alice,

$$I(X;Y) = \sum_{y \in Y} \sum_{x \in X} P_{X,Y}(x,y) \log \left(\frac{P_{X,Y}(x,y)}{P_X(x) P_Y(y)} \right), \tag{3.18}$$

where X is the input random variable at Bob's terminal and Y is the output random variable from Alice's OPA receiver. However, this equation is not the most convenient method to compute Alice's information. Instead, we can simplify the process by writing $I(X;Y)$ in terms of output entropy and conditional entropy,

$$I(X;Y) = H(Y) - H(Y|X). \tag{3.19}$$

Due to the symmetry of the system, Y will be equally likely to be 0 or 1, so that

$$H(Y) = 1, \tag{3.20}$$

where we are using base-2 logarithms for $H(Y) = -\sum_{y=0}^{1} \Pr(y) \log_2(\Pr(y))$. We also have that $\{Y|X=0\}$ and $\{Y|X=1\}$ are $0-1$ random variables, with their error probabilities being the false alarm probability, P_F, and miss probability, P_M, respectively. So we can express the conditional entropy as

$$\begin{aligned} H(\mathrm{Y}|\mathrm{X}=0) &= -P_F \log_2(P_F) - (1-P_F)\log_2(1-P_F) \\ H(\mathrm{Y}|\mathrm{X}=1) &= -P_M \log_2(P_M) - (1-P_M)\log_2(1-P_M), \end{aligned} \tag{3.21}$$

and $H(Y|X) = \frac{1}{2}[H(Y|X=0) + H(Y|X=1)]$.

To find the false-alarm and miss probabilities, we will exploit the high average photon number in $\widehat{N} = \sum_{m=1}^{M} \widehat{a}_m'^{+}\widehat{a}_m'$ that will be present under both $X=0$ and $X=1$ by approximating the conditional photocount statistics by Gaussian distributions. Taking those to have conditional means N_0 and N_1 and conditional variance σ_0^2 and σ_1^2, we will use a threshold test

$$N \underset{\hat{X}=1}{\overset{\hat{X}=0}{\gtrless}} \gamma, \tag{3.22}$$

where $\hat{X}$ denotes the decoded symbol, and γ is chosen to achieve $P_F = P_M = Q\left(\frac{N_1-N_0}{\sigma_1+\sigma_0}\right)$ with $Q(z) = \int_z^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt$.

Fig.3-3 shows the Gaussian approximation, Bhattacharyya upper bound and Bhattacharyya lower bound for Alice's OPA receiver. As we can see from the figure, the error probability is around 10^{-6} when $M = 1.4 \times 10^4$, $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$. It follows that Alice's information is

$$I(X;Y) \approx 1 \quad \text{bit/use} \tag{3.23}$$

at this operating point, although we will use the full Gaussian-approximation error-probability formula later.

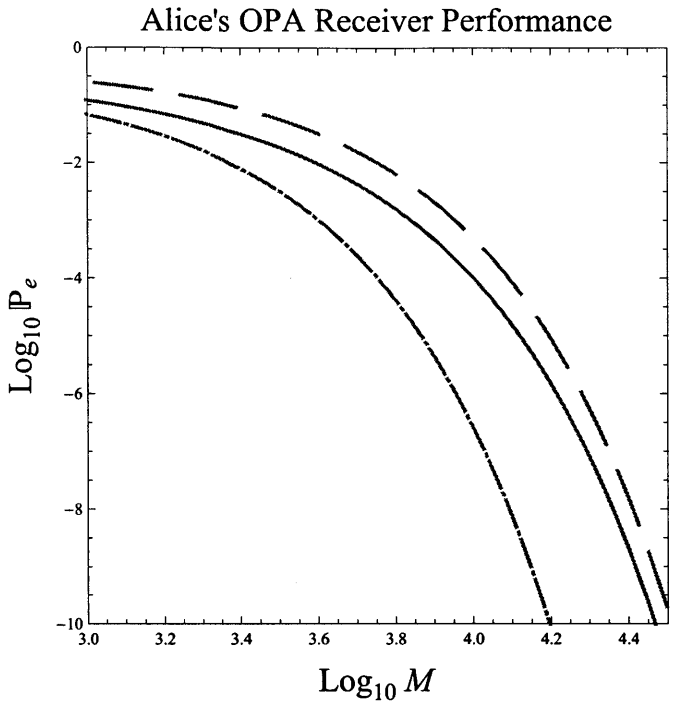

Figure 3-3: Error-probability performance of Alice's OPA receiver for $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$. Solid curve: Gaussian approximation for Pr(e). Dashed curve: Bhattacharyya upper bound for Pr(e). Dot-dashed curve: Bhattacharyya lower bound for Pr(e).

Because Eve can use optimum quantum reception across a sequence of channel uses, we need to evaluate the Holevo information she gains from her passive eavesdropping, namely [26]

$$\chi = M\left[S\left(\hat{\rho}\right) - \frac{1}{2}S\left(\hat{\rho}_0\right) - \frac{1}{2}S\left(\hat{\rho}_1\right)\right] \tag{3.24}$$

for $\hat{\rho} = \frac{1}{2}\left(\hat{\rho}_0 + \hat{\rho}_1\right)$, where $\hat{\rho}_0$ and $\hat{\rho}_1$ are the joint density operators for one of Eve's iid mode pairs —$\hat{c}_S$ and $\hat{c}_R$, and $S\left(\hat{\rho}\right) = -\mathrm{tr}\left(\hat{\rho}\right)\log_2\left(\hat{\rho}\right)$ is the von Neumann entropy.

Von Neumann entropy is difficult compute for general mixed states. However, if the state is Gaussian, the process is straightforward. For example, $\hat{\rho}_0$ and $\hat{\rho}_1$ are Gaussian states, and we can transform these two states into thermal states with average photon numbers N_0 and N_1 via symplectic transformations, which are also

unitary transformations. Moreover, unitary transformations do not change von Neumann entropy, and the von Neumann entropies of the thermal states obtained from the symplectic transformations of $\hat{\rho}_0$ and $\hat{\rho}_1$ are,

$$g(N_k) \equiv (N_k + 1)\log_2(N_k + 1) - N_k \log_2(N_k), \quad \text{for } k = 0, 1. \tag{3.25}$$

Although $\hat{\rho}_0$ and $\hat{\rho}_1$ are Gaussian states, $\hat{\rho} = \frac{1}{2}(\hat{\rho}_0 + \hat{\rho}_1)$ is not. Nevertheless, we can obtain an upper bound on $S(\hat{\rho})$ with the von Neumann entropy of a Gaussian state, because a Gaussian state maximizes the von Neumann entropy for the same Wigner covariance matrix [27]. The Wigner-distribution covariance matrix of $\hat{\rho}_k$ is

$$\mathbf{\Lambda}^{(k)}_{c_S c_R} = \frac{1}{4}\begin{bmatrix} D & 0 & (-1)^k C_e & 0 \\ 0 & D & 0 & (-1)^k C_e \\ (-1)^k C_e & 0 & E & 0 \\ 0 & (-1)^k C_e & 0 & E \end{bmatrix}, \tag{3.26}$$

for $k = 0, 1$. Due to the linearity of the trace operation, the Wigner-distribution covariance matrix of $\hat{\rho}$ is

$$\mathbf{\Lambda} = \frac{1}{4}\begin{bmatrix} D & 0 & 0 & 0 \\ 0 & D & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & E \end{bmatrix}. \tag{3.27}$$

From (3.27), we see that a two-mode product thermal state, $\widehat{\rho}_A$, with $\frac{D-1}{2}$ and $\frac{E-1}{2}$ photons on average in each individual mode has the same Wigner-distribution covariance matrix $\mathbf{\Lambda}$. Thus we get the upper bound on Eve's Holevo information

$$\begin{aligned} \chi &= M\left[S(\hat{\rho}) - \tfrac{1}{2}S(\hat{\rho}_0) - \tfrac{1}{2}S(\hat{\rho}_1)\right] \\ &\leq M\left[S(\hat{\rho}_A) - \tfrac{1}{2}S(\hat{\rho}_0) - \tfrac{1}{2}S(\hat{\rho}_1)\right]. \end{aligned} \tag{3.28}$$

In Fig.3-4, we have plotted, versus the number of modes M, Alice's Shannon information, the upper bound on Eve's Holevo information and the difference between

them for a single channel use. The curves assume $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$. We see that Alice's Shannon information rises much faster than the upper bound on Eve's Holevo information, with the maximum difference between them occurring between $M = 5 \times 10^3$ and $M = 2 \times 10^4$.

Because we have used an upper bound on Eve's Holevo information, the solid curve in Fig.3-4 is a lower bound on Alice's information advantage. At its peak, this lower bound exceeds 0.9 bit/channel use, which is not far from the maximum 1 bit/channel use that could be achieved with binary modulation.

