Squashing Models for Optical Measurements in Quantum Communication

by

Normand James Beaudry

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Science
in
Physics

Waterloo, Ontario, Canada, 2009

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Many protocols and experiments in quantum information science are described in terms of simple measurements on qubits. However, in an experimental implementation, the exact description of the measurement is usually more complicated. If there is a claim made from the results of an experiment by using the simplified measurement description, then do the claims still hold when the more realistic description is taken into account? We present a "squashing" model that decomposes the realistic measurement description into first a map, followed by a simplified measurement. The squashing model then provides a connection between a realistic measurement and an ideal measurement. If the squashing model exists for a given measurement, then all claims made about a measurement using the simplified description also apply to the complicated one. We give necessary and sufficient conditions to determine when this model exists. We show how it can be applied to quantum key distribution, entanglement verification, and other quantum communication protocols. We also consider several examples of detectors commonly used in quantum communication to determine if they have squashing models.

Acknowledgements

First and foremost I would like to thank my supervisor, Norbert Lütkenhaus. I am grateful for his support and insight; they were instrumental to the research leading to this thesis. His precise vision and approach to research has greatly influenced me.

Many thanks to the members of my committee, Norbert Lütkenhaus, Kevin Resch, Michele Mosca, and Joseph Emerson, for their time and feedback.

I would like to thank those whom I have collaborated with: Tobias Moroder, Agnes Ferenczi, Marco Piani, Xiaofeng Ma, Cayle Castor, Ruben Romero-Alvarez, and Otfried Gühne. I would also like to thank the members of the optical quantum communication theory group, especially Agnes Ferenczi, for many helpful discussions.

Thank you to my parents for their continued support.

This research was funded by SECOQC, QAP, NSERC, Quantum Works, OCE, and CSEC.

Contents

List of Figures

Chapter 1

Introduction

Communication technology plays an important role in today's society. Many communication tasks are now possible since the expansion of the internet in the past fifteen years: everything from email to internet banking. All of current communications technology only uses classical communication. However, quantum communication enables new communication tasks that are otherwise impossible using classical communication. Quantum cryptography, for example, allows for a different level of security from classical cryptography.

The problem of implementing quantum communication protocols lies in the fragility of quantum systems. They require extreme precision and control in order to be used effectively. In theory, quantum systems can be simply described, and quantum communication protocols are often devised using small dimensional, simple quantum states. However, in experiments, we currently do not have the control required to create these simple systems exactly. This creates a gap between what systems quantum communication protocols require in theory, and what experimentalists actually use in practice. This begs the question: if an experimentalist implements a quantum communication protocol inexactly, do the claims of any theories requiring an exact implementation still hold true? This thesis tries to answer this question in part, and in particular, we focus on bridging the gap between measurements required in theory, and measurements performed in practice.

First, we give some background on the field of quantum communication. In particular we outline two quantum communication protocols: quantum key distribution and entanglement verification.

1.1 Quantum Communication

Quantum communication is a broad field containing all uses for communication using quantum signals. In contrast, signals in classical communication are called bits, with value either "0" or "1". In quantum communication, signals are typically quantum bits, or qubits. They are represented by a quantum system

with two levels $|0\rangle$ and $|1\rangle$. In experiments, these signals are typically realized using single photons, and information is encoded in one of their degrees of freedom. For example, the polarization of the photon may be used for this purpose: horizontally polarized light could represent the state $|0\rangle$ and vertically polarized light could represent the state $|1\rangle$.

Since quantum signals are used for communication, it can be advantageous for communicating parties to have other quantum mechanical resources at their disposal. For example, many of the protocols in quantum communication take advantage of one of the most striking features of quantum mechanics: entanglement. Entangled states such as $|\psi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ have the property that they cannot be factored into a separable form $|\psi^+\rangle \neq |\phi_A\rangle \otimes |\phi_B\rangle$. This means that there is a strong correlation between the two systems A and B that cannot be represented in a classical way; entanglement is a purely quantum phenomenon. Entanglement is an essential part of quantum communication as it enables many protocols.

For example, there is a quantum communication protocol called superdense coding [BW92] that uses entanglement to communicate two classical bits of information by only sending a single qubit from one party to another. More precisely, each party begins with one qubit of a two-qubit entangled state, such as $|\psi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$. Then the party who wishes to communicate information (usually called Alice) applies a quantum operation on her qubit that depends on which two bits Alice would like to communicate. She then sends her modified qubit to the receiving party (usually called Bob), who jointly measures the qubit Alice sent and his qubit. From this measurement he gets two classical bits. In this way, Alice communicates two bits of information only by sending a single qubit to Bob (with the help of shared entanglement). Superdense coding is just one of many protocols that demonstrate how quantum communication can accomplish tasks that cannot be done by only using classical systems.

There are many other interesting and useful tasks in quantum communication that cannot be performed by only using classical communication, such as quantum teleportation [BBJ$^+$93]. In this thesis we will primarily focus on two such tasks: quantum key distribution, commonly known as QKD, and entanglement verification. However, the results presented in this thesis, Chapter 2 in particular, are more general: they can be applied to many different quantum communication protocols. We now describe these two quantum communication protocols in the following sections.

1.1.1 Quantum Key Distribution

The goal of quantum key distribution (QKD) is to securely distribute a random binary string (a key) between two parties (usually called Alice and Bob) over a public quantum channel. The key generated in QKD can be used in different ways, but typically it is used by Alice and Bob to communicate classically in a secure way. In particular, Alice adds the generated key to a classical binary message, and sends this encrypted message to Bob. Bob then adds the key to the encrypted message to decipher the original message. An eavesdropper can

get no information out of the encrypted message, because to her it is just a list of random 0s and 1s. This method of communication can be proven secure in a more rigorous way, and is called the one time pad (or Vernam cipher [Ver26]) (see Fig. 1.1.1).

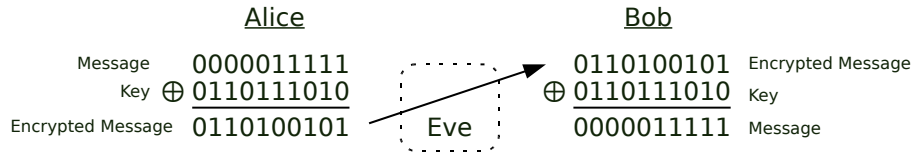

Figure 1.1: The use of the one time pad to encode a message. Alice adds the message she would like to send to the key she shares with Bob. She sends the key over a classical channel to Bob, and an eavesdropper, Eve, may see the encrypted message. Bob adds the encrypted message to the key, and he decrypts the original message. Eve can gain no information about the message because all she sees is the encrypted message: a list of random binary numbers.

The challenge of QKD is to distribute a random binary string by sending quantum signals from one party to another. An eavesdropper, usually called Eve, may interfere with the quantum signals sent. Her goal is to gain as much information about the signals as she can. However, to learn information about the signals, she must modify them, and hence introduce errors in Bob's measurement. Therefore, Eve is trying to maximize the amount of information she can get while trying to minimize the errors she introduces. In addition, Eve is allowed to use anything possible by quantum mechanics to extract information from the quantum signals between Alice and Bob. Despite Eve's powerful attack, it is still possible to perform QKD, as long as the errors observed by Bob are below a certain threshold. To see how QKD is possible, we give a brief outline of the BB84 protocol, one of the first QKD protocols, named after its creators and the year of its invention [BB84].

The BB84 protocol

The BB84 protocol, as well as most other QKD protocols, are broken down into two steps. In the first, Alice sends quantum signals to Bob. In the second, Alice and Bob communicate classically in order to perform some post-processing on their measurement outcomes.

In the first step, Alice randomly chooses one of four states given by the eigenstates of the Pauli operators σ_x or σ_z. The states are grouped into two bases, one for each Pauli operator. In the z basis the states are $|0\rangle$, and $|1\rangle$, while the states in the x basis are $|0_x\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$, and $|1_x\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$. Bob then either chooses a projective measurement that unambiguously discriminates between the states in the x basis or in the z basis. For example, in the z basis, Bob's measurement operators are $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$. If Bob chooses the same basis Alice chose, then Bob determines the bit value (either 0 or 1)

that Alice wanted to send him. If Bob chooses the basis Alice did not choose, he will measure a random bit.

In the second step, after Bob measures the signals sent by Alice, Bob reveals the basis he measured in for each signal. Alice then tells him when he measured in a different basis, in which case they throw away that bit value. When Bob measured in the same basis they keep that bit value. The security of the protocol lies in the fact that Eve does not know beforehand which basis Alice has chosen to send the signals in. This means Eve cannot discriminate between all four possible states Alice could have sent.

Alice and Bob share a small portion of their measurement results with each other in order to estimate how many errors are introduced in the communication of their signals. If Alice and Bob determine that their estimated error rate is below a certain threshold, they proceed with the protocol. Otherwise, they abort the protocol because the large amount of errors implies that an eavesdropper may have tried to gain lots of information about the quantum signals. If the error rate is low enough, Alice and Bob continue with two post-processing steps. First there is error correction, to remove any errors that differ between Alice and Bob's keys. Then they perform privacy amplification, which shortens the length of their key in order to remove any information the eavesdropper may have on the key.

Now that we have outlined the two phases of the BB84 protocol, we now discuss the security of QKD protocols, including the BB84 protocol.

Proving Security

It is important to note that the desired security of the BB84 protocol, as well as other QKD protocols, is what is called "unconditional". This means that despite the eavesdropper being able to do anything allowed by quantum mechanics, Alice and Bob can still perform QKD and form a secret key. In addition, an eavesdropper will never be able to determine the key any time in the future, as long as the key is used in a smart way (for example, using the one time pad). This is quite different from the security claims of classical cryptographic protocols. Classical cryptography claims of security usually depend upon assumptions about the difficulty of a mathematical problem, and on the computational power or memory capacity of an eavesdropper. In addition, some of the problems that are assumed to be difficult, are not difficult for quantum computers. If large-scale quantum computing becomes possible, then these cryptography protocols are no longer viable. However, QKD is robust against (the existence of) quantum computers, and is still secure. The security claims in QKD are stronger as well, because they only depend upon two things: the validity of quantum mechanics, and that the protocol is performed exactly as outlined in the security proof. For more details on the comparison of QKD to other cryptography methods, see [SML09].

In order to prove security for a given QKD protocol, a model is assumed to describe the different components used in the protocol. For example, a source of photons may be assumed to output only single photons. Also, an assumption

may be made about the eavesdropper, to limit her output to Bob's detector as being only single photons. Then Bob's measurement description is only required for the single photon and vacuum subspace, since these are the only signals he receives. The assumption that simple systems are used and measured greatly simplifies proving security. If these assumptions are not made, security proofs for QKD protocols become extremely difficult. This is also true of quantum communication in general: unless simple systems are assumed in a theory, it can be very difficult to make any useful statements about a given quantum communication protocol.

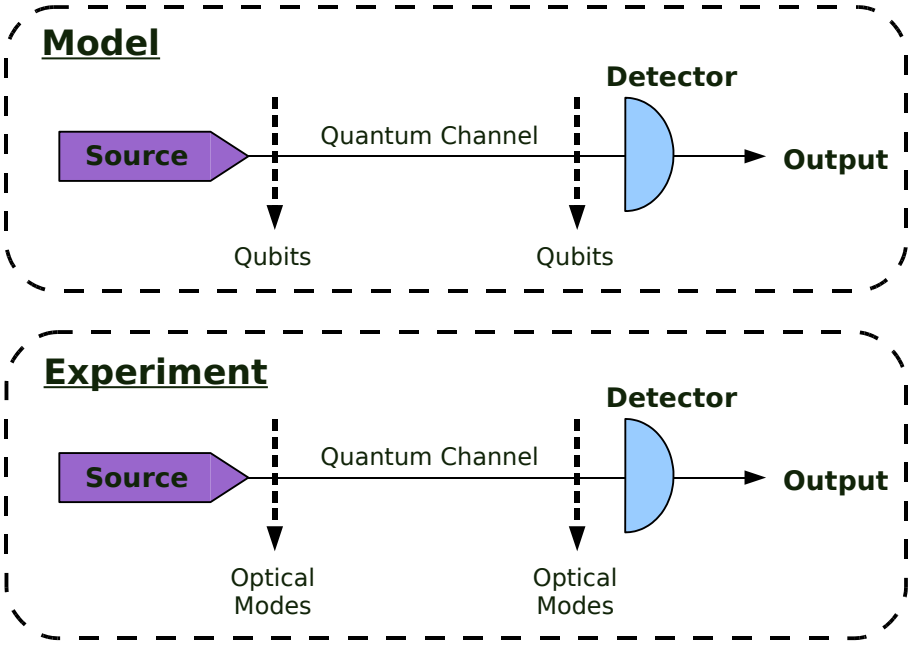

Figure 1.2: Above: A model of a quantum communication protocol. It has a source that outputs qubits, which go through a quantum channel that outputs qubits to a measurement. Below: An experimental implementation of the modelled quantum communication protocol. A source outputs optical modes which then go through a quantum channel that outputs optical modes to a measurement.

However, any assumptions made about a quantum communication or QKD protocol in theory are not necessarily valid in its experimental implementation (see Fig. 1.1.1. For example, current technology only allows for approximate sources of single photons. Usually these sources output single photons or the vacuum. However, they also have a small probability of outputting multi-photon signals. One example of an experimental photon source is weak laser pulses, which are formed by a weakly powered laser that outputs a Poissonian distribution for the output number of photons. This means usually no photon (the

vacuum) is created, sometimes a single photon is created, and with a small probability more photons are output. Another example of a single photon source is parametric down conversion (PDC). In PDC a laser shines on a nonlinear crystal producing the vacuum most of the time, two photons some of the time, and a higher number of photon pairs occasionally. The pairs of photons emitted are spatially separated, and so a detector is used to measure when photons are emitted on one of the spacial outputs. When this detector fires, it means that one or more photons were emitted in the other spacial mode. The signals from this other spacial mode are used as an approximation of a single photon source.

In addition, Eve is not restricted to sending Bob single photons. She should be allowed to send any optical signal she likes. This, combined with imperfect single photon sources, creates a different description of the protocol from what is required in a QKD security proof. Therefore, it is important to be able to connect the security proof that assumes a simple description to the more realistic experimental implementation. One approach would be to do another security proof using a more realistic model for the source and the detector. Consider the scenario where a weak laser is used as an approximate source of single photons. The state output by such a laser is called a *coherent state*, and is of the form

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{1.1}$$

where α is a positive constant, and n is the photon number. Since the sum is over all photon numbers, this state is in an infinite dimensional Hilbert space. This makes a new security proof taking an infinite dimensional Hilbert space into account a challenging task. Instead, it would be convenient to be able to use one or more theoretical tools to say that the security proof that assumes the use of simple systems can also apply to the more realistic experimental implementation.

One tool used to connect security proofs with more complicated implementations is called *tagging* [Lüt99a, Lüt00]. More specifically, tagging connects an experimental source that may be complicated to a theoretical small-dimensional source. To illustrate how tagging works, consider the weak laser source that outputs coherent states (Eqn. 1.1). Suppose that we would like a single photon output from a source for a QKD security proof. Then, when a multi-photon signal is created we assume that a complete classical description of the output state is forwarded to Eve. In the BB84 protocol this means that Eve would discover which basis and bit value Alice has sent, and hence does not introduce any errors in trying to learn information about these signals. Therefore any errors that Eve may introduce by trying to learn the signals are all attributed to the single photon signals sent by the source. Taking into account the probability that single photon signals are created allows the error rate for the single photon contributions to be rescaled, and hence increased. Therefore, under the tagging argument, we take a pessimistic view that ensures that Eve does not get an advantage by exploiting multi-photon signals from the source. This means that the simple security proof may be applied to the scenario when there is a source

with multi-photon contributions.

It would also be desirable to make a similar argument to remove the assumption that Eve sends single photons to Bob. This is one of the goals of this thesis: to show that a theoretical tool exists that can connect simple measurement descriptions with a more realistic, experimental description. In QKD, this has been an assumption that has been made in many security proofs (cf. [GLLP04]) where a model exists in which Eve is forced to restrict her output to a single photon. This thesis will verify under which conditions this model holds. Moreover, this model is not restricted to QKD, it has many other applications in quantum communication, as will be demonstrated.

1.1.2 Entanglement Verification

The assumption that single photons are measured at a detector has not only been made in QKD, but is also made in an area of quantum communication called entanglement verification. Entangled states are a critical resource for many quantum communication protocols, and so it is important to be able to verify that entangled states are indeed created in an experiment. The goal of entanglement verification is to be able to say whether or not a given state is entangled. There are various tests that can be used to verify entanglement, such as Bell inequalities [Bel64]. Entanglement can also be verified by state tomography where a set of measurements are performed in order to completely determine the state. The state can then be checked against necessary and sufficient conditions to verify if the state is entangled.

Here we focus on state tomography, in order to simplify our analysis. In order to do tomography, a particular set of measurements must be performed. We use a positive operator valued measure (POVM) to describe the measurement, which has noncommuting POVM elements. For tomography the POVM elements must form an operator basis for the Hilbert space of the entangled state. A reconstruction technique is then performed using the measurement results to reconstruct the state. For example there is the inversion of Born's rule, and maximum likelihood estimation [Hra97]. The inversion of Born's rule is inverting the linear constraints given by the expectation values obtained from the measurement on the density operator: $E_{i,j} = \mathrm{Tr}(\rho_{AB} F_A^{(i)} \otimes F_B^{(j)})$, where $E_{i,j}$ are the expectation values, ρ_{AB} is the density operator, and $F_A^{(i)}, F_B^{(j)}$ are the POVM elements for the measurements on the two photons. The method of maximum likelihood estimation finds a state that is most likely to come from the measurement data. However, an additional assumption about the dimension of the input space must be made in order to use this method effectively.

