EFFICIENT QUANTUM OPTICAL STATE ENGINEERING AND APPLICATIONS

BY

KEVIN T. MCCUSKER

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Physics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2012

Urbana, Illinois

Doctoral Committee:

Associate Professor Brian DeMarco, Chair
Professor Paul Kwiat, Director of Research
Professor David Ceperley
Associate Professor Peter Abbamonte

Abstract

Over a century after the modern prediction of the existence of individual particles of light by Albert Einstein, a reliable source of this simple quantum state of one photon does not exist. While common light sources such as a light bulb, LED, or laser can produce a pulse of light with an average of one photon, there is (currently) no way of knowing the number of photons in that pulse without first absorbing (and thereby destroying) them. Spontaneous parametric down-conversion, a process in which one high-energy photon splits into two lower-energy photons, allows us to prepare a single-photon state by detecting one of the photons, which then *heralds* the existence of its twin. This process has been the workhorse of quantum optics, allowing demonstrations of a myriad of quantum processes and protocols, such as entanglement, cryptography, superdense coding, teleportation, and simple quantum computing demonstrations. All of these processes would benefit from better engineering of the underlying down-conversion process, but despite significant effort (both theoretical and experimental), optimization of this process is ongoing.

The focus of this work is to optimize certain aspects of a down-conversion source, and then use this tool in novel experiments not otherwise feasible. Specifically, the goal is to optimize the heralding efficiency of the down-conversion photons, i.e., the probability that if one photon is detected, the other photon is also detected. This source is then applied to two experiments (a single-photon source, and a quantum cryptography implementation), and the detailed theory of an additional application (a source of Fock states and path-entangled states, called N00N states) is discussed, along with some other possible applications.

To Mom and Dad.

ACKNOWLEDGEMENTS

This work would not have been possible without the help of many people along the way, both past teachers and current collaborators. I would like those who have directly helped with this work: Brad Christensen for helping with the cryptography experiment, David Schmid for running Zemax simulations, Hee Su Park for helping with the some final work on the single-photon source, Venkat Chandar for help with our error correction, and Daniel Kumor for implementing the error correction. I would like to thank the funding agencies which have supported my work, DARPA (particularly for our grant with Dan Gauthier from Duke for the cryptography experiment), DTO, and IARPA. I would also like to acknowledge the Donald and Shirley Jones fellowship for support. Most of all, I owe my success in my graduate work to my advisor, Paul Kwiat.

Special thanks goes to Mom and Dad, and Pat, Kate, Michael, and Lizzie, for help and support all along the way.

Contents

Chapter 1

INTRODUCTION

The field of quantum information traces its roots back to the early days of quantum mechanics. Although most physical experiments were technologically out of reach, some thought experiments, such as the Einstein-Podolsky-Rosen paradox [1], touched on some fundamental aspects of quantum mechanics, and would, nearly 30 years later, lead to Bell's inequality [2] (which predicts different results for local realism and quantum mechanics), one of the most striking consequences of quantum theory, now tested extensively in several hallmark experiments in quantum optics [3, 4, 5, 6, 7].

Quantum information as its own field began to take shape in the 1980s, with the first proposals of quantum cryptography [8] and quantum computing [9]. The idea that a quantum computer could simulate quantum systems not accessible on a classical computer was suggested by Richard Feynman [10], and once it was shown that quantum computers could solve problems efficiently that were intractable or impossible for a classical computer [11, 12], the field took off. A myriad of other protocols were soon proposed, such as superdense coding [13] and teleportation [14], based on complete control of a simple quantum system, such the polarization of a single photon, or the state of a single atom.

In principle, these protocols can be implemented with nearly any quantum system, and quantum effects at the single-excitation level have indeed been

observed in many systems, such as single atoms [15], microwave cavities [16], and even in some surprising systems such as the motional state of a small mechanical oscillator [17, 18]. All of these systems have different strengths and weaknesses, but in this work I will focus on photons, which are natural physical systems for quantum *communication*. In fact, nearly every quantum information protocol that has been demonstrated in any system has also been demonstrated to some degree optically (e.g., dense coding [19, 20], teleportation [21], quantum logic gates [22], quantum cryptography [23, 24, 25], entanglement distillation [26, 27], and decoherence-free subspaces [28, 29]).

One of the natural advantages of using photons is that many of the tools used to manipulate light at the quantum level are the same as those at the classical level: mirrors and lenses direct and shape a single photon exactly as they would a laser beam. Also, light typically couples very weakly to the environment (unless, of course, it is absorbed). When a photon passes through a lens, bounces off a mirror, or is split by a beam-splitter, the state of the optic is unchanged. This seemingly mundane effect means that when a photon is manipulated (or even sent over hundreds of kilometers of optical fiber [30]), it will maintain its coherence (e.g., entanglement with another particle). This is in stark contrast to most other systems controlled at the quantum level, which must be strictly isolated in vacuum chambers, and cooled near absolute zero. The lack of these requirements makes working with quantum light both convenient and cheap. Unfortunately, the isolation of light is a double-edged sword: two photons will typically only interact with each other very weakly, making a direct interaction between two photons experimentally infeasible. Fortunately, there are ways to make quantum logic gates with linear optics, albeit in a more complicated fashion, requiring many ancilla photons due to the intrinsic probabilistic nature of the basic gate operations [31] (for more on this method, see the beginning of Chapter 3).

To date, nearly all demonstrations of optical quantum information protocols have been using "postselected" results. In a typical experiment, a probabilistic source of photons (or entangled photon pairs) may or may not produce photons,

and these photons may or may not be detected. When using postselection, only the cases when the photons were actually produced and detected are counted. Even in state-of-the-art multi-photon experiments, a successful postselection can happen less than once in a billion attempts (a few events per minute, with an 80 MHz repetition rate laser) [32]. To see why these rates are so low, let us take a step back, and look at the sources used.

Some experiments (such as quantum cryptography) only require one photon at a time. For these experiments, common light sources, from a light bulb to a laser, can be used. If a pulse from such a source is made weak enough, it will typically have either zero or one photons in it (and it is impossible to know how many until we measure it). When there are no photons measured in a pulse, we can just discard that event. When there is one photon measured, we count that result. The possibility of two or more photons (which can be made very unlikely) may add some noise to the experiment, but not prevent it (for more details on this, see the beginning of Chapter 5).

Unfortunately, these simple and easy sources cannot generally be used in experiments involving two or more photons, even using postselection. This is where spontaneous parametric down-conversion (SPDC) comes in. If we shine a laser on a nonlinear crystal, there is a chance that one (or more) photons from this laser will split into two lower-energy photons (called the "signal" and the "idler"). The advantage of this is that if we detect the signal photon (which in practice destroys it), we know the idler photon is present. We have now progressed from not knowing how many photons might be in a pulse until after we measure it to being able to prepare a heralded single photon. This pair production process[1] is the basis of almost all optical quantum information

[1]There is a different pair-production process that is also used in some experiments. SPDC is a three-wave mixing effect (in our case, one pump photon from a laser, and two single down-conversion photons) due to the second-order nonlinearity ($\chi^{(2)}$) of a crystal (only non-centrosymmetric crystals can have this nonlinearity; amorphous glasses cannot). There is also four-wave mixing (FWM), in which two pump photons are converted into two single photons, which is due to a third-order nonlinearity ($\chi^{(3)}$). The strongest $\chi^{(3)}$ available is much weaker than the strongest $\chi^{(2)}$, but common materials such as glass in optical fibers

processing.

Unfortunately, the collection of these photon pairs is typically inefficient. The focus of this work is to optimize this collection, and then demonstrate some applications that take advantage of this. I address the optimization itself in Chapter 2, and show a heralding efficiency that is the best reported so far. Even if the collection of the photons is efficient, the pairs are produced randomly, so multi-photon experiments are not directly scalable ($P_{Npairs} \propto (P_{1pair})^N$). In Chapter 3 I demonstrate a time-multiplexing method to produce sources that can be used for scalable optical quantum computing, and then show how this method can be extended to producing a class of different states in Chapter 4. Finally, I apply the efficient pair source to a novel, ultra-high-speed quantum cryptography system in Chapter 5.

exhibit this nonlinearity at appreciable levels. The upside of this is that very long fibers can be used, making the flux comparable to three-wave mixing. There are advantages (such as always being in a single spatial mode) and disadvantages (such as large background noise from Raman photons) to this method. Here I focus entirely on SPDC, but many of the techniques would be directly applicable to FWM sources as well.

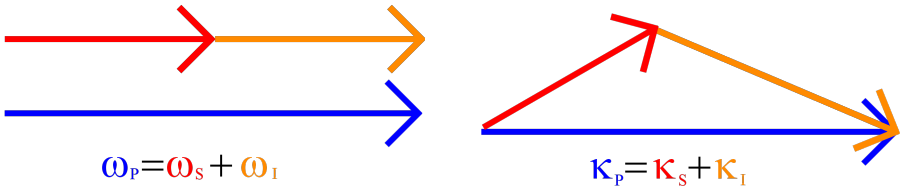
Chapter 2

OPTIMIZING DOWN-CONVERSION

2.1 Introduction to down-conversion

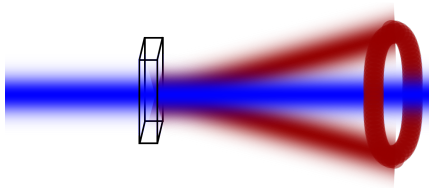
Spontaneous parametric down-conversion (SPDC) is a process in which one high-energy photon splits into two lower-energy photons (called the signal and the idler photons[1]) due to a second-order nonlinear effect inside of a crystal [33]. As discussed in Chapter 1, this process is used in numerous quantum optical experiments because of its easy generation of a useful quantum state. For SPDC to occur, both energy and momentum must be conserved (this condition is called phase-matching) (see Fig. 2.1). Because of dispersion, phase-matching can usually only be met for crystals exhibiting birefringence (i.e., different index of refraction for different polarizations). In a birefringent crystal, there is an asymmetry in the crystal structure, leading to different indices of refraction for the two different polarizations (called the ordinary and extraordinary polarizations). The index of refraction for ordinarily-polarized light is constant

[1] Which photon is the signal and which is the idler is arbitrary. The nomenclature comes from parametric amplification, in which only one beam is typically used.



(a) The total energy of the down-conversion photons must be equal to that of the pump photon.

(b) The total momentum of the down-conversion photons must sum up to that of the pump photon.



(c) The phase-matching is satisfied for a ring, making the down-conversion light come out in a cone (for type I; for type II there are two cones).

Figure 2.1: Phase-matching constraints determine the color and direction of the light that can be created.

(i.e., independent of the propagation direction of the light), while the index for extraordinarily-polarized light depends on the orientation of the beam relative to the crystal optic axis. The phase-matching condition is usually satisfied for a wide range of wavelengths and directions of the down-conversion photons, leading to a very complicated, multi-mode state coming out of the crystal.

Experimentally, there are many different ways to configure a down-conversion system. Following the naming convention of second-harmonic generation [33], the phase-matching possibilities are called type I and type II. In type-I phase-matching, the two photons are the same polarization, and are created traveling on opposite sides of a cone, centered about the pump beam (see Fig. 2.1(c)). Changing the orientation of the crystal axis changes the phase-matching con-

(a) (b) (c)

Figure 2.2: Possible geometries for type-II phase-matching. The cones can be tuned so the cross section of the spatial mode of the down-conversion is (a) noncollinear, (b) collinear, or (c) "beam-like".

ditions, and therefore changes the angle of the cone. This angle is usually set to be a few degrees, though larger [34] or smaller angles are sometimes used. In type-II phase-matching, the two down-conversion photons have different polarizations, and are created in two separate cones, which can also be tuned by changing the crystal axis. The geometry can be noncollinear (Fig. 2.2(a)), collinear (Fig. 2.2(b)), or "beam-like" (Fig. 2.2(c)).

For many experiments, such as tests of Bell's inequality [35] or quantum computing demonstrations [22], pairs of polarization-entangled photons are required. Different methods of creating entangled pairs exist (e.g., collecting from the overlap of the two cones in type II [35] or by combining different paths of an interferometer [36, 37]), but in this work I use the method first proposed in [38]. In this case, two crystals, cut for type-I phase-matching, are placed back-to-back, with one crystal rotated 90° with respect to the other. The first crystal can produce pairs of horizontally-polarized photons, and the second can produce pairs of vertically-polarized photons. If the source is set up carefully (e.g., the crystals are not too thick), then it is impossible to determine in which crystal the pair was created, so the state is a quantum superposition of the two possibilities (i.e., either both photons are horizontally polarized, or both photons are vertically polarized), and the two photons are in an entangled state:

$$|\psi\rangle = |HH\rangle + e^{i\phi(\lambda_i,\lambda_s)}|VV\rangle, \tag{2.1}$$

where the relative phase ϕ depends on several factors, such as the polarization of the pump, the wavelength of the down-conversion[2], and the propagation path of the down-conversion photons in the crystal.

Different experiments have different requirements for the down-conversion source, but the types of sources can be broadly separated into two categories, based on whether or not the photons created must be identical from one pair to the next. In, for example, a Bell-inequality experiment, it is sufficient if any given pair exhibits good polarization entanglement. However, in an experiment involving interfering photons from different pairs, it is critical that these photons be identical and pure (i.e., have the same frequency spectrum, temporal mode, and spatial mode, without any entanglement of those degrees of freedom with any other system), or else the interference will be degraded. Since the phase-matching is typically satisfied for generating light into a multi-mode field, the photons will not be identical from pair to pair (e.g., they will be slightly different colors or be traveling in slightly different directions).

Fortunately, there are ways to overcome this problem. Coupling the photons into a single-mode fiber guarantees the spatial modes of different pairs will be identical (though this coupling is often a lossy process). Removing the spectral correlations is more difficult. If an ultra-short pump is used (which has a large uncertainty in the energy per photon), filters with a bandwidth comparable to (or narrower than) that of the pump will remove most of the spectral correlations [39]. This filtering allows for good multi-photon interference, but it is very lossy. Recently, sources of down-conversion engineered to have no intrinsic spectral entanglement have been demonstrated [40, 41, 42, 34].

In addition to the issue of purity, there are different criteria for a down-conversion source. A few examples of different parameters to optimize are pairs/MHz/s (i.e., generated into a specific narrow bandwidth) [43], pairs/s/mW [44], pairs/s/mW/nm [37], pairs/s [45], pure pairs/s [42], highest visibility [45],

[2]The wavelength-dependence on phase is due to temporal walk-off with the pump, and can cause dephasing, but this effect is negligible for a long pump pulse duration, and correctable for a small duration.

or some combination of these. Each criterion can lead to slightly different optimizations. One criterion of particular relevance for our research is the heralding efficiency. The heralding efficiency is defined as the probability of detecting the idler photon, given that the signal photon was detected (or vice-versa). Since the typical spatial and spectral filtering is very lossy (and also inefficient detectors are used), this number is usually quite low (e.g., in some notable experiments such as [38] and [44], the heralding efficiency is approximately 10% and 1%, respectively).

A low heralding efficiency is a problem, particularly for scaling up experiments to even a few photons. In an 8-photon experiment (requiring 4 pairs), for example, the counting rate scales as the heralding efficiency[3] to the 8th power. If the low counting rate is compensated for by increasing the laser power, higher-order terms begin to occur as well (e.g., five pairs instead of four), which lowers the fidelity with the desired state. A high heralding efficiency will therefore help both to increase rates, and detect noise from higher-pair events. For example, in [32], an increase in the heralding efficiency from 14% to 50% would increase the 8-photon counting rate from 4 per minute to over 100,000 per minute. In addition, multiplexed sources, which must be used in order for SDPC to be scalable beyond a handful of photons, require high heralding efficiency (see Chapters 3 and 4).

There has been significant effort to optimize collection of down-conversion, both theoretical [46, 47, 42, 48, 49, 50] and experimental [51, 52, 53, 54, 55, 56, 57]. Pittman *et al.* were able to couple a heralded single photon into a fiber with 83% efficiency in a noncollinear type-I phase-matching setup (this counts only the spatial-mode collection; overall heralding, including detection efficiency, was 31%) [58]. This was only a one-way heralding, i.e., the signal heralded the idler efficiently, but the idler did not necessarily herald the signal efficiently. Another significant experiment with efficient coupling is [37], with

[3]If the heralding efficiency is symmetric for both sides (i.e., for signal heralding idler and idler heralding signal), the heralding efficiency is the same as the overall collection efficiency for each photon.

an extremely high inferred mode overlap of 95% using a collinear type-II phase-matching setup (overall heralding of 32%), though uncertainty due to detector efficiency is not specified. This paper also had a significant (about 15%) optical loss in coupling, and it is not clear how easily this can be overcome. Recently, Smith *et al.* reported a one-way heralding efficiency of 66% (fiber coupling of 80%), mainly due to using superconducting transition-edge sensors, which can have a very high detection efficiency (>95% [59], compared to 40-65% with conventional APD (avalanche photodiode) single photon detectors) [57].

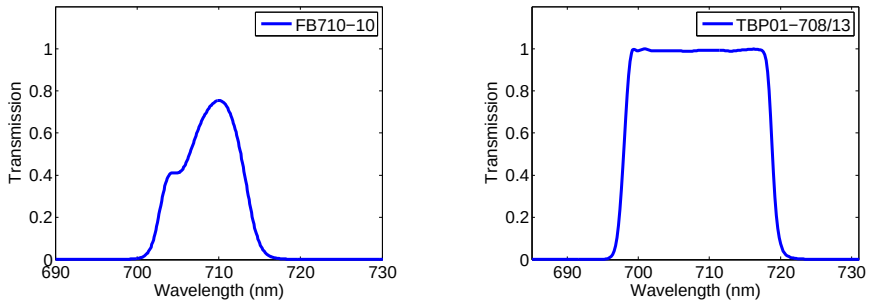
In this chapter we describe our efforts to maximize the overall heralding efficiency of a type-I phase-matched source. Collecting in both pure and mixed spatial modes are considered. No attempt is made to limit spectral entanglement in this work, but the approach is compatible with the strategy discussed in, e.g., [34]. Specific applications are discussed in Section 2.3.

2.2 Optimizing down-conversion collection

The overall heralding efficiency depends on several factors, which I separate into spectral filtering, spatial filtering, and loss (including detector loss).

2.2.1 Spectral filtering

In general, the down-conversion spectrum can be quite broad (e.g., covering the entire visible spectrum with a UV pump). It is impractical to try to collect all of this light, since different colors will be propagating in different directions, and the optics and detectors typically do not perform well over that broad of a bandwidth. We use spectral filters to only look at a relatively narrow range of wavelengths (e.g., a 2-20 nm bandwidth). The easiest way to do spectral filtering is with interference filters, which can be made to have a high peak transmission (>99% is possible), high out-of-band rejection (>OD 6), and variable bandwidths (from a few nanometers to hundreds) (see Fig. 2.3(b) for the spectrum of a typical high-performance interference filter). The high transmis-



(a) A 710-nm filter from Thorlabs.

(b) TBP01-708/13 filter from Semrock.

Figure 2.3: Transmission curves for (a) a typical interference filter and (b) a high-performance filter.

sion and high out-of-band rejection means any given down-conversion photon will either be very likely or very unlikely to pass through the filter, depending on the wavelength. However, it is difficult for an interference filter to have a very sharp edge region (the edge can be defined as the bandwidth between, e.g., 5% and 95% transmission). If the flux in the edge region is a significant fraction of the total flux, the average heralding efficiency will be reduced. For this reason, we use a large bandwidth.

Unfortunately, a filter with exactly the desired transmission, center wavelength, and bandwidth is not likely to be available. Ordering a custom filter from a vendor is possible, but such a filter typically either has poor performance (low transmission and/or slow edges, see Fig. 2.3(a)) or is prohibitively expensive. However, it is possible to tune off-the-shelf filters, so high-performance filters already available from vendors can be combined to effectively make a custom filter. The best vendor I have found for filters for this purpose, both in performance and selection, is Semrock.

The bandwidth of a filter can be shifted down in wavelength by tilting it[4], or up in wavelength by temperature treatment (in the case of Semrock filters, this

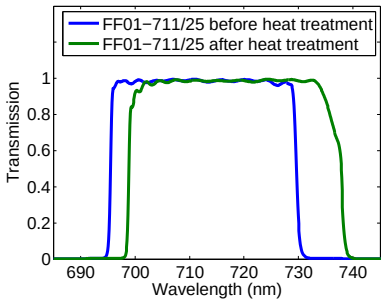
[4]We have recently noticed that a tilted filter has a wavelength-dependent phase between the s- and p-polarized light, which can cause polarization dephasing.

shift is applied by the manufacturer and is permanent). In our case, we want a filter with a center wavelength of 710 nm, and a bandwidth of about 20 nm (710 nm is the wavelength for frequency-degenerate down-conversion with our 355-nm pump, which is from the third harmonic of a 1064-nm YAG laser). We can create such a filter by combining several filters from Semrock. First we take an FF01-711/25 filter, and temperature tune it up a few nm (see Fig. 2.4(a)). We also use an FF01-697/58 filter, and tilt it $\sim 13^\circ$ (Fig. 2.4(b)). Combining these, we can create the desired filter (Fig. 2.4(c)). Comparing this "custom" filter to a typical one (in this case from Thorlabs, see Fig. 2.3(a)), we can see a dramatic difference, with a calculated spectral heralding efficiency[5] increasing from 50% to 95%. We have observed this increase in practice.

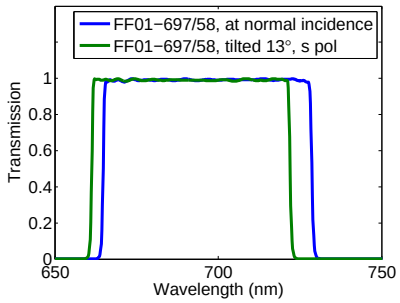
In addition to interference filters, we also examined the use of a diffraction grating for high-efficiency spectral filtering (essentially a low-loss monochromator). We collaborated with Olivier Parriaux from the Université Jean Monnet in Saint-Étienne, France, who has been able to fabricate a diffraction grating with >99% of the incoming light emitted into the negative first order [60] (this establishes the peak transmission of our filter). Let us first look abstractly at the theory of using a grating as a filter. We start with a collimated beam, which has a narrow uncertainty of k-vectors (Fig. 2.5). The action of the grating is to change the direction of the beam depending on the color, which looks like a displacement in the k-vector. The spectral resolution (i.e., edge sharpness) of this filter depends on the amount of this displacement relative to the initial spread of k-vectors. The bandwidth of the filter is determined by the range of k-vectors collected after the grating.

