Implementing quantum gates and channels using linear optics

by

Kent Fisher

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

Waterloo, Ontario, Canada, 2012

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

This thesis deals with the implementation of quantum channels using linear optics. We begin with overviews of some important concepts in both quantum information and quantum optics. First, we discuss the quantum bit and describe the evolution of the states via quantum channels. We then discuss both quantum state and process tomography, methods for how to determine which states and operations we are experimentally implementing in the lab. Second, we discuss topics in quantum optics such the generation of single photons, polarization entanglement, and the construction of an entangling gate.

The first experiment is the implementation of a quantum damping channel, which intentionally can add a specific type and amount of decohering noise to a photonic qubit. Specifically, we realized a class of quantum channels which contains both the amplitude-damping channel and the bit-flip channel, and did so with a single, static, optical setup. Many quantum channels, and some gates, can only be implemented probabilistically when using linear optics and postselection. Our main result is that the optical setup achieves the optimal success probability for each channel. Using a novel ancilla-assisted tomography, we characterize each case of the channel, and find process fideilities of 0.98 ± 0.01 for the amplitude-damping channel and 0.976 ± 0.009 for the bit-flip.

The second experiment is an implementation of a protocol for quantum computing on encrypted data. The protocol provides the means for a client with very limited quantum power to use a server's quantum computer while maintaining privacy over the data. We perform a quantum process tomography for each gate in a universal set, showing that only when the proper decryption key is used on the output states, which is hidden from the server, then the action of the quantum gate is recovered. Otherwise, the gate acts as the completely depolarizing channel.

Acknowledgements

First, I would like to thank my supervisor Kevin Resch. He is a fantastic physicist and teacher, and I am very grateful to have been able to study and research under his guidance. I am excited to continue working in his group during my PhD. I would like to thank the other members of my advising committee, Norbert Lütkenhaus and Joseph Sanderson, as well as Raymond Laflamme for sitting on my examining committee.

Laboratory research is very much a team sport, and so I would like to thank the other members of the Quantum Information and Quantum Optics group, both past and present, for their continual help in the lab. I thank Jonathon Lavoie, Deny Hamel, Krister Shalm and Robert Prevedel for their advice and patience as I learned the ins and outs of quantum optics experiments. I would also like thank Mike Mazurek, John Donahue and Chris Erven, who are always glad to help out and bounce ideas off of.

During the second half of my Master's, I performed the experiment for a protocol designed by Anne Broadbent. I would like to thank Anne for her help as I learned the finer details of the protocol, and also for her patience with the inevitable delays that accompany experiments.

On countless occasions I have needed technical help with certain components in the lab. Rainer Kaltenbaek deserves thanks for laying so much of the groundwork in the lab, particularly with LabView coding. He continues to help from afar. Also, Zhizhong Yan tirelessly helped me in setting up the Pockels cells. It is a very frustrating job, and I am very grateful to him.

I would like to acknowledge the agencies which have provided funding for the experiments which I have been able to work on. These are Ontario Ministry of Research and Innovation ERA, QuantumWorks, NSERC, OCE, Industry Canada and CFI. I would also like to thank NSERC and OGS, who personally funded me during my Master's.

Lastly, I would like to thank my family and friends. Their goodness and prayers have carried me through both joyful and hard times. I treasure their love and support.

By wisdom a house is built, and through understanding it is established; through knowledge its rooms are filled with rare and beautiful treasures.

– *Proverbs 24:3-4*

If I can fathom all mysteries and all knowledge but do not have love, then I am nothing.

– *1 Corinthians 13:2*

My goal is that we may be encouraged in heart and united in love, so that we may have the full riches of complete understanding, in order that we might know the mystery of God, namely Christ, in whom are hidden all the treasures of wisdom and knowledge.

– *Colossians 2:2-3*

Table of Contents

List of Figures

Chapter 1

Quantum Information Background

1.1 Introduction

Quantum computing offers great promise in solving complex problems. Problems such as factoring large numbers, searching, and simulating complex quantum systems find solutions in the ever-nearing quantum computer. One of the biggest hurdles in the way of a fully functional quantum computer is decoherence. Decoherence is the unwanted interaction between a quantum system and its surrounding environment, resulting in the loss of information. This thesis presents two experiments done using linear optics, which is an ideal testbed for quantum information. The first shows the construction of a damping channel, which intentionally adds a highly controllable amount *and* type of decohering noise to our precious quantum information. This is to further our understanding of decoherence in various implementations of quantum information processing and move towards correcting for it. The second experiment shows the realization of a cloud quantum computing protocol. The motivation for a client-server model stems from the realization that the difficulty in implementing large scale quantum computers will limit their widespread availability. The experiment shows how a client can securely use a server's quantum computer, themselves only needing a small amount of quantum information processing capability.

This thesis is comprised of five chapters. In this first chapter we will cover some of the necessary quantum information theory background. In Chapter 2 we will move to discussing how some of these concepts are implemented using quantum optics. In Chapter 3 we show the experiment for the optimal construction of a quantum damping channel. In Chapter 4 we discuss the second experiment, where one can perform quantum computations

on encrypted data. We will then conclude in Chapter 5, and discuss technical details in the Appendices.

1.2 The Qubit

A quantum bit, or qubit, is the elementary unit of quantum information. A qubit can be defined as a superposition of a two-level quantum system,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1 \tag{1.1}$$

This is called a *pure state*. The states $|0\rangle$ and $|1\rangle$ are unit vectors in a Hilbert space $\mathcal{H}$: $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$, respectively. They are referred to as the computational basis states, and form an orthonormal basis in this vector space. Important physical observables of the two-level quantum system are the Pauli operators:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.2}$$

Now suppose you are given some quantum state and are told that it is $|\psi\rangle$ with probabilty p, or $|\phi\rangle$ with probability $1-p$. This is an example of a *mixed state* and cannot be described as the pure states we outlined above. We describe mixed states using the density matrix, ρ, which is general. A density matrix is a $d \times d$, positive semi-definite, Hermitian matrix which has a trace equal to 1. Here, d is the dimension of the Hilbert space of the considered physical system ($d = 2$ for a single qubit, $d = 4$ for two qubits, *etc.*). The density matrix can be written as the statistical mixture of the outer product of pure states.

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad \sum_i p_i = 1 \tag{1.3}$$

Another useful way to view a single qubit is using the Bloch sphere representation. Here, we can rewrite the density matrix in components of the three Pauli matrices X, Y and Z. It is straightforward to verify that

$$\rho = \frac{1}{2}(\mathbb{1} + \mathrm{Tr}(\rho X)X + \mathrm{Tr}(\rho Y)Y + \mathrm{Tr}(\rho Z)Z) \tag{1.4}$$

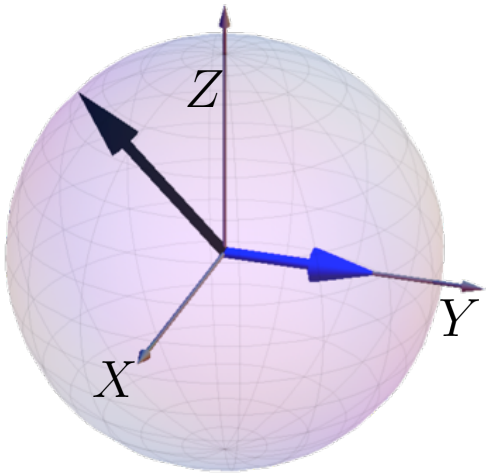


Figure 1.1: The Bloch sphere has axes which correspond to the Pauli matrices, with their eigenstates at the poles. Single qubit states are vectors in the unit sphere, with pure state vectors (black) reaching the surface of the sphere, and mixed state vectors (blue) having magnitude < 1.

Now consider a space where the basis is the set of Pauli matrices. It can be shown that each Pauli matrix is orthogonal to every other under the Hilbert-Schmidt inner product, $(A, B) \equiv \mathrm{Tr}(A^\dagger B)$. Then multiplying ρ by a Pauli matrix and taking the trace gives us the projection of ρ onto one of the axes. In this way we can define a vector in our space of Pauli matrices which completely represents the quantum state. Fig. 1.1 shows a the state vector on a Bloch sphere. The surface of the Bloch sphere contains the pure states, whereas mixed states fill the volume. The sphere then represents the set of states available through single-qubit quantum processes.

Note that in this thesis we are concerned with quantum information encoded in the polarization of single photons. We associate $|0\rangle$ with $|H\rangle$ (horizontal) and $|1\rangle$ with $|V\rangle$ (vertical), the linear polarizations of light. The reader should then be put on notice that the terms qubit and photon may be often used interchangeably.

1.3 Entanglement

Quantum entanglement is the greatest mark of the departure between quantum and classical views of the physical world. It was with entanglement that John Bell showed how we

must leave behind our traditional notion of locality [9], and it is with entanglement that quantum computers will provide dramatic increases in power over their classical counterparts.

We will define entanglement using two qubits, though the concept extends to arbitrary dimensions. Simply put, two particles are *entangled* if they are not *separable*. To properly define separability of states, and therefore entanglement, we must consider mixed states. Suppose ρ_A and ρ_B are density matrices describing the quantum states of the particles A and B. The particles are separable if the total quantum state ρ can be written as a convex sum of separable states

$$\rho = \sum_i p_i \rho_{Ai} \otimes \rho_{Bi} \tag{1.5}$$

where $\otimes$ is the tensor product, $\sum_i p_i = 1$ and each $p_i > 0$. Once again, if the state cannot be written in this way then it is entangled.

For example consider two particles, A and B, in the Bell state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |1_B\rangle)$. Since it is not possible to factor the state into the form $|\Phi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, the state $|\Phi\rangle$ is entangled. Even if they are separated spatially, we can only think of the particles as a single quantum system and not individually. We will come across entangled photon pairs numerous times. In Chapter 2, we will briefly discuss the generation of entangled photon pairs, and in Chapter 3 we will use entangled photon pairs to characterize a single qubit quantum channels.

1.4 Quantum channels

A quantum channel, or process, describes the most general evolution of a quantum state in time and/or space. Quantum channels can include anything from the quantum gates that make up a quantum computer, to the noisy and imperfect transmission of quantum information from one party to another. Formally, a quantum channel can be defined as a completely positive and trace-preserving linear map. Essentially, this means that a quantum channel is mapping that takes a physical density matrix to another physical density matrix. The condition of complete positivity requires that the mapping takes density matrices to density matrices when including an arbitrarily large ancilla space. In order to better understand some of the work later on, particularly Chapter 3, it will be useful to spend some time looking at some of the different representations of quantum channels.

1.4.1 Kraus representation

One way to represent a quantum channel, $\mathcal{E}(\rho)$ is to describe the mapping as a sum of linear operators, called Kraus operators, which individually act from the left and right on the original density matrix ρ. For this reason it is also commonly called the operator sum representation. The quantum state after the quantum channel, ρ', is then

$$\rho' = \mathcal{E}(\rho) = \sum_i A_i \rho A_i^\dagger \tag{1.6}$$

where $\{A_i\}$ are the Kraus operators and have the condition that $\sum_i A_i^\dagger A_i = \mathbb{1}$. The amount of Kraus operators required for the channel depends on the process, up to a maximum of d^2 operators [52].

The most important quantum gates are unitary operations, meaning that if U is a unitary operation then $UU^\dagger = U^\dagger U = \mathbb{1}$. Quantum gates are then, as a consequence, unital processes, meaning that they map the maximally-mixed state, $\rho = \mathbb{1}/d$, to itself. Quantum gates require only one Kraus operator to describe the quantum process. An example of a single-qubit quantum gate is the Hadamard which can be written as the sum of Pauli X and Z operators, $H = (X + Z)/\sqrt{2}$.

A non-unital channel is a process which does not preserve the maximally-mixed state. An important example of this, and one which we will come back to in Chapter 3, is the amplitude damping channel, which has Kraus operators

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}, \tag{1.7}$$

The channel models, for example, the excited state of the two-level system decaying to the ground, and so γ represents the decay rate.

An example of a single-qubit quantum channel which requires all four Kraus operators is the completely depolarizing channel, which maps every input state to the maximally-mixed state. Its Kraus operators are given by the identity and the three Pauli operators, X, Y and Z. We will encounter the depolarizing channel more in Chapter 4 when we look at how to hide quantum states and operations from an eavesdropper.

1.4.2 Superoperator representation

Another common way to represent a quantum channel is using a superoperator, a $d^2 \times d^2$ matrix which is commonly written in the basis of Pauli matrices. We will see this representation much more when we discuss quantum process tomography. We will be using the terms superoperator, process matrix, and χ matrix interchangebly. The process matrix shares many properties with a density matrix. For instance, the process matrix is both Hermitian and positive semi-definite. The superoperator representation is also very convenient since for the single-qubit it gives the direct description of how a state's Bloch sphere coordinates change under the action of the channel. The superoperator can be derived simply from the Kraus operator representation by rewriting each Kraus operator in the basis of Pauli matrices.

$$\begin{aligned} \mathcal{E}(\rho) &= \sum_i A_i \rho A_i^\dagger \\ &= \sum_i \left(\sum_m e_{im} \tilde{E}_m \right) \rho \left(\sum_n e_{in}^* \tilde{E}^\dagger \right) \\ &= \sum_{mn} \chi_{mn} \tilde{E}_m \rho \tilde{E}_n^\dagger \end{aligned} \tag{1.8}$$

where $\chi_{mn} = \sum_i e_{im} e_{in}^*$. As an example, the process matrix for the amplitude damping channel of Eq. 1.7 is shown below.

$$\chi_{\text{AD}} = \begin{pmatrix} \frac{1}{4}\left(1+\sqrt{1-\gamma}\right)^2 & 0 & 0 & \frac{\gamma}{4} \\ 0 & \frac{\gamma}{4} & -\frac{i\gamma}{4} & 0 \\ 0 & \frac{i\gamma}{4} & \frac{\gamma}{4} & 0 \\ \frac{\gamma}{4} & 0 & 0 & \frac{1}{4}\left(-1+\sqrt{1-\gamma}\right)^2 \end{pmatrix} \tag{1.9}$$

where the basis is $\{\mathbb{1}, X, Y, Z\}$. Fig. 1.2 shows the action of the amplitude damping channel on the Bloch sphere as the amount of damping increases.

1.4.3 Choi matrix representation

The final representation of a quantum channel we will discuss is the Choi matrix. In the single qubit case, the Choi matrix is a two-qubit density matrix describing the resulting

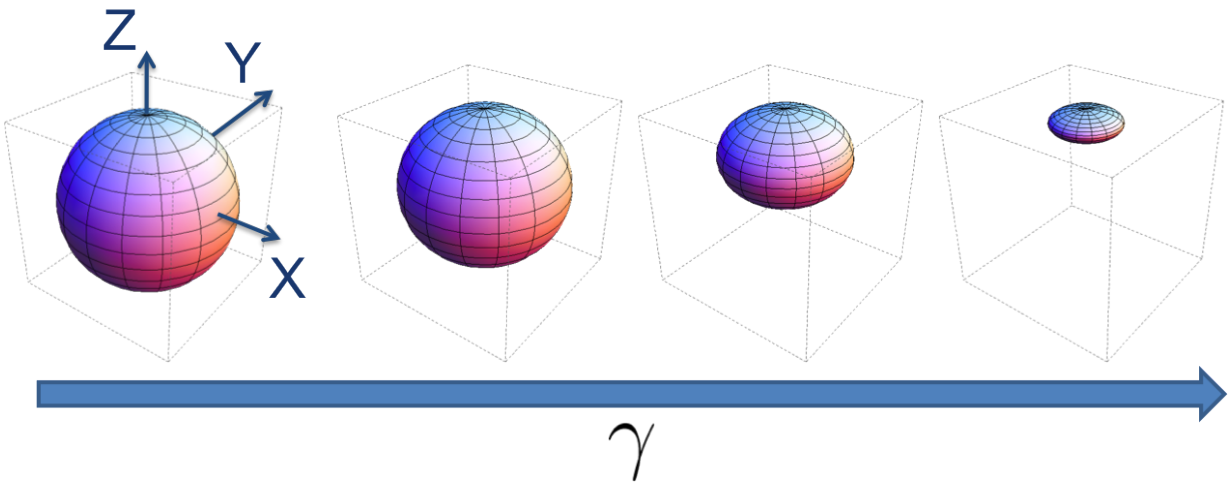


Figure 1.2: The Bloch sphere under the action of the amplitude channel, with increasing γ, the probability that $|1\rangle$ transitions to $|0\rangle$. As $\gamma \to 1$, the Bloch sphere shrinks towards the top pole, where the $|0\rangle$ state is situated.

state when the channel acted on one half of a maximally entangled state. It can be written as $\tau(\mathcal{E}) = (\mathcal{E} \otimes \mathbb{1})(|\Phi^+\rangle\langle\Phi^+|)$, where $\mathcal{E}$ is the quantum channel and $|\Phi^+\rangle$ is a maximally entangled state. It has been shown through the Choi-Jamiołkowski isomorphism [18, 45] that this description of a channel can be transformed to any of the other representations. The Choi matrix will come up again in Chapter 3, when we perform a process tomography on a single-qubit channel but using an entangled pair of photons. In our procedure, we first reconstruct the Choi matrix by doing a state tomography on $\tau(\mathcal{E})$ and then use it to find the superoperator χ.

1.5 Quantum state tomography

We are now in a position to outline how we can go about determining a density matrix ρ from experiment. We will assume that we have many identical copies of ρ available, which we justify in optical experiments by propagating many photons through the same optical setup. The goal is to measure ρ in each of the Pauli bases in order to determine the Bloch sphere vector components. For a single-qubit, we must make a minimum of four measurements, typically $\{|0\rangle, |1\rangle, |+\rangle, |+_y\rangle\}$, which we can think of as measuring the

projection onto each axis of the state vector on the Bloch sphere We need to measure both eigenstates in one of the bases in order to properly normalize the state. Using single photons as an example, we would need to measure in both $|0\rangle$ and $|1\rangle$ in order to know many detectable photons, N, are incident on the measurement apparatus. Knowing N we can then convert our measurements, which are numbers of photons, into probabilities and determine the projections onto each of the Bloch sphere axes. In actuality, we perform an overcomplete tomography, meaning that we measure each eigenstate for each of the Pauli bases. This has been shown to give more accurate results, since the amount of photons propagating through the setup can fluctuate over the time of measurement, skewing the normalization.

1.5.1 Maximum likelihood

Nielson and Chuang [52] describe a method to reconstruct the density matrix from experimental results using a linear inversion. However, following [40] we will, in later chapters, perform maximum likelihood estimations of density matrices. A density matrix $\rho(\vec{t})$ can be parametrized using $d^2 - 1$ independent real numbers thanks to normalization. For ease of calculation we normally use d^2 numbers for the parametrization: $\vec{t} = \{t_1, t_2, ..., t_{d^2}\}$. This is done by first defining a lower triangular matrix T, which for the single-qubit case is given by

$$T = \begin{pmatrix} t_1 & 0 \\ t_3 + it_4 & t_2 \end{pmatrix} \tag{1.10}$$

It can be shown that $\rho = T^\dagger T / \mathrm{Tr}(T^\dagger T)$ has all the properties required for a physical density matrix, for single-qubit or higher dimensional cases. We define n_i as the actual measured counts, and $\bar{n}_i = N\langle\psi_i|\rho(\vec{t})|\psi_i\rangle$ as the expected counts, given the density matrix $\rho(\vec{t})$, measurement basis $|\psi_i\rangle$, and N photons incident on the detectors. We assume that measured counts follow a Poissonian distribution, and so we make the approximation that the standard deviation in the measured counts $\sigma_i \approx \sqrt{\bar{n}_i}$. When N is large, the Poissonian distribution is approximately Gaussian. We can then calculate the probability of receiving the measured counts in all k bases, assuming that the probability of measuring n_i counts follows a Gaussian distribution centred around $\bar{n}_i$.

$$P(n_1, n_2, ..., n_k) = \frac{1}{N_{\mathrm{norm}}} \prod_{i=1}^{k} \exp\left[-\frac{(n_i - \bar{n}_i(\vec{t}))^2}{2\sigma_i^2}\right] \tag{1.11}$$

where N_{Norm} is a normalization constant and σ_i is the standard deviation in the i^{th} measurement. Substituting in $\bar{n}_i$ for the standard deviation, we obtain the likelihood that $\rho(\vec{t})$ produced the measured counts

$$P(n_1, n_2, ..., n_k) = \frac{1}{N_{\text{norm}}} \prod_{i=1}^{k} \exp\left[-\frac{(n_i - N\langle\psi_i|\rho(\vec{t})|\psi_i\rangle)^2}{2N\langle\psi_i|\rho(\vec{t})|\psi_i\rangle}\right] \tag{1.12}$$

As the name of the technique suggests, we want to find the parameters $\vec{t}$ which maximize this likelihood. Instead of maximizing P, it is an equivalent problem to maximize the logarithm of P, which is also equivalent to *minimizing* the following "likelihood" function:

$$\mathcal{L}(\vec{t}) = \sum_{i}^{k} \frac{\left[n_i - N\langle\psi_i|\rho(\vec{t})|\psi_i\rangle\right]^2}{2N\langle\psi_i|\rho(\vec{t})|\psi_i\rangle} \tag{1.13}$$

Minimizing this function over $\vec{t}$ gives the density matrix which most closely represents the actual quantum state in the experiment. In this thesis, restructed density matrices are found using the *NMinimize* function in *Wolfram Mathematica 8.0*.