Regardless of the reconstruction technique, if the reconstructed state is entangled, then entanglement of the source's state is verified.

As an example, entanglement verification of polarized photons is typically done by having a PDC source that outputs entangled two-photon states, and each photon is measured with a separate measurement device. However, the PDC source may output states with more than two photons. In this case it may

be assumed that some of the measurement results come from the tomography of a two-photon entangled state, but in fact come from a higher-dimensional state output by the PDC source. The question arises then: if the state lives in a higher dimensional Hilbert space than that considered in the reconstruction technique, is entanglement still verified? The answer to this question involves a similar model to that used in QKD considered previously. If this model exists, then entanglement verification of a simplified description also implies entanglement is verified for a larger dimensional description. In this thesis we will show under what conditions this model exists.

1.2 Contributions

In Chapter 2 we describe a "squashing" model for a measurement on a large Hilbert space. This large measurement is modelled by a physical map followed by a measurement on a small Hilbert space. This is a convenient decomposition because the map and simplified measurement do not need to be implemented experimentally, they are only a theoretical equivalent to the large measurement. We provide necessary and sufficient conditions to determine whether a squashing model exists. The implication of having such a model in a quantum communication protocol is as follows. If a squashing model exists for a measurement used in a quantum communication protocol's implementation, then it is valid to assume that the measurement has a small dimensional description. In the context of QKD, the existence of a squashing model means that a security proof that requires single photons or qubits to be measured also apply to the QKD protocol's full optical implementation. In the context of other quantum communication protocols, the squashing model allows theories that require measurements to be performed on small dimensional systems to also apply to the full optical implementation of these protocols.

In addition, we consider several examples of detectors used in quantum communication, and in particular QKD, to determine whether a squashing model exists for them. We provide a method in order to always find a squashing model between any two measurements, given some conditions. We also use the squashing model formalism to determine if multiple time modes, as well as multi-photon signals can be reduced to a single time mode single photon signal. We consider how to deal with imperfections such as inefficiencies and dark counts in the context of the squashing model.

The work on the squashing model in Chapter 2 was done in collaboration with Tobias Moroder and Norbert Lütkenhaus. The details of this work are contained in the papers [BML08, BML09].

In Chapter 3 we show how the squashing model introduced in Chapter 2 applies to entanglement verification. In particular, we present necessary and sufficient conditions under which a squashing model exists for entanglement verification. These conditions are similar to those in Chapter 2, except the physical map need not be physical in the context of entanglement, it is only required to be positive. We reference a proposition that allows an alternative

way from the formalism developed in Chapter 2 to find a squashing model in the context of entanglement verification: if tomography is performed in the small dimensional measurement of the squashing model, then the squashing model exists if and only if the set of states compatible with the outcomes of the large dimensional measurement are contained within the same set for the small dimensional measurement [MGB$^+$09]. We use this proposition to show how a measurement used for tomography of polarized single photons has a squashing model for entanglement verification, even though it does not have a squashing model in the context of Chapter 2.

The work on the squashing model used for entanglement verification in Chapter 3 was done in collaboration with Tobias Moroder, Otfried Gühne, Marco Piani, and Norbert Lütkenhaus. The details of this work are contained in the paper [MGB$^+$09].

Chapter 2

The Squashing Model

2.1 Motivation

Quantum communication protocols typically require that single photons are measured at one or more measurements. However, many implementations of quantum communication protocols do not achieve this. For example, a source may occasionally output multiple photons, and then measurements are performed on its output. In QKD the eavesdropper, Eve, is not restricted to sending single photons to the receiver, Bob, she can send any signal with any number of photons (*i.e.*states in a Fock space). These photons can also be sent using whatever optical modes Eve would like. For example, she can change the frequency, polarization, or relative phase of the photons she sends. In QKD, it has been assumed that there exists a model that equates a measurement on optical modes to one that is first preceded by a map that reduces (squashes) the incoming signal to a single photon or the vacuum. The output of this map is input to the same measurement, but now on a low-dimensional Hilbert space [GLLP04]. As an example, there is the measurement performed in the polarization implementation of the BB84 protocol [BB84], where the input goes to a polarizing beam splitter that can be set to separate in one of two bases: either the horizontal/vertical basis (labelled as z) or the +45/-45 degree basis (labelled as x) (see Fig. 2.1). At the end of each arm of the polarizing beam splitter there is a threshold photodetector that cannot resolve the number of incoming photons. If a random choice of basis is done with fixed probabilities, then this measurement can be described by a single POVM with noncommuting POVM elements. This detector has been assumed to have a squashing model, such as in the important simulation [MFL07].

This chapter will specify how to determine whether such a squashing map exists. However, the goal of the squashing model is more general. It is to reduce any large-dimensional measurement to a corresponding small-dimensional one. This provides a powerful tool that can be used to simplify the analysis of optical implementations of quantum communication protocols.

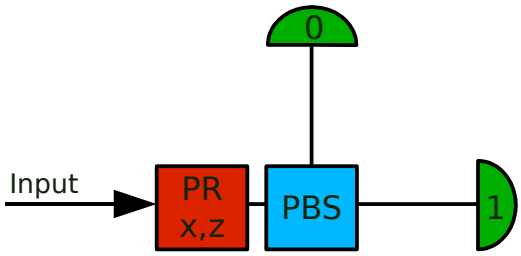

Figure 2.1: The BB84 measurement with an active basis choice. The input goes into a polarization rotator that Bob sets to choose the basis (x or z) he would like to measure. Next there is a polarizing beam splitter that splits between two orthogonal polarization modes, followed by two threshold detectors, which cannot resolve the incident photon number. Bob associates a bit value with each threshold detector, so when one clicks, he records the corresponding bit value.

Also, in the context of QKD, one typically assumes the *calibrated device scenario* in which the detection device is trusted and known. This means that the eavesdropper does not get any information from the measurement device, and Bob has complete control over its settings (for example, the basis he would like to measure). In addition, Bob knows the POVM elements that accurately describe his measurement. This is required in order to find a squashing model, because it depends on the structure of the measurement performed. Then if a squashing model exists, the corresponding squashing map can become part of the eavesdropper's (Eve's) attack, since it occurs right before Bob's measurement. This means that Eve can do whatever attack allowed by quantum mechanics, but at the end of her attack there is the fixed squashing map, which reduces her output signal to a single photon or the vacuum, which is forwarded to Bob. Therefore the existence of the squashing model validates the assumption that, without loss of generality, Eve sends a signal in a qubit and vacuum Hilbert space to the receiver, Bob.

As an example, many security proofs of QKD protocols assume that Eve forwards polarized single photons (qubits) or vacuum states to the receiver. If a given full optical implementation of a polarization measurement used by Bob has a squashing model connecting it to the single photon polarization measurement assumed in the security proof, then this proof is also valid for the full optical implementation of the protocol. Note that our result has implications for measurements beyond those used in QKD, for example, in entanglement verification (Chapter 3), and others (Section 2.8).

Additionally, squashing the detection to a finite-dimensional system from a large- or infinite-dimensional system makes it possible to use the fast converging de Finetti theorems of Renner [Ren07] on the level of the squashed system. In QKD this implies that Eve's attack can be assumed, without loss of generality,

to be simpler than the most general attack she could do. More specifically, she is restricted in applying a collective attack. This means that Eve attacks each signal identically, but she does not need to measure any systems she uses for her attack until a time in the future of her choosing. For a recent review of QKD, including the different classes of attacks Eve can perform that have been studied in the literature, see [SBPC$^+$].

First, in Section 2.2 we define a squashing model more precisely and describe a formalism to find whether a squashing model exists given a realistic model for the detector, and a simplified, desired description. Then, in Section 2.3 we discuss the reduction of the squashing map to finite dimensions. We use this reduction to apply the formalism to examples of detectors commonly used in quantum communication to find if they have squashing models. In Section 2.4 we show that any detector has a squashing model, as long as enough noise is added to the incoming signals and the measurement. Section 2.5 generalizes the examples considered previously to give a squashing map which takes a multi-mode input to a single mode input. In Section 2.6 we consider imperfections such as inefficiencies and dark counts in the context of the squashing model. Next, Section 2.7 discusses some numerical results that either shows there is not a squashing model for certain examples, or suggests that one may exist. Finally, we present how the squashing model is useful in other quantum communication applications (Section 2.8), and some interesting continuations of the squashing model (Section 2.9).

2.2 Formalism

In this section, we provide the description of a formalism that is used throughout this thesis. We begin by defining a squashing model more precisely.

2.2.1 Definition of a Squashing Model

Consider a given experimental setup made up of two parts: a known physical measurement, whose output goes into a post-processing on the raw detection events output by the physical measurement. Together, the physical measurement and the post-processing, we call the full measurement. We would like to equate this measurement to a given small-dimensional measurement, which we call the target measurement. Then a squashing model is the representation of this high-dimensional full measurement, F_M, and a squashing map, Λ, followed by the low-dimensional target measurement, F_Q (see Fig. 2.2). Throughout this thesis, the letter F is used to represent a POVM element. The subscript M corresponds to the full measurement, and stands for "mode", while Q corresponds to the target measurement, and stands for "qubit" (although this measurement may be on any small-dimensional Hilbert space, and not necessarily a qubit). The POVM elements F_M are in the Hilbert space $\mathcal{H}_M$ and the POVM elements F_Q are in the Hilbert space $\mathcal{H}_Q$.

The classical post-processing performed after the full measurement may be

desired due to the quantum communication protocol being performed, and is hence included in the squashing model. Alternatively, there may be events that occur in the full measurement that do not correspond to events in the target measurement. In order to deal with these extra events, they are assigned in a particular way to one or more of the valid outcomes of the small-dimensional measurement.

In the squashing model, it is required that the model (the map and the target measurement) and the full measurement are statistically equivalent. In other words, the probability of any outcome of the measurement F_M for any input is the same as the probability of any outcome of the measurement F_Q when it is preceded by a specific squashing map. If a squashing map exists such that this condition holds, then the full measurement F_M has a squashing model with respect to the target measurement F_Q.

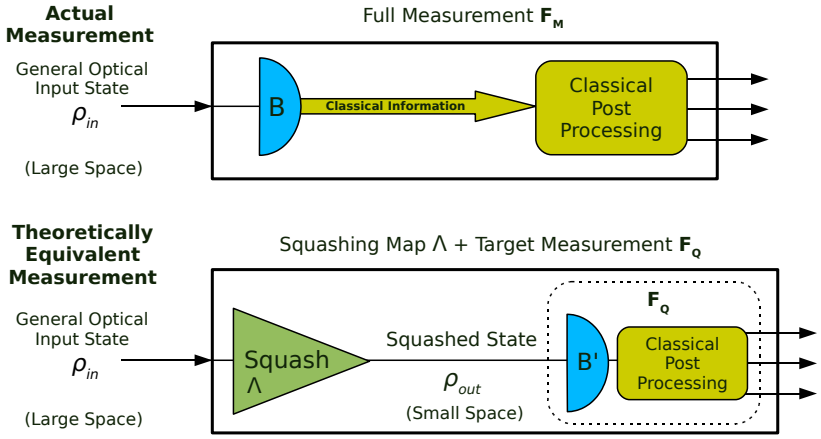

Figure 2.2: The full measurement F_M (above) has a general optical input ρ_{in}, which is first measured by a receiver's physical detector B, followed by classical post-processing. The squashed measurement (below) has the same general optical input ρ_{in}, which is then squashed by a map Λ to a smaller Hilbert space, followed by the target measurement F_Q, which consists of a physical measurement B' (that may be different from B) followed by a classical post-processsing. It is required that both of these measurements produce the same output statistics for all ρ_{in}.

The existence of a squashing model connecting a given fixed full measurement and target measurement depends on the existence of a squashing map that precedes the target measurement. A physical map that does this must be a trace-preserving completely positive map, Λ. We can formulate the restriction on the map Λ formally as:

$$\mathrm{Tr}\left[\rho_{in}F_M^{(i)}\right] = \mathrm{Tr}\left[\Lambda(\rho_{in})F_Q^{(i)}\right] = \mathrm{Tr}\left[\rho_{in}\Lambda^\dagger(F_Q^{(i)})\right] \tag{2.1}$$

where ρ_{in} is the density matrix of the incoming signal, i corresponds to each detection event, and $\Lambda^\dagger$ is the dual, or adjoint, squashing map. The adjoint map is also completely positive, but is not necessarily trace-preserving. However, it is unital, which means that it maps the identity operator on the space $\mathcal{H}_M$ to the identity operator on the space $\mathcal{H}_Q$. It is required that this restriction holds for any input ρ_{in}, which is true if and only if:

$$\begin{aligned} F_M^{(i)} &= \Lambda^\dagger(F_Q^{(i)}) \\ \Lambda^\dagger &\text{ CP and Unital.} \end{aligned} \tag{2.2}$$

Since Λ was a trace preserving map, $\Lambda^\dagger$ must be a unital map. This means that it maps the identity operator on the target space $\mathbb{1}_Q$ to the identity operator on the full space $\mathbb{1}_M$. Now we have the adjoint squashing map taking the target measurement operators to the corresponding full measurement operators. Note that the unital condition is already contained in the first condition of Eqn. (2.2) since the measurement operators on $\mathcal{H}_M$ and $\mathcal{H}_Q$ add up to the identity in their respective spaces: $\sum_i F_M^{(i)} = \mathbb{1}_M, \sum_i F_Q^{(i)} = \mathbb{1}_Q$.

2.2.2 Necessary and Sufficient Conditions

Here we reformulate the problem using the Choi-Jamiołkowski isomorphism [Jam72, BZ06, dP67, Cho82] in order to apply the conditions given in Eqn. (2.2). It provides an isomorphism from the map $\Lambda^\dagger$ to a positive semidefinite operator τ, which maps the Hilbert space $\mathcal{H}_{QQ'}$ to the space $\mathcal{H}_{MQ'}$. Here the Hilbert space $\mathcal{H}_{Q'}$ is the same dimension as $\mathcal{H}_Q$, but has a prime to denote it as a separate space. τ is constructed by applying the adjoint squashing map to half of an unnormalized maximally entangled state $|\psi^+\rangle = \sum_{i=1}^d |i\rangle_Q |i\rangle_{Q'}$, where $d = \dim(Q)$, namely $\tau = \Lambda^\dagger \otimes \mathrm{id}\,(|\psi^+\rangle\langle\psi^+|)$. It is useful to be able to represent the linear constraints Eqn. (2.2) using a different form of the Choi-Jamiołkowski map τ, called the transfer matrix, which is denoted as τ^R. This is a reordering of the coefficients in its matrix representation via $\langle k, k'|\tau^R|l, l'\rangle = \langle k, l|\tau|k', l'\rangle$.

The search for a squashing model for a full measurement F_M with respect to a target measurement F_Q was first contained in solving the constraints Eqn. (2.2). We can now reformulate the problem as the search for the matrix τ corresponding to the adjoint squashing map $\Lambda^\dagger$ under the constraints:

$$\tau^R |F_Q^{(i)}\rangle\rangle = |F_M^{(i)}\rangle\rangle, \tag{2.3a}$$

$$\langle k, k'|\tau^R|l, l'\rangle = \langle k, l|\tau|k', l'\rangle, \tag{2.3b}$$

$$\tau^\dagger = \tau \geq 0. \tag{2.3c}$$

Here we introduce the vector notation of an operator, $V = \sum_{i,j} v_{i,j}|i\rangle\langle j|$, as $|V\rangle\rangle = \sum_{i,j} v_{i,j}|i\rangle|j\rangle$. This allows us to write $|\Lambda^\dagger(V)\rangle\rangle = \tau^R|V\rangle\rangle$ [BZ06].

Overall, we have reformulated the search for a suitable squashing operation as the search for a positive semidefinite operator $\tau \geq 0$ that satisfies a fixed number of linear constraints (Eqn. 2.3a). We will show how these can be solved

analytically in Section 2.3. They can also be efficiently solved via convex optimization; searching for completely positive maps using these techniques has been shown, for example, in [RW05, FSW07].

2.2.3 Reduction

To find a squashing model, it is important to be able to reduce the infinite Hilbert space of the input signals to a finite one in order to solve the constraints Eqns. (2.3a). To do this, we break up the squashing map into two components. First there is a map that reduces the full Hilbert space $\mathcal{H}_M$ to finite dimensions. Second, a map takes the finite Hilbert space, to the desired target measurement space $\mathcal{H}_Q$. In addition, we would like to remove the vacuum component of the squashing map in order to reduce the dimension of the space $\mathcal{H}_Q$ that we need to consider for the target measurement. This will simplify the search for the squashing map.

For the first part of the squashing map we use the fact that typical photodetectors have POVM elements that are block diagonal with respect to the number of incoming photons. This means that there is no loss or gain of photons within the detector. Of course, real detectors have loss as well as other inefficiencies, but we deal with these issues in Section 2.6. If the POVM elements are block diagonal, then the measurement can be preceded by a quantum non-demolition (QND) measurement of the total photon number, without loss of generality. The output of the QND measurement is a finite dimensional Hilbert subspace (which we denote as $\mathcal{H}_M^n$) that increases as the number of incoming photons (n) increases. The squashing map is now decomposed into first a QND measurement of the incoming photon number, followed by a squashing map that takes the space $\mathcal{H}_M^n$ into the target space $\mathcal{H}_Q$ (for example, see Fig. 2.3).

To further reduce the Hilbert space involved in the second part of the squashing map, we can break the vacuum component off from the rest of the squashing map. To do this, we note that the full and target measurements typically have a vacuum projection as one POVM element, and no vacuum component in any of the others. Also, if the outcome of the QND measurement is 0, then the second part of the squashing map is trivial: the squashing map forwards the vacuum to the target measurement. Therefore, when the QND measurement receives a 0 outcome, it forwards a classical message to Bob, to tell him he received the vacuum. This is what is called a "flag". Now the space $\mathcal{H}_Q$ does not contain the vacuum component, which simplifies the analysis that follows.