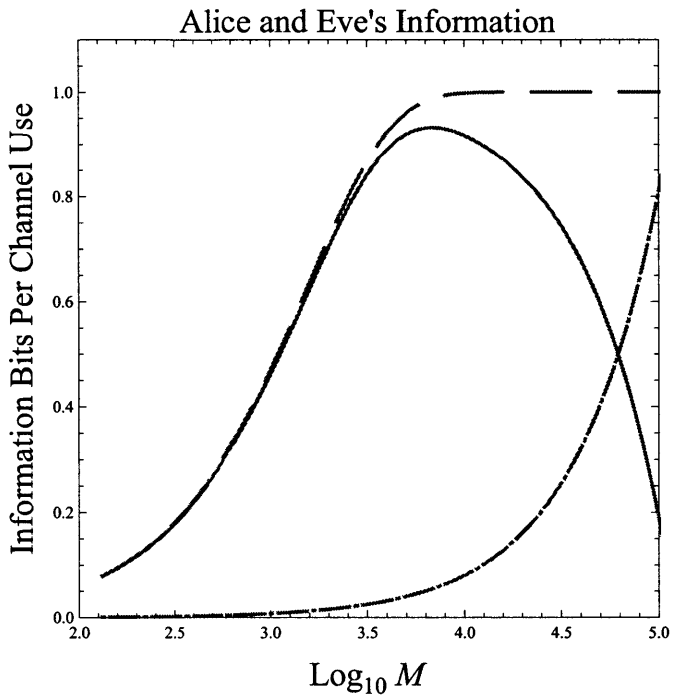

Figure 3-4: Alice's Shannon information and upper bound on Eve's Holevo information per channel use for $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$. Solid curve: Lower bound between Alice's Shannon information and Eve's Holevo information. Dashed curve: Shannon information for Alice's OPA receiver. Dot-dashed curve: upper bound on Holevo information for Eve's optimum quantum receiver.

Before moving on to our treatment of active attacks, it is important to note a key characteristics of the passive-attack we have mentioned. First, although the enormous performance disparity is due to Alice's having employed entangled signal and idler beams, all of the entanglement is destroyed by the Alice-to-Bob-to-Alice chan-

nel. In other words, the joint state of the $\hat{a}_{R_m}$ and $\hat{a}_{I_m}$ modes is classical, i.e., it is a random mixture of coherent states. The reason that Alice's receiver vastly outperforms Eve's is because the strong-than-classical phase-sensitive cross correlation—the off-diagonal elements in Λ_{SI}—of the SPDC source yields a much stronger (although classical) phase-sensitive cross correlation between $\hat{a}_{R_m}$ and $\hat{a}_{I_m}$ than the corresponding phase-insensitive cross correlation between $\hat{c}_{R_m}$ and $\hat{c}_{S_m}$ that is available to Eve. In particular, this is seen in the off-diagonal elements of Λ_{RI} which are much stronger than those of $\Lambda_{C_S C_R}$ when $N_s \ll 1$.

3.3 Alternative Receivers

In this section, we investigate some alternative receivers for Alice to see if we can achieve a better error exponent than she realizes with the OPA receiver.

First, we consider the dual-output OPA receiver, which jointly detects both outputs of the OPA to acquire the information bits. Suppose the measured photon-number on the mth mode for each individual output is $N_i^j(m)$, where $i = 0, 1$ represents Bob's information bit, and $j = 0, 1$ represents the index of the OPA outputs. Then the $\{E[N_i^j(m)]\}$, the average photon number in the jth output of the OPA given i, are given by

$$\begin{aligned} E[N_i^0(m)] &= (G_A - 1)(1 + G_A N_B \kappa + G_B N_S \kappa^2) + G_A N_S \\ &\quad + 2(-1)^i \kappa \sqrt{(G_A - 1) G_A G_B N_S (N_S + 1)} \\ E[N_i^1(m)] &= (G_A - 1)(1 + N_S) + G_A (N_B \kappa + G_B N_S \kappa^2) \\ &\quad + 2(-1)^i \kappa \sqrt{(G_A - 1) G_A G_B N_S (N_S + 1)}. \end{aligned} \tag{3.29}$$

Furthermore, the covariance matrix of the $\{N_i^j(m)\}$, for $j = 0, 1$ is

$$\Lambda_i = \begin{pmatrix} \sigma_i^0 & \lambda_i \\ \lambda_i & \sigma_i^1 \end{pmatrix}, \tag{3.30}$$

where $\sigma_i^0 = E[N_i^0(m)](E[N_i^0(m)] + 1)$, $\sigma_i^1 = E[N_i^1(m)](E[N_i^1(m)] + 1)$, and

$\lambda_i = \left(\sqrt{(G_A-1)G_A}\,(1+N_B\kappa+Ns\,(1+G_B\kappa^2)) + (-1)^i(2G_A-1)\kappa\sqrt{G_BN_S(1+N_S)}\right)^2$.
Ideally, we would like to have a closed-form expression for the error probability, from which we could find the optimum value of G_A. However, as we can see from the expression for $E\left[N_i^1(m)\right]$, this output is very noisy due to the $G_A(N_B\kappa+G_BN_S\kappa^2)$ term. Thus we do not expect to gain much by optimizing G_A. So, because it appears impossible to get a closed-form expression for the error probability in the two-dimensional case, we will continue to use the G_A value from the single-output OPA receiver, $1+\frac{N_S}{\sqrt{\kappa N_B}}$. We expect that the error probability we obtain should be close to the optimum value.

To calculate the error probability, we need to find the joint photon-counting distribution for all M modes when either $i=0$ or $i=1$ is sent. Defining

$$X = \sum_{m=1}^{M} N_i^0\,(m) \tag{3.31}$$

and

$$Y = \sum_{m=1}^{M} N_i^1\,(m) \tag{3.32}$$

when i is sent, we use the Central Limit Theorem to approximate the conditional distributions. We are seeking by the two-dimensional Gaussian

$$p_{X,Y|i}\,(x,y|i) = \frac{\exp\left[-\frac{1}{2}\begin{pmatrix} x-ME\left[N_i^0\right] \\ y-ME\left[N_i^1\right]\end{pmatrix}^T \Lambda_{i,M}^{-1}\begin{pmatrix} x-ME\left[N_i^0\right] \\ y-ME\left[N_i^1\right]\end{pmatrix}\right]}{2\pi|\Lambda_{i,M}|^{1/2}}, \tag{3.33}$$

where $\Lambda_{i,M} = M\Lambda_i$, and we have used the fact that the modes are independent and identically distributed to obtain the means and covariance matrix of X and Y from the modal means and covariance matrix.

Using the preceding joint distributions, we constructed the likelihood-ratio test and found the false-alarm and miss probabilities, P_F and P_M, by performing the

following integrations numerically:

$$P_F = \iint\limits_{(x,y)\in Z_1} dxdyp_{X,Y|i}\,(x,y|i=0) \tag{3.34}$$

and

$$P_M = \iint\limits_{(x,y)\in Z_0} dxdyp_{X,Y|i}\,(x,y|i=0), \tag{3.35}$$

where Z_0 and Z_1 are the X-Y plane decision region for receiving a 0 or a 1 respectively.

Figure 3-5 shows Alice's error probability for the single-output OPA receiver and the dual-output receiver. The abscissa is the logarithm of the number of modes employed, and the ordinate is the logarithm of the error probability, which is the Gaussian approximation of the true error probability. As we can see from the figure, the error exponent improvement is negligible for the dual-output OPA receiver. The reason why the improvement is so small is that only one output of the OPA has high signal-to-noise ratio, while the other output is very noisy. Thus adding another output has little effect on error probability performance.

Next, we consider the beam-splitter heterodyne receiver, which takes $\hat{a}_R$ and $\hat{a}_I$ as the inputs and detects a single output, $\widehat{b}$, to acquire the information bit k, as illustrated in Fig.3-6, where η is the transmittivity of the beam splitter.

As Fig.3-6 shows, we jointly detect both quadratures of $\widehat{b}$, and optimize η. The Wigner-covariance matrix for $\widehat{b}$ when Bob's message bit is k is

$$V_b^{(k)} = \frac{1}{4}\begin{pmatrix} V_b^{(k)}(1,1) & V_b^{(k)}(1,2) \\ V_b^{(k)}(2,1) & V_b^{(k)}(2,2) \end{pmatrix}, \text{ for } k=0,1 \tag{3.36}$$

where $V_b^{(k)}(1,2) = V_b^{(k)}(2,1) = 0$,

$$V_b^{(k)}(1,1) = 1+2N_S\eta+2N_B(1-\eta)\kappa+2G_BN_S(1-\eta)\kappa^2+4(-1)^k\kappa\sqrt{G_BN_S(1+N_S)(1-\eta)\eta}, \tag{3.37}$$

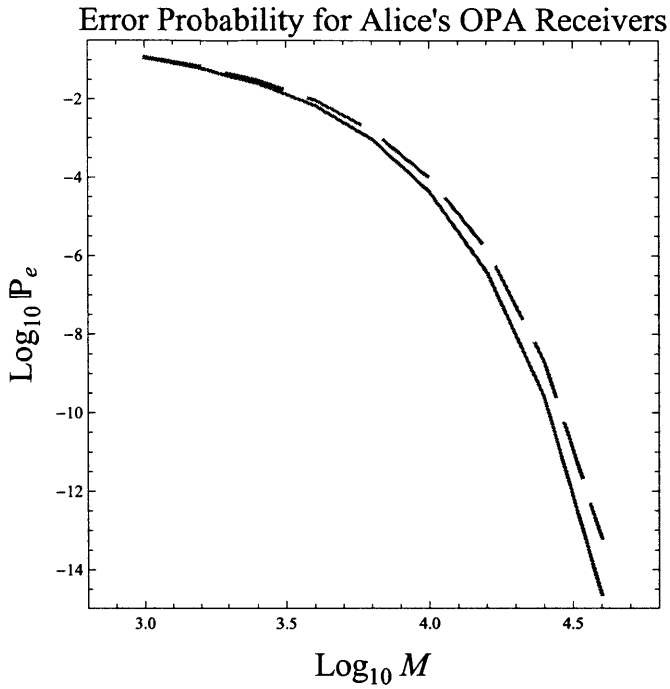

Figure 3-5: Error Probability for Alice's OPA receiver for $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$. Dashed curve: single-output OPA receiver. Solid curve: dual-output OPA receiver.

