

UNIVERSITY OF CALGARY

Entanglement Swapping with
Imperfect Sources and Detectors

by

Regina B. Howard

A DISSERTATION

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF Master of Science

DEPARTMENT OF PHYSICS AND ASTRONOMY
INSTITUTE FOR QUANTUM INFORMATION SCIENCE

CALGARY, ALBERTA

November, 2009

© Regina B. Howard 2009

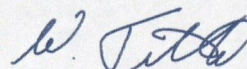
UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

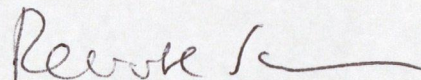
The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a Dissertation entitled "Entanglement Swapping with Imperfect Sources and Detectors" submitted by Gina Howard in partial fulfillment of the requirements for the degree of Master of Science.



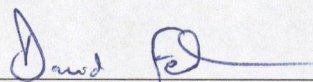
Dr. Barry C. Sanders
Department of Physics and Astronomy



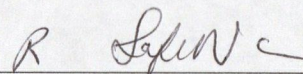
Dr. Wolfgang Tittel
Department of Physics and Astronomy



Dr. Renate Scheidler
Department of Mathematics and Statistics



Dr. David Feder
Department of Physics and Astronomy



Dr. Reihaneh Safavi-Naeini
Department of Computer Science

2 Nov 2009

Date

Abstract

In an effort to overcome the distance limits of quantum key distribution (QKD), entanglement swapping is used as a fundamental building block in quantum relays and quantum repeaters. Although entanglement swapping enables any distance to be achieved in principle, experimental realization suffers from imperfect sources of entangled pairs and detectors.

Here, I incorporate the multi-photon nature of the source and imperfect detectors into a model of entanglement swapping. Specifically, I calculate the resultant entangled state given two parametric down conversion (PDC) sources where one mode of each PDC source meets at a beam splitter and is subjected to photon counting by inefficient detectors. I then calculate the entanglement fidelity of this resultant state.

In addition, detectors used in quantum optical experiments occasionally produce dark counts and do not always detect incoming photons. These imperfections need to be taken into account when performing calculations involving such detectors. I have developed a thermal detector model that predicts the click probability for an inefficient detector subject to dark counts.

Acknowledgements

I thank my supervisor Dr. Barry Sanders and my co-supervisor Dr. Wolfgang Tittel for their many suggestions and gentle prodding during this research.

I thank all the members of the Institute for Quantum Information Science at the University of Calgary for their camaraderie and helpful discussions. In particular, I thank Artur Scherer for his reviews and challenges of this work.

I am ever grateful to my husband Todd Howard for his support and understanding throughout the arduous process of my becoming a Master of Science.

I thank the Informatics Circle of Research Excellence, the Canadian Institute for Advanced Research, the Mathematics of Information Technology and Complex Systems research network, and General Dynamics Canada for their financial support during my time as a student.

Table of Contents

Approval Page	ii
Abstract	iii
Acknowledgements	iv
Table of Contents	v
List of Figures	v
Glossary	viii
1 Introduction	1
1.1 Motivation	1
1.2 Background	3
1.2.1 Spontaneous Parametric Down-conversion	4
1.2.2 The problem of distance	5
1.2.3 Limits of Detection	7
1.3 Summary	9
2 Detector Model	10
2.1 Experimentally Motivated Detector Model	11
2.2 Thermal Detector Model	12
2.3 Summary	24
3 Entanglement Swapping With Perfect Two-Photon Sources	27
3.1 Ideal Source Entanglement Swap	28
3.2 Summary	30
4 Entanglement Swapping With Imperfect Two Photon Sources	32
4.1 Multi-photon Sources	32
4.2 Summary	43
5 Conclusions and Outlook	44
5.1 Closed Form Solution	45
5.2 Incorporating Dark Counts	46
5.3 Effect on Key Rate	47
5.4 Summary	48
Bibliography	49

List of Figures

2.1	Imperfect detector (D) with efficiency η and dark counts provided by the thermal state at mode b . The input state I is inserted at mode a . The perfect detector is a unit efficiency photo-detector.	13
2.2	The probability of a dark count d for various detector efficiencies η over the full range in intensity of the thermal mode q	17
2.3	Imperfect detector with efficiency η , a coherent state input and dark counts provided by the thermal mode. The perfect detector has m photons incident on it, and n photons are absorbed or lost.	18
2.4	Click probabilities P for the experimentally motivated model P_E and the thermal model P_T for dark count probabilities d , detector efficiency η , and mean number of photons in the source mode \bar{n}_s	24
2.5	Click probabilities P for the experimentally motivated model P_E and the thermal model P_T for dark count probabilities d , detector efficiency η , and mean number of photons in the source mode \bar{n}_s	25
2.6	Click probabilities P for the experimentally motivated model P_E and the thermal model P_T for dark count probabilities d , detector efficiency η , and mean number of photons in the source mode \bar{n}_s	26
2.7	Click probabilities P for the experimentally motivated model P_E and the thermal model P_T for dark count probabilities d , detector efficiency η , and mean number of photons in the source mode \bar{n}_s	26
3.1	Entanglement swapping with two parametric down conversion sources (PDCs). One mode of each entangled pair source meets at a balanced beam splitter (B). Its outputs denoted by c' and b' are directed to polarizing beam splitters (PBS) and then detected at four detectors: one for the H and one for the V polarizations of each of the c' and b' modes. The readout of the detectors is denoted ($qrst$) with q the number of photons detected in mode c'_H , r the number of photons detected in mode c'_V , s the number of photons detected in mode b'_V and t the number of photons detected in mode b'_H . The ordering of modes in $qrst$ is dictated by the behavior of the polarizing beam splitter, which allows the horizontal polarization to transmit and reflects the vertical polarization.	28
3.2	The full entanglement swapping operation shows a Bell measurement on modes b' and c' followed by detection of the a and d modes. The polarization rotators (PR) allow for the observation of certain four-fold coincidences for different rotation angles. The four-fold coincidence rates in turn determine the visibility and hence the fidelity of the entanglement swapping operation.	31
4.1	Fidelity (F) of entanglement swapping for ρ_{1010} against the source strength χ	43

5.1	Visibility of entanglement swap against the source efficiency χ with a variety of detector efficiencies and dark count rates ranging from 1×10^{-5} to 3×10^{-5}	47
-----	---	----

Glossary

APD: Avalance photo-diode

BB84: Bennett & Brassard 1984 protocol

BBM92: Bennett, Brassard & Mermin 1992 protocol

PDC: Parametric down conversion

QBER: Quantum bit error rate

QKD: Quantum key distribution

Chapter 1

Introduction

Long distance quantum communication technology may one day enable secure communication around the globe. Quantum relays and the entanglement swapping operations they employ can extend the reach of quantum optical communication toward that goal. This thesis is motivated by the desire to design quantum key distribution experiments for maximum secure key generation rate. The design of experiments must incorporate the imperfect photon sources and imperfect detectors available for quantum key distribution (QKD) deployment today. In this thesis I explore the limiting effects of imperfect sources and detectors on entanglement swapping. I extend a previous challenge to the security of quantum key distribution protocols using imperfect sources in quantum relay systems [1].

1.1 Motivation

A number of research labs around the world are busy developing the worlds first quantum computers. Such computers will have the capability to factor large numbers in a short amount of time. Most classic cryptographic systems in use today, such as the RSA (Ron Rivest, Adi Shamir, and Leonard Adleman, 1977) public-key algorithm, rely on the fact that it is difficult for classical computers to factor large numbers. When the first quantum computers come into use, or a new algorithm for factoring numbers is developed for classical computers, this type of cryptographic system will be broken and our transmitted and stored information will no longer be secure.

The two basic types of cryptographic systems are symmetric or private key systems,

and asymmetric or public key systems [2]. In symmetric key systems, such as the Advanced Encryption Standard (AES) cipher, the sender and receiver of the message are required to have the same key available to them. It is used for both the encryption and the decryption process. The main problem with this type of system is the distribution of the key to the two parties who wish to communicate.

In asymmetric cryptographic algorithms such as RSA, each party has a public key and a private key. Messages are encrypted with the public key and decrypted with the private key. The public key does not need to be secret, but can be given to whomever would like to communicate with you. You keep your private key secret. To send a message to Bob, Alice finds and verifies Bob's public key, encrypts her message with it and sends it to Bob. Bob then uses his private key to decrypt the message. Asymmetric cryptographic systems are more flexible since they don't require the preliminary exchange of a secret key between Alice and Bob for their secret communication. However, the distribution of the private keys to Alice and Bob by an established public key authority remains. Asymmetric key systems are slower and the keys are larger than in symmetric key systems [2].

The only provably secure cryptosystem is the Vernam cypher, or one-time pad, which is a symmetric key algorithm. This algorithm requires as much key material as information to be encrypted. The problem of distributing the symmetric key securely for such a system is one that quantum key distribution addresses [3].

We rely on secure communication in many facets of our lives, from online banking to trusting medical institutions with our most private information. Not only do we want current communication with our bank to be secure, we want our sensitive medical information to remain secure for years to come. We do not want someone who intercepts

encrypted information today to be able to decode it next year. The need to secure information over many years makes quantum cryptography a desirable application to pursue now, in advance of a quantum computer capable of factoring numbers efficiently.

1.2 Background

The first applications considered for the century old field of quantum mechanics center around security and cryptography. In the late 1960s, Wiesner proposed a method of securing money from counterfeiting using the laws of quantum mechanics, specifically the uncertainty principle. This work, known as “Quantum Money”, was not published until 1983 [4]. At that point it gave rise to the subsequent quantum key distribution idea upon which much of the current work in quantum communication is based.

The first proposal for quantum key distribution came from Brassard and Bennett in 1984 [5]. The protocol is known as BB84, and is based on the idea of conjugate coding put forth by Wiesner. BB84 is still the most widely used protocol in QKD experiments. In 1996, Mayers provided the first proof of the information-theoretic security of the BB84 protocol. A further proof was provided by Lo and Chau in 1998, and a relatively simple proof in 2000 by Shor and Preskill [6] based on entanglement distillation seemed to satisfy everyone as to the security of BB84. These proofs considered the theoretic ideal of the protocol without consideration for the imperfections present in implementations.

The main components of quantum key distribution are: a source of photons, single photons or entangled pairs of single photons, a transmission medium such as fibre or free space, and detectors. Each have their own imperfections, which cause the overall scheme to fall short of its theoretical capability in terms of the rate at which it can create secure

key material for secure communication.

1.2.1 Spontaneous Parametric Down-conversion

In 1970, Burnham and Weinberg [7] demonstrated spontaneous parametric down conversion (SPDC) as a way to create an entangled photon pair. Such a pair can be used as a single photon source by detecting one photon of the pair, and then knowing that its partner was created at the same time.

In 1991, Ekert proposed a method of secure communication based on Bell's theorem, utilizing the quantum mechanical fundamental property of entanglement [8]. He considers a source that emits pairs of spin- $\frac{1}{2}$ particles in a singlet state ($|\psi^-\rangle$). The two particles fly off to Alice and Bob where they are detected by analyzers aligned randomly in either of two orthogonal bases. Each measurement results in a spin up or spin down outcome. After Alice and Bob reveal which basis they measured in and keep only those where they both measured in the one, they have a set of correlated bits. These bits can then be used as a key for symmetric key secret communication.

Subsequently in 1992, Bennett, Brassard and Mermin proposed a protocol known as BBM92 [9], which uses entangled pairs of photons to allow Alice and Bob to similarly collect a sequence of highly correlated qubits from which they can distill a secret key. This is the protocol I consider in my motivation for this thesis.

All methods currently available for photon generation, especially at the higher rates desirable for QKD, have a non-zero probability of creating pulses containing more than one photon. The possibility of a multi-photon pulse rather than a perfect single photon

is not only evident in attenuated laser sources such as those used for BB84, but also in pair sources such as parametric down conversion. Parametric down conversion (PDC) is achieved by pumping a laser field into a crystal with a $\chi^{(2)}$ nonlinearity [10]. Photons passing through the crystal can decay into a pair of identical or non-identical photons. Photon pairs created with the same polarization are the ones I consider.

Multi-photon emissions from the source must be taken into account when analyzing entanglement swapping. When multi-photon events occur, it is possible that one of the two photons involved in the swap is actually from a different pair and the entanglement required for a successful swap is absent altogether. This type of occurrence leads to errors in entanglement swapping and limits fidelity of an extended swapping operation.

1.2.2 The problem of distance

Photons carry information at the speed of light through free space or down a fibre optic cable, but they are easily absorbed and thus lost along the way. Loss of photons during transmission is easily accounted for with a simple factor on the transmission success probability

$$t = 10^{-l\beta/10}, \quad (1.1)$$

where t is the transmission coefficient or probability of successful transmission, l is the distance traveled and β is the loss coefficient of the transmission medium in units of dB [1]. The issue then is how to extend the reach of photons as information carriers. In a typical fibre optic cable $\beta = 0.25\text{dB km}^{-1}$ for 1550nm light, which gives us a range of less than 100km. Loss in fibre is wavelength dependent because it is due to Rayleigh backscattering, the scattering of light by particles much smaller than the wavelength of the light. For distances larger than 100km, the probability that the photon would arrive

at the detector becomes smaller than the probability of a dark count at that detector. At that point it is no longer possible to communicate as the noise of the communication (the dark counts) is greater than the signal.

In 1998, Briegel et al. considered a quantum repeater based on entanglement purification to extend the reach of entangled pairs of photons [11]. The distance to be covered is broken into segments and entanglement is distributed to the ends of each segment. Entanglement purification [12] is performed, and Bell measurements are carried out to swap the entanglement to the outer ends of the chain. Such a quantum repeater requires quantum memory to store the results of the intermediate entanglement swapping operations.

To avoid the need for quantum memory, the idea of a quantum relay has been explored by a number of groups including Collins et al. in 2005 [13]. The distance to be covered is again broken into segments and entanglement is swapped at Bell measurement nodes until the two end nodes share entanglement. In the absence of quantum memory, all of the entanglement swapping operations must succeed at the same time. This represents a large scale coincidence requirement that may take many tries. Each time one of the Bell measurements carrying out the entangling operation fails, the entire string of operations must be restarted. This inefficiency reduces the number of times entanglement is successfully distributed to the end nodes and thus the rate at which operations can be performed using the entanglement as a commodity. An entanglement-based QKD protocol, such as BBM92 for example, can be used to distill a key between two distant endpoints without a single photon having to cover the entire distance. The low probability of success in a long relay however, limits the bit rate possible for such a scheme.

