ENTANGLED PHOTON PAIRS: EFFICIENT GENERATION AND DETECTION, AND BIT COMMITMENT

SIDDARTH KODURU JOSHI

B. Sc. (Physics, Mathematics, Computer Science), Bangalore University

M.Sc. (Physics), Bangalore University

A THESIS SUBMITTED
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

CENTRE FOR QUANTUM TECHNOLOGIES

NATIONAL UNIVERSITY OF SINGAPORE

2014

Declaration

I hereby declare that the thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

The thesis has also not been submitted for any degree in any university previously.

SIDDARTH KODURU JOSHI

July 29, 2014

To,
The road not taken...

This thesis is a testament to the path I chose. I would nevertheless, take this contemplative moment to reflect and honor the alternatives: The experiments I did not perform. My grand parents whose hands I could have held. My parents. My girlfriend. My.....

But,
Science is lovely, dark and deep
And I have riddles to solve before I sleep.

Acknowledgements

Being a third generation pure bred academic, this experiment in long term sleep deprivation culminating in a doctoral degree, is almost a right of passage. It is what I always saw myself doing. In reality, it has been all I thought it would and so much more too. But unlike the tribes one hears about on National Geographic, my right of passage was not done in isolation in a remote jungle. I was assisted and guided, helped and consoled, cheered on and lectured to and so much more. And without the help I received, well its best not to contemplate such abysmal scenarios.

Christian Kurtsiefer, my guide, has, much to my enlightenment, been at the receiving end of my doubts, and requests for help. Despite my impeccable ineptitude in timing my interruptions, he has always taken the time to set both me and this experiment on the right tracks. For that I am grateful. "Technical difficulties" or more commonly known as "we don't know why it went boom" were the bane of this experiment. I really value his support, guidance, help, and patience. I have also lost track of the number of dinners he has treated this hungry student to, in appreciation of which I can only quote "So long and thanks for all the fish" – the dolphins.

Alessandro Ceré has been of great help, not only in the experiment but in proof reading this thesis too. Of late, he has been the "go-to" man for discussing ideas and dispelling bewilderment. I owe him much. My girlfriend Kamalam Vanninathan, has stood by me throughout and been the pillar I can lean on. For that and more I thank her. My parents were instrumental in my success and needless to say they have my eternal gratitude.

Antia Lamas Linares, was the one who first showed me the ropes. Brenda Chng, in the perpetually being reorganized lab, continued to show we where everything was till date. Bharath Srivathsan and Gurpreet Gulati, friends,

office mates and brains for me to pick. Are some names I would like to single out. My other friends and coworkers who assisted in so many small ways, I owe you all a debt of deep gratitude. It was fun working with M. Kalenikin, C.C. Ming and Q.X. Leong and I value their assistance. Collaborating with Nelly Ng and Stephanie Wehner was both fun and interesting. To all those in the center from whom I have begged, borrowed or stolen equipment and parts over the years, you have my fond thanks.

Contents

Summary

In this work we use sources of polarization entangled photon pairs for applications in quantum communication and to study fundamental quantum mechanics. This thesis consists of two experiments: bit commitment and the generation and detection of polarization entangled photon pairs with a high heralding efficiency.

Bit commitment is a two-party protocol that can be used as a cryptographic primitive for tasks like secure identification. Secure bit commitment was thought to be impossible [1]. Nevertheless, we experimentally implemented a secure protocol for bit commitment by measurements on polarization-entangled photon pairs, thereby demonstrating the feasibility of two-party protocols in the noisy-storage model [2].

Device independent protocols are of great interest to modern quantum communication. These protocols require a high heralding efficiency ($\gg 66.7\,\%$) [3]. The current implementations of these protocols using single photons are limited by optical losses and the limited detection efficiency of standard single photon detectors. The Transition Edge Sensors (TES), developed at NIST, have a detection efficiency $> 98\,\%$ [4]. We present a highly efficient polarization entangled source of photon pairs obtained from spontaneous parametric downconversion in a PPKTP crystal. Using TESs we observe a $75.2\,\%$ heralding efficiency (pairs to singles ratio) of these photon pairs which is well above the threshold ($66.7\,\%$) for implementing device independent protocols and for a loophole-free Bell test. Key aspects to arrive at this high efficiency were careful mode matching techniques, and elimination of optical losses.

Many device independent protocols make use of a wide range of entangled states, our source is capable of producing both maximally entangled states (with a polarization correlation visibility of $99.4\,\%$) and non-maximally entangled states (with a fidelity of $99.3\,\%$).

Further, to demonstrate non-local effects, Alice and Bob need to implement their

choice of polarization measurement bases within the “time of flight” of the photon pairs. We have constructed a fast ($3\,\mu$s) transverse electro-optical polarization modulator for this purpose.

List of Publications

Some of the results of this thesis have been reported in the following peer reviewed publications

1. Nelly Huei Ying Ng, **Siddarth K Joshi**, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner.. **Experimental implementation of bit commitment in the noisy-storage model.**. *Nature communications*, 3:1326, 2012.

Some of the other results in this thesis have been presented in conferences and are reported in the following proceedings

1. **Siddarth K Joshi**, Felix Anger, Antia Lamas-Linares and Christian Kurtsiefer.. **Narrowband PPKTP Source for Polarization Entangled Photons**. In *The European Conference on Lasers and Electro-Optics*, CD_P24, Optical Society of America, 2011.

2. **Siddarth K Joshi**, Chia Chen Ming, Qixiang Leong, Antia Lamas-Linares, Sae Woo Nam, Alessandro Cerè and Christian Kurtsiefer.. **Towards a loophole free Bell test**. In *CLEO: QELS_Fundamental Science*, QMIC-2, Optical Society of America, 2013.

List of Tables

List of Figures

List of Acronyms

ADP	Ammonium Dihydrogen Phosphate
ADR	Adiabatic Demagnetization Refrigerator
AOM	Acousto-Optical Modulator
APD	Avalanche Photo-Diode
AR	Anti-Reflective
ATM	Automated Teller Machine
BBO	beta Barium Borate
BG	Blue Glass
BS	Beam Splitter
CFD	Constant Fraction Discriminator
CH	Clauser and Horne
CHSH	Clauser, Horne, Shimony and Holt
CPD	Calibrated Photo-Diode
CQT	Center for Quantum Technologie
CW	Continuous Wave
DC	Direct Current
DSHWP	Downconverted Sagnac Half Wave Plate
DSPBS	Downconverted Sagnac Polarizing Beam Splitter
EOM	Electro-Optical Modulator
FAA	Ferric Ammonium Alum
FC/UPC	Flat Cut Ultra polished Physical Contact
FWHM	Full Width at Half Maximum
GGG	Gadolinium-Gallium Garnet
H	Horizontal(ly)
HV	Horizontal(ly)/Vertical(ly)
HWP	Half Wave Plate
IF	Interference Filter
IR	Infra-Red
IV	Current Voltage
KDP	Potassium Dihydrogen Phosphate
KTP	Potassium Titanyl Phosphate
L	Left circular(ly)
LHV	Local Hidden Variable

LN	Lithium Niobate
LR	Left/Right circular(ly)
ND	Neutral Density
NIM	Nuclear Instrumentation Module
NIR	Near Infra-Red
NIST	National Institute of Standards and Technology
NiTi	Niobium Titanium
OPA	Optical Parametric Amplifier
OPO	Optical Parametric Oscillator
PBS	Polarizing Beam Splitter
PD	Photo-Diode
PID	Proportional-Integral-Derivative
PIN	P-type Intrinsic N-type semiconductor
PM	Phase Matching
PM	Polarization Maintaining
PMT	Photo Multiplier Tube
PPKTP	Periodically Poled Potassium Titanyl Phosphate
QKD	Quantum Key Distribution
QPM	Quasi-Phase Matching
QWP	Quarter Wave Plate
R	Right circularly(ly)
RF	Radio Frequency
RLC	Resistance Inductance Capacitance
SHG	Second Harmonic Generation
SPDC	Spontaneous Parametric Down Conversion
SQUID	Superconducting Quantum Interference Device
TES	Transition Edge Sensors
TTL	TransistorTransistor Logic
UPD	Uncalibrated Photo-Diode
UV	Ultra-Violet
V	Vertical(ly)

Definitions of some terms

Some of the terms used in this thesis are often confused with one a *not* her. This section provides a list of these terms and their definitions.

Pairs to singles ratio

When two photons are detected, one on each collection arm, within a certain coincidence time window (τ_c) of each other, then these photons are considered part of a pair. Given the rate of pairs (p) and the rate of individual detection events from each detector (s_1, s_2), the pairs to singles ratio is given by $\frac{p}{\sqrt{s_1 s_2}}$. This is same as the heralding efficiency

Heralding efficiency

The probability that the second photon of a photon pair is detected in the second arm given that the first photon of the same pair was detected in the first arm is called the heralding efficiency. This is the same as the pairs to singles ratio.

Source efficiency

The pairs to singles ratio of the source using ideal detectors is called the source efficiency. This value can *not* be directly measured, but is only inferred by correcting for measured losses in the detectors.

Quantum efficiency

The probability that a single incident photon generates a photo-electron is called the quantum efficiency. This is *not* the same as detection efficiency.

Detection efficiency

The detection efficiency is the probability that an incident photon will generate a detection signal ("click"). This is inclusive of all loss mechanisms present in a real detector such as optical losses, absorption losses, fiber coupling losses, electrical

signal losses, electron hole recombination losses, dead time of the detector, etc. The detection efficiency for non ideal detectors is always lower than the quantum efficiency.

System efficiency

The pairs to singles ratio as measured using all components of an extended system comprising of several components like the source of photon pairs, long fibers, the polarization modulator, measurement polarizers, vacuum feed-throughs, fiber splices, detectors, etc. is called the system efficiency.

Collection efficiency

The probability of coupling a downconverted photon into a collection fiber is called the collection efficiency. This includes all losses within and outside of the downconversion crystal. This is *not* to be confused with the fiber coupling efficiency.

Fiber coupling efficiency

The coupling of an optical signal into optical fibers was, in this work, always done using a lens placed in front of one end of the fiber. The ratio of optical power incident on this lens to the optical power output from the other end of the fiber is known as the fiber coupling efficiency. This is *not* the same as the collection efficiency

Corrected efficiency

The pairs to singles ratio obtained from the source can be corrected for various imperfections such as optical losses, detector efficiencies, dark/background counts, etc. The dark count corrected efficiency refers to the pair to singles ratio corrected for dark/background counts of the detector. The detector corrected efficiency refers to the pairs to singles ratio corrected for the detector efficiency and for dark/background counts.

Errors

All error bars quoted in this work refer to 1 standard deviation.

Chapter 1

Introduction

Quantum entanglement is a physical phenomenon that occurs when groups of particles are generated or interact in ways such that the quantum state of each particle cannot be described independently but only for the system as a whole [18, 19]. Entanglement is a feature of quantum mechanics and is fundamental in several quantum communication, computation and information tasks/protocols [19, 20, 21, 22, 23], as well in quantum metrology [24].

Entanglement has been demonstrated between different degrees of freedom of a number of systems: photons [25], atoms [26], and ions [27], both as single particles and ensembles. Entanglement has also been demonstrated between different kinds of physical systems like atoms and photons [28]. In this thesis I will present my contribution in the generation and study of entanglement in photon pairs. Photons are interesting quantum systems because of their unique properties: they can be easily transported, both in free space and in optical fibers, with very little interaction with the environment; their polarization degree of freedom provides a perfect testbed for fundamental tests of quantum mechanics.

One fundamental test is the so called Bell's test. In 1964, John Bell proposed this test as a way to answer the fundamental questions on the reality and locality of quantum mechanics (posed by Einstein, Podolsky and Rosen in 1935 [29]) and, since then, many efforts have been spent toward a complete experimental demonstration. Several of those attempts are based on polarization entangled photon pairs.

Polarization entangled photons pairs where first generated in 1972 by Freedman and Clauser using an atomic cascade of calcium [25]. In 1981 and 1982 Aspect et al. experimentally performed several Bell tests under different conditions [30, 31, 32]. Since

then many techniques for generating entangled photons pairs have been developed [33, 34, 35, 36], all of them based on non-linear optical properties of materials like crystals, single or ensemble of atoms/ions.

One of the fundamental obstacles for the experimental demonstration of the Bell test is the so called "fair sampling" loophole: one must ensure that a sufficient fraction of all copies of the quantum system are collected. The fair sampling assumption is typically made to overcome losses in a system consisting of pair source, switches, transmission paths and detectors.

In this thesis I will present a source of polarization entangled photon pairs based on Spontaneous Parametric Downconversion (SPDC) [37] using a scheme similar to [38]. This source has been designed and optimized to improve the collection efficiency of the generated photon pairs.

An efficient collection of photon pairs is not enough to reach the threshold required for a loophole free Bell test ($> 66.7\,\%$ [3]); it is also necessary to detect those photons with high detection efficiency.

This is why I coupled this high efficiency source to highly efficient single photon detectors developed and provided by NIST. These superconducting detectors, called Transition Edge Sensors (TES), have losses of less than $2\,\%$ [4]. Coupling the source with the TESs I was able to observe a heralding efficiency (ratio between detected coincidence over total singles) of more than $75\,\%$.

This value is above the threshold indicated by Eberhard, suggesting that the work presented here can be the basis for a loophole free test Bell test, as well for other demonstrations of device independent quantum protocols.

In this thesis I also present a more practical application of polarization entangled photon pairs: an experimental demonstration of bit commitment [2], i.e. a quantum communication and cryptographic protocol that is a primitive for tasks like secure identification.

1.1 Thesis outline

This thesis presents two experiments: the production and detection of polarization entangled photon pairs with a high efficiency and bit commitment. Both these exper-

iments utilize Spontaneous Parametric Downconversion (SPDC) to generate pairs of photons, this process is discussed in the first half of Chapter 2.

The goal of the first experiment is to construct a system capable of implementing a loophole free Bell test. The second half of Chapter 2 explains a Bell's test and its loopholes. In order to rule out the presence of selective losses (detection loophole) we must detect a sufficiently large fraction of all photon pairs. To do so we constructed a high efficiency source of polarization entangled photon pairs (Chapter 3) and connected it to near perfect single photon detectors (Chapter 4). We obtained an efficiency (75.2 %) which is higher than the Eberhard limit (66.7 %) needed to close the detection loophole.

In a Bell's test two parties – Alice and Bob look for correlations between measurements they perform on a shared state. Another loophole in a Bell's test called the locality loophole can only be closed if the experiment is performed faster than any possible communication between Alice and Bob. Since we use polarization entangled photon pairs, Alice and Bob measure the polarization of photons. We use a fast polarization modulator (Appendix A) to perform these measurements.

Quantum communication and cryptography often make use of polarization entangled photon pairs for implementing several of their protocols. Bit commitment (Chapter 5) is one such protocol we implemented for the first time.

Chapter 2

Theory

In this chapter I provide a basic overview of the generation of photon pairs in non-linear optical media by a process called Spontaneous Parametric Downconversion (SPDC) which is used in all experiments presented in this thesis. I also discuss the fundamentals behind a Bell test, the experimental loopholes and how we propose to close them. This chapter provides the theoretical context for understanding the rest of the thesis and does not contain any original work.

2.1 Spontaneous Parametric Down Conversion (SPDC)

At the core of experimental work presented in this thesis, is a non-linear optical phenomenon called Spontaneous Parametric Down Conversion (SPDC), commonly referred to as downconversion. In SPDC, when a laser beam – the pump passes through a non-linear optical material, a pump photon may be converted into a pair of lower energy photons – the signal and idler. The probability of generating a photon pair is determined by factors like the properties of the optical material, the wavelength of the pump, and the geometry of the setup.

Like many other non-linear optical phenomena, SPDC was observed for the first time [37] after the invention of the laser. I introduce here a brief theoretical description of SPDC, along the lines of chapter 2 of [39], to help in understanding how we chose the non-linear materials used in our experiments.

I start by describing the interaction between an electromagnetic field and a material using the polarization density $\mathbf{P}$:

$$\mathbf{P} = \chi \mathbf{E}\,, \tag{2.1}$$

where χ is the susceptibility tensor and is a characteristics of the material. This expression can be expanded in series of increasing higher ranked tensors:

$$\mathbf{P} = \epsilon_0 \left(\chi^{(1)}\mathbf{E} + \chi^{(2)}\mathbf{E}^2 + \chi^{(3)}\mathbf{E}^3 + \dots \right) . \tag{2.2}$$

Expressed in this form, it is easy to identify the linear interaction, described by $\chi^{(1)}$, from the non-linear part. SPDC is a second order non-linear process described by the interaction of the non-linear coefficients $\chi^{(2)}$ [40] with the electric field of the pump, signal and idler:

$$\mathbf{P} = \chi^{(2)} E_1 E_2 . \tag{2.3}$$

This expression connects three electromagnetic fields, one associated with the left-hand side and the two explicit in the right hand one, possibly with different frequencies ω_p, ω_i, and ω_s. If the first field is our pump beam, the two other fields correspond to the field of the photon pairs that are conventionally named signal and idler. This process is subject to two main conservation criteria: energy and momentum conservation. Energy conservation can be easily expressed by noting that the total energy of the photon pairs created equals the energy of the pump photon. Written in terms of frequency:

$$\omega_p = \omega_s + \omega_i . \tag{2.4}$$

Momentum conservation, or phase matching, is almost as straightforward. If we consider the three fields as propagating plane waves in an infinite media, we can associate with each one a wavevector $\mathbf{k}_j = \frac{n_j \omega_j}{c}$, where n_j is the refractive index of the optical material at frequency ω_j. Momentum conservation can be then be written as

$$\mathbf{k}_p = \mathbf{k}_s + \mathbf{k}_i . \tag{2.5}$$

A pictorial representation of those two conditions is shown in Figure 2.1.

Combining equations 2.4 and 2.5, it is evident that phase matching is only possible in materials with suitable indices of refraction. For many anisotropic, birefringent crystals the refractive index depends on the angle of propagation with respect to the crystal axes [41]. Phase matching can then be achieved by choosing the propagation direction and polarization such that the conditions in Equation 2.5 is met. This technique is sensitive to the angle of propagation of the pump though the crystal and correlates the frequency of the generated signal and idler photons with the direction and polarization

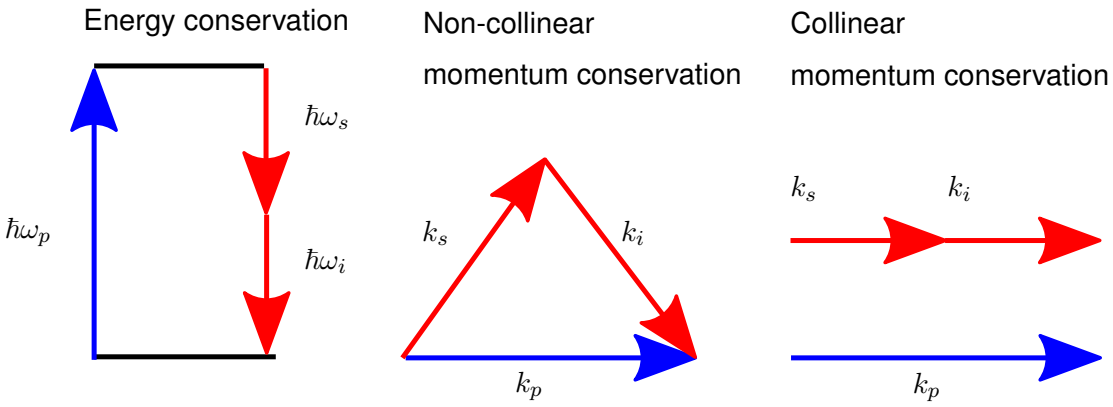


Figure 2.1: The phase matching conditions. Left: The energy of the pump is equal to the sum of the energy of the signal and idler. Center: When angle phase matched the pump and downconverted modes are usually non-collinear. The wave vectors obey momentum conservation. Right: When pumped in a collinear geometry momentum is still conserved. Practically this is feasible with non-critically phase matched or quasi-phase matched media.

of emission. It is usual to distinguish the case when the downconverted photons have parallel or orthogonal polarization: the first case is referred to as Type-I, the second as Type-II. All the downconversion processes presented in this thesis are of Type-II, i.e. the emitted photons have orthogonal linear polarization.

For photon pair generation we need to choose a material [6] with suitable mechanical and chemical properties and a large $\chi^{(2)}$. For the experiments presented in Chapter 5, we use Beta Barium Borate (BBO) as the non-linear medium. The BBO crystal [42] is mechanically hard, chemically stable, only slightly hygroscopic, it has a high damage threshold, a large birefringence and is transparent from 190 nm to 3.5 μm. Table 2.1 lists some of the optical properties of BBO. Non-collinear downconversion in BBO allows us to spatially filter the pump from the downconverted modes without any additional optical components.

2.1.1 Quasi-Phase Matching

For downconversion the wavelengths of the pump, signal and idler are typically far apart (we use a 405 nm pump which is downconverted into a 810 nm signal and idler), this means that the refractive index of the non-linear medium is usually quite different for these wavelengths (see Table 2.1 as an example). The consequence of the different

	Wavelength (nm)	Direction	
Refractive index	405	o	1.6923
		e	1.56797
	810	o	1.66107
		e	1.54599
Non-linear coefficients ($\chi^{(2)}$) at 1064 nm	Tensor element	Value (pm/V)	
	d_{31}	0.16	
	d_{22}	2.3	

Table 2.1: Some optical properties of BBO. Data was taken from [5, 6]. The direction of the ordinary and extraordinary rays are represented by o and e respectively.

refractive indices is a relative phase between the interacting waves which is not maintained and varies along the length of the medium. For a more efficient interaction, some technique must be employed to maintain the phase throughout the length of the crystal such that contributions from different parts can interfere constructively. Quasi-Phase Matching (QPM) is such a technique [43, 44, 45, 46].

The idea behind QPM is to correct the relative phase at regular intervals by means of a structural periodicity built into the non-linear medium. One of the most effective structures was found to be a periodic variation in the sign of the non-linear coefficient along medium [47]. Crystals grown with alternating ferroelectric domain structures and are called periodically poled crystals [46]. For our high efficiency source of polarization entangled photon pairs in Chapter 3, we use a Periodically Poled Potassium Titanyl Phosphate (PPKTP) crystal with a poling period of about 10 μm. Figure 2.2 shows a schematic diagram of periodic poling and quasi phase matching. In birefringent phase matching the interaction builds up amplitude only for the distance where the pump signal and idler are all in phase i.e. one coherence length, then, the sign of the phase changes and the interaction is reversed and loses amplitude. In QPM we flip the sign of the non-linear coefficient ($\chi^{(2)}$) every coherence length. Thus the interaction is allowed to constructively build up along the entire length of the crystal.

QPM does not change the energy conservation conditions but it does modify the wavenumber/momentum conservation equation (Equation 2.5) by introducing an extra

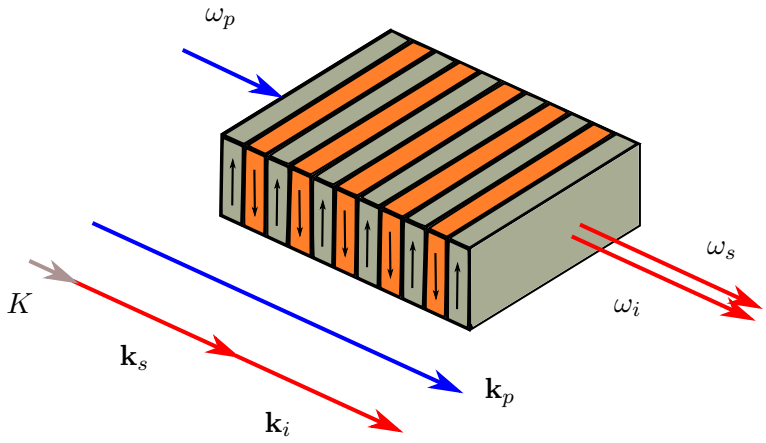


Figure 2.2: Periodic poling of a non-linear optical crystal. The sign of the non-linear optical coefficient ($\chi^{(2)}$) alternates periodically between different zones along the length of the crystal. An input pump at frequency ω_p downconverts into a signal and an idler of frequencies ω_s and ω_i. Periodic poling effectively introduces an extra wave vector $\mathbf{K}$. This ensures that the phase difference between the interacting waves remains constant throughout the length of the crystal.

term – $\mathbf{K} = 2\pi/\mathbf{\Lambda}$, where $\mathbf{\Lambda}$ is the poling period as measured along the direction of propagation of the pump.

All terms in Equation 2.5 are functions of the optical frequency and the temperature T of the crystal. The wavevectors $\mathbf{k}_p$, $\mathbf{k}_s$ and $\mathbf{k}_i$ are functions of ω_p, ω_s and ω_i and the refractive indices (n_p, n_s and n_i) of the medium, which in turn are a function of the optical frequency ω and T (as given by the Sellmeier equations [6]). Further, due to thermal expansion Λ increases with T, thus Equation 2.5 becomes

$$\mathbf{k}_p\big(n_p(\omega_p, T), \omega_p\big) = \mathbf{k}_s\big(n_s(\omega_s, T), \omega_s\big) + \mathbf{k}_i\big(n_i(\omega_i, T), \omega_i\big) + \mathbf{K}\big(T\big)\,. \tag{2.6}$$

By changing the temperature of the medium one can finely control the phase matching conditions. This allows one to tune the frequencies of the signal and idler for a given pump frequency.

The Potassium Titanyl Phosphate (KTP) crystal [48, 49] (see Table 2.2) phase matches nearly non-critically for downconversion from UV to near IR. It has large non-linear susceptibilities, low absorption and scattering losses, high surface damage threshold and a high thermal conductivity. It also has low thermo-optic coefficients which allow for a downconversion process with an excellent environmental stability.

Improving the efficiency of our source requires a good overlap between pump and downconverted modes, co-propagating these these modes using a collinear geometry is

	Wavelength (nm)	Direction	
Refractive index	405	x	1.81028
		y	1.82479
		z	1.93828
	810	x	1.74839
		y	1.75665
		z	1.84475
	Tensor element	Value (pm/V)	
Non-linear coefficients ($\chi^{(2)}$) at 1064 nm	d_{31}	1.4	
	d_{32}	2.65	
	d_{33}	16.9	
	d_{24}	3.64	
	Direction	Value ($\times 10^{-6}$/°C)	
Thermal expansion coefficients	x	11	
	y	9	
	z	0.6	

Table 2.2: Some optical and thermal properties of KTP. Data was taken from [5, 6].

one way to achieve this. For collinear downconversion from 405 nm to 810 nm KTP has one of the smallest refractive index mismatches and therefore requires a large poling period which makes PPKTP easy to manufacture.

For the above reasons we chose periodically poled KTP (PPKTP) as the non-linear optical medium for SPDC in our highly efficient source of polarization entangled photon pairs (see Chapter 3).

2.2 The Bell test

A local-realistic view of the physical world stems from a combination of two axiomatic assumptions: locality and realism. Locality means that the maximum speed of information transfer is upper bounded by the speed of light in vacuum. Realism is the assumption that a measurement outcome is predetermined before the measurement

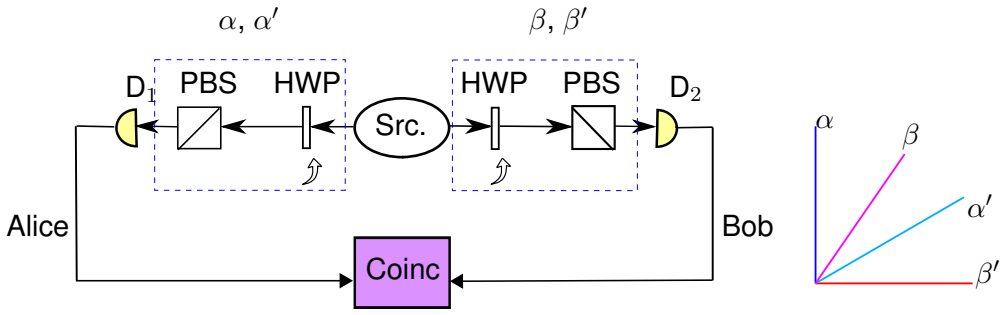


Figure 2.3: Schematic of a CH Bell test using two detectors. A source of polarization entangled photon pairs (Src.) emits one photon of each pair to Alice and the other to Bob. Alice and Bob make measurements in a polarization basis using a combination of their Half Wave Plate (HWP) and their Polarization Beam Splitter (PBS). They choose their measurement basis for each pair by rotating their HWP. Alice measures in either α or α' polarization. Bob measures in either β or β' polarization. Alice and Bob record the measurement outcomes using single photon detectors D_1 and D_2 respectively. The arrival times of each detector's click is recorded by a time stamp unit. From this data, coincidences between Alice and Bob are extracted (Coinc). At the same time the choice of measurement basis is also recorded.

is performed[1]. Quantum mechanics predicts the existence of non-local-realistic states called entangled states. In 1935, Einstein, Podolsky and Rosen suggested that quantum mechanics is either incomplete or must violate one or both assumptions of local-realism [29]. Due to the intuitive nature of the local-realistic assumptions attempts were made to answer the question — can a local-realistic theory explain the behavior of these entangled states?

In 1964, John Bell [50] devised a method to distinguish between local-realistic and non-local-realistic behavior. In the past 50 years there have been several Bell's test experiments with many different types of physical systems. The first [25] was in 1972 and was followed by several others like [31, 32, 35, 51, 52, 53, 54, 55, 56].

Today, there are a whole class of tests all known as Bell tests, they typically take the form of an inequality which, when violated, implies that the system under test is non-local-realistic. In the case of polarization entangled photon pairs (for example with the state $|\psi\rangle = \sin(\theta)|HV\rangle - \cos(\theta)|VH\rangle$), a well known Bell inequality is the CHSH proposed by Clauser, Horne, Shimony and Holt (CHSH) [57] in 1974 (a detailed

[1]We may not know what that outcome will be in advance of the measurement but the outcome is already defined.

explanation can be found in [19]). In the same year, Clauser and Horne (CH) [58] proposed another variant of a Bell's inequality which is the most relevant Bell test for this work.

When independent measurements are performed on both particles of a bipartite entangled state, they can exhibit correlations (or anticorrelations) in multiple bases. Quantum theory does not predict the outcomes of a single measurement, but rather the statistics of possible outcomes. The statistical results of several measurements in different bases are collated and used to compute one or more of the several forms of a Bell's inequality.

Figure 2.3 shows a schematic of a CH Bell's test performed with polarization entangled photon pairs. In each trial one photon pair is emitted from the source and each photon of the pair is sent towards one of the detectors. For each detector D_1 and D_2 a combination of a Half Wave Plate (HWP) and a Polarizing Beam Splitter (PBS) is used to choose a measurement basis α, α' (or β, β'). The CH inequality can be written as [58]:

$$P_{12}(\alpha,\beta) + P_{12}(\alpha,\beta') + P_{12}(\alpha',\beta) - P_{12}(\alpha',\beta') \leq P_1(\alpha) + P_2(\beta)\ , \tag{2.7}$$

where $P_i(x)$ denotes the probability of a single count on detector D_i in a trial with a measurement basis of x and $P_{12}(x,y)$ is the probability of a coincidence count between detectors D_1 and D_2 in a trial with measurement settings x and y respectively. Experimentally we measure the probabilities by normalizing the number of detected events to the number of trials $N(x,y)$ with measurement settings x, y.

$$P_{12}(\alpha,\beta) = \frac{p(\alpha,\beta)}{N(\alpha,\beta)}, \tag{2.8}$$

$$P_{12}(\alpha,\beta') = \frac{p(\alpha,\beta')}{N(\alpha,\beta')}, \tag{2.9}$$

$$P_{12}(\alpha',\beta) = \frac{p(\alpha',\beta)}{N(\alpha',\beta)}, \tag{2.10}$$

$$P_{12}(\alpha',\beta') = \frac{p(\alpha',\beta')}{N(\alpha',\beta')}, \tag{2.11}$$

$$P_1(\alpha) = \frac{s_1(\alpha)}{N(\alpha)}, \tag{2.12}$$

$$P_2(\beta) = \frac{s_2(\beta)}{N(\beta)}, \tag{2.13}$$

where $s_1(\alpha)$ ($s_2(\beta)$) are the number of single events on detector D_1 (D_2) when measuring in basis α (β) and $p(x, y)$ is the number of coincidence events in the x, y basis.

It has been shown [58] that the inequality given in Equation 2.7 will not be violated for any bipartite local-realistic system. However, the CH inequality can be violated by a non-local-realistic system (such as a polarization entangled photon pair state).

2.3 Loopholes in a Bell test

In all the experimental Bell tests to date, violations could only be observed under certain assumptions [59]. This leaves all available experimental results open to local-realistic interpretations. Commonly, this class of interpretations are called Local Hidden Variable (LHV) theories. They postulate the action of local-realistic influences that may alter the outcome of a Bell test. To conclusively rule out the influence of LHVs we must take steps to avoid/close all loopholes. There are three main loopholes in a Bell test: locality, detection, and freedom of choice loopholes. All of which have been closed individually in different experiments. However they have never been closed at the same time.

2.3.1 Locality/communication loophole

This loophole was first addressed by Aspect et al. and Weihs et al. [31, 52]. A Bell test assumes that the measurements on each half of the photon pair are made independently. The measurement and detection on each side can be thought of as belonging to Alice and Bob respectively. For the measurements to be independent there must be no communication between Alice and Bob. For example, a LHV could relay Alice's choice of measurement basis to Bob's apparatus. Any information relayed by a LHV between Alice and Bob can be considered as "signaling". However, any LHV must be limited by the speed of light in vacuum. Consequently, if the components of the experiment are sufficiently space-like separated then this loophole can be closed.

Figure 2.4 shows an experiment consisting of a source in the middle followed by a random number generator, polarization switch and detector on either side. Each of these components must be well separated such that the measurements of every trial are completed before signaling can occur.

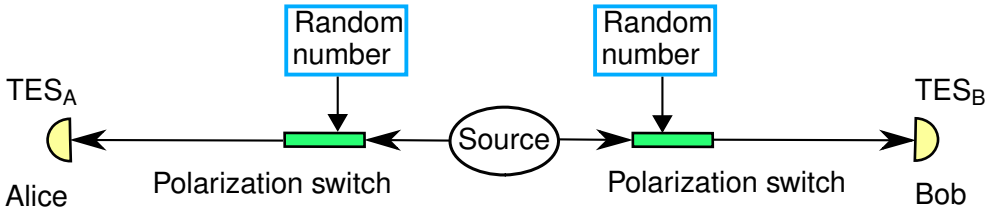


Figure 2.4: Schematic of space-like separated experimental components for closing the locality loophole in a Bell's test. A fast polarization modulator can change the measurement basis faster than a LHV can influence the measurement outcome.

Figure 2.5 shows a space-time diagram of a Bell test. The horizontal axis represents distance or space-like separation; the vertical axis represents time. A 45° line represents the speed of light in vacuum. The source is placed at zero distance (see Figure 2.4) and at time zero emits a photon pair. To close the locality loophole, Alice and Bob must be able to make independent selection (using a random number generator) and implementation (via a fast polarization modulator) of their measurement basis choice. Alice (Bob) must also be able to detect[1] her (his) single photon of the pair before signaling occurs. The intersection of light cones originated from Alice's and Bob's decision of what basis to measure in, forms the "signaling zone" (see Figure 2.5) — a region in space-time wherein Alice and Bob can influence each others measurements.

So far, the locality loophole has only been closed using photons. Aspect et al., were the first to experimentally close this loophole in 1981 [32]. They were followed by Tittel et al., in 1998 [51] who used a separation of more than 10 km. Another experiment in the same year by Weihs et al. used random number generators to close both the locality and freedom of choice loophole [52].

Losses in fiber or free space transmission of the entangled photon pairs limits the distance of space-like separations while closing the detection loophole. To be able to close the locality loophole with a small separation, we must use a fast polarization switch. We have built a electro-optic polarization switch capable of implementing a basis choice in about 3 μs which means that we would need about 900 m of separation between the source and switch. More details about this switch can be found in Appendix A.

[1] The time taken to detect a photon is inclusive of the detection jitter.

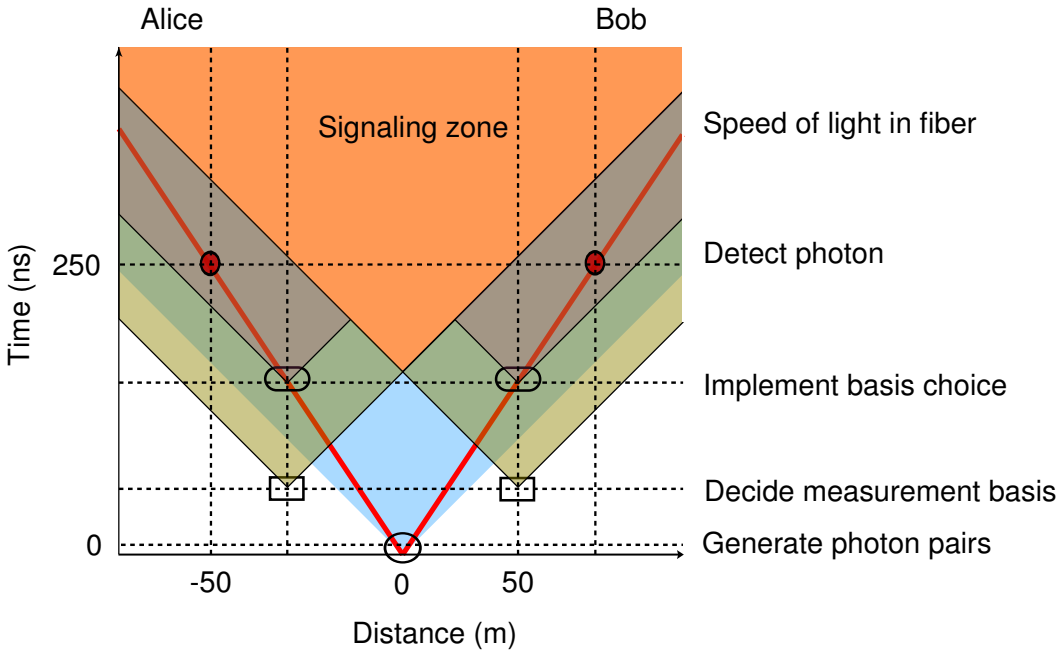


Figure 2.5: The locality loophole in a Bell test can be avoided if the source, random number generators, polarization switches and detectors are sufficiently space-like separated. This figure is a space-time diagram. A 45° line (thin black) represents the speed of light. Each event generates its own "light cone" (colored triangles) and can only influence other events if they are in its light cone. The intersection of light cones on Alice's and Bob's sides from the "signaling zone". In this region Alice and Bob are no longer capable of making truly independent measurements. To close the locality loophole Alice and Bob must complete the experiment outside of the signaling zone. The thick red lines represents the speed of light in the optical fibers.

2.3.2 Detection loophole or fair sampling assumption

No real experiment can have a 100 % system efficiency[1]. There are always some losses. A LHV that could selectively induce losses in the experiment could influence the outcome [60, 61], to avoid this we need to be able to detect a sufficiently large fraction of all pairs. Hence the name detection loophole. Several experiments (for example [31, 62]), have assumed that the signals they detect constitute a fair and unbiased sampling of all generated pairs. This can only be true if the losses are random. This assumption is called the fair sampling assumption, hence the other name for this loophole.

[1]System efficiency refers to the probability that a generated photon pair is detected as a pair. This is inclusive of all losses and is smaller than the detection efficiency.

Fortunately, to close this loophole we do not require a 100 % system efficiency. For a maximally entangled state the minimum efficiency needed to see a violation is $2(\sqrt{2}-1) \approx 83\,\%$ [63, 64] (without making the fair sampling assumption). Even this relaxed requirement on the detection efficiency is difficult to achieve. Using non-maximally entangled states it is possible to reduce this requirement drastically to 66.7 % [3]. Consider a non-maximally entangled state given by $|\psi\rangle = \sin(\theta)|HV\rangle - \cos(\theta)|VH\rangle$. Given a system efficiency, Eberhard [3] shows us how to compute θ of the entangled state which would yield the largest violation of a Bell's inequality without a fair sampling assumption. For a given θ we can choose α and β to minimize the right hand side of Equation 2.7, while choosing α' and β' to maximize the left hand side of the CH inequality.

Imperfections in the detectors and stray light reaching them can cause the detectors to register a detection event ("click") even in the absence of a photon from the system being tested, these photons are called background counts. In the absence of a pair of photons from the source, there is a certain probability that two detectors will click within the time window used to detect a coincidence; the resulting spurious coincidence events are called accidentals. It is important to note that for a loophole free test a correction for background counts and accidentals cannot be applied. Background counts must be minimized because they increase the values of $P_1(\alpha)$ and $P_2(\beta)$ in Equation 2.7 thereby making small violations harder to observe.

There have been a few notable experiments which closed this loophole. In 2001 Rowe et al., closed the detection loophole in a Bell test for the first time [53]; using correlations in the properties of $^9Be^+$ ions, they were able to detect the state of the ions with an efficiency of more than 90 %. However, the two ions were placed only 3 μm away from each other and they were unable to close all of the other loopholes. They were among the first to violate a Bell inequality with a system other than photons. In 2009 Ansmann et al. [56], performed the first experiment testing Bell inequalities with solid-state qubits (superconducting Josephson phase qubits). They violated a Bell inequality by 244 standard deviations. Once more they failed to close the locality loophole. They were only able to separate the qubits by a few mm. Very recently two groups have managed to close the detection loophole with photons [65, 66]. This makes photons the first and, so far, only system where all loopholes have been closed; albeit in different experiments.

2.3.3 Freedom of choice loophole

Alice and Bob must choose measurement bases for each trial. Not only must this choice be done fast enough to prevent signaling but it must also be made at random [67]. Any pattern/predictability in the choice of measurement basis could allow a LHV to influence the measurement outcomes. For a loophole free Bell test one should use a random number generator to make the basis choice. This choice would need to be done outside the light cone of the source (see Section 2.3.1). This loophole was closed along with the locality loophole in several experiments with entangled photons [32, 52].

2.3.4 Other loopholes

There are also several other possible loopholes that must be addressed. For a violation to be conclusive and loophole free, one must also account for all experimental and statistical errors.

The light source might emit several pairs at the same time or within a short timespan causing error at detection. For our source, the probability of emitting two or more photon pairs within the TES jitter time is small (≈ 25/s at FWHM jitter) (but must still be accounted for). A more significant problem is encountered while using a Continuous Wave (CW) pump. Since SPDC is a probabilistic process we cannot know when a photon pair is generated (unless we detect the photons). To define a trial we can use a time bin. If the pair is generated at the end of the first time bin then it may only be detected in the second. Thus, if one is not careful it is possible to mistake the results of previous trial for the next [68].

