Applications of Single-Photon Two-Qubit Quantum Logic to the Quantum Information Science

by

Taehyun Kim

Submitted to the Department of Physics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2008

Author .....
Department of Physics
May 21, 2008

Certified by .....
Franco N. C. Wong
Senior Research Scientist
Thesis Supervisor

Certified by .....
Vladan Vuletic
Associate Professor
Thesis Supervisor

Accepted by .....
Thomas J. Greytak
Chairman, Department Committee on Graduate Students

Applications of Single-Photon Two-Qubit Quantum Logic to the Quantum Information Science

by

Taehyun Kim

Submitted to the Department of Physics
on May 21, 2008, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

In this thesis, I describe demonstration of various quantum information processing tasks using single-photon two-qubit (SPTQ) quantum logic. As an initial state of those tasks, I used various entangled photon pairs, and I describe development of a polarization entangled photon pair source based on a collinear spontaneous parametric down conversion (SPDC) process within a bidirectionally pumped periodically-poled potassium titanyl phosphate (PPKTP) crystal embedded in a polarization Sagnac interferometer and generation of hyper-entangled photon pairs that are simultaneously entangled in the polarization and momentum degrees of freedom. I also introduce deterministic quantum gates based on SPTQ quantum logic where the polarization and momentum degrees of freedom in a single photon are used as two qubits. By applying SPTQ quantum logic to different entangled states, I demonstrate several quantum information tasks such as transferring entanglement from the momentum qubits to the polarization qubits, SPTQ-based complete polarization Bell state measurements, entanglement distillation (Schmidt projection), and a physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 (BB84) quantum key distribution (QKD).

Thesis Supervisor: Franco N. C. Wong
Title: Senior Research Scientist

Thesis Supervisor: Vladan Vuletic
Title: Associate Professor

Acknowledgments

I am indebted to so many people for their help, without which I could not complete my research. First of all, I would like to make a big bow to Dr. Franco Wong for his fatherly supervision. Although I joined the group without any knowledge about optics experiments, he was patient with my slow progress, navigated my research direction, and gave me brilliant suggestions whenever I was stuck with various obstacles. I also like to thank Jeff Shapiro for leading me to the world of interesting research topics, and providing invaluable feedback and supports for my research throughout my graduate course.

I was also very lucky to have excellent committee members: Vladan Vuletic encouraged me to continue to pursue my goal and always remained next to me as a wonderful dissertation co-supervisor. Erich Ippen, with his great expertise, provided me valuable comments and, at the same time, was a critical discussant. Last but not least, Issac Chuang's understanding and knowledge in my field greatly refined my dissertation.

Special thanks go to Frank Würthwein and Dong-il Dan Cho. While I was working at Fermilab in 2002, I was very impressed with Frank's enthusiasm for physics. Even after having moved to UCSD, Frank was still (even more!) supportive. Working with Dong-il Dan Cho changed my life. When I was a undergraduate student studying computer science, I encountered him and his continuous inspiration guided me to step forward to the wonder of physics.

I feel deeply thankful to my labmates, specifically, Onur Kuzucu who joined the group one semester later than me, but had much more experience in nonlinear optics and I learned a lot from him about the experiments, and Marco Fiorentino, Marius Albota, and Chris Kuklewicz who also taught me a lot about the optics and the research from the scratch when I even didn't know how to clean optical components. In addition, there are many labmates who made my research in our group extremely pleasant: Pavel Gorelik, Ingo Stork genannt Wersborg, Dheera Venkatraman, Tian Zhong, Saikat Guha, Baris Erkmen, Mohsen Razavi, Brent Yen, Stefano Pirandola,

Julien Le Gouet, Raul Garcia-Patron Sanchez, and Mankei Tsang.

There is another group of people that I met in the MIT physics or another academic societies. Times that I shared with Keith Seng Mun Lee, Nuno Leonardo, Mark Neubauer, Andreas Korn, and Jedong Lee were very precious pieces in my doctoral student life.

I also have some Korean friends in Boston and, through their good friendship, I have been associated with diverse fields of research. Hence, I cannot miss any of their names: Yanghyo Kim (extra thanks!), Hyungsuk Lee, Byungchan Han, Sejoong Kim, Donghwan Ahn, Euiheon Chung, Kyungbae Park, Sanghyun Lee, Jin-oh Hahn, Dongwoon Bai, Sangwon Byun, Heejae Kim, Jongseung Yoon, Yongsuk Kim, Jongyoon Kim, Jae Hyung Yi, and Sung Hoon Kang.

A gang of buddies all of whom I have known in Korea for more than 20 years, has never stopped spritually supporting me. I thank Sungjun Kim, Jaehyung Lee, Younghoon Sohn, Seunghoon Lee, and Junghyun Yu for their always being there for me.

My college friends who spent four years together studying at Department of Computer Engineering, Seoul National University, and friends that I worked together at MEMS, during my Master's course at Division of Electrical Engineering, Seoul National University are heartily appreciated.

Additionally, Cathy Bourgeois, Josephina Lee, and Sukru Cinar were the best staffs ever. Their friendly helps made my graduate days free from any administrative trouble.

I want to give the warmest credit to my parents, Daekeun and Jungin, parents-in-law, Su, and Jooyoung.

I also like to thank Ilju foundation and HP-MIT alliance for their financial support.

Finally, I would like to express my apologies to any person that I forgot to mention.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In quantum information processing (QIP), information is stored in quantum mechanical systems and processed through the interactions between the quantum systems following the laws of quantum mechanics. There are several candidates for QIP systems, including photons, neutral atoms, ions, nuclear spins, quantum dots, and Josephson junctions, and each quantum system has advantages and disadvantages as a platform to perform QIP tasks. Among these quantum systems, this thesis presents demonstration of QIP tasks using a photonic system.

The photon is an ideal candidate for exchanging qubits between remote sites thanks to its long coherence time, and therefore it has been considered as an essential quantum system for transferring the quantum state in a quantum network [1], establishing entanglement over a long distance [2, 3], and quantum key distribution (QKD) [4]. The photon is also considered as a platform to implement quantum logic, but deterministic quantum operations between two photons generally require strong nonlinearity [5, 6] or efficient coupling between the photon and atomic systems [7], both of which are of current research interest. To avoid these difficult requirements, in 2001, Knill *et al.* [8] showed that efficient quantum computation can be implemented with linear optics using single photons and photon detection, and similar schemes have followed [9, 10, 11]. However, all of these schemes still require ideal single-photon sources and highly-efficient single-photon detectors, which are currently under development by many other groups. Therefore to demonstrate various QIP tasks using

currently available technology, we take a different approach of using the multiple degrees of freedom in a single photon as multiple qubits [12, 13, 14]. This multiple-qubit approach enables us to implement deterministic quantum logic with a relatively simple setup compared to other optical quantum logic approaches, but it is not scalable quantum logic due to the increased complexity of the optical setup as the number of qubits increases. This limitation is acceptable if the photons are entangled in some degrees of freedom and if only few-qubit operations are of interest in small-scale QIP tasks.

In our group, in addition to the usual polarization degree of freedom as one type of qubit (P qubit), we use two separate momentum modes of the same photon (or two parallel paths after collimation) to represent $|0\rangle$ and $|1\rangle$ of another qubit (M qubit). This type of identification allows us to develop reliable single-photon two-qubit (SPTQ) quantum logic such as single-qubit quantum gates and controlled-NOT (CNOT) gates. Previous implementations of SPTQ quantum logic [12, 13, 14, 15, 16] separate the two paths of the M qubit into different directions and combine those two paths whenever the quantum logic operation is necessary. Such implementations are not robust because the apparatus is essentially a large and complex interferometer. The necessary coherence for these paths implies that they must be stabilized, and therefore these interferometric methods are less attractive from a practical standpoint. In contrast, our group collimates two non-parallel momentum vectors into two parallel paths so that their path lengths are identical as they propagate in space. This choice of momentum qubit also allows compact experimental setups and it is compatible with the phase-stable polarization-controlled NOT (P-CNOT) gate developed by Fiorentino and Wong [17]. This P-CNOT is essential in building other phase-stable SPTQ quantum gates used in most of the experiments in this thesis.

To demonstrate interesting QIP tasks with SPTQ quantum logic beyond using a single photon, I first developed a high-quality high-flux polarization photon pair source that generates a singlet state

$$|\psi^-\rangle_{AB} = (|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B)/\sqrt{2}\,, \tag{1.1}$$

where H (V) represents horizontal (vertical) polarization, and the subscript A (B) means the photon is located at Alice's (Bob's) side. Entangled state was originally generated using several different physical systems [18, 19, 20] to test Bell's inequality [21] that can resolve the Einstein, Podolsky, and Rosen (EPR) paradox [22]. Later entangled state also turned out to be an important resource in QIP, and many research groups have tried to find an efficient way to generate the high-quality entangled state.

In 1988, Shih and Alley [23] used photon pairs generated from spontaneous parametric downconversion (SPDC) to test Bell's inequality, but the output state was a product state, and they had to post-select entangled pairs. In 1995, Kwiat *et al.* [24] generated truly polarization entangled photon pairs by collecting the photons at the intersection of two emission cones from SPDC in a single β-barium borate (BBO) nonlinear crystal with type-II phase-matching and obtained a normalized flux of 0.07 pairs/s per mW of pump power in 1-nm bandwidth with a high degree of entanglement. Even though this method is still being used by some of the groups due to its relatively simple setup, this method had some limitations in generating high-flux output mainly due to the non-collinear phase-matching condition of the BBO crystal and the need to use several types of filtering to make the two terms in Eq. (1.1) indistinguishable in their spatial, spectral, and temporal modes. To avoid some of these problems, Kwiat *et al.* [25] combined two orthogonally-polarized output modes from two cascaded BBO crystals with type-I phase-matching, but the maximum output flux is still limited by the non-collinear output modes. To overcome these limitations, our group took a different approach. Kuklewicz *et al.* [26] used a periodically poled $KTiOPO_4$ (PPKTP) crystal in a collinear phase-matched configuration that is a well-known technique in the nonlinear optics to increase the output flux. The collinear geometry increased the output flux, but this setup required post-selection and the same types of filtering as the single BBO setup.

In order to make the output indistinguishable in all other modes except the polarization, Fiorentino *et al.* [27] generated the two terms in Eq. (1.1) by coherently pumping a single PPKTP crystal from two opposite directions and combined the two output modes with a Mach-Zehnder interferometer (MZI). This setup increased the

output flux by removing the requirements for spatial, spectral, and temporal filtering, but the fidelity of the output was limited mainly due to the need for phase stabilization and the large size of the interferometer. To solve these problems, a new phase-stable configuration was devised. I embedded the bidirectionally pumped PPKTP inside a polarization Sagnac interferometer (PSI), and its compact size and excellent phase stability allowed us to obtain a normalized flux of 700 pairs/s/mW/nm with quantum interference visibility of 99.45% making it one of the best bulk-crystal entanglement sources. The development of this system is described in Chapter 2 and published in Ref. [28, 29].

As a first application of SPTQ quantum logic to entangled photon pairs, Marco Fiorentino and I demonstrated the transfer of entanglement from the momentum qubits to the polarization qubits of the same photon pair. Momentum entangled photon pairs were generated by collecting the non-collinear output modes from SPDC process, which was first demonstrated by Rarity and Tapster [30]. The entanglement stored in the momentum qubits was transferred to the polarization qubits by using a quantum SWAP gate constructed by the P-CNOT and momentum-controlled NOT (M-CNOT) gates. At the output, we verified that the polarization qubits were entangled, confirming the coherent transfer of the quantum state between two types of qubits. The experimental results are presented in Chapter 3 and published in Ref. [31].

SPTQ quantum logic is well suited for characterizing hyper-entangled photon pairs. Hyper-entangled state refers to a pair of photons which are entangled in more than one degree of freedom simultaneously [32]. In 2005, Cinelli *et al.* [15, 34] and Yang *et al.* [16] generated a hyper-entangled state which is entangled in the polarization and momentum degrees of freedom, and Barreiro *et al.* [33] generated a hyper-entangled state which is entangled in polarization, spatial mode, and energy-time. However, all of these hyper-entangled sources are based on single or double BBO systems with non-collinear output modes and therefore those systems have restriction in terms of available output spatial mode. In our experiment, to generate hyper-entangled photon pairs which are entangled in polarization and momentum simultaneously, I utilized the polarization entangled photon pair source introduced in

Chapter 2 and collected non-collinear output modes similar to the momentum entangled photon pair source used in Chapter 3. In our system, I picked two near-collinear output modes, which is an ideal input mode for the parallel-beam SPTQ quantum logic gates. To demonstrate that the output photon pairs are hyper-entangled, I performed SPTQ-based complete polarization Bell state measurement that was originally proposed by Walborn *et al.* [35] to distinguish four different polarization Bell states deterministically with the help of momentum entanglement. SPTQ-based complete polarization Bell state measurement was implemented by Schuck *et al.* [36] for the photon pairs that are entangled in polarization and energy-time, and by Barbieri *et al.* [37] for the pairs entangled in polarization and momentum. In contrast, our hyper-entanglement source and SPTQ quantum logic are based on the parallel-beam geometry that is different from other constructions. Our measurements show a much higher accuracy in identifying the four different polarization Bell states, suggesting that we had better entanglement quality in our hyper-entangled state and higher reliability in our SPTQ quantum logic. The experimental setup and measurement results are described in Chapter 4.

With SPTQ quantum logic and the hyper-entangled state, I also experimentally demonstrated Schmidt projection protocol proposed by Bennett *et al.* [38]. There are several methods to extract maximally entangled states out of partially entangled states [39, 40, 41, 42, 43, 44, 45, 46]. Among these methods, Schmidt projection has an interesting property that its distillation efficiency can approach unity when it is applied to infinite number of input pairs. Even with such an advantage, Schmidt projection was avoided in the experimental implementation because it requires a collective measurement on multiple qubits. Implementation of a collective measurement is generally difficult, but for the case of hyper-entangled state, the measurement is simple, thus allowing us to implement the Schmidt projection on the hyper-entangled state using SPTQ quantum logic. In this experiment, one of the interesting challenges was to control the degree of momentum entanglement, and this problem was partially addressed by Walborn *et al.* [59] by moving the double aperture masks at the output of the SPDC source. However this method is not an efficient solution because it is

necessary to realign the experimental setup whenever the double aperture mask is moved. Our solution was to fix the location of the double aperture mask at an asymmetric position, and to utilize the fact that the emission angle of SPDC process can be controlled by the temperature of the PPKTP crystal. In this experiment, I was able to distill the maximally entangled states independent of the initial state, and the efficiency of the distillation agreed with the expected value, thus demonstrating the Schmidt projection protocl for the first time. The details of this experiment and the measurement results are described in Chapter 5.

Finally, we have physically simulated the entangling-probe attack on Bennett and Brassard 1984 (BB84) QKD protocol [4] using SPTQ quantum logic and polarization-entangled photon pair source. The BB84 protocol is the first QKD protocol, and due to its relatively simple configuration, it has been implemented by many groups in free-space [47, 48, 49, 50] as well as in fiber [51, 52, 53]. In BB84 protocol, one of the fundamental question is how much information the eavesdropper (Eve) can gain under ideal BB84 operating conditions, and a series of analyses by Fuchs and Peres [54], Slutsky *et al.* [55], and Brandt [56] showed that the most powerful individual-photon attack can be accomplished with a CNOT gate that entangles the polarization qubit of the BB84 photon with a probe qubit provided by Eve. Shapiro and Wong [57] proposed that this entangling-probe attack can be implemented in a proof-of-principle experiment using single-photon two-qubit (SPTQ) quantum logic. Following the suggestion in this proposal, I implemented the entangling-probe attack on BB84 and confirmed that Eve can obtain nearly the expected amount of information about the secret key for a given level of induced errors between Alice and Bob. The results are noteworthy because they include realistic amounts of error from the optical components in the setup, suggesting that SPTQ-based physical simulation is a useful technique. This experiment is described in Chapter 6 and has been published in Ref. [58].

Organization

This thesis is organized as follows. In Chapter 2, development of polarization entangled photon pair source based on a PSI is described. This chapter starts with a review of SPDC properties, and describes the main problems of previous polarization entanglement sources, then explains the main features of the polarization-entangled photon pair source based on a PSI.

In Chapter 3, I introduce SPTQ quantum logic and demonstrate a two-qubit SWAP gate application. I then describe the implementation of basic quantum gates and a SWAP gate, and I present the experiment of transferring the entanglement originally stored in the momentum qubits to the polarization qubits by using the SWAP gate.

In Chapter 4, generation and verification of a hyper-entangled state is described. This chapter starts by explaining how to generate hyper-entangled photon pairs and presents the experimental setup and the results of SPTQ-based complete polarization Bell state measurements.

In Chapter 5, I describe our physical implementation of Schmidt projection. I first explain the concept of Schmidt projection and describe how to implement such a distillation protocol in an experiment using hyper-entangled photon pairs. Then the experiment setup and results of the Schmidt projection protocol are presented.

In Chapter 6, I describe a physical simulation of the entangling-probe attack on the BB84 quantum key distribution (QKD) using SPTQ quantum logic. I explain how the entangling-probe attack works and how to implement it using SPTQ, followed by the experimental setup and results. Finally I conclude and summarize in Chapter 7.

Chapter 2

Polarization-entangled photon pair source

Entanglement is a key ingredient in quantum information science. Historically, entanglement is the unique quantum property that explains the Einstein-Podolsky-Rosen (EPR) paradox [22] and it was used to formulate the Bell's inequality [21, 69] to distinguish quantum mechanics from hidden-variable theories. More recently, entanglement is used as an important quantum resource in applications such as quantum teleportation [60], quantum cryptography [61], quantum computation [8, 62, 63], and quantum repeater [65]. For efficient quantum operations, these applications generally require a steady and copious supply of highly-entangled quantum states. Also in this thesis, we are using the entangled states to demonstrate various quantum information processing tasks. Therefore the main focus of this chapter is on an innovative photonic entanglement source design with significantly higher output flux and higher entanglement to be used in some of these applications. Our design of a high-flux, high-quality polarization-entangled photon pair source based on spontaneous parametric down conversion (SPDC) takes advantage of many advances in the field of nonlinear optics to achieve our goal.

In the first section we review some of the important properties of SPDC that are useful for understanding polarization-entangled photon pair sources presented in this chapter and utilized in experiments shown in later chapters. The second section

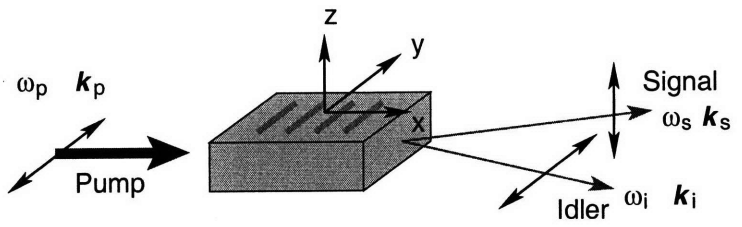

Figure 2-1: Schematic of SPDC process. We used a 10-mm-long (crystallographic X axis), 2-mm-wide (Y axis), 2-mm-thick (Z axis) flux-grown PPKTP crystal with a grating period of $\Lambda = 10.03\,\mu$m.

presents several types of polarization-entangled sources, and explains the limits of their performances. In the next section we show that these limitations can be overcome by combining bidirectionally pumped SPDC with a Sagnac interferometer, and we present an experimental demonstration of a high flux entangled photon pair source based on this design. The last section describes how this system can be optimized, and presents experimental results showing significant improvement in entanglement quality.

2.1 Theory of spontaneous parametric down conversion

SPDC is one of the most successful methods to generate high-quality entangled photon pairs, and therefore it has been used in all the experiments presented in this thesis. In this section, we provide a brief overview of some of the important properties of SPDC, which will be used throughout the subsequent chapters.

Spontaneous parametric down conversion is a second-order nonlinear frequency mixing process in which a pump photon at ω_p is converted into two lower-frequency photons called signal (ω_s) and idler (ω_i). The efficiency of SPDC depends on the phase matching function that typically depends on various parameters such as crystal orientation, temperature, and custom engineered grating structures. Common crystals used for SPDC include β-barium borate (BBO), periodically poled lithium niobate (PPLN), and periodically poled $KTiOPO_4$ (PPKTP).

Typically in our experiments, we pump a PPKTP crystal with a 405-nm laser beam propagating along the x-axis of the crystal, and the pump polarization is oriented along the y-axis as shown in Figure 2-1. For the output, we collect the near-degenerate downconverted signal and idler beams close to the collinear mode. In a type-II phase-matched process, the signal is polarized along the crystal's z-axis while the idler is polarized along the y-axis. The KTP crystal used in our experiment is periodically poled with a grating period $\Lambda = 10.03\,\mu$m for type-II quasi-phase matching condition for collinear near-degenerate SPDC with a 405-nm pump operating near room temperature.

Quantum mechanically SPDC can be described by a simplified effective Hamiltonian

$$\hat{H} \sim \hat{a}_p \hat{a}_s^\dagger \hat{a}_i^\dagger + H.c., \tag{2.1}$$

where $\hat{a}_p$ is the annihilation operator for the pump photon and $\hat{a}_s^\dagger, \hat{a}_i^\dagger$ are the creation operators for the signal and idler photons, respectively. A more complete Hamiltonian is given in Eq. (A.1) in the Appendix A. Eq. (2.1) simply states that when a pump photon is annihilated, a pair of signal and idler photons are created, and the reverse process also happens. In implementing SPDC in the laboratory, there are additional restrictions that can be derived from a more detailed calculation. When the pump laser is in TEM_{00} mode with a beam waist w_0 and frequency $\omega_p = ck/n$ (k is the wavenumber and n is the index of refraction inside the crystal), the output state is proportional to the following state according to Eq. (A.24):

$$|\psi\rangle \sim L_x A_p \int d\omega_s \int d^2k_s^\perp \int d^2k_i^\perp \exp\left[-\frac{w_0^2}{4}\left(k_{p,y}^2 + k_{p,z}^2\right)\right] \mathrm{sinc}(\Delta k_x L_x/2) \hat{a}_{\mathbf{k}_s}^\dagger \hat{a}_{\mathbf{k}_i}^\dagger |0\rangle, \tag{2.2}$$

where L_x is the length of the crystal, A_p is proportional to the amplitude of the pump electric field, $\int d^2k^\perp$ means integration in the transverse plane (yz-plane), the transverse component of the pump wave vector ($\mathbf{k}_p$) is $\mathbf{k}_p^\perp = \mathbf{k}_s^\perp + \mathbf{k}_i^\perp$, the x-component of the pump wave vector is $k_{p,x} = k - |\mathbf{k}_p^\perp|^2/2k$, the x-components of the signal and idler wave vectors ($\mathbf{k}_s, \mathbf{k}_i$) are $k_x = \pm\sqrt{n^2\omega^2/c^2 - k_y^2 - k_z^2}$, $\Delta k_x = k_{x,p} - k_{x,s} - k_{x,i} - 2\pi/\Lambda$, and Λ is the crystal's grating period. The details of the derivation is given in

Appendix A.

In Eq. (2.2), $\omega_i = \omega_p - \omega_s$ is implicitly assumed for the integration, which corresponds to the requirement of photon energy conservation. Momentum conservation is also required in an ideal case, but the finite length of a crystal relaxes this requirement. The finite length of the crystal shows up in terms of $\mathrm{sinc}(\Delta k_x L_x/2)$, which means that as long as the longitudinal momentum mismatch is less than order of $1/L_x$, down conversion is efficient. In contrast, the transverse momentum is conserved as long as the transverse dimension of crystal is larger than the beam waist of the pump, which is typically the case.

In the following subsections, I will discuss several important properties such as the dependence of the momentum correlation on the pump beam waist and the temperature dependence of the spectral distribution and the momentum direction based on Eq. (2.2).

2.1.1 Transverse momentum correlation of SPDC

The output photons from the SPDC process are generated in multi-spatial modes, and we need to consider the flux in each mode, which is governed by the probability amplitude given by Eq. (2.2). Note that Eq. (2.2) is actually a probability amplitude of pair generation, and in addition to the individual flux in each mode, Eq. (2.2) provides information about correlation between two different spatial modes. In this subsection, we will describe how this spatial mode correlation is affected by the pump beam waist (w_0).

The distribution of the transverse momentum of the signal and the idler is mainly governed by the term

$$\exp\left[-\frac{w_0^2}{4}\left((k_{s,y}+k_{i,y})^2+(k_{s,z}+k_{i,z})^2\right)\right] \tag{2.3}$$

in Eq. (2.2). This factor comes from the Gaussian distribution of the transverse momentum of the pump beam as given in Eq. (A.17). According to Eq. (2.3), the transverse components of the signal and idler wave vectors can have completely differ-

ent correlations under two different pump focusing conditions. For a tightly focused pump laser (small w_0), Eq. (2.3) is non-zero even if $\mathbf{k}_s^\perp$ is pointing in the same direction as $\mathbf{k}_i^\perp$, as long as $|\mathbf{k}_i^\perp + \mathbf{k}_s^\perp|$ is smaller than $1/w_0$. In other words, for a tightly focused pump beam, the signal and idler do not have any correlation in their momentum directions, which is useful for efficient coupling of the SPDC output to single-mode fibers which mainly accept photons with no transverse momentum [66]. If we use a loosely focused pump beam ($w_0 \to \infty$), the transverse component of the signal wave vector is anti-correlated with the transverse component of the idler wave vector (i.e., $\mathbf{k}_s^\perp = -\mathbf{k}_i^\perp$). In our experiments, we chose the second option because we were interested in strong momentum correlation. For the pump beam waist, we used $w_0 \approx 160\,\mu$m, and this corresponds to $\sim$4 mrad uncertainty in the wave vector direction inside the crystal.

2.1.2 Spectral distribution of SPDC

In this subsection, we will consider the correlation between the peak output wavelength and the crystal temperature. The peak output wavelength for a given output geometry $(\mathbf{k}_s, \mathbf{k}_i)$ is mainly determined by the phase-matching $\mathrm{sinc}(\Delta k_x L_x/2)$ factor in Eq. (2.2). The wave vector phase mismatch along the crystal's x-axis

$$\begin{aligned}\Delta k_x &= k_{x,p} - k_{x,s} - k_{x,i} - 2\pi/\Lambda \\ &= k_{x,p}(\omega_p, \mathbf{k}_s^\perp + \mathbf{k}_i^\perp, T) - k_{x,s}(\omega_s, \mathbf{k}_s^\perp, T) - k_{x,i}(\omega_p - \omega_s, \mathbf{k}_i^\perp, T) - 2\pi/\Lambda \\ &= \Delta k_x(\mathbf{k}_s^\perp, \mathbf{k}_i^\perp, \omega_p, \omega_s, T) \end{aligned} \tag{2.4}$$

is a function of the transverse momentum vectors ($\mathbf{k}_s^\perp$, $\mathbf{k}_i^\perp$), pump frequency (ω_p), signal frequency (ω_s) and temperature (T). (Δk_x changes with temperature through the temperature dependence of the crystal's Sellmeier equation.) Therefore, the spectrum of the SPDC output depends on the specific configuration one uses in the experiment. In our experiments, we generally start with a fixed pump frequency (ω_p) and a collinear output momentum direction ($\mathbf{k}_s^\perp = \mathbf{k}_i^\perp = \mathbf{0}^\perp$) that is determined by the positions of the signal and idler output apertures. Therefore, if we choose to

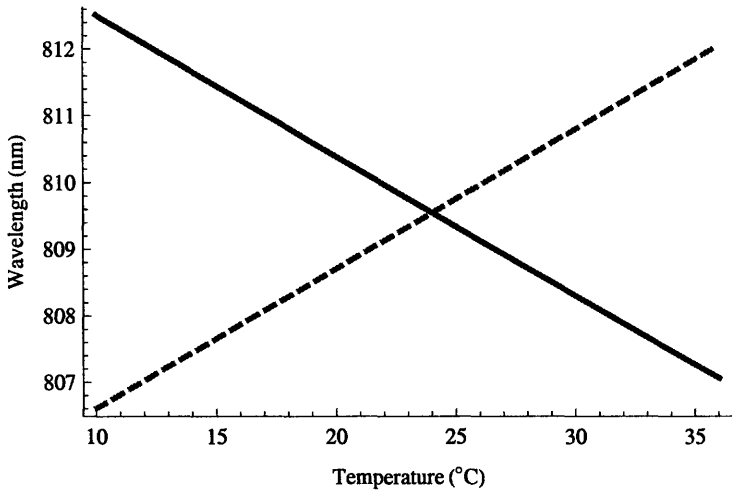

Figure 2-2: Plot of calculated (see Appendix B) signal (solid curve) and idler (dashed curve) peak center wavelength for collinear outputs as a function of crystal temperature. The pump wavelength is assumed to be 404.775 nm.

maximize the output at some frequency ω_s, we can find the optimal temperature by solving the equation

$$\Delta k_x(\mathbf{k}_s^{\perp} = 0, \mathbf{k}_i^{\perp} = 0, \omega_p, \omega_s, T)|_{\text{fixed } \omega_p} = 0. \tag{2.5}$$

In Figure 2-2, we plot the optimal signal and idler wavelength as a function of the crystal temperature for the collinear outputs.

The $\text{sinc}(\Delta k_x L_x/2)$ dependence allows non-zero Δk_x when Δk_x is smaller than $\sim 1/L_x$. Therefore the output will have some frequency components even though they do not completely make Δk_x zero. As shown in Figure 2-3, the output spectrum shows a finite bandwidth around the optimal frequency given by Eq. (2.5). This output signal bandwidth is a function of the crystal length and the type of phase matching. Typically, the bandwidth is inversely proportional to the crystal length. To obtain a narrower bandwidth, a longer crystal should be used. In our setup, the calculated bandwidth is ~ 0.6 nm. In actual experiments, the effective bandwidth can be slightly larger depending on the size of the collection aperture. In our experiment, the output bandwidth is set by a 1-nm bandwidth interference filter centered around 810 nm.

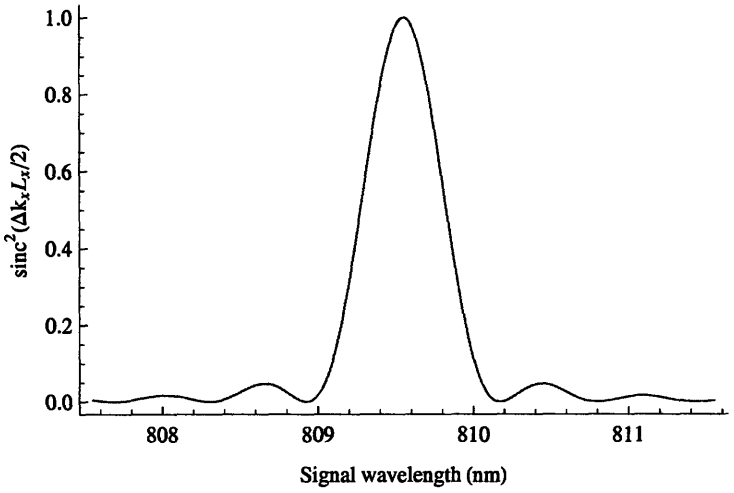

Figure 2-3: Relative pair generation probability along collinear direction ($\mathbf{k}_s^\perp = \mathbf{k}_i^\perp = \mathbf{0}$) as a function of signal wavelength. Temperature is chosen such that degenerate output pair ($\lambda = 809.55$ nm) have the maximum generation probability. In calculation, we assume 10-mm PPKTP with Λ=10.03 nm.

2.1.3 Momentum dependence on temperature

In the previous section, we showed that Δk_x is a function of the transverse momentum vectors, the pump frequency, the signal frequency, and the temperature and once the transverse momentum vectors and the pump frequency are fixed, we can find a functional relationship between the signal frequency and the temperature. In this section we consider how the momentum direction changes as we vary the crystal temperature.

If we fix the signal frequency and allow $\mathbf{k}_s^\perp$ to vary, we can also find a set of $\mathbf{k}_s^\perp$ for a given temperature (T), which satisfy the equation

$$\Delta k_x(\mathbf{k}_s^\perp, \mathbf{k}_i^\perp, \omega_p, \omega_s, T)|_{\text{fixed } \omega_p, \omega_s} = 0. \tag{2.6}$$

For the loosely focused pump case as described in Section 2.1.1, $\mathbf{k}_i^\perp \approx -\mathbf{k}_s^\perp$ and we can find an optimal set of $\mathbf{k}_s^\perp$ vectors satisfying Eq. (2.6) for a given temperature. The optimal set of $\mathbf{k}_s^\perp$ generally forms a circular distribution, and Figure 2-4 shows the distribution of measured output flux in the $\mathbf{k}_s^\perp$ plane. The bright part in this Figure corresponds to the $\mathbf{k}_s^\perp$ vectors satisfying Eq. (2.6). The non-zero thickness of the ring

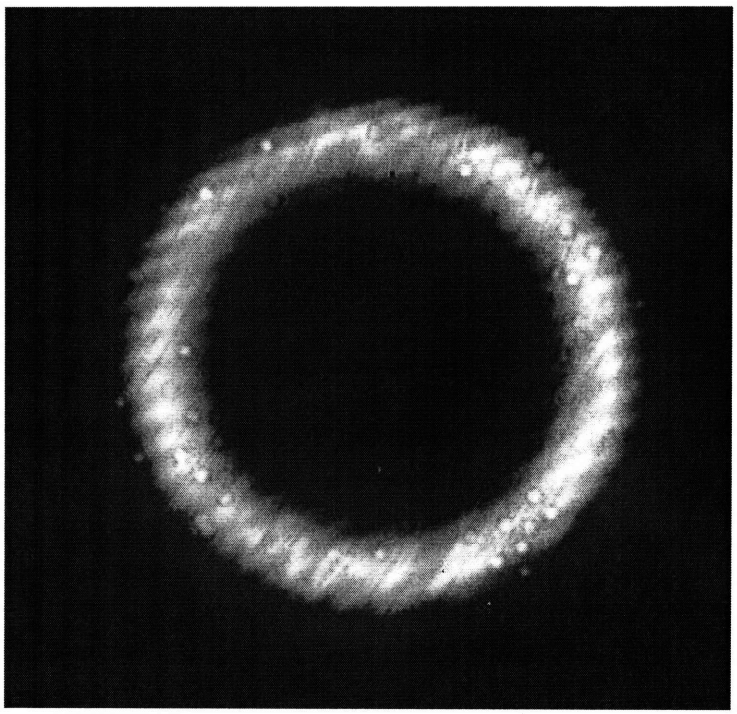

Figure 2-4: Measured spatial distribution of output idler photons ($\lambda_i = 810.050 \pm 0.5$nm) at a temperature $T_{crystal} = 12°C$, with 5 mW of 404.775-nm pump laser. Measurements were done using a CCD camera with a few-photon sensitivity. Collection time of this CCD image is 120 seconds.

shows that, even if $\mathbf{k}_s^\perp$ does not make Δk_x perfectly zero, there is some generation probability of idler photons with $-\mathbf{k}_s^\perp$ due to the finite width of the sinc function. The thickness of the ring is reduced as the length of the crystal (L_x) increases.

If we vary the crystal temperature, the optimal set of $\mathbf{k}_s^\perp$ with maximum output flux changes according to Eq. (2.6). The distribution of the corresponding optimal set of $\mathbf{k}_s^\perp$ is still in a ring shape, and we plot the radial distribution of the photon flux in Figure 2-5. The horizontal axis in this plot is the radial distance from the center of the ring that corresponds to the pump axis. We can use this property to control the relative flux ratio between two output paths which are asymmetrically located with respect to collinear output path. More discussion can be found in chapter 5.