Now all that is left to find is a squashing map for each finite-dimensional photon number subspace $\mathcal{H}_M^n$ to the target measurement input space $\mathcal{H}_Q$ using Eqns. (2.3).

The dimension of $\mathcal{H}_M^n$, the output of the QND measurement, is different for each photon number n. To solve the linear constraints Eqns. (2.3a), it would be convenient to have a fixed finite dimension for each photon number subspace. However, the specific POVM elements are required to find this fixed finite dimension, and so it will be found for each of the examples below.

2.3 Examples: Analytic Solutions

In this section we discuss two examples of detector setups used in quantum communication that detect the polarization of photons: the measurement that is performed in the BB84 protocol, and the measurement performed in the six-state protocol. These two measurements considered here have an active basis choice, *i.e.*the basis measured is actively chosen by an input Bob puts into his detector. We investigate whether there exists a squashing model for these measurements. The full measurement is one that accepts any number of photons in the Hilbert space $\mathcal{H}_M$ of two orthogonal polarization modes and the vacuum. The target measurement is the same setup as the full measurement, but it only accepts single photons, also in two orthogonal polarization modes and the vacuum, $\mathcal{H}_Q$. Note that both of these measurements are of the form discussed above, where the vacuum component can be split off as a flag, and each photon number subspace can be dealt with separately. As such, in this section we search for a squashing map for each fixed input number of photons n to a single photon.

2.3.1 BB84 Active Basis Choice

Here we consider the polarization measurement performed for the BB84 protocol as described previously (see Fig. 2.1). Note that when multiple photons are input to this detector, then double clicks can occur (*i.e.*both threshold detectors fire at the same time). In this case a classical post-processing of these events is chosen. Double clicks are random assigned to one of the single click events (0 or 1). This means that whenever both detectors fire at the same time, instead of recording this event, one of either 0 or 1 will be randomly recorded by Bob's device. One reason why this post-processing is done, is so that the full and target measurements have the same number of outcomes, and therefore the linear constraints Eqn. (2.3a) can be satisfied for every event, indexed by i. Another reason this post-processing is used, is for the security of QKD (see [Lüt99b]).

To derive the squashing map for the BB84 measurement with an active basis choice, we first perform another reduction of the Hilbert space of interest, which takes advantage of the specific form of the POVM elements. The full measurement POVM elements in the n-photon subspace are given by

$$F_{M,\,n}^{(b,\alpha)} = \frac{(-1)^b}{4}\left(|n,0\rangle_\alpha\langle n,0| - |0,n\rangle_\alpha\langle 0,n|\right) + \frac{\mathbb{1}}{4}, \tag{2.4}$$

where $\alpha \in \{x, z\}$ is a label for the basis choice of the polarizing beamsplitter, $b \in \{0, 1\}$ corresponds to the "0" or "1" outcome of the detector, and $|l,k\rangle_\alpha$ is a two-mode Fock state with photon numbers l and k with respect to the polarization mode basis α. Here n is fixed, while b and α determine the POVM element in that space.

It is important to note that the dimension of the Hilbert space $\mathcal{H}_M^n$ is variable with the photon number. The standard basis for the space of two orthogonal

polarization modes is given by $\{|n-i,i\rangle\}, i = 0..n$. This means that $\mathcal{H}_M^n$ is $n+1$-dimensional. This means for large n that solving the conditions given in Eqn. (2.3a) would be difficult, as the dimension of $\mathcal{H}_M^n$ is very large. In addition, we have to solve many of these constraints separately for each fixed n. Therefore, it would be convenient to reduce the incoming Hilbert space dimension to a fixed finite value for all photon numbers n, so that the linear constraints Eqn. (2.3a) can be solved for all photon numbers simultaneously.

To reduce the Hilbert space further we find a projection onto a subspace P, spanned by the four states $\{|n,0\rangle_x, |0,n\rangle_x, |n,0\rangle_z, |0,n\rangle_z\}$, and its orthogonal complement $P_\perp$, which is $n-3$-dimensional (since P is 4 dimensional, and the full n photon space is $n+1$ dimensional). This particular projection is chosen because the single click POVM elements are the projections onto the states in P. This means that states in the space $P_\perp$ will never trigger a single click event, regardless of the basis measured; it will only ever trigger a double click. Since the post-processing is defined to take double clicks to a random bit value, the squashing map on the space $P_\perp$ is clear: the squashing map ignores the input and outputs a mixed qubit state $\mathbb{1}_Q/2$, since this will trigger a random bit value in the target measurement.

The projection map can follow directly after the QND measurement of the photon number in the squashing map, and before the target detector. This projection can be done without loss of generality because it commutes with the measurement operators (see Fig. 2.3). Applying this projection has two advantages: the squashing map in $P_\perp$ is trivial, and then all that is left to find is the squashing map on the space P, which is four dimensional for all photon numbers n.

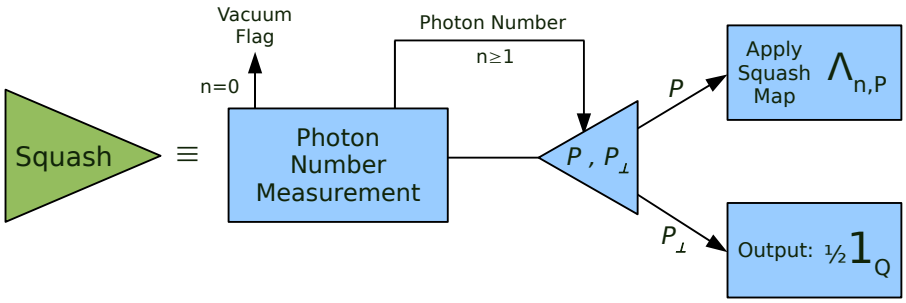

Figure 2.3: Reduction of the squashing map for the BB84 protocol detector. The squashing map can be modelled as a photon number measurement followed by a projection measurement onto a 4-dimensional subspace. Depending on the outcome of these measurements, the squashing map either proceeds with a low-dimensional squashing operation Λ_n^P or outputs a completely mixed qubit state.

We could continue to directly find the squashing map for n photons in the

subspace P via the constraints given in Eqn. 2.3. However we can employ an additional analytic tool (described below) to simplify the proof. For an alternative proof that is more direct and that demonstrates an approach to finding squashing models that is more general, see Appendix 4.1.

To find a squashing map for the subspace P and a given photon number n, we first decompose the adjoint squashing map into $\tau_{n,P} = \tau_{fix} + \tau_{open}$, where τ_{fix} is a fixed matrix of known entries given by the linear constraints and τ_{open} contains any and all open parameters that need to be determined such that $\tau_{n,P} \geq 0$. To determine τ_{fix} we can use the definition of the adjoint squashing map given previously as $\tau = \Lambda^\dagger \otimes \mathrm{id}\,(|\psi^+\rangle\langle\psi^+|)$. Here we may write the input operator $|\psi^+\rangle\langle\psi^+|$ in the basis given by $\{F_Q^{(i)} \otimes \sigma_j\}$, where the σ_j are the Pauli operators and the $F_Q^{(i)}$ are unnormalized. We also define $F_Q^{(y)}$ as the third basis choice measurement performed in the six-state protocol described below. We simply use this operator as part of the operator basis, it does not have any physical meaning here. Now we write

$$|\psi^+\rangle\langle\psi^+| = \frac{1}{2}\left\{\mathbb{1}_Q \otimes \mathbb{1}_{Q'} + \sum_{\alpha=\{x,y,z\}} \left(F_Q^{(0,\alpha)} - F_Q^{(1,\alpha)}\right) \otimes \sigma_\alpha^T\right\}.$$

This decomposition has the advantage that the adjoint map $\Lambda^\dagger$ can be applied directly to the first subsystem by using the substitution $F_Q^{(i)} \mapsto F_M^{(i)}$, $i = x, z$ which is clear from the linear constraints on the adjoint squashing map. Also using the fact that $\Lambda^\dagger$ is unital, $\Lambda^\dagger(\mathbb{1}_Q) = \mathbb{1}_M$, we find

$$\tau_{fix} = \frac{1}{2}\left\{\mathbb{1}_M \otimes \mathbb{1}_{Q'} + \sum_{\alpha=\{x,z\}} \left(F_M^{(0,\alpha)} - F_M^{(1,\alpha)}\right) \otimes \sigma_\alpha^T\right\}.$$

Since the linear constraints do not give any information about the mapping of $F_Q^{(y)}$, this leaves $\tau_{open} = D \otimes \sigma_y$, where the operator D is undetermined. To determine D, we need to impose the second condition $\tau_{n,P} \geq 0$.

The case $n = 1$ trivially has a squashing map. For $n = 2$, the squashing map can be found easily using the direct method found in Appendix 4.1. For $n \geq 3$, we can solve all together at the same time. However, there is a problem in doing this, namely that $F_M^{(0,\alpha)} - F_M^{(1,\alpha)}$ has a different form if n is even or odd. To circumvent this, we use an additional analytic tool to represent $\tau_{n,P}$ in a different way. We use the basis $|\phi_i, j\rangle = |\phi_i\rangle \otimes |j\rangle$, where $|\phi_i\rangle \in \{|n,0\rangle_z, |0,n\rangle_z, |n,0\rangle_x, |0,n\rangle_x\}$, and $|j\rangle \in \{|0\rangle, |1\rangle\}$ is the standard basis for the qubit space, to define the matrix $T(\tau_{n,P})$ as

$$T_{ij,kl}(\tau_{n,P}) = \langle\phi_i, j|\tau_{n,P}|\phi_i, j\rangle. \tag{2.5}$$

This relation can be rewritten using the congruence transformation G, $T(\tau_{n,P}) = G\tau_{n,P}G^\dagger$. According to Sylvester's law of inertia, the number of positive, negative and zero eigenvalues are the same in T and $\tau_{n,P}$ if and only if G is nonsingular [HJ85]. Since the set of states $|\phi_i, j\rangle$ are linearly independent, then G is

nonsingular. Therefore, to verify the positivity of $\tau_{n,P}$ it is sufficient to check the positivity of T.

Clearly the transformation in Eqn. 2.5 is linear, and so $T(\tau_{n,P}) = T(\tau_{fix}) + T(\tau_{open})$. First consider $T(\tau_{open})$, which can be broken down into $T_P(D) \otimes \sigma_y$, where T_P is the transformation on the subspace P. Note that since $T(\tau_{fix})$ only has real entries, the open entries in $T(\tau_{open})$ must also be real (if there was a complex solution, its conjugate would also be a solution, and these could be added to produce a real solution). In order for $T_P(D) \otimes \sigma_y$ to be real, $T_P(D)$ is of the form iS where S is a real skew-symmetric matrix. For convenience we write $T_P(D)$ in two components, however it is still has the form iS and has completely open entries:

$$i \begin{bmatrix} 0 & \delta & 2\nu & -2\nu \\ -\delta & 0 & -2\nu & \pm 2\nu \\ -2\nu & 2\nu & 0 & -\delta \\ 2\nu & \mp 2\nu & \delta & 0 \end{bmatrix} + i \begin{bmatrix} 0 & x_1 & x_2 & x_3 \\ -x_1 & 0 & x_4 & x_5 \\ -x_2 & -x_4 & 0 & x_6 \\ -x_3 & -x_5 & -x_6 & 0 \end{bmatrix},$$

where we define $\nu = 2^{-n/2}$, $\delta(n, \nu) = \nu^2(1 - (-1)^n)$, and $x_i, i = 1..6$ are open parameters. To find the open parameters such that $T(\tau_{n,P}) \geq 0$, consider $T(\tau_{n,P})$ written explicitly as:

$$\begin{bmatrix} 1 & 0 & 0 & 2\delta + x_1 & \nu & \nu + x_2 & \nu & -\nu + x_3 \\ 0 & 0 & -x_1 & 0 & -x_2 & 0 & -x_3 & 0 \\ 0 & -x_1 & 0 & 0 & 0 & x_4 & 0 & x_5 \\ 2\delta + x_1 & 0 & 0 & 1 & \nu - x_4 & \nu & -x_5 & \pm\nu \\ \nu & -x_2 & 0 & \nu - x_4 & 1/2 & 1/2 & \delta & -\delta + x_6 \\ \nu + x_2 & 0 & x_4 & \nu & 1/2 & 1/2 & \delta - x_6 & -\delta \\ \nu & -x_3 & 0 & \mp\nu - x_5 & \delta & \delta - x_6 & 1/2 & -1/2 \\ -\nu + x_3 & 0 & x_5 & \pm\nu & -\delta + x_6 & -\delta & -1/2 & 1/2 \end{bmatrix}. \tag{2.6}$$

All that is left to find are the open parameters x_i. Each subdeterminant of $T(\tau_{n,P})$ must be non-negative in order for the adjoint squashing map to be positive semidefinite. Therefore, consider the 2 by 2 submatrices specified by their diagonal entries (where 1 is the top left of the matrix Eqn. (2.6)): (2,3), (2,5), (2,7), (3,6), (3,8). The determinants of these matrices must be positive giving $-x_i^2 \geq 0, i = 1..5$, and so these open parameters are 0. Considering the 3 by 3 subdeterminant (5,6,8) if n is even and the (6,7,8) subdeterminant for n odd gives $x_6 = 0$. The eigenvalues of the resulting fixed matrix $T(\tau_{n,P})$ can be analytically computed, and are found to be non-negative.

This implies that the complete squashing map for the BB84 active basis detector exists, since τ is positive semidefinite and satisfies the linear constraints. This squashing map has been found also by Tsurumaru and Tamaki [TT08]. The squashing model then generalizes a qubit-based security proof of the BB84 protocol to one that accepts any number of photons. This is also useful in other quantum communication contexts that use this same detector, since the squashing model depends on the detector and not on the method of its use.

2.3.2 Six-State Active Basis Choice

The six-state measurement is the same as the BB84 measurement, except there is a third setting to the polarizing beam splitter which splits photons according to a circular basis (labelled as y). The post-processing of double click events is again randomly assigned to either single detection events. For this detector, we have similar measurement operators as before in Eqn. (2.4), but with $\alpha \in \{x, y, z\}$, as well as performing a renormalization. In this case, the operator τ that represents the squashing map is completely determined by the linear constraints since the measurement operators F_Q form a complete basis for their Hilbert space.

However, it can be easily seen that the squashing map does not exist, since $\tau \not\geq 0$, as follows. First, we can write the adjoint squashing map $\tau = \Lambda^\dagger \otimes \mathrm{id}(|\psi^+\rangle\langle\psi^+|)$ as before. Since the qubit measurements of the six-state protocol are complete, the input operator $|\psi^+\rangle\langle\psi^+|$ can be expanded into the basis $\{F_Q^{(i)} \otimes \sigma_j\}$:

$$|\psi^+\rangle\langle\psi^+| = \frac{1}{2}\left\{ \mathbb{1}_Q \otimes \mathbb{1}_{Q'} + 3 \sum_{\alpha=\{x,y,z\}} \left(F_Q^{(0,\alpha)} - F_Q^{(1,\alpha)} \right) \otimes \sigma_\alpha^T \right\}.$$

As in the BB84 case, we can directly apply $\Lambda^\dagger$ to the first subsystem by using the substitution $F_Q^{(i)} \mapsto F_M^{(i)}$. The operator τ has negative eigenvalues, starting in the three photon subspace. For example, the state

$$|\theta_-\rangle = \frac{1}{\sqrt{2}} \left(|3,0\rangle_{M_z} \otimes |1\rangle_{Q'} - |0,3\rangle_{M_z} \otimes |0\rangle_{Q'} \right), \tag{2.7}$$

is sufficient to show that $\tau \not\geq 0$, where $|0\rangle_{Q'}$ and $|1\rangle_{Q'}$ are canonical orthogonal basis states. We find $\langle\theta_-|\tau|\theta_-\rangle = -1/4$, and so this proves that a squashing map for the six-state protocol with active basis choice does not exist. This implies that a security proof of the six-state protocol cannot be generalized using the squashing model, and another method is required to prove security for the full optical implementation of this protocol.

2.4 How to Always Find a Squashing Map

The examples above show how solving the Eqns. (2.3) will determine whether a given full detection has a squashing map with respect to a target detector. In this section, we consider the case where the Eqns. (2.3) cannot be satisfied. However, all hope it not lost in finding a squashing model between a full and target measurement. There are two methods to recover the squashing model, but at the cost of changing the full measurement. Either noise is introduced via the classical post-processing or the physical detection setup is modified in an intelligible way. A similar approach of implementing non-positive maps has been introduced before in [Hor01].

First, we begin by discussing problems trying to satisfy the linear constraints Eqn. (2.3a). To solve the linear constraints, we require that the full and target

measurement have the same number of outcomes. However, if the full measurement's physical measurement has more outcomes than the target measurement (as we saw with the above examples), then a classical post-processing should be done on the outcomes of the full measurement. It will reduce the number of full measurement outcomes to that of the target measurement. Also, we require that any linear dependence in the POVM elements of the full measurement is the same in the POVM elements of the target measurement. This enables the linear constraints to be satisfied, because for each index i there is a one to one correspondence between full and target POVM elements, and none of these equations contradict any others, because there are no linear dependencies that are not both satisfied by full and target POVM elements. Now that the linear constraints are satisfied, we consider the positivity of the squashing map, τ.