A major problem is that correlation tests are always statistical tests, they are carried out on a finite number of pairs. Thus, the correlation functions have uncertainties which limit the confidence in the degree of violation of a Bell inequality. Therefore, statistical errors must also be treated carefully. The typical approach is to assume a Shot noise error for the number of photon counts. This method of data analysis is primarily intended for characterizing precision not accuracy and is only applicable when the central limit theorem [1] is applicable. The conclusions drawn from such a

[1]The central limit theorem states that the arithmetic mean of a large number of iterates of independent random variables follows a normal distribution. The theorem assumes that the data is sampled randomly and that the sample values are independent of each other. These assumptions are not necessarily justified for a loophole free Bell test.

data analysis are weakened by distributional assumptions. Further, it is also necessary to account for teh posibility of adversarial variations of teh local realistic model in time [69]. The group of Knill argue that the shot noise may not be the best method to evaluate the statistical confidence in a violation, instead they propose an alternative method to evaluate the error in a violation [70]. Their approach is an implementation the statistical p values[1] used in canonical hypothesis testing. They argue that one needs to take into account the possibility that a finite set of N data points generated by a local realistic model can violate a Bell's inequality due to statistical fluctuations.

2.3.5 Practical Considerations

The experimental closing of all loopholes in a Bell test is a large and complex undertaking. Besides the technical challenges there are several logistic issues. The detectors need to be separated by a distance ($\approx 100\,\mathrm{m}$) which depends on their timing jitter. As shown in Figure 2.4, the source of polarization entangled photon pairs needs to be located in-between the detectors and the fast polarization modulators and random number generators should be between the source and detector on each side. Even though we couple the light into optical fibers, the above components should roughly be in a straight line and the fibers should have as few bends as possible. This is because of the reduced speed of light in optical fibers as compared to the maximum speed of LHVs ($\approx\ 3 \times 10^8\,\mathrm{m/s}$). Further, long fibers lead to increased losses.

The fibers connecting the source to the polarization modulator should be maintained polarization neutral, otherwise the birefringence of the optical fibers could affect the choice of measurement basis. Stress induced birefringence within the optical fibers will change the polarization of light propagating through the fiber. Mechanical vibrations, temperature fluctuations, etc will affect the polarization of light at the output of the optical fiber. The choice of measurement basis in our experiment is implemented by Half Wave Plates (HWPs) or an electro-optic polarization modulator. These devices rotate their input polarization by a fixed angle. Consequently, the stress induced variations in the polarization would affect the choice of measurement basis.

With a system efficiency of 75 % the optimal non-maximally entangled state needed is $|\psi\rangle = 0.9688|HV\rangle \pm 0.2477|VH\rangle$ and the optimal measurement bases are $7.506\,^\circ$ and

[1] The p-value is the probability of obtaining a test statistic result at least as extreme or as close to the one that was actually observed, assuming that the null hypothesis is true.

48.322° for Alice and 172.495° and 131.683° for Bob. Deviations from this state or these angles will result in a less than optimum violation. With the optimal settings we expect a violation of 2.0015. To obtain a violation by 6 standard deviations, we need to acquire data for at least 4 days at a rate of 10 000 pairs/s.

Chapter 3

Highly efficient source of polarization entangled photon pairs

Polarization entangled photon pairs or heralded photons are a fundamental resource for a wide range of fields like quantum communication [71], computation [72] and metrology [73]. The underlying protocols behind these applications often require the detection of a large fraction of all photon pairs. To perform such experiments, one needs a source of photon pairs with a high efficiency[1]and single photon detectors with low losses. While photo detectors have come close to unit detection efficiency [4], photon pair sources seem to be the current bottleneck in applications requiring a high efficiency. In this chapter I discuss our high efficiency source of polarization entangled photon pairs[2]. The results presented in this chapter have also been presented in conferences [74, 75].

Photon pairs are produced via collinear SPDC in a PPKTP crystal (see Section 2.1). Section 3.1 explains how we detect these pairs of photons and the efficiency of the source. Entanglement is generated by combining two downconversion paths in a Sagnac interferometer (Section 3.2). The same section also describes the experimental setup we

[1]Efficiency of the source refers to the heralding efficiency or the pairs to singles ratio as mentioned in Section 3.1 and shown in Equation 3.1. It does not refer to the probability that a pump photon will undergo downconversion (also known as the generation efficiency).

[2]Measurements presented in this chapter are all performed with Silicon Avalanche Photo-Diodes (Si APDs). These APDs have detection efficiencies of about 50 % (The measurement of APD detection efficiency can be found in Section 4.3.).

use. The alignment procedure of this setup can be found in Appendix C. The source is capable of producing states with a variable degree of entanglement (see Section 3.2.2) including maximally entangled states. We measured the polarization correlation visibility (Section 3.2.1) and fidelity for these states (Section 3.2.2).

The efficiency of the source depends on the focusing of the pump and collection modes. Section 3.3 shows how they were measured and optimized. We obtained a heralding efficiency of more than 39 % as measured by Silicon Avalanche Photo-Diodes (Si APDs). Section 3.4 discusses the efficiency of the source and the various sources of losses.

In Section 3.5 we demonstrate the wavelength tunability signal and idler photons, while in Section 3.6 we measure their bandwidth.

I have been responsible for building, from scratch, the experimental setups presented in this chapter. I have also performed all the measurements and characterizations shown. I have used methods and predictions developed by others to plan the setup and compare results, these sources are cited where applicable.

3.1 Detecting photon pairs

A single pump photon can decay into two daughter photons (signal and idler) obeying energy and momentum conservation (see Section 2.1). In our case, these daughter photons are of orthogonal polarization (type II SPDC). The standard method for detecting photon pairs is the timing coincidence method first demonstrated by Burnham and Weinberg [76]. Photon pairs emitted from a single crystal in a polarization entangled state was first demonstrated by Kwiat et al., in 1995 [33].

We use type-II downconversion in a Periodically Poled Potassium Titanyl Phosphate (PPKTP) crystal (see Section 2.1.1). To generate entanglement we follow the scheme of Fiorentino et al., [38] and use a Sagnac configuration (see Section 3.2).

To detect photon pairs we separate the signal and idler using a polarizing beam splitter and then collect them into two single mode fibers. The number of events registered by each detector per unit time is called the singles rate denoted by s_1 and s_2. To register a coincidence event we first define a certain "coincidence time window" (τ_c). If the two detectors register an event (click) within this time window then we call it a coincidence/pair. The rate of such pair events is denoted by p. The heralding

efficiency of the source (η) is given by the pair to singles ratio as shown in Equation 3.1 and is also called the heralding efficiency.

$$\eta = \frac{p}{\sqrt{s_1 \times s_2}}\,. \tag{3.1}$$

The measured efficiency of the source can be improved by reducing losses. TESs have a detection efficiency of more than 98 % [4]. We use these detectors (see Chapter 4) to avoid losses due to the limited detection efficiency of Si APDs ($\approx 50\,\%$) . To reduce optical losses, we minimize the number of optical components and use Anti-Reflection (AR) coatings on all optical surfaces (including the fibers). Another important mechanism for losses are imperfections in the mode overlap between the pump and collection modes. In Section 3.3 we optimize these modes for a high efficiency.

3.1.1 Corrections to the efficiency

We apply two corrections to this efficiency: accidentals correction and dark/background count correction. There is a certain probability that two detectors will click within τ_c due to uncorrelated single photons. These events are called accidentals or accidental coincidences; assuming a low count rate, their rate (a) is given by

$$a = s_1 s_2 \tau_c\,. \tag{3.2}$$

Typically we have singles rates of about 10,000 /s and we use $\tau_c \approx 5\,\text{ns}$. This results in an accidental coincidence rate of about 0.5 /s which is not significant compared to our pair rate of about 4000 /s. To ensure that we detect most pairs, τ_c must be larger than the timing jitter of the detectors. The APDs we use have a timing jitter $< 1\,\text{ns}$, but our TESs have a FWHM jitter of about 200 ns. In this case we use $\tau_c \approx 800\,\text{ns}$ resulting in a much larger a (about 80 /s for the same rates) .

The second correction is the dark/background correction. A detector may register spurious counts due to electrical, thermal or optical noise (see Section 4.1). This can often be corrected for by blocking the input/pump and measuring the dark/background count rates of each detector (d_1 and d_2). Thus the corrected heralding efficiency is given by

$$\eta = \frac{p - a}{\sqrt{(s_1 - d_1)(s_2 - d_2)}}\,. \tag{3.3}$$

3.2 Generating entanglement

Pumping the crystal from a single direction generates pairs of photons. In each single pass SPDC process, the genearated signal and idler photons are strongly correlated in time and generated with orthogonal polarizations. However, they are *not* polarization entangled. In order to obtain a polarization entangled state, we combine the output of the two single pass processes onto a Polarizing Beam Splitter (PBS). This scheme was first implemented in 2003 by two independent groups: Fiorentino et al. [38] and Shi and Tomita [34]. The coherence between the two pump paths is transferred to the downconverted modes, resulting in a superposition state with a fixed phase relationship. Figure 3.1 shows the experimental setup with the crystal is placed at the middle of a Sagnac interferometer. It consists of two mirrors and a PBS cube (called the Downconverted Sagnac PBS (PBS_{DS})), forming a right angled isosceles triangle (as shown in Figure 3.1). The PPKTP crystal is placed at the middle of the hypotenuse of this triangle and a HWP (called the Downconverted Sagnac HWP (HWP_{DS})) is oriented at 45 ° and introduced into one arm.

The Sagnac geometry is a common way to generate polarization entanglement in type II collinear downconversion setups. A Sagnac interferometer has two counter propagating paths in the same optical mode. This is useful for combining the two downconverted modes to obtain polarization entanglement. Shi et al., [34] used the same Sagnac mirrors and PBS_{DS} for the pump and downconverted modes. Any slow fluctuations in the path length would effect both the pump and the downconverted modes and would thus be automatically compensated for. We use a different geometry (see Figure 3.2) which allows a decoupling of the alignment degrees of freedom (as in [38]) This also allowed us to independently optimize the individual optical components for each wavelength.

Both the above implementations [34, 38] generated a polarization entangled state in the same manner. Each pump direction results in an independent downconversion process producing a Horizontally polarized (H) signal (s) and a Vertically polarized (V) idler (i). The mode propagating in the clockwise direction within the Sagnac loop is termed “1” while the other is “2” (see Figure 3.1). The output modes of the PBS_{DS} are “3” and “4” which are also referred to as the collection arms. The upward pump (in Figure 3.1) generates a photon pair ($|H_s\rangle_1$, $|V_i\rangle_1$) in mode 1. After passing through

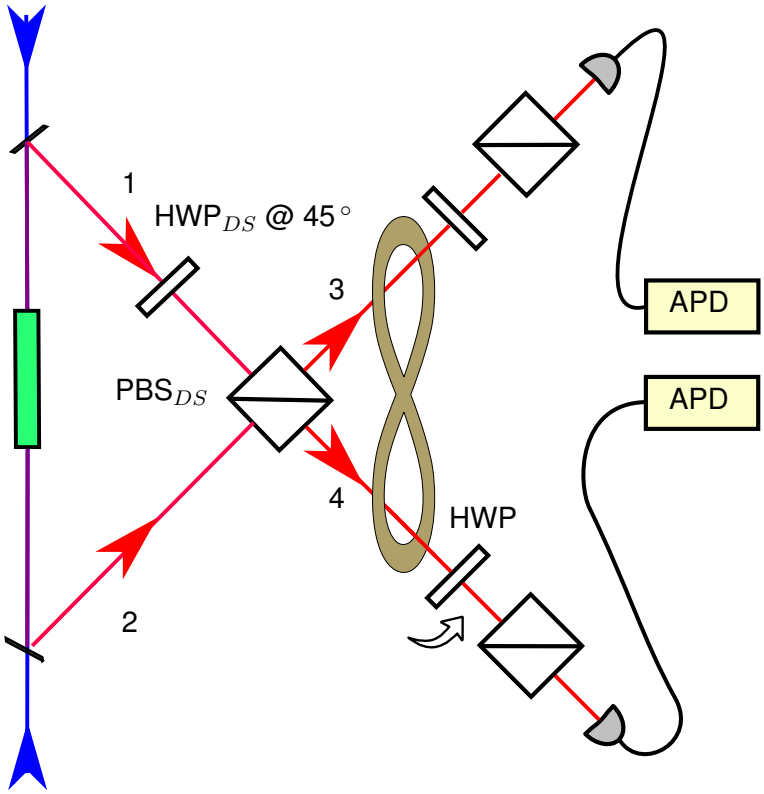


Figure 3.1: To generate polarization entangled photon pairs, the crystal is pumped from both directions in a Sagnac configuration. The downconverted photon pairs are emitted along mode 1 or 2. They are then interferometrically recombined on the Downconverted Sagnac PBS (PBS$_{DS}$). The two photon state between modes 3 and 4 is entangled. A HWP and PBS cube in each collection arm serve as the measurement polarizers. The photon pairs are collected into single mode fibers and detected using APDs.

the HWP$_{DS}$, the polarization of these photons are rotated by 90° into ($|V_s\rangle_1$, $|H_i\rangle_1$). Similarly, the downward pump produces the pair ($|H_s\rangle_2$, $|V_i\rangle_2$) in mode 2. The counter propagating pairs in modes 1 and 2 are combined at the PBS such that ($|V_s\rangle_1$, $|H_i\rangle_1$) is transformed into ($|V_s\rangle_3$, $|H_i\rangle_4$) while ($|H_s\rangle_2$, $|V_i\rangle_2$) is transformed into ($|H_s\rangle_3$, $|V_i\rangle_4$). Thus the two photon state emerging in modes 3 and 4 is

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H_s\rangle_3|V_i\rangle_4 + \mathrm{e}^{\mathrm{i}\phi}|V_s\rangle_3|H_i\rangle_4\right). \tag{3.4}$$

The phase difference (ϕ), between modes 1 and 2, is controlled by the phase difference between the upwards and downwards pump modes. (see Section 3.2.3).

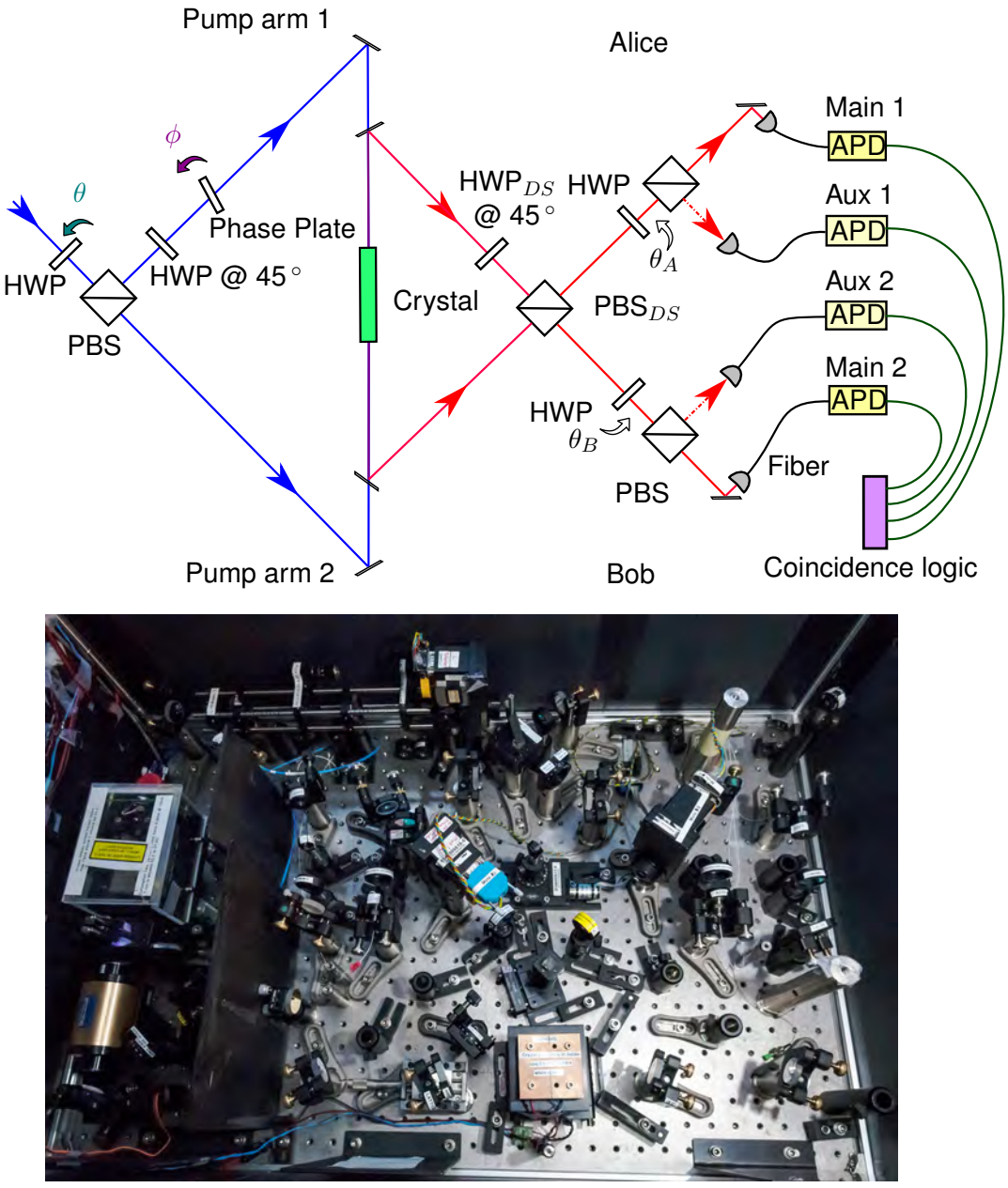


Figure 3.2: The experimental setup showing the high efficiency polarization entangled photon pair source. The pump is mode filtered, spectrally filtered and horizontally polarized by the same optical elements shown in Figure 3.7. The pump is split using a PBS and is directed into the crystal from either end. The balance of pump power in the two pump arms is controlled by a HWP before the pump PBS. The phase difference between the two pump arms is controlled by adjusting the phase plate. Downconverted light is interferometrically recombined at the Downconverted Sagnac PBS (PBS_{DS}) to produce a polarization entangled state as described in Section 3.2. In each collection arm a HWP and a PBS form the measurement polarizers. The two outputs on either collection arms are coupled into single mode fibers connected to APDs.

3. HIGHLY EFFICIENT SOURCE OF POLARIZATION ENTANGLED PHOTON PAIRS

Due to the birefringence of the crystal, orthogonally polarized photons travel at different group velocities leading to a longitudinal walk-off which renders the photons partly distinguishable [77]. The HWP_{DS} removes this distinguishability by inverting the walk-off in mode 1 with respect to mode 2. The polarization correlation visibility of the source of polarization entangled photon pairs depends on the precision and orientation of HWP_{DS}.

The entangled state is not produced from the interference of two different pairs of photons[1], instead it is produced by the indistinguishability of modes 1 and 2 when measuring on modes 3 and 4.

Type-II collinear parametric downconversion from pump light at 405 nm to 810 nm occurs within a 25 mm long periodically poled Potassium Titanyl Phosphate ($KTiOPO_4$, PPKTP). The pump light is generated by a grating stabilized Ondax 405 nm laser diode with a bandwidth of 160 MHz [78]. The spatial mode of the pump is filtered using a single mode fiber and tailored by a two-lens telescope; as shown in Figure 3.7. A blue glass filter is used to reduce the IR fluorescence caused by the pump in the fiber. The initial polarization is set by a Glan-Taylor polarizer and can be rotated using a half wave plate. We use a PBS to split the pump in two modes. Each of the two modes is independently directed and focused separately into the crystal from two opposite directions. The waist of both the pump modes (ω_{0_p}) is 265 μm and they are positioned at the middle of the crystal. We experimentally optimized the focusing of the pump and collection modes for the maximum efficiency (pairs to singles ratio). Section 3.3 provides more information on this.

We use dichroic mirrors to separate the downconverted modes from the pump modes. The modes resulting from the two downconversion processes are combined in a PBS, then focused into single mode 780-HP fibers by a telescope consisting of a plano-convex lens (f = 300 mm) and a C230-B aspheric lens (f = 4.51 mm). We use collection waists (ω_{0_c}) of 160 μm which are also centered in the crystal (see Section 3.3).

As shown in Figure 3.2, each collection arm is coupled into main and auxiliary (aux) couplers/fibers/detectors. The main collection fibers are spliced to the fibers connected to the TES detectors and the other output of the measurement PBSs are coupled into auxiliary APD detectors. Due to geometric constraints, the coupling of downconverted

[1] Using a coincidence window $\tau_c = 5$ ns, such four photon events occur at a rate of about 0.08 /s.

modes was optimized only for the main collection fibers. The auxiliary collection fibers and detectors were used to measure the state produced and lock the phase (ϕ) (see Section 3.2.3).

3.2.1 Polarization correlation visibility

When the crystal is pumped from both directions (see Figure 3.2), the coherence between the two pump paths is transferred to the downconverted modes, resulting in a superposition state with a fixed phase relationship. This phase (ϕ) is the same as the phase difference between the two pump arms. The resulting polarization entangled state can be described as

$$|\psi\rangle = \sin\theta|HV\rangle + e^{i\phi}\cos\theta|VH\rangle\,. \tag{3.5}$$

By controlling the relative intensities between the two pump arms, we adjust the balance (θ) between $|HV\rangle$ and $|VH\rangle$.

Once a state is produced we need to measure the quality of entanglement. For maximally entangled states ($\theta = 45^\circ$ and $\phi = 0$ or π) one such measure is the polarization correlation visibility [79].

In each collection arm (Alice/Bob) there is a motorized HWP and a PBS. By rotating the HWP, Alice and Bob can choose any linear polarization as their measurement basis. During a visibility measurement, we record the number of coincidences as a function of Bob's HWP angle (θ_{Bob}) while keeping Alice's HWP fixed. The visibility (v) is given by the contrast of the maximum (M) and minimum (m) values of the coincidences [79] as

$$v = \frac{M - m}{M + m}\,. \tag{3.6}$$

If Alice's HWP is fixed ($\theta_{Alice} = 0$ or 45°) such that she measures in the H or V basis and the minimum of the coincidences occurs at either $\theta_{Bob} = 0^\circ$ or at $\theta_{Bob} = 45^\circ$ then the visibility measurement is said to be in the H/V basis.

To evaluate the quality of entanglement we must measure the visibility in at least two bases. These bases should be orthogonal on the Bloch sphere[1]. One of the common choices for the measurement bases are H/V and $\pm 45^\circ$.

[1]The Bloch sphere is a geometrical representation of the state of a qubit. For a polarization qubit, it is the same as the Poincarè sphere. A point on the equator, represents plane polarization, the poles represent circular polarization and any other point on the surface represents an elliptical polarization.

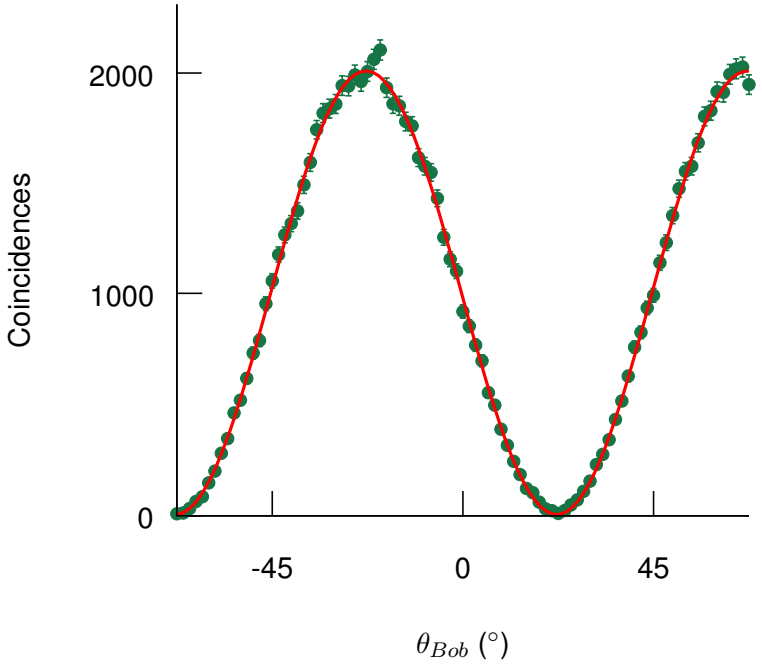


Figure 3.3: Polarization correlation visibility in the $\pm 45^\circ$ basis. The visibility obtained from a fit is $99.4 \pm 0.2\,\%$. The visibility was measured when the source was set to produce a maximally entangled state – $|\psi\rangle^- = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$. The integration time for each point was 800 ms.

For our source, the photon pairs are generated via type II downconversion[1] i.e. one photon is always H and the other V. Hence, the visibility in the H/V basis is limited by the extinction ratios of the PBS$_{DS}$ and measurement polarizers. The visibility measured in the H/V basis is $100.1 \pm 0.2\,\%$ (the visibility in the HV basis is limited by the measurement polarizers we use). This would be the case even if the state produced by our source was not entangled. The measurement in the $\pm 45^\circ$ basis is thus the best indicator of the entanglement quality.

We measured the visibility in two bases H/V and $\pm 45^\circ$. Figure 3.3 shows the data obtained while measuring the visibility in the $\pm 45^\circ$ basis. By fitting to a $\sin^2$ function we obtained the polarization correlation visibility of $99.4 \pm 0.2\,\%$ in the $\pm 45^\circ$ basis.

[1]Type II downconversion generates a signal and idler with orthogonal polarizations. We define these polarizations as H and V and align all other optical elements to follow this convention defined by the crystal axes.

3.2.2 Tunable degree of entanglement

We are not restricted to generating maximally entangled states. Our source is capable of generating a wide class of two photon polarization entangled states of the form:

$$|\psi\rangle = \sin\theta|HV\rangle + \mathrm{e}^{\mathrm{i}\phi}\cos\theta|VH\rangle\,. \tag{3.7}$$

We use a HWP before the pump PBS to control the intensity of the two pump arms. The relative intensity in each pump arm directly controls the relative intensity in each downconverted mode. Thus by rotating that wave plate, we control the balance of $|HV\rangle$ with respect to $|VH\rangle$. In other words, the angle of the pump HWP can be mapped to θ. The phase ϕ can be controlled by tilting the phase plate as discussed in Section 3.2.3.

This ability to generate non-maximally entangled states makes our source ideal for a loophole free Bell test (see Section 2.3.2). With an observed detection efficiency of 75.2 %, a state given by $\phi = \pi$ and $\theta = 1.3205$ rad will provide the maximal violation of a loophole free Bell test (see Section 2.3.5). We set our source to produce such a state and calculated its density matrix σ. We then made measurements in various linear polarization bases to perform an "in-plane" tomography of this state. Since the downconversion process only produces photons in the $|H\rangle$ or $|V\rangle$ states we assume that there are no circularly polarized components. From this we obtain the measured density matrix ρ.

The fidelity is a measure of the "similarity" of these states and is given by

$$F(\rho,\sigma) = \mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]\,. \tag{3.8}$$

We observed a fidelity of 99.3 %. We measured the fidelity for several different non-maximally entangled states which would correspond to observed detection efficiencies between 70 – 80 %. For each of these states the fidelity was measured and the average value was 99.3 ± 0.1 %.

3.2.3 Locking the phase

The phase ϕ of the entangled state produced by the source ($|\psi\rangle = \sin\theta|HV\rangle + e^{i\phi}\cos\theta|VH\rangle$) is sensitive to any change in the relative path length between the pump and downcon-

verted Sagnac loops (see Figure 3.2). The change in path length can be caused by mechanical motion (vibrations, drifts, creeping, etc) of optical components, air currents, temperature fluctuations/gradients, etc. When measuring the polarization correlation visibility of a maximally entangled state in the $\pm 45°$ basis, the effect of this small change in ϕ is seen as a reduction in the measured visibility. Figure 3.4 shows the degradation in visibility with time. Every ≈ 42 min the source was adjusted such that the phase $\phi = \pi$. A loophole free Bell test with our efficiency and count rates requires a measurement time of a few days in order to accumulate enough statistics for a violation by six standard deviations. It is important to ensure that the entangled state produced by the source is the same throughout this period. One way to achieve this is to periodically readjust ϕ.

This adjustment of ϕ was made by tilting a "phase plate" in one of the pump modes (see Figures 3.2 and 3.5). The phase plate is a glass microscope cover slip with a thickness of about 0.1 mm. By rotating the phase plate by an angle θ_p, we can vary the path length difference and hence the phase between the two pump arms. This also varies the phase between the downconverted modes (1 and 2 in Figure 3.1) and consequently the phase ϕ.

To obtain a maximally entangled state we set ϕ to π (or 0). This is done by using the auxiliary detectors in each collection arm of the source. The measurement HWPs in each of the collection arms are rotated such that we measure in the $+45°$ and $+45°$ (or $+45°$ and $-45°$) linear polarization bases. The phase plate was then rotated by an angle θ_p while recording the number of coincidence events. Figure 3.5 shows the results of one such measurement. θ_p was initially scanned in large steps. Once we found the approximate angle of minimum pairs, we scanned θ_p across that region in smaller steps. By fitting the data we obtain the value of θ_p when $\phi = \pi$ (or 0). The phase plate is then rotated to this angle. This procedure is one locking cycle and takes about 94 s.

3.2.4 Stability over time

To demonstrate the stability of the state we set the source to produce a maximally entangled state. We then repeatedly measure the visibility in the $\pm 45°$ basis.

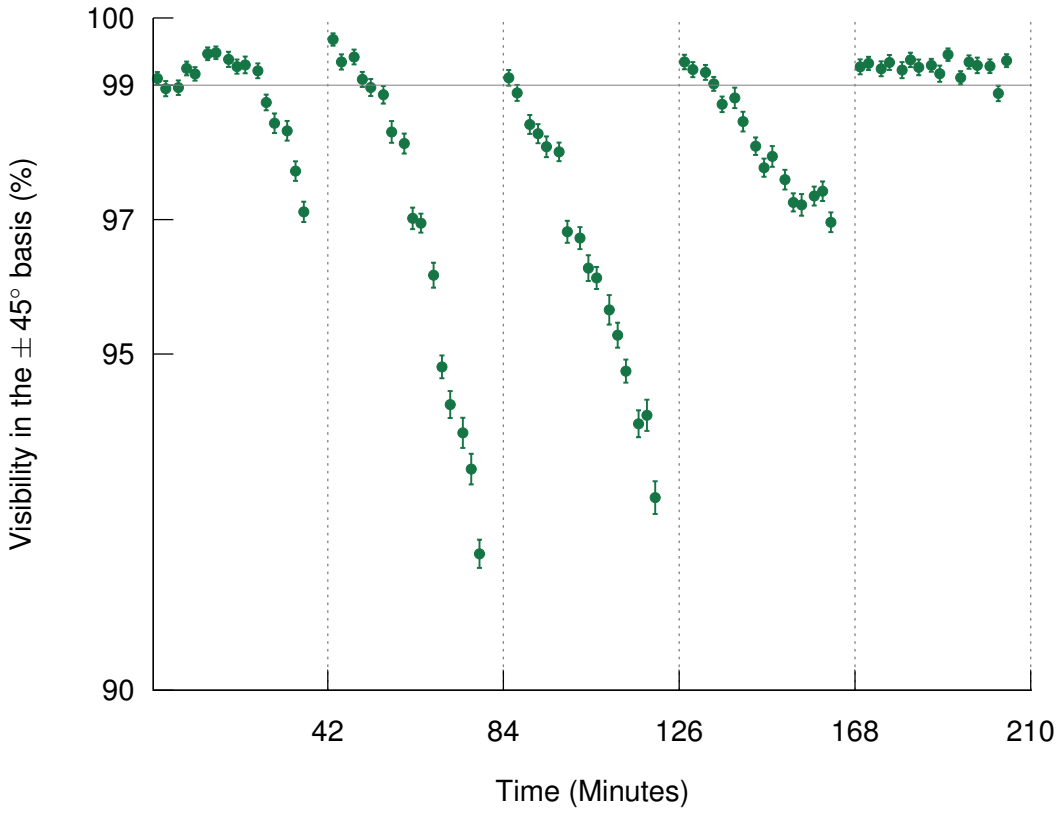


Figure 3.4: Graph showing the drift in the polarization correlation visibility over time. Due to mechanical instabilities, the phase ϕ of the entangled state slowly changes. When the state is no longer maximally entangled, the visibility as measured in the $\pm 45°$ basis drops. We adjusted ϕ every ≈ 42 min (as indicated by the ticks on the x-axis) to be equal to π.

We ran a locking cycle every 5 minutes and measured the visibility for 6 hours. The visibility is plotted as a function of time in Figure 3.6. The visibility remained stable for 6 hours and the average value was 99.3 ± 0.15 %.

The stability of our source over extended periods of time makes it suitable to perform experiments which require long data acquisition times such as a loophole free Bell test.

3.3 Collection optimization

The optimal pump and collection modes for a high heralding efficiency have been the subject of extensive theoretical study. Two notable efforts are the Boyd-Kleinman criteria [80] and the Bennink criteria [14]. The optimal parameters calculated by these

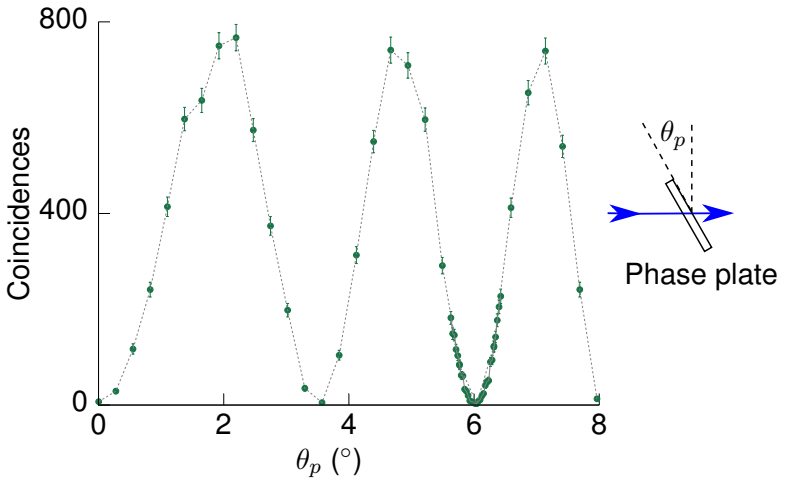


Figure 3.5: Data from a locking cycle. The measurement polarizers are fixed in the 45 ° basis and the phase plate is tilted to minimize the coincidences. We first move the phase plate in coarse steps to find the approximate position of the minimum and then in fine steps near that position. The frequency of the oscillations is least when the phase plate is perpendicular to the pump and increases with tilt.

theories can differ from experimentally optimized ones. This is due to a number of factors including clipping of the beam due to the limited size of the crystal, the deviation of the pump and collection modes from Gaussian, and crystal and alignment imperfections. Consequently it is useful to measure the dependence of the efficiency on the focusing of the pump and collection modes.

3.3.1 Focusing pump and collection modes

We pumped the crystal from a single direction as shown in Figure 3.7. We call this setup the "single pass setup". We use a S405-XP single mode fiber to spatially filter the pump mode coming from the 405 nm laser. The output of this fiber is collimated using a C230-TME-A aspheric lens from Thorlabs with a nominal focal length of 4.51 mm. The spot size of the beam ($\omega(z)_p$) at the output of this coupler is 350 μm. The distance from this coupler to the center of the crystal is 1.35 m. We need to ensure that the beam waists (ω_0) for the pump (ω_{0_p}) and collection (ω_{0_c}) modes are optimal. For the pump, the best ω_{0_p} was found to be 265 μm[1]. This value was obtained by tuning the

[1]The optimum waists for the pump signal and idler modes were obtained experimentally as discussed in Section 3.3.2; for each pump waist, the signal and idler waists were tuned for the best source efficiency.

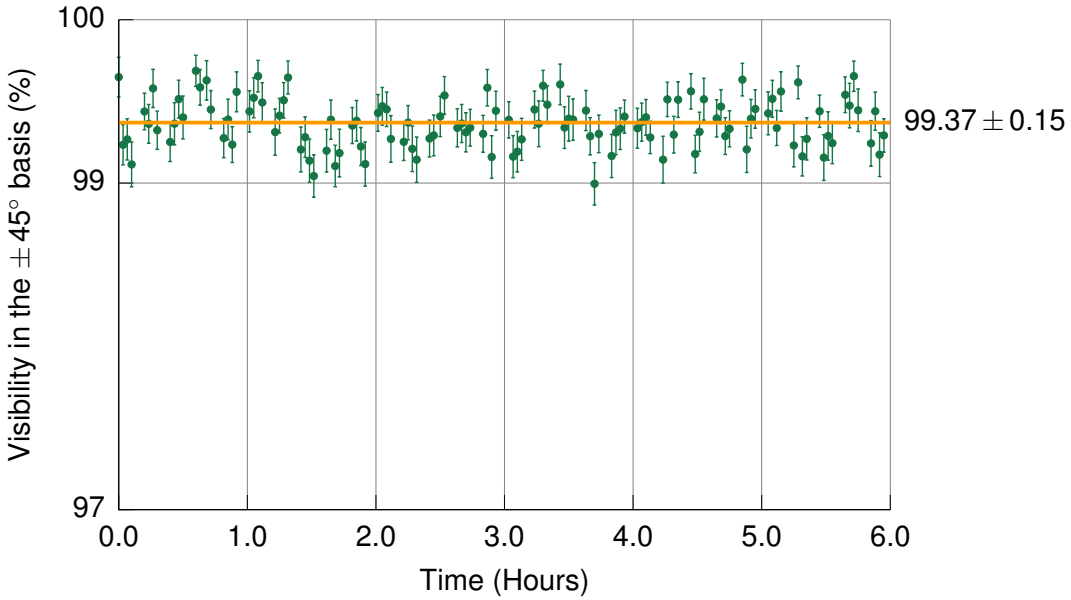


Figure 3.6: Stability of the visibility over time. By phase locking the source every 5 minutes we ensure that the entangled state produced is stable over extended periods of time. Over a duration of 6 hours we measured an average visibility of $99.3 \pm 0.15\,\%$.

signal and idler waists for optimal heralding efficiency for various pump focusings (see Section 3.3.2). A telescope consisting of two lenses of approximate focal length 55 mm and 75 mm spaced about 12 cm apart was used to control the focusing of the pump mode. The telescope was placed about 22 cm away from the fiber coupler.

Each of the two collection modes couple the downconverted light into AR coated 780-HP single mode fibers using A230-B aspheric lenses with a nominal focal length of 4.51 mm. The spot size at the output of the fiber coupler was measured to be 380 μm. We use a fixed plano-convex lens with a nominal focal length of 300 mm at a distance of about 30 cm from the collection fiber. The total distance between each collection fiber and the center of the crystal is ≈ 63 cm. The aspheric and the plano-convex lenses effectively form a two lens telescope which images the downconverted modes into the collection fibers. By adjusting the distance of the aspheric lens from the fiber tip we optimized the collection mode for the highest heralding efficiency.

To measure the collection beam waist, we propagate light from a 810 nm laser back through the crystal via the collection fibers. We measure the spot size ($\omega(z)$) in at least

The crystal length was kept constant during this experiment.

4 locations before the crystal using a knife edge measurement. Appendix B describes how these measurements were made. For a pump waist of $\omega_{0_p} = 256\,\mu$m, the optimal collection waist (ω_{0_c}) was 156 μm centered inside the crystal.

The position of the beam waists for pump and collection modes ($z_{0_{p,c}}$) was centered inside the crystal to within 5 mm. For comparison, Rayleigh range of the pump (z_{R_p}) was 136 mm when $\omega_{0_p} = 265\,\mu$m. It is important to ensure that $z_{0_{p,c}}$ is centered in the crystal to this accuracy (or better) such that the mode is symmetric for both pump directions.

3.3.2 Optimizing the focusing of the pump and collection modes

We use a 25 mm long, 1.5 mm wide and 1 mm high PPKTP crystal with a poling period of about 10 μm. Its poling period was chosen to downconvert the 405 nm pump into 810 nm signal and idler in a collinear geometry. The setup is shown in Figure 3.7. The spatial mode of the pump was first filtered by a single mode fiber, and then focused into the crystal by a telescope. A Blue Glass (BG) filter (with a transmission of $< 3.5 \times 10^{-3}$ at 810 nm) was used to reduce the IR fluorescence caused by the pump in the fiber and the polarization was set by a Glan-Taylor polarizer.

The pump and the generated downconverted modes were collinear. This improves their mode overlap leading to a better efficiency. The pump was filtered from the downconverted signal using a dichroic mirror. The downconverted signal and idler were separated by a Polarizing Beam Splitter (PBS) cube and then collected into single mode fibers. Interference filters are used to block residual pump and stray light. The collection modes are focused by another two lens telescope.

The two collection fibers are connected to Si APDs and the detectors are connected to counting and coincidence circuits. We varied the spot size of the pump mode ($\omega(z)_p$) inside the crystal and optimized the collection modes (ω_{0_c}) to obtain the highest efficiency. The results are plotted in Figure 3.8. We have corrected for the dark counts of the APDs used in this measurement. On the X-axis we plot the spot size of the pump mode ($\omega(z)_p$) at the center of the crystal and not (ω_{0_p}) [1] We measured the size

[1] Here we only pumped the crystal from a single direction. When pumping from both directions, it is important to ensure that the beam waist is at the center of the crystal in order to obtain a symmetrical coupling efficiency in both pump directions.