1.5.2 Monte Carlo error analysis

The question arises of how to perform uncertainty analysis for the reconstructed density matrix. The method which is often used [53, 62], and which we also adopt for the work in this thesis, is to add Poissonian noise to the measured photons counts. We then perform many reconstructions of the density matrix from the adjusted counts in a Monte Carlo fashion, and can find the standard deviation of each density matrix element, or whichever measure desired. In order to analyze uncertainties in this way, we must make the assumption that the original number of photon counts measured is close to the mean, so that we are justified in adding statistical noise in this manner. By counting photons for long times and accumlating many counts we reduce the fractional error, which goes as $1/\sqrt{n_i}$.

1.6 Quantum process tomography

Characterizing quantum processes is of grave importance to implementing quantum technologies. In order to see how close to the ideal implemented gates function, we must

perform a quantum process tomography. Since we are aiming to reconstruct the process matrix χ, which shares all the same properties as a density matrix, we can take some lessons from quantum state tomography. We must still measure an input state in each of a complete set of bases, but now we must also prepare and send in a complete set of input states.

In total, the χ matrix for a process acting on a d-dimensional Hilbert space is described by $d^4 - d^2$ real parameters. We can see where the d^4 amount comes from using the property that a Hermitian matrix cans be constructed using a single triangular matrix and its adjoint. Explicitly, if T is a lower triangular matrix then $TT^\dagger$ is a Hermitian matrix. A triangular matrix, where diagonal elements are constrained to be real, is desribed by a total of d^4 real parameters. Adding the constraint that a process matrix must be trace preserving leaves us with $d^4 - d^2$ real parameters to describe χ [52].

1.6.1 Maximum likelihood

In [52], a method for performing quantum process tomography is outlined using a linear inversion. As in state tomography, the issue arises in this technique where the linear inversion may output a χ matrix that has trace of greater than one, and therefore cannot be a physical mapping. For this reason we turn to a maximum likelihood technique, as for the quantum state tomography, and search for the physical χ matrix which most closely describes the observed measurement results. Following the same logic as the appendix of [19], we will denote n_{ab} as the number of measured counts for the a^{th} input state and b^{th} measurement setting. We can then define the number of expected counts that are output from the quantum channel as $\bar{n}_{ab}$. Since we can write the action of the channel acting on an input state ρ_a as $\mathcal{E}(\rho_a) = \sum_{mn} \chi_{mn} \tilde{E}_m \rho_a \tilde{E}_n^\dagger$, the expected counts are $\bar{n}_{ab} = N\text{Tr}(|\psi_b\rangle\langle\psi_b|\mathcal{E}(\rho_a))$. We define the likelihood function $\mathcal{L}$ in the same way as for state tomography, with one addition. We add a Lagrange multiplier term λ to enforce physical contraints of the χ matrix. Recall that for a physical channel, we require that the Kraus operators $\{E_i\}$ have the relation $\sum_i E_i^\dagger E_i = \sum_{mn} \chi_{mn} \tilde{E}_n^\dagger \tilde{E}_m = \mathbb{1}$. Multiplying both sides by $\tilde{E}_k$ and taking the trace, we can see that $\sum_{mn} \chi_{mn} \text{Tr}(\tilde{E}_n^\dagger \tilde{E}_m \tilde{E}_k) - \text{Tr}(\tilde{E}_k) = 0$, where k runs from 1 to d^2. The likelihood function we seek to minimize takes the form

$$\mathcal{L} = \sum_{ab} \frac{\left[n_{ab} - N \sum_{mn} \chi_{mn} \text{Tr}(|\psi_b\rangle\langle\psi_b| \tilde{E}_m \rho_a \tilde{E}_n^\dagger)\right]^2}{2N \sum_{mn} \chi_{mn} \text{Tr}(|\psi_b\rangle\langle\psi_b| \tilde{E}_m \rho_a \tilde{E}_n^\dagger)} + \lambda \sum_k \left(\sum_{mn} \chi_{mn} \text{Tr}(\tilde{E}_n^\dagger \tilde{E}_m \tilde{E}_k) - \text{Tr}(\tilde{E}_k) \right)^2 \quad (1.14)$$

1.6.2 Ancilla-assisted process tomography

So far we have discussed process tomography where we must input at least d^2 to the quantum channel, and perform d^2 measurements on each. For a single-qubit quantum channel, this makes 4 measurements on 4 input states. Using a second, ancilla, qubit we can shift the work from both preparing and measuring states, to only measurement. By preparing a two-qubit state, ρ_{AB}, and sending one qubit through the quantum channel $(\mathcal{E} \otimes \mathbb{1})(\rho_{AB})$, reconstructing the process $\mathcal{E}$ requires just $d^4 = 16$ measurements on this joint state. We can then perform a maximum likelihood estimation of the process matrix in the same way as outlined above, only now there is one input state and we only sum over measurement settings. It is not necessary for the characterization, but it has been shown that having entanglement between the two qubits of the input state gives better defined results [3]. Using a maximally entangled input state, one actually can perform a state tomography on the output state from the channel, obtaining the Choi matrix for the process. We will use this in Chapter 3, adapting the technique according to the reality of having imperfect resources states to input to the channel.

1.6.3 Monte Carlo error analysis

The uncertainty analysis for the reconstructed process matrix follows the same logic as for the density matrix in the above section. We add Poissonian noise to the measured counts and perform many process tomography reconstructions. We then get an estimate of the uncertainty in the χ matrix, and figures of merit such as the process fidelity, which we discuss in the next section.

1.7 Distance measures

In both Chapters 3 and 4, we will measure quantum states and processes. In order to compare experimental findings to what is expected, it will be useful for us to lay out some quantitative ways [29] to distinguish between ideal and actual quantum states, or processes.

1.7.1 State fidelity

Defined by Jozsa in [41], the measure of the fidelity between two quantum states follows the same intuition as the overlap between two states $|\psi\rangle$ and $|\phi\rangle$, but generalized to mixed states. For two states ρ and σ the quantum state fidelity is defined as

$$F(\rho,\sigma) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2 \tag{1.15}$$

It can be seen that $F = 1$ when ρ and σ are equal, and that $F = 0$ when ρ and σ are orthogonal states. This measure is useful because more often than not, we are wanting to compare an experimentally found density matrix ρ against some pure state $|\psi\rangle$. The fidelity then simplifes as

$$\begin{aligned} F(|\psi\rangle,\rho) &= \left(\mathrm{Tr}\sqrt{\langle\psi|\rho|\psi\rangle \cdot |\psi\rangle\langle\psi|}\right)^2 &(1.16)\\ &= \langle\psi|\rho|\psi\rangle &(1.17)\end{aligned}$$

which is the overlap between $|\psi\rangle$ and ρ.

1.7.2 Process fidelity

The process fidelity is a distance measure between two quantum processes. It is defined as

$$F(\chi_1,\chi_2) = \left(\mathrm{Tr}\sqrt{\sqrt{\chi_1}\chi_2\sqrt{\chi_1}}\right)^2 \tag{1.18}$$

This measure is often quoted against an ideal case when trying to implement a quantum gate. Similar to the state fidelity, when comparing against a unital channel, the fidelity simplifies to the overlap of the χ matrices. However, if we are looking at an implementation of a non-unital channel, as we will in Chapter 3, the process fidelity lacks this operational meaning when comparing experimental and ideal cases. For this we must turn to another distance measure.

1.7.3 Trace distance

The trace distance between two quantum states ρ and σ is defined as

$$D(\rho,\sigma) = \frac{1}{d}\mathrm{Tr}\left|\rho-\sigma\right|, \tag{1.19}$$

where d is the dimension of the Hlibert space ($d = 2$ for a single qubit), and $|M| = \sqrt{M^\dagger M}$. Note that here $D = 0$ when the states ρ and σ are equal, and has a maximum of $D = 1$ when the states are orthogonal. We are interested in how to compare two quantum channels $\mathcal{E}_A$ and $\mathcal{E}_B$, so we look at the maximum trace distance measure. For this we input a state ρ into both channels and find the resulting states $\rho'_A = \mathcal{E}_A(\rho)$ and $\rho'_B = \mathcal{E}_B(\rho)$. Then we can take the trace distance between ρ'_A and ρ'_B, which gives us a measure of the probability of distinguishing between the two states, and therefore the probability of distinguishing between the two channels for the state ρ. We then maximize this quantity over all possible input states ρ. Operationally, this means that we have found the highest probability of telling the two channels apart using the best possible input state. At first glance, this maximization problem seems daunting since even for a single-qubit channel, maximizing over the Bloch sphere volume is difficult. Thankfully, the state which maximizes the trace distance will always be pure, reducing the computational problem dramatically.

Chapter 2

Quantum optics background

2.1 Introduction

In this chapter we will develop some of the quantum optics tools required to perform the types of experiments coming in later chapters. We will briefly overview concepts such as spontaneous parametric downconversion, entanglement generation, birefringence, Hong-Ou-Mandel interference and Pockels cells. Lastly, we will, in some detail, go through the experimental setup for an optical CNOT gate.

We use the polarization of the light field to define our notion of information. Light can be linearly, or circularly polarized (Fig. 2.1). We use the horizontal polarization ($|H\rangle$), defined as being in the plane of the optical table, as the logical state $|0\rangle$. The vertical polarization, $|V\rangle$, is the logical $|1\rangle$.

Then the diagonal polarization, $|D\rangle$, is $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and the anti-diagonal polarization, $|A\rangle$, is $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. These are the eigenstates of the Pauli X operator. Lastly, the left-circular polarization, $|L\rangle$, is $|+_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, and the right-circular polarization, $|R\rangle$, is $|-_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. These are the eigenstates of the Pauli Y operator. Of course, nothing about this information encoding is quantum yet. Polarization optics using a matrix algebra formulation, such as Jones matrices or the Poincaré sphere, dates back well before the Bloch sphere was used to described spin orientations.

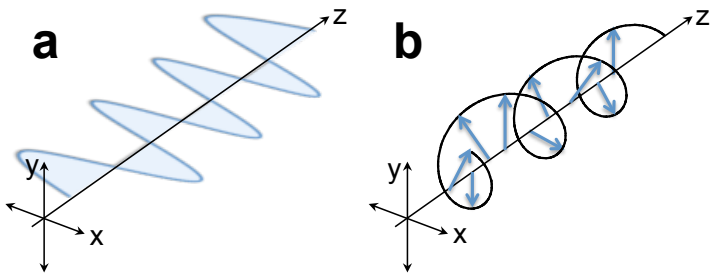


Figure 2.1: Linearly (a) and circularly (b) polarized light propagating in the z-direction. Blue arrows show the direction of the electric field at each point along the z-axis.

2.2 Generation of single photon entangled states

For the work presented in this thesis, we produce single photon states through a nonlinear optical process called spontaneous parametric downconversion (SPDC). Simply put, SPDC is a process whereby an incoming pump photon "splits" into two photons of lower energies, called the signal and idler (Fig.2.2a).

2.2.1 Spontaneous parametric downconversion

SPDC occurs in a nonlinear medium, meaning there is a nonlinear response of the medium's electric field to the electric field of the propagating light. The strength of this nonlinearity is given by the susceptiblity tensor $\vec{\chi}$. This is expressed through the polarization of the medium [12], $P(t) = \epsilon_0 \left[\chi^{(1)}E(t) + \chi^{(2)}E^2(t) + ...\right]$. Here we only consider nonlinear effects due to the $\chi^{(2)}$ term. For the two experiments in this thesis we use potassium titanyl phosphate (KTP), and barium borate (BBO), materials with $\chi^{(2)}$ nonlinearities large enough to be used for efficient downconversion.

SPDC is a quantum effect that the classical nonlinear optics theory does not account for. Classically, we would describe the process of downconversion as a three-wave mixing [51]. For this discussion, we will assume that the input field, called the pump, and two output fields, traditionally called signal and idler, are all plane waves travelling along the z-axis. Each field is then given by an electric field operator $\hat{E}_j^{(+)} = \mathcal{E}_j e^{i(k_j z - \omega_j t)}$, where $\mathcal{E}_j$ is the field amplitude and ω_j is its frequency. For signal, idler and pump field amplitiudes $\mathcal{E}_s, \mathcal{E}_i$, and $\mathcal{E}_p$, the respective coupled field equations for three-wave mixing in a $\chi^{(2)}$ medium are:

$$\frac{d\mathcal{E}_s}{dz} \propto \chi^{(2)}\mathcal{E}_i^*\mathcal{E}_p e^{-i\Delta kz} \tag{2.1}$$
$$\frac{d\mathcal{E}_i}{dz} \propto \chi^{(2)}\mathcal{E}_s^*\mathcal{E}_p e^{-i\Delta kz} \tag{2.2}$$
$$\frac{d\mathcal{E}_p}{dz} \propto \chi^{(2)}\mathcal{E}_s\mathcal{E}_i e^{i\Delta kz} \tag{2.3}$$

where Δk is the phase mismatch defined as $\Delta k = k_p - k_s - k_i$, and z is the distance along the medium which in this case is a non-linear crystal. Now, for downconversion we initially only have amplitude in the pump field $\mathcal{E}_3$, and $\mathcal{E}_1 = \mathcal{E}_2 = 0$. From the equations above, we have that all three derivatives are equal to zero, and so no intensity can build up in the signal and idler modes over the length of the crystal. It is for this reason that we must turn to a quantum mechanical description of downconversion. The interaction Hamiltonian is [36]

$$\mathcal{H}_{\text{int}} = -\frac{\epsilon_0}{3}\chi^{(2)}\int_V dV\, \hat{E}_p^{(+)}\hat{E}_s^{(-)}\hat{E}_i^{(-)} + \hat{E}_p^{(-)}\hat{E}_s^{(+)}\hat{E}_i^{(+)} \tag{2.4}$$

where ϵ_0 is the vacuum permittivity, V is the crystal volume in which the interaction is taking place. For the quantum process we must first quantize the electric fields, such that they describe single photon propagation. For simplicity, we will assume the three fields are all plane waves occupying single modes, and propagating in the positive z direction. Taking the signal and idler modes to be initially in the vacuum state, and the pump mode to be a coherent state $|\alpha\rangle$, the state $|\psi(t=0)\rangle = |\alpha\rangle_p|0\rangle_s|0\rangle_i$ evolves under the interaction Hamiltonian as

$$\begin{aligned} |\psi(t)\rangle &= e^{-i\mathcal{H}_{\text{int}}t/\hbar}|\alpha\rangle_p|0\rangle_s|0\rangle_i \\ &= |\alpha\rangle_p|0\rangle_s|0\rangle_i + i\frac{\epsilon_0\chi^{(2)}t}{3\hbar}\int_0^t dt' \int_V dV\, \hat{E}_p^{(+)}\hat{E}_s^{(-)}\hat{E}_i^{(-)}|\alpha\rangle_p|0\rangle_s|0\rangle_i + ... \end{aligned} \tag{2.5}$$

where higher order terms will be heavily suppressed. Also, the second term in the interaction Hamiltonian, $\hat{E}_p^{(-)}\hat{E}_s^{(+)}\hat{E}_i^{(+)}$, will not contribute since the signal and idler modes are initally in the vacuum. We will focus on the first-order term from here on, since it shows the generation of single photons. We write quantized single-mode electric field operators as

$$E_j^{(+)} = i\sqrt{\frac{\hbar\omega_j}{2\epsilon_0 V}}a_j e^{i(k_j z-\omega_j t)} \tag{2.6}$$

where a_j is the annihilation operator for the j^{th} mode. We can rewrite the state evolution and drop the constant prefactors:

$$\begin{aligned} |\psi(t)\rangle &= \left(\frac{\hbar}{2\epsilon_0 V}\right)^{\frac{3}{2}}\sqrt{\omega_p\omega_s\omega_i}\frac{\epsilon_0\chi^{(2)}t}{3\hbar}\int_0^t dt'\int_V dV a_p a_s^\dagger a_i^\dagger e^{i(k_p z-\omega_p t')-i(k_s z-\omega_s t')-i(k_i z-\omega_i t')}|\alpha\rangle_p|0\rangle_s|0\rangle_i \\ &\propto t\int_0^t dt'\int_V dV\alpha e^{i(k_p-k_s-k_i)z}e^{-i(\omega_p-\omega_s-\omega_i)t'}|\alpha\rangle_p|1\rangle_s|1\rangle_i \end{aligned} \tag{2.7}$$

where single photons have been generated in the signal and idler modes. Since the time interval over which the interaction occurs is long compared to optical frequencies, we can make the approximation that

$$\lim_{t\to\infty}\int_0^t dt' e^{-i(\omega_p-\omega_s-\omega_i)t'} = 2\pi\delta(\omega_s+\omega_i-\omega_p) \tag{2.8}$$

which shows that the process conserves energy, $\omega_s+\omega_i=\omega_p$. Next we must discuss the remaining spatial integration $\int_V dV e^{i(k_p-k_s-k_i)z}$. This integration can be performed if we take the interaction volume to have sidelengths L_x, L_y, and L_z. It is clear to see that the integral is maximized when the phase mismatch term $\Delta k = k_p-k_s-k_i=0$. If we integrate over one direction, we can gain some intuition for how the strength of the interaction varies when $\delta K \neq 0$.

$$\begin{aligned} \int_0^{L_z} dz e^{i\Delta k_z z} &= \frac{i}{\Delta k_z}\left(1-e^{i\Delta k_z L_z}\right) \\ &= e^{i\Delta k_z L_z/2}(-i)\frac{2i}{\Delta k_z}\sin\left(\frac{\Delta k_z L_z}{2}\right) \\ &= e^{i\Delta k_z L_z/2}L_z\mathrm{sinc}\left(\frac{\Delta k_z L_z}{2}\right) \end{aligned} \tag{2.9}$$

The phase mismatch then deviates from the ideal as a product of three sinc functions, one in each direction.

Before moving on to further discussing phase matching, we should note that if we had kept the next-order term in the series expansion of $e^{-i\mathcal{H}_{\mathrm{int}}t/\hbar}$ we would have found a term

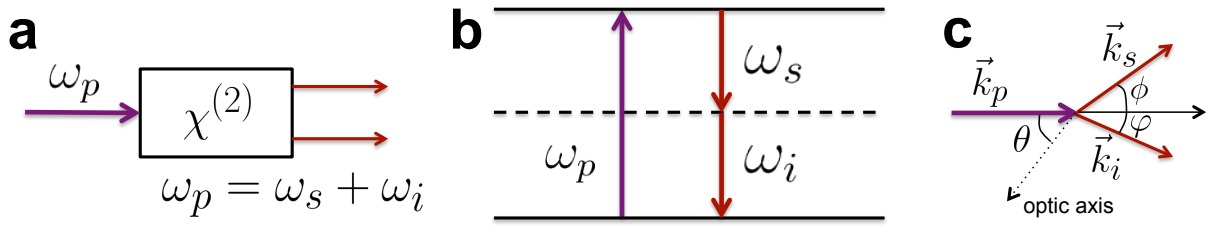


Figure 2.2: (a) A cartoon of the SPDC process in a material with a $\chi^{(2)}$ nonlinearity. Energy is conserved in the process. (b) shows the absorption of a pump photon at frequency ω_p and the spontaneous emission of signal and idler photons at frequencies ω_s and ω_i. (c) shows the conservation of momentum between pump and downconverted photons. Angle tuning (changing θ) allows for variety in signal and idler momenta and wavelengths. Downconverted photons are emitted at angles ϕ and φ from the pump propagation (for co-linear phase matching these angles are both ≈ 0).

which describes two photons generated in the each mode. We call these *"double pairs"* and can be detrimental to experiments based off of postselecting on coincident photon detections, since they can trigger false counts. For this reason we often reduce the pump power while performing experiments to observe higher fidelity quantum operations.

2.2.2 Phase matching

As stated above, $\Delta k = k_p - k_s - k_i$ is the phase mismatch, which we want to minimize. This can be achieved by phase matching techniques such as angle tuning (Fig. 2.2c), as is the case when using BBO, or temperature tuning for KTP. We also use a periodically-poled KTP crystal (PPKTP) to further compensate for the phase mismatch through quasi-phase matching. The idea behind periodic poling is that over the length of the KTP crystal the pump phase oscillates (Fig.2.3a), reducing the downconversion efficiency. However, if after some characteristic length in the material, $\Lambda/2$, we flip the crystal's orientation, the pump is brought back into phase (Fig.2.3b). Performing these flips, called periodic poling, along the entire length of the crystal keeps the pump beam in phase, and allows the downconversion efficiency to continually increase. In practice, the orientation of the crystal is periodically flipped on the micrometer scale by applying a strong electric field.