If there are any open parameters left in τ after solving the linear constraints, then they should be chosen such that τ is positive semidefinite. If this is possible, then the full measurement has a squashing model with respect to the target measurement. Otherwise, we would like to construct a new adjoint squashing map τ_{new} that is positive semi-definite, and as a result, we must also change the full measurement operators. Using the adjoint squashing map that satisfies the linear constraints τ (which we relabel here for clarity as τ_{old}):

$$\tau_{new} = p\tau_{old} + (1-p)\tau_{+}, \tag{2.8}$$

where p is a weight in the interval $[0,1]$, and τ_+ is a unital map and $\tau_+ \geq 0$. Note that the construction of τ_{new} is convex, and therefore there exists a p, and choices for any open parameters left in τ_{old} such that τ_{new} is positive semidefinite. In addition, the squashing map can be thought of as a stochastic process: with probability p the squashing map whose adjoint is τ_{old} is applied, and with probability $1-p$ the squashing map whose adjoint is τ_+ is applied.

Since the squashing map has been changed, we must also modify the full measurement. The new full measurement operators are the combination of the POVM $F_M^{(i)}$ with weight $(1-p)$ and $\tau_+^R|F_Q^{(i)}\rangle\rangle$ with weight p. This is necessary so that a squashing map exists to the desired target measurement:

$$\tau_{new}^R|F_Q^{(i)}\rangle\rangle = p|F_M^{(i)}\rangle\rangle + (1-p)\tau_+^R|F_Q^{(i)}\rangle\rangle. \tag{2.9}$$

Note that here we apply the realignment R to use Eqn. 2.8 (which is linear) to determine how τ_{new}^R acts on $|F_Q^{(i)}\rangle\rangle$.

The important point here is that *any* full detector can have a squashing model with respect to *any* target measurement as long as:

1. The full measurement and target measurement have the same number of outcomes.

2. Any linear dependencies with the POVM elements of the full measurement are identical to the linear dependencies in the target measurement POVM.

3. The full measurement is modified to be that of Eqn. (2.9), where p is suitably chosen.

There are two ways in which we can modify the full measurement operators according to Eqn. 2.9: add noise through classical post-processing or modify the physical full measurement.

The first method is to apply a classical post-processing to the outcome of the full measurement to add noise to the outcomes of the physical detector. For example, in the six-state protocol with an active basis choice, the 0 and 1 outcomes could be kept with probability q and have the bit flipped with probability $1-q$. If $q = 1/2$ the post-processing ignores its input from the detector, and randomly chooses 0 or 1. In this case there is a squashing map that ignores the input and outputs a maximally mixed state $\mathbb{1}_Q/2$. Therefore, there is always a choice of q such that a squashing map exists. For the six-state protocol, the maximal q (and so the minimal noise introduced) is 16.67%. This bound was found using a semidefinite program [FSW07] that searches for a positive semidefinite squashing map that satisfies the linear constraints, while minimizing the noise parameter $1-q$. For more details on finding squashing maps in a numerical way, see Section 2.7. The bound of 16.67% is beyond the maximal tolerable error rate for QKD to be performed (with one way classical communication) [KGR04]. Therefore, in this case, noisy classical post-processing is not a good solution to the problem of finding a squashing map. However, in other contexts, this solution may be helpful.

Another method to find a squashing map is to modify the physical measurement device. We present a specific example of how to do this, with a choice for p and τ_+ from Eqn. (2.8) that is easily implemented experimentally.

2.4.1 Experimental Measurement that Always Has a Squashing Map

First we require K copies of the measurement F_M, which can be placed at each end of a beamsplitter that equally distributes input to its K output arms. If all of the photons arrive to the detector in a single arm, then the measurement is the same as before. Otherwise a post-processing is performed, where the result is assigned (according to a probability distribution) to one of the possible outcomes of F_M.

Now we find the corresponding squashing map τ_{new} that accompanies this new measurement. As we have seen before in Section 2.2.3, as long as the full measurement POVM elements are block diagonal with respect to the photon number, the squashing map can be preceded by a QND measurement of the number of incoming photons. Then in each n-photon subspace the squashing map can be thought of as a stochastic process as in Eqn. (2.8), with $p(n) = K^{(1-n)}$. The adjoint squashing map $\tau_{old,n}$ for each n-photon subspace is known, and any open parameters it may have after applying the linear constraints should be chosen to maximize its smallest eigenvalue. This is so that $p(n)$ is maximized and therefore K is minimized, i.e. the number of copies of the original measurement F_M that are needed is minimized.

Here we choose to pick the squashing map $\tau_{+,n} = \mathbb{1}_n$, which outputs a maximally mixed qubit state $\mathbb{1}_Q/2$. This fixes the post-processing to be such

that the outcome i is assigned with probability $\mathrm{Tr}(\mathbb{1}_Q/2F_M^{(i)})$ whenever multiple arms click at the same time. Now the smallest K should be found such that $(1-p(n))$ is greater than or equal to the smallest eigenvalue of $\tau_{old,n}$ for all n. Therefore $\tau_{new,n} \geq 0$, and there exists a squashing map from the measurement given by Eqn. (2.9) to the target measurement F_Q via the adjoint squashing map τ_{new} from Eqn. (2.8).

2.4.2 BB84 Passive Basis Choice

An implementation of the method of choosing $\tau_+ = \mathbb{1}$ is the passive basis choice for the BB84 or six-state measurements. This consists of each of the two (or three) basis measurements at each end of a beamsplitter with the output ratios 1:1 (or 1:1:1, for the six-state protocol). Also, the probability p depends on the photon number of the incoming signal n, and can be determined by the probability that all of the n photons to go to one arm of the beamsplitter: $p(n) = 2^{(1-n)}$ for the BB84 detector, and $p(n) = 3^{(1-n)}$ for the six-state detector.

In this case, the squashing model exists for the BB84 passive detection scheme, since we are adding a positive map to the already positive active squashing map.

2.4.3 Six-State Passive Basis Choice

For the six-state protocol the linear constraints were satisfied, but the map was not positive semidefinite. Therefore, we would like to find if the passive squashing map τ is positive semidefinite. For the case of a single photon, $n = 1$, there is an active squashing map, and therefore there is also a passive one. For $n \geq 1$ we use the formalism in this section, *i.e.* Eqn. (2.8), to determine if a squashing map exists. To show that τ_{new} is positive semidefinite, it is sufficient to show that its smallest eigenvalue is non-negative. First, we use the reduction arguments from Section 2.2.3 to reduce the squashing map into first a QND measurement of the number of photons, as well as removing the vacuum as a flag. We have $\tau_{old,n}$ from Section 2.3.2, $p(n) = 3^{(1-n)}$ from Section 2.4.2, and $\tau_{+,n} = \mathbb{1}_n$.

To estimate the smallest eigenvalue of τ_{new} we estimate the smallest eigenvalue of τ_{old}. First, the full POVM elements for single clicks are rank 1 projectors of the form $1/3|\psi\rangle\langle\psi|$ (where $|\psi\rangle = |n,0\rangle_{b,\alpha} or |0,n\rangle_{b,\alpha}$), and therefore have a largest eigenvalue of 1/3. Using this, and the fact that the largest and smallest eigenvalue of the Pauli matrices are ± 1, the lower bound on the smallest eigenvalue of τ_{old} is:

$$\langle\psi|\tau|\psi\rangle \geq \frac{1}{2} + \frac{3}{2}\sum_{\alpha}\left(\frac{-1}{3}\right) = \frac{1}{2} - \frac{3}{2} = -1 \tag{2.10}$$

Now consider the smallest eigenvalue of the passive squashing map from Eqn. (2.8), which gives $3^{(1-n)} \cdot (-1) + (1 - 3^{(1-n)}) \cdot 1$. For $n = 2$ the lower bound on the

smallest eigenvalue is 1/3, and since the lower bound increases with the photon number, the smallest eigenvalue is always positive. This proves that the six-state passive detector has a squashing model.

2.5 Time-mode Squashing

The conditions used to find squashing models Eqns. (2.3) have been used so far to find squashing maps that take multiple photon signals to single photon ones. However, there are other high-dimensional degrees of freedom that are not accounted for in experimental measurements. For example, measurements typically accept signals over a time window, whose responses in a measurement (such as detector clicks) are grouped together into what is called an "event". During the time window of an event, it is possible that a measurement receives signals in multiple time modes. However, in theories it is often assumed that signals are received only at a specific instant, or single time mode. Therefore, in this section we discuss under what conditions a squashing model exists that connects a full measurement with multiple time mode inputs to a target measurement that only accepts a single time mode.

First, we would like to reduce the Hilbert space $\mathcal{H}_M$ in order to find a squashing map by solving Eqns. (2.3). Similarly to Section 2.2.3, we decompose a full measurement that accepts multiple time modes into an equivalent measurement whose squashing map acts on a smaller Hilbert space, and is therefore more easily found. In addition, to simplify the analysis, we restrict the full and target measurements to the class of detectors that have outcomes originating from threshold detectors.

For measurements on multiple time modes with threshold detectors, the full measurement can be thought of as many copies of that same detector, each measuring with the same setting (for example, the same basis) and each only receiving one time mode. The output of each detector is then sent to a global post-processing, which does the following: if a specific threshold detector is triggered in any of the copies, then that threshold detector is recorded to have clicked, and otherwise it is recorded not to have clicked (see Fig. 2.4). The many copies of F_M followed by the global post-processing is intuitive because of the nature of threshold detectors. Typically there will be a time period after a threshold detector is triggered where it is recovering, and it will not trigger if more photons arrive. This recovery time is typically longer than the time window allotted to a detection event. Therefore, as long as a threshold detector fires once in the time window of an event, it does not matter if there are more photons arriving, they will not give a different measurement outcome.

In addition, the global post-processing can be applied in the following way: the first two detectors' outcomes are post-processed using the same method described above, and then the outcome of this along with the third detector's outcome is post-processed, and this post-processing is repeatedly cascaded for all of the remaining detector copies. Now the original measurement is broken up into many copies, followed by this cascaded post-processing. If there exists

a squashing map that takes a full measurement on two time modes to a measurement on a single time mode, then the first two detector copies with their respective global post-processing can be reduced to the target measurement (a measurement on one time mode). Now we have the exact same cascaded measurement as before, except now there is a squashing model reducing the first two time modes to a single time mode. Repeating this process for each of the input time modes, the two time mode squashing map can be used to squash all of the time modes into a single time mode.

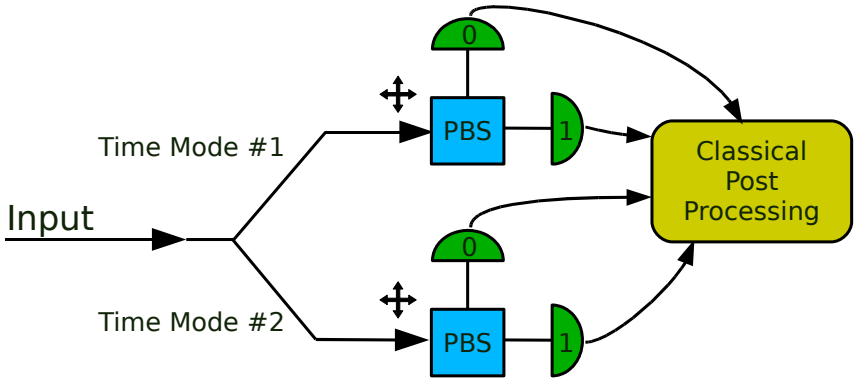

Figure 2.4: Two time modes can be split so that each time mode goes to a measurement, such as the one performed in the BB84 protocol, both with the same setting, followed by threshold detectors. The output is then fed to a global post-processing that outputs a classical signal that corresponds to an outcome of one copy of the measurement.

Now we focus on finding a squashing map from two time modes to a single time mode. Since threshold detectors are being used, we can precede the squashing map with a QND measurement of each of the two time modes. The QND measurement outputs the photon numbers N and M for each time mode respectively (see Fig. 2.5). Clearly if N or M is zero, then that mode can be ignored, and we are only left with a single time mode, as desired. Otherwise we require the specific form of the measurement, and therefore continue for the specific case of the BB84 and six-state measurements discussed earlier. However, the steps outlined below are illustrative of how to find a similar squashing map for other measurements.

First, we reduce the Hilbert space of the input to simplify the search for a squashing map. To do this we perform a projection onto the four (or six, depending on whether there are two or three bases for the measurement) dimensional subspace Π spanned by the states $\{|n,0\rangle_\alpha|m,0\rangle_\alpha, |0,n\rangle_\alpha|0,m\rangle_\alpha\}$, and its orthogonal complement, $\Pi_\perp$. This is very similar to the steps taken in Section 2.3.1. If the incoming signal is projected into $\Pi_\perp$ then the outcome of the measurement followed by the global post-processing is always a double click,

regardless of the choice of basis. In this case the squashing map outputs a state in a single time mode that will always give a double-click output, such as $|\psi_{DC}\rangle = 1/\sqrt{2}(|5,1\rangle - |1,5\rangle)$. If the input is projected into the (four or six dimensional) subspace Π then we need to find an adjoint squashing map τ that satisfies:

$$\tau^R|F^{(i)}_{One}\rangle\rangle = |F^{(i)}_{Two}\rangle\rangle, \tag{2.11}$$

where $F^{(i)}_{One}$ is the POVM element corresponding to a detector setup whose input is in a single time mode in the subspace P (the space spanned by $\{|n,0\rangle_\alpha, |0,n\rangle_\alpha\}$, where $\alpha \in \{x,z\}$) mentioned previously for the BB84 measurement and $F^{(i)}_{Two}$ is the POVM element corresponding to a detector setup whose input is in two time modes in the four dimensional polarization subspace Π. For the six-state measurement, $F^{(i)}_{One}$ is in a similar subspace P_{six}. P_{six} is a six dimensional subspace that is the same as P, except now $\alpha \in \{x,y,z\}$.

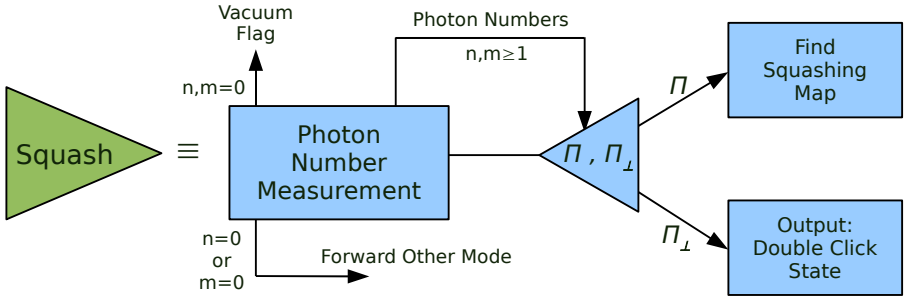

Figure 2.5: The squashing map for two time modes each with two orthogonal polarization modes. Each time mode is input to a QND measurement of the number of photons. The result of this measurement is forwarded to a projection map. Depending on the output of the projection, either a state that always produces double clicks in the measurement is output $|\psi_{DC}\rangle = 1/\sqrt{2}(|5,1\rangle - |1,5\rangle)$, or a squashing map is applied in the subspace Π, which outputs a state in a single time mode and two orthogonal polarization modes.

We can construct a squashing map, and hence a positive semidefinite operator τ that satisfies the linear constraints Eqn. (2.11), in the following way. We define an operator U, which maps subspace P (P_{six}) to the subspace Π:

$$U|N+M,0\rangle_\alpha = |N,0\rangle_\alpha|M,0\rangle_\alpha \tag{2.12}$$

$$U|0,N+M\rangle_\alpha = |0,N\rangle_\alpha|0,M\rangle_\alpha, \tag{2.13}$$

where two sequential kets represent the two time modes. This map is linear since each of these states is linearly independent. This map preserves the inner product of any two of the states above, which can be shown by the Gram matrix; the matrix of inner products between each of the states. Here we show the four

dimensional Gram matrix for the BB84 measurement:

$$\begin{bmatrix} 1 & 0 & 2^{-\frac{N+M}{2}} & 2^{-\frac{N+M}{2}} \\ 0 & 1 & 2^{-\frac{N+M}{2}} & (-\sqrt{2})^{-(N+M)} \\ 2^{-\frac{N+M}{2}} & 2^{-\frac{N+M}{2}} & 1 & 0 \\ 2^{-\frac{N+M}{2}} & (-\sqrt{2})^{-(N+M)} & 0 & 1 \end{bmatrix}$$

This implies that U is unitary.

Let us return to the POVM elements we want to satisfy Eqn. (2.11). First consider the unnormalized POVM elements $F_{One}^{(i)}$:

$$|n,0\rangle_\alpha\langle n,0|_\alpha, |0,n\rangle_\alpha\langle 0,n|_\alpha, \tag{2.14}$$

where n corresponds to the number of photons in the single time mode Hilbert space. The unnormalized POVM elements $F_{Two}^{(i)}$ are

$$\begin{aligned} &|N,0\rangle_\alpha|M,0\rangle_\alpha\langle N,0|_\alpha\langle M,0|, \\ &|0,N\rangle_\alpha|0,M\rangle_\alpha\langle 0,N|_\alpha\langle 0,M|. \end{aligned} \tag{2.15}$$

Clearly $\Lambda(F_{One}^{(i)}) = UF_{Two}^{(i)}U^\dagger$ is a positive semidefinite map that satisfies the linear constraints, and therefore there exists a squashing map between the multimode and single mode detections. Therefore, by concatenating the multimode squashing map with the single mode squashing maps found previously, there exists a squashing model for the BB84 active and passive measurements, as well as the six-state passive measurement for a multiple time mode, multi-photon detector with respect to a single photon, single time mode one.

2.6 Imperfections

So far we have only considered examples of detectors that do not have any imperfections such as inefficiencies or dark counts. Inefficiencies occur when there is a loss of photons within the detector, and dark counts occur when a threshold detector clicks without any input photons. However, these are a realistic factors in experimental measurements that should be considered in determining the existence a squashing model. Here we examine these imperfections for the examples considered previously: the BB84 and six-state measurements.