An experimental setup of this approach is shown in Fig. 2.6. A collimated beam is incident on the grating, which shifts the direction of the beam depending on the color of the light. A spatial filter is implemented by a lens, which focuses the light to a different position depending on the incoming direction, followed

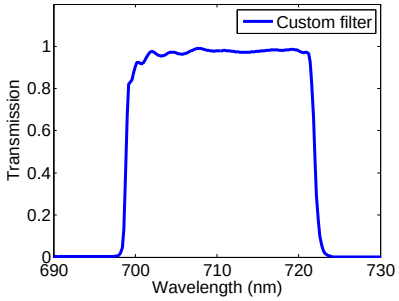
[5]The spectral heralding efficiency only considers the loss of the filter, i.e., it is the probability that, given the signal photon got through its spectral filter, the idler photon also gets through its spectral filter. Spatial heralding efficiency is defined similarly.



(a) A 711-nm filter (FF01-711/25) from Semrock, before and after temperature treatment. Note that the degraded edge sharpness on the high end of the bandwidth will not be a factor, since that edge is defined by the other filter.



(b) A 697-nm filter (FF01-697/58) from Semrock, both at normal incidence and at a 13° incidence angle. S polarization is used since the bandwidth shifts faster than for p polarization.



(c) The effective transmission of our "custom" filter, made by stacking the filters in (a) and (b).

Figure 2.4: Making a "custom" spectral filter by tuning two off-the-shelf filters.

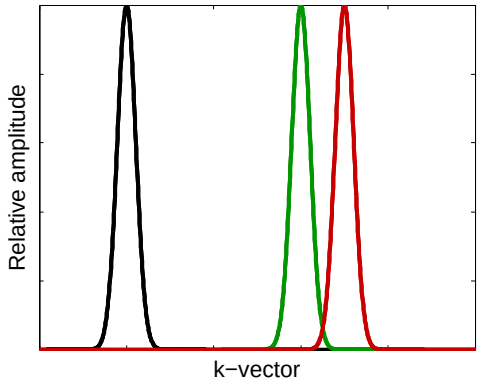


Figure 2.5: Spread of k-vectors for a collimated beam, before (black) and after (green and red) hitting a grating. The amount of the displacement in k-space depends on the wavelength of the light.

by a slit, which can tunably select the central wavelength and bandwidth. If necessary (e.g., for coupling into a fiber), another lens and another grating can then remove the wavelength-dependence on direction. With this approach, we have implemented a high-transmission tunable filter with a measured edge sharpness of 0.02 nm.

There are of course limits on how well we can create a filter using this approach. If we want a sharp edge on our filter, we need to use a grating that has a high dispersion (or increase the beam diameter–reducing the initial k-vector spread–which makes the same k-vector displacement have a relatively larger effect). The dispersion is limited by the geometry of the setup (the extreme case would be the beam incident at a glancing angle, and being reflected straight back), and the beam diameter is limited by the availability, convenience, and aberrations of large optics (including the grating). With these limits, an edge sharpness of about 0.01 nm is possible at 700 nm. However, in the case of a large dispersion and large bandwidth, the light coming from the grating can have a very large angular spread, requiring an optical system with a high nu-

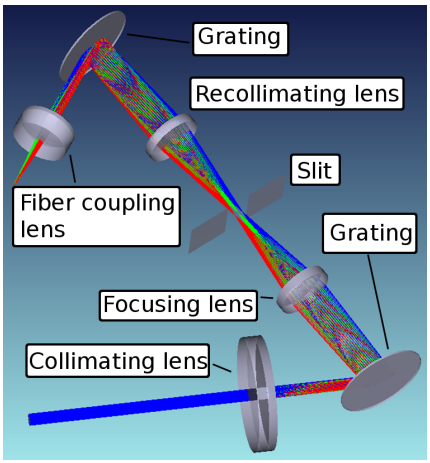


Figure 2.6: Implementing a spectral filter with a grating. A collimated beam hits the grating, and the reflected light is focused down with a lens. A slit then selects which colors are transmitted. If necessary, another lens and grating are used to recombine the different colors. The graphic is from Zemax, the ray-tracing program used for simulations.

merical aperture[6], even over relatively modest bandwidths (e.g., the required NA could be as large as 0.17 (20°) for a bandwidth of 20 nm centered at 700 nm). An optical system to collect and spatially filter this would be impractical, and would suffer large aberrations that would limit the performance. The result of this is that we have a tradeoff between the bandwidth of the filter and the edge sharpness. We used Zemax (a ray-tracing program) to test different configurations. We were able to optimize the system by tuning the grating, beam size, incidence angle, and exact lenses used, with the constraint of keeping reasonably good single-mode fiber coupling (arbitrarily set at 80%). The edge sharpness is near optimal (0.01 nm) for bandwidths up to about 1 nm, and then it begins to grow in proportion to the input bandwidth (due to aberrations). This can be seen in Fig. 2.7, with the bandwidth/edge ratio increasing linearly with the

[6]The numerical aperture characterizes the range of angles an optical system will accept or emit. It is defined as NA=$n\sin(\theta)$, where θ is the half-angle of the maximum cone of light, and ranges from 0 (infinitely narrow divergence) to 1 (180° divergence) in air.

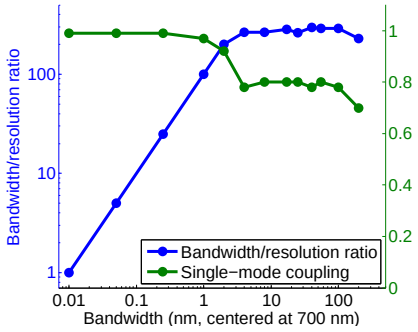


Figure 2.7: Results from ray-tracing simulations. For small bandwidths, the bandwidth/resolution ratio increases linearly with bandwidth, then saturates for larger bandwidths due to aberrations. The single-mode coupling was high for low bandwidth, then decreases for larger bandwidths, also due to aberrations.

bandwidth up until about 1 nm, and then saturating. The fiber coupling is very good up until the edge sharpness degrades, also due to aberrations.

Recently, we have begun investigating putting the lens before the grating. This would allow the first lens of the spatial filter to be unaffected by the large numerical aperture of the light after the grating, which would allow us to have both a large bandwidth and a sharp edge. However, collecting the light after the slit would still be impractical for anything other than immediately focusing onto a large-area detector.

Overall, we concluded that using interference filters is preferable for a high-bandwidth source, due to the ease of use. However, the grating approach is still valuable, due to its high performance even at narrow bandwidths, and its ability to be easily tuned.

2.2.2 Spatial filtering

As discussed in Section 2.1, we are using a type-I phase-matched source, and our down-conversion beams are frequency-degenerate (so we can assume the optimal signal and idler spatial collection modes will be symmetric). For optimizing

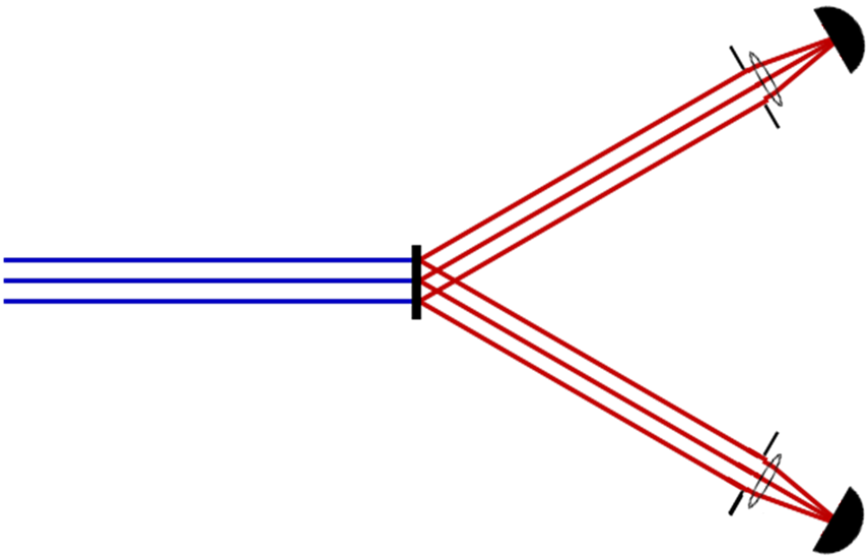
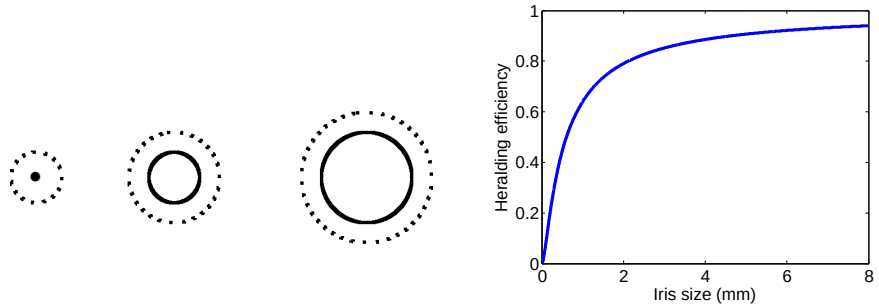


Figure 2.8: Simple down-conversion collection scheme. A collimated pump beam hits the crystal, and the down-conversion light is collected through irises. After the irises, the light is focused down to single-photon detectors.

collection of the down-conversion spatial modes, our adjustable parameters are the length of the crystal, the pump spatial mode (i.e., beam size and focus), and the spatial filter applied to the down-conversion light. The length of the crystal (we typically use either β-Barium Borate (BBO) [61] or Bismuth Barium Borate (BiBO) [62]) affects the phase-matching bandwidth (a longer crystal emits a narrower spectrum into a given direction) and the brightness (a longer crystal emits more light into a given spectrum). For our noncollinear source, we also need to take into account the "walk-off" of the down-conversion photons, both from the pump and from each other. This walk-off can be due to the different directions of the beams (which are typically about 4° apart), but also due to birefringent walk-off of extraordinarily-polarized light (which is also typically about 4°). A 600 μm crystal is a good compromise between brightness, bandwidth, and walk-off.

One of the simplest approaches for spatial collection is shown in Fig. 2.8. A



(a) The heralded mode size (dashed line) given the collected mode size through an iris (solid line).

(b) Heralding efficiency versus iris size, assuming the heralded mode has a 0.5 mm larger diameter.

Figure 2.9: The heralding efficiency increases as iris size increases.

collimated beam is incident on a crystal, and irises are positioned to collect the signal and idler photons, with a lens behind the iris, focusing the light down to single-photon counters; the detector size is typically sufficient to catch all of the incident light, though we must check for any new system[7]. One simple way to model the down-conversion spatial modes is as pairs of collimated beams, with the same waist as the pump beam (but more divergence since the wavelength is longer). The photons in the beams are created in every direction around the phase-matched cone, but always in pairs on opposite sides of the cone. If we imagine collecting through a very small iris (i.e., a pinhole) on the signal side, the heralded idler photon would then be in a pure spatial mode with a definite size (e.g., 1 mm) (see Fig. 2.9(a)). If we instead collect through a 1-mm iris on the signal side, the heralded idler photon would be in a mixture of modes, centered at the same spot as before, but spread out to about 2 mm. As we increase the iris size on the signal side, the heralded idler mode will continue to increase in size, but with an extra $\sim$1 mm diameter. If we have identical irises on both signal and idler sides, the heralding efficiency increases as the iris size increases, since the uncollected portion is relatively smaller (see Fig. 2.9(b)). Determining

[7]We have noticed with careful scans of the detector that there can be a significant change (>10%) in the efficiency over the entire detector surface.

No focusing				
Bandwidth	20 nm	10 nm	5 nm	2 nm
2 mm iris	57%	72%	84%	93%
4 mm iris	79%	84%	95%	95%
6 mm iris	90%	91%	98%	97%
8 mm iris	98%	97%	98%	99%

Table 2.1: Heralding efficiency data for collecting through irises with a collimated pump (see Fig. 2.8).

Focusing through crystal, onto plane of collection irises			
Bandwidth	20 nm	10 nm	5 nm
2.4 mm iris	53%	77%	84%
3.5 mm iris	72%	87%	90%
5.4 mm iris	83%	95%	93%

Table 2.2: Heralding efficiency data for collecting through irises with a focused pump (see Fig. 2.10).

Focusing at crystal (bandwidth 10 nm, similar numbers for 20 nm)	
Single-mode fiber	90(1)%
Few-mode fiber (1550 SMF)	88(2)%
Multi-mode fiber (65 μm core)	82(1)%

Table 2.3: Heralding efficiency data for collecting into fiber (see Fig. 2.11).

the absolute spatial heralding efficiency can be determined by fixing the iris size on one side, and look at the heralding efficiency as the iris is opened on the other side. At some point, the heralding efficiency will saturate, at which point we are collecting the entire mode of the heralded photon. Dividing the heralding efficiency with equal sized irises by this saturated value gives the absolute spatial heralding efficiency:

$$\eta_{spatial} = \frac{\eta}{\eta_{saturated}}. \tag{2.2}$$

This approach of using a collimated beam with irises can achieve a very high

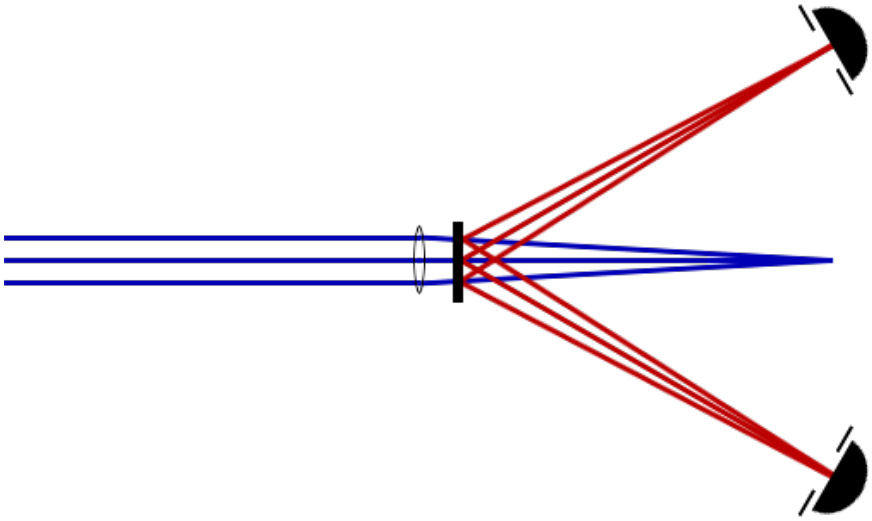


Figure 2.10: A different down-conversion collection scheme, with a focused pump. The idea is that the spatial mode of the down-converted light is also focusing, making the spatial correlations at the irises tighter.

spatial heralding efficiency (>98-99%), but only for large irises and/or small bandwidths (i.e., as we look down and to the right of Table 2.1). The small bandwidth is a problem, because it negatively impacts the spectral heralding efficiency, as discussed in Section 2.2.1. If we use a large iris, there will be a large number of spatial modes. If all we are doing is immediately focusing down to a detector that is large enough for the focused spot, this will not be a problem. However, for some applications, such as coupling to a small detector or cycling in a cavity, a large number of modes is difficult or impossible to work with (see Section 2.3). Another approach, suggested in [63], is to focus the pump to the plane of the irises (see Fig. 2.10). The idea is that the focus of the pump is transferred to the down-conversion beams, so they are effectively focusing to the irises as well, which makes the spatial-mode correlations tighter at that plane (i.e., if we collect through a small pinhole on the signal side, it will herald a beam that is small on the idler side at the same plane). This would allow a relatively small iris to still have high heralding efficiency. The measured

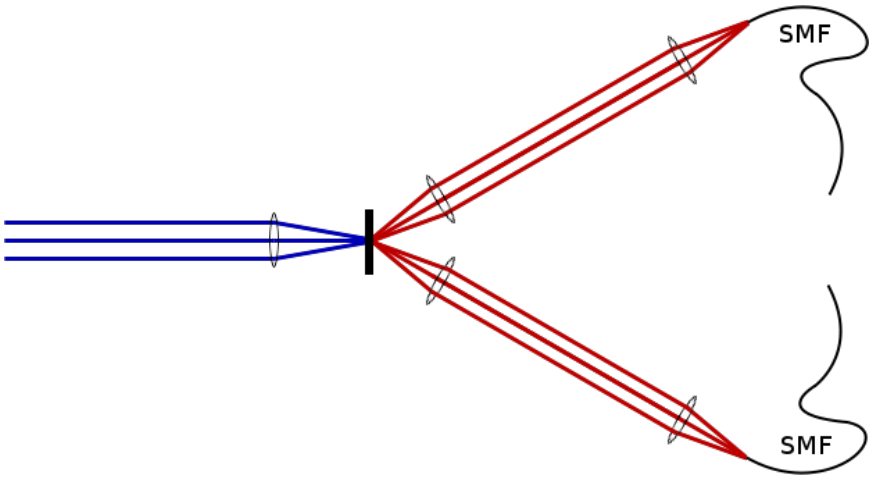


Figure 2.11: Down-conversion collection scheme with the crystal imaged onto a single-mode fiber (SMF). The pump is focused down to the crystal to increase the intensity at the location that is being imaged. The fiber can also be a few-mode or multi-mode fiber.

data did *not* show this effect (see Table 2.3), though it was by no means a thorough investigation of this configuration, and it is possible improvements may be possible with this method.

The next method we used for optimizing spatial heralding efficiency is shown in Fig. 2.11. In this setup, a small spot of the crystal is imaged onto the end of a single-mode fiber. Since we are only collecting over a small portion of the crystal, we focus the pump down to increase the intensity at this area (focusing the pump down also increases the total brightness [64]). The fiber projects the light into a single spatial mode, so the light on the other side must also be a single spatial mode, and it turns out to be very close to a beam with the same spatial mode (on the opposite side of the cone) [46]. This setup led to very high spatial heralding efficiency (see Table 2.3), comparable to the best reported (see Section 2.1). The absolute spatial heralding efficiency in this case was determined by the same method as with irises, i.e., by using a larger filter on one side (in this case, a larger core fiber) to collect the entire spatial mode

of the heralded photon, and then using this efficiency as the normalization. For example, if we observed a (two-way) absolute heralding efficiency of 20% with single-mode fibers on both sides (core=4 μm), which increased to a (one-way) absolute heralding efficiency of 25% with 1550-nm single-mode fiber on one side (core=9 μm), and did not increase any further with a multi-mode fiber (core=65 μm) (saturation at only a slightly higher core diameter is a good indication that the modes we are not collecting into single-mode fiber are very low order, as we would expect). From this, we would calculate a symmetric two-way spatial heralding efficiency of $\eta_{2-way} = \frac{20\%}{25\%} = 80\%$.

Since we are sometimes willing to trade a pure spatial mode for better heralding, we tried using few-mode fibers[8] in place of the single-mode fibers. The idea behind this is that, similar to opening up the irises, using larger fibers will increase the heralding efficiency. However, using larger fibers actually made the heralding efficiency decrease. This is contrary to expectation, and not yet understood. We speculate the reason for this is that the higher-order modes from the fibers are not imaged as precisely as the fundamental mode, leading to decreased correlations.

2.2.3 Overall heralding

In addition to the spatial and spectral filtering, the heralding efficiency can be reduced by loss in the system. The loss is due to reflections or scattering from, e.g., lenses or fibers, and there are also losses due to imperfect detectors. We used optics with minimal reflection losses (though we have not yet used anti-reflection-coated fibers) to reduce this loss down to about 10%, and our detectors (PerkinElmer SPCM-AQR-14) are on average about 65% efficient at our wavelength. We have measured an overall symmetric heralding efficiency of 48.5% (for both the signal photon heralding the idler, and for the idler heralding

[8] A few-mode fiber is a fiber with a core size between that of a single-mode fiber ($\sim$4 μm) and a typical multi-mode fiber ($\sim$65 μm). For example, a fiber that is single mode at 1550 nm supports about seven modes at 710 nm.

the signal). Our predicted heralding efficiency is:

$$\begin{aligned}\eta_{absolute} &= \eta_{spatial filter} \times \eta_{spectral filter} \times \eta_{lossy optics} \times \eta_{detector}, \\ &= 0.90 \times 0.95 \times 0.9 \times 0.65, \\ &= 0.50.\end{aligned}$$

The 1.5-percentage-point deviation from our measured efficiency can be attributed to the detector efficiencies, which have not been precisely characterized. With anti-reflection-coated fibers and the very efficient transition-edge sensor detectors [59], we expect to be able to reach an absolute two-way heralding efficiency of about 80%.

2.3 Applications

Now that we have this efficient source of pairs of photons, we want to consider the applications for it. There are many possibilities, in addition to a single-photon source, Fock & N00N state sources, and a quantum cryptography system discussed in Chapters 3, 4, and 5 respectively, and we consider some of them here.

One application which requires an extremely high heralding efficiency is a loophole-free test of Bell's inequality [2]. The timing loophole[9] can be closed by sending the photons far away from each other, and the detector loophole[10] can be closed with an efficiency as low as 67% (this is for perfect preparation and noiseless measurement of the desired (non-maximally entangled) state; due to noise, polarizer crosstalk, etc., we expect the required efficiency to be 70-80%) [65]. To reach this, we would need to use different detectors, such as the superconducting transition-edge detectors, that can operate with >95% efficiency

[9] Since we are testing locality, we must make the measurements separated in space-time, or else the measurement *setting* on one side could affect the measurement *outcome* on the other, via some sort of sub-light-speed signaling.