It is also necessary to quickly discuss the polarization of the downconverted photons. There are two types of phase matching, which will depend on the birefringence of the

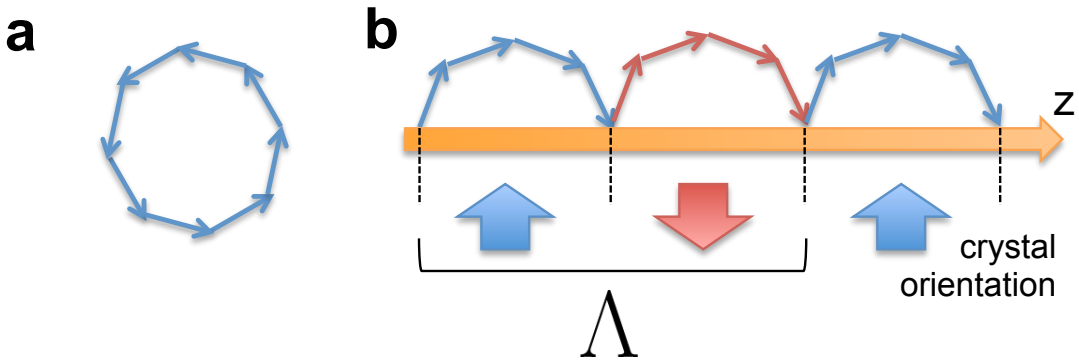


Figure 2.3: (a) Phasor diagram of the pump propagating through the crystal without quasi-phase matching. (b) With quasi-phase matching, the crystal orientation is flipped each half cell, $\Lambda/2$, reversing the phase.

nonlinear material. Type I downconversion emits signal and idler photons with the same polarization, which is opposite to that of the pump, $|H\rangle_p \rightarrow |V\rangle_s|V\rangle_i$. We use type I downconversion with a BBO crystal for the experiment in Chapter 4. Type II downconversion emits signal and idler photons with opposite polarizations, $|H\rangle_p \rightarrow |H\rangle_s|V\rangle_i$. We use type II downconversion for the experiment in Chapter 3, along with an additional condition that the signal and idler photons are emitted collinearly ($\phi, \varphi \approx 0$ in Fig. 2.2c).

2.2.3 Polarization entanglement

In Chapter 3, we use a source of photons, entangled in polarization, to characterize a quantum channel. It is useful for us to review how these entangled states are generated. We use a Sagnac interferometer, shown in Fig. 2.4. The polarization of the pump is set using a half- and quarter-wave plate (HWP and QWP). First suppose that the pump is H-polarized. It will then propagate around the interferometer in the counterclockwise direction. If it downconverts (type II colinear) in the PPKTP crystal, the resulting state is $|H\rangle_s|V\rangle_i$. The photons then pass through the HWP at 45°, and are split into different spatial modes by the polarizing beam splitter (PBS) giving the state $|H\rangle_1|V\rangle_2$, where the subscripts refer to the spatial modes. Now suppose the pump is V-polarized. It then propagates clockwise around the interferometer, is flipped to horizontal polarization by the HWP, and then downconverts to $|H\rangle_s|V\rangle_i$. The photons are separated into spatial modes by the PBS, but this time the resulting state is $|V\rangle_1|H\rangle_2$. Finally, suppose the pump is set to the diagonal polarization $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$. It then propagates around the

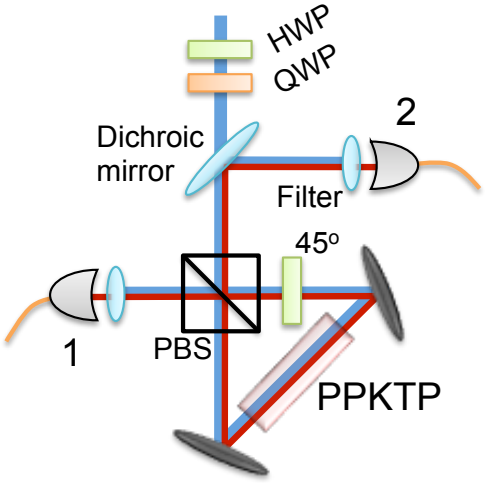


Figure 2.4: A PPKTP crystal placed in a Sagnac interferometer. By controlling the polarization state of the blue pump beam, the downconverted two-photon state can be tailored, and entanglement can be generated.

interferometer in both directions, such that if we detected a downconverted photon pair, we do not know through which direction of the crystal the process occured, and consequently we have generated the entangled state $\frac{1}{\sqrt{2}}(|H_1V_2\rangle + |V_1H_2\rangle)$.

2.3 The beamsplitter and Hong-Ou-Mandel interference

The beamsplitter is of fundamental importance in quantum optics as it allows for interaction between different spatial modes. We describe a beamsplitter using ladder operators for each mode, see Fig. 2.5a. The beamsplitter transforms the ladder operators based on its reflectance and transmittance. They transform as

$$\begin{aligned} a &\mapsto tc + rd \\ b &\mapsto td - rc \end{aligned} \tag{2.10}$$

where r and t are complex numbers with the condition that $|r|^2 + |t|^2 = 1$. We also commonly use polarizing beamsplitters (PBS), which transmit H-polarized light, while

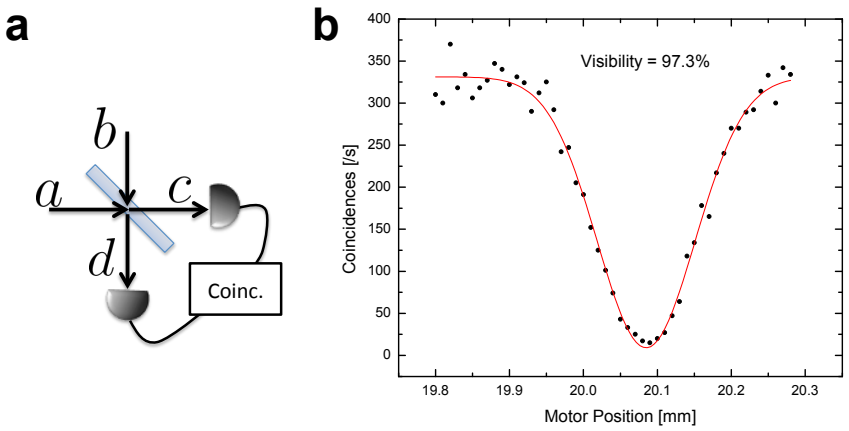


Figure 2.5: (a) A simple HOM inteferometer. A beamsplitter maps photons in input modes a and b to output modes c and d. Simultaneous detections of photons in both output modes triggers the coincidence logic. (b) Detected coincidence counts when changing the path length of input mode a. HOM interference occurs when the path lengths are matched, as shown by the dip.

reflecting V-polarized light. The beamsplitter is often used in describing different interference effects in optics. It is at the heart of the Michelson and Hanbury-Brown-Twiss interferometers. In a later section, we will look at the implementation of a two-photon entangling gate, and so we will primarily be concerned with the Hong-Ou-Mandel (HOM) interferometer [37] (Fig. 2.5a). Photons enter the setup in modes a and b, described in the number state basis as $|\psi_{\text{in}}\rangle = |1_a, 1_b\rangle = a^\dagger b^\dagger |0,0\rangle$. Supposing that we have a 50:50 beamsplitter ($r = t = 1/\sqrt{2}$), the ladder operators a and b are mapped to c and d such that

$$\begin{aligned} |\psi_{\text{out}}\rangle &= \frac{1}{\sqrt{2}}(c^\dagger + d^\dagger)\frac{1}{\sqrt{2}}(d^\dagger - c^\dagger)|0,0\rangle \\ &= \frac{1}{2}\left((d^\dagger)^2 - (c^\dagger)^2\right)|0,0\rangle \\ &= \frac{1}{\sqrt{2}}\left(|0_c, 2_d\rangle - |2_c, 0_d\rangle\right) \end{aligned} \tag{2.11}$$

It can be seen that when the input photons arrive at the beamsplitter in the same time and interference occurs, we get photon bunching, and have no coincidence photons between

modes c and d. If we record coincidence counts while varying one of the input photon path lengths, we then observe the HOM dip (Fig. 2.5b). A more general treatment shows that to observe interference photons must be indistinguishable in frequency, polarization, arrival time, and of course have overlap between output modes. We will discuss HOM interference again shortly when we look at the implementation of an optical CNOT gate.

2.4 Pockels cells

Pockels cells are comprised of a non-linear crystal which is quickly switched between two indices of refraction controlled by fast-switching high voltages. They are based off of the Pockels effect, where a strong electric field applied to a non-linear medium changes the effective index of refraction. In linear optics these cells can be used for fast-unitary operations in feed forwards systems, or to perform one-time pads for encrypting photonic qubits, as we do in Chapter 4.

The Pockels cells are driven by square waves voltages oscillating between high and low states, which then control the oscillation between two amounts of effective bifringence, $\pm\lambda/4$. A quarter-wave plate immediately after each Pockels cell shifts these rotations to 0 and $\lambda/2$, meaning that the Pockels cell either acts as the identity, or a half-wave plate at the angle of the crystal's orientation. Half-waves plates before and after each Pockels cell are used to set the angle of the half-wave rotation about an arbitrary axis in the x-z plane of the Bloch sphere. The crystals in each Pockels cell are aligned at $45 + \delta$ degrees to the plane of the optical table, where δ is small. For the experiment in Chapter 4, we use three Pockels cells to perform X, Hadamard, and Phase gates. In order to perform an X rotation, half-wave plate at 45 degrees, the additional HWPs are both then set to $\delta/2$ degrees.

$$\begin{aligned} \mathbb{1} &= \mathrm{HWP}(\theta = \delta/2) \cdot \mathrm{QWP}(\theta = \pi/4 + \delta) \cdot \\ &\quad \mathrm{PC}(\phi = -\lambda/4, \theta = \pi/4 + \delta) \cdot \mathrm{HWP}(\theta = \delta/2), \\ X &= \mathrm{HWP}(\theta = \delta/2) \cdot \mathrm{QWP}(\theta = \pi/4 + \delta) \cdot \\ &\quad \mathrm{PC}(\phi = \lambda/4, \theta = \pi/4 + \delta) \cdot \mathrm{HWP}(\theta = \delta/2) \end{aligned} \tag{2.12}$$

where the Pockels cell (PC) is modeled as a general waveplate with retardance ϕ and optic axis at angle θ. The second Pockels cell switches between performing the identity and the Hadamard gate. Here we want the HWPs before and after the Pockels cell to be at $11.5 \pm \delta$ degrees, and so it can similarly be shown

$$
\begin{aligned}
\mathbb{1} &= \mathrm{HWP}(\theta = 3\pi/16 + \delta/2) \cdot \mathrm{QWP}(\theta = \pi/4 + \delta) \cdot \\
&\quad \mathrm{PC}(\phi = -\lambda/4, \theta = \pi/4 + \delta) \cdot \mathrm{HWP}(\theta = 3\pi/16 + \delta/2), \\
H &= \mathrm{HWP}(\theta = 3\pi/16 + \delta/2) \cdot \mathrm{QWP}(\theta = \pi/4 + \delta) \cdot \\
&\quad \mathrm{PC}(\phi = \lambda/4, \theta = \pi/4 + \delta) \cdot \mathrm{HWP}(\theta = 3\pi/16 + \delta/2)
\end{aligned} \tag{2.13}
$$

The last Pockels cell switches between performing the identity and the Phase gate ($|0\rangle \mapsto |0\rangle, |1\rangle \mapsto i|1\rangle$). Because this is a quarter-wave rotation, we oscillate the voltage between $\pm\lambda/8$ and require an eighth-waveplate (EWP) afterwards, for which we can use a half-waveplate tilted to give the proper amount of birefringence. It is simple to verify that

$$
\begin{aligned}
\mathbb{1} &= \mathrm{EWP}(\theta = 0) \cdot \mathrm{HWP}(\theta = \pi/8 + \delta/2) \cdot \\
&\quad \mathrm{PC}(\phi = -\lambda/8, \theta = \pi/4 + \delta) \cdot \mathrm{HWP}(\theta = \pi/8 + \delta/2), \\
P &= \mathrm{EWP}(\theta = 0) \cdot \mathrm{HWP}(\theta = \pi/8 + \delta/2) \cdot \\
&\quad \mathrm{PC}(\phi = \lambda/8, \theta = \pi/4 + \delta) \cdot \mathrm{HWP}(\theta = \pi/8 + \delta/2)
\end{aligned} \tag{2.14}
$$

2.5 Optical CNOT gate

The controlled-NOT, or CNOT, gate is of critical importance to quantum computing, and is commonly used in the set of quantum gates required for universal computation [52]. The matrix for the CNOT operation is

$$
\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.15}
$$

The importance of the CNOT can be seen in its ability to entangle two initially separable qubits. For example, suppose a two-qubit state is initialized as $|+0\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, then the output state after applying a CNOT gate with the first qubit as the control is

$$
\mathrm{CNOT}|+0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.16}
$$

which is the maximally entangled state. To build a CNOT using linear optics requires the interaction of the two photonic qubits at some optical element. The scheme used for this project is shown in Fig. 2.6, and is derived from that shown in [42, 46, 53], which gives a gate success probability of 1/9. Photons meet at a partially-polarizing beam splitter (PPBS), where H-polarized light is fully transmitted, and V-polarized light is 1/3 transmitted and 2/3 reflected.

2.5.1 Partially-polarizing beamsplitters

Similar to the PBS we discussed earlier, the partially-polarizing beamsplitter (PPBS) performs the following mappings on the lowering operators:

$$\begin{aligned} a_H &\to c_H \\ a_V &\to \frac{1}{\sqrt{3}} c_V + \sqrt{\frac{2}{3}} d_V \\ b_H &\to d_H \\ b_V &\to \frac{1}{\sqrt{3}} d_V - \sqrt{\frac{2}{3}} c_V \end{aligned} \tag{2.17}$$

Now suppose two indistinguishable V-polarized photons arrive at the PPBS at the same time, one in mode a and one in mode b. Then the PPBS maps

$$a_V^\dagger b_V^\dagger |00\rangle_{ab} \to \frac{1}{3}(-c_V^\dagger d_V^\dagger - \sqrt{2} c_V^{\dagger 2} + \sqrt{2} d_V^{\dagger 2})|00\rangle_{cd} \tag{2.18}$$

When no interference occurs, the maximum probability of observing a coincident photons in each path is $\left(\frac{2}{3}\right)^2 + \left(\frac{1}{3}\right)^2 = \frac{5}{9}$. In the coincidence subspace, detecting one photon in each output mode, we see that the amplitude is 1/3 of the original, giving a reduction to a minimum of 1/9. The visibility of this HOM interference is calculated as follows,

$$\begin{aligned} \text{Vis} &= \frac{\text{Max} - \text{Min}}{\text{Max}} \\ &= \frac{5/9 - 1/9}{5/9} \\ &= 4/5 \end{aligned} \tag{2.19}$$

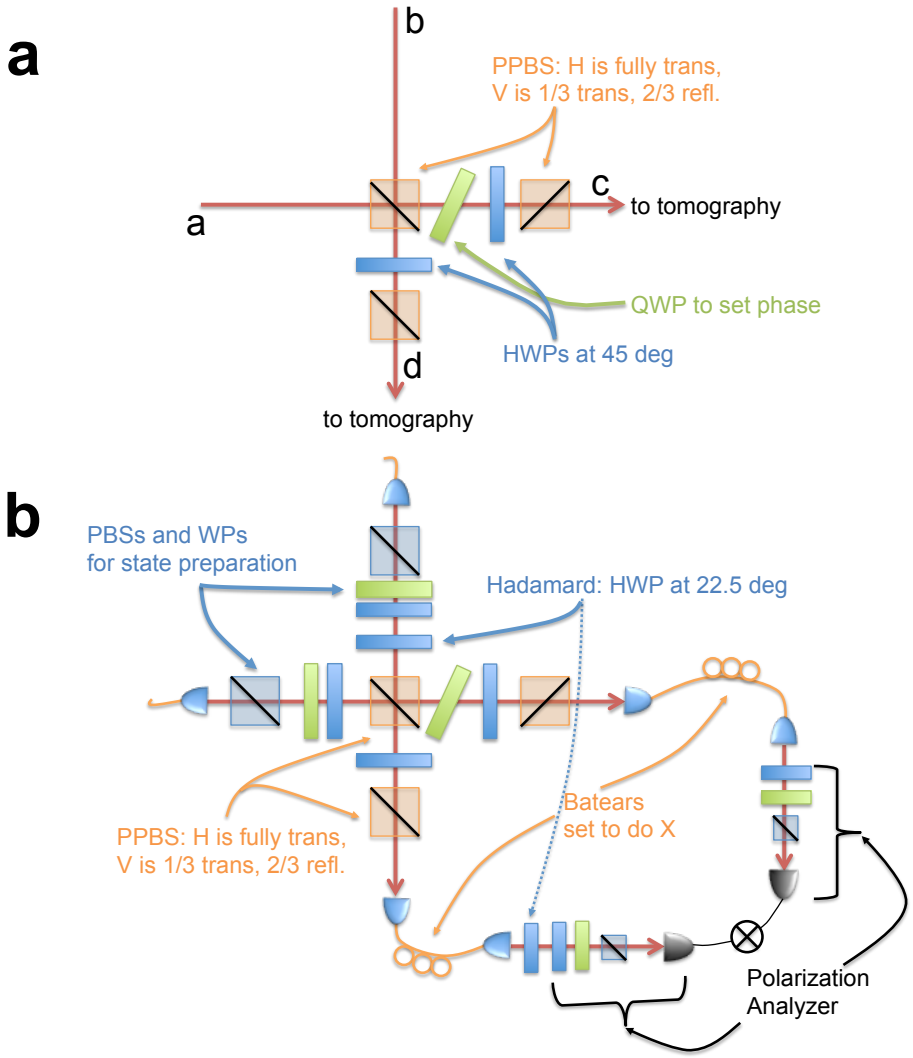


Figure 2.6: (a) Photons of indistinguishable frequency in input modes a and b interfere at the first PPBS. Polarizations are flipped using half-wave plates at 45 degrees. A tilted quarter-wave plate in one mode compensates for unwanted phases due to mismatched path lengths. Two further PPBSs normalize the output state in modes c and d. Post-selecting on coincidences in the c and d modes gives the desired output state with $1/3$ of the original amplitude. (b) Additional Hadamard and Pauli X components transform the setup into a CNOT gate. State preparation and analysis are performed using a PBS, quarter- and half-wave plate, and photons detected within a 3 ns window are recorded.

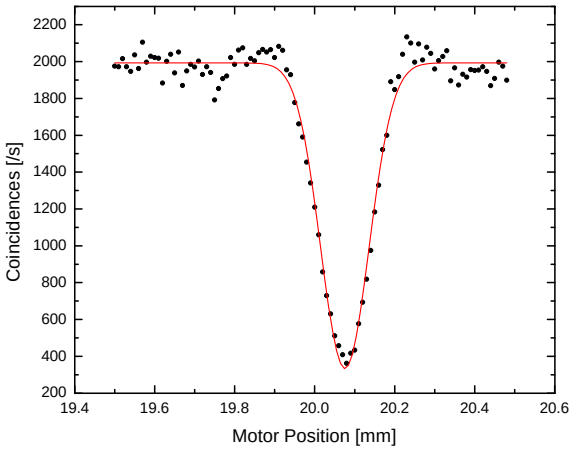


Figure 2.7: Measured coincidences in a 3 ns time window, where one input single-mode fibre coupler was mounted on a motorized stage, stepped at 0.01 mm interval, changing the relative delay between photon paths. Photons interfere and bunch at a PPBS when their path lengths are matched, showing a dip in coincidence counts. Dip visibility is $83 \pm 1\%$.

The PPPSs were purchased from Asahi and had actual reflectivities of 65.5%, 65.3% and 65.6%, where the primary PPBS is listed first followed by those in modes c and d respectively. This discrepancy from ideal reflectivity (2/3) changes the expected HOM dip visibility. For a general reflectivity for the V-polarized light r_V, and assuming the H-polarization is perfectly transmitted, the HOM visibility goes as

$$\text{Vis} = \frac{1}{1 - 2r_V(1 - r_V)} - 1 \tag{2.20}$$

Using the actual reflectivity for the first PPBS, we find the ideal visibility to be 82.5%. Fig. 2.7 shows a HOM dip scan where the state sent into the PPBS was $|VV\rangle$. The visiblility was found to be $83 \pm 1\%$.