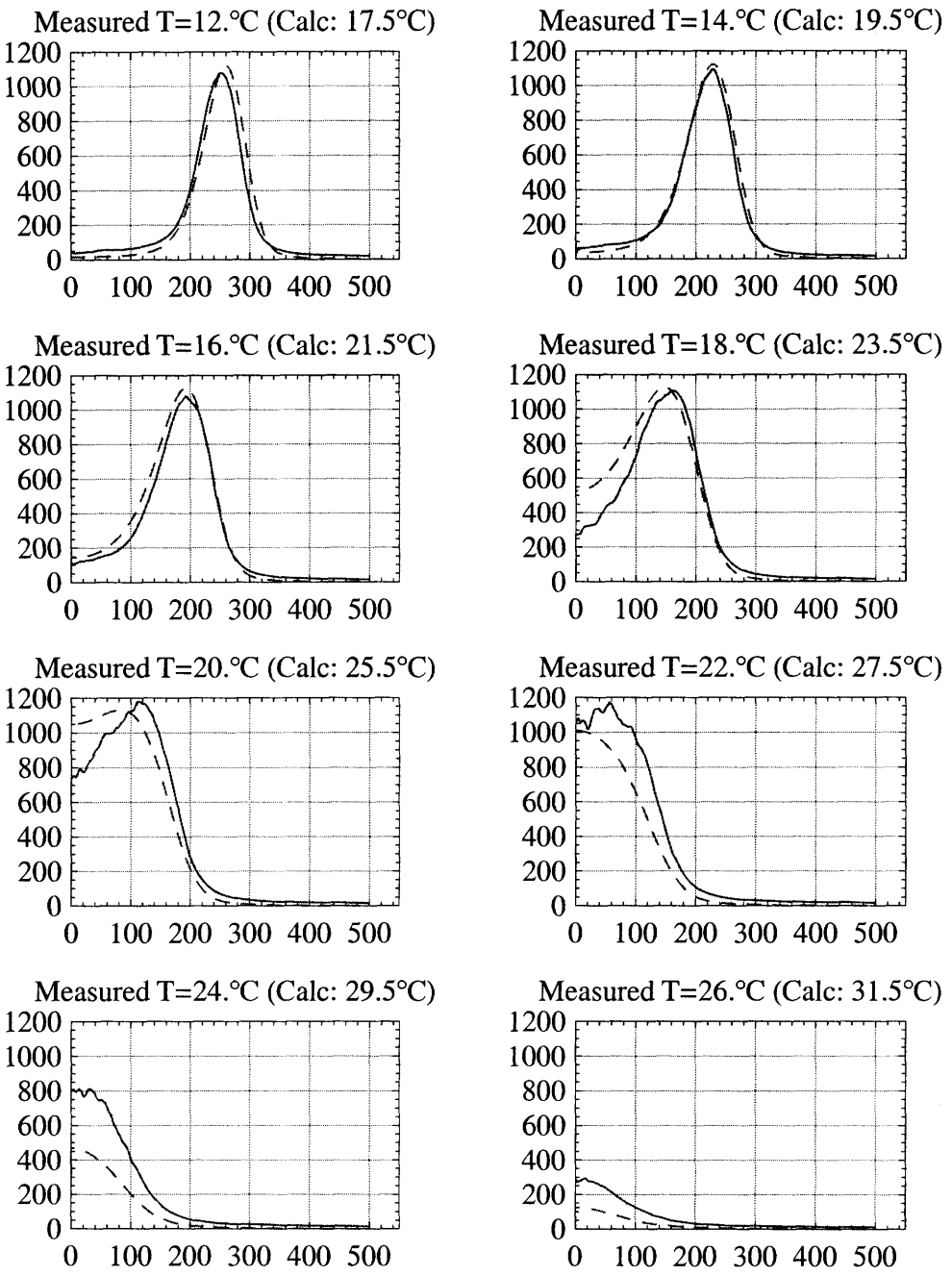

Figure 2-5: Angular distribution of output idler flux at different crystal temperature. Idler photons are collected with a 1-nm bandpass interference filter centered at 810.050 nm. Horizontal axis is the radial distance in the unit of CCD pixels from the center of the ring that corresponds to the collinear output location. The CCD camera is located at 250 mm from the crystal, and each pixel size is 20 μm $\times$ 20 μm. In each plot, theoretical prediction of output flux (dashed curve) is compared with the experimentally measured flux (solid curve). Note that there is a constant offset between the measured temperature and the temperature used for calculation. Collection time of each CCD image is 120 seconds.

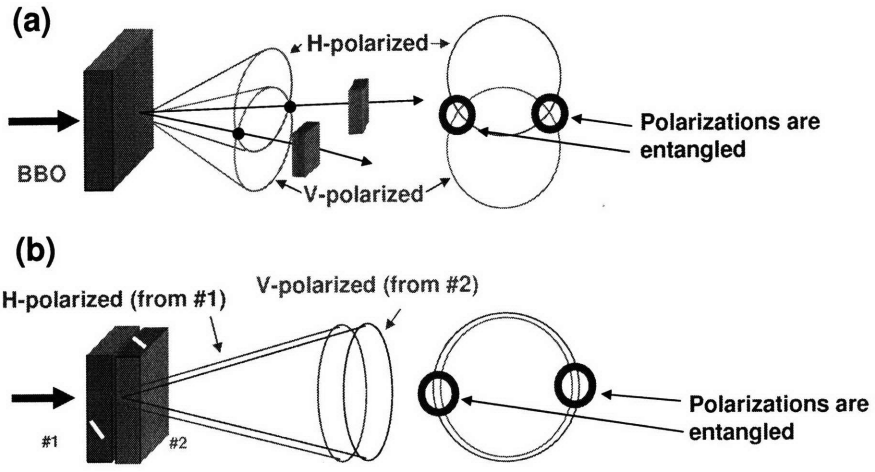

Figure 2-6: Two common methods for generating polarization-entangled photon pairs using BBO.

2.2 Previous polarization entangled photon pair sources based on SPDC

In quantum information processing, the entangled states are being destroyed whenever they are used for some quantum operations. For example, to teleport a qubit, we have to consume an entangled state. Therefore, for efficient quantum information processing requiring a large number of entangled qubits, we need a high flux source generating high-quality entangled states. To achieve this goal, several groups have tried different configurations to increase output flux and entanglement quality. In this section, I review some of the commonly used methods based on the BBO crystal and the PPKTP crystal, and discuss their limitations and how we can avoid the common problems.

Single BBO system

The simplest method that was developed by Kwiat *et al.* [24] is based on a single thin BBO crystal under type-II phase matching to generate non-collinearly propagating photon pairs that are polarization entangled as shown in Figure 2-6 (a). BBO is highly transparent in the UV and visible regions and angle phase matching allows tunable

wavelength operations. The single-crystal method generates polarization-entangled photon pairs in a relatively simple setup, but there are several drawbacks. The main problem is low output flux due to its geometry, because only the output pairs at the intersections of the two output rings are entangled in polarization, and the rest of the rings must be discarded using small apertures. The small apertures are also required in the output paths to increase the field of depth to interfere the pair generation processes occurring at $+x$ and $-x$ from the center of the crystal in order to eliminate spatial-mode distinguishability. However, the apertures reduce the flux throughput. Non-collinear geometry also prevents the use of a long crystal for increasing the flux. All of these considerations restrict the useful output flux. In addition to the restriction on flux, this system requires degenerate output wavelengths, because of the need to erase frequency information to achieve quantum interference between signal and idler in the same path. With this method, Kwiat *et al.* generated a normalized flux of 0.07 pairs/s per mW of pump power in 1-nm bandwidth when the measured quantum interference visibility is 0.978.

Double BBO system

To avoid some of the problems shown in a single BBO system, Kwiat *et al.* [25] introduced a new system using two BBO crystals operated with type-I phase matching. The optic axis of two thin BBO crystals are oriented orthogonal to each other and the output cones from those two crystals overlap as shown in Figure 2-6 (b). Compared to the single BBO system, the signal polarization at each point of the output cone is entangled with the idler polarization at the opposite point on the cone and hence we can expect more entangled pairs from the entire cone. In practice, we cannot collect the entire cone output efficiently, and it again limits the useful output flux. This type of arrangement still suffers the problem of spatial distinguishability and small apertures are required, thus limiting its output flux, and preventing it from using long crystals. With the better overlap of the signal and idler cones in this configuration, Kwiat *et al.* achieved 0.24 pairs/s/mW/nm with a visibility of 0.996 for a small aperture or 28 pairs/s/mW/nm with a lower visibility of 0.9 for a larger aperture[25].

Single PPKTP system

In general, the output flux is proportional to the square of the crystal length (L_x) as can be seen from Eq. (2.2), and BBO systems in a non-collinear geometry cannot utilize a long crystal to increase the flux. To mitigate this problem, Kuklewicz *et al.* [26] used a collinear configuration to allow a long (1-cm) PPKTP to be used under quasi-phase matching condition. This experiment yielded a higher spectral brightness of 300 pairs/s/mW/nm after timing-compensation and postselection with a 50-50 beam splitter, which is an order of magnitude larger than the double BBO system. However similar to BBO systems, the interference between the signal and idler output from type-II SPDC system requires timing-compensation due to crystal birefringence, and this also required a small aperture to avoid spatial-mode distinguishability, and therefore the effective output flux is limited at high visibility.

Double collinear SPDC system

Considering the problems explained above, it is clear that we need a configuration that is compatible with collinear outputs, and that can utilize most of the down-converted output without the restriction of apertures or interference filters. Such requirements can be satisfied by using two coherently pumped SPDC outputs as shown in Figure 2-7. Shapiro and Wong [67] proposed combining collinear signals and idlers from a pair of coherently driven optical parametric downconverters, which allows the use of long crystals for the increased flux, and avoids the needs for timing compensation and degenerate operation. To drive two SPDCs coherently, we can use the pump from the same source as shown in Figure 2-7 (a), forming a Mach-Zehnder interferometer (MZI). Consider a classical pump field at frequency ω_p, whose polarization is given by

$$\vec{E}_p = E_H \hat{e}_H + e^{i\phi_p} E_V \hat{e}_V \,, \tag{2.7}$$

where $\hat{e}_H$ and $\hat{e}_V$ are the horizontal (H) and vertical (V) polarization unit vectors, respectively, and ϕ_p is the relative phase between the H and V components.

The H-polarized pump component excites crystal A and generates an (unnor-

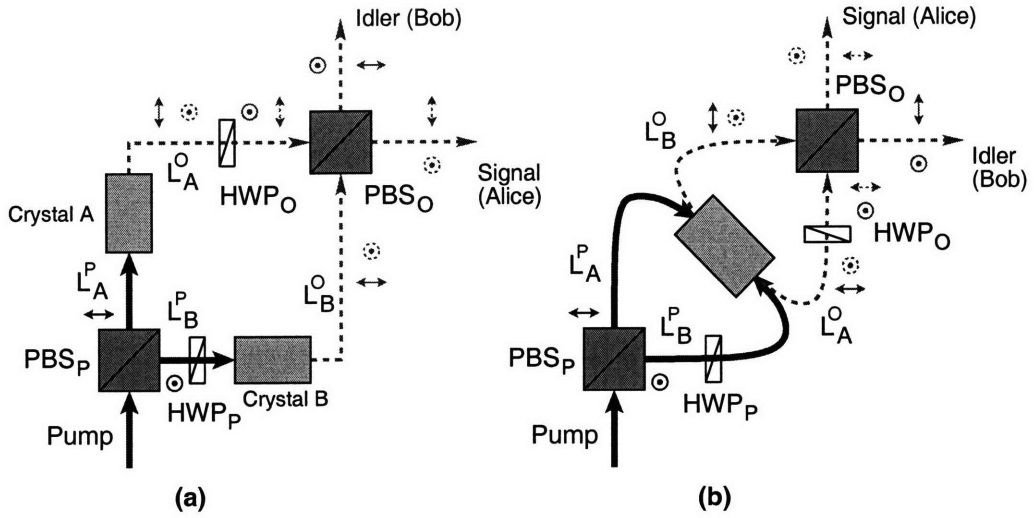

Figure 2-7: Configurations for coherently combining collinear outputs from two SPDCs. (a) A modified version of the configuration proposed by Shapiro and Wong [67], with the pump setup shown explicitly here. (b) Bidirectionally pumped SPDC implemented by Fiorentino *et al.* [27], and modified for clarity of explanation. In the original setup, the pump beam was split by non-polarizing beam splitter instead of $\mathrm{PBS_P}$ and $\mathrm{HWP_P}$, and dichroic mirrors were used to couple the pump into the crystal and to separate the outputs. HWP: half-wave plate, PBS: polarizing beam splitter.

malized) output state given by $\exp(ik_pL_A^P)E_H|V_s\rangle|H_i\rangle$, which represents a collinearly propagating pair of V-polarized signal photon and H-polarized idler photon. As can be seen from Eq. (2.2), in SPDC the pump phase carried by A_p is added to the total phase of the output and hence the output from the crystal A carries the phase picked up by the pump as it travels a length L_A^P from the $\mathrm{PBS_P}$ to the crystal A. This output undergoes a $\pi/2$ polarization rotation by $\mathrm{HWP_O}$ and is separated into two paths by $\mathrm{PBS_O}$. Then this state is given by

$$|\Psi_H\rangle = e^{i[k_pL_A^P+(k_s+k_i)L_A^O+\theta_s+\theta_i]}\,\eta_H E_H|H_s\rangle_A|V_i\rangle_B\,, \tag{2.8}$$

where the subscripts A and B refer to the Alice and Bob ports labeled in Figure 2-7 (a). The phases θ_s and θ_i are unknown but constant over the time, and they are acquired by the signal and idler outputs when they pass through the $\mathrm{HWP_O}$, and η_H^2 is the generation efficiency including propagation and absorption losses.

The V-polarized pump component drives crystal B after the pump polarization is

rotated to H by $\mathrm{HWP_P}$ for proper phase matching in the nonlinear crystal, and the pump beam acquires an unknown but constant phase θ_p. The unnormalized output state at the $\mathrm{PBS_O}$, which is generated by the V-polarized pump component, is

$$|\Psi_V\rangle = e^{i[\phi_p + k_p L_B^P + \theta_p + (k_s+k_i)L_B^O]}\, \eta_V E_V |V_s\rangle_A |H_i\rangle_B \,. \tag{2.9}$$

Note that the relative pump phase ϕ_p originally introduced in Eq. (2.7) now shows up in $|\Psi_V\rangle$ and the generation efficiency η_V^2 for the lower path is not necessarily equal to that for the upper path in Eq. (2.8).

Recognizing that in free space $k_p = k_s + k_i$, the combined MZI output, to the lowest non-vacuum order, is

$$|\Psi\rangle \propto e^{i[k_p(L_A^P + L_A^O) + \theta_s + \theta_i]}\, \eta_H E_H |H_s\rangle_A |V_i\rangle_B + e^{i[\phi_p + k_p(L_B^P + L_B^O) + \theta_p]}\, \eta_V E_V |V_s\rangle_A |H_i\rangle_B \,. \tag{2.10}$$

One difficulty with this system is the requirement for two identical crystals, and this requirement can be relaxed if we use a single crystal to generate both outputs. Fiorentino *et al.* [27] solved this problem by implementing bidirectional pumping similar to Figure 2-7 (b) and obtained a detected flux of ~12 000 pairs $\mathrm{s^{-1}\ mW^{-1}}$ in a 3-nm bandwidth with a quantum-interference visibility of 90%. The polarizations of output photon pairs are entangled over the entire spatial cone and the spectrum of the output does not need to be degenerate, thus allowing a much larger fraction of the output to be collected. However, this type of source still has some problems which limit the visibility. The main problem comes from the MZI geometry which is sensitive to environmental perturbation. Any change in path lengths $(L_A^P, L_A^O, L_B^P, L_B^O)$ affects the relative phase between the two terms in Eq. (2.10). Hence it requires active servo control of the pump interferometer in order to set the phase of the biphoton output state. Another problem in Fiorentino's implementation is that the apparatus suffered from spatial-mode clipping in the arms of the MZI, caused by using dichroic mirrors, not shown in Figure 2-7 (b), that increased the size of the interferometer.

2.3 Bidirectionally-pumped PPKTP in a Sagnac interferometer

It is clear from the discussion of the bidirectionally pumped MZI configuration that the need for stabilizing the path lengths is its major drawback. In classical optics, this problem can be solved by replacing the MZI with a polarization Sagnac interferometer (PSI) and Figure 2-7 (b) shows that it is actually possible. If we fold the MZI along the nonlinear crystal axis, the resulting setup becomes a PSI shown in Figure 2-8. In this section, we describe the construction of our polarization entangled photon pair source based on the PSI, and present the experimental results.

2.3.1 Design consideration of PSI configuration

In this subsection, we show how the PSI setup can solve the problems discussed in the previous section, and how we can control the output quantum state. We also briefly discuss what kind of components are necessary to implement the PSI system.

To generate polarization entangled photon pairs, we use the PSI setup shown in Figure 2-8. Similar to the double collinear SPDC system explained in the previous section, the pump beam is separated by a PBS into two directions. The H-polarized pump traverses the PSI in the counterclockwise direction as shown in Figure 2-8 (a), and generates a two-photon state at the output of the PBS given by

$$|\Psi_H\rangle = e^{i[k_p L_1 + (k_s+k_i)L_2 + \theta_s + \theta_i]}\, \eta_H E_H |H_s\rangle_A |V_i\rangle_B\,, \tag{2.11}$$

similar to Eq. (2.8) except that L_A^P (L_A^O) is replaced by L_1 (L_2). The V-polarized pump follows the clockwise path shown in Figure 2-8 (b) and the output state is

$$|\Psi_V\rangle = e^{i[\phi_p + k_p L_2 + \theta_p + (k_s+k_i)L_1]}\, \eta_V E_V |V_s\rangle_A |H_i\rangle_B \tag{2.12}$$

similar to Eq. (2.9). Using the $k_p = k_s + k_i$ relation, the final state is a superposition

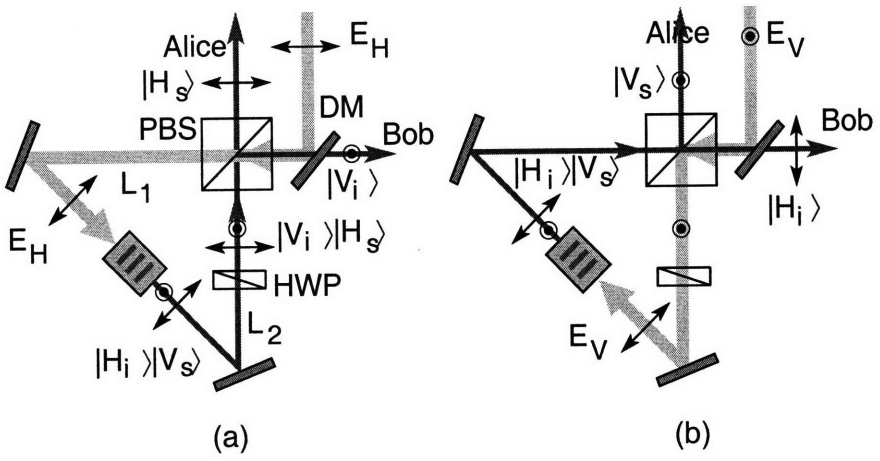

Figure 2-8: Polarization Sagnac interferometer for type-II down-conversion for (a) H-polarized pump component (E_H) and (b) V-polarized pump components (E_V), with their counterclockwise and clockwise propagation geometry, respectively. The pump is directed into the PSI with a dichroic mirror (DM) that is highly reflective for the pump and highly transmissive for the signal (idler) output at ω_s (ω_i). Orthogonally polarized outputs are separated at the PBS to yield polarization-entangled signal and idler photon pairs. HWP: half-wave plate, PBS: polarizing beam splitter.

of $|\Psi_H\rangle$ and $|\Psi_V\rangle$

$$|\Psi\rangle \propto e^{i(L_1+L_2)k_p}(\cos\theta|H_s\rangle_A|V_i\rangle_B + e^{i\phi}\sin\theta|V_s\rangle_A|H_i\rangle_B)\,, \tag{2.13}$$

$$\text{where } \phi = \theta_p + \phi_p - \theta_s - \theta_i\,, \qquad \theta = \tan^{-1}\left(\frac{\eta_V E_V}{\eta_H E_H}\right)\,. \tag{2.14}$$

In Eq. (2.13), all the phases related to propagation lengths (L_1, L_2) are factored out as an unimportant global phase, making the relative phase ϕ insensitive to the change of path lengths L_1 and L_2 of the PSI. The term $\theta_p - \theta_s - \theta_i$ in ϕ is a function of the HWP's material dispersion and does not vary in time. Therefore the PSI setup solves the phase stability problem of the MZI setup as expected. The PSI also allows us to make the entire setup compact, because we do not need any dichroic mirrors inside the interferometer, thus solving the other problem of the MZI setup. Moreover, ϕ is fully adjustable by varying the pump phase ϕ_p. We can also easily control θ which determines the ratio of the two terms in Eq. (2.13) by changing the pump polarization ratio (E_V/E_H). For example, a singlet state can be easily generated by setting $\phi = \pi$

and $\theta = \pi/4$. Therefore, the PSI down-conversion source is robust, phase stable, and adjustable, and similar to the bidirectionally pumped MZI source explained in the previous section, it does not require spatial, spectral, or temporal filtering for the generation of polarization entanglement.

However all of these advantages come at some cost. Compared to the MZI, all the optical components inside the PSI should be appropriately designed for all three interacting wavelengths. A technical design challenge is the triple-wavelength PBS and HWP. In our experimental realization we have chosen to operate near degeneracy, $\omega_s \approx \omega_i$, so that dual-wavelength PBS and HWP can be readily obtained.

2.3.2 Experimental setup

Figure 2-9 shows a schematic of the experimental setup. A continuous-wave (cw) external-cavity ultraviolet (UV) diode laser at 405 nm was used as the pump source. The linearly polarized UV pump laser was coupled into a single-mode fiber for spatial mode filtering and easy transport of the pump light to the PSI. A half-wave plate (HWP1) and a quarter-wave plate (QWP1) transform the fiber-coupled pump light into the appropriate elliptically polarized light of Eq. (2.7) to provide the power balance and phase control of the pump field (θ and ϕ in Eq. (2.13)). We typically used an input pump power of ~3 mW.

We used a 10-mm-long (crystallographic X axis), 2-mm-wide (Y axis), 1-mm-thick (Z axis) flux-grown PPKTP crystal (Raicol Crystals) with a grating period of 10.03 μm for frequency-degenerate type-II quasi-phase-matched collinear parametric down-conversion. The crystal was antireflection coated at 405 and 810 nm and temperature controlled using a thermoelectric cooler to within ± 0.01°C. The pump at ~405 nm was weakly focused to a beam waist of ~160 μm at the center of the crystal. To fine tune the crystal temperature and pump wavelength combination, we measured the single-beam quantum interference in a setup similar to that reported in Ref. [26], obtaining a visibility of 98.9% with a small aperture at the operating temperature of 28.87 ± 0.01°C and a pump wavelength of 404.96 nm.

The PSI consisted of two flat mirrors that were highly reflecting at both wave-

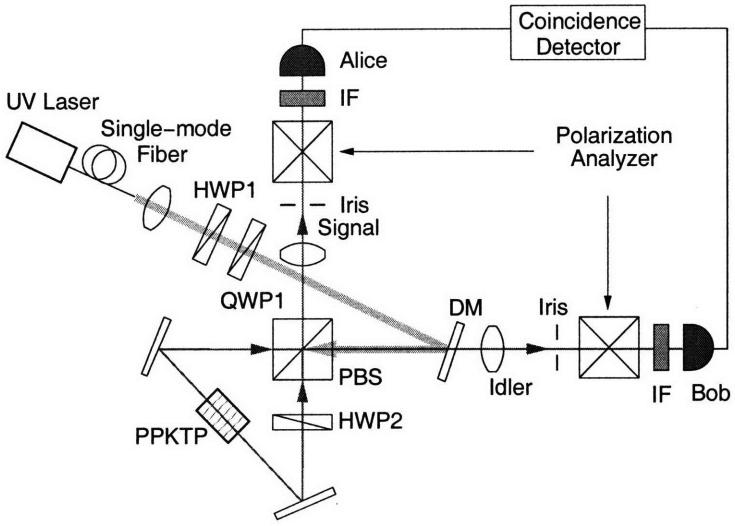

Figure 2-9: Experimental setup for polarization Sagnac interferometer type-II down-conversion. HWP1 and QWP1 are used for adjusting the relative amplitude balance of the two counter-propagating down-conversion paths and the phase of the output biphoton state. HWP: half-wave plate, QWP: quarter-wave plate, DM: dichroic mirror, PBS: polarization beam splitter, IF: 1-nm interference filter centered at 810 nm.

lengths, a dual-wavelength half-wave plate (HWP2), and a dual-wavelength PBS that served as the input/output coupling element. HWP2 (Red Optronics) was antireflection coated at the pump and output wavelengths and HWP2 was designed to work as a half-wave plate at both pump and output wavelengths. For the dual-wavelength PBS, we used a PBS (CVI PBS-800) which was originally designed and coated for only the output wavelength (800 nm), but this worked reasonably well at the pump wavelength. At the pump wavelength, it transmitted 73% of the H component and 3% of the H component leaked into the wrong output port. For the V component of the pump, 80% was reflected into the correct output of the PBS and 5% was transmitted into the unwanted output port. For both polarizations, the rest of the pump power was either back reflected or absorbed by the PBS. The 10% difference between the transmitted H-polarized component and the reflected V-polarized component was compensated for by adjusting the ratio E_H/E_V using HWP1 and QWP1. The unwanted pump components (transmitted V-polarized and reflected H-polarized components) do not contribute to down-conversion because they do not satisfy the

phase-matching condition.

At the PSI output, the polarization states of the signal and idler photons were analyzed with a combination of a HWP and a polarizer before detection by single-photon Si detectors (Perkin-Elmer SPCM-AQR-13). We imposed a spectral bandwidth of 1 nm using an interference filter (IF) centered at 810 nm with a maximum transmission of 75% at the center wavelength. Two irises were used to control the acceptance angle of the detection system. The outputs of the two single-photon detectors were counted and their coincidences were measured using a home-made coincidence detector [68] with a 1-ns coincidence window.

2.3.3 Measurement of polarization-entangled state

To characterize the polarization-entangled photon pairs generated from the PSI setup, we made measurements of the two-photon quantum interference visibility, the CHSH form of Bell's inequality, and quantum state tomography. In this section, we explain the three methods and show that the measurement results are consistent with the expected output from the PSI.

Visibility

A commonly used method for characterizing the entanglement quality is the measurement of two-photon quantum interference visibility. For example, if we generate a singlet state ($|\Psi^-\rangle_{AB} = (|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B)/\sqrt{2}$) by controlling the HWP1 and the QWP1 in Figure 2-9 to set $\theta = 45°$ and $\phi = \pi$ in Eq. (2.13), the polarizations measured by Alice and Bob will always be anti-correlated independent of the polarization measurement bases. In other words, if Alice fixes her polarization analyzer (PA) to detect only vertically polarized photons, the coincident photons on Bob's side should always be horizontally polarized. As Bob changes his PA angle, his single photon counts remain constant, but the coincidence counts between Alice and Bob will have a minimum when Bob's PA is set to detect vertically polarized photons ($\theta_1 = 90°$) and a maximum when Bob's PA measures only horizontally po-

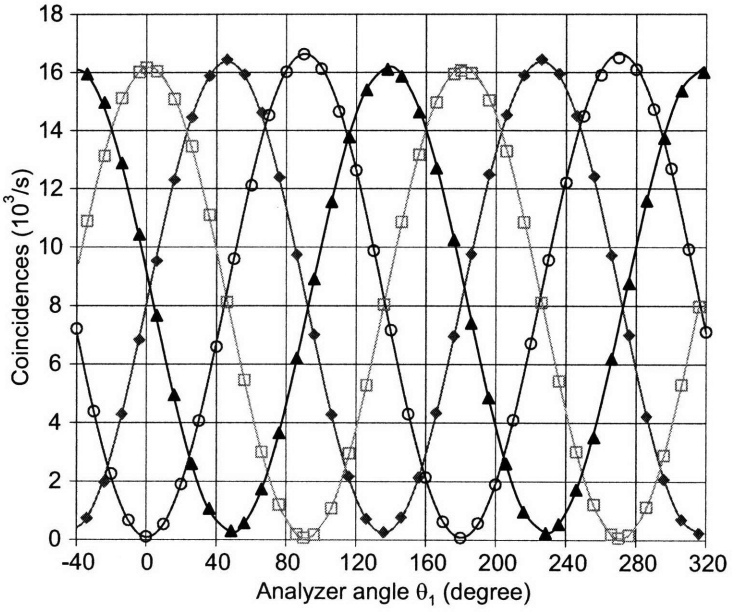

Figure 2-10: Coincidence counts as a function of Bob's polarization analyzer angle θ_1 for different settings of Alice's polarization analyzer angle: 0°(open circles), 46°(solid triangles), 90.5°(open squares), 135°(solid diamonds). The biphoton output was set to be a singlet state. Solid lines are best sinusoidal fits to data. Each data point was averaged over 40 s and the pump power was 3.28 mW.

larized photons ($\theta_1 = 0°$), as shown in Figure 2-10 with open squares. However this sinusoidal curve doesn't necessary mean that we have a singlet state. In fact, the same sinusoidal curve with the same singles count can also be reproduced by a mixed state such as $\rho = \frac{1}{2}|H\rangle_A|V\rangle_{BA}\langle H|_B\langle V| + \frac{1}{2}|V\rangle_A|H\rangle_{BA}\langle V|_B\langle H|$. To distinguish these two possibilities, it is necessary to measure the two-photon quantum interference in an incompatible polarization basis, such as the anti-diagonal/diagonal (A/D) basis. To make a measurement in A/D basis, we set Alice's PA along 45° (D) and measure the coincidences at different angles of Bob's PA. If the state is a singlet state, we will see another sinusoidal curve shifted by $-45°$ because Bob's coincident photons are polarized along $-45°$ (A), whereas, if the input were a mixed state, we would expect a flat horizontal line because Bob's coincident photon can be either H or V. Therefore the quality of this quantum interference fringe pattern in the A/D basis reflects the interference quality between the two terms in a singlet state. When Alice's PA measures along 45° (D), the coincidence counts are denoted by solid triangles in Figure 2-12. To compare the quality of the fringe pattern, we obtain the quantum-interference visibility V defined as $(C_{\max} - C_{\min})/(C_{\max} + C_{\min})$, where $C_{\max}$ is the maximum coincidence counts and $C_{\min}$ is the minimum coincidence counts. The data shown in Figure 2-10 were taken with an input pump power of 3.28 mW (measured before DM), 1-nm IF, and a full divergence collection angle of 12.5 mrad, and we measured a flux of polarization-entangled photon pairs of $\sim$ 5000 detected pairs/s/mW. Measured visibilities are $V_0 = 99.09 \pm 0.07$, $V_{46} = 96.85 \pm 0.12$, $V_{90.5} = 99.32 \pm 0.04$, and $V_{135} = 97.18 \pm 0.09$.

We have also examined the characteristics of the PSI down-conversion source at different collection divergence angles. Figure 2-11 shows the visibility and flux of the generated polarization-entangled photon pairs as we varied the size of the collection irises, showing reduced flux but higher visibility for smaller divergence angles. We attribute the dependence of the visibility on the iris size to wavefront distortion of the PBS used in the PSI. The commercially available PBS was made from two coated prisms that were cemented together at the hypotenuse side with a wavefront distortion of a quarter of a wavelength at 633 nm. This specification is worse than

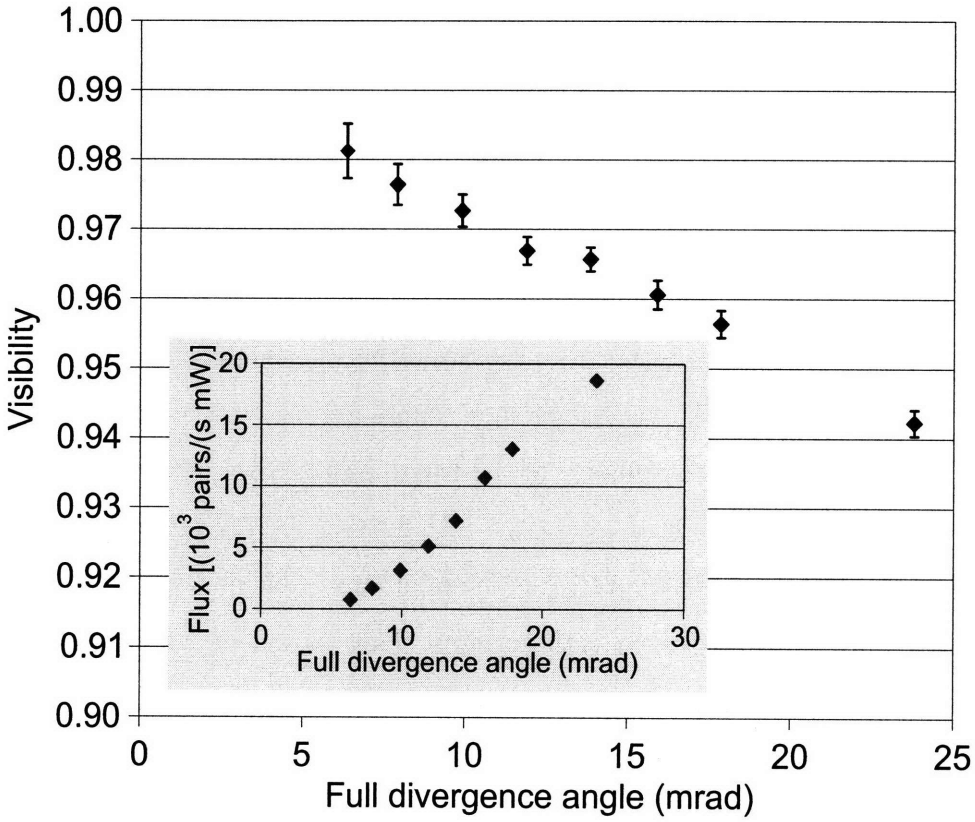

Figure 2-11: Plot of quantum-interference visibility as a function of full divergence angle when Alice's PA is along 45°. Inset: measured flux of polarization-entangled photon pairs versus full divergence angle.

intracavity optics that are typically specified at a tenth of a wavelength at 633 nm. The wavefront distortion is less when the collection divergence angle is small, thus resulting in higher visibilities for smaller apertures, as observed in Figure 2-11.

Clauser-Horne-Shimony-Holt (CHSH) measurement

Another way to characterize an entangled state is to measure the S parameter in Clauser-Horne-Shimony-Holt (CHSH) form of Bell's inequality [69]. To calculate the S parameter, we need to measure four expectation values $E(\theta_A, \theta_B)$. Let us assume that Alice's polarization analyzer (PA) generates $+1$ when PA measures a photon in θ_A basis and -1 when PA measures a photon in $\theta_A + \pi/2$ basis, and similarly Bob's PA also generates $+1$ and -1 for θ_B and $\theta_B + \pi/2$, respectively. Then $E(\theta_A, \theta_B)$ is an expectation value of the product of Alice's measurement and Bob's measurement. In other words, the measured product yields $+1$ if the two polarization measurements correspond to (θ_A, θ_B) or $(\theta_A + \pi/2, \theta_B + \pi/2)$ and -1 if they are equal to $(\theta_A + \pi/2, \theta_B)$ or $(\theta_A, \theta_B + \pi/2)$, and $E(\theta_A, \theta_B)$ is an average of all the measured products for a given (θ_A, θ_B). Ideally, we would use 4 single-photon detectors and simultaneously count the four coincidences for every generated pair. However due to limitations in our setup, we could measure only one type of coincidences at one time. Therefore, we construct E from 4 types of coincidences using

$$E(\theta_A, \theta_B) = \frac{C(\theta_A, \theta_B) - C(\theta_A + \pi/2, \theta_B) - C(\theta_A, \theta_B + \pi/2) + C(\theta_A + \pi/2, \theta_B + \pi/2)}{C(\theta_A, \theta_B) + C(\theta_A + \pi/2, \theta_B) + C(\theta_A, \theta_B + \pi/2) + C(\theta_A + \pi/2, \theta_B + \pi/2)}, \tag{2.15}$$

where $C(\theta_A, \theta_B)$ is the coincidence count when Alice measures θ_A and Bob measures θ_B.

The parameter S is defined in terms of $E(\theta_A, \theta_B)$ as follows:

$$S = |E(0, \frac{7\pi}{8}) + E(-\frac{\pi}{4}, \frac{7\pi}{8}) + E(-\frac{\pi}{4}, \frac{5\pi}{8}) - E(0, \frac{5\pi}{8})|. \tag{2.16}$$

Quantum mechanics predicts that we can obtain $2\sqrt{2}$ for an ideal singlet state, whereas classical theory predicts a maximum S of 2. Therefore a measurement of

S larger than 2 indicates that the generated state is non-classical. In our experiment, we obtained $S = 2.7645 \pm 0.0013$, which corresponds to the violation of the classical limit of 2 by more than 500 standard deviations.