When there are inefficiencies, the loss at each threshold detector can be modelled by a beamsplitter. If each of the threshold detectors used in the full measurement all have a common inefficiency then these inefficiencies commute with the polarizing beamsplitter(s), and, in the passive case, also commute with the non-polarizing beamsplitter (see Fig. 2.6). Therefore, these measurements with inefficiencies are equivalent to first a common inefficiency followed by a perfectly efficient full measurement [Yur85]. If a squashing map exists for the perfect full measurement, then the squashing map for the full measurement with inefficiencies to the perfect target measurement is first a beamsplitter that

models the loss, which is a completely positive map, followed by the squashing map used previously for the perfect full measurement. The same concept can be applied to misalignment errors, which can be described by a fixed depolarizing channel on each photon individually. This is because the depolarizing channel can be exchanged with the polarizing beam splitter, as before.

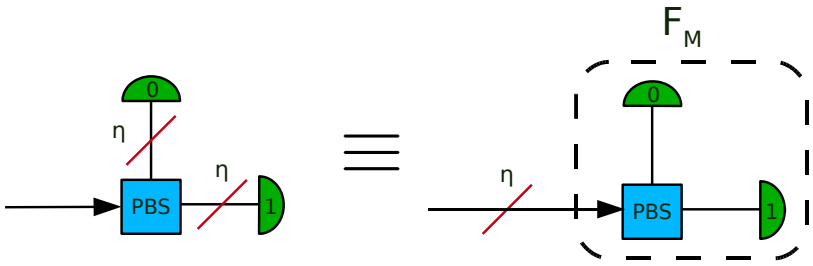

Figure 2.6: Inefficiencies can be modelled by a beamsplitter in front of each threshold detector. Since the lossy beamsplitters commute with the polarizing beamsplitter, it can be brought out in front of the measurement. Since the full measurement F_M has a squashing model, the squashing map for the lossy detector is first a beamsplitter modelling the loss, followed by the squashing map from Section 2.3.

If the inefficiencies of the threshold detectors are different, then a common inefficiency can be removed as before, but the remaining full measurement has a different structure, and its squashing model to a desired target detector has to be found again. We leave this analysis for future work.

Dark counts can be accommodated as well if they obey a model that can be described by a post-processing of the basic detection events [Lüt99a]. More specifically, in a time window allotted to a detection event, each threshold detector can fire with probability q without an incident photon. This means that the full measurement is equivalent to a perfect physical detector followed by a post-processing due to the dark counts and then the standard classical post-processing of the double-click events (see Fig. 2.6). This dark count model allows the classical post-processing used in the BB84 and six-state measurements to be rearranged such that there is first the classical post-processing of the double-click events, followed by a different post-processing caused by the dark counts. In order for the two arrangements of the post-processings to be equivalent, the new dark count post-processing can described by a bit flip of a 0 to a 1 or vice-versa with probability $q/2$, and kept with probability $1 - q/2$, and the vacuum is mapped to a 0 or a 1 with probability $q + q^2/2$, and is kept with probability $1 - 2q - q^2$. Since the combination of the perfect physical detector and the standard classical post-processing has a squashing model, the same squashing map applies, but now the target measurement is the same target measurement as before followed by the dark count post-processing. This means that a squashing model exists for a full BB84 (active or passive) or six-

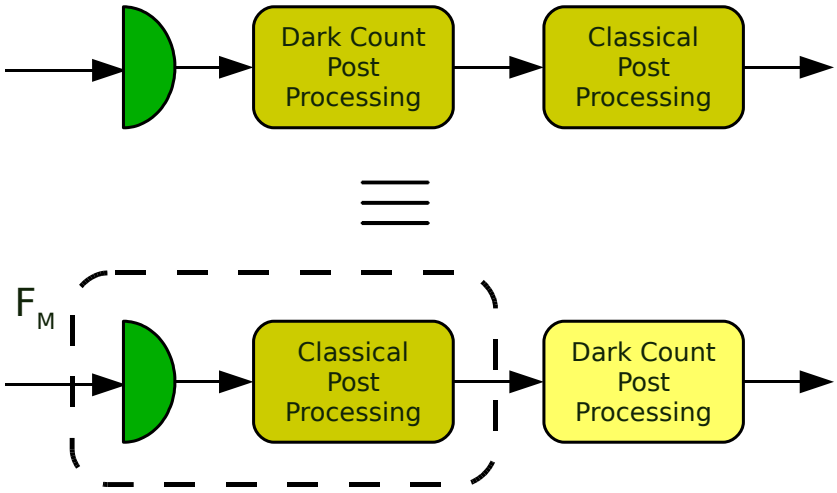

Figure 2.7: Above: The dark counts can be modelled by a classical post-processing, which is then followed by the standard classical post-processing of randomly assigning double click events. Below: The standard post-processing is done first, followed by a different dark count induced post-processing. The squashing model can then be used on the full measurement F_M. The two measurement descriptions, followed by their respective post-processings, are equivalent.

state (passive) measurement with dark counts, to a perfect target measurement followed by the described dark count induced post-processing.

For QKD, a squashing model here means that single photons will be detected in the target measurement, so a qubit security proof would now apply. However, there will be additional noise added to the outputs of the target measurement by the dark count post-processing. This adds an artificial increase in the error rate. Bob cannot distinguish between errors introduced by Eve's attack and the dark count post-processing that adds errors. Therefore, more error correction and privacy amplification will have to be applied, even though some of the error rate is due to the dark count effect in Bob's detector, and not due to Eve.

2.7 Numerical Results

In this section, we outline some numerical results that suggest that there exists (or does not exist) a squashing model between specified full and target detector setups. To find numerical evidence for a squashing model, we consider the typical scenario where the measurement can be preceded by a QND measurement of the number of incoming photons (see Section 2.2.3). This allows us to find a squashing map separately for each photon number subspace. For numerical analysis, we use convex optimization techniques to find if there exists a squash-

ing map by fixing the photon number, and finding the squashing map for each photon number subspace separately. This is simple for low photon numbers, as the dimension of the Hilbert space is small. However, as the photon number becomes larger, the Hilbert space is also large, and it is more difficult to find the squashing map. If in one of the photon subspaces, we find there does not exist a squashing map for that subspace, then the complete squashing map connecting a full and target measurement does not exist. If we find a squashing map for a set of low photon number subspaces, this only suggests that there may exist a squashing map, since we have not found a photon subspace in which there is not a squashing map.

First we consider an example of a detector used in an implementation of the BB84 protocol, using the relative phase of two pulses [Ben92], instead of encoding signals in two orthogonal polarization modes. The detector used at the receiver's end accepts two pulses in different time modes and is described as follows. There is a beamsplitter that has two outputs distributed in a 1:1 ratio. The output arms have a length difference equal to the difference in spacing of the input time slots. Also on the long arm, there is a phase modulator that either does nothing, or applies a π phase shift. The long and short arms are then each connected to the inputs of another beamsplitter with a ratio of 1:1, whose outputs each have a threshold detector (see Fig. 2.8). Since there are two input time slots, and a delay in one of the arms, there are three possible time slots at which clicks of the threshold detectors can occur.

Typically, for QKD, a 0 is recorded when one of the threshold detector clicks in the middle output time slot, and a 1 is recorded when the other threshold detector clicks in the middle time slot. These events occur when the first input pulse goes along the long arm of the detector, and the second input pulse goes along the short arm. Then the two arms interfere at the second beamsplitter to determine the relative phase between the input pulses. In addition, an eavesdropper could input signals before and after the two time slots we are interested in, modifying the detection events. To avoid this, a shutter can be placed in front of the detector so that only the two time slots are allowed to enter the detector, and any additional inputs are blocked.

For quantum communication purposes it would be convenient to have a squashing model that connects this detector, which accepts any number of photons or the vacuum in two time slots as input, to the same detector, which only accepts a single photon in two time slots or the vacuum as input. There is also a classical post-processing of the basic detection events. Here we choose that a 0 or 1 event is kept as it is, and a double click between the two middle output time slots is randomly assigned to either a 0 or 1 event. All other events are mapped to the vacuum. Using semidefinite programming we can solve the linear constraints and positivity condition Eqns. (2.3) for a specified photon number, and in this case we find that at least up to $n = 10$ there is a squashing map for the given full measurement to the given target measurement.

Realistic threshold detectors, such as avalanche photodiodes, have a recovery time (or downtime) where they do not respond to input after a click event. Therefore with phase encoded BB84 measurement, where multiple sequential

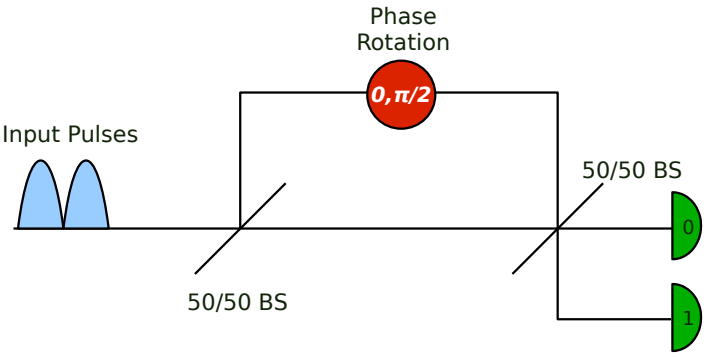

Figure 2.8: The measurement performed in the BB84 protocol with phase encoding. The input is in two time modes separated by a distance equal to the length difference in the two arms of the detector. On the long arm, a phase shift Φ is performed which either does nothing, or applies a π phase shift.

time slots are measured, the threshold detectors do not click in later time slots if they click in an earlier time slot. This means that if there is a click in the first time slot for one of the threshold detectors, then there will not be a click in the second or third time slot for that detector. The same post-processing is used here as before of randomly assigning double clicks in the middle time slot. Note that we do not know in this scenario if the third time slot fires after there are clicks in the middle time slot of each threshold detector. Searching for a numerical solution using the defined post-processing, we find that the linear constraints Eqn. (2.3a) cannot be satisfied for $n = 3$, and therefore a squashing model does not exist. However, different post-processings could be attempted, as well as variations in the target measurement to attempt to recover a squashing model.

Alternatively, shutters can be placed directly before each of the threshold detectors so that only the middle time slot signals are allowed to pass into the detectors. Unfortunately we do not recover the squashing model in this case for the full measurement to the target measurement with post-processing described above; starting at the $n = 2$ subspace the squashing map is not positive. Therefore, a squashing map does not exist. However, as seen in the previous example, changes to the post-processing and target measurement could help result in a squashing map.

2.8 Other Quantum Communication Applications

The examples of squashing maps considered so far are all directly connected to QKD protocols. However, the squashing model has applications in other quantum communication tasks as well. In this section we discuss an example of a measurement performed in a coin flipping protocol. In this protocol two

separated parties, Alice and Bob, try to create a list of common random bits. However, one of the parties is allowed to cheat. Classically a single party who cheats can control the outcome of the bit they share. However, using quantum signals for communication places a bound on the bias that can be introduced by a cheating party [BBB$^+$09]. Since a party may be cheating, it is important to remove any assumptions on their behaviour. As an example, single photons should be used in the protocol, but due to cheating, Alice may send multi-photon signals. In order to remove the assumption that single photons must be sent, it would be useful to find a squashing model connecting the measurement performed by Bob to its single photon equivalent. If such a squashing map exists, then the scenario where multi-photon signals are measured is equivalent to the case where first a squashing map is performed followed by an equivalent measurement that only accepts single photons. Then the squashing map can be given to the quantum communication channel. Since the channel will reduce the signals into a single photon, a cheating Alice that sends multi-photon signals will have them reduced to a single photon. Therefore, the existence of a squashing model in this case ensures that a cheating Alice has no advantage in sending multi-photon signals.

Now we consider finding a squashing map for the measurement used in an implementation of the coin flipping protocol [BSGT]. In this implementation the phase-encoded BB84 measurement is used, as it was described in Section 2.7 with the following differences. There is no phase modulation performed in the long arm of the detector. Also, the outcomes of the two threshold detectors, which can click in one of three time slots, are interpreted differently: a 0 in the z basis occurs when only a particular threshold detector clicks in the middle time slot, and a 1 in the z basis occurs when a other threshold detector clicks in the middle time slot. A 0 in the x basis occurs when when one or both detectors click in the first time slot, and a 1 in the x basis occurs when one or both detectors click in the third time slot. Since double clicks can occur which make the outcome ambiguous, we apply a post-processing to these events, which is described as follows. When both detectors fire in the middle time slot, the outcome is randomly assigned to 0 or 1 in the z basis. When there is at least one click in the first and third time slots, the outcome is randomly assigned to 0 or 1 in the x basis. Any other event is post-processed to be 0 or 1 in either the x or z basis at random.

Now that the detector and corresponding post-processing is defined, we may look for a squashing map that connects this full measurement to its single photon equivalent. Note that the vacuum component can be removed as a flag, since the vacuum projection is only contained in a single POVM element and none of the others (see Section 2.2.3). In addition, the POVM elements that describe this measurement are the same as those for the BB84 polarization measurement with a passive basis choice, except the labelling for the POVM elements have the bit and basis are flipped. For example, $F_{0,x}$ for the BB84 measurement is equal to $F_{1,z}$ for the measurement used here. This equivalence is not surprising, since both measurements begin with a 1:1 beamsplitter that performs the action of choosing a basis, followed by a measurement that determines the bit value.

Therefore, the desired squashing map exists, since we may reuse the squashing map found previously for the BB84 polarization measurement. This ensures that cheating parties in the coin flipping protocol do not have an advantage by sending multi-photon signals.

2.9 Future Work

A formalism has been developed to find whether a squashing model exists that connects a given full and target measurement. It has been applied to several examples of detectors commonly used in quantum communication. There are also many other measurements used in quantum communication whose squashing models would be useful to find. However, we leave the exploration of further examples to future work.

Also, in each of the examples considered in this Chapter, it is always assumed that perfect POVM elements that describe the full measurement setup are an accurate description of the experimental measurement. However, in a practical measurement setup it would be desirable to be able to ensure the squashing model holds even if the full POVM elements are slightly different. This could be due to misalignment of the detectors, or other abnormalities, which would differentiate the measurement from their perfect POVM description. Since the squashing map depends directly on the POVM elements (see Eqn. 2.3), the formalism should then take this deviation into account. More formally, the squashing map should satisfy the linear constraints, as well as the positivity condition for a small parameter region around the desired full POVM elements. This would allow for a more robust squashing map, that could accept some small modifications in the full measurement description. However, this requires a modification of the formalism described in this thesis in order to properly accommodate this "approximate" squashing model.

In addition, it would be advantageous to prove that a general class of measurements has a squashing model to avoid having to find a squashing map for each full and target detection separately. For example, we have seen that the BB84 and six-state passive detection measurements have squashing models. Then perhaps all linear optical networks followed by threshold detectors on the output modes have a squashing map connecting its measurement of many input photons to the equivalent measurement on a single photon. This class of detectors contains many measurements performed in quantum communication, for example the measurement used in the differential phase shift QKD protocol [IWY02].

Chapter 3

Entanglement Verification and Squashing

3.1 Motivation

Because of the key role of entanglement in applications much effort is put into realizing this fragile resource in the lab, for example via parametric down-conversion (PDC) sources or with ion traps, to only name a few. In a real experiment it is of course desirable to unambiguously verify the creation of entanglement, and in fact many different operational tools have been developed over the past years to achieve this task, cf. Ref. [GT09] for a review. A reliable entanglement verification has to satisfy a few crucial criteria [vELK07]; most importantly the verification method should not rely on assumptions from the entanglement generation process, but instead on the information acquired about the system via measurements. Moreover the obtained data should be considered under a worst case scenario, *i.e.*, the test is only considered to be affirmative if the data exclude compatibility with all separable states (in the limiting case of an infinite number of experimental runs), in similar spirit as already motivated in Ref. [HHH99]. This viewpoint is even essential for certain tasks like quantum cryptography [CLL04].

Still it is typical to allow one basic ingredient: since usually quantum mechanics is considered to be true, it is common to assume that an accurate quantum mechanical description of the employed measurement devices exists; to actually test or to "measure" a measurement device is anyway often combined with other assumptions [LAFCR$^+$09] or seems to be unlikely to work in practice if really no assumptions are made [MY04, DMMS07].

An example of a straightforward and hence quite often applied entanglement verification method, *e.g.*, Ref. [JKMW01], is the following procedure which we call the *tomography entanglement test* in the following: since the useful entanglement might be confined to a low dimensional subspace, *e.g.*, the single photon-pair subspace of a PDC source or two very long-lived energy levels of

two ions in a trap, only a few different measurements are needed to obtain tomography on this subspace. After several runs of the experiment there is enough data collected to reconstruct the underlying density operator on this subspace via some reconstruction technique. Note that here the knowledge of the measurement description is employed. In order to check for entanglement the reconstructed density operator can be checked to see if it describes an entangled state or not.

However, is entanglement really verified via this method? The problem lies within the measurement description, because such ideal measurements, as the ones used in the reconstruction mechanism, might not have actually been performed in the experiment. Good examples are the BB84 or six-state polarization measurements, which are often employed in photonic experiments. As we have seen in the previous Chapter, these measurements do not respond solely to the single photon subspace, since such detectors can receive any number of photons. Hence the question arises whether entanglement is still verified if a more realistic measurement description is employed. The main purpose of this chapter is to study this question. Note that the aforementioned scenario often occurs, not because we are not aware of the more realistic model, but because an oversimplified measurement description is employed in order to ease the task of entanglement verification.