[10] Since we are testing a general hidden-variable theory, we must allow for the possibility of the detection probability depending on the measurement settings, which can only be ruled out with very good heralding efficiency (as opposed to postselected coincidences).

[59], or visible-light photon counters, that can operate with similar efficiency [66]. Note that since this would be a two-photon experiment, a pure source is not required, i.e., collecting into multiple spatial and spectral modes is acceptable. However, the fibers used in the superconducting photon-counting system to guide the light to the actual detector must not guide thermal photons, so the core size must be smaller than a typical 65-μm-core multi-mode fiber ($<\sim$30-μm-core for the relevant thermal photons). Thus, collecting through large irises would not be suitable for this detector, though collection into few-mode fiber would be acceptable.

Another application we are working on in our lab is to prepare single- and few-photon states with high fidelity, to test the limits of human vision. It is known that humans can detect as little as 7 photons [67], but no one has tried to test the threshold with a source that has sub-Poissonian statistics (i.e., $g^{(2)}<1$, see Chapter 3). With a good source, we can send exactly one (or two, or three, or more) photon into the eye at a specific time, and test the response of subjects. In this case, "a specific time" does not mean within the picosecond-scale timing of the coherence length of the photons, but rather within the integration time of the eye, which is on the millisecond scale [68]. Thus, we can use a high-efficiency source of gated, (one-way) heralded single photons to create the effective multi-photon states. A pure source is not required here either, since there is no multi-photon interference; however, collecting into a single spatial mode will allow for optimal control of imaging the photons onto the back of the eye.

Chapter 3

SINGLE-PHOTON SOURCE

3.1 Introduction to single-photon sources

Perhaps the simplest non-trivial quantum optical state is exactly one excitation of the electromagnetic field, a single photon. In addition to its simple elegance, a single-photon source would be of immense value for the field of optical quantum information (see [69] for a recent review of single-photon sources). It is even possible to do probabilistic quantum logic with only single photons and linear optics (which, combined with efficient detectors and feed-forward, can be used for scalable quantum computing) [31]. The necessary detectors [59] and switches already exist, so a single-photon source would be an enabling technology for scalable quantum computing.

Conceptually, a single-photon source can be quite simple. If exactly one atom is in a trap, then after it is excited, it will release exactly one identical photon (assuming there is only one decay path). Unfortunately, this photon would not be very useful, since it would be radiated into every direction. It is possible to put such an atom in a cavity, which can force the atom to decay

into a specific mode [70], but the efficiencies of such systems remain low (best is 6.1% in [71]). Collective excitations in an atomic ensemble can be used, but the efficiency for this is low as well (1.8% in [72]). There are promising solid-state versions of a single-photon source, with a simulated atom such as a quantum dot or nitrogen-vacancy center in diamond, but extraction efficiencies into a useful mode are still low (16% for a quantum dot [73] and 2.2% for an NV center [74]), and making these photons identical is challenging as well [75, 76, 77, 78]. Superconducting resonators coupled to Josephson junctions can be used to exercise fine control over the quantum electromagnetic field, with excellent fidelity for the production of arbitrary few-photon states [79], but such a state is necessarily contained in electronics near absolute zero (so it cannot be used as a "flying qubit" for quantum communication), and the coherence times are not quite long enough for significant logic gates, though there has been significant improvement [80]. It is possible in principle to use nonlinear optical phenomena to directly manipulate light at the single-photon level (such as the Kerr effect [81] or strong two-photon absorption [82, 83]), but they are typically several orders of magnitude too weak to be of practical use. Of course, SPDC is one nonlinear optical effect which can be used.

Before we look closer at an SPDC-based source, let us first examine the requirements for a source for quantum computing. Early proposals assumed near-perfect photon sources and detectors [31, 84, 85], but later work showed that scalable computing can be done with single-photon-source efficiencies as low as 67% [86] (or pair-source efficiencies as low as 50% [87]). This work in turn assumed that the higher-order terms of a source (e.g., two photons instead of one or no photon) were zero. In reality, these higher-order terms (quantified by the second-order coherence function, defined as $g^{(2)} = \langle \hat{a}^{\dagger 2} \hat{a}^2 \rangle / \langle \hat{a}^\dagger \hat{a} \rangle^2$) may be quite significant (particularly for a down-conversion-based source, where the underlying source has a thermal distribution [88]). Recently, Jennewein *et al.* determined some specific tolerances for a realistic source, taking into account the $g^{(2)}$ [89] (see Fig. 3.5(b) at the end of this chapter for specific numbers of what is acceptable). These results can help us set the ultimate goal for our

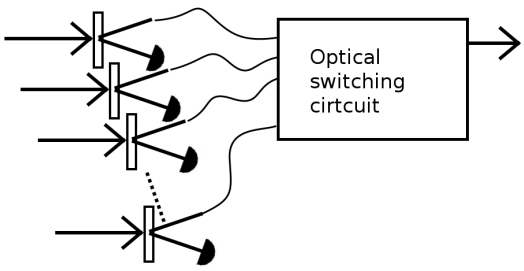


Figure 3.1: Spatially-multiplexed down-conversion sources [90]. Multiple independent sources with independent detectors and collection optics are simultaneously pumped, and one of the heralded single photons is routed to the output.

source.

3.2 Down-conversion-based source

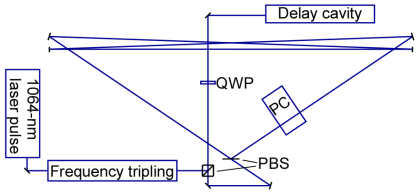
As discussed in Chapter 2, we can, with down-conversion, produce pairs of photons, and collect them efficiently. Although this process is not deterministic (i.e., we do not know if any given pump pulse will produce a pair or not), it is still an efficient source of *heralded* photons (detecting the signal heralds the presence of the idler). The approach for our single-photon source is to use these heralded photons that are produced randomly, but rearrange them with active multiplexing so they appear in the desired mode with high probability.

One way to implement this would be with multiple spatially-multiplexed sources (see Fig. 3.1) [90]. In this case, there are multiple independent sources, each pumped simultaneously (this could be implemented with one crystal, by collecting at multiple points around the cone), with a separate detector for each source. Each time the sources are pumped, the detectors herald where a single photon is, and that photon is routed to the desired output, making the source act as a deterministic source. Recently, this type of source was demonstrated experimentally using four sources; compared to a single source, it showed a 4x increase in flux with no increase in $g^{(2)}$ (which was about 0.49), but with a

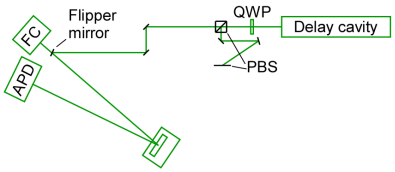
low single-photon probability of less than 0.1% (including detector efficiency) [91]. One significant disadvantage of the spatially-multiplexed scheme is that optics for multiple spatial modes must be used, along with multiple detectors and switching elements.

As an alternative to these requirements, we have developed a temporally-multiplexed source [92, 93]. In this case, one crystal is pumped multiple times, by multiple evenly-spaced pulses. When a single photon is heralded, it is switched into a storage cavity (the cavity length is the same as the length between pump pulses). After a pre-set number of pulses (e.g., 20), the light in the storage cavity is released, which is, with high probability, exactly one photon. For this approach, only a single set of collection optics, detector, and switch are required, and the effective number of sources can be tuned by only changing the electronics (i.e., the number of pulses before releasing the light in the cavity).

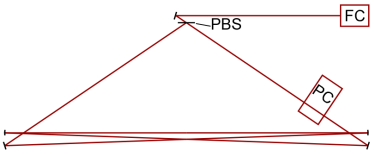
A diagram of our setup is shown in Fig. 3.2. Since a typical high repetition-rate laser (e.g., a Ti:Sapphire laser running at 80 MHz) may not have enough energy per pulse for our purposes, we use a laser with a much lower repetition rate (40 kHz), but much higher pulse energy, and then use the pulse multiple times. First, shown in Fig. 3.2(a), we start with this high-energy (∼20 microjoules) 1064-nm pulse from a Q-switched Nd:YAG laser (DualChip DNP-150010-000 by JDSUniphase), then use second-harmonic generation and sum-frequency generation to produce a UV pulse at 355 nm. Since this laser is not perfectly periodic (there is about a one microsecond jitter in the pulse-to-pulse separation), we add a delay cavity to allow for time to synchronize the electronics (e.g., the switch in the cavity). The pump pulse then enters a storage cavity (about 25 ns per cycle), consisting of a Brewster-angle polarizing beam-splitter (PBS), several mirrors, and a Pockels cell. Initially, the pump pulse is horizontally polarized so it is transmitted through the PBS, then the Pockels cell is fired (for the first pass only), which rotates the polarization to vertical so it is reflected from the PBS. At this point, the pump pulse is stored in the cavity, where it remains until it decays after a few hundred nanoseconds



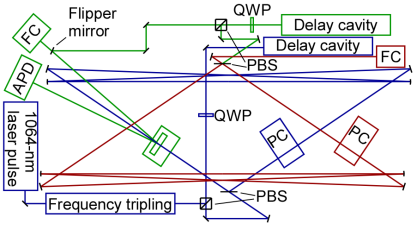
(a) We generate the third harmonic of a 1064-nm pulse, send it through a delay line to allow for time to synchronize the Pockels cell electronics, then switch the pulse into a storage cavity.



(b) In every cycle of the storage cavity, the pump pulse passes through a crystal, with a chance of producing a pair of photons. If a signal photon is detected, then there is a heralded idler photon in the other mode. After passing through a delay line, again to allow for time for the electronics and detector latency, it is sent into a storage cavity. The flipper mirror allows us to switch between aligning the down-conversion modes and the rest of the setup.



(c) The heralded idler photon enters the cavity, and is switched in on the first pass. The light in the cavity is released at a preset time, regardless of when the photon was switched in.



(d) The entire layout of the experiment.

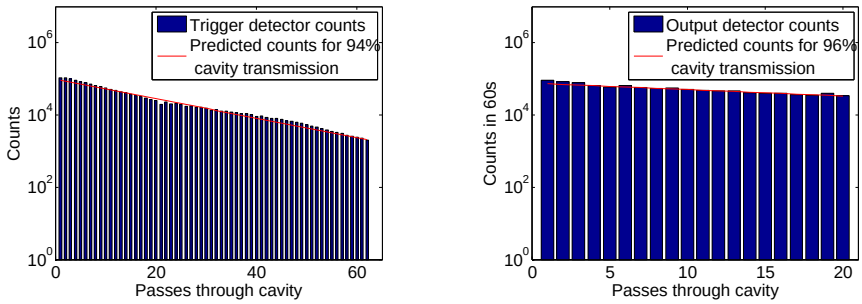
Figure 3.2: Experimental diagram. For convenience, it is broken up into several pieces. (PC: Pockels cell; QWP: quarter-wave plate; PBS: polarizing beamsplitter; APD: avalanche photodiode; FC: fiber coupled APD)

(i.e., ∼30 pulses). The Brewster-angle PBS used in the cavity is very low loss (<0.1%), particularly on reflection (which is how we are using it for the cavity). As shown in the diagram in Fig. 3.2(a), there are four mirrors in the cavity in addition to the PBS. Two of those mirrors, which are curved, periodically focus the beam, making the cavity stable, and the aberrations are reduced by hitting these mirrors at near-normal incidence (the other two mirrors are there to allow for this near-normal geometry).

In each cycle of the pump pulse in the cavity, it passes through the down-conversion crystal, with a chance each time to create a pair of photons (see Fig. 3.2(b)). We have in place a collection system to detect the signal photon, heralding the presence of the idler (see Chapter 2). When a signal photon is detected, after another delay (to allow for the detector latency, and to give us time to synchronize the electronics of the switch), the heralded idler photon is switched into another cavity, of similar design to that for the pump (Fig.3.2(c)). If a subsequent single photon is heralded, it can be switched in (which will switch out the older one), essentially "refreshing" the photon in the cavity. At a predetermined time, the light in the storage cavity (which will be, with high probability, exactly one photon) is released.

Data showing the cycling of the pump storage cavity is shown in Fig. 3.3(a). This figure shows the singles counts on one detector, as a function of the number of passes in the cavity. As expected, there is a smooth exponential decay corresponding to the measured per-pass cavity transmission of 94%. Data showing the cycling of the single photons is shown in Fig. 3.3(b). For this figure, the idler photons created from the first pass of the pump pulse are switched in, stored for a variable number of passes, and then detected. Again, we get a smooth exponential decay corresponding to the expected per-pass cavity transmission of 96%. Most of the loss is due to the Pockels cell, and with a new Pockels cell we have recently obtained (with transmission of 99.5%) and lower-loss mirrors, we expect the next version of the cavity to have a total loss of <1%.

Once the performance of the down-conversion source and the various optics are characterized, we can experimentally vary two parameters to change the per-



(a) Data showing cycling of the pump cavity. Singles counts on the signal side are shown as a function of the number of passes of the pump in the cavity.

(b) Data showing the cycling of the single-photon cavity. Idler photons generated on the first pump pulse are switched into the cavity, stored for a variable number of passes, and then switched out and counted.

Figure 3.3: Cycling of the two cavities.

formance of the source: the initial pump energy, and the number of cycles before we switch out the light in the storage cavity. The anticipated source performance is shown in Fig. 3.4 as a function of these two parameters (see Appendix C for details on the calculations). On the left side of this figure, the probability is shown with the current performance of the individual elements, that is, a UV cavity loss of 6%, a single-photon cavity loss of 4%, a fiber heralding efficiency of 80%, and an overall heralding efficiency of 47% (the difference between fiber heralding and overall heralding is the detector efficiency; see Chapter 2). We also have the limitation of a Pockels cell that can only fire twice in the few hundred nanoseconds before the pump pulse decays. With this limitation, we can only switch in two heralded photons, so eventually the performance actually diminishes as the number of down-conversion passes increases[1]. On the right side of Fig. 3.4, the probability is shown for what is feasible with some improvements, namely with no UV cavity loss (possible with a high-repetition rate laser,

[1] An alternative strategy would be to wait a long enough time in a fixed (optical) delay line, so the last photon could always be selected, which would require less switching (but more loss from the extra optical delay).

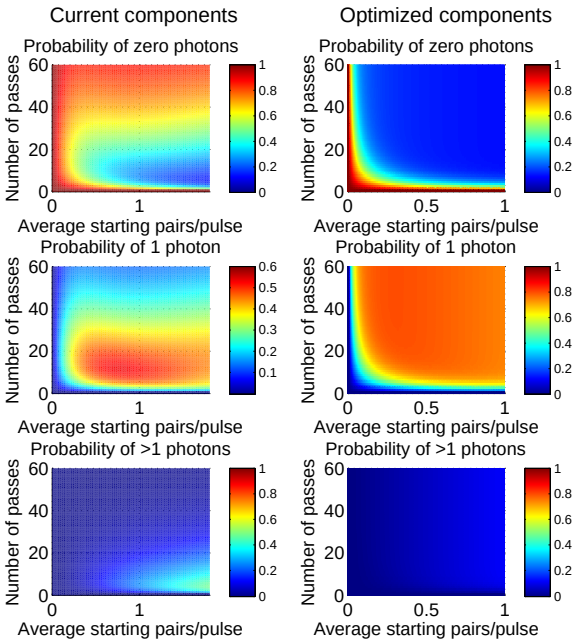
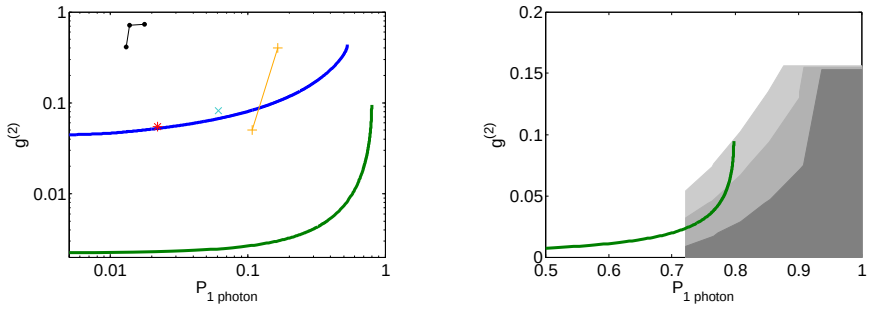


Figure 3.4: Theoretical source performance for current (left) and optimized (right) components (see text for specific definitions of current and optimized), showing the probabilities of zero (top), one (middle), and two or more (bottom) photons. Note the different scale used in the middle plot on the left (for better contrast).



(a) Curves showing predicted trade-off between $P_{1photon}$ and $g^{(2)}$ for current (blue) and optimized (green) components (perfect source would be bottom-right corner). Also shown are current performance for sources based on an atomic ensemble (black points; [72]), single atom (cyan x; [71], nitrogen-vacancy center in diamond (red star; [74]), and quantum dot (orange pluses; [73]).

(b) Zooming in on the curve of $P_{1photon}$ and $g^{(2)}$, now showing the regions calculated in [89] to be acceptable for quantum computing (note that lower efficiency sources means more resources are required to perform a single quantum logic gate). The different regions are assuming the computation is done with different detector efficiencies. From lightest to darkest, the assumed efficiencies are 100%, 95%, and 90%.

Figure 3.5: Plots of predicted and obtained $g^{(2)}$ vs $P_{1photon}$.

such as the one used in our cryptography experiment; see Chap. 5), a single-photon cavity loss of 1% (possible with recently-obtain Pockels cell, see above), a fiber heralding efficiency of 87% (possible with anti-reflection coated fibers), an overall heralding efficiency of 82% with photon-number resolution (both this efficiency and number resolution are possible with superconducting transition-edge sensors [59]; photon-number sensitivity allows us to discard events where two pairs are created at the same time), and a switch able to fire at an arbitrary rate. As shown in the figure, with a fast enough switch, the performance saturates (instead of decreasing) as the number of passes is increased.

As discussed in Section 3.1, both the probability to produce one photon and the $g^{(2)}$ are relevant factors for the usefulness of a source for quantum computing. In our source, there is a trade-off between the two parameters. For example, if we pump very weakly, we can be very confident there are not two photons, and have a low $g^{(2)}$. Of course, we also greatly reduce the probability of one photon. In Fig. 3.5(a), we show the curve of what we can reach with this trade-off, along with points showing the best performance for other sources (note the photons from these sources are not necessarily pure). In Fig. 3.5(b), we zoom in on the bottom-right corner of this curve. The shaded region of this plot is the area that has been shown to be tolerable for quantum computing [89]. The different regions are assuming different efficiencies for the detector to be used in the computation. From lightest to darkest, this efficiency is 100%, 95%, and 90%. As we can see from the graph, with our optimized components (and incorporation of a pure down-conversion source), we can make a source usable for scalable quantum computing in conjunction with a 95% efficient detector!

In our initial implementation of this experiment, the down-conversion collection was just done with irises (see Chapter 2). Although the heralding of the idler was high (due to a larger iris on the idler side), the spatial mode was mixed, leading to poor coupling to the storage cavity. Also, since the heralding of the signal was low (i.e., many more idler photons were detected than signal, again due to the larger iris), unheralded photons were coupled into the cycling mode, raising the $g^{(2)}$. In addition to this, the initial pump pulse energy was

not high enough (due to poor tripling efficiency). These effects led to a significantly lower performance than what we have shown to be reachable in Fig. 3.4. Nevertheless, we were able to show a source with a $g^{(2)}$ less than one ($\sim$0.6), and with a $P_{1photon}$=$\sim$0.01. With the incorporation of our improved heralding and a stronger laser, we will be able to immediately reach any point on the blue curve of Fig. 3.5(a).

Chapter 4

FOCK- AND N00N-STATE SOURCE

4.1 Fock-state creation

In Chapter 3, we used repeated attempts at down-conversion to create pairs of photons, in order to create a single photon with high probability. In that case, although not stated explicitly, the signal and idler modes entering the crystal were always vacuum, and we can consider a heralded down-conversion event as adding a photon to the idler mode. Essentially, the repeated attempts at down-conversion (with suitable heralding) can be considered as deterministically applying the creation operator to the idler mode. In this chapter, I discuss a novel method of efficiently creating a certain class of multi-photon states that exploits this perspective, with significant implications for applications such as quantum metrology. See [94] for a publication of the work presented in this chapter[1].

The experimental approach for this is similar to that for the single-photon source discussed previously. However, instead of the down-conversion crystal

[1]Portions of this chapter

being outside of the storage cavity, it is inside (see Fig. 4.1). Initially, there is a vacuum in the cavity. Multiple attempts at down-conversion are made until the first pair is created (with the presence of the idler heralded by the signal), adding a single photon to the cavity. Repeating this process, we can "build up" a photon-number (Fock) state. Once we have the desired number of photons in the cavity, we release them using a switch, as in the single-photon source. If we have a photon-number-resolving detector for the signal arm, we can add more than one photon on each pass, allowing us to build up the state in fewer passes (although we need to be careful not to overshoot the desired number of photons in the cavity).

Before proceeding onto the expected performance, let us look in more depth at what will be happening in the cavity. We need to distinguish between a true Fock state, where the state is multiple excitations of the same mode of the electromagnetic field, and what we are calling a pseudo-Fock state, which has a definite number of photons, but with multiple modes (e.g., different colors for the different photons, as was the case for the system described in Chapter 2). Also, since we do not always have a vacuum as the input to our down-conversion source, we need to consider the effects of stimulated emission. If we are producing a Fock state (i.e., all photons in the same mode), this stimulated emission will result in pairs being more likely to be produced, which allow us to use a weaker pump. If we are producing a pseudo-Fock state, only the modes that already have photons will be stimulated, which will lead to a type of spontaneous symmetry breaking.

