Realisation of Quantum Operations Using Linear Optics

by

David Pitkanen

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

Waterloo, Ontario, Canada, 2011

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

The main topic of this thesis is linear optics and the implementation of quantum operations (measurements, quantum channels, and unitary rotations) on optical systems. In the opening chapter the basic notions needed to understand the rest of the thesis will be explained. These notions include defining a quantum state, measurement, quantum channel and the linear optics tool set.

The work in this thesis takes both fundamental and practical approaches to studying linear optical networks. For instance in the first chapter a proof is provided that shows that any unitary on a single mode Fock state can be realised with linear optics. The proof is constructive, however the approach to realising the unitary is not suitable for experimental implementation because it requires complicated ancilla states. As in the KLM proposal the procedure works only stochastically however by allowing the size of the ancilla to grow the probability of failure can be made arbitrarly small.

Furthermore we investigate the realisation of arbitrary channels in a specific encoding that we call a d-rail encoding. The only ancilla state that we allow is a vacuum ancilliary state and further restrictions were considered (e.g. photon counting). A proof is provided that using these resources only random unitaries can be applied deterministically using linear optics. An expression for the optimal probability of success for realising more general channels with these resources is also discussed.

As a final topic we also investigate the realisation of a quantum non-demolition measurement onto the dual rail qubit space. The investigation is a blend of both fundamental and practical approaches. To begin we employ a modified KLM-like procedure and show that the scheme can be realised perfectly but stochastically. The probability that the proper measurement is made can be made arbitrarly close to one using a suitably large ancilla state. In addition we consider an existing scheme [9] which uses practical sources (two single photon sources) to perform the measurement. The scheme does not realise the true measurement but instead has a free parameter in it which is the transmittiviy of a beamsplitter. The measurement will project onto a space that has a vacuum component. By adjusting the transmittivity of this beamsplitter the vacuum component can be made arbitrarly small but only at the expense of the probability of success of the procedure. In this thesis a modification that can be made to eliminate the vacuum component without changing the sources is introduced. The modification is surprisingly simple and only involves the addition of a single beamsplitter. In the proposal for the original amplifier it was used in simulations for DIQKD that included device imperfections. To show the improvement of our modification these DIQKD simulations are reproduced using the modified amplifier and its results are compared to the results of the original amplifier.

Acknowledgements

To begin I would like to thank my supervisor Norbert Lütkenhaus. In addition I would also like to thank Marco Piani, a co-supervisor I picked up midway through my Masters thesis work. Over the course of the last two years I believe I have added a lot of frustration to both my supervisors lives. Marco may have received a disproportionate amount of this frustration. However, the advice and guidance that I have recieved from them will no doubt help me in the future. This Master's thesis would have been quite impossible, for me, without both of their help.

I would like to acknowledge the IQC community as a whole. I feel really priveledged to have done my graduate studies here. In particular I would like to thank my fellow graduate students especially Evan Meyer-Scott and Botan Khani for technical advice and for making our graduate student room an interesting place to have worked.

Finally thanks to my committee members, Kevin Resch and Raymond Laflamme for their time and agreeing to be on my committee. Also thank you Joseph Emerson for agreeing to be on the final examining committee.

Dedication

This is dedicated to the quantum computer; I hope someone builds one someday.

Table of Contents

List of Figures

Chapter 1

Introduction

Euclid of Alexandria, nearly 2300 years ago, wrote 13 books on geometry. The collection was meant to be comprehensive, containing many of the important geometrical results that were known at the time. The impressive feature of the work was that he introduced five axioms and five definitions and each of the theorems within the work was derived using only these simple notions.

Euclid started an important trend in mathematics by defining the field he was studying with a set of axioms. The axioms he introduced led his contemporaries to consider the field of study that would result when certain axioms were removed or added. The study of non-Euclidean geometry was created when the fifth of Euclid's axioms was removed.

Classical and quantum computation and information theory differ from each other by an important axiom. If a system has two distinguishable states in classical physics there is an axiom that states that the system will occupy only one of the measurably distinct states. However in quantum mechanics there is no such axiom. Instead the state may exist in a superposition of the two states. Quantum devices, which perform computation and communication tasks on information encoded in quantum states, have been found to be capable of outperforming their classical counterparts [3, 6, 41].

There has been a great deal of interest recently in building quantum computing and communication devices. Linear optics is one of the simplest architectures that has been suggested for the realisation of useful quantum devices. Linear optical devices are simple tools both theoretically and experimentally, consisting only of collections of beamsplitters and phaseshifters. Linear optics provides an ideal testing ground for quantum information protocols. In combination with state preparation, a full scale quantum computer can be

built using linear optics [17]. However the gates used in the scheme only work probabilistically and the states that are required to implement them represent a major challenge to the experimental and theoretical quantum information and quantum optics communities. In this thesis linear optics implementations of quantum information protocols will be considered.

1.1 Basic Quantum Mechanics

1.1.1 Quantum State

If a quantum system has d distinguishable states then it can be described mathematically with a d-dimensional Hilbert space H. Any unit vector in the Hilbert space will describe a valid quantum state that the system may occupy. If we choose an orthonormal basis, $\{|i\rangle\}_{i=1}^{d}$, any state, $|\psi\rangle$, of the system may be written as

$$|\psi\rangle = \sum_{i=1}^{d} \alpha_i |i\rangle \ .$$

The interpretation of the quantum state follows from the fact that the system may exist in a superposition of distinguishably distinct states however when the state is measured only one of the states will be observed. Any orthonormal decomposition of the space will consist of a valid measurement basis that the system can be measured in. The probability that the state $|i\rangle$ is observed when $|\psi\rangle$ is measured is

$$|\alpha_i|^2 = |\langle i|\psi\rangle|^2 \ .$$

The term qubit is used to describe a system whose Hilbert space is two-dimensional.

1.1.2 Density Matrices

Using a state, $|\psi\rangle \in H$, in a Hilbert space a linear operator may be formed on the space, H,

$$|\psi\rangle \rightarrow |\psi\rangle\langle\psi| \ .$$

The resulting operator is a rank one projector and is called the density operator representation of the state, $|\psi\rangle$. In general with a probability distribution, $\{p_i\}_{i=1}^{n}$, and a

corresponding collection of states, $\{|\psi_i\rangle\}_{i=1}^n$, more general operators on the Hilbert space may be formed

$$\{p_i, |\psi_i\rangle\} \rightarrow \rho = \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i| \ .$$

The operator, ρ, represents a physical system that with probability p_i is in the state $|\psi_i\rangle$. The density matrix representation may be used when there is uncertainty about which state, $|\psi_i\rangle$, the system is in.

With a density operator the probability any state $|u\rangle$ is observed when the system is measured is straightforward to calculate. If we choose to measure the state in the basis $\{|u_i\rangle\}$ then the probability, p_i, of getting outcome $|u_i\rangle$ is

$$p_i = Tr(|u_i\rangle\langle u_i|\rho) \ .$$

A density matrix that can be expressed as a rank one projector is called a pure state. If the operator has a larger rank it is called a mixed state. The density matrix has unit trace and is a positive Hermitian operator.

1.1.3 Tensor Products and the Partial Trace

A tensor product is an abstract method of using two Hilbert spaces to build a larger Hilbert space. The tensor product of two Hilbert spaces, H_A and H_B, is denoted as $H_A \otimes H_B$. If two bases for the two Hilbert spaces are $\{|e_i\rangle\}_{i=1}^n$ and $\{|f_j\rangle\}_{j=1}^m$, respectively, then the corresponding basis for the tensor product space will be denoted as $\{|e_i\rangle \otimes |f_j\rangle\}$ where $1 \leq i \leq n$ and $1 \leq j \leq m$. An inner product for the tensor product Hilbert space will be inherited from the inner-products on the smaller spaces

$$(\langle e_i| \otimes \langle f_j|)\,(|e_k\rangle \otimes |f_l\rangle) = \langle e_i \mid e_k\rangle\langle f_j \mid f_l\rangle \ .$$

In quantum mechanics the operational interpretation of the tensor product is that the smaller Hilbert spaces in the product correspond to independent degrees of freedom [25]. A system which is represented as the tensor product of two spaces is referred to as bipartite. A system that is the tensor product of more than two spaces is referred to as multipartite. Here each component space in a tensor product will be referred to as a subsystem of the larger system.

From a density matrix, ρ_{AB}, which has two subsystems labelled A and B respectively, a density matrix that describes only one of the subsystems may be obtained. The procedure

that reduces the number of degrees of freedom in a system is called the partial trace operation. To perform the partial trace on a bipartite system we just select a measurement bases $\{|v_i\rangle\}$ and imagine that the system is measured in this basis but the result of the measurement is not revealed.

Therefore if $\{|v_i\rangle\}_{i=1}^n$ is a measurement basis and $|\psi\rangle = \sum_{i=1}^n \sqrt{p_i}|\psi_i\rangle \otimes |v_i\rangle$ is a state in bipartite system then the partial trace operation will induce the mapping

$$|\psi\rangle\langle\psi| \to \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i| \ .$$

Conversely given any mixed state $\rho_A = \sum_{i=1}^n p_i|\psi_i\rangle\langle\psi_i|$ one can imagine that the state is actually the reduced density matrix of the pure state $|\psi\rangle = \sum_{i=1}^n \sqrt{p_i}|\psi_i\rangle \otimes |v_i\rangle$ in a bipartite system. This pure state in the larger system is known as the purification of the mixed state ρ.

1.1.4 Pauli Matrices

The Pauli matrices are a set of three 2×2 matrices $\{\sigma_x, \sigma_y, \sigma_z\}$ which are linearly independent:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ .$$

When these matrices are combined with the identity matrix, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, they form a basis for the space of 2×2 matrices with complex entries, denoted as $M_2(\mathbb{C})$. An inner product may be defined on this space using the trace operation,

$$\langle A \mid B \rangle = \mathrm{Tr}(A^\dagger B) \ ,$$

if A and $B \in M_2(\mathbb{C})$. With this inner product the Pauli matrices and the identity matrix form an orthogonal set.

The Pauli matrices may be used to parameterize the space of density operators for a qubit system if the two level space is encoded such that

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ .$$

With this encoding the density operator in the qubit space will belong to $M_2(C)$ and can therefore be written as a linear combination of the identity operator and the Pauli matrices,

$$\rho = \frac{1}{2}\left(I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z\right) \ .$$

where the orthogonality of the Pauli matrices and the identity matrix can be used to show $r_i = Tr(\rho\sigma_i)$.

1.2 Quantum Channels and POVMs

The Schrödinger dynamics of a quantum state is a unitary rotation in its Hilbert space determined by a Hamiltonian operator. However if a bipartite state, ρ_{AB}, is evolving unitarily then the evolution of the reduced state ρ_A will not necessarily be unitary. It is rare that a quantum system can be thought of as being totally isolated from its environment. For this reason it is common to consider a form of transformation that takes into account the evolution of a subsystem that is being unitarily rotated in a larger space.

We consider a scenario where we have two subsystems which we label with the letters A and B. It is system A whose dynamics we wish to model and system B will be an n-dimensional space that we wish to ultimately ignore. The basis for system B will be $\{|i\rangle\}_{i=0}^{n-1}$. When system B is in its ground state the action of a unitary acting on this bipartite state may be described as

$$U : \ |i\rangle|0\rangle \rightarrow \sum_j A_j|i\rangle|j\rangle \ . \tag{1.1}$$

To ensure the orthogonality preserving properties of the unitary, the operators A_j must satisfy the property $\sum_{i=1}^{n} A_i^\dagger A_i = I$. After tracing out the second system the evolution of an arbitrary state by linearity of the unitary the transformation can be described by a map

$$\Lambda : |\psi\rangle\langle\psi| \rightarrow \sum_{j=1}^{n} A_j|\psi\rangle\langle\psi|A_j^\dagger \ .$$

The operators $\{A_i\}$ are known as Kraus operators and the transformation Λ is called a quantum channel. In general any set of operators that satisfy the condition $\sum_{i=1}^{n} A_i^\dagger A_i = I$ constitute a set of operators which form a valid channel. The representation of the channel in terms of a unitary and a ancilliary system initially in a fixed state –i.e. $|0\rangle\langle 0|$– is called

the dilation representation of the channel [26]. The quantum channel is considered the most general transformation that can be performed on a quantum system.

With an ancilla system and a measurement basis for the ancilla system the most general form of measurement that can be made on a state can also be described. The most general form of measurement is referred to as a of Projective Operator Valued Measure (POVM) and can be represented with a set of operators, $\{B_i\}_{i=1}^n$.

Similar to the case of a quantum channel if we are interested in measuring the system A we can introduce an ancilla system B in the state $|0\rangle$. Here we assume that the system A is in the state $|\psi\rangle$. We can then rotate the bipartite state $|\psi\rangle \otimes |0\rangle$ as in Eq.(1.1) and measure the ancilla system only, in the basis $\{|e_i\rangle\}_{i=1}^n$. By measuring the state $|e_i\rangle$ in the ancilla the state $A_i|\psi\rangle$ will be left in system A. Therefore the probability that the state $|e_i\rangle$ is measured is simply,

$$\mathrm{Tr}(A_i|\psi\rangle\langle\psi|A_i^\dagger) = \mathrm{Tr}(A_i^\dagger A_i \rho) \; .$$

if $\rho = |\psi\rangle\langle\psi|$. The operators $A_i^\dagger A_i$ are known as POVM elements. Any set of positive Hermitian operators $\{B_i\}$, with $B_i = A_i^\dagger A_i$, that satisfy the relation $\sum_{i=1}^n B_i = I$ are a valid set of POVM's.

The Kraus decomposition of a channel is in general not unique. With a set of n Kraus operators $\{A_i\}_{i=1}^n$ and an isometry, $V : \mathbb{C}^n \to \mathbb{C}^m$ where $m \geq n$, it is possible to construct a new set of Kraus operators,

$$C_i = \sum_{j=1}^n v_{i,j} A_j \; .$$

if $v_{i,j}$ are the matrix elements of the operator V. The operators C_i will form the same channel as the original Kraus operators since,

$$\begin{aligned}
\sum_{i=1}^m C_i|\psi\rangle\langle\psi|C_i^\dagger &= \sum_{i=1}^m \left(\sum_{j=1}^n v_{i,j} A_i\right) |\psi\rangle\langle\psi| \left(\sum_{k=1}^n v_{i,k} A_k\right)^\dagger \; , \\
&= \sum_{j,k=1}^m \left(\sum_{i=1}^n v_{i,j} v_{i,k}^* A_j\right) |\psi\rangle\langle\psi| A_k^\dagger \; , \qquad (1.2) \\
&= \sum_{j}^m A_j|\psi\rangle\langle\psi|A_j^\dagger \; . \qquad (1.3)
\end{aligned}$$

we have used the relation $\sum_{i=1}^n v_{i,j} v_{k,i}^* = \delta_{j,k}$ in Eq. 1.3. In the dilation representation of the channel the choice of basis that the ancilla is measured will not change channel. The

freedom to measure the ancilla in any basis without changing the channel gives rise to the non-uniqueness of the Kraus decomposition of the channel.

1.3 Linear Optics

A physical state of light can be decomposed into a set of optical modes. Each state of an optical mode can be written in terms of a Fock basis, $\{|n\rangle\}$, where the integer labelling the basis states represents the excitation level – or the number of photons it contains. Creation and annihilation operators can then be defined on the Fock space as linear operators that excite and de-excite the state of the mode,

$$\begin{aligned} a^\dagger |n\rangle &= \sqrt{n+1}|n+1\rangle \ , \\ a |n\rangle &= \sqrt{n}|n-1\rangle \ . \end{aligned}$$

Any Fock state $|n\rangle$ may be obtained by the repeated action of the creation operator on the vacuum state, so that $|n\rangle = \frac{1}{\sqrt{n!}} \left(a^\dagger\right)^n |0\rangle$.

A linear optical network will perform a transformation of the creation operators of the modes $\left\{a_i^\dagger\right\}$. These networks conserve the total photon number. The way that a linear optical network transforms a state may be deduced by the way that the network, U, rotates the creation operators, $Ua^\dagger U^\dagger$, as $U\frac{1}{\sqrt{n!}} \left(a^\dagger\right)^n |0\rangle = \frac{1}{\sqrt{n!}} \left(Ua^\dagger U^\dagger\right)^n U|0\rangle$, and for a linear optics network $U|0\rangle = |0\rangle$.

All linear optical networks consist of collections of beamsplitters and phase-shifters. A phase shifter acts on a single optical mode transforming the creation operator of the mode as $a^\dagger \rightarrow e^{i\theta}a^\dagger$. A beamsplitter will act on two optical modes and perform a rotation on them

$$\begin{aligned} a_1 &\rightarrow \cos\theta a_1 + ie^{-i\phi}\sin\theta a_2 \\ a_2 &\rightarrow ie^{i\phi}\sin\theta a_1 + \cos\theta a_2 \end{aligned}$$

The parameters $\cos\theta$ and $\sin\theta$ are the square roots of the transmittivity and reflectivity of the beamsplitter respectively. The factor $ie^{-i\phi}$ is called the phase of the beamsplitter.