2.5.2 Using the PPBS to generate entanglement

To see the entangling operation of the setup in Fig. 2.6a, consider one D-polarized photon in both a and b modes,

$$\begin{aligned} |\psi\rangle &= |DD\rangle \\ &= a_D^\dagger b_D^\dagger |00\rangle_{ab} \\ &= \frac{1}{\sqrt{2}}(a_H^\dagger + a_V^\dagger)\frac{1}{\sqrt{2}}(b_H^\dagger + b_D^\dagger)|00\rangle_{ab} \end{aligned} \tag{2.21}$$

Performing the first PPBS mapping and simplifying by postselecting on the coincidence basis, one photon in each of the c and d modes, we find

$$|\psi\rangle \to \frac{1}{2}\left(c_H^\dagger d_H^\dagger + \frac{1}{\sqrt{3}}c_H^\dagger d_V^\dagger + \frac{1}{\sqrt{3}}c_V^\dagger d_H^\dagger - \frac{1}{3}c_V^\dagger d_V^\dagger\right)|00\rangle_{cd} \tag{2.22}$$

Half-wave plates at 45 degrees then flip H and V polarizations, $H \leftrightarrow V$, and the state after the second set of PPBSs is

$$\begin{aligned} |\psi\rangle &\to \frac{1}{3}\cdot\frac{1}{2}\left(c_V^\dagger d_V^\dagger + c_V^\dagger d_H^\dagger + c_H^\dagger d_V^\dagger - c_H^\dagger d_H^\dagger\right)|00\rangle_{cd} \\ &= \frac{1}{3}\cdot\frac{1}{2}\left(-|HH\rangle + |HV\rangle + |VH\rangle + |VV\rangle\right) \end{aligned} \tag{2.23}$$

which is an entangled state. The factor of 1/3 corresponds to the success probabilty of the gate (1/9), while the rest of the state amplitude is lost when we postselect on coincidences in the two paths. However, the operation that the setup in Fig. 2.6a performs is not a CNOT. One can verify that its operation is given by the following matrix,

$$\mathbb{S} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{2.24}$$

This can be easily transformed into the CNOT gate (Fig. 2.6b) using Hadamards and Pauli X rotations. It is straightforward to see that

$$\mathrm{CNOT} = (\mathbb{1} \otimes \mathrm{H}) \cdot \mathbb{S} \cdot (\mathrm{X} \otimes \mathrm{X}) \cdot (\mathbb{1} \otimes \mathrm{H}) \tag{2.25}$$

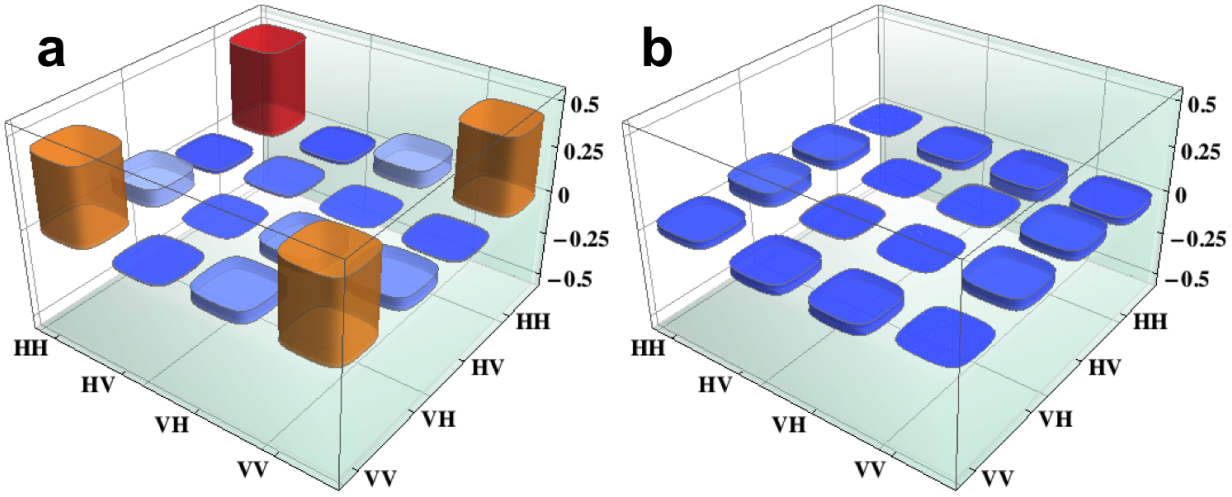


Figure 2.8: The real (a) and imaginary (b) parts of a density matrix reconstructed using a maximum likelihood quantum state tomography. Here, the state $|DH\rangle$ was sent into the optical setup. The resulting density matrix has quantum state fidelity of 0.893 with the $|\Phi^+\rangle$ Bell state.

2.5.3 Experimental setup

Photon pairs were generated by spontaneous parametric downconversion (SPDC) using a Titanium Sapphire (Ti:Saph) laser pulsed at 80 MHz to pump a 1 mm Barium Borate (BBO) crystal at 395 nm producing downconverted photons at 790 nm. Photons were propagated through the optical setup outlined in Fig. 2.6b, and were detected using silicon avalanche photo-diodes (PerkinElmer four-channel SPCM-AQ4C modules) and coincidence photons were counted with a timing window of 3 ns using a 16 channel logic unit.

2.5.4 Results

Preparing the state $|HD\rangle$, we expect to get out the $|\Phi^+\rangle$ Bell state. Fig. B.1 shows the reconstructed two-qubit density measured from the output of the CNOT setup compared with the ideal. The quantum state fidelity was calculated to be 0.893 ± 0.004, where the uncertainty was found using a Monte Carlo simulation adding Poissonian noise to the measured state tomography data.

In order to fully characterize the gate, an overcomplete process tomography was per-

formed, where each of the 36 two-qubit Pauli basis states were input to the setup and photon coincidence counts were measured in all 36 bases. Detailed results of this are shown in Chapter 4. The process fidelity between the ideal and experimental process matrices was found to be 0.869 ± 0.004.

Chapter 3

Optimal linear optical implementation of a single-qubit damping channel

3.1 Notes and acknowledgements

In this chapter we describe the implementation and characterization of a quantum channel which can controllably add a given amount *and* type of noise to a qubit. We build on the discussions of quantum channels and process tomography in Chapter 1, and use the entangled photon source outlined in Chapter 2. We show that the optical setup was realized in an optimal way, maximizing the probabilty of success of the channel.

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

K. A. G. Fisher, R. Prevedel, R. Kaltenbaek and K. J. Resch, Optimal linear optical implementation of a single-qubit damping channel. *New Journal of Physics*, **14**, 033016, 2012.

Author contributions

KF and **RP** performed the experiment and analyzed the data.

RK designed the experiment.

KR contributed to the design and realization of the experiment.

KF took primary responsibility for writing the first draft. **All authors** contributed to editing for the final version.

3.2 Abstract

We experimentally demonstrate a single-qubit decohering quantum channel using linear optics. We implement the channel, whose special cases include the familiar amplitude-damping channel and the bit-flip channel, using a single, static optical setup. Following a recent theoretical result [M. Piani *et al.*, Phys. Rev. A, **84**, 032304 (2011)], we realize the channel in an optimal way, maximizing the probability of success, i.e., the probability for the photonic qubit to remain in its encoding. Using a two-photon entangled resource, we characterize the channel using ancilla-assisted process tomography and find average process fidelities of 0.98 ± 0.01 and 0.976 ± 0.009 for amplitude-damping and the bit-flip cases, respectively.

3.3 Introduction

Time evolution in quantum mechanics converts a density matrix to another density matrix. This evolution is referred to as a quantum channel and can be described mathematically as a completely positive (CP) map [52]. Due to generality of the concept of quantum channels, their use is ubiquitous in quantum information. For example, unitary quantum channels are used in quantum computing to describe quantum gates. Non-unitary channels, on the other hand, describe the interaction of quantum states with an environment, and have recently been connected to fundamental physical questions in quantum information science, such as channel capacity, superadditivity [69, 33] and bound entanglement [38].

Linear optics and single photons have several characteristics that make them an ideal testbed for quantum information. Single-qubit unitaries are easy to implement as, for polarization encoded qubits, they only require waveplates. Photonic qubits also exhibit long decoherence times, and spontaneous parametric downconversion allows the generation of high-quality entangled states, which can be easily manipulated. However, certain operations, such as the two-qubit CNOT-gate, are difficult in this architecture [50, 48], and can only be implemented probabilistically [44, 59, 54].

Unfortunately, the ease of single-qubit operations does not extend to more general CP maps. Some quantum channels, like the depolarizing single-qubit channel [52] can

be implemented with unit probability, but this is not the case in general. For instance, the amplitude-damping channel, a non-unital quantum process, has been implemented in linear optics only with a limited success probability of 1/2 [58, 47]. In one experiment [2], the Kraus operators describing an amplitude-damping channel were implemented using a Sagnac interferometer such that all photons were transmitted. However, because the outputs from each Kraus operator were not coherently recombined on a beamsplitter, our notion of the success probability of a quantum channel does not apply to this case.

Recently, it was shown by Piani *et al.* [56] that, *any* single-qubit quantum channel could be implemented probabilistically using linear optics and postselection, i.e., similar to many two-qubit operations. Moreover, they derived an explicit formula for the optimal success probability.

In the present work, we use this recent theoretical result to design and demonstrate a linear-optics-based implementation of a certain class of non-unital single-qubit quantum channels called "damping channels". The class of channels we focus on can be parametrized by two real numbers: α and β. In the operator-sum representation, the channel's action on an arbitrary quantum state ρ can be written as $\mathcal{E}(\rho) = \sum_i A_i \rho A_i^\dagger$, where the two Kraus operators are [73]:

$$A_0 = \begin{pmatrix} \cos\alpha & 0 \\ 0 & \cos\beta \end{pmatrix}, A_1 = \begin{pmatrix} 0 & \sin\beta \\ \sin\alpha & 0 \end{pmatrix} \tag{3.1}$$

This channel is of great interest as its special cases include the amplitude-damping ($\alpha = 0$) and bit-flip ($\alpha = \beta$) channels, both of which are common sources of error in other implementations of quantum information processing, such as ion traps. Furthermore, it belongs to the small class of quantum channels for which the quantum capacity can be directly calculated via the coherent information [23].

Here, we experimentally realize this single-qubit damping quantum channel using linear optics. We can use the setup to add controlled amounts of noise of various types to a single qubit. The schematics of the experimental setup are shown in Figure 4.4. The key step in the implementation of the channel is the splitting of the polarization encoded information into different spatial modes, which then allows for the manipulation of different logical states independently of one another. An arrangement of half-wave plates and liquid-crystal retarders allows us to probabilistically implement both Kraus operators within a single, static optical setup. We characterize the channel using an ancilla-assisted quantum process tomography method, and show the optimality of our optical setup, with our success rates in the amplitude-damping case surpassing those of previous implementations [58, 47]. In order to characterize the action of the channel on entanglement we study the amount of entanglement of photon pairs when one photon is sent through the channel.

3.4 Optimality of the implementation

Following Ref. [56], it can be shown that the probability of success for a specific Kraus decomposition $\{A_i\}$ is $p_{\text{succ}}(\{A_i\}) = \left(\sum_i \|A_i\|_\infty^2\right)^{-1}$, where the norm $\|M\|_\infty$ is the largest singular value of the operator M. Maximizing over all possible Kraus decompositions A_i describing the channel allows one to achieve the optimal success probability $p_{\text{succ}}^{\text{opt}} = \max_{A_i} \frac{1}{\sum_i \|A_i\|_\infty^2}$. For our particular channel, if we assume that $\cos(\alpha) \geq \cos(\beta)$, this yields:

$$p_{\text{succ}}^{\text{opt}} = \frac{1}{\cos^2\alpha + \sin^2\beta} \tag{3.2}$$

In order to achieve $p_{\text{succ}}^{\text{opt}}$, each Kraus operator is implemented with individual probabilities $p_{A_i} = \|A_i\|_\infty^2 \cdot p_{\text{succ}}^{\text{opt}}$. We find that the optimal probability of success is achieved for $p_{A_0} = \frac{\cos^2\alpha}{\cos^2\alpha+\sin^2\beta}$ and $p_{A_1} = \frac{\sin^2\beta}{\cos^2\alpha+\sin^2\beta}$. We show experimentally that for various values of α and β, which can be independently controlled in our experiment, we indeed achieve this upper bound.

3.5 Ancilla-assisted process tomography

Quantum process tomography (QPT) allows one to experimentally reconstruct the superoperator describing an unknown physical process. Ancilla-assisted QPT (AAQPT) uses ancillary qubits to facilitate and reduce the reconstruction procedure to quantum state measurements only; AAQPT has been applied assuming that the initial state is perfect [3]. AAQPT provides us with the physical matrix that best describes the action of the experimentally channel and has been used to study various unitary quantum gates. However, it has not yet been extended to the characterization of non-unital channels which we address in our work. Here we describe and use a maximum likelihood approach for AAQPT that takes into account the imperfection of the input ancilla state (Maximum likelihood methods have been applied to standard quantum state and process tomography before [40, 53, 27, 39, 6, 49]). To our best knowledge, a maximum likelihood AAQPT technique which includes errors in the state preparation has not been implemented previously.

The standard techniques for QPT and AAQPT are described in [52, 40, 53, 19] and [3], respectively. Below, we outline our method following their nomenclature. Consider a two-qubit state, ρ_{AB}, whose density matrix is known; e.g., it might have been reconstructed using quantum state tomography (QST). The quantum channel $\mathcal{E}$ acts on subsystem A, while subsystem B is unaffected. The transformed two-qubit state after the channel is

$\rho'_{AB} = (\mathcal{E} \otimes \mathbb{1})(\rho_{AB})$. Characterizing ρ'_{AB}, e.g., by performing standard QST, allows for reconstruction of the quantum process using the Choi–Jamiołkowski isomorphism [18, 45].

The quantum process can be written as $\rho'_{AB} = \sum_{m,n=0}^{d^2-1} \chi_{mn}(\tilde{E}_m \otimes \mathbb{1})\rho_{AB}(\tilde{E}_n \otimes \mathbb{1})^\dagger$ where $\{\tilde{E}_i\}$ are operators which form a basis in the space of $d \times d$ matrices ($d = 2$ in our case). It is common to use the basis formed by the Pauli matrices $\{\mathbb{1}, X, Y, Z\}$. The d^2-dimensional process matrix χ then fully describes the quantum process. In our maximum-likelihood technique, we parameterize χ by $d^4 - d^2 = 12$ real numbers [40, 53, 27] and seek to minimize the following function:

$$f = \sum_{i=1}^{\nu} \frac{(n_i - \mathcal{N}\mathrm{Tr}[M_i \rho'_{AB}])^2}{2\mathcal{N}\mathrm{Tr}[M_i \rho'_{AB}]} + \lambda \sum_k \left[\sum_{m,n} \chi_{mn} \mathrm{Tr}(\tilde{E}_n^\dagger \tilde{E}_m \tilde{E}_k) - \mathrm{Tr}(\tilde{E}_k) \right]^2,$$

such that the resulting χ most closely resembles a physical quantum process. Here, i labels the measurement setting in the final QST, ν is the number of measurement settings, n_i is the number of two-fold coincidence counts recorded in the i^{th} setting, $\mathcal{N}$ corresponds to the number of photons incident on the detectors, M_i is the projector of the i^{th} measurement, and λ is a Lagrange multiplier used to force the resulting process matrix to be trace preserving [19].

3.6 Experiment

We use the experimental setup shown in Figure 4.4 to implement the quantum channel defined by the Kraus operators in Equation 3.1. Two 40 mm calcite beam displacers are used to construct an interferometer. Within these beam displacers, photons with horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarization are spatially displaced with respect to each other [54]. Half-wave plates (HWPs) are used to set the amount of damping by allowing to adjust α and β in Equation 3.1. The relations between these parameters and the individual angles a, b, c, d of the four HWPs are given by $\sin 4a = \frac{\cos\beta}{\cos\alpha}$, $b = a - \frac{\pi}{4}$, $\sin 4c = -\frac{\sin\alpha}{\sin\beta}$ and $d = \frac{\pi}{2} - c$. The channel is realized by switching randomly between the Kraus operators A_0 and A_1. The switching is performed using two liquid-crystal retarders (LCRs). We set the two LCRs to X_1 and $\mathbb{1}_2$, respectively, to implement A_0, and we set them to $\mathbb{1}_1$ and X_2 to implement A_1. Here, the subscripts represent the action of the first and the second LCR. The probabilities, p_{A_0} and p_{A_1}, with which each configuration is realized are determined by the values of α and β such that the overall success probability of realizing the channel

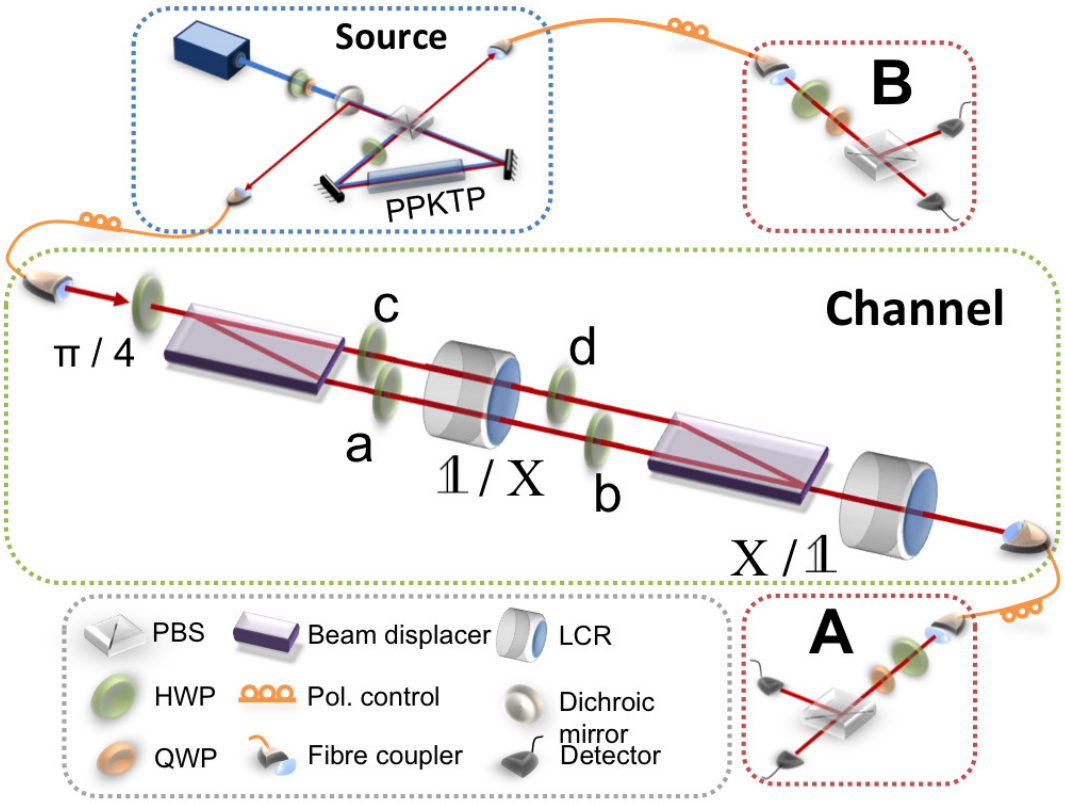


Figure 3.1: The experimental setup. We use spontaneous parametric downconversion in periodically poled $KTiOPO_4$ (PPKTP) to generate entangled photon pairs of the form $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ which are subsequently coupled into single-mode fibres. One of the photons is sent through the damping channel parameterized by α and β, which are set by the angles a, b, c and d of four half-wave plates (HWPs). Two liquid-crystal retarders (LCRs) switch anti-correlatively between the identity, $\mathbb{1}$, and the Pauli X operation. The polarization of each photon is measured by an analyzer (A and B) consisting of a half- and a quarter-wave plate (QWPs) followed by a polarizing beam splitter (PBS). Eventually, the photons are detected by single-photon counting modules.

follows Equation 3.2, and is optimal [56]. The switching rate of the LCRs was chosen to be 10 Hz, significantly faster than the integration time for a single measurement (5 s).

To characterize the channel, we use the AAQPT scheme outlined above. Our resource state is an entangled photon pair generated in a type-II downconversion source in a Sagnac configuration [24, 57]. A 0.5 mW laser diode at 404.5 nm pumps a 25 mm periodically-poled crystal of $KTiOPO_4$ (PPKTP). This typically yielded a coincidence rate of 10 kHz. The characterization of the channel is executed as follows: The HWP angles a, b, c and d are set to zero and the LCRs to X_1 and $\mathbb{1}_2$ such that the channel acts as the identity map. A QST is performed to obtain the density matrix of the input state, ρ_{AB}. The HWP angles and the probabilities for switching the LCRs and the HWP angles are then set according to the values of α and β. Another QST yields the output state, ρ'_{AB}. QST involves recording coincidences for all combinations of the eigenstates of the Pauli X, Y and Z operators. For each of these 36 projective measurements, we integrated coincidence counts for 5 s. The resulting data were then used in conjunction with Equation 3.3 to reconstruct the superoperator describing the quantum process.