Fig. 4.2 shows the predicted performance as a function of cavity transmission, for different detector efficiencies (see Appendix C for details on the calculations). Here we assume a photon-number resolving detector [59], and the ability to tune the pump pulse intensity–and hence the expected number of pairs–for each pass at down-conversion, although producing several pure pairs per pulse remains experimentally challenging (without these assumptions, we would simply need more passes to prepare the desired number of photons). Our predicted performance greatly exceeds current methods: e.g., creating a

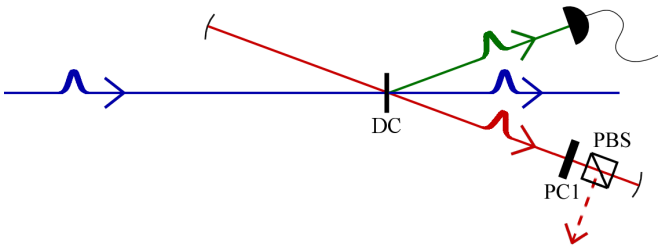


Figure 4.1: Diagram of proposed Fock-state source. A pulsed laser pumps a down-conversion crystal (DC). The signal photon of each created pair is detected, and the idler photon is emitted into a storage cavity. Photons are allowed to accumulate in the cavity until the desired number is reached. The light can be switched out by rotating its polarization with a Pockels cell (PC1), so the polarizing beam-splitter (PBS) reflects rather than transmits it.

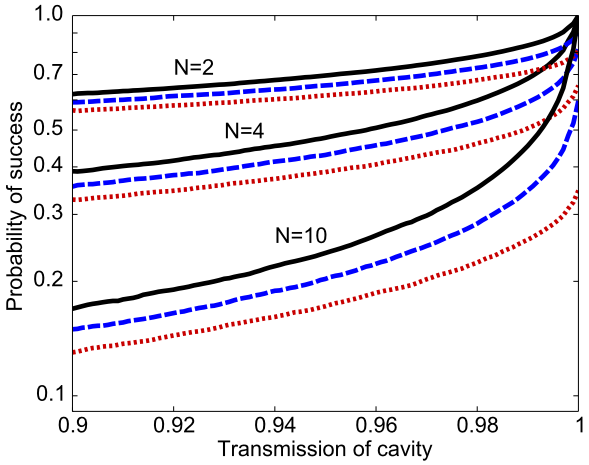


Figure 4.2: Theoretical performance of Fock-state source, showing success probability versus cavity transmission. Curves are shown for several values of N (labeled), and several detector efficiencies (black solid, η=1; blue dashed, η=0.95; red dotted, η=0.9).

heralded four-photon Fock state via single-pass down-conversion is in principle limited to 8.2% probability[2], and the best experimental result is only 0.2% (with fidelity=0.6) [95]; even postselecting on an attenuated coherent source cannot do better than 19.6% probability[3]. Our scheme could realistically produce this state with >50% probability.

4.2 N00N-state creation

In addition to Fock states, this approach can be used to produce states with a definite number of photons, but with different polarizations of these photons. By manipulating the polarization of the photon that is being added (or equivalently, manipulating the polarization of the photons already created before the next one is added), we can efficiently produce any state that is expressible as a product of creation operators of arbitrary polarization on a single mode:

$$|\psi\rangle \quad = \prod_{n=0}^{N-1} (\alpha_n a_H^\dagger + \beta_n a_V^\dagger)|0\rangle. \tag{4.1}$$

One of the more interesting states that we can create of this form is a number-path entangled state of the form $|N_A, 0_B\rangle + |0_A, N_B\rangle$ (known as a "$N00N$" state [96]). A $N00N$ state can be used to reach the Heisenberg limit for precision measurements, achieving a phase uncertainty that scales as $1/N$ [96, 97, 98, 99]. This same state can also be used for quantum lithography [100], demonstrating "super resolution". Originally proposed methods [101, 102] for creating $N00N$ states using linear optics scaled exponentially poorly with increasing N, even assuming perfect optics, on-demand Fock-state sources, and detectors. A recent proposal [103] suggests a method for creating $N00N$ states that scales efficiently using linear optics and feed-forward, but the number of photons making up the $N00N$ state varies nondeterministically in each attempt.

We start with the observation that a $N00N$ state in the right/left circular polarization basis can be expressed as a product of linearly polarized photons

[2]For a single pass, the pair production is a thermal distribution [88], so P_{4pairs}=0.082.

[3]A coherent source has a Poissonian distribution, so P_{4pairs}=0.196.

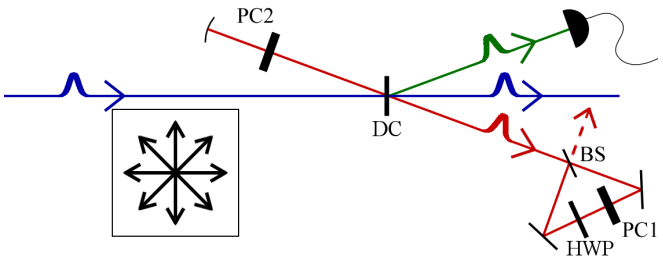


Figure 4.3: Diagram of proposed $N00N$-state source. This is similar to the setup for the Fock-state source (Fig. 4.1), with the addition of a Pockels cell (PC2) in the cavity to rotate the polarization of the photons as they are created, and a polarization-independent switch (made up of a beam-splitter (BS), half-wave plate (HWP), and Pockels cell (PC1)) in place of a polarization-dependent switch. Inset shows the linear polarization of 4 photons in the desired state.

(neglecting normalization) [99]:

$$(\hat{a}_R^\dagger)^N - (\hat{a}_L^\dagger)^N = \prod_{n=0}^{N-1} [cos(n\pi/N)\hat{a}_H^\dagger + sin(n\pi/N)\hat{a}_V^\dagger]. \tag{4.2}$$

This state is the product of N photons superimposed on each other, with the polarization of the photons evenly spaced by 180°/N (see Fig. 4.3 inset). We can construct this state by adding N photons one at a time to the field in the cavity, and rotating the polarization of all photons in the cavity by 180°/N every time a new photon is added. The proposed setup, shown in Fig. 4.3, is similar to the setup for making Fock states, with the addition of a Pockels cell to rotate the polarization of the light in the cavity[4], and a polarization-independent switch[5].

[4]For the cavity design shown in Fig. 4.3, it is experimentally simpler to create a $N00N$ state in the 45°/-45° basis, expressible as a product of elliptical polarization states: $(\hat{a}_{45°}^\dagger)^N - (\hat{a}_{-45°}^\dagger)^N = \prod_{n=0}^{N-1}[cos(n\pi/N)\hat{a}_H^\dagger + isin(n\pi/N)\hat{a}_V^\dagger]$. This is a similar distribution on the Poincaré sphere as Eq. (4.2), but in the vertical instead of horizontal plane. This distribution can be created using PC2 to incrementally rotate the initially horizontally polarized photons around 45° on the Poincaré sphere.

[5]The switch can be realized with a Sagnac interferometer with a half-wave plate at 0° and a Pockels cell able to act as a half-wave plate at 45° (PC1 in Fig. 4.3). When PC1 is on, there is a 180°-phase shift between the path that goes through the HWP then PC1 and the path

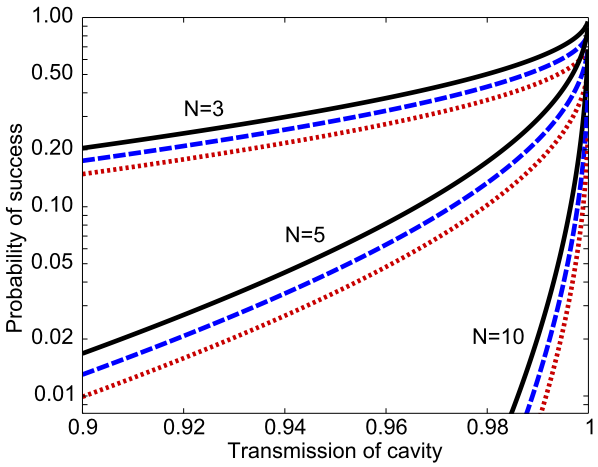


Figure 4.4: Theoretical performance of $N00N$-state source. Curves are shown for several values of N (labeled), and for several different detector efficiencies (black solid, η=1; blue dashed, η=0.95; red dotted, η=0.9).

After the switch-out, wave plates and a polarizing beam-splitter can convert the state to the desired number-path entangled state.

The predicted performance is shown in Fig. 4.4 (again, see Appendix C for details on the calculations). Comparing with Fig. 4.2, we can see that the probability of successfully producing a $N00N$ state is significantly lower than that of producing a Fock state with the same number of photons. The primary reason is that the $N00N$ state *must* be built up exactly one photon at a time, whereas for the Fock state several photons can be added in one pass. The additional passes for $N00N$ state creation increase the sensitivity to cavity loss. Also, the fidelity of the produced state is not perfect due to higher-order terms in the down-conversion Hamiltonian (see below). Nevertheless, our predicted performance exceeds current state-of-the-art experiments [99] (by more than an order of magnitude) and previous proposals using linear optics. For example, the highest probability [102] of creating an N=6 $N00N$ state

that goes through PC1 then the HWP, allowing for on-demand switch-out.

with linear optics is 0.097, assuming perfect on-demand Fock-state sources (12 photons total), perfect optics, and perfect detector efficiency. This level of performance is feasible with our proposal, *without* these assumptions.

We now discuss in detail the limitations of this proposal. For our performance plots in Figs. 4.2 and 4.4, a "success" is defined as an attempt with each created pair collected and detected, with no photons leaking out of the cavity before the process is complete, and with no extra photons (although for creating Fock states, it is still a success if the number of photons lost is equal to the number of extra photons). Photon loss for each pass through the cavity must therefore be minimized[6], and the down-conversion photons must be efficiently collected in pure states.

In addition to these factors, the effect of the higher-order terms of the down-conversion Hamiltonian must be taken into account. Even when no pairs are created, the effect of higher-order terms in the Hamiltonian of the down-conversion can alter the state in the cavity. Treating the pump pulse classically, we have [104]:

$$e^{i\epsilon\hat{H}} = 1 - \epsilon\hat{a}^\dagger\hat{b}^\dagger + \tfrac{\epsilon^2}{2}\hat{a}^{\dagger 2}\hat{b}^{\dagger 2} - \tfrac{\epsilon^2}{2}\hat{a}\hat{a}^\dagger\hat{b}\hat{b}^\dagger, \tag{4.3}$$

where ϵ is the effective interaction strength, and $\hat{a}$ and $\hat{b}$ refer to the idler and signal modes, respectively. Terms of order ϵ^3 are dropped, as are terms where $\hat{b}$ would be acting on the vacuum (giving zero). The second term of Eq. (4.3) creates the desired single pair of photons. The third term creates an undesirable two pairs, which could be detected with a photon-number-resolving detector, and eliminated by driving weakly enough. The fourth term, which can be interpreted as the creation and then destruction of a pair, can alter the state in the cavity, even though it does not add or remove any photons. If, for example, we are trying to create a $N00N$ state with N=4, after the creation and rotation of two photons, the state in the cavity will be (neglecting

[6] If the cavity loss is polarization dependent, it can affect the state even if no photon is lost, as the loss acts as a partial polarizer [99].

normalization)

$$(\hat{a}_H^\dagger + \hat{a}_V^\dagger)\hat{a}_V^\dagger|0_H 0_V\rangle = |1_H 1_V\rangle + \sqrt{2}|0_H 2_V\rangle. \tag{4.4}$$

Applying the Hamiltonian in Eq. (4.3) (assuming no signal photon is present, i.e., projecting out the contribution from the second and third terms), gives

$$(1 - \frac{\epsilon^2}{2}\hat{a}_H\hat{a}_H^\dagger)(|1_H 1_V\rangle + \sqrt{2}|0_H 2_V\rangle) = (1-\epsilon^2)|1_H 1_V\rangle + (1 - \frac{\epsilon^2}{2})\sqrt{2}|0_H 2_V\rangle, \tag{4.5}$$

which differs from the initial state in Eq. (4.4). This change adds *coherently* with each pass, and lowers the fidelity between the produced state and the desired state, even as ϵ approaches zero. However, the effective down-conversion operator in Eq. (4.5) can be undone (to order ϵ^2) by applying the same effective operator with the orthogonal polarization:

$$(1 - \frac{\epsilon^2}{2}\hat{a}_H\hat{a}_H^\dagger)(1 - \frac{\epsilon^2}{2}\hat{a}_V\hat{a}_V^\dagger)|\psi\rangle = (1 - \frac{\epsilon^2}{2}(\hat{a}_H\hat{a}_H^\dagger + \hat{a}_V\hat{a}_V^\dagger))|\psi\rangle. \tag{4.6}$$

Since the state in the cavity $|\psi\rangle$ always has a definite number of photons, it is an eigenstate of $\hat{a}_H\hat{a}_H^\dagger + \hat{a}_V\hat{a}_V^\dagger$, and therefore an eigenstate of the operator in Eq. (4.6). We can approximate the alternate application of these operators by adding the photons to the cavity in a different order, resulting in a higher average overlap with the desired state (e.g., from about 0.56 to 0.83 for N=8). Preliminary results indicate that this state, with a photon distribution on the Poincaré sphere similar to that of a $N00N$ state, is still useful for quantum metrology (see Fig. 4.5); more detailed investigation of this is an interesting possibility for future study.

4.3 Additional states

Let us now consider some alternate states we can make, of the form in Eq. (4.1). Recent research shows that $N00N$ states decohere very rapidly in the presence of loss [105]; however, a similar superposition (of the form $|m, m'\rangle_{A,B} + |m', m\rangle_{A,B}, m > m'$) can greatly improve the robustness against decoherence while keeping the ability to perform sub-shot noise phase estimation [106, 107].

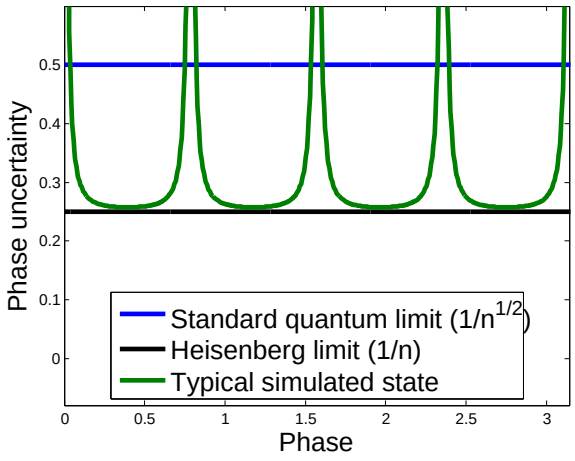


Figure 4.5: Typical phase-sensitivity performance of a 4-photon $N00N$-state generated from our source. This state is clearly still useful for beating the standard quantum limit.

To create such a state, we first observe that it can be expressed as the product of a $N00N$- and Fock-state creation operators:

$$(\hat{a}_A^\dagger)^m(\hat{a}_B^\dagger)^{m'} + (\hat{a}_A^\dagger)^{m'}(\hat{a}_B^\dagger)^m = \left((\hat{a}_A^\dagger)^{m-m'} + (\hat{a}_B^\dagger)^{m-m'}\right)(\hat{a}_A^\dagger)^{m'}(\hat{a}_B^\dagger)^{m'}. \quad (4.7)$$

Since this is a product of the Fock and $N00N$ state creation operators, in order to create this new state, we can create two Fock states in the cavity, and then add a $N00N$ state.

Another possibility for this approach relies on exploiting the similarity between polarization and the first-order orbital angular momentum (OAM) modes [109]. Since they are both two-level systems, polarization and the first-order OAM states can be represented on the Poincaré sphere [108]. Since Eq. (4.2) can be thought of as arising from interference on the Poincaré sphere, we can get the same effect with OAM states. Specifically, if we produce a 4-photon product state with one photon in each of the OAM modes on the equator of the Poincaré sphere (see Fig. 4.6), this will be a $N00N$ state, with all four photons in a superposition of plus OAM spin and minus OAM spin. Such a state

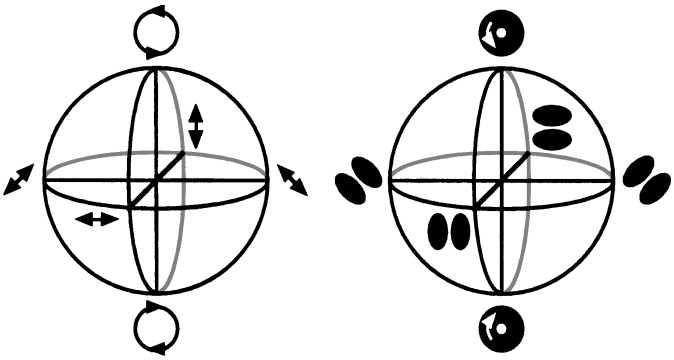


Figure 4.6: Polarization (left) and the first-order orbital-angular momentum modes (right) presented on the Poincaré sphere [108].

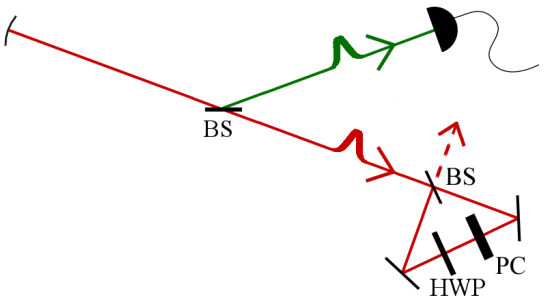


Figure 4.7: Diagram of proposed deterministic photon-subtraction technique. Similar to weakly *adding* a photon to a cavity with down-conversion, we can weakly *subtract* a photon from a cavity with a weak beam-splitter (BS).

may be useful for quantum metrological applications such as precise rotation measurements [110]. Since down-conversion produces light that is correlated in the OAM degree of freedom [111, 112], we can use our approach for creating polarization-based $N00N$ states to create OAM-based $N00N$ states. Unfortunately, since the down-conversion pairs are produced in every OAM state (as opposed to a specific polarization state), the source will not be deterministic, but instead heralded, based on getting exactly one photon in each of the desired OAM modes.

In conclusion, we have proposed a novel technique that can efficiently pro-

duce a variety of multi-photon states with high fidelity, including Fock and $N00N$ states. Although we discussed only the case where we start with the vacuum in the idler mode and build up states with a well-defined number of photons, these techniques can also be applied to states that do not have well-defined photon numbers, such as squeezed or coherent states. Another possibility which may allow for the creation of additional interesting states is supplying something other than the vacuum for the initial *signal* field, such as a weak coherent state [113] or zero-one photon entangled state [114]. Finally, if we replace the weak down-conversion source in our cavity with a weak beam-splitter (see Fig. 4.7), and allow a state to pass through it multiple times until a photon is detected in the reflected path, we can in principle remove a single photon from the state with arbitrarily high efficiency. The ability to subtract photons allows for generation of interesting states, including $N00N$ states [115]. Combining the ability to both add and subtract photons [116] may allow for direct tests of fundamental physics (such as the bosonic commutation relation [117]) as well as creation of otherwise-unreachable states.

Chapter 5

TIME-BIN QUANTUM CRYPTOGRAPHY

5.1 Background

In the 20th century, the field of cryptography began to be approached from a mathematical perspective. In 1949, Claude Shannon was the first[1] to publish a proof of the security of a cryptography system (the one-time pad) based on information theory [119]. In this system, both parties share a secret random key that is as long (or longer) than the message to be sent. They use the key only once to encrypt and decrypt the message. In this case, a potential eavesdropper can only learn the length of the message, but nothing else. If the eavesdropper attempts a brute-force search, she will find that every possible message of that length was equally likely to have been sent. This type of system remains the only (classical) cryptography system that is completely secure.

Unfortunately, the one-time pad is impractical for most uses, since the message length is limited by the key length. In 1972, the US government identified

[1] It is not surprising Shannon was the first, since he essentially single-handedly invented the field of information theory, in a remarkable work published in 1948 [118].

a need for a standard, secure cryptography system [120]. This led to the development of DES (Data Encryption Standard) and eventually AES (Advanced Encryption Standard), which is in use today [121]. AES can be efficiently implemented with both hardware and software, and the best known attack on a properly-implemented AES system is $2^{126.1}$ operations (for a key size of 128 bits), which is sufficiently high for the encryption to be considered secure [122].

AES, however, is a symmetric-key system, which unfortunately requires the two parties to share the key ahead of time. This will not be true in general (e.g., accessing a bank account on a new computer). Fortunately, algorithms have been discovered that can securely distribute a key between two parties. These asymmetric (or public-key) systems use two (mathematically-related) keys, one of which encrypts the message (and is made public), and one of which decrypts the message (and is kept private). The first of these, published in 1976 [123], relies on the computational complexity of the discrete logarithm problem[2]. This was soon followed in 1978 by RSA [124], which relies on the computational complexity of factoring large integers. Either of these can be used in practice to create a shared secret key between two parties that initially share no secret information, with an eavesdropper requiring exponentially more computing time (using any currently-known algorithm) to find the key than for the parties to share it. This secret key can then be used directly with a one-time pad, or for a symmetric-key system such as AES or DES (which are much faster).

While this combination of public-key and symmetric-key cryptography works very well in practice, it is still fundamentally insecure, since it is possible in principle for the key to be found through a brute-force search (or with an as-yet undiscovered efficient algorithm). More importantly, Peter Shor devised an algorithm in 1994 that would allow a quantum computer to solve both the factoring problem and the discrete logarithm problem in polynomial time [11], breaking public-key cryptography (although currently there is no known quantum algorithm to lower the computational complexity for an attack against AES [125]).

[2]The discrete logarithm is the group theory analog of the ordinary logarithm. For example, in the set {1,2,3,4,5}, the solution of $3^x = 4$ is $x = 2$, since $3^2 = 4 \pmod 5$.