Quantum state tomography

In general, a given quantum state is not a pure state, but a probabilistic mixture of many pure states, which can be represented by a density matrix. Quantum state tomography is a technique to measure the entire density matrix using a finite number of measurements [70]. To include all the potential problems such as intensity drift, beam splitter crosstalk, wave plate errors etc., we have to use the maximum likelihood technique to estimate the density matrix (ρ), but in our case, we simplify the calculation by assuming that the errors in the optical components used in our measurements are negligible. Then we can find linear relations between each real and imaginary component of ρ and the coincidence measurements (M) of Alice and Bob. For example, if both Alice and Bob measure horizontal (H) polarizations, the measured coincidence counts M_{HH} is proportional to $\langle HH|\rho|HH\rangle$, and we can get all the diagonal components of ρ by measuring only in the H-V basis. To find off-diagonal components of ρ, we need to measure the diagonal polarization and circular polarization. When Alice measures H polarization and Bob measures $D = (H + V)/\sqrt{2}$ polarization, the measured coincidences M_{HD} is proportional to

$$\begin{aligned}
&\langle HD|\rho|HD\rangle = \langle H|\tfrac{1}{\sqrt{2}}\left(\langle H| + \langle V|\right)\rho|H\rangle\tfrac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right) \\
&= \tfrac{1}{2}\left(\langle HH|\rho|HH\rangle + \langle HH|\rho|HV\rangle + \langle HV|\rho|HH\rangle + \langle HV|\rho|HV\rangle\right) \\
&= \tfrac{1}{2}\left(\langle HH|\rho|HH\rangle + 2\mathrm{Re}(\langle HH|\rho|HV\rangle) + \langle HV|\rho|HV\rangle\right),
\end{aligned} \tag{2.17}$$

where we can find the real part of the off-diagonal component ($\langle HH|\rho|HV\rangle$) from M_{HD}. To find the imaginary part of the off-diagonal component, we need to measure in a circularly polarized basis ($R = (H - iV)/\sqrt{2}$). For example, if Alice measures H polarization and Bob measures R polarization, the measured coincidences M_{HR} is

proportional to

$$\begin{aligned}
&\langle HR|\rho|HR\rangle = \langle H|\tfrac{1}{\sqrt{2}}\left(\langle H| + i\langle V|\right)\rho|H\rangle\tfrac{1}{\sqrt{2}}\left(|H\rangle - i|V\rangle\right) \\
&= \tfrac{1}{2}\left(\langle HH|\rho|HH\rangle - i\langle HH|\rho|HV\rangle + i\langle HV|\rho|HH\rangle + \langle HV|\rho|HV\rangle\right) \\
&= \tfrac{1}{2}\left(\langle HH|\rho|HH\rangle + 2\mathrm{Im}(\langle HH|\rho|HV\rangle) + \langle HV|\rho|HV\rangle\right) .
\end{aligned} \tag{2.18}$$

If we consider all possible coincidence measurements where Alice and Bob can independently choose one of four measurement bases (H, V, D, A), we can deduce the entire ρ in terms of 16 coincidence measurements $(M_{P_A P_B})$ as shown in Appendix C.

An example of quantum state tomography is given in the next section, where the output state of an improved version of the PSI source is characterized.

2.4 Fine tuning of the PSI

The experimental results in the previous section show that the PSI setup can generate entangled photon pairs with much higher visibility than the MZI setup without reducing the flux or losing any benefits of the double SPDC configuration. However the maximum visibility (97%) measured in the previous experiment was still less than expected. In this section, we show additional improvements of the experimental system to achieve a higher level of quantum-interference visibility. These improvements include the fine tuning of the pump laser and optimization of the alignment procedure.

The major problem came from the unstable wavelength of the pump laser. If the pump wavelength changes by 0.01 nm, the phase of the output state can be changed by 0.007 radian due to the HWP's material dispersion. In addition, the pump light is reflected directly back toward the pump source because of the PSI design of Figure 2-8, thus potentially causing instability of the pump laser due to the feedback. To eliminate these two pump problems, we optimized the pump laser operating condition to select the most stable mode, and increased the pump isolation to prevent the feedback into the pump laser.

We also completely redesigned the alignment procedure. In order to collect most of

the degenerate output pairs, we previously aligned the interference filters with respect to the reference output wavelength, thereby making an implicit assumption that the outputs are degenerate. However, since the PSI configuration allows nondegenerate outputs as well, the degenerate output assumption may not be suitable. Instead we varied the center wavelength of the IF by changing the incident angle at IF and balanced the singles counts while maximizing the conditional probability of coincidence counts compared to the singles counts in each arm. Also we changed the way to optimize the pump polarization. In an ideal PSI configuration, to create a singlet output state, the polarization of the pump laser should have the equal amplitudes for the H and V components, and we should be able to control the relative phase between those two components without changing the amplitudes of H and V. In the ideal case, this can be easily done with the setup in Figure 2-9 by fixing the pump polarization after HPW1 to a diagonal polarization. Then the angle of the QWP1 determines the relative phase while maintaining the balance between the V and H components. In our PSI system, we used a non-ideal PBS that has unbalanced transmissivity and reflectivity at the pump wavelength, and this imbalance should be compensated for by the unbalanced pump polarizations (i.e. an elliptical polarization). Therefore, even when we want to change only the relative phase, we always have to change HWP1 and QWP1 simultaneously. This generally makes the fine alignment very difficult, especially when HWP1 and QWP1 are not perfect. Therefore we used a different approach. We first used HWP1 and QWP1 only to balance the pair generation probabilities of the two terms in the output state ($\theta = \pi/4$) of Eq. (2.13). Then the control of the output phase ϕ of Eq. (2.13) was done separately by using an extra quarter wave plate in one of the output paths during the fine alignment of PSI. This allows us to change the output phase independently because during the alignment of PSI we generally measure the polarization along A-D basis, which means the rotation of output QWP will change only the relative phase. Once alignment of PSI was done, we removed the extra quarter wave plate, and we can easily find the optimal pump polarization to generate the singlet state.

With all these efforts to maintain indistinguishability between the two counter-

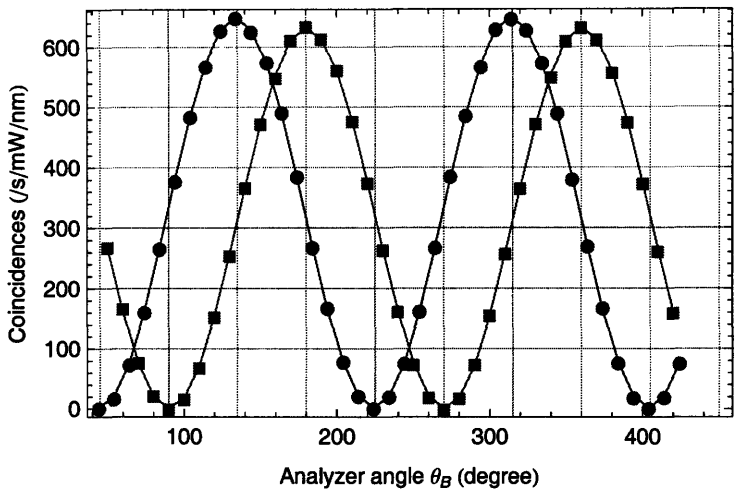

Figure 2-12: Two-photon quantum-interference visibility measurements of the improved PSI source. Coincidence counts as a function of Bob's polarization analyzer angle θ_B for different settings of Alice's polarization analyzer angle θ_A: 45°(solid circle), 90°(solid square). The biphoton output was set to be a singlet state. Solid lines are best sinusoidal fits to data. Each data point was averaged over 40 s and the pump power was 4.7 mW. Measured visibilities without background subtraction are 99.45% for $\theta_A = 45°$ and 99.76% for $\theta_A = 90°$.

propagating beams and extra optimization steps for the crystal temperature, the location and size of the iris, and the orientation of the crystal, we could significantly improve the visibility while maintaining the same flux level of previous experiments. Figure 2-12 shows the new visibility measurement results where we achieved $V_{45°} = 99.45 \pm 0.18\%$ and $V_{90°} = 99.76 \pm 0.12\%$ without any background count subtraction. This set of data was taken with a pump power of 4.7 mW and the full divergence collection angle was 4.85 mrad. At this setting, we measured a flux of ~700 pairs/s per mW of the pump power with 1-nm IF. Figure 2-13 shows the measured visibility and the flux as a function of the full divergence angle of the output. Compared to Figure 2-11, we obtained much higher visibilities with the improved PSI source. We also measured the S parameter for CHSH with the divergence angle of 4.85 mrad and obtained $2.8253 \pm 0.015 \pm 0.0035$, which is very close to the ideal quantum limit of $2\sqrt{2} \approx 2.8284$. The first standard deviation of S is that due to systematic errors (such as wave plate angle settings), while the second standard deviation is due to statistical errors. Finally we performed quantum state tomography on this quantum

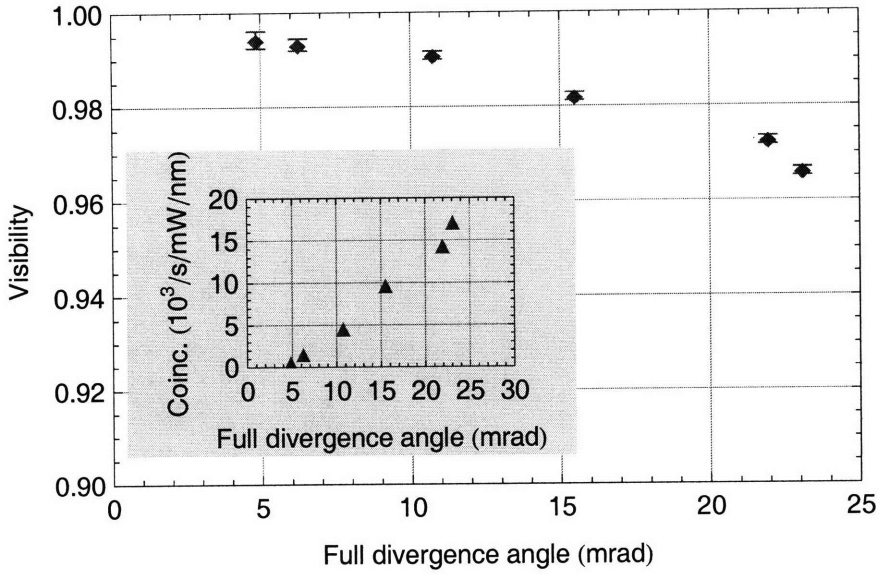

Figure 2-13: Plot of quantum-interference visibility as a function of full divergence angle for $\theta_2 = 45°$. Inset: measured flux of polarization-entangled photon pairs versus full divergence angle.

state as described in the previous section, and the resulting density matrix is plotted in Figure 2-14.

From the measured density matrix, we calculated the fidelity to the singlet state ($|\psi^-\rangle \equiv (|H\rangle|V\rangle - |V\rangle|H\rangle)/\sqrt{2}$) which is defined as $\langle\psi^-|\rho|\psi^-\rangle$ and obtained 0.994.

2.5 Summary

In this chapter, we described how to design, construct, and align a high flux source of polarization-entangled photon pairs in a polarization Sagnac interferometer configuration. The two-photon quantum-interference visibility of this source is one of the highest values measured with polarization entangled photon pairs. Figure 2-15 shows the measurement result compared to other types of the polarization entangled photon pair sources. Compared to initial BBO experiments, we have increased the flux by five orders of magnitude in pairs/(s mW nm), and also improved entanglement quality. The main increase of flux comes from the use of PPKTP which allows the collinear output mode, and the higher entanglement quality comes from the use of

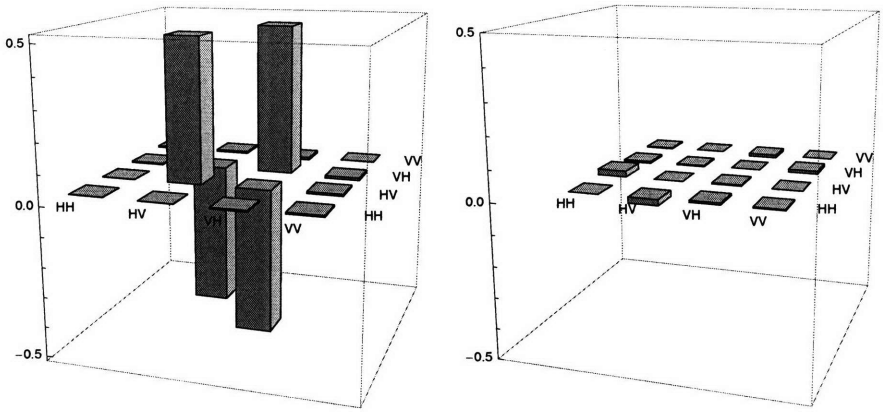

Figure 2-14: Density matrix of polarization-entangled state. Left plot shows the real part and the right plot shows the imaginary part.

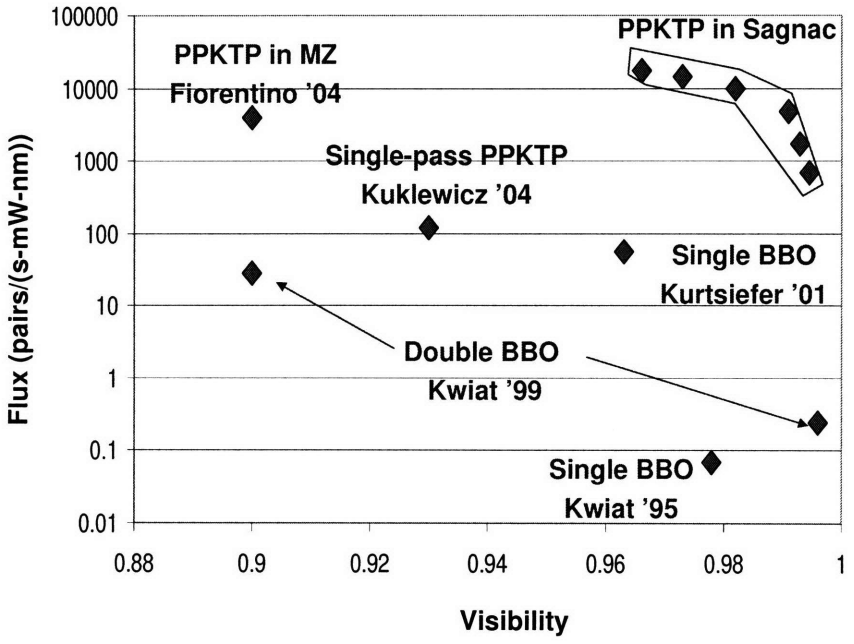

Figure 2-15: Comparison of the entanglement sources with different designs. The horizontal axis shows the two-photon quantum interference visibility and the vertical axis shows the normalized number of photon pairs per second per mW of the pump power within 1-nm bandwidth. PPKTP in Sagnac is the result of our setup. Kwiat '95 from Ref [24], Kwiat '99 from Ref [25], Kurtsiefer '01 from Ref. [74], Kuklewicz '04 from Ref. [26], and Fiorentino '04 from Ref. [27].

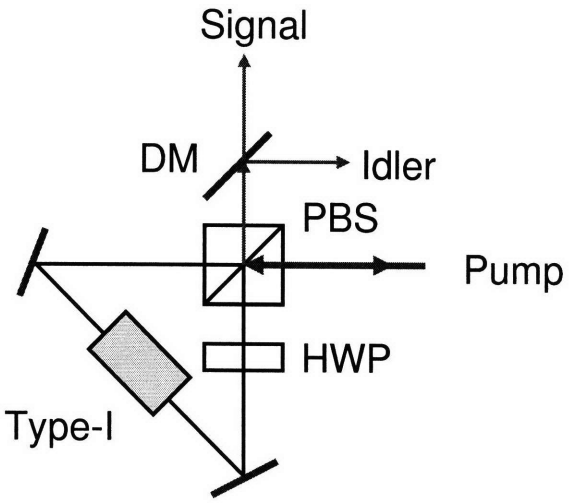

Figure 2-16: Design of polarization entangled photon pair source based on PPKTP with type-I nondegenerate phase-matching condition. The output state is $\alpha|H\rangle_s|H\rangle_i + \beta e^{i\phi}|V\rangle_s|V\rangle_i$. PBS and HWP are designed for triple wavelengths. HWP is tilted by 45°. DM: dichroic mirror reflecting idler wavelength and transmitting signal wavelength.

the phase-stable Sagnac interferometer and the double SPDC configuration.

The collinear output modes allow this source to be easily coupled into a single mode optical fiber [66] and it is suitable for a monolithic design using integrated photonics and photonic crystal stucture [71]. The collinear SPDC geometry implies that it can incorporate a cavity structure [73] to generate narrowband outputs to enhance the spectral brightness. The Sagnac configuration can also be used, with minimal modification, in a pulsed-pumping system for free space quantum key distribution [72]. A similar type of PSI configuration can also be applied to type-I nondegenerate phase-matched PPKTP crystal to take advantage of the higher nonlinear coefficient d_{33} to further increase the flux and efficiency as shown in Figure 2-16. In this case, the challenging part is the design of triple wavelength components. In this thesis, the PSI-based source is used to generate hyper-entangled states which will be described in Chapter 4 and 5.

Chapter 3

Deterministic gates for single-photon two-qubit quantum logic

A photon is an ideal candidate to represent a qubit because of its weak interaction with the environment, which allows for a long coherence time for exchanging qubits between remote sites. However, weak interactions between photons prevent their use in quantum information processing in an efficient way, partly because simple linear optical components cannot implement deterministic quantum logic [75, 76]. In a major discovery, Knill, Laflamme, and Milburn [8] showed that scalable quantum computation is still possible with a linear optical system if one introduces measurement as the nonlinearity by incorporating single-photon sources and single-photon detectors.

Another approach to linear optical quantum computation is to encode multiple qubits in several degrees of freedom of a single photon [12, 13, 14]. This multiple-qubit approach can implement deterministic quantum logic with a relatively simple setup compared to other optical quantum logic approaches, but it is not scalable quantum logic due to the complexity of the optical setup as the number of qubits increases. This limitation is acceptable if the photons are entangled in some degrees of freedom and if only few-qubit operations are of interest in small-scale QIP tasks. The simplest implementation of this multiple-qubit approach is the single-photon two-qubit

(SPTQ) quantum logic in which the polarization degree of freedom (called P qubit) and momentum degree of freedom (called M qubit) of a single photon are utilized. By combining SPTQ quantum logic with entangled photon pairs, one can demonstrate several quantum information protocols including a one-shot demonstration of nonlocality with two observers [77], a complete measurement of Bell's states [35], quantum games [78], a physical simulation of entangling-probe attack on the BB84 protocol [57], entanglement distillation [38], and entanglement purification [79]. To implement these protocols, we need to realize a number of basic quantum gates to form a universal gate set for quantum logical operations. Previous implementation of SPTQ quantum logic involved two separate paths for the momentum qubits and hence a logic circuit based on their different paths is essentially a large and complex interferometer [12, 13, 14, 15, 16]. The necessary coherence for these paths implies that they must be stabilized, and therefore these interferometric methods are less attractive from a practical standpoint. In contrast, we utilize a Sagnac-type interferometric arrangement to implement these SPTQ logic gates such that they are phase-stable and stabilization is not necessary [17].

In our implementation we collimate two non-parallel momentum vectors into two parallel paths as shown in Figure 3-1, so that their path lengths are identical as they propagate in space. Together with the phase-stable SPTQ quantum logic gates, we can build complex SPTQ systems without the need for path length stabilization.

In SPTQ, the quantum state of each photon can be represented as a vector in 4-dimensional Hilbert space, whose orthogonal basis vectors are $a^\dagger_{H,T}|0\rangle$, $a^\dagger_{H,B}|0\rangle$, $a^\dagger_{V,T}|0\rangle$, $a^\dagger_{V,B}|0\rangle$, corresponding to each of the four modes shown in Figure 3-1. H (V) means horizontal (vertical) polarization for the P qubit, and T (B) means top (bottom) path for the M qubit. We can also rewrite each basis vector as the tensor product of two 2-dimensional Hilbert space vectors, such as $|H\rangle_P \otimes |T\rangle_M$, $|H\rangle_P \otimes |B\rangle_M$, $|V\rangle_P \otimes |T\rangle_M$, $|V\rangle_P \otimes |B\rangle_M$, or just $|HT\rangle$, $|HB\rangle$, $|VT\rangle$, $|VB\rangle$ for simplicity. In this chapter, we identify $|H\rangle$, $|T\rangle$ with the logical $|0\rangle$ qubit, and $|V\rangle$, $|B\rangle$ with the logical $|1\rangle$ qubit.

In this chapter, we first describe the implementation of SPTQ quantum gates such

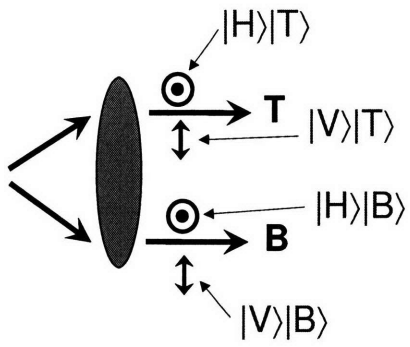

Figure 3-1: Four orthogonal bases used in SPTQ and conversion of momentum qubit to parallel path qubit.

as single qubit operations, controlled-NOT gates, and a SWAP gate. Then as an application of the SWAP gate, we present the experimental setup to demonstrate coherent transfer of the entanglement stored in P qubits to M qubits and the experimental results.

3.1 Basic gates for SPTQ

It is well known that any arbitrary unitary operation can be implemented by using controlled-NOT (CNOT) gates and single-qubit operations. Therefore to show that SPTQ quantum logic is universal, at least within the same photon, we should be able to implement single qubit operations and CNOT gates between the polarization qubit and the momentum qubit. Single P-qubit operation and a momentum-controlled NOT gate can be easily implemented by properly designed wave plates. However, a phase-stable polarization-controlled NOT gate and phase-stable single M-qubit operation require more careful design consideration. For example, Figure 3-2 (b) shows one possible implementation of single M-qubit operation which is composed of a non-polarizing beam splitter, and a right angle prism to control the phase between the two paths. Unfortunately, this type of implementation is undesirable because the relative phase depends on the path length difference which must be stabilized. The reflectivity of a beam splitter must also be controlled depending on the rotation angle

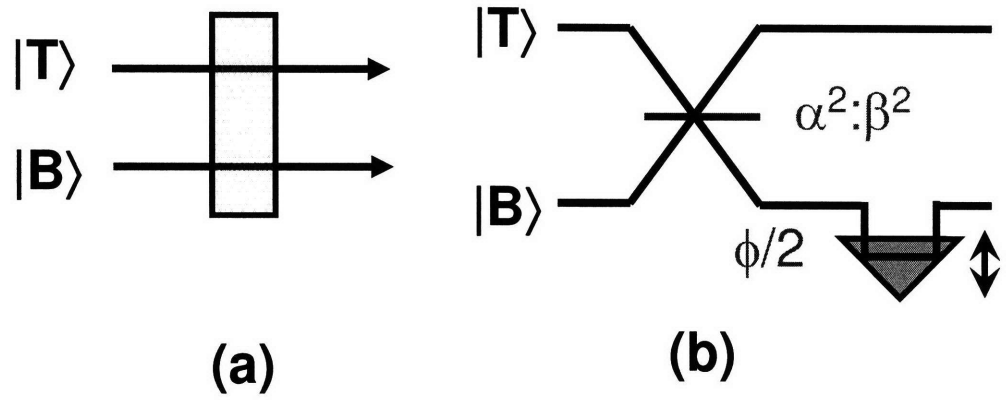

Figure 3-2: Realization of two types of single qubit operation. (a) Single P-qubit operation using a wave plate. (b) Single M-qubit operation using an adjustable beam splitter. α^2 and β^2 is the reflectivity and transmittivity of a non-polarizing beam splitter. Right angle prism changes the relative phase between two paths.

of the qubit, which is unrealistic. In this section, we discuss how we can implement phase stable SPTQ quantum gates based on a polarization Sagnac interferometer geometry. We also show how a quantum SWAP between the P and M qubits can be realized.

3.1.1 Single qubit operation

There are two types of qubits, P and M, in SPTQ quantum logic, and therefore two types of single-qubit operations are necessary. When the M qubit is encoded in two parallel paths as in our laboratory implementation, single qubit operations on the P qubit can be easily implemented by standard wave plates that are inserted in the two parallel paths, as shown in Figure 3-2 (a). This setup guarantees that the two paths acquire the same amount of phase as they propagate through the HWP (or any other type of wave plates).

As discussed in the introduction of this section, single qubit operation on the M qubit is more complicated. Phase-stable single M-qubit operation can be built by wave plates sandwiched by two SWAP gates which swap the quantum information stored in the P and M qubits. This design will be described in Section 3.1.3.

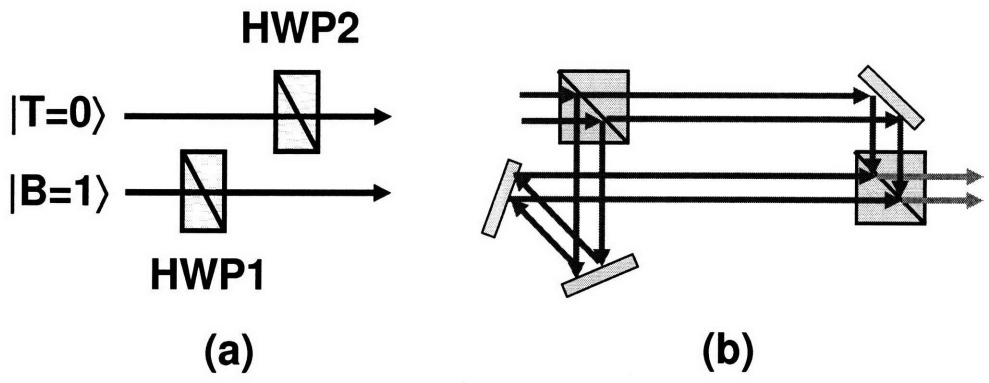

Figure 3-3: Implementation of a CNOT gate between P and M qubits. (a) Momentum controlled NOT gate. M is the control qubit and P is the target qubit. (b) Interferometric version of a polarization-controlled NOT gate, in which P is the control qubit and M is the target qubit.

3.1.2 Controlled-NOT operation between P qubit and M qubit

In SPTQ, two types of controlled-NOT (CNOT) gates are needed. A momentum-controlled NOT (M-CNOT) gate uses momentum as the control qubit and polarization as the target qubit. The M-CNOT gate can be realized with a half wave plate (HWP1) cut in a half-circular D shape with the fast axis forming a 45° angle with the H direction, which is aligned so that it only affects the beam in the bottom path ($|B\rangle = |1\rangle$), as shown in Figure 3-3 (a). Another half wave plate (HWP2), identical to the HWP1 except for the fact that its axis is parallel to the H axis, is in the path of the top part of the beam to compensate for the time delay introduced by HWP1.

Another type of CNOT gate, polarization-controlled NOT (P-CNOT), requires more attention. In principle, it can be implemented as shown in Figure 3-3 (b), but this type of setup has the phase instability problem which is intrinsic to a Mach-Zehnder interferometer. To avoid this problem, Fiorentino and Wong [17] used a polarization Sagnac interferometer (PSI) containing a dove prism whose base is oriented at a 45° angle relative to the horizontal plane, as shown in Figure 3-4. The input polarizing beam splitter (PBS) directs horizontally (vertically) polarized input light to travel in a clockwise (counterclockwise) direction. As viewed by each beam, the dove prism

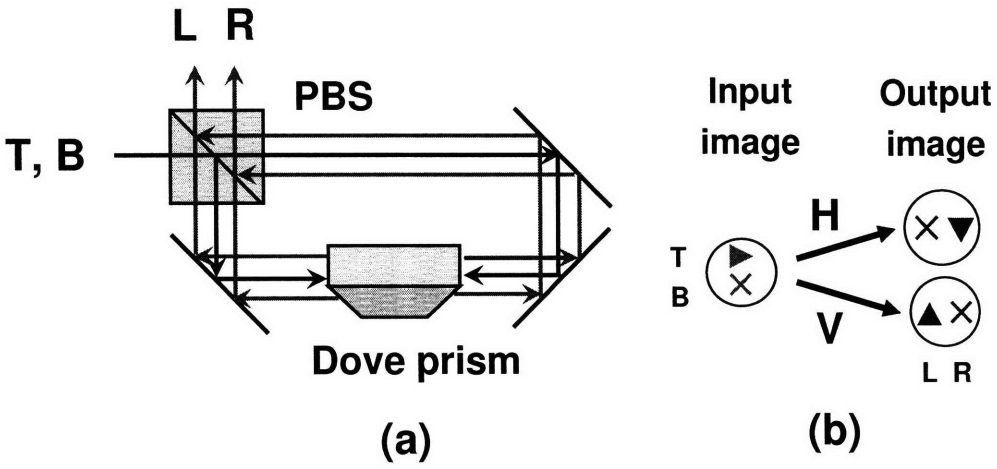

Figure 3-4: Polarization-controlled NOT (P-CNOT) using a phase-stable polarization Sagnac interferometer and an embedded dove prism. (a) Schematic of P-CNOT seen from above. (b) Change of input image to the output image by the P-CNOT gate. The beams are propagating into the paper and the images are viewed from behind.

orientation is different for the two counter-propagating beams such that the transformation of the input spatial image differs for the horizontal (H) and vertical (V) polarizations. Specifically, the top-bottom ($T - B$) sections of the input beam are mapped onto the right-left ($R - L$) sections of the output beam for H-polarized light but onto the $L - R$ sections for V-polarized light. If we identify $|H\rangle$, $|T\rangle$, and $|R\rangle$ as logical $|0\rangle$, and $|V\rangle$, $|B\rangle$, and $|L\rangle$ as logical $|1\rangle$, this setup implements a P-CNOT gate in which the polarization is the control qubit and the momentum (or spatial) mode is the target qubit.

Fiorentino and Wong [17] utilized this setup to demonstrate the logic table of a CNOT gate in the $|0\rangle$ and $|1\rangle$ basis with $\sim 1\%$ error. In addition, They experimentally generated an entangled state between the polarization and momentum qubits of a single photon using the same apparatus as an entangling gate.

We used the phase-stable P-CNOT gate in all of the SPTQ experiments described in this thesis. In using the P-CNOT gate in various experiments, we found that the P-CNOT gate adds a relative phase between the two polarization components. In other words, for an input state $(\alpha|H\rangle + \beta|V\rangle) \otimes |L\rangle$, the output state becomes

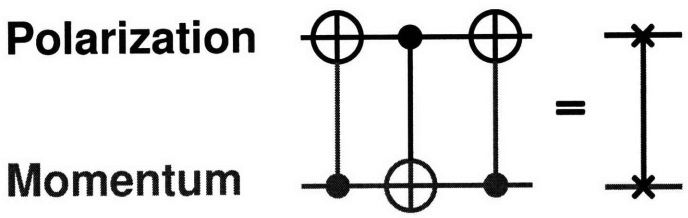

Figure 3-5: Quantum circuit to swap quantum states stored in polarization qubit and momentum qubit and an equivalent symbol for this circuit.

$\alpha|H\rangle \otimes |T\rangle + \beta e^{i\phi}|V\rangle \otimes |B\rangle$ up to a global phase and ϕ is sensitive to the angle between the input beam and the normal vector of the input surface of PBS inside the P-CNOT gate. This phase shift comes from the differential phase shift seen by the two polarizations at total internal reflection [80] in the dove prism. The amount of this phase shift can be easily measured with a laser beam, and in the experiments, we compensated for this phase shift by adding $-\phi$ phase to the vertical component of the input quantum state at the input of P-CNOT gate.

3.1.3 SWAP gate

In our experiments, we occasionally need to swap the quantum states stored in the P qubit and M qubit, and it can be achieved by using three CNOT gates as shown in Figure 3-5 [81]. This circuit is composed of one P-CNOT gate sandwiched by two M-CNOT gates that were discussed in the previous subsection.

We can find an immediate application of the SWAP gate. At the introduction of this Section, we showed that single M-qubit operation based on a beam splitter and path delay cannot guarantee the phase stability, and this problem can be easily solved by using two SWAP gates. Instead of operating directly on the momentum qubit, we can first swap the P and M qubits, then operate on the P qubit (M-qubit before the SWAP) using wave plates, and finally swap P and M qubits back as shown in Figure 3-6. The result is exactly the same as performing single qubit operation on the M qubit directly, and the entire process is completely phase stable because of the phase-stable implementation of P-CNOT gate.

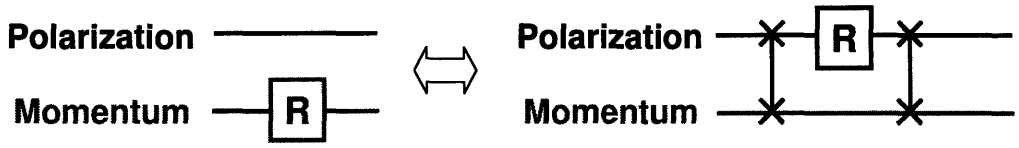

Figure 3-6: Equivalent quantum circuits for single M qubit operation.

Therefore with P-CNOT gates and SWAP gates, we can implement, in principle, any arbitrary unitary operation within a Hilbert space composed of polarization qubit and momentum qubit of the same photon. The only limitation is the gate fidelity of the SWAP gates.

3.2 Entanglement transfer from momentum qubit pair to polarization qubit pair

In this section, we demonstrate one of the interesting applications of the SWAP gate. We will first describe that momentum entangled photon pairs can be generated by SPDC, then show that these momentum entangled photon pairs can be converted into polarization entangled photon pairs by a SWAP gate, and the experimental setups and the measurement results will follow.

3.2.1 Generation of momentum entangled photon pairs

Compared to polarization entanglement which requires extra configurations like timing-compensation or double SPDC, the output from SPDC is naturally entangled in their transverse momentum for the following reason. With the assumption of $w_0 \to \infty$, Eq. (2.2) can be simplified to

$$|\psi\rangle \propto \int d\omega_s \, d\mathbf{k}_s^{\perp} \, \mathrm{sinc}(\Delta k_x L_x/2) \, \hat{a}_V^{\dagger}(\mathbf{k}_s^{\perp}, \omega_s) \, \hat{a}_H^{\dagger}(-\mathbf{k}_s^{\perp}, \omega_p - \omega_s)|0\rangle, \qquad (3.1)$$

where $\int d\omega_s \, d\mathbf{k}_s^{\perp}$ is a triple integral that extends to the whole plane spanned by the transverse (yz-plane) component of the signal wave vector $\mathbf{k}_s$ and over the range of

positive frequencies spanned by the signal frequency ω_s. The creation operators $\hat{a}_V^\dagger$ and $\hat{a}_H^\dagger$ refer to the vertically (V) and horizontally (H) polarized signal and idler, respectively, and ω_p is the pump frequency. Equation (3.1) clearly shows the correlation in momentum between signal and idler photons. We now restrict our attention to two propagation directions: one on the top ($\mathbf{k}_T$) and its conjugate at the bottom ($\mathbf{k}_B$) and their transverse momentum are correlated by $\mathbf{k}_B^\perp = -\mathbf{k}_T^\perp$. We take the signal frequency to be $\omega_s = \omega_p/2$ and assume the phase mismatch Δk_x to be zero. In the experimental setup the two conjugate transverse momentum directions can be defined by a two-hole aperture mask, as shown in Figure 3-7 and the degenerate output frequency condition is enforced by the phase matching condition and interference filters. The state then becomes

$$|\Psi\rangle_{\text{IN}} \simeq \left(\hat{a}_V^\dagger\left(t_V, \mathbf{k}_T, \omega_p/2\right)\hat{a}_H^\dagger\left(t_H, \mathbf{k}_B, \omega_p/2\right) + \hat{a}_V^\dagger\left(t_V, \mathbf{k}_B, \omega_p/2\right)\hat{a}_H^\dagger\left(t_H, \mathbf{k}_T, \omega_p/2\right)\right)|0\rangle. \tag{3.2}$$

This state can also be rewritten, following the convention introduced at the beginning of this chapter, as

$$\begin{aligned} |\Psi\rangle_{\text{IN}} &= \frac{1}{\sqrt{2}}(|VT\rangle_s|HB\rangle_i + |VB\rangle_s|HT\rangle_i) \\ &= \frac{1}{\sqrt{2}}|V_sH_i\rangle \otimes (|T_sB_i\rangle + |B_sT_i\rangle) \\ &\equiv \frac{1}{\sqrt{2}}|0_{P,s}1_{P,s}\rangle \otimes (|0_{s,M}1_{i,M}\rangle + |1_{s,M}0_{i,M}\rangle)\,. \end{aligned} \tag{3.3}$$

From Eq. (3.2)-(3.3) it is clear that the photons emitted by the type-II crystal are not polarization entangled in general, unless signal and idler photons are indistinguishable spectrally (frequency degenerate) and temporally (timing compensated), in which case the T and B beams are polarization entangled, as demonstrated by Fiorentino, Kuklewicz, and Wong [82]. In the present experiment we ensure that initially the photons are *not* polarization entangled by *not* compensating the birefringence-induced time delay.

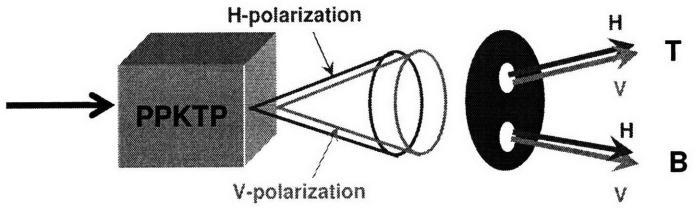

Figure 3-7: Generation of momentum entangled photon pairs from a type-II phase matched nonlinear crystal.