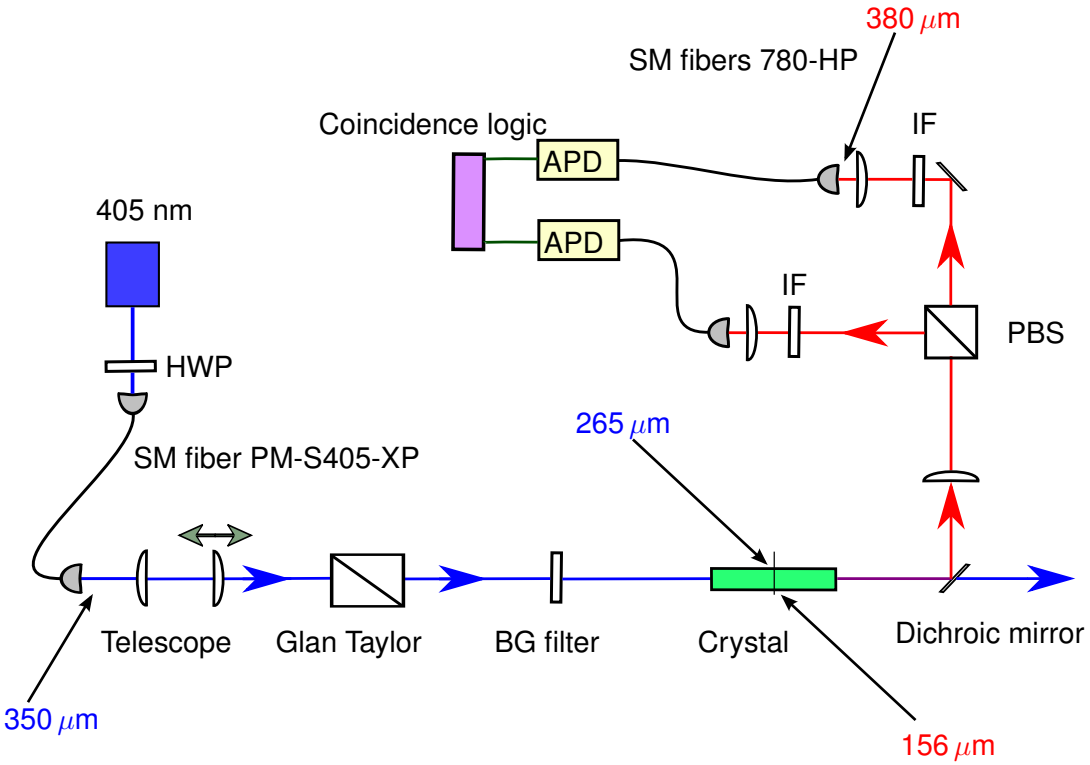


Figure 3.7: Single pass setup used to measure the optimal focusing parameters for the pump and collection modes. The pump is shown in blue and the downconverted modes in red. We used a telescope to focus the pump mode into the crystal. For each waist (ω_{0_p}), we adjusted the coupling into the collection optics and found the focusing conditions for the highest efficiency. The pump and collection modes were measured in at least four locations to determine both the waist and its location. The values indicate the experimentally obtained optimal beam waists.

and position of the pump and collection beam waists using a motorized razor edge to unblock the beam (see Appendix B).

A good mode overlap between the pump and collection modes can be obtained even if the beam waists are not centered in the crystal. For a constant and large pump beam spot size ($\omega(z)_p$) within the crystal we were able to obtain the same heralding efficiency (after re-optimizing the collection waists) when the pump waist (ω_{0_p}) was centered within the crystal as well as 5 Raleigh ranges away from the crystal.

From the graph in Figure 3.8 we observe a large relatively flat region of high efficiency. We choose our operating focal parameters from this region. As we increase

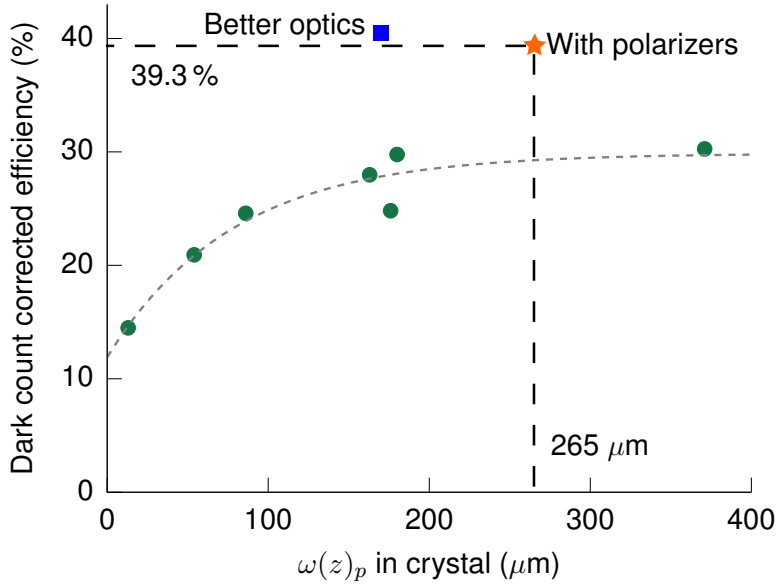


Figure 3.8: Heralding efficiency vs. the size ($\omega(z)_p$) of the pump beam inside the crystal. When the pump spot size in the crystal ($\omega(z)_p$) is comparable to the clear aperture of the crystal there are losses in the downconverted modes due to clipping. We choose a pump spot size of $\approx 265\mu$m for the Sagnac source of entangled photon pairs. To obtain this graph we varied the pump beam's spot size inside the crystal using the lenses in the telescope. For each pump spot size the focusing and alignment of the collection modes was optimized. Blue square represents the efficiency due to improved AR coatings on all optical components, AR coated collection fibers, and low loss interference filters. The orange star represents the efficiency observed with measurement polarizers

the spot size, losses due to clipping at the boundaries of the crystal increase. To avoid clipping we choose our operating point to be $\omega(z)_p = \omega_{0_p} = 265\,\mu$m centered in the crystal and the optimal value of $\omega_{0_c} = 156\,\mu$m. We have presented these results in conferences [74, 75].

Once we have chosen the operating focusing parameters, we tried to reduce losses by improving the AR coating on all optical surfaces. We also AR coated the collection fibers. We changed the interference filters to custom made ones from Semrock with a transmission of more than 97.5 %. Doing so we obtained an efficiency (pairs to singles ratio) of 40.5 % as shown by the blue square in Figure 3.8. We also introduced measurement polarizers into the collection arms; the efficiency obtained with these in place is shown by the orange star in Figure 3.8.

The observed trend is that a larger pump spot size inside the crystal results in a larger heralding efficiency. However, we are limited by the crystal size. Currently our crystal is 2 mm by 1 mm in cross-section. The thickness of the crystals available is limited due to the poling of the crystal. During growth of the KTP crystal the periodic poling is done by attaching a separate electrically conductive mask to the crystal. By passing a current through these masks the sign of the non-linear crystal is periodically flipped. Growing a thicker crystal necessitates higher voltages through the electrically conductive mask which, due to edge effects, results in a larger error in the poling.

Our results are in agreement with the theoretical and numerical results of Bennink [14]. A comparison with these results is shown in Figure 3.9. For a crystal of optical length L and a beam with a wave number k, the focusing parameter ξ is defined as

$$\xi = \frac{L}{k\omega_0^2}\,. \tag{3.9}$$

The graphs shown in [14] were obtained by numerical optimization of the heralding efficiency η_{si}. The computed values of η_{si} assume that there are no optical losses, no lens aberrations and that there are no distortions to the Gaussian mode of the beam (say by clipping of the beam).

We attribute the deviations from the predicted curves [14] to the following factors. Tight focusing ($\xi_p > 0.5$) makes the spatial overlap of the pump and collection modes difficult to achieve. Very tight focusing ($\xi > 9$) has a Raleigh range (z_{R_p}) smaller than the length of our crystal This makes it difficult to correctly overlap positions of the pump (ω_{0_p}) and collection waists (ω_{0_c}). Thus the mode overlap between the pump and downconverted modes was not uniform throughout the crystal. Very weak focusing ($\xi < 0.02$) results in a very large ω_{0_p} ($> 250\,\mu$m) and ω_{0_c} ($> 160\,\mu$m). Due to the physical size of our crystal's transverse cross-section (1 mm $\times$ 2 mm) and the even smaller clear aperture, these beams may undergo clipping at the edges. This can further distort their Gaussian beam profiles and prevent efficient coupling into the

[1] We only calibrated our detectors at certain count rates. The change in detection efficiency with count rates can be modeled using the dead time of the detector as shown in Section 4.3. Since all detectors were not characterized at several count rates we were only able to obtain a typical dead time for our APDs. Instead of correcting for such an inaccurately known quantity, I have included its effect into the error bars shown here.

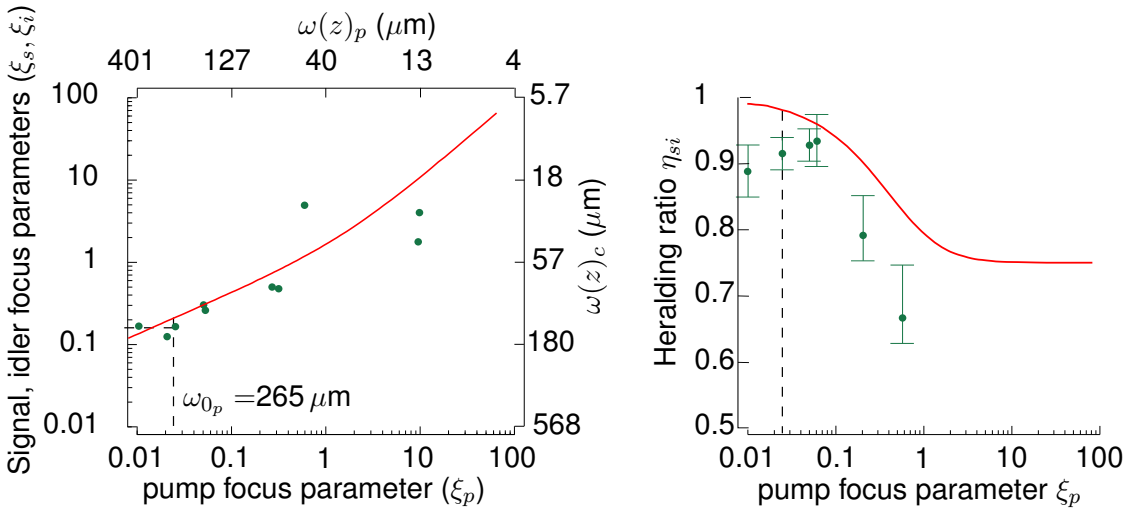


Figure 3.9: Comparison between the simulations of Bennink [14](solid lines) and our experimental data (circles). Left: For each $\omega(z)_p$ at the center of the crystal, we empirically optimized the collection focusing ($\omega(z)_c$) for the maximum collection efficiency. The circles represent measured values. Right: The experimental values have been corrected for all measured losses, but not for lens distortions, clipping of the beam, etc. The asymmetry of the error bars is due to our underestimation of the APD's detection efficiency at large count rates[1].

collection fibers. Furthermore, experimental errors in finding the optimum collection waists (ω_{0_c}) could decrease our measured efficiency. Consequently, the best agreement with predictions of [14] are within a very narrow range of parameters.

We also note that a tighter focusing yields more pairs per milliwatt of pump power, as compared to weak focusing but at lower heralding efficiency. This behavior was also predicted by [14].

3.4 Efficiency

We have designed and built this high efficiency source of polarization entangled photon pairs to be suitable for device independent applications which require a efficiency of more than 66.7 % [3]. The efficiency (η) of the source, as given by the pairs to singles ratio (see Equation 3.1), exceeds this limit when corrected for the losses due to APD detectors (see Section 4.3).

We produced polarization entangled photon pairs using the setup shown in Figure 3.2. Using Si APDs we measured an efficiency of 39.3 % (after correcting for dark

count rates of approximately 190 /s and 5400 /s) between detectors "Main 1" and "Main 2". The APDs used in this measurement were calibrated and had detection efficiencies of $49.7 \pm 2.8\,\%$ and $46.7 \pm 2.5\,\%$ (see Section 4.3). Correcting for the detector efficiencies, the efficiency of our source was $81.6 \pm 3.0\,\%$. This is inclusive of the fiber splicing losses. Without measurement polarizers we had an efficiency of $40.5\,\%$ as measured with APDs and $86.0 \pm \dot{3}.5\,\%$ after correcting for the detectors.

In the optical path of the downconverted light we had 19 optical surfaces[1], 17 of which have a $0.1 - 0.2\,\%$ loss (as estimated from their data sheet and measured). The IF has a measured $2 - 3\,\%$ loss. The splice between the 780-HP collection fibers and SMF-28e fibers has a measured loss of about $2\,\%$. Accounting for all these losses the efficiency of our source is roughly $91 \pm 5\,\%$. This estimate is the coupling efficiency of our source (inclusive of any imperfections in the mode overlap between pump and target modes).

The efficiency of our source remains high even for non-maximally entangled states. We observed an efficiency of $38.8 \pm 0.2\,\%$ for several different non-maximally entangled states. Correcting for only detector efficiencies, the efficiency of the source when producing these states is $80.5 \pm 3.0\,\%$. This marginal decrease in efficiency could be due to a small wedge error in the pump HWP controlling θ. It could also be due to slight misalignment of some components.

We also measured the efficiency using Transition Edge Sensors (TESs) instead of APDs. We observed a dark count corrected efficiency of $75.2\,\%$. These measurements are shown in Section 4.5.3.

We collect the downconverted photon pairs into 780-HP fibers which are single mode at 810 nm. We make a splice from 780-HP to SMF-28e (a telecommunications fiber which supports 2 modes for 810 nm)[2]. The efficiency we measure is inclusive of the splicing losses.

3.5 Wavelength tuning

The phase matching conditions (see Section 2.1.1) for our PPKTP crystal allow a 405 nm pump photon to be collinearly downconverted into a signal and an idler photons.

[1] The other downconverted path does not have the Sagnac HWP and has only 17 surfaces

[2] 780-HP fibers have a large transmission loss (about 4 dB/km [81]). For lengths of more than 25 m we reduce losses by splicing to SMF-28e

The wavelength of the signal and idler can be tuned over a wide range ($\gg 6\,\text{nm}$) by temperature tuning the crystal. When the signal and idler have the same wavelength then, the downconversion process is said to be degenerate. The cut and poling period ($\approx 10\,\mu\text{m}$) of our crystal are optimized for degenerate downconversion from 405 nm to 810 nm at about 31.5 °C.

Operating at this degenerate downconverted wavelength is advantageous for the following reasons:

- The optimal focusing conditions for both collection modes are identical because both the signal and idler are of the same wavelength. This simplifies the alignment of the source and allows us to have symmetric arm efficiencies.
- All optical components can have narrow band coatings, which typically have lower losses than broad band optical coatings.
- The Downconverted Sagnac HWP (HWP_{DS}) (see Figure 3.2) rotates the polarization of both the signal (in mode 1) and idler (in mode 2) identically and vice versa. This improves the polarization correlation visibility of the source.

To ensure that we are operating at the degenerate wavelength, we needed to measure the wavelength of the signal and idler. We did this using a home built grating spectrometer. A schematic of the setup is shown in Figure 3.10. We used a blazed diffraction grating with 1200 lines/mm (Thorlabs GR25-1200) mounted on a motorized rotation stage. The resolution of our spectrometer was 0.4 nm. The spectrometer was calibrated by comparison to both a Helium-Neon laser and a 780 nm laser locked to the D_2 line of rubidium.

A typical measurement using the spectrometer is shown in Figure 3.11. We fit the observed data points to a Gaussian to extract the peak wavelength. However the bandwidth of the light cannot be inferred from this measurement because we were limited by the resolution of the instrument (0.4 nm). To measure the bandwidth we use a Michelson interferometer (see Section 3.6).

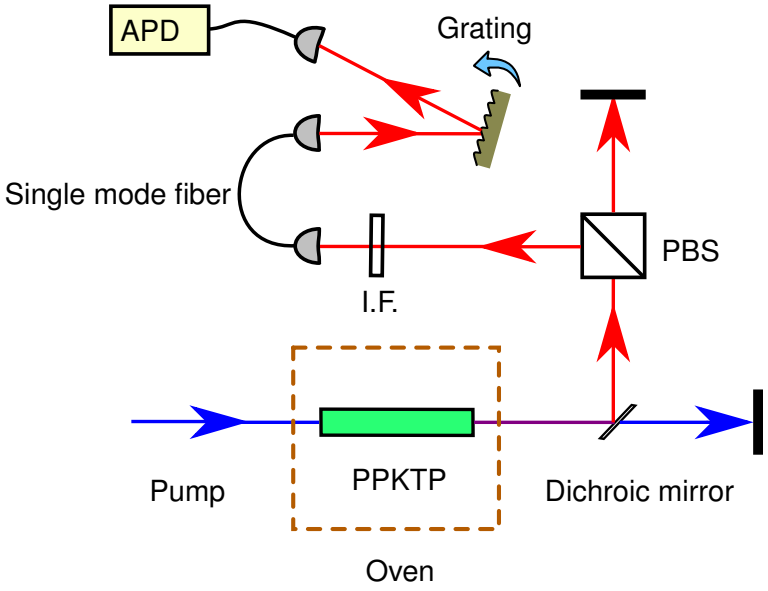


Figure 3.10: Schematic of the wavelength measurement of downconverted light from the high efficiency polarization entangled photon pair source.

Since we use a periodically poled crystal, changing the temperature changes both the refractive index and the poling period (due to thermal expansion) (see Section 2.1.1). Thus we can tune the wavelength of the downconverted light by changing the temperature of the crystal [46, 77]. A large temperature gradient along the length of the crystal results in different phase matching conditions in different regions. This increases the bandwidth of the downconverted modes.

In our source, we place the crystal in a copper block to minimize the temperature gradient across the crystal, and mount it on a Peltier stage. Figure 3.12 shows the oven we used to control the temperature of the crystal. The oven stabilizes the temperature to $\pm$ 10 mK.

Figure 3.13 shows the temperature tunability of the source. The wavelengths of the signal and idler were the same at a temperature of about 31.5 °C. The solid lines represent fits from the theory obtained by considering the change in the poling period and refractive indices with temperature [46, 77]. From Figure 3.13 we measure the slope of the wavelength vs temperature line. This is a measure of the tunability of the source. The downconverted wavelength can be tuned by 0.19 nm/°C. The range over

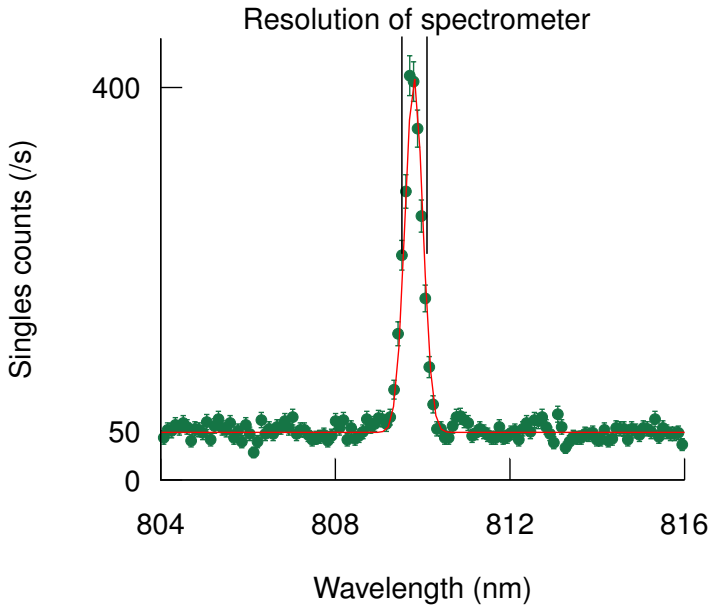


Figure 3.11: Spectrum of the idler when the crystal was pumped from a single direction. The crystal was at 31.03 °C which is close to the degenerate temperature (31.47 °C). This measurement is limited by the resolution of the grating spectrometer used.

which it can be tuned was limited by the maximum temperature range of the crystal oven (50 °C).

3.6 Bandwidth

Downconversion is possible for wavelengths that meet the phase matching criteria. The power spectrum $I(\lambda)$ of the downconverted light is given by [77, 82]

$$I(\lambda) \propto \mathrm{sinc}^2\left(\frac{\Delta\mathbf{k}L}{2}\right), \tag{3.10}$$

where L is the length of the crystal and $\Delta\mathbf{k}$ is the phase mismatch given by

$$\Delta\mathbf{k} = \mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i - \frac{2\pi}{\mathbf{\Gamma}}. \tag{3.11}$$

For a wavelength (λ) of the downconverted light, Equation 3.10 can be reduced to give the FWHM bandwidth ($\Delta\lambda$) as

$$\Delta\lambda = \frac{\lambda^2}{(n_s - n_i)L}. \tag{3.12}$$

Figure 3.12: The oven used to temperature stabilize the PPKTP crystal. It consists of a large 6 cm by 6 cm copper block. This provides a large enough thermal mass to prevent rapid temperature fluctuations. Further, the copper minimizes the temperature gradient along the crystal. There is a 2 mm wide and 2.7 cm long groove in which the crystal sits. This grove is in the center of the copper block such that the end faces of the crystal are not exposed to air currents (which can cause a temperature gradient between the middle and ends of the crystal). There is also a copper lid which covers the crystal. The whole assembly sits on a 4 cm by 4 cm square single stage Peltier. A large aluminum block below the Peltier serves as a mounting pedestal and a heat sink.

where n_s and n_i (1.75665 and 1.84475 for 810 nm light in KTP at 31.5°C [5, 6]) are the refractive indices of the crystal for the signal and the idler (see Table 2.2). Given the length of our crystal (25 mm) this gives the lower bound on the FWHM bandwidth of the downconverted light to be 136 GHz.

A Michelson interferometer (as shown in Figure 3.14) was used to measure the bandwidth of the downconverted light by testing its coherence length (L_c). L_c is related to the bandwidth ($\Delta\nu$) by

$$L_c = \frac{c}{n\Delta\nu}\,, \tag{3.13}$$

where c is the speed of light in vacuum and n is the refractive index of the medium (air). For an expected bandwidth of about 140 GHz, the coherence length is about 2.7 mm. This travel distance was achieved by using a motorized translation stage.

An interference pattern corresponding to a monochromatic field with a coherence time τ_c can be described by

$$I \propto e^{-\pi\left(\frac{\tau}{\tau_c}\right)^2} \cos\left(\frac{4\pi d}{\lambda}\right) + 1\,, \tag{3.14}$$

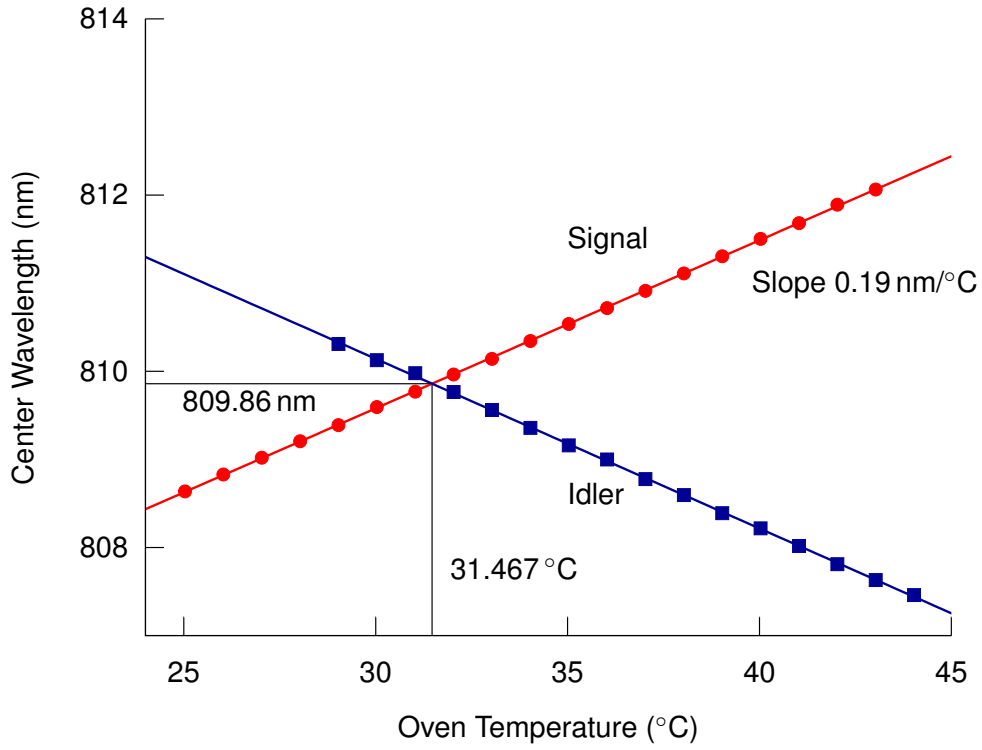


Figure 3.13: Temperature tuning of the wavelengths of the downconverted photons. The wavelength vs. temperature graph for the signal (circles) and for the idler (squares). The crystal was pumped in a single direction and the downconverted pairs were split into two arms using a PBS. Each arm was sent to the single photon spectrometer. The crystal temperature was changed and the wavelengths of the signal and idler were measured again.

where λ is the wavelength, c is the speed of light in vacuum, $\tau = 2\frac{d}{c}$ is the path length difference expressed in time of flight of the photon. The envelope of this pattern is given by the exponential part of the function shown in Equation 3.14.

By scanning the position of the translation stage we should see the fringes predicted by Equation 3.14. To create a path length difference of d we need to scan the motor by only $\frac{d}{2}$. For a bandwidth of 140 GHz at 810 nm, moving the motor by about 0.4 μm corresponds to one period of these fringes. However, the motorized translation stage could only move in steps of 1 μm. Consequently, we under sampled the interference pattern. This data is shown in Figure 3.15. Since we moved the motor in steps much larger than the expected fringe width, we could no longer see the fringe pattern in the

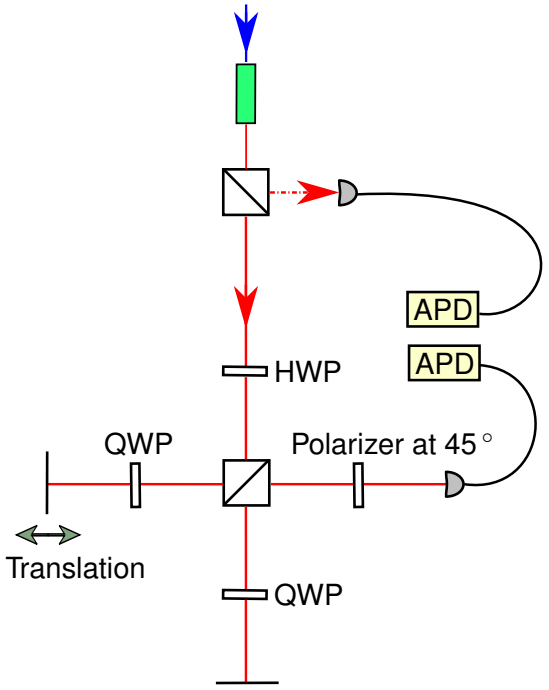


Figure 3.14: Michelson interferometer used to measure the bandwidth of downconverted light. The interferometer consists of two retro-reflecting arms one of which is fixed and the other can be moved. A PBS is used to separate these two arms. The HWP is used to adjust the balance of power between these arms. QWPs in each arm are aligned such that a double pass through them rotates the linear polarization from H to V or vice versa. A polarizer at 45 ° is used to observe the interference. Coincidence events are used for this measurement to improve the signal to noise ratio.

data. The envelope of the fringe patterns obtained from Equation 3.14 can still be seen even though the fringes themselves cannot. We obtain the bandwidth by fitting the data to the exponential part of Equation 3.14 which is a Gaussian with the standard deviation $\sigma = \frac{\tau_c}{\sqrt{2}}$.

To fit the obtained data to the envelope we divided the data into several small bins (of width 20 μm) and calculated the maximum and minimum values for each bin. The set of maximum bin values was fitted to obtain the upper envelope and the set of minimum values was fitted to obtain the lower envelope. The bandwidth of the downconverted light is obtained from the coherence time. The values obtained from fitting the upper and lower envelopes agree to within the error bars of the fit. The measured FWHM bandwidth of the signal and idler to be 186 ± 2.5 GHz.

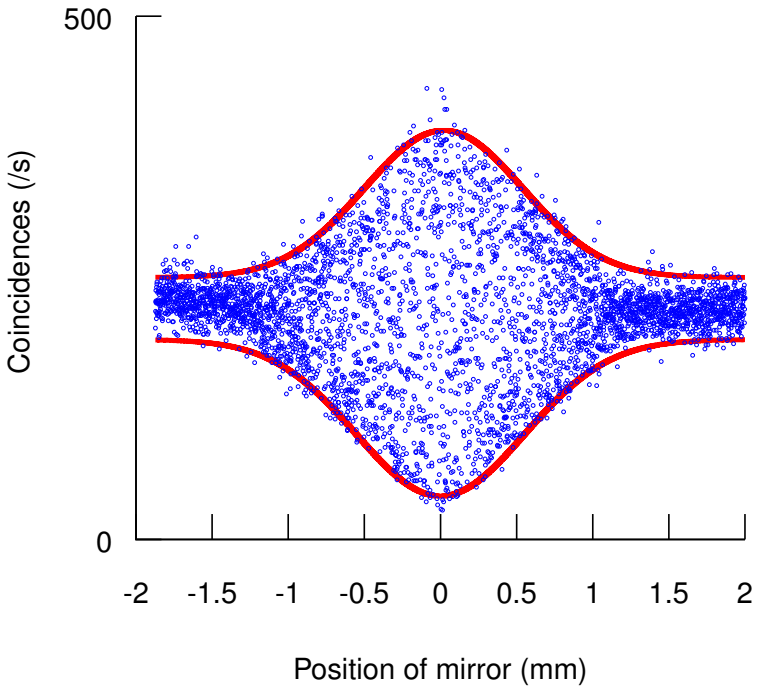


Figure 3.15: Bandwidth measurement of the downconverted light using a Michelson interferometer. The coherence length and hence the bandwidth can be obtained from the envelope (thick line) of the data points (dots). We do not see the complete oscillations inside the envelope because we under sample the interference fringes. The bandwidth was measured using heralded photons to improve the signal to noise ratio. From the fit we obtained a FWHM bandwidth of 186 ± 2.5 GHz.

The measured bandwidth is larger than predicted by Equation 3.10 we attribute this to irregularities in the poling period of the crystal. These irregularities alter the phase matching conditions in different regions of the crystal. A similar effect can be caused by temperature gradients across the crystal. We minimize these gradients by using a copper housing for the crystal which does not expose the crystal end faces to air currents. To estimate the temperature gradient across the crystal we used four thermistors placed along the length of the crystal. These thermistors were glued into the copper oven and placed ¡ 200 μm away from the crystal. We measured a temperature gradient of ¡ 10 mK between any two thermistors[1]. To estimate the contribution of the temperature gradient to the bandwidth of downconverted light, we can assume that the crystal is split into two regions with a temperature difference of 10 mK between them.

[1]We were unable to calibrate the thermistors to an accuracy of better than 10 mK.

The change in refractive indices and polling period will cause a shift in the central wavelength of about 0.9 GHz.

Chapter 4

Detectors

The high efficiency with which we generate pairs of entangled photons (Chapter 3) is of limited practical use unless we are able to detect them. To do so we make use of single photon detectors like Avalanche Photo-Diodes (APD) and Transition Edge Sensors (TES). In this chapter I present the operation and characterization of these detectors followed by measurements of the system efficiency with the TESs connected to our source. The TESs were obtained in collaboration with the group of Sae Woo Nam at NIST. We also used SQUID amplifiers obtained form our collaborators at NIST. My supervisor Christian Kurtsiefer, designed and built the amplifiers, filters, and signal processing and detection electronics used for experiments performed in this chapter.

4.1 Introduction

Single photon detectors are essential for many quantum optics experiments. Such detectors have been extensively studied and improved over the past century. As such there are a large variety of detectors available today. Table 4.1 shows a comparison of some single photon detectors. From a historical perspective, in 1930 Photo Multiplier Tubes (PMTs) became the first single photon detectors [83]. However, their detection efficiency in the visible and near IR wavelengths is limited ($\ll$30 % [7, 84]). Improvements in the fabrication of semiconductor PIN detectors led to the manufacture of Avalanche Photo-Diodes (APDs) which have an internal gain. When first used in the "Geiger" mode, APDs needed some twenty photons for a detectable light pulse [85]. However, with some structural, material and manufacturing changes APDs improved considerably [85]. Today, APDs can detect a single photon with detection efficiencies

of $\approx 50\,\%$ (at 810 nm) and are commercially available [8]. They are manufactured for a wide variety of wavelength ranges and applications.

Both the PMT and APD are based on the photoelectric effect. Recently another class of single photon detectors is being studied extensively [4, 86]. These detectors are superconducting micro bolometers. The Transition Edge Sensor (TES) and nano-wire detectors are examples of this kind. Both detector types have a near unit detection efficiency [4, 86] and very low thermal noise. Currently, TESs have a higher detection efficiency [4]. We use these detectors in conjunction with our high efficiency source of polarization entangled photon pairs to measure a heralding efficiency of $>75\,\%$ (see Section 4.5.3).

Single photon detectors can register a detection event (a click) due to thermal, electrical and or optical noise. These spurious clicks are called background counts, while those due to electrical and thermal noise alone are referred to as dark counts[1]. Typically the dark count rate depends on the operating conditions of the detector and to the first order are insensitive to changes in the incident light levels. The background count rate depends on the amount of stray light reaching the detector which can vary from time to time. When applying corrections, we measure and correct for the background counts at the time of the experiment (rather than the dark counts). This is such common practice that the terms background counts and dark counts are, for the most part, used interchangeably.

4.2 Avalanche Photo-Diodes (APDs)

In an APD an incident photon strikes the N side of a PIN junction and generates a photo-electron. The photo-electron travels towards the P junction passing through a depletion layer. During its passage, it can create other electron hole pairs due to impact ionization. In the presence of a large enough electric field (large reverse bias across the diode) it results in an avalanche breakdown which produces a detectable signal. For

[1] the background count rate of a detector is the dark count rate plus the rate of detection events due to stray light from external sources.

[1] I would like to emphasize that these values are our measured results for the detection efficiency of several different APDs. The detection efficiency is different from the quantum efficiency typically stated in the manufacturer's specifications.

Type of Detector	Wavelength range	Detection Efficiency	Dark count rate (s^{-1})	Dead time (s^{-1})	Jitter (ns)	Photon number resolving
PMT	100 – 900 nm	8 – 28 %	1 – 200	1 μs	<1	×
Si APD	400 – 1100 nm	20 – 55 %[1]	20 – 5000	1 μs	<1	×
InGaAs APD	1000 – 1700 nm	≈ 10 %	20 – 5000	1 μs	1	×
TES	Visible, Near IR	> 98 %	< 1	—	<4	✓
Nano-wire	Visible, Near IR	> 93 %	< 1	40 ns	0.1	✓

Table 4.1: Table comparing some of the available single photon detectors. The data in this table was compiled from various sources [4, 7, 8, 9, 10, 11] and our measurements. It is indicative of the typical performance of these classes of detectors. There are several other types of detectors which are also being studied by various groups [9, 12, 13].

the APDs used in this experiment (PerkinElmer C30902SH) the breakdown threshold voltage is 188 V, and we typically operate them 10–20 V above this.

The probability that a single incident photon generates a photo-electron is called the quantum efficiency. The detection efficiency is the probability that an incident photon will generate a detection signal ("click") in the subsequent detection circuitry. The detection efficiency is lower than the quantum efficiency for the following reasons.

First, the electron-hole pair generated by the incident photon can recombine. To limit this, the PN junction should be thin. However, the quantum efficiency increases with the thickness of the depletion region of the diode due to the increased absorption probability of an incident photon. This forms a trade-off with the recombination probability.

Second, after the detection of a photon, the avalanche process has to be stopped. This is done by the use of an electronic circuit which reduces the bias voltage below the breakdown voltage for a short period of time (a process known as quenching). This necessary recovery time is the dead time during which any incident light will not be detected.

There are two ways to quench APDs: passive and active. In passive quenching a resistor is placed in series with the APD [87, 88]. The quenching occurs simply because there is a voltage drop across this ballast load (quenching resistor); after which the

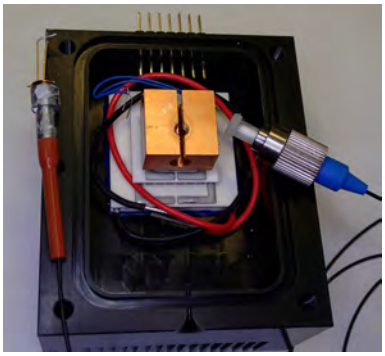


Figure 4.1: A fiber pigtailed APD module under assembly. The diode is seen to the left, and a black multimode fiber has been glued in place illuminating the active surface of the diode. The APD sits in a copper housing atop a three stage Peltier element used to cool the diode. To prevent condensation the whole structure is mounted in a black air tight aluminum housing.

Figure 4.2: A fiber pigtailed APD module, showing the electronics needed to provide a high bias voltage to the APD, quench the APD, and to provide a NIM output signal for each photon detection event.

bias voltage slowly recovers. In active quenching a fast circuit senses the photo-current and quickly reduces the bias voltage. Due to the high operating voltage the power dissipation in the diode is considerable. The ballast resistor in a passively quenched diode limits the maximum current and prevents heat damage due to high count rates. Actively quenched diodes, on the other hand, are prone to damage when exposed to excessive light unless they have a protection circuit. Although active quenching is faster we use passive quenching because of its simplicity (a resistor) and ruggedness. For the passively quenched Si APDs we use, the dead time is on the order of 0.75 μs which limits the maximum count rate to about 490 000 photons per second[1].

Third, APDs have a dark current due to thermal (rather than optical) generation of electron-hole pairs. This dark current limits the minimum amount of light the APD detects. To reduce this noise we cool our APDs to $\approx$ -30 °C. In addition to providing false photon detection events, the dark counts are followed by a dead time. Any photons arriving during these intervals will not result in a detection. This once more limits the

[1]The rate of clicks r_{click} is given by the "paralyzable" model [89, 90] as $r_{click} = Ur_i e^{-Ur_i t_d}$, where t_d is the dead time, U is the unsaturated detection efficiency and r_i is the rate of incident photons.

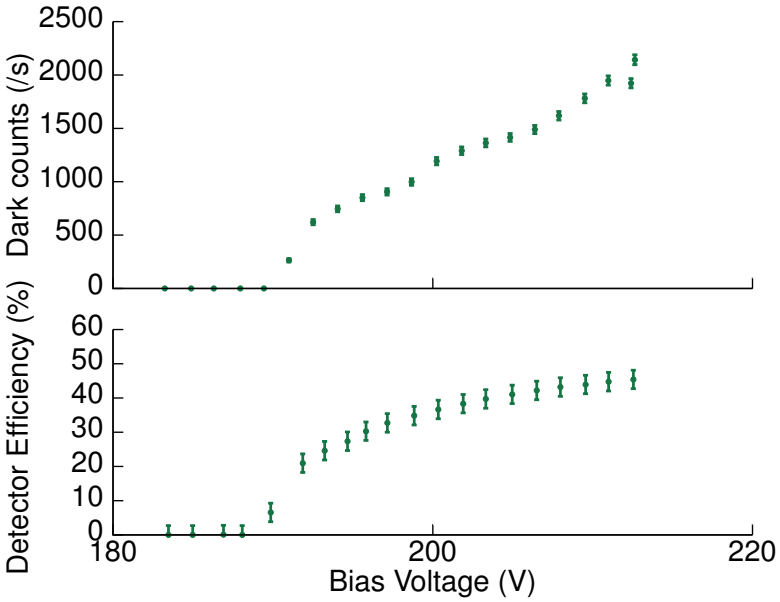


Figure 4.3: As we increase the bias voltage above the breakdown threshold (188 V in this case), the APD starts to detect single photons. Above: The dark count rate increases as the bias voltage is raised. Below: The detection efficiency improves with increased bias voltage[1].

detection efficiency of APDs.

4.3 Measuring the APD detection efficiency

To estimate the collection efficiency of our source (due to the mode overlap) described in Section 3.4, it is important to account for all other losses, the most significant of which comes from the limited detection efficiency of our APD detectors. We calibrate our detectors using a laser attenuated by calibrated Neutral Density (ND) filters. The procedure we use is similar to [91] and described in Appendix D.

The APD modules we use are home built with the APD diode from Perkin Elmer (C30902SH, active area $\varnothing = 500\,\mu$m) The diode is mounted on top of a three stage Peltier element which cools the diode to about -30 °C. The diode and Peltier are enclosed in an air tight housing to avoid condensation. We use passively quenched APDs with a ballast resistor of 390 KΩ. The APDs are fiber pigtailed i.e. a multimode fiber is glued onto the active surface of the diode. This is done such that all light supported by the

[1]The detection efficiency does not assume zero dead time.

fiber is incident on the APD's active surface. A black jacketed fiber was used to avoid stray light. The fiber has a core size of 50 μm and is FC/UPC connectorized on the free end.

For several APDs, we measured the dependence of their efficiency on the bias voltage, temperature and the count rate. The dark count rate was least at the lowest temperature. The detection efficiency was (within a reasonable range of about -20 °C to -30 °C) independent of the temperature. We thus set the temperature as low as possible, limited by the cooling power of the Peltier element.

As seen in Figure 4.3, increasing the reverse bias voltage increased the noise (dark counts) and the efficiency[1]. The dark count rate varies drastically from APD to APD, ranging from as low as 10 /s to 5000 /s. Similarly, the efficiency of the APDs also had a large variation. We characterized several different diodes at a count rate of about 15 000 /s. The Bias voltage of each diode was adjusted for the highest detection efficiency while ensuring a dark count rate of ¡ 4000 /s. The efficiencies of the various detectors we measured ranged from 35 % to 52 %.

The detection efficiency of an APD depends on the incident count rate as seen in Figure 4.4. This is due to the dead time of the detector as mentioned earlier in Section 4.2. From the data we extract the dead time of the detector to be 0.75 μs. We follow the simple model presented in [89, 90]. We assume that the photons incident on the detector follow a Poisson distribution. For a single incident photon, the probability that there will be a "click" is given by the unsaturated detection efficiency of the detector (U). The detector has a dead time t_d and is "paralyzeable" [89, 90]. If a photon arrives during the dead time of the detector then it may be absorbed and trigger another avalanche breakdown, effectively paralyzing the detector for another t_d, this is known as a paralyzable model for the APD[2]. In reality the dead time is not a fixed value but has some variation, we do not consider this. We also ignore afterpulsing, the probability of which is small given our count rates (of about 10,000 /s). More detailed models can be found elsewhere [92, 93, 94]. In the absence of background counts, the

[1] Increasing the bias voltage too high could result in permanent damage to the APD.

[2] A non paralyzeable model would saturate at a constant count rate given by the inverse of its dead time regardless of the incident optical power; however, our detectors display no counts if a sufficiently large optical signal is applied, clearly demonstrating the effect of paralysis.