and

$$V_b^{(k)}(2,2) = 1+2N_S\eta+2N_B(1-\eta)\kappa+2G_BN_S(1-\eta)\kappa^2-4(-1)^k\kappa\sqrt{G_BN_S(1+N_S)(1-\eta)\eta}. \tag{3.38}$$

As we can see from the matrix, $V_b^{(k)}(1,1)$ and $V_b^{(k)}(2,2)$ are different, so they are not the symplectic spectrum, and we need to find the symplectic transformation matrix to convert the covariance matrix into the standard symplectic form whose two diagonal elements are equal. Using

$$S_k = \begin{pmatrix} \left(\frac{V_b^{(k)}(1,1)}{V_b^{(k)}(2,2)}\right)^{1/4} & 0 \\ 0 & \left(\frac{V_b^{(k)}(2,2)}{V_b^{(k)}(1,1)}\right)^{1/4} \end{pmatrix} \tag{3.39}$$

as the symplectic transformation matrix, we can find the symplectic spectrum, and

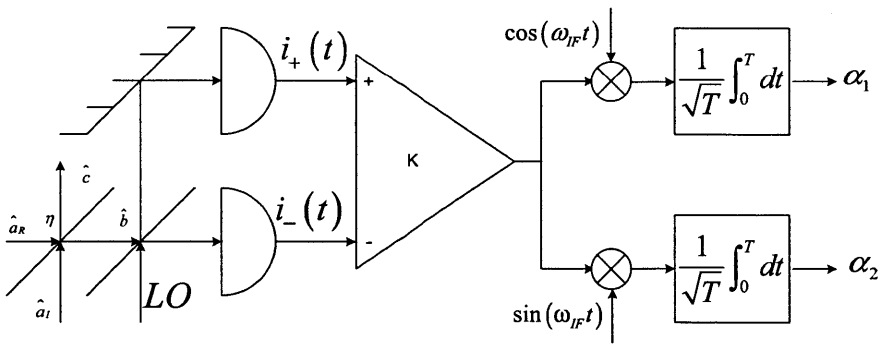

Figure 3-6: Schematic of Alice's Beam Splitter Receiver.

then we can compute the error exponent for the quantum Chernoff bound

$$\epsilon = -\frac{8MG_B\kappa^2(1-\eta)\eta N_S}{(1+2N_B\kappa(1-\eta))^2}, \tag{3.40}$$

where the optimum η is

$$\eta = \frac{1+2\mathrm{N}_B\kappa}{2(1+\mathrm{N}_B\kappa)}. \tag{3.41}$$

Plugging equation 3.41 into equation 3.40, we can get the beam-splitter optimized error exponent

$$\epsilon_{opt} = -\frac{2MG_BN_S\kappa^2}{1+2N_B\kappa} \approx -\frac{MG_BN_S\kappa}{N_B}, \tag{3.42}$$

which is 6 dB inferior to that of the OPA receiver.

Finally, we investigate the joint heterodyne receiver for $\hat{a}_R$ and $\hat{a}_I$. From equation (2.32) and Wigner-covariance matrix (3.7), we can derive the conditional probability density functions of the four outputs, $(\alpha_{R1}, \alpha_{R2}\alpha_{I1}, \alpha_{I2})$, under two hypotheses for one mode-pair:

$$p_0(\alpha_{R1}, \alpha_{R2}, \alpha_{I1}, \alpha_{I2}) = \frac{e^{-\frac{D\left(\alpha_{I1}^2+\alpha_{I2}^2\right)+2E(\alpha_{I2}\alpha_{R2}-\alpha_{I1}\alpha_{R1})+F(\alpha_{R1}^2+\alpha_{R2}^2)}{G}}}{\pi^2 G}, \tag{3.43}$$

$$p_1(\alpha_{R1}, \alpha_{R2}, \alpha_{I1}, \alpha_{I2}) = \frac{e^{-\frac{D\left(\alpha_{I1}^2+\alpha_{I2}^2\right)+2E(\alpha_{I1}\alpha_{R1}-\alpha_{I2}\alpha_{R2})+F(\alpha_{R1}^2+\alpha_{R2}^2)}{G}}}{\pi^2 G}, \tag{3.44}$$

where $D = 1+\kappa N_B+\kappa^2 G_B N_S$, $E = \kappa\sqrt{G_B N_S(1+N_S)}$, $F = 1+N_S$, and $G = 1+\kappa N_B+(1+\kappa N_B)N_S$. From these two joint probability density functions,

we conclude that $\alpha_{I2}\alpha_{R2} - \alpha_{I1}\alpha_{R1}$ is the sufficient statistic. Its mean values are $-\kappa\sqrt{G_B N_S(1+N_S)}$ and $\kappa\sqrt{G_B N_S(1+N_S)}$ under two hypotheses. Moreover, its variance is the same under both hypotheses, and equal to $\frac{1}{2}(1+N_S)(1+\kappa N_B + 2\kappa^2 G_B N_S)$. As a result, using the Central Limit Theorem approximation for the M mode-pair statistics, we get the error probability expression

$$\Pr(e) = Q\left(\sqrt{\frac{2MG_B N_S \kappa^2}{1+\kappa N_B + 2\kappa^2 G_B N_S}}\right). \tag{3.45}$$

For $N_B = G_B \gg 1$, and $N_S \ll 1$, this yields an error exponent

$$\epsilon_{het} = -\frac{MG_B N_S \kappa}{N_B}, \tag{3.46}$$

which is, as we found for the beam-splitter receiver, 6 dB inferior to that of the single-output OPA receiver.

None of the alternative receivers we have studied provide any appreciable reduction in error probability as compared to the single-output OPA receiver. This behavior is summarized in Fig.3-7. Here we have plotted the Central Limit Theorem approximation for the error probability of the single-output OPA receiver, and the heterodyne receiver for $\widehat{a}_R$ and $\widehat{a}_I$, along with upper (Chernoff) and lower (Bhattacharyya) bounds on the performance of the beam-splitter receiver. Even though the beam-splitter receiver's lower bound is slightly below the error probability of the OPA receiver, that is not a true performance advantage in that the Bhattacharyya lower bound is known to be loose.

Not shown in Fig.3-7 is the performance of the dual-output OPA receiver. As argued earlier in this section, its performance—in the practical range of interest—is not significantly better than that of the single-output OPA receiver.

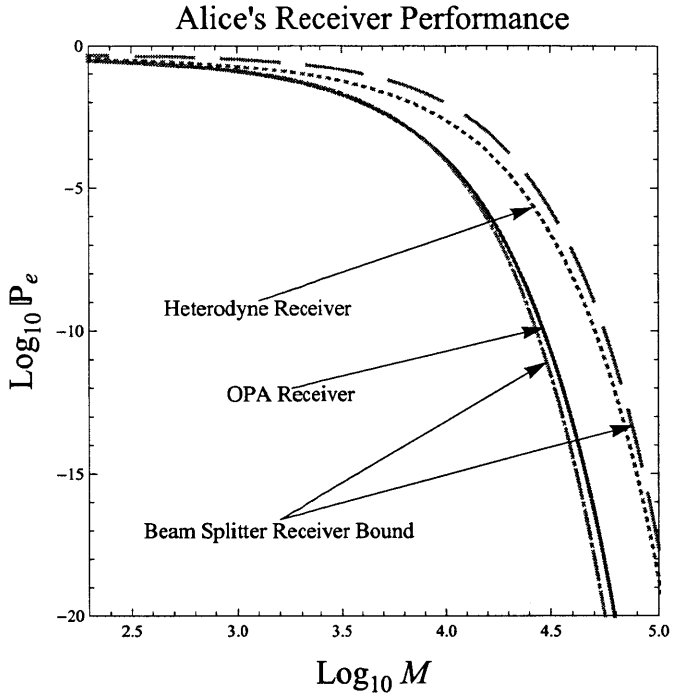

Figure 3-7: Error probabilities for Alice's several practical receivers assuming $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$. Dotted curve: heterodyne receiver for $\hat{a}_R$ and $\hat{a}_I$. Solid curve: single-output OPA receiver. Dashed and dot dashed curves: upper and lower bounds for single-output beam splitter receiver.

3.4 M-ary Modulation Technique

So far, our work with quantum-illumination based secure communication has been limited to binary phase-shift keying. The security of this approach—against both passive and active eavesdropping—relies on the use of a low brightness ($N_S \ll 1$) source. In conventional optical communications, the error probability at a fixed data rate can be reduced by increasing the source strength at constant bandwidth, i.e., increasing source brightness. For quantum illumination, however, we must increase the source bandwidth so that $M = WT$, the number of mode pairs, is increased if we want to reduce the error probability at constant data rate. Because BPSK has a data rate equal to $1/T$, maintaining a constant error probability at increasing data rate in our BPSK quantum illumination system requires an increase in bandwidth. Physical limitations on the phase-matching bandwidth of an SPDC source, as well as band-

width limits in propagation media, then restrict the data rate we can effectively make use of in BPSK quantum illumination. In an attempt to circumvent that bandwidth limit, we now explore the use of M-ary modulation ($M > 2$) in quantum-illumination based communication.