3.2.2 Application of SWAP gate to momentum entangled photon pairs

In this experiment, we start with a momentum entangled photon pair in $|\Psi\rangle_{\text{IN}}$, obtained in the manner of Figure 3-7. We apply a SWAP gate to each of the two photons, so that the quantum state stored in P qubit and M qubit of the same photon can be swapped. That is, the P qubit of the signal (idler) photon is swapped with the M qubit of the signal (idler) photon as follows:

$$\begin{aligned}
|\Psi\rangle_{\text{IN}} &= \frac{1}{\sqrt{2}}|0_{P,s}1_{P,i}\rangle \otimes (|0_{M,s}1_{M,i}\rangle + |1_{M,s}0_{M,i}\rangle) \\
&= \frac{1}{\sqrt{2}}(|0_{P,s}0_{M,s}\rangle|1_{P,i}1_{M,i}\rangle + |0_{P,s}1_{M,s}\rangle|1_{P,i}0_{M,i}\rangle) \\
\xrightarrow{\text{SWAP}} |\Psi\rangle_{\text{OUT}} &= \frac{1}{\sqrt{2}}(|0_{P,s}0_{M,s}\rangle|1_{P,i}1_{M,i}\rangle + |1_{P,s}0_{M,s}\rangle|0_{P,i}1_{M,i}\rangle) \\
&= \frac{1}{\sqrt{2}}(|0_{P,s}1_{P,i}\rangle + |1_{P,s}0_{P,i}\rangle) \otimes |0_{M,s}1_{M,i}\rangle \\
&= \frac{1}{\sqrt{2}}(|H_sV_i\rangle + |V_sH_i\rangle) \otimes |L_sR_i\rangle \qquad (3.4)
\end{aligned}$$

Eq. (3.4) clearly shows that the signal and idler polarizations of the output state are entangled. In principle, we require two SWAP gates, one for the signal and the other for the idler photon. However, Figure 3-7 shows that the signal and idler beams from SPDC share the same paths, and they eventually exit the SWAP gate in separate paths (L and R) according to Eq. (3.4). Therefore, we can use a single SWAP gate to swap both signal and idler photons, and separate them after the SWAP gate with

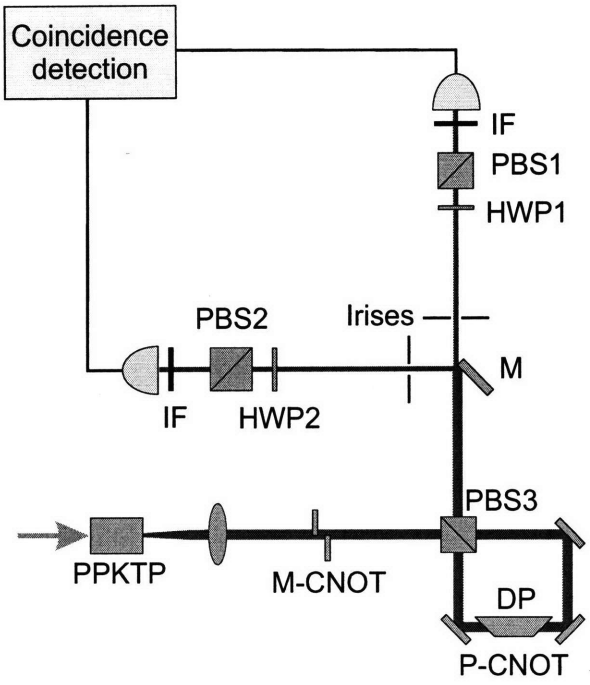

Figure 3-8: Schematic of experimental setup.

a mirror that reflects one part of the beam and not the other as shown in Figure 3-8. Also observe that if we omit the last M-CNOT gate of the SWAP gate, the output state is

$$|\Psi'\rangle_{\text{OUT}} = \frac{1}{\sqrt{2}}(|H_s H_i\rangle + |V_s V_i\rangle) \otimes |L_s R_i\rangle \tag{3.5}$$

which is still polarization entangled, and the signal and idler photons occupy different paths so that they can still be separated with a mirror.

3.2.3 Experimental setup

Figure 3-8 shows our experimental setup for demonstrating the conversion of a momentum-entangled photon pair into a polarization-entangled pair using the quantum SWAP gate. We used pairs of down-converted photons from a 10 mm-long PPKTP crystal that was continuous-wave pumped at 398.5 nm for type-II phase-matched frequency-degenerate parametric down-conversion. The crystal temperature was adjusted so that the signal and idler photons were emitted in two overlapping cones with an ex-

ternal full divergence of ~13 mrad. The momentum modes were chosen with two single apertures after the SWAP gates, instead of placing the two-hole aperture mask right after the crystal as shown in Figure 3-7. We observed a higher gate fidelity with the separate apertures after the gates, probably due to a slight size mismatch of the two-hole mask. To implement the SWAP gate, we used the M-CNOT gate and the P-CNOT gate described in Section 3.1.2. In this experiment, the compensating wave plate in the M-CNOT gate was slightly tilted to change the length of the top beam path, thus allowing one to correct for path mismatch and compensate for the intrinsic phase shift of the P-CNOT gate. After the P-CNOT gate the state of the photon pair is described by Eq. (3.5); we separated the signal and idler photons using the mirror M shown in Figure 3-8 that reflected only the right section of the beam. Signal and idler beams were then separately sent through a 2.2-mm iris, a polarization analyzer formed by a HWP and a polarizer, and a 1-nm interference filter centered at 797 nm. Besides being used for polarization analysis, wave plate HWP2 in Figure 3-8 assumed the role of the second M-CNOT gate, thus completing the SWAP circuit. The photons were detected with single-photon counting modules (PerkinElmer SPCM-AQR-14) and we measured signal-idler coincidences through a fast AND gate with a 1-ns coincidence window [68]. Given the short coincidence window and the observed count rates (singles rates $\leq 100,000$ counts/s), accidental coincidences were negligible.

3.2.4 Measurement results

To test the performance of the SWAP gate we analyzed the resultant polarization entanglement. Figure 3-9 shows the coincidence rates versus the polarization analysis angle θ_2 in arm 2 of Fig. 3-8 when the analyzer in arm 1 was set at 0° (solid squares) and 45° (open circles). The visibility of the sinusoidal fits is $V_0 = 97 \pm 2\%$ for 0° data and $V_{45} = 88 \pm 2\%$ for the 45° data. The difference in visibility is due to the fact that V_{45} is more sensitive than V_0 to the imperfections of the source and the gate interferometer. A measurement of the S parameter for the Clauser-Horne-Shimony-Holt form of the Bell's inequality gives a value of 2.653 ± 0.004 that violates the classical limit of 2 by more than 150 standard deviations. These results clearly show

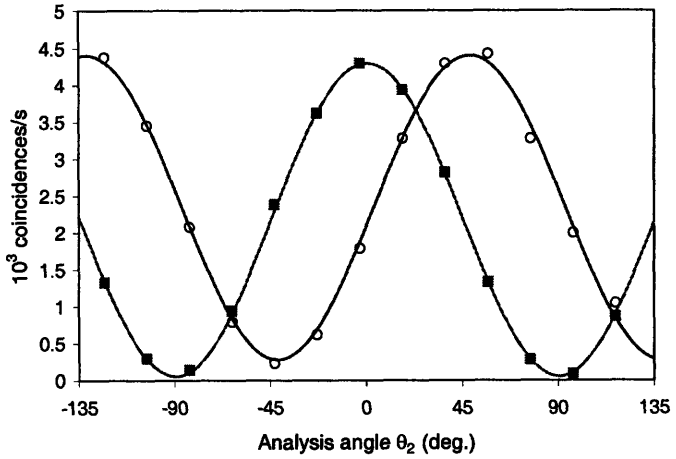

Figure 3-9: Coincidence rates as a function of the polarization analysis angle θ_2 in arm 2 when the analyzer in arm 1 was set at an angle $\theta_1 = 0°$ (solid squares) and 45° (open circles). The lines are sinusoidal fits to the data. Each data point is the result of an average over 10 s.

that our SWAP gate had a good fidelity and that the down-converted photons were indeed initially momentum entangled.

Analysis of error

The V_{45} results in Fig. 3-9 include errors due to imperfect interference at the gate (gate fidelity) and incomplete momentum entanglement of the source (source fidelity). To determine how well our setup approximates the ideal SWAP gate it is useful to separate the two contributions. As a test we sent an attenuated laser beam (filtered through a single-mode fiber and collimated with an aspheric lens) through the gate, with the laser frequency being the same as that of the down-converted photons. By injecting the laser with a linear polarization oriented at 45° relative to the H direction we measured the classical visibility of the SWAP gate. This test measurement gave a visibility V_{C1} of ~93% for the gate. We also verified that the M-CNOT gate did not affect the classical visibility in a measurable way. The classical measurement was repeated without the dove prism in the polarization Sagnac interferometer (of the P-CNOT gate) that yielded a visibility V_{C2} of ~95%. The 2% difference in the classical visibility ($V_{C1} - V_{C2}$) can be attributed to either imperfections in the dove prism or asymmetries in the injected laser beam. To further evaluate the cause, we

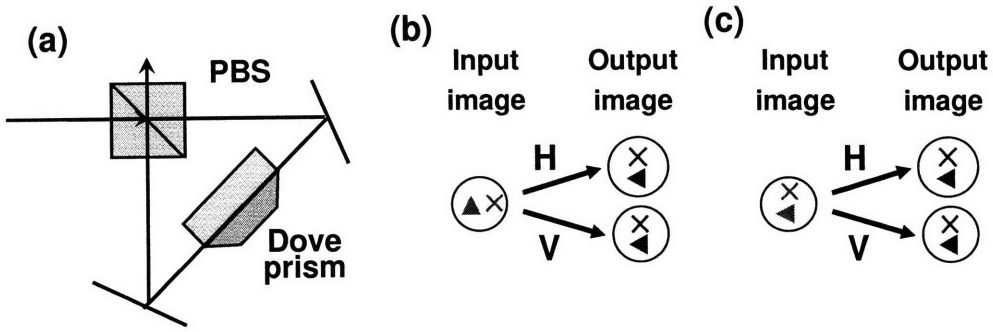

Figure 3-10: Triangular polarization Sagnac interferometer. (a) This geometry is tested with and without a dove prism. (b) Image transformation with the dove prism in PSI. (c) Image transformation without the dove prism in PSI. The beams are propagating into the paper and the images are viewed from behind.

repeated the test experiment with a polarization Sagnac interferometer in a triangular configuration that was insensitive to input beam asymmetry as shown in Figure 3-10. In this configuration the interference at the T position at the output originated from the same spot of the injected beam for both polarizations, with or without the dove prism (and similarly for the B position at the output). For the triangular configuration we obtained a difference in classical visibility with and without the dove prism of $\sim$2.5% that is comparable to that of the non-triangular configuration, indicating that the dove prism was responsible for a loss of $\sim$2% in the visibility of the P-CNOT gate. The remaining $\simeq$5% loss of classical visibility V_{C1} can be attributed to wavefront distortions introduced by the beam splitter cube. Given our quantum visibility V_{45} of 88% and the classical test measurement results of the P-CNOT interferometer we conclude that the source fidelity was 95% that was limited by imperfections in the momentum entanglement of the down-conversion source (probable causes: defects in PPKTP crystal poling and wavefront distortions of the downconverted beams). We therefore estimate that the SWAP gate fidelity was 93% and was limited by less than ideal components (polarizing beam splitter and dove prism).

3.3 Summary

In this chapter, I have shown that we can build reliable SPTQ quantum logics by using linear optical components. Single qubit gates on polarization qubits and M-CNOT gates can be simply implemented by wave plates. However, single qubit gates on momentum qubits and P-CNOT gates generally need an interferometric design that is phase sensitive, and I introduced a phase-stable robust P-CNOT using a Sagnac interferometer with an embedded dove prism which was developed by Fiorentino and Wong [17]. I also showed that we can realize a quantum SWAP gate which can swap the P and M qubits of the same photon using M-CNOT and P-CNOT gates, and how it can be used for building reliable single M-qubit gates. As a concrete demonstration of the utility of the SWAP gate, we applied the SWAP gate to momentum-entangled photon pairs, thereby transferring the entanglement from the momentum to the polarization degree of freedom of two photons. Our experiment opens the way to the demonstration of more complex SPTQ manipulation of entanglement including the manipulation of 3- and 4-photon states. This type of few-qubit quantum information processing combined with the entangled photon pairs is at the core of applications presented in this thesis.

Chapter 4

Generation of hyper-entangled state and complete Bell state measurement

A hyper-entangled photon pair refers to two photons entangled in more than one degree of freedom simultaneously. For example, Cinelli *et al.* [15, 34] and Yang *et al.* [16] generated a hyper-entangled state which is entangled in the polarization and momentum degrees of freedom, and Barreiro *et al.* [33] generated a hyper-entangled state which is entangled in polarization, spatial mode, and energy-time. Generation of the hyper-entangled state is usually done by spontaneous parametric downconversion (SPDC). The strong correlation due to the conservation of energy and the conservation of momentum, together with a superposition of all possible output states, automatically creates entanglement in the energy-time mode and the spatial mode, respectively [33, 34]. The hyper-entangled state has recently received attention in combination with single-photon two-qubit (SPTQ) quantum logic, because SPTQ gates can be utilized to manipulate and connect different types of entanglement contained in a single pair of photons. The hyper-entangled state with SPTQ quantum logic is potentially useful for a number of applications including a demonstration of All-Versus-Nothing violation of local reality [77, 15, 16], complete Bell state measurements [35, 85, 36, 86, 37], a stronger cryptographic scheme [87], and a demonstration

of entanglement distillation and purification.

In this chapter, we present our development of a hyper-entangled photon pair source. The starting point is the polarization entangled photon pair source presented in Chapter 2, which is compatible with both collinear and non-collinear output modes from the PPKTP crystal. We then collect a two-path output for each photon, similar to what we did to implement and test the SWAP gate in Chapter 3. The resulting output is then entangled in both polarization and momentum (or path) between the two photons. We then proceed to verify that the generated state is indeed hyper-entangled by applying it to a demonstration of SPTQ-based complete polarization Bell state measurements which normally are neither complete nor deterministic for polarization-entangled photons. An interesting property of hyper-entanglement is the ability to perform the Bell state measurements analysis deterministically for all four polarization Bell states, thus suggesting its potential utility in quantum information processing.

4.1 Generation of hyper-entangled photon pairs

In this section, we will show how we can generate the hyper-entangled state using the polarization entangled photon pair source introduced in Chapter 2.

In Chapter 2, we showed that the polarization-entangled photon pair can be generated from a bidirectionally pumped PPKTP crystal within a polarization-Sagnac interferometer. In Section 3.2.1, we also showed that the output photons in non-collinear spatial modes are automatically entangled in their momentum because of the conservation of the transverse momentum. In this chapter, we combine these two properties to generate a hyper-entangled photon pairs, whose quantum state can be represented as a tensor product of a polarization-entangled qubit state and a momentum-entangled qubit state:

$$|\Psi_P\rangle\otimes|\Phi_M\rangle = (\cos\theta_P|H\rangle_A|V\rangle_B + \sin\theta_P|V\rangle_A|H\rangle_B)\otimes(\cos\theta_M|L\rangle_A|L\rangle_B + \sin\theta_M|R\rangle_A|R\rangle_B)\ , \tag{4.1}$$

where subscript P (M) refers to polarization (momentum), subscript A (B) indicates that the corresponding qubit is sent to Alice (Bob) side, H (V) represents horizontal (vertical) polarization, and L (R) is the left (right) path. θ_P is completely determined by the pump polarization as discussed in Section 2.3.1, and θ_M can be easily controlled by the location of a double aperture mask and the temperature of the crystal, as will be discussed in Chapter 5. In this chapter, we are only interested in the $\theta_P = \theta_M = 45°$ case and we will show how we can generate such a state.

Assuming $\theta_P = \theta_M = 45°$, Eq. (4.1) can be expanded into the four terms

$$
\begin{aligned}
&|\Psi_P\rangle \otimes |\Phi_M\rangle \\
&\propto (|H\rangle_A|V\rangle_B + |H\rangle_A|V\rangle_B)\,|L\rangle_A|L\rangle_B + (|V\rangle_A|H\rangle_B + |V\rangle_A|H\rangle_B)\,|R\rangle_A|R\rangle_B \quad (4.2)\\
&= |HL\rangle_A|VL\rangle_B + |VL\rangle_A|HL\rangle_B + |HR\rangle_A|VR\rangle_B + |VR\rangle_A|HR\rangle_B \\
&= \hat{a}^\dagger_{H,L_A}\hat{b}^\dagger_{V,L_B}|0\rangle + \hat{a}^\dagger_{V,L_A}\hat{b}^\dagger_{H,L_B}|0\rangle + \hat{a}^\dagger_{H,R_A}\hat{b}^\dagger_{V,R_B}|0\rangle + \hat{a}^\dagger_{V,R_A}\hat{b}^\dagger_{H,R_B}|0\rangle, \quad (4.3)
\end{aligned}
$$

where $\hat{a}^\dagger_{P,M_A}$ ($\hat{b}^\dagger_{P,M_B}$) is the creation operator for a photon with polarization P and momentum M on Alice (Bob) side. Figure 4-1 shows the four possible photon pair modes we are interested in, and (a)-(d) correspond to the terms in Eq. (4.3), in the same order.

Note that left paths (L_A, L_B) and right paths (R_A, R_B) defined by two double aperture masks in Figure 4-1 are intentionally drawn asymmetrically with respect to the pump axis to emphasize that they do not have to be symmetric to create a generalized hyper-entangled state in Eq. (4.1). This might be a little counter-intuitive compared to Figure 3-7, where the double aperture mask has to be located symmetric with respect to the pump axis. The difference here is that the conjugate path of L_A is L_B, and not R_B, as is clear from (a) and (b) of Figure 4-1. In other words, according to Eq. (4.2), the hyper-entangled state is a superposition of two polarization-entangled states: the first polarization-entangled term $((|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B)|L\rangle_A|L\rangle_B)$ in Eq. (4.2) can be obtained by collecting the output propagating in L_A-L_B paths, corresponding to (a) and (b) of Figure 4-1, while the second polarization-entangled term $((|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B)|R\rangle_A|R\rangle_B)$ can be obtained by collecting the output

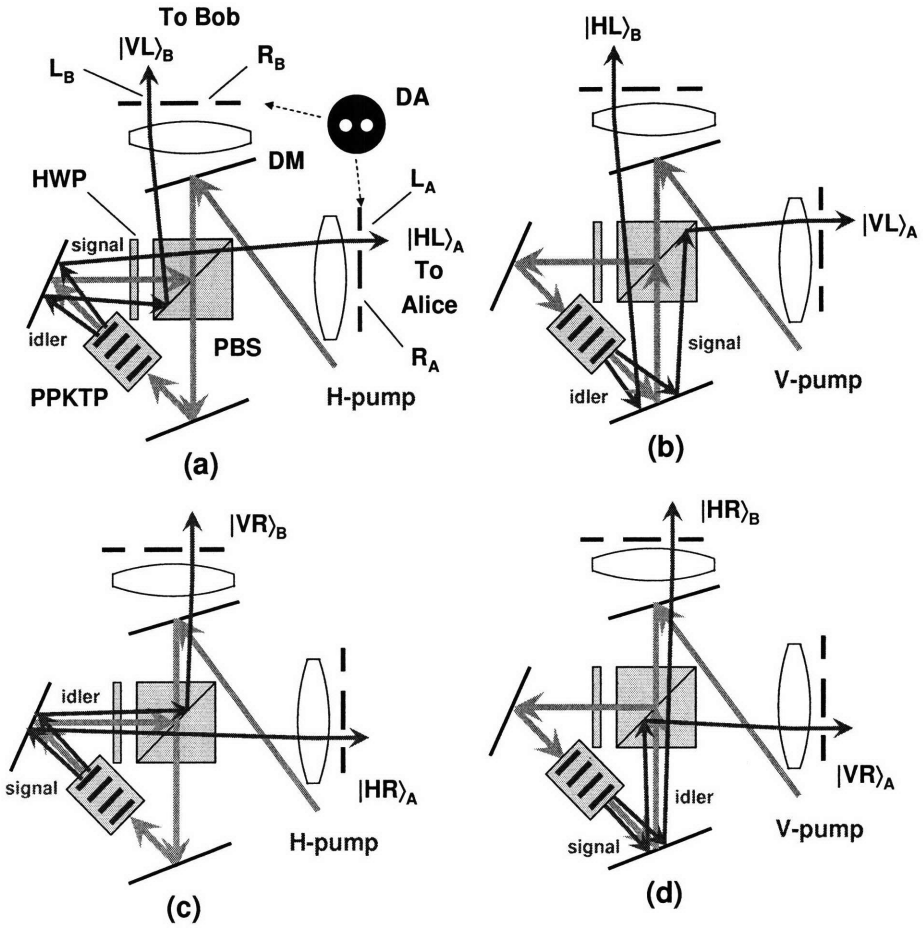

Figure 4-1: Four possible polarization-momentum combinations from bidirectionally pumped SPDC. Generation of (a) $\hat{a}^\dagger_{H,L_A}\hat{b}^\dagger_{V,L_B}|0\rangle$ state, (b) $\hat{a}^\dagger_{V,L_A}\hat{b}^\dagger_{H,L_B}|0\rangle$ state, (c) $\hat{a}^\dagger_{H,R_A}\hat{b}^\dagger_{V,R_B}|0\rangle$ state, (d) $\hat{a}^\dagger_{V,R_A}\hat{b}^\dagger_{H,R_B}|0\rangle$ state. The output state is a superposition of these four output states as shown in Eq. (4.2). DM: dichroic mirror, DA: double aperture mask.

propagating in R_A-R_B paths, corresponding to (c) and (d). Therefore, to create a hyper-entangled state, in principle, we can choose R_A and R_B independent of L_A and L_B, and this freedom is used in Chapter 5. For the experiment in this chapter, we choose symmetric L and R paths to generate the state in Eq. (4.3) because the output from the symmetric paths is more convenient for generating a hyper-entangled state with $\theta_M = 45°$.

4.2 Verification of hyper-entanglement

Incomplete quantum teleportation based on SPTQ quantum logic

In this section, we show that we can verify a hyper-entangled state given in Eq. (4.2) by using incomplete quantum teleportation [60]. Consider first a simpler problem. If we are given one of the four Bell states encoded in two qubits, the most direct way to confirm it is to apply a controlled-NOT (CNOT) gate between those two qubits and a Hadamard gate to the control qubit in sequence, and measure those two qubits as shown in Figure 4-2. The Hadamard gate is a single qubit operation which transforms $|0\rangle$ into $(|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle$ into $(|0\rangle - |1\rangle)/\sqrt{2}$.

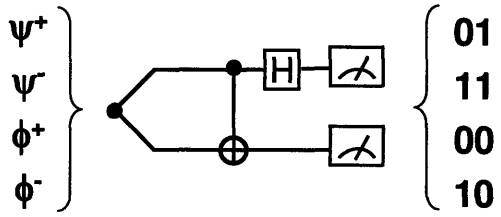

Figure 4-2: Bell basis analyzer. $|\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$, $|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and H is a Hadamard gate [81].

Unfortunately this scheme does not work for the case of two entangled photons, because we do not have a deterministic CNOT gate between two photons (see introduction of Chapter 3). However, we have already confirmed that the output from SPDC is entangled in the momentum qubit in Section 3.2, and we can use this momentum entanglement to show that the polarization degree of freedom is also

entangled simultaneously. Consider that hyper-entangled photon pairs are shared

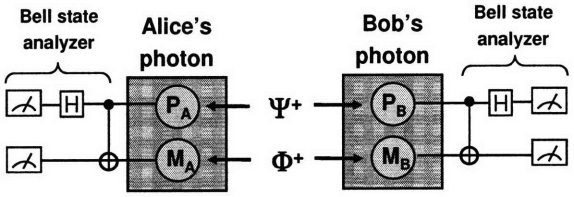

Figure 4-3: Polarization Bell state analyzer with the help of momentum entanglement.

between Alice and Bob as shown in Figure 4-3, and the polarization qubits are entangled in $|\Psi_P^+\rangle_{AB} \equiv (|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B)/\sqrt{2})$ and the momentum qubits are entangled in $|\Phi_M^+\rangle_{AB} \equiv (|L\rangle_A|L\rangle_B + |R\rangle_A|R\rangle_B)/\sqrt{2})$. We can use the entangled momentum qubit pair as a quantum channel to teleport Alice's polarization qubit to Bob's momentum qubit. Then we project the P qubit and M qubit of Alice's photon into one of the four Bell bases defined as $|\psi^\pm\rangle \equiv (|H\rangle|L\rangle \pm |V\rangle|R\rangle)/\sqrt{2}$ and $|\phi^\pm\rangle \equiv (|H\rangle|R\rangle \pm |V\rangle|L\rangle)/\sqrt{2}$. Generally the Bell basis projection can be accomplished by a Bell state analyzer similar to Figure 4-2. In this case, we can build a Bell state analyzer for Alice's photon by using a polarization-controlled NOT (P-CNOT) gate and a Hadamard gate on the polarization qubit as shown on the left-hand side of Figure 4-3. This Hadamard gate is just a half wave plate (HWP) tilted at 22.5° to rotate the polarization by $\pi/4$. Then depending on the measurement result of Alice's Bell state analyzer, the hyper-entangled state will be projected into one of the following four terms:

$$|\Psi_P^+\rangle_{AB} \otimes |\Phi_M^+\rangle_{AB} = |\psi^+\rangle_A|\phi^+\rangle_B - |\psi^-\rangle_A|\phi^-\rangle_B + |\phi^+\rangle_A|\psi^+\rangle_B - |\phi^-\rangle_A|\psi^-\rangle_B\,. \quad (4.4)$$

If we identify $|H\rangle$ and $|R\rangle$ as $|0\rangle$ and identify $|V\rangle$ and $|L\rangle$ as $|1\rangle$, the polarization Bell state $|\Psi_P^+\rangle_{AB} = (|0_A1_B\rangle + |1_A0_B\rangle)/\sqrt{2}$ corresponds to $|\psi^+\rangle_B = (|0_P1_M\rangle + |1_P0_M\rangle)/\sqrt{2}$ and we expect that $|\psi^+\rangle_B$ will be the final state of Bob's photon after a complete quantum teleportation procedure. If we rewrite Eq. (4.4) into the following expression

$$|\Psi_P^+\rangle_{AB} \otimes |\Phi_M^+\rangle_{AB} = \{|\psi^+\rangle_A(I_P \otimes \sigma_{x,M})_B - |\psi^-\rangle_A(I_P \otimes \sigma_{y,M})_B + |\phi^+\rangle_A(I_P \otimes I_M)_B - |\phi^-\rangle_A(I_P \otimes \sigma_{z,M})_B\}|\psi^+\rangle_B , \quad (4.5)$$

it is clear that complete quantum teleportation can be achieved by applying one of the four single qubit operators (I_M, $\sigma_{x,M}$, $\sigma_{y,M}$, $\sigma_{z,M}$) to Bob's momentum qubit depending on Alice's projection result, due to the property of $\sigma_{x,M}^2 = \sigma_{y,M}^2 = \sigma_{z,M}^2 = I_M$. In our scheme, this post-measurement step is omitted and we call it incomplete quantum teleportation. However, we can certainly distinguish Bob's final four Bell states using another Bell basis analyzer on his side as shown in Figure 4-3. This means that if the initial state is hyper-entangled, the results of Bob's Bell basis analyzer and Alice's Bell basis analyzer should be strongly correlated according to Eq. (4.4). This type of relation was also used in an entanglement swapping experiment [88], where only one of the four terms in Eq. (4.4) was measured.

Complete polarization Bell state measurement

The incomplete teleportation discussed in the previous section can be considered in a different context. It is well known that it is impossible to use only linear optical components to completely distinguish the four polarization Bell states stored in a pair of photons [75, 76]. However, if those two photons are also entangled in a different degree of freedom such as momentum [35, 85, 37] or energy-time [36, 86], we can circumvent the problem, and this method is called a SPTQ-based complete Bell state measurement.

Now I will show how incomplete quantum teleportation helps us distinguish four different polarization Bell states. We define four polarization Bell states as $|\Psi_P^\pm\rangle \equiv (|H\rangle_A|V\rangle_B \pm |V\rangle_A|H\rangle_B)/\sqrt{2})$ and $|\Phi_P^\pm\rangle \equiv (|H\rangle_A|H\rangle_B \pm |V\rangle_A|V\rangle_B)/\sqrt{2})$, and if we insert $|\Phi_P^\pm\rangle$ or $|\Psi_P^-\rangle$ instead of $|\Psi_P^+\rangle$ on the left-hand side of Eq. (4.5), $|\psi^+\rangle_B$ on the right-hand side of Eq. (4.5) will also change to $|\phi^\pm\rangle_B$ or $|\psi^-\rangle_B$, respectively. Therefore, even if Alice measures the same $|\psi^+\rangle_A$, Bob will measure different Bell

states depending on the initial polarization Bell states, and this correlation between Alice's Bell state and Bob's Bell state can be used to completely identify the four polarization Bell states. If we explicitly expand all the possible combinations for the four different polarization Bell states, we obtain

$$
\begin{aligned}
|\Phi_P^+\rangle_{AB} \otimes |\Phi_M^+\rangle_{AB} &= |\phi^+\rangle_A|\phi^+\rangle_B + |\phi^-\rangle_A|\phi^-\rangle_B + |\psi^+\rangle_A|\psi^+\rangle_B + |\psi^-\rangle_A|\psi^-\rangle_B \\
|\Phi_P^-\rangle_{AB} \otimes |\Phi_M^+\rangle_{AB} &= -|\phi^+\rangle_A|\phi^-\rangle_B - |\phi^-\rangle_A|\phi^+\rangle_B - |\psi^+\rangle_A|\psi^-\rangle_B - |\psi^-\rangle_A|\psi^+\rangle_B \\
|\Psi_P^+\rangle_{AB} \otimes |\Phi_M^+\rangle_{AB} &= |\psi^+\rangle_A|\phi^+\rangle_B - |\psi^-\rangle_A|\phi^-\rangle_B + |\phi^+\rangle_A|\psi^+\rangle_B - |\phi^-\rangle_A|\psi^-\rangle_B \\
|\Psi_P^-\rangle_{AB} \otimes |\Phi_M^+\rangle_{AB} &= -|\psi^+\rangle_A|\phi^-\rangle_B + |\psi^-\rangle_A|\phi^+\rangle_B - |\phi^+\rangle_A|\psi^-\rangle_B + |\phi^-\rangle_A|\psi^+\rangle_B ,
\end{aligned}
\tag{4.6}
$$

showing all 16 distinct combinations of Alice's Bell state and Bob's Bell state. This type of complete Bell state measurement was demonstrated by Barbieri *et al.* [37] using hyper-entanglement embedded in the polarization and momentum degrees of freedom and by Schuck *et al.* [36] using hyper-entanglement in polarization and time-energy degrees of freedom, and we will use our results of the complete Bell state measurement to compare the quality of our hyper-entangled state with those from other groups.

4.3 Experimental setup

Figure 4-4 shows our experimental setup. As a hyper-entangled photon pair source, we used the bidirectionally pumped type-II SPDC within a polarization Sagnac interferometer (PSI), which is similar to the polarization entanglement source described in Section 2.4. For hyper-entanglement in polarization and momentum we utilized the non-collinear output modes. PPKTP was pumped by a 404.775-nm diode laser with ~5 mW, and, to avoid water condensation at low crystal temperatures, we collected slightly non-degenerate output wavelengths at 809.55±0.5 nm through a 1-nm interference filter (IF) on each side. To generate all four polarization Bell states ($|\Psi_P^{\pm}\rangle$, $|\Phi_P^{\pm}\rangle$), we used the first HWP in Alice's path to switch between $|\Psi_P\rangle$ and $|\Phi_P\rangle$. To switch between $|\Psi_P^+\rangle$ ($|\Phi_P^+\rangle$) and $|\Psi_P^-\rangle$ ($|\Phi_P^+\rangle$) we changed the pump polarization using HWP_P and QWP_P.

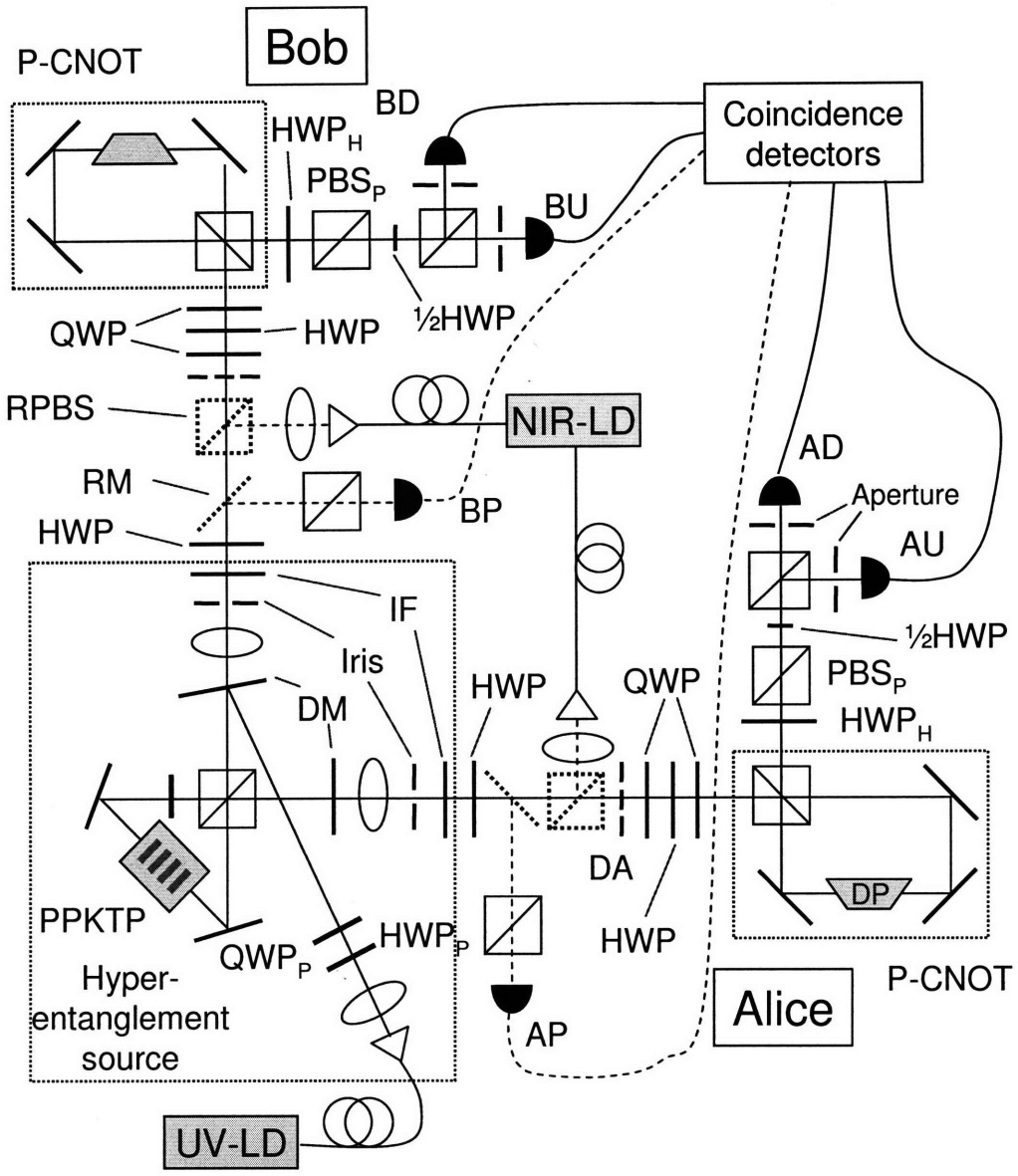

Figure 4-4: Experimental setup for complete Bell state measurements. All the beam splitters shown in this figure are polarizing beam splitter (PBS). RPBS: removable PBS, RM: removable mirror, DM: dichroic mirror, IF: interference filter, DA: dual aperture mask, DP: dove prism, UV-LD: UV-laser diode, IR-LD: IR-laser diode, 1/2HWP: a half-cut HWP that flips the polarization only in the up (U) path.

In Figure 4-4, the removable mirror (RM) in each output path was used to check the quality of the polarization entanglement independent of the momentum entanglement. The removable polarizing beam splitter (RPBS) was mainly used to couple a near-IR laser into the PSI to align the opposite arm. To implement the Bell state analyzer shown in Figure 4-3, each arm had one polarization-controlled NOT (P-CNOT) gate followed by a half wave plate (HWP_H) whose fast axis was tilted by $\pm 22.5°$. In this setup, the HWP_H was used for two purposes: it implemented a Hadamard gate, and also, by switching the fast axis of the HWP_H between $\pm 22.5°$, it selectively transmitted only H or V polarization output from the Hadamard gate through PBS_P to measure the polarization qubit. To measure the momentum qubit, a half-cut HWP (1/2HWP) followed by another PBS was used. The 1/2HWP changed the polarization from H to V only in the up (U) path, so that the photons in the U path and the down (D) path could be spatially separated by the subsequent PBS. On Alice's (Bob's) side, the photons in the U path was measured by the AU (BU) detector and the photons in the D path is measured by the AD (BD) detector. At the input of each P-CNOT gate, we placed one half-wave plate sandwiched by two quarter-wave plates (QWP) whose fast axes were tilted by 45° with respect to the horizontal axis to compensate for the phase shifts intrinsic to the P-CNOT gate, as discussed in Section 3.1.2. This combination of the wave plates added only a relative phase shift to the vertically polarized component without changing the amplitudes of both polarization components, for any arbitrary polarization input.