The field of quantum cryptography begin in 1984, with a proposal from Charles Bennett and Gilles Brassard [8]. The principle of this approach is for the first party (conventionally called Alice) to send the second party (conventionally called Bob) a two-level quantum state (e.g., the polarization of a photon). The state that is sent represents one bit of information (e.g., Alice sends a horizontally (H) polarized photon for a '0', and a vertically (V) polarized photon for a '1'). However, Alice (Bob) does not always send (measure) photons in the H/V basis, but some fraction of the time sends (measures) in another basis, e.g., the diagonal/antidiagonal (D/A) basis. If an eavesdropper (conventionally called Eve) tries to measure the signal (by measuring the polarization of the photons), this will introduce errors in Bob's measurements, since it is assumed she does not know which measurement basis to use for any given photon. Because some level of error will always occur due to experimental imperfections, error correction must be done [126]. Alice and Bob must assume that Eve is responsible for any errors they detect, so "privacy amplification" is then used to remove any knowledge Eve might have of the key [127]. If Alice is sending a randomly-generated message, then this protocol is a completely and *provably* secure way of distributing a random key, which can be used either directly as a one-time pad, or as the key for, e.g., AES (note this still depends on a correct implementation; commercial implementations of quantum key distribution (QKD) have been cracked due to incorrect assumptions about the detectors [128]). Authentication between Alice and Bob must also be done, or they will be susceptible to a man-in-the-middle attack [129], i.e., an eavesdropper pretending to be Alice to Bob and pretending to be Bob to Alice.

Since the original proposal of Bennett and Brassard, there has been immense progress, both experimentally and theoretically [130], with many quantum key distribution systems implemented [131, 132, 133, 134, 30], and even several demonstrations of quantum networks since 2003 [135, 136, 137]. Despite these remarkable achievements, both the rates and distances are quite limited, compared to classical communication. The primary reasons for this are that the detectors used typically run at low rates ($\sim$20 MHz for a typical avalanche

photodiode (APD)) and imperfect efficiency (60-70% for visible-light APDs, or significantly less for detectors at 1550 nm, a commonly-used wavelength due to its low loss in fiber), and photons experience significant loss through many kilometers of fiber. Of course, unlike the situation in classical communication, amplifiers cannot be used to overcome the loss (due to the no-cloning theorem [138]), though quantum repeaters [139] could be used to extend the range. The detector rate and efficiency can be addressed with better detectors, and there has been progress along these lines, such as high-rate InGaAs detectors [132], up-conversion detectors (exploiting the higher efficiency of detectors in the visible spectrum instead of the near infrared) [134], or superconducting detectors with very low dark count rates [140]. Some examples of QKD performance are 1.3 Mbits/s over 10 km of fiber [134], 1.002 Mbit/s over 50 km of fiber [133], 2.37 Mbit/s over 5.6 km of fiber (and 2.88 kbit/s over 100 km of fiber) [132], 15 bit/s over 200 km of fiber [30], and 12.8 bits/s over 144 km of free space [131]. The goal in this work is to use the information of *when* a detector receives a photon to generate a secret key at a higher rate (at the highest rate possible, given the detector performance).

5.2 Time-bin cryptography

5.2.1 Detector entropy

A quantum cryptography system can be thought of as a secure distribution of entropy (in the form of random bits) between two parties. In fact, in order for the protocol to be truly secure, the source of entropy must be quantum [130]. In a typical quantum cryptography experiment, this entropy is detected by one of two detectors firing (e.g., measuring a photon to be either horizontally or vertically polarized). Our approach is to increase the rate of quantum entropy by exploiting the full amount of entropy that can be detected by a single APD.

Let us first look at the problem of extracting entropy from a detector for the purpose of quantum random number generation. A simple way to implement

Figure 5.1: A random number generator, based on the path a photon takes after a beam-splitter (e.g., if the top detector fires, it is a '0', if the bottom fires, it is a '1').

such a system would be to measure the path of a single photon after a beam-splitter [141] (see Fig. 5.1). For each click on one of the detectors placed after the beam-splitter, there will be one bit of entropy generated. The rate will be limited by the saturation rate of the detectors (though running near the saturation rate would in practice cause several issues, due to detector deadtime, or both detectors firing at the same time). However, if we consider the signal that is coming out of a detector that is firing near its saturation rate under continuous illumination, we can extract far more than one bit of entropy per click, by using the exact timing of *when* the detector is seeing the photons (see Fig. 5.2). If the average time between detection events is 100 ns (neglecting deadtime, which may be 10-50 ns) and the detector resolution is 100 ps, the photon can arrive in approximately one out of 1000 time bins. The random selection of one out of 1000 possibilities allows for the extraction of $\log_2(1000) \approx 10$ bits per click (though the arrival-time distribution is not flat, but a decaying exponential). This approach has been used to generate random numbers at rates exceeding 100 Mbits/s, with a single-photon counting rate of <20MHz [142].

The maximization of entropy generation at a single detector can be extended to correlated entropy generation at two detectors by using a source of correlated single photons. Of course, SPDC is exactly such a source. In our QKD system, pairs of photons are randomly generated in time, and then detected by Alice and Bob with single-photon counters (see Fig. 5.3). The arrival times of their detected photons will be correlated, and they can extract an identical random signal after some classical error correction. With the addition of security checks

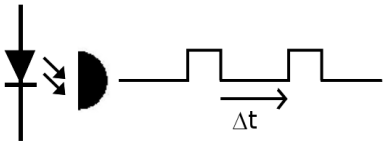


Figure 5.2: The exact amount of time between photon counts at a single detector can be used as a source of quantum random numbers [142].

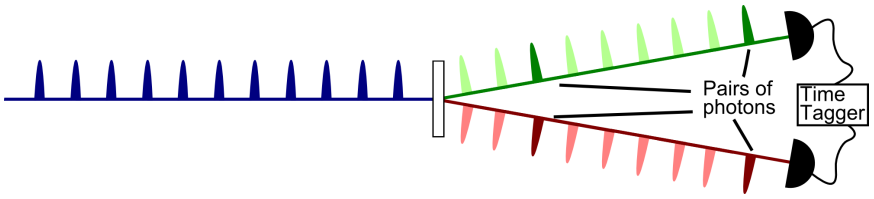


Figure 5.3: Pairs of photons are randomly produced from a pulsed down-conversion source, leading to correlations in the timing of the photons detected at the two sides.

to limit the information an eavesdropper could have, a secure quantum key distribution system can be realized. A system with this approach has been implemented before [143], but with only a small amount of entropy per photon (4 bits) and low overall entropy rate (<60 Hz), and security provided by a single unbalanced interferometer, which we do not believe is secure (see below). Furthermore, error correction was not done, so no final key was ever extracted.

5.2.2 Entropy extraction and error correction

For our source, we have pairs of photons going to Alice and Bob, which then leads to correlations in the arrival time of photons at their detectors. The state being generated for each pump pulse is:

$$|\psi\rangle = \sqrt{1-\epsilon^2}|0_A 0_B\rangle + \epsilon|1_A 1_B\rangle + \mathcal{O}(\epsilon^2). \tag{5.1}$$

We refer to each pump pulse where this state is created as a "time bin". A time bin is labeled as either '0' or '1' depending on the absence or presence of

the detection of a photon, on both Alice's and Bob's side. Using the standard formula for entropy [118], we have, for each time bin

$$H = \sum -p \log_2(p), \tag{5.2}$$

$$H = -(1-\epsilon^2)\log_2(1-\epsilon^2) - \epsilon^2 \log_2 \epsilon^2, \tag{5.3}$$

where H is the entropy, and p is the probability for any given outcome. To get the entropy per single photon, we multiply the per-bin entropy by the average number of bins between photons. For $\epsilon^2 = \frac{1}{1024}$,

$$H_{photon} = 1024 H_{timebin}, \tag{5.4}$$

$$H_{photon} = 1024(-\frac{1023}{1024}\log_2(\frac{1023}{1024}) - \frac{1}{1024}\log_2(\frac{1}{1024})), \tag{5.5}$$

$$H_{photon} = 11.4. \tag{5.6}$$

In the limit of no loss (a detection efficiency of unity), this is the number of bits of entropy that Alice and Bob will share for each pair of photons they detect (see Appendix D for more information on the calculation of entropy for our source).

After some measurement time, Alice and Bob will each have a long string of bits, with mostly 0s and a sparse amount of 1s (ϵ^2 could be $\sim 10^{-4}$ to 10^{-2}). However, because the overall heralding efficiency will typically be significantly less than one, the strings of Alice and Bob will usually contain a significant fraction of errors. The challenge is both to convert the string to a (shorter) string that is not sparse, and also correct the errors.

It was proven by Claude Shannon in his work published in 1948 on information theory that perfect error correction in such a signal is possible, with a fixed ratio of redundant bits (e.g., parity bits) that encode some error correction scheme [118]. Following this paper, we can calculate the mutual entropy between Alice and Bob, and determine the number of classical bits that must be sent publicly in order to correct all of the errors (note that this is not the same as determining a strategy that will allow us to actually do this efficiently). In classical digital communication, an error correction code that sends exactly the minimum required amount is said to reach the channel capacity, or Shannon

limit. Such error correction is now commonplace in classical digital communication, and many codes have been developed. Examples of some of them are the Reed-Solomon code (which is a simple and fast code, but does not approach the channel capacity), turbo codes (which can approach the Shannon limit), and low-density parity-check (LDPC) codes (which can also approach the Shannon limit). In LDPC, Alice sends the result of a series of parity bits[3] to Bob, with each parity bit sampling many signal bits, and each signal bit being sampled by many parity bits. In this way, multiple bit flips change multiple parity bits in a way that Bob can (almost always, if properly implemented) uniquely decode. For our error correction scheme, we use a variant of LDPC codes[4].

In most high-performance digital signals, the goal is to send information at as high of a rate as possible, limited by the signal/noise ratio of the channel (i.e., the channel capacity). LDPC codes (and others) can be very good at providing high-performance error correction, and signals can, in practice, be sent at a rate close to the channel capacity, even for significant error rates. After Alice and Bob have detected their photons, and converted the arrival times into a series of 0s and 1s, we can consider this as a noisy digital channel, with Alice sending Bob a message, but with a significant error rate. However, this channel is very different from a typical classical channel, since it is mostly 0s, with only a few 1s; this is known as a "sparse" channel. Due to this asymmetry, typical LDPC codes cannot be applied (at least not in a way that approaches the channel capacity). However, it is still possible to apply a variant of LDPC to our signal.

The first step in our error correction scheme is to choose "frames", a set of a fixed number of bins (e.g., 1024, for ∼10 bits per photon). Alice and Bob announce publicly the number of photons they received in each frame. Let us first consider the cases where they each detected one photon in a particular frame. The arrival time in this frame of 1024 bins can be treated as a symbol

[3] A parity bit is set by whether the number of bits with the value of one in a set is even or odd.

[4] Turbo codes could also be used, but we chose LDPC for its simpler design and implementation (and lack of potentially-encumbering patents).

from a 1024-letter alphabet. Now, again considering only the frames where both parties detected one photon, they each have strings of random characters from a 1024-letter alphabet, and it is no longer a sparse channel (though the error rate may still be high). On this signal, we can use a high-alphabet LDPC code, which works similarly to the binary LDPC code (i.e., with only a two-letter alphabet).

If there is more than one photon (for either Alice or Bob) in the frame, our approach is to divide the frame into subframes (and then announce the photon number in each subframe), until both sides have one photon in the subframe. We then apply an LDPC code with an alphabet size corresponding to this frame size.

Due to the aggressive nature (i.e., we are sending close to the bare minimum number of parity bits) of our initial LDPC code, we will still have a $\sim 10^{-4}$ error rate. This can be corrected with an additional round of LDPC error correction, bringing the error rate down to $\sim 10^{-9}$ (or lower, if necessary). Once we have established the photon timings with this method, Alice and Bob can implement a standard BB84 error-correction scheme to recover the bits from polarization correlations [126], and apply standard privacy amplification [127] to remove any information Eve may have about the signal. With this approach, we estimate that our final signal will have approximately 80% of the entropy compared to the Shannon limit.

5.2.3 Security

The simplest attack on this protocol would be for Eve to detect the photon Alice sends to Bob, and then send a photon on to Bob in the same time bin. In this way, Eve gains full knowledge of the key, but introduces no errors. Our initial implementation of a security check is designed to detect this attack, by using polarization entanglement of the photons, similar to previous cryptography experiments [144, 23, 24, 25]. In order for Eve to successfully mount her attack against photons that are also entangled in polarization, she would have to use a

polarization-insensitive non-demolition measurement, which is not possible with current technology (though, it must be noted, is possible in principle). A security system that would be robust against a more general quantum attack would have to check correlations in a basis conjugate to timing, by either looking at frequency correlations or directly measuring the phase between time bins.

There is an additional approach to security which we have only recently begun to consider. It is briefly mentioned here for completeness. The approach is to consider the basis states being sent to Bob as either zero or one photon (instead of a single photon in one of many time bins). Referring back to Eq. 5.1, we can see that this is indeed the basis Alice is projecting into, if she measures the photon number on her side. The conjugate basis for this is then a superposition of zero and one photon, with a definite phase between them. This can be closely approximated by a weak coherent state, and then measured on Bob's side with homodyne detection [114]. The full ramifications of this approach are not yet clear, but it appears to be a possible alternative to measuring in a basis conjugate to the time bins.

Polarization security

With the entangled state we are generating ($|HH\rangle + |VV\rangle$), the polarization measured in the linear basis should always be the same on both sides. If Eve attempts the intercept-and-resend attack, it will disturb these correlations. The quality of these correlations are quantified by using the visibility, which is defined in, e.g., the H/V basis as:

$$Visibility = \frac{HH + VV - VH - HV}{HH + VV + HV + VH}, \tag{5.7}$$

where HH is the counts for both sides measuring H, VV for both measuring V, etc. (the definition is similar for the D/A basis; good visibility in both bases is required). In the ideal state HH+VV, the coincidences of VH and HV will never be measured, leading to a visibility of unity. In practice, these coincidences will always occur at some level. Some possible causes are detector

background or dark[5] counts, temporal distinguishability of the photons (due to different group velocity between the pump and down-conversion photons), crosstalk in our polarizers, imperfect rotation with the waveplates, and slight polarization deviation in the down-conversion production due to the "Migdall effect" [145, 146] (note that since we are coupling into single-mode fiber, the common problem in free-space systems of distinguishability due to spatial mode is not an issue [45]).

Any deviation in visibility from unity must be assumed to be caused by an eavesdropper. In the intercept-and-resend attack that we are protecting against, the fraction of information Eve gains is equal to twice the decrease in visibility [130] (i.e., a visibility of 99% corresponds to Eve knowing the polarization (and therefore, we must assume, timing) of at most 2% of the photons [147]). Note that our hybrid scheme (securing timing information by checking in the polarization basis) is still under investigation, and therefore could have some theoretical weakness.

Time-bin superposition measurements

In order to be secure against a general quantum attack, we will need to implement a security check in a basis conjugate to the time-bin basis. Conceptually, the simplest approach would be to project into a complete mutually-unbiased basis, with each basis state in a superposition of all time bins from a frame (see Section 5.2.2), with either positive or negative phase between the terms:

$$|\psi\rangle = \sum_n a_n |t_n\rangle, a_n \in \{-1, 1\}, \tag{5.8}$$

where $|t_n\rangle$ is a single photon in time bin n. In practice, this would require many stabilized interferometers and detectors, with either postselection or fast

[5]Dark counts are the counts a detector will see without any light hitting it, due to, e.g., a thermal excitation of an electron; background counts arise from real photons, but not from down-conversion (e.g., from fluorescence from the laser). The two are sometimes used interchangeably; however, the background is typically proportional to the laser power, while the dark count is independent of it.

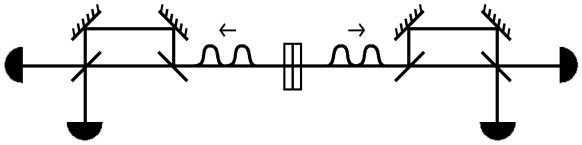


Figure 5.4: A Franson interferometer. Due to the path imbalance, there is no interference on one side, but there are still correlations in the outcomes between the two sides, due to nonlocal correlations of the presence of photons in different time bins.

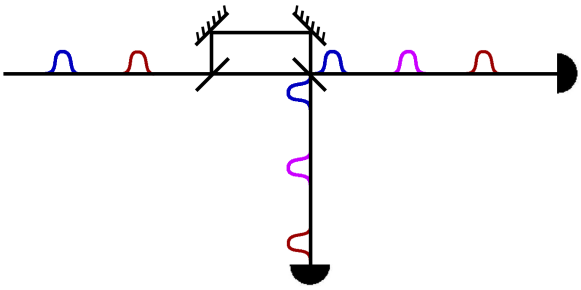


Figure 5.5: The state going into and out of Bob's Franson interferometer. The color is just for labeling the time bins–the pulses indicated are all the same wavelength.

switching, and would be difficult to implement. Let us consider an alternative way to limit the action of an eavesdropper.

A measurement done by Eve on the precise timing of a photon could be detected by using an unbalanced interferometer on both Alice's and Bob's sides (see Fig. 5.4) (this type of interferometer, with nonlocal correlations, is sometimes called a "Franson interferometer" [148]). If Alice detects a click in one of her detectors, she knows a photon was created in one of two time bins (depending on which path the photon took), and so prepares a state such as $|t_0\rangle + |t_1\rangle$ on Bob's side. When this state reaches Bob's interferometer, there are four possible outcomes (see Fig. 5.5): (1) the leading part of the state can take the short path of the interferometer (red), (2) the trailing part of the state can take the long path of the interferometer (blue), (3) the leading part of the state can

take the long path (purple), and (4) the trailing part of the state can take the short path (also purple). Possibilities (1) and (2) are in distinct time bins, and will not interfere (so no useful information is gained). However, possibilities (3) and (4) have terms arriving at the beam-splitter at the same time, so they can interfere (as suggested by red and blue combining to make purple). Alice and Bob compare which detectors fire at the same time, and can thereby determine the visibility of these correlations, exactly the same as they can determine the visibility of polarization correlations. If Eve attempts to completely localize the photon sent to Bob, this interference between time bins will not happen, and the visibility will drop.

As with polarization, perfect visibility guarantees perfect security. When Alice prepares the state $|t_0\rangle + |t_1\rangle$ (by measuring a photon at t=0 on her side, with a path imbalance of precisely one time bin), Alice and Bob are essentially measuring the coherence between time bins 0 and 1. If Alice prepares the state $|t_1\rangle + |t_2\rangle$ (by measuring a photon at t=1 on her side), Alice and Bob are now measuring the coherence between time bins 1 and 2. If bins 0 and 1 are perfectly coherent, and bins 1 and 2 are perfectly coherent, we can infer that bins 0 and 2 are also perfectly coherent. We can continue this inference of the phase to guarantee coherence across all of the time bins.

The visibility of the Franson interferometer will of course not be perfect, so we need to put limits on the knowledge Eve could gain, given a certain visibility. Unfortunately, calculating the information gained from an arbitrary quantum attack is quite difficult [149]. I will describe two approaches we have used, one to put a threshold on the minimum amount of information Eve could get, and one to put a threshold on the maximum amount of information she could get.

A minimum amount can be determined by the information that would be gained using a specific attack. Let us consider what happens if Eve localizes the photon to several time bins, instead of localizing to one time bin. There is then a chance she will not disturb the time-bin superposition state, and not be detected. For example, Eve might measure the photon going to Bob, and

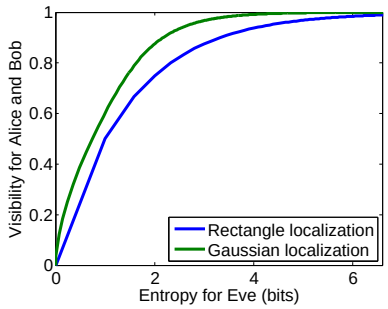


Figure 5.6: Visibility of the Franson interferometer (i.e., detectability of Eve) vs the uncertainty of Eve's localization (this uncertainty is approximately $\log_2(k)$, where k is the number of bins into which Eve is localizing, as in Eqs. 5.9 and 5.10).

project it into a superposition of k time bins (neglecting normalization):

$$|\psi\rangle = \sum_{n=0}^{k-1} |t_{n_0+n}\rangle. \tag{5.9}$$

In this case, she will get most of the timing information (all but $\log_2$(k) bits), but she will only disrupt the interferometer if the photon happens to be on the edge of her localization, i.e. in the states $|t_{n_0-1}\rangle + |t_{n_0}\rangle$ or $|t_{n_0+k-1}\rangle + |t_{n_0+k}\rangle$. This would correlate to a drop in visibility of 1/k (e.g., if $k = 4$, the visibility would be at most 0.75).

A flat distribution such as in Eq. 5.9 is not the only kind of projection Eve could do. Another localization she might try is a Gaussian (again neglecting normalization):

$$|\psi\rangle = \sum_{n=-\infty}^{\infty} e^{-n^2/(k/2)^2} |t_{n_0+n}\rangle. \tag{5.10}$$

Since the parameter k is not quite equivalent in the two equations (it is the total width for the flat distribution, compared to the full width at $1/e^2$ probability for the Gaussian distribution), we should compare the different effects on visibility, compared to Eve's uncertainty (measured in entropy, i.e., bits) on the position of the photon after her measurement. Fig. 5.6 shows the trade-off of visibility

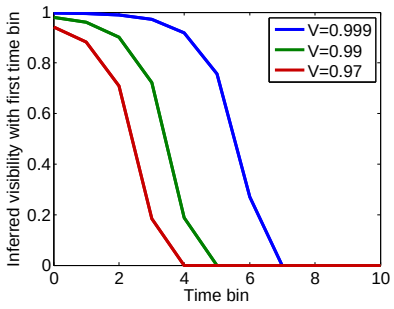


Figure 5.7: Guaranteed visibility between non-adjacent time bins, using only the visibility from adjacent time bins, for different values of the initial visibility.

disturbance vs uncertainty for the two distributions in Eqs. 5.9 and 5.10. As we can see, the Gaussian localization is a significantly better strategy for Eve. For example, if Eve's measurement lowers the visibility from 1 to 0.99, she has an uncertainty of 3.9 bits with the Gaussian distribution (corresponding to the photon being localized to about $2^{3.9} = 15$ time bins), compared to 6.6 for the flat distribution (corresponding to the photon being localized to about $2^{6.6} = 97$ time bins).