1.2.3 Limits of Detection

In addition to the multi-photon nature of the probabilistic PDC sources, errors are also introduced into entanglement swapping by imperfect detectors. Here I study the limits of entanglement swapping due to detector limitations.

Generating entanglement swapping at rates useful for quantum key distribution relies on fast and accurate detection of single photons. Characteristics of detectors that limit its usefulness for QKD are low efficiency, high dark counts, significant time jitter and high dead times. As well, if the detectors only operate at cryogenic temperatures, their use may be limited [14].

An ideal single photon detector would be a photon-number discriminating detector. Such a detector would click when a single photon is incident and it would be able to indicate how many photons were incident during a given detection event. In contrast, single photon detectors today click when at least one single photon strikes their detection surface. They cannot discriminate whether one, two or more photons hit the detector during that one detection window. Such detectors are referred to as threshold detectors [15].

Detectors are also imperfect in that sometimes a single photon will not trigger a detection event. A detector's efficiency η represents the probability that it will click when a photon impacts it.

An additional characteristic of a detector is its dead time, referring to the time required for the detector to become ready to detect again after firing. If the detector is not ready to receive a new photon from a previous event, it will miss detecting the current incident photon. The lower the dead time, the higher the repetition rate and the greater the

communication rate supportable by the detector [14]. Although I do not consider dead time in my calculations, I note that larger dead times will reduce the overall rate at which entanglement can be swapped between two end nodes.

Detectors will sometimes register a click when no source photon was incident upon it. These events are known as dark counts and represent the noise of the detector. A detector's dark count rate d represents the probability per time slot that a detector will register a click when no source photon struck it. It may be that a spurious photon (a photon that enters the detector but was not an intended signal photon) triggered the event, or it may be that an echo cascade occurred in the detector from a previous event. In either case, such a detection count is erroneous from the point of view of counting only photons incident from the source. In this thesis I develop a model for a detector that incorporates dark counts. I do not utilize this model in the entanglement swapping calculations that follow.

For use with time sensitive applications such as entanglement swapping, a detector must also have a small time jitter [14]. Time jitter refers to the time it takes for the detector to signal a click after receiving a photon. This time difference must be as small as possible to accurately coordinate expected and actual arrival times of photons. I do not consider time jitter in my calculations.

Avalanche photodiodes (APD) are semiconductor-based photon detectors that can efficiently detect single photons at close-to-room temperature and are thus a good choice for QKD [14]. They use a strong electric field to accelerate the electrons flowing in the semiconductor. Different semiconductor material is used for detecting different wavelengths to optimize this effect. When a single photon hits the detector, an avalanche of

electrons is generated that readily triggers a signal or “click”, indicating the arrival of the photon.

A popular detector in experiments today is an InGaAs (Indium Gallium Arsenide) avalanche photo-diode (APD) [16]. This detector operates well for 1550nm light, which is the standard for fibre optic cable transmission. It has around 10% efficiency η , a 10^{-5} probability of a dark count per nanosecond gate, a 10MHz repetition rate and 500ps jitter [17]. I consider this kind of detector in my calculations.

1.3 Summary

Motivated by the desire for long distance quantum communication, I consider the necessary components of sources of entanglement, detectors and entanglement swapping operations. The imperfect devices we have available for experimentation today will reduce the fidelity of entanglement between the end nodes of a quantum relay. I focus on the entanglement swapping operation in this thesis. However, I first present a detector model that enables the determination of dark count probability for an arbitrary coherent source.

Chapter 2

Detector Model

The InGaAs APD detectors currently used in experiments are threshold detectors. This means that they indicate a photon detection if one or more photons impact the detection area. The detector cannot distinguish between one, two or more photons striking its detection surface. Additionally, the detector has an efficiency in that it does not always click when a photon impacts the detection area. This efficiency can be measured experimentally and associated with the detector in subsequent calculations.

Current APDs also exhibit dark counts, which are detection events that were not triggered by incoming source photons. The dark count probability or background rate of a detector can be measured before that detector is incorporated into an experiment so that the effect of these events can be taken into account. Such characterization has to be performed on every detector employed in the experiment for accurate overall compensation of the effect.

Here I model such an imperfect detector by adding a beam splitter in front of a theoretical perfect detector. This beam splitter causes the interference of the coherent input signal state with a thermal state, representing the dark counts and the random errors that occur. The detection probabilities produced by this theoretical model of an imperfect detector agree with those derived from an experimentally motivated model while providing a useful generalization.

2.1 Experimentally Motivated Detector Model

I begin by developing an experimentally motivated model of a detector by logical progression of detection considerations. This model forms a comparison point for my subsequent thermal detector model for the pulsed coherent source used to construct it.

The probability that no click is registered due to n photons incident on a detector with efficiency η is given by $(1 - \eta)^n$. The probability of a click due to n photons is then given by

$$p_n = 1 - (1 - \eta)^n. \quad (2.1)$$

If we consider the possibility of dark counts, then the experimentally motivated probability to get a click, given n photons are incident on the detector, is

$$\begin{aligned} P_E &= p_n(1 - d) + (1 - p_n)d + p_nd \\ &= p_n(1 - d) + d, \end{aligned} \quad (2.2)$$

where d is the probability of a dark count.

The number of photons per pulse from a chopped continuous wave laser is given by the Poisson distribution [18]. If the mean number of photons in the source distribution is \bar{n}_s the probability to get a click in the detector due to source photons or dark counts

is given by

$$\begin{aligned}
P_E &= \sum_{n=0}^{\infty} \frac{\bar{n}_s^n e^{-\bar{n}_s}}{n!} \left((1 - (1 - \eta)^n) (1 - d) + d \right) \\
&= e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left((1 - (1 - \eta)^n) (1 - d) \frac{\bar{n}_s^n}{n!} \right) + e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left(d \frac{\bar{n}_s^n}{n!} \right) \\
&= e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left(\frac{\bar{n}_s^n}{n!} \right) - e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left((1 - \eta)^n \frac{\bar{n}_s^n}{n!} \right) + e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left(d \frac{\bar{n}_s^n}{n!} \right) \\
&\quad + e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left(d (1 - \eta)^n \frac{\bar{n}_s^n}{n!} \right) + e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left(d \frac{\bar{n}_s^n}{n!} \right) \\
&= e^{-\bar{n}_s} e^{\bar{n}_s} - e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left((1 - \eta)^n \frac{\bar{n}_s^n}{n!} \right) + e^{-\bar{n}_s} d \sum_{n=0}^{\infty} \left((1 - \eta)^n \frac{\bar{n}_s^n}{n!} \right) \\
&= 1 + (d - 1) e^{-\bar{n}_s} \sum_{n=0}^{\infty} \left((1 - \eta)^n \frac{\bar{n}_s^n}{n!} \right) \\
&= 1 + (d - 1) e^{-\bar{n}_s} e^{(1-\eta)\bar{n}_s} \\
&= 1 + (d - 1) e^{-\eta\bar{n}_s}.
\end{aligned} \tag{2.3}$$

Let us now see how this expression differs in the thermal detector model.

2.2 Thermal Detector Model

I now develop a model for imperfect detectors that incorporates multi-photon pulses from the source and dark count contributions based on a thermal distribution of photons. Other derivations of similar models are explored in [19] and [20]. Although the derivation is different, the models are the same in that they use a thermal mode to represent the dark counts of the detector.

To develop the model, I begin by determining the detector efficiency η . Blocking the thermal mode (mode b) and sending exactly one photon into the input mode (mode a)

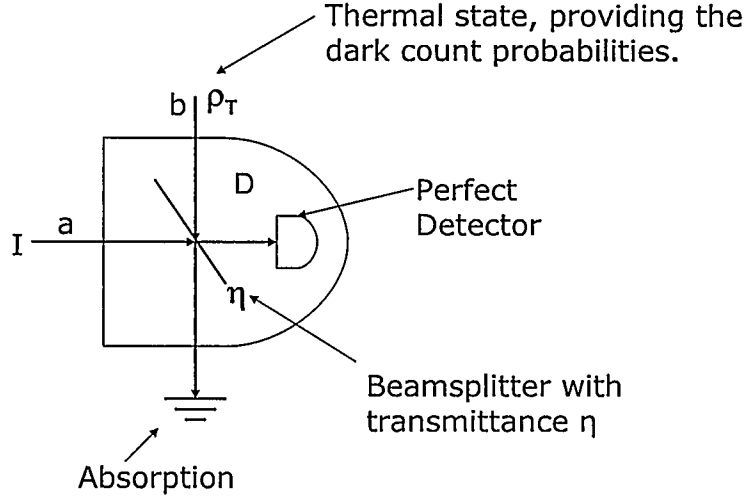


Figure 2.1: Imperfect detector (D) with efficiency η and dark counts provided by the thermal state at mode b . The input state I is inserted at mode a . The perfect detector is a unit efficiency photo-detector.

will allow this determination:

$$|1\rangle_a |0\rangle_b = \hat{a}^\dagger |vac\rangle. \quad (2.4)$$

The beam splitter represents a linear optical transformation of the input state given by the matrix [21]:

$$B = \begin{bmatrix} \cos \theta & e^{i\phi} \sin \theta \\ -e^{-i\phi} \sin \theta & \cos \theta \end{bmatrix}. \quad (2.5)$$

Here, $\cos^2 \theta$ represents the probability of transmittance and $\sin^2 \theta$ represents the probability of reflection at the beam splitter. Setting the transmission of the beam splitter to be η and disregarding the phase induced on reflection (since the photons are detected right away and this phase will be lost) we have:

$$B = \begin{bmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ -\sqrt{1-\eta} & \sqrt{\eta} \end{bmatrix} \quad (2.6)$$

and

$$B^\dagger = \begin{bmatrix} \sqrt{\eta} & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & \sqrt{\eta} \end{bmatrix}. \quad (2.7)$$

Thus the beam splitter transforms the raising operators and likewise the lowering operators as

$$\begin{pmatrix} \hat{a}^\dagger \\ \hat{b}^\dagger \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & \sqrt{\eta} \end{pmatrix} \begin{pmatrix} \hat{a}'^\dagger \\ \hat{b}'^\dagger \end{pmatrix}. \quad (2.8)$$

The single photon input state with the thermal mode blocked off is then modified by the beam splitter as

$$\begin{aligned} |1\rangle_a |0\rangle_b &= \hat{a}^\dagger |0\rangle \\ &= \left(\sqrt{\eta} \hat{a}'^\dagger - \sqrt{1-\eta} \hat{b}'^\dagger \right) |0\rangle \\ &= \sqrt{\eta} |1\rangle_a |0\rangle_b - \sqrt{1-\eta} |0\rangle_a |1\rangle_b. \end{aligned} \quad (2.9)$$

With probability η the single source-photon is detected, giving η as the detection efficiency. The state resulting from the incidence of a single signal-photon and no thermal-mode photons is

$$\sqrt{\eta} |1\rangle |0\rangle + \sqrt{1-\eta} |0\rangle |1\rangle. \quad (2.10)$$

The probability of a detection event with our non-counting perfect detector in the model is then

$$\begin{aligned} P_{\text{det}} &= \left\| \sum_{n=1}^{\infty} |n\rangle \langle n| \otimes \hat{I} \left(\sqrt{\eta} |1\rangle |0\rangle + \sqrt{1-\eta} |0\rangle |1\rangle \right) \right\|^2 \\ &= \|\sqrt{\eta} |1\rangle |0\rangle\|^2 \\ &= \eta. \end{aligned} \quad (2.11)$$

As a second step in developing the model I block the input mode to determine the

background or dark count rate. The thermal state can be written as [21]

$$\rho_{\text{T}} = (1 - q) \sum_{n=0}^{\infty} q^n |n\rangle\langle n|, \quad (2.12)$$

where

$$q = e^{-\frac{\hbar\omega}{k_{\text{B}}T}}. \quad (2.13)$$

Here T and likewise q represent a non-physical temperature that reflects the strength of the thermal source and incorporates all the possible sources of dark counts for the detector. The prefactor of $(1 - q)$ is required since ρ_{T} is a density matrix and as such must have a unit trace.