3.7 Results

We now turn to our main result, the optimality of our quantum channel implementation. Figure 3.2a shows the probability of success for the amplitude-damping, bit-flip, and one in-between case ($\alpha = \frac{2}{3}\beta$). Since amplitude-damping manifests itself as photon loss in our particular implementation, determining the probability of success reduces to measuring the transmission of the channel. The experimental data closely follow the theoretical predictions (solid lines) that are based on Equation 3.2.

Previous optical implementations of the amplitude-damping channel [58, 47] have given at most 50% probability of success, whereas here we find that only in the case of maximum damping ($\beta = \pi/2$) the probability of success decreases to 50%. The experimental results for the success probability closely resemble the theoretical prediction. This is also true for our experimental implementation of the bit-flip channel and the $\alpha = \frac{2}{3}\beta$ case of single-qubit damping.

Fig. 3.2b shows the tangle [74] of the two-photon output density matrix, ρ'_{AB}, for the amplitude-damping, bit-flip, and $\alpha = \frac{2}{3}\beta$ cases, where one of the two photons passes through the quantum channel. Theoretical curves are based on the action of the respective ideal quantum channels on the experimental input density matrix when the channel is turned off. This also explains the rather high deviation of the data points at larger values

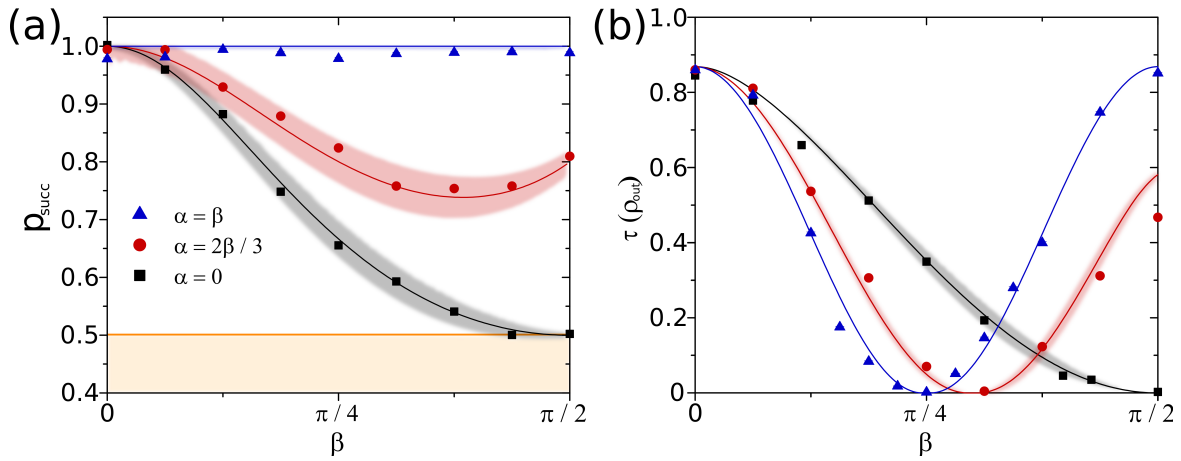


Figure 3.2: (a) Probability of success as a function of damping parameter β for cases $\alpha = 0$, $\alpha = \frac{2}{3}\beta$ and $\alpha = \beta$. The shaded region below 0.5 represents probabilities of success in previous optical implementations of the amplitude-damping channel, see Refs. [58, 2, 47] (b) The tangle, τ, of the resulting two-photon state as a function of damping β after one photon has passed through the damping channel. Errors in the experimental data are calculated from Poissonian noise in the coincidence counts [71] and are not visible on the scale of the plots. The solid lines in both panels represent the theoretically expected dependance. In (b), the experimental density matrix of the input state was used for the calculations. The shaded regions around the theory curves in both plots represent the expected standard deviation in the simulation assuming 1° and 1% rotation errors in the HWPs and LCRs respectively. The margin of error in the $\alpha = \beta$ case is significantly smaller than for the other cases due to the fact that the HWP angles and LCR settings all lie at points where partial derivatives of the Kraus-operator matrix elements are zero.

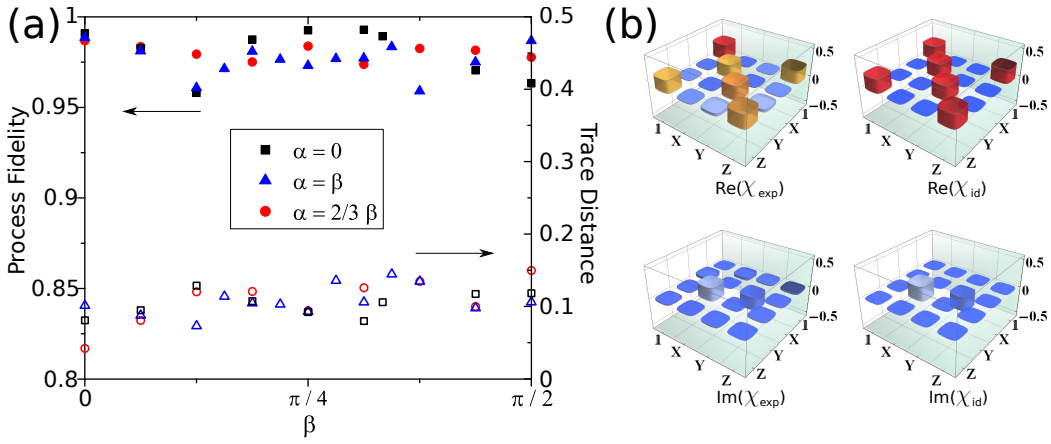


Figure 3.3: (a) Measured process fidelity (solid data points) and trace distance (unfilled data points) as a function of damping for each of the three cases studied. Error bars ($\sim 10^{-3}$), calculated using Monte-Carlo simulations adding Poissonian noise to the measured state tomography counts in each run, are too small to see on this scale due to high photon counting rates. Additional systematic errors are discussed in the text. (b) Real and imaginary parts of the experimentally determined and ideal process matrices at maximum amplitude-damping ($\alpha = 0, \beta = \pi/2$).

of β, as drift in the optical setup can lead to slightly different input states over the course of the experiment.

The process fidelity is defined by $\mathcal{F} = \left(\mathrm{Tr}\sqrt{\sqrt{\chi_{\mathrm{exp}}}\chi_{\mathrm{id}}\sqrt{\chi_{\mathrm{exp}}}}\right)^2$ [41], where χ_{exp} and χ_{id} are the experimental and ideal process matrices, respectively. Process fidelities for the three tested cases, $\alpha = 0$, $\alpha = \beta$ and $\alpha = \frac{2}{3}\beta$ can be seen in Figure 3.3. The uncertainty in the process fidelity of each individual point was estimated by maximum-likelihood assuming Poissonian noise in the measured counts and is on the order of 10^{-3}. However, it is clear from the deviation of process fidelities over the range of damping values that there is an additional systematic error. We attribute this systematic error to the reduced coupling efficiencies when rotating the half-wave plates in the interferometer when setting values of α and β. We then estimate the statistical error in the data and find the average process fidelities to be 0.98 ± 0.01, 0.976 ± 0.009, 0.981 ± 0.004 for the three respective cases.

We also compute the maximum trace distance [52], which is defined as $\mathcal{D} = \max_{\rho_{\mathrm{in}}} \frac{1}{2}\mathrm{Tr}\left|\rho_{\mathrm{out}}^{\mathrm{exp}} - \rho_{\mathrm{out}}^{\mathrm{id}}\right|$, where $|A| = \sqrt{A^\dagger A}$ and $\rho_{\mathrm{out}}^{\mathrm{exp/id}} = \sum_{m,n} \chi_{mn}^{\mathrm{exp/id}} \tilde{E}_m \rho_{\mathrm{in}} \tilde{E}_n^\dagger$. Operationally, $\mathcal{D}$ corresponds to the highest probability of distinguishing between the experimental and ideal channels using the best possible input state. Maximum trace distances for $\alpha = 0$, $\alpha = \beta$ and $\alpha = \frac{2}{3}\beta$

cases can also be seen in Figure 3.3. As with the process fidelities, we can estimate the errors for the three cases from the statistical error of the data points for different values of β. Using this approach, the average maximum trace distances for $\alpha = 0$, $\alpha = \beta$, and $\alpha = \frac{2}{3}\beta$ are 0.10 ± 0.01, 0.11 ± 0.02, and 0.11 ± 0.03, respectively.

3.8 Summary

Decoherence plays an important role in quantum information science. Investigating its effects requires careful and well-controlled implementations of these noisy processes. Non-unital damping channels, like the ones studied here, are crucial in further understanding quantum communication, in determining channel capacities and for the generation of bound-entangled states. We have implemented a general damping single-qubit quantum channel with linear optics in which both type and amount of decohering noise can be precisely controlled. A single, static optical setup can perform as the amplitude-damping channel, the bit-flip channel, or more general cases characterized by two real parameters, α and β. Most importantly, we have shown that this channel has been implemented in an optimal way, so as to maximize the probability of success. The channels were characterized using a new approach to ancilla-assisted process tomography and, in all cases, operate with high fidelity.

Chapter 4

Quantum computing on encrypted data

4.1 Notes and acknowledgements

In this chapter we describe the experimental realization of a protocol for quantum computing on encrypted data. We implement each quantum gate in a universal set in the client-server model outlined by the protocol. We use the notions of quantum process tomography discussed in Chapter 1, and make use of the CNOT gate demonstrated in Chapter 2. We find that when the client encrypts the input state sent to the server and properly decrypts the output, a process tomography gives the action of the gate as expected. However, if the proper decryption is not used, as would be the case for an eavesdropper, process tomography returns the completely depolarizing channel.

Notice: The contents of this chapter will be submitted for publication.

A. Broadbent, K. A. G. Fisher, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein and K. J. Resch. Quantum computing on encrypted data. *In preparation.*

Author contributions

AB designed the protocol and proved its security.

KF performed the experiment and analyzed the data.

KF, LS, ZY, JL, RP and KR contributed to the design and realization of the experiment.

AB and **KF** took primary responsibility for writing the first draft. **All authors** contributed to editing for the final version.

4.2 Introduction

Quantum information technologies promise dramatic increases in computational power for numerous applications[26, 22, 32, 67]. However, the complexity of implementing a large scale quantum computer begs the question of whether they will have widespread availability in the future. One solution is a cloud computing model[34], with relatively few quantum computers that can be accessed remotely by clients. This involves aspects from both quantum computing and cryptography, two integral parts of quantum information processing. Data protection for the client comes from encrypting quantum data using a quantum one-time pad, which provides perfect privacy[4]. Performing classical algorithms on encrypted data is a recently solved problem[28]. Here we present and realize quantum computing over encrypted data. The proof of privacy for our protocol covers all types of prior information known to the cloud. We show that each quantum gate necessary for universal computation is implemented with high fidelity from the point-of-view of the client, whereas the cloud observes completely depolarized states. Our result demonstrates the practicality and current experimental feasibility of a quantum cloud computing model, where the client has very limited quantum power.

Recently, a protocol for blind quantum computation[15, 8] has been put forward which shows how a client can use a cloud quantum computer without the cloud having knowledge of the algorithm it is performing. This provides the client with the desired security, but is expensive in its use of resources. Here we instead present a protocol which allows the cloud to know the circuit, but can never find out the state the client sends it. Specifically, we show that for each gate in a universal set the client can encrypt a qubit, send it to the cloud for computation, and knowing how each gate acts on the encryption, can perform the proper decryption to obtain the desired operation (Fig. 4.1).

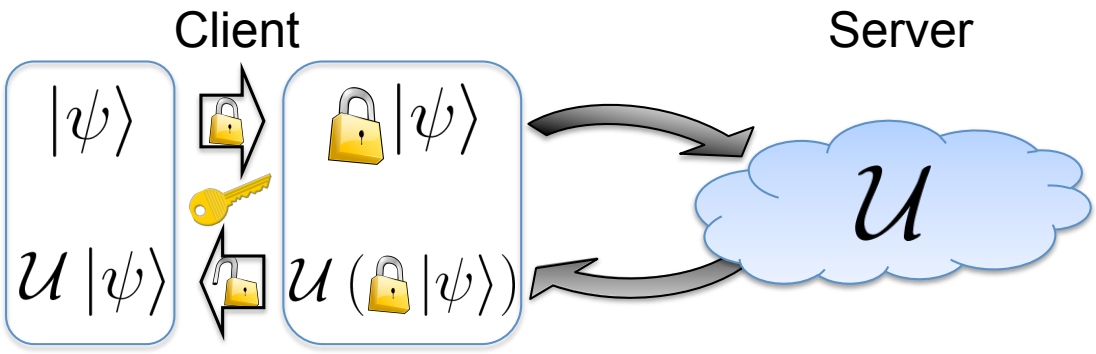


Figure 4.1: A client encrypts a quantum state $|\psi\rangle$ with a quantum one-time pad[4]. He sends the state to a quantum cloud computer which performs a set of unitary operations $\mathcal{U}$. The returned state is then decrypted by the client who then finds the computation performed on the original state $|\psi\rangle$.

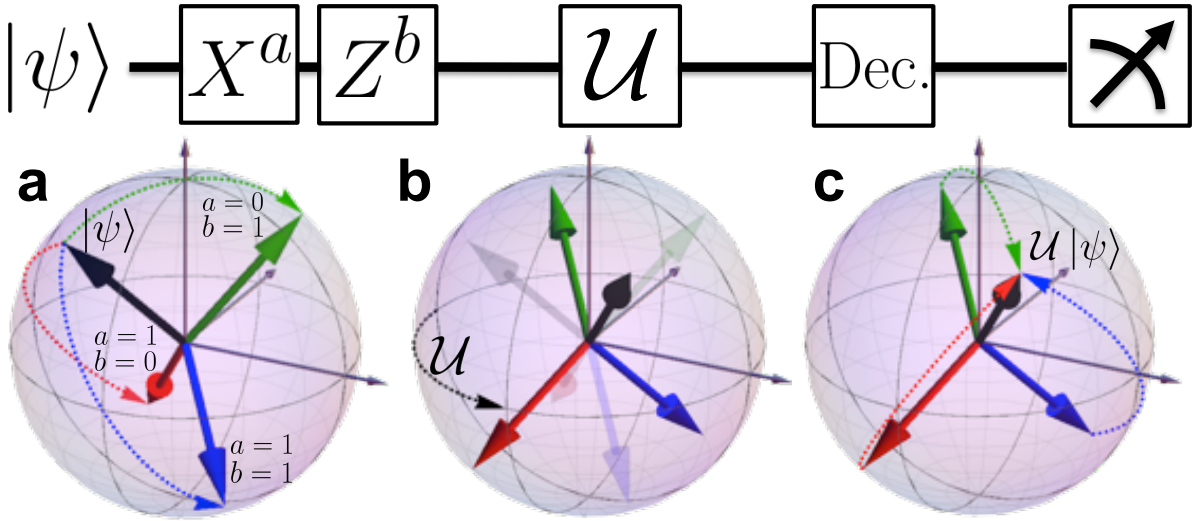


Figure 4.2: The process of encrypting a qubit, performing a gate, decrypting and measuring. (a) shows the encryption's effect on a state $|\psi\rangle$, black vector, in the Bloch sphere. (b) shows the action of $\mathcal{U}$, in this case a P gate shown as a quarter rotation about the z-axis, mapping semi-transparent vectors to opaques. (c) shows the action of decrypting the different cases, each giving the desired result $\mathcal{U}|\psi\rangle$.

4.3 Protocol

A general quantum circuit acting on qubits can be decomposed into a sequence of the following elements: auxiliary qubit preparation in $|0\rangle$, single-qubit computational basis measurements, Clifford gates in $\{\mathsf{X}, \mathsf{Z}, \mathsf{H}, \mathsf{P}, \mathsf{CNOT}\}$, as well a non-Clifford gate, R. If these operations are executed by a cloud who has access only to the input in its encrypted form (where the encryption is a quantum one-time pad with operation $\mathsf{X}^a\mathsf{Z}^b$, $a, b \in \{0, 1\}$), the output can nevertheless be decrypted by the client, and the cloud does not learn anything about the input (Fig. 4.2). Recall that the given gates have the following actions on a qubit $|j\rangle$, $j \in \{0, 1\}$:

$$\begin{aligned}
\mathsf{X} : |j\rangle &\mapsto |j \oplus 1\rangle \\
\mathsf{Z} : |j\rangle &\mapsto (-1)^j |j\rangle \\
\mathsf{H} : |j\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle + (-1)^j |1\rangle) \\
\mathsf{P} : |j\rangle &\mapsto (i)^j |j\rangle \\
\mathsf{CNOT} : |j\rangle|k\rangle &\mapsto |j\rangle|j \oplus k\rangle \\
\mathsf{R} : |j\rangle &\mapsto (e^{i\pi/4})^j |j\rangle
\end{aligned} \tag{4.1}$$

Single-qubit preparations and measurements are easily performed on encrypted data; the actions of the Clifford gates on the encryption are, up to a global phase,

$$\begin{aligned}
\mathsf{X}(\mathsf{X}^a\mathsf{Z}^b|\psi\rangle) &= \mathsf{X}^a\mathsf{Z}^b(\mathsf{X}|\psi\rangle) \\
\mathsf{Z}(\mathsf{X}^a\mathsf{Z}^b|\psi\rangle) &= \mathsf{X}^a\mathsf{Z}^b(\mathsf{Z}|\psi\rangle) \\
\mathsf{H}(\mathsf{X}^a\mathsf{Z}^b|\psi\rangle) &= \mathsf{X}^b\mathsf{Z}^a(\mathsf{H}|\psi\rangle) \\
\mathsf{P}(\mathsf{X}^a\mathsf{Z}^b|\psi\rangle) &= \mathsf{X}^a\mathsf{Z}^{a+b}(\mathsf{P}|\psi\rangle) \\
\mathsf{CNOT}(\mathsf{X}^a\mathsf{Z}^b \otimes \mathsf{X}^c\mathsf{Z}^d|\psi\rangle) &= \\
\mathsf{X}^a\mathsf{Z}^{b+d} &\otimes \mathsf{X}^{a+c}\mathsf{Z}^d(\mathsf{CNOT}|\psi\rangle)
\end{aligned} \tag{4.2}$$

One cannot use this technique for the R gate since it requires a conditional P gate, $\mathsf{R}\mathsf{X}^a\mathsf{Z}^b|\psi\rangle = \mathsf{X}^a\mathsf{Z}^{a\oplus b}\mathsf{P}^a\mathsf{R}|\psi\rangle$. We solve this using a method inspired by the circuit manipulation techniques of [75, 17]: it suffices to use classical interaction (one bit in each direction) and a single forward auxiliary qubit randomly chosen out of four possibilities

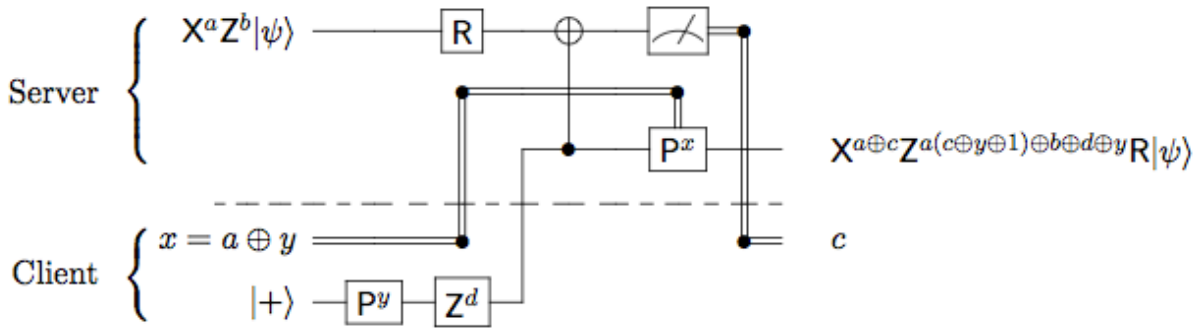


Figure 4.3: A simple protocol for the R gate over encrypted data. An auxiliary qubit is initialized to $\frac{1}{\sqrt{2}}(|0\rangle + i^{y+2d}|1\rangle)$, where y and d are random bits. The server performs the R gate and a hidden P gate, concealed by the combination of x, y and d. The client uses these values, along with the measurement result $c \in \{0, 1\}$ to decrypt the returned qubit.