Since the goal is unconditional security, we really want to establish the maximum amount of information an eavesdropper could have, not just demonstrate what she might know with a given strategy. To do that, our approach is to determine some limits on the state itself, from the measurements we have. Let us assume we know the visibility between time bins 0 and 1, and also between 1 and 2. This allows us to put some limits on the density matrix of this part of the state. Given this density matrix, we can determine the minimum visibility between time bins 0 and 2. With this known visibility, we can then repeat the strategy to determine the minimum visibility between 0 and 3, 0 and 4, etc. In this way, we can determine the minimum visibility between any two non-adjacent time bins, by only measuring adjacent time bins. While this does not tell us the precise amount of information Eve could possibly know, it does place an upper bound on her information. This calculation is ongoing, but some initial

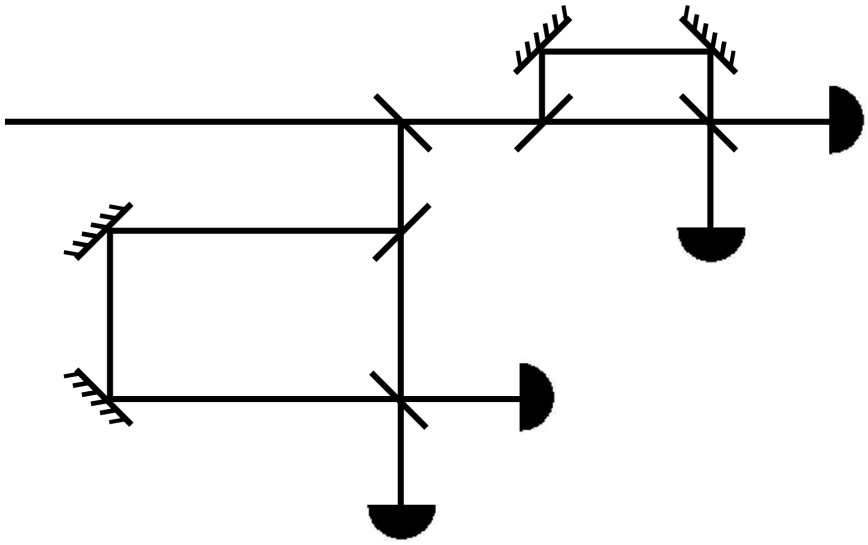


Figure 5.8: Two Franson interferometers, with different path-length imbalances. An incoming photon is randomly directed into one of the interferometers by a passive beam-splitter.

results indicate the guaranteed visibility drops quite quickly (see Fig. 5.7).

We now have some limits for Eve's knowledge. Unfortunately, even the minimum amount of information Eve might have does not give us security across enough time bins with a realistic visibility (approximately 15 time bins, for a visibility of 99%) to yield the performance we want of up to 1024 time bins per frame. The next step to improve the security is to use multiple interferometers. For example, let us consider a setup such as in Fig. 5.8. In this case, there are two Franson interferometers on each side. When Alice's photon and Bob's photon both pass through identical interferometers, and arrive at the same time, then we should see correlations. Let us assume the imbalance in the first interferometer is one time bin (so this interferometer is measuring the coherence between adjacent bins), and that the imbalance in the second interferometer is ten time bins (so this interferometer is measuring the coherence between bins separated by ten time bins). Given that a single interferometer (with 99%

visibility) guarantees security across approximately 15 time bins, the second interferometer can be thought of as guaranteeing security across approximately 150 time bins, but only sampling every 10th bin. The first interferometer then provides security between these bins.

To see this another way, let us look at it from Eve's perspective. If Eve attempts the same measurement as in Eq. 5.10 (with a large enough window that it does not significantly disturb the visibility of the first interferometer), this will now be detected as a disturbance in the second interferometer. Eve could change her projection, so it does not disturb the second interferometer, by separating the bins she projects into by ten (see Fig. 5.9(a)):

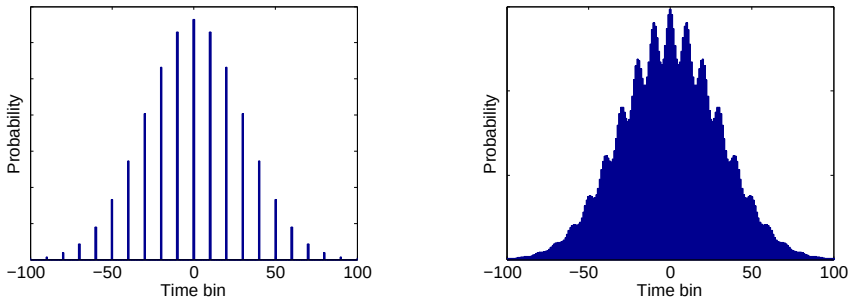
$$|\psi\rangle = \sum_{n=-\infty}^{\infty} e^{-n^2/(k/2)^2} |t_{n_0+10n}\rangle. \tag{5.11}$$

Now, of course, Eve is disturbing the first interferometer. Eve must combine both projections, so she does not disturb either (see Fig. 5.9(b)):

$$|\psi\rangle = \sum_{n=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} e^{-n^2/(k/2)^2} e^{-m^2/(k/2)^2} |t_{n_0+10n+m}\rangle. \tag{5.12}$$

With this measurement, Eve will not be detectable (assuming she chooses her projection widths correctly). However, the photon going to Bob is now projected into approximately k^2 time bins, instead of just k time bins (leaving Eve an uncertainty of $\log_2(k^2)$ bits instead of $\log_2(k)$ bits). This extra factor of k is due to the second interferometer. As Alice and Bob add interferometers, the number of bins Eve must project into scales exponentially, leaving her with more uncertainty of the photon position. This means the approach of multiple interferometers is a scalable way of guaranteeing security.

To summarize, we are guaranteeing the security over a certain number of time bins by measuring the visibility of a Franson interferometer. We have shown a lower bound and initial results for an upper bound for the amount of information an eavesdropper may know, given a certain visibility. We have also shown that the amount of bins secured can be extended exponentially by adding more Franson interferometers (this is true for both the upper and lower



(a) (b)

Figure 5.9: The superposition Eve projects into after applying the strategy in (a) Eq. 5.11 and (b) Eq. 5.12 ($k = 12$, so this projection would lower the visibility by about 1.5%).

bounds). Further work is needed to find the exact amount of information Eve could have using a general quantum attack, given only visibility measurements.

5.2.4 Experimental setup

The experimental setup was based on fiber-coupled SPDC with polarization entanglement, with optimized spatial and spectral heralding, as discussed in Chapter 2 (the basic experimental diagram was the same as Fig. 5.3, but with a double crystal for polarization entanglement)[6]. The pump laser was a Paladin Compact 355-4000 Air-Cooled from Coherent, which is a mode-locked Nd:YVO_4 laser with a 120-MHz repetition rate with 355-nm 5-ps pulses, at an average power of 4 W. The optimal singles/coincidence ratio was measured to be 48.5%, when collecting one polarization. When two polarizations were collected, the

[6]For this source, we used a double-crystal configuration [38], with two 600-μm BiBO crystals [62]. The pump beam waist at the crystal was approximately 500 μm in diameter, and the collected down-conversion modes were approximately 108 μm at the crystal. The down-conversion modes were collected with 250-mm focal length lenses, then coupled into single-mode fibers with 11-mm focal length collimation packages.

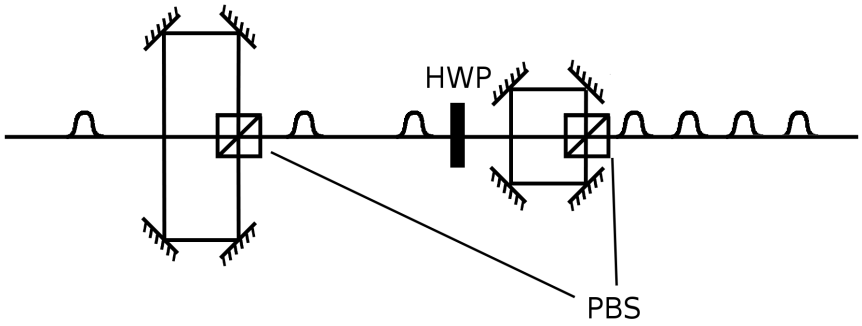


Figure 5.10: Repetition-rate multiplier, in which each pulse is turned into 4. In each cavity, the vertically-polarized component is delayed relative to the horizontally-polarized component. Between delay lines, a waveplate rotates the pulses so they both have equal amplitudes of horizontally- and vertically-polarized light. HWP: half-wave plate @22.5°. PBS: polarizing beam-splitter.

optimal collection is different for each polarization[7], so we chose the collection to be between the individual optimal points, leading to a singles/coincidence ratio of up to 40%.

The detectors we have been using (PerkinElmer SPCM-AQR-14) have a timing jitter of approximately 1 ns. That means our source should be pulsing at less than 1 GHz to prevent time-bin crosstalk, but not too much lower, so we can still come close to saturating the detector timing resolution. To increase our repetition rate from 120 MHz, we used two delay lines, each of which doubled the repetition rate (see Fig. 5.10). The initial pulse is incident on a polarizing beam-splitter, at diagonal (or antidiagonal) polarization, such that half of the light is transmitted and half reflected. The half that is reflected is delayed for half of the separation time between the incident pulses, and then sent back into the other port of the PBS, so that it reflects into the same mode as the

[7]The two polarization modes were approximately 42 μm apart at their waists due to transverse walk-off in the crystal from the non-collinear nature of the down-conversion. This could be addressed with either polarization-dependent mode collection, or a larger spot size for the pump and the down-conversion light (which would, however, lower the brightness).

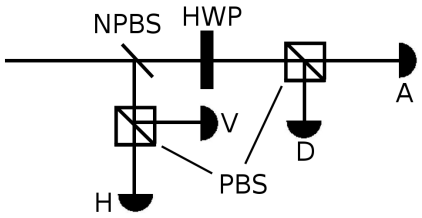


Figure 5.11: After coupling out of the single-mode fiber into free space, the single photons are split into two modes on a non-polarizing beam-splitter, and then each of those is split into two more modes with a polarizing-beam-splitter, so photons are randomly measured in either the H/V or D/A basis. HWP: half-wave plate @22.5°. PBS: polarizing beam-splitter. NPBS: non-polarizing beam-splitter.

original beam. Now there are two pulses leaving this PBS for each pulse incident (though the leading pulse is horizontally polarized, and the trailing is vertically polarized). With a waveplate that rotates horizontal (vertical) polarization to diagonal (antidiagonal), both pulses again have equal parts horizontal and vertical, and this process can be repeated. Our current repetition rate is 4*120 MHz=480 MHz, near the desired rate with our present detectors. Eventually, detectors with a resolution closer to 100 ps may be used, which would require the repetition rate to increase to several GHz.

Now that we have a source that is producing pairs of polarization-entangled photons at a high brightness in a large number of time bins, we need a measurement system. Ignoring polarization for the moment, this can simply be done with one single-photon counter on each side. In our experiment, we recorded the arrival times of the clicks from the detectors using a V1290N 16-channel time tagger from CAEN, with a 25-ps resolution. This device allows us to record the arrival time of photons at 8 detectors, running near their saturation rate, onto a computer.

For securing the channel by monitoring the polarization correlations (see Section 5.2.3), a more complicated detector setup is required. For this case, we

need to be able to simultaneously measure in two "mutually-unbiased" bases (e.g., in the H/V basis and the D/A basis). This could be done with a single detector and fast switchable polarizer (e.g., a Pockels cell followed by a fixed polarizer), but in order to be secure, the setting must be randomly chosen for every photon, which would be very challenging to implement experimentally. Instead, the polarization basis choice can be made passively, using a non-polarizing beam-splitter (NPBS). In one port of the NPBS, the photon is measured in the H/V basis, and in the other it is measured the D/A basis (for a total of 4 detectors each for Alice and Bob) (see Fig. 5.11). We use Brewster-angle polarizing beam-splitters to minimize the loss ($\sim$1%) and crosstalk ($<$0.1%). After the polarizers, we couple the light into multi-mode fibers (since the light is already spatially filtered, there is no need to use a single-mode fiber, which is more difficult to align and would introduce slightly more loss). The additional loss from the extra optics (primarily the uncoated multi-mode fibers) reduces the heralding efficiency to about 30%.

5.2.5 Experimental performance

We have done a full experimental implementation of this system (with the exception of the error correction, which is near completion), and have the performance shown in Table 5.1. In this table, we show data for both high and low power, which demonstrates that we can get a high number of bits per coincidence with a low flux (i.e., many bins between clicks), and a very high rate at full power (note the average visibility[8] is lower at full power due to accidental coincidences from multiple pairs of different polarization being produced at the same time; this is reduced by increasing the repetition rate, since the same numbers of pairs are distributed into more bins). We also show numbers both with and without our repetition-rate multiplier. Note that this data was taken before implementation of our full detection system, so there was only one detector per side (which essentially cuts the entropy generation rate in half).

[8]Defined as the average of the visibilities in the H/V basis and D/A basis (see Eq. 5.7).

Low power			
Repetition rate	120 MHz	240 MHz	
Singles	31.6 kHz	55.5 kHz	
Coincidences	10.9 kHz	19.1 kHz	
Average visibility	0.990	0.985	
Entropy per coincidence	8.99 bits	9.79 bits	
Entropy per second	98.0 kbits	187 kbits	

Full power			
Repetition rate	120 MHz	240 MHz	480 MHz
Singles	1.75 MHz	1.33 MHz	1.11 MHz
Coincidences	496 kHz	385 kHz	336 kHz
Average visibility	0.932	0.966	0.977
Entropy per coincidence	3.14 bits	4.83 bits	6.13 bits
Entropy per second	1.57 Mbits	1.86 Mbits	2.06 MBits

Table 5.1: Data taken with our time-bin QKD system, for both low and full power levels and different multiplication of the laser repetition rate.

5.2.6 Future work

Our current source is approaching the limit of the correlated entropy generation for a single pair of detectors, but there is still some room for improvement. We can increase the repetition rate of the laser another factor of two (to 960 MHz), which will saturate the detector timing entropy, but also start to cause time-bin errors (which can be corrected, with a modification of our LDPC code). We can also increase the pair production rate up to the saturation rate of the detectors (about 10 MHz). We estimate that the heralding efficiency can be increased to about 47% (from about 30%) with anti-reflection-coated fibers and optimized collection for both polarizations. These changes would increase the secure entropy generation rate of a single channel to about 19 Mbits/s. Beyond this, we are going to have to either use different detectors, add more channels, or both. Detectors with lower jitter exist (which can generate more timing entropy per click), but they typically have lower efficiency (which then lowers the entropy). We are currently only collecting a small part of the light generated around the down-conversion cone, and it is possible to collect at different positions to implement additional channels with the same source. Based on the size of the lens diameter in our current collection (12.5 mm), and the circumference of the ring cross section at this point (∼82 mm), 6 channels could potentially be implemented, bring the overall rate to 114 Mbits/s. It is also possible to collect multiple frequency ranges to get another factor of 3-5 (based on the useable bandwidth of our detectors), although we have not tested this experimentally.

Appendix A

EXPERIMENTAL PROCEDURES

A.1 Down-conversion alignment

In this section, I discuss some of the experimental techniques used for aligning down-conversion for optimized coupling into fiber. In our optimized system (see Section 2.2.2), we should have the waists of the pump and collection beams centered at the crystal, and they should be small in order to maximize the brightness [46] (but not too small, see Appendix B). The first step is to shape the pump beam to have the desired size at the desired position (i.e., the center of the crystal).

To control the size and position of the beam at the crystal, we want to control the beam that is incident on the lens focusing onto the crystal, and also the position of that lens. A collimated beam incident on a lens will be focused down to a spot of an easily-predictable size[1] (it is more difficult to control, both experimentally and theoretically, if the focus of the incident beam must be taken

[1] $w_f = \frac{\lambda f}{\pi w_i}$, where w_i, w_f are the initial and final beam waists, respectively, λ is the wavelength, and f is the focal length; this formula assumes paraxial Gaussian beams.

into account as well). If we have a collimated beam, we can decouple the two parameters of the beam (the size and position of the focused spot). The size will be controlled by the size of the beam at the lens (and the focal length of the lens), and the position will be controlled by the position of the lens.

A beam can be made precisely collimated by first focusing it down with a lens, and then controlling the position of a second lens. If we monitor the focus aberration [150] using a wavefront sensor (we use a HASO 32 from Imagine Optic) while moving the lens (by mounting it on a translation stage), we can precisely control the collimation of the beam. The size of the collimated beam can be controlled by selecting the two lenses used to focus down the beam and collimate it. With this collimated beam, we can now precisely control the alignment of the pump spot on the crystal, by translating a lens with the desired focal length along the path of the beam. Let us now move on to initial alignment of the collection system.

For the collection modes, we work with an alignment laser (with the same wavelength as the down-conversion photons) coming out of the collection fiber, so it is propagating the opposite direction as the down-conversion light. This allows for a beam in exactly the same spatial mode as we the one into which we are collecting. Our approach for precisely controlling the collection beam modes is the same as for the pump: start with a collimated beam, and then control the position at the crystal with a focusing lens. In the case of coming out of a fiber, the initial collimation can be done with a single aspheric lens. For this purpose, we use a CFC-11X-B adjustable collimation package from Thorlabs, and again use a wavefront sensor to monitor the focus of the alignment beam. The position and direction of the collimated beam going into the crystal can be controlled either with two mirrors with 2-axis rotation (tip/tilt) control, or with the collimation package on a mount with 2-axis rotation and 2-axis position control. The former is more difficult to align (since the position of the beam cannot be controlled without disturbing the direction), but is significantly cheaper.

The first step in the alignment of the light from down-conversion is done with

the collection beams collimated when they are incident on the crystal (but the pump is still focused down). The alignment beams are set so they are hitting the correct position (the same spot of the crystal that the pump is hitting) and the correct direction (parallel to the table, at the correct angle for the opening angle of the down-conversion light, typically $\sim 3^\circ$). The fibers are then connected to single-photon counters. With the pump beam on, the crystal is rotated slightly (about which axis this rotation is done depends on the phase-matching conditions, i.e., the cut of the crystal). Singles counts should be seen (removing the spectral filtering for this step may make the signal easier to see), and then optimized on one side by iteratively changing the direction of the collection beam and direction of the cone, until the counts are maximized (this will mean the collection and down-conversion are pointed along the same direction). Now, coincidence counts should be optimized by changing the position and direction of the other side, until maximized.

Next, the lenses to focus the collection beam into the crystal are put in place, one focal length away from the crystal. The transverse position of the lens on one side is optimized until the singles counts are maximized, and then the lens on the other side is optimized until the coincidences counts are maximized. At this point, all of the beams are overlapping in position and direction at the crystal, and the only remaining uncertainty is the position of the crystal relative to the beam waists. We can optimize the position of the pump waist by moving it along the path of the beam until the singles counts are maximized (at this point, the intensity of the pump at the crystal is the brightest, which means the beam waist is at the crystal). We can then scan the position of the lenses in the path of the collection beam so the heralding efficiency is maximized. Alignment of the spatial mode filtering is now complete.

Alignment of the spectral mode filtering is much easier. If an interference filter is used at normal incidence, the alignment is trivial. If the interference filter is to be tilted (see Section 2.2.1), then some consideration is needed. Tilting the filter on, e.g., the signal side lowers the upper edge of the spectral filter for that side, to match the lower edge of the filter on the idler side. For example,

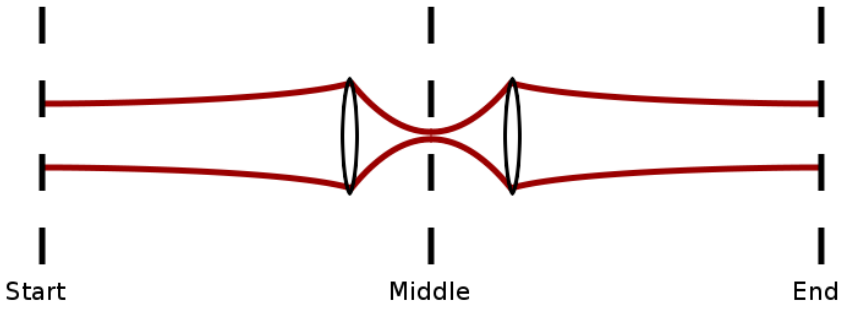


Figure A.1: A symmetric cavity design. The beam is collimated going into the cavity, and then collimated again after a pair of focusing lenses, positioned symmetrically about the center of the cavity. By symmetry, the beam must be the same size and focus at the end of the cavity as the start. Note that this diagram has the path unfolded; in reality, the start and end will be at the same location.

with a 710-nm pump and a desired 20-nm bandwidth, the bandwidth will be (approximately[2]) 700-720 nm on both the signal and idler side. The lower edge (700 nm) is set by a filter at normal incidence, and the upper edge is then set by a filter with an edge higher than 720 nm (e.g., 725 nm). When we lower the upper edge of the signal filter from 725 nm to 720 nm, it will not reduce any coincidences, but only the singles. When the coincidences begin to decrease, we know the filter is at the correct angle. Note that this tilt is polarization dependent, and (at least for the Semrock filters we used), the bandwidth is shifted a larger amount for s polarization (i.e., vertical polarization, assuming the filter is tilted about the vertical axis).

A.2 Aligning storage and delay cavities

For the single-photon source (Chapter 3), a stable, switchable cavity is needed. Our design approach is shown in Fig. A.1. The collimation of the beam going into it is set using a wavefront sensor, as detailed in Section A.1. Two lenses (or curved mirrors) are positioned symmetrically about the center of the path length of the cavity. The exact distance between them is then tuned using a wavefront sensor as feedback to make the beam collimated again after the lenses (more specifically, that the waist of the collimated beam is at the end of the cavity). By symmetry, when the beam returns to the start of the cavity, it has the same amount of focus (i.e., none), and the same size.

The position and the direction of the beam after a pass in the cavity must also be the same as the position and direction of the original beam. This can be tuned using two mirrors in the cavity, and monitored using a wavefront sensor, looking at the tip/tilt aberrations of the beam.