Note that writing the thermal state as a combination of $|n\rangle\langle n|$ terms gives the impression that I have photon-number resolving detectors. I proceed in this way for now and then project down to a two-dimensional space representing a click/no-click detector as $\{|0\rangle\langle 0|, \sum_{n=1}^{\infty} |n\rangle\langle n|\}$ later. Recalling that

$$|n\rangle = \frac{\hat{b}^{\dagger n}}{\sqrt{n!}}|0\rangle, \quad (2.14)$$

the thermal state can be written as

$$\begin{aligned} \rho_{\text{T}} &= (1 - q) \sum_{n=0}^{\infty} q^n \left(\frac{\hat{b}^{\dagger n}}{\sqrt{n!}}|0\rangle\langle 0| \frac{\hat{b}^n}{\sqrt{n!}} \right) \\ &= (1 - q) \sum_{n=0}^{\infty} \frac{q^n}{n!} \left(\hat{b}^{\dagger n}|0\rangle\langle 0|\hat{b}^n \right). \end{aligned} \quad (2.15)$$

The overall state prior to interaction with the beam splitter including vacuum from the source mode and the thermal state is then:

$$\begin{aligned}
\rho &= |0\rangle_a \langle 0| \otimes \rho_T \\
&= (1-q) \sum_{n=0}^{\infty} \frac{q^n}{n!} \left(\hat{b}^{\dagger n} |0, 0\rangle_{a,b} \langle 0, 0| \hat{b}^n \right) \\
&= (1-q) \left(|0, 0\rangle_{a,b} \langle 0, 0| + q \left(\hat{b}^\dagger |0, 0\rangle_{a,b} \langle 0, 0| \hat{b} \right) \right. \\
&\quad \left. + \frac{q^2}{2} \left(\hat{b}^{\dagger 2} |0, 0\rangle_{a,b} \langle 0, 0| \hat{b}^2 \right) + O(q^3) \right). \tag{2.16}
\end{aligned}$$

Transforming the operators according to Eq. (2.8) results in:

$$\begin{aligned}
\rho' &= (1-q) \left(|0, 0\rangle_{a',b'} \langle 0, 0| \right. \\
&\quad + q \left(\sqrt{1-\eta} \hat{a}'^\dagger + \sqrt{\eta} \hat{b}'^\dagger \right) |0, 0\rangle_{a',b'} \langle 0, 0| \left(\sqrt{1-\eta} \hat{a}' + \sqrt{\eta} \hat{b}' \right) \\
&\quad + \frac{q^2}{2} \left(\sqrt{1-\eta} \hat{a}'^\dagger + \sqrt{\eta} \hat{b}'^\dagger \right)^2 |0, 0\rangle_{a',b'} \langle 0, 0| \left(\sqrt{1-\eta} \hat{a}' + \sqrt{\eta} \hat{b}' \right)^2 \\
&\quad \left. + O(q^3) \right) \\
&= (1-q) \left(|0, 0\rangle_{a',b'} \langle 0, 0| \right. \\
&\quad + q \left(\sqrt{1-\eta} \hat{a}'^\dagger + \sqrt{\eta} \hat{b}'^\dagger \right) |0, 0\rangle_{a',b'} \langle 0, 0| \left(\sqrt{1-\eta} \hat{a}' + \sqrt{\eta} \hat{b}' \right) \\
&\quad + \frac{q^2}{2} \left((1-\eta) \hat{a}'^{\dagger 2} + \eta \hat{b}'^{\dagger 2} + 2\sqrt{\eta(1-\eta)} \hat{a}'^\dagger \hat{b}'^\dagger \right) |0, 0\rangle_{a',b'} \langle 0, 0| \\
&\quad \left((1-\eta) \hat{a}'^2 + \eta \hat{b}'^2 + 2\sqrt{\eta(1-\eta)} \hat{a}' \hat{b}' \right) \\
&\quad \left. + O(q^3) \right) \\
&= (1-q) \left(|0, 0\rangle_{a',b'} \langle 0, 0| \right. \\
&\quad + q \left((1-\eta) |1, 0\rangle_{a',b'} \langle 1, 0| + \eta |0, 1\rangle_{a',b'} \langle 0, 1| \right. \\
&\quad + \sqrt{\eta(1-\eta)} |1, 0\rangle_{a',b'} \langle 0, 1| + \sqrt{\eta(1-\eta)} |0, 1\rangle_{a',b'} \langle 1, 0| \left. \right) \\
&\quad + \frac{q^2}{2} \left(2(1-\eta)^2 |2, 0\rangle_{a',b'} \langle 2, 0| + 2\eta^2 |0, 2\rangle_{a',b'} \langle 0, 2| + 2\eta(1-\eta) |1, 1\rangle_{a',b'} \langle 1, 1| \right) \\
&\quad \left. + O(q^3) \right). \tag{2.17}
\end{aligned}$$

Tracing over the b mode, I project onto the state with no photons in the a mode to determine the probability of a dark count. I find that the probability of zero dark counts is $(1 - q)(1 + q\eta + (q\eta)^2 + (q\eta)^3 + (q\eta)^4 + O(q^5))$. Recognizing the geometric series, the probability of zero dark counts is $\frac{1-q}{1-q\eta}$. Thus, the probability of a dark count predicted by the thermal detector model is given by

$$d = \frac{(1 - \eta)q}{1 - q\eta}. \quad (2.18)$$

Checking some limits of the dark count probability shows that when $\eta = 1$, the probability of a dark count is zero as expected. As the strength of the thermal mode goes to infinity, q goes to one, and the probability of a dark count goes to one. Any dark count probability can be modeled for any detector efficiency η between zero and one by choosing an appropriate thermal mode strength as shown in (Fig. 2.2).

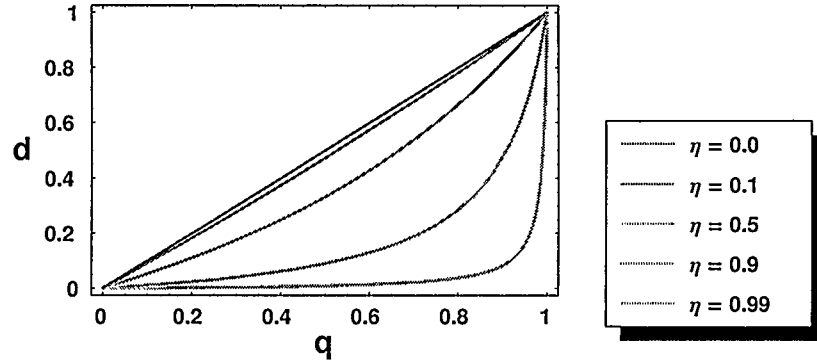


Figure 2.2: The probability of a dark count d for various detector efficiencies η over the full range in intensity of the thermal mode q .

It is important to remember that the thermal temperature and likewise q in the model are not related to a physical temperature. Since the thermal mode is made to arrive at the ideal detector via the beam splitter, the usual intuition that higher thermal radiation would lead to more dark counts does not hold. The message depicted in (Fig. 2.2) is that the model works for any detector efficiency and any dark count probability.

The third step in developing the thermal detector model is to use a coherent state

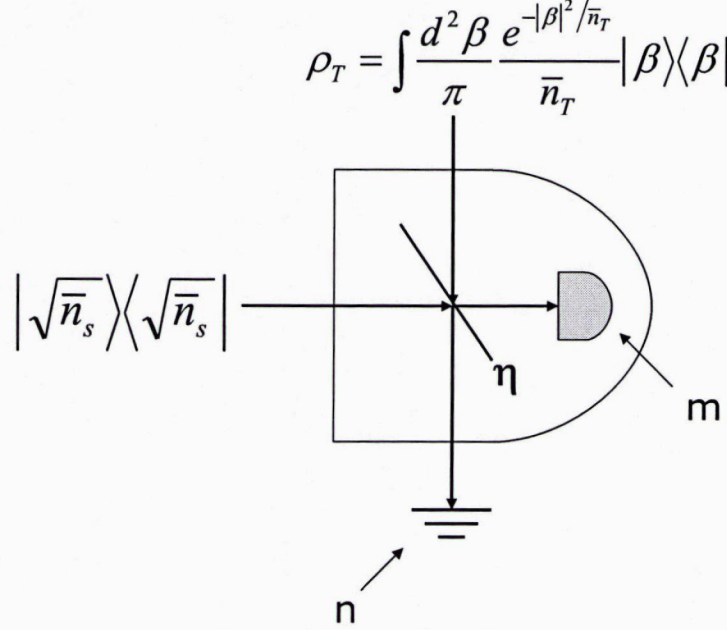


Figure 2.3: Imperfect detector with efficiency η , a coherent state input and dark counts provided by the thermal mode. The perfect detector has m photons incident on it, and n photons are absorbed or lost.

as the input mode similar to what is being used in experiments (Fig. 2.3). A general coherent state is given by $|\alpha\rangle = ||\alpha|e^{i\varphi}\rangle$, I set the phase φ to zero and set $|\alpha| = \sqrt{\bar{n}_s}$, where \bar{n}_s is the mean photon number of the source. The input state going into the detector is then assumed to be given by

$$\rho_{\text{in}} = |\sqrt{\bar{n}_s}\rangle\langle\sqrt{\bar{n}_s}| \otimes \rho_T. \quad (2.19)$$

A beam splitter transforms coherent states as

$$\hat{U}_B|\alpha\rangle_a \otimes |\beta\rangle_b = |\alpha \cos \theta + \beta \sin \theta\rangle_a \otimes |-\alpha \sin \theta + \beta \cos \theta\rangle_b, \quad (2.20)$$

where α is as defined above, and β is as defined in ρ_T . The output state following the beam splitter then becomes

$$\begin{aligned}
\rho_{\text{out}} &= \hat{U}_B \rho_{\text{in}} \hat{U}_B^\dagger \\
&= \int \frac{d^2\beta}{\pi} \frac{e^{-\frac{|\beta|^2}{\bar{n}_t}}}{\bar{n}_t} \left(\hat{U}_B |\sqrt{\bar{n}_s}\rangle \langle\sqrt{\bar{n}_s}| \otimes |\beta\rangle \langle\beta| \hat{U}_B^\dagger \right) \\
&= \int \frac{d^2\beta}{\pi} \frac{e^{-\frac{|\beta|^2}{\bar{n}_t}}}{\bar{n}_t} |\sqrt{\eta\bar{n}_s} + \sqrt{(1-\eta)\beta}\rangle \langle\sqrt{\eta\bar{n}_s} + \sqrt{(1-\eta)\beta}| \\
&\quad \otimes |-\sqrt{(1-\eta)\bar{n}_s} + \sqrt{\eta}\beta\rangle \langle-\sqrt{(1-\eta)\bar{n}_s} + \sqrt{\eta}\beta|. \tag{2.21}
\end{aligned}$$

The resulting probability of m photons contributing to a detection event and n photons being lost is given by

$$\begin{aligned}
P_{mn} &= \langle m, n | \rho_{\text{out}} | m, n \rangle \\
&= \langle m, n | \int \frac{d^2\beta}{\pi} \frac{e^{-\frac{|\beta|^2}{\bar{n}_t}}}{\bar{n}_t} |\sqrt{\eta\bar{n}_s} + \sqrt{(1-\eta)\beta}\rangle \langle\sqrt{\eta\bar{n}_s} + \sqrt{(1-\eta)\beta}| \\
&\quad \otimes |-\sqrt{(1-\eta)\bar{n}_s} + \sqrt{\eta}\beta\rangle \langle-\sqrt{(1-\eta)\bar{n}_s} + \sqrt{\eta}\beta| | m, n \rangle \\
&= \int \frac{d^2\beta}{\pi} \frac{e^{-\frac{|\beta|^2}{\bar{n}_t}}}{\bar{n}_t} \langle m | \sqrt{\eta\bar{n}_s} + \sqrt{(1-\eta)\beta} \rangle \langle\sqrt{\eta\bar{n}_s} + \sqrt{(1-\eta)\beta} | m \rangle \\
&\quad \cdot \langle n | -\sqrt{(1-\eta)\bar{n}_s} + \sqrt{\eta}\beta \rangle \langle-\sqrt{(1-\eta)\bar{n}_s} + \sqrt{\eta}\beta | n \rangle \\
&= \frac{e^{-\bar{n}_s}}{m!n!} \int \frac{d^2\beta}{\pi} \frac{e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2}}{\bar{n}_t} \left| \sqrt{\eta\bar{n}_s} + \sqrt{(1-\eta)\beta} \right|^{2m} \left| \sqrt{\eta}\beta - \sqrt{(1-\eta)\bar{n}_s} \right|^{2n}. \tag{2.22}
\end{aligned}$$

The last expression follows since

$$|\sqrt{\bar{n}_s}\rangle = e^{-\frac{\bar{n}_s}{2}} \sum_{m=0}^{\infty} \frac{(\sqrt{\bar{n}_s})^m}{\sqrt{m!}} |m\rangle,$$

and

$$\langle\sqrt{\bar{n}_s}| = e^{-\frac{\bar{n}_s}{2}} \sum_{n=0}^{\infty} \frac{(\sqrt{\bar{n}_s})^n}{\sqrt{n!}} \langle n|,$$

giving

$$\langle m | \sqrt{\bar{n}_s} \rangle = e^{-\frac{\bar{n}_s}{2}} \frac{(\sqrt{\bar{n}_s})^m}{\sqrt{m!}},$$

and

$$\langle n | \sqrt{\bar{n}_s} \rangle = e^{-\frac{\bar{n}_s}{2}} \frac{(\sqrt{\bar{n}_s^*})^n}{\sqrt{n!}}.$$

Disregarding the lost photons for the time being, I calculate the probability of m photons incident on the perfect detector of the model by tracing over all the lost photons.

$$\begin{aligned} P_m &= \sum_{n=0}^{\infty} P_{mn} \\ &= \frac{e^{-\bar{n}_s}}{m!} \int \frac{d^2\beta}{\pi} \frac{e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2}}{\bar{n}_t} \left| \sqrt{\eta}\bar{n}_s + \sqrt{(1-\eta)}\beta \right|^{2m} \sum_{n=0}^{\infty} \frac{\left| \sqrt{\eta}\beta - \sqrt{(1-\eta)}\bar{n}_s \right|^{2n}}{n!} \\ &= \frac{e^{-\bar{n}_s}}{m!} \int \frac{d^2\beta}{\pi} \frac{e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2}}{\bar{n}_t} \left| \sqrt{\eta}\bar{n}_s + \sqrt{(1-\eta)}\beta \right|^{2m} \exp \left[\left| \sqrt{\eta}\beta - \sqrt{(1-\eta)}\bar{n}_s \right|^2 \right]. \end{aligned} \quad (2.23)$$

The probability of a detection event or “click” in the detector is then given by

$$\begin{aligned} P_T &= 1 - P_0 \\ &= \sum_{m=1}^{\infty} P_m \\ &= e^{-\bar{n}_s} \int \frac{d^2\beta}{\pi} \frac{e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2 + \left| \sqrt{\eta}\beta - \sqrt{(1-\eta)}\bar{n}_s \right|^2}}{\bar{n}_t} \sum_{m=1}^{\infty} \frac{\left| \sqrt{\eta}\bar{n}_s + \sqrt{(1-\eta)}\beta \right|^{2m}}{m!}. \end{aligned} \quad (2.24)$$

Recalling that $\sum_{m=1}^{\infty} \frac{x^m}{m!} = e^x - 1$, I have

$$\begin{aligned} P_T &= \frac{e^{-\bar{n}_s}}{\bar{n}_t} \int \frac{d^2\beta}{\pi} e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2 + \left| \sqrt{\eta}\beta - \sqrt{(1-\eta)}\bar{n}_s \right|^2} \left(e^{\left| \sqrt{\eta}\bar{n}_s + \sqrt{1-\eta}\beta \right|^2} - 1 \right) \\ &= \frac{e^{-\bar{n}_s}}{\bar{n}_t} \int \frac{d^2\beta}{\pi} \left(e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2 + \left| \sqrt{\eta}\beta - \sqrt{(1-\eta)}\bar{n}_s \right|^2 + \left| \sqrt{\eta}\bar{n}_s + \sqrt{1-\eta}\beta \right|^2} - e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2 + \left| \sqrt{\eta}\beta - \sqrt{(1-\eta)}\bar{n}_s \right|^2} \right). \end{aligned} \quad (2.25)$$