To align the P-CNOT gate on Alice's or Bob's side with respect to the output spatial mode of the hyper-entangled photon pairs, we used a near-IR laser diode (NIR-LD) which we fiber-coupled and injected into the main system through the RPBS. The NIR-laser coupled from Bob's arm was used to align the P-CNOT gate on Alice's arm after going through the PSI, and vice versa. To align the NIR laser to overlap with the collinear output of SPDC, we constrained the spatial mode of the collinear SPDC output with an iris near the source shown in the setup of Figure 4-4, and recorded the location of this collinear output on a CCD camera (not show in the setup). We then aligned the NIR laser to coincide with the same position on the CCD camera

after going through the same iris.

Another method we tried to overlap the NIR laser with the collinear SPDC output was to use one fiber as a SPDC output coupler. For example, to overlap the NIR laser from Bob's side with the collinear output propagating to Alice, we first aligned the fiber coupler on Alice's side so that the output for Alice was maximally coupled into Alice's fiber coupler. This guaranteed that Alice's fiber coupler was almost perfectly aligned with the collinear output propagating towards Alice. Then we would couple the NIR laser injected from Bob's side into the fiber at Alice's side. When the coupling was maximized, the NIR laser from Bob should be overlapping with the collinear SPDC output propagating toward Alice. Even though these two methods were good enough for aligning each P-CNOT gate individually to observe a high visibility with the classical interference measurement, they were not optimal for aligning with respect to the hyper-entangled photon pairs. Therefore, for the fine alignment, we used the polarization-entangled collinear output pairs combined with the coincidence measurement. Once the alignment with the collinear output mode is done, we opened up the irises, and inserted dual aperture masks in both arms to collect non-collinear output pairs for the hyper-entanglement.

We also tried different sizes of dual aperture masks (DA) at different locations, and the best result was obtained when we placed the DA before the CNOT gate, and also placed the single apertures with the same diameter directly in front of the detectors. The optimal diameter of each aperture was 1 mm, and the distance between the centers of two apertures was 2 mm.

4.4 Measurement result

To demonstrate the complete Bell state measurement, we measured the coincidence counts (1.6 ns coincidence window [68]) between Alice's Bell state analyzer and Bob's Bell state analyzer. Figure 4-5 shows the coincidence counts per second between Alice's measurements and Bob's measurements. For example, if the polarizations of the two photons shared by Alice and Bob are entangled in $|\Psi_P^+\rangle_{AB}$ state, according

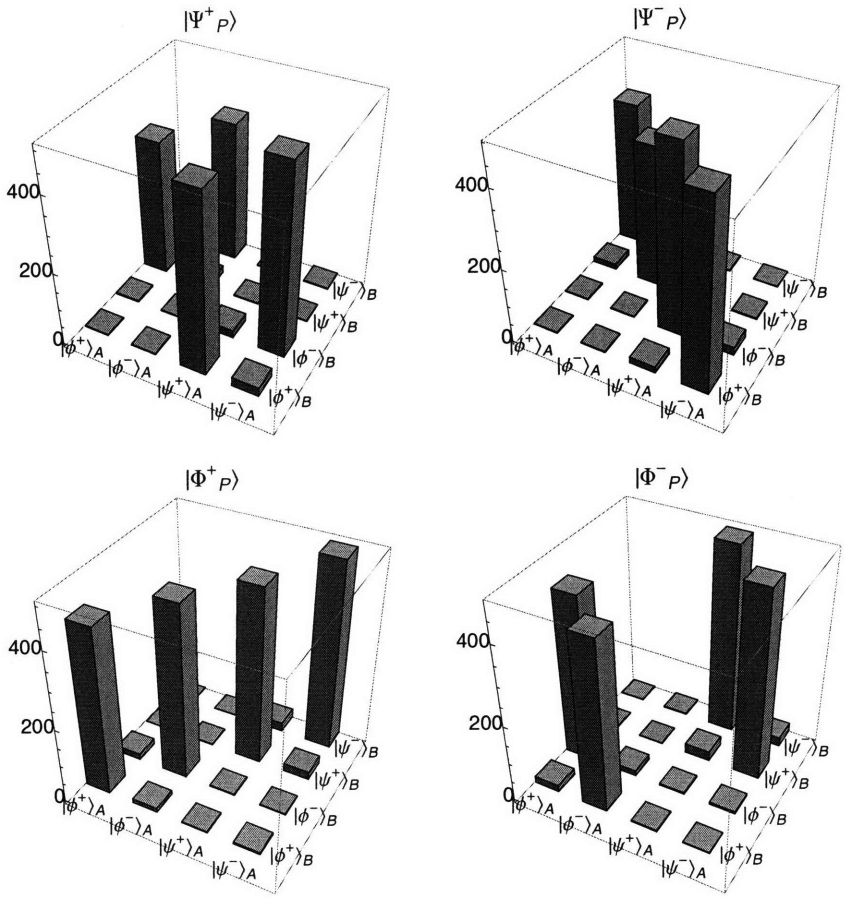

Figure 4-5: Coincidence counts between Alice's Bell state measurement and Bob's Bell state measurement. The unit of z-axis is coincidence counts per second, and each point is averaged over 60 seconds. Pump power was ~5mW, and the output bandwidth was restricted to 1 nm by interference filters.

to Eq. (4.1), we expect to see the same number of coincidences for $|\psi^+\rangle_A|\phi^+\rangle_B$, $|\psi^-\rangle_A|\phi^-\rangle_B$, $|\phi^+\rangle_A|\psi^+\rangle_B$, $|\phi^-\rangle_A|\psi^-\rangle_B$, and no coincidences for other 12 combinations. The distribution for $|\Psi^+_P\rangle_{AB}$ in Figure 4-5 agrees with this prediction. The coincidence distributions in Figure 4-5 clearly show that we can determine the polarization Bell state based on the coincidence signature between Alice and Bob.

We calculate the accuracy of our complete Bell state measurement for different Bell state inputs. For example, if the input Bell state was $|\Phi^+_P\rangle_{AB}$, we have probabilities of $\{0.9527, 0.0363, 0.0040, 0.0069\}$ to identify this state as $\{|\Phi^+_P\rangle_{AB}, |\Phi^-_P\rangle_{AB}, |\Psi^+_P\rangle_{AB}, |\Psi^-_P\rangle_{AB}\}$. We plot these identification probabilities in Figure 4-6. From this plot, we

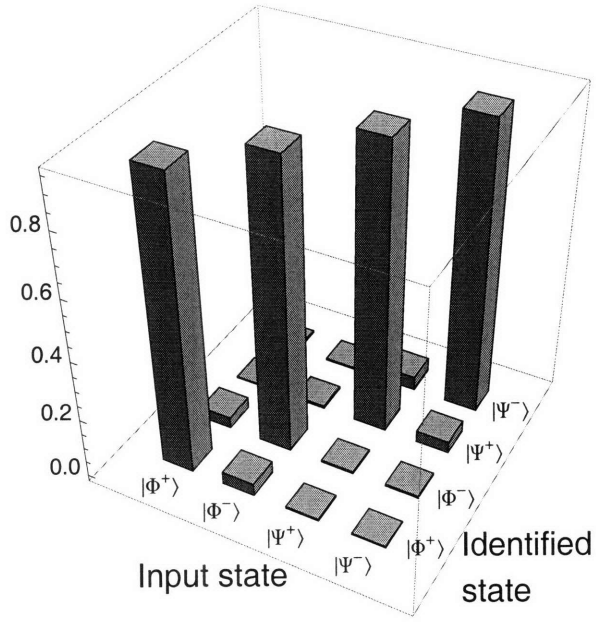

Figure 4-6: Probabilities of correct and incorrect identification for the different input states.

see that the major error (~5%) comes from the wrong identification between $|\Phi_P^+\rangle_{AB}$ and $|\Phi_P^-\rangle_{AB}$ or between $|\Psi_P^+\rangle_{AB}$ and $|\Psi_P^-\rangle_{AB}$. Those states are different only in their phases, and we believe these incorrect phases are due to the limited accuracy of the phase correction in the P-CNOT gates. Our probabilities of four correct identifications are 94.2%~95.3%, which is higher than 87.7%~89.9% obtained by Barbieri *et al.* [37] or 81.1%~88.8% obtained by Schuck *et al.* [36].

4.5 Summary

In this chapter, we have developed a hyper-entangled photon pair source and demonstrated a method to verify the hyper-entanglement. To generate a pair of photons entangled in the polarization degree of freedom and the momentum degree of freedom simultaneously, we extended the collinear polarization entangled photon pair source to operate in the non-collinear mode. To verify the hyper-entangled state, we used incomplete quantum teleportation which teleports the polarization qubit of Alice to the momentum qubit of Bob through a quantum channel established by the

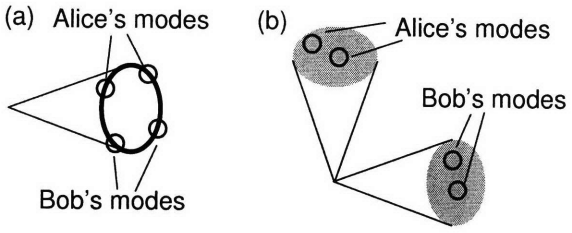

Figure 4-7: Momentum output modes. (a) Possible momentum modes based on a non-collinear polarization source. (b) Possible momentum modes based on a collinear polarization source.

known momentum entanglement, and therefore allows the SPTQ-based complete polarization Bell state measurement. The result of our SPTQ-based complete Bell state measurement shows much higher accuracy in identifying the input polarization Bell states compared to other group's approaches, suggesting the better quality of our hyper-entangled state and the higher reliability of our SPTQ quantum logic.

Our hyper-entanglement source has a unique feature compared to other types of hyper-entanglement sources [15, 34, 16, 33]. Other types of hyper-entangled photon pair sources are generally based on the non-collinear polarization entangled photon pair sources, and therefore the output spatial modes for Alice and Bob are picked from the same ring as shown in Figure 4-7 (a). However the output modes for Alice and Bob in our source are already separated by a PBS so that we can pick any of the output spatial modes in the entire cone including the collinear mode. This gives us more freedom in generating a hyper-entangled state. For example, we can use the entanglement in higher-dimensional momentum qudit [83, 84] or even continuous momentum entanglement.

Chapter 5

Entanglement distillation using Schmidt projection

A shared entangled state is essential in many quantum information processing applications such as quantum teleportation [60], quantum computation [8, 62, 63], quantum cryptography [61], and quantum repeaters [65]. These protocols generally assume that maximally entangled states, such as the Bell states, are available between two remote parties. In reality, these states become non-maximally entangled or partially mixed because of dissipation and decoherence through interactions with the environment. To overcome these problems, several ways to improve the quality of the entanglement have been suggested [38, 79, 89, 39, 40, 41, 42, 90, 45, 46, 91]. Among these methods, Schmidt projection [38] has an interesting property that it can be applied to more than two pairs of entangled qubits at the same time and the distillation efficiency can approach unity when applied to a large number of pairs. Despite these advantages, Schmidt projection is considered difficult to implement because it requires simultaneous collective measurements on multiple qubits.

In this chapter, we present our implementation of Schmidt projection on four qubits using hyper-entangled photon pairs and single-photon two-qubit (SPTQ) quantum logic. We first describe how the Schmidt projection protocol works, and how this protocol can be implemented with hyper-entangled photon pairs. Then we show that we can control the degree of entanglement in polarization and momentum by changing

the pump polarization and the temperature of the crystal, respectively. We also show that the output of Schmidt projection can be converted into polarization entangled state, and the experimental results follow.

5.1 Theoretical background

In this section, we first explain the advantage of Schmidt projection over other methods, and how to extract a maximally entangled state from the partially entangled state with simple examples. Based on these ideas, we also discuss how to implement the Schmidt projection method in the experiment.

If we are given one or more pairs of entangled qubits and we can extract from them a smaller number of pairs with a higher degree of entanglement using local operations and classical communication, this process is called entanglement distillation. In the literature, this process is also called entanglement purification or entanglement concentration, but we are following the convention given by Ref. [39], where entanglement purification refers to the enhanced purity of a mixed state by extracting a number of purer entangled states from a larger number of less pure entangled pairs, and entanglement concentration increases both the degree of entanglement and the purity of a given state.

As a measure of the degree of entanglement, we are using the following definitions. For a partially entangled pure state $|\psi\rangle$ shared by Alice (A) and Bob (B), the von Neumann entropy of the partial density matrix gives a measure of the entanglement $E(\psi)$ [38]:

$$E(\psi) = -\mathrm{Tr}(\rho_A \log_2 \rho_A) = -\mathrm{Tr}(\rho_B \log_2 \rho_B)\,, \tag{5.1}$$

where $\rho_A(\rho_B)$ is the partial trace of $|\psi\rangle\langle\psi|$ over subsystem B (A). In general, $0 \leq E(\psi) \leq \log_2 d$ for a bipartite qudit system in a $2d$-dimensional Hilbert space. A natural extension for a mixed state with a density matrix ρ is the entanglement of formation $E(\rho)$, which is the smallest expectation value of entanglement E of any ensemble of pure states realizing ρ [92]. In other words, to calculate the entanglement of formation (EOF), we need to consider all possible decompositions of ρ, that is,

all ensembles of states $|\psi_i\rangle$ with probabilities p_i satisfying $\rho = \Sigma_i p_i |\psi_i\rangle\langle\psi_i|$. Then EOF is defined as $E(\rho) = \min\Sigma_i p_i E(\psi_i)$. In general this quantity is difficult to calculate. However, for a bipartite qubit system, an explicit formula for entanglement of formation exists [93].

Most of the protocols for enhancing E can only be applied to one [39, 42] or two pairs of entangled qubits at a time [45, 46, 40, 41] and therefore have a fixed distillation efficiency independent of the number of initial pairs. In contrast, Bennett *et al.* showed that Schmidt projection (SP) can be applied to n pairs of partially entangled pure state with $E(\psi)$ to extract $n \cdot E(\psi)$ pairs of maximally entangled Bell state in the limit of large n [38], and this property is used to justify the definition of E in Eq. (5.1) as a measure of the degree of entanglement. Entanglement, and hence the SP technique, forms the basis of or is related to other common measures such as EOF, concurrence, and tangle [94]. Despite its role in the theoretical foundation of quantum information science, SP has been avoided in the experiments due to the difficulty of collective measurements.

To understand how Schmidt projection works, consider two pairs of identically entangled state, $|\psi\rangle_{AB} = \cos\theta|0\rangle_A \otimes |0\rangle_B + \sin\theta|1\rangle_A \otimes |1\rangle_B$, which can be described by

$$
\begin{aligned}
&|\psi\rangle_{A_1B_1} \otimes |\psi\rangle_{A_2B_2} \\
&\quad = \cos^2\theta|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{B_1}|0\rangle_{B_2} + \cos\theta\sin\theta|0\rangle_{A_1}|1\rangle_{A_2}|0\rangle_{B_1}|1\rangle_{B_2} \\
&\quad + \sin\theta\cos\theta|1\rangle_{A_1}|0\rangle_{A_2}|1\rangle_{B_1}|0\rangle_{B_2} + \sin^2\theta|1\rangle_{A_1}|1\rangle_{A_2}|1\rangle_{B_1}|1\rangle_{B_2} \qquad (5.2) \\
&\quad \equiv \cos^2\theta|0\rangle_A|0\rangle_B + \sin^2\theta|3\rangle_A|3\rangle_B + \cos\theta\sin\theta(|1\rangle_A|1\rangle_B + |2\rangle_A|2\rangle_B), \qquad (5.3)
\end{aligned}
$$

where in Eq. (5.3) we replace the binary representation of Alice's qubits and Bob's qubits by qudit notation (decimal number). For two entangled pairs, it is only necessary to project terms with the same coefficient ($\cos\theta\sin\theta$) whose form is that of a maximally entangled state. Eq. (5.3) shows that each term is locally orthogonal to each other, and therefore the result of Alice's local projection is perfectly correlated to that of Bob's local projection, thus making even classical communication unnec-

essary. In contrast, the non-SP methods used in ref. [45, 46] require that Alice and Bob compare their measurement results over a classical channel and change the phase based on their measurements.

When Schmidt projection is applied to $n > 2$ pairs of $|\psi\rangle_{AB}$:

$$
\begin{aligned}
&|\psi\rangle_{AB}^{\otimes n} \\
&\quad = (\cos\theta|0\rangle_{A_1}|0\rangle_{B_1} + \sin\theta|1\rangle_{A_1}|1\rangle_{B_1}) \otimes \cdots \otimes (\cos\theta|0\rangle_{A_n}|0\rangle_{B_n} + \sin\theta|1\rangle_{A_n}|1\rangle_{B_n}) \\
&\quad = \cos^n\theta|0\rangle_{A_1}\ldots|0\rangle_{A_n}|0\rangle_{B_1}\ldots|0\rangle_{B_n} \\
&\quad + \cos^{n-1}\theta\sin\theta(|0\rangle_{A_1}\ldots|0\rangle_{A_{n-1}}|1\rangle_{A_n}|0\rangle_{B_1}\ldots|0\rangle_{B_{n-1}}|1\rangle_{B_n} + \cdots \\
&\qquad\qquad + |1\rangle_{A_1}|0\rangle_{A_2}\ldots|0\rangle_{A_n}|1\rangle_{B_1}|0\rangle_{B_2}\ldots|0\rangle_{B_n}) \\
&\quad + \cdots + \sin^n\theta|1\rangle_{A_1}\ldots|1\rangle_{A_n}|1\rangle_{B_1}\ldots|1\rangle_{B_n}. \qquad (5.4)
\end{aligned}
$$

In Eq. (5.4), among 2^n terms, there are $n+1$ distinct Schmidt coefficients ($\cos^n\theta$, $\cos^{n-1}\theta\sin\theta, ..., \sin^n\theta$), and each group with the same coefficient $\cos^{n-k}\theta\sin^k\theta$ has $\binom{n}{k}$ terms that are maximally entangled, for $n > k > 0$ [38]. Alice and Bob project this state into one of $n-1$ orthogonal subspaces to extract the maximally-entangled states. Such a state can be directly used for faithful teleportation in a $\binom{n}{k}$-dimensional or smaller Hilbert space, or we can convert this state into a tensor product of Bell states, as described by Bennett *et al.* [38]. Consider a projected state

$$|T\rangle_{AB} = (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |2\rangle_A|2\rangle_B)/\sqrt{3}. \qquad (5.5)$$

The easiest but inefficient way to extract a Bell state from Eq. (5.5) is to project this state into a subspace made of $\{|0\rangle, |1\rangle\}$. Then this projection extracts a Bell state with a success probability of 2/3. However, if we have two identical $|T\rangle_{AB}$ states, we can extract the Bell state with a much higher success probability. If we combine the two identical states, the entire state becomes

$$
\begin{aligned}
&|T\rangle_{AB} \otimes |T\rangle_{AB} \\
&\quad = 1/3(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |2\rangle_A|2\rangle_B + |3\rangle_A|3\rangle_B + |4\rangle_A|4\rangle_B + |5\rangle_A|5\rangle_B
\end{aligned}
$$

$$+|6\rangle_A|6\rangle_B + |7\rangle_A|7\rangle_B + |8\rangle_A|8\rangle_B) \tag{5.6}$$

$$= \frac{2\sqrt{2}}{3}\left(\frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}\right)^{\otimes 3} + \frac{1}{3}|8\rangle_A|8\rangle_B\,, \tag{5.7}$$

where we use the qudit notation in Eq. (5.6) and the qubit notation for the tensor product in Eq. (5.7). Eq. (5.7) clearly shows that we can extract the Bell states more efficiently (8/9 of success probability) by combining two copies of $|T\rangle_{AB}$ than a single $|T\rangle_{AB}$. It is also proven that if this type of combining procedure is applied to many higher-dimensional maximally-entangled states, the efficiency of the conversion to a tensor product of Bell states approaches unity [38]. This step is not necessary in our experiment because, when Schmidt projection is applied to two pairs, the successful output is already a Bell state.

In the experiment, we demonstrate a proof-of-principle implementation of Schmidt projection by applying the SP protocol to two pairs of entangled qubits such as those given by Eq. (5.3). In our implementation, as an initial state, we use partially hyper-entangled photon pairs given by

$$\begin{aligned} |\psi_P\rangle \otimes |\psi_M\rangle \;=\; & (\cos\theta_P|V\rangle_A|V\rangle_B + \sin\theta_P|H\rangle_A|H\rangle_B) \\ & \otimes (\cos\theta_M|L\rangle_A|L\rangle_B + \sin\theta_M|R\rangle_A|R\rangle_B)\,, \end{aligned} \tag{5.8}$$

where subscript P (M) refers to polarization (momentum), H (V) represents horizontal (vertical) polarization, and L (R) is the left (right) path shown in figure 5-1. Schmidt projection requires that the two input pairs are identically entangled, and we set $\theta_P = \theta_M = \theta$ by the method described in the next section. With this setting, Eq. (5.8) can be expanded into

$$\cos^2\theta|VL\rangle_A|VL\rangle_B + \sin^2\theta|HR\rangle_A|HR\rangle_B + \cos\theta\sin\theta\,(|VR\rangle_A|VR\rangle_B + |HL\rangle_A|HL\rangle_B)\,. \tag{5.9}$$

Eq. (5.9) shows that we can realize SP protocol by transmitting the V-polarized photon in the R path and the H-polarized photon in the L path, which can be implemented with the SPTQ quantum logic introduced in Chapter 3. In the next

section, we will describe how to implement these ideas in the experiment.

5.2 Experimental setup

In the previous section, we showed that we can demonstrate Schmidt projection by combining the hyper-entangled photon pairs and SPTQ quantum logic. In this section, we first show how to generate a partially hyper-entangled photon pair. Then we proceed to describe the methods for performing the Schmidt projection on the hyper-entangled state using SPTQ quantum logic and for verifying the input and output of the distillation.

5.2.1 Generation of partially hyper-entangled photon pairs

To generate the hyper-entangled state that are entangled in both polarization and momentum degrees of freedom, we utilize spontaneous parametric down-conversion (SPDC) in a type-II phase-matched periodically poled $KTiOPO_4$ (PPKTP) crystal pumped by ~5 mW, similar to that described in Chapter 4. Efficient SPDC generation was accomplished using a polarization Sagnac interferometer (PSI) with bidirectional pumping at a wavelength of 404.775 nm and a crystal temperature of $\sim$ 19°C. The nondegenerate outputs at 809.55 ± 0.5 nm were detected through 1-nm interference filters (IF) to restrict the SPDC output bandwidth, thus obtaining high quality polarization entanglement. Compared to Chapter 4, the setup in this chapter has one important difference. In Chapter 4, to generate the maximally hyper-entangled state, we align the double aperture (DA) mask at a symmetric location with respect to the pump axis, whereas in this chapter, we aligned the right aperture to coincide with the pump axis as shown in Figure 5-1. The diameter of each aperture was 1 mm, and the distance between the centers of two apertures was 2 mm. This asymmetric choice of the two output paths allows us to control θ_M in Eq. (5.8) as follows.

Consider only the output in the collinear mode (R_A-R_B), corresponding to (a) and (b) of Figure 5-1, we showed in Chapter 2 that the output state is proportional

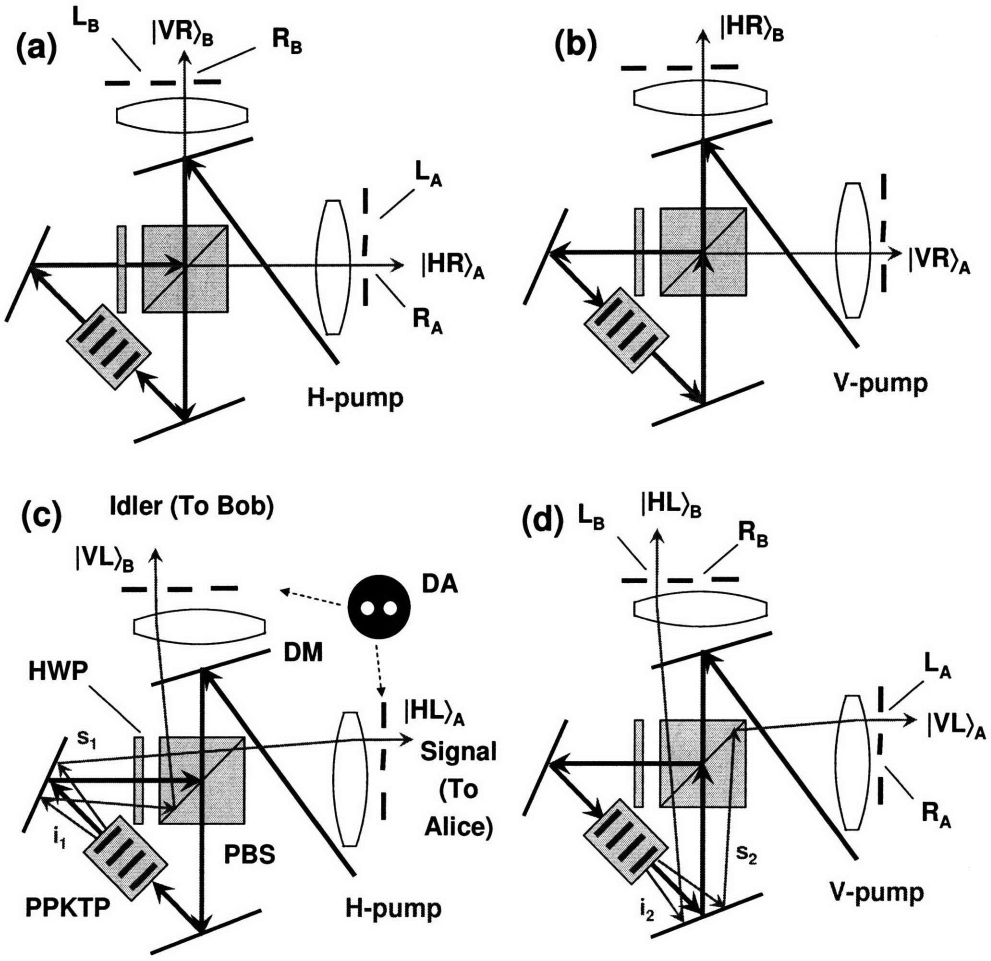

Figure 5-1: Four possible polarization-momentum combinations from bidirectionally pumped SPDC for the generation of (a) $|HR\rangle_A|VR\rangle_B$ state; (b) $|VR\rangle_A|HR\rangle_B$ state; (c) $|HL\rangle_A|VL\rangle_B$ state; (d) $|VL\rangle_A|HL\rangle_B$ state. The output state is a superposition of these four output states with different probability amplitudes. DM: dichroic mirror, DA: double aperture mask.

to

$$|\psi\rangle_{R_A R_B} \equiv (\cos\theta_P \hat{a}^\dagger_{H,R_A} \hat{b}^\dagger_{V,R_B} + e^{i\phi} \sin\theta_P \hat{a}^\dagger_{V,R_A} \hat{b}^\dagger_{H,R_B})|0\rangle\,, \tag{5.10}$$

where $\hat{a}^\dagger_{V,R_A}(\hat{b}^\dagger_{H,R_B})$ is a V (H) polarized photon creation operator for Alice's R_A (Bob's R_B) path, and similarly for $\hat{a}^\dagger_{V,R_B}$ and $\hat{b}^\dagger_{H,R_A}$. The relative amplitude (θ_P) and phase (ϕ) of the output state are determined by the adjustable relative amplitude and phase between the H and V polarization components of the pump. Similarly, if we focus only on the L_A-L_B output, corresponding to (c) and (d) of Figure 5-1, the output state is proportional to

$$|\psi\rangle_{L_A L_B} \equiv (\cos\theta_P \hat{a}^\dagger_{H,L_A} \hat{b}^\dagger_{V,L_B} + e^{i\phi} \sin\theta_P \hat{a}^\dagger_{V,L_A} \hat{b}^\dagger_{H,L_B})|0\rangle\,, \tag{5.11}$$

where θ_P and ϕ are the same as those in Eq. (5.10), because they are generated by the same pump laser. Now we consider the outputs in all four paths, then we have a superposition of Eq. (5.10) and Eq. (5.11). In general, the collinear output modes $(\hat{a}^\dagger_{R_A}, \hat{b}^\dagger_{R_B})$ and the non-collinear output modes $(\hat{a}^\dagger_{L_A}, \hat{b}^\dagger_{L_B})$ are excited with different probability amplitudes depending on the phase-matching condition, as explained in Section 2.1.3. Therefore, the four-path output state is an unbalanced superposition given by

$$\begin{aligned}
&\cos\theta_M|\psi\rangle_{L_A L_B} + \sin\theta_M|\psi\rangle_{R_A R_B} \\
&= \cos\theta_M(\cos\theta_P|HR_A\rangle|VR_B\rangle + e^{i\phi}\sin\theta_P|VR_A\rangle|HR_B\rangle) \\
&+ \sin\theta_M(\cos\theta_P|HL_A\rangle|VL_B\rangle + e^{i\phi}\sin\theta_P|VL_A\rangle|HL_B\rangle) \\
&= (\cos\theta_P|H_A\rangle|V_B\rangle + e^{i\phi}\sin\theta_P|V_A\rangle|H_B\rangle) \otimes (\cos\theta_M|L_A\rangle|L_B\rangle + \sin\theta_M|R_A\rangle|R_B\rangle)\,.
\end{aligned}$$

Figure 2-5 in Chapter 2 shows that we can change the flux ratio between the collinear output mode and the non-collinear output mode by adjusting the crystal phase-matching temperature, thereby allowing us to control θ_M. In the experimental setup, we have a half-wave plate placed in Alice's path, which flips Alice's polarization, and the final state is a partially hyper-entangled state given by Eq. (5.8). As an input state for Schmidt projection, we set $\theta_P = \theta_M = \theta$ except when we characterize the

input state as described in Section 5.3.1.

5.2.2 Implementation of Schmidt projection

To realize Schmidt projection on the hyper-entangled state, we use the SPTQ quantum logic introduced in Chapter 3. Schmidt projection can be implemented by combining a polarization beam splitter and half-wave plates which selectively change the polarizations in two paths (L, R). The output state of the Schmidt projection operation is converted by P-CNOT gates into a form of the polarization-entangled state so that we can analyze the output state in terms of the polarization correlation measurement.

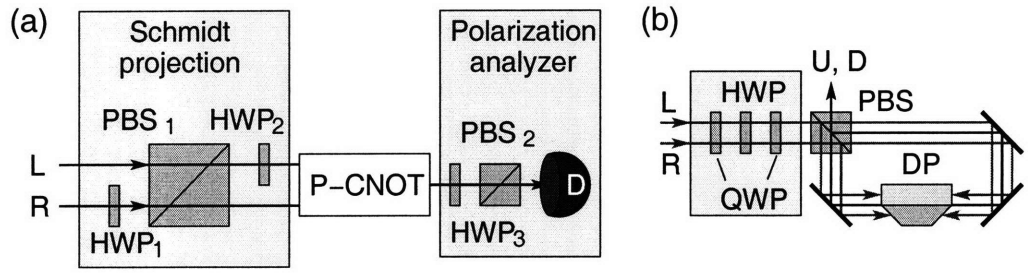

Figure 5-2: Entanglement distillation scheme for hyper-entangled photons. Both Alice and Bob have the same setup. (a) Schmidt projection transmits only two terms ($|VR\rangle$, $|HL\rangle$) of the initial state given in Eq. (5.8). P-CNOT gate combines two paths (R, L) into a common path for polarization state analysis. (b) P-CNOT with the phase compensation.

Figure 5-2 (a) shows the apparatus for implementing the Schmidt projection method. The key step is to project the initial state given by Eq. (5.9) into a subspace composed of $|VR\rangle$ and $|HL\rangle$ for both Alice and Bob without destroying any qubits. In principle, this can be accomplished by using one PBS in the L path transmitting the H-polarized photon in the L path and another PBS rotated by 90° around R axis transmitting the V-polarized photon in the R path. Then the other two cases will be reflected. To simplify the setup, we used HWP_1 to flip the polarization in the R path before using PBS_1 to transmit the desired subspace components. Instead of recovering the polarization state in the R path after PBS_1, we flipped the polariza-

tion state in the L path with HWP_2, so that the output after Schmidt projection was $\cos\theta \sin\theta(|HR\rangle_A|HR\rangle_B + |VL\rangle_A|VL\rangle_B)$. Note that HWP_1 and HWP_2 are essentially M-CNOT gates described in Section 3.1.1, where we showed that each M-CNOT gate needs a dummy HWP to compensate for the path length difference. However, in this setup, we eliminated the need for path-length compensation between the two paths by arranging HWP_1 to be R and HWP_2 to be L.

For analysis of the projected state $(|HR\rangle_A|HR\rangle_B + |VL\rangle_A|VL\rangle_B)$, we first folded the L-path output and the R-path output into a common path (D) by use of a P-CNOT gate in Figure 5-2 (a), which transformed the output of Schmidt-projection into $(|H\rangle_A|H\rangle_B + |V\rangle_A|V\rangle_B)|D\rangle_A|D\rangle_B$, where D was one of the two output paths from the P-CNOT gate. The P-CNOT gate was made of a dove prism (DP) embedded in a polarization Sagnac interferometer to rotate the incoming image (two parallel beams) by $\pm 90°$ depending on the beam polarization as shown in Figure 5-2 (b). The P-CNOT gate has the following mapping: $|HL\rangle \rightarrow |HU\rangle, |HR\rangle \rightarrow |HD\rangle, |VL\rangle \rightarrow |VD\rangle, |VR\rangle \rightarrow |VU\rangle$, where U (D) means up (down). Our P-CNOT implementation introduced a certain amount of fixed phase shifts depending on the input polarization that we compensated by adding two QWPs and a HWP at the input, as described in Section 4.3. This phase compensator was also utilized to add the necessary $\pi/2$ phase shift in our quantum state tomography measurements.

To verify that we had a maximally-entangled final state $(|\phi^+\rangle \equiv (|H\rangle_A|H\rangle_B + |V\rangle_A|V\rangle_B)/\sqrt{2})$ at the output, we recorded the coincidence counts between the measurement from Alice's polarization analyzer and Bob's polarization analyzer. Each polarization analyzer was composed of HWP_3, PBS_2, and detectors (D) as shown in Figure 5-2 (a), and the measurement basis for the polarization analyzer was set by HWP_3.

5.3 Experimental results

To show that our implementation of the SP method works, we provide various measurement results characterizing the initial state before and the output state after

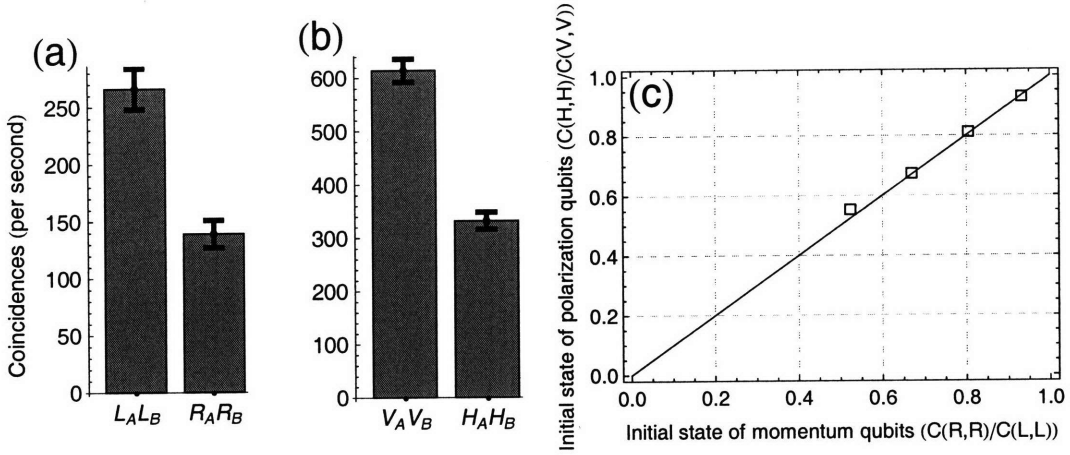

Figure 5-3: Characterization of the initial state. (a) Measured coincidences per second of $|L\rangle_s|L\rangle_i$ and $|R\rangle_s|R\rangle_i$ terms for the input state $\theta_M = 35.9°$ ($\theta_P = 45°$). (b) $|V\rangle_s|V\rangle_i$ and $|H\rangle_s|H\rangle_i$ terms for the input state $\theta_P = 35.9°$ ($\theta_M = 45°$). (c) Initial state of polarization qubits ($C(H,H)/C(V,V)$) as a function of initial state of momentum qubits ($C(R,R)/C(L,L)$). Open square shows the measurement results, and the ideal case is shown with a straight line. Photon pairs were generated by 5 mW UV pump, and the bandwidths of the detected output photons were limited to 1 nm by interference filters.

distillation. For the input state characterization, we compare the degree of entanglement in the polarization qubits (θ_P) and the momentum qubits (θ_M). For the output state, we check how close the output state is to $|\phi^+\rangle$ independent of the input states. In the experiment, we used four different input states ($\theta = 44°, 41.9°, 39.3°, 35.9°$), and the measurement results for these input states are summarized in this section.