1.4 Knill-Laflamme-Milburn (KLM) Procedure

Within the KLM paper [17] a procedure to teleport Fock states that have only single-photon and vacuum components, $c_0|0\rangle + c_1|1\rangle$, is developed. The procedure can be performed using

only linear optical elements but it requires large ancilla states of the form

$$|t_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{i=0}^{n} |1\rangle^{\otimes i} |0\rangle^{\otimes (n-i)} |s_i\rangle \ , \tag{1.4}$$

with $|s_i\rangle = |0\rangle^{\otimes i}|1\rangle^{\otimes (n-i)}$, used as resources. For any positive integer n the teleportation procedure can be implemented, however the probability that the procedure works successfully is $1 - \frac{1}{n+1}$.

For each $1 \leq k \leq n$ the total state of input and ancilla, $(c_0|0\rangle + c_1|1\rangle) \otimes |t_n\rangle$, will contain a superposition of two terms that have k photons in their first $n+1$ modes. These terms with k photons in their first $n+1$ modes will be $c_0|0\rangle|1\rangle^{\otimes k}|0\rangle^{\otimes (n-k)}|s_k\rangle$ and $c_1|1\rangle|1\rangle^{\otimes k}|0\rangle^{\otimes (n-k)}|s_{k-1}\rangle$. The teleportation procedure begins with a Fourier transform, $a_p \rightarrow \sum_{j=0}^{n} \exp \frac{i2\pi pj}{n+1} a_j$, on the first $n+1$ modes of the total state. The next step in the procedure is a photon measurement on the modes that were transformed. Because of the Fourier transform, if $1 \leq k \leq n$ photons are counted, no information will be obtained about where the photons originated from in the original ancilla and input state. Therefore the measurement will leave the unmeasured n modes in the state

$$c_0|s_k\rangle + c_1 e^{i\phi_k} \mid s_{k-1}\rangle \ . \tag{1.5}$$

The phase $e^{i\phi_k}$ will depend on the number of photons counted as well as on the modes the photons are counted in. Since $|s_k\rangle = |0\rangle^k|1\rangle^{n-k}$ the input mode will be teleported into the k^{th} mode of this state if the phase $e^{i\phi_k}$ is corrected.

Here we will be considering different encodings of logical qubits. By using a single mode with the vacuum and single photon states a logical encoding can be made for a qubit. The logical state of the qubit is simply the number of photons in the mode. We will refer to a qubit encoded in this manner as an occupation qubit and denote it with the same notation we use for the single photon and vacuum Fock states. An alternative encoding for a qubit is called a dual rail qubit where the two level space involves a single photon contained in two modes:

$$\begin{aligned} |\underline{0}\rangle &= |10\rangle \ , \\ |\underline{1}\rangle &= |01\rangle \ . \end{aligned}$$

An advantage of the dual rail encoding is that any rotation may be performed on a single dual rail qubit using linear optics [19].

The CSIGN gate is a unitary operation that acts on two qubits at once and performs the operation,

$$\text{CSIGN} : |ij\rangle \rightarrow (-1)^{ij}|ij\rangle \ ,$$

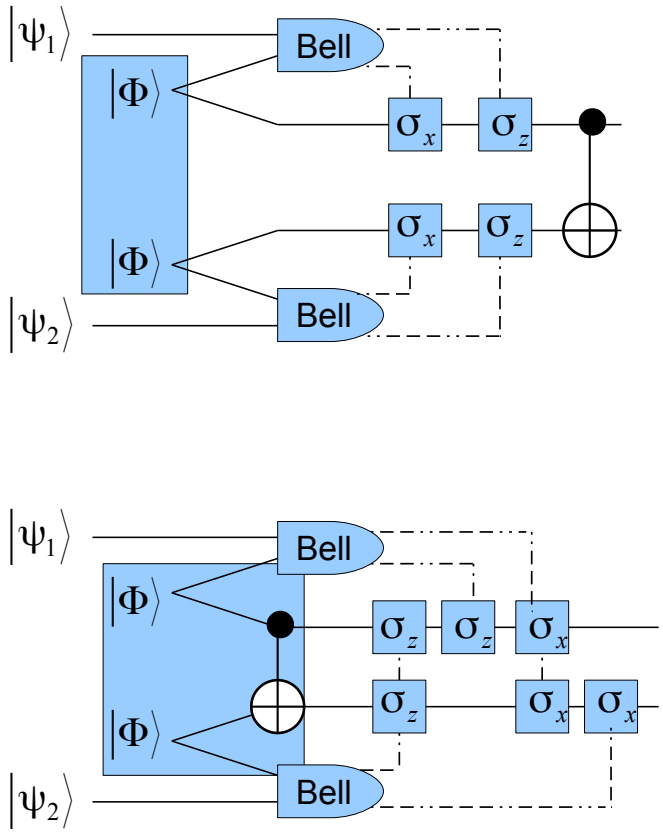

Figure 1.1: Proposed realisation of a CNOT gate using teleportation. Here the state $|\psi_1\rangle$ and $|\psi_2\rangle$ are qubit states and $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is an EPR state (a) To realise a CNOT gate on the qubit inputs teleportation procedures are performed on the qubits. The CNOT gate is performed on the output qubits of the teleportation procedures. (b) The CNOT gate is commuted with the single qubit correction unitaries of the teleportation procedure. This commutation changes the identities of the single qubit correction unitaries. The state $|\Phi\rangle \otimes |\Phi\rangle$ with a CNOT already performed on two of its modes is considered a resource state. Figure follows [22]

if $i, j \in \{0, 1\}$ and we are using the occupation qubit notation to denote the logical state of the dual rail qubit. A procedure called the Gottesman-Chuang (see Fig.1.1)trick showed that a CSIGN gate can be realised on a pair of qubits by performing the teleportation procedure on the qubits in parralel and modifying the ancilla state that is used in the procedure [11]. By applying the KLM teleportation procedure on a pair of dual rail qubits using the state

$$\begin{aligned} |cs_n\rangle &= \sum_{i,j=0}^{n} (-1)^{(n-i)(n-j)} |1\rangle^{\otimes i} |0\rangle^{\otimes (n-i)} |0\rangle^{\otimes i} |1\rangle^{\otimes (n-i)} \\ &\quad |1\rangle^{\otimes j} |0\rangle^{\otimes (n-j)} |0\rangle^{\otimes j} |1\rangle^{\otimes (n-j)} \ , \end{aligned} \tag{1.6}$$

a CSIGN gate may be realised [17]. As the combination of the CSIGN gate and single qubit unitaries form a universal set of gates the KLM procedure showed that universal computation could be performed near deterministically with linear optics.

1.5 Bell Inequality

When the description of a quantum state was introduced as an object capable existing as a superposition of two measurably distinct states it sparked a great deal of controversy [8]. It was suggested that this description of the state was incomplete and that a hidden local variable, λ, was attached to each state. It was suggested that simply the ignorance of this variable made the measurement outcomes appear random. To test the quantum description of the state against a local hidden variable theory a test was developed [2] that could be performed by a pair of distant parties. For the purposes of outlining this test we will refer to the the party members as Alice and Bob respectively.

In order to perform the test both parties need to be able to generate independent random variables that have binary outcomes. We label the two binary outcomes of Alice's variable as $\{a, a'\}$ and we label Bob's as $\{b, b'\}$. These random variables will be used as inputs in the experiment.

If a qubit state is measured in a basis $\{|x_1\rangle, |x_2\rangle\}$ the outcomes of the measurement will define a random variable, X

$$X = \begin{cases} +1 & \text{if } |x_1\rangle \text{ is measured} \\ -1 & \text{if } |x_2\rangle \text{ is measured} \end{cases} \tag{1.7}$$

During the test the parties will share a bipartite state, each party will be in possesion of a qubit, and each party will choose two different measurement bases which they label as

$\{A, A'\}$ and $\{B, B'\}$. From the relation in Eq.(1.7) each of these measurement bases defines a random variable. In the test the parties get many copies of a bipartite state $|\psi\rangle$. For each state that the parties receive they sample an input value from their random variable and use it to choose one of their measurement basis. The parties use their chosen basis to measure their copy of the shared state.

The CHSH inequality is an algebraic expression involving expectation values for the correlations that two parties may share. In the context outlined with the random variables $\{A, A', B, B'\}$ the algebraic expression for the CHSH inequality is

$$\langle AB\rangle + \langle A'B\rangle + \langle AB'\rangle - \langle A'B'\rangle = \langle (A + A')B\rangle + \langle (A - A')B'\rangle \leq 2 \tag{1.8}$$

The algebraic expression involving the quantities $\{A, A', B, B'\}$ is also referred to as a Bell parameter, S, and it is bounded above by 2 if the correlations the parties share can be explained with a local hidden variable. If the systems statistics are governed by a hidden random variable, λ, then each of the members of the set $\{A, A', B, B'\}$ will simply be functions of λ. The variable is hidden and we may only know a probability distribution $\{p(\lambda)\}$ that describes the different values it may assume.

With the hidden variable explanation the quantities in Eq.(1.8) can be evaluated with the relation

$$\langle XY\rangle = \sum_{\lambda} X(\lambda)Y(\lambda)p(\lambda) \ .$$

For the quantum description the brackets have the meaning

$$\langle XY\rangle = Tr(XY\rho) \ ,$$

if $\rho = |\psi\rangle\langle\psi|$ and

$$X = |x_1\rangle\langle x_1| - |x_2\rangle\langle x_2| \ \text{ and } \ Y = |y_1\rangle\langle y_1| - |y_2\rangle\langle y_2| \ ,$$

where $\{|x_1\rangle, |x_2\rangle\}$ is the measurement basis for X and $\{|y_1\rangle, |y_2\rangle\}$ is the measurement basis for Y. A local hidden variable description of the system would imply that for any value of λ one of the quantities $A(\lambda) + A(\lambda)'$ or $A(\lambda) - A(\lambda)'$ is 0 and the CHSH inequality is bounded by 2. However if the system exists in the quantum state,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \ , \tag{1.9}$$

and we choose

$$\begin{aligned} A &= \frac{1}{\sqrt{2}}\left(\sigma_x + \sigma_z\right) \ , \\ A' &= \frac{1}{\sqrt{2}}\left(\sigma_z - \sigma_x\right) \ , \end{aligned}$$

and

$$\begin{aligned} B &= \sigma_x \ , \\ B' &= \sigma_z \ , \end{aligned}$$

then the expectation value of the CHSH inequality will be will be $2\sqrt{2}$.

1.6 Structure of the thesis

The main topic of this thesis is linear optics. As linear optical networks consist of collections of beamsplitters and phaseshifters they are straightforward devices to implement in the lab. As demonstrated in the discussion of the KLM procedure in order to perform some transformations with linear optics ancilla states are often introduced into the schemes as resources. In this thesis we take both a fundamental and a practical approach to studying linear optical networks.

In chapter 1 we consider the implementation of arbitrary unitaries on single mode Fock states. The approach taken is fundamental in nature and is meant to prove that any unitary may be performed on a single mode Fock state. The main result is to show that, similar to the KLM procedure, by allowing the size of the ancilla to grow we can perform the unitary with a probability of failure that is arbitrarily small.

In chapter 2 the approach is more practical. We investigate the realisation of arbitrary channels in a specific encoding that we call a d-rail encoding. The only ancilla state that we allow is a vacuum ancilliary state. A proof is provided that using these resources only random unitaries can be realised deterministically using linear optics. On the other hand an expression for the optimal probability of success for realising arbitrary channels with these resources is also discussed.

In the final chapter we investigate the realisation of a quantum non-demolition measurement onto the dual rail qubit space. The investigation is a blend of both fundamental and practical approaches. To begin we employ a modified KLM-like procedure and show that the measurement can be realised perfectly but stochastically. The probability that the proper measurement is made can be made arbitrarly close to one using a suitably large ancilla states. In addition we consider an existing scheme [9] which uses practical sources (two single photon sources) to perform the measurement. The scheme does not realise the measurement perfectly but instead has a free parameter in it which is the transmittiviy of a beamsplitter. The measurement will project onto a space that has a vacuum component. By adjusting the transmittivity of this beamsplitter the vacuum component can be made

arbitrarly small but only at the expense of the probability of success of the procedure. In this thesis a modification that can be made to the scheme to eliminate the vacuum component without changing the sources is introduced. The modification is surprisingly simple and only involves the addition of a single beamsplitter. In the proposal for the original amplifier it was used in simulations for DIQKD that included device imperfections. To show the improvement of our modification these DIQKD simulations are reproduced using the modified amplifier and its results are compared to the results of the original amplifier.

Chapter 2

Realisation of a unitary rotation on Fock space

2.1 Motivation

Linear optics is concerned with optical transformations on states of light that leave the total photon number of the states they act on fixed. Devices in linear optics achieve transformations by altering the phase between optical excitations in different modes and coherently transmitting and reflecting these excitations along different paths. All linear optical networks consist of collections of beamsplitters and phaseshifters, which are simple devices to implement in the lab. On the space that consists of a single excitation in d optical modes a convenient recipe for decomposing any unitary has been proposed [36].

Many gates that involve multi-photon inputs can only be realised stochastically with linear optics. One example is the non linear sign shift (NSS) gate

$$\text{NSS}: \; c_0|0\rangle + c_1|1\rangle + c_2|2\rangle \rightarrow c_0|0\rangle + c_1|1\rangle - c_2|2\rangle$$

In the linear-optics realisation of this gate an ancilla state is used that is passed through a linear optics network along with the input state. After the state has been passed through the network part of the state is measured with photon-detectors. Only conditioned on specific measurement results will the transformation be realised.

A great deal of work has been done to determine the optimal value for the success probability in the case of the of the NSS gate with specific ancilla states. For instance Knill [16] has shown that with an ancilla that has no more than a single photon in each

mode the optimal probability of success must be less than 1/2. However evidence was found that the upper bound is 1/4 [40] and a simple circuit was designed that is within 3% of this value [37, 35] and one has even been proposed that realises it [17]. Further investigations were then done to determine if the measurements that signal failure in these schemes could be processed to increase the probability of success. Neither of these schemes resulted in a boost of more than 3% above the value of 1/4 [15, 39].

However, in [17] a procedure was suggested – known as the KLM proposal – for the realisation of a subset of transformations on spaces with more than a single optical excitation in them. A dual rail qubit is a quantum bit that is encoded with two optical modes and a single photon. In the KLM proposal it was shown that efficient universal quantum computation could be achieved on the space of many dual rail qubits using linear optics.

As in the realisation of the NSS gate, the KLM gates only work probabilistically and require ancilla states as resources. The probability that the gates work can be made arbitrarily close to unity by increasing the size of the ancilla states. The circuits commonly considered, as mentioned in [15, 39, 37], only use ancilla states that can be generated deterministically from single photon sources. The KLM proposal uses states that can only be generated stochastically from single photon sources. The ancilla states required to implement the procedure are challenging to create in the lab. But the procedure still represents a major achievement in quantum information as it provides a way to implement a full quantum computer (although in a way that does not appear to be practically scalable).

The KLM procedure suggests in principle a constructive method for the manipulation of states with more than a single optical excitation in them. However the implications on spaces with higher numbers of photons not contained in the dual rail space have never been investigated. In this paper we consider arbitrary superpositions of Fock states, with a finite number of optical excitations in them. We show that using the KLM procedure an arbitrary unitary may be realised on this space; the scheme works probabilistically but the probability of success can be made arbitrarily close to one by using sufficiently large ancilla states.

2.2 Problem

We consider the implementation of unitaries on superpositions of single mode Fock states. The procedure we describe for the implementation of these unitaries will be stochastic and the probability of success will depend on three parameters which we will denote n, L and N. As the KLM procedure is non-deterministic we will parameterize the probability of its

success with the dimension of the KLM ancilla state, n, from Eq. 1.4. In our procedure we will map our single mode state into a collection of qubits. The parameter N will describe the number of qubits that we map the state into to perform a rotation using the KLM procedure. This mapping of the input state will be stochastic and the probability of success will increase with N. Finally we will assume that the input state is spanned by the basis elements $\{|i\rangle\}_{i=0}^{L}$ and that the unitary we are considering leaves this space invariant.

We will show that on the states spanned by single mode Fock space of at most L optical excitations any unitary can be implemented stochastically. For finite L in the limit that N and n become infinite the probability of success of our procedure will approach 1.

2.3 Sketch of the Approach

To begin the realisation of the unitary, U, on the single mode, a_1, of the input state we introduce a set of vacuum ancilla modes, $\{a_i\}_{i=2}^{N}$, and perform a Fourier transform on the total set of N modes. The input mode will be transformed into a uniform superposition of the other modes, $FT : a_1^\dagger \rightarrow \sum_{i=1}^{N} a_i^\dagger$, so that we view this operation as a way of splitting the input mode over the ancilla modes. We refer to the restriction of this map to the single mode input as a splitting map. For a Fock state $|i\rangle$ in the single mode of the input the probability of more than one photon ending up in any individual mode of the output will decrease monotonically as N increases; this probability will approach zero as $N \rightarrow \infty$. The portion of the state that has no more than a single photon in any of the N modes may be encoded with a set of N occupation qubits.