(see Fig. 4.3). We manage to halve the size of the set from which random qubits are chosen from 8[15] to 4. This is due to the fact that the cloud directly implements an R gate followed by a hidden P gate, instead of using a hidden R gate. Additionally, we manage to reduce the complexity in terms of communication to null for all but the execution of a non-Clifford group gate; prior work requires for each gate (including the identity), 24 bits of forward communication, 8 bits of backward communication and 8 auxiliary qubits. Note that our protocol also enables the hiding of the computation itself, via the use of a standard universal circuit.

Our protocol provides the same level of security as the one-time pad, that is, it provides perfect (information-theoretic) privacy. In contrast, fully homomorphic encryption [28] provides computational security only because it uses a public-key encryption scheme. Formally, we define privacy based on simulations and provide a proof via an equivalent, entanglement-based protocol[68].

Compared to prior work, our contribution has the advantage of providing a conceptually simple proof of correctness, together with a security definition and proof that is applicable to all types of prior information, including shared entangled quantum registers.

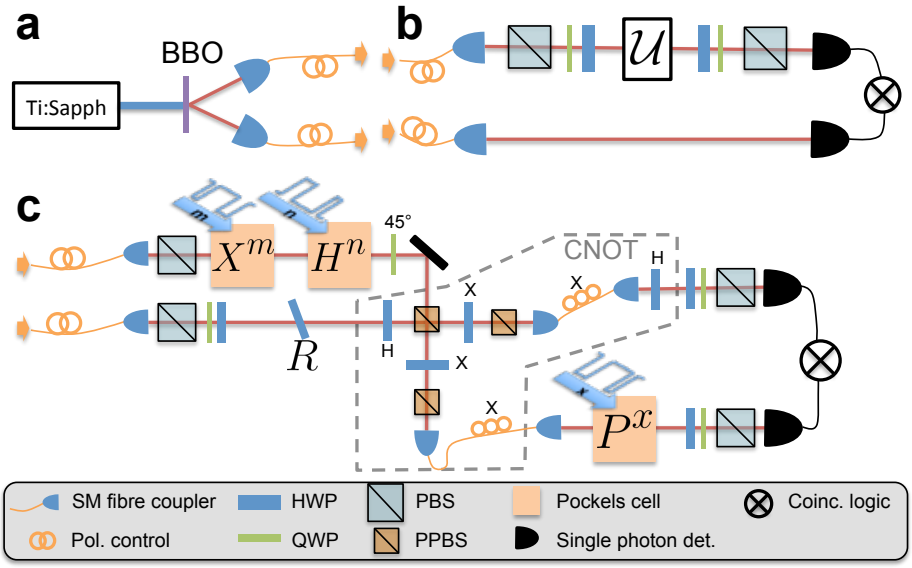


Figure 4.4: The single photon source **(a)**, connects to the single-qubit Clifford gate setup **(b)**, or the CNOT and R gate setup **(c)**.

4.4 Experiment

Using linear optics, we perform an experiment encoding quantum information in the polarization of single photons. The horizontal and vertical polarizations of light, $|H\rangle$ and $|V\rangle$, are $|0\rangle$ and $|1\rangle$ respectively. Eigenstates of the Pauli X and Y operators are encoded in the diagonal ($|D\rangle, |A\rangle$) and circular ($|L\rangle, |R\rangle$) polarizations respectively. Fig. 4.4a shows the single photon source. Single photon pairs are generated by pumping a barium borate (BBO) crystal with a Ti:Sapphire laser beam with $\lambda = 395\,\text{nm}$ through spontaneous parametric down conversion (SPDC). Photons are then propagated through the setup in Fig. 4.4b to perform a single-qubit Clifford gate, or the setup in Fig. 4.4c to perform the CNOT and R gates (see Methods).

We characterize each gate using a maximum likelihood quantum process tomography (QPT) [53, 40, 19] , where we reconstruct the process matrix χ which most closely describing the measurements. We use overcomplete sets of input states and measurements to cover all possible encryptions and to ascertain more accurate count rates.

The X, Z, and H gates are half-wave plates (HWPs) at 45°, 0° and 22.5° respectively, and the P gate is a quarter-wave plate (QWP) at 0°. To quantify the discrepancy between

experimental and ideal gates, we calculate the process fidelity $F = \mathrm{Tr}(\chi_{\mathrm{exp}}\chi_{\mathrm{id}})$. We find process fidelities of 0.984 ± 0.002, 0.985 ± 0.001, 0.983 ± 0.001 and 0.985 ± 0.001 with the ideal X, Z, H and P gates, respectively. Counts were then summed over the different encryption cases, $a, b \in \{0, 1\}$, simulating what an eavesdropper finds, and for each gate we find the fidelity with the completely depolarizing channel $F > 0.999$. Uncertainties were estimated by adding Poissonian noise to count data and performing 100 Monte Carlo iterations of each process matrix reconstruction.

With linear optics and post-selection, the CNOT gate can only be implemented in a probabilistic way [44]. We use a scheme [42, 46] outlined in the Fig. 4.4c inset, which has a 1/9 success probability. Control and target photons interfere at a partially-polarizing beamsplitter (PPBS), which fully transmits H-polarized light, but reflects 2/3 of the V-polarization. Postselecting on coincident photons gives the action of the gate. Results of the QPT are shown in Fig. 4.5. We found a process fidelity of 0.869 ± 0.004 with the ideal CNOT, which is on par with the best demonstrated optical CNOT gates [53, 42, 46]. This less than ideal fidelity comes primarily from emitted double pairs and non-interfering photons passing propagating through the optical setup. When summing over the 16 encryption cases, $a, b, c, d \in \{0, 1\}$, we find $F > 0.995$ with the two-qubit completely depolarizing channel.

The R gate protocol setup is shown in Fig. 4.4c. The gate itself is a HWP at 0° tilted to give the proper phase delay between H- and V-polarizations. The auxiliary photon is initialized to a random choice of $\{|D\rangle, |A\rangle, |L\rangle, |R\rangle\}$ using fast optical switches called Pockels cells (see Methods). Coincident photon detections in conjunction with Pockels cell configurations were recorded into 8 bins, depending on the state of the auxiliary photon and the outcome of the primary photon measurement. Consequently, knowing in which bin a count was recorded is the same as knowing the values of y, d and c. The client, who also knows the values of a and b is then able to properly decrypt the measurement results. Again, we performed a QPT inputting and measuring all single-qubit Pauli basis states. Summing bin counts with knowledge of the proper decryption, we obtained a process matrix, Fig. 4.5, whose fidelity is 0.863 ± 0.004 with the ideal R gate. This fidelity is of course capped by that of the CNOT gate. Summing over bin counts without using the proper decryption gave a process with $F > 0.987$ with the completely depolarizing channel. Additionally, summing over the encryption cases a, b boosted this fidelity to $F > 0.999$.

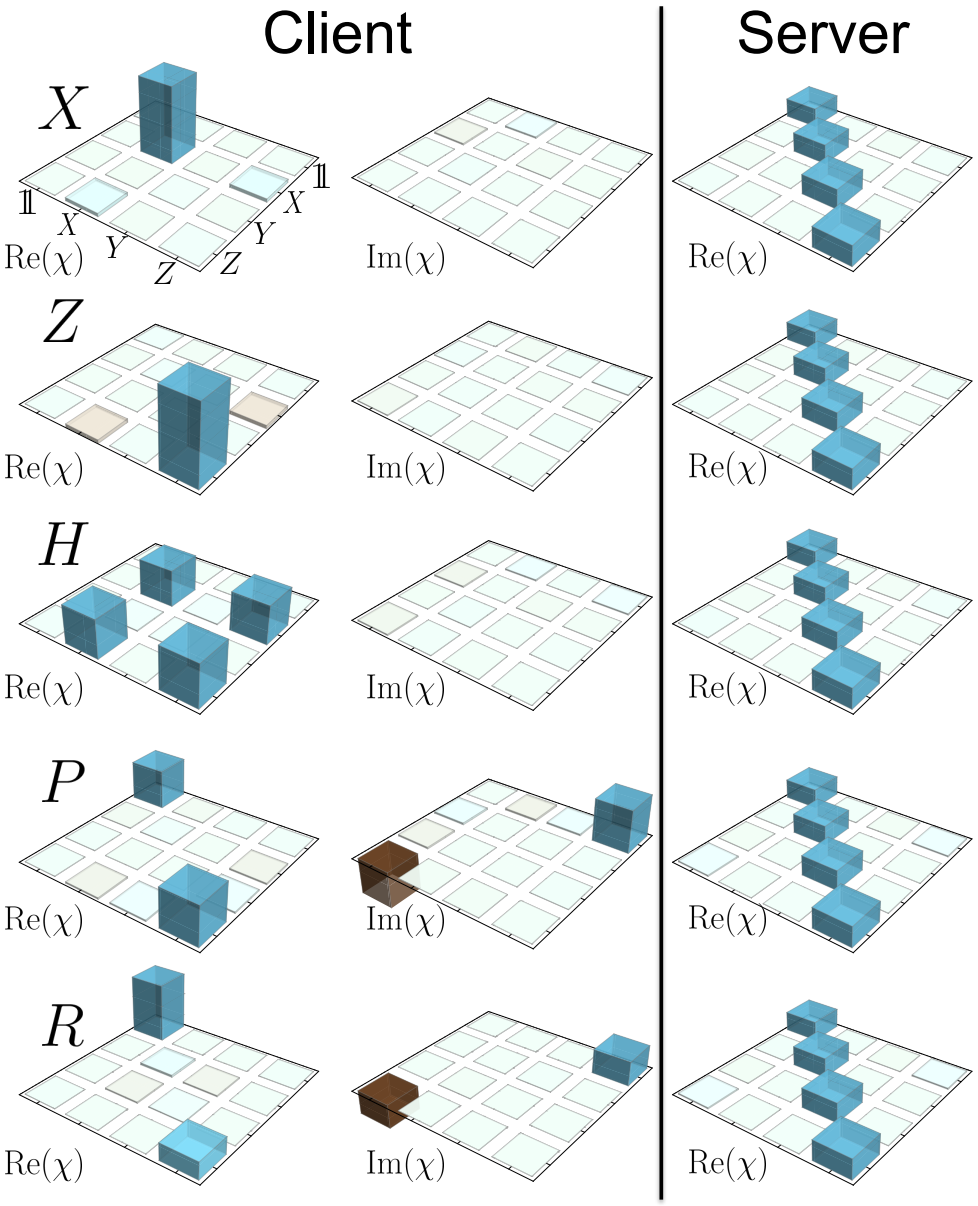


Figure 4.5: The left panel shows real and imaginary parts of reconstructed χ matrices for the single-qubit gates when the proper decrypting operations were used. The right panel shows the real parts (imaginary parts were negligible) of the reconstructed χ matrices when proper decryptions were not known.

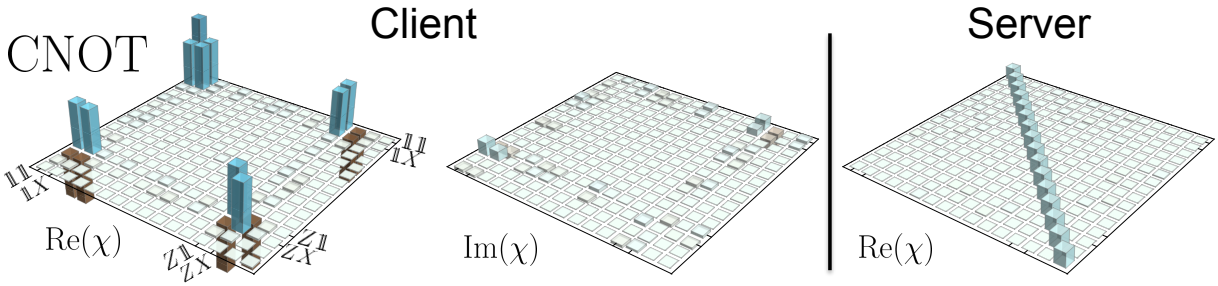


Figure 4.6: Real and imaginary parts of reconstructed χ matrices for the CNOT gate when the proper decrypting operations were (left) and weren't (right) used. The $\mathbb{1}\mathbb{1}$ component of the CNOT matrix has a height of 0.318, and the largest imaginary component is 0.06. Imaginary parts of undecrypted results were negligible (< 0.004).

4.5 Summary

In summary, we have demonstrated how a quantum cloud can perform each gate in a universal set over encrypted data. While the protocol for the Clifford gates is straightforward, as could be expected, we have also shown a simple protocol for the *non*-Clifford R gate. This protocol uses a hidden P gate which calls for one auxiliarly qubit and two more classical classical bits. This reduction in required resources was enough to perform a proof-of-principle experiment using linear optics. We have shown experimentally that we can perform a desired gate with high fidelity when the decryption key is known, and that without the key, as is the case for the cloud, nothing can be learnt about the data. Recent developments such as blind quantum computing, as well as the protocol we have shown here, are paving the way to the eventual reality of being able to remotely and securely perform quantum computations.

4.6 Methods

Single photon pairs of $\lambda = 790\,\text{nm}$ are generated via SPDC by pumping a BBO crystal with a Ti:Sapph laser pulsed at 80 MHz. Photons are then relayed through single-mode fibre to either the setup for single-qubit Clifford gates or for the CNOT and R gates. In the single-qubit Clifford gate setup (Fig. 4.4b), photons in the top rail are initialized to a

given input state using a PBS, QWP and HWP. The gates are then performed using either a HWP or QWP at the angles mentioned in the main text. The state is measured in a given basis using a HWP and QWP followed by a PBS. Measurements are heralded by the detection of coincidence photons in the lower rail within a 3 ns window.

The CNOT and R gate setup is shown in Fig. 4.4c. Photons in the lower, primary, rail are initialized and pass through the R gate. Photons in the upper, auxiliary, rail are rotated from $|H\rangle$ to a uniformly random choice of $\{|D\rangle, |L\rangle, |A\rangle, |R\rangle\}$ using two Pockels cells performing X^m and H^n with $m, n \in \{0, 1\}$, followed by a QWP at 45°. Pockels cells are driven between high and low voltage configurations, triggered randomly at a rate of 1 MHz, to switch between unitary transformation on the photon polarization. Single photon rates were about 7000/ s, where the pump power was reduced to limit the effect of double pairs on the fidelity of the CNOT gate. The auxiliary photon controls the CNOT gate (outlined in grey), interfering at a PPBS with the primary photon, upon which the R has acted. The primary photon is measured in the computational basis, and both $|0\rangle$ and $|1\rangle$ detections are recorded. The conditional P gate on the auxiliary photon is implemented using a third Pockels cell. It is possible to trigger this Pockels cell based on the values of a and y, but in practice it was driven independentally and both correlated and anti-correlated cases were recorded. The auxiliary photon is then measured in each of the single-qubit Pauli bases. The CNOT gate was tested by moving state initialization and analysis to within the grey borders.

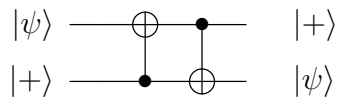
4.7 Supplementary Information

4.7.1 Correctness of the R-gate protocol

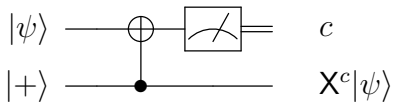
We give below a step-by-step proof of the correctness of the R-gate protocol as given in Figure 4.3. The basic building block is the circuit identity for an X-teleportation from [75], which we re-derive here. Also of relevance to this work are the techniques developed by Childs, Leung, and Nielsen [17] to manipulate circuits that produce an output that is correct *up to known Pauli corrections*.

We will make use of the following identities which all hold up to an irrelevant global phase: $\mathsf{XZ} = \mathsf{ZX}$, $\mathsf{PZ} = \mathsf{ZP}$, $\mathsf{PX} = \mathsf{XZP}$, $\mathsf{RZ} = \mathsf{ZR}$, $\mathsf{RX} = \mathsf{XZPR}$, $\mathsf{P}^2 = \mathsf{Z}$ and $\mathsf{P}^{a\oplus b} = \mathsf{Z}^{a\cdot b}\mathsf{P}^{a+b}$ (for $a, b \in \{0, 1\}$).

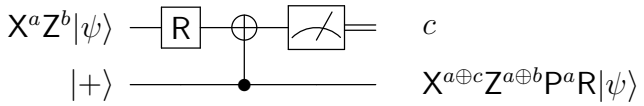
1. Our first circuit identity swaps a qubit $|\psi\rangle$ with the state $|+\rangle$ and is easy to verify.



2. We can measure the top qubit in the above circuit and classically control the output correction. We have thus re-derived the circuit corresponding to the "X-teleportation" of [75].

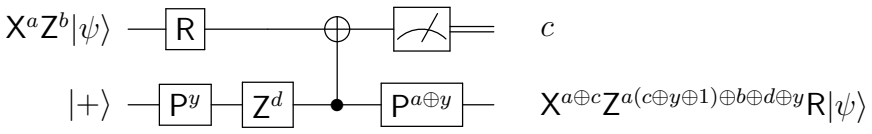


3. Next, we re-define the input to be $\mathsf{R}\mathsf{X}^a\mathsf{Z}^b|\psi\rangle$, so the output becomes $\mathsf{X}^c\mathsf{R}\mathsf{X}^a\mathsf{Z}^b|\psi\rangle = \mathsf{X}^{a\oplus c}\mathsf{Z}^{a\oplus b}\mathsf{P}^a\mathsf{R}|\psi\rangle$.



4. Then add three gates (P^y, Z^d, $\mathsf{P}^{a\oplus y}$) to the bottom wire (see circuit below). Using the fact that the P and Z commute with control, and applying identities given above, we get as output what we expect:

$$\begin{aligned}
\mathsf{P}^{a\oplus y}\mathsf{Z}^d\mathsf{P}^y\mathsf{X}^{a\oplus c}\mathsf{Z}^{a\oplus b}\mathsf{P}^a\mathsf{R}|\psi\rangle &= \mathsf{Z}^{a\cdot y}\mathsf{P}^{a+y}\mathsf{Z}^d\mathsf{P}^y\mathsf{X}^{a\oplus c}\mathsf{Z}^{a\oplus b}\mathsf{P}^a\mathsf{R}|\psi\rangle && (4.3)\\
&= \mathsf{Z}^{d\oplus a\cdot y\oplus y}\mathsf{P}^a\mathsf{X}^{a\oplus c}\mathsf{Z}^{a\oplus b}\mathsf{P}^a\mathsf{R}|\psi\rangle && (4.4)\\
&= \mathsf{Z}^{d\oplus a\cdot y\oplus y}\mathsf{X}^{a\oplus c}\mathsf{Z}^{a(a\oplus c)}\mathsf{P}^a\mathsf{Z}^{a\oplus b}\mathsf{P}^a\mathsf{R}|\psi\rangle && (4.5)\\
&= \mathsf{X}^{a\oplus c}\mathsf{Z}^{d\oplus a\cdot y\oplus y\oplus a^2\oplus a\cdot c}\mathsf{Z}^b\mathsf{R}|\psi\rangle && (4.6)\\
&= \mathsf{X}^{a\oplus c}\mathsf{Z}^{a(c\oplus y\oplus 1)\oplus b\oplus d\oplus y}\mathsf{R}|\psi\rangle && (4.7)
\end{aligned}$$



4.7.2 Security definition and proof

Preliminaries

Quantum registers and channels. A *quantum register* is a collection of qubits in some finite dimensional Hilbert space, say $\mathcal{X}$. We denote $\mathrm{D}(\mathcal{X})$ the set of density operators

acting on $\mathcal{X}$. The set of all linear mappings from $\mathcal{X}$ to $\mathcal{Y}$ is denoted by $\mathrm{L}(\mathcal{X}, \mathcal{Y})$, with $\mathrm{L}(\mathcal{X})$ being a shorthand for $\mathrm{L}(\mathcal{X}, \mathcal{X})$. A linear super-operator $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ is *admissible* if it is completely positive and trace-preserving. Admissible super-operators represent mappings from density operators to density operators, that is, they represent the most general quantum maps.

Given admissible super-operators Φ and Ψ that agree on input space $\mathrm{L}(\mathcal{X})$ and output space $\mathrm{L}(\mathcal{Y})$, we are interested (for cryptographic purposes) in characterizing how "indistinguishable" these processes are. The *diamond norm* provides such a measure: given that Φ or Ψ is applied with equal probability, the optimal procedure to determine the identity of the channel with only one use succeeds with probability $1/2 + \|\Phi - \Psi\|_\diamond/4$. Here,

$$\|\Phi - \Psi\|_\diamond = \max\{\|(\Phi \otimes \mathbb{1}_\mathcal{W})(\rho) - (\Psi \otimes \mathbb{1}_\mathcal{W})(\rho)\|_1 : \rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{W})\}\,, \tag{4.8}$$

where $\mathcal{W}$ is any space with dimension equal to that of $\mathcal{X}$ and $\mathbb{1}_\mathcal{W}$ is the identity in $\mathrm{L}(\mathcal{W})$, and where the *trace norm* of an operator X is defined as $\|X\|_1 = \mathrm{Tr}\sqrt{X^*X}$.