Specific instances of the problems considered here have been investigated in several works in the literature. In Ref. [SU07] inequalities for the detection of entanglement for two qubits have been proposed, where the measurement's devices can be misaligned to a certain degree. Bell-type inequalities which are independent of the spectrum of the measured observables have been recently introduced in Ref. [SV09]. Moreover, for an experiment with photons from atomic ensembles, an entanglement verification scheme which takes multi-photon events into account has been introduced [LvC$^+$09] and implemented [PCD$^+$09].

In this Chapter we proceed along the following lines: In Section 3.1.1 we provide an example of a tomography entanglement test which indeed leads to the wrong conclusion about the presence of entanglement under a small, physical change of the employed measurement description.

In Section 3.2, we modify the formalism introduced in Section 2.2 to arrive at new conditions such that entanglement verification mistakes by assuming a simplified measurement description can be safely be excluded. In short, the entanglement verification process remains valid as soon as the considered set of operators are connected by a positive map (as apposed to the previous chapter, where we had a completely positive map).

In Section 3.3 we reformulate the existence of such a positive map into a necessary and sufficient condition which provides a particular intuitive solution for the tomography entanglement test: the map exists if and only if each classical outcome pattern from the refined set of full observables remains compatible with the oversimplified set of target observables.

Then, in Section 3.4 we prove that the six-state polarization measurement can be linked to its single photon realization by a positive map, even though a completely positive map does not exist (see Section 2.3.2). This analysis con-

cludes that the tomography entanglement test which is typically employed for a PDC source [KBAW00] or even in multipartite photonic experiments [WSK+08] using the single photon assumption can indeed be made valid if the double click events are taken into account.

3.1.1 Example: Ion Trap Entanglement Verification

Let us first mention a simple, yet practically relevant example, which shows that the tomography entanglement test indeed can lead to a false conclusion about the presence of entanglement if the structure of the observables is not properly taken into account.

For a single ^{40}Ca-ion in a trap it is typically to consider only the lowest two energy levels given by a lower level $|S\rangle = |1\rangle$ and the upper level $|D\rangle = |0\rangle$ and treats them as a qubit [HRB08]. Resonance fluorescence provides a mechanism to read out the occupation number of the energy levels: An electron in the $|S\rangle$ state is coupled to a higher energy level $|P\rangle$, and observing photons from the $|S\rangle \leftrightarrow |P\rangle$ transition signals that the qubit was in the state $|S\rangle$. This overall process corresponds to a projection onto the lower energy state and consequently allows to measure the σ_z Pauli operator, while the measurement along different directions is achieved by a local basis rotation prior to the σ_z measurement, cf. Ref. [HRB08].

In order to avoid too many measurements it is common to measure the occupation probability only for the state $|S\rangle$, simply because for qubits the other probability is $p(D) = 1 - p(S)$ due to the normalization, and similarly for the other basis settings. Suppose that this measurement procedure is used to obtain tomography in order to verify the creation of entanglement between two separated ions in a trap. Now consider the example that the observed expectation values, abstractly denoted as $E_{ij}(p)$ and characterized by a noise parameter p, may allow the reconstruction of the state

$$\rho(p) = (1-p)|\psi^+\rangle\langle\psi^+| + p\frac{\mathbb{1}}{4}. \tag{3.1}$$

To test to see if this state is entangled, we use the positive partial transpose (PPT) criterion. This criterion says that if the partial transpose of a bipartite (qubit-qubit) entangled state is not positive semidefinite, then the state was entangled. Using this criteria, the state in Eqn. 3.1, is entangled for $p < 2/3$.

However in practice the situation is more complicated since the ion is not a simple two-level system. To model this, another energy level can be added to only one of the ions, thereby enlarging the two-qubit system to a qubit-qutrit one (see Fig. 3.1.1). Without any additional information about the occupation number of this extra level, it is clear that the assignment $p(D) = 1 - p(S)$ is not correct any more. Consequently the observed data $E_{ij}(p)$ can only verify entanglement for the case $p < 0.63$. This can be checked by using the tools from Ref. [CM07], in which the search for an appropriate separable state was phrased into a semidefinite program. Hence we have the interval $p \in [0.63, 2/3)$, for which the performed tomography entanglement test indicates the presence

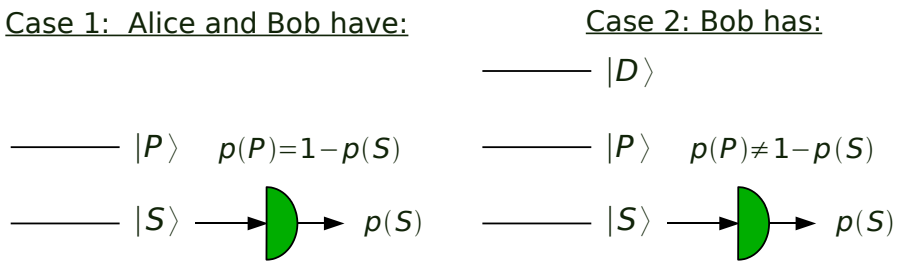

Figure 3.1: An ion in a trap can be modelled by a two level system, and the occupation of the lower level of the ion $|S\rangle$ is measured. Due to normalization, the other energy level $|P\rangle$ may be inferred from the measurement on $|S\rangle$. However, if this model is incorrect, and there is another energy level not taken into account on Bob's side ($|D\rangle$), then the occupation of $|P\rangle$ may different from that inferred from the single measurement on $|S\rangle$.

of entanglement although with the more realistic model it does not. Though this region might be small this error can become important in the multipartite scenario, where current experiments just operate at the border of genuine multipartite entanglement [HHR$^+$05, LKS$^+$05, GLY$^+$08]. Concerning the experimental consequences, however, two facts are important:

1. For experiments with ion traps it is known that the occupation probability for levels apart from the two logical states is very small. Given this additional measurement data, it is possible to provide a quantitative estimate of the resulting error in the used entanglement verification scheme, *e.g.*, the mean value of an entanglement witness. For typical entanglement witnesses employed in those scenarios, this error is far below the unavoidable statistical uncertainty, which is caused by the finite number of copies of a state available in any experiment.

2. Note that the probabilities $p(S)$ and $p(D)$ of each energy level can be measured independently by additional local rotations, hence at the expense of more measurements. Then the resulting probabilities correspond to the unnormalized two-level state ρ_{red} that is obtained from our modeled three-level system ρ_{tot} by a local projection, *i.e.*, $\rho_{\text{red}} = \Pi\rho_{\text{tot}}\Pi$, with $\Pi = |S\rangle\langle S| + |D\rangle\langle D|$. As long as we prove entanglement of the two-qubit system $\rho_{\text{red}}^{\text{AB}} = \mathbb{1}\otimes\Pi\rho_{\text{tot}}^{\text{AB}}\mathbb{1}\otimes\Pi$, this also implies entanglement for the total state $\rho_{\text{tot}}^{\text{AB}}$, since the projection is local.

   For instance, if an entanglement witness is measured, such as: $\mathcal{W} = |00\rangle\langle 00| + |11\rangle\langle 11| - |x^+x^+\rangle\langle x^+x^+| - |x^-x^-\rangle\langle x^-x^-| + |y^+y^+\rangle\langle y^+y^+|$ $+ |y^-y^-\rangle\langle y^-y^-|$, with $|x^\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $|y^\pm\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$ [GT09], then the mean value of this witness is just a linear combination of certain probabilities on the qubit space, and if the mean value is negative,

the state $\rho_{\text{red}}^{\text{AB}}$ and hence $\rho_{\text{tot}}^{\text{AB}}$ is entangled. This shows that additional dimensions of the Hilbert space alone do not invalidate the conclusion that the state is entangled when the measurement devices are characterized properly.

3.2 Positive Squashing Maps

Now we return to the formalism introduced in Section 2.2.1. For each local measurement, we have a target measurement, with POVM elements $F_Q^{(i)}$, which has a simple form that we would like to use for the entanglement verification process. Also there is a full measurement, with POVM elements $F_M^{(i)}$, which describes a realistic model of the actual detector in the experiment. In the above ion-trap example we considered the case of qubit target observables, while our full operators were acting on a qutrit system.

Consider the case where in an experiment the expectation values of the full operators $F_M^{(i)}$ are measured, but instead they are interpreted as the expectation values of the target observables $F_Q^{(i)}$. The question arises, whether this may lead to a false entanglement verification. In the following we provide a simple condition on the two operator sets only which excludes such a possibility, and hence guarantees the presence of entanglement.

As in the previous chapter, we would like a squashing model that equates the full measurement to a squashing map followed by the target measurement (cf. Fig. 2.2). The difference here is that we do not require the squashing map to be completely positive or trace-preserving. However, the squashing map must be positive, so that its output is a valid density operator that will be measured by the target detector. As such, Eqn. 2.1 still applies to the squashing map Λ, rewritten here as:

$$\text{Tr}\left[\rho_{\text{F}} F_M^{(i)}\right] = \text{Tr}\left[\rho_{\text{F}} \Lambda^\dagger(F_Q^{(i)})\right], \tag{3.2}$$

where ρ_{F} is the input density operator in the full Hilbert space. Because of the similarities of this squashing map to the one in the previous chapter, we use the term *positive squashing operation* in order to refer to the map Λ (or its adjoint $\Lambda^\dagger$) in this chapter. Note that we could still consider the case of a trace-preserving map Λ (or unital map $\Lambda^\dagger$) such that density operators are mapped to properly normalized density operators; however this requirement is not mandatory. An example of a non-trace preserving, but positive map between operator sets is given by the matrix of moments, also called the expectation value matrix, [SV05, HML08, MPHH]. The only difference is that we must be careful with entanglement criteria on the target space that explicitly employ the normalization of the density operators, but this can also be dealt with [MPHH].

The advantage of such a positive squashing operation here is that the structure of separable states (from the full to the target Hilbert space) remains invariant, and hence any successful entanglement verification on the target space directly translates to a positive verification statement on the full Hilbert space. More formally, suppose if a positive (but not necessarily completely positive)

trace-preserving squashing map exists for a set of full and target measurements, then it obeys the first line of Eqn. (2.2). If entanglement verification is performed such that two parties, Alice and Bob, use the full measurement, but use their data to verify entanglement with respect to the target observables $F^{(i)}_{Q,A} \otimes F^{(j)}_{Q,B}$, then they also prove the presence of entanglement for the full operator set $F^{(i)}_{M,A} \otimes F^{(j)}_{M,B}$. An analogous statement holds for more than two particles.

To prove this statement, consider the data that provide the expectation values E_{ij}, that obey the identity $E_{ij} = \mathrm{Tr}(\rho_{\mathrm{AB}} F^{(i)}_{M,A} \otimes F^{(j)}_{M,B}) = \mathrm{Tr}[\Lambda_{\mathrm{AB}}(\rho_{\mathrm{AB}}) F^{(i)}_{Q,A} \otimes F^{(j)}_{Q,B}]$ due to the property of the squashing operation. Now for any separable state on the full bipartite Hilbert space $\rho^{\mathrm{sep}}_{\mathrm{AB}} = \sum_k p_k \rho^k_{\mathrm{A}} \otimes \rho^k_{\mathrm{B}}$, we obtain:

$$\sigma^{\mathrm{sep}}_{\mathrm{AB}} := \Lambda_{\mathrm{AB}}(\rho^{\mathrm{sep}}_{\mathrm{AB}}) = \sum_k p_k \, \Lambda_{\mathrm{A}}(\rho^k_{\mathrm{A}}) \otimes \Lambda_{\mathrm{B}}(\rho^k_{\mathrm{B}}), \tag{3.3}$$

which represents a valid (normalized) separable density operator on the bipartite target Hilbert space because of positivity of the corresponding (unital) maps, and is compatible with the observed data. Consequently, if the incompatibility of the mean values of $F^{(i)}_Q$ with all separable states on the target space can be proven, then the density matrix on the full space must be entangled. Note that here we only need positivity of Λ_{A} and Λ_{B} and not complete positivity.

Note that a local squashing operation between operator sets does not represent the most general map between bipartite observable sets that preserve the structure of separable states; however we neglect other options on behalf of the "locality" of this connection. Furthermore note that since we do not require a completely positive map, it can happen that unphysical (not positive semidefinite) density matrix can be obtained on the target space; such an operator is then also incompatible with a separable state. However this situation can only occur for an entangled state on the full bipartite Hilbert space, hence the conclusion of the entanglement verification process remains unaffected.

Finally, let us add that the precise state reconstruction technique needed for the tomography entanglement test, either direct inversion of Born's rule or maximum likelihood estimation [Hra97] (although there are even problems associated with them [BK]), does not conflict with a positive but not completely positive squashing operation. If the corresponding operator on the target space is positive semidefinite both reconstruction techniques deliver the same operator (in the limit where exact knowledge of the expectation value is obtained). Because any separable state is represented by a valid separable target state this excludes the possibility that a separable state is mapped to an entangled state by the reconstruction process. In the case of an unphysical "entangled" target operator a direct inversion of Born's rule the entanglement would be directly "witnessed". Note that in this case it should be convincing that the actual measurement description $F^{\mathrm{A}}_Q \otimes F^{\mathrm{B}}_Q$ cannot be the precise one for the experiment. In contrast the maximum likelihood method produces the closest positive semidefinite operator [BK] (with respect to the likelihood "distance"),

hence an unphysical, entangled target state can be mapped to a separable state via this reconstruction technique and thus escapes the tomography entanglement test. But this does not bother us here, because some entangled states are missed anyway due to the simplified operator set.

3.3 Criteria for the Existence of a Positive Squashing Map

In this section we investigate which requirements need to be fulfilled by the two different operator sets in order to be connected by a positive squashing operation. In the previous chapter, we used the Choi-Jamiłkowski isomorphism to get a handle on the squashing map. We could continue along this vein, and in that case, the Choi-Jamiłkowski operator $\tau_{\mathrm{A}} \otimes \tau_{\mathrm{B}}$ would correspond to an entanglement witness. The linear constraints Eqn. 2.3a could be solved, and then any remaining open parameters would have to be chosen such that the Choi-Jamiłkowski operator is an entanglement witness. However, for our purposes here, we take a different path that provides a clear interpretation for the existence of such a positive linear map and which will also be employed in the next section to try to find the positive squashing model for the six-state polarization measurement.

The linear constraint Eqn. (3.3) directly allows us to read off a necessary condition: it states that for each physical density operator ρ_{F} in the full Hilbert space there exists a valid density operator $\Lambda(\rho_{\mathrm{F}})$ (as long as Λ is trace-preserving) in the target space such that both operators assign the same expectation values for the considered observables. Hence all possible expectation values E_i that can in principle be observed on the full Hilbert space must remain physical with respect to the target observables. As we will see, this condition also becomes sufficient if the target POVM elements $F_Q^{(i)}$ with $i = 1, \ldots, n$ provide a complete tomographic set. We can then make the following statement: *The tomography entanglement test is error-free as long as the full local observables on Alice and Bob's side can only produce measurement results which are also consistent with the local target, or reconstruction observables.*

For the following proposition we need to define the set of possible physical expectation values associated with a given set of observables, defined for the full observables as

$$\begin{aligned} \mathcal{S}_M \quad = \quad & \Big\{ \vec{E} \in \mathbb{R}^n \Big| \text{there is a } \rho \in \mathcal{D}(\mathcal{H}_F) \text{ such that} \\ & E_i = \mathrm{Tr}(\rho F_M^{(i)}) \text{ for all } i = 1, \ldots n \Big\}, \end{aligned} \tag{3.4}$$

and a similar definition for the operator set on the target system $\mathcal{S}_{\mathrm{Q}}$. To conclude, we have the following characterization:

Proposition 3.3.1 (Existence)**.** *The set of full observables $\{F_M^{(i)}\}$ and the tomographically complete set of target observables $\{F_Q^{(i)}\}$ are related by a unital*

squashing operation $\Lambda^\dagger$ if and only if it holds that $\mathcal{S}_M \subseteq \mathcal{S}_Q$. If the set of considered observables on the target space is not tomographically complete, then both observable sets can be extended by appropriate target and full operators in order to meet this condition.

Proof. One direction of the proof is clear: suppose that there exists a positive trace-preserving squashing operation Λ. For any $\vec{E} \in \mathcal{S}_M$ we must have a density operator ρ_F such that $E_i = \mathrm{Tr}(\rho_\mathrm{F} F_M^{(i)}) = \mathrm{Tr}[\Lambda(\rho_\mathrm{F}) F_Q^{(i)}]$. Because of the properties of the corresponding map we receive a valid target density operator $\rho_\mathrm{T} := \Lambda(\rho_\mathrm{F})$ which provides the same expectation values $\vec{E}$, hence $\vec{E} \in \mathcal{S}_Q$. This shows that $\mathcal{S}_M \subseteq \mathcal{S}_Q$, and hence proves the first direction.

For the other direction, we employ the fact that the set of target operators are tomographically complete and the set inclusion $\mathcal{S}_M \subseteq \mathcal{S}_Q$ to explicitly write down the positive squashing operation. First note that for a given set of physical expectation values $\vec{E} \in \mathcal{S}_\mathrm{T}$, the corresponding target density operator is uniquely determined by a direct inversion of Born's rule, $\mathcal{R}_\mathrm{T} : \vec{E} \mapsto \rho_\mathrm{T}(\vec{E})$, *i.e.*, by a linear reconstruction mechanism that maps the expectation values to its explicit density operator. Moreover for a given full density operator ρ_F the corresponding expectation values are already determined, which is described by the linear map $\mathcal{M}_\mathrm{F} : \rho_\mathrm{F} \mapsto \vec{E}$. Combining these two maps according to

$$\Lambda = \mathcal{R}_\mathrm{T} \circ \mathcal{M}_\mathrm{F} \tag{3.5}$$

provides the squashing operation. That is, for a given input state ρ_F, the expectation values E_i of the full operator set are first computed and then these values are used in the reconstruction algorithm (that depends on the target operators) to obtain the corresponding target output state. The set inclusion guarantees that any valid full density operator is mapped to a valid target state, hence the described map is already positive. Since both maps in the decomposition are linear the overall map is linear as well. This proves that we have a unital squashing map $\Lambda^\dagger$, and hence have proved the other direction.