In Section 2.5, we will show that the KLM procedure can be used to perform universal computation on any collection of occupation qubits as well as the dual rail qubit space. We will use the universal computation in our procedure to perform a unitary on the occupation component of our Fourier transformed input state. For finite N the image of the input state under the Fourier transform will of course contain components orthogonal to the occupation space, i.e. states with multiple photons in at least one of the N modes. However, in Section 2.4 we will show that we can perform a projective measurement onto the occupation qubit space of a single mode using linear optics and ancilla states.

Our procedure for the realisation the unitary U will then involve splitting our input state with a set of vacuum modes using a Fourier transform. We will project the image of the Fourier transform onto the occupation qubit space. We will perform a unitary on the occupation space using the KLM procedure. After the rotation we will simply perform the inverse Fourier transform to map the occupation qubit back to the single mode Fock

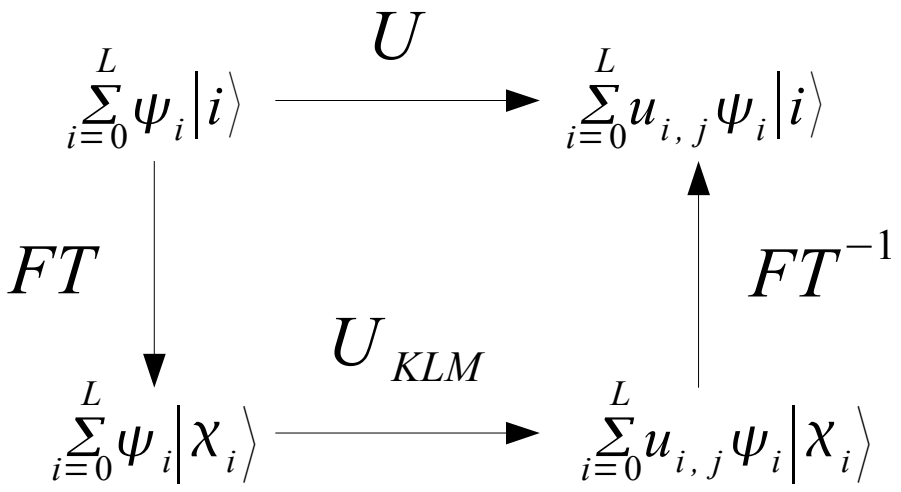

Figure 2.1: The diagram shows two paths for the realisation of the unitary U on a state $|\psi\rangle$. The realisation along one of the directions involves splitting the input over a number of vacuum ancilla with a Fourier transform (FT). The realisation is shown in the limit of an infinite number of modes, $N = \infty$. A rotation U_{KLM} is then performed on the N mode state followed by the inverse Fourier transform (FT^{-1}).

space. The full details of the procedure are discussed in Section 3.4 however a sketch of the procedure in the case $N = \infty$ is shown in Figure 2.1.

2.4 Quantum Scissors

In Figure 2.2 the circuit that realises the KLM procedure in the case $n = 1$ is shown. The KLM state $|t_1\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$ can be generated by passing a single photon, $|1\rangle$, and a vacuum state, $|0\rangle$, through a $50:50$ beamsplitter.

To perform the KLM procedure a Fourier transform needs to be performed on the

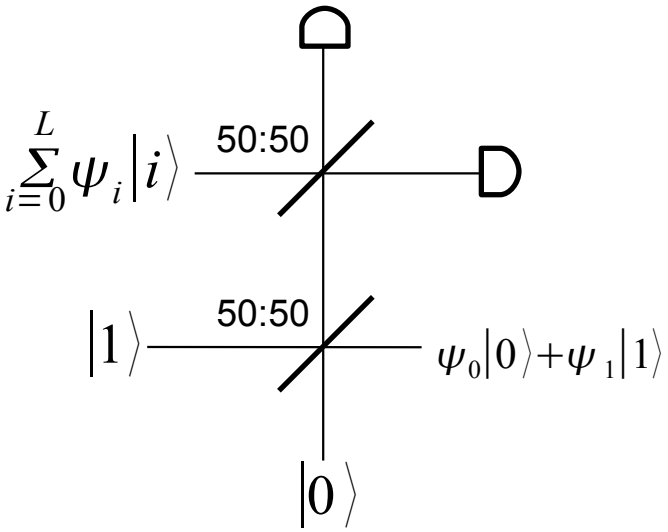

Figure 2.2: In the case n=1 the circuit that realises the KLM procedure (and the circuit is also known as the Quantum Scissors circuit) is shown. The ancilla state used in the procedure is generated by passing the state $|10\rangle$ through the $50:50$ beamsplitter. The ancilla state then interacts with an input mode $|\psi\rangle$ through a different $50:50$ beamsplitter. The KLM transformation is realised when a single photon is detected and the phase error between the vacuum and single photon output is corrected.

mode of the input state and the first mode of the state $|t_1\rangle$. This transformation can be realised by passing these two modes through a second 50:50 beamsplitter. With $n = 1$ in the KLM procedure the modes that are passed through the second beamsplitter (the Fourier transformed modes) are measured with photon counting detectors. The success of the KLM procedure will be conditioned on measuring a single photon in these modes.

Conditioning on the measurement of a single photon, including the correction for the phase in the output of Eq. (1.5), we can view this KLM procedure as a Kraus operator on the higher photon states

$$A_{KLM} : c_0|0\rangle + c_1|1\rangle + \sum_{i=2}^{\infty} c_i|i\rangle \mapsto c_0|0\rangle + c_1|1\rangle \ .$$

The fact that the circuit in Figure 2.2 cuts the higher photon states from the conditional output follows from the fact that there is no optical path connecting the input modes – which contain the higher photon terms – to the output. The input modes only interact with an ancilla state with a beamsplitter and both of the output modes of this beamsplitter are directly connected to photon detectors. Since the success of the procedure is conditioned on the detection of only a single photon, higher photon terms can only contribute to the probability of failure of the scheme. The circuit is known as a pair of quantum scissors [28] because it coherently cuts out the states with more than a single excitation in them while leaving the rest of the state unchanged. The process is of course nondeterministic and works with a probability of

$$\frac{1}{2}\left(|c_0|^2 + |c_1|^2\right)$$

which is half the norm of the conditional output state. The one-half factor in the probability of success arises from the fact that this is the probability of success of the KLM procedure in the case $n = 1$.

For arbitrary n the KLM procedure will act as a set of quantum scissors if an additional measurement is included in the procedure. Applying the KLM procedure using the ancilla state $|t_n\rangle$ and an input state $\sum_{i=0}^{\infty} c_i|i\rangle$ for a k photon measurement we will obtain the state (ignoring normalisation)

$$(c_0|s_k\rangle + c_1|s_{k-1}\rangle) + \sum_{i=2}^{k} c_i' \mid s_{k-i}\rangle \ . \tag{2.1}$$

The coefficients c_i' will in general be different from the initial c_i. We deduce the form of the transformation simply by projecting the first $n + 1$ modes of the initial state of

the KLM procedure, $(\sum_{i=0}^{\infty} c_i|i\rangle) \otimes |t_n\rangle$, onto the k photon space. In addition we use the known behaviour of the KLM procedure on the input space spanned by the basis states $\{|0\rangle, |1\rangle\}$ (see Eq. 1.5). To show that with the inclusion of an additional measurement the KLM procedure will act as a pair of quantum scissors we observe that the index k in state $|s_k\rangle$ denotes the number of trailing $|0\rangle$'s before the $n-k$ leading $|1\rangle$'s in the state. Therefore if we measure the $k-1$ mode of a superposition of states of the form $\sum_{i=0}^{n} c_i|s_i\rangle$ we can project onto either $\sum_{i=0}^{k-2} c_i|s_i\rangle$ or $\sum_{i=k-1}^{n} c_i|s_i\rangle$ depending on whether a $|1\rangle$ or a $|0\rangle$ is measured respectively. By measuring the $k-1$ mode of the output state, in Eq.(2.1), and conditioning on measuring $|0\rangle$ we can realise the same Kraus operator A_{KLM} as the original set of quantum scissors. The probability of success will be

$$\frac{n}{n+1}\left(|c_0|^2 + |c_1|^2\right) \ .$$

The procedure we have suggested consists of two measurements; a KLM measurement and a quantum scissors measurement. The probability that the KLM measurement is successful when we condition on an occupation qubit input is $\frac{n}{n+1}$ and the probability the quantum scissors measurement is successful on the state in Eq. (2.1) is $(|c_0|^2 + |c_1|^2)$. The probability of success of the entire procedure is simply the product of these two probabilities of success.

2.5 Generalisation

With linear optics alone any single qubit operation can be performed on a dual rail qubit. Alternatively the occupation encoding uses states with different photon numbers so that linear optics cannot be used to realise any single qubit unitary on this space. However with the KLM procedure it is straightforward to move back and forth between the dual rail and the occupation encodings.

To begin we consider the mapping from an occupation qubit to a dual rail qubit. We will perform this transformation using a KLM-like procedure. We denote the state used in the second n modes of the KLM procedure, from Eq.(1.4), as $|s_k\rangle = |a\rangle^k|b\rangle^{n-k}$ with the states $|a\rangle$ and $|b\rangle$ arbitrary. For a measurement of $1 \leq k \leq n$ photons, we will realise the transformation

$$c_0|0\rangle + c_1|1\rangle \rightarrow c_0|a\rangle^{\otimes k}|b\rangle^{\otimes(n-k)} + e^{i\phi_k}c_1|a\rangle^{\otimes(k-1)}|b\rangle^{\otimes(n-k+1)} \ .$$

The state $c_0|a\rangle + e^{i\phi_k}c_1|b\rangle$ shown will be the state in the k^{th} mode of the n unmeasured modes. Therefore by using the KLM procedure with $|a\rangle = |\underline{0}\rangle$ and $|b\rangle = |\underline{1}\rangle$ dual rail

qubits the occupation qubit in the input will be present as a dual rail encoded qubit in the output.

We now consider the mapping in the reverse direction,

$$c_0|\underline{0}\rangle + c_1|\underline{1}\rangle \rightarrow c_0|0\rangle + c_1|1\rangle \ , \tag{2.2}$$

with the encoding for the dual rail qubit $|\underline{0}\rangle = |10\rangle$ and $|\underline{1}\rangle = |01\rangle$ as discussed in Section 2.2.

To perform the change of encoding in this direction we could just measure the first optical mode of the dual rail qubit in a basis that would not reveal whether there was a photon present in this mode or not. The Hadamard basis $\{|+\rangle, |-\rangle\}$ may be defined with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. By measuring the first mode of a dual rail qubit in the Hadamard basis and performing a phase flip using the unmeasured mode of the dual rail qubit if the state $|-\rangle$ is measured we can realise the desired transformation from Eq.(2.2).

To perform a measurement that achieves the same result we can again use a KLM-like procedure. We again denote the state that is used in second set of n modes of the KLM procedure as $|s_k\rangle = |a\rangle^k|b\rangle^{n-k}$. We apply the KLM procedure, using this state, to only the first mode of the dual rail encoded qubit. For a measurement of $1 \leq k \leq n$ photons, we realise the transformation

$$c_0|\underline{0}\rangle + c_1|\underline{1}\rangle \rightarrow c_0|0\rangle|a\rangle^{\otimes k}|b\rangle^{\otimes(n-k)} + e^{i\phi_k}c_1|1\rangle|a\rangle^{\otimes(k-1)}|b\rangle^{\otimes(n-k+1)} \ ,$$

in this output state we have only shown the unmeasured mode of the dual rail qubit from the input and the n unmeasured modes of the KLM state. To perform the change in the encoding we let $|a\rangle = |b\rangle$ and correct the phase $e^{i\phi_k}$ using the unmeasured mode of the dual rail qubit. In the case of $|a\rangle = |b\rangle$ the second set of n modes in our KLM-like state can simply be discared since they will add nothing to the procedure. Therefore to perform the change in the encoding we can use just the state

$$\sum_{i=0}^{n} |1\rangle^{\otimes i}|0\rangle^{\otimes(n-i)} \ . \tag{2.3}$$

2.6 Solution

We now show a complete procedure for the realisation of a unitary U which acts on a superposition of single mode Fock states

$$|\psi\rangle = \sum_{i=0}^{L} \psi_i |i\rangle$$

An outline of the procedure is shown in Fig. 2.3. The only resources we allow are linear optical elements and the use of arbitrary ancilla states. In several steps of our procedure we use the KLM procedure which works probabilistically. However the KLM scheme is not the only component of our scheme that is non-deterministic. In the current section we assume the KLM procedure is deterministic and keep track of the probability of success through the norm of the state.

2.6.1 Step 1

As discussed in Section 2.3 the procedure begins with a N mode Fourier transform on the input state, $|\psi\rangle$, and vacuum ancilla modes introduced as a resource. We represent the output of the Fourier transform by the superposition

$$\sum_{i=0}^{L} \psi_i \left(\sqrt{\alpha_{N,i}} |\chi_{N,i}\rangle + \sqrt{1-\alpha_{N,i}} |\phi_{N,i}\rangle \right) \tag{2.4}$$

where the state $|\chi_{N,i}\rangle$ is the normalised projection of the state $FT|i\rangle$ onto the N qubit space in the occupation encoding. The state $|\phi_{N,i}\rangle$ is then a normalised vector orthogonal to $|\chi_{N,i}\rangle$ but still lies in the plane spanned by the $|\chi_{N,i}\rangle$ vector and $FT|i\rangle$.

2.6.2 Step 2

The next step in the procedure is to map the state in Eq.(2.4) into a set of dual rail qubits where we can use the KLM procedure to perform arbitary rotations. However in our procedure we only map the component of this state that lies in the space spanned by basis vectors in the set $\{|\chi_{N,i}\rangle\}_{i=0}^{L}$ into the dual rail encoding. We include a projective measurement in our procedure so that the component of the state that lies in the space spanned by the vectors from the set $\{|\phi_{N,j}\rangle\}_{i=0}^{L}$ will be projected out of the conditional output state.

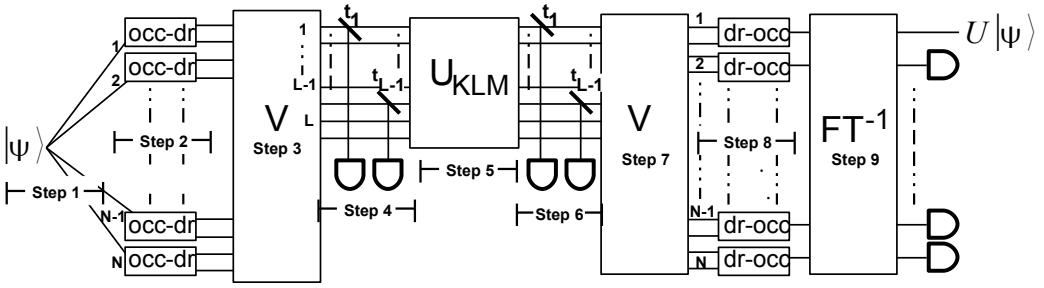

Figure 2.3: An outline showing the steps in our procedure for the realisation of a unitary U on a single mode Fock state $|\psi\rangle$. The divergence of the lines in the first step indicates that the single mode Fock state has been spread over a set of N vacuum ancilla with a Fourier transform (FT). The $occ-dr$ boxes are used to indicate that an occupation qubit encoded input will be output in the dual rail encoding. Alternatively the boxes labelled with the $dr-occ$ perform the encoding in the other direction. The operation V rotates the N qubit encoding into a L qubit encoding. The beamsplitters in steps 4 and 6 have the transmittivities $t_i = \frac{\alpha_{N,i+1}}{\alpha_{N,i}}$. The success of the procedure is conditioned on every photon detector in the diagram measuring the vacuum.

As outlined in section 2.5 we can map an occupation qubit to a dual rail qubit using the KLM procedure with the state

$$\sum_{i=0}^{n} |1\rangle^{\otimes i}|0\rangle^{\otimes(n-i)}|\underline{0}\rangle^{\otimes i}|\underline{1}\rangle^{\otimes(n-i)} \ . \tag{2.5}$$

When performing the KLM procedure a measurement can be made on one of the unmeasured modes in the KLM state, as described in section 2.4, so that the KLM procedure acts as a pair of quantum scissors. When this measurement is applied any components in the input state that have more than a single photon in them will be projected out of the resulting state. By applying the KLM procedure N times – one time for each of the modes of the state in Eq.(2.4) – using the state in Eq.(2.5) and applying the quantum scissors measurement each time we will realise the state

$$\sum_{i=0}^{L} \psi_i \sqrt{\alpha_{N,i}} |\underline{\chi}_{N,i}\rangle \ . \tag{2.6}$$

The states $|\phi_{N,i}\rangle$ consists of a superposition of states that each have at least one mode that has more than a single optical excitation. For this reason these states will be cut out of

this conditional state by the quantum scissors measurements. As the $|\chi_{N,i}\rangle$ is a state in the occupation space, the state $|\underline{\chi}_{N,i}\rangle$ is the image when each of the occupation qubits in the original state has been encoded in a dual rail qubit.