Let us consider quadrature phase-shift keying (QPSK), in which we can express $\widehat{a}_R$ as

$$\widehat{a}_R = (i)^k\sqrt{G_B}\kappa\widehat{a}_S + (i)^k\sqrt{G_B}\sqrt{\kappa}\sqrt{1-\kappa}\widehat{e}_B + \sqrt{G_B-1}\sqrt{\kappa}\widehat{a}_N^{+} + \sqrt{1-\kappa}\widehat{e}_A, \quad (3.47)$$

where $k = 0, 1, 2, 3$ is Bob's data. The OPA receiver cannot be used for QPSK modulation because it cannot distinguish $k = 1$ and $k = 3$ in that their photon-counting statistics are identical. The same argument applies to the joint homodyne receiver that measures $\mathrm{Re}\,(\widehat{a}_R)$ and $\mathrm{Re}\,(\widehat{a}_I)$. Likewise, a joint homodyne receiver that measures $\mathrm{Im}\,(\widehat{a}_R)$ and $\mathrm{Im}\,(\widehat{a}_I)$ will not be able to distinguish $k = 0$ and $k = 2$, because they give identical measurement statistics in this case. Heterodyne detection of $\widehat{a}_R$ and $\widehat{a}_I$ does, however, permit full QPSK reception. For such a measurement, with $\mathbf{x} = [\alpha_{R1}, \alpha_{R2}, \alpha_{I1}, \alpha_{I2}]^T$, we have the following conditional probability densities given the QPSK message value k:

$$p_{\mathbf{x}|k}(\mathbf{X}|k=0) = \frac{\exp\left(-\frac{1}{2}\mathbf{X}^T{\Lambda_0}^{-1}\mathbf{X}\right)}{(2\pi)^2|\Lambda_0|^{1/2}} \quad (3.48)$$

$$p_{\mathbf{x}|k}(\mathbf{X}|k=1) = \frac{\exp\left(-\frac{1}{2}\mathbf{X}^T{\Lambda_1}^{-1}\mathbf{X}\right)}{(2\pi)^2|\Lambda_1|^{1/2}} \quad (3.49)$$

$$p_{\mathbf{x}|k}(\mathbf{X}|k=2) = \frac{\exp\left(-\frac{1}{2}\mathbf{X}^T{\Lambda_2}^{-1}\mathbf{X}\right)}{(2\pi)^2|\Lambda_2|^{1/2}} \quad (3.50)$$

$$p_{\mathbf{x}|k}(\mathbf{X}|k=3) = \frac{\exp\left(-\frac{1}{2}\mathbf{X}^T{\Lambda_3}^{-1}\mathbf{X}\right)}{(2\pi)^2|\Lambda_3|^{1/2}}, \quad (3.51)$$

where

$$\mathbf{\Lambda_0} = \begin{bmatrix} F & 0 & I & 0 \\ 0 & F & 0 & -I \\ I & 0 & G & 0 \\ 0 & -I & 0 & G \end{bmatrix} \tag{3.52}$$

$$\mathbf{\Lambda_1} = \begin{bmatrix} F & 0 & 0 & I \\ 0 & F & I & 0 \\ 0 & I & G & 0 \\ I & 0 & 0 & G \end{bmatrix} \tag{3.53}$$

$$\mathbf{\Lambda_2} = \begin{bmatrix} F & 0 & -I & 0 \\ 0 & F & 0 & I \\ -I & 0 & G & 0 \\ 0 & I & 0 & G \end{bmatrix} \tag{3.54}$$

$$\mathbf{\Lambda_3} = \begin{bmatrix} F & 0 & 0 & -I \\ 0 & F & -I & 0 \\ 0 & -I & G & 0 \\ -I & 0 & 0 & G \end{bmatrix}, \tag{3.55}$$

with $F = \frac{1}{2}(1 + \kappa N_B + \kappa^2 G_B N_S)$, $G = \frac{1}{2}(1 + N_S)$, and $I = \frac{1}{2}\kappa\sqrt{G_B N_S (1 + N_S)}$.

Assuming Bob's quaternary symbols are equally likely, maximum-likelihood reception minimizes Alice's error probability. In particular, she uses the decision rule choose $k = l$ as Bob's message when $P_{\mathbf{x}|k}(\mathbf{X}|k = l) = \max_k P_{\mathbf{x}|k}(\mathbf{X}|k)$. The decision region for H_0 for a single mode-pair can then be shown to be

$$\begin{aligned} &\alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2} > 0 \\ &\alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2} > \alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1} \\ &\alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2} > -(\alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1}). \end{aligned} \tag{3.56}$$

Similarly, the decision region for H_1 for a single mode-pair is

$$\begin{aligned}
&\alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1} > 0 \\
&\alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1} > \alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2} \\
&\alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1} > -(\alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2}),
\end{aligned} \tag{3.57}$$

that for H_2 is

$$\begin{aligned}
&\alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2} < 0 \\
&\alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2} < \alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1} \\
&\alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2} < -(\alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1}),
\end{aligned} \tag{3.58}$$

and the one for H_3 is

$$\begin{aligned}
&\alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1} < 0 \\
&\alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1} < \alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2} \\
&\alpha_{I1}\alpha_{R2} + \alpha_{I2}\alpha_{R1} < -(\alpha_{I1}\alpha_{R1} - \alpha_{I2}\alpha_{R2}).
\end{aligned} \tag{3.59}$$

To visualize these decision regions for M' mode pairs, let us define

$$\beta_m = \alpha_{I1m}\alpha_{R1m} - \alpha_{I2m}\alpha_{R2m}, \tag{3.60}$$

$$\gamma_m = \alpha_{I1m}\alpha_{R2m} + \alpha_{I2}\alpha_{R1m}, \tag{3.61}$$

$$\beta = \sum_{m=1}^{M'} \beta_m, \tag{3.62}$$

and

$$\gamma = \sum_{m=1}^{M'} \gamma_m. \tag{3.63}$$

The detection regions, using all the mode pairs, are then

$$\begin{aligned}
&\text{decide } H_0 \text{ when } \beta > |\gamma| \\
&\text{decide } H_1 \text{ when } \gamma > |\beta| \\
&\text{decide } H_2 \text{ when } \beta < -|\gamma| \\
&\text{decide } H_3 \text{ when } \gamma < -|\beta|,
\end{aligned}$$

as shown in Fig.3-8.

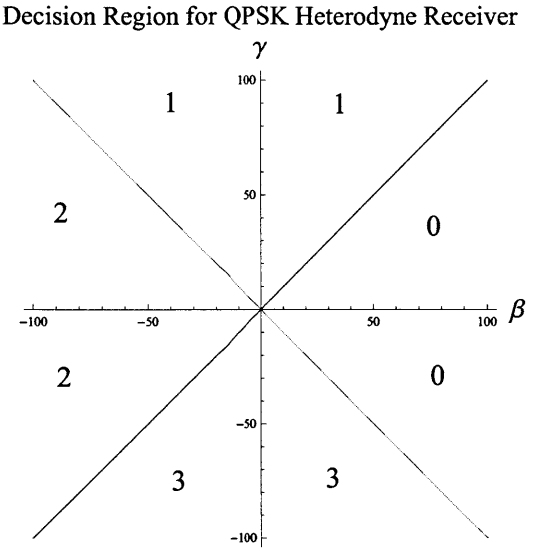

Figure 3-8: Decision regions for QPSK quantum illumination with heterodyne detection

Because QPSK transmits 2 bits per symbol while BPSK system transmits 1 bit per symbol, we use $M' = 2M$ mode pairs for QPSK versus M mode pairs for BPSK to compare their error probabilities at equal data rates in *bits/sec*. Because $M' \gg 1$, we shall employ the Central Limit Theorem to treat β and γ, which determine the decision regions, as jointly Gaussian random variables given k. Thus, to evaluate their full statistics it suffices to find their conditional means, conditional variances, and conditional covariance given k. We find that these conditional moments are as follows. For $k = 0$, we have

$$\begin{aligned}
&\langle\beta\rangle = M'\kappa\sqrt{G_B N_S(1+N_S)} \\
&\langle\Delta\beta^2\rangle = \tfrac{M'}{2}(1+N_S)(1+\kappa(N_B+2G_B N_S\kappa)) \\
&\langle\gamma\rangle = 0 \\
&\langle\Delta\gamma^2\rangle = \tfrac{M'}{2}(1+N_S)(1+N_B\kappa) \\
&\langle\Delta\beta\Delta\gamma\rangle = 0;
\end{aligned} \tag{3.64}$$

for $k = 1$,

$$\begin{aligned}
&\langle\beta\rangle = 0 \\
&\langle\Delta\beta^2\rangle = \tfrac{M'}{2}(1+N_S)(1+N_B\kappa) \\
&\langle\gamma\rangle = M'\kappa\sqrt{G_B N_S(1+N_S)} \\
&\langle\Delta\gamma^2\rangle = \tfrac{M'}{2}(1+N_S)(1+\kappa(N_B+2G_B N_S\kappa)) \\
&\langle\Delta\beta\Delta\gamma\rangle = 0;
\end{aligned}$$

for $k = 2$,

$$\begin{aligned}
&\langle\beta\rangle = -M'\kappa\sqrt{G_B N_S(1+N_S)} \\
&\langle\Delta\beta^2\rangle = \tfrac{M'}{2}(1+N_S)(1+\kappa(N_B+2G_B N_S\kappa)) \\
&\langle\gamma\rangle = 0 \\
&\langle\Delta\gamma^2\rangle = \tfrac{M'}{2}(1+N_S)(1+N_B\kappa) \\
&\langle\Delta\beta\Delta\gamma\rangle = 0;
\end{aligned} \tag{3.65}$$

and for $k = 3$,

$$\begin{aligned}
&\langle\beta\rangle = 0 \\
&\langle\Delta\beta^2\rangle = \tfrac{M'}{2}(1+N_S)(1+N_B\kappa) \\
&\langle\gamma\rangle = -M'\kappa\sqrt{G_B N_S(1+N_S)} \\
&\langle\Delta\gamma^2\rangle = \tfrac{M'}{2}(1+N_S)(1+\kappa(N_B+2G_B N_S\kappa)) \\
&\langle\Delta\beta\Delta\gamma\rangle = 0.
\end{aligned}$$

Because $N_B \gg 2G_B N_S\kappa$, we have $\langle\Delta\beta^2\rangle \approx \langle\Delta\gamma^2\rangle$ for all four k values. Thus we can approximate the QPSK decision problem as one of deterministic QPSK symbols in additive white Gaussian noise. By rotating the β-γ coordinates by 45° to obtain z_1 and z_2, we get the QPSK problem shown in Fig. 3-9, with $\xi \approx M'\kappa\sqrt{G_B N_S/2}$, where we have used $N_S \ll 1$.