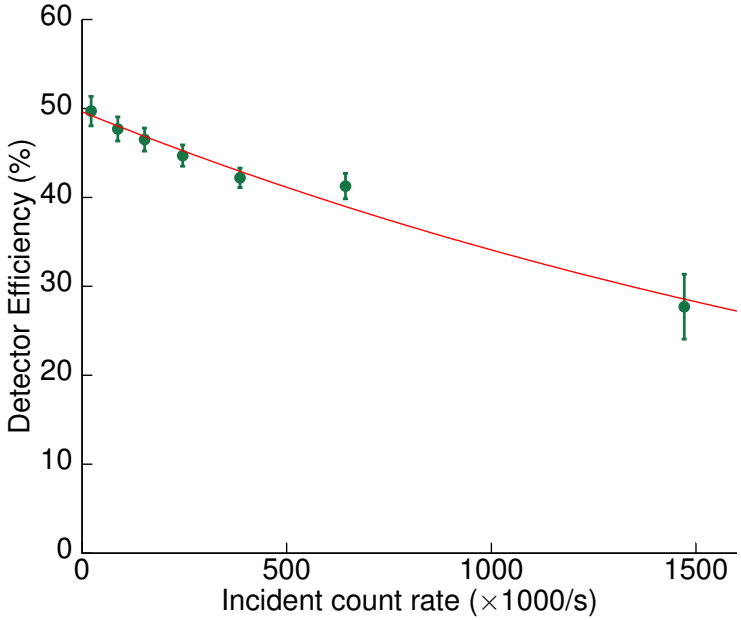


Figure 4.4: The detection efficiency of an APD drops when we vary the incident power (i.e. the rate of photons incident on the APD). This is saturation behavior of the detector and is explained by a dead time of 0.75 μs as obtained from a fit to Equation 4.1.

efficiency of the detector η is given by:

$$\eta = Ue^{-Ur_i t_d}\,, \tag{4.1}$$

where r_i is the average rate of photons incident on the detector [89, 90]. Using Equation 4.1 we can fit the data shown in Figure 4.4 to obtain the dead time of the APD to be about 0.75 μs.

4.4 Transition Edge Sensors

Transition Edge Sensors (TES) are superconducting bolometric detectors used to detect the thermal energy deposited by an incident photon [4]. A TES consists of a superconducting film maintained near its critical temperature T_c such that the energy of a photon is enough to take it part way along the super conducting to normal phase transition (see Figure 4.5). Due to the steep slope of the phase transition, there is a measurable rapid change in the resistance of superconducting film.

The superconducting to normal phase transition was first used to measure IR radiation by Andrews et al. in 1942 [95]. During the first half century after their invention,

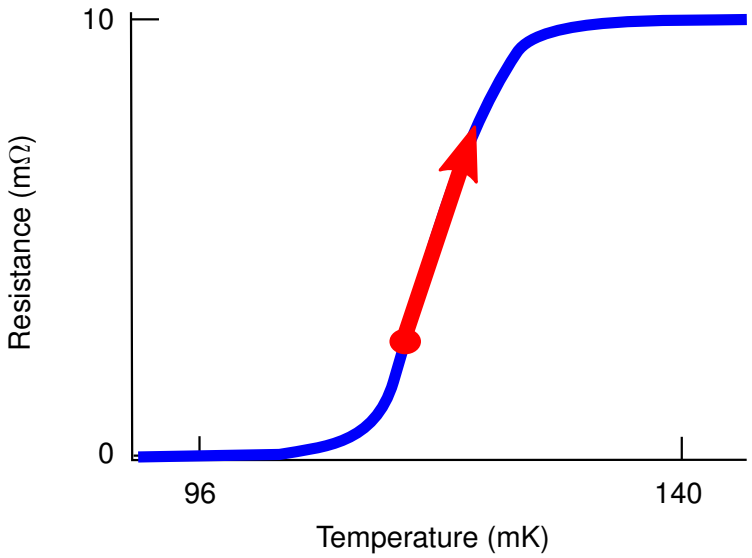


Figure 4.5: Conceptual graph showing the ideal change of the resistance of a superconductor as the temperature increases. Electro-thermal feedback using a voltage bias across the superconductor as described in [15] can be used to bias it partway along this transition (red circle). Thermal energy from a photon increases the temperature of the superconductor partway along the phase transition (red arrow). This causes the resistance of the superconductor to increase.

TES detectors were seldom used in practical applications due to the difficulty of signal readout from a low-impedance ($\approx 8\,\Omega$) system [96]. In recent years, this problem has been largely eliminated by the use of superconducting quantum interference device (SQUID) amplifiers [97], which can be impedance-matched to low-resistance TES detectors [98, 99]. Another barrier to the practical use of TES detectors was the difficulty of operating them within the narrow superconducting phase transition [96]. This issue was addressed by Irwin in 1995 [15] when he described a method of self regulating the TES at its operating point by applying a voltage bias across the device. TES detectors are now being developed for measurements across the electromagnetic spectrum from millimeter wavelengths [100], to near IR [17], to X-ray [101] and even gamma rays [102].

Recently, the group of Sae Woo Nam at NIST manufactured TES detectors with optical coatings that have a very high absorption at 810 nm and consequently a near perfect detection efficiency [4]. The thermal energy of a single photon at 810 nm is only enough to drive the superconducting detector part way along the phase transition to normal conducting, another photon arriving at the same time will drive the detector fur-

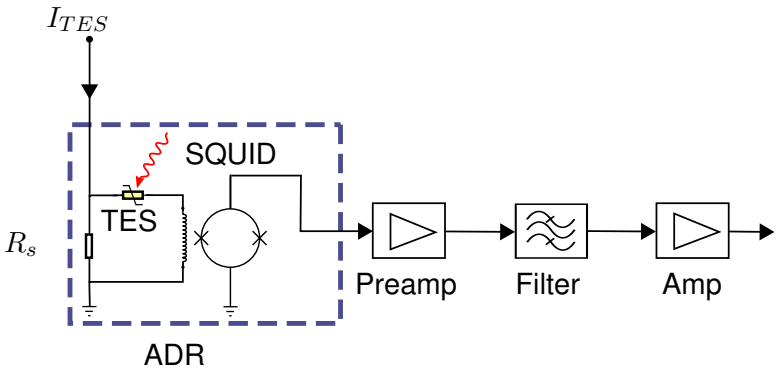


Figure 4.6: The TES is maintained near its superconducting critical temperature using a voltage bias [15]. A current I_{TES} across the shunt resistor R_s creates this voltage bias. The change in resistance of the TES due to an incident photon changes the current flowing through the input coil of a SQUID amplifier. The TES and SQUID operate at 70 mK and 2.5 K, respectively, and are cooled to these temperatures by an Adiabatic Demagnetization Refrigerator (ADR).

ther along the phase transition. This allows the TES to resolve the amount of thermal energy deposited in the superconductor, and for monochromatic input, it is possible to resolve the number of incident photons. We used these TESs from NIST together with our high efficiency source (Chapter 3) to build a system with an uncorrected heralding efficiency of $> 74\,\%$.

The critical temperature T_c of the TES's superconducting film can vary between devices and is about 140 mK for our detectors. We operate the detectors below T_c (at 70 mK) and use the voltage bias to regulate their temperature. We use an Adiabatic Demagnetization Refrigerator (ADR) to cool our detectors.

Figure 4.6 shows the TES connected to the input coil of a SQUID amplifier. The current I_{TES} applied across the shunt resistor R_s creates a voltage bias across the detector. The thermal energy deposited by a photon changes the resistance of the TES and consequently the current flowing through the superconducting input coil of the SQUID. The SQUID input and the wires connecting it to the TES are all superconducting in order to match the low impedance of the detectors. The SQUID is located at a different part of the ADR and is kept at a temperature of 2.5 K. The higher impedance output of the SQUID is further amplified and filtered outside the refrigerator.

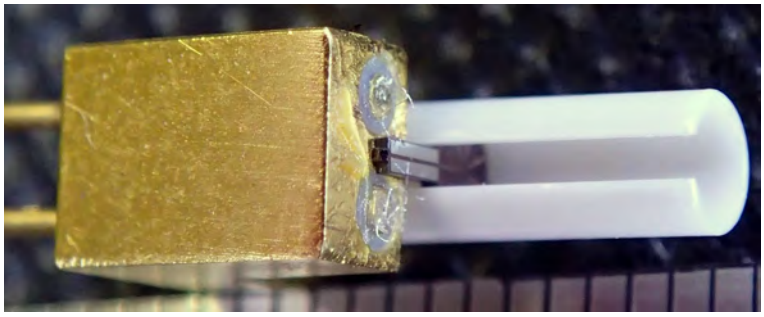


Figure 4.7: The TES is mounted on a sapphire rod and placed inside a white zirconia sleeve. This sleeve guides the fiber ferrule that was inserted into it such that the fiber core is centered 50 μm above the TES. This ensures the optimal alignment of light from the fiber onto the detector surface. There is a slit in the zirconia sleeve through which protrude two gold coated electric terminals shaped liked bars. Bond wires connect these to two gold plated copper prongs that form the terminals of the assembled TES detector.

The single photon signal we need to detect is coupled into SMF-28e optical fibers ending in an AR coated FC/UPC ferule. The fiber is held in place and centered over the TES using a zirconia sleeve (see Figure 4.7) [4]. Our TES detectors consist of a 20 nm thick tungsten film with an area of 25 μm^2 on a silicon substrate [103] (Figure 4.8). The substrate sits on top of a sapphire rod which is heat sunk to a larger copper mass. The sapphire rod supports both the superconducting film and zirconia sleeve, ensuring that the core of the fiber is centered above the TES.

The detection efficiency of a bare thin film of 20 nm thick tungsten is 15–20 % at near IR wavelengths [16]. It is limited by the reflection from the surface and transmission through the film. The detection efficiency is increased by embedding the tungsten film in a stack of optical elements that enhance the absorption of light in the detector (see Figure 4.9).

4.4.1 Electro-thermal feedback

TES detectors are quantum calorimeters [16]. The main parts of a calorimeter are an absorber, a thermometer and a weak thermal link to a heat sink/reservoir. When light impinges on the absorber it first heats up quickly, and then slowly cools through the

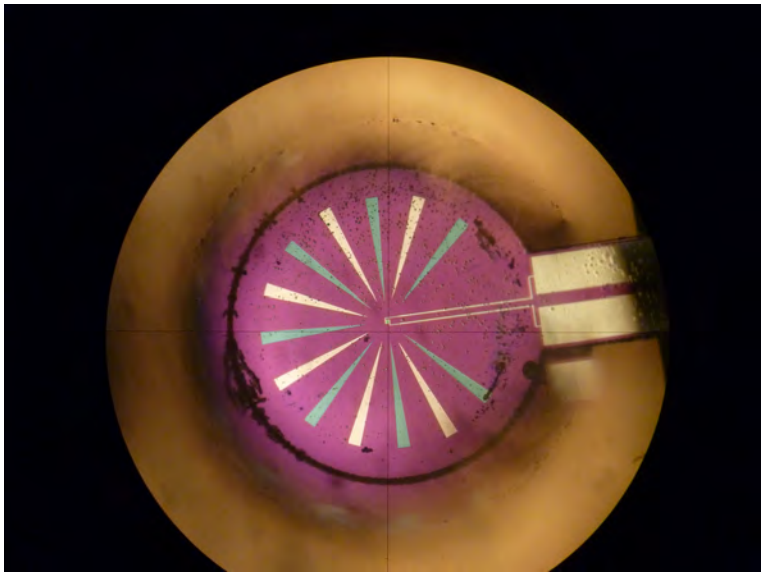


Figure 4.8: A Transition Edge Sensor (TES) seen under a microscope. The small central square is the active area of the detector. The green and yellow triangles are centering arrows. The red base is the sapphire rod. Surrounding the sapphire (yellow halo) is a vertical zirconia sleeve. Emerging from the tungsten film are the two wires connected to prongs.

weak thermal link. The temperature change is measured by the thermometer based on the change in resistance of the superconducting film.

Here I summarize the description of the electro-thermal feedback mechanism found in [104]. Figure 4.10 shows a thermal model of the TES. The superconductor consists of an electron-phonon system and is in thermal contact with a substrate. The electron subsystem of this film plays the role of both absorber and thermometer. The TES detector is cooled below its superconducting transition temperature (T_c) and a voltage bias is applied to it. This increases the electron subsystem's temperature (T_e) above that of the substrate (T_{sub}). At low temperatures the electrons in tungsten have an anomalously low thermal coupling to the phonons. This provides the weak thermal link. An incident photon is absorbed by the electrons and their temperature increases. A rapid change in temperature when near T_c results in a large and rapid change in the resistance of the superconductor. The change of current in the voltage biased detector is measured with a SQUID array (see Section 4.4.2). There is a non-linearity in the temperature dependence of the resistance in the superconducting to normal conducting

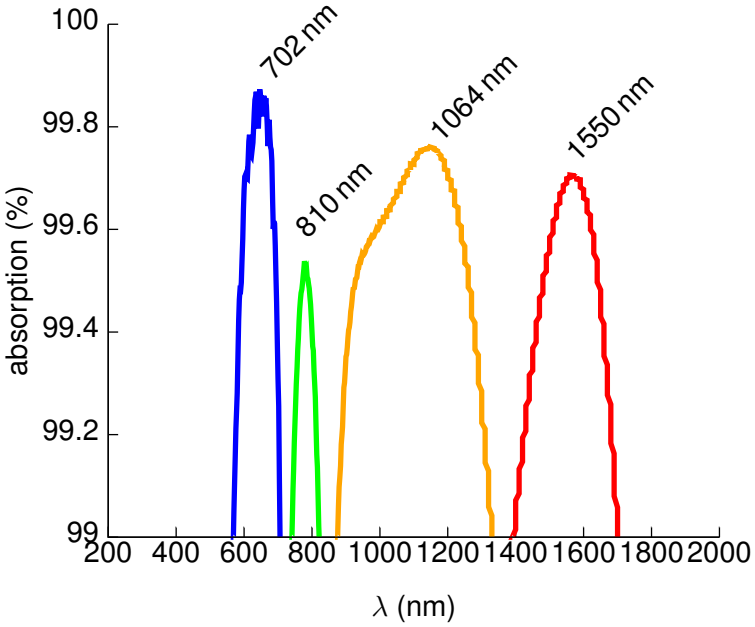


Figure 4.9: The absorption of a TES is largely dependent on the optical coatings. This graph shows the absorption of the various types of tungsten TESs made at NIST. The absorption without optical coatings is about 15 % [16]. This graph is from [17].

phase transition. Thus the sensitivity of the detector and its photon number resolving ability[1] is dependent on where it is biased along this transition.

The applied voltage bias keeps the electrons in the superconducting to normal transition by a process called electro-thermal feedback. The phase transition is very narrow (less than 1 mK wide) and biasing the detector by controlling the cryostat temperature is very difficult. Electro-thermal feedback is effective as long as the temperature of the cryostat/heat reservoir is well below the superconducting temperature of ≈ 140 mK.

Electro-thermal feedback was first used to stabilize the temperature of TES detectors in 1995 by Irwin et al. [15]. Since we are in an electron-phonon decoupled regime, we require a biasing technique capable of injecting power directly into the electron subsystem, rather than into the phonon subsystem. The temperature of the phonons is that of the substrate — T_{sub}. A heater which is coupled thermally to the entire detector will raise T_{sub} in addition to T_e which is undesirable. The electro-thermal feedback technique uses the resistive heating in the electron subsystem itself as a bias

[1]Photon number resolving is due to the energy resolving ability of the detector. It is only possible if the wavelength of incident photons is known.

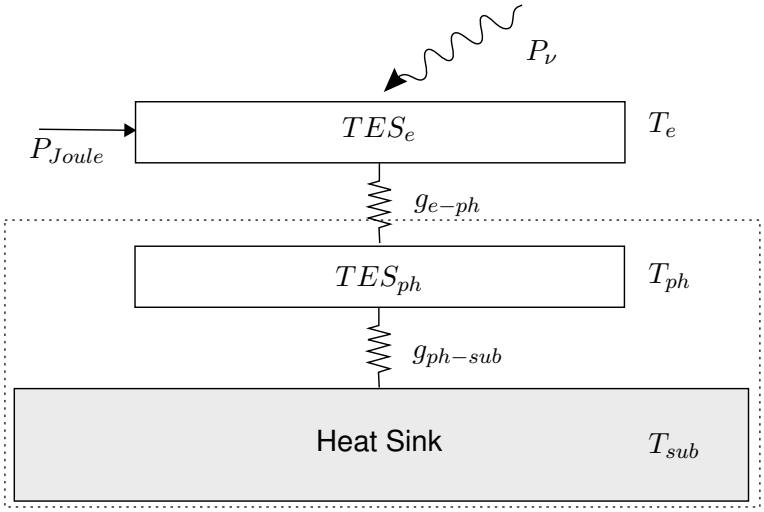


Figure 4.10: Thermal model of a TES showing the Joule heating bias power P_{joule}, incident photon power P_ν, the weak thermal link between the electron and phonon subsystems g_{e-ph} and the strong thermal link between the phonon subsystem and the substrate g_{ph-sub}. At typical transition temperatures $g_{ph-sub} \gg g_{e-ph}$ ensuring that elements inside the dotted box are at a temperature T_{sub}.

heater. This technique is a convenient mechanism for delivering power directly to the electrons. It eliminates the need for external heaters. Most importantly, it allows for a self regulation of each detector, independently of their individually varying T_c.

To understand how electro-thermal feedback works let us assume that the TES starts in a correctly biased state (i.e. partway along its superconducting to normal conducting phase transition). The electron subsystem of the TES has a finite resistance R_e and is maintained at the transition temperature T_c due to an applied voltage across this resistance. The voltage across the detector (V) applies a Joule power $P_{Joule} = V^2/R_e$ directly to the electron subsystem. Any increase in temperature increases the resistance. Due to the constant voltage bias being applied, P_{Joule} will drop proportional to $1/R_e$. This decrease in the Joule heating cools the TES back towards the bias point. Similarly a decrease in temperature will decrease the resistance and warm up the detector. Thus the electro-thermal feedback mechanism automatically regulates the temperature of the electron subsystem of a TES.

Figure 4.11 shows the circuit diagram used for electro-thermal feedback with our TES detectors. The TES is cooled to 70 mK by a cryostat. Its electron subsystem

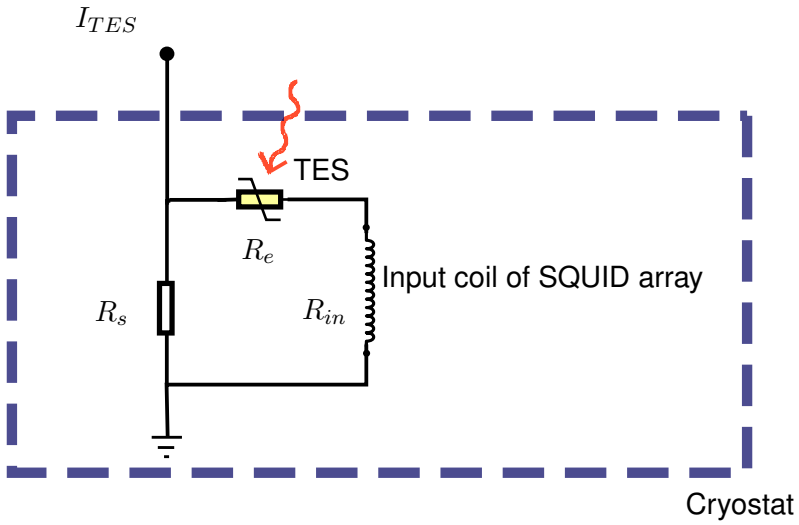


Figure 4.11: Biasing of the TES using electro-thermal feedback. A shunt resistor R_s is used to convert the constant current I_{TES} into a constant voltage bias across the TES. I_{TES} is supplied and controlled from outside the cryostat. The voltage bias causes Joule heating inside the electron subsystem of the TES (which has a resistance R_e and a temperature T_e). When the temperature of the electrons increase (decrease) R_e increases (decreases). This causes the Joule heating to decrease (increase) T_e, maintaining the temperature of the electrons along the superconducting transition. The change in current flowing through the input coil of a SQUID array is measured to detect the resistance change of the TES. The TES is kept at 70 mK, the SQUID array and R_s are at 2.5 K. The TES is connected to the SQUID and shunt via a 30 cm long superconducting NiTi wire.

has a resistance R_e. When a photon is absorbed by the detector the temperature of the electrons T_e increase. This changes the resistance R_e. Biasing and electro-thermal feedback is maintained by a voltage bias across the TES. The input coil of a SQUID array is connected in series with the TES (see Section 4.4.4). This whole circuit is fed with a constant current I_{TES} from outside the cryostat. A shunt resistor R_s, in parallel with the TES, converts I_{TES} to a voltage bias across the TES. This is done to avoid the challenge of using low resistance bias lines feeding the detectors.

The input coil of the SQUID array will have a resistance (R_{in}). R_s should be much smaller than $R_{in} + R_e$ to create a stable voltage bias across the series combination of the input coil and detector. The optical energy deposited in the absorber (tungsten electron subsystem) is given by the product of the bias voltage (V) and the time integral

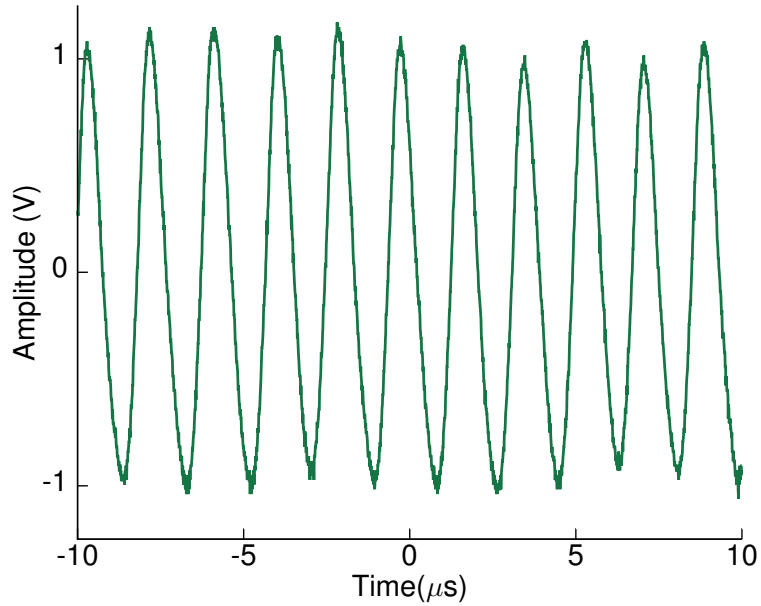


Figure 4.12: Electro-thermal oscillations of the TES. I_{TES} was 25 μA. the temperature was 72 mK. To detect single photon signals we increase I_{TES} until we are beyond the regime of the electro-thermal oscillations

of the change in current (ΔI) through the input coil:

$$E = V \int \Delta I(t) dt \,. \tag{4.2}$$

We use a shunt resistance of about 60 mΩ. This shunt resistance consists of a piece of phosphor bronze wire with AWG 36 about 7 mm long (Lake Shore cryogenics WDY-36-100). The shunt resistor is mounted to the back of the circuit board connected to the SQUIDs and is kept at 2.5 K. Superconducting Niobium-Titanium (NiTi) wire connects the TES to the SQUID array. The value of the shunt resistance was chosen empirically. This was necessary because there was a stray/parasitic resistance on the order of 20 mΩ we could not eliminate.

For the electro-thermal feedback mechanism to work we must be able to provide the right voltage bias to the detector. We control the voltage by adjusting I_{TES}. When this value is too small there is insufficient voltage to warm up the electrons of the TES to their correct biasing point along the superconducting transition. As we increase I_{TES} we encounter an unstable regime wherein there is enough energy deposited to

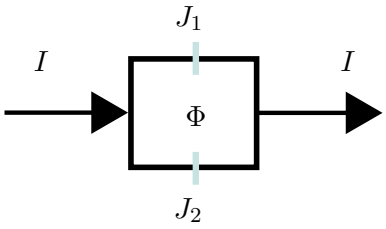


Figure 4.13: Schematic of a SQUID showing the two Josephson junctions J_1 and J_2. Φ represents the applied magnetic flux. A current I is made to flow through the SQUID.

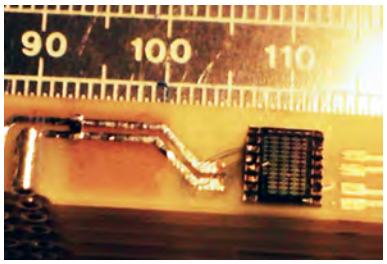


Figure 4.14: Picture showing the array of SQUIDs we use to measure the signal from the TES.

temporarily heat the electrons. As their temperature and resistance increase slightly, P_{Joule} decreases enough to cool the electrons down. This leads to oscillations called electro-thermal oscillations. Figure 4.12 shows such oscillations. I_{TES} was 25 μA and the cryostat temperature was 72 mK. We increase I_{TES} further till there is a strong voltage bias and these oscillations die out. This region is the operating current for the TES bias (typically, $I_{TES} = 38\,\mu$A and $\approx 20\,\mu$A flows through the series combination of the TES and SQUID input coil).

4.4.2 The SQUID amplifier

In order to detect the small change in current flow caused by the change in resistance (of $\approx$ 1–2 Ω) of the superconducting TES we need a very sensitive and low impedance amplifier, such as a Superconducting Quantum Interference Device (SQUID) amplifier. A SQUID is a very sensitive magnetometer capable of measuring fields as low as 10^{-16} T. The signal from the TES is passed to a coil wound near the SQUID. The TES is connected in series with the input coil of the SQUID. The geometry of this coil is such that a current through it is converted into a magnetic field in the SQUID. Practically we do not use a single SQUID because the gain is limited, instead we use an array of about 100 SQUIDs to get the required gain [105] (see Figure 4.14). The SQUIDs we use were obtained from NIST.

The first SQUIDs was made in 1964 [106], and they were first used in conjunction with TES detectors by Seidel in 1990 [98]. In his book [97], Clarke provides an excellent explanation of the working of a SQUID.

A SQUID [106] is essentially a flux to voltage transducer and consists of a superconducting loop with two Josephson junctions[1] (see Figure 4.13). These junctions are in parallel and a current I is applied across the device. In the absence of an external magnetic field the current I is split equally into the two branches. When a small magnetic field is applied to the superconducting loop, a screening current I_s begins to circulate. I_s generates a magnetic field opposite to the applied flux. In one junction I_s is opposite to I, while in the other it is in the same direction. As soon as the current in one branch exceeds the critical current ${I_c}^2$ of the Josephson junction a voltage is developed across the junction.

The magnetic flux enclosed by the superconducting loop is quantized and must be an integer multiple of Φ_0 [107, 108] (where Φ_0 is the magnetic flux quantum[3]). Suppose the SQUID's superconducting loop is initially in a region of 0 external magnetic flux. When the external magnetic flux is increased until it exceeds $\Phi_0/2$, due to the flux quantization, it becomes energetically favorable to increase the flux enclosed by the superconducting loop to Φ_0. This is done by changing the direction of the generated screening current I_s. Thus for every half integer multiple of Φ_0 in the applied magnetic flux, I_s changes direction, causing the voltage developed across the SQUID to oscillate (see Figure 4.17).

The SQUID must be shielded from external magnetic fields. This is done by encasing the SQUID in multiple layers of magnetic shielding. The inner most layer is a μ-metal casing, on top of which there is a niobium shield. We encase this whole structure in a lead box as a secondary superconducting shield. The niobium and lead layers go superconducting (below 9.2 K and 7.1 K respectively) and due to the Meissner effect [109] provide magnetic shielding.

The niobium and lead shields are superconducting which means that their thermal conductivity is near zero, therefore thermal contact of the SQUID amplifiers with the cold fridge is maintained by copper wires in a way that does not interfere with superconducting shielding elements.

[1] Here I only consider DC SQUIDs, information on RF SQUIDS can be found in [97].

[2] I_c is the largest current that can flow through a superconductor, above which it looses its superconductivity. For a Josephson junction I_c depends on the applied magnetic flux.

[3] For a superconducting loop or hole in a bulk superconductor $\Phi_0 = \frac{h}{2e} \approx 2 \times 10^{-15}\, Wb$. The flux Φ threading a normal loop of area $\mathbf{A}$ is given in terms of the magnetic inductance $\mathbf{B}$ as $\Phi = \mathbf{B} \times \mathbf{A}$, and can be arbitrary.

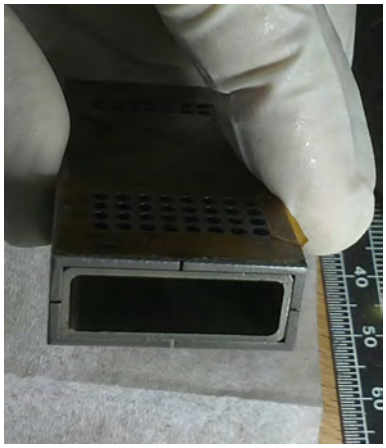


Figure 4.15: Picture of the magnetic shielding encasing the SQUID. Seen here are the μ-metal shield (inner layer) and the niobium shield (outer layer). These rectangular shields are wrapped around the SQUIDs which are mounted upon circuit boards seen in Figure 4.14. The circuit boards are inserted length wise along the shields.

It is important that all SQUIDs in the array stay in phase because when there is a trapped or stray magnetic field in some of them, the over all gain will be reduced. Unwanted magnetic fields may become trapped in parts of the SQUID array for a variety of reasons, for example electronic noise or a magnetized object. To remove these unwanted effects we "zap" the SQUID array: we send a large current ($\approx 2\,\mathrm{mA}$) through the SQUIDs, enough to drive them into a normal conducting mode. This current is applied for about 10 s. Then the SQUIDs are disconnected from all currents and magnetic fields until they are once more superconducting (after about 30 s). The SQUIDs are then all in phase and the SQUID array has recovered the best gain.

The SQUID array is characterized by its $I - V$ characteristic curve. The larger the slope of this $I - V$ characteristic curve, the larger the gain of the SQUID array. For a SQUID to operate there must be a current I_{sq} flowing through it. (see Figure 4.16). For each value of I_{sq} we obtain a different $I - V$curve (see Figure 4.17).

Both the feedback and input coils change the magnetic field near the SQUID array, with the feedback coil having 8 times fewer turns than the input coil. Typically, the TES is connected to the input coil and the feedback coil connected to an adjustable current source. In normal operation the feedback coil is used to adjust the working point of the SQUID array for maximum gain; to characterize its current response, we

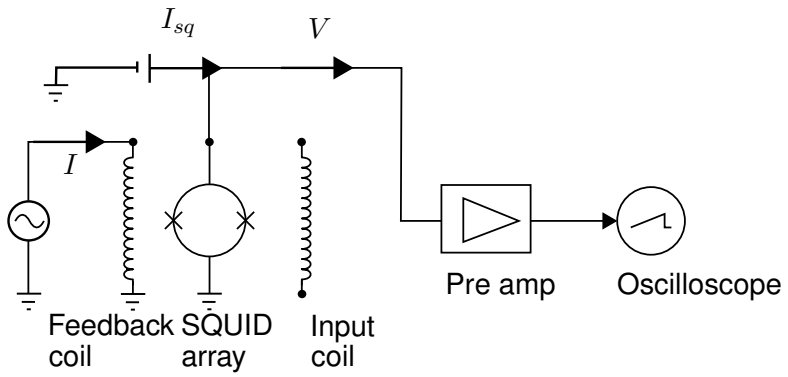


Figure 4.16: A circuit diagram of the SQUID. The SQUID array we use has two inputs. The primary coil is called the input coil and is usually connected to the TES. The secondary coil is called the feedback coil and is used to adjust the phase of the SQUID array. When testing the SQUID we apply a signal to either the input coil or the feedback coil. The signal from the SQUID is amplified by a preamp before it is recorded with an oscilloscope.

sent a varying current through the feedback coil, and recorded the output voltage V for different I_{sq} (see Figure 4.17).

From the $I - V$ curves we obtained the correct operating value of I_{sq} which is when the amplitude of the $I - V$ curve is maximum. For the data shown in Figure 4.17 this is $45\,\mu$A. The slope of the $I - V$ curve is indicative of the sensitivity of the SQUID array at each point. At maximum slope a small change in the input current results in a large change of the output voltage. By finding the points of the largest slopes, we were able to choose the operating value for the feedback coil current (I_{fb}).

The feedback coil current chosen from the $I - V$ curve is not necessarily the final value we used. This is because the TES also requires a bias current to work. This current constantly flows through the input coil of the SQUID array. The TES bias current thus causes a phase shift in the $I - V$ curve. The $I - V$ curve was measured again when the TES bias was set. In practice the $I - V$ curve was measured using a function generator as the source of the feedback coil current and the results were seen on an oscilloscope. This was done repeatedly and in real time to fix the correct operating value of the feedback coil current while we adjust the TES bias. Thus the feedback coil current is used to adjust the phase of the SQUID array such that its sensitivity to a change in the input coil current is maximum. Under typical operating conditions the transimpedance gain of the SQUID array is about $49\,\Omega$ (between the input coil current and output voltage).

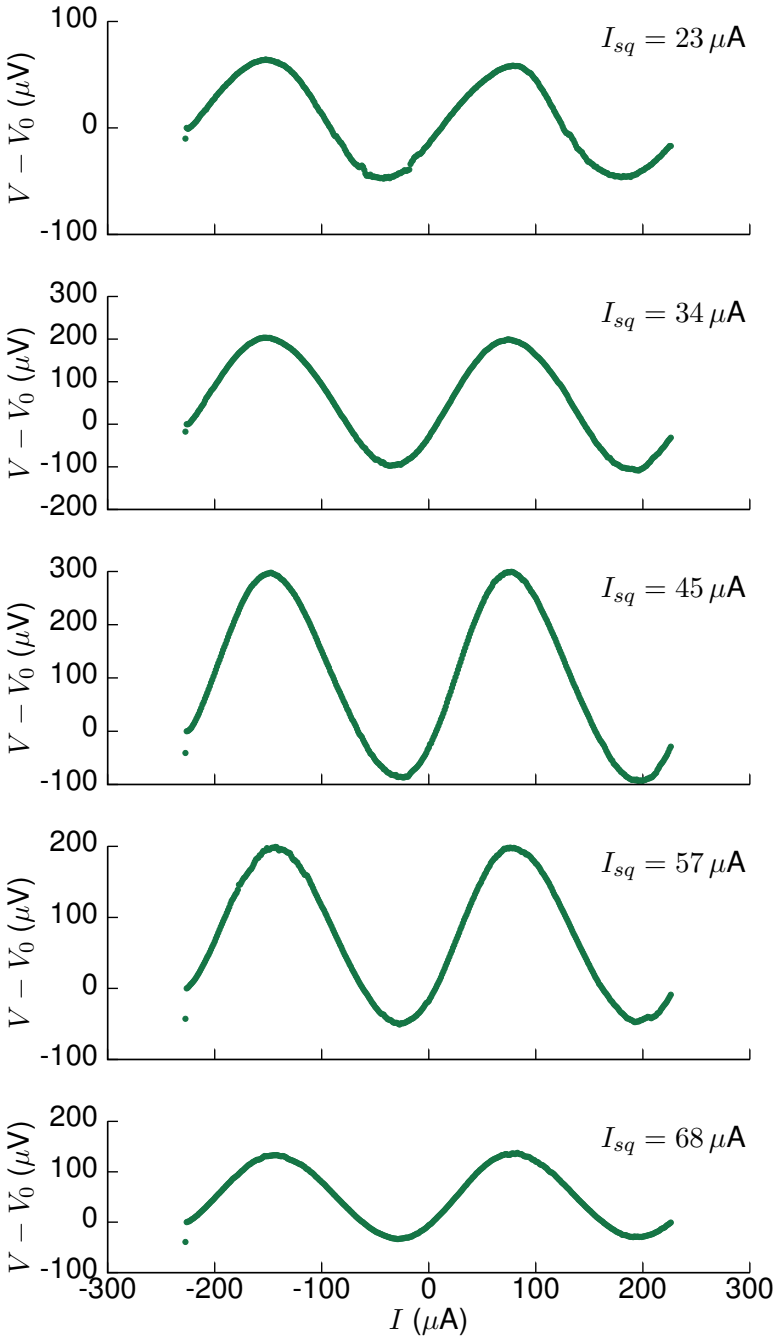


Figure 4.17: I – V curves of one SQUID array. At each value of I_{sq} we vary the current applied to the feedback coil and measure the output voltage from the SQUID V. The best value of I_{sq} (operating current for the SQUID) is when the amplitude of the I – V curve is maximum. In this case it is 45 μA.

4.4.3 Adiabatic Demagnetization Refrigerator

The TES detectors work at about 70 mK and the SQUID arrays work at temperatures below 4 K. We thus need a way to cool the detectors and SQUIDs down to these cryogenic temperatures. Furthermore, at such low temperatures the thermal and black-body noises are minimized.

An Adiabatic Demagnetization Refrigerator(ADR) is a closed cycle apparatus for cryogenically cooling a sample and was first built in 1933 [110]. The working principles of an ADR are discussed in detail in chapter 9 of [111]. In the first step, a pulse tube cooler is used to bring the temperature down to 2.5 K. The pulse tube cooler is a Sumitomo Heavy Industry's F-50 with a cooling power of 400 mW at 2.5 K. Then, in the second step, the adiabatic demagnetization of strongly paramagnetic salts brings the temperature to a minimum of 30 mK. This step is a single shot process[1]. The ADR we use was built by Entropy and has a cooling power of 1 μJ at 100 mK[2].

The pulse tube cooler is connected to a helium compressor via a rotary valve. The rotary valve is used to alternatively connect the pulse tube to high and low pressure lines of helium. The helium is made to flow alternatively into and out of a regenerator[3]. On either side of the regenerator there is a heat exchanger. The first heat exchanger is where thermal energy is dumped to the surroundings. The second is where the useful cooling power is delivered. When there is a high pressure of helium, it enters the regenerator at a high temperature and leaves at a lower temperature. On its return, heat stored within the regenerator is transferred back into the gas. The regenerator can be thought of as thermal memory of the system. Attached to the cold end (i.e. the cool heat exchanger) is the sample that needs to be cooled. Joule-Thompson expansion is used to cool the sample via a non-adiabatic process.

Figure 4.18 shows a picture of the ADR. The pulse tube head is seen at the bottom and the tube itself is seen extending almost all the way to the top. Different regenerator materials are effective in different temperature ranges. Thus for better performance the pulse tube cooler is designed in two stages. The first stage will reduce the temperature

[1] As opposed to the continuous cooling provided by the pulse tube cooler, the demagnetization process can only reduce the temperature of the cold finger once, after which it slowly warms up.

[2] The adiabatic demagnetization cooling is a single shot process and not a continuous one, consequently I express the cooling power of this stage in Joules instead of Watts.

[3] The regenerator is a porous medium with a large specific heat.

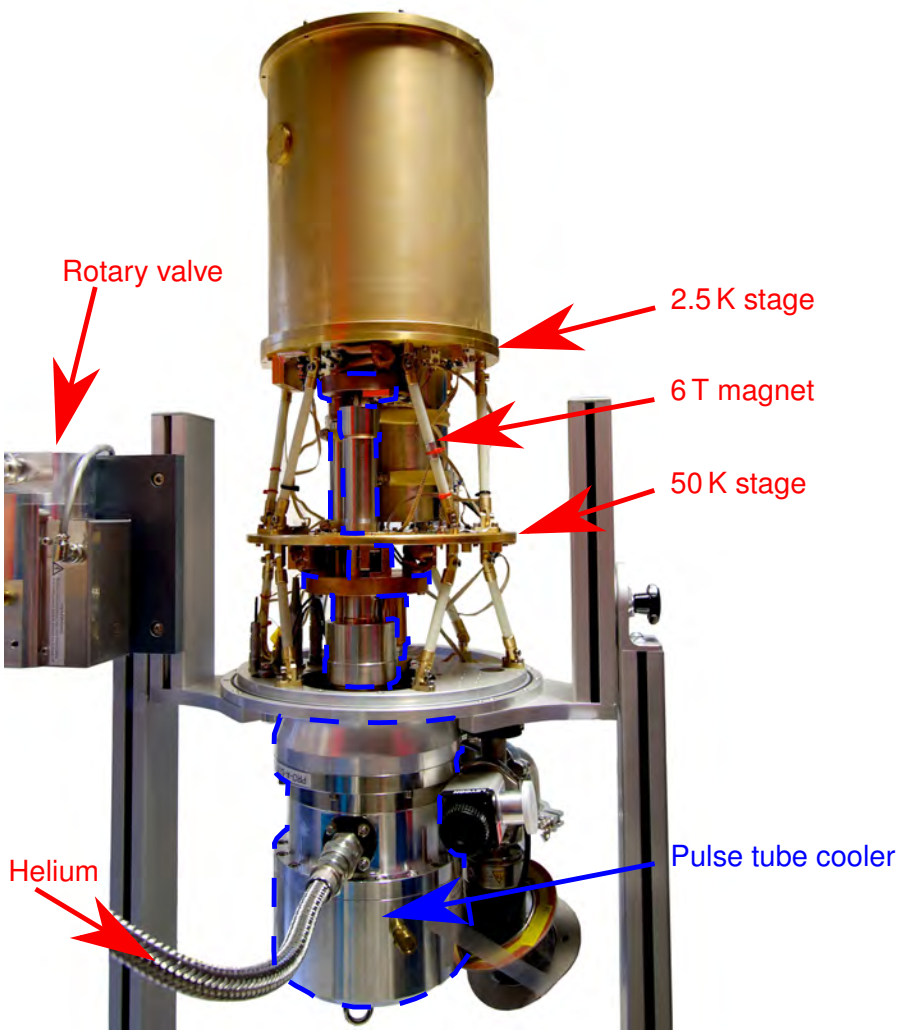


Figure 4.18: The Adiabatic Demagnetization Refrigerator (ADR). The Pulse tube cooler outlined in blue dashes is responsible for cooling the topmost part of the fridge to 2.5 K. This is done via a 50 K stage which is also cooled by the first half of the pulse tube cooler. The helium for the pulse tube cooler is supplied via the rotary valve which alternatively ensures a high and low helium pressure. Suspended from the bottom of the 2.5 K stage is the 6 T magnet. This superconducting magnet is also cooled by the pulse tube cooler.

to 50 K and the second stage to 2.5 K. Each stage is connected to a large circular copper plate. The uppermost plate is shown with an insulating bucket covering it. When in operation, each plate is covered with a similar bucket. A large outer bucket forms a vacuum seal and allows the inside to be evacuated. Hanging just beneath the 2.5 K plate is a large magnet. This magnet is made out of superconducting niobium-titanium (NiTi) wire. In its center it generates fields of more than 6 T when supplied with 40 A.

The center of this magnet contains the paramagnetic salt pills responsible for the second step of cooling. Maintaining the salt pills at <3 K, we gradually ramp up the magnetic field causing the magnetic dipoles to align themselves with the field. We then break the thermal contact between the salt pills and the pulse tube cooler and ramp the magnetic field down adiabatically. Due to the paramagnetic nature of the salts, their magnetic dipoles return to a disordered state. Doing so increases their entropy. At this point the salt pills are only in thermal contact with a copper rod called the cold finger (see Figure 4.19) which supports the detectors in their housing. Since the demagnetization of the salt pills is adiabatic, the entropy they absorb comes from the cold finger. This effectively cools the detectors from 2.5 K to a minimum of 30 mK.