2.6.3 Step 3

In the dual rail space universal computation is possible by the KLM procedure. However the rotation that we apply to the state will depend on the number of ancilla modes that are used in Step 1 and on the specific unitary we wish to apply to the input state. To separate these dependencies we rotate the state from Eq.2.6 to an image that is independent of the parameter N.

The state $|\underline{\chi}_{N,n}\rangle$ is an equally weighted superposition of the orthonormal states in the set

$$\underline{\chi}_{N,i} = \{|\underline{m}_1\rangle ... |\underline{m}_N\rangle \,|\, m_1 + ... + m_N = i \,\text{and}\, m_i \leq 1 \forall i\}$$

We choose to rotate the state so that

$$V : |\underline{\chi}_{N,i}\rangle \mapsto |\underline{1}\rangle^{\otimes i} |\underline{0}\rangle^{\otimes (N-i)} \; . \tag{2.7}$$

By performing this operation the size of the systems encoding will be reduced as all but L of the qubits will be fixed in the logical $|\underline{0}\rangle$ state.

2.6.4 Step 4

With N finite the mapping applied to an input state $|\psi\rangle$ as outlined in the first three steps is not orthogonality preserving because of the i dependence in the coefficients $\alpha_{N,i} = \frac{i!}{N^i}\binom{N}{i}$. However we can re-establish the orthogonality at the expense of the success probability.

We consider the single qubit operation

$$L_i : c_0|\underline{0}\rangle + c_1|\underline{1}\rangle \rightarrow c_0 \sqrt{\frac{\alpha_{N,i+1}}{\alpha_{N,i}}}|\underline{0}\rangle + c_1|\underline{1}\rangle \; .$$

With the sequence of transformations, defined by applying L_i to i^{th} dual rail qubit of the current state, where $1 \leq i \leq L-1$, the orthogonality of the mapping can be re-established. The state after this transformation will be

$$\sqrt{\alpha_{N,L}} \sum_{i=0}^{L} \psi_i |\underline{1}\rangle^{\otimes i} |\underline{0}\rangle^{\otimes (L-i)} \; .$$

Applying this procedure will decrease the probability of success because the norm of the state after the procedure is applied will be $\alpha_{N,L}$.

The mapping L_i can be implemented with a beamsplitter of transmittivity $t_i = \frac{\alpha_{N,i+1}}{\alpha_{N,i}}$ and a vacuum ancilla state. The beamsplitter acts on the mode of the i^{th} dual rail qubit that a photon would be present in when the qubit is in the logical state $|\underline{0}\rangle$. The beamsplitter should act on the vacuum ancilla mode. The operator L_i will be realised if these two modes are split together and the mode initially in the vacuum state is measured and found to still be in the vacuum state.

2.6.5 Step 5

The total transformation that we have achieved up to this point may be represented with the Kraus operator E

$$E : |i\rangle \rightarrow \sqrt{\alpha_{N,L}}|\underline{1}\rangle^{\otimes i}|\underline{0}\rangle^{\otimes(L-i)} \ .$$

We refer to the total procedure that we have realised as the encoding as it maps the $L+1$ dimensional input space into a set of L dual rail qubits.

In later steps we will construct a decoding procedure that will map the state in the L qubit encoding back to the single mode $L+1$ dimensional space of the input. This decoding procedure will be conditioned on specific measurement results and correspond to the Kraus operator,

$$D : |\underline{1}\rangle^{\otimes i}|\underline{0}\rangle^{\otimes(L-i)} \rightarrow \sqrt{\alpha_{N,L}}|i\rangle \ . \tag{2.8}$$

In the sketch of the solution, Section 2.3, we used only an N mode Fourier transform and its inverse to perform the encoding and decoding procedures respectively. After performing the FT and before performing the inverse procedure we applied the mapping U_{KLM}. The unitary was defined so that the composite mapping of the $FT^{-1}U_{KLM}FT$ would realise the the unitary U on the single mode Fock states.

The encoding procedure that we have now suggested, and the decoding procedure that we will show in later steps, is more elaborate than the simple Fourier transform and its inverse. We introduce the complications in the procedure because with N finite our projection into the occupation space, using the quantum scissors measurements, will not preserve orthonormality and in order to apply the KLM procedure our state must be encoded with a set of dual rail qubits. However at this step in the procedure we still choose to perform a rotation, U_{KLM}, so that the composite map of this unitary and the encoding

and decoding procedures, $D\,U_{KLM}\,E$, will realise the unitary U on the single mode Fock states. Therefore we redefine the rotation, U_{KLM} so that

$$\langle i|E^{\dagger}U_{KLM}E|j\rangle = \alpha_{N,L}\langle i|U|j\rangle \ , \tag{2.9}$$

where $|i\rangle$ is just a single mode Fock state and $0 \leq i, j \leq L$. The factor $\alpha_{N,L}$ is present to keep track of the probability that the Kraus operation E will be realised.

2.6.6 Step 6

Now that we have rotated the state we apply the decoding procedure, D, (from Eq. (2.8)). Ideally this procedure would simply be the inverse of the encoding. However many of the steps in the encoding procedure are not reversible.

In the encoding procedure however the loss L_i was applied to each of the L dual rail qubits. The loss was applied because the composition of all the quantum scissor measurements, the unitary V and the loss form an orthogonality preserving map. In our decoding procedure will again involve a different series of measurements. In this first step of the decoding procedure we re-apply the same loss applied in the encoding procedure to ensure the steps that come later will preserve the orthogonality. After the loss has been applied to each of the L dual rail qubits we will realise the state

$$\alpha_{N,L}\sum_{i=0}^{L}\frac{\psi_i}{\sqrt{\alpha_{N,i}}}\alpha_{N,i}U_{KLM}|\underline{1}\rangle^{i}|\underline{0}\rangle^{L-i} \tag{2.10}$$

2.6.7 Step 7

To continue the decoding process we apply the inverse of the mapping V (introduced in step 3) , to realise the state

$$\alpha_{N,L}\sum_{i=0}^{L}\frac{\psi_i}{\sqrt{\alpha_{N,i}}}U_{KLM}|\underline{\chi}_{N,i}\rangle \ . \tag{2.11}$$

2.6.8 Step 8

Next we map each dual rail qubit in the state Eq.(2.11) to an occupation qubit. In Section 2.5 a method for mapping a dual rail qubit into an occupation qubit was outlined. This

method involved the use of a state that resembled the KLM state $|t_n\rangle$,

$$\sum_{i=0}^{n} |1\rangle^i |0\rangle^{n-i} \ .$$

By applying the procedure from Section 2.5 to each of the N dual rail qubits in state (2.11) we can map our state to the occupation encoded state

$$\alpha_{N,L} \sum_{i=0}^{L} \frac{\psi_i}{\sqrt{\alpha_{N,i}}} \alpha_{N,i} U_{KLM} |\chi_{N,i}\rangle \tag{2.12}$$

2.6.9 Step 9

In the final step of the procedure we attempt to map our state back to the single mode of the input. In the first step of the procedure we used a Fourier transform and a sequence of quantum scissors measurements to map the single mode state into a set of occupation qubits. We attempt to use the inverse Fourier transform and a different measurement to map the states in this occupation encoding back into the single mode. The Fourier transform on the input modes of the first step of the procedure can be written as

$$FT : \sum_{i=0}^{L} \left(\sqrt{\alpha_{N,i}} |\chi_{N,i}\rangle + \sqrt{1-\alpha_{N,i}} |\phi_{N,i}\rangle \right)_N \langle 0| \langle i| + T$$

if $|0\rangle_N = |0\rangle^{\otimes(N-1)}$ and T is an operator whose kernel is the single mode Fock space – ie $T|i\rangle|0\rangle_N = 0 \ \forall i$. In the decoding procedure our state will belong to the space spanned by the $|\chi_{N,i}\rangle$. When the inverse Fourier Transform acts on any state in this occupation space we will have $FT^{-1}|\chi_{N,i}\rangle = \alpha_{N,i}|i\rangle|0\rangle_N + T^\dagger|\chi_{N,i}\rangle$. As $T|i\rangle|0\rangle_N = 0$, by measuring the modes that were introduced as vacuum modes –to complement the single mode input– and conditioning on measuring the vacuum in these modes we can measure out the component that is due to T. Applying the inverse Fourier transform to the state in Eq. 2.12 and applying this measurement will realise the state

$$\alpha_{N,L} \sum_{i=0}^{L} \psi_i U |i\rangle \ . \tag{2.13}$$

2.7 Probability of Success

The process that we suggest for the realisation of the unitary is of course non-deterministic. The probability of success is a function of the three parameters n, L and N defined in Section 2.2. The L parameter is the maximum number of photons that will be in the single mode input and output states. The parameter N is the number of modes the input state is split into with the Fourier transform in the first step of the procedure. The final parameter n describes the size of the KLM states in Eq's.(1.4) and (1.6) or KLM-like states from Section 2.5.

With each KLM procedure used in our procedure as outlined in Section 2.3 the probability of success is the norm of the conditional output state which was $\left(\frac{L!}{N^L}\binom{N}{L}\right)^2$. The total probability of success is the product of the probability each KLM procedure is successful times the factor $\left(\frac{L!}{N^L}\binom{N}{L}\right)^2$. To determine the total probability the KLM procedures proceeds successfully we just need to count the number of times the procedure is used. The KLM procedures are used in the procedure to change between the dual rail and occupation encodings and to perform the rotations U_{KLM}, V and V^{-1}. The probability that the KLM procedures proceed successfully will be the product of the probabilities that the encodings are changed successfully and the rotations are realised successfully.

The CSIGN gate and the single qubit rotations together form a universal set of gates so that the rotations U_{KLM}, V and V^{-1} can be decomposed into products of gates from this universal set. We use the KLM procedure to perform the CSIGN gates in our implementation and the probability each CSIGN gate is realised successfully on a pair of dual rail qubits is $\left(\frac{n}{n+1}\right)^2$ with the parameterization shown in Eq.(1.6). The probability of success of realising the unitaries U, V and V^{-1} will be $\left(\frac{n}{n+1}\right)^{G_1(N,L)}$ where $G_1(N,L)$ is the total number of CSIGN operations needed to realise these three rotations. However we do not have explicit decompositions of the gates that we use in terms of gates from our universal set. The parameter n and N in our procedure will define the amount of physical resources we need to realise our procedure. We are not interested in an explicit function for the probability of success in terms of these parameters, but only to show that by increasing our resources, with L fixed, we can make the probability of success of our procedure as close to unity as we like. To show that the probability of success has this property we can use basic scaling arguements. For instance any unitary that acts on a d dimensional system can be decomposed into $O(d^2)$ two level unitaries. In an x-bit encoding any unitary that acts on two distinct strings can be decomposed, in the x-bit encoding, into $O(x^2)$ CSIGN and single qubit rotations [26].

To determine how the function $G_1(N,L)$ will scale with N we begin by considering the

unitary V. The unitary V acts on states encoded with N dual rail qubits. In addition this unitary acts as the identity on all the states encoded with N dual rail qubits that are not in the set $\cup_{i=0}^{L} \underline{\chi}_{N,i}$. The size of this set, hence the dimension of the space that V acts non-trivially on, grows as $o(N^L)$ since each of the L sets $\chi_{N,i}$ has $\binom{N}{i}$ elements in it. Since the dimension of the space grows as $o(N^L)$ our scaling arguements imply that the unitary can be expressed as at most $O(N^{2L})$ two level unitaries. Each of the two level unitaries can be expressed as $O(N^2)$ CSIGN gates and single qubit rotations. The function $G_1(N, L)$ scales as $O(N^{2L}N^2)$. We do not consider the unitary U_{KLM} and its contribution to the function $G_1(N, L)$ as the number of CSIGN gates needed to realise this unitary does not change with N.

To determine the probability that the KLM procedures used to change the between the occupation and dual rail encodings proceed successfully using the parameterisation is $\left(\frac{n}{n+1}\right)^{G_2(N,L)}$ where $G(N, L)$ is the number of qubits whose encoding is changed. As a change in the encoding is only performed two times the function $G_2(N, L) = 2N$.

Therefore the total probability of success of the procedure is

$$p_{succ} = \left(\frac{L!}{N^L}\binom{N}{L}\right)^2 \left(\frac{n}{n+1}\right)^{G_1(N,L)+G_2(N,L)} \tag{2.14}$$

We now show that in the limit of infinite resources this probability of success can be made to approach unity. In the limit $N \to \infty$ the norm of the conditional output state will approach unity, $\left(\frac{L!}{N^L}\binom{N}{L}\right) \to 1$. However, as $G(N, L) = G_1(N, L) + G_2(N, L)$ is $O(N^{2L}N^2)$, for fixed n as $N \to \infty$ we will have $G(N, L) \to \infty$ and the factor $\left(\frac{n}{n+1}\right)^{G(N,L)}$ will approach 0. However by making n scale more quickly with N then $G(N, L)$ we can we can make the probability of success approach unity in the limit that N approaches infinity. To see this just let $y = \frac{n(N,L)+1}{G(N,L)}$ then

$$\begin{aligned} \lim_{N\to\infty} \left(1 - \frac{1}{n(N, L) + 1}\right)^{G(N,L)} &= \lim_{G(N,L)\to\infty} \left(1 - \frac{y}{G(N, L)}\right)^{G(N,L)} \\ &= e^{-y} \end{aligned}$$

if y does not change with N. Therefore if $y \to 0$ as $N \to \infty$ then $p_{succ} \to 1$ in this limit.

Chapter 3

Channel Realisation

3.1 Notes and Acknowledgements

Notice: The content from this chapter has been published in:

M. Piani, D. Pitkanen, R. Kaltenbaek, and N. Lütkenhaus, Phys. Rev. A. **84**, 032304 (2011).

3.2 Motivation

In this chapter we consider transformations on quantum states $\Lambda : \rho \rightarrow \rho'$. If a map Λ satisfies the properties that,

- it acts linearly on input states
- maps density matrices to density matrices
- satisfies the property of complete positivity

it can be written as an object that is referred to as a quantum channel [26]. As discussed in Section 1.2 a quantum channel is the most general physical transformation that can be applied to a quantum system. Many quantum information protocols are not strictly unitary interactions but can be modelled as quantum channels [26]. In addition if a system

interacts with an environment and experiences decoherence this process can be represented as a quantum channel.

Universal computation can be performed on a collection of dual rail qubits using linear optics [17]. Since a dilation representation can be used to represent any quantum channel as a unitary rotation in an extended Hilbert space we expect that in the dual rail encoding any channel using linear optics can be realised [31]. However the only known method, using linear optics, that achieves arbitrary rotations on the dual rail qubit space requires complicated ancilla states to be introduced as resources [17].

If we encode a qudit in a photon that can be in any of d optical modes, then any unitary rotation in this encoding space can be realised deterministically without any ancilla resource states [36] In this section we consider the realisation of quantum channels. We take a practical approach and use simple resouces. With these resources we provide an optimal solution to the channel realisation problem. To make the approach practical we choose the space for the realisation of the channel as the d level space of a single excitation in d modes. The only ancilla state we allow as a resource is the vacuum ancilla states, and we only use linear optics.

3.3 Problem Outline

The dual rail space is a two dimensional Hilbert space spanned by the vectors,

$$|i_L\rangle = a_i^\dagger|0\rangle \tag{3.1}$$

where $i \in \{0, 1\}$ and the operators $\left\{a_i^\dagger\right\}$ are creation operators for two optical modes. The d-rail space is an encoding for d logical states which results when i in Eq. 3.1 is extended to range over the set $i \in \{1, .., d\}$.

We are interested in demonstrating a method that can be used to realise an arbitrary channel that acts on a d-level system. In chapter 1, section 1.2 the dilation representation of a channel was discussed. The dilation representation of a channel expresses the channel in terms of an ancilla system – one that starts in a pure state, i.e. $|0\rangle$ – and a unitary interaction between the ancilla and the input. The channel is realised when the unitary is performed on the bipartite system and the ancilla is subsequently discarded.

The dilation representation of the channel will be the model that we follow for the realisation of the channel. The constraints that we impose in our realisation are the following:

- we restrict our analysis to linear optics (the unitary that we apply to the input and ancilla state will consist of the action of beamsplitters and phaseshifters);
- only vacuum ancilla states are allowed;
- feed-forward is not allowed;
- the channel must act on and preserve d-rail encoded states.

The constraints listed here are imposed to make the scheme practical for experimental realisation. Restricting the ancilla to vacuum states makes the use of complicated sources unnecessary. By not allowing feed forward the need for devices like Pockel cells and high speed voltage switches is removed [32, 4]. In addition requiring that the channel preserves this encoding makes further processing of the channels output straightforward.