The scalar components of the additive white Gaussian noise in this case have variances

$$\sigma_{z_1}^2 = \sigma_{z_2}^2 = \frac{1}{2}M'(1+N_B\kappa), \tag{3.66}$$

where we have again used $N_S \ll 1$. It is now easily shown that the QPSK symbol-error

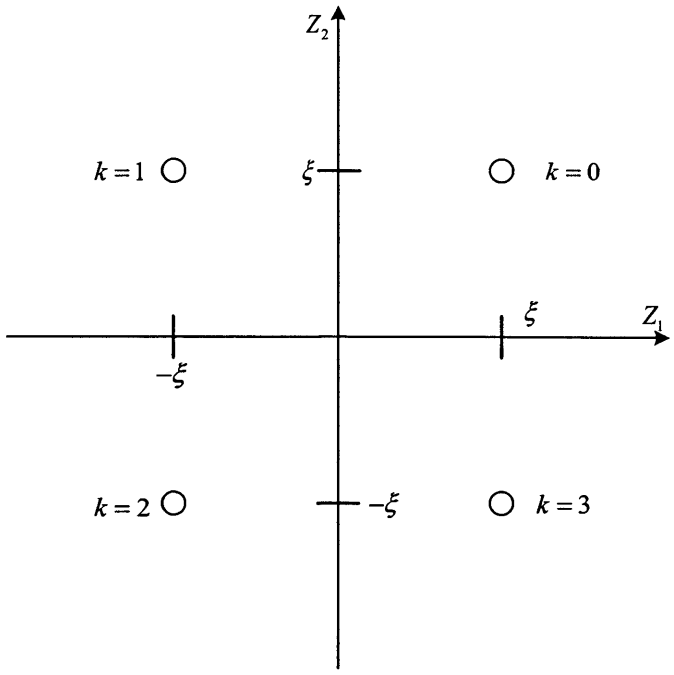

Figure 3-9: QPSK signal constellation

probability is

$$\Pr(e)_{QPSK} = 2Q\left(\sqrt{\frac{M'\kappa G_B N_S}{N_B}}\right) - Q^2\left(\sqrt{\frac{M'\kappa G_B N_S}{N_B}}\right), \tag{3.67}$$

where we have assumed $\kappa N_B \gg 1$.

Let us compare these results with those we have acquired for BPSK with the OPA receiver, the homodyne receiver, and the heterodyne receiver. In doing so, we shall concentrate on low error-probability operation, i.e., $M'\kappa G_B N_S/N_B \gg 1$, so that

$$\Pr(e)_{QPSK} \approx 2Q\left(\sqrt{\frac{M'\kappa G_B N_S}{N_B}}\right) \leqslant \exp\left(-\frac{M'\kappa G_B N_S}{2N_B}\right). \tag{3.68}$$

We shall also compare quaternary symbol error probabilities, so that for BPSK

$$\begin{aligned} &\Pr(e)_{BPSK} \approx 2\Pr(\text{bit error}) - \Pr^2(\text{bit error}) \approx 2\Pr(\text{bit error}) \\ &\leq \exp\left(-\frac{2M\kappa G_B N_S}{N_B}\right) = \exp\left(-\frac{M'\kappa G_B N_S}{N_B}\right) \end{aligned} \tag{3.69}$$

From these two equations, we can conclude that QPSK with heterodyne detection does not gain any advantage over BPSK with OPA receiver. On the contrary, the symbol error rate of QPSK has a 3 dB higher error exponent than that of BPSK at the same data rate.

Chapter 4

Active Eavesdropping

It is evident from Fig.1-2 that Eve can easily probe the state of Bob's BPSK modulator by injecting her own light into Bob via the Alice-to-Bob channel, and then detect the modulated, amplified, and noisy version of that light that is present in the Bob-to-Alice channel. Because Fig.1-2 presumes that *all* of the losses encountered by Alice and Bob are really due to Eve's beam splitter, Eve's active eavesdropping attack is exceedingly powerful. In addition to injecting her own light into the channel, Eve can, in general, modify the Alice-to-Bob and Bob-to-Alice transmissivity in trying to mask her intrusion. So, to minimize their vulnerability to such an attack, Alice and Bob should do the following four things: (1) Bob should use optical filtering to prevent Eve from accessing his BPSK modulator with an out-of-band signal, i.e., one whose spectrum does not overlap Alice's. (2) Alice and Bob should monitor the physical integrity of the propagation channels connecting them, e.g., using optical time-domain reflectometers (OTDRs) on fiber links, to bound Eve's optical couplings to Bob and Alice's terminals. (3) Alice and Bob should employ optical power monitors and optical spectrum analyzers to detect appreciable deviations—in total power or power spectral density—from what they would expect in the absence of Eve. (4) Alice should employ a bit error rate (BER) monitor, to sense appreciable changes from the performance she would expect in the absence of Eve. As a summary, Eve can modify the transmittivity of the Alice-to-Bob channel, which is redefined as κ_B, the transmittivity of Bob-to-Alice channel, which is redefined as κ_A, and choose the

quantum state she injects into the channel. On the other hand, Alice and Bob use power monitors and a BER detector to counteract such modifications.

The optimum quantum state for Eve's active attack is not known. However, our passive eavesdropping analysis has already shown that using the signal beam from an SPDC source—while retaining the idler for a joint measurement—outperforms all classical states of the same average photon number. Thus we will assume that Eve uses SPDC light for her attack. Moreover, to avoid the detection by a spectrum analyzer, she will use the same phase-matching bandwidth as Alice, with $N_E \ll 1$ photons per mode. Suppose, for now, that Eve does not change the channel transmittivities. Then, the error probability for her active attack will be

$$\Pr(e)_{\text{Eve}} \leqslant \frac{1}{2} e^{-4M(1-\kappa)G_B N_E/N_B}, \tag{4.1}$$

when she used the optimum quantum receiver.

If Alice and Bob cannot bound N_E, then Eve's receiver can easily outperform Alice's. Setting (3.14) equal (4.1), which means that Alice and Eve get the same optimum quantum receiver error-probability bound, the amount of the light Eve needs to inject per mode is

$$N_E = \frac{\kappa}{1-\kappa} N_S = \frac{1}{9} N_S, \text{ for } \kappa = 0.1. \tag{4.2}$$

The reason why Eve can easily outperform Alice is that Eve's transmissivity, $1-\kappa = 0.9$, is much higher than Alice's transmissivity, $\kappa = 0.1$.

Suppose that Alice and Bob want to get an error probability 10^{-5} with the OPA receiver while bounding Eve's error probability to be higher than 10^{-1} with the OPA receiver, then $N_E = \frac{1}{90} N_S$ satisfies the condition for $\kappa = 0.1$, when N_S, N_B, M, and G_B give Alice her desired error probability. We will discuss how Alice and Bob can constrain N_E to this value in different cases while employing only 1% of the received light for power monitoring, in order not to affect the normal communication process.

4.1 Active Case I: Eve Injects Light without Modifying Channel Transmittivities

First, consider what happens when Eve just injects her own light into the channel, without changing κ_B and κ_A from κ. Let us see how tightly Bob can constrain Eve's N_E by means of his power monitor. We define $N_{0,m}$ and $N_{1,m}$ to be the number of photons arriving at Bob's power monitor in the mth mode without and with Eve's light injection respectively. Because the M modes that Bob receives are in a product state, the $\{N_{0,m}\}$ are statistically independent, identically distributed random variables, and the $\{N_{1,m}\}$ are too. Moreover, the expectation value of $N_{0,m}$ is

$$\langle N_{0,m} \rangle = \frac{1}{100} \kappa N_S, \text{ for } 1 \leq m \leq M, \tag{4.3}$$

and the expectation value of $N_{1,m}$ is

$$\langle N_{1,m} \rangle = \frac{1}{100} \left[\kappa N_S + (1-\kappa) N_E \right], \text{ for } 1 \leq m \leq M, \tag{4.4}$$

when Bob uses 1% of his received light for power monitoring. In addition, their corresponding variances are

$$\left\langle \Delta N_{0,m}^2 \right\rangle = \langle N_{0,m} \rangle \left(\langle N_{0,m} \rangle + 1 \right) \approx \langle N_{0,m} \rangle \tag{4.5}$$

and

$$\left\langle \Delta N_{1,m}^2 \right\rangle = \langle N_{1,m} \rangle \left(\langle N_{1,m} \rangle + 1 \right) \approx \langle N_{1,m} \rangle , \tag{4.6}$$

where the approximations follow because SPDC sources operate at very low brightness, i.e, we have $\langle N_{0,m} \rangle \ll 1$, and $\langle N_{1,m} \rangle \ll 1$.