5.3.1 Characterization of input state

To characterize the input hyper-entangled state, we utilized our capability to control θ_M and θ_P independently. To measure the distribution of $|L\rangle_A|L\rangle_B$ and $|R\rangle_A|R\rangle_B$, we set $\theta_P = 45°$ in Eq. (5.8), and applied Schmidt projection and P-CNOT operations using the same setup in Figure 5-2 (a). This produced

$$(\sin\theta_M|H\rangle_A|H\rangle_B + \cos\theta_M|V\rangle_A|V\rangle_B)|D\rangle_A|D\rangle_B/\sqrt{2}. \tag{5.12}$$

In Eq. (5.12), the polarization qubits now carry the coefficients related to θ_M which originates from the distribution of the momentum qubits. By measuring coincidences $C(H,H)$ and $C(V,V)$, we obtained the relative size of $\sin^2\theta_M$ and $\cos^2\theta_M$. $C(X,Y)$ denotes the number of detected coincidences per second between X-qubit measurement by Alice and Y-qubit measurement by Bob. Figure 5-3 (a) shows the measured distribution of the momentum qubits for $\theta = 35.9°$. Similarly, to obtain the distribution of $|H\rangle_A|H\rangle_B$ and $|V\rangle_A|V\rangle_B$, we set $\theta_M = 45°$ by choosing an appropriate PPKTP temperature. After Schmidt projection and the P-CNOT gate, this state became

$$(\cos\theta_P|H\rangle_A|H\rangle_B + \sin\theta_P|V\rangle_A|V\rangle_B)|D\rangle_A|D\rangle_B/\sqrt{2}, \tag{5.13}$$

and we measured the polarization distribution. Figure 5-3 (b) shows the distribution of the polarization qubits for the case of $\theta = 35.9°$. Note that Figure 5-3 (a) and (b) have the different scales, because the two measurements were taken at two different temperatures resulting in different output fluxes. We are only interested in the ratios $C(R,R)/C(L,L)$ and $C(H,H)/C(V,V)$ that are functions of θ_M and θ_P, respectively, and Figure 5-3 (a) and (b) show that both ratios are nearly identical, $C(R,R)/C(L,L) \simeq C(H,H)/C(V,V) \simeq 0.5$, as required by the SP protocol. We also measured the momentum qubit distribution and the polarization qubit distribution in the same way for different settings of θ, and plotted $C(H,H)/C(V,V)$ (open squares) as a function of $C(R,R)/C(L,L)$ in Figure 5-3 (c), where we see that the initial polarization states are well matched to the initial momentum states ($\theta_M \approx \theta_P$). The ideal distribution ratio is also shown in Figure 5-3 (c) as a straight line.

5.3.2 Characterization of the output state after Schmidt projection

After the distillation, we expect the resulting state is a maximally entangled state

$$|\phi^+\rangle = (|H\rangle_A|H\rangle_B + |V\rangle_A|V\rangle_B)/\sqrt{2}, \tag{5.14}$$

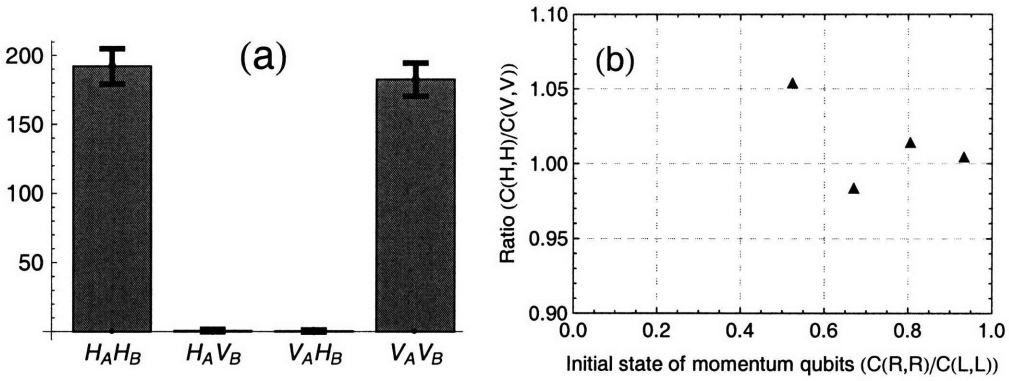

Figure 5-4: Characterization of the output state. (a) Measured coincidences per second of the four terms in Eq. (5.14) for the input state with $\theta = 35.9°$. (b) Plot of $C(H,H)/C(V,V)$ of the output state as a function of $C(R,R)/C(L,L)$ of initial momentum qubits. Photon pairs were generated by 5 mW UV pump, and the bandwidths of the detected output photons were limited to 1 nm by interference filters.

which has the same probability of detecting $|H\rangle_A|H\rangle_B$ and $|V\rangle_A|V\rangle_B$ terms, but zero probability of detecting $|H\rangle_A|V\rangle_B$ and $|V\rangle_A|H\rangle_B$ terms. Figure 5-4 (a) shows the coincidence measurement results of the output from Schmidt projection when the input state is $\theta_P \simeq \theta_M = 35.9°$. This result shows that the output state has nearly balanced $|H\rangle_A|H\rangle_B$ and $|V\rangle_A|V\rangle_B$ terms and negligible $|H\rangle_A|V\rangle_B$ and $|V\rangle_A|H\rangle_B$ terms. For other input states, the coincidence counts for $|H\rangle_A|V\rangle_B$ and $|V\rangle_A|H\rangle_B$ terms were still negligible, and in Figure 5-4 (b), we plot $C(H,H)/C(V,V)$ of the output state (solid triangles) as a function of the input states, and all the measured ratios lie close to the ideal value of unity with less than 5% error.

To show that the distilled output is indeed entangled as a coherent superposition, not as a classical mixture, of $|H\rangle_A|H\rangle_B$ and $|V\rangle_A|V\rangle_B$, we need to make other types of measurements. We performed quantum state tomography on the output state based on 16 coincidence measurements, and the real and imaginary parts of the output density matrix ρ are displayed in Figure 5-5 (a) and (b), showing clearly that the state is $|\phi^+\rangle$ with a fidelity, $\langle\phi^+|\rho|\phi^+\rangle$, of 0.952.

Another useful indicator of its coherence is two-photon quantum interference visibility measured in the diagonal basis ($|H\rangle \pm |V\rangle$). Figure 5-6 plots the measured

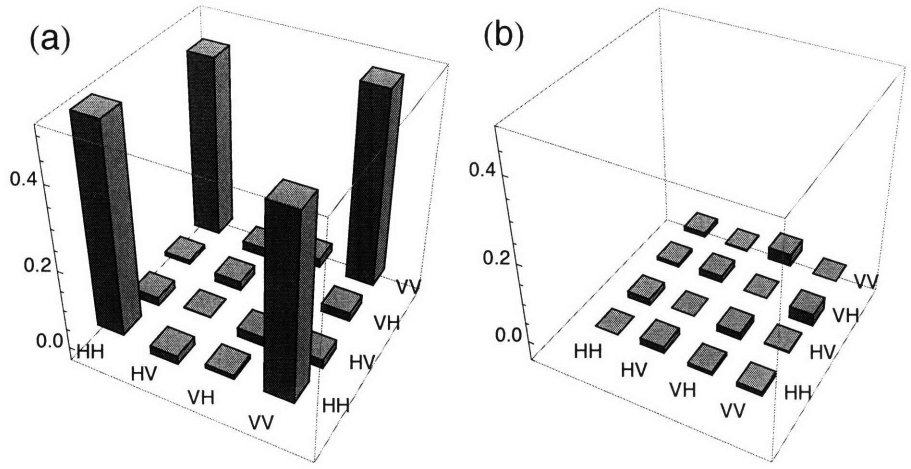

Figure 5-5: Measured density matrix of the output state after Schmidt projection is applied to the initial state with $\theta = 35.9°$. (a) Real part. (b) Imaginary part.

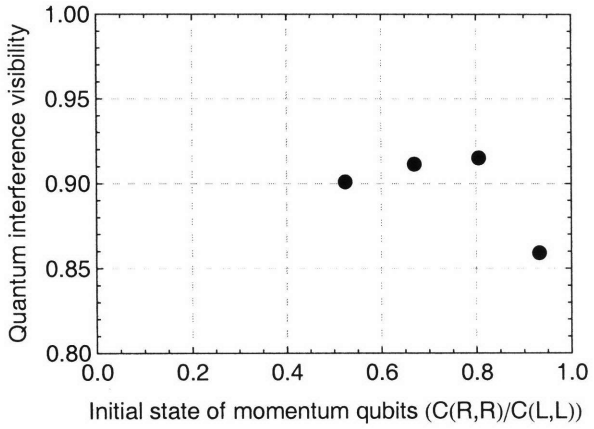

Figure 5-6: Measured quantum interference visibility in the diagonal basis ($|H\rangle \pm |V\rangle$).

visibilities for different input states, all showing ~90% visibility except one lower-visibility point that was caused by a slight misalignment of the apparatus. Part of the visibility loss comes from the imperfect P-CNOT gate that has a classical visibility of ~93% as discussed in Section 3.2.4. Another possible source of the visibility loss is the slight spectral mismatch of the output photons from the asymmetric output spatial modes. The output spectrum of the output photons was mainly governed by the IF, but due to the different spectral distribution depending on the emission angle, the output spectrum after the IF could be slightly different.

From the various measurement results shown in Figure 5-4, 5-5, and 5-6, we

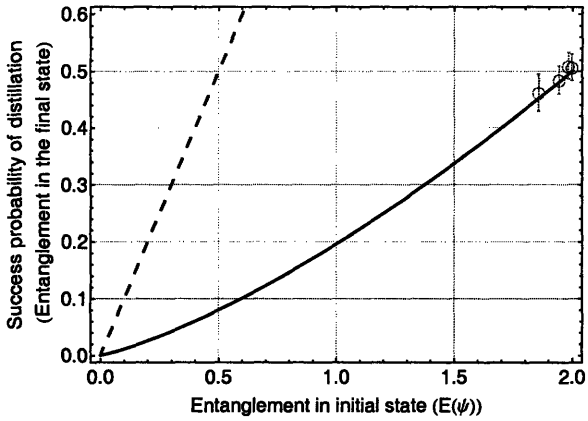

Figure 5-7: Measured efficiency of our Schmidt projection implementation. Success probability of obtaining a maximally entangled pair after Schmidt projection is applied to a pair of hyper-entangled state (or the amount of entanglement remaining in the final state) is plotted as a function of entanglement in the initial state ($E(\psi)$). Open circle is the measured probability and the solid curve is the theoretical prediction when Schmidt projection is applied to a hyper-entangled state. The dashed curve shows the maximum amount of entanglement obtainable with Schmidt projection when it is applied to infinite number of pairs.

conclude that our distillation outputs were in the $|\phi^+\rangle$ state independent of the input states.

One of the key advantages of the Schmidt-projection protocol is its high distillation efficiency, especially for a large number of initial pairs. We have measured the efficiency of our Schmidt projection implementation in terms of the success probability of obtaining distilled pairs from each hyper-entangled photon pair. The measured success probability is plotted in Figure 5-7 as open circles, which agrees well with the theoretically calculated values (solid curve). In comparison, the dashed line shows the maximum efficiency obtainable by the Schmidt projection protocol when it is applied to infinite number of input pairs. In general, Schmidt projection shows a lower yield than Procrustean methods [38, 42] when it is applied to less than 5 pairs, as in our case. However, Schmidt projection still has the advantage that it is unnecessary to adjust the distillation setup as a function of the input states.

5.4 Summary

In this chapter, we have experimentally demonstrated the Schmidt projection method which is one of the most powerful distillation protocols. To generate pairs of partially-entangled states, we used the hyper-entangled state generated by the SPCD process. We have also developed a technique to control the polarization entanglement and the momentum entanglement of the hyper-entangled photon pairs individually and used this capability to prepare the identical pairs for the initial state and also to characterize the initial state. Schmidt projection on the hyper-entangled photon pairs was realized by a PBS and two M-CNOT gates, and a P-CNOT gate was used to convert the output of SP into a polarization Bell state. Our experimental results show that Schmidt projection can distill maximally entangled states independent of the degree of entanglement in the initial state, and our distillation efficiencies agree with the theoretical prediction.

If classical communication is utilized to compare the projection results, then Schmidt projection can also be used to perform purification of certain types of mixed states, such as $\rho = \Sigma p|\psi\rangle\langle\psi| + (1-p)|01\rangle\langle 01|$, as well as a mixture of two identically decohered pairs [45]. It is also important to recognize that the key to our SP implementation is that distinct tensor products of local qubits $(|0\rangle_1|0\rangle_2, |0\rangle_1|1\rangle_2, |1\rangle_1|0\rangle_2, |1\rangle_1|1\rangle_2)$ can be encoded in physically distinguishable states $(|VL\rangle, |VR\rangle, |HL\rangle, |HR\rangle)$. Therefore the same concept can be applied to other qubit systems such as cavity quantum electrodynamics (cQED) [95, 2] or trapped ion [96] systems, where multiple qubit states can be mapped into multiple internal states within the same atom. Further studies of Schmidt-projection implementations in atoms and ions and for mixed states should enhance our expanding collection of tools in quantum information science.

Chapter 6

Complete physical simulation of the entangling-probe attack on BB84 QKD

Quantum key distribution (QKD) has been an active research area of quantum information science, since Bennett and Brassard [4] proposed their QKD protocol in 1984 (BB84), whose security is protected by the no-cloning theorem [97]. Due to its relatively simple configuration, BB84 has been implemented by many groups in free-space [47, 48, 49, 50] as well as in fiber [51, 52, 53]. Security of BB84 also has been the subject of many analyses [98, 99, 47, 100], particularly for configurations that involve non-ideal operating conditions [101, 102, 103], such as the use of weak laser pulses in lieu of single photons. However, a more fundamental question is how much information the eavesdropper (Eve) can gain under ideal BB84 operating conditions. A series of work by Fuchs and Peres [54], Slutsky *et al.* [55], and Brandt [56] show that the most powerful individual-photon attack can be accomplished with a controlled-NOT (CNOT) gate. In this scheme, Eve supplies the probe qubit to the CNOT gate, which entangles this probe qubit with the BB84 qubit that Alice is sending to Bob. Eve then makes her measurement of the probe qubit to obtain information on the shared key bit at the expense of imposing detectable errors between Alice and Bob.

Shapiro and Wong [57] showed that this Fuchs-Peres-Brandt (FPB) entangling

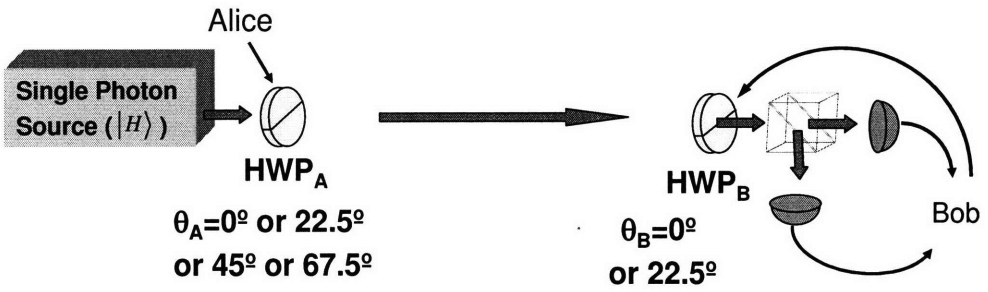

Figure 6-1: Illustration of BB84 QKD protocol. Alice randomly chooses one of the four angles (θ_A) of HWP_A for each photon. Bob also randomly chooses one of the two angles for HWP_B before he measures the single photon.

probe can be implemented in a proof-of-principle experiment, using single-photon two-qubit (SPTQ) quantum logic.

In this chapter, we present our experiment implementing the FPB entangling probe attack as a complete physical simulation including physical errors. This experiment is only a physical simulation because the two qubits of a single photon carrier must be measured jointly, so that Eve needs access to Bob's receiver, but *not* his measurement. The SPTQ probe could become a true attack if quantum non-demolition measurements in Section 6.4 were available to Eve [57].

6.1 Theoretical background

BB84 QKD protocol

In BB84 protocol, in each time interval allotted for a bit, Alice transmits a single photon in a randomly selected polarization, chosen from horizontal (H), vertical (V), +45° diagonal (D), and −45° antidiagonal (A), while Bob randomly chooses to detect photons in either the H-V or D-A bases, as shown in Figure 6-1. After the transmission is over, Alice and Bob compares their choices of polarization bases for each transmitted photon over a classical channel, and keeps the case when both used the same bases. These are the sift events, i.e., bit intervals in which Bob's count has occurred in the same basis that Alice used. An error event is a sift event in which Bob

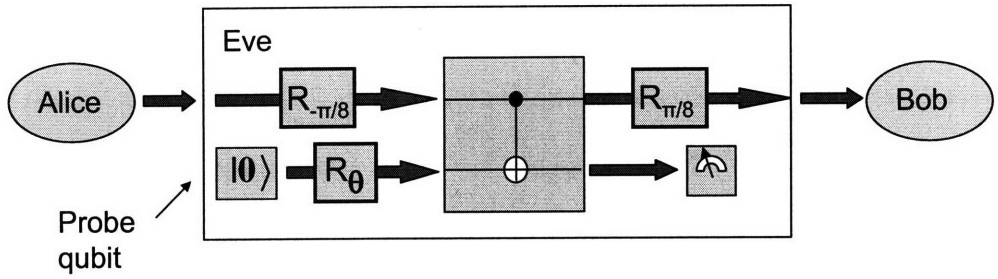

Figure 6-2: Block diagram of the Fuchs-Peres-Brandt probe for attacking BB84 QKD.

decodes the incorrect bit value. Alice and Bob employ a prescribed set of operations to identify errors in their sifted bits, correct these errors, and apply sufficient privacy amplification to deny useful key information to any potential Eve [47, 100]. At the end of the full QKD procedure, Alice and Bob have a shared one-time pad with which they can communicate in complete security.

FPB entangling-probe attack on BB84

In an individual attack on single-photon BB84 QKD, Eve probes Alice's photons one at a time. Fuchs and Peres [54] described the most general way in which an individual attack could be performed. Eve supplies a probe particle which can be any quantum object and lets it interact with Alice's photon in a unitary manner. Eve then sends Alice's photon to Bob, and performs a positive operator-valued measurement (POVM) on the probe particle she has retained. Slutsky *et al.* [55] demonstrated that the Fuchs-Peres construct, with the appropriate choice of probe state, interaction, and measurement, affords Eve the maximum amount of Rényi information about the error-free sifted bits that Bob receives for a given level of disturbance, i.e., for a given probability that a sifted bit will be received in error. Brandt [56] extended the treatment of Slutsky *et al.* by showing that the optimal probe could be realized with a single CNOT gate. Figure 6-2 shows an abstract diagram of the resulting FPB entangling probe. In the following discussion, the photon sent from Alice to Bob will be simply called the BB84 qubit, and Eve's particle or quantum object will be called the probe qubit.

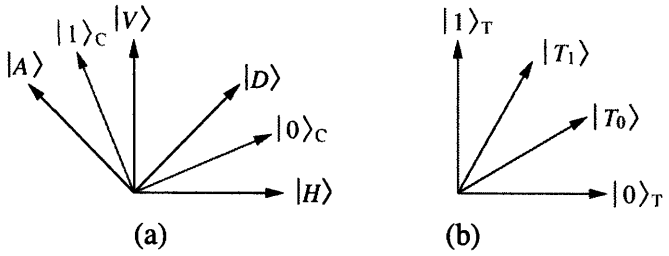

Figure 6-3: Relations between different bases. (a) Control qubit basis for Eve's CNOT gate referenced to the BB84 polarization states. (b) $|T_0\rangle$ and $|T_1\rangle$ relative to the target qubit basis for some $P_E \neq 0$.

To obtain information about the BB84 qubit, Eve needs to set up a CNOT gate whose control-qubit computational basis ($\{|0\rangle_C, |1\rangle_C\}$) is tilted by $\pi/8$ rotation from the BB84 H-V basis, as shown in Figure 6-3 (a),

$$\begin{aligned} |0\rangle_C = &\quad \cos(\pi/8)|H\rangle + \sin(\pi/8)|V\rangle\,, \\ |1\rangle_C = &\quad -\sin(\pi/8)|H\rangle + \cos(\pi/8)|V\rangle\,. \end{aligned} \tag{6.1}$$

This can be easily implemented by a H-V basis CNOT gate with basis transformation operation ($R_{\pm\pi/8}$) before and after the CNOT gate, as shown in Figure 6-2.

Having selected the error probability, P_E, that she is willing to create, Eve prepares her probe qubit (CNOT's target) in the initial state

$$|T_{\text{in}}\rangle = \{(C+S)|0\rangle_T + (C-S)|1\rangle_T\}/\sqrt{2}\,, \tag{6.2}$$

where $C = \sqrt{1-2P_E}, S = \sqrt{2P_E}$, and $\{|0\rangle_T, |1\rangle_T\}$ is the computational basis of the CNOT gate's target qubit. After the CNOT operation—with inputs from the BB84 qubit and the probe qubit—the two qubits become entangled. For each of Alice's four possible inputs, $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$, the output of the CNOT gate is

$$|H\rangle|T_{\text{in}}\rangle \rightarrow |H_{\text{out}}\rangle \equiv |H\rangle|T_0\rangle + |V\rangle|T_E\rangle\,, \tag{6.3}$$

$$|V\rangle|T_{\text{in}}\rangle \rightarrow |V_{\text{out}}\rangle \equiv |V\rangle|T_1\rangle + |H\rangle|T_E\rangle\,, \tag{6.4}$$

$$|D\rangle|T_{\text{in}}\rangle \rightarrow |D_{\text{out}}\rangle \equiv |D\rangle|T_0\rangle - |A\rangle|T_E\rangle\,, \tag{6.5}$$

$$|A\rangle|T_{\rm in}\rangle \;\rightarrow\; |A_{\rm out}\rangle \equiv |A\rangle|T_1\rangle - |D\rangle|T_E\rangle\,, \tag{6.6}$$

where the kets on the left-hand side denote the Alice $\otimes$ Eve state of the control and target qubits at the CNOT gate's input and the kets on the right-hand side denote the Bob $\otimes$ Eve state of the control and target qubits at the CNOT gate's output. The (un-normalized) output target qubit states $|T_0\rangle$, $|T_1\rangle$, and $|T_E\rangle$ are defined in the target qubit's computational basis (see Figure 6-3(b)) as:

$$|T_0\rangle \equiv \left(\frac{C}{\sqrt{2}}+\frac{S}{2}\right)|0\rangle_{\rm T}+\left(\frac{C}{\sqrt{2}}-\frac{S}{2}\right)|1\rangle_{\rm T}\,, \tag{6.7}$$

$$|T_1\rangle \equiv \left(\frac{C}{\sqrt{2}}-\frac{S}{2}\right)|0\rangle_{\rm T}+\left(\frac{C}{\sqrt{2}}+\frac{S}{2}\right)|1\rangle_{\rm T}\,, \tag{6.8}$$

$$|T_E\rangle \equiv \frac{S}{2}\left(|0\rangle_{\rm T}-|1\rangle_{\rm T}\right)\,. \tag{6.9}$$

Consider the case in which Bob measures in the same basis that Alice employed and his outcome matches what Alice sent. Then, according to Eqs. (6.3)–(6.6), the target qubit is projected into either $|T_0\rangle$ or $|T_1\rangle$. After Alice and Bob compare their basis selections over the classical channel, Eve can learn about their shared bit value by distinguishing between the $|T_0\rangle$ and $|T_1\rangle$ output states of her target qubit. To do so, she employs the minimum error probability receiver for distinguishing between $|T_0\rangle$ and $|T_1\rangle$ by performing a projective measurement along $|0\rangle_{\rm T}$ and $|1\rangle_{\rm T}$. Eve can then correlate the measurement of $|0\rangle_{\rm T}$ ($|1\rangle_{\rm T}$) with $|T_0\rangle$ ($|T_1\rangle$). Note that this projective measurement is not perfect unless $|T_0\rangle$ and $|T_1\rangle$ are orthogonal and hence coincide with the target's computational basis, $|0\rangle_{\rm T}$ and $|1\rangle_{\rm T}$.

Figure 6-4 shows the examples of the initial probe qubit state ($|T_{\rm in}\rangle$) and possible final probe qubit states ($|T_0\rangle, |T_1\rangle, |T_E\rangle$) with respect to the computational basis ($|0\rangle_T, |1\rangle_T$) of the target qubit. Figure 6-4 (a) corresponds to the case when Eve causes no error. In this case, $|T_0\rangle$ and $|T_1\rangle$ become identical and Eve cannot distinguish between these two vectors at all, as was expected. Figure 6-4 (b) shows the general situation ($0 < P_E < 1/3$), and Eve cannot get the perfect information about Bob's measurement because $|T_1\rangle$ and $|T_0\rangle$ are not orthogonal. If $P_E = 1/3$ which

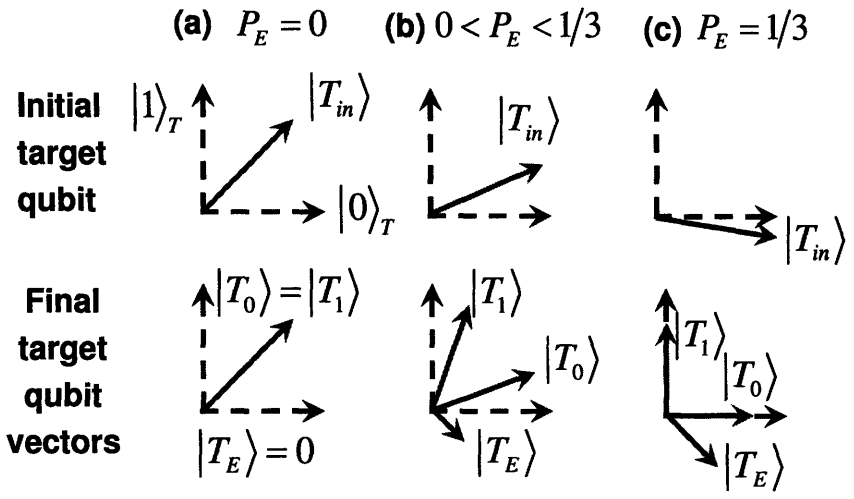

Figure 6-4: Target qubit state before and after the entangling CNOT gate for different error rate P_E. Computation bases of target qubit ($|0\rangle_T$, $|1\rangle_T$) are shown with dashed arrows for reference.

corresponds to Figure 6-4 (c), $|T_1\rangle$ and $|T_0\rangle$ become orthogonal to each other, and Eve can perfectly correlate her measurement with Bob's measurement whenever there is no error between Alice and Bob. Note that regardless of the basis that Alice and Bob choose ($H - V$ or $D - A$), Eve needs only to distinguish between $|0\rangle_T$ and $|1\rangle_T$. Therefore she can measure her probe qubit immediately, obviating the need for any quantum memory in the FPB probe attack.

Eve's information gain comes at a cost: Eve has caused an error event whenever Alice and Bob choose a common basis and Eve's probe output state is $|T_E\rangle$. When Alice sent $|H\rangle$ and Bob measured in the H–V basis, Eq. (6.3) then shows that Alice and Bob will have an error event if the measured output state is $|V\rangle|T_E\rangle$. The probability that this will occur is $\langle T_E|T_E\rangle = S^2/2 = P_E$, as shown with different lengths of $|T_E\rangle$ in Figure 6-4. For the other three cases in Eqs. (6.4)–(6.6), the error event corresponds to the last term in each expression. Therefore the conditional error probabilities are identical, and hence P_E is the unconditional error probability.

We use Rényi information to quantify Eve's information gain about the sift events because privacy amplification [100] requires an estimated upper bound for Eve's Rényi information about the corrected data [55]. Let $B = \{0, 1\}$ and $E = \{0, 1\}$ denote the

ensembles of possible bit values that Bob and Eve receive on an error-free sift event. The Rényi information (in bits) that Eve learns about each error-free sift event is

$$I_R \equiv -\log_2\left(\sum_{b=0}^{1} P^2(b)\right) + \sum_{e=0}^{1} P(e)\log_2\left(\sum_{b=0}^{1} P^2(b|e)\right), \tag{6.10}$$

where $\{P(b), P(e)\}$ are the *a priori* probabilities for Bob's and Eve's bit values, and $P(b|e)$ is the conditional probability for Bob's bit value to be b given that Eve's is e. According to Bayes' rule, $P(b|e)$ can be calculated in terms of the $P(b,e)$ which is the probability of both Bob's bit to be b and Eve's bit to be e:

$$P(b|e) = P(b,e)/\sum_{b=0}^{1} P(b,e), \tag{6.11}$$

where $P(b=0,e) = |(\langle V| \otimes {}_{\mathrm{T}}\langle e|)|V_{\mathrm{out}}\rangle|^2$ and $P(b=1,e) = |(\langle H| \otimes {}_{\mathrm{T}}\langle e|)|H_{\mathrm{out}}\rangle|^2$ in the case of the H-V basis. For the case of the $\pm 45°$ basis, $|+45°\rangle$ corresponds to $b=0$ and $|-45°\rangle$ to $b=1$. With a perfect channel and perfect equipment, this leads to the theoretical prediction [57]

$$I_R = \log_2\left(1 + \frac{4P_E(1-2P_E)}{(1-P_E)^2}\right), \tag{6.12}$$

which we plot in Figure 6-5. Under these ideal conditions, Eve's Rényi information is the same for both bases, but in actual experiments it may differ, owing to differing equipment errors in each basis.

Figure 6-5 shows some of the interesting performance points. The $I_R = 0, P_E = 0$ point in this figure happens when Eve operates her CNOT gate with $|T_{\mathrm{in}}\rangle = (|0\rangle_{\mathrm{T}} + |1\rangle_{\mathrm{T}})/\sqrt{2}$ for its target qubit input, corresponding to Figure 6-4 (a). It is well known that such an input is unaffected by and does not affect the control qubit. Thus Bob suffers no errors, as the zero-length of $|T_E\rangle$ implies, but Eve gets no Rényi information because we cannot discriminate $|T_0\rangle$ from $|T_1\rangle$. The $I_R = 1, P_E = 1/3$ point in Figure 6-5, which also corresponds to Figure 6-4 (c) case, happens when Eve operates her CNOT gate with $|T_{\mathrm{in}}\rangle = \{\left(1+\sqrt{2}\right)|0\rangle_{\mathrm{T}} + \left(1-\sqrt{2}\right)|1\rangle_{\mathrm{T}}\}/\sqrt{6}$, which leads to $|T_0\rangle \propto |0\rangle_{\mathrm{T}}$ and $|T_1\rangle \propto |1\rangle_{\mathrm{T}}$. In this case, Eve can always discriminate $|T_0\rangle$ from $|T_1\rangle$ with no errors,

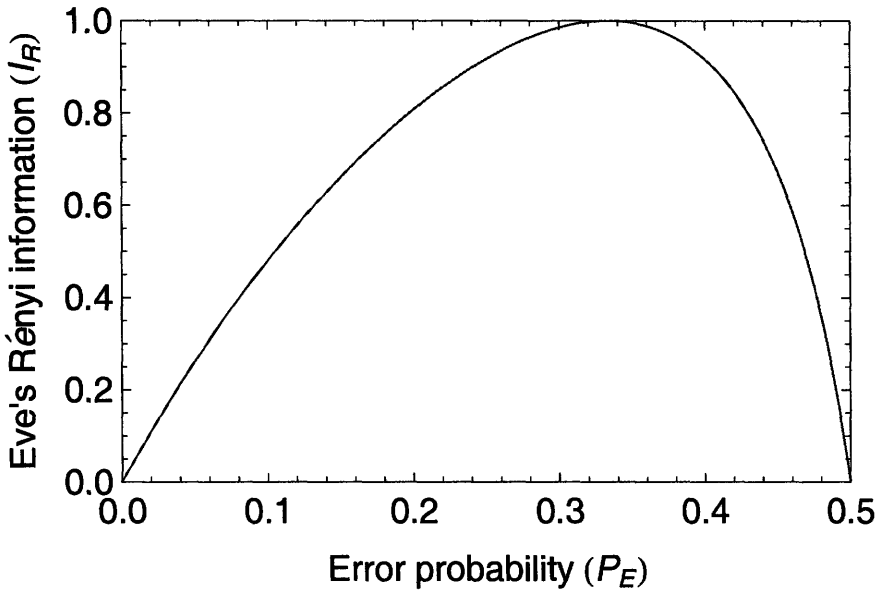

Figure 6-5: Eve's Rényi information about Bob's error-free sifted bits as a function of the error probability that her eavesdropping creates.

so she obtains the maximum (1 bit) Rényi information about each of Bob's error-free bits. The $I_R = 0, P_E = 1/2$ point corresponds to Eve's operating her CNOT gate with $|T_{\text{in}}\rangle = (|0\rangle_{\text{T}} - |1\rangle_{\text{T}})/\sqrt{2}$, which gives $|T_0\rangle = |T_1\rangle = |T_E\rangle = (|0\rangle_{\text{T}} - |1\rangle_{\text{T}})/2$. Here it is clear that Eve gains no information about Bob's error-free bits, but his error probability is 1/2 because of the action of target qubit $((|0\rangle_{\text{T}} - |1\rangle_{\text{T}})/\sqrt{2})$ on the control qubit.

6.2 Experimental setup

To simulate the entangling-probe attack shown in Figure 6-2, we need deterministic quantum logic to manipulate the two qubits, and SPTQ is an excellent candidate for this purpose. In particular, because Alice's BB84 qubit is already encoded in the polarization and it generally propagates in a single spatial mode in free space or in an optical fiber, we can immediately use its spatial mode (momentum) as the probe qubit. Figure 6-6 shows the quantum circuit diagram of our SPTQ implementation of the entangling-probe attack. One difference from Figure 6-2 is that we are using a pair of polarization-entangled photons in the singlet state for a practical reason [57].

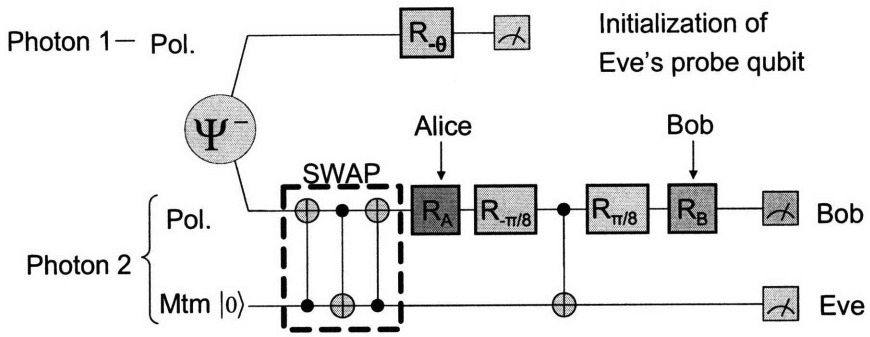

Figure 6-6: Quantum circuit diagram for the FPB-probe attack. Photon 1 of a polarization-entangled singlet-state photon pair heralds photon 2 and sets Eve's probe qubit (momentum qubit) to its initial state. The SWAP gate allows Alice's BB84 qubit to be set in the polarization mode of photon 2, whose momentum mode is Eve's probe qubit. The CNOT gate entangles Alice's qubit with Eve's qubit. $R_{-\theta}$, rotation by Eve; R_A, rotation controlled by Alice; R_B, rotation controlled by Bob; $R_{\pm\pi/8}$, rotation by angle $\pm\pi/8$.

Photon 1 of the singlet-state photon pair serves two purposes. It is obvious that it is used as a trigger to herald photon 2 as a single-photon pulse for the BB84 protocol. Another purpose is to remotely initialize the momentum qubit in the following way: A SWAP operation applied to photon 2 exchanges its polarization and momentum qubits so that the polarization of photon 1 and the momentum of photon 2 are now entangled in a singlet state. Eve can then encode her probe qubit in the momentum state of photon 2 by projecting photon 1 along an appropriate polarization state set by a polarization rotation $R_{-\theta}$. The polarization state of photon 2 after the SWAP gate can be used for Alice's BB84 qubit, which is set by rotation R_A, as usual with the BB84 protocol. Similarly, Bob's polarization analysis of the BB84 qubit is set by R_B. Therefore the quantum circuit in Figure 6-6 produces the same result as in Figure 6-2. In this configuration, Eve is heralding the photon on which Alice is encoding polarization. However, an equivalent experiment could be performed if Alice polarization-encoded a single-photon source, after which Eve imposed her momentum qubit by a single qubit operation on the momentum qubit using a SWAP gate, as described in Section 3.1.3.