3.3.1 Previous work

The realisation of channels with a set of constraints similar to those imposed here is explored by He et al in [12]. Within this paper a method called space extension is used. To simulate a channel that has a Kraus decomposition $\{A_i\}_{i=1}^n$, an additional $d(n-1)$ vacuum modes are introduced and the transformation,

$$U : |i_L\rangle|0\rangle^{\otimes(n-1)d} \rightarrow \sum_{j=1}^{n} |0\rangle^{\otimes(j-1)d} A_j |i_L\rangle |0\rangle^{\otimes(n-j)d} ,$$

is performed on the dn modes. The operation U clearly preserves the norm and orthogonality of the d-rail input states. If $|\phi\rangle$ and $|\psi\rangle$ are arbitrary states in the d-rail encoding then

$$\begin{aligned} \langle 0|^{\otimes(n-1)d}\langle\phi \mid U^\dagger U \mid \psi\rangle|0\rangle^{\otimes(n-1)d} &= \sum_{i=1}^{n}\langle\phi \mid A_i^\dagger A_i \mid \psi\rangle & (3.2)\\ &= \langle\phi \mid \sum_{i=1}^{n} A_i^\dagger A_i \mid \psi\rangle & (3.3)\\ &= \langle\phi \mid \psi\rangle & (3.4) \end{aligned}$$

Since the operation preserves the orthogonality on the d dimensional space of the encoding the operation U can be extended to a unitary operator on the entire set of dn modes

involved in the transformation[20]. Therefore the operation U can be implemented with a set of beamsplitters and phase shifters.

If a state $|\psi\rangle$ is input into a channel with the Kraus decomposition $\{A_i\}_{i=1}^n$ it should be transformed into a classical mixture of the states $A_i|\psi\rangle\langle\psi|A_i^\dagger$. However the transformation from 3.4 will output a state that is a coherent superposition of the terms $A_i|\psi\rangle$. In addition each of the states in the coherent superposition will be in a different set of d modes. In order to realise the channel the coherence between the different terms in the superposition needs to be removed and each of the states needs to be combined into a common set of modes.

In [12] the coherence between each of the terms in 3.4 is removed by applying a random phase to each set of d modes that contains a state $A_i|\psi\rangle$. This map is called a dephasing map. However, no method for combining the states $A_i|\psi\rangle$ into a single set of modes is suggested which works deterministically. Instead a probabilistic scheme is introduced which combines the terms, $A_i|\psi\rangle$, into a fixed set of common modes with probability $1/n$.

3.3.2 Difficulty in realising arbitrary channels with our resources

We now provide a proof that these steps cannot be achieved deterministically with our specified resources. We can reduce any attempt to realise the channel under our constraints to a unitary U_{LO} —that will be applied to the d-rail encoded state— and a set of e vacuum ancilla modes we introduce. If the method is to work deterministically the channel will be realised when the e ancilla modes we introduced are discarded. The action of the unitary on the ancilla state and input can be represented as

$$\begin{aligned} U_{LO}|i_L\rangle_S|0\rangle_E &= U_{LO}a_i^\dagger|0\rangle_S|0\rangle_E \\ &= \sum_{j=1}^{d+e} u_{i,j}a_j^\dagger|0\rangle_S|0\rangle_E \\ &= \left(\sum_{j=1}^{d} u_{i,j}a_j^\dagger|0\rangle_S\right)|0\rangle_E + |0\rangle_S\left(\sum_{j=d+1}^{d+e} u_{i,j}a_j^\dagger|0\rangle_E\right), \end{aligned} \tag{3.5}$$

if $|0\rangle_S = |0\rangle^{\otimes d}$ and $|0\rangle_E = |0\rangle^{\otimes e}$. Since the e ancilla modes will be discarded in the procedure we can imagine that a photon counting measurement is made on these modes but the result of the measurement is not revealed. From the expression in 3.5 it is clear that if the photon is measured in the ancilla then the d remaining modes will be left in the vacuum state, and the input will have been mapped out of its encoding. Therefore

only the single possible measurement of the vacuum state in the ancilla will preserve the encoding. A channel with only a single Kraus operator can be realised deterministically. From the trace preserving condition, $A^\dagger A = I$, we can deduce that channels with only a single Kraus operator are necessarily unitary operators.

3.4 The solution: stochastic implementation

We are interested in the simulation of an arbitrary quantum channel Λ that acts on a qudit, using only passive linear optics. What we want is a realization of Λ on the d-rail qudit, such that the encoding space is mapped onto itself. However we have just shown that we cannot realise a channel that preserves the qudit encoding unless it is a unitary rotation of the qudit encoding. We will refer to the channel to be realized as the logical channel, to distinguish it from physical channels that evolve the state of the modes without necessarily preserving the logical subspace.

In this section we will first see that any logical Kraus operator (i.e., any Kraus operator of the logical channel) can be realised stochastically. Later we will introduce a further resource, randomness, and the ability to switch –according to such randomness– among different optical networks, and we will show that then any logical channel can be realised, albeit only stochastically.

3.4.1 Realisation of a single Kraus operator

Every linear operator A has a singular value decomposition [14]

$$A = USV \ ,$$

where S is a positive diagonal matrix and U and V are unitaries. With the singular value decomposition the infinity norm can be defined on any operator A as

$$||A||_\infty = \max_i s_i \tag{3.6}$$

where the values s_i are the diagonal entries of S from Eq.(3.6). Any linear operator A with $||A||_\infty \leq 1$ has the form of a valid Kraus operator.

In this section we will provide a method for realising any Kraus operator on a d-rail encoded state with a linear optics channel. The singular value decomposition expresses an operator as the product of two unitaries and a diagonal matrix S. On the d-rail space the

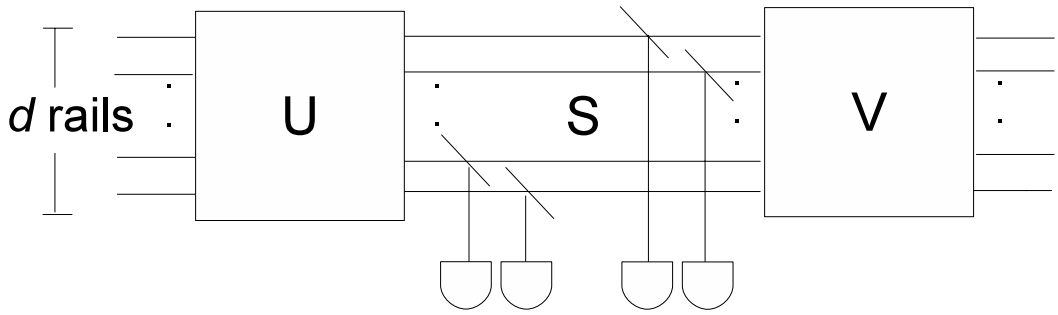

Figure 3.1: The diagram describes an optical circuit for a channel that realises the Kraus operator $A = VSU$ stochastically. The boxes represent optical arrays that perform the unitary that labels them. The S transformation then consists of a set of beamsplitters, one for each mode, whose transmission coefficients are matched to the singular values of the matrix S.

two unitaries can be realised deterministically with linear optics. The challenge in creating a linear optics network that realises the Kraus operator A is implementing the operator S in its singular value decomposition.

In Section 2.6.4 we showed that with a beamsplitter of transmittivity t and a vacuum ancilla state we could realise the single mode transformation

$$L_t \left(c_0|0\rangle + c_1|1\rangle\right) \rightarrow c_0|0\rangle + c_1\sqrt{t}|1\rangle \ . \tag{3.7}$$

To perform this operation we conditioned on measuring the ancilla mode in the vacuum state after it had been through the beamsplitter along with the input. We define L_{t_i} as an operator of the form shown in Eq.(3.7) that acts on the i^{th} mode of a d-rail encoded state. In addition we choose the parameter t_i in L_{t_i} to be the square of the i^{th} diagonal entry of the matrix S. The effect of the operators $L_{t_1} \circ ... \circ L_{t_d}$ acting on a d rail state is

$$L_{t_1} \circ ... \circ L_{t_d} : |i_L\rangle \rightarrow s_i|i_L\rangle$$

so that $L_{t_1} \circ ... \circ L_{t_d} = S$. The construction for an arbitrary linear operator is show in Figure 3.1. Therefore for any Kraus operator A we can choose a linear optics network that realises it stochastically.

3.4.2 Perfect but stochastic implementation of an arbitrary logical channel

A logical channel Λ that we may want to apply on the encoding will in general have a Kraus decomposition $\{A_i\}_{i=1}^n$, with $n \geq 1$. Therefore, by using a fixed linear optical network in the framework defined in Section 3.3 it will not be possible in general to simulate the channel, as only one logical Kraus operator can be realized per fixed optical network.

We will circumvent this problem by realizing separately—and randomly—the various Kraus operators A_i, $i = 1, \ldots, n$, in this way being able to preserve the encoding for each A_i. Roughly speaking, we will do it such that "on average" the logical channel Λ is applied. That is, not knowing which logical Kraus operator is applied when we find the output ancillary modes in the vacuum, the channel is realized. Of course, this is possible only by allowing the linear optical network to change. We will introduce the possibility of switching among various optical networks—one for each A_i—according to a probability distribution $\{p_i\}$. Each fixed optical network that we will introduce to realize the Kraus operator A_i will itself correspond to a quantum channel Γ_i (see Figure 3.2). This "average realization" of the logical channel will anyway be stochastic, because in the implementation of any A_i that is not unitary there will necessarily be a finite probability of ending up outside the encoding, which corresponds to finding the input photon in the output ancillary modes.

One important point is that, given the additional degree of freedom due to the choice of the probability distribution $\{p_i\}$, it is possible to consider the realization of a rescaled version $\tilde{A}_i$ of A_i rather than exactly A_i. Of course each $\tilde{A}_i$ must be a valid Kraus operator, i.e., $\|\tilde{A}_i\|_\infty \leq 1$. We will use this rescaling degree of freedom to maximize the success probability for the realization of the channel.

If we postselect on finding the output ancillary modes in the vacuum state, and if we choose the probability distribution $\{p_i\}$ and the $\tilde{A}_i$ operators such that $\sqrt{p}_i \tilde{A}_i = \sqrt{p_{\text{succ}}} A_i$ for all i and for some $0 \leq p_{\text{succ}} \leq 1$, then the logical input state ρ will be mapped into the (unnormalized) logical state

$$\sum_i p_i \tilde{A}_i \rho \tilde{A}_i^\dagger = p_{\text{succ}} \sum_i A_i \rho A_i^\dagger \, .$$

This will happen with probability $\text{Tr}(\sum_i p_i \tilde{A}_i \rho \tilde{A}_i^\dagger) = p_{\text{succ}}$, and thus the logical channel Λ will be stochastically implemented with probability p_{succ} (independent of the input ρ).

Given that we want the channel to be realized perfectly, the figure of merit we care about is the probability of success p_{succ}, which we want to be maximal. One possible choice for the distribution $\{p_i\}$ and the operators $\tilde{A}_i$ is trivially $p_i = 1/n$ and $\tilde{A}_i = A_i$; this choice

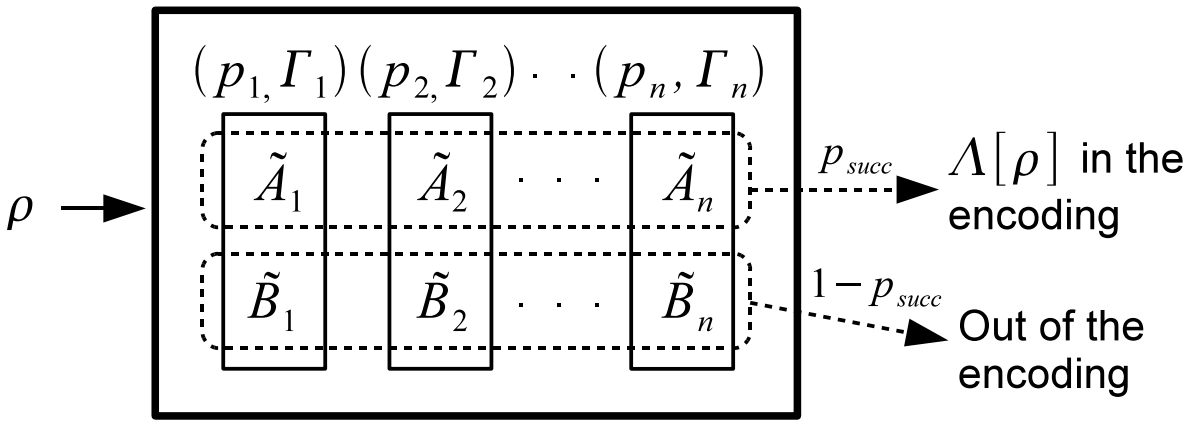

Figure 3.2: Pictorial representation of our scheme. Each solid rectangle represents a channel. The most external box is a mixture of the n channels Γ_i inside of it. Each of these inner channels corresponds to a linear-optics setup and for our scope its action on the encoding can be completely described without loss of generality by two Kraus operators, $\tilde{A}_i$ and $\tilde{B}_i$. Each $\tilde{A}_i$ preserves the d-rail encoding, while the Kraus operators $\tilde{B}_i$ map an encoded state out of the encoding. If the condition $\sqrt{p_i}\tilde{A}_i = \sqrt{p_{\rm succ}}A_i$, for all i, is met, the overall result of randomly switching among the channels Γ_i according to the probability distribution $\{p_i\}$ is that of realizing the target logical channel Λ with probability $p_{\rm succ}$ (independent of the input ρ).

leads to a probability of success $p_{\rm succ} = 1/n$. This strategy is independent of the properties of the Kraus operator $\{A_i\}$ for the particular channel Λ, and depends only on the number of Kraus operators. As such, one can expect it to be non-optimal, and it certainly is in the case of a random-unitary channel

$$\Lambda[\rho] = \sum_i q_i U_i \rho U_i^\dagger,$$

with $\{U_i\}$ unitaries and $\{q_i\}$ a probability distribution. Indeed, in this case an obvious better choice—and actually optimal—is $p_i = q_i$, $\tilde{A}_i = U_i$, for all i, such that $p_{\rm succ} = 1$.

The following theorem provides the optimal choice of the probability distribution $\{p_i\}$ and of the operators $\tilde{A}_i$'s to maximize $p_{\rm succ}$, for any fixed Kraus decomposition $\{A_i\}$.

Theorem 1. *Given the Kraus decomposition $\{A_i\}$ for the channel Λ, the optimal probability of success for its realization is*

$$p_{\rm succ}(\{A_i\}) = \frac{1}{\sum_i \|A_i\|_\infty^2}. \tag{3.8}$$

This can be achieved by the choice $p_i = \frac{\|A_i\|_\infty^2}{\sum_j \|A_j\|_\infty^2}$ *and* $\tilde{A}_i = \frac{1}{\|A_i\|_\infty} A_i$*, for all* i*.*

From the condition $\sqrt{p_i}\tilde{A}_i = \sqrt{p_{\text{succ}}}A_i$, for all i, one finds $p_i \geq p_i \|\tilde{A}_i\|_\infty^2 = p_{\text{succ}}\|A_i\|_\infty^2$, where we used the fact that $\|\tilde{A}_i\|_\infty \leq 1$, because each $\tilde{A}_i$ must be a proper Kraus operator. Summing over i and using $\sum_i p_i = 1$, one arrives at $p_{\text{succ}} \leq 1/\sum_i \|A_i\|_\infty^2$. The probability distribution and Kraus operators in the statement of the theorem saturate the inequality.

Thus, the maximal probability of simulating the channel adopting the Kraus decomposition $\{A_i\}$ in our scheme is the inverse of $\sum_i \|A_i\|_\infty^2$. This quantity will in general depend on the specific Kraus decomposition. With a single decomposition it is possible to use this formula, $\sum_i \|A_i\|_\infty^2$, to put a lower bound on the optimal probability of success for the realisation of the channel in our scheme.

Corollary 1. (Optimal probability of success) *In our scheme, the optimal probability of success in the implementation of* Λ *is*

$$p_{\text{succ}}(\Lambda) = \max_{\{A_i\}} \frac{1}{\sum_i \|A_i\|_\infty^2}, \tag{3.9}$$

where the maximization is over all Kraus decompositions $\{A_i\}$ *of the channel* Λ*.*

For convenience in the analysis to follow, we define the *stochasticity* of a channel as

$$\sigma(\Lambda) = \min_{\{A_i\}} \sum_i \|A_i\|_\infty^2, \tag{3.10}$$

where the minimization is over all Kraus decompositions $\{A_i\}$ of the channel Λ, so that

$$p_{\text{succ}}(\Lambda) = \frac{1}{\sigma(\Lambda)}.$$

The name "stochasticity" is justified by the fact that the larger $\sigma(\Lambda)$, the lower the probability of a successful realization of the channel.

3.5 Analysis

We have now provided a scheme for the realisation of any channel, Λ, that acts on a finite dimensional system. The realisation that we have proposed is stochastic, however, we have

provided an expression for the optimal realisation of the channel with our scheme. The expression for the optimal realisation involves a quantity we call the stochasticity. Evaluating the stochasticity of a channel involves performing a minimization over all possible Kraus decompositions of the channel, which is a computationally expensive task. However in this section we will consider a conceptually simple bound on the probability of success which uses the triangle inequality. We will then consider a specific channel, the amplitude damping channel. The realisation of this channel using resources that we described in Section 3.3 has been investigated in [33]. For this channel we will provide a Kraus decomposition and prove that it minimizes the stochasticity. We will then show that we can improve on the success probability realised in the scheme from [33].

3.5.1 Triangle-inequality bound

By using the triangle inequality, it is straightforward to derive an upper limit on the success probability.