Bob's power monitor measures $N_0 = \sum_{m=1}^{M} N_{0,m}$ if Eve does not inject any light, and $N_1 = \sum_{m=1}^{M} N_{1,m}$ if she does. Due to the Central Limit Theorem, we can approximate the statistics of these random variables as Gaussian, because $M \gg 1$. Their expectation values are

$$\begin{aligned}\langle N_0\rangle &= \frac{M}{100}\kappa N_S \\ \langle N_1\rangle &= \frac{M}{100}\left[\kappa N_S + (1-\kappa)N_E\right]\end{aligned} \tag{4.7}$$

and their variances are

$$\begin{aligned}\langle \Delta N_0^2\rangle &= \frac{M}{100}\kappa N_S \\ \langle \Delta N_1^2\rangle &= \frac{M}{100}\left[\kappa N_S + (1-\kappa)N_E\right].\end{aligned} \tag{4.8}$$

Assume that Eve is equally likely to attack or not attack, and that Bob makes a minimum error probability decision about her absence or presence based on the observation from his power monitor. The error probability he will then get is

$$P_{e,B} = Q\left(\frac{\langle N_1\rangle - \langle N_0\rangle}{\sqrt{\langle \Delta N_1^2\rangle} + \sqrt{\langle \Delta N_0^2\rangle}}\right) = Q\left(\sqrt{M}\frac{(1-\kappa)N_E}{10\left(\sqrt{\kappa N_S} + \sqrt{\kappa N_S + (1-\kappa)N_E}\right)}\right), \tag{4.9}$$

where $Q(x) = \int_x^\infty dt \frac{e^{-t^2/2}}{\sqrt{2\pi}}$. To detect the attack with error probability less than 10^{-6}, Bob needs to monitor the power on a total of $M = 2.36 \times 10^9$ modes, which takes approximately 2.36 ms for an SPDC source with 1 THz phase-matching bandwidth.

4.2 Active Case II: Eve Modifies the Alice-to-Bob and Bob-to-Alice Channels

Now, let us study the case in which Eve increases her injection amount by reducing κ_B so that $\kappa_B N_S + (1-\kappa_B)N_E = \kappa N_S$ is the average number of photons reaching Bob. As a result, Bob's power monitor cannot detect Eve's attack. Because making $\kappa_B < \kappa$ will reduce the power that Alice couples to Bob, her error probability will increase if Eve does nothing else. To at least partially compensate for this effect, Eve increases the Bob's coupling to Alice from κ to κ_A. Let us see how Alice's power monitor can limit the extent to which Eve can increase κ_A. The analysis of this case is rather similar to that for Bob's power monitor, so we use the same notation, i.e., $N_{0,m}$ and

$N_{1,m}$ will be the number of photons arriving at Alice's power monitor in the mth mode without and with, respectively, Eve's changing the Alice-to-Bob transmittivity to κ_B and the Bob-to-Alice transmittivity to κ_A. As in the case for Bob's power monitor, the M modes that Alice receives are in a product state, therefore, the $\{N_{0,m}\}$ and the $\{N_{1,m}\}$ are sets of statistically independent, identically distributed random variables. The relevant expectation values and variances are now

$$\langle N_{0,m}\rangle = \frac{1}{100}\left[G_B\kappa^2 N_S + \kappa N_B\right], \tag{4.10}$$

$$\langle N_{1,m}\rangle = \frac{1}{100}\left[G_B\kappa_A\kappa_B N_S + G_B\kappa_A(1-\kappa_B)N_E + \kappa_A N_B\right], \tag{4.11}$$

$$\left\langle \Delta N_{0,m}^2\right\rangle = \langle \mathrm{N}_{0,m}\rangle\left(\langle \mathrm{N}_{0,m}\rangle + 1\right) \approx \langle \mathrm{N}_{0,m}\rangle^2 \approx \left(\frac{\kappa N_B}{100}\right)^2 \tag{4.12}$$

and

$$\left\langle \Delta N_{1,m}^2\right\rangle = \langle \mathrm{N}_{1,m}\rangle\left(\langle \mathrm{N}_{1,m}\rangle + 1\right) \approx \langle \mathrm{N}_{1,m}\rangle^2 \approx \left(\frac{\kappa_A N_B}{100}\right)^2, \tag{4.13}$$

where Alice has used 1% of her received light for power monitoring, and the approximations follow because the background noise is high-brightness light, whereas the SPDC sources are low-brightness light, so that we have $\langle N_{0,m}\rangle \approx \kappa N_B/100 \gg 1$ and $\langle N_{1,m}\rangle \approx \kappa_A N_B/100 \gg 1$.

Alice's power monitor measures $N_0 = \sum_{m=1}^{M} N_{0,m}$ if Eve does not change κ to κ_A on the Bob-to-Alice path and $N_1 = \sum_{m=1}^{M} N_{1,m}$ if she does. Again invoking the Central Limit Theorem, we approximate the statistics of these random variables as Gaussian, because $M \gg 1$. Their expectation values are

$$\begin{aligned}\langle N_0\rangle &= \frac{M}{100}\left[G_B\kappa\kappa_B N_S + G_B\kappa(1-\kappa_B)N_E + \kappa N_B\right] \approx \frac{M\kappa N_B}{100}\\ \langle N_1\rangle &= \frac{M}{100}\left[G_B\kappa_A\kappa_B N_S + G_B\kappa_A(1-\kappa_B)N_E + \kappa_A N_B\right] \approx \frac{M\kappa_A N_B}{100},\end{aligned} \tag{4.14}$$

and their variances are

$$\begin{aligned}\left\langle \Delta N_0^2 \right\rangle &= M \left\langle \mathrm{N}_{0,m} \right\rangle^2 \approx M \left(\frac{\kappa N_B}{100} \right)^2 \\ \left\langle \Delta N_1^2 \right\rangle &= M \left\langle \mathrm{N}_{1,m} \right\rangle^2 \approx M \left(\frac{\kappa_A N_B}{100} \right)^2 .\end{aligned} \tag{4.15}$$

When Alice makes a minimum error probability decision about that channel modification, based on the observation from her power monitor, under the assumption that Eve is equally likely to leave κ alone or change κ to κ_A, her error probability is

$$P_{e,A} = Q\left(\frac{\langle N_1 \rangle - \langle N_0 \rangle}{\sqrt{\langle \Delta N_1^2 \rangle} + \sqrt{\langle \Delta N_0^2 \rangle}} \right) = Q\left(\sqrt{M} \frac{\kappa_A - \kappa}{\kappa_A + \kappa} \right). \tag{4.16}$$

To detect the channel modification with an error probability less than 10^{-6} for a 0.1% κ_A variation, Alice needs to monitor the power on a total of 9×10^7 modes, which takes approximately 90 μs for an SPDC source with 1 THz phase-matching bandwidth.

We have just seen that Alice's power monitor can readily detect any appreciable modification Eve might make to the transmissibility of the Bob-to-Alice channel. It turns out, however, that Eve has no real motivation to make any such modification. In particular, the error probability bound for Alice's optimum quantum receiver, when Eve leaves the transmissivity of the Alice-to-Bob and Bob-to-Alice channel unchanged is, from (3.14),

$$\Pr(e)_{\text{Alice}} \leqslant \frac{1}{2} e^{-4M\kappa G_B N_S / N_B}, \tag{4.17}$$

whereas it becomes

$$\Pr(e)_{\text{Alice}} \leqslant \frac{1}{2} e^{-4M\kappa_B G_B N_S / N_B} \tag{4.18}$$

when she changes the Alice-to-Bob transmissivity to $\kappa_B < \kappa$, to preclude Bob's detecting her intrusion with his power monitor, and she changes the Bob-to-Alice transmissivity to $\kappa_A > \kappa$ in the hope of keeping Alice's error probability unaffected by her attack. Because Alice's error probability does not depend on κ_A, Eve's attack, in this case, is exposed to two monitors, Alice's power monitor and Alice's BER

monitor. Our next step is to examine the effectiveness of Alice's BER monitor.