Definition and proof of privacy

Our protocol provides the same level of security as the one-time pad, that is, it provides perfect (information-theoretic) privacy. The rest of this section formalizes the definition of privacy based on simulations and gives a proof based on the technique of giving an equivalent, entanglement-based protocol. For our definition of privacy, we have used notions similar to those introduced by Watrous in the context of quantum zero-knowledge interactive proof systems [72]. We use as proof technique the method of transforming a qubit-based protocol into an equivalent protocol that is more easily proved secure, but that involves entanglement. This technique is attributed to Shor and Preskill [68], who used it in the context of proving the security of the BB84 [10] quantum key exchange protocol, and has since appeared in the context of quantum message authentication [7] and cryptography in the bounded-quantum-storage model [21].

Formally, a protocol for delegated computation is specified by a pair (C, S) representing an honest client and an honest server (without loss of generality, both parties are quantum). As the client is always honest, the security property concerns interactions between pairs (C, S') where S' deviates arbitrarily from S. At the onset of the protocol, both parties agree on the classical input q which determines the general quantum circuit to be executed as an ordered series of gates acting on specified wires. The structure of the interaction between C and S is thus determined by q. At the same time, a quantum input $\rho_{\text{in}} \in \mathrm{D}(\mathcal{C} \otimes \mathcal{S})$ is distributed, C receiving the register in $\mathcal{C}$ and S receiving the register in $\mathcal{S}$. A cheating

server S' is any quantum computational process that interacts with C according to the message structure determined by q. By allowing S' access to the input register $\mathcal{S}$, we explicitly allow S' to share prior entanglement with C's input; this also models any *prior* knowledge of S' and formalizes the notion that the protocol cannot be used to *increase* knowledge.

Let $\mathcal{Z}$ denote the output space of S' and let $\Phi_q : \mathrm{L}(\mathcal{S}) \to \mathrm{L}(\mathcal{Z})$ be the mapping induced by the interaction of S' with C. Security is defined in terms of the existence of a *simulator* $\mathscr{S}_{S'}$ for a given server S', which is a general quantum circuit that agrees with S' on the input and output dimensions. Such a simulator does not interact with C, but simply induces a mapping $\Psi_q : \mathrm{L}(\mathcal{S}) \to \mathrm{L}(\mathcal{Z})$ on each input q. Informally, (C, S) is private if the two mappings, Φ_q and Ψ_q are indistinguishable for every choice of q and every choice of ρ_{in}. Allowing for an ϵ amount of leakage, we formalize this as Definition 1.

Definition 1. *A protocol (C, S) for a delegated quantum computation is ϵ-private if for every server S' there exists a simulator $\mathscr{S}_{S'}$ such that for every classical input q,*

$$\|\Phi_q - \Psi_q\|_\diamond \leq \epsilon\,, \tag{4.9}$$

where Φ_q is the mapping induced by the interaction of S' with the client C on input q and Ψ_q is the mapping induced by $\mathscr{S}_{S'}$ on input q.

Taking $\epsilon = 0$ gives the strongest possible security against a malicious server: it does not allow for even an ϵ amount of leakage, and allows the server to deviate arbitrarily (without imposing any computational bounds). Theorem 1 states that this is the level of privacy achieved in our protocol.

Our proof technique will construct a sequence of protocols. For clarity, we refer to the protocol in the main paper as **Protocol 1**.

Theorem 1. ***Protocol 1*** *is an ϵ-private protocol for delegated quantum computation, with $\epsilon = 0$.*

Proof. Fix a value for q. We construct a simulator $\mathscr{S}_{S'}$ by giving instructions how to prepare messages that replace the messages that the client C would send to the server S' in the real protocol. Privacy follows since we will show that these transmissions are identical to those in the real protocol.

A high-level sketch of the proof is that we modify the behaviour of the client in the main protocol (**Protocol 1**) in a way that the effect of the protocol is unchanged, yet the client delays introducing her input into the protocol until after her interaction with the

server has ended (this makes the simulation almost trivial). In order to do so, we describe below an entanglement-based protocol (**Protocol 2**) as well as a delayed-measurement protocol (**Protocol 3**).

We first consider **Protocol 2**, which is an entanglement-based version of **Protocol 1**. In **Protocol 2**, we modify how the client prepares her messages, without modifying the server's actions or the effect of the protocol. Thus, the preparing and sending of an encrypted quantum register is replaced by an equivalent teleportation-based protocol, as given in Figure 4.7. Also, the R-gate protocol is replaced by an equivalent protocol as given in Figure 4.9. The protocol of Figure 4.9 can be seen to be correct via an intermediate protocol (Figure 4.8), in which the classical bit x from the client to the server becomes a uniformly random bit; this transformation is possible because in the R-gate protocol, $x = a \oplus y$ with y a random bit. Then choosing x to be random and $y = a \oplus x$ gives an equivalent protocol. The final entanglement-based protocol of Figure 4.9 is seen to be correct via the circuit identity given in Figure 4.10. The remaining protocols for stabilizer circuit elements (Clifford gates, qubit preparation and measurements) are non-interactive and thus unchanged in **Protocol 2**.

The main advantage of considering **Protocol 2** instead of **Protocol 1** is that we can delay all the client's measurements (in Figures 4.7 and 4.9) until the output register is returned, without affecting the computation or the server's view of the protocol (because actions on different subsystems commute); call the result **Protocol 3**. In this delayed-measurement protocol, the messages from the client to the server can be chosen *before* any interaction with the server, and are thus clearly independent of the actions of S'.

Thus we construct a simulator $\mathscr{S}_{S'}$ that plays the role of the client in **Protocol 3**, *but that never performs any measurements* (thus, access to the actual input is not required). By the argument above, $\mathscr{S}_{S'}$ actually prepares the same transmissions as would C in **Protocol 1** interacting with S' on any input ρ_{in}. It follows that simulating S' on these transmissions will induce the same mapping as S' in the real protocol, and thus $\|\Phi_q - \Psi_q\|_\diamond = 0$. □

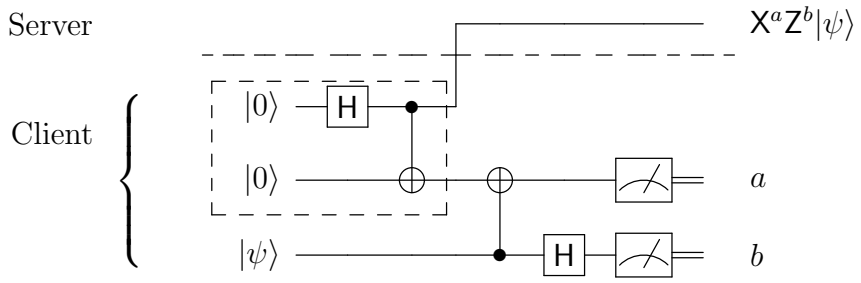


Figure 4.7: Protocol to encrypt and send a qubit using teleportation[11]. The circuit in the dashed box prepares an EPR-pair.

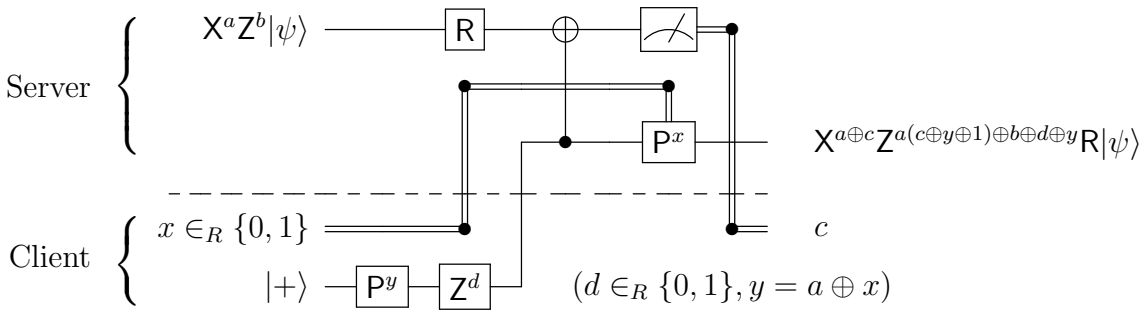


Figure 4.8: Intermediate Protocol for an R-gate. Compared to Figure 4.3, the classical message from the client to the server is chosen uniformly at random. This protocol performs the same computation as the protocol in Figure 4.3.

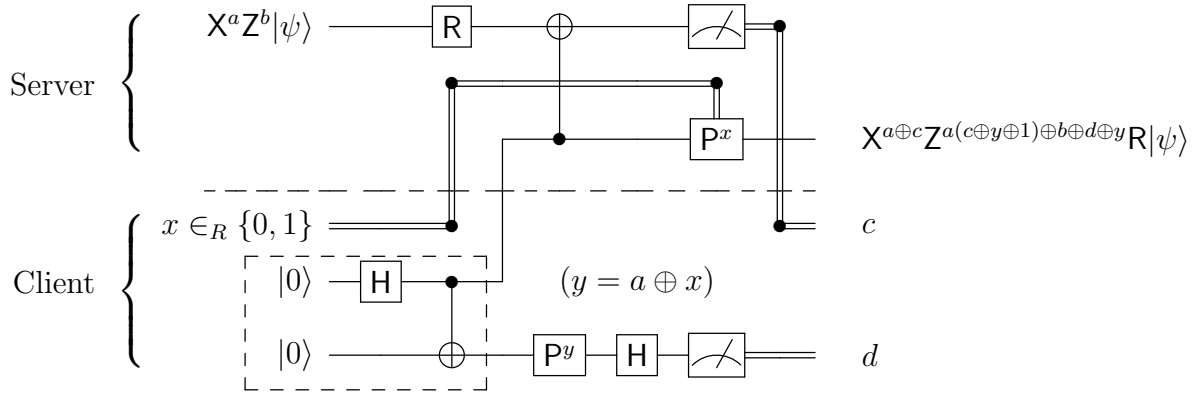


Figure 4.9: Entanglement-based protocol for an R-gate. This protocol performs the same computation as the protocols in Figures 4.3 and 4.8. The circuit in the dashed box prepares an EPR-pair.

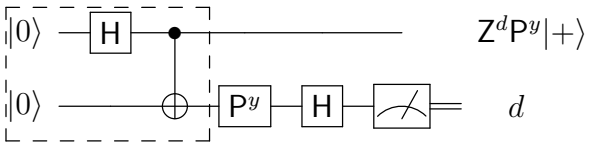


Figure 4.10: Circuit identity: entanglement-based circuit that prepares a qubit $\mathsf{Z}^d\mathsf{P}^y|+\rangle$ for uniformly random bits y and d (here, y is chosen uniformly at random, and d is determined by the measurement). The circuit in the dashed box prepares an EPR-pair.

Chapter 5

Conclusion

In this thesis we have covered a broad spectrum of quantum information processing with linear optics. In Chapter 3, we demonstrated an optimal realization of a single-damping channel. This channel could add a controllable amount and type of decoherence to a qubit. We characterized the channel using a novel ancilla-assisted quantum process tomography, where we took into account the imperfection of the two-qubit resource state.

A natural next step is to implement a recently developed error correction code for the detected jump channel [31], which is the amplitude damping channel where the decay is marked by the detection of a photon. The error correction protocol calls for the use of a CNOT gate, which was also implemented in this thesis. Realizing this correction scheme will require constructing and characterizing a second amplitude damping channel to run in parallel with the current one.

In Chapter 4 we showed the implementation of a protocol for performing quantum computations on encrypted data. We showed that for each quantum gate in a universal set that if data is encrypted and decrypted properly the proper action of the gate is observed, and with high fidelity. On the other hand, if the proper decryption is not known, as is the case for an eavesdropper, the gate becomes a completely depolarizing channel, mapping every state to the maximally-mixed state. A next step in this work might include performing some simple algorithms, such as a two-qubit Grover search, over encrypted data.

APPENDICES

Appendix A

Configuring Pockels cells

The Pockels cells used in the experiment in Chapter 4 were purchased from Bergmann Messgeraete Entwicklung KG (BME). They drive a rubidium titanyl phosphate, $RbTiOPO_4$ (RTP), with voltage oscillating between high (set to given the desired amount of retardance, polarization rotation). We drove the Pockels cells between $\pm V_{\lambda/4}$, using splitter boxes electronics designed by Thomas Jennewein and programmed by Zhizhong Yan. This different from previous experiments which operated the cells between 0 and $V_{\lambda/2}$.

The basic protocol for aligning and configuring a Pockels cell follows these steps.

1. Aligning the isogyre (Fig. A.1). An isogyre is an image which results from sending polarized and somewhat dispersed light through a birefringent material (Pockels cell) and placing a crossed polarizer on the other end. Light propagating along the material's optic axis will not change polarization and will be absorbed by the second polarizer, leaving a dark line in the resulting image, showing where the axis is. Ideally, the isogyre image is a cross, but some alignment is required to observe this. Here we performed many iterations of:

   (a) Using 2 of the 4 tilting degrees of freedom in the Pockels cell to back reflect the crystal.

   (b) Using the other 2 degrees of freedom to centre the isogyre crossing on the observed image (Note that until properly aligned, the dark bands may not form a cross, but rather look like an avoided crossing. But just keep repeating the steps and it will all be fine.)

2. Use single photons in a setup like that of Fig. A.2a.

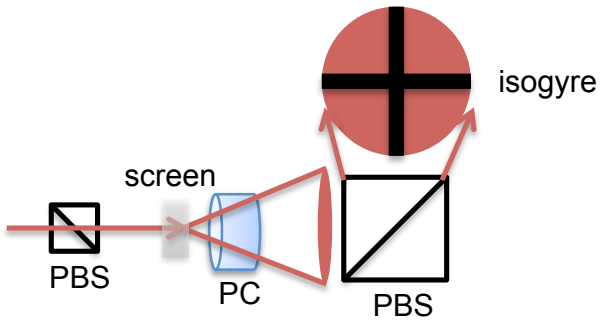


Figure A.1: Polarized light is dispersed through some cloudy screen (a sticky note was used) and propagated through the birefringent Pockels cell. Placing a crossed polarizer afterwards allows for the observation of the isogyre, an image which when properly aligned looks like a cross.

3. Send in each of two orthogonal input states (eg. $|H\rangle$ and $|V\rangle$), and looking at coincidence counts, vary driving voltage while measuring the state you expect output from the Pockels cell when the voltage is high (eg., for a Hadamard $\langle D|$ and $|A\rangle$). Choose the voltage that gives the best contrast between the two measurement bases.

4. Same as step 3, but vary the angle δ, changing the HWPs and QWP, to find the best contrast again.

5. Same as steps 3 and 4, but now vary the delay of the signal into the Pockels cell. The idea here is that when the Pockels changes from low to high voltage states, there is some "ringing", meaning the voltage is not instantly constant at the desired $V_{\lambda/4}$, and so changes the desired rotation. (Note that for the experiment in Chapter 4, we did not have to perform this step).

6. Iterate step 3-5 until the the contrast is reasonably high ($\sim 100:1$ should be easy to attain. With changing the delay $\sim 1000:1$ is possible).

The tables below show an example of data taken when configuring the second Pockels cell (performing $\mathbb{1}/H$). First, we set all the waveplates such that $\delta = 0$. We send in $|H\rangle$ and $|V\rangle$ and scan over the voltage while measuring coincidence counts over 5 seconds in both $\langle A|$ and $\langle D|$, to find the best contrast.

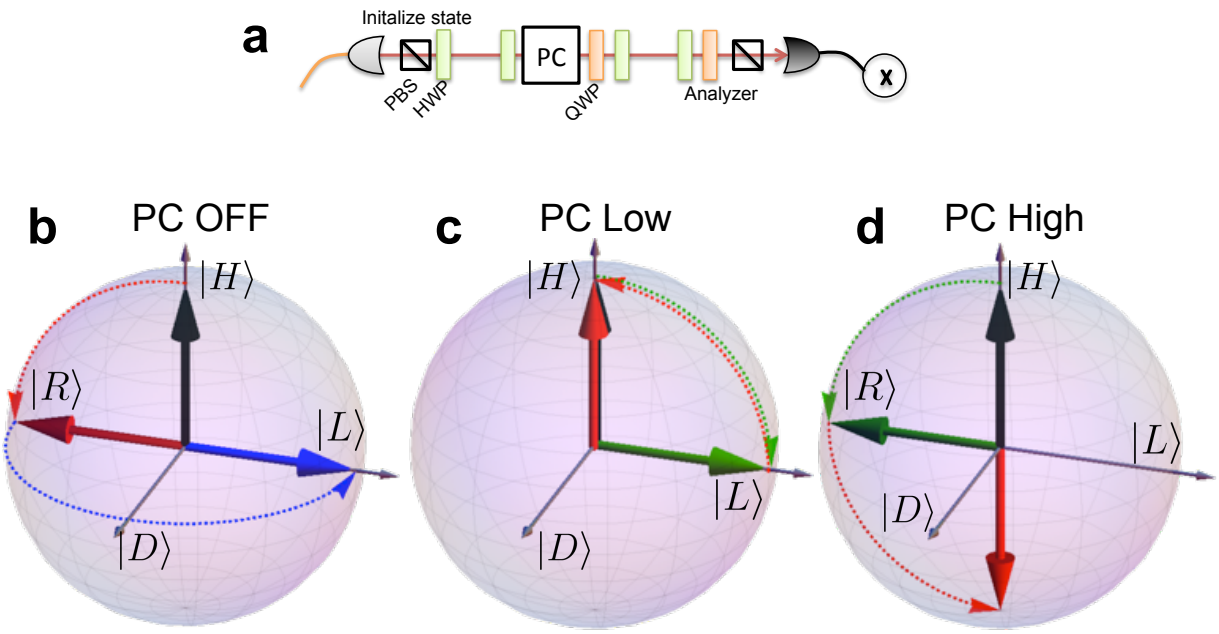


Figure A.2: (a) A simple setup to configure the Pockels cell. Photons are initialized as $|H\rangle$ from the PBS. The Pockels cell is sandwiched by HWPs, and a QWP. Finally, a polarization analyzer and photon detection. Coincidence counts with another photon detection should be used. (b)–(d) show the action of the HWP-PC-QWP-HWP setup when the Pockels cell is OFF, at low voltage, and at high voltage, respectively. For this example, the desired operation of the setup is to perform the identity when the PC is at low voltage, and an X rotation at high voltage. Recall from the discussion in Chapter 2 that this requires the HWPs to be at $\delta°$, and the QWP at $(45+\delta)°$ (since the PC crystal is aligned at $(45+\delta)°$ where $|\delta| \ll 1$).

	$\|H\rangle$		$\|V\rangle$	
$V(dial)$	$\langle A\|$	$\langle D\|$	$\langle A\|$	$\langle D\|$
1.5	156	3437	3382	61
1.6	113	3371	3255	59
1.7	96	3482	3248	56
1.8	69	3335	3135	61
1.9	56	3402	3153	84
2.0	40	3338	3101	85
2.1	52	3334	3071	117
2.2	45	3323	3118	192
2.3	64	3325	3009	217

The best contrast for $|H\rangle$ is $\sim 83:1$ at $V = 2.0$. For $|V\rangle$ it is $\sim 58:1$ at $V = 1.7$. We then set the voltage to $V = 1.85$, in between the two optima. Next, with the voltage set, we vary the angle discrepancy δ, changing the angle of each waveplate. We measure coincidence counts over 5 seconds for both $\langle A|$ and $|D\rangle$. Sending in $|H\rangle$ and $|V\rangle$ we get:

	$\|H\rangle$		$\|V\rangle$	
$\delta(^\circ)$	$\langle A\|$	$\langle D\|$	$\langle A\|$	$\langle D\|$
-3	72	3487	3374	40
-2	55	3471	3441	20
-1	47	3568	3391	27
0	61	3547	3387	52
1	112	3341	3432	138

The best constrast for $|H\rangle$ is $\sim 76:1$ at $\delta = -1^\circ$, and for $|V\rangle$ is $\sim 172:1$ at $\delta = -2^\circ$. The next step would be to scan over the delay time of the input signal to the Pockels cell. However, because of the nature of the experiment in Chapter 4, the time intervals for PC switching where long in comparison to other experiments, and so fine tuning of the delay was not necessary. Taking $\delta = -1.5^\circ$, we again scan over the voltage:

	$\|H\rangle$		$\|V\rangle$	
$V(dial)$	$\langle A\|$	$\langle D\|$	$\langle A\|$	$\langle D\|$
1.6	94	2982	2798	14
1.65	65	2874	2833	17
1.7	66	2984	2845	13
1.75	59	3072	2757	25
1.8	57	3047	2674	15
1.85	30	2901	2706	27
1.9	35	2993	2656	36
1.95	34	3114	2671	33
2.0	19	3113	2826	51
2.05	36	2962	2758	57
2.1	14	2931	2830	67
2.15	18	2972	2817	76
2.2	25	2955	2684	102

The best contrasts are again at $V = 2.1$ for $|H\rangle$ and $V = 1.7$ for $|V\rangle$, are greatly improved ($\sim 209:1$ and $\sim 218:1$). Taking the voltage to be in between, $V = 1.85$ we get contrasts $\sim 100:1$ for both inputs.