Now considering that

$$\begin{aligned} \left| \sqrt{\eta}\beta - \sqrt{(1-\eta)}\bar{n}_s \right|^2 &= \left(\sqrt{\bar{n}_s}\beta^* - \sqrt{(1-\eta)}\bar{n}_s \right) \left(\sqrt{\eta}\beta - \sqrt{(1-\eta)}\bar{n}_s \right) \\ &= \eta|\beta|^2 - \sqrt{\eta(1-\eta)}\bar{n}_s(\beta + \beta^*) + (1-\eta)\bar{n}_s, \end{aligned}$$

I have

$$\left| \sqrt{\eta}\beta - \sqrt{(1-\eta)\bar{n}_s} \right|^2 + \left| \sqrt{\eta\bar{n}_s} + \sqrt{1-\eta}\beta \right|^2 = \bar{n}_s + |\beta|^2.$$

Substituting this back into Eq. (2.24) and recalling that $(\beta + \beta^*) = 2\text{Re}\beta$, I have

$$\begin{aligned} P_T &= \frac{e^{-\bar{n}_s}}{\bar{n}_t} \int \frac{d^2\beta}{\pi} \left(e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2 + \bar{n}_s + |\beta|^2} - e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2 + \eta|\beta|^2 - 2\sqrt{\eta(1-\eta)\bar{n}_s}\text{Re}\beta + (1-\eta)\bar{n}_s} \right) \\ &= \frac{e^{-\bar{n}_s}}{\bar{n}_t} \left(e^{\bar{n}_s} \int \frac{d^2\beta}{\pi} \left(e^{-\frac{|\beta|^2}{\bar{n}_t}} - e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2 + \eta|\beta|^2 - 2\sqrt{\eta(1-\eta)\bar{n}_s}\text{Re}\beta} e^{(1-\eta)\bar{n}_s} \right) \right) \\ &= \frac{1}{\bar{n}_t} \int \frac{d^2\beta}{\pi} e^{-\frac{|\beta|^2}{\bar{n}_t}} - \frac{e^{-\eta\bar{n}_s}}{\bar{n}_t} \int \frac{d^2\beta}{\pi} e^{-\frac{1+\bar{n}_t}{\bar{n}_t}|\beta|^2 + \eta|\beta|^2 - 2\sqrt{\eta(1-\eta)\bar{n}_s}\text{Re}\beta}. \end{aligned} \quad (2.26)$$

Recalling that $\beta = \beta_r + i\beta_i$ so that $|\beta|^2 = (\beta_r + i\beta_i)(\beta_r - i\beta_i) = \beta_r^2 + \beta_i^2$, the first integral can be written as

$$\frac{1}{\bar{n}_t} \int_{-\infty}^{\infty} \frac{d^2\beta_r}{\sqrt{\pi}} e^{-\frac{\beta_r^2}{\bar{n}_t}} \int_{-\infty}^{\infty} \frac{d^2\beta_i}{\sqrt{\pi}} e^{-\frac{\beta_i^2}{\bar{n}_t}}. \quad (2.27)$$

Now

$$\int_0^{\infty} e^{-ax^2} x^n dx = \frac{(n-1)!!}{2^{\frac{n}{2}+1} a^{\frac{n}{2}}} \sqrt{\frac{\pi}{a}}, \quad n \text{ even} \quad (2.28)$$

$$= \frac{(\frac{1}{2}(n-1))!}{2a^{\frac{n+1}{2}}}, \quad n \text{ odd}. \quad (2.29)$$

Here we have $x^n = 1$ so $n = 0$ and $a = \frac{1}{\bar{n}_t}$ so that

$$\int_{-\infty}^{\infty} \frac{d^2\beta_r}{\sqrt{\pi}} e^{-\frac{\beta_r^2}{\bar{n}_t}} = \frac{2(0-1)!!}{2\sqrt{\pi}} \sqrt{\pi\bar{n}_t} = \sqrt{\bar{n}_t} \quad (2.30)$$

and the first integral above becomes

$$\frac{1}{\bar{n}_t} \sqrt{\bar{n}_t} \sqrt{\bar{n}_t} = 1. \quad (2.31)$$

Returning to my expression for the probability of a click using the thermal detector model

I have

$$\begin{aligned}
P_T &= 1 - \frac{e^{-\eta \bar{n}_s}}{\bar{n}_t} \int \frac{d^2 \beta}{\pi} e^{-\frac{1+\bar{n}_t}{\bar{n}_t} |\beta|^2 + \eta |\beta|^2 - 2\sqrt{\eta(1-\eta)\bar{n}_s} \text{Re} \beta} \\
&= 1 - \frac{e^{-\eta \bar{n}_s}}{\bar{n}_t} \int_{-\infty}^{\infty} \frac{d\beta_r}{\sqrt{\pi}} \int_{-\infty}^{\infty} \frac{d\beta_i}{\sqrt{\pi}} e^{-\frac{1+\bar{n}_t}{\bar{n}_t} (\beta_r^2 + \beta_i^2) + \eta (\beta_r^2 + \beta_i^2) - 2\sqrt{\eta(1-\eta)\bar{n}_s} \beta_r} \\
&= 1 - e^{-\eta \bar{n}_s} \int_{-\infty}^{\infty} \frac{d\beta_r}{\sqrt{\pi \bar{n}_t}} e^{-\frac{1+\bar{n}_t}{\bar{n}_t} \beta_r^2 + \eta \beta_r^2 - 2\sqrt{\eta(1-\eta)\bar{n}_s} \beta_r} \int_{-\infty}^{\infty} \frac{d\beta_i}{\sqrt{\pi \bar{n}_t}} e^{-\frac{1+\bar{n}_t}{\bar{n}_t} \beta_i^2 + \eta \beta_i^2}. \quad (2.32)
\end{aligned}$$

Looking at the second integral, I note that it is a gaussian with $x^n = 1$ so $n = 0$:

$$\int_0^{\infty} e^{-ax^2} dx = \frac{1}{2} \sqrt{\frac{\pi}{a}}. \quad (2.33)$$

The second integral above then becomes

$$\begin{aligned}
\int_{-\infty}^{\infty} \frac{d\beta_i}{\sqrt{\pi \bar{n}_t}} e^{\left(-\frac{1+\bar{n}_t}{\bar{n}_t} + \eta\right) \beta_i^2} &= \frac{2}{\sqrt{\pi \bar{n}_t}} \frac{1}{2} \sqrt{\frac{\pi}{\frac{1+\bar{n}_t}{\bar{n}_t} - \eta}} \\
&= \frac{1}{\sqrt{\bar{n}_t \left(\frac{1+\bar{n}_t}{\bar{n}_t} - \eta\right)}} \\
&= \frac{1}{\sqrt{1 + \bar{n}_t - \bar{n}_t \eta}} \\
&= \frac{1}{\sqrt{1 + (1 - \eta) \bar{n}_t}}. \quad (2.34)
\end{aligned}$$

Returning to the first integral above:

$$\int_{-\infty}^{\infty} \frac{d\beta_r}{\sqrt{\pi \bar{n}_t}} e^{-\frac{1+\bar{n}_t}{\bar{n}_t} \beta_r^2 + \eta \beta_r^2 - 2\sqrt{\eta(1-\eta)\bar{n}_s} \beta_r} = \int_{-\infty}^{\infty} \frac{d\beta_r}{\sqrt{\pi \bar{n}_t}} e^{\left(-\frac{1+\bar{n}_t}{\bar{n}_t} + \eta\right) \beta_r^2 - 2\sqrt{\eta(1-\eta)\bar{n}_s} \beta_r}. \quad (2.35)$$

Then since

$$\int_{-\infty}^{\infty} e^{-ax^2 + bx} dx = \sqrt{\frac{\pi}{a}} e^{\frac{b^2}{4a}} \quad (2.36)$$

with $a = \frac{1+\bar{n}_t}{\bar{n}_t} - \eta$ and $b = -2\sqrt{\eta(1-\eta)\bar{n}_s}$ the last integral becomes

$$\begin{aligned}
\frac{1}{\sqrt{\pi\bar{n}_t}} \sqrt{\frac{\pi}{a}} e^{\frac{b^2}{4a}} &= \frac{\sqrt{\pi}}{\sqrt{\pi\bar{n}_t \left(\frac{1+\bar{n}_t}{\bar{n}_t} - \eta \right)}} \exp \left[\frac{4\eta(1-\eta)\bar{n}_s}{4 \left(\frac{1+\bar{n}_t}{\bar{n}_t} - \eta \right)} \right] \\
&= \frac{\exp \left[\frac{\eta(1-\eta)\bar{n}_s}{\left(\frac{1+\bar{n}_t}{\bar{n}_t} - \eta \right)} \right]}{\sqrt{1 + \bar{n}_t - \bar{n}_t\eta}} \\
&= \frac{\exp \left[\frac{\eta(1-\eta)\bar{n}_s\bar{n}_t}{1+\bar{n}_t-\eta\bar{n}_t} \right]}{\sqrt{1 + (1-\eta)\bar{n}_t}} \\
&= \frac{\exp \left[\frac{\eta(1-\eta)\bar{n}_s\bar{n}_t}{1+(1-\eta)\bar{n}_t} \right]}{\sqrt{1 + (1-\eta)\bar{n}_t}}.
\end{aligned} \tag{2.37}$$

The probability of a click for the thermal model detector is then given by:

$$\begin{aligned}
P_T &= 1 - \frac{e^{-\eta\bar{n}_s}}{\sqrt{1 + (1-\eta)\bar{n}_t}} \frac{e^{\frac{\eta(1-\eta)\bar{n}_s\bar{n}_t}{1+(1-\eta)\bar{n}_t}}}{\sqrt{1 + (1-\eta)\bar{n}_t}} \\
&= 1 - \frac{e^{\frac{\eta(1-\eta)\bar{n}_t\bar{n}_s}{1+(1-\eta)\bar{n}_t} - \eta\bar{n}_s}}{1 + (1-\eta)\bar{n}_t}.
\end{aligned} \tag{2.38}$$

I now compare this click probability to that produced by the experimentally motivated model as given in Eq. (2.3). The mean photon number in the thermal mode is given by:

$$\bar{n}_t = \frac{1}{e^{\frac{\hbar\omega}{k_B T}} - 1}. \tag{2.39}$$

Then, since $q = e^{-\frac{\hbar\omega}{k_B T}}$, $q = \frac{\bar{n}_t}{1+\bar{n}_t}$, $\bar{n}_t = \frac{q}{1-q}$, and recalling that $d = \frac{(1-\eta)q}{1-q\eta}$:

$$\begin{aligned}
P_T &= 1 - \frac{e^{\frac{\eta(1-\eta)\bar{n}_t\bar{n}_s}{1+(1-\eta)\bar{n}_t} - \eta\bar{n}_s}}{1 + (1-\eta)\bar{n}_t} \\
&= 1 - e^{-\eta\bar{n}_s} \left(\frac{1-q}{1-\eta q} \right) \exp \left[\frac{\eta(1-\eta)\bar{n}_s q}{1-\eta q} \right].
\end{aligned} \tag{2.40}$$

Expressing P_T in terms of dark count probabilities rather than thermal mode intensity for direct comparison with Eq. (2.3) gives:

$$P_T = 1 + (d-1)e^{-\eta\bar{n}_s}e^{\eta\bar{n}_s d}. \tag{2.41}$$

To compare the click probabilities predicted by the two models for the full range of dark counts, fixed detector efficiencies and source mode intensities, refer to Figs. 2.4, 2.5, 2.6, and 2.7. The two models differ most notably for large detector efficiencies and large signal mode intensity. For reasonable experimental values of $\bar{n}_s = 0.24$, $d = 10^{-5}$ and $\eta = 0.1$ [22], they have click probabilities within 0.001% of each other. This deviation is much less than the detector inefficiency of 90%.

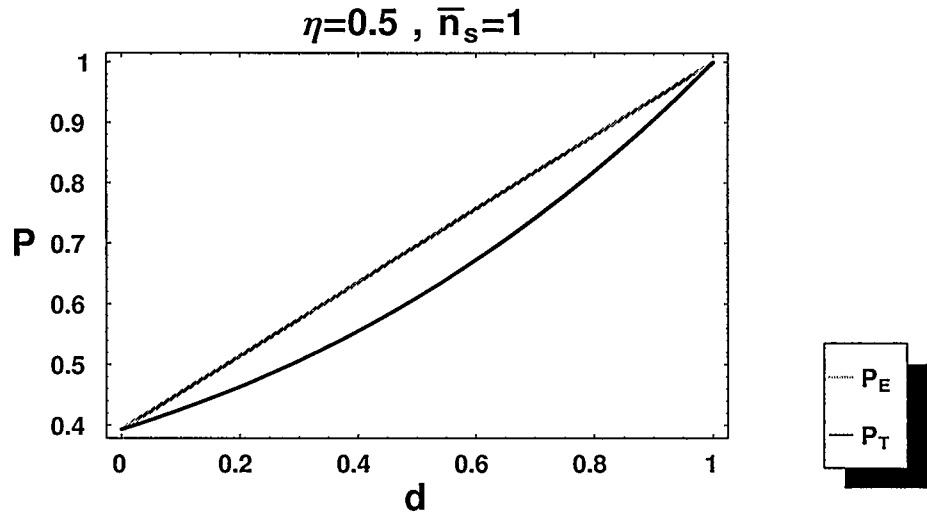


Figure 2.4: Click probabilities P for the experimentally motivated model P_E and the thermal model P_T for dark count probabilities d , detector efficiency η , and mean number of photons in the source mode \bar{n}_s .