4.3 Active case III: Eve Injects Light Undetectable by Power Monitoring

Suppose that Eve decides to attack in a manner that cannot be detected by Alice and Bob's power monitors. Specifically, she reduces κ to κ_B on the Alice-to-Bob channel and injects N_E satisfying $\kappa_B N_S + (1 - \kappa_B)N_E = \kappa N_S$, thus defeating Bob's power monitor. She does not modify the Bob-to-Alice transmittivity from its κ value, thus defeating Alice's power monitor. So, if Alice and Bob make no attempt to monitor the physical integrity of the propagation channels, they must rely on Alice's BER monitor to detect Eve's presence. Bit errors form a Bernoulli process, Let $E_{0,k}$ and $E_{1,k}$ be 0 for a correct reception and 1 for an erroneous reception of Bob's kth bit without $(E_{0,k})$ and with $(E_{1,k})$ Eve's active attack. Since each bit Bob sends is statistically independent and identically distributed, the $\{E_{0,k}\}$ are statistically independent and identically distributed random variables, and the $\{E_{1,k}\}$ are too. The mean values of $E_{0,k}$ and $E_{1,k}$ are Alice's error probability in the absence and presence of Eve's attack. Moreover, the variances of $E_{0,k}$ and $E_{1,k}$ are

$$\begin{aligned} \langle \Delta E_{0,k}^2 \rangle &= \langle E_{0,k} \rangle (1 - \langle E_{0,k} \rangle) \\ \langle \Delta E_{1,k}^2 \rangle &= \langle E_{1,k} \rangle (1 - \langle E_{1,k} \rangle) \end{aligned} . \tag{4.19}$$

So we have

$$\begin{aligned} \langle \Delta E_{0,k}^2 \rangle &\approx \langle E_{0,k} \rangle \\ \langle \Delta E_{1,k}^2 \rangle &\approx \langle E_{1,k} \rangle \end{aligned} , \tag{4.20}$$

when Alice's error probability is low.

Alice's BER monitor measures $E_0 = \frac{1}{K} \sum_{k=1}^{K} E_{0,k}$ if Eve does not attack the channel and $E_0 = \frac{1}{K} \sum_{k=1}^{K} E_{1,k}$ if she does. Again using the Central Limit Theorem, we approximate the statistics of these random variables as Gaussian, because we will take $K \gg 1$. Assume that Eve is equally likely to attack or not attack, and that Alice

makes a minimum error probability decision about her absence or presence based on the her BER monitor's output. The error probability she will get is then

$$P_{e,BER} = Q\left(\sqrt{K}\frac{\langle E_{1,k}\rangle - \langle E_{0,k}\rangle}{\sqrt{\langle E_{1,k}\rangle} + \sqrt{\langle E_{0,k}\rangle}}\right). \tag{4.21}$$

To detect the attack with error probability less than 10^{-6} for 60% BER variation, which corresponds to 5% κ_B variation for $N_S = 0.004$, $\kappa = 0.1$, and $G_B = N_B = 10^4$ with the OPA receiver, Alice needs to continuously monitor the bit errors for 4×10^8 bits in order to achieve this goal. At 50 Mbit/s, such BER monitoring will take 8 sec, which is far longer than the times needed to detect Eve's intrusion when her presence was detectable by Alice and Bob's power monitors. Thus we need to examine ways to make Eve more detectable by Alice's BER monitor. To do so, we will later back away from some of the extravagant capabilities that, thus far, we have assumed Eve possesses. Before doing that, however, let us complete our treatment of the omnipotent Eve by explaining the performance of Bob-to-Alice communication and Bob-to-Eve eavesdropping when Eve is limited to reducing κ on the Alice-to-Bob path to a value satisfying $\kappa \geq \kappa_B \geq 0.95\kappa$ while operating in the manner that precludes her being detected by Alice and Bob's power monitors.

Under the preceding conditions, we have that

$$\kappa N_S = \kappa_B N_S + (1 - \kappa_B) N_E \tag{4.22}$$

so that

$$N_E = \frac{N_S}{181} \tag{4.23}$$

when $\kappa = 0.1$, and $\kappa_B = 0.95\kappa$.

Her corresponding Wigner-distribution covariance matrix for $\hat{c}_R$ and $\hat{c}_I$ is

$$\Lambda^{(k)}_{C_R C_I} = \frac{1}{4}\begin{bmatrix} A & 0 & (-1)^k C & 0 \\ 0 & A & 0 & (-1)^{k+1} C \\ (-1)^k C & 0 & S & 0 \\ 0 & (-1)^{k+1} C & 0 & S \end{bmatrix}, \tag{4.24}$$

where $A \equiv 1 + 2N_B(1-\kappa) + 2G_B(1-\kappa)(N_E(1-\kappa_B) + N_S\kappa_B)$, $S \equiv 1 + 2N_E$, and $C \equiv 2\sqrt{G_B N_E(1+N_E)(1-\kappa_B)(1-\kappa)}$. Furthermore, the Chernoff upper bound for Eve's optimum quantum receiver is

$$\Pr(e)_{Eve} \leq \frac{1}{2}\exp\left(-\frac{4MG_B N_E(1-\kappa_B)}{N_B}\right). \tag{4.25}$$

If, instead, Eve uses a gain $G_E = 1 + \frac{N_E}{\sqrt{(1-\kappa)N_B}}$ optical parametric amplifier, taking $\hat{c}_I$ as the signal input mode and $\hat{c}_R$ as the idler input mode, and then direct detects the information bit, then her error probability Bhattacharyya upper bound is

$$\Pr(e)_{Eve} \leq \frac{1}{2}\exp\left(-\frac{2MG_B N_E(1-\kappa_B)}{N_B}\right). \tag{4.26}$$

For $N_S = 4 \times 10^{-3}$, $N_E = 2.7 \times 10^{-5}$ and $G_B = N_B = 10^4$, we have plotted results for Alice and Eve's error probability versus the number of modes in Fig.4-1. The two dashed lines are error-probability upper bounds for Alice and Eve's OPA receivers, and the two dot-dashed lines are the corresponding lower bounds for these receivers. The solid lines in Fig.4-1 are error probabilities obtained from the Central Limit Theorem. We see from the error-probabilities approximations that when Alice achieves the error rate 10^{-5}, Eve's error probability is approximately 0.12.

Although the results in Fig.4-1 are promising, they rely on constraining Eve to $\kappa \geq \kappa_B \geq 0.95\kappa$, something which requires an unreasonably long-duration BER monitoring on Alice's part. This occurs because we have assumed that Eve collects all the photons from Bob that do not reach Alice. For both fiber-optic and free-optic implementation this assumption is very conservative. Optical time-domain reflectometers can certainly limit Eve's capability in this regard on a fiber link. Likewise, visual ob-

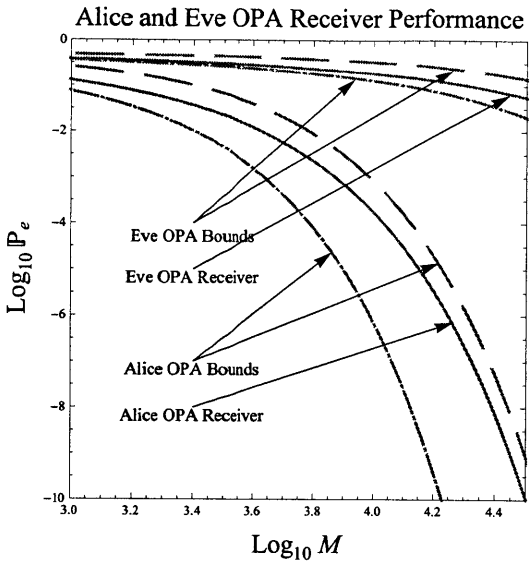

Figure 4-1: Alice and Eve's OPA Receiver Performance

servation of the propagation path, combined with fairly tight beam divergences can do the same thing over a line-of-sight terrestrial channel. So, to assess the degree to which Alice and Bob can be immune to active eavesdropping under more reasonable assumptions about Eve's photon-capture capability, consider Fig.4-2. Here, we show three beam splitters in the Alice-to-Bob and Bob-to-Alice paths with Eve only having access to one. The first beam splitter represents the loss from Alice to Eve, and the last beam splitter characterizes the loss from Eve to Bob. However, the middle beam splitter accounts for how much light Eve can get from these channels. We will assume that the overall effect of the three beam splitters on the light propagation from Alice to Bob is a pure loss κ, with the same being true for the Bob-to-Alice path. We shall also assume that Eve has the same κ transmittivity to and from Bob.

Fig. 4-3 plots the Central Limit Theorem approximation for the error probabilities of Alice's OPA receiver and Eve's active-attack OPA receiver. Also included is the lower bound on Eve's passive-attack optimum quantum receiver when she collects all the light from Alice that does not reach Bob and all the light from Bob that does not reach Alice. The parameter used in the computation are: $N_S = 4 \times 10^{-3}$, $N_E = 4 \times 10^{-4}$ $G_B = N_B = 10^4$, $W = 1\,\mathrm{THz}$, and $\kappa = 0.1$. From the figure we see that

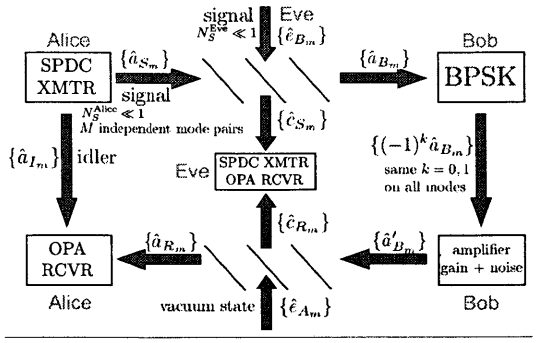

Figure 4-2: Schematic of realistic quantum-illumination two-way communication protocol with active-eavesdropper Eve using an SPDC source and an OPA receiver.

Alice can achieve an error probability below 10^{-3} at 150 Mbps data rate. This error probability is low enough that standard forward error-correction (FEC) techniques can be used to achieve reliable communication. However, at this same 150 Mbps data rate, the error probability of Eve's active-attack OPA receiver is 0.16, which means her receiver cannot benefit from the FEC algorithm. Note that the error-probability lower bound on Eve's passive attack with an optimum quantum receiver is 0.37 at the 150 Mbps data rate, even though she receives all the light that does not reach its intended destination. This shows how much more powerful Eve's active attack is in comparison with her passive attack.