Figure A.3 shows the splitter box and electronics setup for Pockels cells in Chapter 4.

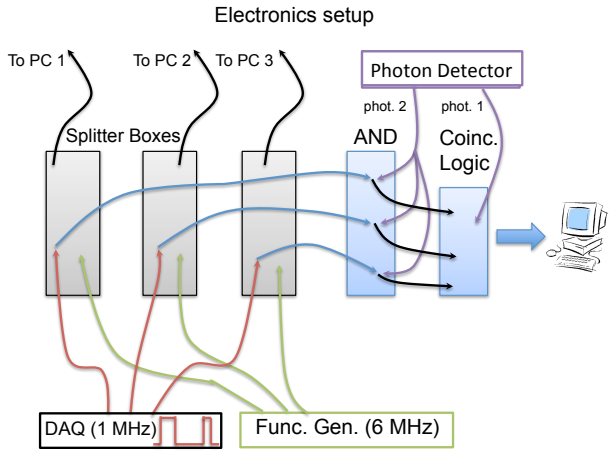


Figure A.3: Detected photons cause a TTL pulse to be generated from the single-photon counting modules. TTL pulses are passed through an array of AND logic with the square-wave pulses which drove the Pockels cell, originally produced from the DAQ. This results in TTL pulses sorted into times when the Pockels cell were acting as the identity, or as the assigned unitary.

Appendix B

Imperfection in the CNOT gate

B.1 Imperfect interference

The operation of the optical CNOT entirely depends on the quality of the two-photon interference at the initial partially-polarizing beamsplitter (PPBS). We used a motorized stage to adjust path delays, ensuring that we were operating the gate in the bottom of the HOM dip, which had the desired visibility. Nonetheless, we can see the effects of imperfect interference on the measured output state. This could be due to path lengths drifting over the course of the experiment. As can be seen in Fig. B.1, we have non-negligible contributions to the density matrix from what looks like a mixture of $|DH\rangle\langle DH|$ and $|VA\rangle\langle VA|$.

This can explained by considering the state $|D_a H_b\rangle$ in input modes a and b. Since they don't interfere at the PPBS we can consider their propagations through the setup separately. Recall from CNOT setup outlined in Chapter 2, that we begin with a Hadamard gate in path b before a and b modes interfere at a PPBS. Half-wave plates (HWP) at 45° are next, followed by another PPBS in each mode, now called c and d. Batears then perform an X operation on each mode, and finally another Hadamard acts on mode d. The $|D_a\rangle$ state then propagates as follows:

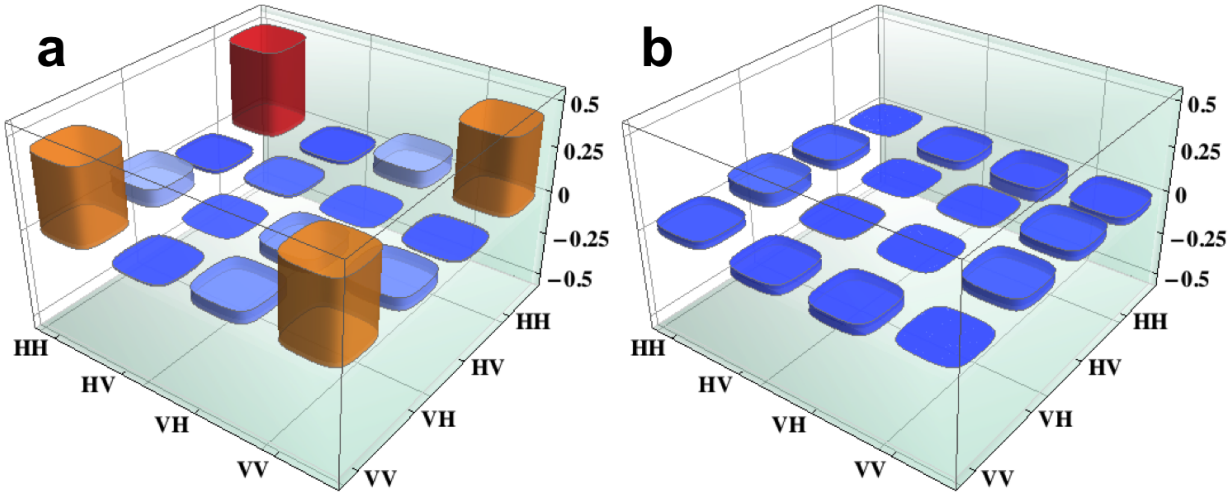


Figure B.1: The real (a) and imaginary (b) parts of an output density matrix from the CNOT. The input state was $|DH\rangle$.

$$
\begin{aligned}
|D_a\rangle \quad &= \quad \frac{1}{\sqrt{2}}\left(a_H^\dagger + a_V^\dagger\right)|0\rangle \\
&\xrightarrow{\text{PPBS}} \quad \frac{1}{\sqrt{2}}\left(c_H^\dagger + \frac{1}{\sqrt{3}}c_V^\dagger + \sqrt{\frac{2}{3}}d_V^\dagger\right)|0\rangle \\
&\xrightarrow{\text{HWPs}} \quad \frac{1}{\sqrt{2}}\left(c_V^\dagger + \frac{1}{\sqrt{3}}c_H^\dagger + \sqrt{\frac{2}{3}}d_H^\dagger\right)|0\rangle \\
&\xrightarrow{\text{PPBS}} \quad \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{3}}c_V^\dagger + \frac{1}{\sqrt{3}}c_H^\dagger + \sqrt{\frac{2}{3}}d_H^\dagger\right)|0\rangle \\
&\xrightarrow{\text{batears}} \quad \frac{1}{\sqrt{3}}\left(c_D^\dagger + d_V^\dagger\right)|0\rangle \\
&\xrightarrow{\mathbb{1}\otimes H} \quad \frac{1}{\sqrt{3}}\left(c_D^\dagger + d_A^\dagger\right)|0\rangle \\
&= \quad \frac{1}{\sqrt{3}}\left(|D_c\rangle + |A_d\rangle\right)
\end{aligned}
\tag{B.1}
$$

The input state $|H_b\rangle$ propagates as:

$$
\begin{aligned}
|H_b\rangle \quad &= \quad b_H^\dagger|0\rangle \\
&\xrightarrow{\mathbb{1}\otimes H} \quad \frac{1}{\sqrt{2}}\left(b_H^\dagger + b_V^\dagger\right)|0\rangle \\
&\xrightarrow{\text{PPBS}} \quad \frac{1}{\sqrt{2}}\left(d_H^\dagger + \frac{1}{\sqrt{3}}d_V^\dagger - \sqrt{\frac{2}{3}}c_V^\dagger\right)|0\rangle \\
&\xrightarrow{\text{HWPs}} \quad \frac{1}{\sqrt{2}}\left(d_V^\dagger + \frac{1}{\sqrt{3}}d_H^\dagger - \sqrt{\frac{2}{3}}c_H^\dagger\right)|0\rangle \\
&\xrightarrow{\text{PPBS}} \quad \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{3}}d_V^\dagger + \frac{1}{\sqrt{3}}d_H^\dagger - \sqrt{\frac{2}{3}}c_H^\dagger\right)|0\rangle \\
&\xrightarrow{\text{batears}} \quad \frac{1}{\sqrt{3}}\left(d_D^\dagger - c_V^\dagger\right)|0\rangle \\
&\xrightarrow{\mathbb{1}\otimes H} \quad \frac{1}{\sqrt{3}}\left(-c_V^\dagger + d_D^\dagger\right)|0\rangle \\
&= \quad \frac{1}{\sqrt{3}}\left(-|V_c\rangle + |D_d\rangle\right)
\end{aligned}
\tag{B.2}
$$

Since we measure coincidence photons between c and d modes, we would measure a mixture of $|D_cA_d\rangle$ and $|V_cA_d\rangle$. Moving the motor stage to completely outside of the HOM dip, this is precisely what we observe, see Fig. B.2. Refer back to Fig.B.1 and notice that thesis components are clearly visible in the density matrix, and diminish the state fidelity with the ideal Bell state.

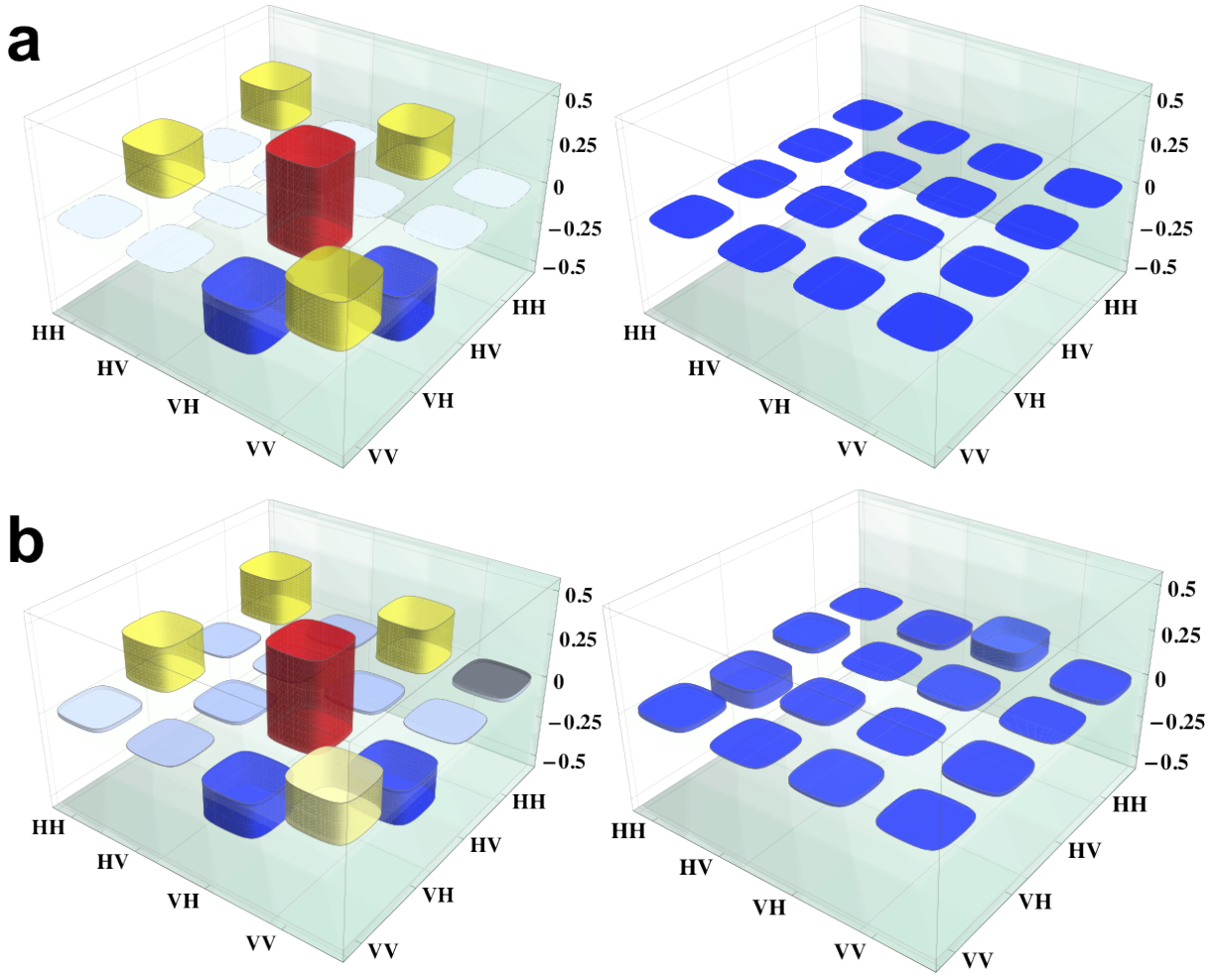


Figure B.2: Theoretical (a) and measured (b) density matrices for propagating $|DH\rangle$ through the CNOT setup when operating outside of the HOM dip. These components are still clearly visible when trying to operate the CNOT with the HOM dip.

References

[1] D. Aharonov, M. Ben-Or, and E. Eban. Interactive proofs for quantum computations. In *Proceeding of Innovations in Computer Science 2010 (ICS 2010)*, pages 453–469, 2010.

[2] M. P. Almeida, F. de Melo, M. Hor-Meyll, A. Salles, S. P. Walborn, P. H. Souto Ribeiro, and L. Davidovich. Environment-induced sudden death of entanglement. *Science*, 316(5824):579–582, 2007.

[3] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White. Ancilla-assisted quantum process tomography. *Phys. Rev. Lett.*, 90:193601, May 2003.

[4] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf. Private quantum channels. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2000)*, pages 547–553, 2000.

[5] P. Arrighi and L. Salvail. Blind quantum computation. *Int. J. Quantum Inf.*, 4:883898, 2006.

[6] K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi. Maximum-likelihood estimation of the density matrix. *Phys. Rev. A*, 61:010304, Dec 1999.

[7] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02)*, pages 449–458, 2002.

[8] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther. Demonstration of blind quantum computing. *Science*, 20:303–308, 2012.

[9] J.S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964.

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

[11] C .H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, pages 1895–1899, 1993.

[12] R.W. Boyd. *Nonlinear Optics*. Academic Press. Academic Press, 2008.

[13] S. Bravyi and A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Physical Review A*, 71:022316, 2005.

[14] H.J. Briegel, D.E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009.

[15] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, pages 517–526, 2009.

[16] A. Childs. Secure assisted quantum computation. *Quantum Information and Computation*, 5:456–466, 2005.

[17] A. M. Childs, D. W. Leung, and M. A. Nielsen. Unified derivations of measurement-based schemes for quantum computation. *Physical Review A*, 71:032318, 2005.

[18] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285 – 290, 1975.

[19] J. M. Chow, J. M. Gambetta, L. Tornberg, Jens Koch, Lev S. Bishop, A. A. Houck, B. R. Johnson, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf. Randomized benchmarking and process tomography for gate errors in a solid-state qubit. *Phys. Rev. Lett.*, 102:090502, Mar 2009.

[20] M. Christandl and S. Wehner. Quantum anonymous transmissions. In Bimal Roy, editor, *Advances in Cryptology - ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 217–235. Springer Berlin / Heidelberg, 2005.

[21] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded-quantum-storage model. In *Proceedings of the 46th IEEE Symposium on Foundations of Computer Science (FOCS 2005)*, 2005. Full version in SIAM Journal on Computing 37:1865-1890, 2008.

[22] D. Deutsch and R. Jozsa. Rapid Solution of Problems by Quantum Computation. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 439(1907):553–558, December 1992.

[23] I. Devetak and P. W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Communications in Mathematical Physics*, 256:287–303, 2005. 10.1007/s00220-005-1317-6.

[24] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Express*, 15(23):15377–15386, Nov 2007.

[25] S. Fehr and C. Schaffner. Composing quantum protocols in a classical environment. In *Proceedings of the Theory of Cryptography Conference (TCC '09)*, pages 350–367, 2009.

[26] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, June 1982.

[27] J. Fiurášek and Z. Hradil. Maximum-likelihood estimation of quantum processes. *Phys. Rev. A*, 63:020101, Jan 2001.

[28] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Theory of Computing (STOC '09)*, pages 169–178, 2009.

[29] A. Gilchrist, N. K. Langford, and M. A. Nielsen. Distance measures to compare real and ideal quantum processes. *Phys. Rev. A*, 71:062310, Jun 2005.

[30] D. Gottesman. The Heisenberg representation of quantum computers. In *Group 22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43, 1998.

[31] Markus Grassl, Zhengfeng Ji, Zhaohui Wei, and Bei Zeng. Quantum-capacity-approaching codes for the detected-jump channel. *Phys. Rev. A*, 82:062324, Dec 2010.

[32] L. K. Grover. A fast quantum mechanical algorithm for database search. In *ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING*, pages 212–219. ACM, 1996.

[33] M. B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5:255–257, April 2009.

[34] B. Hayes. Cloud computing. *Commun. ACM*, 51(7):9–11, July 2008.

[35] C. W. Helstrom. Detection theory and quantum mechanics. *Information and Control*, 10(3):254–291, 1967.

[36] M. Hillery and L. D. Mlodinow. Quantization of electrodynamics in nonlinear dielectric media. *Phys. Rev. A*, 30:1860–1865, Oct 1984.

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

[38] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, 80:5239–5242, Jun 1998.

[39] Z. Hradil and Řeháček J. Quantum measurement and information. *Fortschritte der Physik*, 51(2-3):150–156, 2003.

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

[41] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[42] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter. Linear optics controlled-phase gate made simple. *Phys. Rev. Lett.*, 95:210505, Nov 2005.

[43] A. Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):11911249, 1997.

[44] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, January 2001.

[45] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275 – 278, 1972.

[46] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White. Demonstration of a simple entangling optical gate and its use in bell-state analysis. *Phys. Rev. Lett.*, 95:210504, Nov 2005.

[47] J.-C. Lee, Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim. Experimental demonstration of decoherence suppression via quantum measurement reversal. *Opt. Express*, 19(17):16309–16316, Aug 2011.

[48] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen. Bell measurements for teleportation. *Phys. Rev. A*, 59:3295–3300, May 1999.

[49] A I Lvovsky. Iterative maximum-likelihood reconstruction in quantum homodyne tomography. *Journal of Optics B: Quantum and Semiclassical Optics*, 6(6):S556, 2004.

[50] G. J. Milburn. Quantum optical fredkin gate. *Phys. Rev. Lett.*, 62:2124–2127, May 1989.

[51] P.W. Milonni and J.H. Eberly. *Laser Physics*. John Wiley & Sons, 2010.

[52] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[53] J. L. O'Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White. Quantum process tomography of a controlled-not gate. *Phys. Rev. Lett.*, 93:080502, Aug 2004.

[54] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning. Demonstration of an all-optical quantum controlled-NOT gate. *Nature*, 426(6964):264–7, November 2003.

[55] D. W. Leung P. H. Hayden and D. Mayers. The universal composable security of quantum message authentication with key recycling. Unpublished manuscript, 20xx.

[56] Marco Piani, David Pitkanen, Rainer Kaltenbaek, and Norbert Lütkenhaus. Linear-optics realization of channels for single-photon multimode qudits. *Phys. Rev. A*, 84:032304, Sep 2011.

[57] R. Prevedel, D. R. Hamel, R. Colbeck, K. Fisher, and K. J. Resch. Experimental investigation of the uncertainty principle in the presence of quantum memory and its application to witnessing entanglement. *Nature Physics*, 7(10):757–761, July 2011.

[58] L. Qing, L. Jian, and G. Guang-Can. Linear optical realization of qubit purification with quantum amplitude damping channel. *Chinese Physics Letters*, 24(7):1809, 2007.

[59] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White. Linear optical controlled-not gate in the coincidence basis. *Phys. Rev. A*, 65:062324, Jun 2002.

[60] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[61] R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation with cluster states. *Physical Review A*, 68:022312 [32 pages], 2003.

[62] K. J. Resch, P. Walther, and A. Zeilinger. Full characterization of a three-photon greenberger-horne-zeilinger state using quantum state tomography. *Phys. Rev. Lett.*, 94:070402, Feb 2005.

[63] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. In *Foundations of Secure Computation*, pages 169–177, 1978.

[64] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[65] B. Rosgen and J. Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Proceedings of the 20th Conference on Computational Complexity*, pages 344–354, 2005.

[66] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[67] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[68] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, 2000.

[69] G. Smith and J. Yard. Quantum communication with zero-capacity channels. *Science (New York, N.Y.)*, 321(5897):1812–5, September 2008.

[70] R. R. Smith. Completely bounded maps between C^*-algebras. *Journal of the London Mathematical Society*, s2-27(1):157, 1983.

[71] J. Řeháček, D. Mogilevtsev, and Z. Hradil. Tomography for quantum diagnostics. *New Journal of Physics*, 10(4):043022, 2008.

[72] J. Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39:25–58, 2009. Preliminary version in *Proceedings of the 38th ACM Symposium on Theory of Computing (STOC '06)*, pages 296–305, 2006.

[73] M. M. Wolf and D. Pérez-Garçia. Quantum capacities of channels with small environment. *Phys. Rev. A*, 75:012303, Jan 2007.

[74] W. K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245–2248, Mar 1998.

[75] X. Zhou, D. Leung, and I. L. Chuang. Methodology for quantum logic gate construction. *Physical Review A*, 62:052316, 2000.