Practically we need to use two different salts. A Gadolinium-Gallium Garnet (GGG) pill is used along with a very strong magnetic field to reduce the temperature to 300 mK. A Ferric Ammonium Alum (FAA) pill is placed inside the GGG. This works at a weaker magnetic field and reduces the temperature from 300 mK to 30 mK. Once a demagnetization cycle is complete the cold finger slowly warms up. It takes about 12 hours for its temperature to exceed 70 mK; this is called the hold time of our ADR. When the temperature exceeds the operating point of the TESs we have to repeat the magnetization and adiabatic demagnetization cycle. The minimum temperature we attain with our ADR is 30 mK, but the operating temperature of the TES is about 70 mK. We increase the temperature by applying a small magnetic field to the salt pills. To regulate the temperature at 70 mK we gradually decrease this magnetic field. We automated this by implementing a software PID control loop.

4.4.4 Detecting a photon

With the TES cryogenically cooled (see Section 4.4.3) and biased (as described in Section 4.4.1), we connect it to the input coils of a SQUID array (see Section 4.4.2)

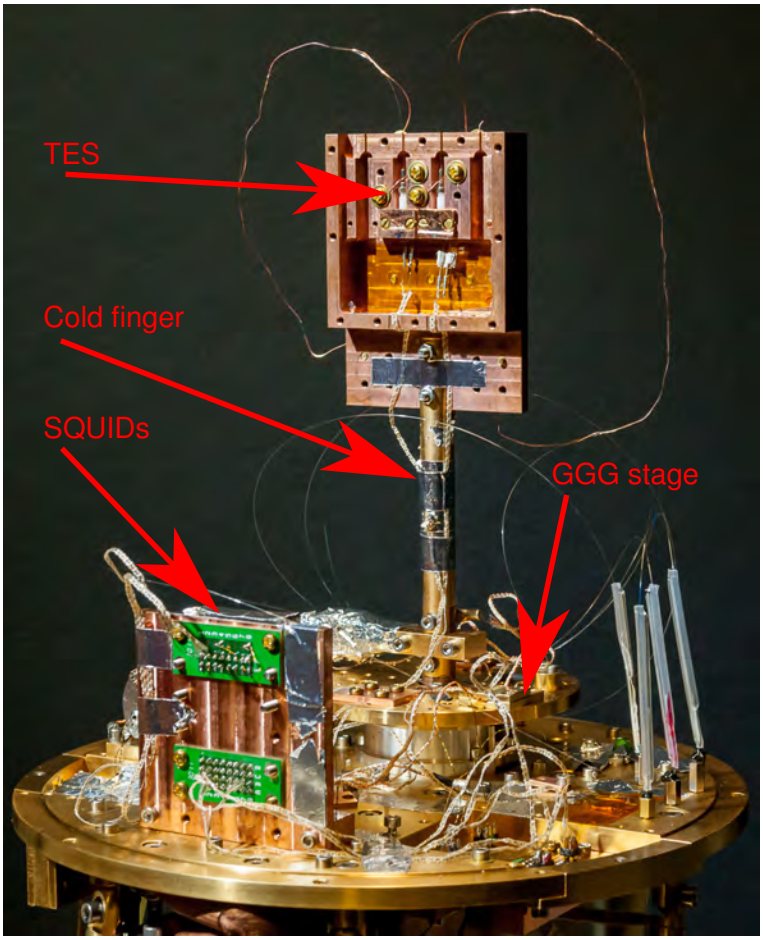


Figure 4.19: TES detectors are mounted at the top of the cold finger. The SQUIDs are mounted on the 2.5 K stage.

which is used to detect the change in resistance of the TES. The feedback coil current I_{fb} is adjusted for maximum sensitivity to a change in the input coil current. The output from the SQUID array is fed to a preamp consisting of two AD797 low noise ($0.9\,\mathrm{nV}/\sqrt{Hz}$) amplifiers and has a gain of about 40 dB ($97\times$). The preamp has a bandwidth from DC to 10 MHz. The output of the preamp is sent to an Stanford Research System's SR560 low noise amplifier with a bandwidth of 10 KHz – 1 MHz and a gain of 46 dB ($200\times$).

The amplifier is connected to an oscilloscope or a Constant Fraction Discriminator (CFD). The CFD is an electronic signal processing device, designed to mimic the mathematical operation of finding a maximum of a pulse by finding the zero of its time

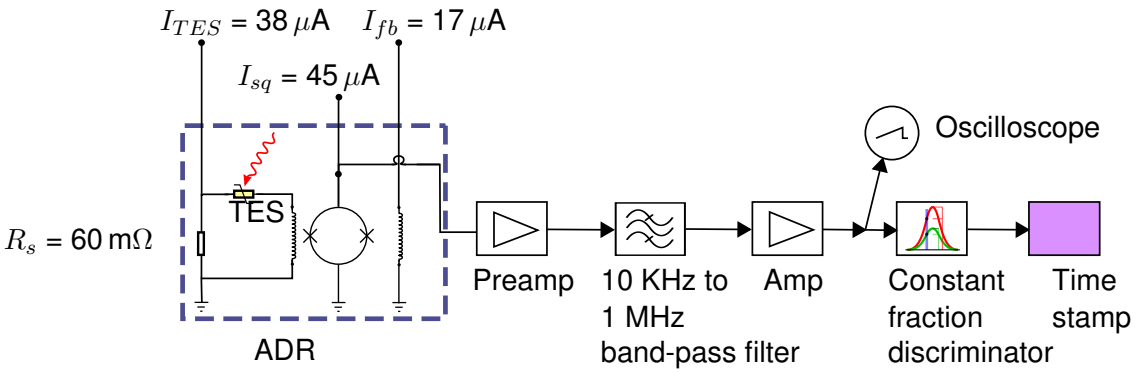


Figure 4.20: The TES is voltage biased by the shunt resistor R_s and the current source I_{TES}. The SQUID array is powered by I_{sq} and is set to peak sensitivity by controlling the feedback coil current I_{fb}. Typical operating values are shown. The output from the SQUID array passes through a preamp, a set of filters and an amplifier. The signal is then sent to either an oscilloscope or a Constant Fraction Discriminator(CFD). The CFD is used to distinguish the pulses due to photons. A time stamp device records the time of arrival of each detection event.

derivative. Chapter 4 of [112] provides a good description of a CFD. This is useful when the signal does not always have a sharp or constant maximum but has timing information. The CFD is better than simple threshold triggering. Consider pulses which have a large rise time and whose maximum height varies slightly. Threshold triggering on these pulses results in a different triggering time based on the peak height. This problem is eliminated by a CFD. Effectively a CFD will trigger at a constant fraction of the pulse height.We use a CFD with the TES signals because the peak height varies (due to multiple photon events, noise, thermal coupling and response of the SQUID) and the timing information of these peaks is crucial to both reducing the timing jitter of the detector and detecting coincidences with as small a coincidence time window as possible.

Our CFD only detects signals whose amplitude exceeds a chosen threshold value. Typically this threshold is set at $\approx 300\,\text{mV}$. The value is chosen, by measuring the pulse height distribution, to be larger than that of the noise amplitude but significantly smaller than the single photon peak amplitude (see Section 4.5.1 for more details). A good choice of this value will avoid most of the noise. This value is chosen by measuring the pulse height distribution. Alternatively, we choose this value to be larger than that of the noise amplitude but significantly smaller than the single photon peak amplitude.

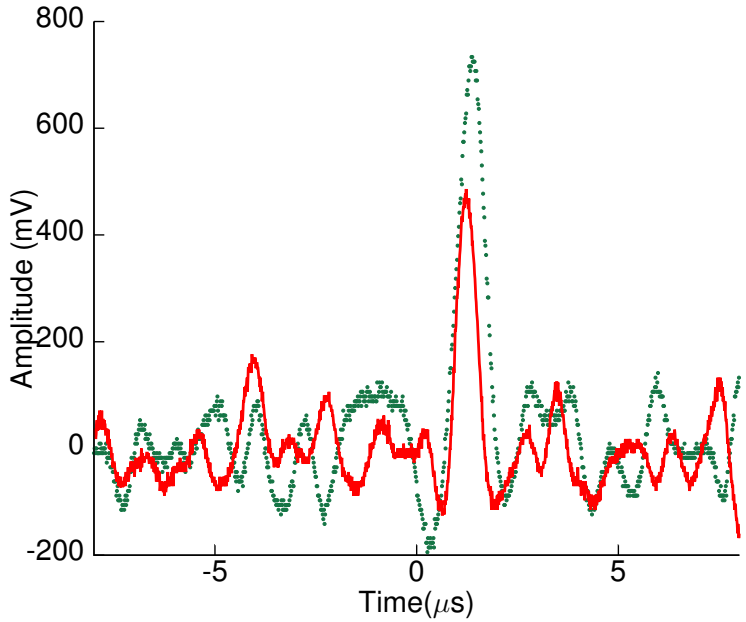


Figure 4.21: Typical detection pulses (after a net amplification with $\approx$ 119 dB voltage gain) due to single (solid red) and double (dotted green) photon signals as seen by a TES. An attenuated laser was used to generate the photon pulses. A function generator was used to drive an attenuated laser and served as the trigger for this measurement.

The operating currents I_{sq} and I_{fb}, were set by measuring the $I - V$ curves of the SQUID array. We then increased I_{TES} to see the electro-thermal oscillations. The value of I_{TES} was chosen to be slightly more than needed for electro-thermal oscillations to die out. With the value of I_{TES} set we once more needed to adjust the value of I_{fb}. This is because any current flowing through the input coil of the SQUID array will cause the $I - V$ curve to shift. This means that we may no longer have been in the regime of maximum sensitivity. Consequently, I_{fb} was readjusted by measuring the $I - V$ curve again.

The TES detectors were connected to SMF-28e fibers. These fibers exit the fridge and can be connected to a light source. Initially they were connected to an attenuated laser which was in turn driven by a function generator. This allowed us to send in triggered pulses of light. We adjusted the laser intensity to less than one photon per pulse. This allowed us to correctly adjust the CFD threshold value. In Figure 4.21 we see a typical single photon detection pulse.

Careful attention must be paid to noise filtering at each and every stage of the experiment. In addition to isolating the SQUIDs from magnetic disturbances we must also make sure that the TESs are shielded from large magnetic fields. Applying a large magnetic field to the TES could drive the tungsten film normal conducting. Fluctuating magnetic fields are seen as electrical noise on the signal. Black-body radiation may strike the detector giving raise to background counts. To avoid this, the TES detectors are encased in their own housing. Also each temperature plate of the ADR is optically isolated from the others by means of large thermally conductive buckets.

Electrical noise is the major contributor to the observed noise. All detector wiring is separated from potential noise sources. The electrical wiring of the fridge sensors and heat switch are potential noise sources. We placed low pass RC filters, with a cut-off frequency of about 15 Hz, on both the TES bias and feedback coil bias lines. These filters are on the 2.5 K stage as well as outside the fridge. Instrumentation amplifiers and isolation transformers are used to break ground loops.

4.5 Measurements with the high efficiency source and TESs

As described in the Chapter 3 we have a source of photon pairs with a very high heralding efficiency. As measured using Si APDs, this efficiency is 39.3 ± 0.2 %[1]. To perform any experiment requiring a higher efficiency, we need to replace the APDs with the TESs.

The downconverted light (at 810 nm) is coupled into 780-HP[2] fibers which are then spliced onto the SMF-28e fibers connected to the TESs. Due to the lower loss [113] (about 3.5 dB/km lower than 780-HP) in SMF-28e fibers, such a splice is useful if the detectors need to be several meters away from the source[3].

4.5.1 Peak height distribution

The CFD threshold must be set such that we measure only those peaks which are due to photons from the source. Under good operating conditions the noise peaks due to

[1] Correcting for the measured detection efficiencies of our APDs (51.9 ± 2.8 % and 46.7 ± 2.5 %) our source has an efficiency of 81.6 ± 3.0 % as discussed in Section 3.4.

[2] The 780-HP fiber from Nufern is a single mode optical fiber for 780 nm to 970 nm.

[3] One example of an experiment where such a separation is necessary would be a loophole free Bell test.

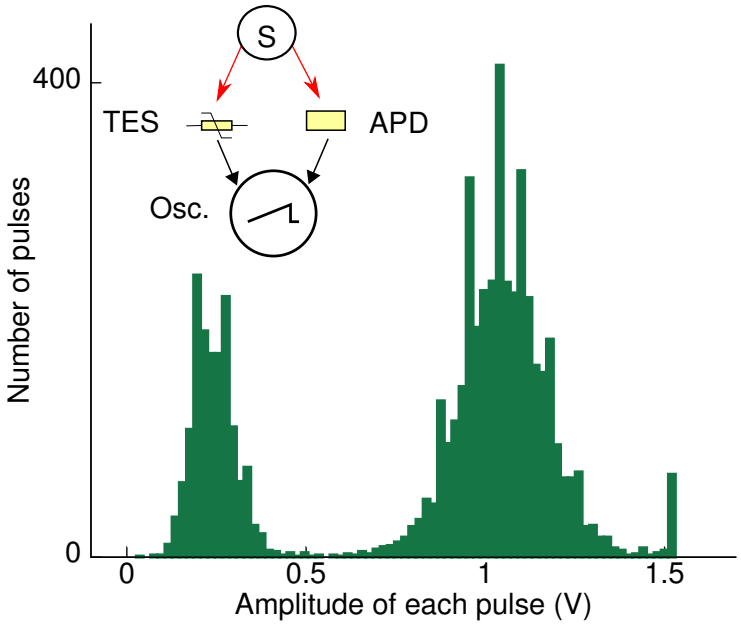


Figure 4.22: Pulse height distribution of pulses seen from the TES and APD connected to the photon pair source. We triggered on the APD and measured on the TES. The first peak represents the noise we see in the electrical signal. The second represents the pulse height distribution due to a single photon. The third very small peak represents 405 nm pump photons that were allowed to enter the collection fibers by removing the interference filter. Some peaks in the histogram are abnormally high due to a digitization error of the oscilloscope (Osc.) used to acquire the data.

thermal noise and many forms of electrical and magnetic noise are smaller than the photon peaks. This is clearly seen in a histogram of the amplitudes of all peaks (see Figure 4.22). There is a clear distinction between the first peak and the second. Since the first peak represents the noise amplitudes and the second the amplitudes of valid photon pulses, we choose a value inbetween (say 0.6 V) to be the CFD threshold.

To measure the graph shown in Figure 4.22 we connected a TES and an APD to the high efficiency source. We pumped the source from a single direction only to produce heralded photon pairs. This simplifies the alignment process. One photon of each pair was sent to the TES; the other was sent to the APD. The signal from the APD was used as a trigger for an oscilloscope. The TES parameters (TES bias, SQUID bias, feedback bias) were optimized for the highest heralding efficiency and least noise. The signal from the TES was also sent to the same oscilloscope. The oscilloscope recorded the maximum amplitude of the signal each time it was triggered. The SRS amplifier

(see Section 4.4.4) was set to have a gain of 500 ×, and the filtering had a pass band of 10 KHz to 1 MHz with a 6 dB/octave roll-off.

The first peak represents the contribution due to noise. We see that the noise typically has an average peak amplitude of 0.25 V. It is also clear that there is very little noise contribution with peak amplitudes > 0.6 V. Consequently, we set the CFD threshold at 0.6 V. The second peak is due to single photon detection pulses. A useful cross-check is to divide the area under the photon peak with the area under the noise peak. Since we are triggering on the APD signal, this ratio should be the same as the arm efficiency[1] of the source as seen by the other detector (the APD in this case). At the time of this measurement the source had an efficiency of 38.0 % as seen by two Si APDs and 47.4 % as seen by one TES and one APD[2]. By comparing the integral of the two peaks we measure an arm efficiency of 38.5 % for the arm connected to the APD. Which is what we expect.

Further, a third peak in the pulse height distribution would correspond to two photon events. However we do not pump our crystal with enough power to generate a significant rate of two photon events. Instead, for this measurement, we removed the interference filter in that collection arm allowing some 405 nm pump photons to reach the TES. The energy of these photons is double that of the downconverted photons. Thus the pulse height from these photons should be identical to the pulse generated when two photons are incident on the detectors at the same time. When calculating the arm efficiency of the source, these pump photons were treated as background noise.

When the TES is operating properly, each peak in the pulse height distribution must be well resolved. Suppose the interval between the noise peak and the photon's peak in Figure 4.22 is not clearly resolved i.e. the number of pulses never drops to near zero, then it is indicative of excessive noise in the system.

Setting the TES bias (I_{TES}) too high decreases the spacing between the peaks, i.e., the photon number resolving capabilities of the TES are lost. This is because changing I_{TES} changes the biasing point of the TES along its superconducting phase transition (see Section 4.4.1). An increased value of I_{TES} biases the TES at a higher

[1]The arm efficiency of detector 2 is $\frac{p}{s_1}$, where s_1 is the singles rate as seen by detector 1 and p is the pair/coincidence rate between detectors 1 and 2.

[2]The system efficiency in this case was low due to losses in several fiber to fiber joins. These were replaced with splices for the high efficiency measurements shown in section **??**.

temperature and consequently a higher resistance. Due to the non-linear nature of the phase transition the photon number resolving ability is affected.

From Figure 4.22 we can also estimate the energy resolution of the detector itself. The energy of a 810 nm photon is approximately 1.53 eV. The FWHM of the 810 nm photon peak in the figure is about 0.8 eV. The electron subsystem of the TES absorbs roughly 30–40 % of the energy of a photon [114, 115], the rest is absorbed by the phonon subsystem[1]. Thus a crude estimate of the energy resolution of our TES detectors is about 0.28 eV. This value is slightly higher than reported in [16, 115] we attribute this to a spurious 20 mΩ parasitic resistance in the TES biasing circuit.

4.5.2 Background counts

There is a certain probability that the TES registers photon detection events when the was no "valid" incident photon from a light source e.g. the photon pair source. This may be caused by stray light including black-body radiation or by noise on the electrical signal. It is important to measure and minimize these counts. Such spurious detection events are a significant problem for many experiments, as a sufficiently high fraction of such events will result in skewed photon counting statistics (see Section 2.3.2).

The major contributor to the observed dark count rate is electrical and or magnetic noise. We took several steps to reduce their contribution to dark counts. We used several layers of magnetic shielding and extensive electronic filtering of all input lines. Isolation transformers and instrumentation amplifiers help in breaking up ground loops where necessary. Ferrite beads reduce common mode noise in the frequency band of 0.1 — 100 MHz. Phosphor bronze cryogenic twisted pair wires help reduce pick up noise. Despite these steps the sensitivity of the system is such that there was a very large day-to-day fluctuation in the dark count rate. Typically, the dark count rate ranged from several hundred per second to about ten per second.

On occasion, we were able to reduce the background counts to less than $\approx 10/\mathrm{s}$, and a large fraction of those counts were due to stray light that reaches the detector via the optical fibers even with the room lights off.

[1]The probability that the photon is absorbed by the electron subsystem can be improved by a suitable choice of material and manufacturing process.

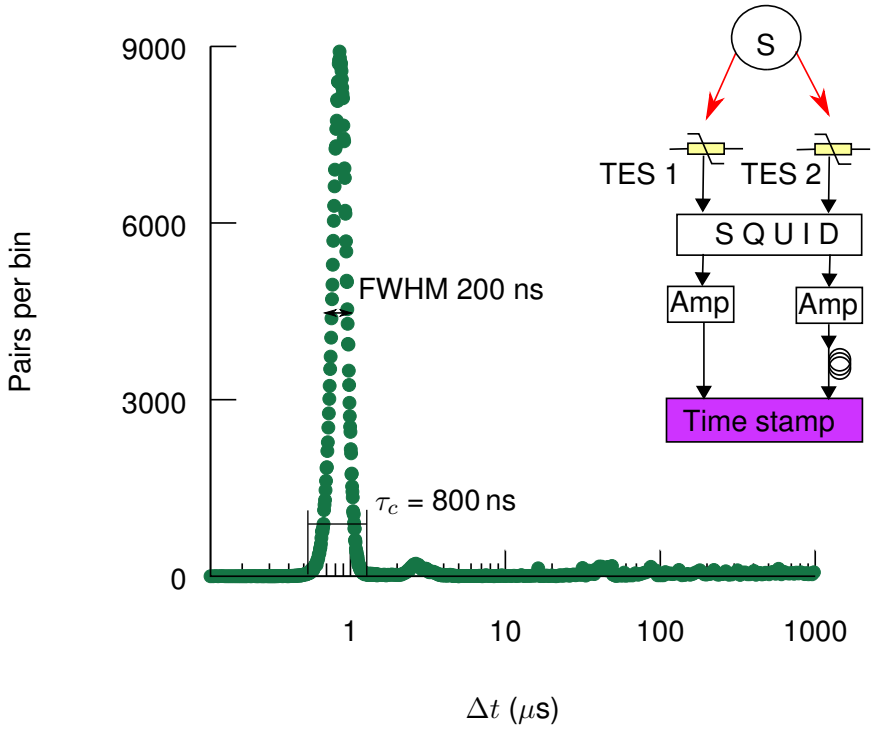


Figure 4.23: The $G^{(2)}$ measured between two TESs connected to the high efficiency source. We observe a dark count corrected system efficiency of 75.2 %. The measurement was taken for 30 s and we used a coincidence time window (τ_c) of 800 ns. We observe a pair rate of 13366.3 /s and singles rates of 19477.2 /s and 16646.0 /s. The error in the efficiency was estimated using the shot noise on each of the count rates. The singles rate seen by one detector is larger due to the presence of The Full Width at Half Maximum (FWHM) of the $G^{(2)}$ gives us the timing jitter of the TESs. We see that the jitter is 200 ns.

4.5.3 Heralding efficiency measurement

One of the aims of this work has been to create a system capable of performing a loophole free Bell test. To close the detection loophole in a Bell test we must have an uncorrected heralding efficiency higher than the Eberhard limit (66.7 %) [3]. In Chapter 3 I discussed the construction of the high efficiency source of photon pairs and in the preceding sections I have discussed the near perfect TES detectors. Connecting the source to the TESs we measure an uncorrected efficiency of 74.20 ± 0.07 % which is more than sufficient to close the detection loophole.

Measurements of the overall efficiency of the source-TES system were made by recording the arrival time of each photon signal from each TES t_1, t_2. From this data we extract the rate of singles events s_1 and s_2. Coincidences (p) were identified by first computing the temporal cross correlation function $G^{(2)}(\Delta t = t_1 - t_2)$[1] of the photon signal times between the two TES detectors (see Figure 4.23), and then integrating the $G^{(2)}$ within a coincidence time window τ_c. The system efficiency η was then computed using Equation 4.3.

$$\eta = \frac{p}{\sqrt{s_1 \times s_2}}\,. \tag{4.3}$$

The peak of the $G^{(2)}$ function shown in 4.23 is centered at 0.85 μs due to the insertion of an electrical delay line used for one of the detectors. This circumvents the 0.2 μs dead time of our time stamp unit.

To estimate the performance of the TES detectors we can compare the measured 74.2 % system efficiency with the efficiency of the source correcting for the APD detectors (81.6 %) (see Section 3.4). We attribute the reduced efficiency seen with TESs to after pulsing and electronic noise in the signal from one of the two TES detectors. The dark count corrected arm efficiencies ($\eta_1 = p/s_2$ and $\eta_2 = p/s_1$) were 69.2 % and 81.2 % (the dark count rate was 513 /s and 231 /s). We estimate the detection efficiency of one of the TES detectors to be $\approx$ 99 % (after correcting for dark counts) which is in agreement with measurements done at NIST [4].

4.5.4 Timing jitter

We use the term timing jitter to define the variation in the time interval between the absorption of a photon and the generation of the corresponding output electrical pulse from the detector. This is a relevant measure to characterize the performance of our detection, that also has a strong impact on the feasibility of a loophole-free bell test: the timing jitter determines the minimum physical separation of the source from the detectors (see Section 2.3.1). Increasing the separation between the source and detectors is undesirable because of losses in the fibers.

[1] The $G^{(2)}(\Delta t)$, as explained in chapter 5 of [112], is a function that, given the arrival time of one photon on one detector (t_1) computes the likelihood of another photon arriving on the other detector (at t_2) after a time $\Delta t = t_1 - t_2$.

A large time jitter can also affect the measurement of the efficiency based on coincidence counts from an SPDC source [76]. In order to collect all the relevant coincidence events, the coincidence window needs to be much larger than the time jitter: the number of collected pairs follows a cumulative distribution function that depends on the statistical distribution of the jitter. The number of accidental and dark counts instead increases linearly with the width of the coincidence window.

We can clearly see how this works out with a practical example, consider the measurement in Figure 4.23; the width of a $G^{(2)}$ function of photon pairs produced in a SPDC process is determined by the detector jitter and not the source coherence time (which is several orders of magnitude smaller than the jitter). The combined timing jitter τ_j of the two TES detectors can be measured from the width of the $G^{(2)}$ peak shown in Figure 4.23. From the data we see that at FWHM, τ_j for two TESs is $\approx 200\,\text{ns}$.

To obtain the number of coincidence events we integrate the $G^{(2)}$ peak in a region given by τ_c; to ensure that this integration includes almost all pairs $\tau_c \gg \tau_j$. Using $\tau_c = 800\,\text{ns}$ we detect $\approx 99.99\,\%$ of the $G^{(2)}$ peak. However, using $\tau_c = 800\,\text{ns}$, $s_1 = 19477\,/\text{s}$ and $s_2 = 16646\,/\text{s}$ in Equation 3.2 tells that we have an accidental count rate $a = 259\,\text{pairs/s}$.

For the TES detector, the largest contribution to the time jitter comes from the limited bandwidth of the SQUID amplifier [116]. TESs made on the same wafer as our detectors have been demonstrated to have a timing jitter of 4 ns [116]. We have already procured new SQUID amplifiers (Magnicon XXF-1 C6) which are much faster than our current ones and will help us reduce the observed timing jitter of our TESs.

Chapter 5

Bit Commitment

Here I present the first experimental demonstration of a bit commitment protocol. This experiment was preformed using polarization entangled photon pairs produced by type-II downconversion in a BBO crystal [117]. The work presented in this chapter is part of the publication [2]. This experiment was performed using a different photon pair source than discussed in earlier chapters. The objective of this experiment is to demonstrate the feasibility of a bit commitment protocol. The theory was devised by Stephanie Wehner and Nelly Ng Huei Ying. I was responsible for the experimental implementation of the protocol and calculation of various experimental parameters.

5.1 Introduction

Traditionally, the main objective of cryptography has been to protect communication from the prying eyes of an eavesdropper. Yet, with the advent of modern communications new cryptographic challenges arose: we would like to enable two-parties, Alice and Bob, to solve joint problems even if they do not trust each other. Examples of such tasks include secure auctions or the ever present problem of secure identification such as that of a customer to an ATM machine. While protocols for general two-party cryptographic problems may be very involved, it is known that they can in principle be built from basic cryptographic building blocks known as oblivious transfer [118] and bit commitment [119].

The task of bit commitment is particularly simple and has received considerable attention in quantum information [120, 121, 122]. A bit commitment protocol consists of two phases. In the *commit phase*, Alice provides Bob with some form of evidence,

that she has chosen a particular bit $C \in \{0, 1\}$. Later on in the *open phase* Alice reveals C to Bob. A bit commitment protocol is secure if Bob cannot gain any information about C before the open phase and yet Alice cannot convince Bob to accept an opening of any bit $\hat{C} \neq C$. Lets consider a simple guessing game between Alice and Bob only. The objective is for Alice to guess the outcome of a fair coin toss. Alice and Bob are not trustworthy and will try to cheat. They can cheat in two ways - by altering the guess after the coin toss or by obtaining information about their rivals guess. To avoid the former, a fair game would need to be *binding*, while to avoid the latter the game would need to be *hiding*. For example, Alice writes down her guess on a slip of paper and places it in a safe. She then gives the safe to Bob. This scheme is perfectly binding because Alice no longer has access to her guess in order to alter it. However, it is not perfectly hiding since Bob could break into the safe. Alternatively, if Alice remembers her own guess and does not exchange any information before the toss the scheme will be perfectly hiding but not binding.

As long as we assume that Alice and Bob have infinite powers and capabilities (limited only by the known laws of physics), it has been shown that it is impossible (classically or quantum mechanically) to make a scheme that is both perfectly binding and perfectly hiding [1, 123, 124, 125, 126]. Even though a perfectly secure bit commitment scheme is not possible, we were able to implement a *practically* secure one. A perfectly hiding scheme would require an *un-hackable* safe. This is generally not possible. So a hiding scheme only encrypts enough of Alice's message such that Bob can verify its correctness later. However Alice can hack this encryption and change her message. Quantum mechanically one could ask why a Quantum Key Distribution (QKD) type scheme is not both perfectly hiding and perfectly binding. In QKD both parties share a key so, if Alice and Bob are not *honest*, then neither can trust that the shared key is random. Note that in (QKD), Alice and Bob *trust* each other and want to defend themselves against an outside eavesdropper Eve. In particular, this allows Alice and Bob to perform checks on what Eve may have done, ruling out many forms of attacks. This is in sharp contrast to two-party cryptography where there is no Eve and Alice and Bob *do not trust* each other. It is this lack of trust that makes the problem considerably harder.

Nevertheless, because two-party protocols form such a central part of modern cryptography, one is willing to make *assumptions* on how powerful an adversary can be

in order to implement them securely. Here, we consider *physical* assumptions that can enable us to solve such tasks. In particular, can the sole assumption of a limited storage device lead to security [127]? This is indeed the case and it was shown that security can be obtained if the attacker's *classical* storage is limited [127, 128]. Yet, apart from the fact that classical storage is cheap and plentiful, assuming a limited classical storage has one rather crucial caveat: If the honest players need to store N classical bits to execute the protocol in the first place, *any* classical protocol can be broken if the attacker can store more than roughly N^2 bits [129]. Motivated by this unsatisfactory gap, it was thus suggested to assume that the attacker's *quantum* storage was bounded [130, 131, 132, 133], or, more generally, noisy [134, 135, 136]. The central assumption of the so-called noisy-storage model is that during waiting times Δt introduced in the protocol, the attacker can only keep quantum information in his quantum storage device $\mathcal{F}$. By assuming a limit on the size of the attacker's quantum memory we showed that a secure bit commitment protocol is possible [2]. By assuming that the attacker has a noisy quantum storage we can further increase the security of our protocol. Otherwise, the attacker may be all-powerful. In particular, he can store an unlimited amount of classical information, and perform any computation instantaneously without errors. Note that the latter implies that the attacker could encode his quantum information into an arbitrarily complicated error correcting code to protect it from any noise in his storage device $\mathcal{F}$.

The assumption that storing a large amount of quantum information is difficult is indeed realistic today, as constructing large scale quantum memories that can store arbitrary information successfully in the first attempt has proved rather challenging [1]. [137] provides a review of quantum memory and [138, 139, 140] are several recent works indicative of current advancements. While noting that perpetual advances in building quantum memories fundamentally affect the feasibility of all protocols in the Noisy Storage Model, yet we explain below that given any upper bound on the size and reliability of a future quantum storage device, security is in fact possible - we need to send more qubits during the protocol.

Let us now explain more carefully what we mean by quantum storage device. We consider perfectly efficient quantum memories (where no qubits are lost), with

[1] We emphasize that this model is not in contrast with our ability to build quantum repeaters. For these, it is sufficient to store e.g. one entangled pair when making several attempts.

a bounded storage size and fidelity less or equal to unity.

Of particular interest, are storage devices consisting of S "memory cells", each of which may experience some noise $\mathcal{N}$ itself.

It is intuitive that security should be related to "how much" information the attacker can squeeze through his storage device. That is, one clearly expects a relation between security and the capacity of $\mathcal{F}$ to carry quantum information. Indeed, it was shown that security can be linked to the classical capacity [136], the entanglement cost [141], and finally the quantum capacity [142] of the adversary's storage device $\mathcal{F}$.

When evaluating security we start with a basic assumption, on the maximum size and the minimum amount of noise in an adversary's storage device. Such an assumption can for example be derived by a cautious estimate based on quantum memories that are available today [1]. Given such an estimate, we then determine the number of qubits that we need to transmit during the protocol to effectively overflow the adversary's memory device and achieve security.

5.2 Protocol and its security

A brief overview of the protocol aids in understanding it better. This paragraph, aided by Figure 5.1, provides an outline of the protocol. The first steps are similar to a regular QKD protocol: Alice has a source of polarization entangled photon pairs. Alice prepares a state and sends one photon of each pair to Bob. Alice and Bob, each, randomly choose a measurement basis form one of the standard BB84 [21] bases. This is repeated n times such that Alice has a string X^n of length n. Alice then shares her choice of measurement basis with Bob. Bob chooses all instances where both their measurement basis were the same. This allows Bob to create a substring $\widetilde{X}_I$ and a list of corresponding locations I. Since the communication is one way, Alice has no knowledge of $\widetilde{X}_I$ or I. The rest of the bit commitment protocol is similar to classical cryptography. Alice then encodes her information using a type of hashing function and the syndrome. Ideally the combination of the syndrome and hashing function would be unique to a given string without revealing the string. Such steps are common practice

[1] Note that we need a memory that can store arbitrary states on the first attempt. Such memories presently exist for a handful of qubits.

for privacy amplification [1]. Alice then shares this hash function and syndrome with Bob, thus committing her secret message to Bob. This constitutes the commit phase of the protocol. If Bob wanted to cheat he could store all n qubits that Alice sends and only perform measurements on them after Alice reveals her set of measurement bases. If there is a limit on either the size of Bob's memory or on the noise of the memory then one can show that this protocol can be secure. When Alice reveals the message to Bob by sending the complete string X^n (i.e. in the open phase) Bob will compute the syndrome and hash of the string to verify it. If both Alice and Bob are honest then the only problem is the communication losses (due to the noisy channel between them). If Bob is honest while Alice cheats then it will be detectable (provided errors $<$ threshold). The acceptable error rate is calculated based on experimental parameters and the number of rounds and an analysis can be found in supplementary material of [2]. For our experiment an error rate of 4.1 % was more than enough to ensure security. If Alice is honest and Bob cheats, the protocol will work only if Alice chooses an appropriate error correcting code (Hash function and syndrome). Here Alice must make this choice based on the length of her message and her assumptions about Bob's limited or noisy quantum storage. If both of them are dishonest then the protocol does not work. The protocol is designed to protect the honest party. A rigorous description of the protocol is given below.

We consider the bit commitment protocol from [136] with several modifications to make it suitable for an experimental implementation with time-correlated photon pairs. In the supplementary material of [2], we provide a general analysis that can be used for any experimental setup.

To understand the security constraints, we first need to establish some basic terminology. In our experiment, both Alice and Bob have four detectors, each one corresponding to one of the four BB84 states [143] (see Section 5.3 and Figure 5.3). If Alice or Bob observes a click of exactly one of their detectors [2] , we refer to it as a *valid click*. Cases where more than one detector clicks at the same instant on the same side are ignored. A *round* is defined by a valid click of *Alice's* detectors. A *valid round*

[1] Privacy amplification is a way of turning a long string x about which an adversary (Eve) knows some information into a shorter string z about which Eve knows very little. This is usually written as $z = \mathrm{Ext}(x)$.

[2] By detector we mean the real detector combined with a symmetrization procedure as outlined in Section 5.5.

is where both parties, Alice and Bob, registered a valid click in a corresponding time window, i.e., where a photon pair has been identified.

First, to deal with losses in the channel we introduce a new step in which Bob reports a loss if he did not observe a valid click. Second, to deal with bit flip errors on the channel, we employ a different class of error-correcting codes, namely a random code[1][144]. Usage of random codes is sufficient for this protocol since decoding is not required for honest parties. The main challenge is then to link the properties of random codes to the protocol security.

Before we can discuss the correctness and security of the proposed protocol, let us introduce four crucial figures of interest that need to be determined in any experimental setup. The first two are the probabilities p^0_{sent} and p^1_{sent}, that none or just a single photon was sent to Bob respectively, conditioned on the event that Alice observed a round. The third is the probability $p^h_{\text{B,noclick}}$ that honest Bob registers a round as missing, i.e. Bob does not observe a valid click when Alice does. Again, this probability is conditioned on the event that Alice observed a round [2]. Finally, we will need the probability p_{err} of a bit flip error, i.e. the probability that Bob outputs the wrong bit even though he measured in the correct basis.

Since Alice and Bob do not trust each other, they cannot rely on each other to perform the said estimation process. Note, however, that the scenario of interest in two-party cryptography is that the honest parties essentially purchase off the shelf devices with standard properties, for which either of them could perform the said estimate. It is only the dishonest parties who may be using alternate equipment.

Let us now sketch why the proposed protocol remains correct and secure even in the presence of experimental errors. A detailed analysis is provided in the supplementary material of [2] (see Section D.3 of [2] on how it is applied to our experimental parameters). In our analysis, we take the storage device $\mathcal{F}$, as well as a fixed overall security error ϵ as given. Let M be the number of rounds *Alice* registers during the execution of the protocol. Let n be the number of valid rounds. In the supplementary

[1] A random code is one where each entry in the encoding matrix is either 0 or 1, chosen randomly.

[2] Note that by no-signalling, Alice's choice of better (or worse) detectors should not influence the probability of Bob observing a round.

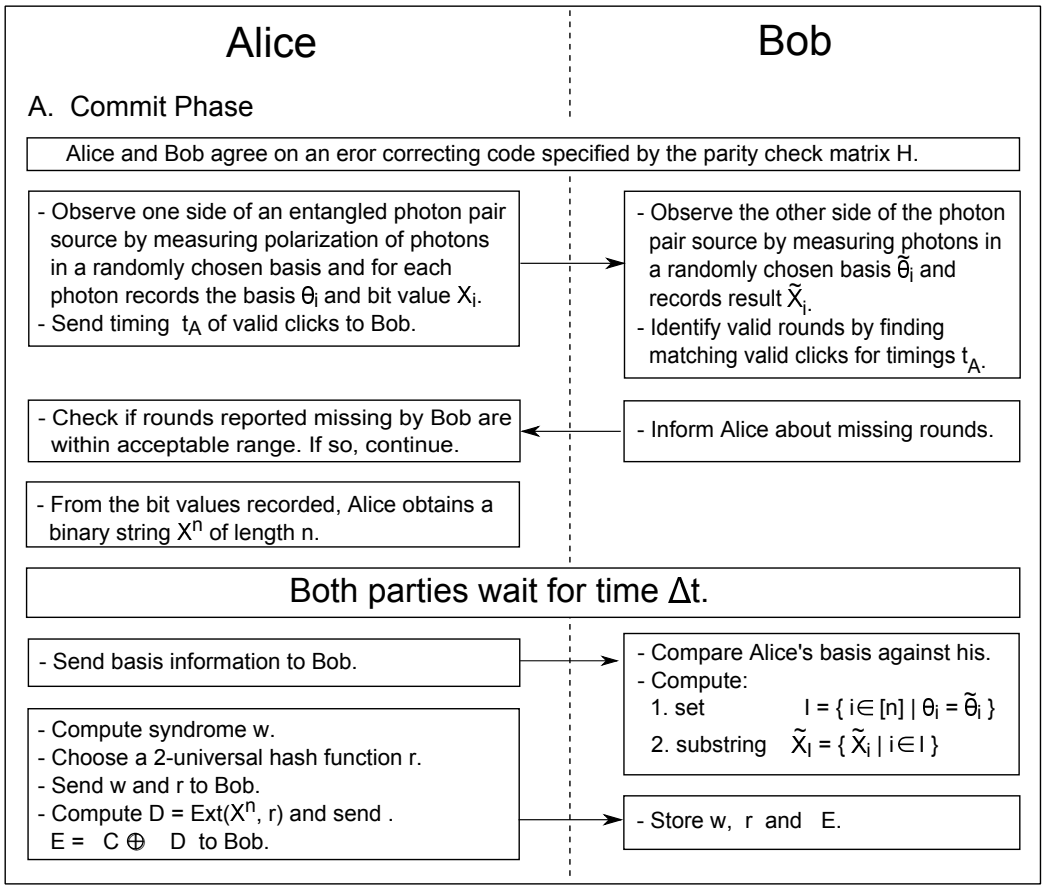


Figure 5.1: Flowchart of the bit commitment protocol *commit phase*, that allows Alice to commit a single bit $C \in \{0,1\}$. Alice holds the source that creates the entangled photon pairs. The function Syn maps the binary string X^n to its syndrome as specified by the error correcting code H. The function Ext : $\{0,1\}^n \otimes \mathcal{R} \to \{0,1\}$ is a hash function indexed by r, performing privacy amplification. We refer to the supplementary material of [2] for a more detailed statement of the protocol including details on the acceptable range of losses and errors. Note that the protocol itself does not require any quantum storage to implement.

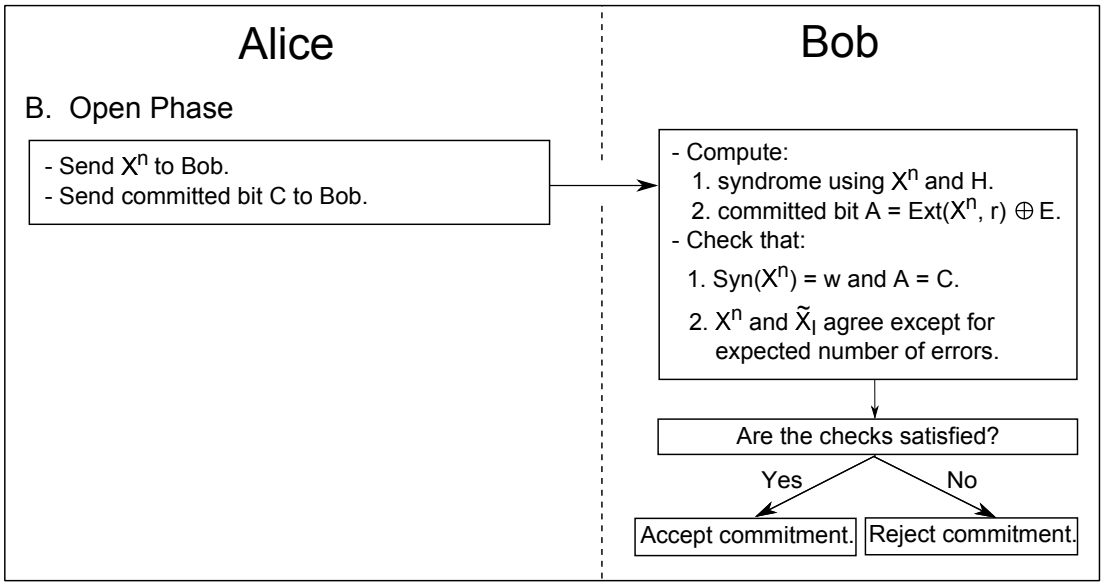


Figure 5.2: Flowchart of the bit commitment protocol *open phase*, that allows Alice to commit a single bit $C \in \{0, 1\}$. Alice and Bob may choose to perform the open phase of the protocol at any time they find mutually suitable. In the open phase Bob can verify the committed bit based on the information exchanged during the commit phase.

material of [2], it is shown that M and n are directly related to each other, given some fixed experimental parameters. In particular, n is a function of M and $p^h_{\mathrm{B,noclick}}$

$$n \approx (1 - p^h_{\mathrm{B,noclick}})M \ . \tag{5.1}$$

We can now ask, how large does M (or equivalently n) need to be in order to achieve security. If n is very small, for example if $n \approx 100$, it is relatively easy to break the protocol since a cheating party might be able to store enough qubits. Also many terms from our finite n analysis reach convergence only for sufficiently large n. As these terms depend on experimental parameters, security can be achieved for a larger range of experimental parameters if n is large. By fixing the assumption on quantum storage size, experiment parameters and security error values, our analysis allows us to determine a value of n where security is achievable.