To align the delay cavities which increase the laser repetition rate (see Section 5.10), we follow a similar strategy. In this case, stability of the spatial mode through multiple passes is not an issue, since the longest total path length is the length between pulses ($\frac{c}{120MHz} = 2.5$ m). If the Rayleigh range of the beam is much longer than this distance, focusing in the delay line is not needed. We can make this the case by using a large diameter collimated beam (∼5-mm diameter) as the input to our delay line. The Rayleigh range is then $\frac{\pi w_0^2}{\lambda} = 55$ m (which is much more than the maximum 2.5-m delay). Aligning the position of such a large beam is easily done by eye, but it is much more sensitive to angle deviations. We set this using a motorized tip/tilt mirror mount (Newport Agilis AG-M100N), and looking at the down-conversion counts (though a wavefront sensor could also be used).

[2]The energy of the two down-conversion photons is not linear with the sum of their wavelengths, but the sum of their frequencies.

Appendix B

DOWN-CONVERSION WALK-OFF

When working with birefringent materials, it is important to consider the effects the polarization has on the pump position, both temporal and spatial. In a noncollinear double-crystal down-conversion setup, it is also important to consider the separation of the two beams from different crystals. In this section, we quantify these effects, and determine corrections for them. A good reference for the effects discussed in this section (and how it affects type-I down-conversion) is [151].

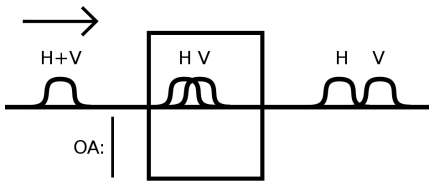


Figure B.1: A pulse propagating through a birefringent crystal exhibiting temporal walk-off. The optic axis (OA) is parallel with the V-polarized light. Since both ordinary and extraordinary polarizations are present, the two pulses separate from each other due to the different group velocities.

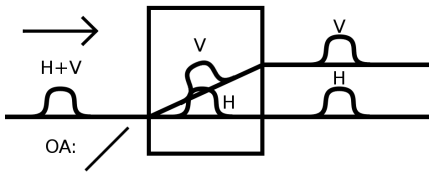


Figure B.2: A pulse propagating through a birefringent crystal exhibiting spatial walk-off. The optic axis (OA) is in the plane of the figure, but not completely parallel with the V polarization. The extraordinarily-polarized pulse undergoes birefringent walk-off. In general, the pulse will also have some temporal walk-off, but that is not indicated here.

The first effect we will look at is temporal walk-off (see Fig. B.1). In the simplest case, the optic axis (OA) is along the direction of the vertical polarization. While the separation between the pulses is small (340 fs at 355 nm for 600 μm of BBO), it can be significant with an ultra-short pulse (e.g., the laser used in the cryptography experiment in Chapter 5 has a pulse width of 5 ps). This effect will be present in each of the two down-conversion crystals, for both the pump and down-conversion light (but with different amounts), and must be compensated for. Without a compensation crystal, our visibility for the source in Chapter 5 is 98%, while with a compensation [151] crystal we were able to get >99.5%.

In addition to the temporal separation of pulses in a birefringent crystal, we also need to take into account spatial walk-off (see Fig. B.2). This is due to the asymmetry of how the wavefronts of the beam propagate in a birefringent material [33]. Under tight focusing conditions, this effect must be considered. For example, in a 600-μm crystal of BBO with the optic axis at 33.7° (the phase-matching angle used for our source), the spatial walk-off for a 355-nm pump is 45 μm. If our focused pump spot is much large than this ($\sim$500 μm) we can ignore this effect. The birefringent walk-off will also be significant for the down-conversion beams. However, even though we are focusing tightly enough ($\sim$100 μm) that we cannot ignore the walk-off, it turns out to have no effect.

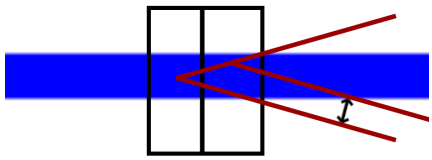


Figure B.3: The down-conversion beams coming from the two different crystals. Note that if we are collecting into a certain mode on one side, the heralded mode on the other side depends on which crystal in which it is created.

This is because it merely changes which parts of the pump beam are being collected, and it is not a problem if the horizontally-polarized photons are being collected from a different part of pump as the vertically-polarized photons.

One other walk-off effect we need to consider is due to the noncollinear nature of our two-crystal setup, as shown in Fig. B.3. Consider the pair being created from the center of the pump beam in the first crystal. When we detect a photon from this crystal in this mode, we know the conjugate photon must be in the bottom path shown in the figure. When we detect a photon in the top mode, but from the other crystal (i.e., the other polarization), then the conjugate photon is heralded into a different spatial mode. In our case, with a $\sim 3^{\circ}$[1] half-opening angle for the cone and 600-μm-thick crystals, the walk-off between the two heralded modes is 40 μm (compared to a beam waist of $\sim$100 μm). Our current strategy is to collect between the two modes, which lowers the heralding efficiency from about 49% to 38%. However, it is possible to compensate this effect (which would allow for no decrease in heralding efficiency), either with a birefringent crystal to induce an opposite spatial walk-off, or with a birefringent wedge after the collimating lens. Since the action of a lens is to do the Fourier transform, an angular deviation at one focal length before the lens will be projected to a displacement in position one focal after the lens. A birefringent wedge will create a polarization-dependent angular deviation, which will then be a polarization-dependent displacement after a lens.

[1] The angle is measured with respect to the cone in free space, not inside the crystal.

Appendix C

SOURCE PERFORMANCE CALCULATIONS

C.1 Single-photon source

C.1.1 Deriving calculations

In this section, I discuss the calculations used to determine the performance of the single-photon source in Chapter 3. I assume a Poissonian distribution for the number of pairs produced, which is valid if the number of modes is large. If there is only one mode (i.e., an unentangled source), then the distribution would be thermal [88]. For these calculations, I also assume a single pulse stored in a cavity (with per-pass transmission T_{Pump}) is used to pump the crystal (as in the 40 kHz laser used for the source in Chapter 3). The calculations can be adapted for a high-rate pulsed laser (as in the 120 MHz laser used in Chapter 5) by setting T_{Pump} to unity.

The outcome of any given trial of our down-conversion source depends on

when the heralding signal photon(s) is detected. In the general case, any number of heralding photons may be detected, but exactly which are used depends on the number of times we can switch the cavity in a given trial. If we can only switch once, then we always use the first pair that is produced, and if we can switch an unlimited number of times, we always use the last pair that is produced. Let us first consider the case of switching only once.

The approach for this calculation is to determine the probability of any given pulse being used, and then to determine the different outcomes from that pulse. Since we always use the first pair produced, using the outcome of pump pulse N first relies on detecting no heralding photon from pulses 1 to $N-1$, and also detecting at least one heralding photon from pump pulse N. The overall output then depends on the pairs produced from pump pulse N, and the transmission of the remaining optics:

$$\begin{aligned} P_{0\ photons} =& P_{No\ detected\ pair,\ 1\ to\ N_{Total}} + \sum_{N=1}^{N_{Total}} (P_{No\ detected\ pair,\ 1\ to\ N-1} \\ & \times \sum_{m=1}^{\infty} P_{m\ pairs\ produced} P_{\geq 1\ pair\ detected} P_{All\ photons\ lost}), \\ P_{1\ photons} =& \sum_{N=1}^{N_{Total}} (P_{No\ detected\ pair,\ 1\ to\ N-1} \\ & \times \sum_{m=1}^{\infty} P_{m\ pairs\ produced} P_{\geq 1\ pair\ detected} P_{All\ but\ 1\ photon\ lost}), \end{aligned}$$

where N_{Total} is the number of pump passes before switching the down-conversion light out of the cavity. Let us look at each term in detail. For $P_{0\ photons}$, the first term is the probability of no pairs being produced at all, in which case the output is of course zero photons ($P_{No\ detected\ pair,\ 1\ to\ N_{Total}}$). The second term is a sum of the contributions from each pump pass. A pass can only contribute if its output can be switched into the storage cavity, which can only happen if no other pair was detected prior to that pass ($P_{No\ detected\ pair,\ 1\ to\ N-1}$). If that is the case, then we consider the different possibilities from the Poissonian pair

production distribution. We multiply the probability of m pairs being produced ($P_{m\ pairs\ produced}$) by the probability that at least one of the m signal photons is detected ($P_{\geq 1\ pair\ detected}$), and then multiply that by the probability that none of the m pairs reach the output (i.e., they are lost by some of the filtering or intervening optics) ($P_{All\ photons\ lost}$). We now have the overall probability of zero photons being sent to the output of the source. The probability of one photon being sent to the output is determined similarly, but without the contribution of the first term (which is no pairs being produced at all), and with exactly one of the m photons produced in pass N reaching the output ($P_{All\ but\ 1\ photon\ lost}$).

Now we just need to calculate the individual terms of these formulas, and we can determine the probabilities:

$$\begin{aligned}
P_{No\ detected\ pair\ 1\ to\ N} &= \prod_{k=1}^{N} e^{-\lambda(k)\eta}, \\
\lambda(k) &= \lambda T_{Pump}^{k-1}, \\
P_{m\ pairs\ produced} &= \frac{\lambda(N)^m e^{-\lambda(N)}}{m!}, \\
P_{\geq 1\ pair\ detected} &= 1-(1-\eta)^m, \\
P_{All\ photons\ lost} &= (1-T_{Misc.}T_{Storage\ cavity}^{N_{Total}-N})^m, \\
P_{All\ but\ 1\ photon\ lost} &= (1-T_{Misc.}T_{Storage\ cavity}^{N_{Total}-N})^{m-1} \\
&\quad \times m T_{Misc.}T_{Storage\ cavity}^{N_{Total}-N},
\end{aligned}$$

where λ is the average number of pairs produced with the initial pulse energy, η is the detection efficiency, T_{Pump} is the per-pass transmission of the pump storage cavity, $T_{Misc.}$ is the loss coupling the heralded photon into the storage cavity (e.g., from spatial and spectral filters, and any loss from optics such as mirrors or lenses), and $T_{Storage\ cavity}$ is the per-pass transmission of the down-conversion storage cavity.

We can now consider what will change in the above calculations if we use the *last* heralded photon instead of the first. In this case, a pair is used if no other pair is detected *after* it (as opposed to above, where a pair is used if no

other pair is detected *before* it). This changes the probabilities to:

$$\begin{aligned}
P_{0\ photons} =& P_{No\ detected\ pair,\ 1\ to\ N_{Total}} + \sum_{N=1}^{N_{Total}} (P_{No\ detected\ pair,\ N+1\ to\ N_{Total}} \\
&\times \sum_{m=1}^{\infty} P_{m\ pairs\ produced} P_{\geq 1\ pair\ detected} P_{All\ photons\ lost}), \\
P_{1\ photons} =& \sum_{N=1}^{N_{Total}} (P_{No\ detected\ pair,\ N+1\ to\ N_{Total}} \\
&\times \sum_{m=1}^{\infty} P_{m\ pairs\ produced} P_{\geq 1\ pair\ detected} P_{All\ but\ 1\ photon\ lost}).
\end{aligned}$$

We can also consider the case of a photon-number-resolving (PNR) detector, with which we can select the cases when we detect exactly one heralding photon, and discard some of the events where two photons are produced. We now have:

$$\begin{aligned}
P_{0\ photons} =& P_{No\ detected\ single\ pair,\ 1\ to\ N_{Total}} \\
&+ \sum_{N=1}^{N_{Total}} (P_{No\ detected\ single\ pair,\ 1\ to\ N-1} \\
&\times \sum_{m=1}^{\infty} P_{m\ pairs\ produced} P_{1\ pair\ detected} P_{All\ photons\ lost}), \\
P_{1\ photons} =& \sum_{N=1}^{N_{Total}} (P_{No\ detected\ single\ pair,\ 1\ to\ N} \\
&\times \sum_{m=1}^{\infty} P_{m\ pairs\ produced} P_{1\ pair\ detected} P_{All\ but\ 1\ photon\ lost}),
\end{aligned}$$

where

$$P_{No\ detected\ single\ pair,\ 1\ to\ N} = \prod_{k=1}^{N} (1 - \lambda(k)\eta e^{-\lambda(k)\eta}),$$

$$P_{1\ pair\ detected} = m\eta(1-\eta)^{m-1}.$$

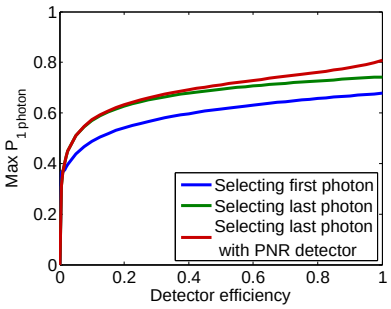
We could of course apply both of these changes for a PNR detector with the selection of the last detected pair.

C.1.2 Optimizing individual components

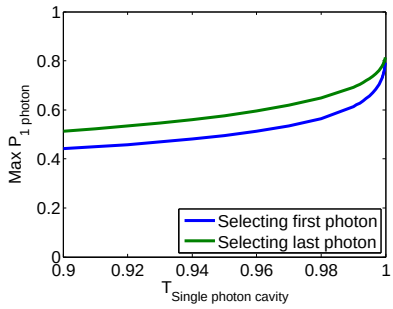
In addition to the performance we expect we can reach with expected component performances (as shown in Section 3.2), we can determine how the performance changes as we vary different parameters, so we can see on which parameters we should focus our efforts on improvement. Fig. C.1 shows the performance of the best $P_{1photon}$ as we fix every parameter but one, and vary that parameter. For every figure, the parameters are as follows (except for parameter being varied): $\eta = 0.485$, $T_{Pump} = 1$ (i.e., using a high-rate laser), $T_{Misc.} = 0.83$, $T_{Storage\ cavity} = 0.99$, with a non-PNR detector. Every plot is shown with both selecting the first heralded photon and the last heralded photon. From this figure, we can see that the biggest single parameter to focus on is the transmission of the single-photon storage cavity.

C.2 Fock- and $N00N$-state sources

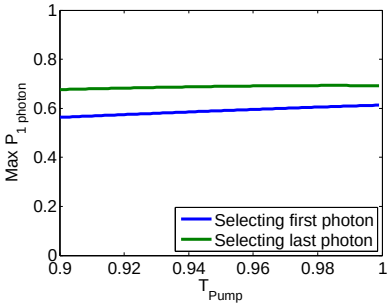
In this section I discuss the predicted performance of the Fock- and $N00N$-state sources. I first address the $N00N$-state performance, since it is easier to calculate due to the requirement of photons being produced one at a time. Here we calculate the probability of successfully adding the next photon to the cavity (e.g., from n photons to $n+1$ photons), and then the total success probability if we successfully add each of the N photons in this manner. It is also required that all of the N photons are collected and detected, but that is simply a factor of η^N. In this case, since an unentangled source is required to exhibit the desired multi-photon interference, a thermal distribution is used instead of a Poissonian



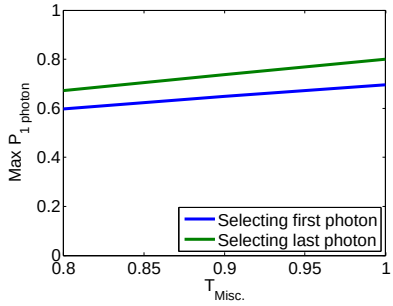
(a) Performance vs detector efficiency, for both a non-PNR and a PNR detector. Note that number resolution only has a significant effect if the detection efficiency is high (which is a requirement to be able to reliably discriminate between one pair and two pairs).



(b) Performance vs the single photon cavity transmission. The performance jumps sharply as this transmission approaches unity.



(c) Performance vs the pump cavity transmission. This indicates there is no significant improvement in the source performance with the use of a high-rate laser (though it may still be easier experimentally with such a laser).



(d) Performance vs the transmission of the miscellaneous optics. Since this is a loss that every photon would experience, the single-photon probability is approximately linear with the transmission.

Figure C.1: Source performance vs changes in different internal performance parameters of the source.

one. This approach gives us:

$$\begin{aligned}
P_{Success} =& \eta^N \prod_{n=0}^{N-1} P_{n\ to\ n+1} \\
P_{n\ to\ n+1} =& \sum_{k=0} \infty T^{n(k+1)} P_{No\ pairs}(\lambda)^k P_{One\ pair}(\lambda), \\
P_{0\ to\ 1} =& 1, \\
P_{No\ pairs}(\lambda) =& \frac{1}{1+\lambda}, \\
P_{One\ pair}(\lambda) =& \frac{1}{1+\lambda}\frac{\lambda}{\lambda+1},
\end{aligned}$$

where T is the per-pass cavity transmission and λ is the average number of down-conversion pairs produced per pass. The probability of successfully proceeding from n photons to $n+1$ photons (the first equation) is the sum of the probability of the different numbers of passes made without a pair until exactly one pair is produced (if two or more pairs are produced at any time, production of the state is a failure). For each of the passes where no pair is produced, each of the n photons must be transmitted without loss through the cavity. Finally, the last pass must produce exactly one pair.

Clearly, the performance depends on the strength of the down-conversion source λ. This can be optimized by taking the derivative of $P_{n\ to\ n+1}$ with respect to λ, setting this equal to zero, and solving for λ. From this, we determine:

$$\lambda(n) = \sqrt{1 - T^n}.$$

In the limiting case of, e.g., no loss in the cavity ($T = 1$), then we want to pump the source very weakly, so that a two-pair event never happens, which matches with a low λ from this equation. In another limit, with many photons in the cavity, we want to pump harder, so that exactly one pair is produced as quickly as possible (which is most likely to happen if $\lambda = 1$).

Calculating the expected performance of the Fock-state source is more difficult, since the case of a photon being lost in the cavity, but replaced with

an extra (unheralded) photon must be considered a success. To do a complete calculation, we would need to take into account the probability of different numbers of extra photons being added and lost over the course of the run of the experiment, and taking into account every possibility quickly becomes cumbersome. While such a calculation is likely possible, my approach was to simply simulate the source.

For this simulation, I assume a thermal distribution for the pair production probability, as was the case for the $N00N$-state source. The simulations were done by keeping track of the number of photons generated into and lost out of the cavity with each pass of the pump pulse. The strength of the pump pulse used was determined by running simulations for the different possible internal states of the source (the internal state is determined by the current number of heralded photons, and the number of desired photons).

Appendix D

ENTROPY CALCULATIONS

For our cryptography system described in Chapter 5, the random generation of pairs of photons is used as a source of entropy, which will lead to correlations in the arrival times of photons in the detectors of the two parties (Alice and Bob). The entropy can be thought of as a measure of uncertainty. Formally, the amount of entropy H on one side can be calculated by determining the different possibilities (i.e., either a photon was detected or no photon was detected, labeled '1' and '0' respectively) in each time bin:

$$H = -\sum_{x \in \{0,1\}} p(x) \log_2(p(x)).$$

Of course, what we want to know is not the entropy on one side, but rather, how much we can extract in a secure fashion. Given a correlated (but noisy) signal between Alice and Bob, we need to know how much additional (classical) information must be transferred to resolve the errors. We can determine this by considering the entropy of Bob's knowledge about Alice's signal, given only his own signal. We can calculate this by first looking at the probabilities of various

events:

$$\begin{aligned}
P(0_{Alice}, 0_{Bob}) =& (1-\lambda) + \lambda(1-\eta)^2, \\
P(0_{Alice}, 1_{Bob}) =& \lambda\eta(1-\eta), \\
P(1_{Alice}, 0_{Bob}) =& \lambda\eta(1-\eta), \\
P(1_{Alice}, 1_{Bob}) =& \lambda\eta^2,
\end{aligned}$$

where λ is the probability of a pair being produced in any given time bin and η is the detector efficiency[1]. The entropy of Bob's knowledge (or lack thereof) of Alice's signal can then be calculated from these probabilities:

$$\begin{aligned}
H(X_{Alice}|Y_{Bob}) &= \sum_{y\in\{0,1\}} p(y) H(X_{Alice}|Y_{Bob}=y), \\
H(X_{Alice}|Y_{Bob}=y) &= -\sum_{y\in\{0,1\}} p(x|y)\log_2(p(x|y)), \\
H(X_{Alice}|Y_{Bob}) &= -\sum_{y\in\{0,1\}}\sum_{x\in\{0,1\}} p(x,y)\log_2(\frac{p(y)}{p(x,y)}).
\end{aligned}$$

We can now calculate how much additional information Alice must send Bob (e.g., over a noiseless classical channel) in order for him to reconstruct her string. This information must of course be considered to be known by an eavesdropper, so it must be subtracted from the entropy of the original signal to obtain the amount of usable entropy I between Alice and Bob:

$$I(X_{Alice}, Y_{Bob}) = H(X_{Alice}) - H(X_{Alice}|Y_{Bob}).$$

This is also the amount of shared (or mutual) entropy between Alice and Bob in the first place, which can be calculated directly:

$$I(X_{Alice}, Y_{Bob}) = \sum_{\{x,y\}\in\{0,1\}} p(x,y)\log(\frac{p(x,y)}{p(x)p(y)}).$$

The mutual entropy is the maximum amount of entropy per time bin which our quantum cryptography system could distribute between Alice and Bob, assuming perfect security (i.e., no eavesdropping) and perfect error correction (i.e., reaching the channel capacity).

[1]Two-pair events are assumed to be negligible for any given time bin (reasonable for our expected values of $\lambda \sim 10^{-3}$), but could easily be added to the above equations.

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935), http://prola.aps.org/abstract/PR/v47/i10/p777_1.

[2] J. S. Bell, Physics **1**, 195 (1964).

[3] S. J. F. ad John F. Clauser, Phys. Rev. Lett. **28**, 938 (1972), http://prl.aps.org/abstract/PRL/v28/i14/p938_1.

[4] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982), http://prl.aps.org/abstract/PRL/v49/i25/p1804_1.

[5] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998), http://prl.aps.org/abstract/PRL/v81/i17/p3563_1.

[6] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998), http://prl.aps.org/abstract/PRL/v81/i23/p5039_1.

[7] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Nature **409**, 791 (2001), http://www.nature.com/nature/journal/v409/n6822/abs/409791a0.html.

[8] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984), p. 175.

[9] D. Deutsch, Proc. Roy. Soc. London A **400**, 97 (1985), http://dx.doi.org/10.1098/rspa.1985.0070.