The CNOT gate that Eve employs in Figure 6-6 is a polarization-controlled NOT

(P-CNOT) gate that uses the polarization qubit as the control and the momentum qubit of the same photon as the target (Section 3.1.2). The SWAP gate is composed of one P-CNOT gate sandwiched by two momentum-controlled NOT (M-CNOT) gates as described in Section 3.1.3.

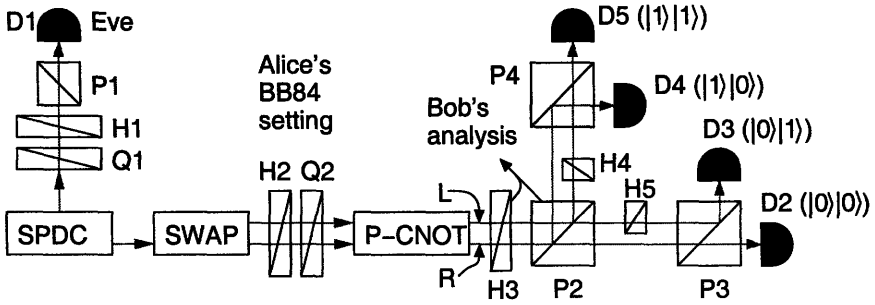

Figure 6-7: Experimental configuration for a complete physical simulation of the FPB attack on BB84. SPDC, spontaneous parametric down-conversion source; H, half-wave plate; Q, quarter-wave plate; P, polarizing beam splitter; D, single-photon detector. R, L refer to spatial paths.

Figure 6-7 shows our experimental setup for implementing the quantum circuit given in Figure 6-6. We used the singlet output state at $\sim$ 810 nm generated from the polarization-entangled photon pair source using a periodically poled $KTiOPO_4$ (PPKTP) crystal, described in Section 2.4. This source was pumped by a continuous-wave laser with 4.9 mW power and $\lambda_p = 404.757$ nm. The output bandwidth was limited to 1 nm by interference filters, and the collimated output beam had a beam waist of $w_0 = 0.53$ mm. In a collimated configuration, the momentum state of a photon is the same as the spatial orientation of the beam, for which we use the right-left (R–L) basis and we aligned the output path of photon 2 to match the R input path of the SWAP gate as shown in Figure 6-7. This is equivalent to setting the momentum qubit to $|0\rangle$ in Figure 6-6 under the mapping of R (L) to $|0\rangle$ ($|1\rangle$). The centers of the L and R beams were separated by $\sim$2 mm.

To align this output with respect to the SWAP gate and the subsequent CNOT gate, we first overlapped this output with a classical laser with the same wavelength and the same beam waist at a far distance using a single-photon counter for detection. Then we used the classical interference to align the SWAP gate and the CNOT gate

along the center path of those gates. Finally we shifted the classical beam by ~1 mm to the right while the classical interference at the output of CNOT gate was monitored.

For each photon pair, photon 1 is used to herald the arrival of photon 2 and also to remotely control the momentum qubit of photon 2 by postselection. The $R_{-\theta}$ polarization rotation by Eve was implemented using a quarter-wave plate (QWP) Q1 and a half-wave plate (HWP) H1, followed by a polarizing beam splitter (PBS) P1 and a single-photon detector (D1). In principle, Eq. (6.2) requires only the polarization rotation without any phase shift, and therefore we need only H1. However, Q1 was added to compensate for an intrinsic phase shift ξ imposed by the SWAP gate on the target-qubit basis $\{|0\rangle_T, |1\rangle_T\}$, as explained in Section 3.1.3. We have independently measured $\xi \simeq 88°$ during the alignment procedure using classical laser light. Therefore, the $R_{-\theta}$ operation prepared the momentum qubit in $|T'_{in}\rangle$ with an extra phase shift ξ

$$|T'_{in}\rangle \equiv \cos\theta_{in}|0\rangle_T + e^{i\xi}\sin\theta_{in}|1\rangle_T\,. \tag{6.13}$$

The extra but opposite phase shift of the SWAP gate would bring Eve's probe qubit to be in $|T_{in}\rangle$ of Eq. (6.2).

After the SWAP gate, R_A and $R_{-\pi/8}$ were combined in a single operation. The P-CNOT gate had the same phase shift problem as the SWAP gate, so we used a HWP (H2) and a QWP (Q2) to compensate for this phase shift and to impose the required rotation. After H2 and Q2, the BB84 qubit becomes

$$|\Psi_A\rangle \equiv \cos\theta_A|0\rangle_C + e^{i\chi}\sin\theta_A|1\rangle_C, \tag{6.14}$$

where χ ($\simeq 98°$) is the compensating phase shift and θ_A, which is the sum of Alice's angle and $-22.5°$, is $-22.5°, 22.5°, 67.5°$, or $112.5°$ for $|H\rangle, |D\rangle, |V\rangle$ or $|A\rangle$, respectively, as shown in Figure 6-3(a). Similarly we combined $R_{\pi/8}$ and R_B into a single HWP (H3) in Figure 6-7 and a PBS (P2) was used by Bob to analyze the polarization of the BB84 qubit.

Eve measured her qubit by a projective measurement along the $|0\rangle_T$–$|1\rangle_T$ (spatially, *R*–*L*) basis. A HWP (H4/H5) was placed in the *R* or *L* beam path, as indicated

Alice	P_E	Coincidence $\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|0\rangle$	Estimated $\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|0\rangle$
	0	1356	1836	23408	23356	0.027	0.037	0.469	0.468
$\|D\rangle = \|0\rangle$	0.1	2840	4220	9664	32592	0.058	0.086	0.196	0.661
	0.33	7512	9496	1512	30916	0.152	0.192	0.031	0.625
	0	22664	23388	1140	1112	0.469	0.484	0.024	0.023
$\|A\rangle = \|1\rangle$	0.1	8480	34492	4088	2052	0.173	0.702	0.083	0.042
	0.33	1096	32360	9384	6564	0.022	0.655	0.19	0.133

Alice	P_E	Expected $\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$	$\|0\rangle\|1\rangle$	$\|0\rangle\|0\rangle$
	0	0	0	0.500	0.500
$\|D\rangle = \|0\rangle$	0.1	0.050	0.050	0.167	0.733
	0.33	0.167	0.167	0	0.667
	0	0.500	0.500	0	0
$\|A\rangle = \|1\rangle$	0.1	0.167	0.733	0.050	0.050
	0.33	0	0.667	0.167	0.167

Table 6.1: Data samples, estimated probabilities, and theoretical values for D and A inputs with Bob using the same basis as Alice, and for predicted error probabilities $P_E = 0, 0.1$, and 0.33. $|0\rangle|1\rangle$ corresponds to Bob's measuring $|D\rangle$ and Eve's measuring $|1\rangle_{\mathrm{T}}$. Column 1 shows the state Alice sent and column 2 shows the predicted error probability P_E. "Coincidence" columns show coincidence counts over a 40-s interval. "Estimated" columns show the measured coincidence counts normalized by the total counts of all four detectors, and "Expected" shows the theoretical values under ideal operating conditions.

in Figure 6-7, so that the R and L beams would be distinguished by their orthogonal polarizations. This polarization tagging simplified their measurements by a PBS (P3/P4) and single-photon detectors. The four detectors uniquely identified the two qubits of photon 2. D2, D3, D4, D5 correspond to $|H\rangle|R\rangle$, $|H\rangle|L\rangle$, $|V\rangle|R\rangle$, $|V\rangle|L\rangle$ ($|D\rangle|R\rangle$, $|D\rangle|L\rangle$, $|A\rangle|R\rangle$, $|A\rangle|L\rangle$), respectively, when the H–V (D–A) basis is chosen. Therefore, in our physical simulation, these joint measurement yield Bob's polarization information and Eve's momentum information.

6.3 Measurement results

In data collection, we measured coincidences between D1 and one of the detectors for photon 2. Table 6.1 shows two data sets for Alice's input of D and A polarizations

and compares with the expected values for the ideal case. The estimated probabilities are calculated based on the measured coincidence counts, and we can see that these estimated probabilities are close to the theoretical values. From the raw data, we calculate the Rényi information I_R based on Eq. (6.10), and Figure 6-8 plots I_R as a function of the error probability P_E. The solid curve is the theoretically allowed maximum I_R which is the same curve as that in Figure 6-5. At the beginning of the experiment, we were not aware of the intrinsic phase shift problem in the SWAP gate and the CNOT gate. Therefore we took the data *without* the phase shift compensation, which is plotted in Figure 6-8 (a). Figure 6-8 (b) shows the data with the proper compensation. Diamonds (triangles) in Figure 6-8 represent I_R for the measured values with inputs in the H–V (D–A) basis. The comparison of those two plots immediately shows that the phase shift compensation was very important to obtaining the correct results. We note that accidental coincidences were negligible and the coincidence window was $\sim$3 ns.

In the ideal case, when $P_E = 0$, Eve gets no information ($I_R = 0$), and Alice and Bob have no error bits. However, due to experimental errors such as imperfect gate fidelities, we found that $\sim$5% of the sifted bits had errors. For $P_E = 1/3$, Eve obtains perfect information, $I_R = 1$ under ideal conditions, but in our experiment, Eve gained a maximum $I_R = 0.9$, corresponding to her having 95% probability of correctly receiving one of Alice and Bob's error-free sifted bits.

Error analysis

To understand the errors involved in the experiment, we model our experimental setup with some non-ideal parameters. We assume that estimation of the phases ξ in Eq. (6.13) and χ in Eq. (6.14) could be inaccurate, and similarly for the setting of θ_A in Eq. (6.14) that might be caused by the wave plates. We also model the unitary

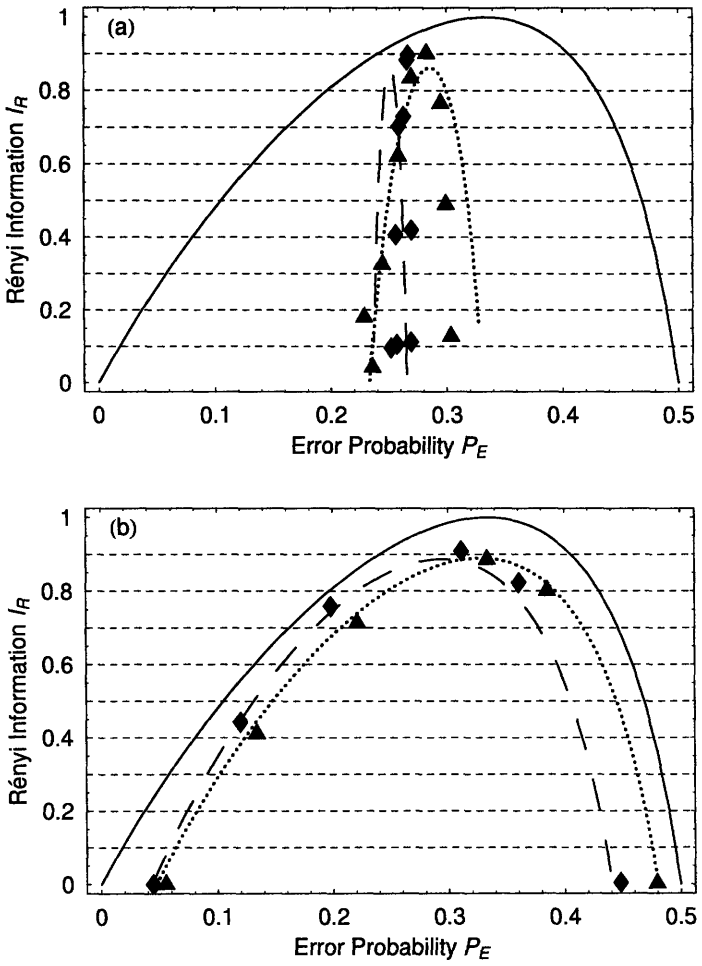

Figure 6-8: Eve's Rényi information I_R about Bob's error-free sifted bits versus the error probability P_E that her eavesdropping creates (a) without phase shift compensation and (b) with phase shift compensation. Solid curve: theoretical result. Diamonds (triangles): measured values for H-V (D-A) basis. Dashed (dotted) curves are fits to the data for H-V (D-A) basis.

P-CNOT gate as

$$\begin{pmatrix} \cos\alpha & ie^{-i\delta}\sin\alpha & 0 & 0 \\ ie^{i\delta}\sin\alpha & \cos\alpha & 0 & 0 \\ 0 & 0 & -ie^{i\delta}\sin\alpha & \cos\alpha \\ 0 & 0 & \cos\alpha & -ie^{-i\delta}\sin\alpha \end{pmatrix}, \tag{6.15}$$

where $\alpha = 0$ and $\delta = 0$ for an ideal P-CNOT gate. Finally we assume that Bob's HWP (H3) setting of θ_B was imperfect, so that

$$|H\rangle \rightarrow \cos\theta_B|0\rangle_C - \sin\theta_B|1\rangle_C\,, \tag{6.16}$$

$$|V\rangle \rightarrow \sin\theta_B|0\rangle_C + \cos\theta_B|1\rangle_C\,, \tag{6.17}$$

where θ_B should equal 22.5° (−22.5°) in the H–V (D–A) basis.

We fit the data by minimizing the differences between 96 measurements and the calculated numbers based on this error model. The fitting results were $\Delta\xi \simeq 3°$, $\Delta\chi \simeq -11°$, $\Delta\theta_A(H,D,V,A) = \{3.2°, 0.9°, -0.7°, -2.3°\}$, $\alpha = 12.3°$, $\delta = 3.6°$, $\Delta\theta_B(H/V, D/A) = \{-1.8°, 0°\}$. As expected, the phase errors are relatively small and those associated with θ_A and θ_B are within the resolution of the rotating mounts housing the wave plates. The non-zero α also agrees with the measured classical visibility of 94% for the P-CNOT gate. Figure 6-8 (b) shows the fitted I_R based on this model for the H–V basis (dashed curve) and the D–A basis (dotted curve).

6.4 Real attack with quantum non-demolition measurement

The SPTQ scheme used in this chapter is limited to a physical simulation mainly due to the requirement of a joint measurement between Eve and Bob. However, this can be turned into a real attack with quantum non-demolition measurement (QND), as shown by Shapiro and Wong [57]. As shown in the Appendix of Ref. [57], it is

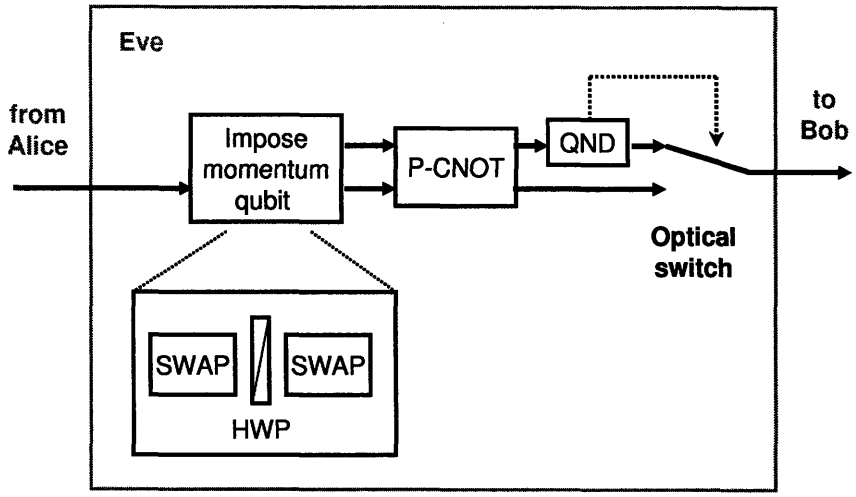

Figure 6-9: Deterministic entangling-probe attack on polarization-based BB84 protocol that can be realized with polarization-preserving QND measurement and SPTQ quantum logic.

possible, in principle, to use cross-phase modulation between a strong coherent-state probe beam and an arbitrarily polarized signal beam to make a QND measurement of the signal beam's total photon number while preserving its polarization state. Cross-phase modulation QND measurement of photon number is not currently available, but once it is developed, we can easily realize a real attack with SPTQ as shown in Figure 6-9.

Here, Eve imposes a momentum qubit on Alice's polarization-encoded photon using single momentum-qubit operation made of two SWAP gates and wave plates, as discussed in Section 3.1.3. Then she can entangle polarization and momentum qubit using a P-CNOT operation, and measure the momentum qubit with the polarization-preserving QND measurement device. Depending on the QND measurement result, we can couple the outgoing photon using an optical switch, and Bob will only see a photon in a single spatial mode. Therefore the entangling-probe attack will be completely transparent to Alice and Bob, except for the increased amount of errors between them.

6.5 Summary

In this chapter, we have experimentally demonstrated the first complete physical simulation of the entangling-probe attack using SPTQ quantum logic. This is, to our knowledge, the first experiment on attacking the BB84 protocol, and the results are in good agreement with theoretical predictions. Our result shows that Eve can gain Rényi information up to 0.9 under realistic operating conditions, including a CNOT gate that does not have an ultrahigh fidelity. Our results suggest the possible amount of information gain by Eve with current technology and evaluate the minimum level of privacy amplification required for a given level of error. Implementation of the entangling-probe attack using SPTQ quantum logic can be turned into a real attack once the polarization-preserving QND measurement device becomes available.

Chapter 7

Conclusion

For the past two decades, quantum information science research has shown that application of quantum mechanics to computer science and information theory can provide us with enormous gains compared to classical computation and classical communication. However, before we can combine various ideas in quantum information processing (QIP) to build a realistic large-scale system, we need to demonstrate individual QIP tasks to verify the concepts and identify potential challenges in their practical implementations. In this thesis, I have used a photonic system combined with single-photon two-qubit (SPTQ) quantum logic as a platform to demonstrate a number of QIP tasks, benefiting from the ease of preparation and manipulation of various photonic states and from the long coherence time associated with photons. With SPTQ quantum logic, we can implement deterministic quantum operations that are useful for QIP. However, SPTQ quantum logic is not scalable because of a significant increase in the complexity of the optical setup as the number of qubits increases. This scalability limitation is acceptable for few-qubit operations and for photons that are initially entangled in one or more degrees of freedom. Therefore in addition to the demonstration of QIP tasks using SPTQ quantum logic, this thesis also focuses on entanglement source development to evaluate its effects on QIP implementations.

For efficient implementation of SPTQ quantum logic, I have developed a high-flux, high-visibility source of polarization-entangled photons based on spontaneous parametric down conversion (SPDC) using a polarization Sagnac interferometer (PSI).

Polarization entanglement was obtained by coherently combining the collinear outputs from the bidirectionally-pumped type-II phase-matched PPKTP crystal, and the PSI geometry was utilized to generate phase-stable output states and to increase the entanglement quality. With this polarization-entangled photon pair source, I have achieved a two-photon quantum-interference visibility of more than 99.4%, with a measured flux of ~700 pairs/s within 1-nm bandwidth per mW of pump power, which is one of the highest values measured with polarization-entangled photon pairs [28, 29]. The Sagnac source served as a reliable workhorse for various experiments performed in this thesis. Since we introduced the PSI-type polarization entangled photon pair source [28], the same type of systems have also been replicated by several groups including two recent published results [66, 72]. The collinear SPDC geometry of this system implies that it can incorporate a cavity structure [73] to generate narrowband outputs to enhance the spectral brightness and it can be applied to integrated optical sources. A similar type of system can also be applied to a type-I phase-matched PPKTP crystal where we can utilize the higher nonlinear coefficient d_{33} to further increase the flux and efficiency.

I have also developed a hyper-entanglment source which generates pairs of photons that are entangled in polarization and momentum simultaneously. The hyper-entangled state is generated by utilizing the intrinsic momentum entanglement included in the non-collinear outputs from the PSI-based polarization-entangled photon pair source. Our hyper-entangled photon pair source has a unique feature that its polarization entanglement and momentum entanglement can be easily and independently controlled by the polarization of the pump beam and the temperature of the PPKTP crystal, respectively. The generation of the maximally hyper-entangled state was verified by implementing complete polarization Bell state measurements with SPTQ quantum logic based on phase-stable polarization-controlled NOT (P-CNOT) gate developed in our group [17]. Our polarization Bell state measurements had a ~5% error which is less than a half of the errors incurred by other groups in their Bell state measurements [37, 36], suggesting that our SPTQ quantum logic platform is well built and robust in operation. The hyper-entangled state can find several

applications such as super-dense coding [108], enhanced QKD systems [87], demonstration of All-Versus-Nothing violation of local reality [77, 15, 16], and other types of applications where more than one type of entanglement may be used to improve performance. It is possible to utilize our hyper-entangled source to use more than two momentum paths, thus allowing a single photon to carry more than the two qubits we have used in this thesis and therefore to further increase the dimension of the useful Hilbert space.

The single-photon two-qubit (SPTQ) quantum logic based on the phase-stable P-CNOT gate enabled us to demonstrate various QIP tasks. Phase-stable quantum SWAP gate was constructed by combining two momentum-controlled NOT (M-CNOT) gates and one P-CNOT gate. As an application, we applied the SWAP gate to transfer entanglement initially stored in the momentum qubits of two photons to the polarization qubits of the same photon pair, and thus we indirectly confirmed that the non-collinear SPDC outputs are entangled in their momentum [31]. Because it is so much easier to perform single-qubit operation in the polarization space, the SWAP operation can be used to implement phase-stable single-qubit operations in the momentum space.

SPTQ quantum logic was also applied to partially hyper-entangled photon pairs to distill the maximally entangled state using the Schmidt projection method. The resulting polarization-entangled state showed two-photon quantum-interference visibility of ~90% independent of the input degree of entanglement. This is the first demonstration of the Schmidt projection protocol whose distillation efficiency can approach unity when applied to a large number of input pairs simultaneously. The concept of physical mapping used in this demonstration can, in principle, be applied to other physical systems such as atomic qubits or ionic qubits.

Finally, we have used SPTQ quantum logic and the polarization entangled photon pair source to implement a physical simulation of the entangling-probe attack on the BB84 quantum key distribution (QKD) [57]. Fuchs-Peres-Brandt (FPB) entangling-probe attack is the most powerful individual attack on BB84 QKD and the theoretical upper-bound on the potential leakage of secret key information under this attack is

well known. Through this simulation, I demonstrated that, using real quantum devices with realistic fidelity, the eavesdropper can gain nearly the expected amount of information about the secret key for a given level of induced error between the two parties involved in the BB84 QKD protocol [58]. This attack can become a real attack once a polarization-preserving QND measurement device becomes available, and therefore our measurement result provides a realistic upper-bound on the potential information gained by an eavesdropper.

In summary, I have conducted a number of quantum information processing experiments using single-photon two-qubit quantum logic and a high-flux, high-visibility entanglement source. The highly stable polarization Sagnac interferometric source enabled the generation of adjustable hyper-entangled photons that were utilized throughout the many experiments in this thesis. More significantly, I have shown convincingly that the phase-stable implementation of single-photon two-qubit quantum logic is robust and can serve as a versatile and flexible platform for studying and physically simulating few-qubit quantum algorithms and protocols. I believe that further development of the single-photon two-qubit platform encompassing additional qubits would be very useful in the exciting field of quantum information science.

Appendix A

Quantization of field inside a nonlinear crystal

Quantization of the electromagnetic (EM) fields inside a nonlinear crystal generally requires slightly different choice of canonical variables than the regular field quantization used in quantum electrodynamics (QED), as pointed out by Hillery and Mlodinow [104] and many other authors [105, 106]. However for our purpose, traditional field quantization with the modified wave vector with the refractive index works well, and I will use this approach [107].

In this appendix, operators are denoted by hat ($\hat{O}$) and vectors are shown in the bold face ($\mathbf{k}$). When an individual component is considered, it is written in normal face (k_x). $\mathbf{k}^{\perp}$ means the transverse components (y, z) of the $\mathbf{k}$ vector.

In the interaction picture, the effective Hamiltonian $\hat{H}$ for the optical parametric process in a nonlinear crystal is

$$\hat{H} = \epsilon_0 \int_V d^3r \chi^{(2)}_{ijk} \hat{E}^{(+)}_{p,i} \hat{E}^{(-)}_{s,j} \hat{E}^{(-)}_{i,k} + H.c., \tag{A.1}$$

where V is the volume of the crystal, $\chi^{(2)}_{ijk}$ is the second-order nonlinear susceptibility tensor, and $H.c.$ means Hermitian conjugate. The three field operators is

$$\hat{\mathbf{E}}_p^{(+)} = \int \frac{d^3k_p}{(2\pi)^{3/2}} \sum_{s_p} \left(\frac{\hbar\omega(\mathbf{k}_p)}{2\epsilon_0 n_{\mathbf{k}_p s_p}} \right)^{1/2} \varepsilon_{\mathbf{k}_p s_p} \hat{a}_{\mathbf{k}_p s_p} e^{i(\mathbf{k}_p \cdot \mathbf{r} - \omega(\mathbf{k}_p)t)} \tag{A.2}$$

$$\hat{\mathbf{E}}_s^{(-)} = \int \frac{d^3k_s}{(2\pi)^{3/2}} \sum_{s_s} \left(\frac{\hbar\omega(\mathbf{k}_s)}{2\epsilon_0 n_{\mathbf{k}_s s_s}} \right)^{1/2} \varepsilon_{\mathbf{k}_s s_s} \hat{a}^\dagger_{\mathbf{k}_s s_s} e^{-i(\mathbf{k}_s \cdot \mathbf{r} - \omega(\mathbf{k}_s)t)} \tag{A.3}$$

$$\hat{\mathbf{E}}_i^{(-)} = \int \frac{d^3k_i}{(2\pi)^{3/2}} \sum_{s_i} \left(\frac{\hbar\omega(\mathbf{k}_i)}{2\epsilon_0 n_{\mathbf{k}_i s_i}} \right)^{1/2} \varepsilon_{\mathbf{k}_i s_i} \hat{a}^\dagger_{\mathbf{k}_i s_i} e^{-i(\mathbf{k}_i \cdot \mathbf{r} - \omega(\mathbf{k}_i)t)}, \tag{A.4}$$

where $\mathbf{k}$ is the wave vector of a plane wave, s is an index for two possible polarization vectors, $\hbar$ is the Planck's constant, ϵ_0 is the permittivity of free space, $n_{\mathbf{k}s}$ is the index of refraction which is generally a function of $\mathbf{k}$ and s, ω is the frequency of the plane wave, $\varepsilon_{\mathbf{k}s}$ is the polarization vector, and $\hat{a}^\dagger_{\mathbf{k}s}$ is a creation operator for a photon in the plane wave with wave vector $\mathbf{k}$ and polarization vector $\varepsilon_{\mathbf{k}s}$.

In general, $\chi^{(2)}_{ijk}$ is a tensor, and we have to consider all its non-zero components and the corresponding polarization components of the $\hat{\mathbf{E}}$ field operators. However in our experiment, we are pumping a crystal using a narrowband cw laser with a definite polarization, and therefore it will primarily excite only a limited set of output modes and the Hamiltonian simplifies to

$$\hat{H} = \epsilon_0 \int_V d^3r \chi^{(2)} \hat{E}_p^{(+)} \hat{E}_s^{(-)} \hat{E}_i^{(-)} + H.c., \tag{A.5}$$

and vector field operators given in equations (A.2)-(A.4) can be simplified to

$$\hat{E}_p^{(+)} = \int \frac{d^3k_p}{(2\pi)^{3/2}} C(\mathbf{k}_p) \hat{a}_{\mathbf{k}_p} e^{i(\mathbf{k}_p \cdot \mathbf{r} - \omega(\mathbf{k}_p)t)} \tag{A.6}$$

$$\hat{E}_s^{(-)} = \int \frac{d^3k_s}{(2\pi)^{3/2}} C(\mathbf{k}_s) \hat{a}^\dagger_{\mathbf{k}_s} e^{-i(\mathbf{k}_s \cdot \mathbf{r} - \omega(\mathbf{k}_s)t)} \tag{A.7}$$

$$\hat{E}_i^{(-)} = \int \frac{d^3k_i}{(2\pi)^{3/2}} C(\mathbf{k}_i) \hat{a}^\dagger_{\mathbf{k}_i} e^{-i(\mathbf{k}_i \cdot \mathbf{r} - \omega(\mathbf{k}_i)t)}, \tag{A.8}$$

where $C(\mathbf{k})$ is defined to be $\left(\frac{\hbar\omega(\mathbf{k})}{2\epsilon_0 n_{\mathbf{k}}}\right)^{1/2}$. Our nonlinear crystal is periodically poled along the x-axis for quasi-phase matching and this effect can be included in the Hamiltonian by using periodic square function for $\chi^{(2)}(\mathbf{r})$ with a period of Λ. Then

we can expand $\chi^{(2)}(\mathbf{r})$ in terms of a Fourier series as

$$\chi^{(2)} = \chi_2 f(\mathbf{r}) = \chi_2 \sum_{m=0}^{\infty} f_m e^{-im\mathbf{K}_\Lambda \cdot \mathbf{r}}, \tag{A.9}$$

where $\mathbf{K}_\Lambda = \frac{2\pi}{\Lambda}\mathbf{e}_x$ is a reciprocal vector of period. Except for the DC term, either $f_{\pm 1}$ is the largest term, and considering our operating condition, we can approximate $\chi^{(2)}(\mathbf{r})$ by $\chi_2 f_1 e^{-i\mathbf{K}_\Lambda \cdot \mathbf{r}}$.

The evolution of the quantum state is given by

$$|\psi\rangle = \exp\left[\frac{1}{i\hbar}\int_0^T dt\hat{H}(t)\right]|\psi_0\rangle \approx \left[1 + \frac{1}{i\hbar}\int_0^T dt\hat{H}(t)\right]|\psi_0\rangle, \tag{A.10}$$

where $|\psi_0\rangle$ is the initial state, and T is the interaction time, which effectively becomes infinite due to the long coherence time of the monochromatic pump.

By inserting the simplified electric field operators (A.6) - (A.8) into the Hamiltonian (A.5), the time integral of the Hamiltonian in state evolution Eq. (A.10) can be simplified to

$$\begin{aligned}\int_{-\infty}^{\infty} dt\hat{H}(t) = \; & \frac{\chi_2 f_1}{(2\pi)^{9/2}} \int d^3k_p \, d^3k_s \, d^3k_i \, C(\mathbf{k}_p)C(\mathbf{k}_s)C(\mathbf{k}_i)\hat{a}_{\mathbf{k}_p}\hat{a}^\dagger_{\mathbf{k}_s}\hat{a}^\dagger_{\mathbf{k}_i} \\ & \times \int_{-\infty}^{\infty} dt e^{-i(\omega_p - \omega_s - \omega_i)t} \int_V d^3r \, e^{i\Delta\mathbf{k}\cdot\mathbf{r}} + H.c.,\end{aligned} \tag{A.11}$$

where $\Delta\mathbf{k} = \mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i - \mathbf{K}_\Lambda$. The time integral of $e^{-i(\omega_p - \omega_s - \omega_i)t}$ leads to $2\pi\delta(\omega_p - \omega_s - \omega_i)$ which implies energy conservation. To calculate the volume integral $\int_V d^3r$, we use the Cartesian coordinates $\int_{-L_x/2}^{L_x/2} dx \int_{-L_y/2}^{L_y/2} dy \int_{-L_z/2}^{L_z/2} dz$, where the pump beam is propagating along the x-axis. Then in paraxial approximation, the size of the beam in the transverse plane (yz-plane) is generally smaller than the transverse dimension of the crystal (L_y, L_z), and we can extend the transverse domain of integration to ∞. Then

$$\int_{-L_x/2}^{L_x/2} dx \int_{-\infty}^{\infty} dy \int_{-\infty}^{\infty} dz \, e^{i\Delta\mathbf{k}\cdot\mathbf{r}} = (2\pi)^2 L_x \mathrm{sinc}(\Delta k_x L_x/2)\delta(\Delta k_y)\delta(\Delta k_z), \tag{A.12}$$

and Eq. (A.11) becomes

$$\begin{aligned}\int_{-\infty}^{\infty} dt\hat{H}(t) = \; & \frac{\chi_2 f_1 L_x}{(2\pi)^{3/2}} \int_{\mathbf{k}_p^{\perp}=\mathbf{k}_s^{\perp}+\mathbf{k}_i^{\perp}} dk_{p,x}\, d^3k_s\, d^3k_i\, C(\mathbf{k}_p)C(\mathbf{k}_s)C(\mathbf{k}_i) \\ & \times \mathrm{sinc}(\Delta k_x L_x/2)\delta(\omega_p - \omega_s - \omega_i)\hat{a}_{\mathbf{k}_p}\hat{a}^{\dagger}_{\mathbf{k}_s}\hat{a}^{\dagger}_{\mathbf{k}_i} + H.c.,\end{aligned} \tag{A.13}$$

where $\mathbf{k}^{\perp}$ means the transverse components (y, z) of $\mathbf{k}$.

The initial state $|\psi_0\rangle$ is a cw pump laser propagating along x-axis with a TEM_{00} (Gaussian) spatial mode given by

$$u_G(\mathbf{r}, k, b) \equiv \frac{-ik}{2\pi}\frac{1}{x - ib}\exp\left[ik\left(x + \frac{y^2+z^2}{2(x-ib)}\right)\right], \tag{A.14}$$

where b is the confocal parameter and related to the beam waist w_0 by $b = \pi w_0^2/\lambda$, λ is the wavelength inside the crystal, and k is the magnitude of wave vector propagating inside the crystal. To represent this coherent state (laser) quantum mechanically, we need to define a creation operator $\hat{a}^{\dagger}_G$ for a single photon in a Gaussian mode by

$$\hat{a}^{\dagger}_G(k, b) \equiv \int d^3r\, u_G(\mathbf{r}, k, b)\hat{a}^{\dagger}(\mathbf{r}), \tag{A.15}$$

where $\hat{a}^{\dagger}(\mathbf{r}) \equiv \frac{1}{(2\pi)^{3/2}}\int d^3k\, e^{i\mathbf{k}\cdot\mathbf{r}}\hat{a}^{\dagger}_{\mathbf{k}}$ is an inverse Fourier transform of $\hat{a}^{\dagger}_{\mathbf{k}}$. Then

$$\hat{a}^{\dagger}_G(k, b) = \int d^3k\hat{a}^{\dagger}_{\mathbf{k}}\frac{1}{(2\pi)^{3/2}}\int d^3r\, e^{i\mathbf{k}\cdot\mathbf{r}}u_G(\mathbf{r}, k, b) \equiv \int d^3k U^*_G(\mathbf{k}, k, b)\hat{a}^{\dagger}_{\mathbf{k}}, \tag{A.16}$$

where $U^*_G(\mathbf{k}, k, b)$ is a Fourier transform of $u_G(\mathbf{r}, k, b)$, and can be calculated from Eq. (A.14)

$$U^*_G(\mathbf{k}, k, b) = \frac{1}{(2\pi)^{1/2}}\exp\left[-\frac{b}{2k}(k_y^2 + k_z^2)\right]\delta\left(k_x - \left(k - \frac{k_y^2+k_z^2}{2k}\right)\right). \tag{A.17}$$

By using $\hat{a}^{\dagger}_G(k, b)$, the initial state can be written as

$$|\psi_0\rangle = \sum_{n=0}^{\infty}\frac{e^{-|A_p|^2/2}}{n!}\left(A_p\hat{a}^{\dagger}_G(k, b)\right)^n|0\rangle, \tag{A.18}$$

where A_p is proportional to the amplitude of the electric field of the pump laser. From

the following relations between $\hat{a}_G^\dagger(k,b)$ and $\hat{a}_{\mathbf{k}'}$,

$$\left[\hat{a}_{\mathbf{k}'}, \hat{a}_G^\dagger(k,b)\right] = \int d^3k\, U_G^*(\mathbf{k},k,b)\left[\hat{a}_{\mathbf{k}'}, \hat{a}_{\mathbf{k}}^\dagger\right] = U_G^*(\mathbf{k}',k,b) \tag{A.19}$$

$$\hat{a}_{\mathbf{k}}\left(A_p\hat{a}_G^\dagger(k,b)\right)^n|0\rangle = nA_pU_G^*(\mathbf{k},k,b)\left(A_p\hat{a}_G^\dagger(k,b)\right)^{n-1}|0\rangle, \tag{A.20}$$

we can show that the initial state $|\psi_0\rangle$ is an eigenstate of the annihilation operator $\hat{a}_{\mathbf{k}}$ with eigenvalue $A_pU_G^*(\mathbf{k},k,b)$, as follows:

$$\hat{a}_{\mathbf{k}}|\psi_0\rangle = \sum_{n=0}^{\infty}\frac{e^{-|A_p|^2/2}}{n!}nA_pU_G^*(\mathbf{k},k,b)\left(A_p\hat{a}_G^\dagger(k,b)\right)^{n-1}|0\rangle = A_pU_G^*(\mathbf{k},k,b)|\psi_0\rangle. \tag{A.21}$$

Inserting the simplified Hamiltonian (A.13) and the initial state (A.18) into the state evolution (A.10), and use the relation in Eq. (A.21), the output state $|\psi\rangle$ becomes

$$\begin{aligned}|\psi\rangle = |\psi_0\rangle + \; & \frac{\chi_2 f_1 L_x A_p}{i\hbar(2\pi)^2}\int d^3k_s\, d^3k_i\, C(\mathbf{k}_p)C(\mathbf{k}_s)C(\mathbf{k}_i)\exp\left[-\frac{b}{2k}\left(k_{p,y}^2+k_{p,z}^2\right)\right] \\ & \times\mathrm{sinc}(\Delta k_x L_x/2)\delta(\omega_p-\omega_s-\omega_i)\hat{a}_{\mathbf{k}_s}^\dagger\hat{a}_{\mathbf{k}_i}^\dagger|\psi_0\rangle,\end{aligned} \tag{A.22}$$

where the pump wave vector $\mathbf{k}_p$ sets the transverse components $(\hat{y},\hat{z})$ of the signal and the idler wave vectors $(\mathbf{k}_s^\perp,\mathbf{k}_i^\perp)$ by $\mathbf{k}_p^\perp = \mathbf{k}_s^\perp + \mathbf{k}_i^\perp$ and $k_{p,x} = k - |\mathbf{k}_p^\perp|^2/2k$ which are required by the δ-functions used during the calculation. The first term in Eq. (A.22) is just the pump laser with no pair generation, but the second term shows that a pair of photons (signal and idler) is generated by the nonlinear process in addition to the coherent pump state. In the experiment, the pump beam is separated from the signal and the idler by dichroic mirrors, so we are mainly interested in the distribution of $\mathbf{k}_s$ and $\mathbf{k}_i$, which is dictated by the constraint inside the integral.