Correctness: First of all, we must show that if Alice and Bob are both honest, then Bob will accept Alice's honest opening of the bit C. Note that the only way that honest Bob will reject Alice's opening is when too many errors occur on the channel.

A standard Chernoff style bound[1] shows that the deviation from the expected number of $p_{\text{err}}n$ errors is not too large.

Security against Alice: Second, we must show that if Bob is honest, then Alice cannot get him to accept an opening of a bit $\hat{C} \neq C$. In our protocol, Alice is allowed to be all powerful, and is not restricted by any storage assumptions. If she is dishonest, we furthermore assume that she can even have perfect devices and can eliminate all errors and losses on the channel. The analysis of the steps before the syndrome is sent is thereby identical to [145] (see Figure 5.1). The outcome of this step is that even though Bob reports some bits as missing, Alice can nevertheless not gain any information about which bits of X are known to honest Bob. This relies crucially on the fact that Bob's losses are independent of his choice of measurement basis. The loss imbalance of a real detection scheme can be dealt with by symmetrizing losses as outlined in Section 5.5. The properties of the error-correcting code then ensures that if the syndrome of the string matches and Alice passes the first test, then she must flip many bits in the string to change her committed bit. However, since Alice does not know which bits are known to Bob she will get caught with a high probability. The only difference to the analysis of [136] is that Bob must accept some incorrect bits since there are indeed some bit flip errors on the channel. We hence use a different error-correcting code from [136].

Note that if Alice is dishonest, n is nevertheless well defined as the number of rounds that she declares as valid.

Security against Bob: Finally, we must show that if Alice is honest, then Bob cannot learn any information about her bit C before the open phase. Again, dishonest Bob may have perfect devices and eliminate all errors and losses on the channel. His only restriction is that during the waiting time Δt he can only store quantum information in the device $\mathcal{F}$. Intuitively, the fact that Bob cannot learn about the committed bit C comes from the fact that his knowledge about X^n as shown in Figure 5.1 is limited. Privacy amplification with the function Ext removes any knowledge Bob has about bit C. Our analysis is thereby very similar to [136], requiring only a very careful balance between the distance of the error-correcting code above, and the syndrome

[1]The Chernoff bound gives exponentially decreasing bounds on tail distributions of sums of independent random variables.

length. In addition, we employ a novel uncertainty relation which unlike the one used in [136] allows us to obtain security at reasonable block lengths.

We provide a detailed analysis in the supplementary material of [2], where a general statement for arbitrary storage devices is included. For the case of bounded storage, Lemma D.2 in [2] provides a formula telling us how large M needs to be in order to achieve security against both Alice and Bob, when an error parameter ϵ is fixed. The total execution error of the protocol is obtained by adding up all sources of errors throughout the protocol analysis.

The syndrome w (based on the parity check matrix H) would give Bob some information about X^n. However we have shown in the supplementary material of [2] that this is insufficient for Bob to reconstruct the committed bit C.

The case where Alice and Bob are both dishonest is not of interest, because the aim of this protocol is to perform correctly while both players are honest, and protect the honest players from dishonest players.

5.3 Experiment

We implement this protocol with a series of entangled photons, with the polarization degree of freedom forming our qubits. This allows for reliable measurements in two complementary bases. Basis 1 corresponds to horizontal/vertical (HV) polarization, and basis 2 to $\pm 45°$ (+-) linear polarization. The polarization-entangled photon pairs are prepared via spontaneous parametric down conversion (SPDC), collected into single mode optical fibers, and guided to polarization analyzer (PA) located with Alice and Bob (see Figure 5.3). Each PA consists of a non-polarizing beam splitter (BS) providing a random basis choice, followed by two polarizing beam splitters (PBS) and a pair of Silicon Avalanche Photo Diodes (APD) as single photon detectors in each of the BS outputs. A half wave plate before one of the PBS rotates the polarization by 45° degrees. This detection setup was used in a number of QKD demonstrations [117, 146, 147].

The SPDC source is similar to [117], with a continuous wave free running laser diode (398 nm, 10 mW) pumping a 2 mm thick beta Barium Borate crystal cut for type-II non-collinear parametric down conversion and the usual walk-off compensation to obtain

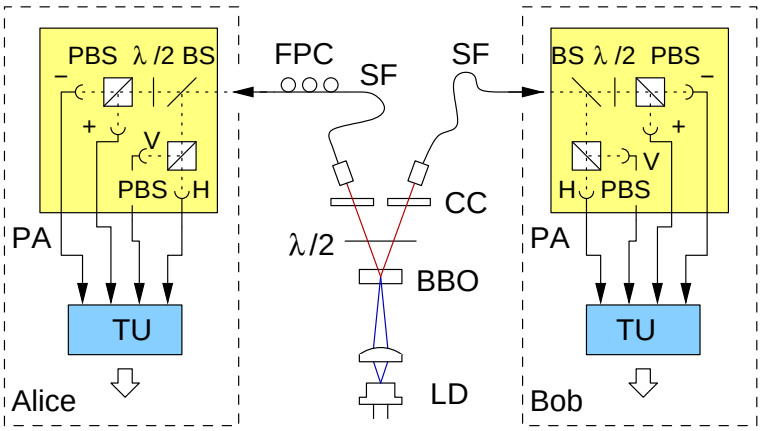


Figure 5.3: Experimental setup. Polarization-entangled photon pairs are generated via non-collinear type-II spontaneous parametric down conversion of blue light from a laser diode (LD) in a beta Barium Borate crystal (BBO), and distributed to polarization analyzers (PA) at Alice and Bob via single mode optical fibers (SF). The PA are based on a nonpolarizing beam splitter (BS) for a random measurement base choice, a half wave plate ($\lambda/2$) at one of the of the outputs, and polarizing beam splitters (PBS) in front of single-photon counting silicon avalanche photo-diodes. Detection events on both sides are timestamped (TU) and recorded for further processing. A polarization controller (FPC) ensures that polarization anti-correlations are observed in all measurement bases.

polarization-entangled photon pairs [148]. We collect photon pairs into single mode optical fibers such that we observe an average pair rate $r_p = 2997 \pm 82\,\mathrm{s}^{-1}$.

Such a source generates photon pairs in a stochastic manner, but with a strong correlation in time. Therefore, valid clicks are time stamped on both sides first. In a classical communication step, detection times t_A, t_B are compared, and valid rounds are identified if valid clicks fall into a coincidence time window of $\tau_c = 3\,\mathrm{ns}$, i.e., $|t_A - t_B| \leq \tau_c/2$, similar to [147] with the code in [149]. The visibility of the polarization correlations in the Singlet state are $97.7 \pm 0.6\%$ and $94.7 \pm 0.9\%$ in the HV and 45° linear basis. Individual detection rates for Alice's and Bob's sides are $r_A = 23758 \pm 221\,\mathrm{s}^{-1}$ and $r_B = 22227 \pm 247\,\mathrm{s}^{-1}$ respectively. In an initial alignment step, the fiber polarization controller was adjusted such that we see polarization correlations corresponding to a singlet state with a quantum bit error ratio (QBER) of about $p_{\mathrm{err}} = 4.1\%$. The QBER is not to be confused with the failure probability of bit commitment protocol.

Calculations of the latter are explicitly stated in Section 5.4. As reported in our results section, this quantity is much smaller than the former.

For carrying out a successful bit commitment, we need to determine the parameters p^1_{sent}, p^0_{sent}, and $p^h_{\text{B,noclick}}$. Depending on these probabilities and the desired error parameter ϵ, we choose a particular error correcting code and number of rounds M needed for a successful bit commitment. To estimate these probabilities out of the experimental parameters of our source/detector combination, we model our setup by a lossless SPDC source emitting only photon pairs at a rate r_s, and assign all imperfections (losses, limited detection efficiency, and background events) to the detectors at Alice and Bob. Since the coherence time of the photons in our case is much shorter than the coincidence detection time window τ_c, the distribution of photon pairs in time can be well described by a Poisson process, which allows an assessment of multiphoton events. A detailed derivation of bounds for the probabilities is given in Section 5.4, we just summarize the results necessary for evaluating the security of the protocol:

$$
\begin{aligned}
p^0_{\text{sent}} &\leq (r_A - r_p)/r_A = 0.875 \pm 0.009\,, && (5.2)\\
p^{n>1}_{\text{sent}} &< \frac{r_A r_B}{r_p}\tau_c = 5.32 \pm 0.17 \times 10^{-4}\,, && (5.3)\\
p^1_{\text{sent}} &= 1 - p^0_{\text{sent}} - p^{n>1}_{\text{sent}} > 0.125 \pm 0.009\,, && (5.4)\\
p^0_{\text{sent}} + p^1_{\text{sent}} &= 1 - p^{n>1}_{\text{sent}} > 0.99947 \pm 0.000017\,, && (5.5)\\
p^h_{\text{B,noclick}} &= 1 - r_p/r_A = 0.875 \pm 0.009\,. && (5.6)
\end{aligned}
$$

Due to small differences in the detection efficiency of the APD and imperfections in polarization components in the actual experiment, there is an asymmetry in the probability of detecting each bit in each basis. Furthermore, the beam splitter for the random measurement basis choice are not completely balanced. A summary of these imperfections over a number of bit commitment runs is shown in Figure 5.4. This can be corrected for by discarding rounds until the probabilities for both bits are equal. Discarded bits can be modeled as losses without affecting the security of the protocol. A detailed analysis of this can be found in Section 5.4.

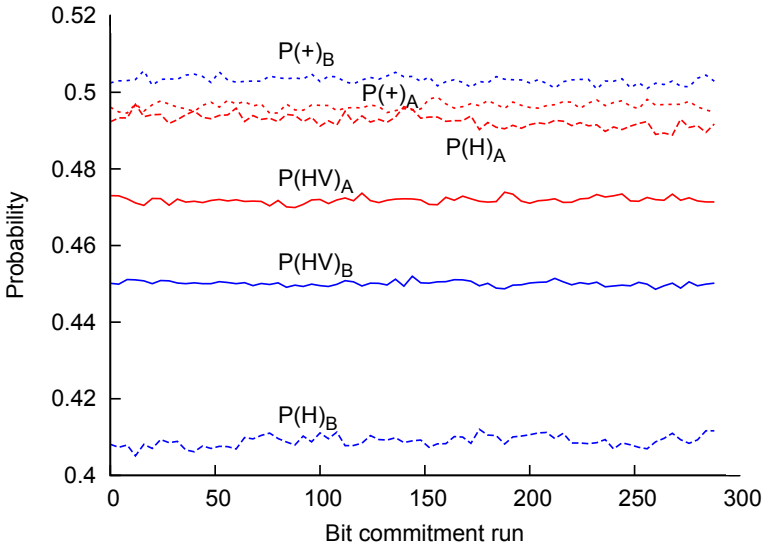


Figure 5.4: Bias in measurements. Solid lines indicate the probabilities $P(HV)$ of a HV basis choice for both Alice and Bob for data sets of 250000 events each. Dashed lines indicate the probability $P(H)$ of a H in the HV measurement basis, the dotted lines the probability $P(+)$ of a $+45°$ detection in a $\pm 45°$ measurement basis. Red is used to represent the probabilities for Alice while blue represents those of Bob. These asymmetries arise form optical component imperfections and are corrected in a symmetrization step.

5.4 Experimental parameters

To analyze our bit commitment protocol in any practical experiment, several probabilities have to be determined. The Table 5.4 summarizes all the probabilities we will need to estimate. We emphasize that all such probabilities are conditioned on the event that Alice registers a round, i.e. sees a valid click.

A difficulty in estimating the probabilities of success in a "round" arises from the fact that generation of photon pairs in a parametric down conversion source is a stochastic process. Furthermore, losses in the system may occur in the source or in detectors, and we do not have an easy way of assessing the losses reliably. We thus try to estimate bounds of the required probabilities for the bit commitment protocol out of observable quantities both Alice and Bob can agree upon. For this purpose, we model losses and background events in our system in a way shown in Figure 5.5.

Probabilities	Description
p^1_{sent}	Probability that a single photon was sent to Bob.
$p^h_{\text{B,noclick}}$	Probability that honest Bob observes no click.
$p^d_{\text{B,noclick}}$	Probability that dishonest Bob observes no click. Note: this value is equal to p^0_{sent}, i.e., the probability that no photons were sent to Bob.
p_{err}	Probability that the measurement outcome for honest Alice and honest Bob is different, when the same basis is used for both parties.

Table 5.1: Parameters required for security proof of bit commitment. All the above quantities are conditioned on the event that Alice registered a valid click.

The rates (i.e., events per unit of time) observed at Alice are then given by

$$r_A = \eta_A(r_s + r_{bA})\,, \tag{5.7}$$

where η_A indicates the detection efficiency and r_{bA} a background event rate; a similar expression holds for Bob. The observed coincidence rate in this model is given by

$$r_p = \eta_A\eta_B r_s + r_{\text{acc}}\,, \tag{5.8}$$

where r_{acc} reflects the so-called accidental coincidence rate, caused by detection events on both sides happening within the coincidence time window τ_c that are not due to valid clicks from the same photon pair. This rate can be bounded from observed rates r_A and r_B to

$$r_{\text{acc}} < r^{\max}_{\text{acc}} = r_A r_B \tau_c\,, \tag{5.9}$$

assuming that all detection events on both sides are caused by uncorrelated events. In our experiment, this quantity would result in a value of $r^{\max}_{\text{acc}} = 14.9 \pm 0.18\,\text{s}^{-1}$, and is negligible compared to the observed coincidence rate r_s. This quantity was independently assessed by recording the rate of detection time pairings t_A, t_B in a time window that was displaced by $\tau_d = 20\,\text{ns}$ from the "true" coincidences, i.e., $|t_A - t_B - \tau_d| \leq \tau_c$ [147]. We found a rate of $r_{\text{acc}} = 5.3 \pm 3.3\,\text{s}^{-1}$ over the course of several bit commitment runs. Since $r_{\text{acc}} \ll r_p$, we, from now on, neglect these events in the rate estimations, and interpret their occurrence just as events that increase the error ratio.

To evaluate the probability p^1_{sent} that exactly one photon was sent to Bob in the interval τ_c around a time when Alice has seen an event, we first consider the probability

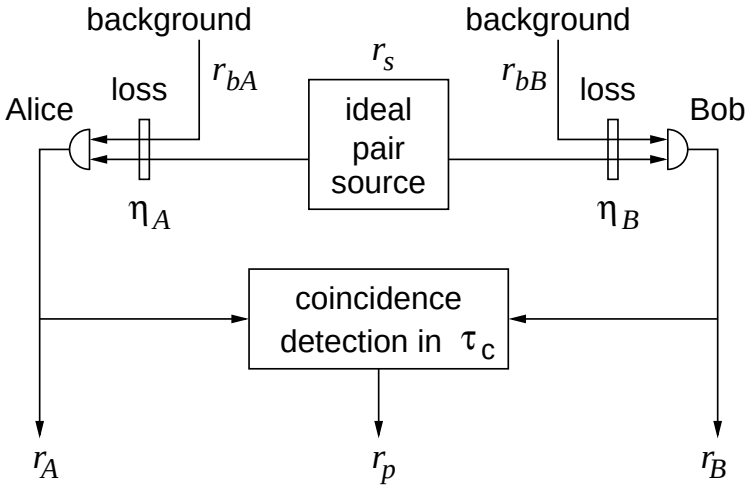


Figure 5.5: Model of the experimental setup with an imperfect pair source and detectors. An ideal source generates time-correlated photon pairs with a rate r_s and sends them to detectors at Alice and Bob; losses are modeled with attenuators with a transmission η_A and η_B, respectively. To account for dark counts in detectors, fluorescence background and external disturbances, we introduce background rates r_{bA}, r_{bB} on both sides. Valid rounds are identified by a coincidence detection mechanism that recognizes photons corresponding to a given entangled pair. Event rates r_A and r_B reflect measurable detection rates at Alice and Bob, while r_p indicates the rate of identified coincidences.

p^0_{sent} that no photon was sent to Bob, given Alice has seen an event. This can only be caused by a background event with Alice. Thus, p^0_{sent} equals the probability that a detection event on Alice's side is caused by background, which is given by

$$\begin{aligned} p^0_{\text{sent}} &= \frac{r_{bA}}{r_{bA}+r_s} = 1 - \frac{r_s}{r_{bA}+r_s} \\ &= 1 - \frac{\eta_A r_s}{\eta_A(r_{bA}+r_s)} = 1 - \frac{\eta_A r_s}{r_A} \\ &= 1 - \frac{r_p}{\eta_B r_A}\,. \end{aligned} \tag{5.10}$$

Since the efficiency η_B is not known exactly, we set it to 1 and thereby obtain an upper bound for p^0_{sent}:

$$p^0_{\text{sent}} < 1 - \frac{r_p}{r_A} = 0.875 \pm 0.009\,. \tag{5.11}$$

Next, we consider the probability $p^{n>1}_{\text{sent}}$ that more than one photon has been sent to Bob, given that Alice has seen an event. This probability is the product of the

probability that Alice's event was caused by a photon pair, and the probability that at least one other photon pair than the one causing the event on Alice's side was generated in the coincidence time window τ_c. From equation 5.10, the first probability is given by $r_p/(\eta_B r_A)$. For the latter, we consider the statistics of photon pairs emerging from a continuously pumped SPDC source. While light emerging from a downconversion process is known to follow thermal photon counting statistics, the coherence time of the photons in our case (0.73 ps for an optical bandwidth of 3 nm) is much shorter than τ_c. In this case, the statistics of several photon pairs in the time window τ_c follows a Poisson distribution. Since the creation of an additional photon pair is then independent of the first photon pair, and the probability that no photon pair is created in τ_c is given by $e^{-r_s\tau_c}$, the probability of creating at least one more photon pair is given by $1 - e^{-r_s\tau_c}$. This brings us to

$$\begin{aligned} p_{\text{sent}}^{n>1} &= \frac{r_p}{\eta_B r_A}(1 - e^{-r_s\tau_c}) \\ &< \frac{r_p}{\eta_B r_A} r_s\tau_c = \frac{r_p}{\eta_B r_A}\frac{r_p}{\eta_A\eta_B}\tau_c \\ &= \frac{r_p^2}{r_A\eta_A\eta_B^2}\,. \end{aligned} \tag{5.12}$$

The efficiencies η_A, η_B are not accessible directly from the experiment, but can be bounded by $\eta_A > r_p/r_B$ and $\eta_B > r_p/r_A$ via 5.7. With this, we can further bound expression 5.12 and arrive at

$$p_{\text{sent}}^{n>1} < \frac{r_A r_B}{r_p}\tau_c = 5.32 \pm 0.17 \times 10^{-4}\,, \tag{5.13}$$

which is much smaller than the uncertainty on p_{sent}^0. With this, we arrive at

$$p_{\text{sent}}^1 = 1 - p_{\text{sent}}^0 - p_{\text{sent}}^{n>1} > 0.125 \pm 0.009 \tag{5.14}$$

and

$$p_{\text{sent}}^1 + p_{\text{sent}}^0 = 1 - p_{\text{sent}}^{n>1} > 0.99947 \pm 0.000017\,. \tag{5.15}$$

Finally, the probability that an honest Bob does not see an event (within the coincidence time window) given that Alice has detected something is the complement to the probability that Bob sees something given that Alice has seen something. The latter, by definition, is given by the ratio r_p/r_A. Thus, we have

$$p_{\text{B,noclick}}^h = 1 - r_p/r_A = 0.875 \pm 0.009\,. \tag{5.16}$$

5.5 Symmetrizing losses

In practice, not all detectors have the same efficiency. Losses will be higher for some detectors than for others. This will lead to imbalances in the choice of basis and the choice of BB84 encoded qubit. In our protocol, such imbalances affect the security in two places. First, if Alice is honest but Bob is trying to cheat, such imbalances give him additional information about which bit or basis was used. His advantage is similar to the advantage that an eavesdropper in QKD would gain from knowing such extra information. Second, if Bob is honest but Alice is trying to cheat, having higher losses in one basis does reveal information to Alice i.e. the basis in which Bob measured. Because if Bob does not report a loss it is more likely that he used the basis for which losses occur less often.

We describe a method to deal with such imbalances securely - the same method can be used to address imbalances on Alice's and Bob's side. For simplicity, we outline the procedure in detail for Alice; exactly the same method can be used to symmetrize Bob's detectors. The essential idea is to make all detectors equally inefficient, by throwing away (i.e., declaring as lost) rounds where detectors with higher efficiencies registered a click. Note that in our protocol, Alice can discard additional rounds without consequences for security parameters. Meanwhile, discarding additional rounds on Bob's side increases $p^h_{\mathrm{B,noclick}}$. Detection events combining with such post-processing procedures, define the occurrence of a valid round. In other words, if a single click occurred on both sides and was not manually discarded for symmetrizing purposes, this event is considered a valid round.

In our setup, Alice has four detectors, one for each bit in each basis. Let x, θ label the detector corresponding to a bit $x \in \{0, 1\}$ in basis $\theta \in \{0, 1\}$. Let p_θ denote the probability that basis θ is chosen, and let $p_{x|\theta}$ denote the probability that bit x occurs given basis θ. Finally, let $t_{x,\theta}$ denote the probability that Alice keeps bit x in basis θ when the detector x, θ clicks. That is, Alice discards bit x in basis θ with probability $1-t_{x,\theta}$ even though a click occurred. Our goal will be to determine the $t_{x,\theta}$ that renders $\Pr[x, \theta|\mathrm{keep}]$, the probability that x, θ occurs conditioned on the event that Alice keeps a particular detection event the same for all x and θ.

First of all, note that the probability that a particular detection event is *not* discarded, i.e. Alice accepts it as a round, can be written as

$$\Pr[\text{keep}] = \sum_{x,\theta\in\{0,1\}} p_\theta p_{x|\theta} t_{x,\theta}\,. \tag{5.17}$$

By Bayes' rule

$$\Pr[x,\theta|\text{keep}] = \frac{\Pr[\text{keep}|x,\theta]\Pr[x,\theta]}{\Pr[\text{keep}]} \tag{5.18}$$

$$= \frac{t_{x,\theta} p_{x|\theta} p_\theta}{\Pr[\text{keep}]}\,. \tag{5.19}$$

Ideally, all probabilities are the same, i.e., for all x and θ

$$\Pr[x,\theta|\text{keep}] = \frac{1}{4}\,. \tag{5.20}$$

This yields 4 equations, in 3 free parameters since $\sum_{x,\theta}\Pr[x,\theta|\text{keep}] = 1$. These can easily be solved for $t_{x,\theta}$.

For our setup, the parameters for symmetrization on Alice' side are as follows[1] :

$$\begin{aligned} t_{0,0} &= 1 \\ t_{0,1} &= 0.963077 \\ t_{1,0} &= 0.882305 \\ t_{1,1} &= 0.871353\,. \end{aligned} \tag{5.21}$$

Symmetrization on Bob's side is dealt with in the same manner. This, however, increases the value of $p^h_{\text{B,noclick}}$, since now an honest Bob deliberately throws away more clicks. This leads to a new value of

$$\tilde{p}^h_{\text{B,noclick}} = 1 - (1 - p^h_{\text{B,noclick}}) \cdot \Pr[\text{keep}]\,. \tag{5.22}$$

For our setup, the parameters for symmetrization on Bob's side are:

$$\begin{aligned} t_{0,0} &= 0.679745 \\ t_{0,1} &= 1 \\ t_{1,0} &= 0.665591 \\ t_{1,1} &= 0.662890\,. \end{aligned} \tag{5.23}$$

[1] To calculate these values for symmetrization, we chose a sufficiently large set of data in order to obtain the parameters to the accuracy shown. A different experimental run would result in different values for $t_{x,\theta}$.

The probability of Bob keeping a click during symmetrization is $\Pr[\text{keep}] = 0.729646$. This combining with the initial estimate of $p^h_{\text{B,noclick}}$ gives $\tilde{p}^h_{\text{B,noclick}} = 0.909$, implying a high amount of losses. Even so, the protocol remains secure due to the fact that the source provides multiphotons to Bob with an extremely small probability, whenever Alice observes only a single detection event. In other words, $p^1_{\text{sent}} + p^d_{\text{B,noclick}}$ is extremely high, as stated in Equation 5.15. In such cases, even a high amount of losses do not compromise security of the protocol.

Also, it should be stressed that p_{err} should be evaluated for the set of data after all symmetrization procedures, since there can be bias in the error rates for each bit and basis. For the set of symmetrized data, $p_{\text{err}} = 0.0412$, in comparison with before symmetrization, $p_{\text{err}} = 0.0428$. In general p_{err} may increase or decrease after symmetrizing the data depending on whether the the errors occurred between the more efficient detectors or not.

5.6 Results and Conclusion

We have implemented a quantum protocol for bit commitment that is secure in the noisy-storage model. For this, $n = 250\,000$ valid rounds were used at a bit error rate of $p_{\text{err}} = 4.1\%$ (after symmetrization) to commit one bit with an error of less than $\epsilon = 2 \times 10^{-5}$ (see Section D.3 of [2]). This protocol is secure under the assumption that Bob's storage size is no larger than 972 qubits, where each qubit undergoes a low depolarizing noise with a noise parameter $r = 0.9$. We stress that our analysis is done for finite n, and all finite size effects and errors are accounted for [1]. Our experimental implementation demonstrates for the first time that two-party protocols proposed in the bounded and noisy-storage models are well within today's capabilities. Like so many experiments in quantum information, our experiment is extremely similar to QKD. We however, emphasize that the experimental parameter requirements and analysis are entirely different to QKD. In the supplementary material of [2], we provided a detailed analysis of our modified bit commitment protocol including a range of parameters for which security can be shown. Our analysis could be used to implement the same protocol using a different, technologically simpler setup, with potentially lower error

[1] The ϵ includes the error in the choice of random code, finite size effects that need to be bounded, smoothing parameters from an uncertainty relation, etc.

rates or losses. Our analysis can also address the case of committing several bits at once. Implementing other protocols in the noisy storage model will be of interest for future work.

The protocol we have demonstrated can be used in realistic scenarios. The combination of this bit commitment protocol and existing quantum communication protocols can be used to implement oblivious transfer. Most two party protocols can be implemented using combinations of bit commitment oblivious transfer and secure communication. In and of itself bit commitment can be used to implement a secure and fair coin toss which is already of use to the gambling industry.

Finally, note that our analysis rests on a fundamental assumption made in the analysis of *all* cryptographic protocols, namely that Alice does not have access to Bob's lab and vice versa. In particular, this means that Alice cannot tamper with the random choices made by Bob, potentially forcing him to measure e.g. only in one basis, or by manipulating apparent detector losses [150, 151].

Chapter 6

Conclusion and outlook

In this thesis I have presented an efficient[1] source of polarization entangled photon pairs and how to detect these photon pairs with minimal loss. One application of our experiment is a loophole free Bell test, which, as mentioned in a recent editorial by Wiseman [152], is considered to be a "worthy challenge" in physics.

The source has a corrected heralding efficiency of $86\pm3.5\dot{\%}$ [2] (Section 3.4). In Section 4.5.3 we used Transition Edge Sensors (made by the group of Sae Woo Nam in NIST with a detection efficiency >98 % [4]), connected to our source via 40 m of optical fiber, to measure an uncorrected heralding efficiency of 74.2 %.

It is possible to violate a detection loophole free Bell's inequality using a particular set of non-maximally entangled states provided that the heralding efficiency exceeds 66.7 % [3]. We have demonstrated (Section 3.2) that our source of entangled photon pairs is capable of producing such states with a fidelity of 99.3 % in addition to maximally entangled states with a polarization correlation visibility of $99.4 \pm 0.1\%$.

The significance of a loophole free Bell test has motivated many research groups to actively pursue projects similar to ours. Table 6.1 shows a comparison between our work and other similar efforts.

In order to close the locality loophole in a Bell test, we need to implement the choice of measurement basis during the "time of flight" of the photon from the source to the detector. To do so we built a fast polarization modulator with a 3 μs switching time and a 99.1 ± 0.6 % transmission (Appendix A).

[1] Efficiency refers to the pairs to singles ratio also known as the heralding efficiency.
[2] After correcting for detector losses and background counts.

	Efficiency corrected for APD losses	Efficiency with TESs	Visibility	Mode coupling efficiency	TES jitter
Gaithersburg, USA [91]	84.4±0.5 % and 83.7±0.5%	N/A	Not Entangled	91.6±0.6 %	N/A
Urbana. USA [65]		75±2 % corrected for 7 % loss	99.70±0.05 % in HV 99.50±0.05 % in ±45 °	90 %	
Vienna, Austria [55, 153]	83.0±0.2± %	76.1 % [55] and 79.7±0.2 % [153]	97.5 %		155 ns
This thesis	86.0±3.5 %	75.20±0.07 % (81.4 % and 69.6 %)	≈100 % in HV 99.4±0.1 % in ±45 °	91±5 %	200 ns

Table 6.1: Table comparing the various high efficiency sources of photon pairs. We can see that our source is very similar to the others. Our efficiency after correcting for the detection efficiency of the APDs is the highest. We also observed a very high arm efficiency of 81.4 % when measuring with the TESs. We are also capable of producing non-maximally entangeld states with a high fidelity.

During the course of my work I had the opportunity to work with computer scientists Prof. S. Wehner and Nelly Ng. Together we were able to implement a quantum communication and cryptography protocol useful for secure identification called bit commitment. Such collaborations between experiments and theory are essential for real world applications. It was thought that secure bit commitment was impossible [1]. We assumed limits on an attacker's quantum memory (i.e. the noisy storage model) and were able to experimentally implement a bit commitment protocol [2]. This demonstrated the feasibility of the protocol and led to other experiments. It was later

demonstrated that absolutely secure bit commitment is possible if we include relativistic effects [154].

6.1 Future outlook

The TES detectors, fast polarization modulator, and high efficiency source of polarization entangled photon pairs, put together, form a system which is ideal for several applications. The most important of which, we feel, is a loophole free Bell test. Thus the natural continuation of this experiment is to work towards performing one. To that end we are working on reducing the noise seen by the TES detectors and improving their timing jitter, making a faster polarization modulator, reducing fiber splicing losses, and physically separating the source, detectors and modulators.

Closing all loopholes in a Bell test is central to implementing several device independent protocols like the generation of certified randomness. We are currently working towards implementing one such protocol [155].

Appendix A

Fast polarization modulator

Usually in quantum communication experiments, Alice and Bob need to choose measurement bases and randomly switch between them. Mechanical switching (by say, rotating a motorized wave plate) takes a long time (on the order of about a millisecond) and consequently limits communication speeds. Switching measurement bases faster than $3\,\mu$s is possible using the electro-optic effect. In order to close the locality loophole in a Bell test, the speed of the switch imposes a limit on the distance needed between the detectors of Alice and Bob. A fast switch reduces this distance and consequently the transmission losses in the optical fibers. My supervisor Christian Kurtsiefer designed and built the high voltage and fast electronic driver for the polarization modulator presented here.

A.1 Introduction

To switch the polarization of an input state within a few microseconds we cannot use a mechanical switch. Instead, we utilize the linear electro-optic effect — called the Pockels effect [156, 157, 158]. In addition to being fast, the polarization switch must have a very low loss because any loss the modulator has will reduce the overall heralding efficiency of the source. Further, the spatial/optical distortion, of the input mode, due to the switch must be small otherwise this may affect the coupling of the output mode back into the optical fibers. Modulators based on waveguides can be extremely fast. For example, Melikyan et al., [159] built an electro-optic modulator with a switching time of about 16 ps. However, the drawback with such waveguide technologies are their losses. The coupling into and out of these waveguides is nowhere near ideal (typically

transmission is <90 % [160, 161]). To avoid these losses we utilized bulk crystals. The absorption losses inside several crystal materials are negligible and the AR coatings can be made to reduce losses to an acceptable level (less than 0.2 % per surface). Bulk crystals can also be made with sufficiently large clear apertures to minimize clipping losses and optical distortions.

The basis choice, for applications like a loophole free Bell test, has to be random, consequently the modulator must be able to work at a wide frequency range. This means that we cannot use resonant tank circuits to improve the performance of the switch at specific frequencies. Although there are many fast electro-optic modulators available, we only found a few candidates which match all the above criteria at the same time.

To simplify the driving electronics, it is desirable to have a fast switch capable of functioning at about 150 V or lower. To achieve this in a bulk crystal with a large aperture we must increase the crystal's length. Long ($\approx$ 5–10 cm) crystals of some materials can be hard to grow and too brittle to handle. The most suitable material for our Pockels' cell is Lithium Niobate (LN or $LiNbO_3$). This material is chosen for its low loss, easy availability in large sizes and large electro-optic coefficients.

A.2 The Pockels effect

The Pockels effect is an electro-optical effect where the birefringence is proportional to the electric field. The Pockels effect occurs within non-centro-symmetric crystals which lack inversion symmetry. The electric field can be applied perpendicular to the crystal optical axis which is in the same direction as the incident light. This geometry is referred to as 'longitudinal'. A longitudinal modulator is unsuitable for our needs since it relies on transparent electrodes at the crystal's optical end faces. Such electrodes always induce an additional loss. Instead we use transverse modulators where the field is applied perpendicular to the optic axis of the crystal. The light propagates perpendicular to the optical axis of the crystal. Figure A.1 shows a z-cut non-linear optical crystal with a transverse electric field applied to it.

A comprehensive explanation and derivation of the Pockels effect can be found in [162]. The effect of an electric field on the birefringence of a crystal is best understood with the help of the 'index ellipsoid' which is a representation of the relative magnitudes

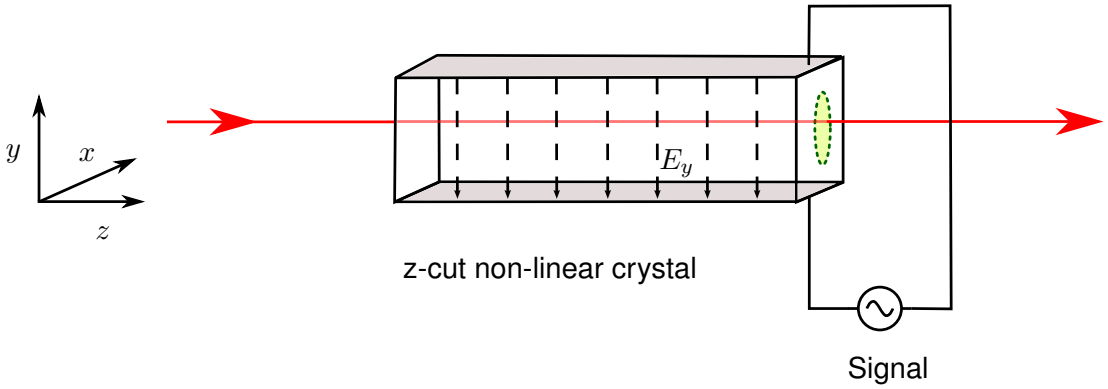


Figure A.1: Transverse electro-optic modulator. The crystal is z-cut (i.e. its optical axis is along the x direction) and an electric field is applied along the y axis. Light propagates perpendicular to the optical axis of the crystal. The index ellipsoid is projected onto the plane perpendicular to the input laser mode, this projection (onto the xy plane) is shown with green dashes.

and orientations of the refractive indices. Ideally, in the absence of an electric field a suitable crystal would be uniaxial i.e. the polarization state of an input optical mode remains unchanged. In terms of the index ellipsoid, a uniaxial crystal would have a circular projection of the index ellipsoid (when projected onto the plane perpendicular to the optical axis)[1].

For a uniaxial medium the index ellipsoid is given by

$$1 = \sum_{j=i}^{3} \frac{{x_j}^2}{n_{x_j}^2} = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} . \begin{bmatrix} \frac{1}{n_{x_1}^2} & 0 & 0 \\ 0 & \frac{1}{n_{x_2}^2} & 0 \\ 0 & 0 & \frac{1}{n_{x_3}^2} \end{bmatrix} . \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} , \tag{A.1}$$

[1] In reality, all available crystals are slightly birefringent (i.e. the index ellipsoid has a slight elliptical projection) but this effect is in our case negligible.

where n_{x_1}, n_{x_2}, n_{x_3}, are the refractive indices in the directions x_1, x_2, x_3[1] respectively. In the presence of an electric field directed transversely, the index ellipsoid becomes

$$1 = \sum_{j=i}^{3} \frac{{x_j}^2}{n_{x_j}^2} + \begin{bmatrix} x_1^2 & x_2^2 & x_3^2 & 2x_2x_3 & 2x_1x_3 & 2x_1x_2 \end{bmatrix} . \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \\ r_{41} & r_{42} & r_{43} \\ r_{51} & r_{52} & r_{53} \\ r_{61} & r_{62} & r_{63} \end{bmatrix} . \begin{bmatrix} E_1 \\ E_2 \\ E_3 \end{bmatrix} , \quad \text{(A.2)}$$

where r_{ij} are the electro-optic coefficients of the crystal and the 6×3 matrix of electro-optic coefficients is the electro-optic tensor. Most materials do not have all 18 elements of the electro-optic tensor. Several elements are typically 0 due to symmetry of the crystal. Further, several other elements are related to each other. For LN (the material we use) this tensor becomes

$$\begin{bmatrix} 0 & -r_{22} & r_{13} \\ 0 & r_{22} & r_{13} \\ 0 & 0 & r_{33} \\ 0 & r_{51} & 0 \\ r_{51} & 0 & 0 \\ -r_{22} & 0 & 0 \end{bmatrix} . \quad \text{(A.3)}$$

The values of these surviving coefficients depend on the wavelength and the frequency of switching. Approximate values for LN can be found in Table A.1. Further we are only interested in the transverse Pockels cell so we consider only $\mathbf{E}_2$. This now reduces Equation A.2 to

$$1 = \left(\frac{1}{n_{x_1}^2} - r_{22}E_2 \right) x_1^2 + \left(\frac{1}{n_{x_2}^2} + r_{22}E_2 \right) x_2^2 + \frac{x_3^2}{n_{x_3}^2} + 2r_{51}E_2x_2x_3 \, . \quad \text{(A.4)}$$

From Equation A.4 we see that in the absence of an electric field it is the same as Equation A.1 for a uniaxial crystal. Which means that when no voltage is applied across the crystal, there is no change in the polarization state of an input optical beam. If we were to write Equation A.4 in the same form as Equation A.1 then, by comparison we could find new principle axes x_i' along which there would be new effective refractive indices $n_{x_i'}'$. That is to say

$$1 = \sum_{i=0}^{3} \frac{x_i'^2}{n_{x_i'}'^2} \, . \quad \text{(A.5)}$$

[1]The directions x_1, x_2, x_3 correspond to the x, y, z crystal axes.

More details about this can be found in [158]. We can also write the refractive indices of the crystal with no electric field applied as the refractive index of the ordinary ray n_o and the refractive index of the extraordinary ray n_e. Applying a static electric field along the x_2 axis of the crystal gives, to a first order approximation, the following results

$$\begin{aligned} n'_{x'_1} &= n_o + \tfrac{1}{2} n_o^3 r_{22} E_2 \\ n'_{x'_2} &= n_o - \tfrac{1}{2} n_o^3 r_{22} E_2 \\ n'_{x'_3} &= n_e \,. \end{aligned} \tag{A.6}$$

We can now calculate the new birefringence due to the applied electric field as

$$\Delta n = \left(n'_{x'_1} - n'_{x'_2} \right) = n_o^3 r_{22} E_2 \,. \tag{A.7}$$

Equation A.7 clearly shows the linear dependence of the birefringence on the applied electric field. This is the essential nature of the Pockels effect. There is a phase difference Γ between the e-ray and the o-ray. This is given by

$$\Gamma = \frac{2\pi}{\lambda} L \Delta n = \frac{2\pi}{\lambda} L n_o^3 r_{22} E_2 \,, \tag{A.8}$$

where λ is the wavelength of the incident light and L is its length of propagation along the crystal. If we rewrite this in terms of the half wave voltage V_π and the applied voltage V then

$$\Gamma = \pi \frac{V}{V_\pi} \,, \tag{A.9}$$

where

$$V_\pi = \frac{1}{2 n_o^3 r_{22}} \frac{\lambda d}{L} \,. \tag{A.10}$$

Here d is the distance between the two electrodes used to apply electric field E_2. The voltage V is applied to these electrodes.

A.3 Experiment and results

The largest polarization rotation that we intend to use the fast switch for is from H/V to L/R (or 90° on the Bloch sphere)[1]. This is achieved when Γ is $\frac{\pi}{2}$ i.e. when the applied voltage V is $\frac{V_\pi}{2}$. This voltage is called the quarter wave voltage. Consequently,

[1] These angles would be optimal for a Bell test with maximally entangled states. For a loophole free Bell test we would use a non-maximally entangled state whose optimal measurement bases will always be at angles smaller than those for a maximally entangled state.

Optical properties	Refractive Index	n_o	2.25401
	at 810 nm	n_e	2.17438
	Birefringence	$n_e - n_o$	-0.07963
Acoustic properties	Impedance		19.071 10^5 gm/cm^2
	Speed of sound	Quasi-shear wave	4271 m/s
		Shear wave	4795 m/s
		Longitudinal wave	7316 m/s
		y-z Surface wave	3488 m/s
Electro-optic properties at 633 nm	Electro-optic coefficients (high frequency)	r_{33}	31 pm/V
		r_{13}	9 pm/V
		r_{22}	3.4 pm/V
		r_{51}	28 pm/V
	Electro-optic coefficients (low frequency)	r_{33}	32 pm/V
		r_{13}	10 pm/V
		r_{22}	6.8 pm/V
	Quarter wave voltage of our crystal at 810 nm	High frequencies	78 V
		Low frequencies	39 V

Table A.1: Properties of Lithium Niobate (LN). LN is the material we use to make a fast electro-optic polarization switch. This table shows some of its important properties. The quarter wave voltages are calculated for a z-cut 100 mm long 1.5 mm thick crystal, according to Equation A.10.

a demonstration of a working and a suitable fast Pockels cell can be done by applying a quarter wave voltage pulse and showing the polarization rotation from the HV to the LR basis or vice versa.