2.3 Summary

The thermal detector model developed in this section provides a simplification to models that include separate loss and dark count modes. By combining photon loss and detector efficiency on the beam splitter, we have created a simpler model than one which treats those modes separately. This model allows for simpler calculation with fewer modes at

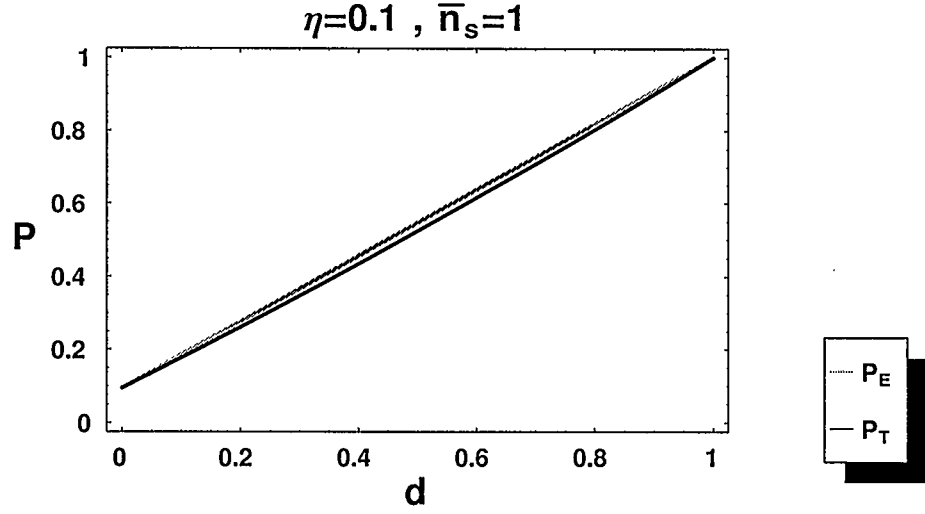


Figure 2.5: Click probabilities P for the experimentally motivated model P_E and the thermal model P_T for dark count probabilities d , detector efficiency η , and mean number of photons in the source mode \bar{n}_s .

very small cost to accuracy. In comparing the click probability predictions of this model with an experimentally motivated one, I find that deviation becomes significant as the detector efficiency and the source strength increase. Agreement between the two models is within 0.001% at the efficiencies and source strengths in use today. This is a very small component of overall errors and inefficiencies of quantum detectors.

In this section I have described a simple framework for predicting detector clicks for various input distributions, while taking the multi-photon nature of imperfect signal sources and dark counts into consideration. Detector performance is a fundamental aspect of any quantum communication operation including entanglement swapping.

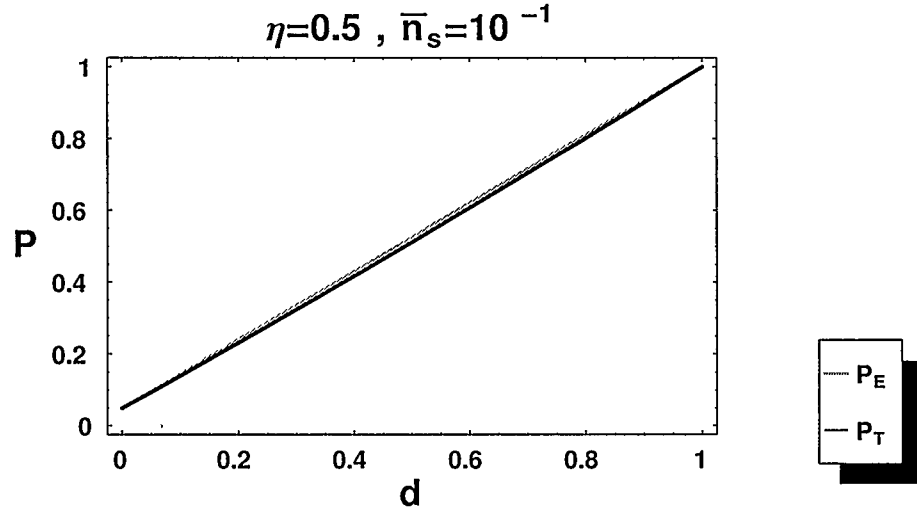


Figure 2.6: Click probabilities P for the experimentally motivated model P_E and the thermal model P_T for dark count probabilities d , detector efficiency η , and mean number of photons in the source mode \bar{n}_s .

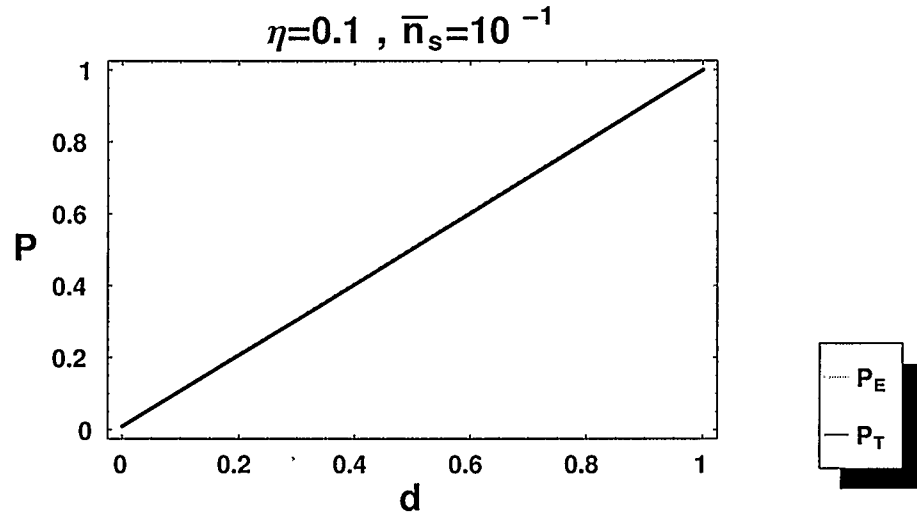


Figure 2.7: Click probabilities P for the experimentally motivated model P_E and the thermal model P_T for dark count probabilities d , detector efficiency η , and mean number of photons in the source mode \bar{n}_s .

Chapter 3

Entanglement Swapping With Perfect Two-Photon Sources

Ideal entanglement swapping would have ideal photon-pair sources as inputs, as well as ideal Bell measurements. Although such ideal components are not available, I calculate the resultant state of an entanglement swapping operation resulting from perfect parametric down conversion sources and perfect detectors in this chapter. This exploration of the ideal case will allow me then to consider the effects of imperfections in the next chapter.

In order to overcome the distance limits of quantum key distribution (QKD), entanglement swapping [23] is used as a fundamental building block in creating quantum relays and quantum repeaters. Entanglement swapping allows us to entangle two modes at any distance in principle. Imperfections in all aspects of the system are what limit achievable distance between entangled modes using this method.

Physically separated, Alice and Bob can distill a shared secret key from a successful entanglement swapping operation. They do this by randomly choosing one of two publicly agreed upon non-orthogonal bases to measure any incoming photons, and publicly announcing their basis choice. When they choose the same basis for measurement, they will have perfectly correlated values in their measured sequence, provided the photons emitted by the sources were perfectly correlated. The values obtained when different bases were chosen are simply discarded. The sequence of measurement results remaining following additional compression for privacy amplification forms their shared key. The complete protocol is known as BBM92 [9].

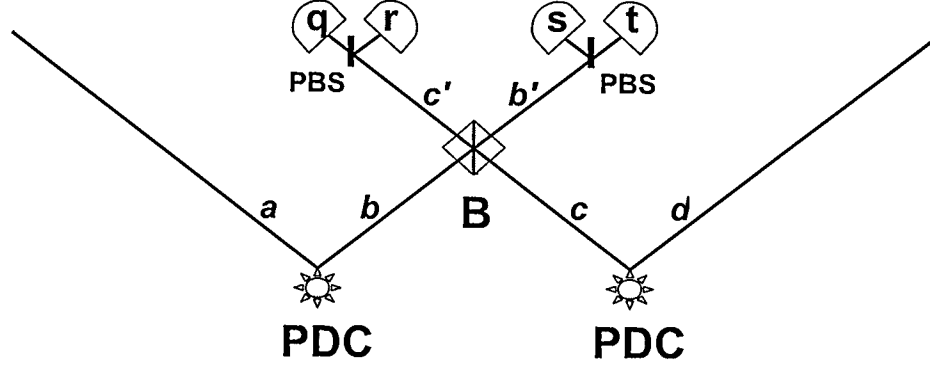


Figure 3.1: Entanglement swapping with two parametric down conversion sources (PDCs). One mode of each entangled pair source meets at a balanced beam splitter (B). Its outputs denoted by c' and b' are directed to polarizing beam splitters (PBS) and then detected at four detectors: one for the H and one for the V polarizations of each of the c' and b' modes. The readout of the detectors is denoted $(qrst)$ with q the number of photons detected in mode c'_H , r the number of photons detected in mode c'_V , s the number of photons detected in mode b'_V and t the number of photons detected in mode b'_H . The ordering of modes in $qrst$ is dictated by the behavior of the polarizing beam splitter, which allows the horizontal polarization to transmit and reflects the vertical polarization.

3.1 Ideal Source Entanglement Swap

A maximally entangled pair of photons can be represented by a Bell state [3]:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (3.1)$$

The two opposing states $|0\rangle$ and $|1\rangle$ could equally be represented by horizontal or vertical polarization in a given spatial mode

$$\frac{1}{\sqrt{2}} \left(\hat{c}_H^\dagger \hat{d}_H^\dagger + \hat{c}_V^\dagger \hat{d}_V^\dagger \right) |0\rangle. \quad (3.2)$$

Given two ideal parametric down conversion sources that produce perfectly entangled pairs, with exactly one photon in each mode of the pair, the resultant state in four modes would be

$$|\Psi_{\text{id1}}\rangle = \frac{1}{\sqrt{2}} \left(\hat{a}_H^\dagger \hat{b}_H^\dagger + \hat{a}_V^\dagger \hat{b}_V^\dagger \right) |0\rangle \otimes \frac{1}{\sqrt{2}} \left(\hat{c}_H^\dagger \hat{d}_H^\dagger + \hat{c}_V^\dagger \hat{d}_V^\dagger \right) |0\rangle. \quad (3.3)$$

A beam splitter produces operator conversions as [3]

$$\begin{pmatrix} \hat{b}_H^\dagger \\ \hat{c}_H^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \hat{b}_H^\dagger \\ \hat{c}_H^\dagger \end{pmatrix} \quad (3.4)$$

and

$$\begin{pmatrix} \hat{b}_H^\dagger \\ \hat{c}_H^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \hat{b}_H^\dagger \\ \hat{c}_H^\dagger \end{pmatrix}. \quad (3.5)$$

By interaction of the b and c modes on the beam splitter (Fig. 3), the state of the system is transformed as

$$\begin{aligned} |\Psi_{\text{id2}}\rangle &= \frac{1}{\sqrt{2}} \left(\hat{a}_H^\dagger \frac{1}{\sqrt{2}} (\hat{b}_H^\dagger - \hat{c}_H^\dagger) \right) + \hat{a}_V^\dagger \frac{1}{\sqrt{2}} (\hat{b}_V^\dagger - \hat{c}_V^\dagger) |0\rangle \\ &\quad \otimes \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} (\hat{b}_H^\dagger + \hat{c}_H^\dagger) \hat{d}_H^\dagger + \frac{1}{\sqrt{2}} (\hat{b}_V^\dagger + \hat{c}_V^\dagger) \hat{d}_V^\dagger \right) |0\rangle. \\ &= \frac{1}{2} \left(\hat{a}_H^\dagger \hat{b}_H^\dagger - \hat{a}_H^\dagger \hat{c}_H^\dagger + \hat{a}_V^\dagger \hat{b}_V^\dagger - \hat{a}_V^\dagger \hat{c}_V^\dagger \right) |0\rangle \\ &\quad \otimes \frac{1}{2} \left(\hat{b}_H^\dagger \hat{d}_H^\dagger + \hat{c}_H^\dagger \hat{d}_H^\dagger + \hat{b}_V^\dagger \hat{d}_V^\dagger + \hat{c}_V^\dagger \hat{d}_V^\dagger \right) |0\rangle \\ &= \frac{1}{4} \left(\hat{a}_H^\dagger (\hat{b}_H^\dagger)^2 \hat{d}_H^\dagger + \hat{a}_H^\dagger \hat{b}_H^\dagger \hat{c}_H^\dagger \hat{d}_H^\dagger + \hat{a}_H^\dagger \hat{b}_H^\dagger \hat{b}_V^\dagger \hat{d}_V^\dagger + \hat{a}_H^\dagger \hat{b}_H^\dagger \hat{c}_V^\dagger \hat{d}_V^\dagger - \hat{a}_H^\dagger \hat{c}_H^\dagger \hat{b}_H^\dagger \hat{d}_H^\dagger \right. \\ &\quad - \hat{a}_H^\dagger (\hat{c}_H^\dagger)^2 \hat{d}_H^\dagger - \hat{a}_H^\dagger \hat{c}_H^\dagger \hat{b}_V^\dagger \hat{d}_V^\dagger - \hat{a}_H^\dagger \hat{c}_H^\dagger \hat{c}_V^\dagger \hat{d}_V^\dagger + \hat{a}_V^\dagger \hat{b}_V^\dagger \hat{b}_H^\dagger \hat{d}_H^\dagger + \hat{a}_V^\dagger \hat{b}_V^\dagger \hat{c}_H^\dagger \hat{d}_H^\dagger + \hat{a}_V^\dagger (\hat{b}_V^\dagger)^2 \hat{d}_V^\dagger \\ &\quad \left. + \hat{a}_V^\dagger \hat{b}_V^\dagger \hat{c}_V^\dagger \hat{d}_V^\dagger - \hat{a}_V^\dagger \hat{c}_V^\dagger \hat{b}_H^\dagger \hat{d}_H^\dagger - \hat{a}_V^\dagger \hat{c}_V^\dagger \hat{c}_H^\dagger \hat{d}_H^\dagger - \hat{a}_V^\dagger \hat{c}_V^\dagger \hat{b}_V^\dagger \hat{d}_V^\dagger - \hat{a}_V^\dagger (\hat{c}_V^\dagger)^2 \hat{d}_V^\dagger \right) |0\rangle. \quad (3.6) \end{aligned}$$