[10] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982), http://dx.doi.org/10.1007/BF02650179.

[11] P. Shor, in *Proc. 35th Ann. Symp. Found. Comp. Sci.* (IEEE Comp. Soc. Press, Los Alamitos, California, 1994), p. 124, http://dx.doi.org/10.1109/SFCS.1994.365700.

[12] L. K. Grover, in *Proc. 28th Ann. ACM Symp. Theory Comp.* (1996), p. 212, http://dx.doi.org/10.1145/237814.237866.

[13] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992), http://prl.aps.org/abstract/PRL/v69/i20/p2881_1.

[14] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993), http://prl.aps.org/abstract/PRL/v70/i13/p1895_1.

[15] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995), http://dx.doi.org/10.1103/PhysRevLett.74.4091.

[16] A. Blais, R.-S. Huang, A. Wallraff, S. M. Girvin, and R. J. Schoelkopf, Phys. Rev. A **69**, 062320 (2004), http://dx.doi.org/10.1103/PhysRevA.69.062320.

[17] A. D. OConnell, M. Hofheinz, M. Ansmann, R. C. Bialczak, M. Lenander, E. Lucero, M. Neeley, D. Sank, H. Wang, M. Weides, et al., Nature **464**, 697 (2011), http://dx.doi.org/10.1038/nature08967.

[18] J. D. Teufel, T. Donner, D. Li, J. W. Harlow, M. S. Allman, K. Cicak, A. J. Sirois, J. D. Whittaker, K. W. Lehnert, and R. W. Simmonds, Nature **475**, 359 (2011), http://dx.doi.org/10.1038/nature10261.

[19] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996), http://prl.aps.org/abstract/PRL/v76/i25/p4656_1.

[20] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Nature Phys. **4**, 282 (2008), http://www.nature.com/nphys/journal/v4/n4/full/nphys919.html.

[21] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature **390**, 575 (1997), http://www.nature.com/nature/journal/v390/n6660/full/390575a0.html.

[22] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Nature **426**, 264 (2003), http://www.nature.com/nature/journal/v426/n6964/full/nature02054.html.

[23] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000), http://prl.aps.org/abstract/PRL/v84/i20/p4729_1.

[24] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000), http://dx.doi.org/10.1103/PhysRevLett.84.4733.

[25] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000), http://prl.aps.org/abstract/PRL/v84/i20/p4737_1.

[26] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996), http://dx.doi.org/10.1103/PhysRevLett.76.722.

[27] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Nature **423**, 417 (2003), http://dx.doi.org/10.1038/nature01623.

[28] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, Science **290**, 498 (2000), http://dx.doi.org/10.1126/science.290.5491.498.

[29] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998), http://dx.doi.org/10.1103/PhysRevLett.81.2594.

[30] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, et al., Opt. Exp. **18**, 8587 (2010), http://www.opticsinfobase.org/abstract.cfm?uri=oe-18-8-8587.

[31] E. Knill, R. Laflamme, and G. J. Milburn, Nature **409**, 46 (2001), http://www.nature.com/nature/journal/v409/n6816/abs/409046a0.html.

[32] R. Krischek, W. Wieczorek, A. Ozawa, N. Kiesel, P. Michelberger, T. Udem, and H. Weinfurter, Nature Phot. **4**, 170 (2010), http://www.nature.com/nphoton/journal/v4/n3/full/nphoton.2009.286.html.

[33] R. W. Boyd, *Nonlinear Optics* (Academic Press, 2003).

[34] R. Rangarajan, L. E. Vicent, A. B. URen, and P. G. Kwiat, J. Mod. Opt. **58**, 318 (2011), http://dx.doi.org/10.1080/09500340.2010.529515.

[35] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergieko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995), http://prl.aps.org/abstract/PRL/v75/i24/p4337_1.

[36] P. G. Kwiat, P. H. Eberhard, A. M. Steinberg, and R. Y. Chiao, Phys. Rev. A **49**, 3209 (1994), http://dx.doi.org/10.1103/PhysRevA.49.3209.

[37] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, Opt. Exp. **15**, 15377 (2007), http://dx.doi.org/10.1364/OE.15.015377.

[38] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999), http://dx.doi.org/10.1103/PhysRevA.60.R773.

[39] M. Zukowski, A. Zeilinger, and H. Weinfurter, Ann. NY Acad. Sci. **755**, 91 (1995), http://dx.doi.org/10.1111/j.1749-6632.1995.tb38959.x.

[40] A. Valencia, A. Ceré, X. Shi, G. Molina-Terriza, and J. P. Torres, Phys. Rev. Lett. **99**, 243601 (2007), http://dx.doi.org/10.1103/PhysRevLett.99.243601.

[41] P. J. Mosley, J. S. Lundeen, B. J. Smith, P. Wasylczyk, A. B. URen, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100**, 133601 (2008), http://dx.doi.org/10.1103/PhysRevLett.100.133601.

[42] L. E. Vicent, A. B. U'Ren, R. Rangarajan, C. I. Osorio, J. P. Torres, L. Zhang, and I. A. Walmsley, New J. Phys. **12**, 093027 (2010), http://dx.doi.org/10.1088/1367-2630/12/9/093027.

[43] F. Wolfgramm, X. Xing, A. Cerè, A. Predojevic, A. M. Steinberg, and M. W. Mitchell, Opt. Exp. **16**, 18145 (2008), http://dx.doi.org/10.1364/OE.16.018145.

[44] S. Tanzilli, H. D. Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. D. Micheli, D. Ostrowsky, and N. Gisin, Electron. Lett. **37**, 26 (2001), http://dx.doi.org/10.1049/el:20010009.

[45] J. Altepeter, E. Jeffrey, and P. G. Kwiat, Opt. Exp. **13**, 8951 (2005), http://dx.doi.org/10.1364/OPEX.13.008951.

[46] R. S. Bennink, Phys. Rev. A **81**, 053805 (2010), http://dx.doi.org/10.1103/PhysRevA.81.053805.

[47] A. Dragan, Phys. Rev. A **70**, 053814 (2004), http://pra.aps.org/abstract/PRA/v70/i5/e053814.

[48] R. Andres, E. Pike, and S. Sarkar, Opt. Exp. **12**, 3264 (2004), http://www.opticsinfobase.org/oe/abstract.cfm?URI=OPEX-12-14-3264.

[49] P. Kolenderski, W. Wasilewski, and K. Banaszek, Phys. Rev. A **80**, 013811 (2009), http://dx.doi.org/10.1103/PhysRevA.80.013811.

[50] A. Ling, A. Lamas-Linares, and C. Kurtsiefer, Phys. Rev. A **77**, 043834 (2008), http://pra.aps.org/abstract/PRA/v77/i4/e043834.

[51] C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, Phys. Rev. A **64**, 023802 (2001), http://pra.aps.org/abstract/PRA/v64/i2/e023802.

[52] F. A. Bovino, P. Varisco, A. M. Colla, G. Castagnoli, G. D. Giuseppe, and A. V. Sergienko, Opt. Commun. **227**, 343 (2003), http://dx.doi.org/10.1016/j.optcom.2003.09.064.

[53] S. Castelletto, I. P. Degiovanni, G. Furno, V. Schettini, A. Migdall, and M. Ware, IEEE Trans. on Instr. and Meas. **54**, 890 (2005), http://dx.doi.org/10.1109/TIM.2005.843571.

[54] D. Ljunggren and M. Tengner, Phys. Rev. A **72**, 062301 (2005), http://dx.doi.org/10.1103/PhysRevA.72.062301.

[55] P. J. Mosley, J. S. Lundeen, B. J. Smith, P. Wasylczyk, A. B. URen, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100**, 133601 (2008), http://dx.doi.org/10.1103/PhysRevLett.100.133601.

[56] P. G. Evans, R. S. Bennink, W. P. Grice, T. S. Humble, and J. Schaake, Phys. Rev. Lett. **105**, 253601 (2010), http://dx.doi.org/10.1103/PhysRevLett.105.253601.

[57] D. H. Smith, G. Gillett, M. P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H. M. Wiseman, et al., Nature Comm. **3**, 625 (2012), http://dx.doi.org/10.1038/ncomms1628.

[58] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Opt. Comm. **246**, 545 (2005), http://dx.doi.org/10.1016/j.optcom.2004.11.027.

[59] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Exp. **16**, 3032 (2008), http://dx.doi.org/10.1364/OE.16.003032.

[60] N. Destouches, A. Tishchenko, J. Pommier, S. Reynaud, O. Parriaux, S. Tonchev, and M. Ahmed, Opt. Exp. **13**, 3230 (2005), http://dx.doi.org/10.1364/OPEX.13.003230.

[61] D. N. Nikogosyan, Appl. Phys. A: Mat. Sci. Proc. **52**, 359 (1991), http://dx.doi.org/10.1007/BF00323647.

[62] R. S. Bubnova, S. V. Krivovichev, S. K. Filatov, A. V. Egorysheva, and Y. F. Kargin, J. Sol. State Chem. **180**, 596 (2007), http://dx.doi.org/10.1016/j.jssc.2006.11.001.

[63] C. H. Monken, P. H. S. Ribeiro, and S. Pádua, Phys. Rev. A **57**, R2267 (1998).

[64] Ö. Süzer and T. G. Goodson, Opt. Exp. **16**, 20166 (2008), http://dx.doi.org/10.1364/OE.16.020166.

[65] P. H. Eberhard, Phys. Rev. A **47**, R747 (1993), http://dx.doi.org/10.1103/PhysRevA.47.R747.

[66] S. Takeuchi, J. Kim, Y. Yamamoto, and H. H. Hogue, Appl. Phys. Lett. **74**, 1063 (1999).

[67] S. Hecht, S. Shlaer, and M. H. Pirenne, J. Gen. Physiol. **25**, 819 (1942), http://dx.doi.org/10.1085/jgp.25.6.819.

[68] F. Rieke and D. A. Baylor, Rev. Mod. Phys. **70**, 1027 (1998), http://dx.doi.org/10.1103/RevModPhys.70.1027.

[69] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Rev. Sci. Instrum. **82**, 071101 (2011), http://dx.doi.org/10.1063/1.3610677.

[70] J. McKeever, A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich, and H. J. Kimble, Science **303**, 1992 (2004), http://dx.doi.org/10.1126/science.1095232.

[71] J. Bochmann, M. Mcke, G. Langfahl-Klabes, C. Erbel, B. Weber, H. P. Specht, D. L. Moehring, and G. Rempe, Phys. Rev. Lett. **101**, 223601 (2008), http://dx.doi.org/10.1103/PhysRevLett.101.223601.

[72] D. N. Matsukevich, T. Chanelire, S. D. Jenkins, S.-Y. Lan, T. A. B. Kennedy, and A. Kuzmich, Phys. Rev. Lett. **97**, 013601 (2006), http://dx.doi.org/10.1103/PhysRevLett.97.013601.

[73] S. Strauf, N. G. Stoltz, M. T. Rakher, L. A. Coldren, P. M. Petroff, and D. Bouwmeester, Nature Phot. **1**, 704 (2007), http://dx.doi.org/10.1038/nphoton.2007.227.

[74] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, Phys. Rev. Lett. **89**, 187901 (2002), http://dx.doi.org/10.1103/PhysRevLett.89.187901.

[75] E. B. Flagg, A. Muller, S. V. Polyakov, A. Ling, A. Migdall, and G. S. Solomon, Phys. Rev. Lett. **104**, 137401 (2010), http://dx.doi.org/10.1103/PhysRevLett.104.137401.

[76] R. B. Patel, A. J. Bennett, I. Farrer, C. A. Nicoll, D. A. Ritchie, and A. J. Shields, Nature Phot. **4**, 632 (2010), http://dx.doi.org/10.1038/nphoton.2010.161.

[77] P. Tamarat, T. Gaebel, J. R. Rabeau, M. Khan, A. D. Greentree, H. Wilson, L. C. L. Hollenberg, S. Prawer, P. Hemmer, F. Jelezko, et al., Phys. Rev. Lett. **97**, 083002 (2006), http://dx.doi.org/10.1103/PhysRevLett.97.083002.

[78] L. C. Bassett, F. J. Heremans, C. G. Yale, B. B. Buckley, and D. D. Awschalom, Phys. Rev. Lett. **107**, 266403 (2011), http://dx.doi.org/10.1103/PhysRevLett.107.266403.

[79] M. Hofheinz, H. Wang, M. Ansmann, R. C. Bialczak, E. Lucero, M. Neeley, A. D. O'Connell, D. Sank, J. Wenner, J. M. Martinis, et al., Nature **459**, 546 (2009), http://dx.doi.org/10.1038/nature08005.

[80] H. Paik, D. I. Schuster, L. S. Bishop, G. Kirchmair, G. Catelani, A. P. Sears, B. R. Johnson, M. J. Reagor, L. Frunzio, L. I. Glazman, et al.,

Phys. Rev. Lett. **107**, 240501 (2011), http://dx.doi.org/10.1103/PhysRevLett.107.240501.

[81] N. Imoto, H. A. Haus, and Y. Yamamoto, Phys. Rev. A **32**, 2287 (1985), http://dx.doi.org/10.1103/PhysRevA.32.2287.

[82] B. C. Jacobs, T. B. Pittman, and J. D. Franson, Phys. Rev. A **74**, 010303(R) (2006), http://dx.doi.org/10.1103/PhysRevA.74.010303.

[83] Y.-P. Huang and P. Kumar, Phys. Rev. Lett. **108**, 030502 (2012), http://dx.doi.org/10.1103/PhysRevLett.108.030502.

[84] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001), http://dx.doi.org/10.1103/PhysRevLett.86.5188.

[85] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005), http://dx.doi.org/10.1103/PhysRevLett.95.010501.

[86] M. Varnava, D. E. Browne, and T. Rudolph, Phys. Rev. Lett. **100**, 060502 (2008), http://dx.doi.org/10.1103/PhysRevLett.100.060502.

[87] Y.-X. Gong, X.-B. Zou, T. C. Ralph, S.-N. Zhu, and G.-C. Guo, Phys. Rev. A **81**, 052303 (2010), http://dx.doi.org/10.1103/PhysRevA.81.052303.

[88] B. R. Mollow and R. J. Glauber, Phys. Rev. **160**, 1097 (1967), http://dx.doi.org/10.1103/PhysRev.160.1097.

[89] T. Jennewein, M. Barbieri, and A. G. White, J. Mod. Opt. **58**, 276 (2011), http://dx.doi.org/10.1080/09500340.2010.546894.

[90] A. L. Migdall, D. Branning, and S. Castelletto, Phys. Rev. A **66**, 053805 (2002), http://dx.doi.org/10.1103/PhysRevA.66.053805.

[91] X. song Ma, S. Zotter, J. Kofler, T. Jennewein, and A. Zeilinger, Phys. Rev. A **83**, 043814 (2011), http://dx.doi.org/10.1103/PhysRevA.83.043814.

[92] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **66**, 042303 (2002).

[93] E. Jeffrey, N. A. Peters, and P. G. Kwiat, New J. Phys. **6**, 100 (2004).

[94] K. T. McCusker and P. G. Kwiat, Phys. Rev. Lett. **103**, 163602 (2009), http://dx.doi.org/10.1103/PhysRevLett.103.163602.

[95] E. Waks, E. Diamanti, and Y. Yamamoto, New Journal of Physics **8**, 4 (2006).

[96] J. P. Dowling, Contemp. Phys. **49**, 125 (2008).

[97] E. J. S. Fonseca, C. H. Monken, and S. Pádua, Phys. Rev. Lett. **82**, 2868 (1999).

[98] P. Walther *et al.*, Nature **429**, 158 (2004).

[99] M. W. Mitchell, J. S. Lundeen, and A. M. Steinberg, Nature **429**, 161 (2004).

[100] P. Kok *et al.*, Phys. Rev. A **63**, 063407 (2001).

[101] P. Kok, H. Lee, and J. P. Dowling, Phys. Rev. A **65**, 052104 (2002).

[102] X. Zou, K. Pahlke, and W. Mathis, Phys. Rev. A **66**, 014102 (2002).

[103] H. Cable and J. P. Dowling, Phys. Rev. Lett. **99**, 163604 (2007).

[104] C. Simon and D. Bouwmeester, Phys. Rev. Lett. **91**, 053601 (2003).

[105] M. A. Rubin and S. Kaushik, Phys. Rev. A **75**, 053805 (2007).

[106] S. D. Huver, C. F. Wildfeuer, and J. P. Dowling, Phys. Rev. A **78**, 063828 (2008).

[107] U. Dorner *et al.*, Phys. Rev. Lett. **102**, 040403 (2009).

[108] M. J. Padgett and J. Courtial, Opt. Lett. **24**, 430 (1999), http://dx.doi.org/10.1364/OL.24.000430.

[109] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Phys. Rev. A **45**, 8185 (1992), http://dx.doi.org/10.1103/PhysRevA.45.8185.

[110] S. Franke-Arnold, G. Gibson, R. W. Boyd, and M. J. Padgett, Science **333**, 6038 (2011), http://dx.doi.org/10.1126/science.1203984.

[111] H. H. Arnaut and G. A. Barbosa, Phys. Rev. A **85**, 286 (2000), http://dx.doi.org/10.1103/PhysRevLett.85.286.

[112] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature **412**, 313 (2001), http://dx.doi.org/10.1038/35085529.

[113] J. Clausen, H. Hansen, L. Knöll, J. Mlynek, and D.-G. Welsch, Appl. Phys. B **72**, 43 (2001).

[114] S. A. Babichev, J. Ries, and A. I. Lvovsky, Europhys. Lett. **64**, 1 (2003).

[115] F. W. Sun, Z. Y. Ou, and G. C. Guo, Phys. Rev. A **73**, 023808 (2006).

[116] V. Parigi, A. Zavatta, M. Kim, and M. Bellini, Science **317**, 1890 (2007).

[117] M. S. Kim, H. Jeong, A. Zavatta, V. Parigi, and M. Bellini, Phys. Rev. Lett. **101**, 260401 (2008).

[118] C. E. Shanon, Bell Sys. Tech. J. **27**, 379 (1948).

[119] C. Shannon, Bell Sys. Tech. J. **28**, 656 (1949).

[120] W. Tuchman, in *Internet besieged*, edited by D. E. Denning and P. J. Denning (ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 1998), chap. A brief history of the data encryption standard, pp. 275–280, ISBN 0-201-30820-7, URL http://dl.acm.org/citation.cfm?id=275737.275754.

[121] B. Burr, J. Res. Nat. Inst. Stand. Tech. **107**, 307 (2002), http://nvlpubs.nist.gov/nistpubs/jres/107/3/j73nbr.pdf.

[122] A. Bogdanov, D. Khovratovich, and C. Rechberger, *Biclique cryptanalysis of the full aes*, Cryptology ePrint Archive, Report 2011/449 (2011), http://eprint.iacr.org/.

[123] W. Diffie and M. Hellman, in *AFIPS Proceedings* (1976), vol. 45, p. 109, http://dx.doi.org/10.1145/1499799.1499815.

[124] R. R. ad A. Shamir and L. Adleman, Comm. ACM **21**, 120 (1978), http://dx.doi.org/10.1145/359340.359342.

[125] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Comput. **26**, 1510 (1997), http://dx.doi.org/10.1137/S0097539796300933.

[126] G. Brassard and L. Savail, Lect. Notes. Comput. Sci. **765**, 410 (1994), http://dx.doi.org/10.1007/3-540-48285-7_35.

[127] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995), http://dx.doi.org/10.1109/18.476316.

[128] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Phot. **4**, 686 (2010), http://dx.doi.org/10.1038/nphoton.2010.214.

[129] M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981), http://dx.doi.org/10.1016/0022-0000(81)90033-7.

[130] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002), http://dx.doi.org/10.1103/RevModPhys.74.145.

[131] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).

[132] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **92**, 201104 (2008), http://link.aip.org/link/doi/10.1063/1.2931070.

[133] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010), http://link.aip.org/link/doi/10.1063/1.3385293.

[134] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, et al., New J. Phys. **11**, 045010 (2009), http://dx.doi.org/10.1088/1367-2630/11/4/045010.

[135] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, eprint arXiv:quant-ph/0503058 (2005), arXiv:quant-ph/0503058.

[136] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., Opt. Exp. **19**, 10387 (2011), http://dx.doi.org/10.1364/OE.19.010387.

[137] D. Stucki1, M. Legr, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, et al., New J. Phys. **13**, 123001 (2011), http://dx.doi.org/10.1088/1367-2630/13/12/123001.

[138] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982), http://dx.doi.org/10.1038/299802a0.

[139] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[140] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, et al., Opt. Exp. **18**, 8587 (2010), http://dx.doi.org/10.1364/OE.18.008587.

[141] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (2007), http://dx.doi.org/10.1080/09500349414552281.

[142] M. A. Wayne and P. G. Kwiat, Opt. Exp. **18**, 9351 (2010), http://dx.doi.org/10.1364/OE.18.009351.

[143] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007), http://dx.doi.org/10.1103/PhysRevLett.98.060503.

[144] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991), http://dx.doi.org/10.1103/PhysRevLett.67.661.

[145] A. Migdall, J. Opt. Soc. Am. B **14**, 1093 (1997), http://dx.doi.org/10.1364/JOSAB.14.001093.

[146] R. Rangarajan, A. B. U'Ren, and P. G. Kwiat, J. Mod. Opt. **58**, 58 (2011), http://dx.doi.org/10.1080/09500340.2010.515753.

[147] D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson, and P. G. Kwiat, New J. Phys. **4**, 45 (2002), http://dx.doi.org/10.1088/1367-2630/4/1/345.

[148] J. D. Franson, Phys. Rev. A **44**, 4552 (1991), http://dx.doi.org/0.1103/PhysRevA.44.4552.

[149] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Duek, N. Ltkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009), http://dx.doi.org/10.1103/RevModPhys.81.1301.

[150] A. E. Siegman, *Lasers* (University Science Books, 1986).

[151] R. Rangarajan, M. Goggin, and P. Kwiat, Opt. Exp. **17**, 18920 (2009), http://dx.doi.org/10.1364/OE.17.018920.