In the experiment, we select the output based on the frequency rather than the x-component of the wave vector $\mathbf{k}$, so it is more useful to rewrite Eq. (A.22) in terms of the integral over frequency rather than k_x. Using the relation between k_x and ω

$(k_x^2 = n^2\omega^2/c^2 - k_y^2 - k_z^2)$, we can convert the integration variable from k_x to ω:

$$\int dk_x = \int \frac{dk_x}{d\omega} d\omega = \int d\omega \left(\frac{n}{c}\right)^2 \frac{\omega}{k_x}. \tag{A.23}$$

Replacing k_x variables with ω using (A.23) and redefining $C(\mathbf{k}^\perp, \omega) = \left(\frac{n}{c}\right)^2 \frac{\omega}{k_x} C(\mathbf{k})$, we can reach the following output state after removing the pump,

$$\begin{aligned} |\psi\rangle = \; & \frac{\chi_2 f_1 L_x A_p}{i\hbar(2\pi)^2} \int d\omega_s \int d^2k_s^\perp \int d^2k_i^\perp \, C(\mathbf{k}_p) C(\mathbf{k}_s^\perp, \omega_s) C(\mathbf{k}_i^\perp, \omega_i) \\ & \times \exp\left[-\frac{w_0^2}{4}\left(k_{p,y}^2 + k_{p,z}^2\right)\right] \mathrm{sinc}(\Delta k_x L_x/2) \hat{a}_{\mathbf{k}_s}^\dagger \hat{a}_{\mathbf{k}_i}^\dagger |0\rangle, \end{aligned} \tag{A.24}$$

where $\omega_i = \omega_p - \omega_s$ from the δ-function, $\mathbf{k}_p^\perp = \mathbf{k}_s^\perp + \mathbf{k}_i^\perp$, $k_{p,x} = k - |\mathbf{k}_p^\perp|^2/2k$, $k_x = \pm\sqrt{n^2\omega^2/c^2 - k_y^2 - k_z^2}$ for the signal and the idler, $\Delta k_x = k_{x,p} - k_{x,s} - k_{x,i} - 2\pi/\Lambda$, and w_0 is the pump beam waist.

In Eq. (A.24), the effective domain of integration is determined by the sinc function and the Gaussian function, and within this domain, $C(\mathbf{k}_p), C(\mathbf{k}_s^\perp, \omega_s), C(\mathbf{k}_i^\perp, \omega_i)$ remain almost constant. In the main chapters, the discussion of the momentum distribution of the output photons is based on this equation.

Appendix B

Numerical calculation

In this appendix, we describe how to calculate the numerical results related to spontaneous parametric downconversion (SPDC) presented in Figure 2-2 and Figure 2-5. The relation between the crystal temperature and the peak center wavelength of signal shown in Figure 2-2 can be easily obtained by solving the longitudinal phase-matching condition. The angular distribution of output idler flux for a given temperature in Figure 2-5 can be calculated by integrating the two-photon probability for all possible signal output modes.

To calculate the longitudinal phase mismatch given by $\Delta k_x = k_{x,p} - k_{x,s} - k_{x,i} - 2\pi/\Lambda$, we need to know the x-components of the wave vectors which depend on the refractive index (n) in the propagating direction and the transverse components of the wave vector by the relation $k_x = \pm\sqrt{n^2\omega^2/c^2 - k_y^2 - k_z^2}$. Sellmeier equation provides the refractive indices for three fundamental axes (n_x, n_y, n_z), and we can find a formula for refractive index for a specific propagation direction as given by Ref. [110]. With this formula and simple dispersion relations, we can express k_x in terms of k_y, k_z, three refractive indices (n_x, n_y, n_z), and frequency (ω) as shown in

the following formula:

$$
\begin{aligned}
&v_1 \equiv \left(\frac{c}{n_x}\right), v_2 \equiv \left(\frac{c}{n_y}\right), v_3 \equiv \left(\frac{c}{n_z}\right), \\
&A \equiv v_2^2 v_3^2, \\
&B \equiv -\omega^2(v_1^2+v_3^2) + k_y^2(v_1^2+v_2^2)v_3^2 + k_z^2(v_1^2+v_3^2)v_2^2, \\
&C \equiv \omega^4 - \omega^2\{k_y^2(v_1^2+v_3^2) + k_z^2(v_1^2+v_2^2)\} + (k_y^2+k_z^2)(k_y^2 v_1^2 v_3^2 + k_z^2 v_1^2 v_2^2), \\
&k_x = \left(\frac{-B \pm \sqrt{B^2-4AC}}{2A}\right)^{1/2},
\end{aligned}
\tag{B.1}
$$

where the + (−) sign gives k_x for the signal (idler). Note that refractive index depends on the frequency and the temperature, and we used the temperature dependence of Sellmeier equation given by Ref. [109]. With Eq. (B.1), we can express Δk_x as a function of the transverse momentum vectors ($\mathbf{k}_s^\perp$, $\mathbf{k}_i^\perp$), pump frequency (ω_p), signal frequency (ω_s) and temperature (T) as shown in Eq. (2.4). Then we can calculate the relation between the crystal temperature and the peak center wavelength of signal by solving the equation $\Delta k_x(\mathbf{k}_s^\perp, \mathbf{k}_i^\perp, \omega_p, \omega_s, T) = 0$ with $\mathbf{k}_s^\perp = \mathbf{k}_i^\perp = \mathbf{0}^\perp$ and the fixed pump wavelength ($\lambda = 404.775$ nm), and the result is shown in Figure 2-2.

The calculation for the angular distribution of the idler flux is based on the following two-photon probability amplitude given by Eq. (A.24) with the assumption of constant $C(\mathbf{k}_p), C(\mathbf{k}_s^\perp, \omega_s)$, and $C(\mathbf{k}_i^\perp, \omega_i)$:

$$
|\psi\rangle_{s,i} \sim L_x A_p \int d\omega_s \int d^2k_s^\perp \int d^2k_i^\perp \exp\left[-\frac{w_0^2}{4}\left(k_{p,y}^2 + k_{p,z}^2\right)\right] \mathrm{sinc}(\Delta k_x L_x/2) \hat{a}_{\mathbf{k}_s}^\dagger \hat{a}_{\mathbf{k}_i}^\dagger |0\rangle, \tag{B.2}
$$

where L_x is the length of the crystal, A_p is proportional to the amplitude of the pump electric field, $\int d^2k^\perp$ means integration in the transverse plane (yz-plane), the transverse component of the pump wave vector ($\mathbf{k}_p$) is $\mathbf{k}_p^\perp = \mathbf{k}_s^\perp + \mathbf{k}_i^\perp$, the x-component of the pump wave vector is $k_{p,x} = k - |\mathbf{k}_p^\perp|^2/2k$, the x-components of the signal and idler wave vectors ($\mathbf{k}_s, \mathbf{k}_i$) are $k_x = \pm\sqrt{n^2\omega^2/c^2 - k_y^2 - k_z^2}$, $\Delta k_x = k_{x,p} - k_{x,s} - k_{x,i} - 2\pi/\Lambda$, and Λ is the crystal's grating period. To calculate the generation probability for some given idler mode, we need to consider all the possible signal modes with which the given idler mode can have non-zero probability

amplitude. Therefore for each transverse momentum for idler ($\mathbf{k}_i^{\perp}$), we integrated the two-photon probability $\left|\exp\left[-\frac{w_0^2}{4}\left(k_{p,y}^2+k_{p,z}^2\right)\right]\mathrm{sinc}(\Delta k_x L_x/2)\right|^2$ over all the possible transverse momentum modes of signal ($\mathbf{k}_s^{\perp}$). Note that this procedure is equivalent to calculating a partial trace of a density matrix formed by $|\psi\rangle_{s,i}$ over the signal modes. For each transverse momentum mode of idler, we calculated this generation probability for different idler wavelengths, and summed them up with proper weighting factors to reflect the interference filter effect. Figure 2-5 shows these computational results compared to the experimental measurements. We noticed that there is a constant offset between the calculation and the measurement. This offset mainly comes from the fact that the temperature dependence we adopted for our calculation [109] was measured in different wavelength range than ours.

Appendix C

Quantum state tomography

In Section 2.3.3, we described that we can find a linear relations between each real and imaginary component of ρ and the coincidence measurements (M) of Alice and Bob. In this appendix, we will show that 16 coincidence measurement combinations between Alice and Bob are enough to find all independent components of ρ by expressing each M in terms of components of ρ. We assume that Alice and Bob will choose one of the four polarization measurement bases $\{|H\rangle, |V\rangle, |D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}, |R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}\}$. Then as shown in Section 2.3.3, when Alice measures H polarization and Bob measures D polarization, the measured coincidences M_{HD} is proportional to

$$\begin{aligned}
&\langle HD|\rho|HD\rangle = \langle H|\tfrac{1}{\sqrt{2}}\left(\langle H| + \langle V|\right)\rho|H\rangle\tfrac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right) \\
&= \tfrac{1}{2}\left(\langle HH|\rho|HH\rangle + \langle HH|\rho|HV\rangle + \langle HV|\rho|HH\rangle + \langle HV|\rho|HV\rangle\right) \\
&= \tfrac{1}{2}\left(\langle HH|\rho|HH\rangle + 2\mathrm{Re}(\langle HH|\rho|HV\rangle) + \langle HV|\rho|HV\rangle\right) .
\end{aligned}$$

If we repeat this type of calculation for other combinations, we can find the following relations:

$$\begin{aligned}
M_{HH} &\propto \mathrm{Re}(\langle HH|\rho|HH\rangle), \\
M_{HV} &\propto \mathrm{Re}(\langle HV|\rho|HV\rangle), \\
M_{VH} &\propto \mathrm{Re}(\langle VH|\rho|VH\rangle), \\
M_{VV} &\propto \mathrm{Re}(\langle VV|\rho|VV\rangle),
\end{aligned}$$

$$
\begin{aligned}
M_{HD} \propto\ & 1/2(\mathrm{Re}(\langle HH|\rho|HH\rangle) + 2\mathrm{Re}(\langle HH|\rho|HV\rangle) + \mathrm{Re}(\langle HV|\rho|HV\rangle))\,, \\
M_{HR} \propto\ & 1/2(2\mathrm{Im}(\langle HH|\rho|HV\rangle) + \mathrm{Re}(\langle HH|\rho|HH\rangle) + \mathrm{Re}(\langle HV|\rho|HV\rangle))\,, \\
M_{VD} \propto\ & 1/2(\mathrm{Re}(\langle VH|\rho|VH\rangle) + 2\mathrm{Re}(\langle VH|\rho|VV\rangle) + \mathrm{Re}(\langle VV|\rho|VV\rangle))\,, \\
M_{VR} \propto\ & 1/2(2\mathrm{Im}(\langle VH|\rho|VV\rangle) + \mathrm{Re}(\langle VH|\rho|VH\rangle) + \mathrm{Re}(\langle VV|\rho|VV\rangle))\,, \\
M_{DH} \propto\ & 1/2(\mathrm{Re}(\langle HH|\rho|HH\rangle) + 2\mathrm{Re}(\langle HH|\rho|VH\rangle) + \mathrm{Re}(\langle VH|\rho|VH\rangle))\,, \\
M_{RH} \propto\ & 1/2(2\mathrm{Im}(\langle HH|\rho|VH\rangle) + \mathrm{Re}(\langle HH|\rho|HH\rangle) + \mathrm{Re}(\langle VH|\rho|VH\rangle))\,, \\
M_{DV} \propto\ & 1/2(\mathrm{Re}(\langle HV|\rho|HV\rangle) + 2\mathrm{Re}(\langle HV|\rho|VV\rangle) + \mathrm{Re}(\langle VV|\rho|VV\rangle))\,, \\
M_{RV} \propto\ & 1/2(2\mathrm{Im}(\langle HV|\rho|VV\rangle) + \mathrm{Re}(\langle HV|\rho|HV\rangle) + \mathrm{Re}(\langle VV|\rho|VV\rangle))\,, \\
M_{DR} \propto\ & 1/4(2\mathrm{Im}(\langle HH|\rho|HV\rangle) + 2\mathrm{Im}(\langle HH|\rho|VV\rangle) - 2\mathrm{Im}(\langle HV|\rho|VH\rangle)\,, \\
& +2\mathrm{Im}(\langle VH|\rho|VV\rangle) + \mathrm{Re}(\langle HH|\rho|HH\rangle) + 2\mathrm{Re}(\langle HH|\rho|VH\rangle) \\
& +\mathrm{Re}(\langle HV|\rho|HV\rangle) + 2\mathrm{Re}(\langle HV|\rho|VV\rangle) + \mathrm{Re}(\langle VH|\rho|VH\rangle) + \mathrm{Re}(\langle VV|\rho|VV\rangle))\,, \\
M_{RD} \propto\ & 1/4(2\mathrm{Im}(\langle HH|\rho|VH\rangle) + 2\mathrm{Im}(\langle HH|\rho|VV\rangle) + 2\mathrm{Im}(\langle HV|\rho|VH\rangle) \\
& +2\mathrm{Im}(\langle HV|\rho|VV\rangle) + \mathrm{Re}(\langle HH|\rho|HH\rangle) + 2\mathrm{Re}(\langle HH|\rho|HV\rangle) \\
& +\mathrm{Re}(\langle HV|\rho|HV\rangle) + 2\mathrm{Re}(\langle VH|\rho|VH\rangle) + \mathrm{Re}(\langle VH|\rho|VV\rangle) + \mathrm{Re}(\langle VV|\rho|VV\rangle))\,, \\
M_{RR} \propto\ & 1/4(2\mathrm{Im}(\langle HH|\rho|HV\rangle) + 2\mathrm{Im}(\langle HH|\rho|VH\rangle) + 2\mathrm{Im}(\langle HV|\rho|VV\rangle) \\
& +2\mathrm{Im}(\langle VH|\rho|VV\rangle) + \mathrm{Re}(\langle HH|\rho|HH\rangle) - 2\mathrm{Re}(\langle HH|\rho|VV\rangle) \\
& +\mathrm{Re}(\langle HV|\rho|HV\rangle) + 2\mathrm{Re}(\langle HV|\rho|VH\rangle) + \mathrm{Re}(\langle VH|\rho|VH\rangle) + \mathrm{Re}(\langle VV|\rho|VV\rangle))\,, \\
M_{DD} \propto\ & 1/4(\mathrm{Re}(\langle HH|\rho|HH\rangle) + 2\mathrm{Re}(\langle HH|\rho|HV\rangle) + 2\mathrm{Re}(\langle HH|\rho|VH\rangle) \\
& +2\mathrm{Re}(\langle HH|\rho|VV\rangle) + \mathrm{Re}(\langle HV|\rho|HV\rangle) + 2\mathrm{Re}(\langle HV|\rho|VH\rangle) \\
& +2\mathrm{Re}(\langle HV|\rho|VV\rangle) + \mathrm{Re}(\langle VH|\rho|VH\rangle) + 2\mathrm{Re}(\langle VH|\rho|VV\rangle) + \mathrm{Re}(\langle VV|\rho|VV\rangle))\,.
\end{aligned}
$$

If we solve the above relations in terms of each component of the density matrix ρ, then we can get the following relations:

$$
\begin{aligned}
& \mathrm{Re}(\langle HH|\rho|HH\rangle) \propto M_{HH}\,, \\
& \mathrm{Re}(\langle HV|\rho|HV\rangle) \propto M_{HV}\,, \\
& \mathrm{Re}(\langle VH|\rho|VH\rangle) \propto M_{VH}\,, \\
& \mathrm{Re}(\langle VV|\rho|VV\rangle) \propto M_{VV}\,, \\
& \mathrm{Re}(\langle HH|\rho|HV\rangle) \propto 1/2(2M_{HD} - M_{HH} - M_{HV})\,, \\
& \mathrm{Re}(\langle HH|\rho|HV\rangle) \propto 1/2(2M_{HD} - M_{HH} - M_{HV})\,,
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{Im}(\langle HH|\rho|HV\rangle) \propto\ & 1/2(-M_{HH}+2M_{HR}-M_{HV})\,,\\
\mathrm{Re}(\langle VH|\rho|VV\rangle) \propto\ & 1/2(2M_{VD}-M_{VH}-M_{VV})\,,\\
\mathrm{Im}(\langle VH|\rho|VV\rangle) \propto\ & 1/2(-M_{VH}+2M_{VR}-M_{VV})\,,\\
\mathrm{Re}(\langle HH|\rho|VH\rangle) \propto\ & 1/2(2M_{DH}-M_{HH}-M_{VH})\,,\\
\mathrm{Im}(\langle HH|\rho|VH\rangle) \propto\ & 1/2(-M_{HH}+2M_{RH}-M_{VH})\,,\\
\mathrm{Re}(\langle HV|\rho|VV\rangle) \propto\ & 1/2(2M_{DV}-M_{HV}-M_{VV})\,,\\
\mathrm{Im}(\langle HV|\rho|VV\rangle) \propto\ & 1/2(-M_{HV}+2M_{RV}-M_{VV})\,,\\
\mathrm{Re}(\langle HV|\rho|VH\rangle) \propto\ & 1/2(2M_{DD}-M_{DH}-M_{DV}-M_{HD}+M_{HH}-M_{HR}\\
& +M_{HV}-M_{RH}+2M_{RR}-M_{RV}-M_{VD}+M_{VH}-M_{VR}+M_{VV})\,,\\
\mathrm{Im}(\langle HV|\rho|VH\rangle) \propto\ & 1/2(M_{DH}-2M_{DR}+M_{DV}-M_{HD}+M_{HR}+2M_{RD}\\
& -M_{RH}-M_{RV}-M_{VD}+M_{VR})\,,\\
\mathrm{Re}(\langle HH|\rho|VV\rangle) \propto\ & 1/2(2M_{DD}-M_{DH}-M_{DV}-M_{HD}+M_{HR}+M_{RH}\\
& -2M_{RR}+M_{RV}-M_{VD}+M_{VR})\,,\\
\mathrm{Im}(\langle HH|\rho|VV\rangle) \propto\ & 1/2(-M_{DH}+2M_{DR}-M_{DV}-M_{HD}+M_{HH}-M_{HR}\\
& +M_{HV}+2M_{RD}-M_{RH}-M_{RV}-M_{VD}+M_{VH}-M_{VR}+M_{VV})\,.
\end{aligned}
$$

We used these relations to find the density matrix with normalization condition of $\mathrm{tr}(\rho)$=1.

Bibliography

[1] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, Quantum State Transfer and Entanglement Distribution among Distant Nodes in a Quantum Network. *Phys. Rev. Lett.* **78,** 3221-3224 (1997).

[2] S. Lloyd, M. S. Shahriar, J. H. Shapiro, and P. R. Hemmer, Long Distance, Unconditional Teleportation of Atomic States via Complete Bell State Measurements. *Phys. Rev. Lett.* **87,** 167903 (2001).

[3] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414,** 413-418 (2001).

[4] C.H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, 1984* (IEEE, New York, 1984) pp. 175-179.

[5] G. J. Milburn, Quantum optical Fredkin gate. *Phys. Rev. Lett.* **62,** 2124-2127 (1989).

[6] I. L. Chuang and Y. Yamamoto, Simple quantum computer. *Phys. Rev. A* **52,** 3489-3496 (1995).

[7] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Measurement of Conditional Phase Shifts for Quantum Logic. *Phys. Rev. Lett.* **75,** 4710-4713 (1995).

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

[9] E. Knill, Quantum gates using linear optics and postselection. *Phys. Rev. A* **66,** 052306 (2002).

[10] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn, Simple scheme for efficient linear optics quantum gates. *Phys. Rev. A* **65,** 012314 (2001).

[11] XuBo Zou, K. Pahlke, and W. Mathis, Teleportation implementation of nondeterministic quantum logic operations by using linear optical elements. *Phys. Rev. A* **65,** 064305 (2002).

[12] N. J. Cerf, C. Adami, and P. G. Kwiat, Optical simulation of quantum logic. *Phys. Rev. A* **57,** R1477-R1480 (1998).

[13] B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Universal unitary gate for single-photon two-qubit states. *Phys. Rev. A* **63,** 032303 (2001).

[14] Y.-H. Kim, Single-photon two-qubit entangled states: Preparation and measurement. *Phys. Rev. A* **67,** 040301 (2003).

[15] C. Cinelli, M. Barbieri, R. Perris, P. Mataloni, and F. De Martini, All-Versus-Nothing Nonlocality Test of Quantum Mechanics by Two-Photon Hyperentanglement. *Phys. Rev. Lett.* **95,** 240405 (2005).

[16] T. Yang *et al.*, All-Versus-Nothing Violation of Local Realism by Two-Photon, Four-Dimensional Entanglement. *Phys. Rev. Lett.* **95,** 240406 (2005).

[17] M. Fiorentino and F. N. C. Wong, Deterministic Controlled-NOT Gate For Single-Photon Two-Qubit Quantum Logic. *Phys. Rev. Lett.* **93,** 070502 (2004).

[18] M. Lamehi-Rachti and W. Mittig, Quantum mechanics and hidden variables: A test of Bell's inequality by the measurement of the spin correlation in low-energy proton-proton scattering. *Phys. Rev. D* **14,** 2543-2555 (1976).

[19] A. R. Wilson, J. Lowe, and D. K. Butt, Measurement of the relative planes of polarization of annihilation quanta as a function of separation distance. *J. Phys. G: Nucl. Phys.* **2,** 613-624 (1976).

[20] A. Aspect, P. Grangier, and G. Roger, Experimental Tests of Realistic Local Theories via Bell's Theorem. *Phys. Rev. Lett.* **47,** 460-463 (1981).

[21] J. S. Bell, On the Einstein Podolsky Rosen Paradox. *Physics* **1,** 195-200 (1964).

[22] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **47,** 777-780 (1935).

[23] Y. H. Shih and C. O. Alley, New Type of Einstein-Podolsky-Rosen-Bohm Experiment Using Pairs of Light Quanta Produced by Optical Parametric Down Conversion. *Phys. Rev. Lett.* **61,** 2921-2924 (1988).

[24] P. G. Kwiat *et al.* New High-Intensity Source of Polarization-Entangled Photon Pairs. *Phys. Rev. Lett.* **75,** 4337-4341 (1995).

[25] P. G. Kwiat it et al. Ultrabright source of polarization-entangled photons. *Phys. Rev. A* **60,** R773-R776 (1999).

[26] C. E. Kuklewicz *et al.* High-flux source of polarization-entangled photons from a periodically poled $KTiOPO_4$ parametric down-converter. *Phys. Rev. A* **69,** 013807 (2004).

[27] M. Fiorentino *et al.* Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints. *Phys. Rev. A* **69,** 041801 (2004).

[28] T. Kim, M. Fiorentino, and F. N. C. Wong, Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. *Phys. Rev. A* **73,** 012316 (2006).

[29] F. N. C. Wong, J. H. Shapiro, and T. Kim, Efficient Generation of Polarization-Entangled Photons in a Nonlinear Crystal. *Laser Physics* **16,** 1517-1524 (2006).

[30] J. G. Rarity and P. R. Tapster, Experimental violation of Bell's inequality based on phase and momentum. *Phys. Rev. Lett.* **64,** 2495-2498 (1990).

[31] M. Fiorentino, T. Kim, and F. N. C. Wong, Single-photon two-qubit SWAP gate for entanglement manipulation. *Phys. Rev. A* **72,** 012318 (2005).

[32] P. G. Kwiat, Hyper-entangled states. *J. Mod. Opt.* **44,** 2173-2184 (1997).

[33] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Generation of Hyperentangled Photon Pairs. *Phys. Rev. Lett.* **95,** 260501 (2005).

[34] M. Barbieri, C. Cinelli, P. Mataloni, and F. De Martini, Polarization-momentum hyperentangled states: Realization and characterization. *Phys. Rev. A* **72,** 052110 (2005).

[35] S. P. Walborn, S. Pádua, and C. H. Monken, Hyperentanglement-assisted Bell-state analysis. *Phys. Rev. A* **68,** 042313 (2003).

[36] C. Schuck, G. Huber, C. Kurtsiefer, and H. Weinfurter, Complete Deterministic Linear Optics Bell State Analysis. *Phys. Rev. Lett.* **96,** 190501 (2006).

[37] M. Barbieri, G. Vallone, P. Mataloni, and F. De Martini, Complete and deterministic discrimination of polarization Bell states assisted by momentum entanglement. *Phys. Rev. A* **75,** 042317 (2007).

[38] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations. *Phys. Rev. A* **53,** 2046-2052 (1996).

[39] R. T. Thew, and W. J. Munro, Entanglement manipulation and concentration. *Phys. Rev. A* **63,** 030302 (2001).

[40] W. Xiang-bin, and F. Heng, Entanglement concentration by ordinary linear optical devices without postselection. *Phys. Rev. A* **68,** 060302 (2003).

[41] M. J. Hwang, and Y. H. Kim, Practical scheme for non-postselection entanglement concentration using linear optical elements. *Phys. Lett. A* **369,** 280-284 (2007).

[42] P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, and N. Gisin, Experimental entanglement distillation and 'hidden' non-locality. *Nature* **409,** 1014-1017 (2001).

[43] T. Yamamoto, M. Koashi, and N. Imoto, Concentration and purification scheme for two partially entangled photon pairs. *Phys. Rev. A* **64,** 012304 (2001).

[44] Z. Zhao, J.-W. Pan, and M. S. Zhan, Practical scheme for entanglement concentration. *Phys. Rev. A* **64,** 014301 (2001).

[45] T. Yamamoto, M. Koashi, S. Özdemir, and N. Imoto, Experimental extraction of an entangled photon pair from two identically decohered pairs. *Nature* **421,** 343-346 (2003).

[46] Z. Zhao, T. Yang, Y. A. Chen, A. N. Zhang, and J. W. Pan, Experimental Realization of Entanglement Concentration and a Quantum Repeater. *Phys. Rev. Lett.* **90,** 207901 (2003).

[47] C. H. Bennett *et al.*, Experimental quantum cryptography. *J. Cryptology* **5,** 3-28 (1992).

[48] B. C. Jacobs and J. D. Franson, Quantum cryptography in free space. *Opt. Lett.* **21,** 1854-1856 (1996).

[49] W. T. Buttler *et al.*, Daylight Quantum Key Distribution over 1.6 km. *Phys. Rev. Lett.* **84,** 5652-5655 (2000).

[50] C. Kurtsiefer *et al.*, Quantum cryptography: A step towards global key distribution. *Nature* **419,** 450 (2002).

[51] J. D. Franson and H. Ilves, Quantum cryptography using optical fibers. *Appl. Opt.* **33,** 2949-2954 (1994).

[52] C. Marand and P. D. Townsend, Quantum key distribution over distances as long as 30 km. *Opt. Lett.* **20,** 1695-1697 (1995).

[53] R. J. Hughes, G. L. Morgan, C. G. Peterson, Quantum key distribution over a 48km optical fibre network. *J. Mod. Opt.* **47,** 533-547 (2000).

[54] C. A. Fuchs and A. Peres, Quantum-state disturbance versus information gain: Uncertainty relations for quantum information. *Phys. Rev. A* **53,** 2038-2045 (1996).

[55] B. A. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman, Security of quantum cryptography against individual attacks. *Phys. Rev. A* **57,** 2383-2398 (1998).

[56] H. E. Brandt, Quantum-cryptographic entangling probe. *Phys. Rev. A* **71,** 042312 (2005).

[57] J. H. Shapiro and F. N. C. Wong, Attacking quantum key distribution with single-photon two-qubit quantum logic. *Phys. Rev. A* **73,** 012315 (2006).

[58] T. Kim, I. Stork genannt Wersborg, F. N. C. Wong, and J. H. Shapiro, Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol. *Phys. Rev. A* **75,** 042327 (2007).

[59] S. P. Walborn, P. H. Souto Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner, Experimental determination of entanglement with a single measurement. *Nature* **440,** 1022-1024 (2006).

[60] C. H. Bennett *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895-1899 (1993).

[61] A. K. Ekert, Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661-663 (1991).

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

[63] R. Raussendorf, and H. J. Briegel, A One-Way Quantum Computer. *Phys. Rev. Lett.* **86,** 5188-5191 (2001).

[64] P. Walther *et al.* Experimental one-way quantum computing. *Nature* **434,** 169-176 (2005).

[65] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Phys. Rev. Lett.* **81,** 5932-5935 (1998).

[66] A. Fedrizzi *et al.*, A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Optics Express*, **15,** 15377-15386 (2007).

[67] J. H. Shapiro, and N. C. Wong, An ultrabright narrowband source of polarization-entangled photon pairs. *J. Opt. B: Quantum Semiclass. Opt.* **2,** L1 (2000).

[68] T. Kim, M. Fiorentino, P. V. Gorelik, and F. N. C. Wong, Low-cost nanosecond electronic coincidence detector. e-print arXiv:physics/0501141v1 (2005).

[69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.* **23,** 880-884 (1969).

[70] J. B. Altepeter, D. F. V. James, and P. G. Kwiat, Qubit Quantum State Tomography, *Lect. Notes Phys.* **649,** 113-145 (2004).

[71] M. J. A. de Dood, W. T. M. Irvine, and D. Bouwmeester, Nonlinear Photonic Crystals as a Source of Entangled Photons. *Phys. Rev. Lett.* **93,** 040504 (2004).

[72] O. Kuzucu and F. N. C. Wong, Pulsed Sagnac source of narrow-band polarization-entangled photons. *Phys. Rev. A* **77,** 032314 (2008).

[73] C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro, Time-Bin-Modulated Biphotons from Cavity-Enhanced Down-Conversion. *Phys. Rev. Lett.* **97,** 223601 (2006).

[74] C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, High-efficiency entangled photon pair collection in type-II parametric fluorescence. *Phys. Rev. A* **64,** 023802 (2001).

[75] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Bell measurements for teleportation. *Phys. Rev. A* **59,** 3295-3300 (1999).

[76] L. Vaidman and N. Yoran, Methods for reliable teleportation. *Phys. Rev. A* **59,** 116-125 (1999).

[77] Z.-B. Chen, J.-W. Pan, Y.-D.. Zhang, Č. Brukner, and A. Zeilinger, All-Versus-Nothing Violation of Local Realism for Two Entangled Photons. *Phys. Rev. Lett.* **90,** 160408 (2003).

[78] K.-Y. Chen, T. Hogg, and R. Beausoleil, A Quantum Treatment of Public Goods Economics. *Quantum Inf. Process.* **1,** 449-469 (2002).

[79] C. H. Bennett, *et al.* Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Phys. Rev. Lett.* **76,** 722-725 (1996).

[80] M. Born and E. Wolf, *Principles of optics: Electromagnetic theory of propagation, interference and diffraction of light* (Cambridge Univ. Press, Cambridge, 1999).

[81] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2000).

[82] M. Fiorentino, C. E. Kuklewicz, and F. N. C. Wong, Source of polarization entanglement in a single periodically poled $KTiOPO_4$ crystal with overlapping emission cones. *Optics Express* **13,** 127-135 (2004).

[83] M. N. O'Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, Pixel Entanglement: Experimental Realization of Optically Entangled d=3 and d=6 Qudits. *Phys. Rev. Lett.* **94,** 220501 (2005).

[84] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro, Quantum Key Distribution with Higher-Order Alphabets Using Spatially Encoded Qudits. *Phys. Rev. Lett.* **96,** 090501 (2006).

[85] P. G. Kwiat and H. Weinfurter, Embedded Bell-state analysis. *Phys. Rev. A* **58,** R2623-R2626 (1998).

[86] X.-F. Ren, G.-P. Guo, and G.-C. Guo, Complete Bell-states analysis using hyper-entanglement. *Phys. Lett. A* **343,** 8-11 (2005).

[87] H. Bechmann-Pasquinucci and A. Peres, Quantum Cryptography with 3-State Systems. *Phys. Rev. Lett.* **85,** 3313-3316 (2000).

[88] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Experimental Entanglement Swapping: Entangling Photons That Never Interacted. *Phys. Rev. Lett.* **80,** 3891-3894 (1998).

[89] J. W. Pan, C. Simon, Č. Brukner, and A. Zeilinger, Entanglement purification for quantum communication. *Nature* **410,** 1067-1070 (2001).

[90] J. W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Experimental entanglement purification of arbitrary unknown states. *Nature* **423,** 417-422 (2003).

[91] R. Reichle, *et al.* Experimental purification of two-atom entanglement. *Nature* **443,** 838-841 (2006).

[92] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54,** 3824-3851 (1996).

[93] W. K. Wootters, Entanglement of Formation of an Arbitrary State of Two Qubits. *Phys. Rev. Lett.* **80,** 2245-2248 (1998).

[94] W. K. Wootters, Quantum entanglement as a quantifiable resource. *Phil. Trans. R. Soc. Lond. A* **356,** 1717-1731 (1998).

[95] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, Decoherence, Continuous Observation, and Quantum Computing: A Cavity QED Model. *Phys. Rev. Lett.* **75,** 3788-3791 (1995).

[96] F. Schmidt-Kaler, *et al.* Realization of the Cirac–Zoller controlled-NOT quantum gate. *Nature* **422,** 408-411 (2003).

[97] W.K. Wootters and W.H. Zurek, A Single Quantum Cannot be Cloned, *Nature* **299,** 802-803 (1982).

[98] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **85,** 441-444 (2000).

[99] H.-K. Lo, A simple proof of the unconditional security of quantum key distribution. *J. Phys. A* **34,** 6957-6967 (2001).

[100] C. H. Bennett *et al.*, Generalized Privacy Amplification. *IEEE Trans. Inf. Th.* **41,** 1915-1923 (1995).

[101] B. Slutsky *et al.*, Effect of channel imperfection on the secrecy capacity of a quantum cryptographic system. *J. Modern Opt.* **44,** 953-962 (1997).

[102] G. Brassard *et al.*, Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **85,** 1330-1333 (2000).

[103] V. Makarov and D. R. Hjelme, Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **52,** 691-705 (2005).

[104] M. Hillery and L. D. Mlodinow, Quantization of electrodynamics in nonlinear dielectric media. *Phys. Rev. A* **30,** 1860-1865 (1984).

[105] I. Abram and E. Cohen, Quantum theory for light propagation in a nonlinear effective medium. *Phys. Rev. A* **44,** 500-517 (1991).

[106] L.-M. Duan and G.-C. Guo, Alternative approach to electromagnetic field quantization in nonlinear and inhomogeneous media. *Phys. Rev. A* **56,** 925-930 (1997).

[107] D. Ljunggren and M. Tengner, Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers. *Phys. Rev. A* **72,** 062301 (2005).

[108] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Beating the channel capacity limit for linear photonic superdense coding. *Nature Physics* **4,** 282-286 (2008).

[109] W. Wiechmann, S. Kubota, T. Fukui, and H. Masuda, Refractive-index temperature derivatives of potassium titanyl phosphate. *Opt. Lett.* **18,** 1208-1210 (1993).

[110] N. Boeuf *et al.* Calculating characteristics of noncollinear phase matching in uniaxial and biaxial crystals. *Opt. Eng.* **39,** 1016-1024 (2000).