I now project this state onto the subspaces corresponding to the different possible successful Bell state measurements. A successful entanglement swap represents the transfer of entanglement from between the a and b modes and the c and d modes to the a and d modes, with the photons in the b and c modes destroyed by detection. The resulting state

present in the a and d modes is one of the maximally entangled Bell states as follows:

$$\begin{aligned}\langle 0|\hat{c}'_H\hat{c}'_V|\Psi_{\text{id}2}\rangle &= \frac{1}{4} \left(-\hat{a}_H^\dagger\hat{d}_V^\dagger - \hat{a}_V^\dagger\hat{d}_H^\dagger \right) |0\rangle \\ &= -\frac{1}{4}|\Psi^+\rangle\end{aligned}\tag{3.7}$$

$$\begin{aligned}\langle 0|\hat{c}'_H\hat{b}'_V|\Psi_{\text{id}2}\rangle &= \frac{1}{4} \left(-\hat{a}_H^\dagger\hat{d}_V^\dagger + \hat{a}_V^\dagger\hat{d}_H^\dagger \right) |0\rangle \\ &= \frac{1}{4}|\Psi^-\rangle\end{aligned}\tag{3.8}$$

$$\begin{aligned}\langle 0|\hat{c}'_V\hat{b}'_H|\Psi_{\text{id}2}\rangle &= \frac{1}{4} \left(\hat{a}_H^\dagger\hat{d}_V^\dagger - \hat{a}_V^\dagger\hat{d}_H^\dagger \right) |0\rangle \\ &= \frac{1}{4}|\Psi^-\rangle\end{aligned}\tag{3.9}$$

$$\begin{aligned}\langle 0|\hat{b}'_H\hat{b}'_V|\Psi_{\text{id}2}\rangle &= \frac{1}{4} \left(\hat{a}_H^\dagger\hat{d}_V^\dagger + \hat{a}_V^\dagger\hat{d}_H^\dagger \right) |0\rangle \\ &= \frac{1}{4}|\Psi^+\rangle.\end{aligned}\tag{3.10}$$

A four-fold coincidence is required to prove a successful entanglement swap: two specific detectors in the b' and c' modes and one in each of the a and d modes (Fig. 3.1). By causing interference of the middle two modes of this four photon state on a beam splitter, we are able to transfer entanglement to the outermost photons in the chain, thereby creating a quantum relay. Such a quantum relay can extend the distance at which two photons can be entangled. Given that we require photons to be entangled at large distances in order to perform quantum key distribution utilizing the BBM92 protocol at large distances, we can see how this relay will be useful.

3.2 Summary

An ideal quantum relay is composed of ideal parametric down conversion sources, ideal beam splitters and ideal detectors. With these components, entanglement can theoretically be perfectly transferred to the endmost nodes of a relay configuration allowing

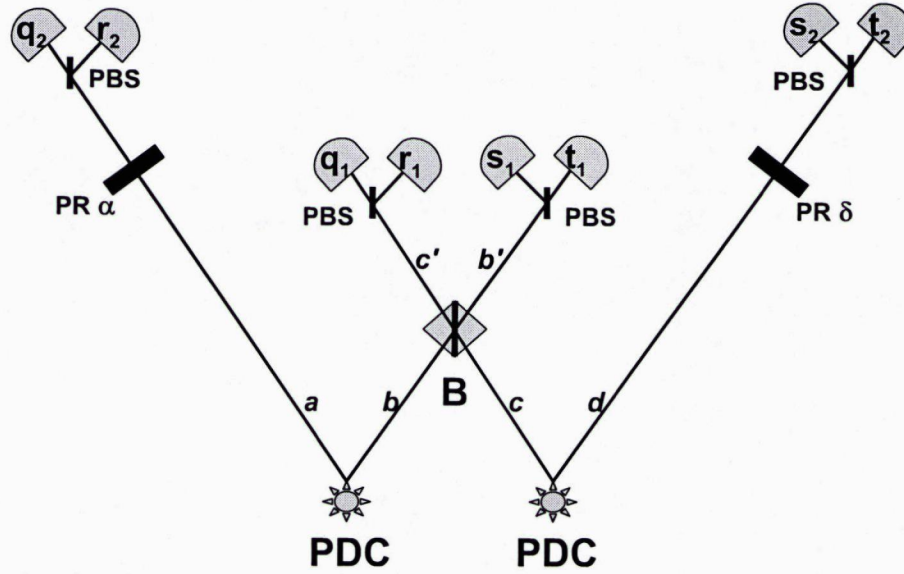


Figure 3.2: The full entanglement swapping operation shows a Bell measurement on modes b' and c' followed by detection of the a and d modes. The polarization rotators (PR) allow for the observation of certain four-fold coincidences for different rotation angles. The four-fold coincidence rates in turn determine the visibility and hence the fidelity of the entanglement swapping operation.

subsequent quantum communication operations to be implemented with perfect entanglement as a resource. Optical Bell state measurements can distinguish half of the Bell states, so that they have an efficiency of 50% maximum. In addition, we must deal with a number of imperfections, which I consider in the next chapter.

Chapter 4

Entanglement Swapping With Imperfect Two Photon Sources

Since ideal sources and detectors are not available for experiment, the entanglement swapping operation presented in the previous chapter must be modified to take into account various imperfections. In this chapter I consider imperfection in the source and the detector. I calculate the resultant state of an entanglement swapping operation resulting from parametric down conversion sources and detectors that are inefficient, but without taking dark counts into consideration.

Where two entangled pair sources are required to work together such as in the entanglement swapping operation the added issue of timing needs to be considered. Since the two photons that meet at the beam splitter for the Bell state measurement must interact, they must arrive at the same time. Such precise timing for the pump lasers is a challenge when the sources are separated by significant distance. I will not consider this issue in this thesis.

4.1 Multi-photon Sources

Experimental realization is very different from theoretical models of quantum relays [13] due to imperfect sources of entangled pairs. Rather than assuming ideal single and single-pair photon sources, I model the sources as distributions in agreement with their faint pulse or parametric down conversion origins.

In PDC a $\chi^{(2)}$ non-linear crystal is pumped by a strong laser and photons passing through the crystal emerge as two down-converted photons with some probability. As shown in [24], the PDC process can be described mathematically by

$$\Upsilon(\gamma)|vac\rangle = \exp\left[\imath\gamma\frac{1}{2}\left(\hat{a}_V^\dagger\hat{b}_V^\dagger + \hat{a}_V\hat{b}_V\right)\right]|vac\rangle. \quad (4.1)$$

Each pump-field photon can decay into a pair of of entangled photons. If two PDC crystals are combined with their axes orthogonal to each other, then polarization-entangled pairs are generated:

$$|\Phi\rangle = e^{\imath\chi(\hat{a}_H^\dagger\hat{b}_H^\dagger + \hat{a}_H\hat{b}_H + \hat{a}_V^\dagger\hat{b}_V^\dagger + \hat{a}_V\hat{b}_V)}|0\rangle. \quad (4.2)$$

The parameter χ^2 can be viewed as the brightness of the source as larger values of χ^2 result in more photon pairs being created. I shall refer to χ as the source efficiency.

For entanglement swapping we require two PDC sources. The state prepared by two PDC sources configured to produce polarization-entangled pairs with efficiency χ is given as

$$|\Psi_1\rangle = e^{\imath\chi(\hat{a}_H^\dagger\hat{b}_H^\dagger + \hat{a}_H\hat{b}_H)}e^{\imath\chi(\hat{a}_V^\dagger\hat{b}_V^\dagger + \hat{a}_V\hat{b}_V)}e^{\imath\chi(\hat{c}_H^\dagger\hat{d}_H^\dagger + \hat{c}_H\hat{d}_H)}e^{\imath\chi(\hat{c}_V^\dagger\hat{d}_V^\dagger + \hat{c}_V\hat{d}_V)}|0\rangle. \quad (4.3)$$

I approximate the exponentials using their series expansions so that each of the four terms of $|\Psi_1\rangle$ expands as

$$1 + \imath\chi\left(\hat{a}_H^\dagger\hat{b}_H^\dagger + \hat{a}_H\hat{b}_H\right) - \frac{\chi^2}{2}\left(\hat{a}_H^\dagger\hat{b}_H^\dagger + \hat{a}_H\hat{b}_H\right)^2 + \dots. \quad (4.4)$$

The next step is to normally order the operators with the following rules.

$$\hat{a}\hat{a}^\dagger = 1 + \hat{a}^\dagger\hat{a} \quad (4.5)$$

$$\left(\hat{a}_H^\dagger\hat{b}_H^\dagger + \hat{a}_H\hat{b}_H\right)^2 = \hat{a}_H^{\dagger 2}\hat{b}_H^{\dagger 2} + 1 + \hat{a}_H^\dagger\hat{a}_H + \hat{b}_H^\dagger\hat{b}_H + \hat{a}_H^\dagger\hat{a}_H\hat{b}_H^\dagger\hat{b}_H \quad (4.6)$$

The last three terms in this last equation have no effect on the vacuum state and similarly for other expansions so that we are left with each of the four exponentials of $|\Psi_1\rangle$

represented as follows:

$$\begin{aligned}
e^{i\chi(\hat{a}_H^\dagger \hat{b}_H^\dagger + \hat{a}_H \hat{b}_H)} &= 1 + i\chi \hat{a}_H^\dagger \hat{b}_H^\dagger \\
&\quad - \frac{\chi^2}{2} \left(\hat{a}_H^{\dagger 2} \hat{b}_H^{\dagger 2} + 1 \right) \\
&\quad - \frac{i\chi^3}{6} \left(\hat{a}_H^{\dagger 3} \hat{b}_H^{\dagger 3} + 5\hat{a}_H^\dagger \hat{b}_H^\dagger \right) \\
&\quad + \frac{\chi^4}{24} \left(\hat{a}_H^{\dagger 4} \hat{b}_H^{\dagger 4} + 14\hat{a}_H^{\dagger 2} \hat{b}_H^{\dagger 2} + 5 \right) \\
&\quad + \frac{i\chi^5}{5!} \left(\hat{a}_H^{\dagger 5} \hat{b}_H^{\dagger 5} + 30\hat{a}_H^{\dagger 3} \hat{b}_H^{\dagger 3} + 61\hat{a}_H^\dagger \hat{b}_H^\dagger \right) \\
&\quad - \frac{\chi^6}{6!} \left(\hat{a}_H^{\dagger 6} \hat{b}_H^{\dagger 6} + 55\hat{a}_H^{\dagger 4} \hat{b}_H^{\dagger 4} + 331\hat{a}_H^{\dagger 2} \hat{b}_H^{\dagger 2} + 61 \right) \\
&\quad + \dots .
\end{aligned} \tag{4.7}$$

Combining the b and c modes on a 50 : 50 beam splitter translates the modes as

$$\begin{aligned}
\hat{b}_H^\dagger &= \frac{1}{\sqrt{2}} \left(\hat{b}_H'^\dagger - \hat{c}_H'^\dagger \right) \\
\hat{b}_V^\dagger &= \frac{1}{\sqrt{2}} \left(\hat{b}_V'^\dagger - \hat{c}_V'^\dagger \right) \\
\hat{c}_H^\dagger &= \frac{1}{\sqrt{2}} \left(\hat{b}_H'^\dagger + \hat{c}_H'^\dagger \right) \\
\hat{c}_V^\dagger &= \frac{1}{\sqrt{2}} \left(\hat{b}_V'^\dagger + \hat{c}_V'^\dagger \right) .
\end{aligned}$$

Passing the input state Ψ_1 through the beam splitter while considering the raising operator rule $\hat{a}^{\dagger n}|0\rangle = \sqrt{n!}|n\rangle$, I then collect terms for each detector event. The resultant

state can be written as

$$\begin{aligned}
|\Psi_2\rangle = & \left(1 - 2\chi^2 + \frac{7\chi^4}{3} - \frac{94\chi^6}{45} + O(\chi^8)\right) |0\rangle \\
& + \hat{c}_H^\dagger \left(\left(-\frac{i\chi}{\sqrt{2}} + \frac{7i\chi^3}{3\sqrt{2}} - \frac{47i\chi^5}{15\sqrt{2}} + O(\chi^7) \right) \hat{a}_H^\dagger \right. \\
& + \left. \left(-\frac{i\chi}{\sqrt{2}} + \frac{7i\chi^3}{3\sqrt{2}} - \frac{47i\chi^5}{15\sqrt{2}} + O(\chi^7) \right) \hat{d}_H^\dagger \right) |0\rangle \\
& + \hat{b}_H^\dagger \left(\left(\frac{i\chi}{\sqrt{2}} - \frac{7i\chi^3}{3\sqrt{2}} + \frac{47i\chi^5}{15\sqrt{2}} + O(\chi^7) \right) \hat{a}_H^\dagger \right. \\
& + \left. \left(-\frac{i\chi}{\sqrt{2}} + \frac{7i\chi^3}{3\sqrt{2}} - \frac{47i\chi^5}{15\sqrt{2}} + O(\chi^7) \right) \hat{d}_H^\dagger \right) |0\rangle \\
& + \hat{b}_H^\dagger \hat{c}_H^\dagger \left(\left(\frac{1}{2}\chi^2 - \frac{4}{3}\chi^4 + \frac{91}{45}\chi^6 + O(\chi^8) \right) \hat{a}_H^{\dagger 2} \right. \\
& - \left. \left(\frac{1}{2}\chi^2 - \frac{4}{3}\chi^4 + \frac{91}{45}\chi^6 + O(\chi^8) \right) \hat{d}_H^{\dagger 2} \right) |0\rangle \\
& + \dots
\end{aligned} \tag{4.8}$$

At this point I am assuming I have photon counting detectors that can determine the number of photons causing the detection event. Detecting the four modes that have interacted at the beam splitter, we get a four-tuple of integers representing the number of photons detected at each of the four detectors. Given an actual detector readout $(qrst)$, I infer what an ideal four-tuple of detectors would have yielded. An ideal set of detectors would have yielded a readout of $(ijkl)$ with probability $P(ijkl|qrst)$, given an actual detector readout of $(qrst)$. Given an ideal readout of $(ijkl)$, I calculate the resultant pure state $|\Phi_{ijkl}\rangle$ by a projection measurement on $|\Psi_2\rangle$:

$$|\Phi_{ijkl}\rangle = \frac{(|ijkl\rangle_{bc'} \langle ijkl| \otimes \mathbb{1}_{ad}) |\Psi_2\rangle}{\| (|ijkl\rangle_{bc'} \langle ijkl| \otimes \mathbb{1}_{ad}) |\Psi_2\rangle \|}. \tag{4.9}$$

The resultant mixed state given the readout $(qrst)$ at the inefficient detectors is

$$\rho_{qrst} = \sum_{ijkl} P(ijkl|qrst) |\Phi_{ijkl}\rangle \langle \Phi_{ijkl}|. \quad (4.10)$$

Given the actual detector readout $(qrst)$, I sum over all the ideal four-tuple detector combinations and their probabilities, that could have resulted in the actual measurement.