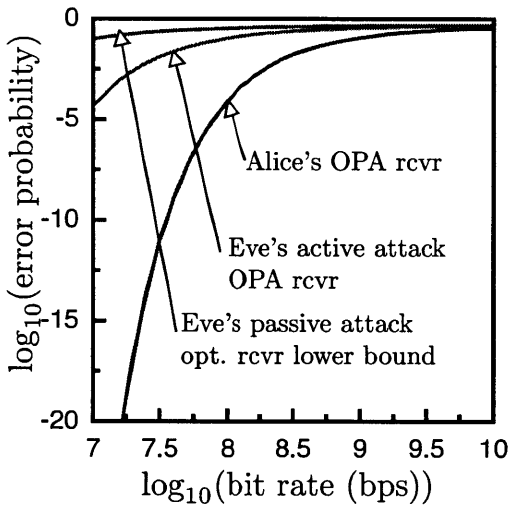

Figure 4-3: Error probability versus bit rate for Alice and Eve's OPA receivers. Lower bound on the error probability of Eve's optimum quantum receiver for passive eavesdropping is also included.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

In this thesis we have studied secure communication based on quantum illumination. It has been known for more than twenty years that quantum mechanics can enable two remote users to develop a shared secret key of random binary digits. Used as a one-time pad by these users, they can then communicate with complete immunity to eavesdropping. Called quantum key distribution, the protocols for creating the shared key rely on the no-cloning theorem for their security. This thesis, however, has addressed a very different quantum paradigm for secure communication, one that is based on the entanglement of the signal and idler beams from a spontaneous parametric downconverter (SPDC), rather than the no-cloning theorem. Moreover, quantum illumination aims for secure transmission of data, whereas quantum key distribution first creates a key that is then used for data communication.

Prior theoretical work on quantum illumination showed that Alice and Bob—the communication parties—could enjoy an enormous (approximate 6 orders of magnitude) advantage over a passive eavesdropper (Eve) in a 50 Mbit/s, 50-km-long idealized fiber communication link. However, that work did not evaluate the information rate advantage that Alice and Bob enjoy over the passive eavesdropping Eve. Thus, the first important accomplishment of this thesis was to show that Alice's Shannon information about Bob's message bit can exceed Eve's Holevo information about that

bit by more than 0.9 bits/channel use, confirming the security when Eve only listens to the communication between Alice and Bob. What is remarkable about the quantum illumination protocol is that although the loss and noise in the channel destroy the quantum entanglement between the signal beam and the idler beam, the correlation between the return beam and the idler beam still enables the secure communication between Alice and Bob under passive eavesdropping.

The quantum illumination protocol is vulnerable to the active eavesdropping, because Eve can gain the same entanglement advantage by injecting her own SPDC light into the channel. We have evaluated a series of techniques that Alice and Bob can use to reduce this vulnerability. These techniques limit the amount of SPDC light that Eve can inject without being detected. With these techniques we showed that Alice and Bob achieve an error probability advantage of about 4 order of magnitude in comparison to Eve, although this performance presumed Eve's capabilities—with respect to her channel coupling and her receiver technology—were more limited than we allowed for in the passive-eavesdropping analyses.

In addition to the preceding analyses of communication security, we made several, somewhat fruitless, attempts to improve on the basic binary-modulation, optical parametric amplifier (OPA) quantum-illumination protocol. Specifically, we found that dual-OPA reception offered a minimal error probability improvement in comparison with OPA reception, and that both beam-splitter and dual-heterodyne receivers had appreciably worse performance than the OPA receivers. Finally, one attempt to achieve increased data rate by going to quadrature phase-shift keying (QPSK) revealed an error probability that was worse than that for binary phase shift keying (BPSK).

5.2 Future Work

Currently, quantum-illumination based communication relies on the OPA receiver, whose BPSK error exponent is known to be 3 dB worse than that of the optimum quantum receiver. Thus the principal open theoretical problem is to find a way

to bridge that gap. A similar gap exists between the performance of conventional coherent (homodyne and heterodyne) detection of BPSK-modulated coherent-state light and that of the optimum quantum receiver (the Helstrom bound). The Kennedy receiver [29], which injects a local oscillator that converts BPSK into on-off keying (OOK) prior to direct detection, is known to be within a factor of two of the optimum quantum receiver's performance at low error probability. The Dolinar receiver [28], which augments the Kennedy receiver with feedback control of the local oscillator, exactly realizes the optimum quantum receiver. Thus, lessons drawn from this earlier work could help conceivably help in finding an improved, perhaps optimum, receiver for quantum illumination. There are, however, some significant challenges along that path, of which the most significant is that the Kennedy and Dolinar receivers work for pure-state hypotheses, whereas those for quantum illumination are mixed states.

Other receiver-related problems that could be addressed arise because the OPA receiver requires phase knowledge, i.e., the quantum illumination communication protocol involves an interferometric measurement. How to acquire the necessary phase information may be considered in future work. It is possible that differential phase-shift keying will be a valuable approach in this regard.

Another problem area for consideration is the use of quantum-illumination based communication over a line-of-sight path through the atmosphere. Here there will be spatial-mode effects and turbulence-induced fading to contend with, but visual monitoring of the path from Alice and Bob's terminal may provide a strong limit on Eve's ability to do active eavesdropping.

Bibliography

[1] Shannon, C. E., The mathematical theory of communications, Bell System Tech **27**, 379-423, 623-656 (1948).

[2] Shannon, C. E., Communication theory of secrecy systems, Bell System Tech **28(4)**, 656-715, (1949).

[3] Buzek, V. and Hillery, M., Physics World 14 (11) (2001)

[4] Bennett, C. H. and Brassard, G., *Proc of IEEE International Conf on Computers, Systems, and Signal Processing*, Bangalore, India, 1984 IEEE, New York, 1984, p. 175.

[5] Guha, S. and Erkmen, B. I., Gaussian-state quantum-illumination receivers for target detection, Phys. Rev. A **80**, 052310 (2009)

[6] Shapiro, J. H., Defeating passive eavesdropping with quantum illumination, Phys. Rev. A **80**, 022320 (2009)

[7] Shapiro, J. H., Quantum Optical Communication Lecture Notes, Lecture 17 (2008) http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-453-quantum-optical-communication-fall-2008/

[8] Kong, J. A., Electromagnetic Wave Theory, EMW Puslishing, Cambridge (2008)

[9] Orfanidis, S. J., Electromagnetic Waves and Antennas, Rutgers University, Piscataway (2008)

[10] Gum, B. S. and Hiziroglu, H. R., Electromagnetic Field Theory Fundamentals, PWS Publishing, Boston, (1998)

[11] Shapiro, J. H., Quantum Optical Communication Lecture Notes, Lecture 04 (2008) http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-453-quantum-optical-communication-fall-2008/

[12] Gerry, C. C. and Knight, P. L., Introductory Quantum Optics, Cambridge University Press, Cambridge (2005)

[13] Glauber, R. J., The quantum theory of optical coherence, Phys. Rev. (1963)

[14] Walls, D. F. and Milburn, G. J., Quantum Optics, Springer, Berlin (1998)

[15] Shapiro, J. H., Quantum Optical Communication Problem Set 03 (2008) http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-453-quantum-optical-communication-fall-2008/

[16] Shapiro, J. H., Quantum Optical Communication Lecture Notes, Lecture 09 (2008) http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-453-quantum-optical-communication-fall-2008/

[17] Mandel, L. and Wolf, L., Optical Coherence and Quantum Optics, Cambridge University Press, Cambridge (1995)

[18] Garrison, J. C. and Chiao, R. Y., Quantum Optics, Oxford University Press, New York (2008)

[19] Orszag, M., Quantum Optics, Springer, Berlin (1998)

[20] Vogel, W., and Welsch, D. G., Quantum Optics, John Wiley, New York (2006)

[21] Mori, S. and Soderholm, J., On the distribution of 1550-nm photon pairs efficiently generated using a periodically poled lithium niobate waveguide, arXiv:quant-ph/0509186 (2005)

[22] Shapiro, J. H., Quantum Optical Communication Lecture Notes, Lecture 13 (2008) http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-453-quantum-optical-communication-fall-2008/

[23] Audenaert, K.M.R., Calsamiglia, J., Masanes, Ll., Munoz-Tapia, R., Acin, A., Bagan, E., and Verstraete, F., The quantum Chernoff bound, Phys. Rev. A **77,** 032311 (2008)

[24] Helstrom, C. W., Quantum Detection and Estimation Theory, Academic Press, New York (1976)

[25] Pirandola, S. and Lloyd, S., Computable bounds for the discrimination of Gaussian states, Phys. Rev. A **78**, 012331 (2008)

[26] Wilde, M. M., From classical to quantum Shannon theory, arXiv:quant-ph/1106.1445v2

[27] Holevo, A. S., Sohma, M., and Hirota, O., Capacity of quantum Gaussian channels, Phys. Rev. A **59** 1820 (1999)

[28] Dolinar, S. J., An optimum receiver for the binary coherent state quantum channel, Res. Lab Electron., MIT, Quarterly Progress Rep. **111**, pp. 115-120 (1973)

[29] Kennedy, R. S., A near-optimum receiver for the binary coherent state quantum channel, Res. Lab Electron., MIT, Quarterly Progress Report, **108**, pp. 219-225, (1973)