Observation 1. (Triangle-inequality bound) *We let I represent the un-normalised maximally mixed state with $Tr(I) = d$ where d is the rank of I. Then for any quantum channel Λ,*

$$p_{\text{succ}}(\Lambda) \leq \frac{1}{\|\Lambda(I)\|_\infty}. \tag{3.11}$$

Proof. If $\{A_i\}$ is any Kraus decomposition for the channel Λ then we have for the stochasticity:

$$\begin{aligned}
\sigma(\Lambda) &= \min_{\{A_i\}} \sum_i \|A_i\|_\infty^2 \\
&= \min_{\{A_i\}} \sum_i \|A_i A_i^\dagger\|_\infty \\
&\geq \min_{\{A_i\}} \|\sum_i A_i A_i^\dagger\|_\infty \\
&= \|\Lambda(I)\|_\infty,
\end{aligned}$$

where the inequality is due to the triangle inequality, and the dependence on the choice of the Kraus decomposition is lost because $\sum_i A_i A_i^\dagger = \Lambda(I)$, for any Kraus decomposition of Λ. □

This bound proves that it is necessary for a channel to be unital in order for us to implement it deterministically using our scheme, because only for a unital channel $\|\Lambda(I)\|_\infty = 1$. This is consistent with the already argued fact that under our scheme only random-unitary channels can be deterministically implemented. The bound is easily evaluated, being independent of any particular Kraus decomposition.

3.5.2 Amplitude Damping Channel

The amplitude damping channel is a map on a two-level system and it can be described with two Kraus operators,

$$A_1 = \sqrt{\epsilon}|0_L\rangle\langle 1_L| \text{ and } A_2 = |0_L\rangle\langle 0_L| + \sqrt{1-\epsilon}|1_L\rangle\langle 1_L| \; . \tag{3.12}$$

To model the channel we imagine that we have the state, $c_0|0\rangle + c_1|1\rangle$, where the states $|0\rangle$ and $|1\rangle$ are Fock states. The damping of the channel will occur if there is some path that connects this single mode state to the environment (which is modelled as a vacuum state $|0\rangle$). Then imagine that the process occurs as a beamsplitting of our input state with an ancilliary vacuum state,

$$\left(c_0|0\rangle + c_1|1\rangle\right)|0\rangle \rightarrow \left(c_0|0\rangle + c_1\sqrt{\epsilon}|1\rangle\right)|0\rangle + c_1\sqrt{1-\epsilon}|0\rangle|1\rangle \; . \tag{3.13}$$

The free parameter ϵ is then the transmittivity of the beamsplitter that connects the input state to the vacuum ancilla. In the modelling of the amplitude damping channel we imagine that the ancilla state is discarded so that the transformation can be described with the two Kraus operators corresponding to the two possible states that the environment can be found in (see Eq.(3.12)).

We would like to apply this channel to dual rail encoded states, where we have replaced the vacuum and single photon states with the states $|0_L\rangle = a_1^\dagger|0\rangle$ and $|1_L\rangle = a_2\dagger|0\rangle$ defined in Eq.(3.1). We can express the Kraus operators that correspond to the transformation in Eq.(3.13) with the basis $\{|0_L\rangle, |1_L\rangle\}$ as,

In [33] a scheme for the realisation of this channel that works with a probability of 1/2 is suggested. The scheme follows the same constraints that we apply in our scheme (see Section 3.3) To find the exact value for probability of success for our scheme we need to determine the stochasticity of the amplitude damping channel. To find the value of the stochasticity we need to find the Kraus decomposition, $\{A_i\}$, of the channel that minimizes the quanitity $\sum ||A_i||_\infty^2$. However, every Kraus decomposition of the channel will provide a upper bound on the stochasticity and a lower bound on the probability of

success. Therefore with the decomposition shown in Eq.(3.12) we can determine an upper bound on the stochasticity

$$\begin{aligned}
\sigma(\Lambda) &\leq ||A_1||_\infty^2 + ||A_2||_\infty^2 && (3.14)\\
&\leq ||A_1^\dagger A_1||_\infty + ||A_2^\dagger A_2||_\infty && (3.15)\\
&\leq ||\epsilon|0_L\rangle\langle 0_L|||_\infty + ||(1-\epsilon)|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|||_\infty && (3.16)\\
&= 1+\epsilon && (3.17)
\end{aligned}$$

Therefore the optimal probability of success is greater then $1/(1+\epsilon)$. With this lower bound we can see that at the extreme point, $\epsilon = 0$, the channel is just the identity channel which we can implement deterministically with our chosen resources.

The lower bound $1+\epsilon$ is actually the exact value for the stochasticity of the channel, so that the decomposition shown in Eq.(3.12) is the optimal decomposition for our scheme. To see that this decomposition is optimal we can use the bound from 3.5.1,

$$\begin{aligned}
\sigma(\Lambda) &\geq ||\sum_{i=1}^{2} A_i A_i^\dagger||_\infty \\
&= ||\epsilon|0_L\rangle\langle 0_L| + (1-\epsilon)|1_L\rangle\langle 1_L + |0_L\rangle\langle 0_L|||_\infty \\
&= ||(1+\epsilon)|0_L\rangle\langle 0_L| + (1-\epsilon)|1_L\rangle\langle 1_L||_\infty \\
&= 1+\epsilon\ . && (3.18)
\end{aligned}$$

As both the upper and lower bounds on the stochasticity are equal we can conclude that the optimal probability of succes for our scheme is $\frac{1}{1+\epsilon}$.

The probability of success decreases as ϵ increases. Therefore for small ϵ our scheme will have a clear advantage – in terms of probability of success over the scheme in [33]. Only in the case that $\epsilon = 1$ is the probability of success $1/2$. In this case the channel outputs the fixed state, $|0\rangle\langle 0|$.

Chapter 4

Efficient Heralding of Photonic Qubits with Applications in Device Independent Quantum Key Distribution (DIQKD)

Notice: The content of this chapter has been published in:

D. Pitkanen, X. Ma, R. Wickert, P. van Loock, Norbert Lütkenhaus, Phys. Rev. A, **84**, 022325 (2011).

4.1 Motivation

The verification of entanglement for quantum communication, and the establishment of security proofs in Device Independent Quantum Key Distribution (DIQKD) [29] have generated an increasing interest in long distance violations of Bell's inequalities. A violation of Bell's inequality is supposed to be a test for a non-local correlation between the outcomes of pairs of events; however, it is difficult to design an experiment that rigorously shows this non-locality. Imperfections in the experimental equipment can open loopholes, in the perceived Bell violation, which allow for local Hidden Variable (HV) explanations of the measured data. For example, signal loss in optical implementations generates the so-called detection efficiency loophole [27].

In experiments, with growing distance the transmission loss increases. Consequently, the resulting low total detection probabilities make violations of Bell's inequality virtually impossible. To overcome this issue, the use of heralding devices [34, 9] has been suggested. Such an apparatus performs a measurement that resembles a quantum non-demolition (QND) measurement, raising a flag to indicate whenever the desired signal successfully traversed the channel. The state generated by conditioning on this flag can then be employed in a Bell test. This procedure does not lead to a detection loophole as long as the flagging is independent of the measurement choice.

Gisin et al. [9] have considered an implementation of a heralding device in a DIQKD scheme employing realistic sources, linear optical components and photon-number resolving detectors. However even with perfect devices their proposed scheme does not achieve a perfect QND measurement onto the desired space. Instead the scheme has an adjustable parameter in it, the transmissivity of a beam splitter, which regulates the ratio between the vacuum and single photon components in the conditional output state. The scheme works probabilistically and the single photon component in the conditional output state can only be increased by decreasing the probability of success of the scheme. With input signals consisting only of vacuum and single-photon states, increasing the single-photon component to unity in the conditional output can only be achieved in a limit of vanishing success probability. If the input also contains multiphoton signals, then the fraction of single photon signals in the conditional states cannot reach unity.

Within this chapter two schemes which overcome the limitations of the Gisin amplifier are investigated. In the first scheme a KLM-like teleportation procedure is considered which performs the desired QND measurement. As in the original KLM proposal the probability the procedure succeeds depends on the size of the ancilla state that is used. With this scheme the measurement works perfectly, and deteministically in the limit of an infinitely large ancilla.

The ancilla state used in the original Gisin qubit amplifier is simpler than any of the ancilla states in the KLM-like scheme we suggest. For this reason we propose a second scheme which uses the simple ancilla from the original amplifier. In fact the second scheme only differs from the original Gisin qubit amplifier by the addition of two beamsplitters.

DIQKD simulations were included in the proposal for the original amplier. For this reason we run these same simulations with our improved amplifier to show quantitatively that it is an improvement over the original amplifier.

4.2 Photonic and Qubit Amplifier

We begin by revisiting the noiseless linear photonic amplifier proposal of Ralph and Lund [34], see Fig. 4.1. A single-photon state passes through a beam splitter of transmissivity t to create an entangled state of two modes involving vacuum and single photons. One of the modes will be the output of the device, while the other is mixed with the input mode, ρ_{in}, on a 50:50 beam splitter. Both output modes of the $50:50$ beam splitter are measured with photon detectors and the observation of exactly one photon in the measured modes is taken as the successful heralding flag.

Depending on which of the two detectors is triggering the flag, an optical phase correction has to be applied at the output of the device. This feed-forward mechanism is not essential to our discussions, and we incorporate it directly into the description of the device. In practise one will have to do this feed-forward, unless the action of the phase correction can be combined with a subsequent measurement in such a way that, instead of active feed-forward, just a re-interpretation of the measurement results takes place.

For $t = \frac{1}{2}$, this scheme amounts to quantum scissors circuit discussed in Chapter 2 and Section 2.4. For $t > \frac{1}{2}$, the vacuum component $|0\rangle$ of the outgoing mode ρ_{out} is reduced and the single-photon term $|1\rangle$ emerges enhanced relative to the vacuum component. This corresponds to a mapping induced by a Kraus operator A,

$$A\left(c_0|0\rangle + c_1|1\rangle\right) = \sqrt{1-t}c_0|0\rangle + \sqrt{t}c_1|1\rangle \ , \tag{4.1}$$

which has the important property that, as $t \to 1$, this circuit approaches a projection onto the single photon state, $|1\rangle$. We use non-normalized states in our description, so that the success probability of the heralding device is given by the norm of the conditional output state.

We have defined the two-dimensional Hilbert space of exactly one excitation in two optical modes as a photonic or dual-rail qubit 1.4. It is the central idea of the work by Gisin et al. [9] to use two Ralph-Lund amplifiers [34] in parallel on the two modes to herald such a photonic qubit. A successfully heralded event is defined as the joint success of both amplifiers. The action is then represented as

$$A \otimes A\left(c_{00}|00\rangle + c_{10}|10\rangle + c_{01}|01\rangle\right) = \\ (1-t)c_{00}|00\rangle + \sqrt{t(1-t)}\left(c_{10}|10\rangle + c_{01}|01\rangle\right) \ . \tag{4.2}$$

The circuit for this qubit amplifier is shown in Fig. 4.1, where the dual-rail qubit is encoded in the polarization. The weight of the dual-rail qubit component in this conditional state

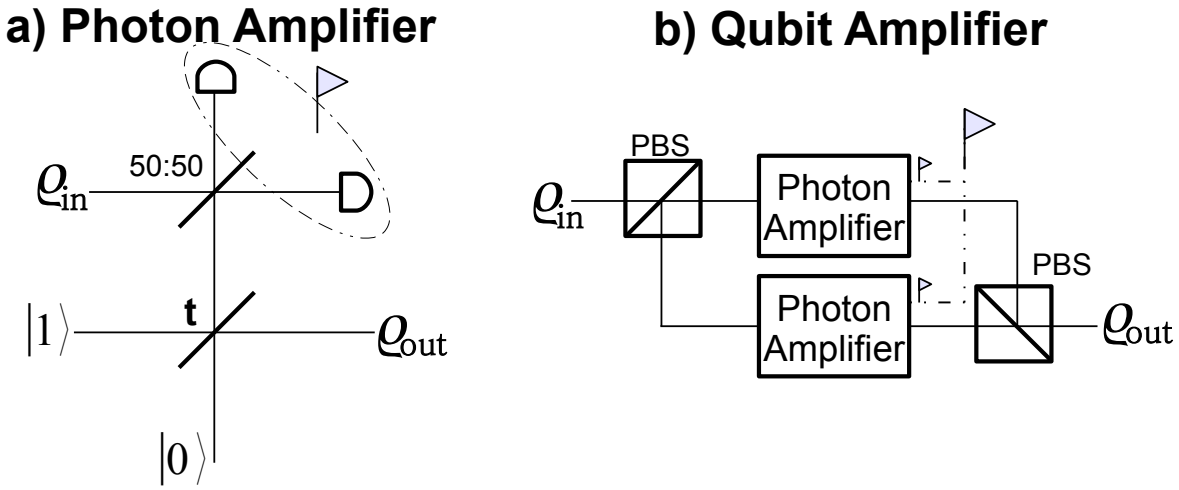

Figure 4.1: (color online) (a) The Ralph-Lund noiseless linear amplifier scheme: an input mode ρ_{in} interacts with an ancilla state through a $50:50$ beam splitter. Conditioned on a successful detection pattern, which raises the heralding flag, the output ρ_{out} is shifted towards the single-photon state. The parameter t is the transmissivity of the beam-splitter (b) The Gisin-Pironio-Sangouard qubit heralding device: two amplifiers are combined to amplify states in the horizontal/vertical (h/v) basis; the flag is only raised if both the amplifiers are successful. The input state ρ_{in}, encoded in the polarisation basis h/v, is sent through a polarising beam-splitter (PBS) to spatially separate its modes so that the different amplifiers may be applied. A second PBS is used to combine the different spatial modes of the output into the h/v basis. In both schemes the feed-forward mechanism has been omitted.

can reach unity in the limit $t \to 1$. In this limit the probability of successful heralding vanishes, indepedendently of the input state. If the input state also contains a multiphoton component, $c_{11}|11\rangle$, then the weight of the dual-rail qubit in the output state can no longer reach unity, as the output will also contain the component $tc_{11}|11\rangle$. In that case, the choice $\frac{t}{1-t} = \frac{|c_{00}|}{|c_{11}|}$ optimizes the qubit fraction of the output. This optimal qubit fraction in the heralded signals is then given by

$$\frac{|c_{10}|^2 + |c_{01}|^2}{2|c_{11}||c_{00}| + |c_{10}|^2 + |c_{01}|^2} \ . \tag{4.3}$$

Although we have only considered the case of a pure state input, this bound also applies to mixed states if $\sqrt{\langle ij|\rho_{in}|ij\rangle}$ is used instead of $|c_{ij}|$.

4.3 KLM Solution

Before proposing a practical scheme to overcome the limitations of the heralding setup by Gisin et al., let us take a more fundamental point of view. We remain restricted to the linear optics toolbox, but allow for the use of more complicated sources for the ancilla states, and show that, in this context, the heralding measurement for dual-rail qubits can be performed asymptotically perfectly. Our approach is based on the KLM framework, discussed in Section 1.4, which successfully accomplishes the teleportation of an arbitrary state of the form $c_0|0\rangle + c_1|1\rangle$ with a probability that can be brought asymptotically close to 1.

The implementation of such procedure relies on the use of an ancilla state

$$|t_n\rangle \ = \ \frac{1}{\sqrt{n+1}} \sum_{i=0}^{n} |t_{n,i}\rangle \ , \tag{4.4}$$

where $|t_{n,i}\rangle = |1\rangle^{\otimes i}|0\rangle^{\otimes(n-i)}|s_i\rangle$ and $|s_i\rangle = |0\rangle^{\otimes i}|1\rangle^{\otimes(n-i)}$ using the notation from Section 1.4. We refer to the first n modes of this state as the teleporting modes, while the second n modes are referred to as output modes. In the KLM procedure the teleporting modes and the input modes are Fourier transformed and then measured with photon counting detectors. If $1 \leq k \leq n$ photons are detected, the remaining unmeasured output modes are left in the state

$$c_0|0\rangle^k|1\rangle^{n-k} + e^{-i\phi_k}c_1|0\rangle^{k-1}|1\rangle^{n-k+1} \ . \tag{4.5}$$

The phase ϕ_k depends on the number of counted photons, k, and the observed detection pattern, and can be corrected with an appropriately adjusted phase shifter. As in the case of the linear photonic amplifier, we will incorporate this correction automatically into our description. Overall, the input state will then be found in the k-th mode of the above state.