The quantities I need are the $P(ijkl|qrst)$ and I can infer these values using Bayes' Rule, which allows us to compute "backward probabilities" $P(x|y)$ given the "forward probabilities" $P(y|x)$ as [25]

$$P(x|y) = \frac{P(x)P(y|x)}{P(y)}. \quad (4.11)$$

In this case I have

$$P(ijkl|qrst) = \frac{P(qrst|ijkl)P(ijkl)}{\sum_{i'j'k'l'} P(qrst|i'j'k'l')P(i'j'k'l')}. \quad (4.12)$$

Here $P(i'j'k'l') = \|(|i'j'k'l'\rangle_{b'c'} \langle i'j'k'l'| \otimes \mathbb{1}_{ad}) |\Psi_2\rangle\|^2$ and the $P(ijkl)$ are the perfect detection probabilities. For example, utilizing mathematica, the perfect detection probability for modes c'_H and b'_V is

$$\begin{aligned} P(1010) &= \|(|1010\rangle_{b'c'} \langle 1010| \otimes \mathbb{1}_{ad}) |\Psi_2\rangle\|^2 \\ &= \chi^4 - \frac{16\chi^6}{3} - \frac{76\chi^8}{5} + O(\chi)^9. \end{aligned} \quad (4.13)$$

For the $P(qrst|ijkl)$ values, I note that since the detectors are all independent of each other, I can write

$$P(qrst|ijkl) = P(q|i)P(r|j)P(s|k)P(t|l). \quad (4.14)$$

Since the photon is either detected or not, each of the individual probabilities in $Pqrst|ijkl)$ can be obtained from the Bernoulli distribution [21]

$$P_\eta(n) = \sum_{m=n}^{\infty} \binom{m}{n} \eta^n (1-\eta)^{m-n} P(m). \quad (4.15)$$

Here $P(m)$ is the probability that m photons were incident, n is the number of photons detected, and m is the number of photons in the incoming mode. In my case, I have for example

$$P(q|i) = \frac{i!}{q!(i-q)!} \eta^q (1-\eta)^{i-q}. \quad (4.16)$$

This is the probability that an imperfect detector with efficiency η would detect q photons, given that a perfect detector would detect i , or that i photons were incoming.

I work within a truncated space such that for a PDC source of efficiency χ , probabilities of $O(\chi^7)$ and higher are ignored. This space is large enough to allow me to predict failures in entanglement swapping due to multi-photon events. The largest probability of such an event occurring is $O(\chi^6)$.

The state often post-selected in entangled state selection experiments is the singlet state, so I examine it here. As we saw in Chapter three, this state would result from a single photon detection event in each of modes c'_H and b'_V or vice versa. Recalling the naming convention for $qrst$, this represents a sequence of 1010 or 0101:

$$\rho_{1010} = \sum_{ijkl} P(ijkl|1010) |\Phi_{ijkl}\rangle \langle \Phi_{ijkl}|. \quad (4.17)$$

The possible values for $ijkl$ in a successful swap (requires at least two photons), if I allow for loss but not dark counts and limit the overall state in the four modes to three photons, are (1010), (1011), (1110), (2010), and (1020). I must sum over these possible states, weighted by the probability of their occurrence, to arrive at the mixed state

resulting from the 1010 detection at the beam splitter:

$$\begin{aligned}
\rho_{1010} &= \sum_{ijkl} P(ijkl|1010) |\Phi_{ijkl}\rangle \langle \Phi_{ijkl}| \\
&= P(1010|1010) |\Phi_{1010}\rangle \langle \Phi_{1010}| \\
&\quad + P(1011|1010) |\Phi_{1011}\rangle \langle \Phi_{1011}| \\
&\quad + P(1110|1010) |\Phi_{1101}\rangle \langle \Phi_{1110}| \\
&\quad + P(2010|1010) |\Phi_{2001}\rangle \langle \Phi_{2010}| \\
&\quad + P(1020|1010) |\Phi_{1002}\rangle \langle \Phi_{1020}| + O(\chi^7).
\end{aligned} \tag{4.18}$$

Given my previously calculated conditional probabilities for these possibilities and my sixth order approximation, the un-normalized states remaining in modes a and d are

$$\begin{aligned}
|\Phi_{1010}\rangle_{\text{un}} &= \left(\frac{\chi^2}{2} - \frac{4\chi^4}{3} + \frac{91\chi^6}{45} + O(\chi^8) \right) |1100\rangle \\
&\quad + \left(-\frac{\chi^2}{2} + \frac{4\chi^4}{3} - \frac{91\chi^6}{45} + O(\chi^8) \right) |0101\rangle \\
&\quad + \left(\frac{\chi^2}{2} - \frac{4\chi^4}{3} + \frac{91\chi^6}{45} + O(\chi^8) \right) |1010\rangle \\
&\quad + \left(-\frac{\chi^2}{2} + \frac{4\chi^4}{3} - \frac{91\chi^6}{45} + O(\chi^8) \right) |0011\rangle.
\end{aligned} \tag{4.19}$$

Here the subscript “un” indicates that this is as yet an un-normalized state. Normalization must be maintained in the quantum state over these optical processes.

$$\|\Phi\rangle = \sqrt{\langle \Phi | \Phi \rangle} = 1$$

$$\begin{aligned}
\| |\Phi_{1010}\rangle_{\text{un}} \|^2 &= 2 \left| \frac{\chi^2}{2} - \frac{4\chi^4}{3} + \frac{91\chi^6}{45} + O(\chi^8) \right|^2 \\
&\quad + 2 \left| -\frac{\chi^2}{2} + \frac{4\chi^4}{3} - \frac{91\chi^6}{45} + O(\chi^8) \right|^2 \\
&= \chi^4 - \frac{16\chi^6}{3} + \frac{76\chi^8}{5} - \frac{2912\chi^{10}}{135} + \frac{331124\chi^{12}}{2025} + O(\chi^{14})
\end{aligned} \tag{4.20}$$

This gives us a normalization factor for the $|\Phi_{1010}\rangle$ state of the square root of the last expression as

$$\| |\Phi\rangle \| = \chi^2 - \frac{8\chi^4}{3} + \frac{182\chi^6}{45} + O(\chi^{13}), \quad (4.21)$$

resulting in

$$\begin{aligned} |\Phi_{1010}\rangle = & \left(\frac{1}{2} + O(\chi^{11}) \right) |1100\rangle \\ & + \left(-\frac{1}{2} + O(\chi^{11}) \right) |0101\rangle \\ & + \left(\frac{1}{2} + O(\chi^{11}) \right) |1010\rangle \\ & + \left(-\frac{1}{2} + O(\chi^{11}) \right) |0011\rangle. \end{aligned} \quad (4.22)$$

Two of these terms are due to two photon pairs emanating from one source and none from the other. I have to post-select this situation out as it would not lead to a successful entanglement swap even with ideal sources and detectors. This post-section is accomplished by projecting onto a subspace corresponding to the situation where there is at least one photon in each of modes a and d . After re-normalizing again I have the final state for this component of ρ_{1010} up to the eighth order in χ

$$|\Phi_{1010}\rangle\langle\Phi_{1010}| = \frac{1}{2}|0101\rangle\langle 0101| + \frac{1}{2}|1010\rangle\langle 1010|. \quad (4.23)$$

Once all five of these relevant states are summed, I have the final expression for the state shared in modes a and d following the detection of modes b' and c' . Prior to post-selection,

the full state is as follows:

$$\begin{aligned}
\rho_{1010} = & \frac{P(1010|1010)}{4} (|1100\rangle\langle 1100| + |0101\rangle\langle 0101| + |1010\rangle\langle 1010| + |0011\rangle\langle 0011|) \\
& + \frac{P(1011|1010)}{4} (|2100\rangle\langle 2100| + |0102\rangle\langle 0102| + |2010\rangle\langle 2010| + |0012\rangle\langle 0012|) \\
& + \frac{P(1110|1010)}{4} (|1200\rangle\langle 1200| + |0201\rangle\langle 0201| + |1020\rangle\langle 1020| + |0021\rangle\langle 0021|) \\
& + P(2010|1010) \left[\frac{1}{4} (|1101\rangle\langle 1101| + |1011\rangle\langle 1011|) \right. \\
& + \left. \frac{1}{8} (|2100\rangle\langle 2100| + |0102\rangle\langle 0102| + |2010\rangle\langle 2010| + |0012\rangle\langle 0012|) \right] \\
& + P(1020|1010) \left[\frac{1}{4} (|1110\rangle\langle 1110| + |0111\rangle\langle 0111|) \right. \\
& + \left. \frac{1}{8} (|1200\rangle\langle 1200| + |0201\rangle\langle 0201| + |1020\rangle\langle 1020| + |0021\rangle\langle 0021|) \right] \\
& + O(\chi^7).
\end{aligned} \tag{4.24}$$

I confirm the accuracy of these calculations by verifying that the resultant state is a density operator. It must be non-negative and have a trace of 1. The state is non-negative by inspection and

$$\text{Tr}(\rho_{1010}) = 1 - O(\chi^7). \tag{4.25}$$

Thus I have calculated the resultant entangled state given two parametric down conversion (PDC) sources, where one mode of each PDC meets at a beam splitter and is subjected to photon counting by inefficient detectors. This state contains terms that do not have photons in both the a and d modes and that would clearly not result in an entangled state. To continue, I must post-select on getting detection in both the a and d modes. To see why this is necessary, I can consider the fidelity between an ideal single photon-pair entangled source and the $|\Psi^-\rangle$ state.

$$\begin{aligned}
|\Psi^-\rangle &= \frac{1}{\sqrt{2}} (|HV\rangle - |VH\rangle) \\
&= \frac{1}{\sqrt{2}} (|1010\rangle - |0101\rangle)
\end{aligned} \tag{4.26}$$

Remembering that $ijkl$ represent modes $a_H a_V d_V d_H$ we have

$$|\Phi_{1010}\rangle = \frac{1}{2} (|1100\rangle - |0101\rangle + |1010\rangle - |0011\rangle), \quad (4.27)$$

and

$$\langle \Phi_{1010} | \Psi^- \rangle = \frac{1}{2\sqrt{2}} + \frac{1}{2\sqrt{2}} = \frac{1}{\sqrt{2}}. \quad (4.28)$$

This indicates that $|\Phi_{1010}\rangle$ is a completely mixed state. However, if I post-select on detecting something in each of the a and d modes, then after re-normalization

$$|\Phi_{1010}\rangle = \frac{1}{\sqrt{2}} (|1010\rangle - |0101\rangle). \quad (4.29)$$

This is the entangled state I am trying to produce and that would result in a fidelity of 1.

Thus, to determine the entanglement present in the resultant ρ_{1010} state, I calculate the fidelity [3] between the post-selected resultant state and the maximally entangled state that would have resulted from a single photon source.

$$f(|\Psi^-\rangle, \rho_{qrst}) = \sqrt{\langle \Psi^- | \rho_{qrst} | \Psi^- \rangle} \quad (4.30)$$

$$\begin{aligned} \langle \Psi^- | \rho_{qrst} | \Psi^- \rangle &= \langle \Psi^- | \sum_{ijkl} P(ijkl|qrst) |\Phi_{ijkl}\rangle \langle \Phi_{ijkl} | \Psi^- \rangle \\ &= \sum_{ijkl} P(ijkl|qrst) \langle \Psi^- | \Phi_{ijkl} \rangle \langle \Phi_{ijkl} | \Psi^- \rangle \\ &= \sum_{ijkl} P(ijkl|qrst) |\langle \Psi^- | \Phi_{ijkl} \rangle|^2 \end{aligned} \quad (4.31)$$

The state I am looking at after post-selection and re-normalization then becomes the following.

$$\begin{aligned}
\rho_{1010} = & \frac{P(1010|1010)}{2} (|0101\rangle\langle 0101| + |1010\rangle\langle 1010|) \\
& + \frac{P(1011|1010)}{2} (|0102\rangle\langle 0102| + |2010\rangle\langle 2010|) \\
& + \frac{P(1110|1010)}{2} (|0201\rangle\langle 0201| + |1020\rangle\langle 1020|) \\
& + \frac{P(2010|1010)}{4} (|1101\rangle\langle 1101| + |1011\rangle\langle 1011| + |0102\rangle\langle 0102| + |2010\rangle\langle 2010|) \\
& + \frac{P(1020|1010)}{4} (|1110\rangle\langle 1110| + |0111\rangle\langle 0111| + |0201\rangle\langle 0201| + |1020\rangle\langle 1020|) \\
& + O(\chi^7)
\end{aligned} \tag{4.32}$$

$$\langle \Psi^- | \rho_{1010} | \Psi^- \rangle = P(1010|1010) \tag{4.33}$$

$$f(|\Psi^-\rangle, \rho_{1010}) = \sqrt{P(1010|1010)} \tag{4.34}$$

For example with $\eta = 0.1$ and $\chi = 10^{-3}$, $f(|\Psi^-\rangle, \rho_{1010}) = \sqrt{0.999995} = 0.999997$. The detector efficiency η is part of the conditional probability as was described in Eq. (4.15), and since my expression for P is dependent on χ , this fidelity is not exactly one.

The entanglement present in the final state in modes a and d decreases with source efficiency as there are more multi-photon pairs generated, leading to error (Fig. 4.1). Multi-photon pairs lead to error as it is possible that the two photons interacting at the beam splitter come from different pairs than those detected at modes a and d . In such a case, the detector clicks would indicate four-fold coincidence, when in fact, entanglement swapping had not taken place.