The non-tomographic case directly follows from the tomographic one, since the positive linear map $\Lambda^\dagger$ requires that it is defined on the complete target operator space, or equivalently on a set of operators that provides tomography. Therefore, the addition of operators to ensure that tomography is performed allows a squashing map to exist. □

In a concrete example the proposition only helps if the sets $\mathcal{S}$ are known. Although in general this can be a non-trivial task, approximation techniques can be employed for a special set of observables or even a hyperplane characterization for the exact determination, see Ref. [MKL08] for more details.

Finally, let us note that a completely positive map can be characterized by a set inclusion requirement as well, if an additional reference system R is added with dimension equal to that of the full space (or of the target space, in the case the dual map) on each side, because complete positivity of Λ just means that $\mathrm{id}_\mathrm{R} \otimes \Lambda$ is positive. However, we could also use the formalism developed in the previous Chapter, which might be a more useful approach.

3.4 Example: Six-State Active Basis Choice

In this section, we apply the developed formalism to a relevant physical measurement setup: the six-state polarization measurement with an active basis choice, as described in Section 2.3.2. This measurement is not only useful for QKD, but can also be used in entanglement verification as it performs tomography on an input qubit space. We would like to find a squashing map for the full measurement on a multi-photon input in the space of two orthogonal polarization modes to the same measurement, but on a single photon and vacuum input in two orthogonal polarization modes. First, we know from the previous chapter that there does not exist a completely positive squashing map (cf. Section 2.3.2). As such, a positive squashing map may exist instead, so we apply the formalism developed in this section, and in particular Prop. 3.3.1.

In order to find a squashing map, the double click events must be post-processed, since these events are incompatible with a single photon interpretation, but they nevertheless contribute to the normalization. This is typically done by the process of randomly assigning double click events in each basis to a random bit value in the same basis, which was introduced in the previous chapter. We start with a perfect polarization mode description of the full operators; imperfections like finite efficiency or dark counts are considered later (see also Ref. [Lüt99a]). The "no click" outcome is independent of the chosen polarization basis and becomes $F_{\mathrm{vac},\alpha} = |0,0\rangle\langle 0,0|$. All other observables are block-diagonal with respect to the photon number subspace, *i.e.*, $F_{i,\alpha} = \sum_{n=1}^{\infty} F_{i,\alpha}^n$ and for a fixed number of photons the POVM elements have the same form as in Eqn. 2.4, since this is essentially the same measurement performed in the BB84 case, except with an addition of another basis:

$$F_{i,\alpha}^n = \frac{1}{2}\left[\mathbb{1}_n + (-1)^i \left(|n,0\rangle_\alpha\langle n,0| - |0,n\rangle_\alpha\langle 0,n|\right)\right], \tag{3.6}$$

with $i \in \{0,1\}$, α is one of the bases $\{x,y,z\}$, and $\mathbb{1}_n$ represents the identity operator in the n-photon subspace, which appears because of the chosen post-processing scheme. This perfect polarization description is also employed for the target operators, however only acting on the vacuum $F_{\mathrm{vac},\alpha}^Q = |0,0\rangle\langle 0,0|$ or on the single photon subspace $F_{i,\alpha}^Q = F_{i,\alpha}^1$ with $i = 0,1$.

Let us further comment on these observable sets: Note that if the following standard basis for the single photon subspace $|1,0\rangle_z = |0\rangle$ and $|0,1\rangle_z = |1\rangle$ is selected, then each difference of the single click outcomes equals to a familiar Pauli operator, *i.e.*, $\sigma_\alpha = F_{0,\alpha}^1 - F_{1,\alpha}^1$ for all α. Hence each of the single click operators $F_{i,\alpha}^Q$ with $i = 0,1$ corresponds to a projection onto one of the two different eigenstates of the related Pauli operator σ_α. Furthermore the corresponding difference between the full observables $F_\alpha = F_{0,\alpha} - F_{1,\alpha}$ is again block-diagonal and each n-photon part is given by

$$F_\alpha^n = F_{0,\alpha}^n - F_{1,\alpha}^n = |n,0\rangle_\alpha\langle n,0| - |0,n\rangle_\alpha\langle 0,n|, \tag{3.7}$$

according to Eqn. (3.6). Note that these observables are also accessible with a different polarization measurement that only uses a single threshold detector,

and which has alternatively been employed for polarization experiments, cf. Ref. [JKMW01]. In this setup, only one of the outputs of the polarizing beam splitter. It is direct that the operators F_α can be obtained by using the difference of the two outputs. However in order to obtain the normalization, the overall input has to be measured via a threshold detector, *i.e.*with no polarizing beam splitter. Therefore, the measurement should include both threshold detectors, one at each end of the polarizing beamsplitter.

The following theorem proves the positive squashing property between the two given sets of observables; however it also applies to the other measurement description of Ref. [JKMW01].

Theorem 3.4.1. *There exists a positive, but not completely positive unital squashing operation $\Lambda^\dagger$ for the operator sets $\{F^Q_{i,\alpha}\}$ and $\{F_{i,\alpha}\}$,* i.e. $\Lambda^\dagger(F^Q_{i,\alpha}) = F_{i,\alpha}$. *Therefore, the interpretation of the $\{F_{i,\alpha}\}$ as single photon measurements $\{F^Q_{i,\alpha}\}$ does not invalidate the entanglement verification scheme.*

Proof. In order to prove the existence of a positive squashing operation we only need to focus on the "click" events, since the vacuum part can be directly removed by a projection discriminating between the vacuum and all other Fock states, *i.e.*it can be removed as a flag. Note that it is sufficient to prove the squashing operation for a complete set of linear independent target operators only, because other linear dependencies are implicitly present in the linear map. In short, it is equivalent to prove a unital squashing operation $\Lambda^\dagger(\sigma_\alpha) = F_\alpha$ for all $\alpha \in \{x, y, z\}$, where F_α is the described difference between the click outcomes of the full observables.

Since we only concentrate on the single photon subspace we are equipped with a full tomographic set and hence can readily apply Prop. 3.3.1, such that it remains to prove $\mathcal{S}_M \subset \mathcal{S}_Q$. Since each full observable is photon number diagonal, $\mathcal{S}_M$ is given by the convex hull of all n-photon sets $\mathcal{S}^n_M$, *i.e.*, the set of physical expectation values on an n-photon state. Hence we need to verify that each n-photon state can only produce expectation values which are also compatible with a single photon state, *i.e.*, $\mathcal{S}^n_M \subset \mathcal{S}^1_M = \mathcal{S}_Q$ for all $n \geq 1$. The set $\mathcal{S}^1_M$ directly equals the familiar Bloch sphere. Hence we prove the existence of a positive squashing operation if we can show that

$$\sum_{\alpha\in\{x,y,z\}} [\mathrm{Tr}(\rho F^n_\alpha)]^2 \leq 1 \tag{3.8}$$

holds for all n-photon density operators ρ, and for all photon numbers $n \geq 1$.

In order to simplify the analysis in the following, each operator F^n_α can be regarded as an operator acting onto an n-qubit space. Indeed, the n-photon Hilbert space $\mathcal{H}^n_M = \mathbb{C}^{n+1}$ is isomorphic to the symmetric subspace $\mathrm{Sym}(\mathcal{H}_n)$ of an n-qubit system $\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}$. Using the given standard basis definition we obtain:

$$F^n_z = |0\rangle\langle 0|^{\otimes n} - |1\rangle\langle 1|^{\otimes n}, \tag{3.9}$$

while for any other operator F^n_α the states $|0\rangle, |1\rangle$ are replaced with the eigenvectors of the corresponding Pauli matrix σ_α.

Expanding these operators in a multi-qubit basis gives

$$\begin{aligned} F_\alpha^n &= \left(\frac{\mathbb{1}+\sigma_\alpha}{2}\right)^{\otimes n} - \left(\frac{\mathbb{1}-\sigma_\alpha}{2}\right)^{\otimes n} \\ &= \frac{1}{2^{n-1}} \sum_{j \text{ odd}} \sum_{\pi} \pi \left(\sigma_\alpha^{\otimes j} \otimes \mathbb{1}^{\otimes(n-j)}\right), \end{aligned} \tag{3.10}$$

where $\sum_\pi$ denotes the sum over all possible permutations $\pi(\cdot)$ of the subsystems that yield different terms.

Next, we exploit the result from Ref. [TG05] that for odd j every quantum state ρ, hence also each state on the symmetric space, satisfies

$$\sum_{\alpha=x,y,z} \left\langle \pi(\sigma_\alpha^{\otimes j}) \right\rangle_\rho^2 \leq 1, \tag{3.11}$$

with the abbreviation

$$\left\langle \pi(\sigma_\alpha^{\otimes j}) \right\rangle_\rho = \mathrm{Tr}\left[\rho\, \pi\Big(\sigma_z^{\otimes j} \otimes \mathbb{1}^{\otimes(n-j)}\Big)\right]. \tag{3.12}$$

This inequality is based on the property that the observables $\pi(\sigma_\alpha^{\otimes j} \otimes \mathbb{1}^{\otimes(n-j)})$ with $\alpha \in \{x, y, z\}$ have all eigenvalues equal to ± 1 and anti-commute pairwise. To prove this property, let M_i be anti-commuting observables (*i.e.*, $M_i M_j + M_j M_i = 0$ for all $i \neq j$) with $M_i^2 = \mathbb{1}$ for all i and let λ_i be real coefficients with $\sum_i \lambda_i^2 = 1$. Then $(\sum_i \lambda_i M_i)^2 = \mathbb{1}$. Therefore, $(\sum_i \lambda_i \langle M_i\rangle)^2 \leq \langle (\sum_i \lambda_i M_i)^2\rangle = 1$, hence $\sum_i \lambda_i \langle M_i\rangle \leq 1$, and, since the λ_i are arbitrary, $\sum_i \langle M_i\rangle^2 \leq 1$.

Note that this identity holds for all occurring j and for all possible permutations π. Consequently we obtains

$$\begin{aligned} &\sum_\alpha \left[\mathrm{Tr}(\rho F_\alpha^n)\right]^2 \\ &= \frac{1}{2^{2n-2}} \sum_{j,j' \text{ odd}}^{n} \sum_{\pi,\pi'} \left[\sum_\alpha \left\langle \pi(\sigma_\alpha^{\otimes j}) \right\rangle_\rho \left\langle \pi'(\sigma_\alpha^{\otimes j'}) \right\rangle_\rho\right] \leq 1, \end{aligned} \tag{3.13}$$

where the inequality Eqn. 3.11 and the Cauchy-Schwarz inequality was used to upper bound each term in the squared bracket by 1. For the final result the numbers of distinct permutations π need to be counted, which is given by a corresponding binomial coefficient. □

How can we now use this result in the tomography entanglement test of a PDC source? First each party measures along all three different polarization axes. Next an active post-processing of the double click events needs to be done or the corresponding rates and/or probabilities of the full operators need to be computed. Afterwards both parties can safely use the single photon assumption, or more precisely, the set of perfect single photon target operators $\{F_{i,\alpha}^Q\}$ to compute the corresponding two-qubit state ρ_{AB} (single photon subspace on each side) via their preferred reconstruction technique. In case that this reconstructed

state is entangled, the observed data still verify entanglement if both parties believe in the more realistic measurement description $\{F_{i,\alpha}^M\}$.

Next we consider imperfections of the photo-detectors. We can apply the same tools used in Section 2.6 to the detector here. This means that if there is a common inefficiency for the threshold detectors, then the squashing map for the imperfect measurement is first a beamsplitter modelling the loss, followed by the perfect squashing map. The same is true for misalignment errors, which can be modeled by a fixed depolarizing channel on each photon individually. For dark counts that can be modeled as a particular post-processing scheme on the classical outcomes, the same procedure in Section 2.6 applies. Even the extension to a multi time-mode description is possible using the map found in Section 2.5. Therefore we can use the squashing map to first turn multiple time modes into a single one, followed by a squashing map that takes multi-photon signals, to a single photon.

Concerning real experiments, note that double-clicks in a spatial mode can occur due to different physical mechanisms. First, it can happen that due to the higher orders in the PDC process more than the desired number of photons are generated and injected into the setup. Second, dark counts may lead to double click events. Finally, double click events can arise from the statistical nature of the state preparation: In many experiments (cf. Ref. [LZG$^+$07]) entangled multi-photon states are generated by producing several entangled photon pairs first, and then letting them interact via beam splitters. However, the desired state is typically only produced if all the photons are distributed uniformly over all the spatial modes, but which normally does not happen all the time. Hence it can occur (due to the state preparation process) that one of the spatial modes contains more than just one photon, which then drastically increases the double click rate at the outcome side.

While the double click rates by the described first two mechanisms are typically very small, the contribution of the last mechanism can be quite large. For instance using the state preparation setup from Ref. [LZG$^+$07] the probability that one of the spatial modes contains two photons is as high as 75%.

Then, it is worth mentioning that the post-processing used in the above scheme is usually not applied in real experiments: double click events are typically just thrown away. It should be stressed that for double click events from the third mechanism this is justified: Since in this case some spatial mode does not contain any photon, disregarding these events is equivalent to projecting the total multi-photon state onto the space where each mode contains at least one photon. Since this is a local projection it cannot produce fake entanglement. For the other mechanisms, this depends (similar to the ion trap example before) on the actual double count rates and hence on the concrete experiment.

Usually the amount of these undesired events is usually small. For instance, see the 4-photon experiment of Ref. [WSK$^+$08]. It should be noted, however, that in experiments with more and more photons, these rates can be higher [LWZ$^+$09], so that the penalty effect of the post-processing scheme becomes larger.

Additionally, it can be proved that the corresponding squashing map is *com-*

pletely positive on the single and two photon subspace (cf. Section 2.3.2). Hence a violation of positivity of the corresponding target density operator is only observed if the local multi-photon contributions are very large in comparison to the single and double photon part (and even then only for very particular entangled states); consequently it is very unlikely to observe such a non-positive target operator in a real PDC experiment.

As a last point we should make it clear that the Theorem 3.4.1 cannot always be applied. Especially in multipartite experiments, it can happen that we do not want to obtain full tomography on the multipartite target space but instead tries to measure an entanglement witness with the least number of different global measurement settings. This may require more than three different settings on each photon. For instance, in the six-photon experiment of Ref. [LZG$^+$07] an entanglement witness was measured which required seven measurements settings of the type $M_i \otimes M_i \otimes ... \otimes M_i$, which is a significant advantage compared with the $3^6 = 729$ settings required for state tomography. However, on each photon, seven polarization measurements have been made and the target observables are tomographically overcomplete. In such cases this theorem does not apply, because the linear dependencies imposed by the target operators are not satisfied by the full observable set, cf. Eqn. (3.2), hence the local squashing operation does not exist. Here one might proceed with a global, separable squashing operation as was discussed in Section 3.2.

3.5 Further Directions

The formalism used to connect a full measurement to a target measurement (cf. Eqn. 3.3) uses a specific form of the squashing map. Namely, for each party, there is a local map that reduces their part of the full state to the target space. However, we could think of a more general map between bipartite, or multipartite, observable sets that preserve the structure of separable states, *i.e.*that never map a separable state in the full space to an entangled state in the target space. This extra condition adds an additional complication in finding the squashing map, however it also allows a map which is more general, which could provide a broader formalism to handle a wider variety of measurements in entanglement verification.

Another possibility for future work could be to find a quantitative measure of entanglement of the full system, given a reconstruction on the level of the target system. To do this we first consider an entanglement measure E. An entanglement measure is simply a function used to quantify the amount of entanglement a given state has [HHHH09]. Its input is a quantum state, and its output is a constant: $E(\rho) = c$. Typically entanglement measures are chosen such that if the output $c = 0$, then the input state ρ was separable. If the output $c > 0$, then state was entangled. Another property of entanglement measures is that they should not increase the amount of entanglement in a state under the application of local operations and classical communication (LOCC). In other

words, E is LOCC monotone: (where here we focus on the bipartite case)

$$E(\rho_{\mathrm{AB}}) \geq E(\Lambda_{\mathrm{LOCC}}[\rho_{\mathrm{AB}}]), \tag{3.14}$$

where Λ_{LOCC} is a LOCC transformation—a particular case of a CPTP map. In particular this means that E is monotone with respect to CPTP local operations:

$$E(\rho_{\mathrm{AB}}) \geq E((\Lambda_{\mathrm{A}} \otimes \Lambda_{\mathrm{B}})[\rho_{\mathrm{AB}}]). \tag{3.15}$$

Thus, if we use the squashing model realized by local CPTP maps, the entanglement of the reconstructed squashed state $(\Lambda_{\mathrm{A}} \otimes \Lambda_{\mathrm{B}})[\rho_{\mathrm{AB}}]$ is a lower bound for the entanglement of the physical state actually prepared. It can be shown that it is possible to generalize Eqn. 3.15 to the case of positive but not completely positive maps, at least for the entanglement measure called negativity [Z$^+$98, VW02], which is one of the few entanglement measures that can be easily computed (cf. [MGB$^+$09]). This may make it possible to use the reconstructed state in the target space to give a quantitative bound on the amount of entanglement in the full state.

Chapter 4

Conclusion

The ultimate goal of the squashing model is to help, along with other theoretical tools, to accurately describe experimental setups in quantum communication. We have provided necessary and sufficient conditions to find whether a given full measurement is connected to a target measurement via the squashing model. The existence of a squashing model in QKD implies that a security proof that assumes a small-dimensional input (such as a qubit) is measured, can be applied to a full optical implementation of the same protocol. In entanglement verification, a positive entanglement verification for a simplified set of target measurement operators is valid, even when the full measurement operators more accurately describe the measurement. In other quantum communication contexts, the squashing model validates the assumption that a simple target measurement is performed, even when the full measurement is what really describes the measurement.