We investigated a self built modulator using a LN crystal and a commercially available one using Magnesium Oxide (MgO) doped LN crystals. The experimental setup, alignment procedures are identical in both cases. The performance of the two devices varies as do their operating voltages, and mechanical housings. In Section A.3.1 I shall talk about the experimental setup and alignment which is identical for the two modulators. The self bulit modulators had a better transmission than the commercial ones. They are discussed in more detail in Section A.3.2. Section A.3.2 also contains

information on the construction of these fast polarization modulators.

A.3.1 Setup

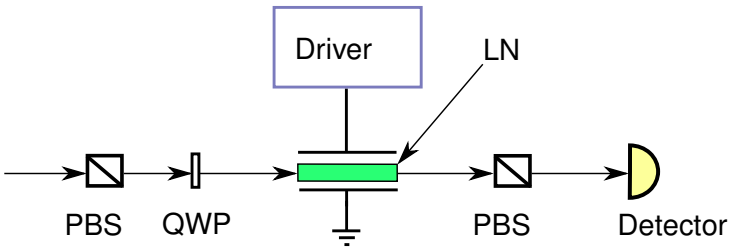


Figure A.2: The fast polarization modulator consists of a z-cut Lithium Niobate crystal placed between two electrodes. When a high voltage is applied across the crystal, the electro-optic effect causes a rotation in the output polarization. For testing and characterizing the crystal it is placed between two Polarizing Beam Splitters (PBSs). A Quarter Wave Plate (QWP) can be used to ensure a circular input polarization.

The experimental setup to characterize the fast polarization modulators is extremely simple and shown in Figure A.2. It consists of an input light beam which is polarized by a Polarizing Beam Splitter (PBS). The desired input polarization is then controlled by adjusting a Quarter Wave Plate (QWP) The fast modulator consists of a crystal placed between two electrodes and connected to a self built driver. The modulator is placed such that the input beam goes through the crystal perpendicular to the optic axis of the crystal. Another PBS at the output along with a photo-diode (detector) is used to analyze the output polarization state.

The alignment of the crystal consists of two steps. First, one makes sure that the light passes through the crystal with minimum loss. This is done by focusing the input mode such that there are no losses due to clipping of the beam. At the same time care must be taken to ensure that the beam profile inside the crystal is as uniform as possible. This is achieved by increasing the focal spot size such that the Rayleigh range is much longer than the crystal. For a 100 mm long and 1.5 mm thick crystal, we used a beam waist of 180 μm with a Rayleigh range of 126 mm. The calculated clipping losses for this beam is $\approx 0.5\,\%$.

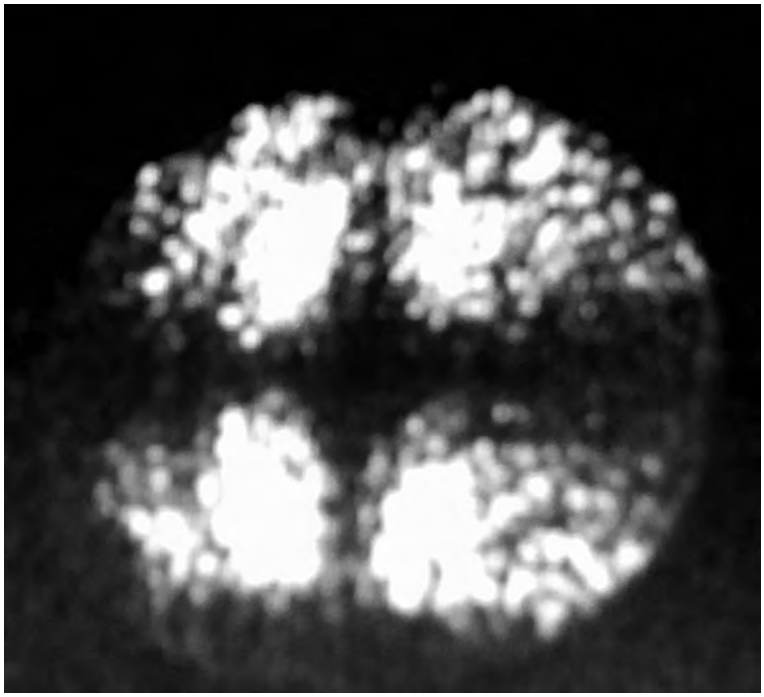


Figure A.3: The conoscopic pattern seen when the axis of the crystal is correctly aligned with the input beam. The pattern is also known as an isogyre. To see this pattern we illuminated the crystal with a diffuse laser beam. The axes of the crystal can be identified by the Maltese cross pattern.

Second, the crystal should be aligned such that the input beam is perpendicular to the optical axis of the crystal. This can be achieved by looking for the conoscopic pattern. This pattern is shown in Figure A.3. The pattern is obtained when the crystal is correctly aligned with respect to the optical beam. To see this pattern, the birefringent crystal was placed between crossed polarizers and was illuminated by a diffuse beam. The optical axis of birefringence is clearly apparent in the image, as it is indicated by the symmetry of the cross like pattern formed by the dark fringe. In our experiment, the optical axis is parallel to the entry and exit surfaces (i.e. perpendicular to the direction of propagation). This is why the interference pattern consists of two sets of hyperbolas rotated by 90° with respect to each other [163]. The real/transverse axis of one hyperbola is set parallel to the optical axis while that of the other is perpendicular. Applying a voltage to the crystal at this stage will cause the hyperbolas to move closer or further away from the center. Typically we perform this alignment step using diffuse light. A piece of translucent scotch tape introduced into the path of the input beam is

enough to sufficiently diffuse the light.

A.3.2 Acoustic ringing during fast polarization modulation

Using the values given in Table A.1 we can see that the quarter wave voltage for LN which is 1.5 mm thick and 1 mm long, is 7800 V. A practical constraint in the development of a fast polarization modulator is the electronics needed to drive it. Particularly, the transistor needed to quickly switch such a high voltage. Further, the crystal has an effective capacitance and the current needed to quickly modulate the high voltage across our crystal is about 5 A. The quarter wave voltage can be reduced by either decreasing the thickness of the crystal or increasing its length. If we decrease the thickness of the crystal too much it can be difficult to couple light into and out of the crystal with a low loss, so we increased the length of the crystal to 100 mm. This decreased the quarter wave voltage to 78 V.

The crystal used was a 1.5 mm × 10 mm × 100 mm LN crystal. The 10 mm width of its rectangular cross-section was used to increase the mechanical durability of the brittle and long LN crystal. The crystal was z-cut i.e. the direction of propagation of light was along the z-axis of the crystal. The optical axis was perpendicular to the z-axis. The 10 mm × 100 mm surfaces were gold coated and acted as the electrodes for the Pockels cell.

The LN crystal was AR coated at 810 nm with a specified loss of less than 0.2 % per surface. When measured the crystal had a transmission of 99.1 ± 0.6 %.

We first used the LN crystal resting on a printed circuit board without mechanical strain. The electrical contacts were secured with conductive copper tape. The driver circuit was connected to the crystal and supplied with current. The crystal was aligned as above. The input polarization was set to Vertical (V). The detector was placed in the Horizontally (H) polarized output arm of the analyzing polarizer. A bias voltage equal to the quarter wave voltage was applied to rotate the polarization to Left circularly (L) polarized output. This voltage was reduced off by the driver to rotate the output polarization.

The driver was connected to a function generator that produced a 200 ns wide trigger signal once every ms. When the driver received the trigger pulse it would, for the duration of the trigger, drop the voltage applied by 24 V. This voltage is smaller

than the quarter wave voltage but is enough to see the electro-optic effect. The results are shown in Figure A.4.

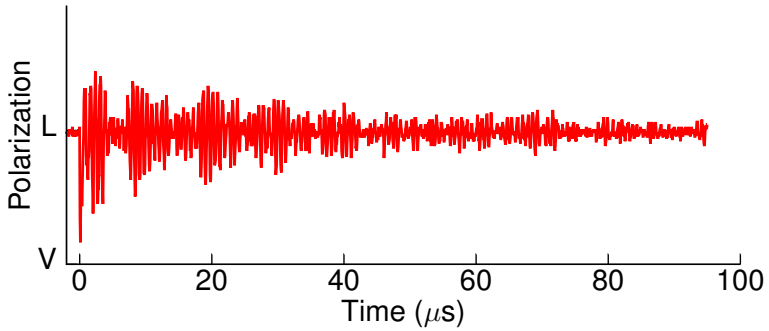


Figure A.4: Optical response of a $100\times10\times1.5\,\mathrm{mm}^3$ LN crystal, mounted without mechanical strain on a circuit board. At time 0 a voltage pulse of 24 V amplitude was applied to the crystal for 200 ns. The output polarization oscillates due to the effects of the acoustic waves. With no additional mechanical or electrical damping the acoustic waves took a long time ($> 90\,\mu$s) to die out.

At time 0 a 24 V pulse was applied to a LN crystal for a duration of 200 ns. Immediately after the pulse the polarization of the output changed until it was almost Vertically (V) polarized. Since we applied a voltage less than the quarter wave voltage, the polarization rotation caused by the LN modulator was not enough to change the L polarized light to V polarized. This can be seen by the sharp dip at time 0 in Figure A.4. This is the desired change. However, the output polarization continued to oscillate for about 90 μs afterwards. This oscillation of the output polarization means that the switch takes a very long time to settle into a steady birefringent state. Since we require a polarization modulator that can completely switch the polarization state within a few ns, these oscillations that take several μs to die out must be damped (If not, the effective switching time is too long for use in our loophole free Bell test experiment).

The oscillations seen in Figure A.4 are caused by acoustic waves in the crystal and this phenomenon is often called acoustic ringing. Any material that is suitable for the Pockels effect is also piezoelectric in nature. Thus, the application of a quick electric pulse causes the crystal to vibrate. These vibrations cause the output polarization to oscillate due to the acousto-optic effect. The amplitude of the vibrations in polarization slowly dies out because the acoustic wave is damped.

The frequencies observed in the polarization oscillations correspond to the physical dimensions of the crystal. Wang et al., [164] showed that acoustic waves are generated in directions both parallel and perpendicular to the applied electric field. Further they said that it is important to damp both. The frequencies observed in the polarization fluctuations are consistent with this. We observe two frequency components compatible with sound waves along the 1.5 mm height of the crystal and the 10 mm width of the crystal. We do not observe an oscillation frequency compatible with the 100 mm length of the crystal. Such a frequency would be very difficult to observe.

Many electro-optic devices solve the issue of acoustic ringing in several ways [165, 166]:

- Waveguide structures are so small that their quarter wave voltage is a few volts. This drastically reduces the amplitude of sound waves caused by the piezo-electric effect. Further, waveguides are typically smaller than the wavelength of the acoustic waves and are often set in bulk media with similar acoustic properties. Thus any sound waves generated do not affect the optical signal. Unfortunately the coupling losses [161] ($\gg 5\,\%$) into such waveguides render them unsuitable for our purpose.

- Many electro-optic devices avoid acoustic ringing by shaping the crystal to scatter sound waves. The simplest way is to cut all end faces at an angle such that the sound waves are reflected out of the crystal. Unfortunately, we cannot use this technique because the angled faces can cause distortions in the optical mode which reduce the coupling back into a fiber.

- Embedding the crystal in a medium with similar acoustic impedance is also a common way of mechanically damping out the sound waves (see Figure A.5).

- Electronic filters can be used to remove energy from the crystal at particular frequencies (see Figure A.7).

To mechanically damp an acoustic wave one must allow the wave to propagate into another medium where it can be scattered. Ideally the other medium would have a similar acoustic impedance. We tried to sandwich the LN crystal in between larger slabs of LN. Since, we can be sure of a good acoustic impedance match. This did not help because LN is not electrically conductive and could not be used as electrodes.

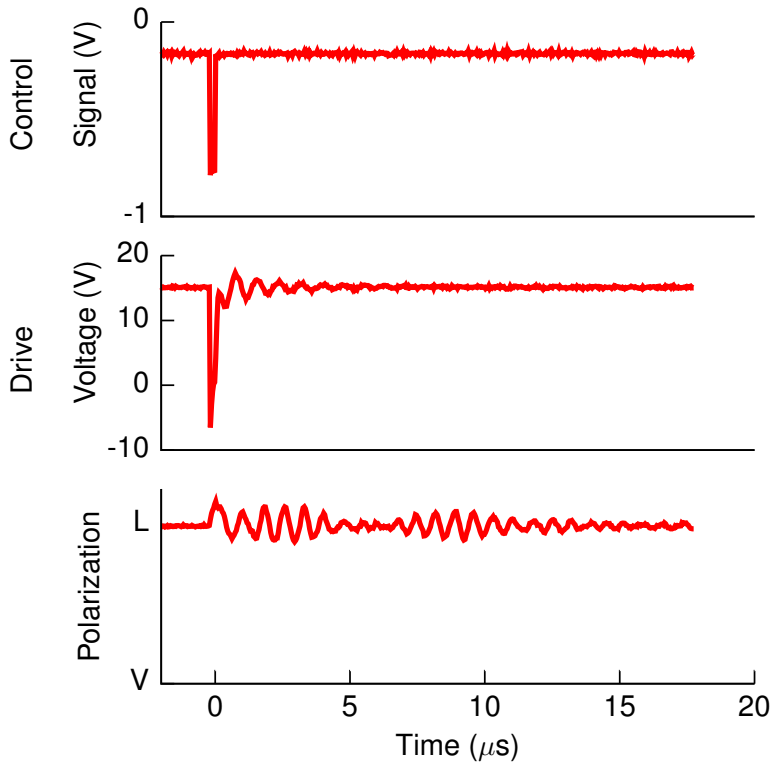


Figure A.5: Mechanical damping of the acoustic ringing was achieved by sandwiching the LN crystal between two large copper blocks. The polarization switching time is reduced to about 15 μs. The topmost graph shows the trigger pulse. The drive voltage applied across the crystal is shown in the middle graph. The bottom most graph shows the optical response of the polarization modulator.

Introducing thin copper electrodes provided a boundary with an impedance mismatch. Although this increased the damping the reduction of the acoustic ringing was not large enough. Another method was to surround the crystal with LN powder and compact the powder all around the crystal. We attempted this with both LN powder and Manganese Oxide (MnO) which also has a similar impedance (18.91×10^5 gm/cm^2 s for MnO and 19.07×10^5 gm/cm^2 s for LN). We used powder because we believed that the many granules would better scatter any acoustic waves they absorbed. This approach also failed. We had to compact the powder around the crystal in order for the sound waves to travel into the surrounding medium. However this resulted in the breakage of the brittle LN crystal.

Copper has an acoustic impedance (20.21×10^5 gm/cm^2 s) only slightly larger than

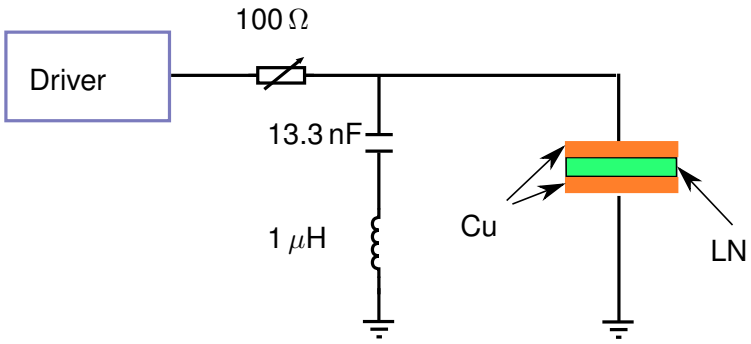


Figure A.6: Using this RLC filter on the drive voltage line, we were able to reduce the acoustic ringing as can be seen in Figure A.7. The electrical damping was done in addition to the mechanical damping by two copper slabs.

LN. We used two large copper slabs (11 mm × 11 mm × 100 mm) to sandwich the LN crystal. These copper slabs were connected to the driver circuit and formed the electrodes of the Pockels cell. A good contact between the copper slabs and crystal was ensured by a thin layer of Arctic Silver - an electrically conductive silver nano-particle paste. Plastic clamps were used to secure this sandwich in place and apply a firm and uniform pressure.

Figure A.5 shows the result of mechanical damping using two large copper blocks. The crystal is aligned in the same way as before. A DC bias voltage of 15 V was applied to the crystal. The input polarization was then rotated such that the output polarization was L. At time 0 a function generator produces a trigger pulse which is fed to the driver. This trigger pulse is shown in the topmost graph of Figure A.5. For the duration of the trigger the driver reduces the voltage across the crystal. We used a probe connected to the electrodes of the crystal to measure the change in the drive voltage. This value is seen in the middle graph. Once again by measuring the intensity of light incident on the photo-diode we measure the polarization state of the output.

From Figure A.5 we can clearly see that the oscillations in the output polarization die down much quicker (in about 15 μs as opposed to about 90 μs in Figure A.4). This shows the utility of sandwiching the LN crystal between large copper slabs.

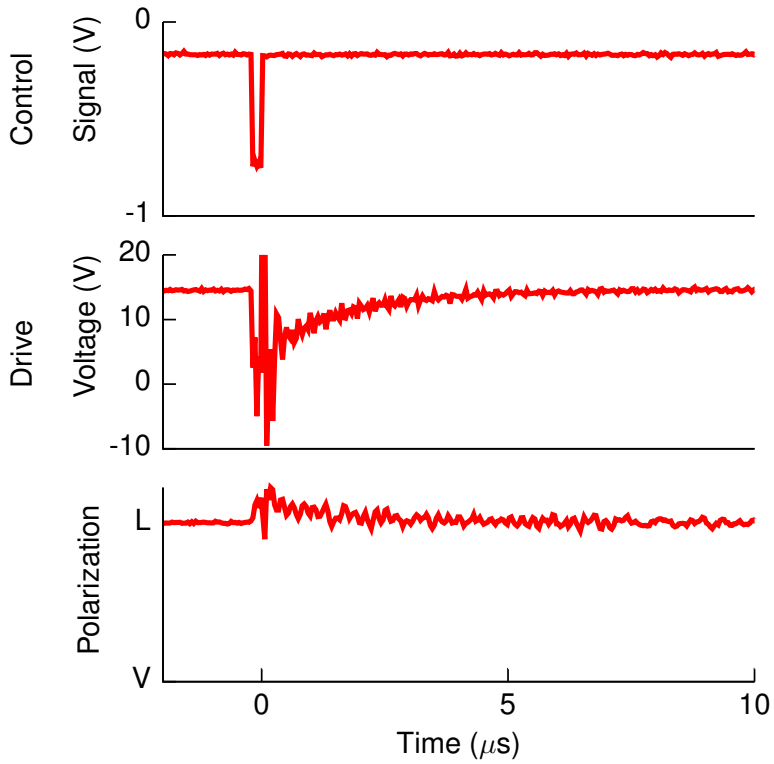


Figure A.7: Electronic damping of the acoustic ringing. The same sandwiched structure as before was subjected to electrical damping. We used RLC filters on the high voltage drive lines. These filters were designed to damp the acoustic resonance frequencies. The topmost graph shows the trigger pulse. The drive voltage applied across the crystal is shown in the middle graph. The bottom most graph shows the optical response of the polarization modulator. There is significant reduction of the acoustic ringing which is now suppressed after about 4 μs.

We were not able to completely eliminate all acoustic ringing. We could only place copper slabs above and below the crystal. We could not place copper strips along the length of the crystal because it could have shorted the two terminals of the fast polarization modulator. Due to mechanical constraints we could not damp these vibrations along the width of the crystal using some other material. Even though the acoustic impedances of LN and copper are similar they are not the same thus there is always some reflection at the boundary. The copper blocks and the LN crystal formed a distinct boundary with two different lattice structures, so the transfer of acoustic vibrations into the copper was not always perfect. Acoustic waves propagating in the LN crystal can travel in several modes. The surface waves (Rayleigh waves) are best coupled into the copper. However, modes like the shear waves and plate waves are not

so well coupled.

To further reduce the acoustic ringing we can try to electrically damp these oscillations. We introduced an RLC filter along the drive voltage line as shown in Figure A.6. This was in addition to the mechanical damping discussed earlier. The filter used was a band stop filter with a center rejection frequency of about 1.4 MHz. This is close to the resonance frequency of the acoustic waves. The filter we used was over damped with a damping ratio of 5.7 and an attenuation of more than -40 dB at the center rejection frequency.

The results of electrically damping the acoustic ringing are shown in Figure A.7. It can be seen that the amplitude of oscillation of the polarization state is smaller than before with just mechanical damping (see Figure A.5). The duration of the ringing is reduced to about 3 μs.

A.4 Conclusion

We currently have a modulator capable of switching in 3 μs. Work is ongoing to reduce this even further.

Lithium tantalate is a promising material because it has smaller piezo-electric coefficients [167].

Appendix B

Measurement of Gaussian beams

The high efficiency source of polarization entangled photon pairs requires a good mode overlap between the pump and collection modes. As such it is important to measure the beam profile and focusing parameters (beam waist, and its position). The method used for these measurements is outlined in this Appendix. This appendix does not contain any original contribution.

B.1 Gaussian beams

The transverse electric field intensity of a Gaussian beam is well approximated by a Gaussian function. Mathematically, a Gaussian beam is a solution to the paraxial form of the Helmholtz equations. The behavior of a Gaussian beam, at any point (z) along the propagation of the beam, can be described by its spot size ($\omega(z)$), radius of curvature ($R(z)$) and Gouy phase. For a focused Gaussian beam, the smallest $\omega(z)$ is called the waist ω_0. The position of this waist is at z_0. The intensity or irradiance distribution (I) can be written as a function of z and the radial distance from the center axis of the beam as

$$I(r,z) = I_0 \left(\frac{\omega_0}{\omega(z)}\right)^2 e^{\left(\frac{-2r^2}{\omega^2(z)}\right)}, \tag{B.1}$$

where $I_0 = I(0,0)$ is the intensity at the center of the beam waist (ω_0). Further, $\omega(z)$ is the radius at which the intensity drops to $\frac{1}{e^2}$ of its axial value.

For a given wavelength (λ),

$$\omega(z) = \omega_0 \sqrt{1 + \left(\frac{z}{z_R}\right)^2}, \tag{B.2}$$

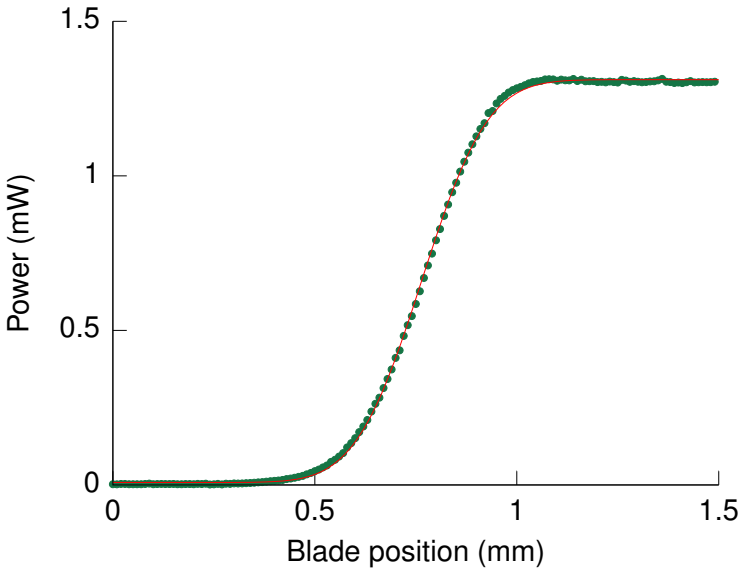


Figure B.1: Sample measurement of a beam radius made by moving a blade out of the beam. This graph shows the beam profile in the vertical direction for the left collection arm at a distance of about 30.8 cm away from the fiber. The solid line is the fit and the circles are the measured values. The beam radius of this data is $257 \pm 1.5\,\mu$m.

where z_R is called the Rayleigh range and is given by

$$z_R = \frac{\pi\omega_0^2}{\lambda}\,. \tag{B.3}$$

To ensure that $\omega(z)$ is approximately uniform throughout the length of the crystal (L), we ensure that $z_R \gg L$.

B.2 Waist measurement

To measure ω_0 and z_0 and to verify the Gaussian beam profile ($I(r,z)$) of both the pump and collection modes we measured $\omega(z)$ at at least four different locations. Fitting them to Equation B.2 we obtain ω_0 and z_0. The presence of an aperture can distort the mode, thus, we only measured the beam size before the crystal. We also took into account the increased path length due to the various optical components (like the Glan-Taylor, PBS, PPKTP crystal, etc.).

Each measurement of the beam size was made by moving a knife edge perpendicular to the beam. We placed the knife edge such that it completely blocked the beam at a location z. We then moved the knife in steps of $10\,\mu$m. After each step we measured the power in the unblocked portion of the beam using a photo-diode. For a beam with a Gaussian profile the resultant power vs. knife position graph was in the shape of an error function[1]. We fit the data obtained to an error function and obtain $\omega(z)$. Figure B.1 shows one such measurement and fit. To verify that the beam profile is Gaussian, we can repeat the measurement by moving the knife in two perpendicular directions (both perpendicular to the direction of propagation of the beam).

Figure B.1 is an example, this data was taken for collection arm Main 1 (see Figure 3.2) at a distance of 30.8 cm from the fiber.

[1]The error function, also known as the Gauss error function, is the integral of the Gaussian beam profile in one dimension.

Appendix C

Alignment of the high efficiency polarization entangled source

The key to obtaining a high efficiency is correctly engineering the mode overlap between the pump and the collection modes and eliminating losses. The correct focusing of the pump and collection modes is crucial to attaining a high heralding efficiency (see Section 3.3.2). The spatial overlap of the pump and collection modes is just as critical. The alignment procedure of the high efficiency source is outlined here. For portability we built the source on top of an optical breadboard. I developed this alignment procedure to ensure a high efficiency and visibility form the source of polarization entangled photon pairs presented in Chapter 3.

1. Starting from an empty breadboard, the first step was to mark the approximate locations of all components. We chose the distance between the pump and crystal (1.35 m) and collection optics and crystal (0.63 m) to be the same as the single pass experiment. Hence we could use the same focusing conditions described in Section 3.3.

2. As shown in Figure C.1, we started the alignment by placing the optics for the collection arm Main 1. An AR coated fiber was used with an aspheric lens to collimate light from an 810 nm laser. To direct the beam we used a dichroic mirror, from Lattice Electro Optics, which is highly reflective (R>99.8 %) for 810 nm and transparent (T> 99 %) for 405 nm. The coatings were designed for a 22.5 ° angle of incidence and are made from fused silica to avoid fluorescence due to the UV pump.

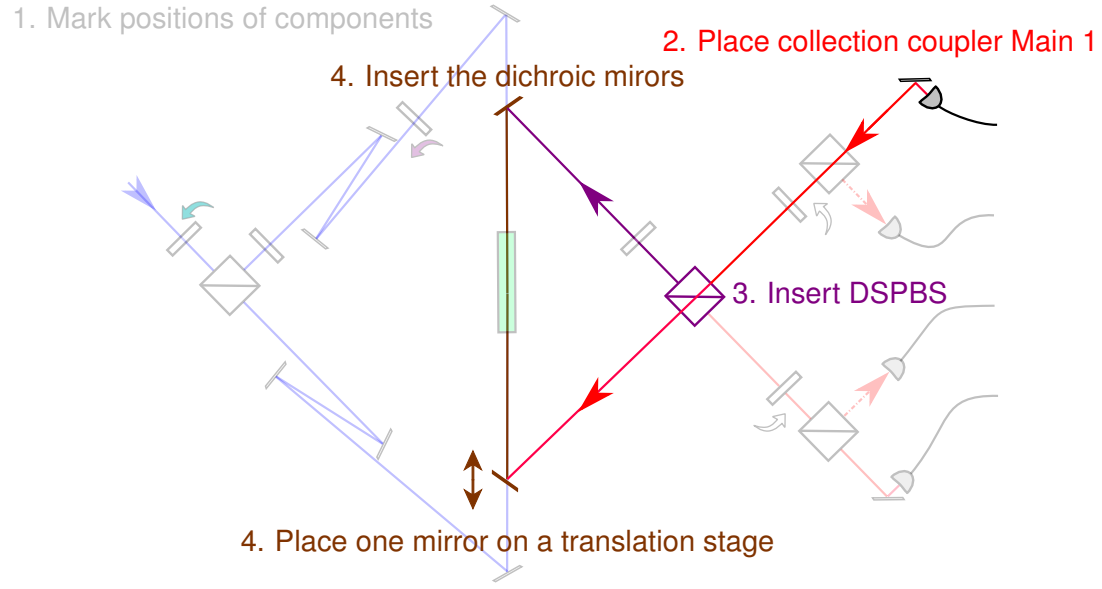


Figure C.1: The Figure shows the first few steps in the alignment of the high efficiency polarization entangled source. We first marked the locations of the components on the breadboard. We then placed collection fiber Main 1, it's collimator and a mirror after which we introduced the Downconverted Sagnac PBS (DSPBS). After which we complete the Sagnac loop by placing two mirrors, symmetrically, to form a triangle with the PBS at one corner.

3. We then placed the Downconverted Sagnac PBS (DSPBS) (as shown in Figure C.1). This is the PBS which is used to interferometrically recombine the two downconverted paths.We used an, optically contacted, fused silica PBS from AG-optics; AR coated at 810 nm with less than 0.2 % loss per surface. The extinction ratio of this PBS was 300:1 for *all*[1] ports. The PBS was placed in the beam and leveled such that both output beams were parallel to the surface of the breadboard. The PBS was placed perpendicular to the input beam and its extinction ratio verified.

[1]Typically a PBS consists of two right angled prisms glued together with the polarization selective coating on the hypotenuse surface of one of the prisms. The best extinction ratio of such a PBS is obtained when the incident light reaches the polarization selective coating without passing through the glue. In our setup, the PBS and the Sagnac interferometer are aligned using one port as the input. However, when the crystal is pumped from two directions, two other ports of the PBS serve as input ports. For a good alignment, it is desirable to have an optically contacted PBS (without glue) that has the same extinction ratio for both the transmitted and reflected arm irrespective of the input direction.

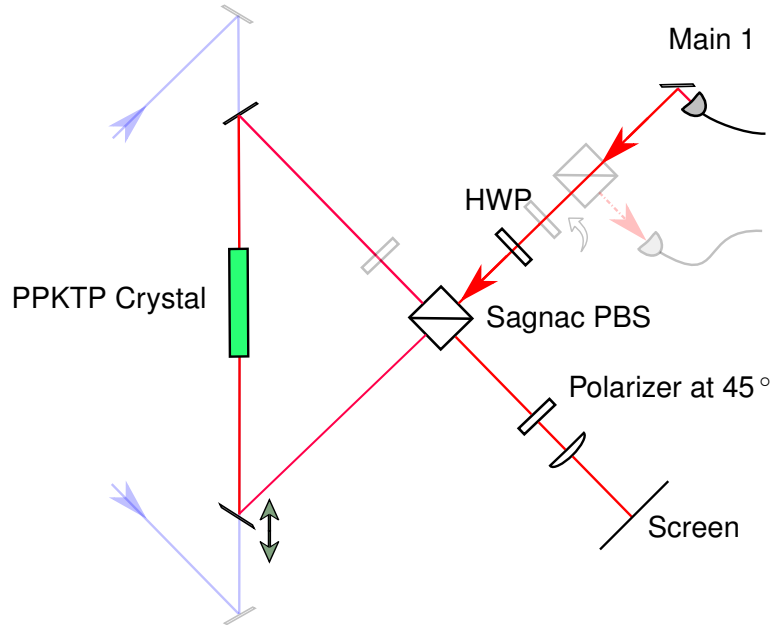


Figure C.2: Alignment of the Sagnac interferometer. A film polarizer at 45 ° is used to project the H and V polarized components on to the same polarization basis. The fringes are expanded by a lens and projected onto a screen. See alignment steps 5, 6 and 7.

4. We then complete the Sagnac loop by adding two dichroic mirrors so as to form a right angled isosceles triangle with the PBS at the right angled apex. This is depicted in Figure C.1. It is useful, but not necessary, to place one of these mirrors on a translation stage. This results in a better degree of control when aligning the Sagnac interferometer. These mirrors are the same as those described in alignment step 2. We are not sensitive to losses in pump power as long as the mode remains undistorted.

5. To align the Sagnac interferometer, we first placed a HWP in the collection arm Main 1 and rotated it such that the optical power in the two output arms of the PBS are equal. We then visually overlapped the two beams from the two output ports of the PBS. This was done using a translucent piece of paper to see both beams at once. For the initial alignment of the Sagnac interferometer, we overlapped the beams by horizontally tilting the mirror upon a translation stage and compensating by moving the stage. This allowed us to find the position at which both mirrors formed an isosceles triangle. This adjusts the beams horizontally, for the vertical alignment we tilted one mirror and compensated by tilting

the other mirror. To observe interference fringes, we placed a film polarizer at the output of the PBS. The polarizer was rotated to 45 ° such that the H and V polarized light at the output of the PBS would be projected on to the same polarization basis. This allows the two modes to interfere. The fringes produced are enlarged and imaged onto a screen by a lens. The mirrors are adjusted such that we observe the central/zeroth fringe. The setup for aligning the Sagnac loop is shown in Figure C.2. When aligning the Sagnac, the interference observed is at the location of the polarizer. If the beams overlap at the location of the polarizer, but have a small angle between them, then we will also observe the fringes. To ensure the beams are overlapped everywhere, we must observe the zeroth fringe with the polarizer in at least two different and distant locations.

6. The PPKTP crystal was mounted inside its oven (see Figure 3.12) and placed on top of a 5 axis translation mount (9082 from Newfocus). The crystal was placed such that its center corresponded to the midpoint of the Sagnac loop. We adjusted the crystal for maximum transmission of the 810 nm beams. We also ensured that these beams passed through the center of the crystal.

7. After inserting the crystal the Sagnac interferometer must be realigned. While looking at the fringe pattern we tweaked the pitch, roll and yaw of the crystal till we were once more at the central/zeroth fringe. This ensures that the crystal surfaces are perpendicular to the beams.

8. As shown in Figure C.3, we removed the polarizer, lens and screen used to observe the interference pattern and coupled the output from the Sagnac into collection fiber Main 2. Like collection fiber Main 1, this fiber is also single mode at 810 nm and AR coated on one end. To reduce the amount of UV we once again use a dichroic mirror. The coupling into collection fiber Main 2 is about 95 %.

9. We use a 405 nm 10 mW Ondax laser diode as the pump. We coupled the pump into a single mode polarization maintaining fiber after passing it through an anamorphic prism pair and through an optical isolator. The output of the fiber is connected to the source via a Blue Glass (BG) filter and a Glan-Talor polarizer. As discussed in Section 3.3.2 the pump was focused using a telescope. The pump was directed into the crystal and aligned such that it visually overlaps the 810 nm

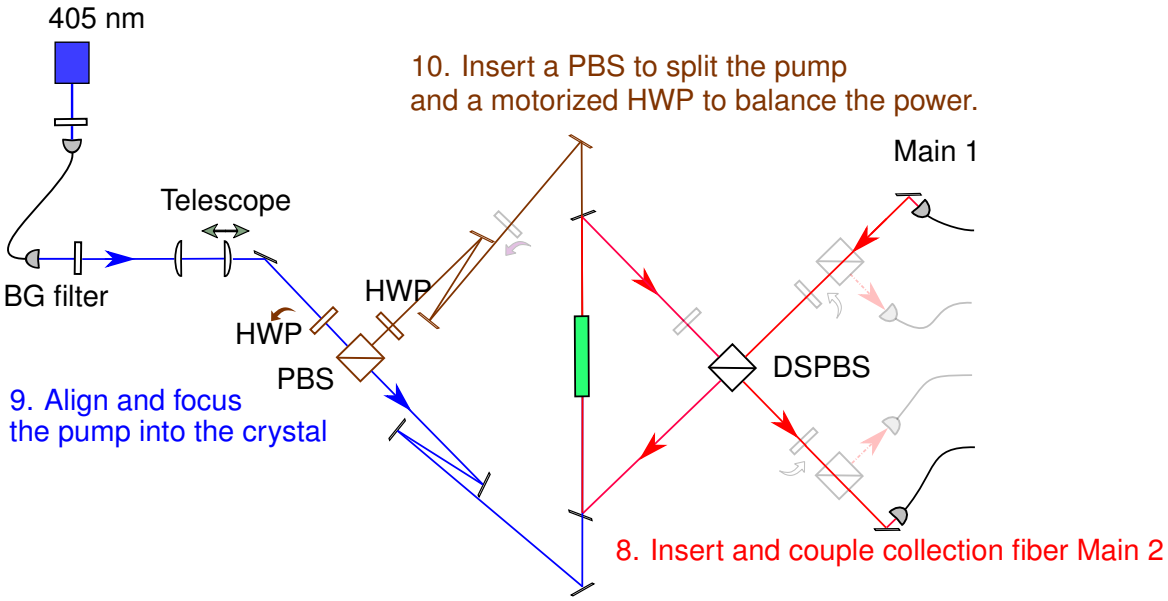


Figure C.3: After aligning the interferometer we coupled the light into the other collection fiber. We also aligned the pump, fiber coupled it and adjusted the focus. The focus of the pump was set to be 265 μm and was centered in the crystal. We then inserted a PBS in the pump's path to split the pump into two arms. Both pump arms were aligned independently to overlap with the 810 nm beams.

beam. Figure C.3 shows how we control the position and direction of the pump beams by inserting two mirrors.

10. To pump the crystal from both directions we need to split the pump. This is achieved by inserting a PBS as shown in Figure C.3. We also insert a motorized HWP before this PBS. By rotating the HWP we can control the relative pump intensities in each pump arm. The reflected arm of the PBS is V polarized. However, downconversion in our crystal requires the pump to be H polarized. We use another HWP at 45° for this purpose. Using mirrors, we direct this pump beam (the upper pump arm in Figure C.3 along the 810 nm beam and through the crystal.

11. Both the collection fibers were connected to APDs (see Figure C.4). The signals from the APDs were connected to a coincidence detection circuit. We walked the pump beams, one at a time, to observe downconverted pairs. We then inserted

Interference Filters (IFs) to reduce uncorrelated counts. The IFs are custom made by Semrock to have a transmission of more than 98 % at 810 nm with a bandwidth of 5 nm. They block all other frequencies from 350 nm – 1120 nm by a factor of at least 10^{-6}. At 405 nm they have a transmission of at most 10^{-7}. After inserting the IFs we continue to walk the pump arms to maximize the heralding efficiency.

12. Section 3.5 describes the wavelength tuning of the source. We adjust the temperature of the crystal for degenerate downconversion wavelengths.

13. In each collection arm we insert measurement polarizers (see Figure C.4). These consist of a motorized HWP followed by a PBS. By rotating the HWP we can measure in any linear polarization basis. The PBSs used were manufactured by Linos and have an extinction ratio of 1000:1 in the transmitted arms. The transmission through these PBSs is >99.5 %. We first inserted the PBSs and aligned them perpendicular to the collection modes by looking at the back reflection from the co-propagating 405 nm light. A finer adjustment of their alignment was made so as to maximize their extinction ratio. We then inserted the motorized HWPs. We used true zero order single plate HWPs AR coated to have a loss of less than 0.2 % per surface. It is important to use polarizers with a high transmission and a high extinction ratio. Further care must be taken to ensure that these polarizers do not distort the mode of the downconverted light as this increases the coupling loss into the single mode collection fibers.

14. Once the HWPs are inserted we need to calibrate them. To do so we use the downconverted signal. We pump from one direction only and rotate the HWPs while measuring the number of pairs. We fit the collected data to obtain the position of the minimum. Depending on the direction in which we pump this position is either 0 ° or 45 °.

15. An additional 300 mm focal length lens is used in each collection arm to help focus the collection modes (see Figure C.4). The position on these lenses was adjusted until we obtained the desired focusing conditions. This lens along with the aspheric lens used in the fiber coupler forms a two lens telescope that allows us to optimize the collection focus. Section 3.3.2 explains how we do this. Once this

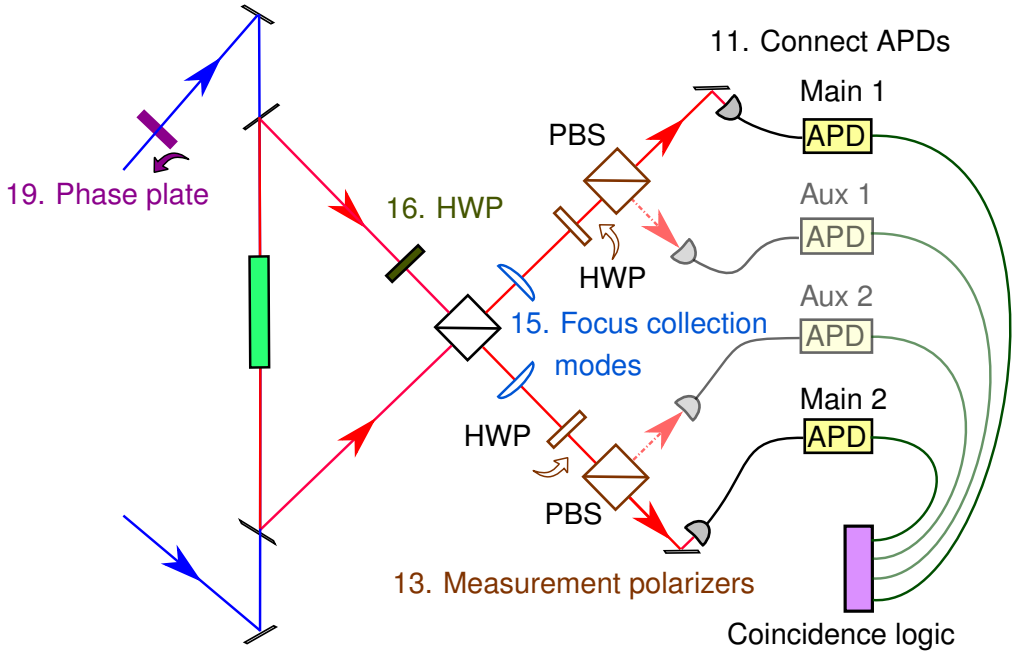


Figure C.4: We connected APDs to the collection fibers and observed downconverted pairs (see Figure C.4). After which, we inserted measurement polarizers into the collection arms. We calibrated these polarizers and then inserted a HWP inside the Sagnac loop. Using an additional lens we then optimized the focusing of the collection modes. A phase plate was introduced into one of the pump arms. Auxiliary (Aux) collection fibers were coupled and connected to APDs.

step was completed we observed a high heralding efficiency. Further alignment of the source only improved this efficiency by a couple of percent.