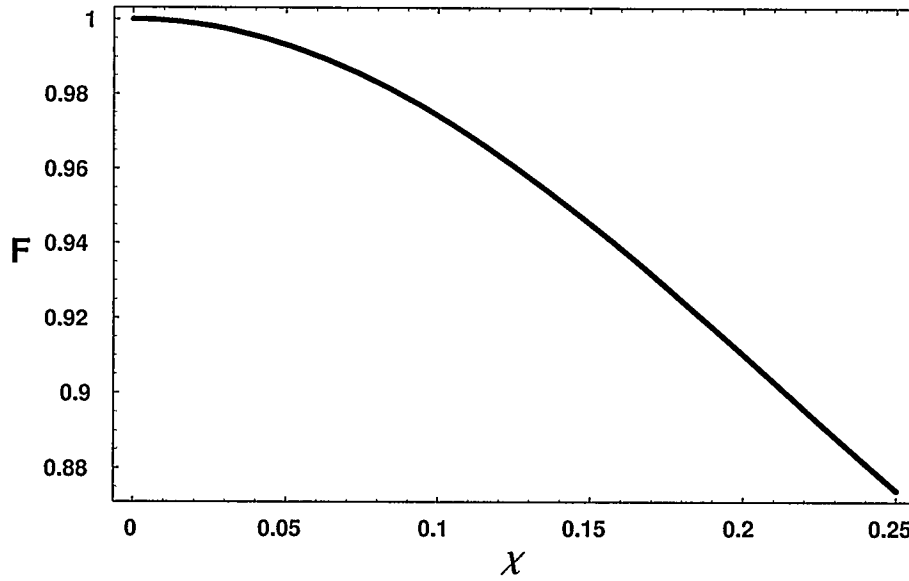


Figure 4.1: Fidelity (F) of entanglement swapping for ρ_{1010} against the source strength χ .

4.2 Summary

I have calculated the shared state remaining at the two end nodes after an entanglement swapping operation to sixth order in the efficiency of the parametric down conversion sources. I have further calculated the fidelity of entanglement of this state with the $|\Psi^-\rangle$ state. The fidelity of entanglement of the final shared photon pair of such a relay is of fundamental importance when this entanglement is subsequently utilized in a further quantum operation such as quantum key distribution. This analysis has not taken into account the effect of dark counts at the detectors. Analysis including dark counts was completed by Artur Scherer subsequent to this work in [26], which I briefly describe in the next chapter.

Chapter 5

Conclusions and Outlook

The thermal detector model I have developed here provides a framework to take into account dark count attributes and input distributions from a variety of sources. This will provide flexibility and consistency in quantum key rate calculations as various sources are utilized in experiment.

The impact of imperfect components, including sources and detectors, must be modeled in order to understand the potential of the experiment under design. Incorrect assumptions about the number of photons present in an input pulse lead to incorrect conclusions about the security of a quantum key exchange. In the case of the BB84 protocol, multi-photon events from the source can lead to a successful photon number splitting attack. In such an attack, the adversary takes one of the identical photons while the other is used in quantum key distillation. The adversary then has one bit of the key after listening to the public discussion during key distillation. In the case of the BBM92 protocol, multi-photon events lead to higher error rates, and subsequently lower secure key generation rates.

The magnitude of the problem of multi-photon events from the source for the BBM92 protocol is of the order of χ^6 , where χ is the efficiency of the source. A term of the order of χ^6 represents the situation where there are three pairs of photons in the relay rather than the ideal two. Two pairs have emanated from one source and one from the other. In this situation, detector clicks may indicate a successful swap when that was not the case.

5.1 Closed Form Solution

The lowest order in source efficiency for which multi-photon sources causes errors for entanglement swapping is χ^6 , and my perturbative work of the previous chapter looked at the entanglement swap to that level of accuracy. My colleague Artur Scherer subsequently re-examined the mathematics involved in the issue and found a closed form solution that includes all multi-photon contributions from the parametric down conversion sources [26]. This formulation allows for simpler calculations and incorporation of the dark count model.

The closed form expression for $|\Phi_{ijkl}\rangle$ in Eq. (4.10) is

$$\begin{aligned}
 |\Phi_{ijkl}\rangle &\equiv \frac{1}{\sqrt{i!j!k!l!}} \left(\frac{\hat{d}_H^\dagger - \hat{a}_H^\dagger}{\sqrt{2}} \right)^i \left(\frac{\hat{d}_V^\dagger - \hat{a}_V^\dagger}{\sqrt{2}} \right)^j \left(\frac{\hat{a}_V^\dagger + \hat{d}_V^\dagger}{\sqrt{2}} \right)^k \left(\frac{\hat{a}_H^\dagger + \hat{d}_H^\dagger}{\sqrt{2}} \right)^l |\text{vac}\rangle \\
 &= \frac{1}{(\sqrt{2})^{i+j+k+l} \sqrt{i!j!k!l!}} \sum_{\mu=0}^i \sum_{\nu=0}^j \sum_{\kappa=0}^k \sum_{\lambda=0}^l (-1)^{\mu+\nu} \binom{i}{\mu} \binom{j}{\nu} \binom{k}{\kappa} \binom{l}{\lambda} \\
 &\quad \times (\hat{a}_H^\dagger)^{\mu+\lambda} (\hat{a}_V^\dagger)^{\nu+\kappa} (\hat{d}_H^\dagger)^{i+l-\mu-\lambda} (\hat{d}_V^\dagger)^{j+k-\nu-\kappa} |\text{vac}\rangle. \tag{5.1}
 \end{aligned}$$

Evaluating $|\Phi_{1010}\rangle$ using this formula reproduces Eq. (4.27) to within an overall phase.

The closed form expression for the corresponding probability of the hypothetical ideal measurement readout $(ijkl)$ is

$$p(ijkl) = \frac{[\tanh \chi]^{2(i+j+k+l)}}{\cosh^8 \chi}. \tag{5.2}$$

Expanding this expression to sixth order in χ for comparison with my perturbative method, I find for example

$$p(1010) = \chi^4 - \frac{16\chi^6}{3} - \frac{76\chi^8}{5} + O(\chi^9), \tag{5.3}$$

in perfect agreement with Eq. (4.13).

5.2 Incorporating Dark Counts

Most experimental analyses discuss the visibility of an entanglement swap rather than the fidelity:

$$V = \frac{R_{\text{Max}} - R_{\text{Min}}}{R_{\text{Max}} + R_{\text{Min}}}, \quad (5.4)$$

where R_{Max} and R_{Min} are the maximum and minimum coincidence rates between four detectors in a successful entanglement swap. For a single qubit state, visibility relates to fidelity as $V = 2F - 1$ [22]. For a two qubit state, the relation is $V = \frac{4F-1}{3}$.

The work I have presented here has been taken further by my co-author Artur Scherer [26]. Once dark counts at the detectors are taken into account, the visibility of the entanglement swap versus efficiency of the source χ initially rapidly rises and then falls off (Fig. 5.2). For a two qubit state such as we have here, fidelity ranges from 0.25 to 1 while visibility ranges from 0 to 1. In Fig. 5.2 it is clear that at low values of source efficiency, dark counts dominate and destroy the visibility of the swap. Once source rates are appreciably larger than dark count rates, the visibility rises quickly. Maximum visibility occurs at a relatively low source efficiency below 10^{-2} . This is due to the detrimental effect of multiple pairs being generated from the source as source intensity grows.

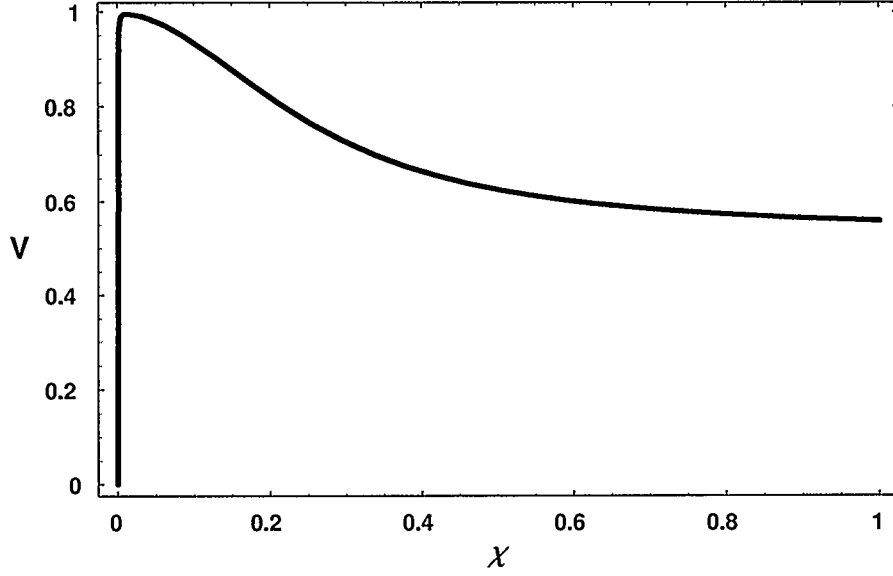


Figure 5.1: Visibility of entanglement swap against the source efficiency χ with a variety of detector efficiencies and dark count rates ranging from 1×10^{-5} to 3×10^{-5} .

5.3 Effect on Key Rate

When employing entanglement swapping operations to quantum key distribution, poor visibility of the swap affects the rate at which secret key bits can be generated. The secret key rate decreases proportionally to the binary entropy of the quantum bit error rate (QBER) as

$$R_{\text{sec}} = \frac{1}{2} \frac{1}{2} \chi^2 \chi^2 \eta_1^2 \eta_2^2 (1 - K h_2(\text{QBER}) - h_2(\text{QBER})). \quad (5.5)$$

One factor of one half is due to key sifting: Alice and Bob discard all bits where they did not measure in the same basis. The another factor of one half is due to the fact that the optical beam splitter is only 50% efficient. The two separate values for χ^2 allow for two sources of different efficiency. The two separate values of η^2 allow for different detector efficiencies at the end nodes as compared to the Bell state measurement, recalling that a four-fold coincidence is required. K is a factor related to error correction, the first binary entropy (h_2) term is for error correction and the second is for privacy amplification. For

each bit of error, the bits in the final key string have to be either corrected or discarded, both of which result in shorter final key strings and thus lower key generation rate.

The quantum bit error rate is related to visibility as $QBER = \frac{1-V}{2}$ [14]. Thus, the greater the visibility, the lower the quantum bit error rate. Redefining fidelity as $F = f^2 = \langle \Phi^- | \rho_{qrst} | \Phi^- \rangle$, gives a relation of $QBER = \frac{1-2F}{3}$. However, since the source and detector efficiencies have significant impact on the overall secret key rate as detailed in Eq. (5.5), it is insufficient to simply maximize visibility or fidelity to achieve maximum key rate.

5.4 Summary

The methods provided in this thesis provide base components needed to develop a model that will determine the best source efficiency to employ in an entanglement swapping system to ensure maximal entanglement in the final modes. My efforts have been expanded upon by my fellow researcher Artur Scherer to develop such a model. Maximizing entanglement fidelity or visibility may be only one of the factors that need to be considered for the application of interest. However, as a fundamental resource in a number of quantum processes, maximizing entanglement fidelity will surely be of interest.

Bibliography

- [1] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85(6):1330–1334, August 2000.
- [2] S. Singh. *The Code Book*. Anchor Books, New York, 1999.
- [3] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
- [4] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. unpublished manuscript written ca 1970.
- [5] C. H. Bennett and G. Brassard. Quantum cryptography, and its application to provably secure key expansion, public-key distribution, and coin tossing. In *Proceedings of the International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE, New York, 1984. Bangalore, India.
- [6] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, July 2000.
- [7] D. C. Burnham and D. L. Weinberg. Observation of simultaneity in parametric production of optical photon pairs. *Phys. Rev. Lett.*, 25(2):84–87, July 1970.
- [8] A. K. Ekert. Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.*, 67(6):661–663, August 1991.
- [9] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell’s theorem. *Phys. Rev. Lett.*, 68(5):557–559, February 1992.

- [10] P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75(24):4337–4341, December 1995.
- [11] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81(26):5932–5935, December 1998.
- [12] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76(5):722–725, January 1996.
- [13] D. Collins, N. Gisin, and H. de Riedmatten. Quantum relays for long distance quantum cryptography. *Journal of Modern Optics*, 52(5):735–753, March 2005.
- [14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, March 2002.
- [15] S. D. Bartlett and B. C. Sanders. Universal continuous-variable quantum computation: Requirements of optical nonlinearity for photon counting. *Phys. Rev. A*, 65(4):042304, March 2002.
- [16] F. Zappa, A. Lacaita, S. Cova, and P. Webb. Nanosecond single-photon timing with InGaAs/InP photodiodes. *Optics Letters*, 19(11):846–848, June 1994.
- [17] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. A framework for practical quantum cryptography. [arXiv.org:0802.4155](https://arxiv.org/abs/0802.4155), February 2008.
- [18] L. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, Cambridge, 1995.

- [19] P. P. Rohde and T. C. Ralph. Modeling photo-detectors in quantum optics. *Journal of Modern Optics*, 53(11):1589–1503, July 2006.
- [20] A. A. Semenov, A. V. Turchin, and H.V. Gomonay. Detection of quantum light in the presence of noise. *Phys. Rev. A*, 78(5):055803, November 2008.
- [21] U. Leonhardt. *Measuring the Quantum State of Light*. Cambridge University Press, Cambridge, 1997.
- [22] H. de Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden, and N. Gisin. Long distance entanglement swapping with photons from separated sources. *Phys. Rev. A*, 71(5):050302, May 2005.
- [23] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. ‘Event-ready-detectors’ Bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71(26):4287–4290, December 1993.
- [24] S. D. Bartlett, D. A. Rice, B. C. Sanders, J. Daboul, and H. de Guise. Unitary transformations for testing Bell inequalities. *Phys. Rev. A*, 63(4):042310, March 2001.
- [25] A. A. Bruen and M. A. Forcinito. *Cryptography, Information Theory, and Error-Correction*. John Wiley & Sons, Inc., Hoboken, 2005.
- [26] A. Scherer, R. B. Howard, B. C. Sanders, and W. Tittel. Quantum states prepared by realistic entanglement swapping. *Phys. Rev. A*, accepted, arXiv.org:0904.1184, October 2009.