We prove that several examples of detectors have squashing models, such as the BB84 measurement with active or passive basis choice, and the six-state measurement with a passive basis choice. While most of the examples do have a squashing model, it is important to note that some do not. For example, the six-state polarization measurement with an active basis choice does not have a squashing model which would be useful for QKD. Therefore the squashing model cannot be assumed for a given measurement; its existence should be verified. The formalism in this thesis provides a systematic method to find squashing models both analytically, and numerically. In the numerical case, it may be possible to find evidence supporting the existence of a squashing model, or disprove its existence.

We have also considered imperfections in measurements to see their effect on the existence of a squashing model. Although some imperfections have been accounted for, it is important to include a more general characterization of imperfections within the full measurement of the squashing model. This can be done with the formalism provided in this thesis, but requires a reevaluation of the examples considered previously.

References

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179, New York, dec 1984. IEEE.

[BBB+09] G. Berlin, G. Brassard, F. Brussieres, N. Godbout, J. Slater, and W. Tittel. Flipping quantum coins. *quant-ph/0904.3946*, 2009.

[BBJ+93] C. H. Bennett, G. Brassard, C. Jozsa, R. Crépeau, A. Peres, and W. K. Wooters. Teleporting an unknown quantum state via dualclassical and einstein- podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[Bel64] J. S. Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1:195–200, 1964.

[Ben92] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, may 1992.

[BK] R. Blume-Kohout. Optimal, reliable estimation of quantum states. quant-ph/0611080.

[BML08] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101:093601, 2008.

[BML09] N. J. Beaudry, T. Moroder, and N. Lütkenhaus. Squashing models for optical measurements. *in preparation*, 2009.

[BSGT] F. Brussieres, J. Slater, N. Godbout, and W. Tittel. *in preparation*.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69(20):2881–2884, Nov 1992.

[BZ06] Bengtsson and Życzkowski. *Geometry of Quantum States*. Cambridge University Press, 2006.

[Cho82] Man-Duen Choi. Positive linear maps. *Proc. Symp. Pure Math.*, 38:583, 1982.

[CLL04] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004.

[CM07] Marcos Curty and Tobias Moroder. Single-photon quantum key distribution in the presence of loss. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 75(5):052336, 2007.

[DMMS07] W. van Dam, F. Magniez, M. Mosca, and M. Santha. Self-testing of universal and fault-tolerant sets of quantum gates. *SIAM Journal on Computing*, 37(2):611–629, 2007.

[dP67] John de Pillis. Linear transformations which preserve hermitian and positive semidefinite operators. *Pacific J. Math.*, 23:129, 1967.

[FSW07] A. S. Fletcher, P. S. Shor, and M. Z. Win. Optimum quantum error recovery using semidefinite programming. *Phys. Rev. A*, 75:7, 2007.

[GLLP04] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.*, 4(5):325, 2004.

[GLY+08] Wei-Bo Gao, Chao-Yang Lu, Xing-Can Yao, Ping Xu, Otfried Gühne, Alexander Goebel, Yu-Ao Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. Experimental demonstration of a hyper-entangled ten-qubit Schrödinger cat state, 2008. arXiv:0809.4277.

[GT09] O. Gühne and G. Tóth. Entanglement detection. *Phys. Rep.*, 474:1, 2009.

[HHH99] R. Horodecki, M. Horodecki, and P Horodecki. Entanglement processing and statistical inference: The Jaynes principle can produce fake entanglement. *Phys. Rev. A*, 59:1799, 1999.

[HHHH09] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865, 2009.

[HHR+05] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al-kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt. Scalable multiparticle entanglement of trapped ions. *Nature*, 438:643, 2005.

[HJ85] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, 1985.

[HML08] H. Häseler, T. Moroder, and N. Lütkenhaus. Testing quantum devices: Practical entanglement verification in bipartite optical systems. *Phys. Rev. A*, 77:032303, 2008.

[Hor01] P. Horodecki. From limits of quantum nonlinear operations of multicopy entanglement witnesses and state spectrum estimation. *arXiv:quant-ph/0111036*, 2001.

[Hra97] Z. Hradil. Quantum-state estimation. *Phys. Rev. A*, 55:R1561, 1997.

[HRB08] H. Häffner, C. F. Roos, and R. Blatt. Quantum computing with trapped ions. *Phys. Reports*, 469:155, 2008.

[IWY02] K. Inoue, E. Waks, and Y. Yamamoto. Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89:037902, 2002.

[Jam72] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Mat. Phys.*, 3:275, 1972.

[JKMW01] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White. Measurement of qubits. *Phys. Rev. A*, 64:052312, 2001.

[KBAW00] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White. Experimental verification of decoherence-free subspaces. *Science*, 290:498, 2000.

[KGR04] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret key rate for qkd protocols using one–way classical communication. quant-ph/0410215, 2004.

[LAFCR+09] J. S. Lundeen, A. A. Feito, H. Coldenstrodt-Ronge, K. L. Pregnell, C. Silberhorn, T. C. Ralph, J. Eisert, M. B. Plenio, and I. A. Walmsley. Measuring measurement. *Nature Physics*, 5:27, 2009.

[LKS+05] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle, and D. J. Wineland. Creation of a six-atom 'Schrödinger cat' state. *Nature*, 438:639, 2005.

[Lüt99a] N. Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A*, 59:3301, 1999.

[Lüt99b] N. Lütkenhaus. Quantum key distribution: theory for application. *Appl. Phys. B*, 69:395, 1999.

[Lüt00] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000.

[LvC+09] Pavel Lougovski, S J van Enk, Kyung Soo Choi, Scott B Papp, Hui Deng, and H J Kimble. Verifying multipartite mode entanglement of w states. *New J. Phys.*, 11(6):063029, 2009.

[LWZ+09] Wieslaw Laskowski, Marcin Wiesniak, Marek Żukowski, Mohamed Bourennane, and Harald Weinfurter. Interference contrast in multi-source few photon optics. *J. Phys. B*, 42:114004, 2009.

[LZG+07] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan. Experimental entanglement of six photons in graph states. *Nature Physics*, 3:91, 2007.

[MFL07] X.-F. Ma, C.-H. Fung, and H.-K. Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, 2007.

[MGB+09] Tobias Moroder, Otfried Gühne, Normand J. Beaudry, Marco Piani, and Norbert Lütkenhaus. Entanglement verification with realistic measurement devices via squashing operations. *quant-ph/0909.4212*, 2009.

[MKL08] T. Moroder, M. Keyl, and N. Lütkenhaus. Truncated su(2) moment problem for spin and polarization states. *J. Phys. A: Math. Theo.*, 41:275302, 2008.

[MPHH] A. Miranowicz, M. Piani, P. Horodecki, and R. Horodecki. Inseparability criteria based on matrices of moments. arXiv.org/quant-ph/0605146.

[MY04] D. Mayers and A. Yao. Self testing quantum apparatus. *QIC*, 4:273, 2004.

[PCD+09] Scott B. Papp, Kyung Soo Choi, Hui Deng, Pavel Lougovski, S. J. van Enk, and H. J. Kimble. Characterization of multipartite entanglement for one photon shared among four optical modes. *Science*, 324:764, 2009.

[Ren07] R. Renner. Symmentry of large physical sysytems implies independance of subsystems. *Nature Physics*, 3:645–649, 2007.

[RW05] M. Reimpell and R. F. Werner. Iterative optimization of quantum error correcting codes. *Phys. Rev. Lett.*, 94:080501, 2005.

[SBPC+] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *quant-ph/0802.4155*.

[SML09] D. Stebila, M. Mosca, and N. Lütkenhaus. The case for quantum key distribution. *quant-ph/0902.2839*, 2009.

[SU07] Michael Seevinck and Jos Uffink. Local commutativity versus Bell inequality violation for entangled states and versus non-violation for separable states. *Phys. Rev. A*, 76:042105, 2007.

[SV05] E. Shchukin and W. Vogel. Inseparability criteria for continuous bipartite quantum states. *Phys. Rev. Lett.*, 95:230502, 2005.

[SV09] E. Shchukin and W. Vogel. Bell-type inequalities for arbitrary observables, 2009. arXiv:0902.3962.

[TG05] G. Tóth and O. Gühne. Entanglement detection in the stabilizer formalism. *Phys. Rev. A*, 72:022340, 2005.

[TT08] T. Tsurumaru and K. Tamaki. Security proof for qkd systems with threshold detectors. *Phys. Rev. A*, 78:032302, 2008.

[vELK07] S. J. van Enk, N. Lütkenhaus, and H. J. Kimble. On experimental procedures for entanglement verification. *Phys. Rev. A*, 75:052318, 2007.

[Ver26] G. S. Vernam. Cipher printing telegraph systems. *Journal of the AIEE*, 45:295, 1926.

[VW02] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65(3):032314, 2002.

[WSK+08] W. Wieczorek, C. Schmid, N. Kiesel, R. Pohlner, O. Gühne, and H. Weinfurter. Experimental observation of an entire family of four-photon entangled states. *Phys. Rev. Lett.*, 101:010503, 2008.

[Yur85] B. Yurke. Wideband photon counting and homodyne detection. *Phys. Rev. A*, 32:311, 1985.

[Z+98] K. Zyczkowski et al. Volume of the set of separable states. *Phys. Rev. A*, 58(2):883–892, 1998.

Appendix

4.1 Alternate Proof of the BB84 Measurement Squashing Map: Active Basis Choice

Here we perform an alternate proof for the existence of a squashing model for the BB84 measurement with an active basis measurement. This proof is an elaboration of the proof in Section 2.3.1. The proof that follows is more illustrative of a general procedure of solving the conditions given in Eqn. 2.3 explicitly than the proof given in the main text. We start from Section 2.3.1, where we are concerned with finding a squashing model for n photons to a single photon in the subspace P.

Depending on the parity of the number of incoming photons detected by the QND measurement proceeding the squashing map, n, one of the squashing maps, τ_{odd} or τ_{even}, will be applied. Consider the case where the photon number, n, is odd. The case where $n = 1$ is clearly trivial. The following is an orthonormal basis we use to represent the 4-dimensional subspace P: $|\phi_1\rangle = |n, 0\rangle_z$, $|\phi_2\rangle = |0, n\rangle_z$,

$$\begin{aligned} |\phi_3\rangle &= \frac{1}{C_1}\left[\sqrt{2^{n-2}}(|n,0\rangle_x + |0,n\rangle_x) - |n,0\rangle_z\right], \\ |\phi_4\rangle &= \frac{1}{C_1}\left[\sqrt{2^{n-2}}(|n,0\rangle_x - |0,n\rangle_x) - |0,n\rangle_z\right], \end{aligned} \tag{4.1}$$

where we define $C_g \equiv \sqrt{2^{n-g}-1}$. The qubit POVM elements $F_Q^{(b,\alpha)}$ are given by:

$$\left\{\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\right\} \tag{4.2}$$

in the standard basis. The full measurement operators $F_{M,\,n}^{(b,\alpha)}$ from Eqn. (2.4) in the basis given by Eqn. (4.1) are

$$F_{M,\,n}^{(b,z)} = \begin{bmatrix} \frac{1-b}{2} & 0 & 0 & 0 \\ 0 & \frac{b}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{bmatrix}, F_{M,\,n}^{(b,x)} = \frac{\mathbb{1}}{4} + \frac{(-1)^b}{4}\begin{bmatrix} 0 & s & 0 & t \\ s & 0 & t & 0 \\ 0 & t & 0 & u \\ t & 0 & u & 0 \end{bmatrix}$$

where $\mathbb{1}$ is the 4×4 identity matrix and we define the constants $s \equiv 2^{1-n}, t \equiv sC_1, u \equiv 1 - s$. To obtain the vectorized forms of the POVM elements $|F_Q^{(b,\alpha)}\rangle\rangle$ and $|F_M^{(b,\alpha)}\rangle\rangle$, the columns of their matrix form can be concatenated into vectors.

We can now impose Eqns. (2.3a) on the adjoint squashing map for the subspace P. Note that τ^R maps real vectors into real vectors (Eqn. (2.3a)), and therefore the complex conjugate $(\tau^R)^*$ also maps these same vectors to eachother. Therefore, the average of these two also performs the mapping, so we can assume that τ^R only contains real entries, without loss of generality. Also note that the POVM elements $|F_Q^{(b,\alpha)}\rangle\rangle$ do not span their complete vector space, and so τ^R is not completely determined by the linear constraints. Here we keep the undetermined entries as open parameters a_i, and after applying the linear constraints we have τ_{odd}:

$$\begin{bmatrix} 1 & 0 & 0 & a_1 & 0 & a_2 & 0 & a_3 \\ 0 & 0 & s-a_1 & 0 & -a_2 & 0 & t-a_3 & 0 \\ 0 & s-a_1 & 0 & 0 & 0 & a_4 & 0 & a_5 \\ a_1 & 0 & 0 & 1 & t-a_4 & 0 & -a_5 & 0 \\ 0 & -a_2 & 0 & t-a_4 & \frac{1}{2} & 0 & 0 & a_6 \\ a_2 & 0 & a_4 & 0 & 0 & \frac{1}{2} & u-a_6 & 0 \\ 0 & t-a_3 & 0 & -a_5 & 0 & u-a_6 & \frac{1}{2} & 0 \\ a_3 & 0 & a_5 & 0 & a_6 & 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

Next, we find the remaining open parameters to ensure that this map is positive semidefinite. To ensure this, all of its subdeterminants must be positive. Consider the following two-by-two determinants listed by the rows and columns they come from in the matrix for τ_{odd} above: $(2,3), (2,5), (2,7), (3,6), (3,8)$. From these we get $a_1 = s, a_2 = 0, a_3 = t, a_4 = 0, a_5 = 0$. This only leaves one open parameter, a_6, which can be found by applying the vector $(0,0,0,0,0,1,-1,0)$ to both sides of the above matrix, which should result in a positive scalar. This implies that $a_6 \geq 1/2 - s$. Similarly applying $(1,0,0,-1,C_1,0,0,-C_1)$ gives $a_6 \leq 1/2 - s$, and therefore $a_6 = 1/2 - s$. With all of the parameters determined, the eigenvalues of this map are found to be non-negative. Therefore, the adjoint squashing map exists. This means that there exists a squashing map for an odd number of photons, and since there are no open parameters left, it is unique.

Now consider the case where the QND measurement of the number of photons is even, $n \geq 2$. Following a similar procedure to the odd case, we have the same orthonormal basis as before except with the last two vectors of the basis for the subspace P changed to:

$$\begin{aligned} |\phi_3\rangle &= \tfrac{1}{\sqrt{2}} \left(|n,0\rangle_x - |0,n\rangle_x\right) \\ |\phi_4\rangle &= \tfrac{1}{C_2} \left(\sqrt{2^{n-3}}(|n,0\rangle_x + |0,n\rangle_x) - \tfrac{|n,0\rangle_z + |0,n\rangle_z}{\sqrt{2}}\right) \end{aligned} \tag{4.3}$$

In this basis the full measurement operator $F_{M,\,n}^{(b,z)}$ is the same as before, however

we now have:

$$F^{(b,x)}_{M,\,n} = \frac{\mathbb{1}}{4} + \frac{(-1)^b}{4}\begin{bmatrix} 0 & 0 & \sqrt{s} & 0 \\ 0 & 0 & \sqrt{s} & 0 \\ \sqrt{s} & \sqrt{s} & 0 & v \\ 0 & 0 & v & 0 \end{bmatrix}$$

where $v = \sqrt{2s}C_2$. Solving the linear equations (2.3a), we get the adjoint squashing map τ_{even} with open parameters d_i:

$$\begin{bmatrix} 1 & 0 & 0 & d_1 & 0 & d_2 & 0 & d_3 \\ 0 & 0 & -d_1 & 0 & \sqrt{s}-d_2 & 0 & -d_3 & 0 \\ 0 & -d_1 & 0 & 0 & 0 & d_4 & 0 & d_5 \\ d_1 & 0 & 0 & 1 & \sqrt{s}-d_4 & 0 & d_5 & 0 \\ 0 & \sqrt{s}-d_2 & 0 & \sqrt{s}-d_4 & \frac{1}{2} & 0 & 0 & d_6 \\ d_2 & 0 & d_4 & 0 & 0 & \frac{1}{2} & v-d_6 & 0 \\ 0 & -d_3 & 0 & d_5 & 0 & v-d_6 & \frac{1}{2} & 0 \\ d_3 & 0 & d_5 & 0 & d_6 & 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

Note that if $n = 2$ then $|\phi_4\rangle$ vanishes, so τ_{even} is given by removing the last two rows and columns in this matrix. Looking at the same locations for the two-by-two subdeterminants as in the odd case it can be seen that: $d_1 = 0, d_2 = \sqrt{s}, d_3 = 0, d_4 = 0, d_5 = 0$. Now consider the two three-by-three determinants $(1, 6, 7)$ and $(4, 5, 8)$. From the first we get $v^2/4 - d_6^2 \geq 0$ and so $d_6 \leq v/2$. From the second we get $-d_6^2 + 2\sqrt{1 - 2^{2-n}}d_6 + 3 \cdot 2^{-n} - 3/4 \geq 0$. This can be rewritten as $\Delta d(\Delta d - v) \leq 0$, where $\Delta d = d_6 - v/2$, which implies that $v/2 \leq d_6$. Combining these results gives $d_6 = v/2$. The eigenvalues of this map can also be shown to be non-negative. Therefore, the squashing map exists, and is uniquely determined.