16. To achieve entanglement, it is necessary to have a HWP inside the Sagnac loop (see Section 3.2). At this stage we insert a HWP into the Sagnac loop (see Figure C.4). This HWP must be set at 45° such that it converts H to V and vice versa. To align the interferometer this HWP must be set to 0° (since at 45° all input light is effectively retro-reflected). Thus, any wedge error or tilt of this wave plate will ruin the visibility of the interferometer. Which in turn adversely affects the polarization correlation visibility of the source. We mounted the HWP on a tip tilt rotation mount to reduce such effects.

17. With the Sagnac HWP in place we once again aligned the Sagnac interferometer. We used a temporary mirror in collection arm Main 2 to observe the fringes.

While aligning the Sagnac, we tilted/rotated the DSPBS and compensated by moving/tilting the mirror mounted on a translation stage. After realigning the Sagnac loop we rotated the Sagnac HWP to 45 °.

18. The free output ports of the measurement polarizers are coupled into single mode fibers and connected to APDs. These are called the auxiliary fibers/detectors and are labeled Aux in Figure C.4. The auxiliary detectors provide a signal for locking the phase of the generated state. The main collection fibers can be connected to the TES detectors to observe a $\approx 75\,\%$ efficiency.

19. A phase plate consisting of a 0.1 mm thick and 12.2 mm diameter glass microscope cover slip was used to adjust the phase of one pump arm with respect to the other. The phase plate is mounted on a motorized rotation stage that tilts it with respect to the pump beam. Details on phase locking the source can be found in Section 3.2.3

20. To correct for minor alignment issues and improve the efficiency of the source by about 2 % we aligned the source by following an iterative cyclic procedure. First we walk the upper pump for the highest rate of pairs and then we walked collection Main 1 followed by collection Main 2 for the highest efficiency. We then walk the lower pump for the highest efficiency. We repeated these steps until there was no further improvement in efficiency.

21. To ensure that we are at the optimum focusing conditions we make minor adjustments to the pump focus and compensate by adjusting the collection focus. For each adjustment of the collection focus we repeat step 20. We also measure the focusing of the pump and collection modes to ensure that the beam waists are all centered in the crystal. Further, we measure the efficiency from both the upper and lower pump arms to verify that they are the same.

22. We now adjust the coupling into the auxiliary detectors and verify the alignment of the source by testing the visibility, phase locking, efficiency, etc.

Appendix D

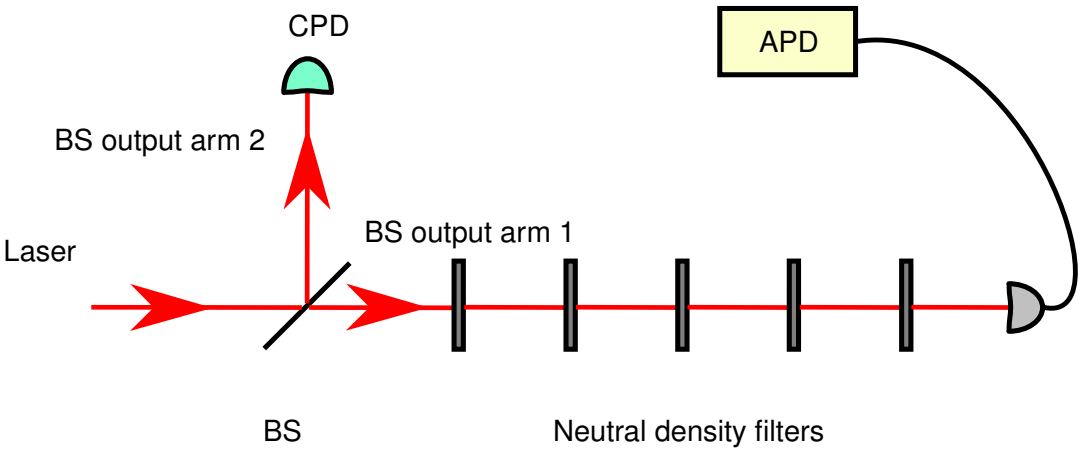
Calibration of APD detectors

The measured efficiency of our source was limited by the losses in the Si APDs we used. Calibrating these and other losses allows us to find the mode coupling efficiency of our source. It also allows us to estimate the expected heralding efficiency while using TES detectors. As described in Section 4.3 we measure the detection efficiency of our APDs using a procedure similar to [91]. Our detector consists of the diode enclosed in its housing and cooled to a set temperature along with the multimode fiber it is pigtailed to and the associated control electronics. The detector is connected to the source of polarization entangled photon pairs via a fiber to fiber join. We define the detection efficiency of the APD to mean the ratio of the number of detection events (seen by the electronics) to the number of photons injected into the APD's multimode fiber through this fiber to fiber join. The photo diodes we used for experiments presented here were calibrated in ASTAR. All other measurements presented here were performed by me.

We calibrate our APDs at 810 nm and correct for the background counts. To apply a correction for the background counts, we first measure them by blocking the light near the input laser and then subtract this value from the signal counts. In doing so we ignore afterpulsing effects[1]. Nevertheless, we typically operate our APDs at very low count rates ($\approx$ 10,000 /s). Consequently, the effect of afterpulsing can be neglected.

The setup to measure the detection efficiency of an APD is shown in Figure D.1(a). We started with one bolometrically calibrated Si photo-diode (CPD). This photo-diode was calibrated by the National Metrology Center in A*STAR, Singapore [168]. The photo-current seen by the photo-diode depends on the size of the incident beam, the

[1]Electron hole recombination emits photons which can also be detected by the APD. This is called afterpulsing.



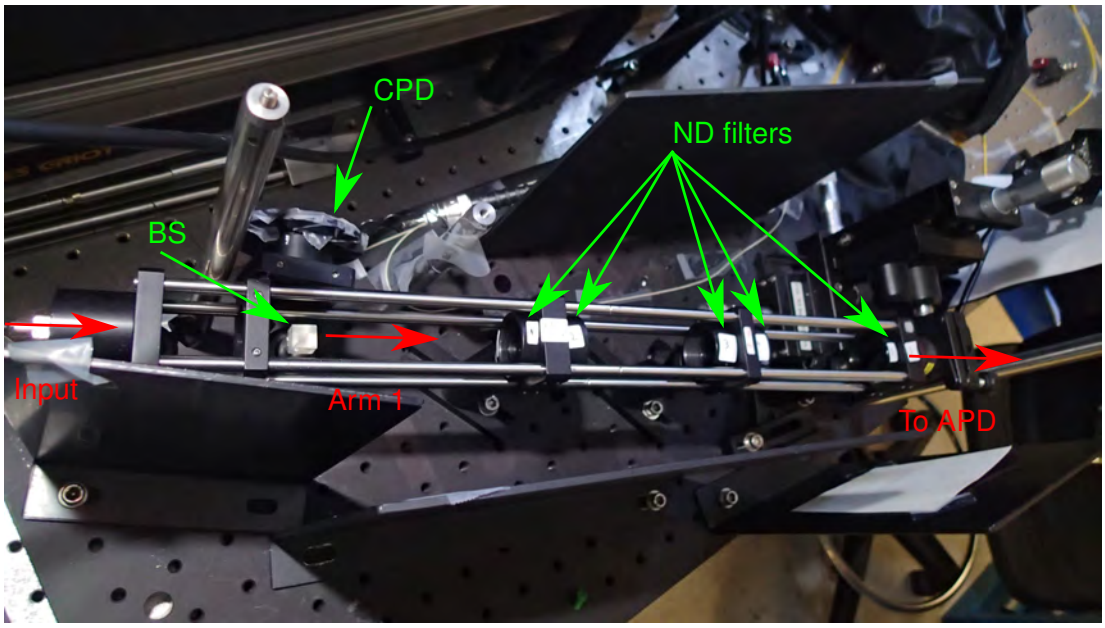


Figure D.1: Above: Schematic of the setup used to characterize APDs. CPD is a bolometrically calibrated Si photo-diode. BS is calibrated beam splitter, with two output arms. Arm 1 is attenuated by ND filters and coupled to the test APD. Arm 2 is used as a reference for the input power. Below: A photograph of the same setup.

angle of incidence, wavelength, and surface quality of the photo-diode. The photo-diodes we used were Hamamatsu S5107 with a surface area of $1\,\mathrm{cm}^2$. The chosen photo-diodes had a very clean and scratch free surface. They were mounted onto a cage system in a manner designed to repeatedly ensure the same angle of incidence (see Figure D.1(b) for a photo of the experimental setup).

Before we can calibrate our APDs we must first calibrate losses in the other optical components we use, to do so we require two calibrated photo diodes. The process of transferring the calibration form our one calibrated photo diode – CPD onto another photo diode (PD2) involves the temporary use of a third and Uncalibrated Photo Diode – UPD. The transfer of calibration from CPD to PD2 was the first step in the process of characterizing the APDs. We used an 810 nm grating stabilized diode laser coupled into a 780-HP singlemode fiber. The output from the fiber was collimated using an aspheric lens attached to a cage system. The polarization of this mode was set to H using a fiber polarization controller[1]. The light was split using a (as of yet uncalibrated) non polarizing Beam Splitter (BS). One output of the BS (arm 2) had the third and uncalibrated photo-diode (UPD) while the other output of the BS (arm 1) had alternatively, either CPD or PD2.

The photo-current from each photo-diode was measured by a HP-3458A ammeter with a precision of 1 pA (The photo current from the photo-diodes was a few μA.). We averaged over 200 measurements, the integration time for each was set to 40 power line cycles (approximately 0.8 s). One output port of the BS (arm 2) was used to monitor and correct for laser power fluctuations using UPD. On the other output port (arm 1), we alternatively attached CPD and PD2. By comparing the current from CPD and PD2, we transferred the calibration of one on to the other.

The second step was the calibration of the BS splitting ratio. With the input polarization kept constant, we used the two calibrated photo-diodes (CPD and PD2) on either output of the BS to determine its splitting ratio.

We used five ND filters to attenuate the laser to a single photon level. The filters we used had a transmission of (calibrated values) 0.33 %, 0.0085 %, 0.037 %, 0.165 % and 0.0017 % with a relative error of about 0.5 % each. The ND filters were sufficient

[1]The splitting ratio of a non-polarizing Beam Splitter (BS) is, in most cases, dependent on the input polarization. Repeated checks to ensure that there were no large drifts in the polarization and consequently changes in the BS splitting ratio were carried out

to reduce a 190 nW CW 810 nm laser to about 23000 photons/s. The third step was the calibration of each of these ND filters. Once again we used arm 2 with the CPD as a reference and measured the power with and without each ND filter. The attenuation of the ND filters is dependent on their thickness and consequently their angle. The ND filters we used were not AR coated so there was a reflection from each surface. Stacking two ND filters perpendicular to the beam results in an increase in the net transmission as compared to the two filters calibrated individually, this is due to multiple back reflections creating an "etalon-like" effect. To avoid this problem each ND filter was placed at a small angle with respect to the beam and its nearest neighbors. Consequently each ND filter needed to be calibrated at the angle it would eventually be used at. The angles of the ND filters were set by using a series of cage mounts each at a small angle to the other. The mounting of the ND filters is seen in Figure D.1(b). The ND filters were individually mounted into short SM1 tubes (from Thorlabs) and screwed into their designated holders. We confirmed the absence of an etalon-like effect by measuring pairs of nearby ND filters.

The final step was to measure the detection efficiency of the APDs. Without any ND filters in place the light from one output port of the BS was coupled into an singlemode 780-HP fiber. The coupling into this fiber was measured each time and was typically 90–91 %[1]. The ND filters were replaced and the 780-HP fiber was connected to the multimode fiber of the detector to be measured. The NIM output of the APD was converted to TTL and connected to a DT340 counter (from DataTranslation). We again optimized the fiber coupling to compensate for any beam deviation due to the ND filters. The other output port of the BS was used to monitor the power via the calibrated PD.

Knowing the BS's splitting ratio and the power measured by the calibrated photodiode we calculated the power incident on the first ND filter. We knew the attenuation from each ND filter and the fiber coupling loss. We then calculated the number of photons inside the singlemode output fiber and compared this result with the number of photons seen by the APD.

[1] We did not use AR coated fibers. The coupling with AR coated fibers we use is typically 94–95 %.

References

[1] D. Mayers. **Unconditionally Secure Quantum Bit Commitment is Impossible**. *Phys. Rev. Lett.*, **78**:3414–3417, 1997.

[2] Nelly Huei Ying Ng, Siddarth K Joshi, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner. **Experimental implementation of bit commitment in the noisy-storage model**. *Nature communications*, **3**:1326, 2012.

[3] Philippe H. Eberhard. **Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment**. *Phys. Rev. A*, **47**:R747–R750, Feb 1993.

[4] A. E. Lita, B. Calkins, L. A. Pellouchoud, A. J. Miller, and S. Nam. **Superconducting transition-edge sensors optimized for high-efficiency photon-number resolving detectors**. *Proc. SPIE*, **7681**:76810D–76810D–10, 2010.

[5] refractiveindex.info. [link].

[6] V. G. Dmitriev, G. G. Gurzadyan, and D. N. Nikogosyan. *Handbook of Nonlinear Optical Crystals (Springer Series in Optical Sciences, Vol 64)*. Springer-Verlag, 1997.

[7] Hamamatsu Photonics K.K. **Photomultiplier Tubes, Basics and Apllications**. *Commercial white paper*.

[8] Laser Components GmbH. **Single photon counting modules**.

[9] Alfonso David and Rincon Guzman. **Single Photon Detectors**. *Ecole Polytechnique de Montreal*, 2008.

[10] Burm Baek, Adriana E. Lita, Varun Verma, and Sae Woo Nam. **Superconducting a-WxSi1x nanowire single-photon detector with saturated internal quantum efficiency from visible to 1850 nm**. *Applied Physics Letters*, **98**(25):–, 2011.

[11] Migdall, Polyakov, Fan, and Bienfang, editors. *Single-Photon Generation and Detection*. Academic Press, 2013.

[12] Shigehito Miki, Mikio Fujiwara, Masahide Sasaki, Burm Baek, Aaron J. Miller, Robert H. Hadfield, Sae Woo Nam, and Zhen Wang. **Large sensitive-area NbN nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates**. *Applied Physics Letters*, **92**(6):–, 2008.

[13] K S Il'in, A A Verevkin, G N Gol'tsman, and Roman Sobolewski. **Infrared hot-electron NbN superconducting photodetectors for imaging applications**. *Superconductor Science and Technology*, **12**:755, 1999.

[14] Ryan S Bennink. **Optimal collinear Gaussian beams for spontaneous parametric down-conversion**. *Physical Review A*, **81**(5):053805, 2010.

[15] K. D. Irwin. **An application of electrothermal feedback for high resolution cryogenic particle detection**. *Applied Physics Letters*, **66**(15):1998–2000, 1995.

[16] Danna Rosenberg, Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. **Noise-free high-efficiency photon-number-resolving detectors**. *Phys. Rev. A*, **71**:061803, Jun 2005.

[17] A. Lita et al. **13th Annual SquintWorkshop(Southwest Quantum Information and Technology)**. 2011.

[18] Wikipedia.org. **Quantum Entanglement**.

[19] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[20] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. **A scheme for efficient quantum computation with linear optics**. *Nature*, **409**(6816):46–52, 2001.

[21] Charles H Bennett, Gilles Brassard, et al. **Quantum cryptography: Public key distribution and coin tossing**. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, **175**, page 8. New York, 1984.

[22] Artur K. Ekert. **Quantum cryptography based on Bell's theorem**. *Phys. Rev. Lett.*, **67**:661–663, Aug 1991.

[23] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. **Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels**. *Phys. Rev. Lett.*, **70**:1895–1899, Mar 1993.

[24] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. **Advances in quantum metrology**. *Nature Photonics*, **5**(4):222–229, 2011.

[25] Stuart J Freedman and John F Clauser. **Experimental test of local hidden-variable theories**. *Physical Review Letters*, **28**(14):938, 1972.

[26] Stephan Ritter, Christian Nölleke, Carolin Hahn, Andreas Reiserer, Andreas Neuzner, Manuel Uphoff, Martin Mücke, Eden Figueroa, Joerg Bochmann, and Gerhard Rempe. **An elementary quantum network of single atoms in optical cavities**. *Nature*, **484**(7393):195–200, 2012.

[27] QA Turchette, CS Wood, BE King, CJ Myatt, D Leibfried, WM Itano, C Monroe, and DJ Wineland. **Deterministic entanglement of two trapped ions**. *Physical Review Letters*, **81**(17):3631, 1998.

[28] D. N. Matsukevich and A. Kuzmich. **Quantum State Transfer Between Matter and Light**. *Science*, **306**(5696):663–666, 2004.

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

[30] Alain Aspect, Philippe Grangier, and Gérard Roger. **Experimental Tests of Realistic Local Theories via Bell's Theorem**. *Phys. Rev. Lett.*, **47**:460–463, Aug 1981.

[31] Alain Aspect, Philippe Grangier, and Gérard Roger. **Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities**. *Phys. Rev. Lett.*, **49**:91–94, Jul 1982.

[32] Alain Aspect, Jean Dalibard, and Gérard Roger. **Experimental Test of Bell's Inequalities Using Time- Varying Analyzers**. *Phys. Rev. Lett.*, **49**:1804–1807, Dec 1982.

[33] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih. **New High-Intensity Source of Polarization-Entangled Photon Pairs**. *Phys. Rev. Lett.*, **75**:4337–4341, Dec 1995.

[34] Bao-Sen Shi and Akihisa Tomita. **Generation of a pulsed polarization entangled photon pair using a Sagnac interferometer**. *Phys. Rev. A*, **69**:013803, Jan 2004.

[35] J. G. Rarity and P. R. Tapster. **Experimental violation of Bell's inequality based on phase and momentum**. *Phys. Rev. Lett.*, **64**:2495–2498, May 1990.

[36] Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. **Experimental two-photon, three-dimensional entanglement for quantum communication**. *Physical Review Letters*, **89**(24):240401, 2002.

[37] David C. Burnham and Donald L. Weinberg. **Observation of Simultaneity in Parametric Production of Optical Photon Pairs**. *Phys. Rev. Lett.*, **25**:84–87, Jul 1970.

[38] Marco Fiorentino, Gaetan Messin, Christopher E Kuklewicz, Franco NC Wong, and Jeffrey H Shapiro. **Ultrabright tunable photon-pair source with total-flux polarization-entanglement**. In *Digest of Quantum Electronics and Laser Science Conference*, 2003.

[39] Zhe-Yu Jeff Ou. *Multi-photon quantum interference*. Springer, 2007.

[40] J. A. Armstrong, N. Bloembergen, J. Ducuing, and P. S. Pershan. **Interactions between Light Waves in a Nonlinear Dielectric**. *Phys. Rev.*, **127**:1918–1939, Sep 1962.

[41] D. A. Kleinman. **Nonlinear Dielectric Polarization in Optical Media**. *Phys. Rev.*, **126**:1977–1979, Jun 1962.

[42] A. Jiang G. You C. Chen, B. Wu. *Sci. Sin., Ser. B.*, **28**:235, 1985.

[43] J. A. Armstrong, N. Bloembergen, J. Ducuing, and P. S. Pershan. **Interactions between Light Waves in a Nonlinear Dielectric**. *Physical Review*, **127**:1918–1939, September 1962.

[44] P. A. Franken and J. F. Ward. **Optical Harmonics and Nonlinear Phenomena**. *Rev. Mod. Phys.*, **35**:23–39, Jan 1963.

[45] PA Franken and JF Ward. **Optical harmonics and nonlinear phenomena**. *Reviews of Modern Physics*, **35**(1):23, 1963.

[46] M.M. Fejer, G.A. Magel, Dieter H. Jundt, and R.L. Byer. **Quasi-phase-matched second harmonic generation: tuning and tolerances**. *Quantum Electronics, IEEE Journal of*, **28**(11):2631–2654, Nov 1992.

[47] David S Hum and Martin M Fejer. **Quasi-phasematching**. *Comptes Rendus Physique*, **8**(2):180–198, 2007.

[48] F. C. Zumsteg, J. D. Bierlein, and T. E. Gier. **KxRb1-xTiOPO4 A new nonlinear optical material**. *Journal of Applied Physics*, **47**(11):4980–4985, 1976.

[49] John C. Jacco. **KTiOPO4 (KTP) Past, Present, And Future**. *Proc. SPIE*, **0968**:93–99, 1989.

[50] Bell John. **On the Einstein Podolsky Rosen Paradox**. *Physics*, **1**:195–200, 1964.

[51] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin. **Experimental demonstration of quantum correlations over more than 10 km**. *Phys. Rev. A*, **57**:3229–3232, May 1998.

[52] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger. **Violation of Bell's Inequality under Strict Einstein Locality Conditions**. *Phys. Rev. Lett.*, **81**:5039–5043, Dec 1998.

[53] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. **Experimental violation of a Bell's inequality with efficient detection**. *Nature*, **409**(6822):791–794, February 2001.

[54] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. **Detection-Loophole-Free Test of Quantum Nonlocality, and Applications**. *Phys. Rev. Lett.*, **111**:130406, Sep 2013.

[55] Marissa Giustina, Alexandra Mech, Sven Ramelow, Bernhard Wittmann, Johannes Kofler, Jorn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, Rupert Ursin, and Anton Zeilinger. **Bell violation using entangled photons without the fair-sampling assumption**. *Nature*, **497**(7448):227–230, May 2013.

[56] Markus Ansmann, H. Wang, Radoslaw C. Bialczak, Max Hofheinz, Erik Lucero, M. Neeley, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, A. N. Cleland, and John M. Martinis. **Violation of Bell's inequality in Josephson phase qubits**. *Nature*, **461**(7263):504–506, September 2009.

REFERENCES

[57] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. **Proposed Experiment to Test Local Hidden-Variable Theories**. *Phys. Rev. Lett.*, **23**:880–884, Oct 1969.

[58] John F. Clauser and Michael A. Horne. **Experimental consequences of objective local theories**. *Phys. Rev. D*, **10**:526–535, Jul 1974.

[59] Jan-Åke Larsson. **Loopholes in Bell Inequality Tests of Local Realism**. *arXiv preprint arXiv:1407.0363*, 2014.

[60] Philip M Pearle. **Hidden-variable example based upon data rejection**. *Physical Review D*, **2**(8):1418, 1970.

[61] Anupam Garg and N David Mermin. **Detector inefficiencies in the Einstein-Podolsky-Rosen experiment**. *Physical Review D*, **35**(12):3831, 1987.

[62] Stuart J. Freedman and John F. Clauser. **Experimental Test of Local Hidden-Variable Theories**. *Phys. Rev. Lett.*, **28**:938–941, Apr 1972.

[63] Jan-Åke Larsson. **Bells inequality and detector inefficiency**. *Phys. Rev. A*, **57**:3304–3308, May 1998.

[64] Anupam Garg and N. D. Mermin. **Detector inefficiencies in the Einstein-Podolsky-Rosen experiment**. *Phys. Rev. D*, **35**:3831–3835, Jun 1987.

[65] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. **Detection-Loophole-Free Test of Quantum Nonlocality, and Applications**. *Phys. Rev. Lett.*, **111**:130406, Sep 2013.

[66] Marissa Giustina, Alexandra Mech, Sven Ramelow, Bernhard Wittmann, Johannes Kofler, Jorn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, Rupert Ursin, and Anton Zeilinger. **Bell violation using entangled photons without the fair-sampling assumption**. *Nature*, **497**(7448):227–230, May 2013.

[67] Thomas Scheidl, Rupert Ursin, Johannes Kofler, Sven Ramelow, Xiao-Song Ma, Thomas Herbst, Lothar Ratschbacher, Alessandro Fedrizzi, Nathan K Langford, Thomas Jennewein, et al. **Violation of local realism with freedom of choice**. *Proceedings of the National Academy of Sciences*, **107**(46):19708–19713, 2010.

[68] J-Å Larsson and Richard D Gill. **Bell's inequality and the coincidence-time loophole**. *EPL (Europhysics Letters)*, **67**(5):707, 2004.

[69] Jonathan Barrett, Daniel Collins, Lucien Hardy, Adrian Kent, and Sandu Popescu. **Quantum nonlocality, Bell inequalities, and the memory loophole**. *Phys. Rev. A*, **66**:042111, Oct 2002.

[70] Yanbao Zhang, Scott Glancy, and Emanuel Knill. **Efficient quantification of experimental evidence against local realism**. *Phys. Rev. A*, **88**:052119, Nov 2013.

[71] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. **Quantum cryptography with entangled photons**. *Physical Review Letters*, **84**(20):4729, 2000.

[72] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. **A scheme for efficient quantum computation with linear optics**. *nature*, **409**(6816):46–52, 2001.

[73] Alan Migdall. **Correlated-Photon Metrology Without Absolute Standards**. *Physics Today*, **52**(1):41–46, 2008.

[74] Siddarth Joshi, Felix Anger, Antia Lamas-Linares, and Christian Kurtsiefer. **Narrowband PPKTP Source for Polarization Entangled Photons**. In *The European Conference on Lasers and Electro-Optics*, page CD_P24. Optical Society of America, 2011.

[75] Siddarth Koduru Joshi, Chen Ming Chia, Qixiang Leong, Antia Lamas-Linares, Sae Woo Nam, Alessandro Cerè, and Christian Kurtsiefer. **Towards a loophole free Bell test**. In *CLEO: QELS_Fundamental Science*, pages QM1C–2. Optical Society of America, 2013.

[76] David C. Burnham and Donald L. Weinberg. **Observation of Simultaneity in Parametric Production of Optical Photon Pairs**. *Phys. Rev. Lett.*, **25**:84–87, Jul 1970.

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

[78] Ondax Inc. **SureLock 405nm Wavelength Stabilized Doide**.

[79] Zbigniew Ficek and Stuart Swain. *Quantum interference and coherence: theory and experiments*, **100**. Springer, 2005.

[80] G. D. Boyd and D. A. Kleinman. **Parametric Interaction of Focused Gaussian Light Beams**. *Journal of Applied Physics*, **39**(8):3597–3639, 1968.

[81] Nufern Inc. **780-HP**.

[82] Morton H Rubin, David N Klyshko, YH Shih, and AV Sergienko. **Theory of two-photon entanglement in type-II optical parametric down-conversion**. *Physical Review A*, **50**(6):5122, 1994.

[83] B.K.Lubsandorzhiev. **On the history of photomultiplier tube invention**. *Institute for Nuclear Research of RAS*, 2011.

[84] Inc. Thorlabs. **Photomultiplier Modules**.

[85] D. Renker. **Geiger-mode avalanche photodiodes, history, properties and problems**. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, **567**(1):48 – 56, 2006. Proceedings of the 4th International Conference on New Developments in Photodetection {BEAUNE} 2005 Fourth International Conference on New Developments in Photodetection.

[86] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam. **Detecting single infrared photons with 93% system efficiency**. *Nature Photonics*, **7**:210–214, March 2013.

[87] DL Robinson and DA Hays. **Photon detection with cooled avalanche photodiodes: Theory and preliminary experimental results**. *TDA Progress Report 42*, **81**:9–16, 1985.

[88] Robert GW Brown, Kevin D Ridley, and John G Rarity. **Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching**. *Applied Optics*, **25**(22):4122–4126, 1986.

[89] Craig Meeks and PB Siegel. **Dead time correction via the time series**. *American Journal of Physics*, **76**(6):589–590, 2008.

[90] V Bécares and J Blázquez. **Detector Dead Time Determination and Optimal Counting Rate for a Detector Near a Spallation Source or a Subcritical Multiplying System**. *Science and Technology of Nuclear Installations*, **2012**, 2012.

[91] Marcelo Da Cunha Pereira, Francisco E Becerra, Boris L Glebov, Jingyun Fan, Sae Woo Nam, and Alan Migdall. **Demonstrating highly symmetric single-mode, single-photon heralding efficiency in spontaneous parametric downconversion**. *Optics letters*, **38**(10):1609–1611, 2013.

[92] Sergey V Polyakov, Michael Ware, and Alan Migdall. **High-accuracy calibration of photon-counting detectors**. In *Optics East 2006*, pages 63720J–63720J. International Society for Optics and Photonics, 2006.

[93] CC Chen. **Effect of detector dead time on the performance of optical direct-detection communication links**. *Telecommunications and Data Acquisition Progress Report*, **42**:93, 1988.

[94] Michael Ware, Alan Migdall, Joshua C Bienfang, and Sergey V Polyakov. **Calibrating photon-counting detectors to high accuracy: background and deadtime issues**. *Journal of Modern Optics*, **54**(2-3):361–372, 2007.

[95] D. H. Andrews, W. F. Brucksch, W. T. Ziegler, and E. R. Blanchard. **Attenuated Superconductors I. For Measuring Infra-Red Radiation**. *Review of Scientific Instruments*, **13**(7):281–292, 1942.

[96] K.D. Irwin and G.C. Hilton. **Transition-Edge Sensors**. In Christian Enss, editor, *Cryogenic Particle Detection*, **99** of *Topics in Applied Physics*, pages 63–150. Springer Berlin Heidelberg, 2005.

[97] John Clarke and Alex I Braginski. *The SQUID handbook*. Wiley Online Library, 2006.

[98] W. Seidel, G. Forster, W. Christen, F. von Feilitzsch, H. Gobel, F. Probst, and R.L. Mossbauer. **Phase transition thermometers with high temperature resolution for calorimetric particle detectors employing dielectric absorbers**. *Physics Letters B*, **236**(4):483 – 487, 1990.

[99] KD Irwin, SW Nam, B Cabrera, B Chugg, GS Park, RP Welty, and JM Martinis. **A self-biasing cryogenic particle detector utilizing electrothermal feedback and a SQUID readout**. *Applied Superconductivity, IEEE Transactions on*, **5**(2):2690–2693, 1995.

[100] Adrian T Lee, Paul L Richards, Sae Woo Nam, Blas Cabrera, and KD Irwin. **A superconducting bolometer with strong electrothermal feedback**. *Applied Physics Letters*, **69**(12):1801–1803, 1996.

[101] KD Irwin, GC Hilton, DA Wollman, and John M Martinis. **X-ray detection using a superconducting transition-edge sensor microcalorimeter with electrothermal feedback**. *Applied physics letters*, **69**(13):1945–1947, 1996.

[102] M. F. Cunningham, J. N. Ullom, T. Miyazaki, S. E. Labov, John Clarke, T. M. Lanting, Adrian T. Lee, P. L. Richards, Jongsoo Yoon, and H. Spieler. **High-resolution operation of frequency-multiplexed transition-edge photon sensors**. *Applied Physics Letters*, **81**(1):159–161, 2002.

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

[104] Aaron Joseph Miller. *Development of a broadband optical spectrophotometer using superconducting transition-edge sensors*. PhD thesis, Stanford University, 2001.

[105] M.E. Huber, A.M. Corey, K.L. Lumpkins, F.N. Nafe, J.O. Rantschler, G.C. Hilton, J.M. Martinis, and A.H. Steinbach. **DC SQUID series arrays with intracoil damping to reduce resonance distortions**. *Applied Superconductivity*, **5**(7):425–429, 1998-07-12T00:00:00.

[106] R. C. Jaklevic, John Lambe, A. H. Silver, and J. E. Mercereau. **Quantum Interference Effects in Josephson Tunneling**. *Phys. Rev. Lett.*, **12**:159–160, Feb 1964.

[107] Bascom S. Deaver and William M. Fairbank. **Experimental Evidence for Quantized Flux in Superconducting Cylinders**. *Phys. Rev. Lett.*, **7**:43–46, Jul 1961.

[108] R. Doll and M. Näbauer. **Experimental Proof of Magnetic Flux Quantization in a Superconducting Ring**. *Phys. Rev. Lett.*, **7**:51–52, Jul 1961.

[109] W. Meissner and R. Ochsenfeld. **Ein neuer Effekt bei Eintritt der Supraleitfhigkeit**. *Naturwissenschaften*, **21**(44):787–788, 1933.

[110] W. F. Giauque and D. P. MacDougall. **Attainment of Temperatures Below 1degree Absolute by Demagnetization of $Gd_2(SO_4)_3 8H_2O$**. *Phys. Rev.*, **43**:768–768, May 1933.

[111] Frank Pobell. *Matter and methods at low temperatures*, **2**. Springer, 2007.

[112] Wolfgang Becker. *Advanced time-correlated single photon counting techniques*, **81**. Springer, 2005.

[113] Corning Inc. **SMF-28e**.

[114] B. Cabrera, R. M. Clarke, P. Colling, A. J. Miller, S. Nam, and R. W. Romani. **Detection of single infrared, optical, and ultraviolet photons using superconducting transition edge sensors**. *Applied Physics Letters*, **73**(6):735–737, 1998.

[115] AE Lita, AJ Miller, and S Nam. **Energy collection efficiency of tungsten transition-edge sensors in the near-infrared**. *Journal of Low Temperature Physics*, **151**(1-2):125–130, 2008.

[116] Antia Lamas-Linares, Brice Calkins, Nathan A. Tomlin, Thomas Gerrits, Adriana E. Lita, Jorn Beyer, Richard P. Mirin, and Sae Woo Nam. **Nanosecond-scale timing jitter for single photon detection in transition edge sensors**. *Applied Physics Letters*, **102**(23):–, 2013.

[117] Alexander Ling, Matthew P. Peloso, Ivan Marcikic, Valerio Scarani, Antia Lamas-Linares, and Christian Kurtsiefer. **Experimental quantum key distribution based on a Bell test**. *Phys. Rev. A*, **78**:020301, 2008.

[118] J. Kilian. **Founding cryptography on oblivious transfer**. In *Proceedings of 20th ACM STOC*, pages 20–31, 1988.

[119] Ernest F Brickell, David Chaum, Ivan B Damgård, and Jeroen van de Graaf. **Gradual and verifiable release of a secret**. In *Advances in CryptologyCRYPTO87*, pages 156–166. Springer, 1988.

[120] Moni Naor. **Bit commitment using pseudorandomness**. *Journal of cryptology*, **4**(2):151–158, 1991.

[121] Ari Juels and Martin Wattenberg. **A fuzzy commitment scheme**. In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 28–36. ACM, 1999.

[122] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. **A practical secret voting scheme for large scale elections**. In *Advances in CryptologyAUSCRYPT'92*, pages 244–251. Springer, 1993.

[123] H.F. Chau and H-K. Lo. **Making an Empty Promise with a Quantum Computer**. *Fortschritte der Physik*, **46**:507–520, 1998.

[124] H-K. Lo. **Insecurity of Quantum Secure Computations**. *Phys. Rev. A*, **56**:1154, 1997.

[125] H-K. Lo and H. F. Chau. **Is quantum bit commitment really possible?** *Phys. Rev. Lett.*, **78**:3410, 1997.

[126] G. D'Ariano, D. Kretschmann, D. Schlingemann, and R.F. Werner. **Quantum Bit Commitment Revisited: the Possible and the Impossible**. arXiv:quant-ph/0605224v2, 2007.

[127] U. Maurer. **Conditionally-Perfect Secrecy and a Provably-Secure Randomized Cipher**. *Journal of Cryptology*, **5**:53–66, 1992.

[128] C. Cachin and U. M. Maurer. **Unconditional Security Against Memory-Bounded Adversaries**. In *Proceedings of CRYPTO 1997*, pages 292–306, 1997.

[129] S. Dziembowski and U. Maurer. **On Generating the Initial Key in the Bounded-Storage Model**. In *Proceedings of EUROCRYPT*, pages 126–137, 2004.

[130] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. **A Tight High-Order Entropic Quantum Uncertainty Relation With Applications**. *Proceedings of CRYPTO*, pages 360–378, 2007.

[131] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. **Cryptography in the Bounded-Quantum-Storage Model**. *Procedings of FOCS*, pages 449–458, 2005.

[132] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. **Secure Identification and QKD in the Bounded-Quantum-Storage Model**. *Proceedings of CRYPTO*, pages 342–359, 2007.

[133] C. Gonzales-Guillen N. J. Bouman, S. Fehr and C. Schaffner. *Theory of Quantum Computation, Communication, and Cryptography Lecture Notes in Computer Science*, chapter An All-But-One Entropic Uncertainty Relations, and Application to Password-based Identification, pages 29–44. Springer, 2011. arXiv:1105.6212v1.

[134] S. Wehner, C. Schaffner, and B. Terhal. **Cryptography from Noisy Storage**. *Physical Review Letters*, **100**:220502, 2008. arXiv:0711.2895v3.

[135] C. Schaffner, B. Terhal, and S. Wehner. **Robust Cryptography in the Noisy-Quantum-Storage Model**. *Quantum Information & Computation*, **9**:11, 2008. arXiv:0807.1333v3.

[136] R. König, S. Wehner, and J. Wullschleger. **Unconditional security from noisy quantum storage**. *IEEE Transactions on Information Theory - To appear*, 2009. arXiv:0906.1030v3.

[137] Alexander I. Lvovsky, Barry C. Sanders, and Wolfgang Tittel. **Optical quantum memory**. *Nature Photonics*, **3**:706–714, 2009.

[138] I. Usmani, M. Afzelius, H. de Riedmatten, and N. Gisin. **Mapping multiple photonic qubits into and out of one solid-state atomic ensemble**. *Nature Communications*, **1**:12 (7 pp.), 2010.

[139] M. Bonarota, J-L Le Gouet, and T. Chaneliere. **Highly multimode storage in a crystal**. *New Journal of Physics*, **13**:013013, 2011.

[140] Han-Ning Dai, Han Zhang, Sheng-Jun Yang, Tian-Ming Zhao, Jun Rui, You-Jin Deng, Li Li, Nai-Le Liu, Shuai Chen, Xiao-Hui Bao, Xian-Min Jin, Bo Zhao, and Jian-Wei Pan. **Holographic Storage of Biphoton Entanglement**. *Phys. Rev. Lett.*, **108**:210501, May 2012.

[141] M. Berta, F. Brandao, M. Christandl, and S. Wehner. **Entanglement cost of quantum channels**. arXiv:1108.5357, 2011.

[142] M. Berta, O. Fawzi, and S. Wehner. **Quantum to classical randomness extractors**. arXiv:1111.2026 - To appear in CRYPTO '12, 2012.

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

[144] Alexander Barg and GD Forney. **Random codes: Minimum distances and error exponents**. *Information Theory, IEEE Transactions on*, **48**(9):2568–2573, 2002.

[145] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo. **Implementation of two-party protocols in the noisy-storage model**. *Physical Review A*, **81**:052336, 2010. arXiv:0911.2302v2.

[146] C. Kurtsiefer, P. Zarda, M. Halder, P. M. Gorman, P. R. Tapster, J. G. Rarity, and H. Weinfurter. **Long distance free space quantum cryptography**. *Proc. SPIE*, **4917**:25–31, 2002.

[147] Ivan Marcikic, Antia Lamas-Linares, and Christian Kurtsiefer. **Free-space quantum key distribution with entangled photons**. *Appl. Phys. Lett.*, **89**:101122, 2006.

[148] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih. **New High-Intensity Source of Polarization–Entangled Photon Pairs**. *Phys. Rev. Lett.*, **75**:4337, 1995.

[149] C. Kurtsiefer. **QCrypto: an open source code for experimental quantum cryptography**. http://code.google.com/p/qcrypto/, 2008.

[150] Vadim Makarov and Dag R. Hjelme. **Faked states attack on quantum cryptosystems**. *J. Mod. Opt.*, **52**:691, 2005.

[151] I. Gerhardt, Q.Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer. **Experimentally faking the violation of Bell's inequalities**. *Phys. Rev. Letters*, **107**:170404, 2011.

[152] Howard Wiseman. **Physics: Bells theorem still reverberates**. *Nature*, 2014.

[153] Sven Ramelow, Alexandra Mech, Marissa Giustina, Simon Gröblacher, Witlef Wieczorek, Jörn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, Anton Zeilinger, and Rupert Ursin. **Highly efficient heralding of entangled single photons**. *Opt. Express*, **21**(6):6707–6717, Mar 2013.

[154] Yang Liu, Yuan Cao, Marcos Curty, Sheng-Kai Liao, Jian Wang, Ke Cui, Yu-Huai Li, Ze-Hong Lin, Qi-Chao Sun, Dong-Dong Li, et al. **Experimental unconditionally secure bit commitment**. *Physical Review Letters*, **112**(1):010504, 2014.

[155] Jean-Daniel Bancal, Lana Sheridan, and Valerio Scarani. **More Randomness from the Same Data**. *arXiv preprint arXiv:1309.3894*, 2013.

[156] F. Pockels. *Abhandl., Gesell., Wiss., Gottingen,*, **39**(1), 1893.

[157] Robert Goldstein. **Pockels Cell Primer**. *Commercial white paper.*

[158] C. C. Davis. *Lasers and Electro-Optics Fundamentals and Engineering.* Cambridge University Press, 1996.

[159] A. Melikyan, L. Alloatti, A. Muslija, D. Hillerkuss, P. C., Schindler, L. J. Li, R. Palmer, D. Korn, S. Muehlbrandt, Van Thourhout, D., S. B. Chen, R. Dinu, M. Sommer, C. Koos, M. Kohl, W. Freude, and J. Leuthold. **High-speed plasmonic phase modulators**. *Nat Photon*, **8**(3):229–233, March 2014.

[160] EOSpace Inc. **Our Exceptionally-Low-Loss Products**.

[161] María L Calvo and Vasudevan Lakshminarayanan. *Optical waveguides: from theory to applied technologies.* CRC Press, 2010.

[162] E. G. Sauter. *Nonlinear Optics.* John Wiley & Sons, Inc,, 1996.

[163] Max Born and Emil Wolf. *Principles of Optics.* Pergamon Press, 1970.

[164] X. D. Wang, J. Sweetser, I. A. Walmsley, P. Basséras, and R. J. Dwayne Miller. **Regenerative pulse amplification in the 10-kHz range**. *Opt. Lett.*, **15**(15):839–841, Aug 1990.

[165] Dennis R Pape, Akis P Goutzoulis, and Sergeĭ Kulakov. *Design and fabrication of acousto-optic devices.*

[166] Kuniharu Takizawa. **Electro-Optical Devices**. *Wiley Encyclopedia of Electrical and Electronics Engineering.*

[167] Wikipedia.org. **Lithium Tantalate Properties**.

[168] A*STAR. **National Metrology Center**.