This approach can also be adapted to perform a non-demolition measurement onto the single-photon input space of two modes. To do this, we will consider the auxiliary state

$$|\tilde{t}_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{i=0}^{n} |t_{n,i}\rangle |t_{n,n-i}\rangle \ , \tag{4.6}$$

which corresponds to those terms in $|t_n\rangle \otimes |t_n\rangle$ containing exactly n photons in the two sets of teleporting modes in the $|t_{n,i}\rangle$ states. We now show that the application of the KLM-type procedure, employing the alternative state above, realizes a QND measurement onto the total photon-number space of the input modes. To verify this, we first note that this procedure effectively measures the photon number in the input: as the total number of photons in the two pairs of teleporting auxilliary modes is known to be n, the observed photon number on the input and these $2n$ modes tells us how many photons have entered the heralding device. In a second step, we need to verify that the output state corresponds to that of a QND measurement: if the two Fourier measurements acting each on one input mode and one set of teleporting modes yield the observation of i and $n-i+1$ photons respectively, giving exactly $n+1$ photons in total, and these individual photon numbers are neither 0 nor $n+1$, then the corresponding conditional state of the remaining $2n$ output modes is

$$c_{01}|0\rangle^i|1\rangle^{n-i}|0\rangle^{n-i}|1\rangle^i + c_{10}|0\rangle^{i-1}|1\rangle^{n-i+1}|0\rangle^{n-i+1}|1\rangle^{i-1} \ . \tag{4.7}$$

This means that the input state has been teleported into the mode pair with indices $(i, 2n-i+1)$ of the above state. The probability of failure of this scheme, just as in the original KLM proposal, is connected to occurence of 0 or $n+1$ photons in the individual Fourier measurements, and is given by $\frac{1}{n+1}$. Thus, one can perform a probabilistic perfect heralding measurement and the probability of success can be made arbitrarily close to unity.

4.4 Modified Amplifier Circuit

An obvious strength of the scheme proposed in [9] lies in the relative simplicity of its ancilla states, which can be generated with a single-photon source and vacuum states. Here we take

a practical approach, keeping the same ancilla states, and look for simple modifications we can make to the amplifier to improve its performance. We focus on modifying the amplifier so that a vacuum input will no longer trigger the heralding flag at all. We begin by examining the original scheme, which consists of two separate Ralph-Lund amplifiers, each with their own auxilliary single photon states.

In order for the signal to be heralded by the qubit amplifier, both of the flags on the separate Ralph-Lund amplifiers need to be raised by detecting exactly one photon respectively, after each of the 50:50 beam-splitters. This set-up can lead to false flagging for a vacuum input. These false heralding flags occur if both of the auxiliary photons from the separate amplifiers travel 'upwards' in our diagram towards the heralding detectors behind the 50:50 beam-splitters.

We suppress this component by adding another 50:50 beam-splitter between these upward directed modes; the Hong-Ou-Mandel effect [13] ensures that the component with two photons in each mode will now bunch to either of the outgoing modes of the beam-splitter. This means that the heralding detectors of one of the Ralph-Lund amplifiers will see zero photons, while the other will see two, and therefore, the heralding condition of the qubit amplifier will no longer be met. A second 50:50 beam-splitter is added to the output modes of the qubit amplifier, so that the transformation effected by the amplifier to the single-photon input does not change. On the other hand, the action of the second beam-splitter corresponds to a change of polarization basis on the single-photon subspace, and can be absorbed into the action of any device that is acting on the output of the heralding device. With these two additional beam-splitters (see Fig. 4.2), we find that the successful heralding is connected to the Kraus operator A_{mod} given by

$$\begin{aligned} & A_{mod}\left(c_{00}|00\rangle + c_{10}|10\rangle + c_{01}|01\rangle + c_{11}|11\rangle\right) \\ &= \sqrt{t(1-t)}\left(c_{01}|01\rangle + c_{10}|10\rangle\right) + t\frac{1}{\sqrt{2}}c_{11}\left(|20\rangle + |02\rangle\right) \ . \end{aligned} \tag{4.8}$$

This Kraus operator already accounts for the required phase correction that depends on the exact pattern of single-photon detection after each of the two 50:50 beamsplitters.

The transformation overcomes both of the problems discussed in Section 4.2: first, assuming only vacuum and single photon input signals ($c_{11} = 0$), this amplifier can perform a perfect, heralded projection onto the dual-rail component. Second, even if multiple photons are present in the input ($c_{11} \neq 0$), the single-photon fraction in the output can still be made arbitrarily close to unity in the limit of vanishing success probability ($t \longrightarrow 0$) .

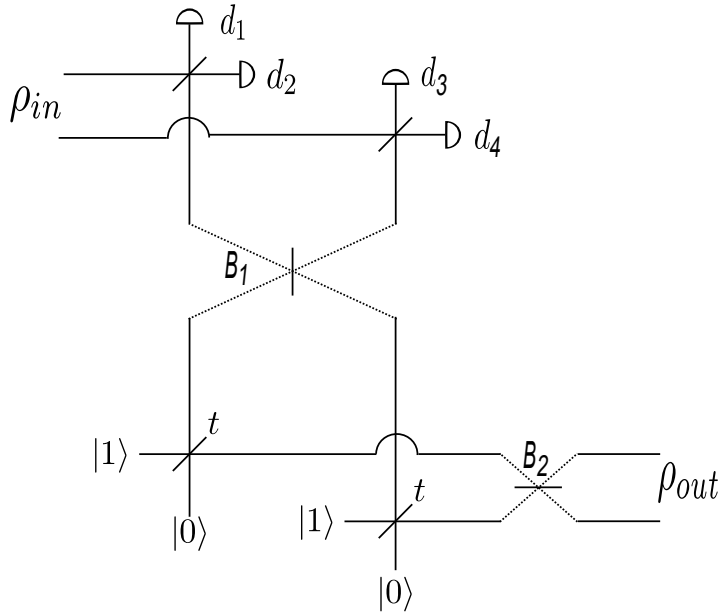

Figure 4.2: The proposed circuit for the improved qubit amplifier. Without the two $50:50$ beam-splitters, marked B_1 and B_2, it corresponds exactly to the amplifier suggested by Gisin et al. The circuit's inputs are the two modes of ρ_{in}. The amplifier is only meant to output a signal, ρ_{out}, when a single photon is measured in each of the detector sets (d_1, d_2) and (d_3, d_4). The required feed-forward mechanism to correct optical phases is omitted.

4.5 Application to Device Independent QKD

4.5.1 Background Device Independent QKD

If two parties share a string, k, that is n-bits long they can use this string to securely communicate an arbitrary n-bit message, m. With two binary values x, $y \in \{0, 1\}$ we can define the binary addition operation, $\oplus$, as $x \oplus y = x + y \bmod 2$. With this definition, to perform the secure communication the sending party can simply send the message $m \oplus k$ over a public channel. As $k \oplus m \oplus k = m$ the recieving party will be able to use their key to decode the message m. As obtaining information about m given the message $m \oplus k$ is equivalent to having knowledge on the key k the message will be as secure as the initial key shared by the parties. This procedure for sending information securely is known as the one-time pad protocol.

The pad makes the distribution of secure keys between parties a valuable resource

for secure information transfer. Quantum mechanics makes it possible to distribute keys between two parties in a method that is provably secure. The study of key distribution using quantum mechanics is called quantum key distribution.

In a typical QKD protocol a pair of communicating parties will share a quantum state ρ_{AB} that has been sent to them over a channel that they do not trust. Therefore the parties will be unaware of the state ρ_{AB} that they share. As an adversary may have interacted with the state as it is passed over the channel the state will exist as the reduced state of the tripartite state ρ_{ABE}.

Depending on the protocol they are following the two parties will both perform local measurements on their state in order to bound the information that an observer may have gained on their measurement results and to generate correlated data so that they may generate a secure key. The first party, called Alice, performs a set of measurements whose outcomes are denoted by the set A and the second party, called Bob also performs a measurements on his state whose outcomes are denoted by B. The Devetak-Winter bound provides an achievable lower bound on the rate, r, the parties can transmit information using their measurements [7]

$$r = I(A, B) - \chi(B : E) \tag{4.9}$$

where the mutual information,

$$I(A, B) = \sum_{a \in A,\, b \in B} p(a, b) \log \frac{p(a, b)}{p(a)p(b)}$$

and the Holevo quantity,

$$\chi(B, E) = S(\rho_E) - \sum_{b \in B} p_b S(\rho_{E|b})$$

and the von Neuman entropy

$$S(\rho) = Tr\left(\rho \log \rho\right)$$

The reduced state of the adversary is defined as $\rho_E = Tr_{AB}\left(\rho_{ABE}\right)$ and the state $\rho_{E|b}$ is the reduced state of Eve conditioned on Bob obaining the measurement outcome b. Both the states ρ_{ABE} and ρ_{AB} are in general unknown. For a fixed ρ_{AB} the key rate in Eq.(4.9) is lowest when Eve is given the purification of the state [7]. Therefore by finding the state ρ_{AB} that is compatible with all the measurements made by the two parties and whose purification minimizes Eq.(4.9) a lower bound on the key rate can be determined.

The simulations we will consider are in Device Independent Quantum Key Distribution (DIQKD). In DIQKD there is a well known result that if two parties share a state ρ_{AB} and perform a Bell test on this state then the maximum amount of information that a third party can obtain is upper bounded the expression [29],

$$\chi(B,E) \leq h\left[\frac{1+\sqrt{(S/2)^2-1}}{2}\right]$$

if S is the Bell parameter from Eq.(1.8). The expression is a upper bound that holds regardless of the of the POVM choices of the parties use for the Bell test they perform and it is also independent of the dimension size of the space that they are measuring. It is only important that the results of their measurements have binary outcomes.

To bound information of an eavesdropper in DIQKD, Alice and Bob both randomly and independently select two measurements which are designed to verify the violation of Bell's inequality by evaluating a Bell parameter S. To generate the key, the receiver also makes use of a third measurement, σ_z, which is designed to obtain highly correlated data with the sender. These data serve as the raw key from which the final key will be distilled. On these data, we expect to find binary error rates Q.

4.5.2 Application to Device Independent QKD

In the proposal for the original qubit heralding device, a DIQKD simulation was performed to demonstrate how heralding overcomes transmission losses. The simulation included imperfect sources and detectors. We perform analogous simulations to demonstrate the improvement that our heralding device offers. For this comparison, we consider three main scenarios. The first one is motivated by the simulation reported in Gisin et al. [9], where the authors introduced a theoretical framework to deal with inconclusive outputs due to imperfect devices. In this framework restrictions on the eavesdropping strategies are assumed; we therefore refer to this framework in our simulations as *Restricted Device Independent Theory*, in subsection 4.5.3. In addition we also run simulations which deal with the inconclusive results by randomly assigning to them a conclusive binary value, thereby allowing us to apply the usual *Unrestricted Device Independent Theory*, in subsection 4.5.3. As a third framework, we explore the so-called *Detection Device Independent Theory*, in subsection 4.5.3, where knowledge of the source is assumed, but one can remain ignorant about the measurement device of one of the parties. The assumed knowledge of the source, in this framework, makes it useful not only for entanglement-based setups, but also for prepare-and-measure schemes.

4.5.3 Experimental Setup

We now describe the proposed experimental setup for DIQKD. To mediate the communication, a Spontaneous Parametric Down-Conversion source (EPR-SPDC) is used which generates entangled photons. The (unnormalized) state obtained through this process is given by

$$\rho_{source} = |vac\rangle\langle vac| + p|\phi^+\rangle\langle\phi^+| + p^2|\phi^{+2}\rangle\langle\phi^{+2}| + O(p^3) \ , \tag{4.10}$$

where $|\phi^+\rangle$ is a dual rail EPR pair, $|1010\rangle + |0101\rangle$; and $|\phi^{+2}\rangle = |2020\rangle + |1111\rangle + |0202\rangle$, up to a normalization. The parameter p is related to the pumping power. This EPR-SPDC source is located near one of the parties, Alice, and the two-mode signal that is received by the more distant party, Bob, is subject to transmission loss η_t. The loss which results from using imperfect detectors and coupling into fibers is taken into account with efficiency parameters η_d and η_c respectively. In our simulations we assume that all the detectors have the same efficiency so we model the detectors as perfect and include the detector loss in the coupling efficiency $\eta_{cd} = \eta_c\eta_d$. The photons employed in the auxilliary states of the amplifiers are generated from a heralded SPDC process that outputs the state [30]

$$\begin{aligned} \rho_{aux} \ &= \ p'\eta_{cd}|1\rangle\langle 1| + 2(1-\eta_{cd})\eta_{cd}p'^2|2\rangle\langle 2| + \\ &\quad 3(1-\eta_{cd})^2\eta_{cd}p'^3|3\rangle\langle 3| + O(p'^4) \ , \end{aligned} \tag{4.11}$$

where p' is again the pumping power. The amplifier therefore acts on the state

$$\rho_{total} = \rho_{source} \otimes \rho_{aux}^{\otimes 2} \otimes |0\rangle\langle 0|^{\otimes 2} \tag{4.12}$$

which incluces both components of the source states: the one that remains at Alice's site, and that which enters the amplifier. The whole set-up is depicted in Fig. 4.3 to indicate where coupling and detection efficiencies are included. Note that we include coupling efficiencies for the heralding detectors . Omitting these reproduces for the original heralding device the simulation shown in [9]. The source is on Alice's side of the set-up. Therefore, transmission loss affects only the signal travelling from the source to the amplifier, which is located in Bob's site.

In order to maximize the key rate, an optimization is performed over the pump parameter p and over the transmissivity t of the beam-splitter used in the heralding device. The range of the parameters p and p' are restricted to $0 \leq p, p' \leq 10^{-2}$, as we use a perturbative approach in our simulations. This constraint, however, affects only the simulations of the Detection Device Independent Scenario.

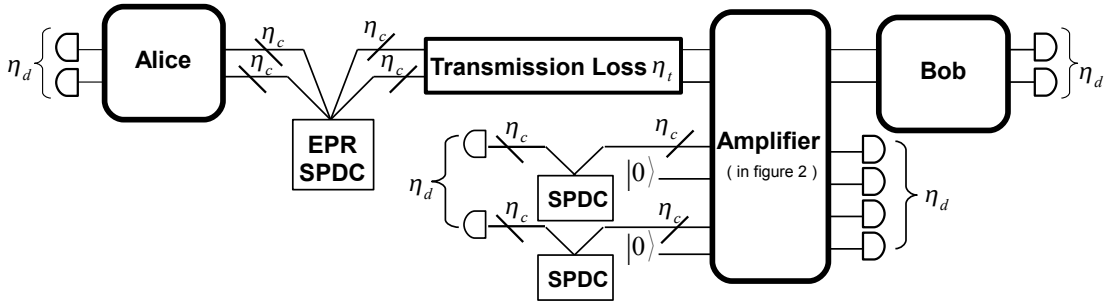

Figure 4.3: Experimental setup for the amplifier in the DIQKD simulations we consider. An EPR SPDC source is used to generate photons that are sent to the two distant parties. Two additional SPDC sources are used as heralded single photon sources for the amplifier. Each wire in this diagram represents a separate optical mode — i.e. we use two wires to represent a single spatial mode if we are using both of the polarisation, horizontal/vertical (h/v), degrees of freedom. The signal received by Bob is only processed if the right detection pattern appears on the amplifier.

Our simulations are done as perturbative *approximations* in the pump parameters p and p'. To bound the error in this approximation, we also provide *lower bounds* on the expected key rates by calculating the total weight of the neglected terms, and by using this weight in independent worst case values for the Bell parameters S and quantum bit error rates Q.

For simulation purposes, we follow the choices made in [9]. This includes modelling our detectors with photon-number resolving capabilities, neglecting dark counts, assuming a detection efficiency as high as 95% and running the sources at a repetition rate of 10 GHz. Dark counts can be neglected if the total dark count rate is negligibe compared to the total rate of heralded events.

Superconducting nanowire single-photon detectors and transition-edge superconducting detectors have shown these properties, although not in a single device [10, 21]. Transition-edge superconducting detectors are photon number resolving detectors and have also been demonstrated to work at an efficiency of 95%. However the repetition rate of the sources we use, 10 GHz, is several orders of magnitude higher then the optimal clock rate of these detectors, which run at 1000 counts per second. Alternatively, superconducting nanowire single-photon detectors are capable of working at the clock rates we consider in our simulations. These detectors are not photon-number resolving; however, a cascade of

single photon detectors may be used to approximate a number resolving detector. However, the nanowire detectors work at efficiencies that are much lower than what we have assumed in our simulations; typically the efficiency is 20%[10].

Restricted Device Independent Theory

The framework proposed by Gisin *et al.* follows the standard device independent protocol [1], but augments it by an analysis which makes an additional assumption about the eavesdropping strategies. Thanks to this assumption, all of the inconclusive results can be discarded during post-processing, though the rate of inconclusive results affects the resulting key rate. The key rate, which is given by

$$\begin{aligned} K \geq \quad & \mu_{cc}\Bigg\{1 - h[Q_{cc}] \\ & - \left[\left(1 - \frac{\mu_c}{\mu_{cc}}\right)\chi\left[\frac{\mu_{cc}S_{cc} - 4\mu_c}{\mu_{cc} + \mu_c}\right] + \frac{\mu_c}{\mu_{cc}}\right]\Bigg\}\ , \end{aligned} \tag{4.13}$$

with

$$h[x] = -x\log_2[x] - (1-x)\log_2[1-x] \ \text{ and} \tag{4.14}$$

$$\chi[x] = \begin{cases} h\left[\frac{1+\sqrt{(x/2)^2-1}}{2}\right] & \text{if } x > 2 \\ 1 & \text{otherwise} \end{cases}\ . \tag{4.15}$$

Here, μ_{cc} is the probability that both parties obtain a conclusive result. Within this set of conclusive data, S_{cc} is the measured Bell parameter, and Q_{cc} is the error rate. The probability that only one of the parties obtains a conclusive result is denoted by μ_c. The results are shown in Fig. 4.4. We find that our heralding device improves the distance and rate significantly.

Unrestricted Device Independent Theory

The scheme utilizing the unrestricted device independent theory differs solely from the setting in the previous section in its data post-processing stage. Any inconclusive measurement result on either side has binary outcomes assigned at random. Knowledge of the placements of such inconclusive results is later used in the error correction step [23]. For

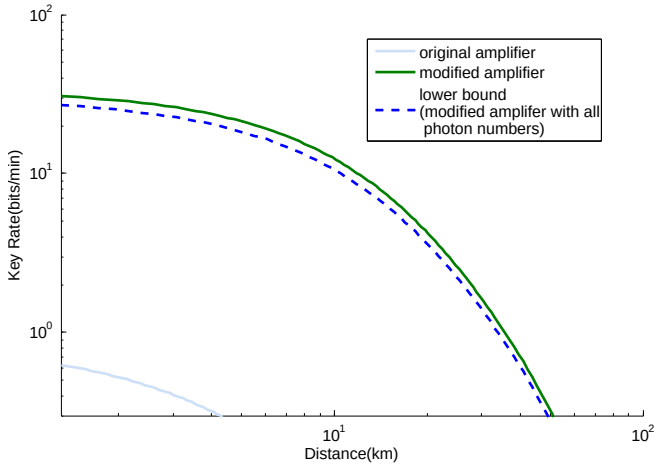

Figure 4.4: (color online) Key Rate vs. Distance, plotted for both the original [9] and the modified amplifier. The simulations are done using the *Restricted Device Independent Theory* framework. The key rate is calculated from Eq.(4.13), multiplied by the repetition rate of the source and the probability that the amplifier successfully heralds the signal. The efficiency parameters are chosen as $\eta_d = 0.95$ and $\eta_c = 0.90$, resulting in an overall efficiency of $\eta_{cd} = 0.855$.

this reason, the key rate includes quantities that reflect the fraction of conclusive results. The resulting key rate is

$$K = \mu_{-c}\,(1 - h[Q_{-c}]) - \chi[S]\;. \tag{4.16}$$

Here, μ_{-c} is the probability of Bob obtaining a conclusive result and Q_{-c} is the error rate within Bob's conclusive measurement results. Finally, $h[x]$ and $\chi[x]$ are the same as in Eqs. (4.14) and (4.15). The Bell parameter S is evaluated using the data from all of the measurement results, including the random assignments of inconclusive results.

From Eq.(4.16), we can see that the parties need non-classical correlations with at least $S > 2$ to generate a positive key, since $\chi[S] = 1$ otherwise. With our chosen post-processing strategy, we randomly assign binary outcomes to inconclusive measurement results, so that only the subset of measurements that yield conclusive outcomes on both sides make non-zero contributions to the Bell parameter, S. As quantum mechanics bounds the Bell parameter in any subset to $2\sqrt{2}$ the requirement that $S > 2$ leads to the bound $\mu_{cc} > \frac{1}{\sqrt{2}} \sim 0.707$, on the probability of conclusive-conclusive measurement outcomes. However, if we use a SPDC source to generate the signals, we find from Eq. (4.3) that the qubit fraction

after heralding is bounded by $\mu_{cc} < 3/5$ when using the original heralding device, even when using ideal detectors and single-photon sources. Therefore, such amplifier cannot be employed to generate positive key rates in this framework, unless a different source is used to generate the entangled photons. Note that other assignments of inconclusive results are possible [29] which may allow the extraction of a secret key with the original heralding device. The discussion requires more detailed analysis, as it depends on the exact configuration of the set-up. It is omitted here, as these studies go beyond the scope of the current research. However, some discussion of this question can be found in the work by Moroder and Curty [5].

Due to the above, the simulations for the unrestricted device independent theory are performed only for the newly proposed amplifier (see Fig 4.5). This framework is the most demanding on coupling and detection efficiencies that need to be used in order to generate a positive key: in our simulations, we use a total loss term $\eta_{cd} = 0.93$.

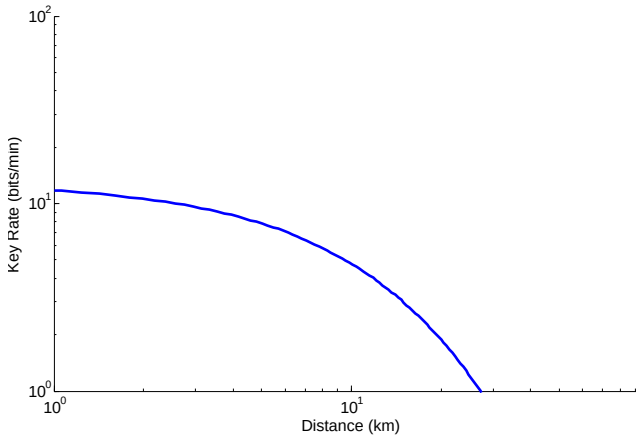

Figure 4.5: (color online) Key Rate vs Distance, plotted on a logarithmic scale for our proposed amplifier using the *Unrestricted Device Independent Theory* framework. We calculate the key rate from Eq. (4.16), multiplied by the repetition rate of the source, 10 GHz, and the probability that the amplifier successfully heralds the signal. The efficiency parameter is $\eta_{cd} = 0.95$. The bound for the influence the higher photon terms is not included in this plot since the bound differed negligibly from the perturbative calculation.

Detector Device Independent Theory

The final framework we consider is not fully device independent and, as a result, the security does not require a loophole-free violation of Bell's inequality. Here, the standard BB84 protocol is used [3] and we trust the source on Alice's side only. Bob's detectors remain uncharacterized. This scenario has been considered by Mayers [24], and later also by Koashi[18]. The scenario makes random assignment of inconclusive results on Bob's side necessary and therefore places a constraint on the detection probability that is required in order to generate a secure key [23]. Again we use the fact that the position of events with random assignment are known to Bob, who can utilize this knowledge in the later error correction step. The security proof [23] is therefore a variation of corresponding proofs of Koashi [18]. This scenario is more tolerant to transmission loss. For example, with perfect photon pair sources and detection devices, this scenario tolerates a total efficiency accounting for transmission, coupling and detection loss of 64.5% without heralding [23]. The key rate for this scheme is given by [23]

$$K \geq \mu_{-c}\left(1 - h[Q_{-c}]\right) - h[\delta_b] \; . \tag{4.17}$$

Here, $\delta_b = \mu_{-c}Q_{-c} + (1-\mu_{-c})\frac{1}{2}$ is an effective phase error rate; as in Eq.(4.16), μ_{-c} is the probability of Bob obtaining a conclusive result, and Q_{-c} is the error rate when Bob's measurement is conclusive. This framework is the least demanding on the coupling and detector efficiencies.

The simulations' results are shown in Fig. 4.6. In this case the pump parameters are larger compared to the other two scenarios. Therefore, the gap between the approximated rates and the lower bounds is more pronounced.

4.6 Conclusions

Heralding devices can play an important role in quantum key distribution. In principle, they allow to overcome the limitation posed by transmission losses to device independent quantum key distribution. In addition, other areas of quantum communication can benefit from such heralding devices. For example, some quantum memory approaches do not provide intrinsic heralding devices. Using external heralding, as proposed in this paper, will allow the use of such memories in quantum repeater technologies [38].

In this regard, we have explored the KLM framework and employed it in the implementation of a conceptually optimal heralding strategy which, in the limit of asymptotic

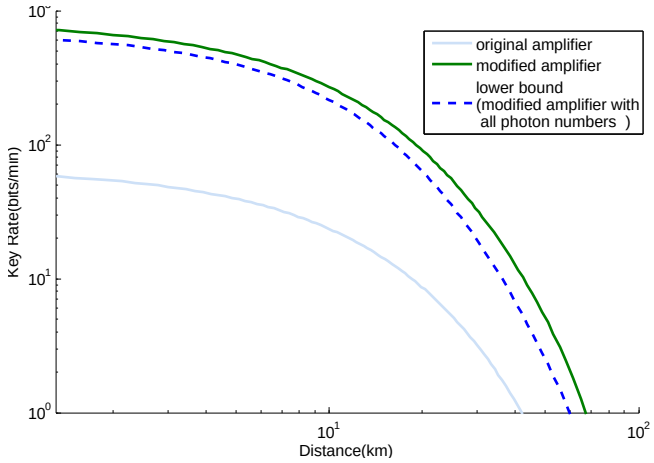

Figure 4.6: (color online) Key Rate vs Distance, plotted for both the original and the modified amplifier using the *Detection Device Independent Theory* framework. We calculate our key rate from Eq. (4.17), multiplied by the repetition rate of the source, 10 GHz, and the probability that the amplifier successfully heralds the signal. The efficiency parameter is $\eta_{cd} = 0.75$.

resources, achieves a perfect QND-like measurement onto the desired signal subspace with success probability approaching unity.

Departing from the conceptual scenario, we discussed a simple and experimentally-viable improvement on the original work by Gisin *et al.* [9], enhancing the performance of the heralding device. Specifically, we were able to overcome the undesired relation between how reliably the device works in heralding its input, and the success probability of the heralding process. Our device allows, in an idealistic implementation, perfect operation on the important input subspace containing at most one photon in each of the optical modes that define the dual-rail qubit.

This improvement not only increases the achievable key rates, in the context of a restricted device independent theory, by roughly one order of magnitude in distance and rate as compared to the scheme in [9], but also allows us to enter the domain of fully unrestricted device independent theory. Our simulations show that, under similar assumptions as those made in [9], we can obtain positive key rates in this desirable scenario. Note, however, that the requirements on detection and coupling efficiency are more demanding.

Finally, we showed that, for detector device independent theories with a well characterized source but uncharacterized detection devices, a secret key can be generated with relaxed requirements on the detection and coupling efficiencies, pushing these scenarios

now into the domain where experimental realization can be attempted.

Chapter 5

Conclusion

A variety of problems have been considered in this thesis although the focus has been using the linear optics toolset to realise different quantum operations. Linear optics is a practical tool for the manipulation of optical quantum states. In this thesis we have explored the types of transformations that are in principle possible with linear optics and state preparation. In Chapter 2 we showed that in principle any unitary rotation could be applied to a superposition of Fock states. However we used complicated ancilla states and did not suggest any reasonable experimental method for their generation. However in the next chapter we fixed the ancilla state, to be a set of vacuum modes, and showed that on the d rail encoding any channel could be realised stochastically. We then showed an optimal scheme for the realisation of these channels. In chapter 4 we considered the realisation of a QND measurement onto the dual rail space using linear optics. A linear optics device had already been suggested that realised this measurement and uses only single photon sources, however the device was imperfect and only worked probabilistically. We showed that using more complicated ancilla states we could increase the probability of success arbitrarily close to unity and realise the perfect measurement. Motivated by our scheme we suggested simple improvement that could be made to the existing amplifier.

In chapter 2 only a proof was provided that any unitary operator could be performed on a single mode Fock state. The proof was made by construction however the realisation of the scheme was by no means optimal (in terms of cost of resources). A natural direction for future research would be to somehow attach a cost to the generation of different ancilla states and study the tradeoff between the cost of realising different unitaries and their probability of success.

In chapter 3 we studied the realisation of different channels with fixed ancilla states. In

this chapter one could study how the problem changes when the use of more complicated ancilla states is allowed.

In chapter 4 a heralding device was investigated and used in DIQKD simulations. The simulations that were provided did not include many important experimental imperfections. For instance the phase matching of the pulses and the dark count rate of the detectors was not included. Including these details might lead one to determine the range of imperfections that could be tolerated by the devices that are used in order to realise different DIQKD schemes.

Bibliography

[1] Antonio Acin, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8(8):126, 2006. 54

[2] J. S. Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1:195–200, 1964. 10

[3] 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. 1, 57

[4] D. N. Biggerstaff, R. Kaltenbaek, D. R. Hamel, G. Weihs, T. Rudolph, and K. J. Resch. Cluster-State Quantum Computing Enhanced by High-Fidelity Generalized Measurements. *Physical Review Letters*, 103(24):240504, Dec 2009. 32

[5] M. Curty and T. Moroder. Heralded qubit amplifiers for practical device-independent quantum key distribution. arXiv:1105.2573v1. 56

[6] D. Deutsch and R. Jozsa. Rapid Solution of Problems by Quantum Computation. *Royal Society of London Proceedings Series A*, 439:553–558, December 1992. 1

[7] I. Devetak and A. Winter. Distillation of secret key entanglement from quantum states. *Proc. of the Roy. Soc. of London Series A*, 461(2053):207–235, 2005. 50

[8] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935. 10

[9] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.*, 105(7):070501, Aug 2010. iii, 12, 43, 44, 47, 51, 52, 53, 55, 58

[10] G. N. Gol'sman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski. Picosecond superconducting singl-photon optical detector. *Appl. Phys. Lett.*, 705:79–81, 2001. 53, 54

[11] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390–393, 1999. 10

[12] Bing He, János A. Bergou, and Zhiyong Wang. Implementation of quantum operations on single-photon qudits. *Phys. Rev. A*, 76(4):042326, Oct 2007. 32, 33

[13] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59(18):2044–2046, Nov 1987. 48

[14] R. A. Horn and C. R. Johnson. *Topics in matrix analysis*. Cambridge University Press, 1991. 34

[15] Kurt Jacobs and Jonathan P. Dowling. Concatenated beam splitters, optical feedforward, and the nonlinear sign gate. *Phys. Rev. A*, 74(6):064304, Dec 2006. 15

[16] E. Knill. Bounds on the probability of success of postselected nonlinear sign shifts implemented with linear optics. *Phys. Rev. A*, 68:064303, 2003. 14

[17] E. Knill, R. Laflamme, and G. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46, 2001. 2, 7, 10, 15, 31

[18] M Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, 2009. 57

[19] Pieter Kok, W. J. Munro, Kae Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn. Publisher's note: Linear optical quantum computing with photonic qubits [rev. mod. phys. 79, 135 (2007)]. *Rev. Mod. Phys.*, 79(2):797, Jun 2007. 8

[20] S. Lang. *Linear Algebra*. Springer, 3 edition, 1987. 33

[21] Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. Counting near-infrared single-photons with 95% efficiency. *Opt. Express*, 16(5):3032–3040, Mar 2008. 53

[22] N. Lütkenhaus. *Lectures on Quantum Information, Chapter 19: Probabilistic Quantum Computation and Linear Optical Realizations*. Wiley, 2007. 9

[23] Xiongfeng Ma and Norbert Lütkenhaus. Detection-device-independent quantum key distribution. in preparation. 54, 57

[24] D. Mayers. Unconditional security in quantum cryptography. *JACM*, 48(3):351–406, May 2001. 57

[25] Albert Messiah. *Quantum Mechanics*, volume 1. John Wiley & Sons, 1966. 3

[26] M. A. Nielsen and I. L Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. 6, 28, 30

[27] Philip M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2(8):1418–1425, Oct 1970. 42

[28] David T. Pegg, Lee S. Phillips, and Stephen M. Barnett. Optical state truncation by projection synthesis. *Phys. Rev. Lett.*, 81(8):1604–1606, Aug 1998. 19

[29] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009. 42, 51, 56

[30] T.B. Pittman, B.C. Jacobs, and J.D. Franson. Heralding single photons from pulsed parametric down-conversion. *Optics Communications*, 246(4-6):545 – 550, 2005. 52

[31] J. Preskill. Lecture note for physics: Quantum information and computation. 31

[32] Robert Prevedel, Philip Walther, Felix Tiefenbacher, Pascal Bohi, Rainer Kaltenbaek, Thomas Jennewein, and Anton Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445:65, 2007. 32

[33] L. Qing, L. Jian, and G Guang-Can. Linear optical realisation of qubit purification with quantum amplitude damping channel. *Chinese Physics Letters*, 24:1809, 2007. 39, 40, 41

[34] T. C. Ralph and A. P. Lund. Nondeterministic noiseless linear amplification of quantum systems. In *Proceedings of 9th International Conference on Quantum Measurement and Computing*, pages 155–160. AIP, New York, 2009, 2008. 43, 44

[35] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn. Simple scheme for efficient linear optics quantum gates. *Phys. Rev. A*, 65:012314, 2002. 15

[36] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, 1994. 14, 31

[37] T. Rudolph and J. W. Pan. A simple gate for linear optics quantum computing. arXiv:quant-ph/0108056v1. 15

[38] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83(1):33–80, Mar 2011. 57

[39] S. Scheel, W. J. Munro, J. Eisert, K. Nemoto, and P. Kok. Feed-forward and its role in conditional linear optical quantum dynamics. *Phys. Rev. A*, 73(3):034301, Mar 2006. 15

[40] Stefan Scheel and Norbert Lütkenhaus. Upper bounds on success probabilities in linear optics. *New Journal of Physics*, 6(1):51, 2004. 15

[41] P. W. Shor. *SIAM J. Comput.*, 26:1484, 1997. 1